Critical Information Infrastructures Protection approaches in EU

Executive Summary

An increasing number of countries in the European Union have developed a National Cyber Security Strategy (NCSS) a key policy document, which includes the measure a state should take to tackle cyber risks that could impact the economic and social benefits. Twenty (20) European Union Member States have published a NCSS, some of them in initial implementation stage and some are now into the second or third implementation round.

Critical information infrastructure protection (CIIP) is a key priority in most of these strategies (15 out of 20 have an objective to protect the national critical infrastructure[1]). However the approach each country takes on the topic is diverse and according to their national requirements, i.e. some countries have developed specific CIIP Action Plans drawn by legislation, some others have created working groups per critical sector to focus on tackling the CIIP issues, others include CIIP in the mandate of the body responsible of national cyber security etc. This diversity in the governance model, the bodies involved and the objectives' prioritisation constitutes the scope of this short paper.

The goal of this short paper is to present the different approaches the MS follow on the governance of Critical Information Infrastructures, as described under the NCSS. This information will be helpful for the Member States that are still working on designing and implementing their national strategy and include, in a brief way, the priorities and governance models followed. This paper would also be of assistance to the private sector to better understand their role in the implementation of the provisions of the national strategy.

ENISA has been working on the field of NCSS since 2012, when introduced the notion of "the lifecycle of a NCSS". ENISA has taken stock of the cyber security activities in Europe, has analysed trends and resulted into recommendations for the countries to design, implement and evaluate a strategy. Several reports have been published[2] to support the Member States in following the steps of that lifecycle. In 2013, ENISA launched the NCSS working group; representatives from 14 Member States and 1 EFTA country collaborate on topics related to the cyber security status in their country, supporting other MSs that haven't yet implemented a strategy to accelerate the process. This year the WG decided to focus on the specific objectives of a NCSS and provide information on each country's approach; one of the first topics to present is the CIIP perspective as a component of NCSS.

[1] Source ENISA Evaluation framework for NCSS: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1

[2] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss

1 Introduction

Many European Union Member States have published or are in the process of publishing an NCSS. Of these, several have also updated their strategies since their first edition. National Cyber Security Strategies aim to ensure that Member States are prepared to face serious risks, are aware of their consequences, and are equipped to appropriately respond to breaches in the network and information system. However, it is not always clear if and how the effectiveness of these strategies is evaluated. Evaluation can be interpreted as a tool to assess if and how well the expected objectives have been achieved and whether the costs involved were justified, given the changes which have been achieved.
The European Commission understands that "there are still gaps across the EU, notably in terms of national capabilities, coordination in cases of incidents spanning across borders, and in terms of private sector involvement and preparedness"[4]. The 2013 EU Cyber Security Strategy (EUCSS) asks ENISA to "encourage good practice in information and network security" to assist and support Member States in developing strong national cyber resilience capabilities, notably by building expertise on security and resilience of industrial control systems, transport and energy infrastructure.

One of the most important aspects covered in the national strategies is the governance of critical information infrastructures; currently 18 out of 20 Member States' strategies include CIIP as an objective (the other two have specific regulation). The scope of this short paper is to present in brief how the MS perceive critical information infrastructure so as to provide advice to countries that are now working on designing their strategy, or are updating into a next version.

2 Country reports in CIIP

This section includes the summarized approach each country takes on CIIP. More it explains what is the structure and the governance model in each MS, who are the stakeholders involved and under what capacity, is there the presence and nature of relative legal basis etc. Below you can read the summary report from 15 EU MSs.

2.1 Austria (AT)

In 04/11/2014 the Austrian Federal Government decided on a new program for the protection of critical infrastructure (CIP) called the 'APCIP (Austrian Program for Critical Infrastructure Protection) Masterplan 2014'. This is based on the 2008 program, which does not include distinct sections for cyber security and CIIP; both are however relevant parts of this program and are included in all of its activities (public and private). The focal point of this Masterplan lies in identifying Strategically Important Organizations (SIOs) that operate CIs and engaging them in a security partnership.

The overall process of implementing the Masterplan in Austria is overseen by the Federal Chancellery and the Federal Ministry of Interior. It is supported by a consortium consisting of representatives from the ministries, the Austrian states and various groups of interest. Collaboration is based on a voluntary self-commitment. This security partnership is to be regulated by legally non-binding cooperation agreements. Legal action is to be taken only in case the voluntary measures prove to be ineffective. The responsibilities in the form of tasks and capacities of the public agencies are regulator under the Federal Security Policy Act and include activities such as identification of SIOs, assisting organizations to create a security architecture, ensure physical protection and organization of cyber security exercises.

The Cyber Security Platform (CSP) was established on 17/03/2015. Its members are mainly CII operators and other companies and organizations of strategic importance from sectors such as industry, traffic, finance, health and the public sector.

Responsibilities of these SIOs are:

- Creation of an extensive security architecture (including risk-, crisis- and security management) to enhance resilience, particularly against cyber threats
- Nomination of Points of Contact (POCs)
- Implementation of common security standards (including standards against cyber threats, as mentioned in the Austrian Cyber Security Strategy)
- Notification about incidents (including cyber incidents, as mentioned in the Austrian Cyber Security Strategy-ACSS)
- Participation in exercises (including cyber exercises)
  The ACSS includes the protection of CI by also linking to APCIP and naming resilience a top priority for future planning measures. Some of the measure proposed are cyber crisis management plan, appointment of an information security officer, definition of standards, incident reporting. Both APCIP and ACSS have action plans in order to implement the corresponding measures in a timely, coordinated way.

