FINAL REPORT
JLS/2007/D1/037

STUDY: STOCK-TAKING OF EXISTING CRITICAL INFRASTRUCTURE PROTECTION ACTIVITIES

CONTRACTING AUTHORITY: EUROPEAN COMMISSION

PREPARED FOR:

European Commission

Directorate-General “Justice, Freedom And Security” Directorate D: Internal Security And Criminal Justice

Unit D4: Financial Support

PREPARED BY:

Booz & Company (Italia) S.r.l.

via dei Bossi 4

Milano

BOOZ & COMPANY REFERENCE NO: JLS-2007-D1-037_EU_CIP_StockTaking_Final_Report

Date: 16 OCT 2009

Foreword

(in charge of the European Commission)

Table of Contents

Table of Figures

1 Executive Summary

1.1 Understanding of the situation

The terrorist attacks of September 11, 2001 in New York, the Madrid train bombing in 2004, and the London Underground attacks in July 2005 indicated terror groups' willingness to target critical infrastructures worldwide. Additional reports of the arrest of terrorist cells and individuals aligned with Al Qaeda in Austria, Germany, and Denmark point to the fact that the threat of terrorism still exists within the EU. In addition to the need to be vigilant on terrorism, the European Union must continue to factor threats from natural and manmade disasters and incidents into their Critical Infrastructure Protection (CIP) strategies and initiatives. Examples abound: the 2003 blackout which left 56 million people in Italy and part of Switzerland without power; the flooding in Romania and the multi-State power outages in 2006 that crippled commerce and left millions without electricity, are indicators that terrorism is not the only cause for concern and attention. Beyond the EU, the 2005 hurricanes in the US (Katrina and Rita) devastated communications, energy, and transportation networks, delaying crucial emergency management efforts and making Federal situational awareness difficult.

In response to these and other events, the European Union has increased the pace of the development of CIP initiatives within the EU and across Member States—becoming one of the key EU priorities for the 2007-2013 planning period. The recent legislative activities by the European Commission on CIP, as well as the continuing policy discussions regarding the specifics surrounding the definition and quantification of European Critical Infrastructure (ECI), stem from initial steps taken to address European security needs. As modern societies across the EU come to depend on a wide range of physical and cyber infrastructures, the ever present threat takes advantage of vulnerabilities found at the joining of sectors with the potential to cause cascading effects not only limited to the Member State, but also across the larger domain of the EU.

The European Union possesses a complex, extensive, technologically advanced, and interdependent system of infrastructures. Residents have become accustomed to the extent of highway networks, ubiquitous communications, availability of electric power, quality and abundance of clean drinking water, and readily accessible supply of food. Constructed and cultivated over the course of the 20th century, these infrastructures represent a source of great economic strength for Member States. Available, reliable, efficient, and affordable infrastructure services have allowed hundreds of thousands of businesses—large and small—to flourish; offered EU industry a competitive advantage over its foreign rivals; produced a highly mobile, flexible, and productive workforce; improved the quality of life, safety, health, and security.

Strategic Value of Infrastructures in the European Union

The strategic value of infrastructures in the EU is unquestioned. They enable Member States (MS) to enjoy a high standard of living in comparison to many other parts of the world, provide the backbone for the production of goods and services for one of the world's largest economies, employ millions of workers, and ensure Member States can protect national security interests. Government, businesses, and individuals rely on infrastructures to deliver safe, reliable, efficient, and affordable services. Perhaps the best measure of the importance of infrastructures is not simply captured in a plethora of statistics, but in the perceptions of

customers. The average EU citizen expects their lights will turn on; they will have dial tone and an Internet connection; their homes will be heated; airplanes, trains, and buses will run on schedule; mail will arrive daily; food will be stocked in grocery stores; police and emergency service workers will ensure the safety and security of the public; and water will flow and be safe.

Assuring the availability, reliability and sustainability of these lifeline infrastructures is one of the core themes of the European Union. To support this need, the Commission has created the European Programme on Critical Infrastructure Protection (EPCIP) with a focus both on the identification and designation of ECI, as well as the assessment of the need to improve its protection. To ensure that these objectives are achieved in a timely and effective manner, the EU has created an all-hazards based framework concerning the protection of critical infrastructures. There are six key principles that serve as a foundation for the implementation of EPCIP.

Subsidiarity	▪ The Commission's efforts in the CIP field will focus on infrastructure that is critical from a European perspective, rather than national, regional, or local
Complementarity	▪ The Commission will avoid duplicating existing efforts, whether at EU, national or regional level, where these have proven to be effective in protecting critical infrastructure. EPCIP will therefore complement and build on existing sectoral measures
Confidentiality	▪ Both at EU level and MS level, Critical Infrastructure Protection Information (CIPI) will be classified appropriately and access granted only on a need-to-know basis. Information sharing regarding CI will take place in an environment of trust and security
Stakeholder Cooperation	▪ All relevant stakeholders will, to the extent possible, be involved in the development and implementation of EPCIP, including the owners/operators of critical infrastructures designated as ECI, as well as public authorities and other relevant bodies
Proportionality	▪ Measures will only be proposed where a need has been identified following an analysis of existing security gaps and will be proportionate to the level of risk and type of threat involved
Sector-by-Sector approach	▪ Since various sectors possess particular experience, expertise, and requirements with CIP, EPCIP will be developed on a sector-by-sector basis and implemented following an agreed list of CIP sectors

Figure 1: Six Key Principles of EPCIP

European Union's Critical Infrastructure Policy Platform

Over the last few years, the European Union has developed many initiatives under the general theme of infrastructure protection and security. This is testimony of the emerging objective regarding the creation of a European–wide shared security environment. As

indicated in Figure 2, the EU has been aggressively working the process of developing the EPCIP.

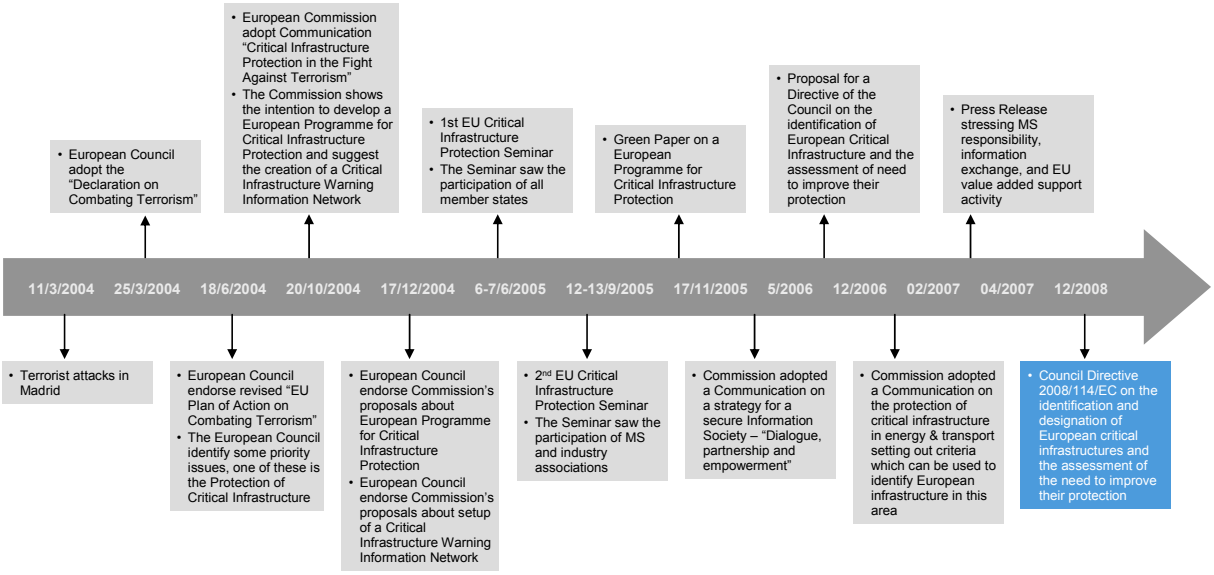


Figure 2: Key Milestones of European Union Critical Infrastructure Protection

In December 2006, an EPCIP communication adopted by the Commission identified the following elements of the overall EPCIP framework:

- A procedure for the identification and designation of European Critical Infrastructures (ECI)
- Measures designed to facilitate the implementation of EPCIP
- Support for Member States concerning National Critical Infrastructures (NCI)
- Contingency Planning
- An external dimension
- Accompanying financial measures and in particular the proposed EU 2007-2013 programme

In support of developing measures designed to facilitate implementation, this communication also defined EPCIP as an ongoing process. Regular review will be carried out in the form of the EPCIP Action Plan which outlines the actions, actors, and timeframes of EPCIP development and will be updated regularly based on the progress made. These CIP related activities are divided into three work streams:

EPCIP Work Streams
▪ **Work Stream 1:** Deals with the strategic aspects of EPCIP and the development of measures horizontally applicable to all CIP work ▪ **Work Stream 2:** Deals with European Critical Infrastructure and implemented at a sectoral level ▪ **Work Stream 3:** Supports the Member States in their activities concerning National Critical Infrastructures

Figure 3: EPCIP Work Streams

Specifically, in support of the implementation element of the EPCIP framework, Phase 1 of Work Stream 1 calls for the on-going commitment of the Commission, the Member States, and other stakeholders in the creation of an inventory of existing national, bilateral, and EU CIP programmes, as well as the collection of CIP-related best practices, risk assessment tools, and methodologies. The Commission envisions utilizing the Critical Infrastructure Warning Information Network (CIWIN) currently under development as the vehicle for dissemination of these best practices, thereby contributing support to the Member States in the protection of National Critical Infrastructures.

In December 2006, the Council also adopted a directive on the identification and designation of European Critical Infrastructure (ECI) and a common approach to the assessment of the need to improve the protection of such infrastructures. In this proposal, the Commission defined ECI as critical infrastructures in the European Union, which if disrupted or destroyed, would affect two or more Member States or a Member State other than that in which the critical infrastructure is located.

More recently, the Council adopted a conclusion in April 2007 emphasising the ultimate responsibility of the Member States for managing arrangements for the protection of critical infrastructures within their national borders. At the same time, the Council reiterated that action at EU level will add value by supporting and complementing Member States' activities, further emphasising the need for a common data collection point covering all on-going activities. The conclusion specifically cites the importance of exchanging information between Member States, owners/operators, and the Commission.

The Council also emphasized the creation of a CIP Contact Group consisting of Member States' points of contact for CIP in order to facilitate the coordination and exchange of information and best practices. The Council further stated that the Commission may set up EU-level CIP expert groups, together with the CIP Contact Group, in order to benefit from practical professional expertise.

In December 2008, the Council of the European Union adopted Council Directive 2008/114/EC on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection. This Directive concentrates on the energy and transport sectors (Figure 4).

Sector	Subsector	
I. Energy	1. Electricity	Infrastructures and facilities for generation and transmission of electricity in respect of supply electricity
	2. Oil	Oil production, refining, treatment, storage and transmission by pipelines
	3. Gas	Gas production, refining, treatment, storage and transmission by pipelines LNG Terminals
II. Transport	4. Road transport 5. Rail transport 6. Air transport 7. Inland waterways transport 8. Ocean and short sea shipping and ports	

Figure 4: List of ECI sectors and subsectors

The review of the Directive 2008/114/EC shall begin on 12 January 2012. Member States shall take the necessary measures to comply with the Directive by 12 January 2011.

1.2 Purpose and scope of stock-taking initiatives

In August 2008, DG JLS awarded a tender for a stocktaking study of existing CIP activities in EU Member States under the EPCIP framework. Three specific parts of the EPCIP framework are particularly relevant for this study:

- 1. The EPCIP Action Plan (Work Stream 1, Phase 1) identifies two actions:
  - Creation of an inventory of existing national, bilateral and EU critical infrastructure protection programmes
  - Collection of CIP related best practices, risk assessment tools and methodologies
- 2. Support for Member States concerning National Critical Infrastructures (NCI), which can be taken forward optionally at the request of a Member State. The dissemination of the best practices identified under the EPCIP Action Plan would contribute to this process
- 3. The creation of the Critical Infrastructure Warning Information Network (CIWIN), which could constitute the information platform for the dissemination of best practices and other CIP relevant information

The purpose of this particular study was to:

- **Provide the European Commission with:**
  - I **A detailed description of existing critical infrastructure protection activities in the EU**
  - II **Identification of key insights and trends in the CIP field based on the above information**
  - III **Arrange the gathered information into a modular format which can be uploaded to the CIWIN prototype**

Figure 5: Purpose of the Study

In order to meet these objectives, the study included CIP oversight, coordination, and on-going programmes in the EU Member States. The Commission required a detailed understanding of the structure of such institutional programmes, in particular in the sectoral context, as well as their content. The study identified the methodologies that the Member States are currently utilizing both to identify critical infrastructures and to assess risk where possible. The scope of the project included all 27 EU Member States. In addition, the EU itself (as the "28th" Member State) and Norway were evaluated.

Original Member States in 1957	Belgium, France, Germany, Italy, Luxembourg, Netherlands		Total: 6 States
New Member States 1958-1995	Austria, Denmark, Finland, Greece, Ireland	Portugal, Spain, Sweden, United Kingdom	Total: 15 States
New Member States 1996-2008	Bulgaria, Cyprus, Czech Republic, Estonia, Hungary, Ireland, Latvia	Lithuania, Malta, Poland, Romania, Slovakia, Slovenia	Total: 27 States
Others	EU, Norway		Total: 29 States

Figure 6: Scope of the Study

The sectoral division of CIP programmes is clearly among the most important aspects of understanding Member State activity. The study identified if and how the MS CIP programmes are divided into sectors (or services) and defined the approaches used to analyze and take into account sectoral and geographic interdependencies. It explored both legislation and soft approaches related to the sectors set out in Figure 8:

I Energy
II Nuclear industry
III Information, Communication Technologies, ICT
IV Water
V Food
VI Health
VII Financial
VIII Transport
IX Chemical industry
X Space
XI Research facilities

Figure 7: EU CIP Sectors and Sub-sectors

The sector-specific analysis focused on CIP-related issues rather than a detailed review of sector-specific security and safety regulations. For example, in the air transportation field alone, a detailed study of security regulations would have quickly overwhelmed the project team and extended well-beyond the scope of the study. However, where deemed applicable, the study at times extended into emergency and crisis management activities as these are often tightly interwoven with CIP-related topics.

The study then extended beyond EU borders by identifying important worldwide CIP-related research activities. Combined with the above information, this provided the Commission with a collection of leading practices based on the needs of the Member States.

The results gathered by way of this study were then assembled into the form of a modular inventory which can be uploaded to the CIWIN prototype. This modular format consists of a sectoral-based framework developed during the project.

1.3 Project Approach

Throughout the project, the team followed a three-phase approach:

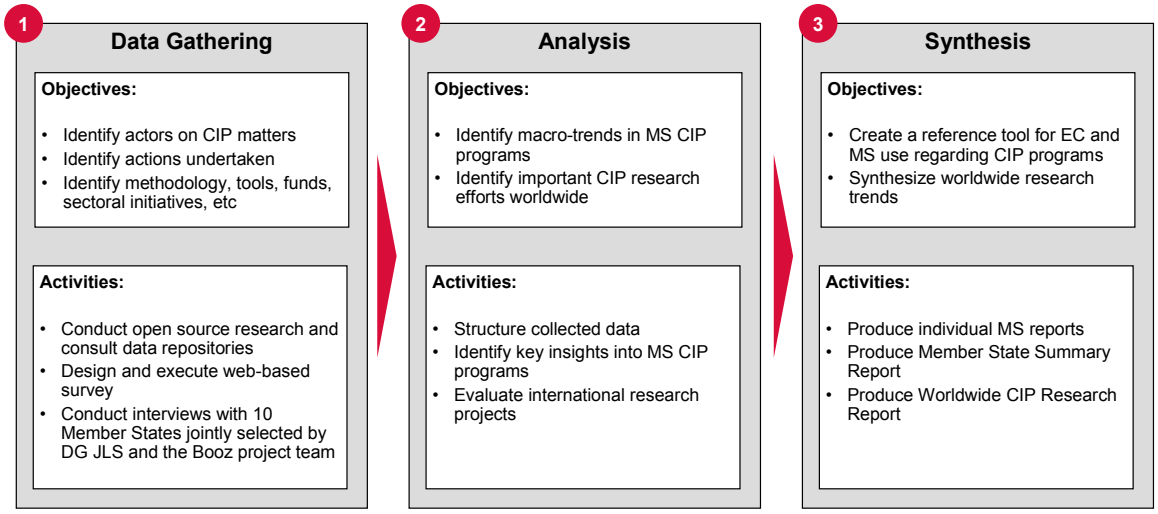


Figure 8: Project Approach

1.3.1 Data Gathering

Given the variations in population, government structures, political cultures, geographic ranges, etc., across the 29 countries covered in the study, the manner in which data can be categorized varies greatly from country to country. Therefore, prior to beginning the data gathering phase, the project team worked with the Commission to define a series of categories that would be comprehensive enough to cover the range of relevant topics without becoming too complex for later analysis. In the end, for each of the 29 countries covered, we gathered data across seven main functional categories:

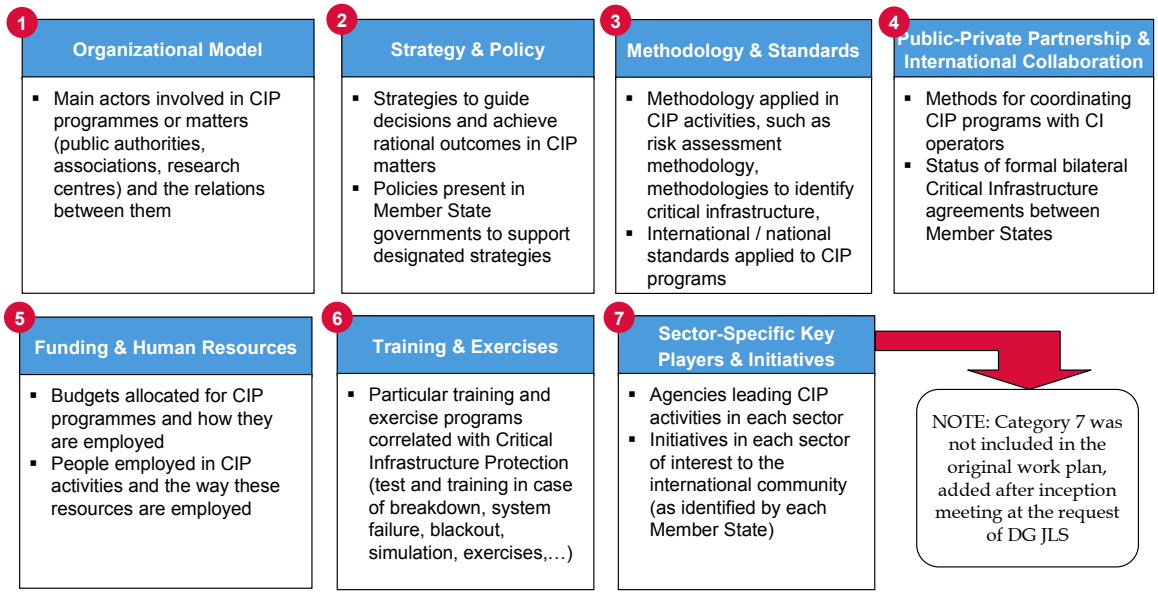


Figure 9: Data Collection Framework

Open Source Data and Data Repositories

The project team employed discrete open source research techniques to supplement, enhance, and validate data. Through our extensive industry and academic relationships—such as the Italian Association of CIP Experts—and by supporting multiple government clients, Booz & Company has maintained and refined trusted relationships with agencies and operators worldiwede which often permitted the project team to obtain information that might otherwise be very difficult to find for the general public.

To obtain information required for the study, we also requested assistance from the Commission in establishing open channels of communication to multiple Member State agencies.

Web-Based Surveys

In order to reach all of the relevant stakeholders in the different Member States (and worldwide for the portion of the study related to CIP research programmes), Booz & Company developed a secure web-based survey. This automated technique allowed us to obtain information across the widest possible geographic coverage. Once our open source research efforts had identified specific targets amongst public and private experts, we first initiated direct contact with them to open the CIP discussion and explain the purpose, context, and objectives of the EU-sponsored program. We then executed the survey with detailed but clear questions regarding each of the areas we had identified.

We took the necessary precautions to address the security issues related to transferring information in this manner. In order to ensure that the participants of the survey were comfortable providing potentially sensitive information to the project (sensitive but not classified), part of the questionnaire package included an explanation of the security measures taken.

Figure 10: EU CIP Stocktaking Web-Based Survey

Interviews

After initial contact and assessment of selected Member States and their key critical infrastructure points-of-contact, we determined together with the Commission which

organizations required face-to-face, in-depth interviews. In addition to building a strong foundation of participation, these visits to the competent authorities, associations, and research centers also completed the process of data acquisition.

Worldwide CIP-Related Research

Booz & Company catalogued the major CIP-related research projects and centers worldwide based on their potential to add value to the Commission's CIP development efforts. This analysis concentrated on who is calling for the research, what the requested research focuses on, and the resources and methodologies used to carry it out.

A comprehensive analysis of worldwide CIP-related programs to the level of detail covered in our analysis of the EU Member State programs was beyond the scope of this study. Therefore, we provided the Commission with a report focused on relevance, rather than a simple (and potentially overwhelming) list of on-going projects.

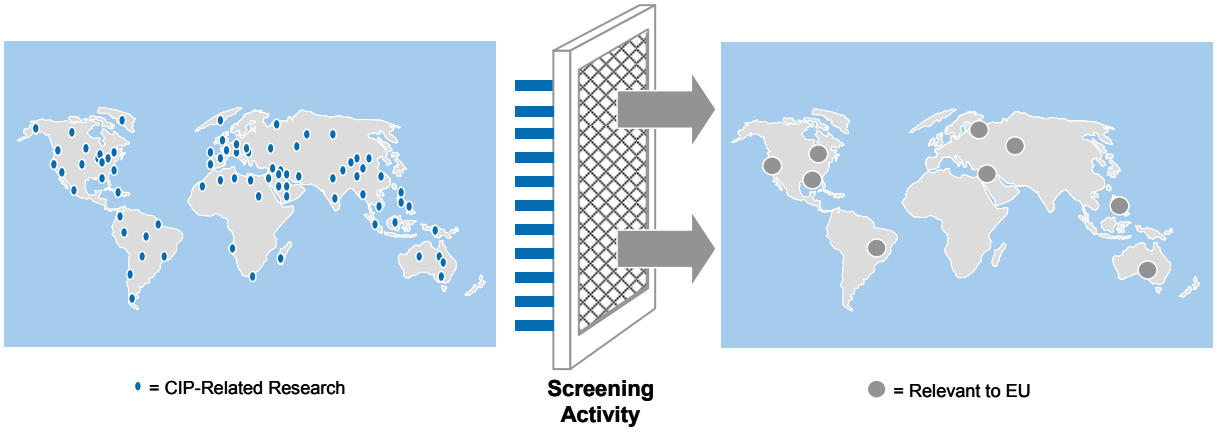


Figure 11: Research Screening

In order to determine which research projects and centers were of interest to the EU, our project team worked closely with the Commission throughout the study to identify the key aspects in the CIP research field and how they relate to EU CIP strategic objectives.

Based on the aspects identified, and in conjunction with the Commission, we developed a list of screening questions to determine which major projects would be included in the study.

1.3.2 Analysis

CIP Activities

After completing our data gathering activities, we produced baseline reports on all 29 countries covered in the study by integrating all of the data collected into the analytical framework illustrated in Figure 17:

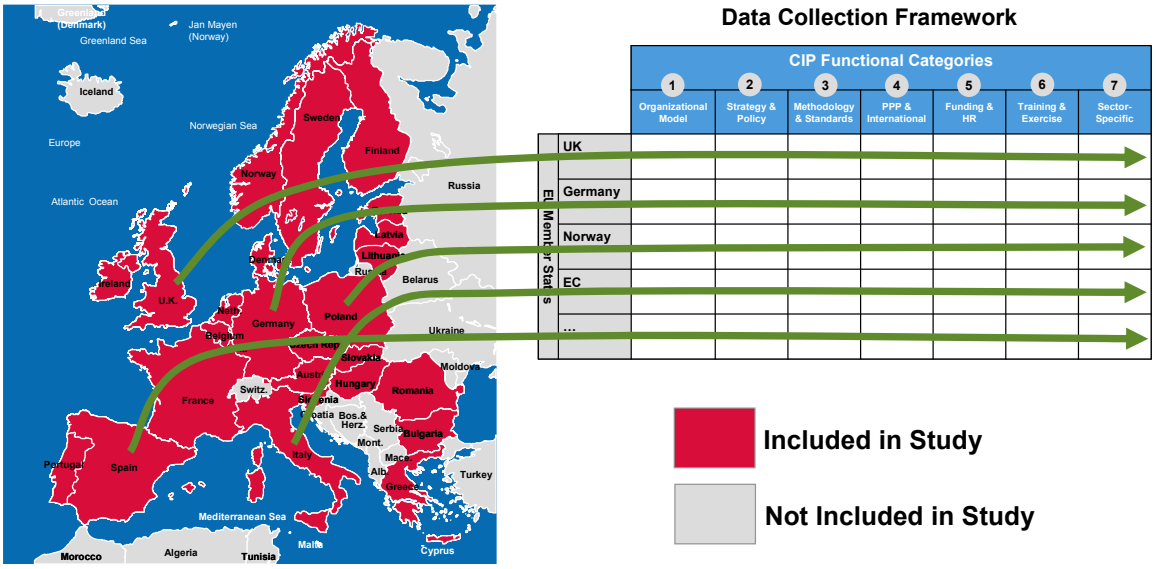


Figure 12: Introducing Data into Analytic Framework

This report structure provided the common ground needed to analyse the complex nature and structure of CIP programmes across 29 countries, notwithstanding fundamental differences in culture, politics, and geographies which made fitting some aspects of individual Member State activities into the framework difficult at times.

CIP-Related Research

Once a research project had passed the screening activity, we elaborated in detail to ensure maximum value retention by the Commission. This included a summary of the strengths and weaknesses of the research, as well as how the results might fit into the EPCIP and align with EU strategic objectives.

Figure 13: Research Project Analysis

Answering these questions had allowed us to ensure that we identified the specific strengths and weaknesses of each project as they relate to EU interests. This facilitated identification of how the results might fit into the EPCIP program and align with EU CIP strategic objectives.

1.3.3 Synthesis

During Work Stream 3, we organized all of the information gathered in order to present four outputs:

Individual Member State Reports

For each Member State covered during the study, we produced a detailed report which outlines all activities identified across all seven functional catoegories. We shared the individual Member State reports with each member State in order to give them the opportunity to ensure that the final report accurately represented the status of CIP-related activities in their countries.

29 x 7 Member State Summary Report

In order to provide a concise reference tool, we summarized all CIP activities in all of the Member States of the EU in a grid format as shown in this example (the actual grid is included in the appendix of this report):

		CIP Functional Categories						
		Organizational Model	Strategy & Policy	Methodology & Standards	PPP & International	Funding & HR	Training & Exercise	Sector-Specific
EU Member States	UK	▪ Model A ▪ …	▪ Strategy A ▪ Policy B ▪ …	▪ Method 1 ▪ Standard 2 ▪ …	▪ Model 1 ▪ Model 2 ▪ …	▪ Funds X ▪ Resource Y	▪ Training 1 ▪ Exercise 2 ▪ …	▪ Energy ▪ TLC ▪ …
	Germany	▪ Model B ▪ …	▪ Strategy B ▪ Policy A ▪ …	▪ Method 1 ▪ Standard 2 ▪ …	▪ Model 3 ▪ Model 2 ▪ …	▪ Funds Z ▪ Resource Y	▪ Training 1 ▪ Exercise 2 ▪ …	▪ Energy ▪ TLC ▪ …
	Norway	▪ Model A ▪ …	▪ Strategy A ▪ Policy D ▪ …	▪ Method 1 ▪ Standard 2 ▪ …	▪ Model 1 ▪ Model 4 ▪ …	▪ Funds X ▪ Resource Y	▪ Training 1 ▪ Exercise 2 ▪ …	▪ Energy ▪ TLC ▪ …
	EU	▪ Model C ▪ …	▪ Strategy A ▪ Policy C ▪ …	▪ Method 1 ▪ Standard 2 ▪ …	▪ Model 3 ▪ Model 4 ▪ …	▪ Funds X ▪ Resource Y	▪ Training 1 ▪ Exercise 2 ▪ …	▪ Energy ▪ TLC ▪ …
	…	▪ …	▪ …	▪ …	▪ …	▪ …	▪ …	▪ …

Figure 14: EU CIP Activity Summary Report

This tool provides the Commission and Member States with a simple, effective reference to use when comparing programmes. The information contained in each block is terse to avoid over-complication of the tool, yet complete enough to clearly represent the activities of the Member States.

Worldwide CIP Research Report

We identified the leading research practices and programmes worldwide based on their relevance to the EU and suggested methods for the EU to integrate these ideas into EPCIP development.

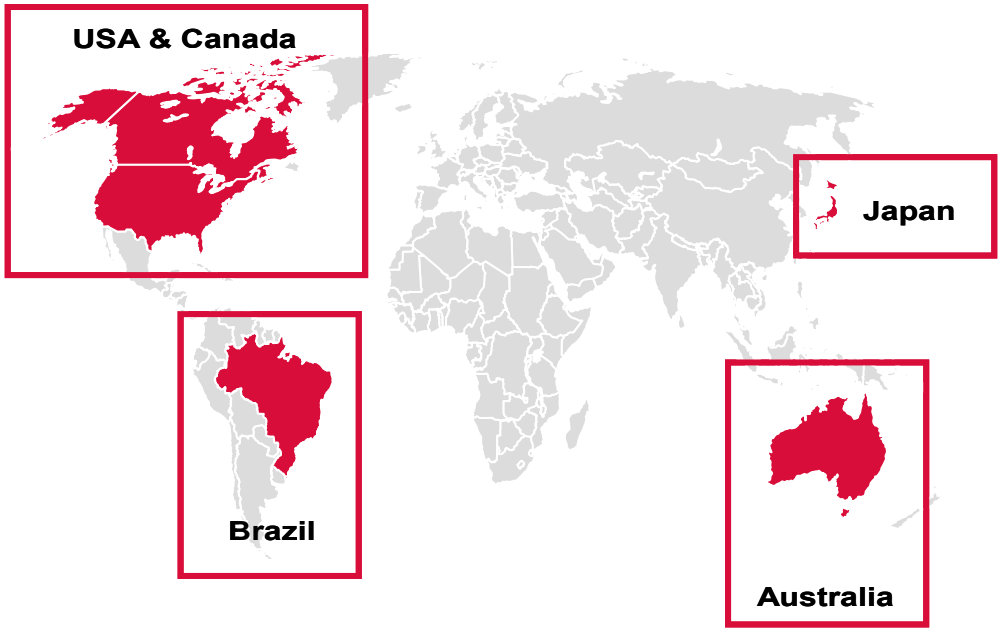


Figure 15: Top Worldwide CIP Research Activity Areas

To limit the scope of the report to a reasonable scale, we included only the research programmes that add value to strategic objectives agreed upon with the Commission:

- Early Warning
- Information Sharing
- Sectoral Interdependencies
- Modelling & Simulation
- Academic Forums & Journals

CIWIN Modular Inventory:

We assembled the information gathered throughout the study into a format which can be uploaded to the CIWIN prototype. This included geographic, functional, and sectoral dimensions of data gathering and analysis in order to provide maximum flexibility during the data processing stage of CIWIN implementation.

1.4 Key Insights and Trends

This section describes some of the key insights and trends identified through the study. For a detailed discussion of each category for each Member State, please refer to the summary report in the appendix or the individual Member State reports.

1.4.1 Organizational Model

The level of interaction between the various ministries involved in CIP activities varied between Member States. While some working groups were very informal and meet only occasionally, others followed strict protocols regarding interaction and responsibilities. Overall, the study showed that the most common organizational model is based on a central agency leading a workgroup of other minstires, as shown in Figure 16:

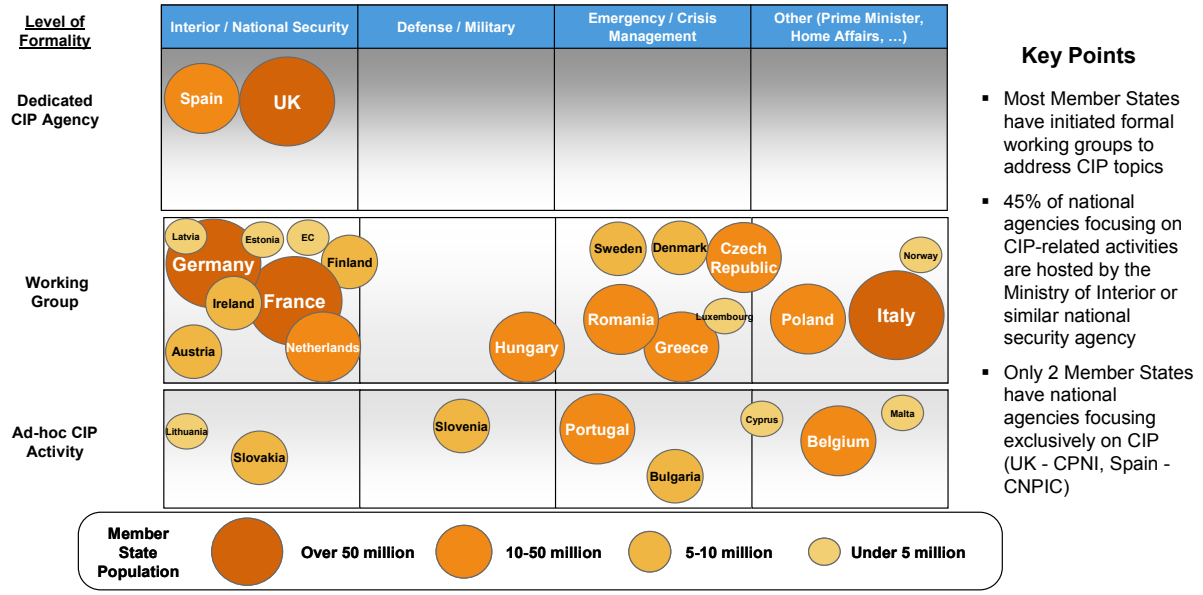


Figure 16: Government Organizations Coordinating National CIP Activities

In addition, we found that:

- Most Member States have initiated working groups to address CIP topics
- 45% of national agencies focusing on CIP-related activities are hosted by the Ministry of Interior or similar national security agency
- Only 2 Member States have national agencies focusing exclusively on CIP (UK - CPNI, Spain - CNPIC)

In most cases, the central agency cited above tends to focus on overall CIP coordination, while individual ministries handle sector-specific responsibilities. For example, a central agency might focus on international relations (i.e. EU CIP points of contact), organzing and hosting inter-ministerial working groups, central policy developments, etc.

