CIIP Governance in the European Union Member States (Annex)

JANUARY 2016

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Project Team

Sarri Anna, Secure Infrastructure & Services Unit, ENISA

Moulinos Konstantinos, Secure Infrastructure & Services Unit, ENISA

Contact

For contacting the authors please use resilience@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements

The analysis in this document was produced in collaboration with Pillokeit Pascal Dustin and Weissmann Paul from KPMG Germany. Special thanks to the MS experts that provided input for this report and especially the NCSS Working Group.

ISBN 978-92-9204-144-1, doi: 10.2824/028519

Table of Contents

Introduction

This analysis is part of a bigger study regarding Stocktaking, Analysis and Recommendation on the Protection of critical information infrastructure (CII), and uncovers the different governance structures for critical information infrastructure protection (CIIP) in 15 EU Member States and 1 EFTA country.

The analysis focuses on CIIP Governance and specifically on the following topics:

- Leading Authorities
- Management Structures
- Roles & Responsibilities
- Relevant Framework (papers and regulations)
- Obligations and requirements for operators of CII (Are operators obligated to implement security measures, e.g. Business Continuity Management?)

The collection of information was based on the following methods:

- Desktop research: Included the analysis of various documents, such as national cyber security strategies, white papers, policy papers, laws, acts and regulations, official internet websites and secondary sources.
- Online surveys: ENISA developed an online survey which has been answered by representatives of thirteen EU Member States.
- Interviews: ENISA has conducted focus interviews or received written answers from representatives of the national authorities for CIIP of fifteen EU Member States and one EFTA country.

The purpose of this analysis is to better understand the CIIP governance structure in the EU Member States and to analyse the different profiles based on the approaches and commonalities followed by different countries.

List of Abbreviations

ABBREVATION	DESCRIPTION
ACSS	Austria Cyber Security Strategy
Act on Cyber Security	Act no. 181/2014 Coll., on Cyber Security and Change of Related Acts
ANSSI	Agence nationale de la sécurité des systèmes d'information (France)
APCIP	Austrian Program for Critical Infrastructure Protection
BBK	Federal Office of Civil Protection and Disaster Assistance (Germany)
BfV	Federal Office for the Protection of the Constitution (Germany)
BKA	Federal Criminal Police Office (Germany)
BKK	Federal Office of Civil Protection and Disaster Assistance (Germany)
BMI	Federal Ministry of the Interior (Germany)
BND	Federal Intelligence Service (Germany)
BNetzA	Federal Network Agency (Germany)
BPoL	Federal Police (Germany)
BSI	Federal Office for Information Security (Germany)
C4	Cyber Crime Competence Center (Austria)
CERT	Computer Emergency Response Team
CERT.LV	Information Technology Security Incident Response Institution of the Republic of Latvia
CFCS	Centre for Cyber Security (Denmark)
CII	Critical Information Infrastructures
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
CIP Strategy	National Strategy for Critical Infrastructure Protection (Germany)
CNAIPIC	Anti-Crime Computer Centre for Critical Infrastructure Protection (Italy)
CoPS	Political Strategic Committee (Italy)
Crisis Act	Act no. 240/2000 Coll., on Crisis Management (Czech Republic)
CSIRT	Computer Security Incident Response Team
CSP	Cyber Security Platform (Austria)
CSS	Cyber Security Strategy of Latvia for 2014 – 2018
CSSG	Cyber Security Steering Group (Austria)
DEC	Department of Electronic Communications (Cyprus)
DIGST	National Digitalisation Board (Denmark)
DKCERT	Danish Computer Security Incident Response Team (Denmark)
ECI	European Critical Infrastructure

EFTA	European Free Trade Association
ENISA	European Network and Information Security Agency
EU	European Union
FDF	Federal Department of Finance (Switzerland)
FICORA	Finnish Communications Regulatory Authority
FINMA	Finanzmarktaufsicht (Switzerland)
FIS	Federal Intelligence Service (Switzerland)
FITSU	Federal IT Steering Unit (Switzerland)
FRA	Swedish National Defence Radio Establishment
GCS	Government Centre for Security (Poland)
GCSS	German Cyber Security Strategy
GovCERT	Governmental CERT
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISP	Internet Service Provider
LPM	Military Programming Law (France)
MCW	Ministry of Communications and Works (Cyprus)
MELANI	Reporting and Analysis Centre for Information Assurance (Switzerland)
MS	Member States (EU)
MSB	Swedish Civil Contingencies Agency (Sweden)
NASK	The Research and Academic Computer Network (Poland)
NC3	National Cyber Crime Center (Denmark)
NCIPP	The National Critical Infrastructure Protection Programme (Poland)
NCS	National Strategy for the Protection of Switzerland against Cyber Risks
NCSC	National Cyber Security Centre (Netherlands)
NCSC-FI	National Cyber Security Centre Finland
NCSS	National Cyber Security Strategy
NCTV	National Coordinator for Security and Counterterrorism (Netherlands)
NDN	National Detection Network (Netherlands)
NEIH	National Electronic Information Security Authority (Hungary)
NESA	National Emergency Supply Agency (Finland)
NISP	Nucleus Inter Ministerial Unit for Situation and Planning (Italy)
NPSI	National Plan for Information Infrastructure Protection (Germany)
NRN	National Response Network (Netherlands)

NSA	National Security Authority (Czech Republic)
NTSG	National Telecommunications Coordination Group (Sweden)
OCECPR	Office of the Commissioner of Electronic Communications & Postal Regulation (Cyprus)
OEP	Office of Emergency Planning (Ireland)
OFCOM	Federal Office of Communication (Switzerland)
OIC	Operation Information Centre (Switzerland)
OIV	Operators of vital importance (France)
PET	National Intelligence Service (Denmark)
PPPs	public-private partnerships
PTS	Swedish Post and Telecom Agency
RCB	Government Centre for Security (Poland)
RIA	Estonian Information System Authority
RKP	Investigation Service (Sweden)
SAMFI	Cooperation Group for Information Security (Sweden)
Säpo	Swedish Security Service
SBN	Data Security Breach Notification (Netherlands)
SCE	Swiss Cyber Experts
SEG	Information Technology and Information Systems Security Experts Group (Latvia)
SGDSN	General Secretariat for Defence and National Security (France)
SKI	The Federal Council's Strategy for Critical Infrastructure Protection 2012 (Switzerland)
SMEs	small and medium enterprises
SOPs	Standard Operating Procedures (Czech Republic)
SPOCs	Single Point of Contacts
UP KRITIS	KRITIS implementation plan (Germany)
VSF	Vital Societal Functions (Sweden)
ZKA	Customs Criminological Office (Germany)

1. CIIP Governance in the EU Member States

The following chapter describes the governance of CIIP in fifteen EU Member States and one EFTA country. References for country-specific sources are given at the end of every profile. A number of general sources have been used for several Member States (ENISA 2014; ENISA 2015; Kaska, Trinberg 2015).

1.1 Austria

Leading Authority

Because of a decentralised approach, there is no single authority responsible for CIIP in Austria. The main coordinative body is the **Cyber Security Steering Group (CSSG)**.

TYPE	ACTOR OR INSTITUTION
Leading (coordinative)	• Cyber Security Steering Group (CSSG)
Ministerial	• Federal Chancellery of Austria • Federal Ministry of the Interior • Beirat APCIP
Operational	• GovCERT • CERT.at • MilCERT • Cyber Crime Competence Center (C4) • Austrian Energy CERT
Private/PPPs	• Cyber Security Platform (CSP)

Management Structure

There are several relevant agencies in Austria that are part of an “operative coordination structure”. The governance model for CIIP follows a cooperative and decentralised approach.

In general the Federal Chancellery of Austria and the Federal Ministry of the Interior share responsibility for CIP on a strategic-political level. On an operational level the coordination structure is divided between an “Inner circle” and an “Outer circle”. The Inner Circle includes several public agencies, the most significant of which are the Cyber Security Center, the Cyber Defense Center, GovCERT, MilCERT and the Cyber Crime Competence Center (C4). The Outer circle includes private organisations such as the several sector-specific CSIRTs and the national CSIRT (CERT.at).

The operative coordination structure introduced a concept of 'sector CERTs', which are CSIRTs charged with supporting a defined sector based on their sector-specific expertise. At the moment there are only two such sector CSIRTs: GovCERT as the sector CSIRT of the public administration and an energy CSIRT for the Austrian energy sector.

Steering and coordinating the different agencies is the responsibility of the Cyber Security Steering Group (CSSG). Cooperation between the public and private sector is fostered by Cyber Security Platform (CSP).

Roles and Responsibilities

Cyber Security Steering Group (CSSG)

The CSSG is tasked with the coordination of the different public agencies and the processes within the operative coordination structures. It serves as an advisory body to the Federal Government on Cyber Security matters and coordinates the implementation of the Austria Cyber Security Strategy. In case of an actual Cyber Crisis, coordination of operative measures falls to the Cyber Security Centre (situated in the Federal Ministry of the Interior) or, in case of a military threat to the Austrian sovereignty, to the Cyber Defense Centre (situated in the Federal Ministry of Defense and Sports).

Cyber Security Platform (CSP)

The CSP was established in March 2015 as a public-private partnership (PPP). It is comprised of representatives from private and public operators of CII as well as relevant public agencies. The aim is to facilitate communication between them by serving as an information sharing hub. It also serves as an umbrella platform for the different private sector initiatives.

Beirat APCIP

An inter-ministerial advisory board (Beirat APCIP) has been established in order to support the relevant ministries or other stakeholders on CIIP. It is comprised of representatives of several ministries, such as the Ministry of National Defence and Sport, the Ministry of Science, Research and Economy, the Ministry for Transport, Innovation and Technology, the Ministry of Finance, the Ministry for Agriculture, Forestry, Environment and Water Management and the Federal Ministry of Health. The advisory board supports BKA (the Federal Chancellery) and BM.I (the Ministry of the Interior) in the development and implementation of APCIP and coordinates their actions with other fields such as disaster control and cyber security. BKA and BM.I regularly report to the advisory board on the progress of the implementation of APCIP.

GovCERT

GovCERT Austria is the Austrian Government Computer Emergency Response Team. It was founded in 2008 and its responsibilities are to collect and assess incidents and coordinate countermeasures for the public administration and operators of CII.

CERT.at

CERT.at is the national CSIRT of Austria and is tasked with the coordination of incident response. CERT.at is a private initiative of nic.at, the Austrian domain registry, and is partially funded by the Federal Chancellery.

Relevant Framework Papers and Regulations

The topic of CIIP is handled in several strategy and policy papers:

The main paper for CIIP is the Masterplan of the **Austrian Program for Critical Infrastructure Protection (APCIP)**. The Masterplan was first published in 2008 and renewed in 2014.

CIP is also embedded in the broader context of Cyber Security and covered partially in the **National ICT Security Strategy (2012)** and the **Austria Cyber Security Strategy (ACSS)** (2013) strategy papers.

At the moment, Austria lacks the legal foundation for the responsibilities of its authorities in the area of CIIP. With the exception of the telecommunications sector, there is also an absence of legal obligations for

operators of CII. It is planned to develop a Federal Cyber Security Law after the European NIS Directive has been passed.