In a nutshell, in Austria the governance model followed is based on a partnership between authorities and CII operators on voluntary self-engagement. Identification of assets is under the public authorities and operators need to support protection of them by following specific security measures. Only in case these measures are inadequate, legal implications may follow.

2.2 Cyprus (CY)

Cyprus has recognised that the protection of CIIs is vital and of extreme importance to the functions of the society since they have penetrated in almost every part of citizens' lives. The Cyber Security Strategy of Cyprus () is focused on the protection of CIIs, resulting into a set of 17 specific actions further described in the strategy document.

To prevent threats and protect critical infrastructures, Cyprus has a number of priority actions that have been identified. These are:

- coordination of governmental stakeholders to ensure correct and efficient cooperation,
- creation of a comprehensive legal framework by the competent authorities of the state, that covers all aspects of network and information security, including cybercrime and the protection of personal data,
- formulation of technical and organisational measures and procedures to harden the security of relevant hardware, software and physical spaces,
- development of the necessary skills, training and awareness in security topics, for those that are directly involved and also for the public,
- productive collaboration between the public and private sector, on both the national and international level,
- creation or adaptation of the necessary structures and instruments within the competent authorities and the more generally the Cyprus government, to secure the demands and capabilities of immediate incident response.

Legislation in the Republic of Cyprus already covers a large number of areas relating to network and information security, as well as cybercrime (and other electronic crimes). However, it is still considered necessary to identify all relevant laws in Cyprus and to update them.

There are a number of authorities within the Republic of Cyprus that are active in the security of networks, services, information technology systems and information itself, in addition to having direct or indirect input on critical security matters. The competent/related authorities that are involved at this stage are Office of the Commissioner of Electronic Communications and Postal Regulation (OCECPR), the Department of Information Technology Services (DITS), the Cyprus Police, the National Guard General Staff, the National Security Authority, the Central Intelligence Service, the Office of the Commissioner for Personal Data Protection, the Ministry of Communications and Works (MCW), the Department of Electronic Communications (DEC), the Civil Defence Force and the Cyprus Fire Service.

2.3 Czech Republic (CZ)

Special attention is given to Critical information infrastructure protection in new NCSS of the Czech Republic for the period from 2015 to 2020. NCSS goes hand by hand with the new Czech legislation in the area of cyber security, called "Act on Cyber Security" which has been recently adopted and became effective on 1st January 2015 and this new law legally obliges all CII entities to take security measures (standardization), to report cyber security incidents and to take countermeasures, it means response to incidents.

One of the visions of NCSS represents effectively secured individual elements of a critical information infrastructure and the overall security of networks and cyberspace used by Czech population, which are essential to the latter's Czech economic and social interests. Protection of CII also embodies one of the main aims of the NCSS.

Besides the strategy, the Czech Republic intensively works on the update of the Action Plan that will define specific steps for their fulfilment of the goals in NCSS related to CIIP.

Czech Republic has set in the new NCSS e.g. to:

- Pursue a continuous analysis and control of CII security in the Czech Republic based on a clearly defined protocol.
- Enhance, on a continuous basis, the CII and IIS networks' resistance, integrity and trustworthiness.
- Share information among the state and CII subjects.
- Perform regular testing of and detect errors and vulnerabilities in information systems and networks used by the state, based on CII penetration testing principles.
  Czech Republic does not have a lack of direct government control over CII like other countries. In the Czech Republic, the National Security Authority (NSA CZE) is the body responsible for cyber security, the only national authority in this field and it leads coordination across government departments and agencies. For this purpose NSA CZE has recently established a specialized department, the National Cyber Security Centre (NCSC) and this department is responsible for mapping and identifying of services to be part of CII as well as supervising the fulfilment of obligations under the Act on Cyber Security for the entities managing elements of CII.

In short, NCSC operates as the centre of the protection for the state and CII as well as a body for critical management in case of a massive attack on a national scope.

2.4 Estonia (EE)

The Estonian approach to critical information infrastructure protection builds upon the concept of "vital services". These are services that are essential for the maintenance of vital societal functions, healthcare, security and people's economic and social well-being. 43 vital services are listed in the Emergency Act (adopted in 2009)[3] and grouped in sectors[4].

The Emergency Act imposes duties on authorities to maintain the sustainability of vital services and on service providers to provide vital services. The specific regulatory measures were defined by Government in 2013 in "Security Measures for Vital Service Information Systems and Related Information Assets"[5]. These measures were developed on the basis of the results of a critical information infrastructure mapping project conducted by Information System Authority in 2010, which identified the dependencies of vital services on information systems.

While the key objective of the Cyber Security Strategy of 2008-2013 was raising awareness and developing requirements for strengthening the security of critical infrastructures, the second version – Cyber Security Strategy 2014-20176 – focuses on managing cross-dependencies between vital services as well as cross-border interdependencies. The goal is to keep up to date the information relating to dependencies on critical services provided from outside Estonia, evaluate the extent of their impact on the functioning of services, and systematically reduce associated risks.

According to the Emergency Act, the providers of vital service can be both state or local government authorities and legal persons, depending on their actual supply of any of the 43 vital services listed in the Act.