The national CIP organizational structure of Norway illustrates these key points well:

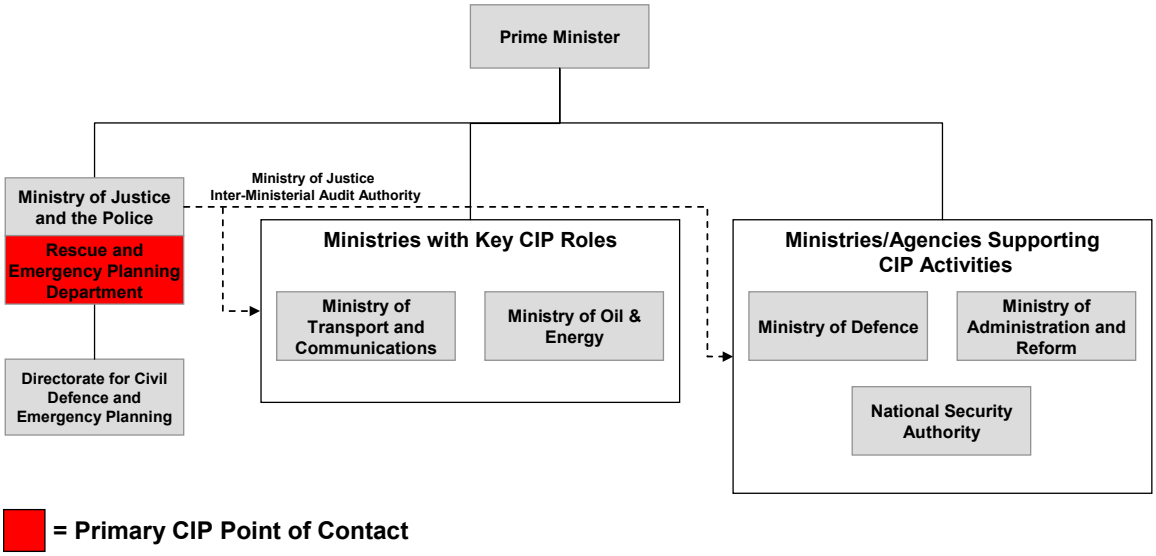


Figure 17: Example of Common National Organizational Structure: Germany

In addition to the common traits of a central agency coordinating a formal working group of other ministries (in this case clearly delinated into active and supporting roles), the program in Norway also includes some unique factors:

- Inter-ministerial coordinating role also **includes auditing other ministries** to determine the effectiveness of CIP processes within each Ministry
- Audit points include basic questions such as:
  - Has a **risk assessment** been performed?
  - Are **contingency plans** in place?
- The department provides audit results to the Ministry of Justice, as well as the audited Ministry, with **recommendations for improvement**

1.4.2 Strategy & Policy

Numerours government agencies consulted during the study indicated that the deregulation and privatization of some critical infrastructure sectors over the last several years has made it challenging at times to guarantee maximum service availability for all citizens. With many critical infrastructures now owned and operatored by private sector organizations, government agenices have adapted their style of interfacing with these operators from a regulatory stance to a mutually beneficial approach.

In fact, the study showed that most Member States continue to employ policy-based strategies for public agency coordination, but prefer cooperation-based models for managing relationships with operators.

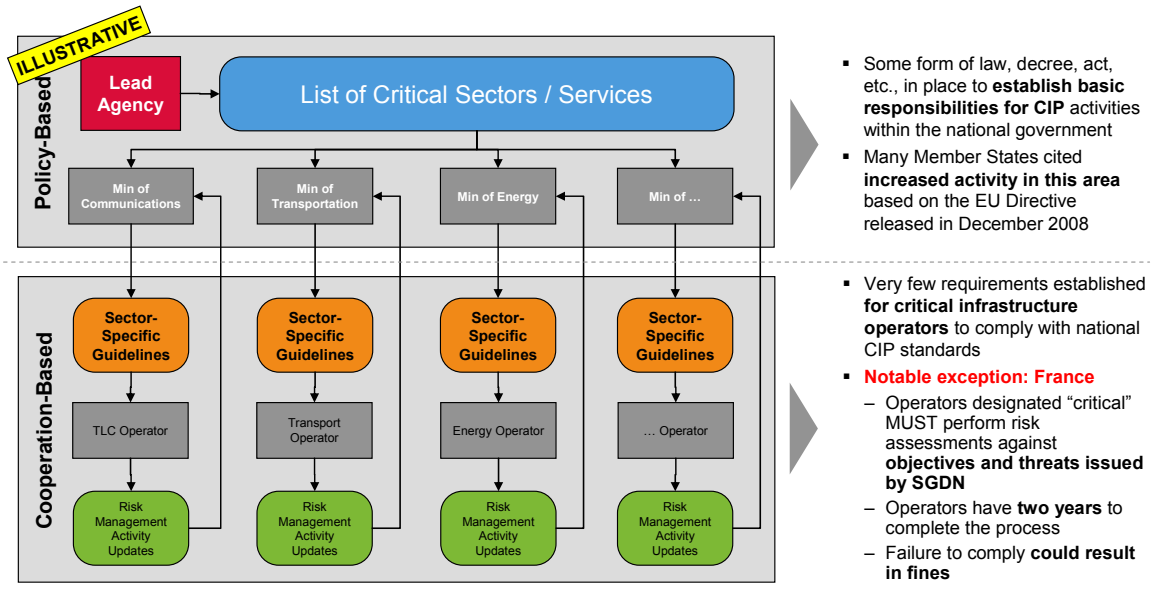


Figure 18: Common National Strategy for Protecting Critical Infrastructures

The study showed that decisions surrounding the designation of critical sectors and / or services, as well as the ministerial responsibilities for these sectors / services at the government level, tend to be defined through laws, decrees, acts, etc, issued by the national government. However, after the responsibility for a specific sector has been assigned to a Ministry, that Minsitry tends to adopt a softer "guideline" approach to interfacing with operators. By building trusted relationships with the CIP managers at the operator level, the Ministries are generally able to foster an environment in which the operators voluntarily adapt their risk management programs to meet the guidelines issued by the Minsitries and provide updated information in this regard to the Ministry on a regular basis.

When focusing on the levels of implementation of policy surrounding CIP-related activities, the study revealed two major trends, primarily related to the timeframes in which the policy in question was created:

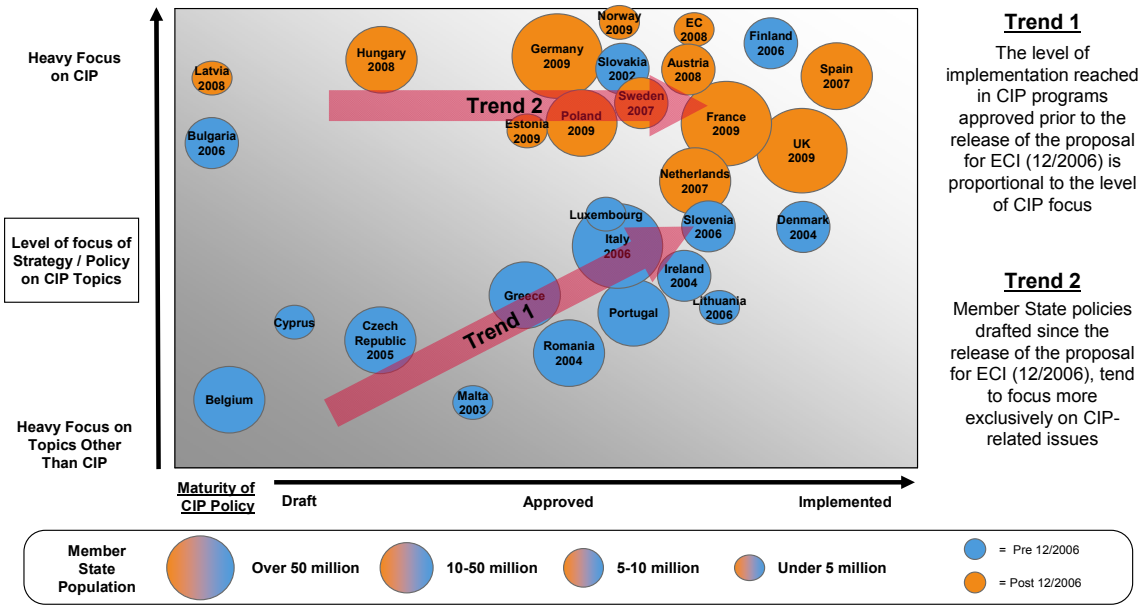


Figure 19: Trends in National CIP Strategy / Policy Implementation

Generally speaking, when referring to CIP policy enacted prior to the release of the proposal for ECI (12/2006) (Trend 1), the study showed that more focus on CIP-specific activities during policy draft and approval tended to result in better implementation of these activities.

This sets a promising precedent for the demonstrated continuance of new policy activity focused specifically on CIP-related topics since the release of the proposal for ECI (Trend 2). If the pattern shown in Trend 1 continues, it would be reasonable to assume that the new slate of policy developments with specific CIP focus will eventually reach further states of implementation than their predecessors.

1.4.3 Methodology & Standards

The study showed differences in the approach and critieria various Member States use to identify critical national infrastructures. In particular, the “starting point” of anlaysis varied widely. For example, some Member States begin by determing what are the basic services that society needs to function, and in-turn which infrastructures support these services. Others begin by identifying which infrastructures in each sector are key, and then determine what the impact to society would be in the event of failure. Yet others begin by identifying the key operators in each critical sector, and then let the operators determine which infrastructures are critical to the continuation of their services. This range of approaches is illustrated in Figure 20:

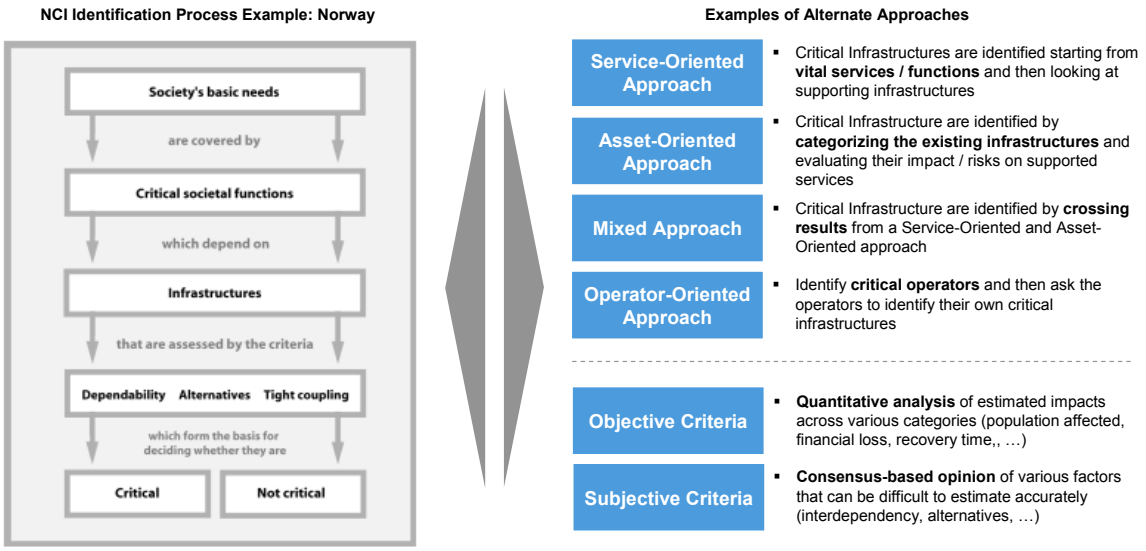


Figure 20: Different Approaches for Identifying Critical Infrastructure

After having narrowed the complete range of infrastructures down to a "potentially critical" list, the criteria used to make the final evaluations also varied. While some Member States cited specific, objective criteria such as financial loss or number of citizens affected, others relied on more subjective criteria that drew on the expert opinions of senior members of the government agencies and private operators responsible for the given sector.

Notwithstanding this differentiation in the process of designating Critical National Infrastructure, the process of managing risks against these infrastructures (once they had been identified) was generally in-line with international best practices.

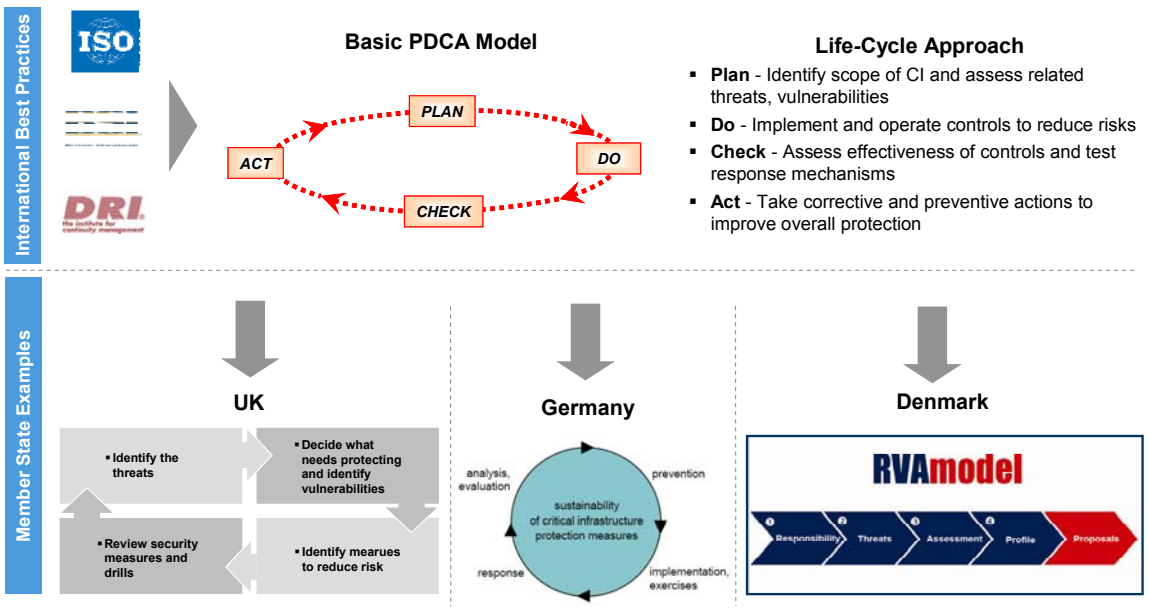


Figure 21: Common Approaches to Protecting Critical Infrastructure

This most often included a life cycle approach to governance, risk management, integrated security, incident management, "business" continuity, and continuous improvement. The Plan, Do, Check, Act life cycle was a commonly cited guideline, as well as well-recognized sector-specific standards such as BS 25999-1:2006 (Business Continiuity Management) and ISO/IEC 27001:2005 (Information Security Management System Requirements).

1.4.4 Public-Private Partnership & International Collaboration

The study showed that cooperative information sharing between government (public) agencies and infrastructure (private) operators plays a key role in many programs. Although there are many information sharing programs underway across the EU, the most commonly cited program was the Information Exchange model developed and implemented by CPNI in the UK:

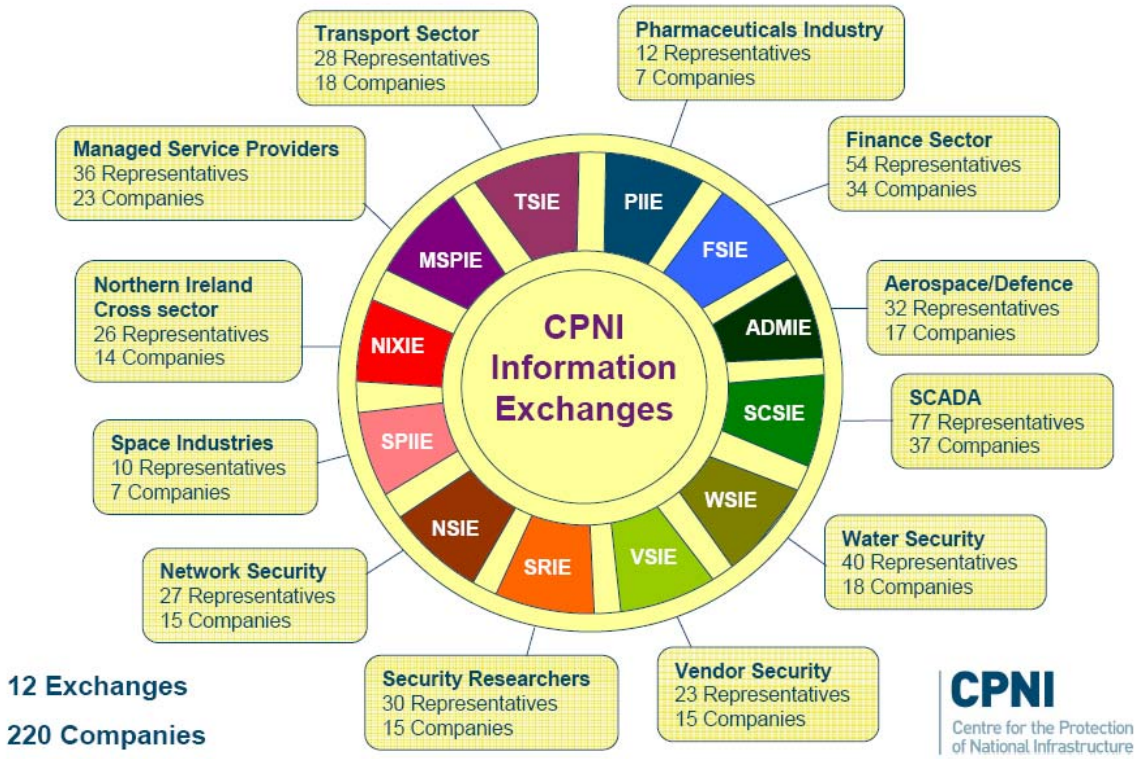


Figure 22: Public-Private Information Sharing Example: UK

The key aspects of the structure of this model that appear to contribute to its success include:

- Made up of a trusted group of industry and government representatives
- Stimulates discussions around security incidents, vulnerabilities, trends, and best practices
- Based on simple rules of membership
  - No cost to members

  - 2 members per organisation
  - Designated members cannot delegate participation (the same members must be present at every meeting)
- Information sharing protocol agreed by all members

In addition, many Member States are also engaged in multinational initiatives focusing on interdependencies and international information sharing. Some examples include:

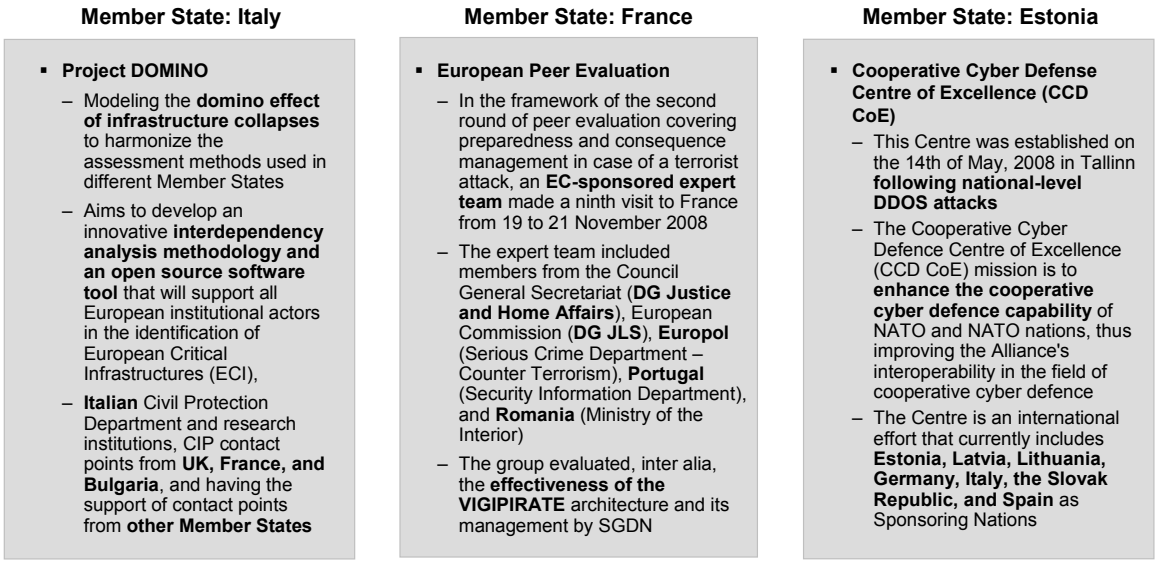


Figure 23: Examples of International Initiatives

Several recurring themes appear across the initiatives including interdependency studies, building trusted relationships, and a heavy focus on the ICT sector and cyber security.

1.4.5 Funding & Human Resources

The study showed that no Member State government is providing funding to operators to offset the costs of compliance with CIP programs. Instead, the majority of national-level funding tends to be focused on emergency management and security programs, and remains within the government agencies managing these topics. As the agencies coordinating CIP activities tend be located inside these higher-level functional agencies, this primary funding stream keeps government-level CIP acitivites moving forward. At the same time, the private owners and operators of critical infrastructure must fund compliance with government CIP programs out of their own internal risk management and business continuity programs.Figure 24 illustrates this relationship:

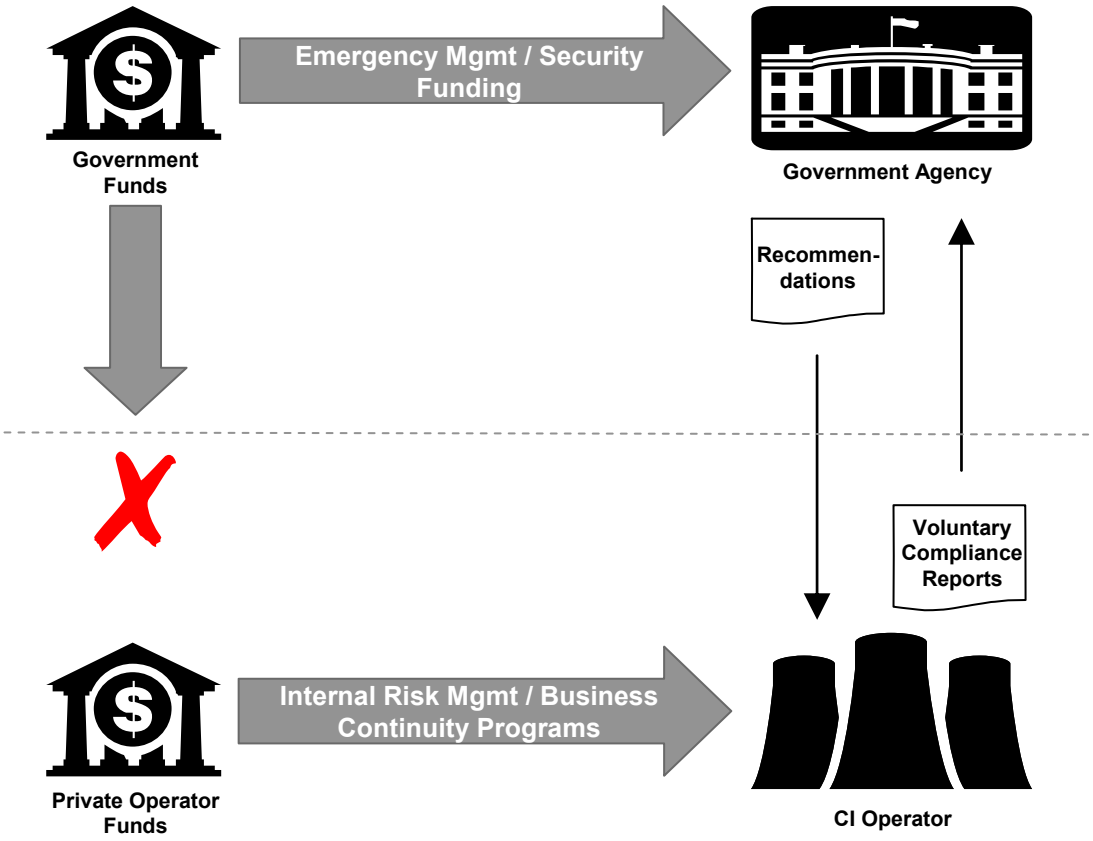


Figure 24: Typical CIP-Related Cash Flow

Several Member States cited several challenges to the development of CIP programs that this funding model presents:

- Few dedicated CIP staff in Member State governments and operators, mostly managed as additional duty
- Many Member States expressed difficulty enforcing the “stick” (compliance) without the “carrot” (funding)
- Misaligned priorities between government agencies and CI operators (i.e. terrorism focus) can make obtaining internal funding difficult for the operators
- Subsidizing sub-par performers could distort market conditions by improving reliability and continuity of infrastructures

1.4.6 Training & Exercises

The study showed that, while training programs with a specific focus on CIP-related topics are beginning to emerge, most exercise activity still focuses on crisis or emergency management activities. Some examples of this trend include:

Examples of Training and Education Programs

Germany

Many Universities and universities of applied science *(Fachhochschulen)* at present include CIP-related and risk management subjects or have introduced specific courses of studies on security-relevant subjects (i.e. rescue services; security and crisis management). For example, Bonn University and the Federal Office of Civil Protection and Disaster Assistance *(BBK)* jointly offer a Master's degree course which covers a broad range of subjects related to civil protection / disaster management and also deals with critical infrastructure protection

Poland

Poland is in the process of preparing a concept of a research centre which will work on issues dealing with crisis management, where a big part of its work will be issues dealing with CIP. Some of the funding for this effort may come from GCS

Examples of Exercise Programs

Finland

The UUSIMAA-2008 consequence management field exercise organised by the Euro-Atlantic Disaster Response Coordination Centre (EADRCC) included over 1000 participants from 37 countries

Czech Republic

The ZONE 2008 Exercise tested the performance of crisis management authorities, the integrated rescue system, and other emergency authorities at a simulated radiation incident at the Dukovany Nuclear Power Plant

Denmark

Since 2003, large national crisis management exercises (called KRISØV) have been conducted every second year. The complexity of the exercises has increased each time and more and more levels have been exercised simultaneously. During KRISØV 2009, to be conducted during the autumn of 2009, exercise participants from all levels of government will take part, including local government.
The KRISØV-exercises last from two to five days

While CIP, emergency management, national security, and other related topics are relatively easily to differentiate conceptually, several Member States noted that they can be difficult to seperate in a practical sense when it comes to training and exercises. The life cycle approach to managing all of these issues leads to areas of overlap that would unnecessarily complicate matters by trying to separate them. For example, when simulating an event to test the effectiveness of a CIP program that focuses on prevention, it would seem natural to combine this with testing of the management capabilities surrounding the impact of the same event used to test prevention measures.

1.4.7 Sector-Specific Key Players & Initiatives

The ECI Directive puts forward in Annex 1 a list of 11 critical infrastructure sectors. The list of CIP sectors contained in Annex 1 may be amended through the comitology procedure in so far as this does not broaden the scope of the Directive. The degree to which this list has been adapted into national approaches varies. Within their national programmes, several countries have identified critical sectors or services that are not currently identified as critical by the European Commission, and several national programmes do not include some of the sectors included in the EC list. Some examples include:

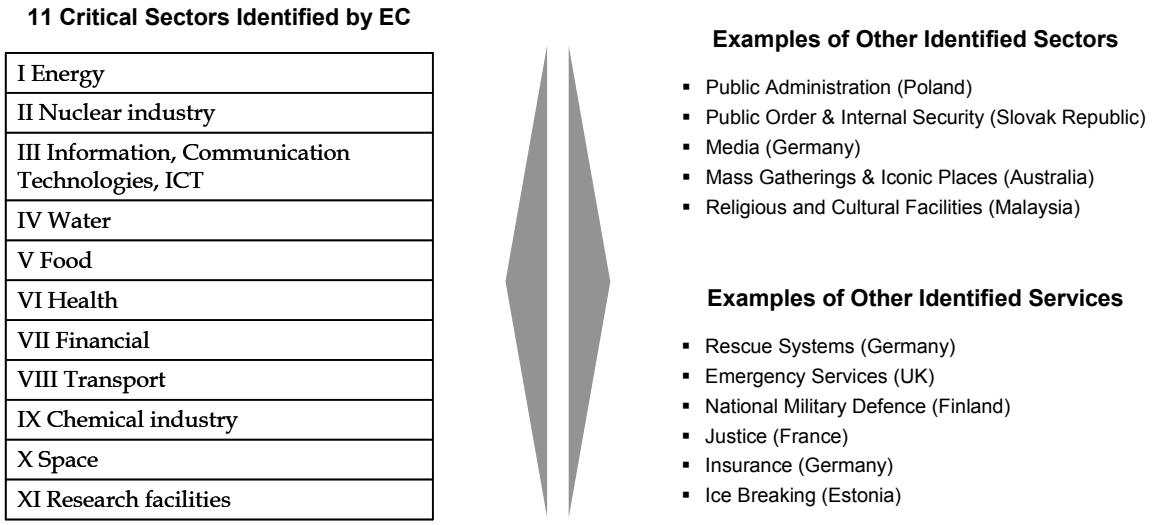


Figure 25: Comparison of Critical Sectors / Services

Regardless of the sectors or services identified as critical within national programmes, most Member States emphasized government agency leadership within the identified sectors and preferred not to name "key" operators. Along these lines, most Member States have assigned specific sectoral responsibilities to specific ministries or agencies in a format similar to the example shown in Figure 26:

Sector	Responsible agency/ministry
I Energy	Danish Energy Agency
II Information, Communication Technologies, ICT	National IT and Telecom Agency
III Water	Agency for Spatial and Environmental Planning
IV Food	Danish Veterinary and Food Administration
V Health	National Board of Health
VI Financial	The Danish National Bank Danish Financial Supervisory Authority
VII Public & Legal Order and Safety	Danish Ministry of Justice Danish National Police Danish Security and Intelligence Service
VIII Civil administration	Ministry of Defence DEMA Ministry of Foreign Affairs
IX Transport	Ministry of Transport The Danish Coastal Authority Danish Maritime Authority
X Chemical and nuclear industry	DEMA
XI Space and Research	Ministry of Science Technology and Innovation

Figure 26: Sector Responsibility Example: Denmark

There were several reasons cited by the Member States for this structure:

- Identifying and providing detailed information for all operators in all sectors was beyond the scope of the study
- Criteria for identifying "key" operators is not standardized across Member States
- Most Member State agencies with overall lead roles in CIP activities preferred to list only the responsible ministries / government agencies on the sectoral level rather than the private owners / operators
- A few Member State agencies with overall lead roles in CIP activities preferred to list only themselves (no other ministries) as a central point of contact and handle all requests for sector-specific information directly (rather than publish ministerial responsibilities by sector)

When discussing CIP-related initiatives on a sectoral level, many Member States called particular attention to their initiatives addressing the ICT sector and cyber security. While this does not necessarily indicate a lack of initiatives in the other sectors, it does tend to indicate that the centralized agencies with overall CIP responsibilities are focusing more in certain sectors than in others. Some examples of initiatives cited by these agencies include:

UK (Sector ICT)

- **Cyber Security Strategy - 2009**
  - The Government has published its **first national Cyber Security Strategy** alongside the annual update of the National Security Strategy
  - The Cyber Security Strategy refers to cross-Government partnership with business, international partners and the public on cyber security and announces the establishment of an **Office of Cyber Security and a Cyber Security Operations Centre**
  - CPNI is highlighted in the strategy as one of the organisations that interface on cyber security and as an example of partnership working with industry
  - CPNI has been fully engaged in the process for developing the strategy along with **Cabinet Office, GCHQ and other Government departments**, and supports it as a means of ensuring safety, security and resilience in cyber space.

Italy (Sector ICT)

- **Ministerial Decree of 9 January 2008**
  - The **Ministry of Interior** initiated activity to **identify critical information infrastructures** on a national scale
  - Identifies information infrastructures that support central government institutions and societies operating in the field of telecommunications, energy, health, and water management as **national critical information infrastructures**
  - The owners of these national critical information infrastructures must stipulate a **bilateral agreement with the CNAIPIC** to improve their security against cyber attack
  - Multiple ICT sector operators have begun to approach the government to **define the framework for bilateral agreements**

France (Sector ICT)

- **The Defence and National Security Whitebook - June 2008**
  - The **new strategy for defence and national security** includes, inter alia, the creation of a French **information security agency.** The mission of the agency will be to ensure the coordination of ministries in the prevention, alerting, and protection against cyber attacks, as well as cyber-crisis management
  - Within the new strategy, cyber-defence is considered a key capacity, and the cyber threat is given a high level of priority amongst the emerging threats. Early warning and detection are considered essential elements of the planned approach to **protecting the Internet,** which the strategy considers as a critical infrastructure
  - The Agency will report to SGDSN, which in-turn reports directly to the Prime Minister.

Figure 27: Examples of Sector-Specific Initiatives

Overall, the level of activity in cited each sector varied greatly from one country to another. However, as the detailed analysis of all initiatives in all sectors across all 29 countries studied was beyond the scope of the project, the initiatives cited should not be considered as all-inclusive. Instead, they represent the initiatives cited by the centralized national CIP agencies as potentially being of interest to other Member States. Deeper discussions with the responsible national ministries in any sector may result in more detailed information.

2 Austria

Figure 28: Austria

2.1 Summary

	Organisational Model	Strategy & Policy	Methods, & Standards	Public-Private Partnership & International Collaboration	Funding & Human Resources	Training & Exercises	Sector-specific Key-Players & Initiatives
Austria	▪ *No single national CIP organisation in place* ▪ *Federal Alarm Centre coordinates information in case of emergency*	▪ *Government resolution on CIP approved and under implementation* ▪ *Voluntary relief services integrated into Civil Protection system at regional level*	▪ *Government Resolution and Master Plan for CIP under implementation*	▪ *Bilateral Disaster Assistance Agreements in place with main confining states* ▪ *PPPs regarding ICT (A-SIT and CIRCA)*	▪ *€ 5-10 Mn budget in 2008 aimed at CIP programs*	▪ *Basic and advanced training for relief workers available* ▪ *Special training available at Universities*	▪ *Central European Gas Hub* ▪ *Adoption of a Transport Master Plan*

An Austrian national resolution and master plan for Critical Infrastructure Protection (CIP) was approved on April 2nd 2008. However, Austria currently maintains a decentralised CIP system, with no single national institution held solely responsible.

2.2 Organisational Model

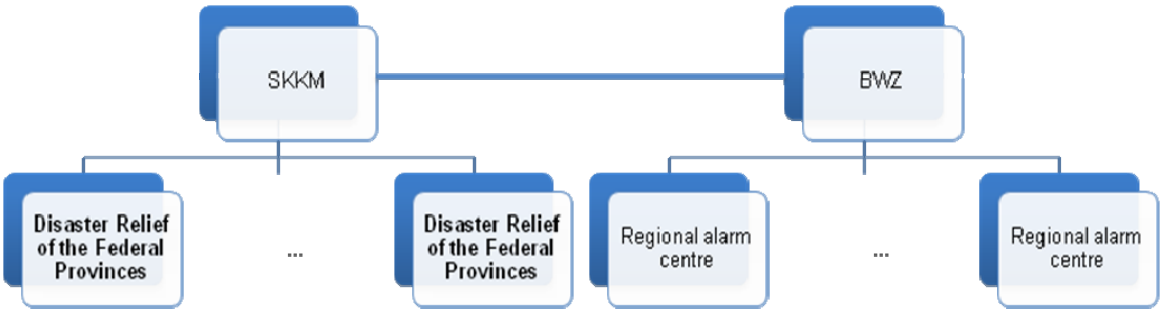


Figure 29: Organisational Chart (only CIP-related agencies shown)

Main Actors/Responsibilities:

- ***Federal Ministry of the Interior (Bundesministerium für Inneres)***[1]

  Department II/4 of the Federal Ministry of the Interior is responsible for civil defence, crisis and disaster management. This Department is organised in two units, the "National Crisis and Disaster Protection Management" and "International Civil Protection and Disaster Relief".
  Should a disaster affect the whole of Austria or several federal provinces simultaneously, the Department is responsible for providing coordination. An example of such a situation would be an accident involving a nuclear plant near the border, or perhaps another large-scale event occurring within the EU or elsewhere in the international community of nations. In addition to representatives from the Ministries, the Department also includes officers from the federal provinces responsible for disaster protection. The Department also represents Austria in the European Union on these matters.

- ***Austrian Civil Protection Association (Zivilschutz in Österreich ÖZSV)***[2]

  The "Austrian Civil Protection Association (ÖZSV)" is a collective comprising ten component associations – one federal organisation and nine regional offices. Their task is to provide civil defence information to the Austrian population, particularly on the actions they should undertake during an emergency situation.
  According to their 1993 statutes, the ÖZSV-Federal Association is responsible for:

  - improving civil self-protection through events, presentations and the dissemination of information to the population;

[1] http://www.bmi.gv.at
[2] http://www.zivilschutzverband.at

- coordinating collaboration with the regional offices of the ÖZSV;
- training and advising the population in matters of civil defence;
- preparing and assessing proposals for the creation of legal regulations within the framework of civil protection, and
- exchanging experience with foreign civil protection organisations.

The ÖZSV is, unlike the fire brigade and rescue organisations, not an intervention organisation active on an operational level, but one whose main task is to disseminate information to the population.
The Federal Association of ÖZSV acts on behalf of the Federal Ministry of the Interior and forwards information on self-protection to the public through two different channels:

- general public information on civil protection, and
- the organisation of safety and security information centres (SIZ) at a local community level.

- **The Federal Alarm Centre (Bundeswarnzentrale)**[3]

  The Federal Alarm Centre (BWZ) serves as the Federal operational hub for the coordination of relief measures in the event of a severe disaster. It has been part of the Action and Crisis Coordination Centre (EKC) at the Federal Interior Ministry since the beginning of 2006. The Centre is permanently staffed.