Sources

(Computer Emergency Response Team Austria 2015)

(ENISA 2015)

(ENISA, KPMG 2015)

(Federal Chancellery of the Republic of Austria 2012)

(Federal Chancellery of the Republic of Austria 2013)

(Federal Chancellery of the Republic of Austria 2014)

(Federal Chancellery of the Republic of Austria, Ministry of Finance 2015)

(GovCERT Austria 2014)

1.2 Cyprus

Leading Authority

The **Office of the Commissioner of Electronic Communications & Postal Regulation (OCECPR)** acts as the main coordinating body for CIIP in Cyprus.

TYPE	ACTOR OR INSTITUTION
Leading	• Office of the Commissioner of Electronic Communications & Postal Regulation (OCECPR)
Ministerial	• Department of Electronic Communications (DEC), which is part of the Ministry of Communications and Works (MCW)
Operational	• Several law enforcement and intelligence agencies • Cyprus Fire Service • Civil Defence Forces • Governmental CSIRT & National CSIRT
Network/Forum/Council	• CYBER Conference (energy sector)

Management Structure

Roles and responsibilities in the field of CIIP are spread across a variety of different actors in Cyprus. Each agency and authority holds responsibility in its own sector. Cyprus recognises that effective security can only be accomplished through cooperation between public agencies within a coordinative framework.

Close cooperation between public agencies is one of the strategies outlined in the Cyber Security Strategy. For the purpose of CIP and CIIP a steering committee has been established, which works together with the relevant ministries. Cyber fraud and crime is the responsibility of the police, which will look to cooperate with other public agencies if necessary.

Public-Private Partnerships do not exist, but working groups and forums, such as the CYBER Conference for the energy sector are in place. In addition, exchanges and cooperation sometimes occur as part of national awareness programs and initiatives.

Roles and Responsibilities

Office of the Commissioner of Electronic Communications & Postal Regulation (OCECPR)

The Office of the Commissioner of Electronic Communications & Postal Regulation (OCECPR) has been established as the principal regulator of electronic communications and is headed by the Commissioner of the Electronic Communications and Post, who is appointed by the Council of Ministers. The OCECPR is responsible for ensuring and encouraging the adequate access, interconnectivity and interoperability of services. The Office can impose obligations on telecommunications operators in order to ensure accessibility and connectivity for end-users. These obligations may prescribe technical or operational conditions relevant to international standards (such as ITU, ISO or IEC). According to the "Subsidiary Administrative Act Number 371/2012" CII operators in the electronic communications sector need to inform OCECPR of security incidents that have an impact on the availability or the personal data.

In addition it has been tasked to act as the coordinating body for the development and implementation of the different actions laid out in the Cyber Security Strategy.

Governmental CSIRT & National CSIRT

A governmental CSIRT has been established in early 2015. However, the specific tasks and services of the governmental CSIRT are still in development. It is expected to be functional in 2015 and will most likely be under the authority of the OCECPR.

A national CSIRT, as described in the National Cyber Security Strategy, is in development. Its set-up and organisational structure is currently under evaluation.

Relevant Framework Papers and Regulations

The **Cybersecurity Strategy of the Republic of Cyprus** has been published in April 2012 and contains several "strategic responses" around the issue of CIIP.

Additional framework papers have only been developed for some critical sectors, for example the electronic communications or finance sector.

Subsidiary Administrative Act Number 371/2012 obligates CII operators in the electronic communications sector to inform OCECPR of security incidents that affect availability or personal data.

Currently, a programme is underway to review legislation and frameworks for CIP and CIIP sectors. It is expected to be finished at end of 2016.

Sources

(ENISA, KPMG 2015)

(Office of the Commissioner of Electronic Communications & Postal Regulation (OCECPR) 2012)

1.3 Czech Republic

Leading Authority

The overarching authority is the **National Security Authority (NSA)**, which is responsible for cyber security as well as the protection of classified information, security clearances and cryptographic authority. CII is handled by the National Cyber Security Center that is an integral part of the NSA. The NSA is directly under the Prime Minister.

TYPE	ACTOR OR INSTITUTION
Leading	• National Security Authority (NSA)
Operational	• GovCERT (part of the NSA) • CSIRT.cz
Private/PPPs	• CZ.NIC Association

Management Structure

During a national cyber crisis (State of Cyber emergency), or in case of cyber security incidents, the National Security Agency (NSA) acts as the main authority and coordinative body for relevant bodies and agencies (including the different public and private CSIRTs). Relevant entities can be bound by the decisions of the NSA during a State of cyber emergency or when dealing with the threat of a cyber security incident. The NSA supports and advises operators of CII in emergency response and provides forensic analysis if requested.

The NSA and the interest association CZ.NIC have established the national CSIRT CSIRT.cz based on a memorandum in 2012. Further collaboration with the private sector in form of public-private partnerships are currently under development. On an international level, working groups with Microsoft and Cisco on the issue of botnets have been established.

Roles and Responsibilities

National Security Authority

The NSA is authorised to issue decisions on reactive measures which binds the relevant public and private bodies (including CII) to carry out measures which need to be adopted to solve or prevent cyber security incident. The NSA can also issue corrective actions towards the relevant bodies under its supervision in case of imminent danger to the information or communication system caused by a cyber security incident (§ 24 of the Act on Cyber Security). As part of its supervisory role, the NSA performs security audits and controls the fulfilment of obligations set out in the Act on Cyber Security. For this purpose, it can demand compliance tests. In case of a cyber security incident, operators are also obligated to inform the NSA and to submit log records on request.

The NSA also operates the governmental CSIRT (GovCERT). It receives cyber security reports, evaluates events and can provide support and vulnerability analysis. The protection of CII has been assigned to GovCERT.

Furthermore, the authority acts as the main information hub. The NSA conducts seminars for operators of CII and advises them on legal obligations, the role of the NSA and the responsibilities of operators. In

addition, an E-learning platform is currently under development. The long-term goal is to build an information platform, which should also include sectoral information for operators.

Ministry of Interior

The Ministry is a central state administrative body for the area of public administration information systems and a coordinator for information and communication technologies.

The NSA communicates with the Ministry of Interior during the identification of CII. The Ministry of Interior partners with academia to conduct Cyber Security Research.

CZ.NIC Association

The CZ.NIC Association is an interest association of legal entities associating significant legal entities operating in the Czech Republic in the area of domain names and on the electronic communications market which operates the top-level domestic domain.cz (ccTLD.cz) and is engaged in the area of internet security and computer security. It operates the national CSIRT CSIRT.cz.

CSIRT.cz (National CSIRT)

The national CSIRT is CSIRT.cz, which was established in 2010 by a memorandum concluded between the Ministry of Interior and the interest association CZ.NIC. The memorandum has been superseded in 2012 by a new memorandum arranged with the NSA. It coordinates security incident response across computer networks of the Czech Republic. It also collects and evaluates data on reported incidents. CSIRT.cz takes the role of a national Point of Contact in the field of information technology. The national CSIRT is mainly (but not exclusively) designated for private bodies.

Relevant Framework Papers and Regulations

The main strategy paper is the **National Cyber Security Strategy of the Czech Republic** for years 2015 – 2020 (NCSS), which was adopted in February 2015.

This document is followed by the **Action plan to NCSS** for years 2015 – 2020, which defines the concrete tasks, steps, deadlines, responsibilities and the supervision of the implementation. The Action Plan also defines several tasks for the implementation of the Act on Cyber Security.

The legal framework for CIIP is set out by **Act no. 181/2014 Coll., on Cyber Security and Change of Related Acts (Act on Cyber Security)**, which came into force in January 2015. It defines roles and responsibilities in cyber security for private bodies and public agencies.

The **Act no. 240/2000 Coll., on Crisis Management (Crisis Act)** provides the basic framework for the identification of CII and operations during a crisis.

Regulation No 316/2014 Coll. implements the Act on Cyber Security and aims to define minimal requirements for the implementation and the execution of the Information Security Management System (ISMS) for administrators of CII. It is based on the standards ISO/IEC series 27k.

The Act on Cyber Security is accompanied by the **Action Plan for the National Cyber Security Strategy**. **Standard Operating Procedures (SOPs)** on a technical level are currently under development.

Sources

(ENISA 2015)

(ENISA, KPMG 2015)

(National Security Authority 2015a)

(National Security Authority 2015b)

(Parliament of the Czech Republic 2014)

(Parliament of the Czech Republic 2015)

1.4 Denmark

Leading Authority

The National Cyber and Information Security Strategy (NCSS) The NCSS designates the **Centre for Cyber Security (CFCS)** and its subordinate GovCERT as the main authority for the security of IT Systems and infrastructure.

TYPE	ACTOR OR INSTITUTION
Leading	• Centre for Cyber Security (CFCS)
Ministerial	• Ministry of Defence
Operational	• GovCERT (part of the CFCS) • National Intelligence Service (PET) • National Digitalisation Board (DIGST) • National Cyber Crime Center (NC3) (part of Danish Police)^ • Danish Computer Security Incident Response Team (DKCERT)
Private/PPPs	• Contact forums

Management Structure

Denmark follows the principle of sector-responsible, which means that every authority is responsible for its own respective sector.

Contact forums between public and private sectors have been established. High-level representatives of the major companies and high ranking officials of Ministries are invited to share classified information within the forums, which are headed by the Centre for Cyber Security (CFCS). The goal is to foster information sharing about security incidents between companies and between authorities. The forums meet 3-4 times per year. Furthermore, a Business Advisory Board has been established.

Roles and Responsibilities

Centre for Cyber Security (CFCS)

The Centre for Cyber Security (CFCS) and its subordinate GovCERT is an independent authority under the Ministry of Defence. It is responsible for three main tasks: 1. Contribute to protecting against cyber threats, 2. Assist in securing a solid and robust ICT critical infrastructure and 3. Warn of, protect against and counter cyber attacks. For this purpose it is responsible for incident response, advisory and acting as the main point of contact for CII-related incidents.

The CFCS has direct responsibility for the telecommunications sector. It can enforce the documentation of security policies, but there are no obligations with regard to the content and the quality of the documentation. Furthermore, telecommunication companies are obligated to report incidents and to prepare emergency and exercise plans. In addition, the military sector and government institutions must report major incident to CFCS. It has no authority over companies of other sectors.

The CFCS is also hosting the Danish GovCERT and MilCERT. The Danish GovCERT was established in 2009 and is tasked with the protection of Danish critical internet infrastructure. Its constituency are governmental institutions and private companies. GovCERT obtains an overview of risks in relation to Internet use and supports a coordinated response to threats in case of an emergency through the communication with the proper authorities. GovCERT also offers incident handling and will issue alerts in case of security risks. There is a specific legal mandate for the Centre for Cyber Security including GovCERT. MilCERT is the Danish military CSIRT, responsible for military networks.

National Intelligence Service (PET)

The PET is the national security intelligence agency of Denmark, which focuses solely upon domestic security. It offers advice to the Danish government, public authorities and Danish companies on matters such as counter terrorism and counter espionage. It is also responsible for "identifying, preventing and countering threats to freedom, democracy and safety in Danish society."