The vital service providers have the following obligations:

- Preparing a continuous operation risk assessment (at least once in every two years);
- Preparing a continuous operation plan for the vital service provided (at least once in every two years);
- Immediately notifying events which significantly disturb the continuous operation of the vital service, or an impending risk of such incident; and
- Subjecting themselves to the supervision of competent authorities over the continuous operation of the vital service. Guidelines for implementing these obligations are defined in secondary legislation.

Nine government ministries and public bodies are assigned by the Emergency Act with responsibilities in managing the continuous operation of the vital services. Ministry of the Interior bears the overall national coordinator role. The obligations of the nine "vital service organizing authorities" include coordination of vital service operation, advising vital service providers, supervision over ensuring the continuous operation of vital services; and regular reporting to the national coordinator (Ministry of the Interior). The Act authorises these organizing authorities to issue secondary legislation for establishing the description of the vital service and establishing continuous operation requirements for the vital services.

The supervisory body over compliance with electronic security requirements of provision of vital service is the Information System Authority (RIA) with the mandate of a law enforcement authority as defined in the Law

[3] The Estonian Emergency Act is available at: https://www.riigiteataja.ee/en/eli/517122014005/consolide

[4] These sectors are: justice system; utilities, transport, and communications; public security and public order; medical services; environmental services; food safety; financial services; government and public administration

[5] https://www.ria.ee/public/KIIK/Security_measures_for_information_systems_of_vital_services_and_related_information_assets.pdf

[6] https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf

Enforcement Act.7 RIA is responsible for developing an emergency risk assessment to address the risk of a vital service-relevant cyber incident, and for preparing the national emergency plan for large scale cyber incidents. In case of a large scale cyber incident, the Information System Authority also leads incident response activities.

2.5 Finland (FI)

The Finnish Cyber Security Strategy has been adopted as a government resolution in December 24th 2013. The strategy sets an objective to maintain and improve the abilities of businesses and organizations critical to the vital functions of society as regards detecting and repelling cyber threats and disturbances that jeopardise any vital function, and their recovery capabilities as part of the continuity management of the business community.

In their security and contingency plans the businesses and organisations critical to the vital functions of society will comprehensively take into account the cyber threat factors related to the vital functions, and maintain the required capabilities to protect themselves. The goal is to detect and identify any disturbances to the vital functions appearing in risk assessments and to respond to them in a manner which minimises their detrimental effects. The key actors will improve their tolerance, including contingency planning and exercises, so as to be able to operate under cyber-attacks. The Finnish National Emergency Supply Agency will support this activity through reports, instructions and training.

The Finnish government emphasized in its cyber security strategy that cyber security is not meant to be a legal concept the adoption of which would lead to granting new competences to authorities or other official bodies. Government also stated that cyber security arrangements follow the division of duties between the authorities, businesses and organisations, in accordance with statutes and agreed cooperation. According to the strategy most of the critical infrastructure in society is in private business ownership. This is why cyber know-how and expertise, as well as services and protection measures are for the most part provided by companies.

The strategy states that national cyber security legislation must provide a favorable environment for the development of business activities. In many cases the Finnish national legislation aims to protect certain vital services and their security rather than critical information infrastructure itself. It is important to bear in mind, that there is a quantity of such sector specific EU legislation and national legislation in place which obliges different operators to do risk management, take specific security measures and notify security incidents. Such legislation obliges the service providers for example in the fields of energy, transport, finance, healthcare, and communications and so on. These provisions oblige service providers whether they utilize information and communication technology in their businesses or not.

In some sectors there is specific regulation on how service providers must tackle the risks related to the use of ICT in their service production. In this respect the competitiveness aspects need to be considered, as well as ensuring that administrative burden is not unreasonably increased.

In a nutshell, Finland has made all provisions necessary to protect critical infrastructures before the cyber security strategy was published. The strategy has a vision that citizens, authorities and businesses can effectively utilize a safe cyber domain and the competence arising from cyber security measures, both nationally and internationally.

[7] https://www.riigiteataja.ee/en/eli/522082014007/consolide

2.6 France (FR)

In France, identification of critical information infrastructures is derived from the identification of CIP, which follows the doctrine of defence and national security approach focusing on "operators of vital importance": "an operator whose unavailability could strongly threaten the economical or military potential, the security or resilience of the nation". For CIP (Secteurs d'Activité d'Importance Vitale, SAIV in French), the relevant provisions are included in the Code of Defence, which constitutes the legislative and regulatory framework for the national security system.

12 critical sectors are identified in this framework (the precise list of operators is classified):

- Civil activities
- Judicial activities
- Military activities
- Food
- Electronic, audiovisual and information communications
- Energy
- Space and research
- Finance
- Water management
- Industry
- Health
- Transportation

The French White Paper (29 April 2013) [8] on National Security and Defence set as priorities, amongst others, the protection of critical information infrastructures.

The Agence Nationale de la Securité des Systèmes d'Information (ANSSI), created by the decree 2009-834 (7 July 2009)[9], is a service with national responsibility and jurisdiction which reports to the General Secretariat for Defence and National Security. On 11 February 2011, the decree 2011-170[10] appointed ANSSI as the French Cyberdefence Authority. Since then ANSSI oversees laws and decrees related to CIIP.

In this regard, ANSSI participated to the development of a new law, passed on 19 December 2013 (Loi de Programmation Militaire, LPM 2014-2019[11]) which amended the aforementioned 'Code of Defence'. In particular, it includes four main provisions of interest to CIIP, which were further detailed in the decree 2015-351, 27 March 2015[12]:

- The ability for ANSSI to set minimum cybersecurity requirements at the technical and organisational levels as well as timeframes for their implementation by the operators. These requirements include the implementation of detection systems operated either by public entities (including ANSSI) in the case of a public administration, or service providers in the case of private operators. It is worth noting that detections systems must be qualified by ANSSI (both the products and service providers relied upon by the operator to set up its detection system).