  In the event of disaster, the Centre serves as a central point for information collation and provision for the Federal Crisis and Disaster Protection Management (SKKM), as well as other national and international civil defence and disaster protection organisations. In the event of a natural or technological disaster in Austria or abroad, relevant information is forwarded to the BWZ, whose task is to rapidly secure the appropriate communication means and to coordinate all other crisis and disaster management activities. The BWZ serves as the Austrian focal point for several CIP organisations and systems, including:

  - The Temelin information hotline
  - The ECURIE System (European Community Urgent Radiological Information Exchange)
  - The IAEO (in accordance with the agreement on the early notification of nuclear accidents)
  - The European Commission's Directorate-General for Environment's Monitoring and Information Centre (MIC)
  - The EADRCC (Euro Atlantic Disaster Relief Coordination Centre within the framework of NATO-PfP)
  - The ESA/ESOC (European Space Agency/Operation Centre)
  - Notifications within the framework of the Agreement on the Transboundary Effects of Industrial Accidents (UN ECE).

[3] http://www.umweltbundesamt.at/umweltschutz/strahlenfruehwarnsys/

- **Federal Crisis and Disaster Protection Management *(Staatliches Krisen- und Katastrophenschutzmanagement, SKKM)*[4]**

  The SKKM is the crisis management body of the Federal Chancellery, and was established in 1986.

  Since May 2003, the coordination of national crisis and disaster protection management as well as international disaster relief, has fallen within the responsibility of the Federal Ministry of the Interior. Following a decision by the Council of Ministers on 20 January 2004, the "Federal Crisis and Catastrophy Protection Management (SKKM)" was reorganised. The most significant reform was the combination of the coordination bodies previously belonging to different portfolios into a new coordination committee, chaired by the Director General for Public Safety and Security. The committee includes representatives from all relevant federal ministries and provinces, operational organisations and the media. in the event of threats to larger geographic areas, the coordination of all measures necessary on a federal and provincial level fall within their responsibility.

  The committee becomes active not only in the event of a disaster, but is also responsible for coordinating planning and preparation prior to an incident occurring. Eight technical groups, for example, legal, technical and operational, undertake this role.

- **Disaster relief of the Federal Provinces (Katastrophenhilfe der *Bundesländer)*[5]**

  Measures to avert, respond to or recover from disasters (including both disaster relief and action planning) fall primarily within the responsibility of the Federal Provinces. The legal basis for this is provided by the Catastrophe Aid Act. This Act defines responsibilities particularly during the establishment of the disaster response, including operational responsibilities on a community, district and provincial level.

- ***Safety and Security Information Centres (Sicherheits Informations Zentrum, SIZ)*[6]**

  Under a Federal Ministry of the Interior initiative, initial steps were taken to establish "Information Centres on Self-Protection" in Austria´s local communities beginning in 1986. These Centres fall within the control of the local mayors, who also have existing responsibility for managing localised emergencies.

  In 2001, the Austrian Civil Defence Association was charged with the nationwide organisation and supervision of these centres, which were renamed "Safety and Security Information Centres (SIZ) ". These centres are given technical help by the relief and rescue organisations and financial support from the Federal Ministry of the Interior. The main tasks of these centres are providing general information to the public in matters of civil and self-protection, the organisation of courses, presentations and training at a local level, and the promotion of neighbourhood assistance.

[4] http://www.bmi.gv.at/zivilschutz/skkm.asp
[5] http://www.katastrophenschutz.steiermark.at
[6] http://www.sicherheitsinformationszentrum.at

- ***Ministry for Traffic, Innovation, and Technology (BMVIT)***[7]

  The Ministry for Traffic, Innovation, and Technology (BMVIT) is responsible for the safety of public critical infrastructure. It also operates as a coordinating centre for private owners and operators of critical infrastructure, and a centre for security research. The Ministry is also responsible for presenting options for CIP measures, targets, missions, and visions. The BMVIT also coordinates the Austrian Security Research Program, in which CIP will be considered. One of its recent activities has been to order an ICT master plan that is intended to analyse the strengths and weaknesses and the state of the art of Austria's critical infrastructure.

2.3 Strategy & Policy

- **APCIP Government Resolution (April 2008)**

  The Austrian government approved a resolution and a Master Plan regarding Critical Infrastructure Protection. Among other priorities, the resolution established the following sectors as critical:

  1. Constitutional Institutions
  2. Energy
  3. ICT
  4. Water
  5. Food
  6. Health and Social Affairs
  7. Finance
  8. Transport and Distribution Systems
  9. Chemical Industry
  10. Research Facilities
  11. Relief Units (Military, Red Cross, Fire Brigades)

  The resolution outlined an all-hazards approach focusing on the following factors:

  1. Man: consciousness, qualification, failure, criminal acts and terrorism, espionage
  2. Organization: concentration, outsourcing, logistic, participation of foreign capital (state funds), liberalization
  3. Nature, Ecology and Technology: catastrophes, epidemics
  4. ICT: complexity, dependence, interlinks, cycles of innovation, standardization, mobility
  5. Interdependence: dependencies, interaction, Domino effects

[7] ETH Zurich – CIIP Handbook – 2008

While implementing the resolution, the Austrian government has taken specific measures to ensure compliance with EU Directive 2008/114/EC. For example, since 2006 Austria has managed an EPCIP working group with members of responsible ministries. This group informed the Chamber of Commerce of the coming directive at an early stage and included it in planning activities. This effort was expanded to include informal information to regulators (electricity and gas) and companies in early 2009. The first official meeting with owners / operators of gas pipelines took place in May 2009, and with owners / operators of oil pipelines June 2009. The first official meeting with owner / operators of electricity networks was planned for June 2009. As of yet, the Ministry of Transport has not identified any ECI.

2.4 Methodology & Standards

The 2008 resolution and Master Plan for Critical Infrastructure Protection is the starting point for CIP activities in Austria, and it contains six key objectives:

- Objective 1: List of Austrian Critical Infrastructure (ACI)
- Objective: 2 Setting Priorities
- Objective: 3 Commitment of Standards for Security
- Objective: 4 Implementation of Commitments
- Objective: 5 Information management, Developing Partnerships CIP
- Objective: 6 Evaluation and Follow-up

Implementation has already begun on Objectives 1 and 5. An Interim Report to Federal Government is projected to be delivered at the end of 2009, and the completion of the implementation should take approx 5 to 10 years.

Although the private sector is the main actor, it is acknowledged that risk management should also be considered and implemented within the government and ministries. Several operators developed risk assessment methodologies and risk managements capabilities prior to the EPCIP or the Austrian Program. Standards such as ONR 4900 and ISO 31000 are the basis of these, and within the Austrian Standards Institute several working groups are seeking to develop a more detailed risk assessment methodology[8]

2.5 Public – Private Partnership & International Collaboration

The objectives of cross-border CIP cooperation typically include the improvement of early warning systems, the introduction of national focal points for disaster communications, the maintenance and provision of resources for cross-border operations, joint projects for training and simulation exercises, and cooperation in disaster prevention. Since the 1980s therefore, international organisations, particularly the United Nations (UN), the NATO Partnership for Peace, as well as the EU, have aspired to develop concepts for the improvement of international assistance and cooperation in the event of disasters.

[8] Booz&Company survey “Stock-taking of Existing Critical Infrastructure Protection Activities”

Austria has signed bilateral disaster assistance agreements with almost all of its immediate neighbours and with several other countries within and outside Europe. These agreements most commonly regulate cooperation for the prevention and management of disasters, especially by defining communications focal points, facilitating border transits for emergency teams, and simplifying the entry and exit of goods and equipment required for the provision of assistance. For example, Austria has concluded 25 bilateral agreements in the fields of emergency aid, radiation and environmental protection, and aerial ambulance services. Such bilateral emergency agreements have been concluded with Germany, Liechtenstein, Switzerland, Slovakia, Slovenia, Czech Republic, Hungary, and Jordan.

In the field of nuclear security, bilateral agreements with Slovenia, Hungary, Poland and the Ukraine have been negotiated. These are in addition to the IAEO agreement on early and immediate notification and mutual assistance in the case of nuclear incidents. Furthermore, a pertinent agreement with Switzerland was signed. The agreement completed with the Former German Democratic Republic is now applicable to the entire Federal Republic of Germany. The same principal applies to the agreement agreed with the former Czechoslovakia, which is now applicable to the Czech Republic and Slovakia.

To enhance environmental protection, an agreement on the transnational effects of industrial accidents was signed within the framework of UN/ECE (Economic Commission for Europe). Furthermore, special treaties on cooperation in the field of environmental protection have been signed between Austria and the Czech Republic, Hungary and Poland.[9]

Information and Communication Technology Public-Private Partnerships[10]

- Computer Incident Response Coordination Austria

Within Austria, the electronic communication network of the private sector is managed by the Federation of the Austrian Internet Service Providers (ISPA), whereas the Federal Chancellery has the lead for the public sector. Computer Incident Response Coordination Austria (CIRCA) is Austria's main IT early-warning system. It is a Public-Private Partnership (PPP) whose core contributors are the Federal Chancellery, ISPA, and A-SIT. Other members include representatives of the social partners (economic interest groups), the federal states and other critical infrastructure providers. It is established as "a web of trust" between participating Internet Service Providers (ISPs), IP network operators from the public and private sectors, and IT security providers.

The aim of CIRCA is to provide an early-warning system against worms, viruses, distributed denial-of-service attacks, and other threats that endanger IP networks and their users. To do so, they issues alerts and risk assessments and provides information about precautionary measures. Its strategy is both proactive and reactive, and involves a continuous exchange of information and news between the Federal Chancellery and CIRCA.

[9] http://www.unisdr.org/eng/mdgs-drr/national-reports/Austria-report.pdf
[10] ETH Zurich – CIIP Handbook – 2008

2.6 Funding & Human Resources

The main funding for CIP in Austria is provided by the Ministry of Research. In 2008, the budget was approx. € 5-10 Mn, and this is expected to remain stable for the next three years.

These funds have been used to foster CIP research, development and analysis. Currently, CIP activities employ 1-10 public employees, primarily working on countermeasures implementation and coordination[11].

Austria also deploys a world-class network of non CIP-specific emergency management resources. These include more than 4800 fire fighting squads and 900 ambulance centres employing 250,000 active fire fighters and more than 40,000 emergency medical technicians. These services receive their financial resources from both federal and provincial government.

2.7 Training & Exercises

Training of disaster relief workers is provided by Provincial Civil Protection Schools, schools run by relief organisations themselves, and by the Civil Protection School of the Federal Ministry of the Interior. The Civil Protection School of the Federal Ministry of the Interior is an interdepartmental institution that provides basic as well as advanced training. Courses at the Civil Protection School of the Federal Ministry of the Interior include disaster relief, radiation protection, and transport of dangerous goods. The "Security Academy" of the Ministry of the Interior offers training for police forces as well as for other authorites.

Some universities also offer special training. For example, the University for Health Sciences, Medical Informatics and Technology (UMIT) in Innsbruck offers an interdisciplinary two year part-time course in "socioeconomic and psychosocial crisis and disaster-management".

2.8 Sector-Specific Key Players & Initiatives

ENERGY

Initiatives:

In 2008, OMV and Gazprom developed the Central European Gas Hub, based on the Baumgarten underground gas storage facility, as one of continental Europe's leading hub platforms, and to establish a gas exchange there for trading on spot and futures markets for gas products.

INFORMATION AND COMMUNICATION TECHNOLOGIES

Public authorities:

[11] Booz & Company survey "Stock-taking of Existing Critical Infrastructure Protection Activities"

- **Austrian Regulatory Authority for Broadcasting and Telecommunications *(Rundfunk und Telekom Regulierungs GmbH RTR-GmbH)*[12]**

  The Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR) provides operational support for the Austrian Communications Authority (KommAustria) and the Telekom-Control Commission (TKK) in the fulfilment of their duties.

- **Austrian Communications Authority *(Kommunikationsbehörde Austria KommAustria)*[13]**

  The Austrian Communications Authority, also known as KommAustria, is the regulatory authority for the Austrian broadcasting industry. KommAustria is responsible for issuing licenses to private television and radio stations, managing broadcasting frequencies, handling the legal supervision of private broadcasters, and preparing and launching digital broadcasting in Austria.

FOOD

Public authorities:

- **Austrian Agency for Health and Food Safety *(AGES)*[14]**

  The Austrian Agency for Health and Food Safety (AGES) was formed from the June 2002 merger of five Federal Public Health Laboratories, three agricultural research centres, five food control institutes and four veterinary institutes. The legislation governing the establishment of the Agency mandates that its main objective is to ensure the health protection of humans, animals and plants by an effective and efficient evaluation of food safety and by the epidemiological surveillance of communicable and non-communicable infectious diseases.

  On February 1, 2004, the Agency was also made responsible for the supervision of medicine and medical devices inspections.

FINANCIAL

Public authorities:

- **The Federal Ministry of Finance *(Bundesministerium für Finanzen)*[15]**

  The Federal Ministry of Finance is the nation's highest financial authority and is the centre of financial and economic policy of Austria.

TRANSPORT

Public authorities:

[12] http://www.rtr.at
[13] http://www.rtr.at
[14] http://www.epiet.org/institutes/Vienna.html
[15] https://www.bmf.gv.at/

- **Federal ministry for transport, innovation and technology *(Bundesministerium für Verkehr, Innovation und Technologie BMVIT)*[16]**

  The Federal ministry for transport, innovation and technology (BMVIT) is the nation's peak civil transportation authority. It is divided into five departments, three of which are devoted to transportation affairs. These are:

  Department II Roads and Aviation (Group Roads, Group Aviation)

  Department IV Rail, Water Transport and Transport Labour Inspectorate (Group Transport Labour Inspectorate)

  Department V Infrastructure Planning and Financing, Coordination

- ***Austro Control GmbH*[17]**

  Austro Control is the official aviation agency and provides air navigation services such as air traffic management, aeronautical information services, air traffic telecommunications, and air safety systems. As the nation's official aviation agency, Astro Control is also responsible for the inspection of airworthiness and operational safety, the supervision of aviation companies, airworthiness certification, staff identity documents for civil aviation personnel, monitoring of compliance with aviation regulations, and the authorisation of flights into and out of Austrian airports and overflight transits.

SPACE

Public authorities:

- ***Austrian Space Agency*[18]**

  The Austrian Space Agency (ASA) was established in 1972 by the federal government in Vienna. Its purpose is to serve as a focal point for the co-ordination of space activities in Austria and is the Austrian link to international space activities. In 1987, Austria became a member state of the European Space Agency.

RESEARCH FACILITIES

Public authorities:

- **The Austrian Research Promotion Agency *(Österreichische Forschungsförderungsgesellschaft)*[19]**

  The Austrian Research Promotion Agency (FFG) is the national funding institution for applied industrial research in Austria. It offers a comprehensive range of services for Austrian enterprises, research institutions and researchers. These include the management of public funding programmes, consulting services in all phases of technology development and innovation, support for integration into

[16] http://www.bmvit.gv.at/en/verkehr/index.html
[17] http://www.bmvit.gv.at
[18] http://www.asaspace.at/
[19] http://www.ffg.at

European research programmes and networks, and the promotion of Austria's interests at the European and the international level.

3 Belgium

Figure 30: Belgium

3.1 Summary

	Organisational Model	Strategy & Policy	Methodology & Standards	Public-Private Partnership & international Collaboration	Funding & Human Resources	Training & Exercises	Sector-specific Key-Players & Initiatives
Belgium	▪ There is no single specific agency dedicated to CIP ▪ Presence of a Crisis Centre, but not specifically dealing with CIP	▪ Belgium has a decentralised approach to CIP ▪ Each Ministry is responsible for its own competence area	▪ Not Applicable	▪ Participation in alert networks (Ecurie, BICHAT, MIC, etc…)	▪ Not Applicable	▪ Not Applicable	▪ No specific CIP-related initiatives available

20

CIP in Belgium is managed in a decentralised manner, with no single agency dedicated to the issue. Each Ministry or agency is responsible for its own area of competence or responsibility.

In Belgium a distinction is made between emergency situations that arise as a result of a national crisis and those that arise as a result of an international crisis. Severe accidents, natural and industrial disasters fit into the national category. International crises usually fit into a political and/or military framework, and typically originate beyond national borders. These types of crises are generally managed within a framework of multilateral organisations.

20 Not Applicable = Open source research, web-based surveys and individual interviews have not provided information/data on this data point

3.2 Organisational Model

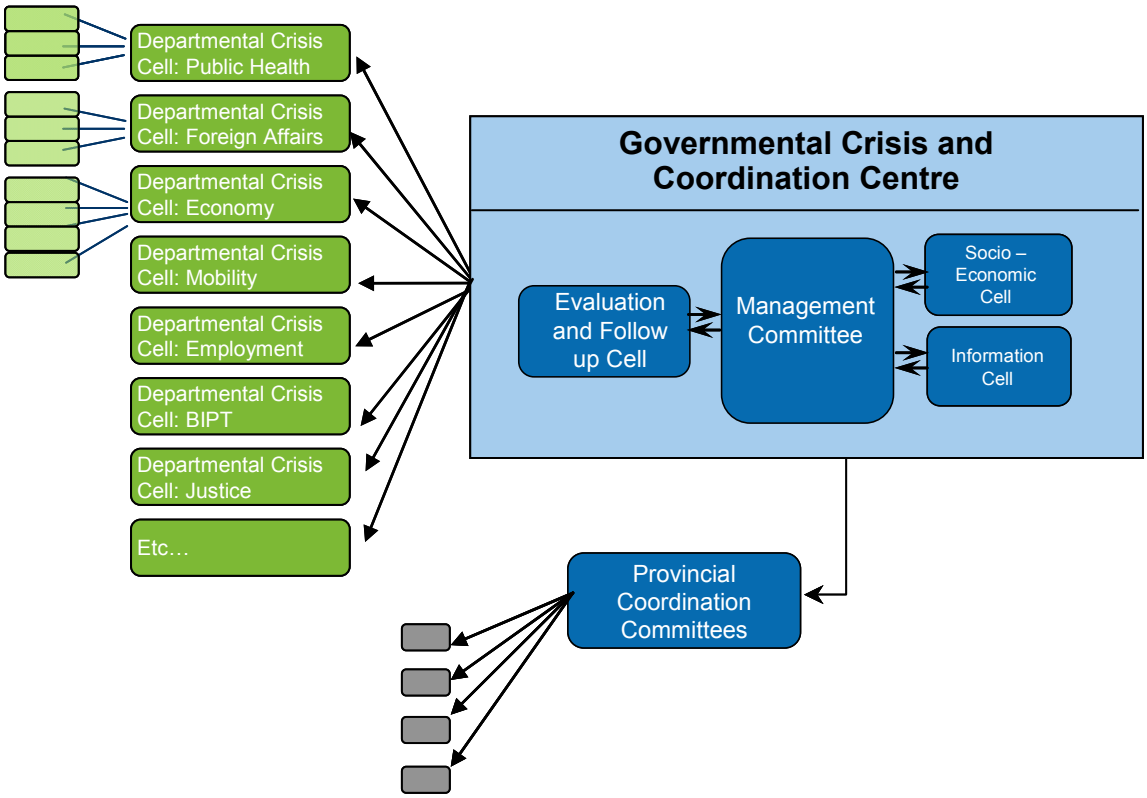


Figure 31: Organisational Chart (only CIP-related agencies shown)

Main Actors/Responsibilities

Federal Public Services, FPS[21]

In Belgium the federal administrative structure is no longer based on the ministries. Under the 2000 'Copernic' reforms, the 'ministries' were renamed 'Federal Public Services' (FPS). The Ministry of Defence alone retained its former name.

The tasks entrusted to the FPSs are the same as those given to the former ministries. This means that each FPS still has a minister, even though the emphasis is now on providing services to citizens.

A number of Federal Public Planning Services (PPS) have also been created alongside the FPSs. PPS handle ad hoc matters associated with socially-based issues that require coordination between several FPS.

Home Affairs FPS[22]

The Home Affairs FPS is responsible for preparing and implementing policies for police, civil security, and crisis management.

Centre Gouvernamental de Coordination et de Crises, CGCCR

[21] http://www.belgium.be/en/about_belgium/government/federal_authorities/federal_and_planning_public_services/

[22] http://www.ibz.be/news/nl/default.shtml

(Governmental Coordination and Crisis Centre)[23]

The Governmental Coordination and Crisis Centre has been established to assist the federal government in the planning and interdepartmental management of crises and major events. Its main tasks are:

- Risk analysis and emergency planning.
- Evaluation of unfolding global events and news reporting to assess the possible impact on Belgium and Belgian interests.
- 24hr a day continuous monitoring in collaboration with the police and information services.
- Planning, coordination and follow-up of major events.
- Infrastructure and organisation for crisis management.
- Coordinating the security of important persons and institutions in Belgium, including visiting dignitaries, embassies, consulates and international institutions.
- Providing a focal point for national and international alarms.

Belgium Institute for Postal Services

Together with the Mixed Committee for Telecommunications (Comixtelec), the Belgium Institute for Postal Services is responsible for the resilience of public e-communications networks. Comixtelec primarily supervise the crisis planning undertaken by and for public electronic communications.[24]

3.3 Strategy & Policy

In Belgium, the federal Government and the ministries have overall responsibility for national security issues. Each minister is responsible for his competence area. In a national crisis, the Minister responsible for the Home Affairs FPS becomes the highest executive agent. They are responsible for overall co-ordination of the response, and supervises the standing Co-ordination and Crisis Centre of the Government (*CGCCR)*. Through this Centre, he or she manages national emergencies and works with the Integrated Police, the rescue services and the Civil Protection Corps.

3.4 Public – Private Partnership & International Collaboration

The CGCCR is the Belgian international focal point for the following alert networks and agreements:

- Ecurie (Nuclear alert system)
- BICHAT (Biological and Chemicals Attacks and Threats)
- IAEA (International Atomic Energy Agency)
- MIC (Monitoring and Information Centre - European Union)

[23] http://crisis.ibz.be/
[24] ENISA – Stock taking eCommunications Resilience – 2008

- EMSC (European Mediterranean Seismological Centre)
- Helsinki Convention on the transboundary effects in industry

3.5 Funding & Human resources

There is no evidence of CIP-specific funding and dedicated resources.

Regarding the management of crises, the General Directorate of Civil Safety has a staff of about 120 persons at the federal level and 650 permanent agents in its 6 operational units.

3.6 Sector-Specific Key Players & Initiatives

NUCLEAR INDUSTRY

Public authorities:

- ***Centre d'Étude de l'énergie Nucléaire, SCK•CEN (Centre for the Study of Nuclear Energy)***[25]

  SCK•CEN is the Belgian Nuclear Research Centre, a centre of excellence for research on nuclear science and technology and ionising radiation. The SCK•CEN mission gives priority to research on problems of societal concern such as the safety of nuclear installations, radiation protection, safe treatment and disposal of radioactive waste, the fight against uncontrolled proliferation of fissile materials, and education and training.

  SCK•CEN's main tasks are:

  - nuclear safety and radiation protection;
  - the medical and industrial applications of radiation;
  - the back end of the nuclear fuel cycle (nuclear reprocessing and management of radioactive waste);
  - nuclear decommissioning and decontamination of nuclear sites, and
  - the fight against nuclear proliferation

  SCK•CEN contributes research and development, training, communication and advisory services. This is done with a view to sustainable development, and takes into account environmental, economical and social factors.

INFORMATION AND COMMUNICATION TECHNOLOGIES

Initiatives:

In the event of a national crisis, the National crisis coordination centre gathers all the pre-prepared plans and works to coordinate the available civilian and military response assets. Comixtelec, with its constituent BIPT, and the military would be one of the advisors providing

[25] http://www.sckcen.be/sckcen_en/

the National Crisis Coordination Centre with information about the status of the e-communication networks.

The Electronic Communications Act (Articles 114-115)[26] imposes a series of security obligations on operators and providers. Article 115 also defines the priority categories of restoration in case of infrastructure disruption. In addition, the authorities have imposed additional measures on the operators, notably regarding the warning and information process. The security measures imposed on the operators are required to be financed by the operator.[27]

WATER

Public authorities:

In Belgium, it is the regions who are empowered to determine water policy in their territories.

FOOD

Public authorities:

- ***Health, Food Chain Safety and Environment FPS[28]***

  The Health, Food Chain Safety and Environment FPS is responsible for preparing and implementing strategies for public health (funding care establishments, organising the healthcare professions, and providing emergency medical assistance). It also has the task of preparing and implementing strategies for food safety and the protection of public health and the environment (standardisation of products, checks on cosmetics and tobacco, animal welfare, and sustainable production and consumption).

FINANCIAL

Public authorities:

- ***Finance FPS[29]***

  The Finance FPS collects and manages some 70 billion EUR in taxation annually. This FPS also responds to a series of collective needs. For example, it carries out audits on products and ensures that property transactions are conducted in a legally sound manner.

TRANSPORT

Public authorities:

- ***Mobility and Transport FPS[30]***

[26] Loi du 13 juin 2005 relative aux communications électroniques (Law on electronic communications) Moniteur Belge. 13 June 2005 (– not available in English). http://www.ibpt.be/ShowDoc.aspx?objectID=951&lang=fr , released on 20 June.
[27] ENISA – Stock Taking eCommunications Resilience 2008
[28] https://portal.health.fgov.be/portal/page?_pageid=56,512460&_dad=portal&_schema=PORTAL
[29] http://minfin.fgov.be/portail2/nl/index.htm
[30] http://www.mobilit.fgov.be/nl/index.htm

The Mobility and Transport FPS prepares and implements federal policy on mobility. In doing so, this FPS focuses on safety, the environment, social issues and the optimal integration of all modes of transport.

4 Bulgaria

Figure 32: Bulgaria

4.1 Summary

	Organisational Model	Strategy and Policy	Methodology & Standards	Public-Private Partnership & International Collaboration	Funding & Human Resources	Training & Exercises	Sector Specific Key Players & Initiatives
Bulgaria	▪ There is no single agency dedicated to CIP ▪ Ministry of State Policy for Disasters and Accidents created in 2006, and is on a developmental path to fully deal with CIP	▪ Bulgaria does not presently have a single centralised strategy to deal with CIP ▪ Each Ministry is responsible for their competence area in case of crisis	▪ Not Applicable	▪ National Fire Safety and Protection of Population Service collaborate with peers in the Balkans and in several countries over the world	▪ Not Applicable	▪ General training and education on civil protection available	▪ Summit on Natural Gas For Europe Security And Partnership

[31]

At the moment, Bulgaria has chosen to not employ a highly-structured centralised approach to CIP-specific issues. In 2006, the Ministry of State Policy for Disasters and Accidents[32] was established. Given its recent formation, it is still on a developmental pathway and has not yet fully matured its policies for emergency preparedness, security and critical infrastructure protection.

Due to the General elections in Bulgaria in July 2009, there is new Council of Ministers with a new structure. The new government is developing the Policy for Critical Infrastructure Protection in order to fulfil Bulgaria's requirements under COUNCIL DIRECTIVE 2008/114/EC (8 December 2008) on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. They expect this policy to be complete in late 2009.

[31] Not Applicable = Open source research, web-based survey and individual interviews were not able to determine any information for this element

[32] Decree of the Council of Ministers No 137 of 06.06.2006)

4.2 Organisational Model

Bulgarian legislation on accident prevention, preparedness and response includes:

- The Environmental Protection Act[33] which governs major accident prevention. This Act sets framework requirements for accident prevention, defines competent authorities, defines procedures for cooperation and coordination between the authorities, the operators and the public, and requires the drafting of on-and off-site emergency plans.
- The Crisis Management Act.
- The Ordinance on accident preparedness and response which define details for accident preparedness and response

Within Bulgaria, accident prevention, preparedness and response are managed as follows[34]:

- ***Competent authorities*** are the Ministry of Environment and Water[35] and a set of Technical and Control Authorities (TCA). The TCAs include: The Ministry of Health[36]; The State Agency for Civil Protection/Ministry of State Policy for the state policy in disaster prevention and management; The National Fire and Emergency Service; The State Agency for Metrology and Technical Surveillance[37]; The regional and local authorities.

- ***Preventive measures*** are coordinated by the Ministry of Environment and Water which is responsible for the consistent assessment of operator documentation, the establishment of common criteria and requirements; the shared training of experts; joint inspections, and establishing common reporting techniques.

- ***Emergency preparedness and response*** is coordinated by the national, regional and local committees for crisis management chaired by the State Agency for Civil Protection.

The **Ministry of Interior**[38] is composed of the following main units:

- ***The National Police Service*** is a specialised operational, search and guarding service of the Ministry of Interior. The Service undertakes its activities both independently and in co-operation with other state bodies, organisations and members of the public. It has the following main tasks: maintaining of public order; prevention, detection and investigation of crimes; countering the criminal activities of local and cross-border criminal groups or organisations; guarding the state border and carrying out border control, combating illegal migration and the traffic in human

[33] http://archive.bild.net/legislation/docs/9/epa.html
[34] Milena Novakova, "Building an effective partnership among competent authorities among competent authorities", High-level Commitment Meeting Under the Convention of the Transboundary Effects of Industrial Accidents 14-15 December 2005, Geneva
[3535] http://www.moew.government.bg/index_e.html
[36] http://www.mh.government.bg/
[37] http://www.damtn.government.bg/
[38] http://www.mvr.bg/en/default.htm

beings; the prevention of terrorist acts and neutralisation of terrorist and subvesive groups; organisation and implementation of security at sites of national importance; and administrative control over the residence of foreigners in Bulgaria.

- ***National Fire Safety and Protection of Population Service (NFSPPS)*** is a specialised service authorised to carry out state fire control, fire fighting and emergency rescue operations. The NFSPPS undertakes its activities through 28 regional units and a central Directorate, which manages and coordinates the regional units. There are district fire services and fire stations in each the municipalities and their distribution provides for good protection against fires, disasters and emergencies in the outermost regions of the country. One of the most important activities of the NFSPPS is fire prevention, and this is particularly achieved through working with children and youths.

- ***National Civil Protection Service Directorate General***[39] is a structure under the Ministry of State Policy for Disasters and Accidents. It was established by the Decree of the Council of Ministers No 137 in June 2006. The Service is an important part of Bulgaria's Life-Saving Integrated Rescue System. There are 28 Civil Protection Service regional directorates providing 15 professional life-saving teams. The main activities of the Service are the protection of the population, the national economy, and the nation's material and cultural assets. In the event of a disaster, the Service organises and conducts life-saving and urgent emergency-reconstruction activities. The Service and its territorial structures undertake these tasks in both peace and war-time.

- ***Specialised Directorates****:* Operative and Technical Information Directorate; Communications Directorate; Protection of Communications Directorate; Operational Search Directorate; Inspectorate Directorate; Information and Archives Directorate; Crisis Management and Mobilisation Directorate; Coordination, Information and Analysis Directorate; Legal Directorate; International Co-operation Directorate; Press Office and Public Relations Directorate; Human Resources Directorate; Financial Directorate; Logistic and Social Support Directorate; Financial Audit Directorate.

The Ministry of Foreign Affairs[40]

The Ministry of Foreign Affairs is the institution in the central state administration responsible for the foreign policy of the Republic of Bulgaria. The Ministry's activities are derived from the Constitution and laws of Bulgaria, and in the foreign policy sphere are in full compliance with the principles and norms of international law and the international treaties to which the Republic of Bulgaria is signatory.

The Ministry of Economy and Energy[41]

The Ministry of Economy and Energy was incorporated by decision of the Bulgarian Parliament in August 2005 through the merger of the Ministries of Economy and Ministry of

[39] http://www.cp.mes.bg/home?set_language=en
[40] http://www.mfa.bg/en/
[41] http://www.mi.government.bg/eng/

Energy and Energy Resources. It is responsible for the development of the economic and energy policy of the Bulgaria. Typical objectives of this policy include increasing the competitiveness of the national economy and its institutions, encouraging investment, innovations, entrepreneurship, exports, modernisation of the industrial base, stimulating measures on energy efficiency in industry, and the use of renewable energy resources. It also takes part it the implementation of the integration policy and effecting foreign economic cooperation.

Ministry of Environment and Water[42]

Is the leading state authority for environmental protection and its main objective is the high level protection for man and environment and sustainable development. The ministry is responsible for the management and control over dangerous substances, included major accident risk management (Prevention, Control and Containment, Mitigation, Restoration).

4.3 Strategy & Policy

Although Bulgaria maintains a wide range of capabilities for the protection of its citizens and national interests, "presently due to a variety of reasons, there is no comprehensive, well-focused and sustainable security and defence policy of the country that is clearly linked to its security and defence objectives."[43]

Security Policy[44] In today's globalised world and against the backdrop of new trans-national threats to international security Bulgaria is working to strengthen the cooperation among international institutions, both regionally and globally. A major foreign policy priority of Bulgaria is to be seen as a reliable and predictable ally and partner in NATO, the Organisation for Security and Cooperation in Europe (OSCE) and other international organisations. As an active member of these organisations Bulgaria plays an instrumental role in contributing to the achievement of a fairer and stable international order, based on the principles of international law, rule of law, democracy and respect for human rights.

Bulgaria is a committed contributor to NATO's political dialogue, to transatlantic relations, the strategic NATO-EU partnership, the operations and missions of the Alliance, and the development of allied military capabilities. Bulgaria actively participates in OSCE activities to further strengthening her role in maintaining European security, in conflict prevention and regulation, and in post-conflict rehabilitation. An important dimension of Bulgarian foreign policy is the implementation of international treaties for non-proliferation, disarmament and arms control, and her participation in international organisations and regimes for export control.

Energy Act[45][46] This Act regulates the generation, importation, export, transmission, transit transmission, and distribution of electricity, heat and natural gas, and the transmission of

[42] http://www.moew.government.bg/index_e.html
[43] Hadjitodorov, S., Tagarev, T., and Pavlov, N. Shaping Bulgaria's Defence and Security R&T Policy, In proceedings of "Policy and Models for R&D Management in Support of Defence Industrial Transformation", Sofia, University of National and World Economy, 2007
[44] http://www.mfa.bg/en/index.php?option=com_content&task=view&id=7908&Itemid=363
[45] http://www.mi.government.bg/eng/norm/rdocs/mdoc.html?id=187497
[46] Promulgated in the State Gazette No. 107 of 9 December 2003, amended in the State Gazette No. 18 of 5 March 2004, amended in the State Gazette No. 18 of 25 February 2005, amended in the State Gazette No.

crude oil and petroleum products through pipelines, trade in electricity, heat and natural gas, and utilisation of renewable energy sources, as well as the powers of state bodies in formulating energy policy, regulation and control.

The principal purposes of this Act are to create conditions for:

- High-quality and secure supply of electricity, heat and natural gas to the population.
- Energy development and the energy security of the country through efficient use of energy and energy resources.
- Creation and development of a competitive and financially stable energy market.
- Energy provision at minimum cost.
- Sustainable development in renewable energy sources, including the production of electricity from these sources in the interests of environmental protection.
- Promotion of cogeneration.
- The development of infrastructures for the transmission of electricity, natural gas, crude oil or petroleum products within and through Bulgaria. The Act requires that the generation, import, export, transmission, transit transmission, distribution and trade in electricity, heat, natural gas, crude oil and petroleum products shall be carried out while guaranteeing the protection of the life and health of citizens, property, the environment, and the interests of consumers and the nation.[47]

4.4 Public – Private Partnership & International Collaboration

The National Fire Safety and Protection of Population Service co-operates with similar fire services in the Balkans and the rest of the world. NFSPPS staff contribute to international rescue operations in accordance with their EU obligations for co-operation and participation in international crises.

4.5 Training & Exercises

The ***training of the population in Civil Protection*** is achieved through the education system, higher school, the mass media and the specialised Civil Protection training centres. The aim of this training is to provide people with the knowledge and skills so that they behave correctly and are able to render help during a disaster or accident. Students are provided training in all grades of the primary and secondary school in special classes, providing them with a base level of knowledge and skill. For higher school students, the training is carried out by the disaster protection departments, according to their speciality. The training of the remainder of the population is carried out through the mass media and the specialised Civil Protection centres.

The Civil Protection forces themselves are trained according to a special programme. Special attention is paid to the development of high moral and psychological qualities, equipment proficiency, rescue and urgent emergency restoration techniques, and

95 of 29 November 2005, amended in the State Gazette No. 30 of 11 April 2006, amended in the State Gazette No. 65 of 11 August 2006, amended in the State Gazette No. 74 of 8 September 2006

[47] SG No. 74/2006, effective 8.09.2006.

interoperability during fires and other disasters and accidents. The training of the management authorities and the Civil Protection forces is financed under a separate budget by the State Agency for Civil Protection.