National Digitalisation Board (DIGST)

The Agency for Digitisation is an agency of the Ministry of Finance and was established in 2011. The DIGST understands information security as one of the prerequisites of the further digitisation in Denmark and wants to broaden awareness of the ICT security challenges for citizens and businesses.

National Cyber Crime Center (NC3)

The Danish police have set up the National Cyber Crime Center (NC3) whose mission is to prevent and investigate IT crime conducted online.

Danish Computer Security Incident Response Team (DKCERT)

DKCERT is under the authority of UNIC – the Danish IT Centre for Education and Research, a national organization under the Danish Ministry of Education. The Team was established in 1991 and its constituency is the Danish Network for Research and Education. DKCERT can be contacted in case of an incident and will offer advice and propose solutions. It also coordinates information between different parties involved in case of an emergency. On its website, the CSIRT regularly publishes information about security vulnerabilities as well as precautionary measures. CKCERT has no authority to issue binding instructions.

Relevant Framework Papers and Regulations

In December 2014 the Danish government presented a **National Cyber and Information Security Strategy (NCSS)** which was launched in 2015. The Danish government intends to update the plan in 2016.

The **Danish Defence Agreement 2013-2017** briefly describes the role of the CFCS with respect to protection of ICTs against cyber-attacks.

The Act 192 on the Danish Cyber Security Centre defines the centre's role and responsibilities.

The **sectorial criteria for the identification of critical infrastructure** are defined in detail in the relevant law (Amendment 430/2010 Call. of the Act 240/2000 Coll.)

Sources

(Centre for Cyber Security 2015)

(Danish Defence Intelligence Service et al. 2014)

(ENISA, KPMG 2015)

(Government of Denmark 2012)

(Government of Denmark 2014)

1.5 Estonia

Leading Authority

The **Estonian Information System Authority (RIA)** is the main authority for the protection of critical information systems at a strategic level.

TYPE	ACTOR OR INSTITUTION
Leading	• Estonian Information System Authority (RIA)
Ministerial	• Ministry of Economic Affairs and Communications • Ministry of Interior • Several sectoral Ministries and public bodies (sector-responsibility)
Operational	• CERT Estonia
Network/Forum/Council	• Cyber Security Council
Private/PPPs	• CIIP Council

Management Structure

Nine government ministries and public bodies (such as the Ministry of Finance, and the five largest cities) are designated to act as an organising authority for their sector and to ensure the continuous operation of the vital services. They are also responsible to advise operators of vital services and to report to the Ministry of Interior, which takes the role of national coordinator. The Emergency Act authorises the organising authorities to issue secondary legislation in order to establish requirements for providers of vital services.

In order to strengthen the “strategic level inter-agency” cooperation, the Cyber Security Council was added to the Government Security Committee in 2009. It serves as a regular forum for decision makers from key governmental agencies involved in cyber security and oversees the implementation of the National Cyber Security Strategy, including CIIP activities.

A CIIP Council was established in 2011 with the objective of fostering public-private cooperation. The council brings together experts from both sides and acts as a platform to exchange information about problems and best practices for the improvement of the security of critical infrastructure. The Council is managed by the RIA.

Roles and Responsibilities

Estonian Information System Authority (RIA)

Estonian Information System Authority (RIA) was established as a government agency in 2010. It is an authority under the Estonian Ministry of Economic Affairs and Communications and responsible "for organising protection of the state's information and communication technology (hereinafter ICT) infrastructure, and exercising supervision over the security of information systems." The RIA has the mandate of a law enforcement authority as defined in the Law Enforcement Act.

For the purpose of CIIP, the Section for Critical Information Infrastructure Protection as formed within the Risk Analysis Department.

Pursuant to the Law Enforcement Act, the RIA has the authority to perform supervisory activities as they are described in the law. The agency is authorised to confirm the compliance of operators in regard to security measures outlined in laws and regulations. In case of non-compliance, it can issue warnings or impose sanctions or financial penalties.

RIA holds periodic events and media campaigns for raising awareness. In addition it organises technical and end-user training. These are performed for Governmental Authorities and vital service providers. In addition to training, the RIA organises annual CIIP Seminar every autumn. It is also offers a public web-blog, which disseminates relevant information.

CERT Estonia

CERT Estonia was established in 2006 and is responsible for the management of security incidents in Estonian computer networks. Its activities among others are preventive measures and the handling of incidents. CERT Estonia also issues warnings and information about security vulnerabilities, holds periodic events and media campaigns for raising awareness. The CSIRT is under the control of the RIA, within Cyber Security Branch.

Ministry of Economic Affairs and Communications

The Estonian Ministry of Economic Affairs and Communications is responsible for the development of the cyber security policy and the coordination of its implementation. The implementation involves several ministries and government agencies.

Relevant Framework Papers and Regulations

Estonia published its first **Cyber Security Strategy** 2008 – 2013 in 2008, and released an updated version in 2014. The new Cyber Security Strategy 2014-2017 describes recent developments, new threats and the progress in implementing the strategy.

The Emergency Act, passed in June 2009, provides the legal bases for crisis and emergency management:

Providers of vital services are "obligated to ensure the continuous application of security measures in regards to the information systems used for the provision of vital services and the related information assets" (Emergency Act 2009: §40(1))[1].

The Regulation **Security measures for information systems of vital services and related information assets**, which has been established on the basis of subsection 40 (2) of the Emergency Act, is the main legal framework for CIIP in Estonia. It was adopted in 2013 and contains several legal obligations for providers of vital services with regard to the implementation of security measures and incident notification.

The **Act for the Amendment for and Application of the Law Enforcement Act** entered into force on 1 July 2014. It grants supervision competencies and obligations to the Estonian Information System Authority (RIA).

Sources

(ENISA 2015)

(ENISA, KPMG (2015)

(Government of Estonia 2008)

(Government of Estonia 2009)

(Government of Estonia 2013)

(Information System Authority 2012)

1.6 Finland

Leading Authority

There is no single authority responsible for CIIP across all sectors. Within the communications sector, the **National Cyber Security Centre Finland (NCSC-FI)** at the Finnish Communications Regulatory Authority (FICORA) is the main governmental agency responsible for CIIP.

TYPE	ACTOR OR INSTITUTION

Leading	• National Cyber Security Centre Finland (NCSC-FI) at the Finnish Communications Regulatory Authority (FICORA) for the telecommunication sector
	• National Emergency Supply Agency (NESA)
	• Other sector-specific authorities:
	  ○ Energy Authority and to the Radiation and Nuclear Safety Authority
	  ○ Supervisory Authority for banking
	  ○ National Supervisory Authority for Welfare and Health
	  ○ Transport Safety Agency

Ministerial	• Ministry of Transport and Communications • Ministry of Finance • Ministry of employment and the Economy • Ministry of Social Affairs and Health • Ministry of Justice

[1] Estonian Emergency Act, June 2009: http://www.legaltext.ee/et/andmebaas/paraframe.asp?loc=text&lk=en&sk=et&dok=XXXXX26.htm&query=H%E4daolukorra+seadus&tyyp=X&ptyyp=RT&fr=no&pg=1

Operational	• CERT-FI (part of FICORA)

Management Structure

The FICORA has authoritative powers to secure the provision of communication networks and services as well as privacy and confidentiality of communications. Other sector specific authorities have been given tasks that contribute to ensuring critical information infrastructure protection in their respective field.

There are no institutionalised forms of cooperation for the sole purpose of national CIIP in Finland. Nevertheless cooperation concerning critical information infrastructure protection is handled in the context of general risk management and the protection of the supply of infrastructure and services.

Representatives from the public and private sector collaborate for example in the National Emergency Supply Organisation (NESO). NESO's work is related to the security of supply in Finland.

Roles and Responsibilities

The National Cyber Security Centre Finland (NCSC-FI) at the Finnish Communications Regulatory Authority (FICORA)

The Finnish Communications Regulatory Authority consolidates the duties of the National Cyber Security Centre Finland (NCSC-FI) the CERT-FI and National Communications Security Authority (NCSA).The NCSC-FI is part of the Finnish Communications Regulatory Authority (FICORA), which also ensures the versatility of the provision of communications services.

FICORA acts under the Ministry of Transport and Communications, which steers both the work of FICORA and the NCSC. Other responsibilities include legislation and policy development related to communications networks and services, as well as data protection and data security in communications. FICORIA collects and disseminates information on technical information security risks and threats to private and public stakeholders.

The NCSC-FI at FICORA is the main governmental agency responsible for CIIP within the communications sector. The agency offers support and advisory to operators of CII and monitors the compliance in regard to information security regulations. FICORA has authoritative powers in the provision of communication networks and services as well as privacy and confidentiality of communications. Other sector specific authorities have been entitled tasks that contribute to ensuring critical information infrastructure protection in their respective field.

Telco operators are obliged to report information security violations and disruptions of their services to FICORA.

National Emergency Supply Agency (NESA)

In addition to the mentioned agencies, the National Emergency Supply Agency (NESA) holds an important role in CIIP on a national level. NESA has been established by the Security of Supply Act. It works under the Ministry of Employment and the Economy and is tasked with planning and handling measures related to developing and maintaining the security of supply. Because of the importance of technical systems for the security of supply, part of NESA's responsibilities is to ensure the continuity of national critical infrastructure.

Relevant Framework Papers and Regulations

Finland adopted and implemented two national **Information security strategies in 2003 and 2008** and a **Cyber Security Strategy in 2013**. The strategies describes the overall approach to information and cyber security and an implementation plan.

Relevant framework papers are the **Constitution of Finland** and **Emergency Powers Act**, which includes obligations with regard to emergency preparation for public authorities. There are also several sector specific legislation. Important examples are the **Information Society Code**, the **Electricity Provision Act**, **Act on the Financial Supervisory Authority**, the **Act on Medical Devices and Equipment**, **Nuclear Energy Act**, **Railway Act**, **Personal Data Act** which set obligations for companies within their sectors.

The Finish government is currently preparing a **new information security strategy** in order to increase trust in the internet and in digital modes of operation. The new strategy will be issued in February 2016.

Sources

(ENISA 2015)

(ENISA, KPMG 2015)

(Government of Finland 2006)

(Ministry of Defence 2010)

(Ministry of Justice, Finland 2003)

(Ministry of Transport and Communications, Finland 2014)

(National Emergency Supply Agency 2013)

(Prime Minister's Office Finland 2015)

(Secretariat of the Security Committee 2013)

(The National Emergency Supply Agency 2013)

1.7 France

Leading Authority

The **Agence nationale de la sécurité des systèmes d'information (ANSSI)** is the main cybersecurity agency and national authority in the area of NIS and CIIP.

TYPE	ACTOR OR INSTITUTION
Leading	• Agence nationale de la sécurité des systèmes d'information (ANSSI)
Ministerial	• General Secretariat for Defence and National Security (SGDSN)
Operational	• CERT-FR (part of ANSSI)

Management Structure

The coordinating body for CIP in France is the **General Secretariat for Defence and National Security (SGDSN)**. The SGDNS is an inter-ministerial organisation and is under the authority of the Prime Minister of France. ANSSI is an inter-ministerial agency under strategic guidance of SGDSN's Strategic Committee. These

are the main two agencies for CIP and CIIP and there are no other formal forms of cooperation with other public agencies.