[8] http://www.livreblancdefenseetsecurite.gouv.fr/
[9] http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020828212
[10] http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023571320&dateTexte=&categorieLien=id
[11] http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&categorieLien=id
[12] http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030405967&dateTexte=&categorieLien=id

- As a logical consequence to the enforcement of detection systems, the law introduces mandatory cybersecurity incident notification from critical operators to ANSSI.
- Mandatory cybersecurity audits, performed either by a public entity (including ANSSI) or a service provider qualified by ANSSI. Operators can undergo maximum 1 audit per year, except if previous audits revealed vulnerabilities, failures to comply with minimum security requirements or ongoing incidents. Audits reports are classified and provided to ANSSI.
- Crisis management provisions – notably the ability for ANSSI to lead cross-ministerial crisis management activities and to take or request necessary actions from the operators.

ANSSI is currently working on the categorisation of assets according to their criticality, as well as drafting sector specific security requirements and implementation guidelines.

2.7 Hungary (HU)

The National Directorate General for Disaster Management is responsible for the Critical Infrastructure Protection (CIP) in Hungary. The main tasks are to identify the potential critical infrastructure elements and to keep them under authoritative control.

The Hungarian Parliament accepted the Critical Infrastructure Protection Act (number: 166/2012) by a qualified majority. The second part of the Hungarian legislation procedure came with the Government Framework Decree which was entered into force in March 2013. (number: 65/2013). Through the legislation common terms and procedures for designating national and European critical elements had been created. It is a framework decree (65/2013) including regulation of sectors and sub-sectors, which came into force in three separate periods. In four sectors starting with Energy and followed by Agriculture, Water, and Public Safety the legislation procedure has been finished, in the sector of Transport the legislative process is still ongoing.

The identification process for Public Safety and Agriculture has been completed. The designating procedure is still ongoing in all the other sectors. There is no designated European Critical Infrastructure Element in Hungary yet. According to the law, in six sectors (Transport; Financial; Medical; Industry; Information, Communication Technologies; Law and Governmental) further government decrees are necessary for starting the identification process.

Hungary has created a CIP Network Safety Center acting as the national security authority of Hungary. The center has been established to provide safety and to help the operator companies (only if they became CI elements) to protect themselves against network and cyber security incidents (for example: hacker activity).

The National Directorate General for Disaster Management has monitoring, controlling and coordination role, and includes the CIP CSIRT.

National Directorate General for Disaster Management of Hungary eligibilities (CIP):

- Special authority
- Registering authority
- Audit Coordination
- Network Safety
- Incident management
- National contact point

2.8 Latvia (LV)

Critical infrastructure in Latvia in general is designated on the basis on the National Security Law, which defines critical infrastructure as “objects, systems or parts of systems located on the territory of Republic of Latvia, which are important for implementation of functions vital to society and for provision of health protection, security, economic and social welfare, and destruction or malfunction of which would significantly affect the functions of the State.” While this definition also includes critical information infrastructure, a specific act on cyber security – the Law on the Security of Information Technologies – further addresses “critical infrastructure of information technologies”. In addition, once a year the Cabinet of Ministers establishes and reviews the critical infrastructure whose termination can substantially threaten the existence of the state.[13]

The Latvian approach to CI does not rely on specified critical sectors; rather, any infrastructure found to meet the criteria of criticality can be designated as critical infrastructure. The decision to designate a particular infrastructure – including IT infrastructure – as critical is taken by The Commission of Intermediary Institutions for State Security[14] and approved by the government cabinet in accordance with the National Security Law.

Direct legal responsibility for the security and functioning of critical information infrastructure lies with the owner or legal possessor of the critical infrastructure. The CI owner is required to define security measures based on identified risks, document these measures, and present the documents of security measures to the Constitution Protection Bureau upon the latter’s request. It has a legal obligation to ensure the security of the CI in such a way that the identified risks are managed. The CI owner shall appoint a person responsible for the security of the critical infrastructure, who will be in charge for *planning security measures* of the critical infrastructure, and, in cooperation with the Constitution Protection Bureau and the national CERT, ensure the assessment and management of the current risks of the critical infrastructure.[15]

The role of coordinating security measures is shared between the state security service, Constitution Protection Bureau,[16] and the national CERT (the Information Technology Security Incident Response Institution of the Republic of Latvia – CERT.LV), operating under the Ministry of Defence of the Republic of Latvia[17]). The activities of both agencies in the area of CII are governed by the Law on the Security of Information Technologies and a Cabinet regulation that further specifies the planning and implementation of security measures.

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 a 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

[13] Cabinet Regulation No. 496 of 1 April 2010 “Planning and Implementation Procedure of Identification and Security Measures for the Critical Infrastructure, including the Critical Infrastructure of Europe”

[14] It is an advisory collegial institution, chaired by the Ministry of Internal Affairs and consisting of representatives from government ministries; public agencies such as the Police, State Fire and Rescue Service; Armed Forces; security agencies such as Security Police, Military Intelligence and Security Service, Constitution Protection Bureau; CERT.LV; and the National Bank.