4.6 Sector – Specific Key Players & Initiatives

ENERGY

Initiatives:

- **The Summit on Natural Gas for Europe Security and Partnership**[48] is part of Bulgaria's efforts to achieve active, equitable and mutually beneficial dialogue with countries of the Black Sea and Caspian regions, Central Asia, the Middle East, and the EU. The goals of the Summit are to:
  - shape a new European energy policy;
  - seek new international arrangements and ensure durable guarantees for the energy security of Bulgaria, the region, and Europe as a whole;
  - help implement strategic energy resource transmission projects, and
  - help mitigate crisis situations related to oil and natural gas supplies to Europe.

NUCLEAR

Public Authorities:

- ***Nuclear Regulatory Agency***[49]
  State regulation of the safe use of nuclear energy and ionising radiation, the safety of radioactive waste management, and the safety of spent fuel management is implemented by the Chairman of the Nuclear Regulatory Agency (NRA). The Chairman is an independent specialised authority of the executive power. In accordance with the Safe Use of Nuclear Energy Act [50] and the Rules of Procedure[51] of the Nuclear Regulatory Agency (NRA), the Chairman of the Agency works with the executive authorities who have regulatory and control responsibilities for the use of nuclear energy and ionising radiation and the safe management of radioactive waste and spent fuel. He or she is required to propose to the Council of Ministers measures for coordinating these activities. Such coordination is continuous and is typically undertaken with the Ministry of Health, Ministry of Interior, Ministry of Environment and Water, Ministry of Defence, Civil Protection National Service, Customs, and the State Agency for Metrological and Technical Control.

INFORMATION AND COMMUNICATION TECHNOLOGY

Public Authorities:

[48] http://www.energysummit2009.bg/en/
[49] http://www.bnsa.bas.bg/
[50] http://www.bnsa.bas.bg/en/documents-en/legislation/laws/act-eng.pdf
[51] http://www.bnsa.bas.bg/en/documents-en/legislation/rulesofproced/rules-of-procedure.pdf

- **CERT Bulgaria**[52]

  CERT Bulgaria is the National Computer Security Incidents Response Team. It provides information and assistance to its constituencies to assist them in implementing proactive measures to reduce the risks of computer security incidents and respond to such incidents when they occur. CERT maintains an IT security database, sharing this information to help make Bulgarian IT environments more secure.

[52] http://www.govcert.bg/EN/Pages/default.aspx

5 Cyprus

Figure 33: Cyprus

5.1 Summary

	Organisational Model	*Strategy and Policy*	*Funding and Human Resources*	*Public-Private Partnership and international collaboration*	*Test, training and exercises*	*Methods, standards, operating plans and technology*	*Sector-specific initiatives*
Cyprus	▪ There is no single agency specifically dedicated to CIP ▪ CIP is managed under the same arrangements as any other emergency situations by the existing Civil Defence arrangements	▪ Cyprus dealing in an unstruc-tured way with CIP	▪ Not Applicable	▪ International Search and Rescue Advisory Group (INSARAG)	▪ International Urban Search and Rescue Exercise	▪ In the ICT industry, ISO27001 is a standard commonly used	▪ Not Applicable

53

The Republic of Cyprus does not maintain an agency devoted solely to Critical Infrastructure Protection (CIP) issues. CIP is not managed explicitly as a separate issue, and the management of emergencies in Cyprus relies on the Civil Defence organisations.

[53] Not Applicable = Open Source Research, Web-based survey and individual interviews have not shown information/data on the given argument

5.2 Organisational model

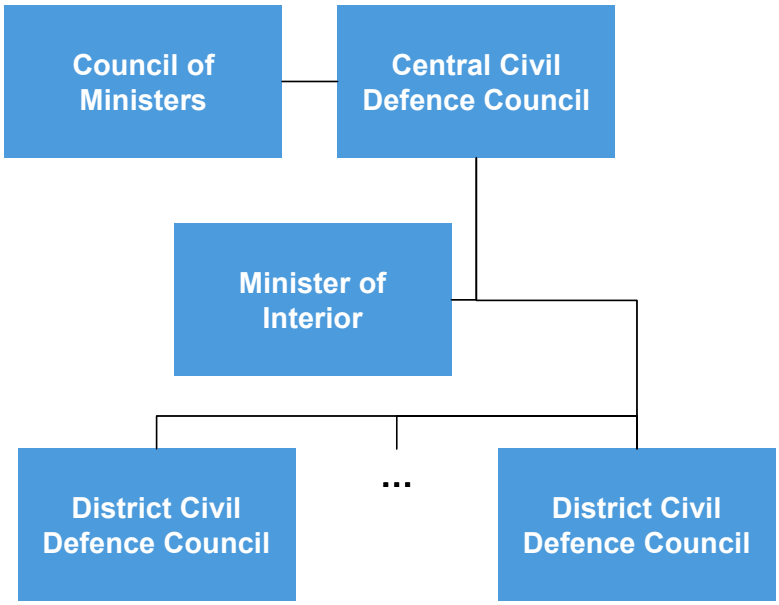


Figure 34: Organisational Chart (only CIP-related agencies shown)

Main Actors/Responsibilities

Minister of Interior[54]

The Minister of Interior on behalf of the Council of Ministers[55] is responsible for the implementation of the Civil Defence Law and the relevant regulations and has the overall supervision and control of the Civil defence System. Accordingly, civil defence in general is under the responsibility of the Ministry of Interior.

Council of Ministers[56]

The Council of Ministers may declare the administration of any Minister, any Governmental Department/Service or Independent Office, or any public or private corporation, as an "Essential Service" for civil defence purposes. Any such declaration has legal implications for the services concerned. It requires them to undertake planning and training, improving their preparedness and response capabilities in order to participate effectively in the Civil Defence System. The Council of Ministers may appoint a Central Civil Defence Council.

[54] http://www.moi.gov.cy
[55] http://www.presidency.gov.cy
[56] http://www.presidency.gov.cy

Civil Defence[57]

Civil Defence is a Department of the Ministry of Interior and its primary mission is the execution of measures to prevent natural or manmade disasters and to overcome their consequences.

5.3 Strategy and policy

The Council of Ministers is required to approve the General Civil Defence Plan which mandates the roles, duties and responsibilities of all the components of the Cypriot Civil Defence system when dealing with contingencies arising either because of war or disaster.

The Civil Defence Plan considers six main threats and defines the responsibilities of the Ministries of the Government:

- **Earthquakes**. Primary responsibility for the co-ordination of relief activities rests on the Ministry of Interior - Civil Defence Force.
- **Forest Fires.** Primary responsibility belongs to the Department of Forest of the Ministry of Agriculture, Natural Resources and Environment.
- **Rural Fires.** The Cyprus Fire Service (which belongs under the jurisdiction of the Ministry of Justice and Public Order through the Police) is responsible for fighting rural fires which are up to a distance of 1km from forests boundaries. The Fire Service is also responsible for fighting urban fires and those at airports.
- **Marine Pollution.** Primary responsibility rests on the Fisheries Department of the Ministry of Agriculture, Natural Resources and Environment. An existing contingency plan establishes the necessary arrangements for the effective and timely response to a marine pollution incident. A Regional Agreement has been signed between Cyprus, Egypt, and Israel to combat major pollution accidents in the Eastern Mediterranean.
- **Radiological emergencies.** The system for response to radiological emergencies is currently under preparation.
- **War.** Primary responsibility for civil defence in case of war lies with the Ministry of Interior - Civil Defence Force.

According to this national Plan, each component of the civil defence system has to develop their own subordinate Civil Defence Plans These plans are furnished to the Central or District Civil Defence Councils (respectively, depending on their level) for validation and co-ordination.

5.4 Funding and human resources

CIP activities in Cyprus are resourced through the funding provided to the Civil Defence organisations. The Civil Defence agencies are staffed by three different classes of member:

[57] http://www.moi.gov.cy/moi/cd/cd.nsf/dmlindex_en/dmlindex_en?opendocumen

- **Permanent Staff.** 31 organic, 45 secretarial, 10 supportive staff.
- **Volunteers.** 650 people serving under specific arrangements. 150 of them are rescuers. They serve for five years under special terms (renewable).
- **Conscript.** 7000 people (both male and female) serve for two years obligatory service. Women begin their service when they reach the age of 18, men after finished their service to the Military reserves.

5.5 Public – private partnership and international collaboration

Cyprus is member of:

- International Search and Rescue Advisory Group (INSARAG)[58]
- World Trade Organisation (WTO)[59]
- European Union[60] (Member state)
- Organisation for Security and Co-operation in Europe (OSCE)[61]

5.6 Test, training and exercises

INSARAG and Cyprus Civil Defence jointly organised the International Urban Search and Rescue Exercise in Cyprus in February 2006.

5.7 Methods, standards, operating plans and technology

In the Information and Communication Technology industry the ISO/IEC 27001 Information Security Management System (ISMS) appears to be the most commonly used standard.

5.8 Sector – key players and specific initiatives

ENERGY

Public authorities:

- ***Energy Service***[62]

[58] http://ochaonline.un.org/Coordination/FieldCoordinationSupportSection/INSARAG/tabid/1436/language/en-US/Default.aspx
[59] http://www.wto.org/
[60] http://europa.eu/
[61] http://www.osce.org/
[62] http://www.mcit.gov.cy/mcit/mcit.nsf/dmlenergyservice_en/dmlenergyservice_en?OpenDocument

The Energy Service of the Ministry of Commerce, Industry and Tourism[63] has primary responsibility for energy in Cyprus, specifically including:

– Monitoring and coordinating the supply and availability of sufficient energy capacity for domestic needs.

– Monitoring and participating in the development of European policy on energy issues.

Main operators:

- ***Electricity Authority of Cyprus (EAC)[64]***

  The Electricity Authority of Cyprus (EAC) currently holds a monopoly on electricity generation in Cyprus, although the market is open to other companies

Initiatives:

The energy policy of Cyprus is fully harmonised with the energy policy of the European Union. The main aim of the energy policy is the security of the energy supply and fulfilling the nation's energy demands.

NUCLEAR INDUSTRY

Public authorities:

- ***Department of Labour Inspection[65]***

  The core role of the Department of Labour Inspection (Ministry of Labour and Social Insurance[66]) is the safeguarding of adequate levels of work-place safety and health, the protection of the public and the environment from risks arising from workplace activities, major accidents, chemical substances, and from the use of ionizing radiation, and the preservation of the quality of the parts of the atmosphere of Cyprus. The Department comprises five Sections, the Safety and Health at Work Policy Section, the Industrial Pollution Control Policy Section, the Field Operations Section, the Quality of Air Section, and the Radiation Protection, Nuclear Safety and Radioactive Waste Management Section.

INFORMATION AND COMMUNICATION TECHNOLOGIES

Public authorities:

- ***Office of the Commissioner of Electronics Communications and Postal Regulation (OCECPR)[67]***

[63] http://www.mcit.gov.cy
[64] http://www.eac.com.cy/
[65] http://www.mlsi.gov.cy/mlsi/mlsi.nsf/dmlinsurance_en/dmlinsurance_en?OpenDocument&4 - 4
[66] http://www.mlsi.gov.cy/
[67] ENISA – Stock taking eCommunications Resilience – 2008

The OCECPR is the regulator responsible for issues related to the resilience of eCommunications networks. The OCECPR advises the Ministry for Communication and Work (responsible for electronic communications) and the Ministry for Finance (responsible for information society in general) on policy development, implement policies, and cooperate with providers.
Currently, the provisions concerning the resilience of Cyprus' eCommunication networks are very general and are typically inscribed in the licenses issued to providers.

- ***Ministry of Communications and Works, Department of Electronic Communication (DEC)***[68]

  The Minister of Communications and Works has overall responsibility for policy on all radio matters. The DEC is responsible for the management of the radio spectrum and advises the Minister on radio spectrum policy issues. DEC develops and maintains the National Frequency Plan, authorises the use of the radio spectrum (including the assignment of frequencies to broadcasting stations), and monitors spectrum usage.

- ***Cyprus Radio-Television Authority***[69]

  The Cyprus Radio-Television Authority is an independent regulatory body established under the Radio and Television Stations Law. The Authority responsible for private radio and television stations broadcasting in Cyprus, issuing and renewing their broadcasting licenses.

Main operators:

- ***Cyta***[70]

  Cyta is a semi-government organisation. It was established with the aim of providing, maintaining and developing a comprehensive telecommunications service, both nationally and internationally. Cyta is considered to be the leading provider of integrated electronic communications services in Cyprus.

- ***MTN Cyprus (ex Areeba)***[71]

  MTN is one of the largest telecommunications providers in Cyprus

- ***Cyprus Broadcasting Corporation (CyBC)***[72]

  The Cyprus Broadcasting Corporation (CyBC) is the public broadcaster of the Republic of Cyprus.

WATER

Public authorities:

- ***Water Development Department***[73]

[68] http://www.mcw.gov.cy/mcw/dec/dec.nsf/DMLindex_gr/DMLindex_gr?opendocument
[69] http://www.crta.org.cy
[70] http://www.cyta.com.cy/
[71] http://www.mtn.com.cy/
[72] http://www.cybc.com.cy

The Water Development Department is responsible for implementing the water policy of the Ministry of Agriculture, Natural Resources and Environment. The main objective of this policy is the rational development and management of the water resources of Cyprus. In achieving this, the responsibilities of the department are diverse and include:

– The collection, processing and classification of hydrological, hydrogeological, geotechnical and other data necessary for the study, maintenance and safety of the water development works.

– The study, design, construction, operation and maintenance of works, such as dams, ponds, irrigation, domestic water supply and sewerage schemes, water treatment works, sewage treatment and desalination plants.

– The protection of the water resources from pollution.

- ***Public Health Services***[74]

The Public Health Services of the Ministry of Health[75] are responsible for a wide spectrum of activities for the protection of consumers´ health. These include controls on the quality of the drinking water, the inspection of both public and private premises, the investigation of communicable diseases, the implementation of health education programs, the management and implementation of antimalaria work, and the control of bathing water quality.

Initiatives:

Cyprus' water policy focuses on the maximum potential exploitation of non-conventional water resources, such as recycled water, the use of which produces quantities of good quality water. Tertiary treated recycled water is used for the irrigation of existing cropping land and for recharging aquifers. Full exploitation of recycled water is a long-term and costly process, but its success will decrease or potentially eliminate the necessity to build more desalination plants.

As provided for in the Strategic Water Development Plan (for the period up to 2015) a number of additional water works are under development. In line with this plan Arminou dam has already been constructed on the Diarizos River, the construction of Tamassos Dam on Pediaios River, the construction of Kannaviou Dam on Ezousa River, and the construction of Klirou - Malounda - Akaki Dam on Akaki River are underway. The design stage of the Solea Irrigation Project has already commenced, while other small projects are at the feasibility stage.

FOOD

Public authorities:

[73] http://www.moa.gov.cy/moa/wdd/Wdd.nsf/
[74] http://www.moh.gov.cy/moh/mphs/phs.nsf/DMLindex_en/DMLindex_en?OpenDocument
[75] http://www.moh.gov.cy

- ***Public Health Services***[76]

  The objective of the Public Health Services of the Department of Medical and Public Health Services Department of the Ministry of Health[77] is the adoption of comprehensive preventive measures in the Environmental Health sector. To achieve this various programs are being implemented in cooperation with Local Authorities and other Departments. The Public Health Service is also responsible for food safety, and in protecting this they undertake the inspection of food premises, the monitoring and control of imported foodstuffs, and the official control of the food consumed, distributed, marketed or produced in the island.

HEALTH

Public authorities:

- ***Ministry of Health***[78]
  The mission of the Ministry of Health is the continuous improvement of the health of the population of Cyprus. They do this through the prevention of disease, and the provision to every citizen of high level health care - respecting the rights of every patient to high quality medical care delivered with dignity.

- ***Health Insurance Organisation (HIO)***[79]
  The HIO's main responsibilities are to:
  - Administer the fund established by the Law N.89(I)/2001 for financing of the National Health System.
  - Make the required arrangements to obtain affordable healthcare for all beneficiaries by contracting with healthcare providers that satisfy the relevant conditions and specifications
  - Coordinate and ensure the provision of high quality healthcare services by the contracted healthcare providers
  - Collect, analyse and report data on the provision of healthcare services

FINANCIAL

Public authorities:

- ***Ministry of Finance***[80]

[76] http://www.moh.gov.cy/moh/mphs/phs.nsf/DMLindex_en/DMLindex_en?OpenDocument
[77] http://www.moh.gov.cy
[78] http://www.moh.gov.cy
[79] http://www.hio.org.cy
[80] http://www.mof.gov.cy/

The Ministry of Finance aims to create conditions of internal and external financial stability by strengthening the economy's infrastructure and promoting social policy targets.

Main operators:

- ***Bank of Cyprus***[81]
  The Bank of Cyprus is the leading financial services organisation in Cyprus, with a dynamic presence in Greece and Russia and operations in the United Kingdom, Australia, Romania and Ukraine. The Bank is licensed by the Central Bank of Cyprus and operates under its regulation and supervision. The Bank's market share in total banking system deposits and loans in Cyprus, including credit cooperatives, is approximately 30% and 29%, respectively.

TRANSPORT

Public authorities:

- ***Department of Civil Aviation***[82]

  Department of Civil Aviation manages the operation, development and exploitation of airports, and controls air traffic and the connection of Cyprus with other countries by air. It began its operation in 1960 when Cyprus declared its independence.

CHEMICAL INDUSTRY

Public authorities

- ***Department of Labour Inspection***[83]

  The Department of Labour Inspection of the Ministry of Labour and Social Insurance is the competent authority for chemicals management and control in Cyprus. Special inspections that focus on the implementation of the legislation for proper classification, packaging and labelling of chemical products are performed by inspectors of the Department on local industries and outlets where these products are sold (e.g. importers, warehouses, stores, specialised shops for professionals, and supermarkets).

Initiatives:

In 2005, to reduce the burden of using the Greek language, the Department of Labour Inspection modified the regulations to allow the use of English language on the labels of dangerous products, which are used in research, analytical, pharmaceutical or other relevant laboratories, in packages up to 2.5 litres in volume.

[81] http://www.bankofcyprus.com/
[82] http://www.mcw.gov.cy/mcw/dca/dca.nsf/DMLindex_en/DMLindex_en?OpenDocument
[83] http://www.mlsi.gov.cy/mlsi/mlsi.nsf/dmlinsurance_en/dmlinsurance_en?OpenDocument&4

A similar problem is encountered with the Safety Data Sheets (SDS) of products that are intended to be used by professional users. The producing companies provide the Cyprus importers with the English or German version of the SDS, which the importers have to translate into Greek.

6 Czech Republic

Figure 35: Czech Republic

6.1 Summary

	Organisational Model	Strategy & Policy	Methodology s, Standards	Public-Private Partnership & International Collaboration	Funding & Human Resources	Training & Exercises	Sector-Specific Key Players & Initiatives
Czech Republic	▪ There is no specific Agency dedicated to CIP ▪ CIP-related issues are addressed by the Civil Emergency Planning Committee	▪ CIP is addressed in the "Security Strategy Document of the Czech Republic" document - but in an unstructured way	▪ Integrated Rescue System (rescue and clean-up operations)	▪ Cooperation with Austria on radiation emergency	▪ Managed within operators and agencies as an additional duty	▪ Nuclear safety Exercise "Zone 2008"	▪ No specific CIP-related initiatives available

[84]

In the Czech Republic, there is no single agency specifically devoted to CIP issues. Security matters, security policies and civil protection are under the control and supervision of the Czech Ministry of Interior. The Civil Emergency Planning Committee (June 2008) is responsible for civil emergency planning and for the coordination and planning of measures to safeguard the population and the economy, and the protection of critical infrastructure.

[84] Not Applicable = Open source research, web-based survey and individual interviews have provided information for these areas.

6.2 Organisational Model

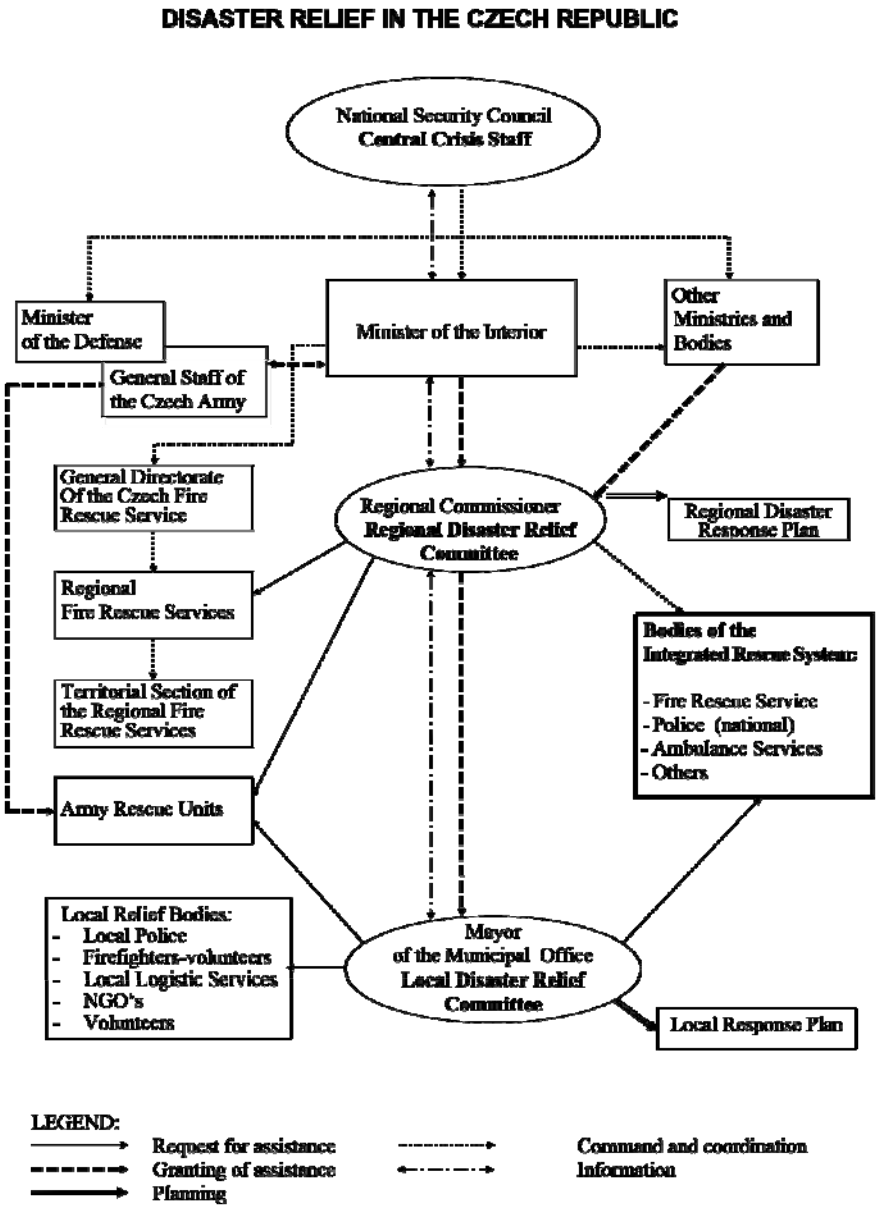


Figure 36: Organisational Chart (only CIP-related agencies shown)

Main Actors/Responsibilities

The Ministry of Interior[85]

The Ministry of Interior of the Czech Republic is the main body responsible for the overall coordination of CIP activities on both the national and international level. This role results from the Czech legislation particularly addressing areas of civil protection, public order provision and internal security, civil emergency preparedness, crisis management and integrated rescue systems.

This coordination role includes close and active cooperation with other central bodies of the state administration in the wide range of areas of the national economy. Regarding the selected and
at the national level approved areas of the critical infrastructure in the CR there are mainly cooperation in the areas of energy industry (electric power, gas, heat energy, oil), water resources management, food production and agriculture, public health, transport, communication and information systems, banking and financial sector, emergency service and public administration. The competent persons responsible were designated for the stated areas.

The Committee on Defence[86]

The Committee on Defence was established in the Chamber of Deputies[87] of the Czechoslovak National Council in 1920. It focused primarily on monitoring the emerging Czechoslovak Armed Forces. During the time of the Czechoslovak Federation, the national defence came under the competence of the federal authorities. After the election in 1992, the Committee for Legal Protection and Security was established at the first session of the Czech National Council at the instigation of a group of Deputies. After the 1993 dissolution of the Federation, the Committee became a committee of the Chamber of Deputies of the Czech Parliament. By its resolution of 27th January 1993 it changed the Committee's name to the Civil Defence and Security Committee. In the subsequent electoral terms, the Committee on Defence and Security was established. Its responsibilities include both internal and external security, and two separate committees, the Committee on Defence and the Committee on Security, were established.

Committee on Security[88]

The Committee on Security was established by a resolution of the Chamber of Deputies. It contributes to consideration of the Czech security budget, which includes funding for the Czech Ministry of the Interior, the Security Information Service, and the Czech Ministry of Justice (Prison Services Division).

Civil Emergency Planning Committee[89]

In its Resolution No. 671 of 2 June 2008, accompanying the Report on the Activities of the National Security Council, the Government of the Czech Republic has, among other items,

[85] http://www.mvcr.cz/mvcren/default.aspx
[86] http://www.psp.cz/cgi-bin/eng/sqw/fsnem.sqw?f1=8&f2=6&id=765
[87] http://www.psp.cz/
[88] http://www.psp.cz/cgi-bin/eng/sqw/fsnem.sqw?f1=8&f2=6&id=766
[89] http://www.vlada.cz/en/pracovni-a-poradni-organy-vlady/brs/pracovni-vybory/civilni-nouzove-planovani/civil-emergency-planning-committee-37864/

approved the "Statutes of the Civil Emergency Planning Committee"[90] [91]. The Committee is a standing working body of the National Security Council. It is responsible for civil emergency planning and for the coordination and planning of measures to safeguard the protection of the population and the economy and the ***protection of critical infrastructure.*** These include the implementation of measures to be taken in the event of a nuclear accident, preventative measures to be taken against the use of weapons of mass destruction – including solutions to mitigation any consequences of their use – and the harmonisation of requirements for any civil resources that might be required in order to maintain the security of the Czech Republic. The Committee is also involved in coordinating Czech security research.

The Committee is primarily responsible for the following activities:

- The evaluation and review of preparatory and conceptual planning.
- Facilitation of any necessary interdepartmental coordination of preparatory and conceptual planning.
- Evaluate the execution of the preparatory planning and conceptual measures and activities and propose the implementation of any necessary preventative measures.
- Evaluate, review and coordinate the activities of the Czech Republic representatives appointed to the bodies of the European Union, the North Atlantic Treaty Organisation (NATO) and other international entities.
- Review the Plan for the Creation of Civil Resources Required to Facilitate the Security of the Czech Republic.
- Coordinate Czech security research.

The Committee has 22 members under the Chair of the Interior Minister. The First Deputy Interior Minister is the Executive Vice-Chairperson of the Committee. Other members of the Committee include: Deputy Minister of Foreign Affairs; Deputy Minister of Agriculture; Deputy Minister of Defence; Deputy Minister of Finance; Deputy Minister of Industry and Trade; Deputy Minister of Transportation; Deputy Minister of Labour and Social Affairs; Deputy Minister of Culture; Deputy Minister of the Environment; Deputy Minister of Education, Youth and Sport; Deputy Minister of Health; Deputy Minister of Justice; Chairperson of the Council of the Czech Telecommunication Office; Chairperson of the State Office for Nuclear Safety; Vice-Governor of the Czech National Bank; Chairperson of the Administration of State Material Reserves; Director of the National Security Authority; Director of the Secretariat of the National Security Council; Director General of the Fire Rescue Service of the Czech Republic; President of the Police.

General Directorate of Fire Rescue Service of the Czech Republic[92]

The Czech Fire Rescue Service is one of the core elements of the Integrated Rescue System, which has been operating since 2001. The primary mission of Fire Rescue Service

[90] The Procedural Rules are being issued in accordance with Article 8 of the Committee's Statutes, approved under the Resolution of the Government of the Czech Republic No. 813 of 22 August 2001. Procedural Rules are approved In the Resolution No. 171 of 15 April 2008, issue by the National Security Council of the Czech Republic.

[91] The Committee was established under Resolution of the Government of the Czech Republic No. 391 of 10 June 1998 on the National Security Council and on the planning of measures to safeguard the security of the Czech Republic.

[92] http://web.mvcr.cz/archiv2008/hasici/indexen.html

is to protect the life, health and property of citizens against fire and to provide effective help in emergencies.

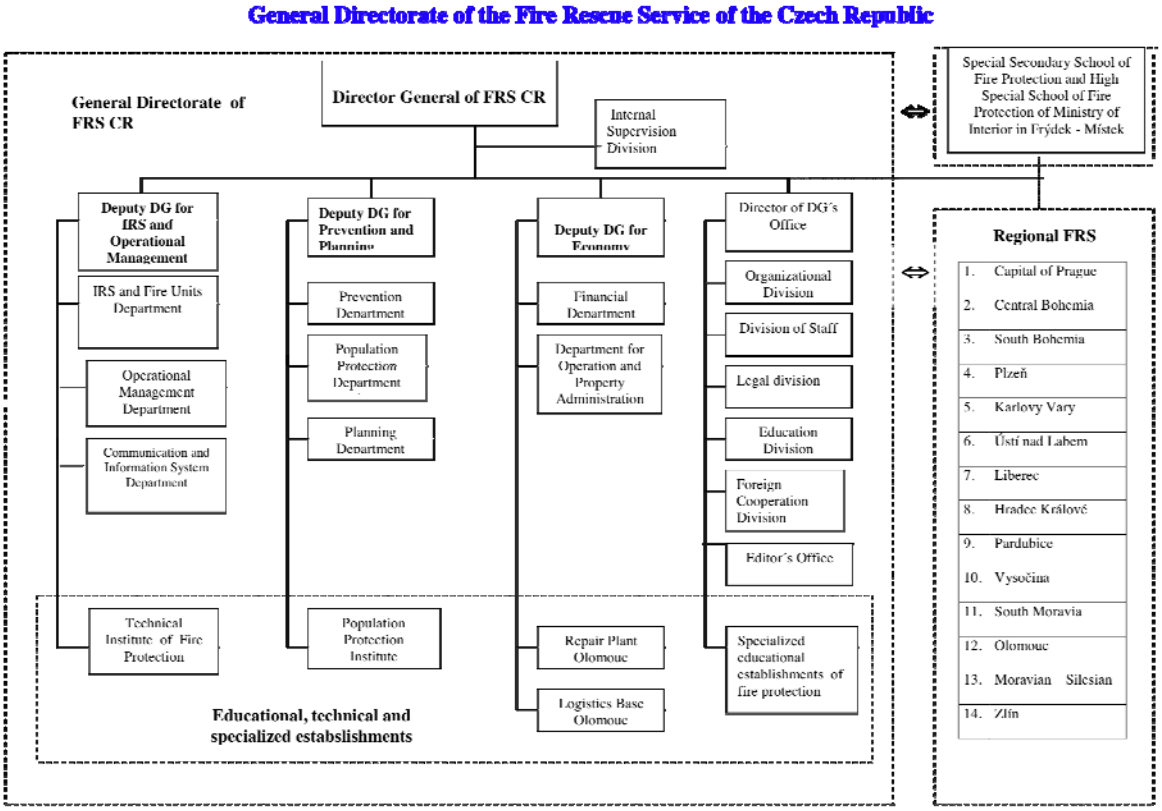


Figure 37: Organisational diagram – Czech Fire and Rescue Service[93]

Fire protection units[94]

Besides fire fighting, fire protection units contribute to rescue and clean-up operations during traffic accidents and HazMat leakage incidents, in technical interventions and to natural disaster response. They also undertake special tasks such as those connected with the prevention of spread of dangerous infections and diseases, with citizen protection against terrorist attacks, and dealing with disasters caused by unfavourable weather conditions.

Civil Protection[95]

The tasks of the Civil Protection include warning and evacuation, and the provision of emergency shelter.

The main objective of civil protection measures and procedures is to minimise the consequences of emergencies and to protect citizens, property and the environment. These measures and procedures are not undertaken in isolation, but as parts of an integrated crisis, emergency, or defence planning process. The Integrated Rescue System is an important tool for the co-ordination of organisations and services, both during and while preparing for emergencies, rescue and recovery.

[93] http://web.mvcr.cz/archiv2008/hasici/indexen.html
[94] http://web.mvcr.cz/archiv2008/hasici/izs/jednotkyen.html
[95] http://www.icdo.org/pdf/struc/czech-en.pdf

The Ministry of Industry and Trade[96]

The Ministry of Industry and Trade is the central Czech government body responsible for:

- The national industry policy, trade policy, foreign-economic policy, integrated raw materials policy, the use of mineral resources, energy, gas and heat production, mining, crude oil, natural gas, solid fuels, nuclear materials, and ores and non-ores treatment and conversion.
- Metallurgy, machinery, electrical engineering and electronics, the chemical industry, crude oil processing, the rubber and plastic materials industry, the glass and ceramics industry, the textile and clothing industry, the leather and print industry, the paper, cellulose and wood-working industry, building materials production, building industry production, medical production, junk and metal waste
- Technical standardisation, metrology and state quality control.
- Industrial research, engineering and technology development.
- Electronic communication and postal services.

The Ministry of the Environment[97]

The Ministry of the Environment (MoE) is the central state administrative authority and supreme inspection authority in environmental affairs. Its responsibilities include the protection of natural water accumulation, protection of water resources and the quality of groundwater and surface water, air protection, nature and landscape protection, conservation of agricultural land, operation of the National Geological Survey, protection of the rock environment including mineral resources and groundwater, geological works and environmental supervision of mining, waste management, environmental impact assessment of activities and their consequences, including transboundary, gamekeeping, fisheries and forestry in national parks, and national environmental policy.

Specific environmental risks are safeguarded under the jurisdiction of the ***Environmental Risk Department*** **(ERD).** They include environmental risks posed by chemical substances, related serious industrial accidents, and the handling of genetically modified organisms (GMOs). The ERD develops national damage prevention policies for these areas, develops systems for evaluating these risks, proposes indicators for their monitoring, and executes specialised state administration where provided for in relevant legislation.

The EDR also guarantees activities resulting from the country's membership in international organisations (UNEP, OECD – Chemicals Programme and Working Groups on Industrial Accident Prevention, Biotechnologies, and Nanomaterials) and from ratified international treaties (Rotterdam Treaty, Helsinki Convention on Transboundary Effects of Industrial Accidents, Cartagena Protocol on Biosafety, Stockholm Convention on Persistent Organic Pollutants) in its jurisdiction.

The Environmental Damage Department

The Environmental Damage Department is an element of the MoE and is the competent authority for contaminated sites management in the Czech Republic. The area of **prevention of serious accidents** caused by selected hazardous chemicals and preparations is

[96] http://www.mpo.cz/
[97] http://www.mzp.cz/

managed by the Ministry of the Environment as part of civilian emergency planning. The Act on Prevention of Serious Industrial Accidents is the basic legal regulation covering the prevention of serious accidents.

The Ministry of Transport (MT)[98]

The Ministry of Transport is a central state administration authority responsible for the Czech Republic's transportation policy and some elements of its implementation. Some of its main tasks include:

- The preparation, creation, and monitoring of the Czech Transportation Policy, including developing strategic and conceptual documents for the Ministry.
- Developing proposals for the construction of transportation networks, based on their economic efficiency, risk, and benefit analysis.
- The implementation of the State Environmental Policy, in the sphere of transportation..

6.3 Strategy & Policy

The basic principle of approach to protecting critical infrastructure in the Czech Republic is the provisioning and functioning of key and strategic infrastructures with the aim to ensure the protection of citizens. The starting point is to provide basic living conditions and needs of citizens and to ensure the necessary scope of management in the state and private areas that are focused on the maintenance of designated living conditions and needs.

For CIP issues in particular, the Committee for Civil Emergency Planning (CCEP) is responsible. This Committee is a working body of the State Security Council (SSC) and it has working groups that operate in ad-hoc mode. The outcomes of meetings are presented at the sessions of CCEP, SSC and the Government of the Czech Republic.

The Czech Republic began addressing CIP issues as they relate to natural disasters prior to EU institutional initiatives beginning to address this question. Therefore, individual steps were taken in keeping with the imminent needs. The Czech Republic has accounted for implementation of EU 2008/114/EC (dated to 8 December 2008), into the Czech legal order.