ANSSI cooperates with the private sector in 18 different working groups on matters such as the identification of systems of vital importance, definition of relevant sectorial technical rules and measures or the definition of processes (e.g. incident notification).

Roles and Responsibilities

Agence nationale de la sécurité des systèmes d'information (ANSSI)

In July 2009, the French Network and Information Security Agency (ANSSI) was created. ANSSI is an inter-ministerial agency attached to the Prime Minister's office and acts under the strategic guidance of SGDSN's Strategic Committee for the Security of Information Systems. The agency's role was strengthened in 2011, when it was declared the main national authority for the defence of information systems. The agency is currently armed with 400 people.

It is responsible for preventing and reacting to cyber-attacks performed against the government of France's networks and to offer support and advice to operators of CII and government agencies in their efforts to strengthen the security of their information and networks.

ANSSI develops and implements different measures for the protection of information systems proposed by the Prime Minister. Furthermore, it has been empowered to define the implementing and enforcement of measures of the Military Programming Law. According to the Law, "operators of vital importance" are obligated to report cybersecurity incident notifications to ANSSI, comply with the listed technical and organisational measures, and undergo cybersecurity audits. The agency is currently working with the government as well as with private entities to define the application conditions of this law. Other responsibilities of ANSSI include regulatory tasks and the evaluation and approval of security products.

When a national crisis with an impact on the security of information systems of public authorities or critical infrastructure operators occurs, ANSSI acts as a contingency agency for CIIP and decides on the measures that operators must take to respond to the crisis and coordinates the action of the government against the crisis. There is an "operations centre" within ANSSI for the purpose of crisis management.

Part of ANSSI is a training centre which offers around 20 different training courses such as pen-testing or cryptography. These courses are meant for public employees, but can be attended by employees of private operators under special circumstances. Additionally, ANSSI is offering awareness raising information on its website. Furthermore, the agency is offering technical guidelines such as the document "40 essential measures for a healthy network".

CERT-FR

CERT-FR is part of ANSSI and the national CSIRT of France. Its main scope is public administration and the operators of CI, but it is trying to expand its services to SMEs and citizens. Its main tasks are detection of threats, incident response, forensic investigation, pen-tests and audits.

Relevant Framework Papers and Regulations

France's **Information systems defence and security strategy** was adopted in 2011. One of the four major objectives is to strengthen the cybersecurity of critical national infrastructures.

There are several decrees, which set the legal framework for CIIP in France. Among those are:

- **Decree 2009-843** (7 July 2009) and **Decree 2011-170** (11 February 2011) based on which the French Network and Information Security Agency (ANSSI) has been established and appointed as the French Cyber defence Authority
- **2013 French White Paper Defence and National Security**. The White Paper recognizes the risk of sabotage against critical infrastructures.
- The **Military Programming Law (LPM)** was promulgated on the 18th December 2013, following the measures announced by the 2013 White Paper. It has been further detailed in the decree 2015-351 on 27 March 2015, which amended the Code of Defence with provisions of interest to CIIP. Article 22 of the LPM introduces 4 main measures to enhance the cybersecurity of operators of vital importance.
- The Prime Ministers 's Order of 2 June 2006 "**Establishing on the List of the Sectors of Critical Infrastructure and Designating Coordinating Ministers of these Sectors**" lists 12 vital sectors

Sources

(ENISA, KPMG (2015)

(French Ministry of Defence 2013)

(French Network and Information Security Agency (ANSSI) 2011)

(French Network and Information Security Agency (ANSSI) 2015a)

(French Network and Information Security Agency (ANSSI) 2015b)

(French Senate 2013)

1.8 Germany

Leading Authority

The **Federal Office for Information Security (BSI)** is the main national authority responsible for the protection of critical information infrastructures at the federal level.

TYPE	ACTOR OR INSTITUTION
Leading	• Federal Office for Information Security (BSI)
Ministerial	• Federal Ministry of the Interior (BMI)
Operational	• Federal Network Agency (BNetzA) • Federal Office of Civil Protection and Disaster Assistance (BBK) • Federal Office for Information Security (CERT-Bund, National Cyber Response Center, IT Crisis Reaction Centre) • Several CSIRTs on state level (Bavaria, Baden-Württemberg, Brandenburg and North Rhine-Westphalia)
Network/Forum/Council	• National Cyber Response Centre • National Cyber Security Council
Private/PPPs	• UP KRITIS • Alliance for Cyber Security

Management Structure

Due to the complexity and breadth of the issue, CIP is seen as a networking task involving diverse bodies at various levels.

The National Cyber Security Council has been established pursuant to the German Cyber Security Strategy (GCSS). It is comprised of representatives from relevant ministries and public agencies as well as selected business representatives. The council meets three times a year and has the goal of discussing and coordinating actions between the different stakeholders on a political-strategic level.

The National Cyber Response Centre has been established in accordance to the GCSS between April 2011 and March 2013. Here, representatives from the different relevant public authorities and law enforcement agencies come together to share information and to assess cyber security incidents from different perspectives.

UP KRITIS is a public-private partnership between operators of CII, industry associations and the responsible public agencies. The partnership covers eight out of the nine critical sectors (energy, health, ICT, transport and traffic, media and culture, water, finance and insurance, food). The goals are information sharing, joint assessments of the security situation as well as the development of incident management structures.

The Alliance for Cyber Security is an initiative of the Federal Office for Information Security (BSI) and has been established in cooperation with the industry association Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM). Participants work together to establish a knowledge base and to foster the sharing of information and good practices. Currently, more than 1283 “institutions” are participating in the alliance.

Roles and Responsibilities

Federal Ministry of the Interior (BMI)

The Federal Ministry of the Interior is the Department responsible for internal security in Germany. It coordinates and supervises all activities of its subordinate agencies (including BBK and BSI).

Federal Office for Information Security (BSI)

BSI is the central IT security service provider of the German Federal Government. The BSI operates the office of the UP KRITIS.

In cases where audits reveal security flaws, the BSI, in accordance with the respective regulatory authority, can obligate operators to resolve these issues (According to the IT Security Act, Art. 1 §8a (3)). According to the IT Security Act, operators of CII are obligated to implement appropriate technical and organisational measures in order to ensure the security of their information systems that are necessary for the availability of their critical services. The BSI can impose fines in cases of non-compliance.

This however does not extend to governmental authorities. While the BSI can issue minimum standards for federal authorities, they are only binding if the German Federal Ministry of the Interior makes these minimum standards compulsory.

The BSI has established an IT Crisis Reaction Centre, which was set up to ensure an immediate response to serious incidents. In addition the Centre coordinates the cooperation with affected companies and industry

SPOCs (Single Point of Contacts). In case of an incident on a national scale, the Centre can invoke a committee consisting of relevant departments.

CERT-Bund

CERT-Bund (Computer Emergency Response Team for federal agencies) is part of the BSI and the central point of contact for preventive and reactive measures regarding security-related computer incidents. The CSIRT publishes recommendations for preventive measures and detected vulnerabilities. Its services are primarily available to the federal authorities: Analysis of incident reports, incident response support, active alerting of the Federal Administration in case of imminent danger.

Federal Network Agency (BNetzA)

The Federal Network Agency is the German regulatory office for electricity, gas, telecommunications, post and railway markets. It is a federal government agency under the German Federal Ministry of Economics and Technology. Telecommunication companies have to notify the Federal Network Agency (BNetzA) about security incidents and implement appropriate technical and organisational measures. Like the BSI, the BNetzA can impose fines in cases of non-compliance.

Federal Office of Civil Protection and Disaster Assistance (BBK)

The BBK performs the tasks of civil protection and disaster relief. It develops preventive measures and policies designed to protect the population in case of a catastrophe. In addition, it is responsible for diverse projects focusing on the protection of critical infrastructures.

Federal States (Bundesländer)

The 16 individual states within Germany are responsible for the civil protection within their own state. Thereby, diverse connections are also established with the respective local Critical Infrastructures.

Relevant Framework Papers and Regulations

The **German Cyber Security Strategy (GCSS)** was adopted in February 2011. It outlines guidelines, strategic goals and several measures for the implementation of the strategy.

The legal framework for CIP/CIIP in Germany is set out by a number of laws and regulations:

- 2005 – **National Plan for Information Infrastructure Protection (NPSI)** (outdated)
- 2007 – **KRITIS implementation plan (UP KRITIS)** (obsolete, revised in 2014)
- 2009 – **National Strategy for Critical Infrastructure Protection (CIP Strategy)**
- 2014 – **UP KRITIS: Public-Private Partnership for Critical Infrastructure Protection - Basis and Goals**
- 14 August 2009 – **Act to Strengthen the Security of Federal Information** : Defines the competences of the Federal Office for Information Security
- 17 July 2015 – **IT Security Act**: The newly passed law obligates operators to implement adequate organisational and technical measures for information security as far as it is necessary for the availability of their critical services. Furthermore organizations are to conduct security audits, to establish a contact point within their organisation and to report major IT security incidents if they could possibly affect the availability of their critical services.

Sources

(Federal Office for Information Security 2015a)

(Federal Office for Information Security 2015b)

(Federal Office for Information Security 2015c)

(Federal Office for Information Security, Federal Office of Civil Protection and Disaster Assistance 2013a)

(Federal Office for Information Security, Federal Office of Civil Protection and Disaster Assistance 2013b)

1.9 Hungary

Leading Authority

The Responsibility is shared between the **National Directorate General for Disaster Management** and the **National Electronic Information Security Authority (NEIH)**.

TYPE	ACTOR OR INSTITUTION
Leading	• National Directorate General for Disaster Management • National Electronic Information Security Authority (NEIH)
Ministerial	• Ministry of Interior
Operational	• GovCERT • Sector-specific authorities, e.g. National Bank (finance sector)
Network/Forum/Council	• National Cyber Security Coordination Council • National Cyber Security Forum

Management Structure

The National Cyber Security Coordination Council is responsible for coordinating the cooperation of relevant organisations performing cyber security responsibilities.

The National Cyber Security Forum provides a framework for cooperation between governmental and non-governmental actors. Non-governmental professionals are invited to join the forum to exchange information.

In addition, the National Cyber Security Centre and GovCERT have the responsibility to exchange information with the private sector.

Roles and Responsibilities

National Directorate General for Disaster Management

The National Directorate General for Disaster Management is tasked with the supervision of CIP in Hungary, which includes monitoring the critical infrastructure of critical operators in Hungary.

It also operates the CIP CERT, which can be described as a network safety centre that maintains trusted communication channels with operators and public agencies. It has been established to offer support to operators of CII.

In a crisis situation, the National Directorate General for Disaster Management is responsible for coordinating national actions for the protection of critical infrastructure. It will be supported by GovCERT.

National Electronic Information Security Authority (NEIH)

The National Electronic Information Security Authority (NEIH) oversees the compliance of government agencies in regard to Act L. of 2013. It verifies compliance with legal requirements applicable to the classification of IT systems and security levels of public organizations.