[15] Cabinet Regulation No. 100, adopted 1 February 2011 “Procedures for the Planning and Implementation of Security Measures for the Critical Infrastructure of Information Technologies”

[16] www.sab.gov.lv

[17] https://www.cert.lv/section/show/12

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[18] regarding current threats to critical infrastructure.

The Information Technologies Security Incidents Response Institution (CERT.LV) provides support for and coordinates CII incident prevention, inter alia by cooperating with the Constitution Protection Bureau and CI owners in risk assessment and risk management. 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.

Cyber Security Strategy of Latvia for 2014 – 2018 marks Critical Infrastructure as one of the key areas of action under the section on Governance and Resources of Cyber Security. It highlights the fact that critical infrastructure of information technology has been established for the performance of basic functions essential for state and society to ensure the integrity, accessibility and confidentiality of the critical infrastructure. Regular trainings organized by CERT.LV for the representatives of critical infrastructure are recognized a significant tool to exchange the knowledge and experience, as well as to improve the procedures.

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. However, detailed information on the specific tasks regarding the Critical Infrastructure is not publicly available.

2.9 Lithuania (LT)

In Lithuania, the Law on Cyber Security (which entered into force on 1 January 2015) introduces the definition of critical information infrastructure (CII) in national level. In addition to setting of organization, management and control of the national cyber security system, the Law defines the following responsibilities of CII owners:

- CII owners are responsible for cyber security of their critical information infrastructure and implementation of organizational and technical cyber security requirements;
- CII owners shall inform the National Cyber Security Centre (NCSC) about cyber incidents and cyber threats.
- CII owners shall inform State Data Protection Inspectorate about cyber incidents related to personal data.
- CII owners shall inform police about suspected cyber-crime cases.
- CII owners shall develop, implement and exercise their cyber incident management plans.
- CII owners shall designate contact points responsible for cyber security.
- CII owners when necessary shall create necessary conditions for installation and management of NCSC owned cyber security tools in their CII.

The law sets the responsibility of the Ministry of Interior to develop methodology for identification of CII, draft a list of CII and present it to the Government for approval. The Law establishes National Cyber Security Centre (NCSC) as the authority responsible for CIIP. In accordance with the law, the Government by its decree has approved the establishment of Cyber Security Council (CSC), which consists of public, private sectors and academia

[18] The Council determines the development of cyber security policy at a national level, as well as coordinates the planning and implementation.

representatives. The main tasks of CSC are to analyse cyber security situation, tendencies, cyber threats, and provide an advice on improvement of national cyber security, including CIIP.

The Law requests the establishment of cyber security information platform, which will be used to exchange information between competent authorities and CII.

CIIP is one of three main objectives in the Lithuanian NCSS (Programme for the development of electronic information security (cyber security) for 2011-2019 (2011)[19]). NCSS sets more than 10 assessment criteria which should be achieved for better CIIP.

2.10 The Netherlands (NL)

Working with international partners, the Netherlands aims to create a secure and open digital domain, in which the opportunities for our society offered by digitisation are used to the full, threats are countered effectively and fundamental rights and values are protected.

The correlation between security, freedom and social and economic benefits proposed in the NCSS2 is a dynamic balance that is intended to be realized in a constantly open and pragmatic dialogue between all stakeholders, both national and international. The objectives serve as a guideline to the 2014-206 action program linked to the NCSS2. This action program comprises 37 actions concerning a broad spectrum of cybersecurity issues, Annual progress reports will be drawn up and the action program will be updated when necessary.

However the Dutch government started the CIP project (Bescherming Vitale Infrastructuur) early 2002 with the objective to develop an integrated set of measures to protect the infrastructure of government and industry. The critical sectors considered are:

- Energy: electricity, natural gas and oil
- Telecommunication and ICT: land-line and mobile telephony, radio, broadcasting and the internet
- Drinking water: the water supply
- Food: the food supply (including in supermarkets) and food safety
- Health: emergency and hospital care, medicines, vaccines
- Financial sector: payments and money transfers by public bodies
- Surface water management: water quality and quantity (control and management)
- Public order and safety
- Legal order: the courts and prisons; law enforcement
- Public administration: diplomacy, public information, the armed forces, decision-making
- Transport: Amsterdam Schiphol Airport, the port of Rotterdam, highways, waterways, railways
- The chemical and nuclear industries: the transport, storage, production and processing of materials.

Within the framework of the protection of critical infrastructure, the government, working with vital parties, identifies critical ICT-dependent systems, services and processes. These efforts are linked to a program that will establish basic security requirements on the basis of risk analyses.

The position of the National Cyber Security Centre (NCSC) is bolstered by means of a stronger structure for confidential information-sharing and analysis. Furthermore, the NCSC assumes the role of expert authority, providing advice to private and public parties involved, both when asked and at its own initiative. Finally, based on

[19] Programme for the development of electronic information security (cyber security) for 2011-2019 (2011)

its own detection capability and its triage role in crises, the NCSC develops into Security Operations Centre (SOC) 3 in addition to its role as a Computer Emergency Response Team (CERT).

2.11 Poland (PL)

In Poland the CIP action plan (National Critical Infrastructure Protection Program) is set up since 2013 under the provisions of the Crisis Management Act. It was created by the Government Centre for Security in close collaboration with the ministers and heads of central offices competent in matters of national security, as well as responsible for the sectors or systems considered as critical for the proper functioning of the state. ICT is treated as one of the critical systems.