The main strategy that regulates Civil Protection and Critical Infrastructure Protection is the **"Security Strategy of the Czech Republic[101]".**

Other strategies related to sector specific security include:

- ***State Energy Policy (2004-2030)***[99] This policy is a reflection of the state's responsibility for creating conditions suitable for the reliable supply of energy. The policy establishes the legislative framework and rules for the operation and development of energy sector. In safety and security matters the policy provides for the safety of energy sources including nuclear safety; the reliability of supplies of all kinds of energy, and the reasonable decentralisation of energy systems.

[98] http://www.mdcr.cz/
[99] http://www.mpo.cz/dokument12265.html

- ***Transportation Policy of Czech Republic (2005-2013)***[100] This policy provides for the improvement of transport safety and security in such fields as road transport safety, rail transport safety, the transport of dangerous materials, transport security, and protecting civil aviation against unlawful acts.

The Security Strategy of the Czech Republic[101]

The Security Strategy of the Czech Republic is a fundamental document in the framework of the Czech Republic's security policy. It forms the basis of other security strategies and concepts, for example, the relevant parts of the Military Strategy of the Czech Republic and the Concept of the Foreign Policy of the Czech Republic.

The Security Strategy is a government document drafted in consultation with the Office of the President of the Republic and the Parliament of the Czech Republic on a non-partisan basis. The Czech Republic's security community, including representatives of public administration and the non-governmental sector, also took part in the drafting process.

The basic framework for formulating and implementing the Security Strategy is provided by the Constitution of the Czech Republic and Constitutional Act No. 110/1998. An integral part of the framework is the international commitments arising from the Czech Republic's membership of the North Atlantic Treaty Organisation (NATO), the European Union (EU), the United Nations (UN), and the Organisation for Security and Co-operation in Europe (OSCE).

6.4 Methodologies & Standards

Regarding the sector-specific and cross-cutting nature of the CIP, individual key decision makers and stakeholders respect relevant established methods, standards, and technologies. Regarding operational plans, duties to elaborate crisis plans and plans of crisis preparedness are integrated into Czech legislation. Other parts of established regulations include operational plans for the case of emergencies at different levels. Furthermore, enterprises are encouraged to elaborate their Business Continuity Plans.

Crisis, emergency and civilian emergency planning

Crisis management in the Czech Republic is managed under a complex set of procedures and provisions. These control the actions of relevant public administrations and authorities, and aim to minimise the undesirable impact of disasters on society. The processes to be followed are different depending upon whether the situation is connected with the defence of the Czech Republic against external attack (external safety) or more related to internal safety and security.

These crisis management arrangements are codified in Law No. 240/2000. Based on this, a state of danger can be proclaimed when a crisis is underway or imminent. Applied with other laws, this allows the proclamation of an emergency, or a state of country jeopardy or belligerency.

Crisis management includes not only the preparedness for crisis situations and for their solution, but also those activities which prevent incidents, and those necessary for the recovery of vital infrastructure following a disaster.

[100] Resolution of The Government of The Czech Republic of 13 July 2005, No 882
[101] (accessed on 2009/04/25)
http://www.mzv.cz/jnp/en/foreign_relations/security_policy/security_strategy_of_the_czech_republic.html

Crisis preparedness is provided by different means: organisational (creating of organisational structures, emergency planning, crisis planning), technical (system facilities - equipment etc.), and special abilities (training and education).

The response to and solution of a crisis situation involves providing rescue and clean-up operations, the implementation of measures for population protection, emergency survival, and measures to ensure public administration remains functional. These measures are commonly applied to protect critical infrastructure.

The Integrated Rescue System[102] (IRS) facilitates the co-ordination of rescue and clean-up operations when a situation requires the involvement of resources of several agencies, e.g. fire-fighters, police, medical rescue service. It may also be used where the rescue and clean-up operation is to be co-ordinated from the Ministry of Interior, the regional leadership, or by mayors of municipalities with extended responsibilities.

The IRS is also used to co-ordinated the activities of these agencies during the preparations for emergencies.

Agencies and organisations that participate in the IRS include the Fire Rescue Service of CR and fire protection units, Police of CR; Medical Rescue Service, the Civil Protection establishments, and those non-government Organisations (NGOs) and associations which can be assist the rescue and clean-up.

The coordination of the agencies working under Integrated Rescue is managed from the operational centres of regional Fire Rescue Services and the operational and information centre of General Directorate of Fire Rescue Service.

In 2005 fire protection units co-operated with other IRS bodies in 78,458 operations.

6.5 Public – Private Partnership & International Collaboration

PPP in the Czech Republic is based on established rules that take into account the ownership of vital parts of infrastructure. In the area of international cooperation, contacts are realised first at the level of main point of contact responsible for particular topics, and then followed-up with further networking within appropriate sectors at the expert level. Mutual information sharing is provided by the appropriate communication channels based on horizontal and vertical information flows.

Long-term information exchange and co-operation between Austria and the Czech Republic[103]

This agreement allows for the exchange of information and cooperation in the field of radiation emergency preparedness and the evaluation of the radiological consequences of nuclear power plant accidents. This program was initiated by the 'Melk Protocol' between the Czech and Austrian governments in December 2000.

Seminar of Crisis and Consular Unit Heads[104]

[102] http://web.mvcr.cz/archiv2008/hasici/izs/indexen.html
[103] http://rpd.oxfordjournals.org/cgi/content/abstract/109/1-2/105
[104] (accessed on 2009/04/25)
http://www.mzv.cz/jnp/en/issues_and_press/events_and_issues/x2009_04_02_seminar_crisis_consular.html

In April 2009, during the Czech Presidency of the EU Council, a seminar was conducted in Prague. It was attended by the Member States' crisis and consular unit heads and representatives of the European Commission and the EU Council's Joint Situation Centre. The event focused on the instruments of the European Commission and the EU Council used for the management of different types of crises, cooperation between Member States' consular and crisis centres and EU institutions, voluntary registration of travellers, and the sharing of experience with centres for consular assistance.

Water Management & Emergency Preparedness Knowledge Transfer[105]

The purpose of this project was to improve information management within the Morava River Basin of the Czech Republic. As such, the primary objective was to address training needs in the field of flood forecasting and warning systems, and in emergency management at the Water Authority, State Departments, District and local government as well as with the general public. The project demonstrated the roles and cooperation between municipal and provincial levels of authority in Canada during emergencies, with the objective of strengthening the interactions between the Water Authority and other national and local levels of government during and after flooding events within the Czech Republic.

Through a variety of activities that included workshops, know-how transfer and information management appraisal the project achieved the following objectives:

- Emergency preparedness and response were strengthened.
- Emergency management planning and communications were strengthened.
- Short-term flood warning systems will be improved.
- The ability of Water Authority and other stakeholders to build a cooperative and integrated response to emergencies will be strengthened.
- The ability to use remote sensing to assist in the emergency management process and to support the public information process will be strengthened.

6.6 Funding & Human Resources

CIP-activities are managed within the activities of individual stakeholders and integrated into the common approach of emergency and crisis management preparation.

6.7 Training & Exercises

The test of operation of vital infrastructures proceeds in accordance with established technical checks and regulations within the given sectors.

The Civil Protection Institute and the training centres of regional fire rescue brigades train the civil protection staff and general population in the field of citizen protection, protection against disasters and crisis management. This is provided by special courses and by information and

[105] http://www.golder.com/default.asp?PID=270&VID=353&LID=1

advisory services. The theme "Protection of Man at Extraordinary Situations" is taught in many subjects at primary and secondary schools.

ZONE 2008 Exercise[106]

The Ministry of Interior in co-operation with the State Office for Nuclear Safety (SÚJB) and Ministry of Defence prepared the national exercise "ZONE 2008". Held during November the exercise tested the performance of crisis management authorities, the integrated rescue system, and other emergency authorities at a simulated radiation incident at the Dukovany Nuclear Power Plant. According to the scenario, radioactive material is released from the power plant endangering the population in its vicinity.

The purpose of the ZONE 2008 exercise was to practise the central administrative bodies in the Vysočina and the South Moravia regions and municipalities in response to a simulated radiation incident, including urgent and consequent measures. The aim of the exercise was also to practise the activity of the integrated rescue system, the Czech Army and other stakeholders while implementing the external emergency plan for the Dukovany Nuclear Power Plant.

OASIS Exercise

The Czech Republic Ministry of Interior participates in the OASIS Project[107] (EU FP6). The objective of OASIS is to define and develop an Information Technology framework based on an open and flexible architecture and using standards, existing or proposed by OASIS, that will be the basis of a European Disaster and Emergency Management system. A series of exercises are conducted as part of the project. One of them was held in the Czech Republic in June 2008 involving a major flood – the most probable crisis for the country.

6.8 Sector – Specific Key Players & Initiatives

The range of sector-specific initiatives varies in accordance with the importance and activity of individual sector-specific representatives ,and it is dependent on the development of current and future situations in each sector. Early initiatives place more emphasis on increasing the awareness of experts, public administration representatives, private sector, and the population itself.

NUCLEAR INDUSTRY

Public Authorities:

- ***State Office for Nuclear Safety (SUJB)***[108]

  The SÚJB is a regulatory body responsible for the governmental administration and supervision of the use of nuclear energy and radiation, and of radiation protection (licensing, nuclear safety, waste management, safeguards).

[106] http://www.sujb.cz/
[107] http://www.oasis-fp6.org/index.html
[108] http://www.sujb.cz/?r_id=26

TRANSPORT

Public Authorities:

- ***Rail Safety Inspection Office***[109]

  The Rail Safety Inspection Office performs state supervision in rail-related matters of more than 900 rail infrastructure and transport operators, and investigates the causes of accidents and incidents of both domestic and foreign operators on Czech rail system.

- ***Railway Infrastructure Administration***[110]

  The Railway Infrastructure Administration manages the operation, maintenance and repair of national and regional rail assets and systems owned by the state. It allocates route capacity to carriers, drafts and releases the Railway Timetable, and is responsible for the modernisation of the Czech railway infrastructure.

- ***Civil Aviation Department***[111]

  The Civil Aviation Department manages issues related to the operation of air transportation and provides state administration and supervision of civil aviation. The functions as the supreme aviation authority, and is responsible for conceptual and systematic development of civil aviation and its operating systems, and the protection against relevant unlawful acts. Within the sphere of its expertise the Civil Aviation Department represents the Czech Republic in international organisations, it functions as an appellate body in administrative proceedings and contributes to the European Communities' legislation harmonisation program. It is composed of the following divisions: Air Transport Division; Flight Operations and Safety Division; Security Division; Conception and Development Division.

RESEARCH FACILITIES

Public Authorities:

- ***University of Defence***[112]

  The University of Defence (UoD) began operation in September 2004 to build on the traditions of the three former military colleges – Brno Military Academy, Military University of the Ground Forces (Vyskov) and Purkyne Military Academy (Hradec Kralove). The UoD's primary mission is the propagation of literacy, the development of thinking and independent scientific research in the issues vital for the Czech Republic's security, and the accomplishment of its Alliance obligations. The UoD's scope of work also includes the education and training of military professionals for the Army of the Czech Republic and undertaking research projects for the Ministry of Defence.

  However, the UoD's scope reaches beyond the defence department or even Czech Republic, where education and scientific research are concerned. It supports and develops specific branches focused on issues of national security and defence

[109] http://www.dicr.cz/
[110] http://www.szdc.cz/english/index.php
[111] http://www.mdcr.cz/en/Air+Transport/Civil+Aviation+Department/
[112] http://www.unob.cz/en/zakladni_informace.aspx

(particularly those of importance to defence industry) missing in other colleges and universities in the Czech Republic.

UoD's mission also includes the improvement of thinking on operational, strategic and military policy, providing support to departmental top management in those issues, and contributing to conceptual projects within the MoD's responsibility. It follows the principles of the Act 111/1998 on Universities, but in matters of organisation and personnel it is responsive to directions issued by the Czech MoD.

- ***Centre for Transport and Energy***[113]

  The Centre for Transport and Energy (CDE) is a non-profit non-governmental organisation that originated in 2000 by renaming the former Energy Efficiency Programme. The Programme was founded in 1995 as part of the Slunicko Foundation, and has functioned independently since 1998. The CTE sees its role as building and reinforcing a wide platform of groups and individuals who are interested in working towards a sustainable transport and energy future.

[113] http://cde.ecn.cz/index-en.htm

7 Denmark

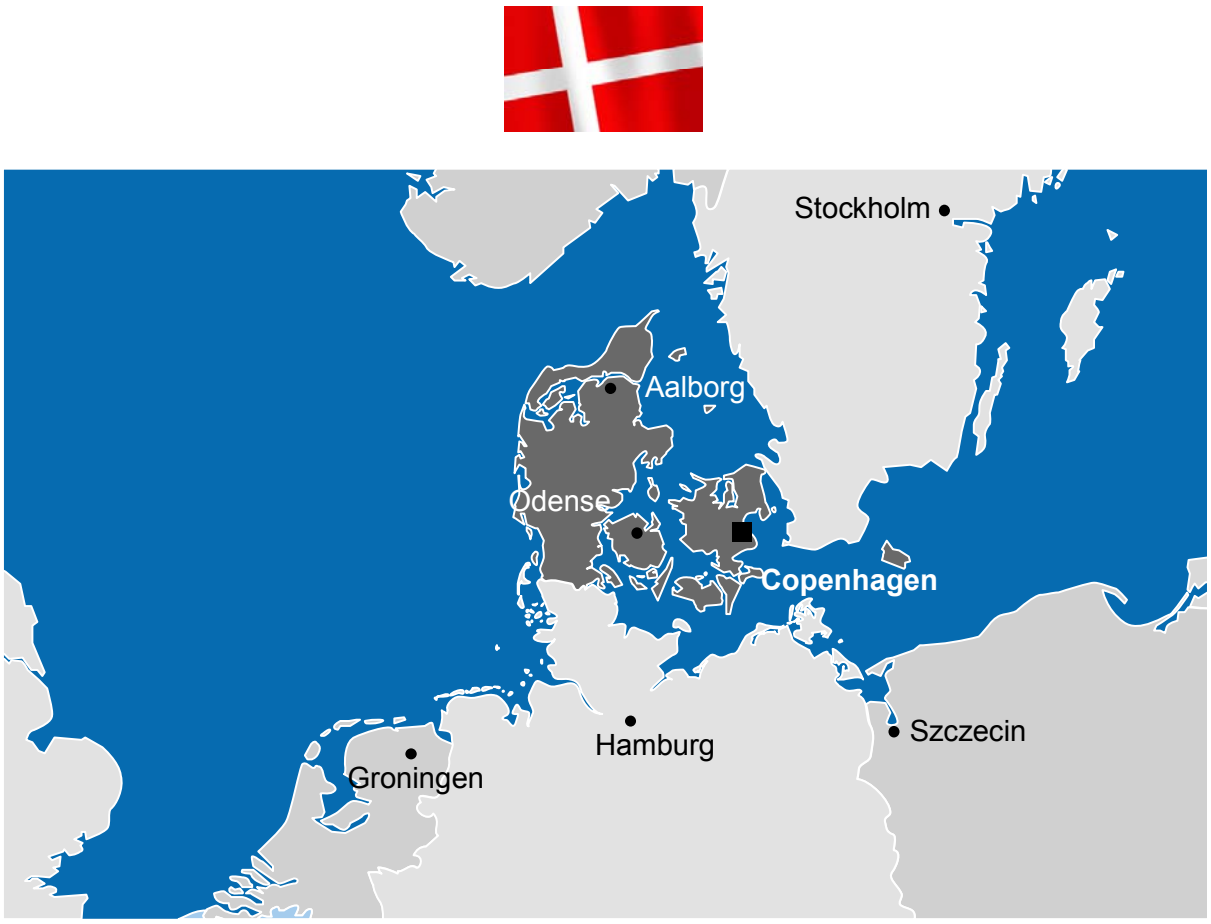


Figure 38: Denmark

7.1 Summary

	Organisational Model	*Strategy & Policy*	*Methodology & Standards*	*Public-Private Partnership & International Collaboration*	*Funding & Human Resources*	*Training & Exercises*	*Sector-Specific Key Players & Initiatives*
Denmark	▪ Emergency Management Agency (DEMA) with CIP responsibility reporting to Ministry of Defence ▪ CIP Contact Group (KG/KI)	▪ CIP activities guided by the Danish Preparedness Act	▪ DEMA RVA model defines methodology for defining Responsibility, Threats, Assessment, and Profile	▪ DSIS hosts a cross-sectoral public-private contact group	▪ No CIP-specific budget, integrated into Preparedness activities ▪ Approx. 30 government employees have secondary CIP responsibilities	▪ National KRISOV exercise on emergency mgmt ▪ Exercise Secretariat within DEMA to track exercises nationwide	▪ BERIT Forum for communi-cation infra-structures

The Danish Emergency Management Agency (DEMA) chairs the CIP Contact Group (KG/KI), which is the principal forum concerning cross-sectoral cooperation concerning CIP. The overall purpose of KG/KI is to serve as a forum for exchange of information and knowledge among relevant national authorities regarding CIP. Specific issues regarding sectoral CIP activities are dealt with at the level of the single responsible Ministry/Agency.

The main policy guiding the management of CIP activities in Denmark is the Emergency Management Act[114]. It is defined as a plan for the continual function of society under extraordinary conditions. It aims to ensure that the resources of civil society are utilised in a coordinated manner.

[114] http://www.beredskabsstyrelsen.dk/uk/danish_preparedness_act.htm#Part_4_

7.2 Organisational Model

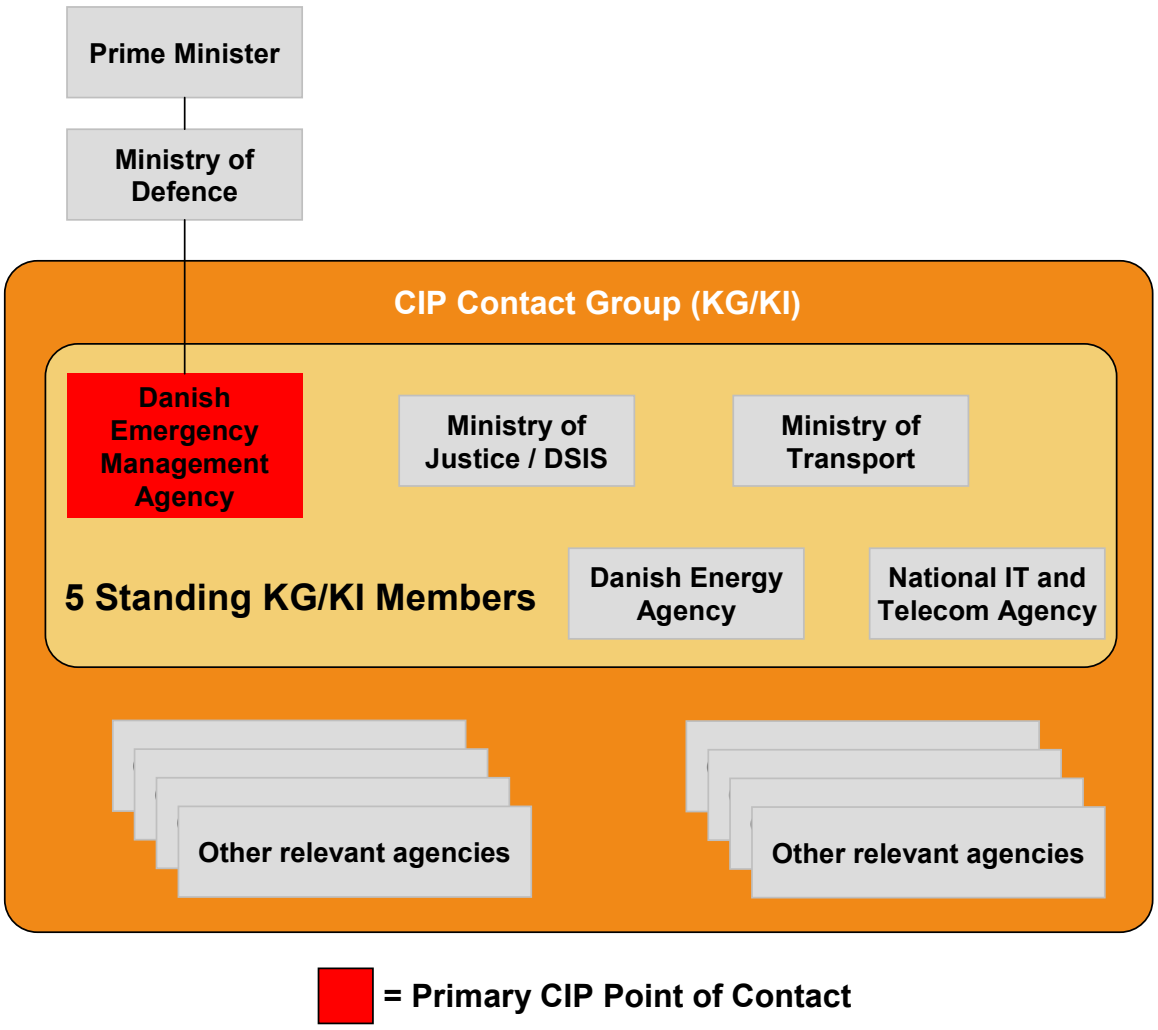


Figure 39: Organisational Chart (only CIP-related agencies shown)

Main Actors/Responsibilities:

- ***Forsvarsministeriet*** **(The Ministry of the Defence)**[115]

  The Ministry's work comprises overall planning, development, steering, and control of the entire ministerial area, including military defence. This Ministry also includes, DEMA, Defence Command Denmark, Home Guard Command, the Defence Intelligence Service, the Defence Judge Advocate General, the Defence Construction Service, the Royal Danish Administration of Navigation and Hydrography, the Office for Information and Welfare Service, Danish Defence Internal Audit, Ministry of

[115] http://www.fmn.dk/Eng/Pages/Front%20page.aspx

Defence Accounting Secretariat and others. The Ministry of Defence manages assignments for all Danish defence and civil functions associated to these assignments, including international assignments and co-operation activities in support of maintaining or establishing peace. Further assignments concern the establishment of secure navigation and surveillance of the waters around Denmark, Greenland, and the Faroe Islands including maintaining sovereignty of the territorial waters and similar tasks for the airspace.

- ***Beredskabsstyrelsen, DEMA*** **(The Danish Emergency Management Agency)**[116]

  The Emergency Management Agency is a government agency under the Ministry of Defence. The agency is the primary actor in work concerning coordination of CIP-related activities in Denmark. In addition, the Emergency Management Act tasks DEMA to manage the national fire and rescue service, supervise national and municipal fire and rescue services, and advise the authorities on matters of preparedness. The agency is also the primary actor in CIP-related activity in Denmark.

  By means of a number of political agreements, the emergency management has been continuously developed and adapted to the changing demands made by society and changes in the security-policy climate. This ensures an emergency management that is capable of intervening swiftly and flexibly in response to all types of accidents and disasters.

  DEMA works in closely structured co-operation with the EU, UN, NATO and several neighbouring countries.

- **Politiets Efterretningstjeneste, PET (Danish Security and Intelligence Service,DSIS)**[117]

  DSIS is the national security intelligence agency of Denmark. The agency is responsible for domestic security. The aim of DSIS is to prevent, investigate, and counter operations and activities that pose or may pose a threat to the preservation of Denmark as a free, democratic, and safe country. The main objectives of DSIS are to counter terrorism, counter extremism, counter espionage and prevent the proliferation of weapons of mass destruction. DSIS is part of the Danish police, but reports directly to the Minister of Justice.

- **Ministry of Transport**

  The Ministry of Transport creates the framework for transport and mobility. Mission includes roads and traffic, railways, airports, harbours, public transport and postal services.

- **IT og Telestyrelsen, NITA (National IT and Telecom Agency)**

  NITA is an agency under the Ministry of Science Technology and Innovation. NITA is responsible for central parts of the government's IT- and telecommunications policy. In addition, NITA is also the responsible agency as regards coordination of

[116] http://www.brs.dk/uk/
[117] http://www.pet.dk/

preparedness planning and CIP in Denmark within the IT- and telecommunications sector.

- **Danish Energy Agency**

  The Danish Energy Agency engages nationally and internationally in production, supply and consumption of energy - as well as the efforts to reduce emissions of greenhouse gases. The Agency is responsible for the whole chain of tasks linked to the production, transportation, and utilisation of energy, and the impact on the climate. The task is to ensure the legal and political framework for reliable, affordable, and clean supply of energy in Denmark. It is an agency under the Ministry of Climate and Energy.

7.3 Strategy & Policy

The extensive work undertaken in Denmark regarding CIP, as well as emergency preparedness and planning, is based on the fundamental principle of sectoral responsibility. Sectoral responsibility is described in Danish Emergency Management Act, where it is stated that each sector-responsible department, within its own sector, is required to plan for the maintenance of essential services in case of disasters and catastrophes. This planning responsibility also includes a duty to protect critical infrastructure since, by definition, this infrastructure makes up a substantial part of the foundation for the nation's essential services. As such, CIP is carried out as an integrated part of the overall emergency preparedness planning.[118]

Supplementing the efforts carried out by the sector responsible authorities, a number of authorities provide general advice and guidance on CIP, including the Danish National Police, Danish Security Intelligence Service (DSIS) and the Danish Emergency Management Agency (DEMA). In addition, DEMA, in accordance with the Danish Emergency Management Act, maintains a general responsibility of coordination concerning CIP. DEMA promotes emergency preparedness planning and ensures cross-sectoral coherence in the preparedness planning of the individual sectors.

- ***The Emergency Management Act***[119]

  Emergency intervention by the fire and rescue services, is regulated by The Emergency Management Act LBK no. 137 of 01/03/2004. The Emergency Management Act has replaced the Civil Defence Act, the Fire Services Act and the Civil Preparedness Act.

  Part 5 of the Act focuses on preparedness planning in the civil sector. Specifically, within their respective fields of administration, individual ministers shall plan for the maintenance and continuation of society's functions in the event of accidents and disasters, including actions of war, and in order to provide support to the defence forces.

[118] Booz & Co EU CIP Stocktaking Web-Based Survey, 2009
[119] http://www.beredskabsstyrelsen.dk/uk/danish_preparedness_act.htm

Further, the Act establishes a subsidiary approach by assigning the responsibility of drawing up of an overall plan for the preparedness of municipalities and counties to their respective councils, and by requiring the councils to send the plans to the Emergency Management Agency.

- **Danish Civil Preparedness**[120]

  Danish Civil Preparedness is defined as the planning for the continual function of society under extraordinary conditions. Civil Preparedness is basically a planning concept, or a principle – rather than an organisation. Its aim is to ensure that the resources of the civil society are planned and utilised in a coordinated manner. Areas of responsibility are, for example, water, food, health, electricity, and transport. The guiding principle is the principle of sector responsibility.

  The individual ministries are responsible for planning within their own respective areas in accordance with the principle of sector responsibility (§ 24,1 of the Emergency Management Act). Their tasks are to maintain the functions of the Government and public administration, producing necessary legislation and providing guidance to regional and municipal authorities.

  Furthermore municipalities and regional councils must likewise prepare contingency plans for all assignments that they are responsible for.

  DEMA has the coordinating responsibility on behalf of the Minister of Defence.

7.4 Methodology & Standards

Denmark follows an all hazards approach to risk assessment for critical infrastructure, not focusing on any single threat category.

As established in the government's emergency management policy from 2005, energy, transport and ICT have been identified as priority sectors for CIP. These sectors have, in addition, identified critical infrastructures within their own area of responsibility. Each sector is free to develop its own methodology to identify critical infrastructure. However, the RVA model (described in detail below) is made available as a general offer to interested sectors.

The methodology used in Denmark to evaluate the potential impact of/to a critical infrastructure is primarily assessed according to geographical impact. That is, how large the impact due to a loss of service is at local, regional or national levels.

National operators are required to have individual crisis management plans. However, they are not required to submit them to any national agency/body.

- **RVAmodel – DEMA's Model for Risk and Vulnerability Analysis**

  DEMA has developed the RVA model to promote risk and vulnerability analyses as a basis for preparedness planning. The RVA model is primarily intended as a generally applicable tool for voluntary use among government authorities. However, in principle

120 http://www.brs.dk/fagomraade/tilsyn/csb/Eng/civilpreparedness.htm

the model can be used by all interested parties with preparedness responsibility, both public and private entities.

The model provides for risk and vulnerability analyses conducted for a general purpose rather than at detail level. The model should therefore not replace other more specialised analytical tools that are already in use. It is, on the contrary, intended for organisations that want to use a general tool for risk and vulnerability analyses in their preparedness planning.

The model is devised to assess threats, risks and vulnerabilities in relation to those functions that are particularly critical for the effective functioning of society, including during major accidents or catastrophes. The concept "critical functions" denotes ***those activities, goods and services that comprise the basis for the ability of society to function*** and, therefore, must be upheld and continued during major accidents or catastrophes. Examples of such critical functions include electricity supply, telecommunications, hospital services, etc.

The RVA model is primarily based on the use of qualitative rather than quantitative data. This means that the analysis will not be a purely objective process. It has to be recognised that risk and vulnerability is often something that is cognitively "perceived" and that the assessments are affected by the participants' prior experience, competencies and convictions. Normative considerations can thus not be avoided. It is therefore important to focus on professional expertise and transparency, as well as ensuring that the assumptions that form the basis of the risk and vulnerability assessment are described underway.

All assessments are conducted using the index method, in which a level for probability, consequences and vulnerabilities is stated on a scale from 1 to 5, where "1" is best and "5" is worst.

The RVA model is divided into four parts:

Part 1 - Starting point for the analysis

Part 2 – Identification of threats

Part 3 – Analysis of threat scenarios

Part 4 – Risk and vulnerability profile

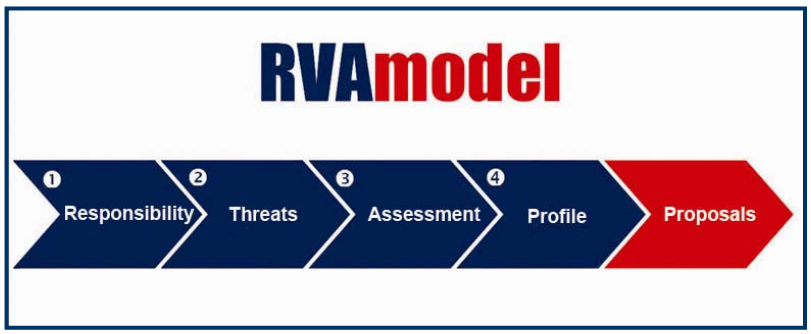


Figure 40: DEMA's RVAmodel

Purpose of Part 1	Part 1 is used to identify the participants in the analysis work, the organisation's preparedness responsibility, and the critical functions that are to be included in the particular risk and vulnerability analysis (the object of the analysis). If separate analyses of individual critical functions or of underlying organisations are required, it is possible to use the model several times among different working groups.
Purpose of Part 2	The RVA model takes as its starting point scenario-based analyses of extraordinary events that can harm critical functions and result in loss of life, health, prop-erty or other values. In Part 2, therefore, the task is to formulate one or more real-istic scenarios that are representative for different types of threats. Each scenario will be analysed subsequently in Part 3 of the model. The purpose of choosing scenarios is to narrow down the field of potential threats in order to focus on areas, where preliminary discussions suggest that substantial risks and vulnerabilities may exist. The purpose is not to draw up a comprehen-sive list of every imaginable threat.
Purpose of Part 3	In Part 3, separate risk and vulnerability analyses will be made for each scenario created in Part 2. To begin with, the critical functions, which must be upheld and continued if the type of incident in question occurs, must be specified. Thereafter, the probability of that type of incident occurring and the consequences are assessed. This gener-ates an overall risk level. Finally, vulnerabilities regarding the organisation's ability to counteract, manage and recover from the type of incident are assessed.
Purpose of Part 4	In Part 4, the results from the various scenario analyses (Part 3) are compared. The result is a risk and vulnerability profile that provides a collective overview of which types of incidents comprise the greatest danger. First, each scenario is placed in a risk matrix based on the assessments from Part 3 of probability and consequences. This generates a clear graphic presentation of risk levels in which the various scenarios can be compared to each other. Secondly, each scenario is placed in a vulnerability overview based on the assessments from part 3 of the organisation's various preparations, its capacities for response and relief, and its capacities for recovery. Just like the risk matrix, the vulnerability overview provides for comparisons, by displaying how relatively resil-ient or vulnerable the organisation's is with respect to counteracting, managing and recovering from the incidents described by the scenarios.

7.5 Public – Private Partnership & International Collaboration

DSIS hosts a cross-sectoral public-private contact group focusing on exchange of information aimed at increasing the resilience of society against security-related threats. Participants in the contact group represent all sectors. The contact group is primarily based on large group discussions on general topics and focused group discussions on more specific topics. Within the partnership information is shared via meetings, informal relationships, and circulation of general threat assessments.

7.6 Funding & Human Resources

CIP is carried out as an integrated part of overall emergency preparedness planning. This implies that funding for CIP-related activities is an integrated part of the resources dedicated to emergency preparedness within DEMA and within relevant sector authorities. Although portions of this overall resource allocation are being applied to CIP-related activities, there are no specific estimates of CIP funding or annual budgets.

DEMA estimates that approximately 30 public employees are involved in CIP-related activities. These resources work in the Ministry of Defence, DEMA, and DSIS, as well the sector responsible departments/agencies. These employees are primarily involved in analysis and supervision concerning CIP. However, it must be stressed that public employees involved in CIP-related activities in Denmark do not focus solely on CIP. Instead, CIP-related work is carried out as an integrated part of the general work concerning emergency preparedness planning.

7.7 Training & Exercises

Training activities on CIP-related matters are carried out as an integrated part of courses on crisis management. Training courses on crisis management arranged in cooperation between DEMA, the Danish National Police, the Danish Defence, and other public authorities are conducted biannually. Participants include public authorities and private operators.

In Denmark, exercises focusing on the national and local levels are conducted regularly. The exercises may vary in nature and distinguish between: crisis management exercises, table top exercises, and field exercises. Since 2003, large national crisis management exercises (called KRISØV) have been conducted every second year. The complexity of the exercises has increased each time and more and more levels have been exercised simultaneously. During KRISØV 2009, which took place on 21 and 22 October 2009, exercise participants from all levels of government took part, including local government.

The KRISØV-exercises last from two to five days and this year's KRISØV was the first where exercise activity took place at night.

A KRISØV-exercise is planned and carried out in the following stages:

- Preparation and approval of the exercise specifications
- Planning, wherein the main elements are:
  - Exercise instructions (including lead-in and 'facts at your fingertips')
  - Directing Staff Instructions (including Exercise framework – story lines)
  - Combined Events List
- Execution
- Evaluation

- Follow-up

The KRISØV-exercises are directed by a Directing Staff (DISTAFF) comprised by representatives from DEMA (Exercise Director) and the National Police. Moreover, all relevant authorities and actors are included in the DISTAFF. Great emphasis is placed on ensuring a high level of professional expertise in the DISTAFF. This is to ensure that exercises are constructed correctly, with relevant high quality input to the participants, and also to ensure that the DISTAFF – during an exercise – is adequately prepared to respond to questions from the participants. It is emphasized that representatives of the DISTAFF are not taking part in the exercise as participants.