GovCERT

GovCERT is Hungary's national CSIRT. It will assist system administrators in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to incident coordination and resolution. The GovCERT has no power to interfere with networks, unless requested by governmental agencies or the operators of the CII. The CSIRT is within the Special Service for National Security.

GovCERTs tasks include raising awareness in the field of information and network security. It does this by providing timely information on security topics, issue alerts and warnings, publishes newsletter and holding conferences about cyber security related issues.

Public agencies are obligated to notify GovCERT about major security incidents. GovCERT will then provide the NEIH with the relevant information.

Relevant Framework Papers and Regulations

The **National Cyber Security Strategy (NCSS)** of Hungary was adopted in 2013. It covers the topic of cyber security in general and names the "protection for its national data assets, to ensure the operational safety of the cyberspace functions of its vital systems and facilities…" as one of its main objectives.

A **greenbook on the National Programme for CIP** has been published in 2008.

A legal framework is set out by **Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies** and by **Act CLXVI of 2012 on the assignment and the protection of critical infrastructure** of Hungary.

Act L. of 2013 defines the roles and responsibilities with regard to the security of electronic information systems of government agencies and municipalities.

Act CLXVI defines the vital sectors and the basic provisions for the identification, designation and protection of vital systems. So far, is has been followed by four governmental decrees for the transport, energy, agriculture and law enforcement sector. The decrees further specify the criteria and the process of identification. Decrees for other sectors such as telecommunications are planned.

Act C. of 2003 on Electronic Communications obligates Internet Service Providers to notify their respective public agencies in case of security breaches.

Sources

(ENISA, KPMG 2015)

(Government of Hungary 2003)

(Government of Hungary 2012)

(Government of Hungary 2013a)

(Government of Hungary 2013b)

1.10 Ireland

Leading Authority

There is no leading or designated authority for CIIP in Ireland.

TYPE	ACTOR OR INSTITUTION
Leading	• Every Ministry holds responsibility for its own sector (doctrine of subsidiarity)
Operational	• CSIRT-IE (under development) • Sectorial CSIRTs

Management Structure

With regard to security matters, Ireland follows a “doctrine of subsidiarity”. In case of an incident, the impacted entity is responsible for its own security. Security is considered to be a matter for the market, unless legislation is required as necessitated by this country's membership of the European Union. Therefore, responsibilities lie with the individual operators. Investigations by law enforcement is possible provided formal reporting by the victim to law enforcement takes place. The national CSIRT can provide assistance provided the incident has been reported. Therefore, investigations in companies of the energy or telecommunications sector tend to be much easier, since many of these are state-owned. Awareness raising or similar training programmes are also considered to be the responsibility of companies.

In case of an incident, the Government Task Force on Emergency Planning will act as a top-level structure with the responsibility of steering and coordinating emergency responses. It is set up and chaired by the Ministry of Defence and brings together key officials from other relevant public authorities. The Office of Emergency Planning (OEP) provides support to the Government Task Force. It offers advice to the Minister of Defence and develops improvements for the existing emergency management processes. The OEP is part of the Ministry of Defence and includes civil and military personnel.

The specific form and degree of cooperation between public and private actors vary, depending on sector operators and authorities. Generally, cooperation within the telecommunications and energy sector tends to be stronger.

Roles and Responsibilities

The responsibility for the identification of CII, risk assessment and sector-security lies with each Ministry for their respective sector. In general, sectors and private companies are responsible for their own security. There is no agency in Ireland that holds the formal responsibility for the entirety of these tasks.

The Department of Communications, Energy and Natural Resources and its National Cyber Security Centre are responsible for cyber security in general. A CSIRT-IE is currently under development in the Department of Communications. It shall act as a national Point of Contact for companies, offer incident response management, threat intelligence, alerting and advisory. The main constituency of the CSIRT will be government departments and agencies.

The Ministry of Defence covers the CIP in its entirety for emergencies within its Office of Emergency Planning. However, there is no formal establishment of a specific entity to cover only CIIP in Ireland.

Relevant Framework Papers and Regulations

A **National Cyber Security Strategy** is currently under development. A CIIP or similar programmes are not in place.

There are no specific regulations at a national level. Only sectorial legislation and regulation, for example in the energy or telecommunications sector, exists.

Sources

(Department of Defence 2015)

(ENISA 2015)

(ENISA, KPMG 2015)

1.11 Italy

Leading Authority

The leading authority in Italy is the **Cybersecurity Unit** of the Prime Minister's Military Advisor's Office.

TYPE	ACTOR OR INSTITUTION
Leading	• Cyber Security Unit and Inter Ministerial Unit for Situation and Planning (NISP)
Ministerial	• Interministerial committee for the security of the republic (CISR): • Ministry of Foreign Affairs, • Ministry of Interior, • Ministry of Defence, • Ministry of Justice, • Ministry of Treasure • Department of Civil Protection of the PCM, • Ministry of Economic Development • Ministry of Infrastructure and Transport • AGID-Italian Agency for the Digital Agenda
Operational	• IT-CERT • CERT-PA (Public Administration CERT); • CNAIPIC (Anti-Crime Computer Centre for Critical Infrastructure Protection) • Anti-Crime Computer Centre for Critical Infrastructure Protection (CNAIPIC) **Italian Intel Community:** • Security Intelligence Department (DIS) • External Intelligence and Security Agency (AISE) • Internal Intelligence and Security Agency (AISI)

Management Structure

The Unit is chaired by the Prime Minister's Military Advisor and composed of a representative of each Administration, such as: DIS, AISE, AISI, Ministry of Foreign Affairs, Ministry of Interior, Ministry of Defence, Ministry of Justice, Ministry of Treasure, Ministry of Economic Development, Department of Civil protection, AGID-Italian Agency for the Digital Agenda. As for classified information, the Unit shall be integrated by a representative of the DIS-Central Secrecy Office (under art.9, Law n.124/2007).

Roles and Responsibilities

Cybersecurity Unit

The Cyber Security Unit coordinates the different components across the institutional architecture relevant for cyber security and ICT security, responsible for CIIP (Critical Information Infrastructures Protection) in their respective sectors. It is tasked with preventing and preparing for crisis situations as well as ensuring information sharing and early warning crisis management, closely working with public administrations and civil protection. It maintains, on a 24/7 basis, the operational readiness of the warning and response unit in case of cyber crisis. The Unit acts as a national point of contact during national cyber crisis emergencies.
In case of cyber crisis or national emergency situations, the Cyber Security Unit will call upon the Resilience Response Cabinet: the Inter Ministerial Unit for Situation and Planning (NISP) that acts as "Interministerial board in case of cyber crisis". It ensures the coordination of all stakeholders' activities and responses and manages emergency with the help of National CERT.

IT-CERT

The national CERT has established an information sharing platform in cooperation with private operators ranging from energy, telecommunication and banking sectors. CERT-N is the national CERT of Italy, established in 2014, offers technical advisory to the Council of Ministers and creates partnerships with CII operators for information sharing.
Furthermore, CERT-N is responsible for coordinating activities of similar institutions or other bodies involved in IT security in case of a national incident. CERT-N is under the Ministry of Economic Development.
CERT-N also participates in awareness raising, for this purpose the National CERT has built up a website for citizens and to develop awareness raising programs for small and medium enterprises (SMEs).

CERT-PA

CERT-PA within AGID-Italian Agency for the Digital Agenda shares and analyzes information, forwards warnings, develops tools and promotes security culture and awareness in Public Administrations, also through training courses. Since March 2014, there's an incident response unit in order to deal with cyber incidents.

Intelligence System for the Security of the Republic: DIS, AISE and AISI

The DIS has the major duty of coordination and reporting to the Government ensuring a fully unified approach in setting intel requirements and drawing up strategic analysis and assessments.

AISE and AISI role in cyber sector consists of acting at an operational level, gathering information and providing tactical analyses.

Ministry of Economic Development

According to the Electronic Communication Code, operators of public communication services and networks accessible to the public are legally obliged to notify the Ministry of Economic Development of significant violations of their computer systems and networks and to provide information on the adoption of best practices and measures for cyber security.

Anti-Crime Computer Centre for Critical Infrastructure Protection (CNAIPIC)

At law enforcement level, CNAIPIC (Anti-Crime Computer Centre for Critical Infrastructure Protection) acts as a police authority for prevention, repression and contrast of criminal actions committed against the different critical infrastructure through the cyberspace.

Relevant Framework Papers and Regulations

Directive laying down **guidelines for cybernetic protection and the national cyber security** (Decree of the President of the Council of Ministers, January 24, 2013)

Law n.124 of August 3rd 2007 amended and integrated by **Law n.133 of August 7th 2012** states that special directives shall strengthen the intelligence activities to protect material and immaterial critical infrastructures with particular attention to national cyber protection and intelligence computer security

Decree of the President of the Council of Ministers, January 24, 2013: Directive laying down guidelines for cyber protection and the national cyber security

The **National Strategic Framework for Cyberspace Security** outlines a comprehensive strategy for topics related to Italy's cyber security. It describes the roles and responsibilities of relevant ministries and agencies.

The **National Plan for Cyberspace Protection and ICT Security** sets out a roadmap for the implementation of the National Strategic Framework.

The Presidential Directive of August 1st 2015 defines a better organisation and roles of the Intel system components, emphasizes the need to strengthen the reaction system capacities and outlines some guidelines to **align the Italian cyber assets** with the international standards

Decree of the Minister of the Interior on the Identification of CII of national interest (Decree of the Ministry of Internal Affair, 9 January 2008): The Decree lists the CI which have been designated by the Italian government and establishes the CNAIPIC (Anti-Crime Computer Centre for Critical Infrastructure Protection)

National Organisation of Crisis Management (Decree of the President of the Council of Ministers of 5th May 2010): Provides the legal basis for the Political Strategic Committee (CoPS) and the Nucleus Inter Ministerial Unit for Situation and Planning (NISP) (see A.1)

Legislative Decree 11 April 2011 represents the **implementation of the EU Directive 2008/114/CE** and the definition of CI.

Legislative Decree N. 259/2003 (**Electronic Communication Code**): Envisages obligations for operators within the telecommunications sector.

Legislative Decree N.82 June 22nd 2012 that gives the Agency for the Digital Agenda (AgiD) the functions to assure, among other actors, networks security as well as functions of coordination, orientation and control yet assigned to the DigitPA (National Center for the Public Administration Digitalization)

Motion approved on May 23rd 2012 that sets out that the Government will implement any initiative in order to establish, at the Presidency of the Council of Ministers, an Interministerial Committee with the task of developing a National Strategy for cyber space security, defining general orientations and directives within the framework of national and international policy on this matter and to identify the regulatory policy if deemed necessary.

Sources

(ENISA 2015)

(ENISA, KPMG 2015)

(Ministry of Internal Affair 2008)

(Presidency of the Council of Ministers 2010)

(Presidency of the Council of Ministers 2011)

(Presidency of the Council of Ministers 2013a)

(Presidency of the Council of Ministers 2013b)

(Presidency of the Council of Ministers 2013c)

1.12 Latvia

Leading Authority

The role of coordinating security measures is shared between the state security service, **Constitution Protection Bureau**, and the national CSIRT (the **Information Technology Security Incident Response Institution of the Republic of Latvia – CERT.LV**), both operating under the Ministry of Defence.