In general the approach of the Program was to create conditions for improving the security of critical infrastructures, and prevent the malfunctioning of critical infrastructure, prepare for crisis situations that could adversely affect critical infrastructure, respond in the event of destruction or disruption of critical infrastructure functioning, reconstruct the critical infrastructure.

The Program shall specify:

- national priorities, objectives, requirements and standards, to ensure the smooth functioning of critical infrastructure;
- the ministers in charge of government administration units and heads of central offices responsible for the systems mentioned above;
- detailed criteria which enable to identify objects, installations, facilities and services included in the critical infrastructure systems, taking account of their importance for the functioning of the state and satisfying the needs of the citizens

In particular the programme created the PPP forum for private and public owners of CIP. The Polish NCSS (Cyber Space Protection Policy of the Republic of Poland) is complementary to the efforts aimed at protection of CIP based on National Critical Infrastructure Protection Program. This programme is due to be updated every second year.

Governance of legislation initiative and CIP coordination is assigned to Government Centre for Security. However GCP is cooperating with all the ministers and heads of central offices competent in matters of national security as well as responsible for the sectors or systems considered as critical for the proper functioning of the state.

Pursuant to Article 3 (2) of the current Act of 26 April 2007 on crisis management, critical infrastructure – shall be understood as systems and mutually bound functional objects contained therein, including constructions, facilities, installations and services of key importance for the security of the state and its citizens, as well as serving to ensure efficient functioning of public administration authorities, institutions and enterprises.

Critical infrastructure in Poland is listed as:

- Energy, fuel and energy supply systems,
- Communication systems,
- Tele-information network systems,
- Financial systems,
- Food supply systems,
- Water supply systems,
- Health protection systems,
- Transportation systems,

- Rescue systems,
- Systems ensuring the continuity of public administration activities,
- k)Systems of production, storing and use of chemical and radioactive substances, including pipelines for dangerous substances.

2.12 Slovenia (SI)

In the field of CIP and especially CIIP the draft of Slovenian National Cyber Security Strategy proposes the establishment of national network of trust between critical infrastructure owners/operators and all the CERTs, the newly established National Cyber Security Authority and also Intelligence agency/agencies. Participants from academia and R&D organisations could also be part of this network. The network itself could be connected to/part of European Critical infrastructure warning information network – CIWIN.

According to the draft of National Cyber Security Strategy, Slovenia should also strengthen the capacity in the national CERT specially dedicated to critical infrastructures and especially to the two most important of them (Electricity supply and ICT communications).

Critical sectors in Slovenia are defined on the basis of the basic and sectoral criteria for determination of critical infrastructure of national importance prepared by the Slovenian Ministry of defence (responsible body for critical infrastructure in Slovenia) and approved by the Slovenian Government[20].

Critical infrastructures are categorised based on the type (energy, ICT, water etc) into sub sectors (electric supply, oil supply etc) and prioritised based on the ownership structure (public or private).

According to the research project "Intersectoral overview of the situation regarding critical infrastructure and its protection in the Republic of Slovenia (2008)", the majority of critical infrastructures in Slovenia is in mixed ownership and only a small share is exclusively in public ownership (15 % of sub-sectors).

The priority levels of sub-sectors are determined on the basis of interdependence and interaction between sectors of critical infrastructure, as malfunctions of one sector can significantly affect the performance of other sectors.

The sectorial criteria in determining the critical infrastructures are developed on the basis of the definition of critical infrastructure and basic criteria for determining critical infrastructure, taking into account the specifics of each sector.

2.13 Spain (ES)

The Spanish Law 8/2011 (April 28) that includes measures for protecting critical infrastructure in Spain, covers the baseline requirements by the public and private sectors. Beyond compliance with EU legislation on protection of critical infrastructure, the primary purpose of the Law and the implementing regulations (Royal Decree 704/2011, 20 May), is setting up a pool of measures at national level to protect the critical infrastructures, by providing good support for effective coordination between public administration and managing authorities or operators of infrastructures which provide essential services to the society, in order to achieve a better security in total.

Moreover, the National Cyber Security Strategy adopted on December 5, 2013 by the National Security Council, as strategic document, and according to the forecast for the protection of cyberspace contained in the National Security Strategy, envisages the structure and implementation of several actions for prevention, defence, detection and reaction against cyber threats. Regarding the protection of Critical Infrastructure of the Information, the National

[20] http://www.mo.gov.si/fileadmin/mo.gov.si/pageuploads/zki/SklepVlade-potrditev_osnovnih_in_sektorskih_kriterijev_kriticnosti2012.pdf

Cybersecurity Strategy includes, in its Action Line 3, the goal of ensuring the security of Information and Telecommunications Systems which support the Critical Infrastructures. Particularly, this Action Line will be implemented in an Action Plan, to be completed in the next that will include measures to be developed in next years.

Last but not least, the Instruction 15/2014 of Secretary of State - Ministry for Home Affairs - must be emphasized. This Instruction provides the creation of the Cyber Coordination Office, as a tool for technical coordination between the different organisations with mandate on cybersecurity within the Secretary of State. The core function of this Coordination Office is to advise the Secretary of State on cybersecurity topics, provide the strategic and technical information needed for decision making and coordinate the CERT for Security and Industry (CERTSI) and the technical units in the different law-enforcement agencies at State Level (National Police and Civil Guard).