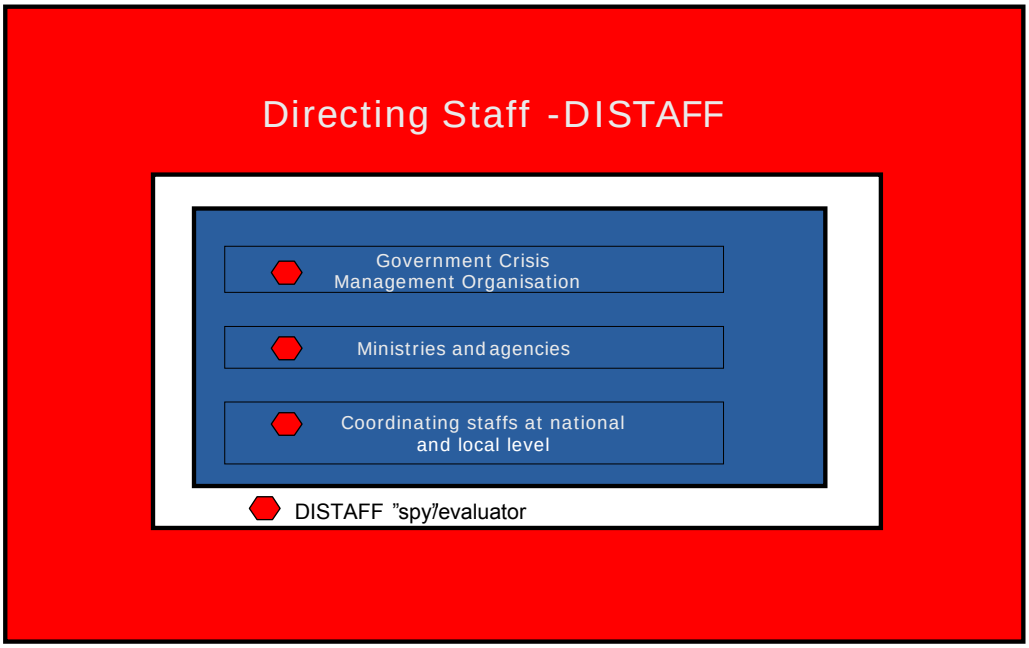


Figure 41: The Directing Staff of the KRISØV Exercises

During the exercise, the DISTAFF is organised according to a number of functions:

- Exercise director
- The Response Cell, including intelligence, policy, and scenario groups
- Media Simulation Cell
- Evaluation Cell
- Service Support Cell

During the conduct of exercises, it has become apparent that it is advantageous to have the DISTAFF gathered in one location. As such, no local DISTAFF's are established with participating authorities/actors. Contact (during the exercise) between the DISTAFF and exercise participants is maintained via locally-placed controlling staff officers (who are part of the exercise evaluation team).

Concurrently with KRISØV, warning and alarming exercises are conducted for individuals and authorities involved in national crisis management. Similarly, technology exercises are carried out to exercise the use of secure communications equipment (VTC etc.).

To the greatest possible extent, Danish authorities participate in international exercises. These include, *inter alia*, NATO's CMX-exercises and the EU's CCA exercises.

The aforementioned exercise activity is documented in an action plan for exercise activity. The action plan is a living document and is reviewed each quarter in, *inter alia*, the Crisis Management Group, which is a group comprised of high-level civil servants chaired by the Prime Minister's Office.

An Exercise Secretariat has recently been established in the Danish Emergency Management Agency (DEMA). The Secretariat is tasked with ensuring a better overview of local exercises and to provide support for such exercises. A priority task is, among other things, to establish an exercise calendar, in which all relevant exercises are listed and which is accessible to all relevant actors.

7.8 Sector – Specific Key Players & Initiatives

Discussions concerning the development of the EPCIP-directive highlighted the need to establish a cross-sectoral forum for Danish authorities involved in preparedness planning. This led to the establishment of the coordination group on EPCIP (KG/EPCIP) which was established as a temporary advisory group (to be dismantled after the adoption of the EPCIP-directive) chaired by DEMA.

With a view to ensure effective cross-sectoral coordination between national authorities regarding CIP in the future, KG/EPCIP has now been replaced by another group. Formed in 2009, the CIP Contact Group (KG/KI) is now the principal forum concerning cross-sectoral cooperation in relation to CIP. The overall purpose of KG/KI is to serve as a forum for exchange of information and knowledge among relevant national authorities regarding CIP. The group is chaired by DEMA and its permanent members are (see Figure 2):

- DEMA
- Danish Energy Agency
- Ministry of Transport
- National IT and Telecom Agency
- DSIS

Other authorities may take part in KG/KI meetings on an ad hoc basis.

DSIS, in 2009, established a project – "Projekt Sikkerhedsrådgivning" (Project Security Counselling) – which provides advice concerning CIP to the energy, transport and ICT sectors. In order to identify the infrastructures, within each sector, which should be given particular priority, DSIS in close cooperation with the sectors, assesses the individual infrastructure's significance to society. This is done with a point of departure in three

criteria: criticality, vulnerability, and threat[121]. "Projekt Sikkerhedsrådgivning" focuses on three types of security: Physical security; information security; and personnel security.

[121] The criteria are mentioned according to the importance attached to each, with criticality being given most weight.

8 Estonia

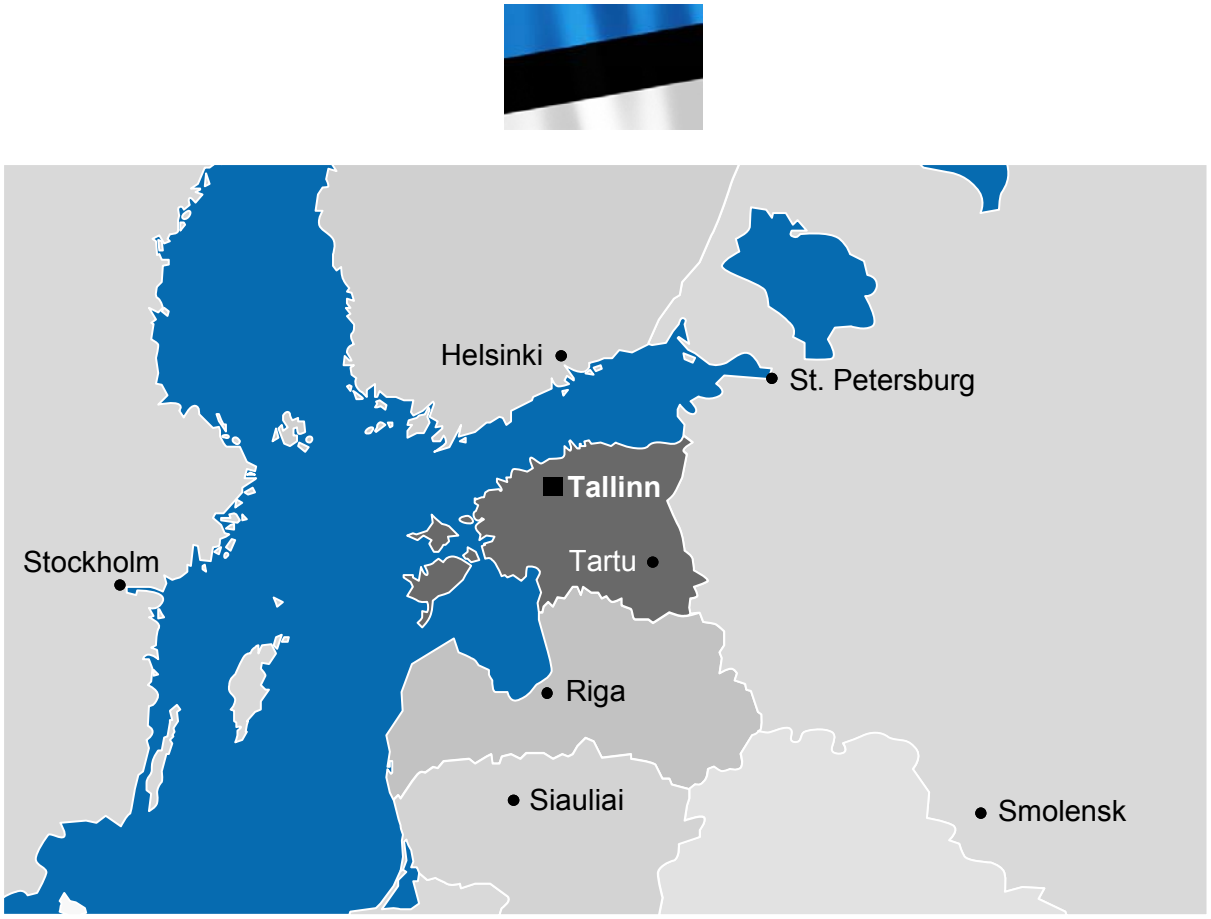


Figure 42: Estonia

8.1 Summary

	Organisational Model	Strategy & Policy	Methodology & Standards	Public-Private Partnership & International Collaboration	Funding & Human Resources	Training & Exercises	Sector-Specific Key Players & Initiatives
Estonia	▪ There is no specific Agency dedicated to CIP ▪ Ministry of Interior leads CIP working group	▪ CIP is addressed as "continuation of vital services" in the Emergency Act of 15 June 2009	▪ Emergency Act establishes risk assessment and continuous operation plan methodology	▪ Cooperative Cyber Defence Centre of Excellence	▪ Not available	▪ Pandora Exercise on pandemic crisis	▪ Refer to Ministry of Interior

Estonia manages Critical Infrastructure Protection through the Ministry of Interior. There is no dedicated, CIP-specific coordinating agency, and specific issues regarding Sectoral CIP activities are dealt with at the level of the single responsible Ministry/Agency.

The Emergency Act, approved on 15 June 2009, addresses vital services, the continuous operation thereof, and the agencies responsible for continuous operation. The continuous operation of vital services is defined as the capability of consistent functioning of vital services and the ability to restore the consistent functioning of vital services after a disruption. The Act defines the continuous operation risk assessment methodology, as well as continuous operation plan requirements.

Established on the 14th of May, 2008, the Cooperative Cyber Defence Centre of Excellence (CCD CoE) mission is to enhance the cooperative cyber defence capability of NATO and NATO nations, thus improving the Alliance's interoperability in the field of cooperative cyber defence. The Centre is an international effort that currently includes Estonia, Latvia, Lithuania, Germany, Italy, the Slovak Republic, and Spain as Sponsoring Nations.

8.2 Organisational Model

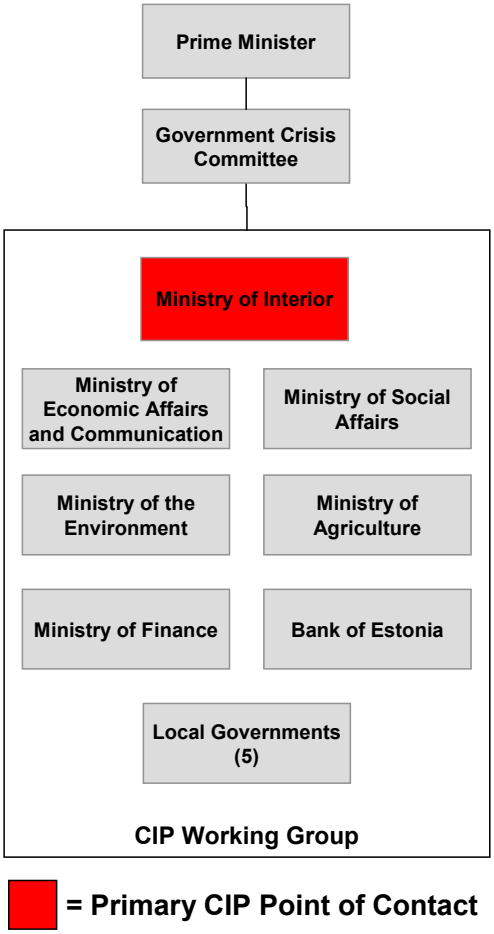


Figure 43: Organisational Chart (only CIP-related agencies shown)

Main Actors/Responsibilities:

- ***Eesti Siseministeerium (Estonian Ministry of the Interior)*** [122]

  In the field of internal security, the Ministry of the Interior and the institutions in its governing area have the mission to assure the internal security of the state and to protect the public order, to guard and protect the state border and assure the border regime. The Ministry of the Interior (and the institutions in its governing area) also has the task to regulate the crisis management and rescue works as well as citizenship and migration. In the field of internal security the Ministry of the Interior has the

[122] www.siseministeerium.ee/?lang=eng

mission to assure the internal security of the state and to protect the public order, to guard and protect the state border and assure the border regime. The Ministry of the Interior has also the task to regulate the crisis management and rescue works as well as citizenship and migration. Officials of the internal security structures are taught in the Estonian Public Service Academy operating in the administrative area of the Ministry of the Interior.

- ***Eesti Majandus-ja Kommunikatsiooni-ministeerium (Estonian Ministry of Economic Affairs and Communication)*** [123]

  The MEAC plays a leading role with regard to information security, since two central agencies for the national IT policy are subordinated to the MEAC: The Department of State Information System (RISO), which is the central body for overall ICT coordination; and the Estonian Informatics Centre (RIA), which constitutes the implementing body under the MEAC[124]

- ***Eesti keskkonnaministeerium (Ministry of the Environment)*** [125]

  The area of government of the Ministry of the Environment includes the management of national environ-mental and nature protection, the performance of tasks relating to land and databases containing spatial data, the management of the use, protection, recycling and registration of natural resources, radiation protection, environmental supervision, the management of meteorological observation, nature and marine research, geological, cartographic and geodetic operations, the maintenance of the land cadastre and water cadastre, and the preparation of corresponding draft legislation. In other words, the task of the Ministry of the Environment is to organise and coordinate environmental policy.

8.3 Strategy & Policy

The Emergency Act, approved on 15 June 2009, addresses vital services, the continuous operation thereof, and the agencies responsible for continuous operation. The continuous operation of vital services is defined as the capability of consistent functioning of vital services and the ability to restore the consistent functioning of vital services after a disruption. The Act assigns these responsibilities as follows:

- The **Ministry of the Interior** shall organise the continuous operation of the following vital services:

  1) functioning of the maintenance of public order;

  2) functioning of rescue work;

  3) functioning of the processing of emergency aid messages;

  4) functioning of air and sea rescue;

  5) functioning of marine pollution monitoring and control;

[123] www.mkm.ee/index.php?id=326384
[124] ETH Zurich – CIIP Handbook 2008
[125] www.envir.ee/58737

6) functioning of the operative radio communication network;

7) ensuring the functioning of the work of the Riigikogu, the Government of the Republic and the President of the Republic.

In addition to fulfilling these responsibilities of an organiser of vital services the Ministry of the Interior shall also:

1) co-ordinate the fulfilment of the responsibilities established in section 34 of this Act by the agencies organising the continuous operation of vital services;

2) develop the policy of ensuring the continuous operation of vital services;

3) provide advice to agencies in organising the continuous operation of vital services;

4) present an overview of the status of the organisation of the continuous operation of vital services to the Government of the Republic and the crisis management committee of the Government of the Republic once in every two years.

- The **Ministry of Economic Affairs and Communication** shall organise the continuous operation of the following vital services:

1) functioning of electricity supply;

2) functioning of gas supply;

3) functioning of liquid fuel supply;

4) functioning of airports;

5) functioning of air navigation services;

6) functioning of the management of public railway;

7) functioning of railway transport services, incl. public passenger transport;

8) functioning of ice-breaking operations;

9) functioning of ports;

10) functioning of the system for organising shipping traffic;

11) functioning of the maintenance of main and basic roads in the country;

12) functioning of the telephone network;

13) functioning of the mobile telephone network;

14) functioning of the data communication network;

15) functioning of marine radio communication;

16) functioning of the cable-casting network;

17) functioning of the broadcasting network;

18) functioning of the postal network.

- The **Ministry of Social Affairs** shall organise the continuous operation of the following vital services:
    1) functioning of stationary special medical care;
    2) functioning of emergency medical care;
    3) functioning of drinking water safety control;
    4) functioning of blood donor service.
- The **Ministry of the Environment** shall organise the continuous operation of the following vital services:
    1) functioning of air monitoring and early warning;
    2) functioning of hydrological and meteorological monitoring and early warning;
    3) functioning of the risk of radiation early warning system.
- The **Ministry of Agriculture** shall organise the continuous operation of the functioning of the control of food safety as a vital service.
- The **Ministry of Finance** shall organise the continuous operation of the functioning of payments and settlements, including the collection of state taxes, as a vital service.
- The **Bank of Estonia** shall organise the continuous operation of the following vital services:
    1) functioning of payments and settlements, including securities payments;
    2) availability of cash.
- **Local government units** shall organise the continuous operation of the following vital services in their administrative territory:
    1) functioning of the district heating system and network;
    2) functioning of the maintenance of rural municipality roads and city streets;
    3) functioning of water supply and sewerage, including waste water treatment plants;
    4) functioning of waste management;
    5) functioning of public transport in the rural municipality or city.

The Act further specifies that agencies or persons organising the continuous operation of vital services shall:

1) co-ordinate the activities to ensure the continuous operation of vital services and provide advice to providers of vital services;

2) perform itself or appoint a sub-agency to perform supervision over ensuring the continuous operation of vital services;

3) present an overview of the status of organising the continuous operation of vital services to the Ministry of the Interior once every two years. If there are more than two providers of the same vital service, the overview shall contain a description of the

measures to mitigate the consequences of a partial or complete interruption of the service as a whole and the measures to restore the continuous operation of the service.

According to the Act, a provider of vital services is a state or local government agency or a legal person, whose competence includes the fulfilment of a public administration duty defined as a vital service or a person operating as an entrepreneur providing vital services.

Providers of vital services shall be obligated to:

1) prepare a risk assessment of the continuous operation of the vital services provided by them (hereinafter the continuous operation risk assessment);

2) prepare a plan for ensuring the continuous operation of the vital services provided by them (hereinafter the continuous operation plan);

3) give immediate notice to the agency organising the vital service or the agency appointed by them of events significantly disturbing the continuous operation of the vital service or an impending risk of the occurrence of such events;

4) give the agency organising the vital service of the agency appointed by them to perform supervision over the continuous operation of the vital service information concerning the provision of the vital service upon the agency's request;

5) fulfil other responsibilities assigned to them with legal acts to ensure the continuous operation of vital services.

In addition to the Emergency Act, the Estonian government has promoted various initiatives to strengthen the IT-sector. The first policy paper, "Principles of Estonian Information Society"[126], was set out in 1999 which defined the principles of the Estonian information policy; and in January 2007, the Estonian IT policy has been defined the Estonian Information Society Strategy 2013[127]. Duo to these strategies and their efficient implementation, Estonia succeeded in making considerable progress on the way towards an information society (for example, Estonia successfully launched new ID card in 2002 that can also be used for issuing digital signatures and for using web-based services of the state).[128]

The National Security Concept 2004[129] refers explicitly to the risks stemming from threats to information security. It is stated that the constantly increasing rate at which electronic information systems are adopted in Estonia, and their connection with and dependence on world-wide information systems, increases the threat of computer crime as well as the vulnerability of information systems, including spheres of primary importance to national security.

[126] http://www.esis.ee/ist2004/105.html
[127] http://www.riso.ee/en/system/files/Estonian%20Information%20Society%20Strategy%202013.pdf
[128] www.id.ee/?id=11019
[129] http://web-static.vm.ee/static/failed/067/National_Security_Concept_2004.pdf.

One of the aims of the policy paper for the Estonian information policy 2004-2006[130] was to define basic principles of a common IT security policy. The purpose of the Estonian Information Security Policy is to contribute to the development of a secure and security-aware information society. More specifically, the policy includes the following goals elimination of non-acceptable risks to electronic communication networks and communication systems, defence of basic human rights; raising awareness about IT security and providing the respective training; participation in international initiatives related to e-security; and increasing the competitiveness of the Estonian economy.[131]

Since January 2007, the new Estonian Information Society Strategy 2013[132] entered into force, setting out the general framework, objectives, and respective action fields for the development of the information society in Estonia. The strategy emphasizes the importance of cooperation between the public and private sectors and the need for coordination among all ministries involved. Three objectives are mapped out by the strategy:

- Development of a citizen-centred and inclusive information society: The percentage of internet users in Estonia is to be further increased
- Development of a knowledge-based economy: ICT uptake by enterprises is to be promoted and the competitiveness of the ICT sector to be increased
- Development of citizen-centred, transparent, and efficient public administration by improving the efficiency of the public sector and providing user-friendly e-services in the public sector[133]

8.4 Methodology & Standards

The new Emergency Act defines the **continuous operation risk assessment** methodology. The continuous operation risk assessment is a document describing the following:

1) the risks causing a partial or complete interruption in the provision of vital services;

2) the probability of a partial or complete interruption in the provision of vital services;

3) the possible consequences of a partial or complete interruption in the provision of vital services;

4) other important information.

The continuous operation assessment shall be approved by the head of the agency providing the vital service or, in the case of a legal person, the management board or a substituting body. The agency or person that prepared the risk assessment shall submit the risk assessment to the agency organising the vital service or a sub-agency appointed by the agency organising the vital service. The agency organising the vital service shall

[130] www.riso.ee/en/files/Policy.pdf.
[131] www.riso.ee/en/information-policy/security.
[132] http://www.riso.ee/en/system/files/Estonian%20Information%20Society%20Strategy%202013.pdf
[133] www.riso.ee/files/IYA/

maintain the confidentiality of information, which the person has upon forwarding designated as trade secrets.

The agency or person that has prepared a continuous operation risk assessment shall at least once in every two years assess the up-to-date value of the risk assessment and make amendments as necessary. The Minister of the Interior holds overall responsibility for establishing the guidelines for preparing the continuous operation risk assessments by regulation.

After completing the continuous operation risk assessment, agencies providing vital services must then complete a **continuous operation plan**. The continuous operation plan is a document describing the following:

1) the measures that need to be taken to prevent partial or complete interruptions in the provision of vital services;

2) the measures that need to be taken to mitigate the consequences of partial or complete interruptions in the provision of vital services;

3) the measures that need to be taken to restore the continuous operation of vital services in the event of a partial or complete interruption in the provision of vital services;

4) other important issues.

The continuous operation plan shall be approved by the head of the agency providing the relevant service or, in the case of a legal person, by the management board or a substituting body. The agency or person that has prepared a continuous operation plan shall submit the continuous operation plan to the agency organising the vital service or a sub-agency appointed by the agency organising the vital service. The agency organising the vital service shall maintain the confidentiality of information, which the person has upon forwarding designated as trade secrets.

The agency or person that has prepared a continuous operation plan shall at least once in every two years assess the up-to-date value of the continuous operation plan and make amendments as necessary. The Minister of the Interior also establishes guidelines for preparing continuous operation plans by regulation.

As a result of, or independently of, the continued operation risk assessment, the Government of the Republic will establish a list of objects with high risk of attack by order. An object of high risk of attack is the territory, building or equipment used for the provision of vital services, the physical damage to or destruction of which would significantly disturb the continuous operation of the entire vital service and which are therefore highly likely to be attacked. The Government of the Republic shall establish the physical protection measures of objects of high risk of attack.

Possessors of objects with high risk of attack shall be obligated to:

1) ensure the continuous application of physical protection measures on the site;

2) cover the risk of a physical attack on the object in the continuous operation risk assessment;

3) take account of the physical protection measures of the object in the continuous operation plan;

4) give the Police immediate notice of circumstances on the site or in the immediate vicinity, which may indicate a threat of a physical attack.

In addition, in order to ensure the electronic security of the provision of vital services, providers of vital services shall be 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. The Government of the Republic holds the responsibility for establishing the security measures for vital service information systems and the related information assets.

8.5 Public – Private Partnership & International Collaboration

- **Cooperative Cyber Defence Centre of Excellence (CCD CoE)**[134]

  This Centre was established on the 14th of May, 2008 in Tallinn (Estonia). The Cooperative Cyber Defence Centre of Excellence (CCD CoE) mission is to enhance the cooperative cyber defence capability of NATO and NATO nations, thus improving the Alliance's interoperability in the field of cooperative cyber defence. The Centre is an international effort that currently includes Estonia, Latvia, Lithuania, Germany, Italy, the Slovak Republic, and Spain as Sponsoring Nations.

8.6 Funding & Human Resources

Resources for CIP activities are integrated into Crisis Management functions. There is no “CIP” agency or department, and therefore no specific CIP funding.

8.7 Training & Exercises

In 2006, the Ministry of Interior organized the Pandora exercise focusing on national crisis management around the pandemic theme.[135]. It was the largest simulation of a crisis situation to date in Estonia. Pandora involved hundreds of volunteers in various fields and has included an airport, a prison, and several hospitals.

---

134 http://www.ccdcoe.org/

135 www.siseministeerium.ee.&26hl%3Dit%26rz%3D1N1RNWN_it%26sa%3DG

8.8 Sector – Specific Key Players & Initiatives

The critical services identified by the Government of the Republic, as well as the agencies responsible for the continued provisioning of these services, have been identified in the Emergency Act of 15 June 2009 and can be found in the Strategy & Policy section of this chapter.

Any requests for further information regarding sectoral CIP activities in Estonia should be directed to the Ministry of the Interior.

9 European Union

Figure 44: The European Union

9.1 Summary

	Organisational Model	Strategy & Policy	Methodology & Standards	Public-Private Partnership & International Collaboration	Funding & Human Resources	Training & exercises	Sector-Specific Key Players & Initiatives
EU	▪ CPI is dealt with at the EU Commission Level	▪ EU is dealing in a structured way with CIP ▪ Directives, Communications, Regulations and Green Papers are in place	▪ No Methods, standards, operating plans and technology regarding CIP	▪ No PPP and international collaboration on CIP	▪ No CIP-specific budget and headcount known ▪ Funding provided partially by European Commission	▪ Exercises, simulations and trainings are performed are performed	▪ Initiative is in place in the ICT (CI^2RCO) ▪ Rapid Alert System for Food and Feed (RASFF)

136

The first European definition of what comprises Critical Infrastructure (CI) is provided by the Communication COM (2004)702 on "Critical Infrastructure Protection in the Fight against Terrorism, adopted on 20 October 2004[137]. It also provides criteria for the identification of, and for determining the importance of a piece of CI.

CI is defined as "those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States".

According to the above mentioned Communication, CI includes:

- Energy installations and networks
- Communications and information technology
- Finance (banking, securities and investment)
- Health care
- Food
- Water (dams, storage, treatment and networks)
- Transport (airports, ports, intermodal facilities, railway and mass transit networks, traffic control systems)
- Production, storage and transport of dangerous goods (e.g. chemical, biological, radiological and nuclear materials)
- Government (e.g. critical services, facilities, information networks, assets and key national sites and monuments)

The European Commission has noted the fundamental role played by the private sector in the operation and protection of CI. This Communication evolved from the terrorist attacks of

136 Not Applicable = Open Source Research, Web-based survey and individual interviews have not shown information/data on the given argument

137 *Communication from the Commission to the Council and the European Parliament: Critical infrastructure protection in the fight against terrorism [COM(2004)702 final],* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52004DC0702:EN:HTML

9/11 and those that affected Span and UK, to trigger a wide debate about the security and the protection of European Critical Infrastructure. This debate included also a public consultation, the Green Paper on a European Programme for Critical Infrastructure Protection [COM (2005) 576 final]138, and a strong cooperation among EU Commission, EU Counsil and Member State.

One of the output of these activities was the establishment of a program framework, named *EPCIP (European Programme on Critical Infrastructure Protection)*, within which all the political and strategic CIP activities of the Commission are performed.

One of the cornerstone elements of the EPCIP is Council Directive 2008/114/EC of 8 December 2008[139] on the identification and designation of European critical infrastructure, and the assessment of the need to improve their protection. The Directive indicates the two priority sectors for consideration are:

- Energy: Electricity, Oil and Gas, and
- Transport: Road transport, Rail transport, Air transport, Inland waterways transport, Ocean and short-sea shipping and ports.

These two priorities areas are to be followed by the ICT sector.

The criticality of an infrastructure can be determined, according to the European Commission, through the following criteria:

- **Scope:** a CI is critical proportionally to the extent of the geographic area that could be affected by damages, losses or service unavailability.
- **Magnitude:** the degree of the impact or loss can be categorised as “none”, “minimal”, “moderate”, or “major”. Among the criteria for assessing the potential magnitude of an incident are:
  - Public impact (number of citizens affected, loss of life, medical illness, serious injury, evacuation)
  - Economic impact (GDP effect, significance of economic loss and/or degradation of products or services)
  - Environmental impact (effect on the public and the environment)
  - Interdependency (with other critical infrastructure elements)
  - and finally, political impact (confidence in the ability of the government to cope)
- **Effects of time:** criterion related to the time an element could have a serious impact (e.g., immediately, within 24 to 48 hours, within one week).

9.2 Organisational Model

Main Actors/Responsibilities:

- ***Directorate-General for Justice, Freedom and Security***[140]

[138] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005DC0576:EN:HTML
[139] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:01:EN:HTML
[140] http://ec.europa.eu/dgs/justice_home/index_en.htm

The role of the Directorate-General for Justice, Freedom and Security of the European Commission is to make proposals for European Union legislation and to monitor its implementation once it has been adopted by the EU Council of Ministers. The role of this DG is to ensure that the European Union is an area of freedom, security and justice. Its specific tasks and responsibilities are laid down by the Treaty of Rome, the Treaty of Amsterdam which came into force on 1 May 1999, and the conclusions of the European Council meeting in Tampere (Finland) in October 1999.

The European Commission has been involved from the beginning in the discussions to bring justice, freedom and security matters within the ambit of the European Union. It set up a small task force for justice and home affairs when the Maastricht Treaty was signed in 1992. This was expanded into a full directorate-general in October 1999.

- ***Directorate-General for Enterprise and Industry***[141]

  The aim of the Directorate-General for Enterprise and Industry of the European Commission is to guarantee that EU policies contribute to the sustainable competitiveness of EU enterprises and facilitate job creation and sustainable economic growth. It has the task of ensuring that the single market runs smoothly and is a major contributor to the implementation of the Lisbon strategy for growth and jobs.

  the Directorate-General pays particular attention to the needs of the manufacturing industry and to small and medium-sized enterprises. It manages programmes to encourage entrepreneurship and innovation, and ensures that EU legislation is cognisant of businesses' concerns.

- ***Directorate General Information Society and Media, DG INFSO***[142]

  The European Commission's DG INFSO undertakes research, policy and regulation in the areas of information and communication technology and media. Its regulation has cultural, societal and economic objectives, and covers some of the largest and most visible economic sectors in Europe. The Directorate-General supports the development and use of Information and Communication Technologies (ICTs) for the benefit of all citizens.

  The DG's roles are to:

  – Support innovation and competitiveness in Europe through excellence in ICT research and development.
  – Define and implement a regulatory environment that enables rapid development of services based on information, communication and audio-visual technologies, so fostering competition that supports investment, growth and employment.
  – Encourage the widespread availability and accessibility of ICT-based services, especially those that have the greatest impact on quality of life.

[141] http://ec.europa.eu/enterprise/dg/index_en.htm
[142] http://ec.europa.eu/dgs/information_society/index_en.htm

– Foster the growth of content industries drawing on Europe's cultural diversity.
– Represent the European Commission in international dialogue and negotiations in these fields, and promote international cooperation in ICT research and development.

- ***Directorate-General for Energy and Transport, DGTREN***[143]

  The DG TREN of the European Commission was created by merging the Directorate-General for Transport and the Directorate-General for Energy. Since June 2002, the Directorate-General has included the the Euratom Safeguards Office.

  DG TREN is responsible for developing and implementing European policies in the energy and transport. Its mission is to ensure that energy and transport policies benefit of sectors of society. DG TREN carries out these tasks using legislative proposals and programme management, including the financing of projects. The current goals of DG TREN are:

  – Complete the internal market in energy and transport.
  – Ensuring sustainable development of transport and energy.
  – Deployment of major networks in Europe.
  – Airspace management, i.e. air traffic congestion management.
  – Improving transportation and energy safety.
  – Accomplishing enlargement.
  – Developing international cooperation.

- ***European Defence Agency, EDA***[144]

  The European Defence Agency is an agency of the European Union founded in July 2004, based in Brussels. It is a Common Foreign and Security Policy (CFSP) body reporting to the Council of the European Union. All EU member states, except Denmark, take part in the agency.

  The aim of EDA is "to support the Member States and the Council in their effort to improve European defence capabilities in the field of crisis management and to sustain the European Security and Defence Policy as it stands now and develops in the future". Its main functions are:

  – Development of defence capabilities in the field of crisis management.
  – Promotion and enhancement of European armaments cooperation.
  – Strengthening the defence technology and industrial base and the creation of an internationally competitive European defence equipment market.
  – Enhancing the effectiveness of European Defence Research and Technology.

- ***European Gendarmerie Force, EGF*** [145]

[143] http://ec.europa.eu/dgs/energy_transport/index_en.htm
[144] http://www.eda.europa.eu/default.aspx

The EGF was launched in 2006 by an agreement between five EU members: France, Italy, Spain, Portugal and the Netherlands. In December 2008 the Romanian Gendarmerie joined the EGF. More countries will be permitted to join in the future.

The aim of the EGF is to create a European intervention force, with militarised police specialised in crisis management. The EGF is based in Vicenza, Italy, and has a core of 800-900 members ready to deploy within 30 days. An additional 2,300 reinforcements are available in standby.

The EGF was declared fully operational in July 2006 following the High Level Interministerial meeting in Madrid, Spain, and its second successful Command Post exercise (CPX), which took place in April 2006. The first CPX was held at the National Gendarmerie Training Centre in Saint Astier, France, in June 2005.

- ***European Union Institute for Security Studies, EUISS***[146]

  The EUISS is an agency of the European Union based in Paris, operating under the EU's second pillar, the Common Foreign and Security Policy (CFSP). It aims to develop a common European culture for security, develop the CFSP, and enrich Europe's strategic debate.

  It was established by the Council Joint Action of 20 July 2001 (revised by Council Joint Action of 21 December 2006) and inaugurated on 1 January 2002 as a replacement to the Western European Union Institute for Security Studies (established in July 1990). The EUISS is an autonomous agency with full intellectual freedom. As a think-tank it researches security issues of relevance to the EU and provides a forum for debate.

  The Institute has relations with the US, the Western Balkans, Africa, the Mediterranean, the Middle East/Gulf, Russia, the Eastern neighbourhood and Asia, as well as the thematic areas of counter-terrorism, disarmament and non-proliferation, conflict prevention and crisis management, development and governance, and EU enlargement.

9.3 Strategy & Policy

Over the last few years, the European Commission has paid considerable attention to the protection of Critical Infrastructure. Since 2004 the Commission published a series of specific legislative documents. The last and most important of these is the Council Directive 2008/114/EC of 8 December 2008. Other Regulations and Communications concern specific sectors.

- ***Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection***[147]

[145] http://www.eurogendfor.org/
[146] http://www.iss.europa.eu/

This Directive describes a series of measures for the identification of the ECI (European Critical Infrastructure) and for the evaluation of the need for improvement of their protection. An ECI is defined by this directive as “critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States”.

One of the main concepts of the directive is the identification of the ECIs through a consistent procedure, with different criteria depending on the sector. Each Member State has to identify its ECIs and to communicate them to the Commission. At the moment, the priority has been given to the energy and transport sectors, and will be extended in the future, initially to the ICT sector.

Each Member State also must establish a contact point with the other MSs and with the Commission, and communicate a complete national risk and threat evaluation.

The Directive also establishes the measures that each ECI owner must apply, including the designation of a Security Liaison Officer, that will act as a contact point with national authorities and the establishment of Operator Security Plans (OSP).

- ***Communication from the Commission on a European Programme for Critical Infrastructure Protection [COM(2006)786]***[148]

  This Communication sets out the principles, processes and instruments proposed for the implementation of the EPCIP. The implementation of EPCIP will be supplemented where relevant by sector specific Communications setting out the Commission's approach concerning particular CI sectors.

- ***Communication from the Commission to the Council and the European Parliament: Critical infrastructure protection in the fight against terrorism [COM(2004)702 final]***[149]

  In this Communication, the European Commission proposes additional measures to strengthen existing CIP instruments. It defines Critical Infrastructure and invites all Member States to list the infrastructure critical to them. The Commission also suggests a methodology for the identification of potential Critical Infrastructure.

  This Communication established the EPCIP for “identifying critical infrastructure, analysing vulnerability and interdependence, and coming forward with solutions to protect from, and prepare for, all hazards. The programme should include helping industrial sectors determine the terrorist threat and potential consequences in their risk assessments. Member States' law enforcement bodies and civil protection services should ensure that EPCIP forms an integral part of their planning and awareness-raising activities”. Its also describes the establishment of the Critical Infrastructure Warning Information Network (CIWIN).

147 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:01:EN:HTML
148 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006DC0786:EN:HTML
149 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52004DC0702:EN:HTML

- ***Green Paper on a European Programme for Critical Infrastructure Protection [COM(2005) 576 final]***[150]

  The main objective of the green paper is to receive feedback concerning possible EPCIP policy options by involving a broad number of stakeholders. It outlines the need for enhanced prevention, preparedness and response in protecting CI from terrorist or other malicious attacks, natural disasters or incidents, and to guarantee short lasting, manageable, infrequent and geographically isolated consequences.