TYPE	ACTOR OR INSTITUTION
Leading	• Constitution Protection Bureau • Information Technology Security Incident Response Institution of the Republic of Latvia (CERT.LV)
Ministerial	• Ministry of Defence
Network/Forum/Council	• Information Technology and Information Systems Security Experts Group (SEG)

Management Structure

Formal cooperation between governmental agencies occurs in the framework of The Commission of Intermediary Institutions for State Security and to a certain extent is defined in the Law on the Security of Information Technologies. Informal cooperation takes place on a bilateral basis (state and CII owner), where on the one side there is CERT.LV and the Constitution Protection Bureau, and on the other side there are CII owners.

CERT.LV also cooperates with the private association Safer Internet Centre Net-Safe Latvia in the "Responsible Internet Service Provider (ISP)" – Programme. Responsible ISP is a symbol of quality, received by ISPs that cooperate with CERT.LV, provide incident information to end users and cooperate with Net-Safe Latvia for illegal material takedown of the Internet. Currently, 14 ISPs have joined the initiative, covering approximately 77% of the market.

The Information Technology and Information Systems Security Experts Group (SEG) is a voluntary IT/IS security experts group aiming to advance IT/IS security and security awareness culture in Latvia. SEG unites experts both from public and private sector. SEG members support CERT.LV sharing their expertise and knowledge with technical experts and general public

Roles and Responsibilities

Constitution Protection Bureau

The Constitution Protection Bureau cooperates with the CERT.LV and CI owners (incl. 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 the right to examine personnel related to ensuring the operation of the CI, request the CERT.LV to conduct inspections on 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 institutions who supervise the CI owners. Furthermore, the Bureau, together with the CERT.LV, periodically informs the National Information Technologies Security Council regarding current threats to critical infrastructure.

Information Technology Security Incident Response Institution of the Republic of Latvia (CERT.LV)

The Information Technologies Security Incidents Response Institution (CERT.LV) coordinates and provides support for CII incident prevention, inter alia by cooperating with the Constitution Protection Bureau and CI owners in risk assessment and risk management. In order to determine the vulnerability and security risks of the relevant critical information infrastructure, the primary tool foreseen by the regulation is security inspection (e.g. penetration tests) of the critical infrastructure. Based on such security inspections, CERT.LV may issue recommendations to the CII operator. The CSIRT also prepares information on newest viruses and threats available and tailored for everyone, including technical experts and general public. According to the Law on IT Security, internet providers and CII owners have to report incidents to CERT.LV.

CERT.LV is heavily engaged in the education of various groups of users including those responsible for the IT security in their organisations, employees, managers, students and pupils as well as general public. CERT.LV develops recommendations; shares best practices and examples for IT security principles and rules. It organises and participates in about 50 events yearly reaching out to more than 3000 people. It is planned to increase this capacity every year.

Regular training organized by CERT.LV for the representatives of critical infrastructure are recognized as a significant tool to exchange the knowledge and experience, as well as to improve the procedures.

Relevant Framework Papers and Regulations

The **Cyber Security Strategy of Latvia for 2014 – 2018 (CSS)** marks Critical Infrastructure as one of the key areas of action under the section on Governance and Resources of Cyber Security.

The **Action plan of the CSS** outlines definite actions to be implemented by 2018. It defines the institution responsible for the implementation of the specific task, necessary financial resources as well as the desired outcome

Critical infrastructure in Latvia is designated based on the **National Security Law**, which defines critical infrastructure

The **Law on the Security of Information Technologies** further addresses "critical infrastructure of information technologies".

Sources

(Ministry of Defence, LV 2015)

1.13 Netherlands

Leading Authority

The **National Cyber Security Centre (NCSC)** within the National Coordinator for Security and Counterterrorism (NCTV) is the major CIP agency for CIP in the Netherlands.

TYPE	ACTOR OR INSTITUTION
Leading	• National Cyber Security Centre (NCSC) within the National Coordinator for Security and Counterterrorism (NCTV)
Ministerial	• Ministry of Security and Justice
Network/Forum/Council	• Dutch Cyber Security Council (within NCSC)

Management Structure

The Netherlands follow a network approach with regard to CIIP. Public-private partnerships are considered to be essential in order to maintain a resilience against cyber threats. For this purpose various public-private partnerships have been set up within the NCSC.

In 2014, the National Response Network (NRN) and the National Detection Network (NDN) were launched. The NRN is a collaboration between the NCSC and public-private ICT response organisations from various sectors. Within the NRN knowledge and experiences can be shared between the different stakeholders and response capacities can be organised. The NDN serves as an information platform, where information about threats and digital dangers are exchanged.

The Ministry of Security and Justice takes the lead in coordinating the efforts of the different relevant public agencies in daily business and during crisis situations.

Roles and Responsibilities

National Cyber Security Centre (NCSC) within the National Coordinator for Security and Counterterrorism (NCTV)

The NCSC is set up as a public-private partnership within the NCTV. Its responsibilities are: Crisis coordination on an operational level, incident response, Point of Contact for operators of CII and to advise and support operators. The centre is not authorized to issue binding instructions as its role is a coordinating and supporting one.

The NCTV acts as a coordinator for the different relevant public agencies. It cooperates with several Dutch Ministries, which are responsible for their respective domain.

Ministry of Security and Justice

The Ministry holds responsibility for CIP in the Netherlands and hosts the NCTV and NCSC. During a crisis situation the Ministry of Security and Justice and the NCTV within the Ministry have the responsibility to coordinate the different public agencies.

Dutch Cyber Security Council

The Dutch Cyber Security Council offers advice to on a strategic and political level. The council is comprised of representatives from different Ministries, academia and the private sector and has a strong public-private character.

Relevant Framework Papers and Regulations

The first **Dutch National Cyber Security Strategy** (NCSS) has been released in 2011 and has been updated in 2013

To date the framework for CIIP in the Netherlands is more based on policy rather than on law and regulation. Relevant policy papers include:

- Data Security Breach Notification (SBN)
- Policy letter on Protecting Critical Infrastructure (2005)
- Third progress letter on National Security (2010)
- List of Critical Infrastructure 2009 and 2015 (issued by the Ministry of Interior in 2009, and by the Ministry of Security and Justice in 2015)
- Regulatory frameworks for CSIRTs

A regulatory framework for CIP is in development. A first draft has been published in February 2015. The new law shall provide a legal basis for roles and responsibilities with respect to cyber security.

Sources

(KPMG (2015)

(Ministry of Interior 2009)

(Ministry of Interior 2015)

(National Coordinator for Security and Counterterrorism 2013)

(National Cyber Security Centre 2015)

1.14 Poland

Leading Authority

The **Government Centre for Security (RCB)** is a supra-ministerial structure and the main authority for CIP in Poland.

TYPE	ACTOR OR INSTITUTION
Leading	• Government Centre for Security (RCB)
Ministerial	• The Ministry of Administration and Digitization

Operational	• The Research and Academic Computer Network (NASK) • CERT.gov.PL • CERT Polska (part of NASK) • Several sectoral CSIRTs, such as MilCERT and CERT Orange (telecommunications sector)
Network/Forum/Council	• Cooperation forums between public agencies and CI operators

Management Structure

On a political level, representatives from relevant ministries are meeting every few months to discuss CIP-related issues. In addition, an expert group of relevant representatives of government institutions meets every two weeks to draft recommendations for the Secretary of State.

The National Critical Infrastructure Protection Programme (NCIPP) outlines cooperation forums between private and public actors on a national, sectoral and local level. Representatives from the respective public agencies and the CI operators come together within these forums to discuss current CIP-related issues. On the local level, this would be the local government, representatives from local services such as the fire department and the police and representatives from local CI operators. The national forum meets once a year, the sectoral forums meets twice a year and the local forums meet four times a year.

Roles and Responsibilities

The Government Centre for Security (RCB)

The RCB is the main authority for CIP in Poland and is under the direct authority of the Prime Minister. The RCB serves as a national centre for crisis management. It is serving as “the leader in the construction of the critical infrastructure protection system based on shared responsibilities, cooperation and trust…”. Its tasks include but are not limited to establishing partnerships between relevant stakeholders, monitoring potential threats, building a network for the exchange of information, conducting risk assessment and developing and implementing recommendations, guidelines and CIP tasks.

In addition, the RCB is conducts training for personnel of CI operators. Workshops for public agencies are organised in cooperation with the private sector and regular conferences on cyber security offer information on good practices and new technical applications.

The Research and Academic Computer Network (NASK)

The Research and Academic Computer Network (NASK) is a Polish data network operator and has the status of a research & development organisation. It is maintaining the CERT Polska.

CERT.gov.PL

CERT.gov.PL is the main CSIRT for public agencies, but also offers its services to CI operators based on formal agreements. Its tasks are to publish security notifications, to detect incidents in public networks and to resolve and analyse incidents. It was established in 2008. The CERT.GOV.PL team is a part of the IT Security Department at the Polish Internal Security Agency.

CERT Polska

CERT Polska was the first CSIRT in Poland and is part of the NASK. It holds special expertise in the analysis and research of security incidents and provides information on threats and incidents. Information is available on a database that can be used by private and public entities.

The Ministry of Administration and Digitization

The Ministry of Administration and Digitization is responsible for critical infrastructure related to "tele-information network systems". CI operators of the telecommunications sector have to report security incidents to the Office for Electronic Communications. The Office will then report to the Ministry of Administration and Digitization.

In case of an emergency related to CII, the Ministry of Administration and Digitization will take a leading role in advising other Ministries and the Council of Ministers in crisis situations.

Relevant Framework Papers and Regulations

In Poland the issue of CIIP is covered under the broader scope of CIP. This means that official documents make no distinction between Critical Infrastructure and Critical Information Infrastructure.

The **Cyberspace Protection Policy of the Republic of Poland (NCSS)** was published on the 25th of June 2013. It outlines objectives for cyberspace protection as well as concrete actions and measures. The policy is only addressed to the public administration.

The **National Critical Infrastructure Protection Programme (NCIPP)** under provision of the **Crisis Management Act** has been adopted by the Council of Ministers on the 26th of March 2013. It outlines a series of actions with the purpose of improving the security and resilience of critical infrastructure in Poland. The program is addressed primarily to the public administration sector and to CI operators.

Sources

(ENISA, KPMG 2015)

(Government Centre for Security (RCB) 2007)

(Government Centre for Security (RCB) 2013)

(Ministry of Administration and Digitisation, Internal Security Agency 2013)

(Research and Academic Computer Network (NASK) 2015)

1.15 Sweden

Leading Authority

On a national level, the **Swedish Civil Contingencies Agency (MSB)** is the main authority for contingencies.