The Law 8/2011 establishes the following strategic areas:

- Administration
- Chemical Industry
- Energy
- Financial and Tax System
- Food Supply Chain
- Health
- Information and Communication Technologies (ICT)
- Nuclear Industry
- Research Laboratories
- Space
- Transport
- Water

Different planning instruments were established by Law 8/2011 and Royal Decree 704/2011 act on these strategic sectors:

- **National Plan for Critical Infrastructure Protection**, strategic approach and State responsibility.
- **Sectorial Strategic Plans** for each of the defined sectors or subsectors that are approved by the CIP Commission. Applying horizontal criteria of criticality defined by law, the Sectorial Strategic Plans finish with the appointment of operators and critical infrastructure.
- In addition to those plans mentioned above, critical operators have to develop **Operator Security Plans** and **Operator Specific Protection Plans** (both with a more limited scope and responsibility of critical infrastructure owners), and the Plans Operational Support Plans (operational nature and responsibility of law-enforcements, and therefore, the Administration)

  All this information is stored in the National Catalogue for Strategic Infrastructure that has being classified as Secret (the top Level of classification in Spain). It stores all information on national and European critical infrastructures, including the level of security.

2.14 Switzerland (CH)

On 27 June 2012, the Federal Council ratified the national strategy for the protection of Switzerland against cyber risks (the NCS), laying hereby the foundation for a comprehensive, integrated and holistic approach in tackling cyber risks. The NCS is located in MELANI (reporting and analysis centre for information assurance), which in turn is part of the Federal Finance Department. The NCS seeks among other things to make Switzerland’s critical infrastructures as a whole more resilient to cyber-attacks (in other words, the ability to resume normal operations as quickly as possible) and generally reduce cyber risks (cybercrime, espionage and sabotage). The NCS also reflects some key concepts such as the need for a culture of (cyber) security, shared responsibility of all participants and the need for a risk-based approach. It also advocates a government coordination, economic (Private-Public Partnership Model) and international cooperation.

The strategy comprises 16 measures that should be in place and in regular use by 2017. In order to guarantee the effective and timely implementation of these measures, the Federal Council has ratified a detailed implementation plan in 2013 and created a steering committee, which is comprised of a representative of each department, who is in charge of one of the measures.

The NCS Steering Committee is mandated to secure the coordinate purposeful implementation of this strategy, by means of a strategic controlling tool. It then reports its findings to the Federal Council. In support of the work of the NCS Steering Committee, there is also a NCS Coordination Unit, which coordinates the implementation of the strategy at an operational and technical level. The Steering Committee meets biannually or annually to verify that the implementation of the 16 measures (they range from vulnerability and risk analysis, continuity and crisis management to threat analysis and incident handling) is on track and on time.

At the heart of the NCS is the protection of critical infrastructures, as they ensure the availability of essential goods and services and are therefore in the interest of national security. Any cyber-attack on them will not only have cascading effects, but will be detrimental to the state and its population.[21] Regarding the protection of Switzerland's critical infrastructure, the NCS strategy builds upon the national strategy for the protection of critical infrastructures (SKI strategy) from the Federal Office for Civil Protection (FOCP). The protection of critical infrastructures involves all measures that reduce the probability and/or extent of damage of a disruption, failure or destruction of such a critical infrastructure. The SKI strategy has identified 28 critical sub-sectors and categorized them into three levels of criticality ranging from high to low. Criticality means the significance of this sub-sector for the population, the economy and its dependence on other critical infrastructures. Moreover, it has to be evaluated what the probability of occurrence is and what the damage of such an occurrence would mean for Switzerland and its population. The findings are summarized in an inventory.

In a nutshell, Switzerland pursues a decentralised approach, whereby the state is mandated to give those critical infrastructure operators subsidiary support. However, implementation of security measures lies within the sole jurisdiction of the process owners. The idea underlying this process is that the process owners are best equipped to identify the cyber risks to their critical processes and decide on implementation of appropriate security measures.

2.15 United Kingdom (UK)

The UK's response to CIIP is set out as part of Objective 2 (Making the UK more resilient to cyber-attacks and better able to protect our interests in cyber space) in the National Cyber Security Strategy; the action plan which is included in the objective 3[22] of the strategy is helping to shape an open, vibrant and stable cyberspace which the UK public can use safely and that supports open societies.

The approach is based on two pillars:

a. Helping to shape the development of cyberspace by promoting both an open and interoperable cyberspace and the fundamental rights of the society

[21] Critical infrastructure refers to infrastructure whose disruption, failure or distraction would have serious implications for society, the private sector and the state. It includes, for example, control and switchgear for energy supply or telecommunications. An inventory of critical infrastructure will be compiled by the national strategy for the protection of critical infrastructure.

[22] https://www.gov.uk/government/publications/cyber-security-strategy (p.39)

b. Protecting the way of life by ensuring security without compromising values.

The specific actions included:

1. Continue the process started by the London Conference on Cyberspace to establish international norms of acceptable behaviour in cyberspace.
2. Undertake a review of policy and regulation of the UK communication sector, with a view to publishing a Green Paper early in 2012 followed by a White Paper and a draft Bill in 2013.
3. Support the open internet, working with the Broadband Stakeholder Group to develop industry-wide principles on traffic management and nono-discrimination and reviewing its transparenct code of practice in early 2012.
4. Implement bilateral commitment set out in high-level communiques (agreed in 2010 and 2011) with the US, Australia and France.
5. Develop new bilateral relationships on cyber with those emerging powers that are active in cyberspace.
6. Encourage international and regional organisations to support capacity building, for example working with the Commonwealth to promote model legislation on cybercrime, with the International Telecommunications Union (ITU) to support training on technical standards, with the Council of Europe (during the chairmanship starting in November 2011) and with the Organisation for Security and Co-operation in Europe (OSCE) to promote freedom of expression online.
7. Use multilateral and bilateral channels to discuss how to apply the framework of international human rights law in cyberspace and new challenges in guaranteeing such rights.
8. Strengthen international systems to build confidence among states in cyberspace, including through engagement within the OSCE on confidence-building measure.