  The Green Paper provides options on how the Commission may respond to the Council's request to establish an EPCIP and a CIWIN and constitutes the second phase of a consultation process concerning the establishment of a EPCIP

- ***Communication from the Commission to the European Parliament, the Council, the European Economic Committee and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" [COM(2009)149]***[151]

  In this Communication, the Commision develops the European policy to strengthen the security of and the trust in the information society. The Commission proposes to "complement existing and prospective measures in the area of police and judicial cooperation to prevent, fight and prosecute criminal and terrorist activities targeting ICT infrastructures". The action plan is based on:

  – Preparedness and prevention: the Commission invites Member States to enhance capabilities and services for cooperation, establishing national CERTs, Forums and other initiatives, also through the support of ENISA
  – Detection and response: developing and support of European Information Sharing and Alert System (EISAS)
  – Mitigation and recovery: developing of national and pan-European plans and exercises, and cooperation between National/Governmental CERTs
  – International cooperation: developing internet resilience and stability and global exercises on recovery and mitigation of large scale internet incidents
  – Criteria for European Critical Infrastructures in the ICT sector: continuing to identify European critical infrastructures for the ICT sector.

- ***Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security***[152]

[150] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005DC0576:EN:HTML
[151] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52009DC0149:EN:HTML
[152] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:310:0028:01:EN:HTML

The aim of this Directive is to introduce a security system in all port areas, establishing a Community framework to guarantee a high and comparable level of security in all European ports. The final objective is to provide the necessary framework for protecting the whole chain of maritime transport logistics (from the ship to the port) against the risk of attacks on Community territory.

The Directive encourages the designation of a port security authority for each port. This authority is responsible for identifying and taking the necessary port security measures in line with port security assessments and plans.

- ***Regulation (EC) No 725/2004 of the EP and of the Council of 31 March 2004 on enhancing ship and port facility security***[153]

The objective of this regulation is to enhance the security of ships for international trade and domestic shipping and port facilities, against international malicious threats.

- ***Regulation (EC) No 2320/2002 of the European Parliament and the Council of 16 December 2002 establishing common rules in the field of civil aviation security***[154]***; and its implementing regulations and amendments***

This Regulation aims to enhance security measures for of civil aviation within the European Union. Specifically, it "establishes a system of unannounced inspections, introduced more rigorous screening of passengers, luggage and staff, and required Member States to introduce national security programmes and common standards for equipment".

Among other, it describes the adoption by each MS of a national civil aviation security programme to ensure that common standards are applied, and the designation of a competent authority to be responsible for coordinating and monitoring the implementation of its national quality control programme.

- ***Regulation (EC) No 300/2008 of the EP and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002***[155]

The aim of this Regulation is to establish common rules for the protection of civil aviation against acts of unlawful interference, setting common rules and standards on aviation security and mechanism for monitoring compliance.

- ***Regulation (EC) No 2096/2005 of 20 December 2005 laying down common requirements for the provision of air navigation services***[156]

153 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0725:EN:HTML
154 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002R2320:EN:HTML
155 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:097:0072:01:EN:HTML
156 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:335:0013:01:EN:HTML

This Regulation establishes common requirements for the provision of air navigation services. It identifies and adopts the mandatory provisions of the Eurocontrol Safety Regulatory Requirements (ESARRs), relevant for the certification of air navigation service providers, regarding the use of safety management systems, the risk assessment and mitigation, the services' personnel, requirements for engineering and technical personnel undertaking operational safety related tasks.

- ***Regulation (EC) No 550/2004 of the EP and of the Council of 10 March 2004 on the provision of air navigation services in the single European sky***[157]

  The aim of this Regulation is to establish common requirements for the safe and efficient provision of air navigation services within the Community. Inter alia, it defines the tasks of National Aviation Supervisory Authorities.

- ***Regulation (EC) No 1315/2007 of 8 November 2007 on safety oversight in air traffic management and amending Regulation (EC) No 2096/2005***[158]

  This Regulation aims at the relevant mandatory provisions of the Eurocontrol Safety Regulatory Requirement on safety oversight in air traffic management (ATM) (ESARR 1) issued on 5 November 2004, adopting a safety oversight function concerning air navigation services, air traffic flow management (ATFM) and air space management (ASM) for general air traffic. This Regulation is addressed to national supervisory authorities and recognised organisations acting on their behalf regarding the safety oversight of air navigation services, ATFM and ASM.

9.4 Funding & Human Resources

- ***European Programme for Critical Infrastructure Protection, EPCIP***[159]

  The EPCIP was established as a result of a consultation in 2004 by the European Council[160], seeking a programme to protect critical infrastructure, and the Green Paper on the European Programme for Critical Infrastructure Protection[161]. It foresees a number of funding sources for activities related to the protection of critical infrastructures in Europe.

  The Commission is prepared to participate in the funding of CIP related measures including relevant studies and the development of specific methodologies. Funding for specific hardware updates, however, would have to be found from other sources.

[157] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0550:EN:HTML
[158] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:291:0016:01:EN:HTML
[159] http://ec.europa.eu/justice_home/funding/2004_2007/epcip/funding_epcip_en.htm
[160] *Communication from the Commission to the Council and the European Parliament: Critical infrastructure protection in the fight against terrorism [COM(2004)702 final], http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52004DC0702:EN:HTML*
[161] *Green Paper on a European Programme for Critical Infrastructure Protection [COM(2005) 576 final],* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005DC0576:EN:HTML

The Communication on EPCIP adopted on the 12th of December 2006[162] also contemplates the possibility of financing EPCIP by way of the Programme "Prevention, Preparedness and Consequence management of Terrorism".

- ***Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks (CIPS)[163]***

  On 12 February 2007, the Council adopted Decision No 2007/124/EC[164], establishing the programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security related Risks for the Period 2007-2013" as part of the general programme on "Security and safeguarding liberties".

- ***Seventh Framework Programme, FP7[165]***

  The Seventh Framework Programme for research and technological development is the European Union's main instrument for funding research in Europe. FP7, which applies to the years 2007-2013, is the natural successor to the Sixth Framework Programme (FP6), and is the result of years of consultation with the scientific community, research and policy making institutions, and other interested parties. The Seventh Framework Programme for research and technological development offers, under the theme "Security", possibilities for funding of security related projects.

9.5 Training & Exercises

As emphasised by the Communication COM (2004)701[166], the European Commission organises training and simulation exercises. The aim of these exercises has been to test existing procedures, to identify problems and to gain experience.

9.6 Sector – Specific Key Players & Initiatives

ENERGY

Public authorities:

- ***European Environment Agency, EEA[167]***

[162] *Communication from the Commission on a European Programme for Critical Infrastructure Protection [COM(2006)786], http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006DC0786:EN:HTML*

[163] http://ec.europa.eu/justice_home/funding/intro/funding_intro_en.htm

[164] Council Decision of 12 February 2007 establishing for the period 2007 to 2013, as part of General Programme on Security and Safeguarding Liberties, the Specific Programme Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks 2007/124/EC, Euratom, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:058:0001:01:EN:HTML

[165] http://cordis.europa.eu

[166] Communication from the Commission to the Council and the European Parliament of 20 October 2004 entitled "Preparedness and consequence management in the fight against terrorism" [COM (2004) 701 final], http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0701:FIN:EN:PDF

[167] http://www.eea.europa.eu/

The European Environment Agency is an agency of the European Union which aims to provide independent information on the environment. It is an information source for those involved in developing, adopting, implementing and evaluating environmental policy, and also the general public. The EEA has 32 member countries.

The regulation establishing the EEA was adopted by the European Union in 1990. It came into force in late 1993 and the work started in 1994. The EEA's objectives are to:

– help the Community and member states make informed decisions about improving the environment, integrating environmental considerations into economic policies and moving towards sustainability, and
– coordinate the European environment information and observation network (Eionet)

Main clients are the European Union institutions — the European Commission, the European Parliament, the Council — and the member states.

NUCLEAR INDUSTRY

Public authorities:

- ***Euratom Supply Agency***[168]

The mission of the Euratom Supply Agency is to ensure a regular and equitable supply of nuclear fuels for Community users. It is under the supervision of the European Commission.

The Agency has operated since 1960, aiming at ensuring the establishment of the basic installations necessary for the development of nuclear energy in the Community, and ensuring that all users in the Community receive a regular and equitable supply of ores and nuclear fuels, as stated in the European Atomic Energy Community (Euratom) Treaty.

The Euratom Treaty gives the Supply Agency the right of option to acquire ores, source materials and special fissile materials produced in the Community and an exclusive right to conclude contracts for the supply of such materials from inside the Community or from outside. In order to be valid under Community law, supply contracts must be submitted to the Supply Agency for conclusion.

The Supply Agency and the Commission pursue the objective of long term security of supply through a reasonable diversification of supply sources and to ensure that in a context of fair trade, the viability of the nuclear fuel cycle industry is maintained.

INFORMATION AND COMMUNICATION TECHNOLOGIES

Public authorities:

- ***European Network and Information Security Agency, ENISA***[169]

[168] http://ec.europa.eu/euratom/index_en.html

The European Network and Information Security Agency is an agency of the European Union. It was created in 2004 by EU Regulation No 460/2004 and has been fully operational since the 1st of September 2005.

ENISA aims to improve network and information security in the European Union. The agency contributes to the development of a culture of network and information security for the benefit of citizens, consumers, enterprises and public sector organisations of the European Union, and consequently will contribute to the smooth functioning of the EU Internal Market.

ENISA assists the Commission, the Member States and, consequently, the business community in meeting the requirements of network and information security, including present and future Community legislation. ENISA ultimately strives to serve as a centre of expertise for both Member States and EU Institutions to seek advice on matters related to network and information security.

Policy:

- ***Communication from the Commission to the European Parliament, the Council, the European Economic Committee and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" [COM(2009)149]***

Initiatives:

- ***Critical Information Infrastructure Research Co-ordination (CI2RCO)***[170]

  CI^{2}RCO is a Co-ordination Action co-funded by the Information Society Technologies (IST) Priority of the 6th Framework Programme by the European Commission (IST-2004-15818).

  The main objective of the Critical Information Infrastructure Research Co-ordination project is to create and co-ordinate a European taskforce to encourage a co-ordinated Europe-wide approach for Research and Development on Critical Information Infrastructure Protection (CIIP), and to establish a European Research Area (ERA) on CIIP as part of the larger Information Society Technologies Strategic Objective to integrate and strengthen the ERA on Dependability and Security.

WATER

[169] http://enisa.europa.eu/
[170] http://www.ci2rco.org/

Public authorities:

- ***Directorate-General for the Environment, DG Environment***[171]

  This DG's objective is to define environmental legislation and to ensure that measures, which have been agreed, are implemented in the Member States.

  The overall mission statement for 2005 is: "Protecting, preserving and improving the environment for present and future generations, and promoting sustainable development". The mission statement is divided into the following sub-statements:

  – To maintain and improve the quality of life through the high level protection of natural resources, effective risk assessment and management and the timely implementation of Community legislation.
  – To foster resource-efficiency in production, consumption and waste-disposal measures.
  – To integrate environmental concerns into other EU policy areas.
  – To promote growth in the EU that takes account of the economic, social and environmental needs of citizens and future generations.
  – To address the global challenges combating climate change and the conservation of biodiversity.
  – To ensure that all policies and measures in the above areas are based on a multi-sectoral approach, involve all stakeholders in the process and are communicated in an effective way.

FOOD

Public authorities:

- ***Directorate-General for Agriculture and Rural Development, DG AGRI***[172]

  The DG AGRI of the European Commission is responsible for the European Union policy area of agriculture. The mission statement of DG Agri is linked to the Common Agricultural Policy (CAP). The DG undertakes:

  – managing and developing the CAP;
  – reinforcing rural development policy;
  – safeguarding the European model of agriculture, and
  – conducting the enlargement process.

- ***Directorate-General for Health and Consumer Protection, DG SANCO***[173]

  The DG SANCO of the European Commission is responsible for the implementation of EU laws on the safety of food and other products, on consumers' rights and on the protection of people's health. It manages three independent Scientific Committees:

[171] http://ec.europa.eu/dgs/environment/index_en.htm
[172] http://ec.europa.eu/dgs/agriculture/index_en.htm
[173] http://ec.europa.eu/dgs/health_consumer/index_en.htm

- The Scientific Committee on Consumer Products (SCCP)
- The Scientific Committee on Health and Environmental Risks (SCHER)
- The Scientific Committee on Emerging and Newly Identified Health Risks (SCENIHR)

These Scientific Committees provide the European Commission with advice on non-food products to assist in preparing policy and proposals relating to consumer safety, public health and the environment. The Committees also draw the Commission's attention to new or emerging problems which may pose an actual or potential threat.

Three agencies of the European Union are linked to DG-SANCO:

- The European Food Safety Authority (EFSA), which the European Commission consults on questions concerning the safety of food products
- The Community Plant Variety Office (CPVO), which administers a system of plant variety rights
- The European Centre for Disease Prevention and Control (ECDC), which helps the European Union combat communicable diseases and other serious health threats

- ***European Food Safety Authority, EFSA***[174]

The European Food Safety Authority is an agency of the European Union that provides independent scientific advice and communication on existing and emerging risks associated with the food chain. It was established in January 2002 and provides risk assessment regarding food and feed safety. The Authority's work covers all matters with a direct or indirect impact on food and feed safety, including animal health and welfare, plant protection and plant health and nutrition.

EFSA supports the European Commission, European Parliament and EU member states in taking effective and timely risk management decisions to ensure the protection of the health of the European consumers and the safety of the food and feed chain.

The Authority communicates to the public in an open and transparent way on all matters within its remit.

Initiatives:

- ***Rapid Alert System for Food and Feed, RASFF***[175]

The Rapid Alert System for Food and Feed provides the control authorities with an effective tool for exchange of information on measures taken to ensure food safety. it has been in place since 1979.

[174] http://www.efsa.europa.eu/EFSA/efsa_locale-1178620753812_home.htm
[175] http://ec.europa.eu/food/food/rapidalert/index_en.htm

The RASFF was created on the basis of the Regulation EC/178/2002 which states the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety (O.J. N° L 31 of 1 February 2002). The scope and procedures of the RASFF are defined in Articles 50, 51 and 52.

HEALTH

Public authorities:

- ***European Agency for Safety and Health at Work, EU OSHA***[176]

  The European Agency for Safety and Health at Work was established in 1996. It aims "to make Europe's workplaces safer, healthier and more productive. This is done by bringing together and sharing knowledge and information, to promote a culture of risk prevention".

  The European Risk Observatory was set up in 2005 as an integral part of the European Agency for Safety and Health at Work. The Risk Observatory aims to identify new and emerging risks and to promote early preventive action. It describes trends and underlying factors and anticipates changes in the working environment and their consequences to health and safety.

- ***European Medicines Agency, EMEA***[177]

  The European Medicines Agency is a European agency for the evaluation of medicinal products. From 1995 to 2004, the European Medicines Agency was known as The European Agency for the Evaluation of Medicinal Products.

  EMEA operates as a decentralised scientific agency of the European Union and is responsible for the protection and promotion of human and animal health, specifically through the coordination of the evaluation and monitoring of centrally authorised product. It provides national referrals, develops technical guidance and provides scientific advice to sponsors. Its scope of operations is medicinal products for human and veterinary use including biologics/TEPs and herbal medicinal products.

- ***European Centre for Disease Prevention and Control, ECDC***[178]

  The European Centre for Disease Prevention and Control was established as an independent agency of the European Union in 2005. It is responsible for strengthening Europe's defences against infectious diseases. Since 2007, the ECDC has had experts in place covering all 49 of the infectious diseases that are notifiable at EU level.

[176] http://osha.europa.eu/en
[177] http://www.emea.europa.eu/
[178] http://www.ecdc.europa.eu/

The ECDC has established six cross-cutting programmes: Respiratory Tract Infections (Influenza – Tuberculosis); STI including HIV and Blood-Borne Viruses; Vaccine Preventable Diseases; Antimicrobial Resistance and Healthcare-Associated Infections; Food and Water-Borne Diseases and Zoonoses and Emerging and Vector-Borne Diseases.

FINANCIAL

Public authorities:

- ***Directorate General for Economic and Financial Affairs, DG ECFIN***[179]

The main responsibility of the Directorate-General for Economic and Financial Affairs of the European Commission is to encourage the development of economic and monetary union, both inside and outside the European Union, by advancing economic policy coordination, conducting economic surveillance and providing policy assessment and advice. The competences of the DG include:

– Economic surveillance
– Monitoring budgetary policy and public finances
– Economic policy coordination
– Legal, practical and institutional aspects of the euro
– Financial markets and capital movement
– Economic relations with third countries
– Financing

TRANSPORT

Public authorities:

- ***European Maritime Safety Agency, EMSA***[180]

The European Maritime Safety Agency (EMSA) is a European agency founded in 2002. EMSA has the following mission:

– Assist the Commission in preparing Community legislation in the field of maritime safety and prevention of pollution by ships.
– Assist the Commission in the effective implementation of Community legislation on maritime safety and maritime security.
– Organise training activities, develop technical solutions and provide technical assistance related to the implementation of Community legislation.
– Help develop a common methodology for investigating maritime accidents.
– Provide data on maritime safety and on pollution by ships and help improve the identification and pursuit of ships making unlawful discharges.

[179] http://ec.europa.eu/dgs/economy_finance/index_en.htm
[180] http://www.emsa.europa.eu/

In doing so, EMSA closely cooperates with the Member States' maritime services.

- ***European Aviation Safety Agency, EASA***[181]

  The European Aviation Safety Agency is a European agency, which has been given specific regulatory and executive tasks in the field of civilian aviation safety. Created on 28 September 2003, its responsibilities include:

  – Providing advice to the European Union for drafting new legislation.
  – Implementing and monitoring safety rules in the Member States.
  – Type-certification of aircraft and components, as well as the approval of organisations involved in the design, manufacture and maintenance of aeronautical products.
  – Authorisation of third-country (non EU) operators.
  – Safety analysis and research.

RESEARCH FACILITIES

Public authorities:

- ***The Directorate-General for Research, DG Research***[182]

  The mission of the DG Research of the European Commission includes:

  – Developing the European Union's policy in the field of research and technological development and contributing to the international competitiveness of European industry.
  – Coordinating European research activities with those carried out at the level of the Member States.
  – Supporting the Union's policies in other fields such as environment, health, energy, regional development etc.
  – Promoting a better understanding of the role of science in modern societies and stimulating a public debate about research-related issues at European level

- ***EC Joint Research Centre, JRC***[183]

  The JRC is a Directorate-General of the European Commission. It provides independent scientific and technical advice to the European Commission and Member States of the European Union in support of EU policies.

  The JRC provides specific technical and scientific support for the development, implementation and monitoring of EU policies. It acts as a reference centre of science and technology in the EU.

[181] http://easa.europa.eu/ws_prod/g/g_about.php
[182] http://ec.europa.eu/dgs/research/index_en.html
[183] http://ec.europa.eu/dgs/jrc/index.cfm

10 Finland

Figure 45: Finland

10.1 Summary

	Organisational Model	Strategy & Policy	Methodology & Standards	Public-Private Partnership & International Collaboration	Funding & Human Resources	Training & Exercises	Sector-Specific Key Players & Initiatives
Finland	▪ There is no specific Agency dedicated to CIP	▪ CIP approach explained in "The Strategy for Securing the Functions Vital to Society" document	▪ Implementation of the Government Report on Security and Defence Policy	▪ NBED and NESC ▪ CIVPRO Network (risk management) ▪ Bilateral Agreements with Sweden and Norway	▪ Not Applicable	▪ UUSIMAA 2008 Exercise (consequence management field exercise)	▪ Not Applicable

[184]

Finland does not have a single agency solely dedicated to CIP, but has developed a CIP strategy titled the "The Strategy for Securing the Functions Vital to Society"[185] [186] (hereafter "The Strategy"). This document takes a broad view compared to the CIP approaches of many other EU countries and with the EU's own definition of CIP.

This Strategy is the cornerstone for the development of CIP in Finland.

[184] Not Applicable = Open Source Research, Web-based survey and individual interviews have not shown information/data on the given argument

[185] The Strategy for Securing the Functions Vital to Society (2003) http://www.defmin.fi/index.phtml?l=en&s=195

[186] The Strategy for Securing the Functions Vital to Society (2006) http://www.defmin.fi/index.phtml?l=en&s=335

10.2 Organisational Model

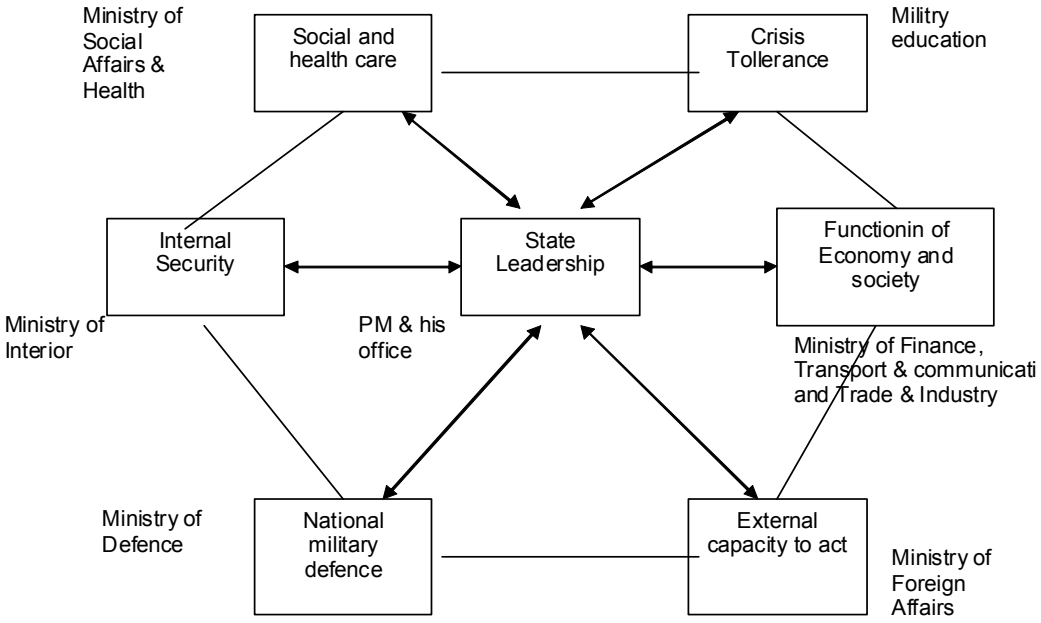


Figure 46: Organisational Chart (only CIP-related agencies shown)

The President of the Republic[187]

The President of the Republic conducts Finland's foreign policy in cooperation with the Government. The President and the Cabinet Committee on Foreign and Security Policy[188] coordinate important aspects of foreign and security policy and other matters concerning Finland's international relations, associated key internal security issues, and significant national defence issues.

The Government[189]

The Government is responsible for Finland's preparation of decisions to be made in the European Union, and decides on concomitant Finnish measures, unless the decision requires the approval of Parliament. The Government directs, supervises and coordinates the securing of functions vital to society. Each competent ministry does the same within its respective administrative sector. In order to facilitate preparedness and to instigate activities, all competent authorities employ their statutory powers, which are already quite exhaustive in normal conditions.

The Emergency Powers Act and the State of Defence Act can be authorised to provide the government and its agencies with additional powers to deal with threats to Finland and its interests. In emergency conditions, the Government, subject to a Parliament decision, may be authorised to use the additional emergency powers provided in the Emergency Powers

[187] http://www.tpk.fi/en/
[188] http://www.valtioneuvosto.fi/hallitus/ministerivaliokunnat/en.jsp
[189] http://www.government.fi/etusivu/en.jsp

Act[190]. The decision to begin using powers pursuant to the State of Defence Act[191] is taken by Presidential Decree, subject to a Parliament decision. Separate provisions provide for the President of the Republic, the Prime Minister, relevant ministers and the Chief of Defence in dealing with military command matters relating to the Defence Forces and the Border Guard.

The Prime Minister[192]

The Prime Minister directs the activities of the Government and oversees the preparation and consideration of matters within the mandate of the Government.

The Ministry of Defence

The Ministry of Defence is responsible for coordination of Finland's defence activities. The Security and Defence Committee[193] assists the Ministry of Defence and the Cabinet Committee on Foreign and Security Policy on matters relating to total defence and its coordination. The Committee monitors changes in the security and defence situation and considers their effects on existing defence arrangements. The Committee also has the task of monitoring and coordinating the different administrative sectors' total defence measures.

The Ministry of Employment and the Economy[194] The sphere of authority of the Ministry of Employment and the Economy includes employment, unemployment, public employment service, working environment issues, collective agreements, arbitration of labour disputes, the development of regions; industrial policy; energy policy and integration of the national preparation and implementation of climate policy; innovation and technology policy, internationalisation and technical safety of enterprises, functionality of markets, promotion of competition and consumer policy, and non-military service.

The National Emergency Supply Agency (NESA)[195] is a body working under the auspices of the TEM. Its role is planning and managing activities to maintain and develop the country's security of supply, and analysing threats and risks to critical information infrastructures. NESA manages the Security of Supply Fund, which is an independent fund outside the State Budget. The Fund is used to finance security of supply stockpiling and for certain emergency arrangements to safeguard technical infrastructures. NESA is the secretariat of the National Board of Economic Defence (NBED). NESA and NBED analyse threats against the security of supply and they also formulate plans and guidelines to help public authorities and businesses manage and control of such threats.

The National Board of Economic Defence[196] is a network of committees consisting of leading experts from both public administration and the business world. Its tasks are to analyse threats against the country's security of supply and to plan measures to control these

[190] Emergency Powers Act (1080/1991) http://www.finlex.fi/fi/laki/kaannokset/1991/en19911080.pdf

[191] The **State of Defence Act** (1083/1991) is designed to strengthen the national defence system in order to safeguard the country's independence and to maintain law and order, and to reinforce national security under the circumstances specified in Section 16 A of the Constitution (under national emergencies) by declaring a state of defence, if the powers allowed under the Readiness Act are insufficient for the purpose. The President institutes a state of defence by decree, initially for three months. If necessary, the state of defence may be extended for up to one year at a time. A state of defence may also be put into effect regionally. The relevant decree must be approved by Parliament.

[192] http://www.vnk.fi/etusivu/en.jsp

[193] http://www.defmin.fi/?l=en&s=36

[194] http://www.tem.fi/index.phtml?l=en&s=2072

[195] http://www.nesa.fi/organisation/national-emergency-supply-agency/index.html

[196] http://www.nesa.fi/organisation/national-board-of-economic-defence/index.html

threats. The Committee's plenary session consist of 60 members, and nearly 500 people are assigned to various tasks in the entire NBED.

The Ministry of Transport and Communications[197] advances the operation of society and the well-being of the population by ensuring that the public and the business community have access to safe and inexpensive transportation and communications services and that enterprises can operate in a competitive environment.

The Finnish Communications Regulatory Authority[198] ***(FICORA)*** is a general administrative authority for issues concerning electronic communications and information services. It promotes the Information Society, as well as technical regulation and standardisation. A specific duty of the FICORA is to safeguard the functionality and efficiency of the communications markets in order to ensure that consumers have access to competitive and technically advanced communications services that are both of good quality and affordable.

The Ministry of the Interior[199] prepares Acts, decrees and other decisions concerning the internal administration of the Finnish Government and Parliament, prepares international agreements, decisions and matters related to the European Union, and steers internal administration. The Police Department of the Ministry of the Interior is the Supreme Police Command in Finland. The supreme command of the rescue services is held by the Department for Rescue Services. The Frontier Guard Department is also the Headquarters of the Frontier Guard.

Ministry of Defence[200] As part of the Government, and the leading authority in the area of national defence, the Ministry of Defence is in charge of national defence policy, national security and international cooperation in defence policy matters.

The Ministry for Foreign Affairs[201] ***(MFA)*** promotes the security and prosperity of Finnish nationals. Tthe MFA contributes to enhancing international solidarity and to consolidating peace on the basis of the principles of democracy, equality, respect for human rights, sustainable development and rule of law. As an organisation with high professional competence in the field of international relations, the MFA prepares and implements the Government's foreign policy and brings together the expertise of different national players to facilitate the formulation of coherent policies.

The Ministry of Finance[202] provides a macroeconomic and fiscal policy framework for the Government, drafts the annual budget, and offers experience in tax policy matters. The Ministry is responsible for strategic policy on the financial markets, State employer and personnel policy, and for overall development of government budgets. It also participates in the work of the European Union and several international organisations.

[197] http://www.mintc.fi/
[198] http://www.ficora.fi/englanti/index.html
[199] Ministry of Interior http://www.intermin.fi/english/ministry
[200] http://www.defmin.fi/
[201] http://formin.finland.fi/english
[202] http://www.vm.fi/english

10.3 Strategy & Policy

The main documents that define the strategies and policies on CIP and national security matters in Finland are:

- The Strategy for Securing the Functions Vital to Society 2003 and 2006
- Report on Finnish Security and Defence Policy (2001)[205]
- Report on Finnish Security and Defence Policy (2004)206
- Defence and Security Industrial Strategy[203]

The CIP strategy in the document *Strategy for Securing the Functions Vital to Society* states that the aim of securing the vital functions of society[204] is to safeguard the country's independence, preserve security in society and maintain the livelihood of the population. The EU strategy focused on "those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments". The Finnish approach focuses on the functions themselves rather than infrastructure that support them. Thus, the Finnish vital sectors are more or less the same as the EU's – especially in the areas dealing with the 'functioning of the economy and infrastructure' and 'the population's income security and capability to function', but the main emphasis is on the functioning of society and government in all circumstances, not only in the protection of its critical infrastructures during extreme events. As such Finland's approach is much more based on 'resilience' (a concept discussed in more detail below) than protection.

The Government's report on Finnish Security and Defence Policy 2001[205] played a fundamental role in the development of their CIP program. The report paid particular attention to the threats associated with increasing international integration. In accordance with the report, the Government embarked on a project to define areas vital to the functioning of society and to draft action and development plans. This project culminated with the Government Resolution and the development of the 2003 *Strategy for Securing the Functions Vital to Society* document.

In 2004 the Finnish Parliament considered the *Finnish Security and Defence Policy Report*[206], which provided the principles, objectives and implementation criteria for Finland's security and defence policy. One of the tasks called for in the report was the 2006 review of the 2003 Resolution. This was conducted by the Security and Defence Committee and the resulting Resolution and report replaced the 2003 version. The 2006 Resolution takes into account increasing internationalisation as well as changes in the security environment and societal structures.

[203] Defence and security industrial strategy (Jan. 2007) http://www.defmin.fi/index.phtml?l=en&s=376

[204] The functions vital to society are as follows: state leadership, external capacity to act, the nation's military defence, internal security, functioning of the economy and society, securing the livelihood of the population and its capacity to act, and their ability to tolerate a crisis.

[205] Finnish Security and Defence Policy 2001, http://www.defmin.fi/index.phtml?l=en&s=388

[206] Finnish Security and Defence Policy Report 2004 http://www.defmin.fi/index.phtml?l=en&s=181

Strategy for Securing the Functions Vital to Society

This strategy coordinates the administrative sectors' measures which contribute to preparedness and securing vital functions by defining:

- vital functions of Finnish society and their desired end states;
- common threat scenarios and associated special situations, including preparedness obligations;
- the strategic tasks to be undertaken by the various Ministries' to secure nationally important functions, including development requirements, and
- focus areas, schedules, monitoring arrangements and exercises.

The Strategy aims to both avoid duplication of development efforts and prevent a situation in which capabilities required for securing the vital functions are not developed. Ministries are to direct the preparedness efforts and related legislative measures based upon the guidance contained in the Resolution.

In addition to the government authorities, the Strategy provides information and harmonises the principles of preparedness for the business community and NGOs. Furthermore, it provides information to the general public on tangible Government-led measures being undertaken to strengthen the security of society and the population. The Strategy also conveys information to Finland's international partners on the basic principles of its policies and thinking on its national security.

Society must be able to secure its vital functions in all circumstances in which a special situation may arise, these include normal, abnormal and emergency conditions. In normal conditions, the focus in securing vital functions is on preventing, combating and managing threats and on recovering from them using legislation and available resources.

Emergency conditions are laid down in the Emergency Powers Act and in the State of Defence Act. The statutory powers provided by these acts may be invoked and exercised only in situations that can no longer be controlled by the authorities' regular powers. The Treaty Establishing the European Community defines situations in which Member States must enter into negotiations with each other to ensure that the measures which an individual single Member State may take cause the least possible disturbance to the functioning of the common market.

The Strategy defines a set of threat scenarios and identifies special situations in which unanticipated or sudden threats or events in normal, abnormal or emergency conditions might endanger the security of society or the population. Special situations may require non-standard management and communications responses, and a particular special situation can be included in several threat scenarios.

A threat scenario is a general description of disturbances in the security environment which could jeopardise the security of society, the livelihood of the population or the sovereignty of the state. The threat scenarios included in the Strategy are:

- a disturbance in the electricity grid;

- a serious disturbance affecting health and income security of the population;
- a serious disturbance in the functioning of the economy;
- major accidents and natural disasters;
- environmental threats;
- terrorism and organised or serious crime;
- threats linked to migratory flows;
- political, economic and military pressure, and
- the use of military force.

Threat scenarios are maintained as part of state administration's normal prediction and follow-up work and are updated during time of the Resolution is reviewed. On the basis of the described scenarios, the competent authorities compile more detailed threat estimates for their own fields of responsibility. These estimates specify the origin of the threat, the target, the form it takes, its probability, the way it affects the authorities' capability to carry out their tasks as well as response options.

Finnish Defence Policy

The main participants in defence policy formulation are the Finnish Parliament (the centre of legislative power), the President of the Republic, and the Finnish Government (especially the Cabinet Committee on Foreign and Security Policy). The Ministry of Defence presides over defence policy and coordinates all aspects of total defence within the State administration.

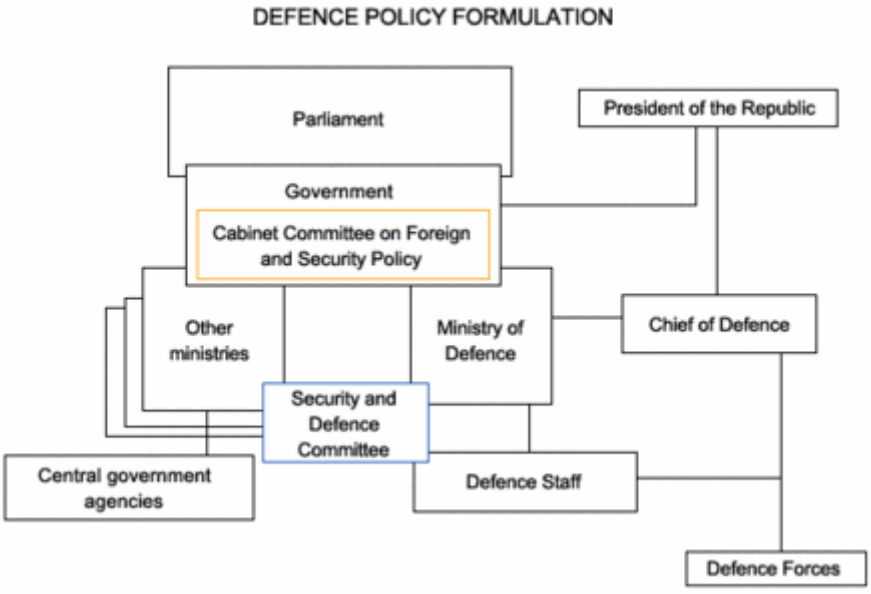


Figure 47: Finnish Defence Policy Formulation [207]

[207] www.defmin.fi

The White Paper, The Report on Finnish Security and Defence Policy, published in September 2004, guides national defence policy. The document is prepared cooperatively in different ministries and is approved by Parliament. The latest report focuses on Finland's changing security environment and defines the line of action in the field of defence policy. The Ministry of Defence monitors changes in security political environment and focuses to update defence political lines according to the needs of the Finnish society.

10.4 Methodologies & Standards

Implementation of the Government Report on Security and Defence Policy of 2004[208]

On 16 March 2005, the Finnish Minister of Defence presented to the Defence Committee and the Finance Committee his decision on the implementation of the Government Report on Security and Defence Policy (2004) taking into consideration also the confirmed decision on spending limits made for the nation's economy by the Council of State on 10 March 2005.

The Defence Forces will be developed for the 2010s in accordance with the framework laid out in the Government Report on Security and Defence Policy. The planned war and peacetime compositions of the Defence Forces is being made lighter.

10.5 Public – Private Partnership & International Collaboration

Partnership between the public and private sectors has a long tradition in Finland.