TYPE	ACTOR OR INSTITUTION

Leading	• Swedish Civil Contingencies Agency (MSB)
	• Various sector-specific authorities (with varying mandates):
	  ○ Swedish Post and Telecom Agency (PTS)
	  ○ Swedish National Defence Radio Establishment (FRA)
	  ○ Swedish Security Service (Säpo) and the Swedish Criminal
	  ○ Investigation Service (RKP)
	  ○ Swedish Defence Materiel Administration (FMV)/ Swedish

	○ Certification Body for IT Security (CSEC) ○ Swedish Armed Forces (FM)/Military Intelligence and Security Service (MUST)
Operational	• CERT-SE (part of the MSB)
Network/Forum/Council	• Cooperation Group for Information Security (SAMFI)
Private	• National Telecommunications Coordination Group (NTSG)

Management Structure

Sweden uses a system perspective, which means that work on the protection of "Vital Societal Functions" (VSF) and CI is carried out in cooperation with the private sector and across all societal sectors.

Public entities (municipalities, councils, national authorities) are responsible for the identification of VSF & CI as well as the coordination and support of VSF & CI operators. Operators of VSF & CI are responsible for the implementation of safety measures and have to report completed actions to the responsible entity. The final definition of the general roles and responsibilities for crisis management is still a work in progress.

Emergency preparedness in Sweden is based on the principle of responsibility. The responsibilities during normal conditions are the same as during emergencies, which means that every agency is responsible for the emergency preparedness in its own area of expertise.

The MSB has the right to issue regulations for government authorities in the area of information security. Issuing legislation with obligations for companies within specific sectors is the responsibility of the respective public authorities.

The MSB is tasked with coordinating the efforts of the various agencies. This is realised through the Cooperation Group for Information Security (SAMFI). SAMFI is a cooperative network of different relevant sector-specific authorities with societal information security responsibilities.

Institutionalised cooperation mechanisms or schemes between the public and private sectors are not yet established. Cooperation with the private sector is realised through usual communication channels between public authorities and private companies. The private sector has organised itself with the establishment of the National Telecommunications Coordination Group (NTSG) (see "Roles and responsibilities" for details).

Roles and Responsibilities

Swedish Civil Contingencies Agency (MSB)

The MSB's role in general is to develop and monitor the protection of VSF & CI. More specifically, the MSB provides advice and support on prevention to public and private entities. It also takes a coordinating role for work on national societal information security and during periods of heightened alert.

The agency has also been commissioned to conduct a national risk assessment which began in 2011. 27 particularly serious (national) events have been identified and eleven scenarios based on a selection of these events have been developed.

In the field of information security, its tasks are:

- Support and coordinate societal information security as well as analyse and assess global developments in the field.
- Provide advice and support, in relation to preventive work, to other authorities, municipalities, county councils, the private sector and organisations.
- Report to the government on the conditions in the information security field that can give rise to a need for measures on different levels and within different areas of society.
- Shall be responsible for a Swedish national service tasked with supporting society in its efforts to prevent and manage IT incidents.
- Administer the national strategy and action plan for information security.
- Coordinate the work of civil authorities with secure cryptographic services.
- Support media companies with their preparedness planning.

Furthermore, the MSB has development training and education programmes for organisations, public authorities and individuals.

The MSB has the right to issue regulations for government authorities in the area of information security, but not for companies within specific sectors. Also, The MSB does not have the authority to investigate cases of non-compliance nor to issue binding instructions to public administrations or market operators.

Cooperation Group for Information Security (SAMFI)

The purpose of SAMFI is to "guarantee societal information assets" through the exchange of information and cooperation between government agencies. Representatives from the different authorities meet at SAMFI around six times a year to discuss current work and issues, such as strategies and legislation, exercises and training or technical issues and standardization. The cooperation group is funded by the contributions of the different authorities.

Swedish Post and Telecom Authority (PTS)

The PTS holds responsibility for the telecommunications sector. Based on secondary legislation, the PTS can obligate operators to implement certain technical or organisational security measures. Furthermore, Telecommunications companies have to inform the PTS about security incidents

CERT-SE

CERT-SE is the national and governmental CSIRT in Sweden. It is responsible for advising governmental authorities and companies as well as coordinating incident responses. The CSIRT is part of the MSB.

National Telecommunications Coordination Group (NTSG)

The NTSG is a voluntary cooperation platform of the telecommunications sector. Members may assist each other in dealing with emergencies or extraordinary events.

Relevant Framework Papers and Regulations

Sweden adopted the "**Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure**" in July 2014. It was published by the Swedish Civil Contingencies Agency (MSB).

Other relevant framework papers include:

Swedish Civil Contingencies Agency's **Regulations on Government Agencies' Information Security 2009**: Contains obligations for public authorities in the area of information security.

National Risk Assessment 2012: The report includes the results of the national risk assessment conducted by the MSB.

Various sector-specific secondary legislation, such as the Electronic Communications Code that contains obligations for companies of the telecommunications sector.

Sources

(ENISA, KPMG (2015l))

(Swedish Civil Contingencies Agency (MSB) 2013)

(Swedish Civil Contingencies Agency (MSB) 2014)

(Swedish Civil Contingencies Agency (MSB) 2015a)

(Swedish Civil Contingencies Agency (MSB) 2015b)

(Swedish Post and Telecom Authority (PTS) 2015)

1.16 Switzerland

Leading Authority

The **"Reporting and Analysis Centre for Information Assurance" (MELANI)** is the national information exchange hub between the private and public sector. It can be described as the main authority for CIIP in Switzerland during a cyber incident.

TYPE	ACTOR OR INSTITUTION
Leading	• Reporting and Analysis Centre for Information Assurance (MELANI)
Ministerial	• Federal Department of Finance

Operational	• GovCERT (part of MELANI)
	• Sector-specific CSIRTs
	• Sector-specific regulators, for example:
	  ○ FINMA – independent supervisory authority and financial-markets regulator
	  ○ Federal Office of Communication (OFCOM)

Private/PPPs	• Swiss Cyber Experts (SCE)

Management Structure

In general, Switzerland follows a decentralised approach, which is based on the principle of subsidiarity. Hence, a strong central authority with strong competencies would be contrary to this principle. Much emphasis is placed on self-responsibility and decentralized authority, where possible. It is believed that the critical subsectors know their own processes and systems best and should therefore be in charge of identifying the cyber-risks for these processes and systems; they should also be in charge of deciding on appropriate security measures. The government supports this process where it can. Accordingly, CI operators are responsible for their own security, but the state offers subsidiary support.

No public agency is authorized to issue binding instructions to the operators of CII across all sectors in Switzerland. MELANI is mandated to only support other agencies or operators, but has not regulatory function and cannot force the CII to either report a cyber incident or force the implementation of security measures. However, some regulators in sectors such as banking (FINMA – Switzerland's independent financial-markets regulator) or the telecommunication sector (Federal Office of Communication – OFCOM) can impose sanctions on companies, if those do not comply with sector-specific regulations or standards. In addition MELANI does not want a mandatory disclosure of cyber incidents, as it is believed that incident reporting and cooperation in general should be voluntary and based on a high trust-level.

MELANI fosters Public-Private cooperation and supports the voluntary information exchange with CI operators. In addition, the cooperation with the private sector is realised through the Swiss Cyber Experts (SCE) (see below).

Roles and Responsibilities

Reporting and Analysis Centre for Information Assurance (MELANI)

MELANI is responsible for providing subsidiary support for information assurance within the critical infrastructure. It acts as a centralised information hub by receiving information on cyber incidents and threats from private operators and public agencies. It then evaluates this information before passing the results on to the operators of CII. Often, the information shared by MELANI comes from publically unavailable sources such as Intelligence Services, Police Entities or technical analysis. MELANI's constituency consists of more than 100 enterprises that operate critical infrastructures.

MELANI follows a central (operational support)-decentralised (responsibility) approach:

1. Central: MELANI is the central information sharing hub for its Closed Constituency of CI operators from all relevant sectors. It centrally receives information from agencies and operators, identifies, analyses, evaluates and contextualises this information and then distributes it. MELANI consists of two chambers:
   - The strategic part belongs to the Federal IT Steering Unit (FITSU) of the Federal Department of Finance (FDF). Switzerland's GovCERT.ch is attached to the strategic part of MELANI.
   - The operational part, the so called Operation Information Centre (OIC) belongs to the Federal Department of Defence (DDPS).
2. De-central: responsibility lies with the members of the closed user group. MELANI works closely together with the members of this "closed user group", which consists of selected operators of CII (from sectors such as banking, telecommunications, energy, etc.). The work and the shared information within this group is confidential. Furthermore, cooperation with the operators of CII is fostered through sector-specific workshops.

Switzerland has a GovCERT.ch, which is the Computer Emergency Response Team (GovCERT.ch) of the Swiss government and the official national CSIRT of Switzerland and part of MELANI. They are in charge of cyber incidents. Should the cyber incident be too much to handle the Swiss Cyber Experts can be asked toassist.

In case of CII-related security incidents, MELANI and other relevant agencies will form a crisis management steering group.

Swiss Cyber Experts (SCE)

The Swiss Cyber Experts (SCE) is a Public-Private Partnership and was established on the basis of a cooperation agreement with MELANI. The SCE allow privately managed companies and government agencies to fall back on highly specialised experts in the event of a grave cyber incident. The goal of the public private partnership is to quickly deliver a diagnosis and thus the basis for the problem solution in case of severe cyber incidents that go beyond the resources of the victims and/or MELANI. It consists of a pool of highly qualified experts in the ICT industry, the private and public sector and science. It also guarantees the protection of the client's anonymity. It is a trustworthy platform that allows the exchange of experiences and the sharing of important insights about cyber threats.

The goal of the SCE is to provide a quick analysis of security incidents and to assist MELANI in its tasks. Any company can apply for membership, but the SCE tries to equally represent every sector. MELANI will always act as the Single Point of Contact and calls the SCE when incidents occur that cannot be handled by the MELANI staff.

Relevant Framework Papers and Regulations

The Federal Council ratified the **creation of the Reporting and Analysis Centre for Information Assurance MELANI** in 2003. MELANI is operational since October 1st 2004.

The Federal Council ratified the **National Strategy for the Protection of Switzerland against Cyber Risks (NCS)** in 2012. The protection of critical information infrastructure is an essential part of the strategy.

The Swiss national strategy for CIP is named **The Federal Council's Strategy for Critical Infrastructure Protection 2012 (SKI)**. It defines the critical sectors, which in turn are the basis for the CII in the NCS.

In order to guarantee the implementation of the NCS, the Federal Council ratified an **implementation plan** in 2013.

Sources:

(ENISA 2015)

(ENISA, KPMG 2015)

(Federal Department of Defense, People's Protection and Sports, DDPS, 2012)

List of References

General

ENISA (2014): Methodologies for the identification of Critical Information Infrastructure assets and services - Annex A. Draft, V1.0, checked on 04.06.15.

ENISA (2015): How is CIIP addressed in National Cyber Security Strategies in the EU28. Draft v0.3. Edited by ENISA, checked on 04.06.15.

Kaska, Kadri; Trinberg, Lorena (2015): Regulating Cross-Border Dependencies of Critical Information Infrastructure. Edited by NATO Cooperative Cyber Defence Centre of Excellence, checked on 04.06.15.