The UK's general approach is based on partnership with industry, academia and international partners to ensure a stable and secure cyber space.

As part of the National Cyber Security Strategy UK has the National Cyber Security Programme which funds initiatives to meet the four key cyber security objectives. This is managed by the UK's Cabinet Office who coordinates cross government work on this issue.

With respect to critical national infrastructure including CIIP our approach is from an 'all risk perspective'. This enables to consider the scale of cyber risk and the necessary response against other threats and hazards facing the UK's CNI. In the interests of national security the UK does not makes its critical sectors public. However they do include those public and private sectors which ensure the provision of critical services to the UK and whose loss or disruption may carry a significant economic, social or health consequence.

3 Summary key points

The perception of Critical Information Infrastructures varies in the EU Member States according to their priorities and impact. In some cases CIIP was one of the objectives of the national cyber security strategy so as to better coordinate the respective parties (public and private sector); in other cases CIIP has a separate role to play for the country’s prosperity thus is not part of the NCSS but a standalone policy area.

3.1 Key points

1. Governance of the CII Action Plans in national level also varies in the Member States: in some cases the National Security Authority has full supervision of specific activities and stakeholders involved, in other cases a decentralised models is followed. This depends on the already setup framework in national level, of the budget and resources and of course on the priorities of the state.
2. Collaboration with the private sector is not achieved through a formal way. Specific settings are introduced like working groups, public-private partnerships and in some cases even through legal procedure to make sure that all relevant stakeholders are involved in the critical information infrastructures protection.
3. Awareness raising and enhancing capabilities is another aspect that governments invest on when talking about critical information infrastructures. Even if the CII operator is a private company the requirement of cyber security trainings to the staff is another requirement included in the strategy or the CII action plan.
4. Legislation is in many cases the way to make sure that a specific framework will be followed. However many countries have established non mandatory, voluntary schemes that work equally well. All depends in the approach of the state.
5. Specific cyber security requirements such as incident reporting, business continuity plans and baseline security measures implementation are often part of the national CIIP action plan and need to be implemented by both public and private CII providers.
6. Critical sectors are not the same for each country, they depend on the national risk assessment results and on the impact any disruption would have in the vital services to the society. The critical sectors identified are summarised in the table below, even though there are cases where there is no specific distinction but ad hoc impact assessment and immediate actions.

	Energy	Water	Food	Health	Finance	Transport	Public admin.	ICT	Civil admin	Space & research
AT	x	x	x	x	X	x	x	x	x	
CY	x	x		x	X		x	x	x	
CZ	x	x	x		X	x	x	x	x	
EE	x	x	x	x	X	x	x	x	x	
FI	x	x	x	x	X	x	x	x		
FR	x	x	x	x	X	x	x	x	x	x
HU	x	x	x	x	X	x	x	x		
LV	Not applicable									
LT	x	x	x	x	X	x		x		

NL	x	x	x		X	x		x	x	
PL	x	x	x	x	X	x		x		
SI	x	x	x	x	X	x		x		
ES	x	x	x	x	X	x	x	x	x	x
CH	x	x	x	x	X	x	x	x	x	
UK	x	x	x	x	X	x		x		

3.2 Next Steps

ENISA has compiled this report together with the NCSS working group to offer visibility to the relevant stakeholders of the Member States to understand the different approaches in the implementation of a strategy. Of course each approach is different as they are tailored to the needs of each state. This document presented 15 MS and how they structure critical information infrastructures protection governance models.

ENISA will continue offering support to the MS by issuing similar short papers that can be of value for the stakeholders designing and implementing a strategy and its specific components.

Special thanks to:

ENISA Authors: Dimitra Liveri, Anna Sarri, Critical Infrastructures and Services Unit, ENISA.

This work has been carried out in collaboration with the National Cyber Securities Strategies Working Group. We would like to thank the WG for the valuable input and feedback and in particular:

Anita Tikos, Ministry of Interior, National Electronic Information Security Authority, HU

Antonis Antoniades, Electronic Communications and Postal Regulation, CY

Daniel Bagge, National Security Authority, CZ

Elīna Neimane, Ministry of Defence, LV

Emma Dickens, Cyber Crime Office for Cyber Security and Information Assurance, UK

Jos Leenheer, Ministry of Security and Finance, NL

Krzysztof Silicki, NASK Institute, Poland; ENISA MB & EB, PL

Liina Areng, RIA, EE

López Gil, María del Mar, National security depoartment- presidency of the government cabninet, ES

Marjan Kavcic, Ministry of Education, Science and Sports, SI

Peter Knøster, Danish Defense Intelligence Service Centre for Cyber Security, DK

Roman Packa, National Security Authority, CZ

Stefanie Frey, MELANI, CH

Timo Mischitz, Federal Chancellery, AT

Timo Kievari, Ministry of transport and communications, FI

Tomas Stamulis, Ministry of National Defence, LT

Yann Salamon, ANSSI, FR