Austria

Computer Emergency Response Team Austria (2015): Österreichische Strategie für Cyber Sicherheit - CERT.at. Available online at https://www.cert.at/reports/report_2014_chap06/content.html, updated on 29.05.15, checked on 04.06.15.

ENISA (2015): ENISA Online Survey: Austria, checked on 04.06.15.

ENISA; KPMG (2015): CIIP in Austria. Interview with Timo Mischitz-Schilcher. Andreas Reichard. Phone conference.

Federal Chancellery of the Republic of Austria (2012): National ICT Security Strategy Austria, checked on 04.06.15.

Federal Chancellery of the Republic of Austria (2013): Austrian Cyber Security Strategy, checked on 04.06.15.

Federal Chancellery of the Republic of Austria (2014): Austrian Program for Critical Infrastructure Protection, checked on 04.06.15.

Federal Chancellery of the Republic of Austria; Ministry of Finance (Eds.) (2015): IKT-Sicherheitsportal - IT-Notfall- und Krisenübungen. Available online at https://www.onlinesicherheit.gv.at/nationale_sicherheitsinitiativen/it_notfall_und_krisenuebungen/71384.html, checked on 04.06.15.

GovCERT Austria (2014): National Responsibilities - GovCERT.gv.at. Available online at http://www.govcert.gv.at/home/scope/content_en.html, updated on 17.03.14, checked on 04.06.15.

Cyprus

ENISA; KPMG (2015): CIIP in Cyprus. Interview with Antonis Antoniades. Phone conference.

Office of the Commissioner of Electronic Communications & Postal Regulation (OCECPR) (2012): Cybersecurity Strategy of the Republic of Cyprus. Network and Information Security and Protection of Critical Information Infrastructures.

Czech Republic

ENISA (2015): ENISA Online Survey: Czech Republic, checked on 04.06.15.

ENISA; KPMG (2015): CIIP in the Czech Republic. Interview with Daniel Bagge. Phone conference.

National Security Authority (2015a): Action Plan for the National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020, checked on 04.06.15.

National Security Authority (2015b): National Cyber Security Strategy. Available online at https://www.govcert.cz/en/info/events/the-government-of-the-czech-republic-adopted-the-national-cyber-security-strategy-for-the-upcoming-five-years/, checked on 03.06.15.

Parliament of the Czech Republic (2014): Act No. 181 On Cyber Security and Change of Related Acts. Act on Cyber Security´. Available online at http://www.govcert.cz/en/legislation/legislation/, checked on 03.06.15.

Parliament of the Czech Republic (2015): Regulation No 316/2014 Coll. on Security Controls, Cyber Security Incidents, Reactive Actions and on the Determination of the Requirements for the Applications in the Field of Cyber Security. Regulation on Cyber Security´. Available online at http://www.govcert.cz/en/legislation/legislation/, checked on 04.06.15.

Denmark

Centre for Cyber Security (2015): The Danish Cyber and Information Security Strategy.

Danish Defence Intelligence Service; 30, Kastellet; DK-2100; Copenhagen (2014): Organization Chart (DDIS). Edited by Danish Defence Intelligence Service. Available online at https://fe-ddis.dk/eng/About-DDIS/Pages/Organization.aspx, checked on 15.07.15.

ENISA; KPMG (2015): CIIP in Denmark. Interview with Peter Knøster. Phone conference.

Government of Denmark (2012): Danish Defence Agreement 2013-2017.

Government of Denmark (2014): National Cyber and Information Security Strategy.

Estonia

ENISA (2015): ENISA Online Survey: Estonia, checked on 04.06.15.

ENISA; KPMG (05.06.15): CIIP in Estonia. Interview with Urmo Sutermäe. Phone conference.

Government of Estonia (2008): Cyber Security Strategy 2014-2017, checked on 08.06.15.

Government of Estonia (2009): Emergency Act, checked on 08.06.15.

Government of Estonia (2013): Security measures for information systems of vital services and related information assets.

Information System Authority (2012): IT Baseline Security System ISKE. Available online at https://www.ria.ee/iske-en, checked on 08.06.15.

Finland

ENISA (2015): ENISA Online Survey: Finland, checked on 04.06.15.

ENISA; KPMG (2015): CIIP in Finland. Interview with Kievari Timo. Phone conference.

Government of Finland (2006): The Strategy for securing the functions vital to society.

Ministry of Defence (2010): The Security Strategy for Society.

Ministry of Justice, Finland (2003): Emergency Powers Act 2003, checked on 08.06.15.

Ministry of Transport and Communications, Finland (2014): Information Society Code.

National Emergency Supply Agency (2013): Funding and Legislation | Organisation | National Emergency Supply Agency |. Available online at http://www.nesa.fi/organisation/funding-and-legislation/, checked on 08.06.15.

Prime Minister's Office Finland (2015): Strategic Programme of Prime Minister Juha Sipilä's Government. Available online at http://vnk.fi/documents/10616/1095776/Ratkaisujen+Suomi_EN.pdf/c2f3123a-d891-4451-884a-a8cb6c747ddd?version=1.0., checked on 24.09.15.

Secretariat of the Security Committee (2013): Finland's Cyber Security Strategy.

The National Emergency Supply Agency (2013): National Emergency Supply Agency | Organisation | National Emergency Supply Agency |. Available online at http://www.nesa.fi/organisation/national-emergency-supply-agency/, checked on 08.06.15.

France

ENISA; KPMG (2015): CIIP in France. Interview with Yann Salamon. Phone conference.

French Ministry of Defence (2013): French White Paper Defence and National Security.

French Network and Information Security Agency (ANSSI) (2011): Information systems defence and security strategy.

French Network and Information Security Agency (ANSSI) (2015a): Guide d'hygiène informatique | Agence nationale de la sécurité des systèmes d'information. Available online at http://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/, updated on 09.07.15, checked on 16.07.15.

French Network and Information Security Agency (ANSSI) (2015b): Overview of the French cybersecurity approach. Presentation of ANSSI.

French Senate (2013): Military Programming Law (LPM).

Germany

Federal Office for Information Security (2015a): ACS: Informationen zur Allianz für Cyber-Sicherheit. Available online at https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Ueber_uns/ueber_uns.html, checked on 07.07.15.

Federal Office for Information Security (2015b): BSI: CERT-Bund. Available online at https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/Cert-Bund/cert-bund_node.html, checked on 07.07.15.

Federal Office for Information Security (2015c): Completed interview questionnaire.

Federal Office for Information Security, Federal Office of Civil Protection and Disaster Assistance (2013a): Partners in Critical Infrastructure Protection. Available online at http://www.kritis.bund.de/SubSites/Kritis/EN/partners/partners_node.html, checked on 07.07.15.

Federal Office for Information Security, Federal Office of Civil Protection and Disaster Assistance (2013b): UP KRITIS. Available online at

http://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/UPK/upk_node.html, updated on 07.07.15, checked on 07.07.15.

Hungary

ENISA; KPMG (2015): CIIP in Hungary. Interview with Anita Tikos, Illes Solt, Dr. Sápi Gergely, Vereckei Béla Ferenc. Phone conference.

Government of Hungary (2003): Act C of 2003 on Electronic Communications.

Government of Hungary (2012): Act CLXVI of 2012 on the assignment and the protection of the critical infrastructures of Hungary.

Government of Hungary (2013a): National Cyber Security Strategy.

Government of Hungary (2013b): Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies.

Ireland

Department of Defence (2015): Home // Office of Emergency Planning. Edited by Office of Emergency Planning. Available online at http://www.emergencyplanning.ie/_home.aspx, checked on 05.06.15.

ENISA (2015): ENISA Online Survey: Ireland, checked on 04.06.15.

ENISA; KPMG (2015): CIIP in Ireland. Phone conference.

Italy

ENISA (2015): ENISA Online Survey: Italy, checked on 11.06.15.

ENISA; KPMG (2015): CIIP in Italy. Interview with Sandro Mari. Phone conference.

Ministry of Internal Affair (2008): Decree of the Minister of the Interior on the Identification of CII of national interest, revised Decree of the Ministry of Internal Affair.

Presidency of the Council of Ministers (2010): National Organisation of Crisis Management. Decree of the President of the Council of Ministers.

Presidency of the Council of Ministers (2011): Legislative Decree 11 April 2011, n. 61108.

Presidency of the Council of Ministers (2013a): National Strategic Framework for Cyberspace Security.

Presidency of the Council of Ministers (2013b): The National Plan for Cyberspace Protection and ICT Security.

Presidency of the Council of Ministers (2013c): Legislative Decree no 259. Electronic Communications Code.

Latvia

Elīna Neimane (2015): Completed interview questionnaire.

Netherlands

KPMG (2015): CIIP in Netherlands. Interview with Barend Sluijter. Phone conference.

Ministry of Interior (2009): List of Critical Infrastructure 2009.

Ministry of Interior (2015): List of Critical Infrastructure 2015.

National Coordinator for Security and Counterterrorism (2013): National Cyber Security Strategy 2. From awareness to capability.

National Cyber Security Centre (2015): Cooperation. Available online at https://www.ncsc.nl/english, checked on 11.08.15.

Poland

ENISA; KPMG (2015): CIIP in Poland. Interview with Krzysztof Silicki, Maciej Pyznar, Magdalena Wrzosek. Phone conference.

Government Centre for Security (RCB) (2007): Act on Crisis Management.

Government Centre for Security (RCB) (2013): National Critical Infrastructure Protection Program.

Ministry of Administration and Digitisation; Internal Security Agency (Eds.) (2013): Cyberspace Protection Policy of the Republic Poland.

Research and Academic Computer Network (NASK) (2015): NASK SENSE OF TELECOMMUNICATIONS - Who we are. Available online at https://www.nask.pl/run/n/Who_we_are, updated on 09.07.15, checked on 16.07.15.

Sweden

ENISA; KPMG (2015): CIIP in Sweden. Interview with Peter Wallström. Phone conference.

Swedish Civil Contingencies Agency (MSB) (2013): Swedish National Risk Assessment 2012.

Swedish Civil Contingencies Agency (MSB) (2014): Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure.

Swedish Civil Contingencies Agency (MSB) (2015a): Cooperation Group for Information Security (SAMFI). Available online at http://rib.msb.se/Filer/pdf/26177.pdf, checked on 29.06.15.

Swedish Civil Contingencies Agency (MSB) (2015b): Msb.se - Myndigheten för samhällsskydd och beredskap. Available online at https://www.msb.se/en/, checked on 29.06.15.

Swedish Post and Telecom Authority (PTS) (2015): PTS - About PTS. Post- och telestyrelsen, PTS. Available online at http://www.pts.se/en-GB/About-PTS/, checked on 29.06.15.

Switzerland

ENISA (2015): ENISA Online Survey: Switzerland, checked on 04.06.15.

ENISA; KPMG (2015): CIIP in Switzerland. Interview with Dr. Stefanie Frey. Phone conference.

Federal Department of Defence, People's Protection and Sports, DDPS, (2012): National strategy for Switzerland's protection against cyber risks.

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

Catalogue Number **TP-04-15-822-EN-N**

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-144-1
doi: 10.2824/028519