The National Board of Economic Defence

The National Board of Economic Defence (NBED) was established in 1955. The NBED and its constituent bodies plan and co-ordinate preparations for various kinds of disturbances and emergency situations. It provides for co-operation on an expert level between public authorities and the business world. It covers the most important social sectors - IT Society, transport logistics, food supply, energy supply, and health care services. In each of the groups representatives of the ministries, government agencies, the private sector, and various organisations are included.

National Emergency Supply Council[209]

Established in 1955, the National Emergency Supply Council (NESC, previously National Board of Economic Defence), under the auspices of the Ministry of Employment and the Economy, supports and assists NESA activities. NESC also plans and coordinates economic preparations for implementation in the event of exceptional circumstances in Finland. NESC is a network of committees consisting of the leading experts from both the public administration and the business world. Its tasks are to analyse threats against the country's security of supply, to plan measures to control these threats, and to promote readiness planning at individual industrial sites.

INTERNATIONAL COLLABORATION

[208] http://www.mil.fi/selonteko2004/index_en.dsp
[209] ETH Zurich – CIIP Handbook 2008

As defined in “The Strategy”, international activity refers to the capability of maintaining communication with foreign states and guaranteeing that Finnish messages reach the institutions of the European Union, international organisations and actors. Furthermore, it is being able to obtain any needed external assistance and support as well as providing these to other states, assisting Finnish citizens abroad and safeguarding the preconditions for foreign trade.

Towards a Baltic Sea Region Strategy in Critical Infrastructure Protection[210]***.*** This study was sponsored by the European Commission Directorate-General for Justice, Freedom and Security. The project started in December 2006 and was led by from Nordregio, the Nordic Centre for Spatial Development.

The ***CIVPRO Network***[211] conduct studies addressing research questions in civil protection, risk management and emergency preparedness. CIVPRO consists of a variety of partners, and its activities cover all of the Baltic Sea region. It is coordinated by the Aleksanteri Institute, the Finnish Centre for Russian and Eastern European Studies, and the University of Helsinki.

NATO Euro-Atlantic Partnership Council[212] NATO's civil sector mainly operates under the auspices of the Euro-Atlantic Partnership Council (EAPC), and Finland is a participant. Although, questions concerning common defence are dealt with exclusively by the representatives of the Member States, these questions cover only a minor part of the committees' work. This means that countries participating in the Partnership for Peace Programme operate in the civil sector under almost the same conditions as NATO's Member States. In recent years, Austria, Finland, Sweden and Switzerland have made considerable contributions in the civil sector.

BILATERAL CO-OPERATION

Finland and Sweden have concluded a bilateral agreement on economic co-operation in international emergency situations. However, the implementation of the agreement has been interrupted because of organisational reforms in Sweden. National security of supply authorities are still persuing negotiations to modernise the agreement to meet today's threats.

Finland and Norway have negotiated a bilateral agreement on security of supply. The agreement has been signed in April 2005.

The stockpiling obligation imposed by the EU can also be met by stockpiling products in another Member State. That requires bilateral agreements concerning administration. Currently, Finland has concluded such an agreement with Sweden.

10.6 Training & Exercises

Exercise “UUSIMAA 2008”[213]

[210] www.nordregio.se/Files/r0705.pdf
[211] http://www.aleksanteri.helsinki.fi/civpro/about.php
[212] http://www.nato.int/issues/eapc/index.html
[213] http://www.nato.int/eadrcc/2008/06-uusimaa/070618.htm

Exercise UUSIMAA 2008 is a consequence management field exercise organised by the Euro-Atlantic Disaster Response Coordination Centre (EADRCC) and was conducted in June 2008 in Finland. The five day drill was based on the fictitious scenario of a serious civil emergency situation on the southern coast of the country. Around 1000 participants representing 25 NATO and partner countries, as well as other international organisations, assisted Finland in dealing with the consequences of heavy thunderstorms, floods and chemical spills. Urban Search and Rescue Teams worked to locate and rescue casualties, while medical teams provided first aid in the field hospitals deployed to the exercise locations. Several Chemical, Biological, Radiological and Nuclear (CBRN) Response teams were also present, dealing with damage done to energy facilities and chemical installations.

Finland's provision of suitable areas for international exercises[214]

On 31 January 2006, the Ministry of Defence appointed a commission to determine whether Finland could make suitable land and sea areas as well as air space available for international exercises. The commission was established pursuant to the Government Report on Finnish Security and Defence Policy 2004 (VNS 6/2004). The goal of the practice range commission was to study the need for practice ranges from an international and commercial perspective, the opportunities available and ramifications.

10.7 Sector – Specific Key Players & Initiatives

ENERGY

Public Authorities:

- ***The Energy Market Authority***[215]

  An expert body subordinate to the Ministry of Employment and the Economy, the mission of the Energy Market Authority is to supervise and to promote the efficient and effective functioning of the electricity and natural gas markets and to establish preconditions for emission trading.

- ***Finnish Natural Gas Association***[216]

  The Finnish Natural Gas Association was established in 1986. Its main objectives are to improve the operational conditions of the gas supply, to oversee the common interests of the natural gas industry, and to provide expert services. To achieve these objectives the association maintains contacts with authorities and other interest groups[217].

NUCLEAR

Finland has four nuclear power units. Two of them are situated in Loviisa and operated by FORTUM[218] The other two are situated in Olkiluoto and operated by Teollisuuden Voima Oyj (TVO)[219].

[214] Finland's possibilities for making suitable land and sea areas as well as air space available for international exercises. (Jan. 2007), http://www.defmin.fi/index.phtml?l=en&s=352
[215] http://www.energiamarkkinavirasto.fi/
[216] http://www.maakaasu.fi/
[217] http://www.maakaasu.fi/frame_in_engl.html
[218] http://www.fortum.com/

In Espoo, there is also the FiR1 research reactor operated by the Technical Research Centre of Finland (VTT)[220].

INFORMATION AND COMMUNICATION TECHNOLOGIES

Public Authorities:

- ***CERT-FI[221] (Computer Emergency Response Team FICORA)***
  CERT-FI focuses on information security incidents and their control at FICORA. The CERT-FI cooperates with national and international CERT players and representatives of trade, industry and the public administration. FICORA also coordinates a CERT working group, which acts as a cooperative body for different players in the field of information security incident disclosure and resolution. This working group also monitors and promotes general development in the field and distributes information about it.

  Telecommunications operators are mandated to notify CERT-FI of information security incidents and threats. Notifications from other private and public organisations as well as from private persons are also encouraged. In addition, CERT-FI continuously monitors current global information security events, security problems and incidents in information systems, and reacts to them. The responsibilities of CERT-FI also include monitoring incidents at national level, and documenting and compiling statistics.

- ***Finnish Information Security Association[222]***

  The Finnish Information Security Association (FISA) is the largest information security association in Finland. FISA is a non-profit association whose objective is to advance information security professionalism, awareness and best practices. Its activities include member meetings, discussion groups, company visits, conferences, CISSP certification and participation in various information security programs.

- ***Finnish Network Enabled Defence[223]***

  In 2003 the Finnish Defence Force, proposed a new program, called Finnish Network-Enabled Defence (FiNED), aimed at achieving network-centric operations within a decade. FiNED aims to transform Finland's homeland security and crisis management infrastructure through improved interagency and international collaboration. This includes collaboration with groups such as Customs, Border Guard, Police, Fire and Rescue, state ministries and industry, and international organisations such as NATO and the European Union. FiNED is hoped to result in a new kind of partnership and a co -operative culture between information technology, organisational, and process structures.

HEALTH

Public Authorities:

[219] http//www.two.fi
[220] http://www.vtt.fi
[221] http://www.cert.fi/en/index.html
[222] http://www.tietoturva.fi
[223] www.nordac.org/?DocID=284

- ***The Ministry of Social Affairs and Health***[224]

  The Ministry of Social Affairs and Health (STM) works to provide the Finnish population with a healthy living environment, good health, and an adequate income and social protection in different life situations. STM directs and guides the development of social protection and social and health care services policies. It defines the main course of development, prepares legislation and key reforms, steers their implementation, and manages links with the political decision-making process.

- ***STM Preparedness Unit***[225]

  The STM Preparedness Unit was established under the Administrative Department for the purposes of emergency planning. The Unit has specialist expertise and provides guidance and development initiatives for social welfare and health care emergency planning. It develops and coordinates the resources required to meet not only exceptional circumstances but also disruptive situations occurring under normal circumstances, and maintains arrangements for incident management and security.

FINANCIAL

Public Authorities:

- ***National Board of Economic Defence***[226]

  The National Board of Economic Defence (NBED) is a network of committees consisting of the leading experts from both the public administration and the business world. Its tasks are to analyse threats against the country's security-of-supply and to plan measures to control these threats. At present, the public-private-partnership in NBED is considered to be unique in the world.

  NBED is particularly important in today's interlinked technological society. Its organisation has recently been modified to be better adapted to new and changed conditions. Sectors have been established to focus on different domains and facilitate co-operation between authorities, federations, and important business actors. Their main task is to manage, co-ordinate, and monitor preparations within their respective security of supply area. The NBED sectors are IT Society, transport logistics, food supply, energy supply, and health care services. Representatives of ministries, government agencies, the private sector and various organisations are members of these sectors.

TRANSPORT

Public Authorities:

- ***Finnish Rail Administration***[227]

[224] http://www.stm.fi/Resource.phx/eng/index.htx
[225] http://www.stm.fi/Resource.phx/eng/subjt/prep/index.htx
[226] http://www.nesa.fi/organisation/national-board-of-economic-defence/
[227] http://www.rhk.fi/in_english/

The Finnish Rail Administration (RHK) is responsible for managing, maintaining and developing Finland's rail network. Through planning, construction, maintenance and traffic control, RHK provides the infrastructure on which traffic can operate reliably and safely. The RHK's goal is to keep the present rail network in the condition necessary to meet traffic needs so that services are safe and efficient.

- ***The Finnish Rail Agency***[228]

  The Finnish Rail Agency is the nation's Railway Safety Authority. The tasks of the Finnish Rail Agency include managing railway safety in general and tasks provided or indicated by legislation, participating in international cooperative activities in the field, and supervising railway safety compliance. The Finnish Rail Agency improves the safety of the Finnish railways and the interoperability of the railway system, and develops standards and rules for railway traffic. The Finnish Rail Agency cooperates with the European Railway Agency, the European Commission and the national safety authorities of the EU Member States in developing a safe European railway system that will extend over the Union. The Finnish Rail Agency monitors compliance with the provisions of the Railway Act.

- ***The Finnish Maritime Administration***[229]

  The Finnish Maritime Administration has responsibility for the development and maintenance of channels and waterways. This includes both fairway maintenance and the construction of new channels. The Finnish Maritime Administration also administers the thirty-nine lock canals in the country. The Saimaa Canal, which is an important link between the Gulf of Finland and the great lakes of the Lake District, is the best-known of these. The Finnish Maritime Administration is also responsible for the assistance of winter navigation. Its experts participate in the development of the joint icebreaker management policy for the Baltic Sea, which takes into account the needs of shipowners, industry, and the society. Icebreaker services are commissioned from the Finnish State Shipping Enterprise or private shipping companies.

- **The Finnish Road Administration**[230]

  It is responsible for Finland's highway network. Its mission is to provide smooth, safe and environmentally friendly road connections. The Traffic Management Centre collects real-time information on road and traffic conditions using various roadside detectors and cameras. Valuable information on the traffic situation is also received from the Police, Rescue Centres, municipalities and other cooperating partners and road users.

CHEMICAL INDUSTRY

Public Authorities:

- ***Advisory Committee on Chemicals***[231]

[228] http://www.rautatievirasto.fi/en/front_page
[229] http://www.fma.fi
[230] http://www.tiehallinto.fi/
[231] http://www.stm.fi/Resource.phx/eng/orgis/board/chemicals/chemicals.htx

The Advisory Committee on Chemicals oversees co-operation between the authorities and businesses in the Chemicals sector. One of the main goals of legislation on chemicals is to prevent environmental damage. Under the Chemicals Act[232], businesses are obliged wherever possible to use the chemicals that result in the lowest risks, or adopt methods that avoid using chemicals altogether. The environmental authorities co-operate on the supervision of the use of chemicals with other organisations, including health and safety authorities, the agricultural authorities, officials responsible for safety standards, and several research institutes.

RESEARCH FACILITIES

- ***The Emergency Services College[233]***

  The Emergency Services College is supervised by the Ministry of the Interior and provides vocational training to the rescue services and emergency response centres. In addition, the College provides preparedness training for disturbances in normal conditions and emergency conditions as well as for international civil crisis management tasks. The College contributes to research and development. The College is also responsible for maintaining the assignment register of the rescue services (PRONTO) and the central library of the rescue profession.

- ***Technical Research Centre of Finland[234]***

  The Technical Research Centre of Finland (VTT) is an impartial expert organisation whose objective is to develop new technologies, create new innovations and increase its customer's competitiveness. With its expertise, VTT undertakes research, development, testing and information services for the public sector and companies as well as international organisations. VTT conduct a research program on “managing risks, safety and security”[235]

[232] http://www.finlex.fi
[233] http://www.pelastusopisto.fi/pelastus/home.nsf/pages/index_eng
[234] http://www.vtt.fi/?lang=en
[235] http://www.vtt.fi/palvelut/cluster3/topic3_8/index.jsp?lang=en

11 France

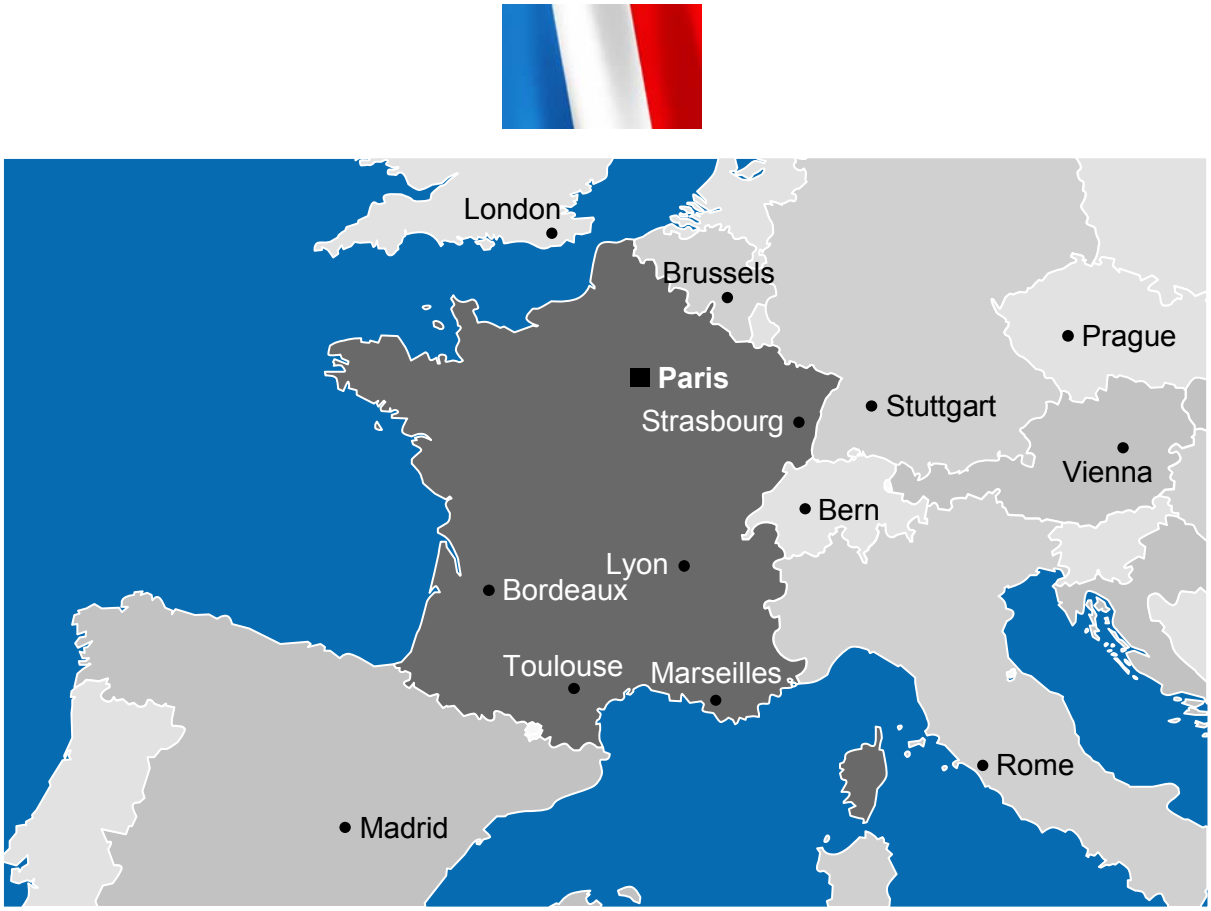


Figure 48: France

11.1 Summary

	Organisational Model	Strategy & Policy	Methodology & Standards	Public-Private Partnership & International Collaboration	Funding & Human Resources	Training & Exercises	Sector-Specific Key Players & Initiatives
France	▪ Defence and national security agency (SGDN) with CIP responsibility reporting to Prime Minister	▪ CI Sectors and objectives defined (Decree No. 2006-212)	▪ EBIOS for CIIP ▪ Specific Methodolog and Tool for Risk Analysis for CIP	▪ CIParis 2008 ▪ National committee for CIP ▪ Security liaison officers meetings ▪ CSTI (Strategic Advisory Board on Information	▪ Approximately 500 people across all levels of government have additional duties related to CIP	▪ CFSSI (Training Centres on systems security) ▪ National exercises at government level, with private operators	▪ Multiple initiatives identified for ICT sector

France manages Critical Infrastructure Protection through a centralized approach: the defense and national security agency (SGDSN), on behalf of Prime minister, coordinates the CIP policy. The ministries in charge of specific sectors are responsible for the implementation.

A decree[236] issued in 2006 contemplates the protection of the national infrastructure through the protection of the essential economic sectors and aims to enhance protection of vulnerabilities, analysing the threats by their nature. In 2008, the Whitebook on Defence and National Security[237] was released and confirmed the importance of CIP.

The approach of the French regulatory framework is based on risk management, prevention and Intervention plans, and information sharing is encouraged.

236 Decree No. 2006-212 of 23 February 2006, now in defense code, articles R. 1332-1 to R. 1332-42
237 http://www.livreblancdefenseetsecurite.gouv.fr/en/

11.2 Organisational Model

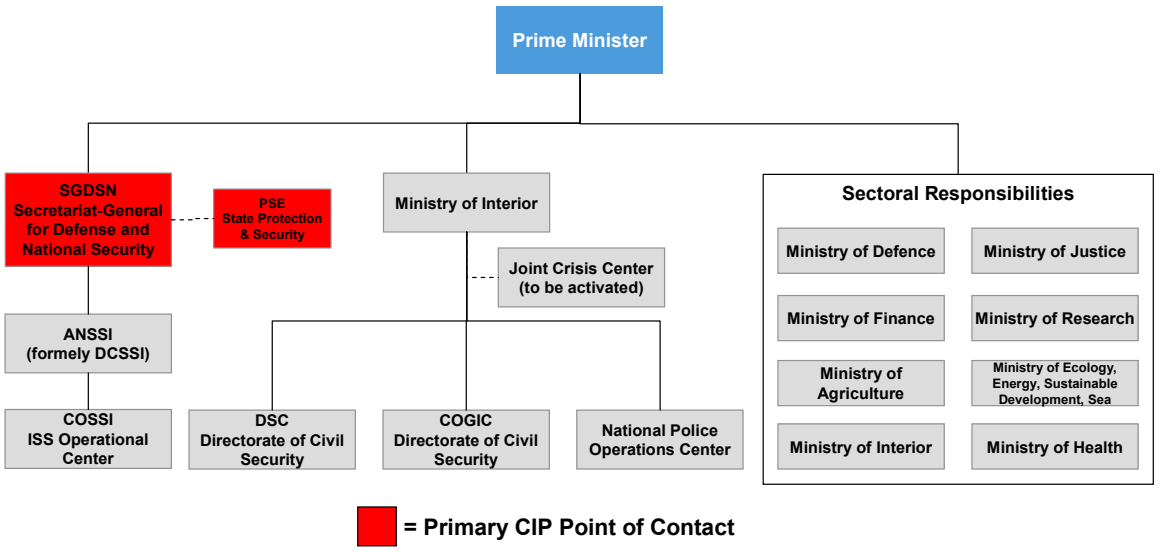


Figure 49: Organisational Chart (only CIP-related agencies shown)

Main Actors/Responsibilities:

- ***Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN)* (General Secretariat for Defence and National Security)**[238]

  In addition to its primary duties of national and international security affairs, the SGDSN bears complete responsibility for organizing CIP. It is directly subordinated to the French prime minister and assists the Prime Minister's office in the co-ordination of the preparation, implementation, and follow-up of the government's decisions regarding defence and security policy, including the security of information systems.[239]

  The State Protection and Security (PSE) division of SGDSN deals with security planning, esp. "Vigipirate plans", CBRN, major exercises, and Security Technologies. The CIP unit is part of PSE.

  In the Defence and National Security Whitebook produced by the SGDN, a new Organisational Chart for the asset of the National Security is defined (see below). This innovation includes the introduction of a Defence and National Security Council, composed of the President of the Republic, the Prime Minister, the Minister of Foreign and European Affairs, the Minister of the Interior, the Minister of Defence, the Minister

238 http://www.sgdn.gouv.fr/sommaire_en.php
239 ETH Zurich – CIIP Handbook 2008

of the Economy and the Minister of the Budget. Other Ministers may be convened depending on the subjects discussed.

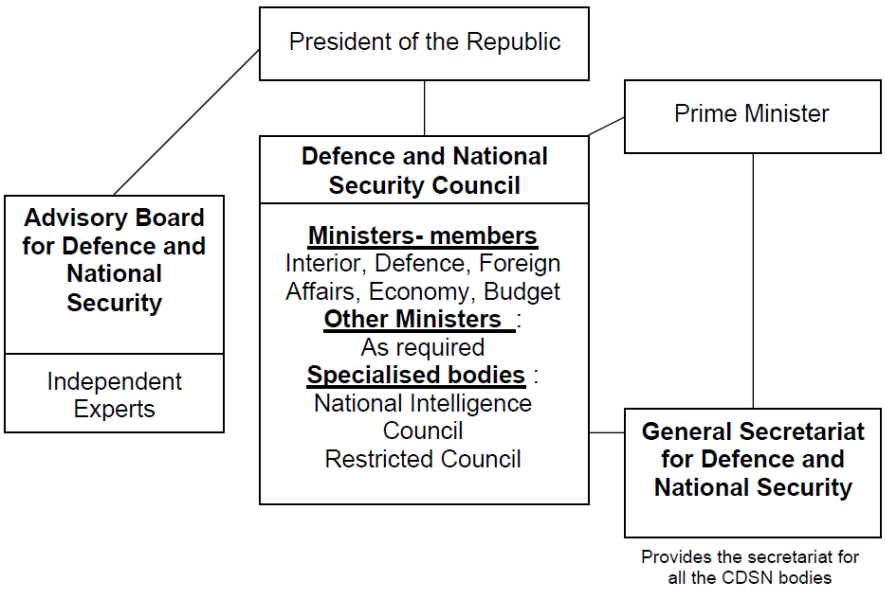


Figure 50: The Defence and National Security Council (CDSN)

- ***Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI – formerly DCSSI)*** **(National Agency for Information Systems Security)**[240]

  The DCSSI was founded in July 2001, and it replaced in its functions the *Service Central de la Sécurité des Systèmes d'Information* (Central Service for Information System Security), responsible for information systems security. This department has very recently been elevated to agency status, and its name has changed appropriately to ANSSI. It is under the responsibility of the General Secretariat for Defence and National Security.

  The main responsibilities of ANSSI are:

  - Contributing to the interdepartmental definition and to the expression of the government concerning information system security
  - Assuring the function of the national regulatory authority for information system security, delivering agreements, warnings, and certificates for national information systems, the products for cryptography used by administrations and public services, and controlling the centres for the evaluation of information technology security (CESTI)
  - Evaluating threats against information systems, giving warnings, and developing the capacity to prevent and deal with emergencies
  - Assisting public services on ISS

[240] http://www.ssi.gouv.fr/fr/dcssi/

- Developing scientific and technical expert knowledge concerning ISS for administrations and public services
- Training for ISS, through the *Centre de Formation à la Sécurité des Systèmes d'Information CFSSI* (ISS Training Centre)

- ***Centre Opérationnel en Sécurité des Systèmes d'Information, COSSI* (ISS Operational Centre)**

  The COSSI is a French service of the DCSSI tasked to defend information systems, including government networks. It coordinates the intervention of ministries in case of attack. It also prepares and implements the specific ISS measures of Vigipirate plan against terrorist attacks, under the responsibility of PSE.

  It is composed of two entities:

  1. The Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques (CERTA)[241], assuring expertise
  2. The Centre de Veille Permanente de Conduite et de Synthèse (CEVECS)

- ***Ministère de l'Intérieur* (Ministry of the Interior)[242]**

  The Ministry of the Interior (Ministère de l'Intérieur) in France is responsible for:

  - Managing the National Police Force
  - The general interior security of the country, with respect to criminal acts or natural catastrophes
  - The granting of identity documents and driving licenses through the network of *préfectures*
  - Relations between the central government and local governments
  - Logistics and organisation of political elections at the national and prefectoral levels
  - All departemental *préfets* and sub-prefects are subordinated to the Ministry of the Interior
  - Attached to the Ministry of the Interior there is the *Institut National des Hautes Études de Sécurité*, INHES (National Institute of Security Studies)[243]

- ***Joint Crisis Center (To be activated)***

  The Ministry of Interior has recently approved the activation of a joint crisis center that will operate in a subsidiary structure with three key components:

  1. National Police Operations Center
  2. National Guard ("gendarmerie")
  3. Civil Protection

241 http://www.certa.ssi.gouv.fr/
242 http://www.interieur.gouv.fr/
243 http://www.inhes.interieur.gouv.fr/

In addition to this joint center, each responsible ministry will continue to operate its own individual crisis center.

- ***Direction de la Sécurité Civile, DSC* (Directorate of Civil Security)[244]**

  Operating for the French Ministry of the Interior, the *Direction de la Sécurité Civile* is a civil defence agency, employing roughly 2500 civilian and military personnel over 60 sites. Known as the *Protection Civile* until 1976, the *Sécurité Civile* is split into several branches. It is responsible for the management of threats in France such as incidents and natural catastrophes.

  The DSC works in four different sectors of competence:

  - The national operational services
  - The *sapeurs-pompiers* (firefighters) and the other rescue actors
  - The management of risks
  - Administration and logistics

- ***Le centre opérationnel de gestion interministérielle des crises, COGIC* (Operational Centre of Interministerial Crisis Management)[245]**

  The COGIC is a centre created by the government and the Ministry of Interior for crisis management and civil defence and security. It is in contact with the Operational Centre of the National Police and the *Centre de Planification et de Conduite des Opérations* (Operational Planning and Execution Centre) of the Ministry of Defence. In case of crisis, the COGIC coordinates the rescue teams, public and private as well as local and national.

- ***Ministère de la Défense (Ministry of Defence)[246]***

  The Ministry of Defence is responsible for the security of the French people and their interests in France and abroad. It guarantees an active policy on diplomatic, economic and cultural issues in all continents, the security of French people, and the respect of international agreements. In addition to the traditional mission of national interest defence, this Ministry aims to support the conditions for European defence development, to contribute to international stability and to the establishment of a new global conception of defence that can manage new risks and threats.

NOTE: Although **no formal working group has been established,** the following Ministries have sector-specific CIP responsibilities and meet regularly with the Ministry of Interior and SGDSN to discuss threats, intervention plans, and other CIP-related topics:

- ***Ministère de la Justice* (Ministry of Justice)[247]**

  The French Minister of Justice is a top-level cabinet position in the French government. The Minister's roles are to:

  - oversee the building, maintenance and administration of courts;

244 http://www.interieur.gouv.fr/sections/a_l_interieur/defense_et_securite_civiles/presentation/view
245 http://www.interieur.gouv.fr/sections/a_l_interieur/defense_et_securite_civiles/gestion-risques/cogic
246 http://www.defense.gouv.fr/
247 http://www.justice.gouv.fr/

- sit as vice-president of the judicial council (which oversees the judicial performance and advises on prosecutiorial performance);
- supervise public prosecutions;
- direct corrections and the prison system
- propose legislation affecting civil or criminal law or procedure.

- ***Ministère de l'Économie, de l'industrie et de l'emploi*** **(Ministry of Finance)**[248]

  The Minister oversees, inter alia, national funds and financial and economic system, especially with the Office of the Treasurer and Receiver General (Direction générale du Trésor et de la politique économique); the development, regulation and control of economy including industry, tourism, small business, competition, and consumer security, and other matters excluding energy, industrial security, environmental affairs and transportations which are under the authority of the Ministre d'Etat, Minister for Ecology, Energy, Sustainable Development and Sea.

- ***Ministère de l'Enseignement supérieur et de la Recherche*** **(Ministry of Research)**[249]

  The Ministry of Research is charged, inter alia, with running France's public educational system and with the supervision of agreements and authorizations for private teaching organizations.

- ***Ministère de l'alimentation, de l'agriculture et de la pêche*** **(Ministry of Agriculture)**[250]

  The Ministry of Agriculture is the governmental body charged with regulation and policy, for agriculture, fisheries, forestry, and food.

- ***Ministère de l'Écologie, de l'Énergie, du Développement durable et de la Mer*** **(Ministry of Ecology, Energy, Sustainable Development, and Sea)**[251]

  The Ministry works in close collaboration with many other ministries so that public policy (transport, infrastructure, energy, industry, agriculture, regional development, health, research, sea, urban planning, education, etc.) promotes sustainable development and incorporates more environmental concerns.

11.3 Strategy & Policy

- ***Secteurs d'Activités d'Importance Vitale***[252] ***(Decree No. 2006-212 of 23 February 2006)***

  Decree No. 2006-212 on the protection of essential economic sectors (dated February 23, 2006) stated:

  - The necessity to carry out a risk analysis by sector (defined below)

248 http://www.minefe.gouv.fr/
249 http://www.enseignementsup-recherche.gouv.fr/pid20002/ministere.html
250 http://agriculture.gouv.fr/
251 http://www.developpement-durable.gouv.fr/rubrique.php3?id_rubrique=768
252 http://sra-e-2006.ijs.si/files/contributions/100/106_SALVI_public.ppt#375,6,And now ?

- Operators must establish an “Operator Security Plan”
- Public authorities must establish an “External Security Plan”

The decree also defines which sectors are considered critical, as vital to the social and economic processes and infrastructure. These sectors are[253]:

- State sectors: civilian activities, justice, military activites (including defense industries)
- Human: food, water, health
- Economics: energy (incl. nuclear), financial, transport
- Technology: communication technologies and broadcasting, industry, space and research

Each of the 12 essential economic sectors will include a national security directive for operators.

- ***Défense et Sécurité Nationale: Le Livre Blanc*** **(The Defence and National Security Whitebook[254]) June 2008**

  The Defence and National Security Whitebook presents new national security strategy that includes an all-hazards approach with particular emphasis on the terrorist threat. The document outlines strategic analysis for the next 15 years and supports a global approach to security interests. It outlines five key strategic functions.

  1. intelligence and anticipation: Citizens expect State understanding and preparation
  2. Prevention: Prevent or limit the occurrence of threats or wars
  3. Deterrence: Prevent any State from considering an attack on the vital interests of France
  4. Protection: Ensure the security of citizens, society, and the economic well-being of the country **(NOTE: This is the key function regarding CIP activities)**
  5. Intervention: Provide national security in close cooperation with European partners and allies

  Implementation of the Whitebook also changed the name of SGDN to Secretariat-General for Defense and National Security (SGDSN). It will also include the creation of the French information security agency, reporting directly to the new SGDSN.

253 *Elgin M. Brunner and Manuel Suter,* INTERNATIONAL CIIP HANDBOOK 2008/2009, Centre for Security Studies, ETH Zurich

254 http://merln.ndu.edu/whitepapers.html

11.4 Methodology & Standards

There are 5 priority work streams identified for implementing the new defence and national security strategy:

- Regulations revision
- Anticipation fo external and international crises
- Crises management improvement
- **Resilience (namely CIP and BCP)**
- Detections of CBRNE threats

SGDSN's CIP-related work around these work streams, and in particular around resilience, is based in the protection measures of the VIGIPIRATE architecture:

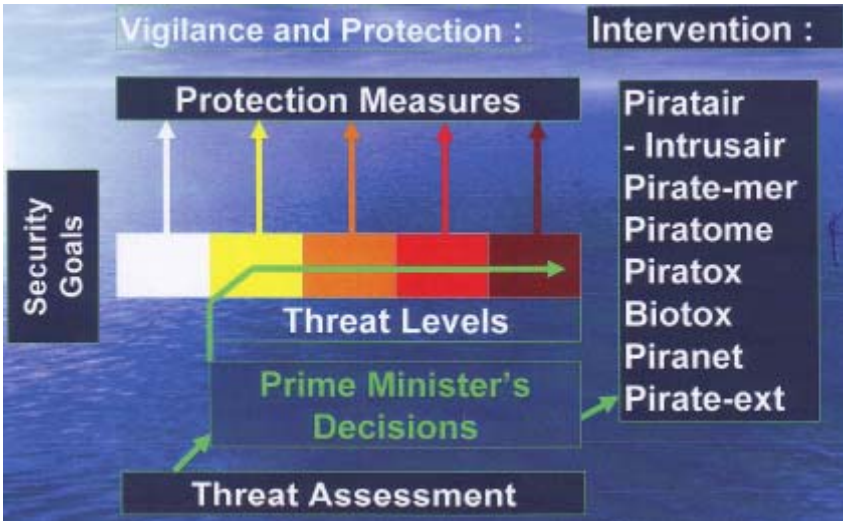


Figure 51: VIGIPRATE Architecture

The PIRATE Intervention Plans (Pitarair – Intrusair, Pirate-mer, …) within the overall VIGIPRIATE architecture are managed by the SGDSN and approved by the Prime Minister. Each plan includes provisions for progressive phases of alert, "reflex" action, and sustained action. Operators and public authorities share the responsibility for security in the Prevention and Protection Plans, with an understood shift toward public authorities as the threat levels elevate (as illustrated in figure 5):

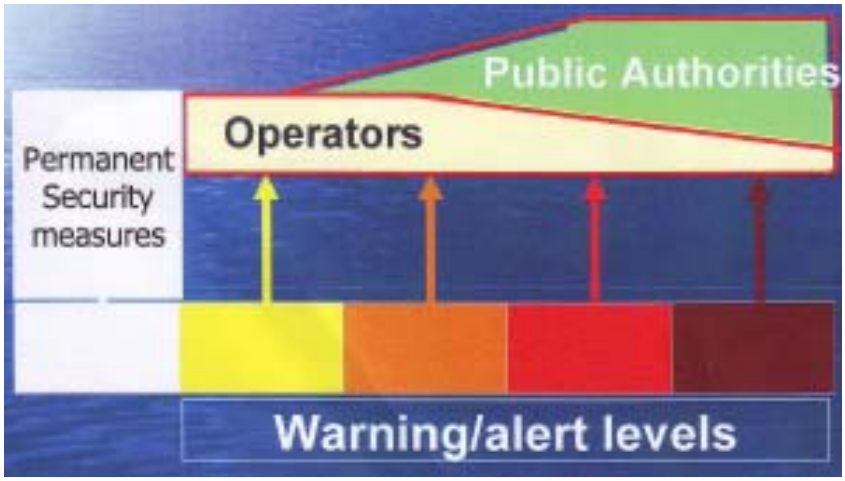


Figure 52: Shifting Security Responsibilities in VIGIPIRATE Prevention and Protection Plans

The Intervention Plans cover many aspects of Intervention and Crisis Management:

- Intelligence and/or detection
- Threat identification
- Alert and preparation
- Governmental organisation management, inter-agency crisis centre activation & communication
- Law enforcement and first responders pre-positioning
- Mitigation / intervention plan activation
- Specific measures activation
- Secondary attack prevention

The Critical Infrastructure Protection programme plays a key role in the VIGIPIRATE architecture by ensuring better application of the national warning / alert, prevention, and protection plan. Through their involvement in CIP activities, operators better protect their installations of vital importance and their key assets. They also coordinate with public authorities in prevention, detection, and intervention measures.

The architecture of the CIP program in particular promotes an interactive top-down / bottom-up approach toward identifying and protecting critical infrastructure.

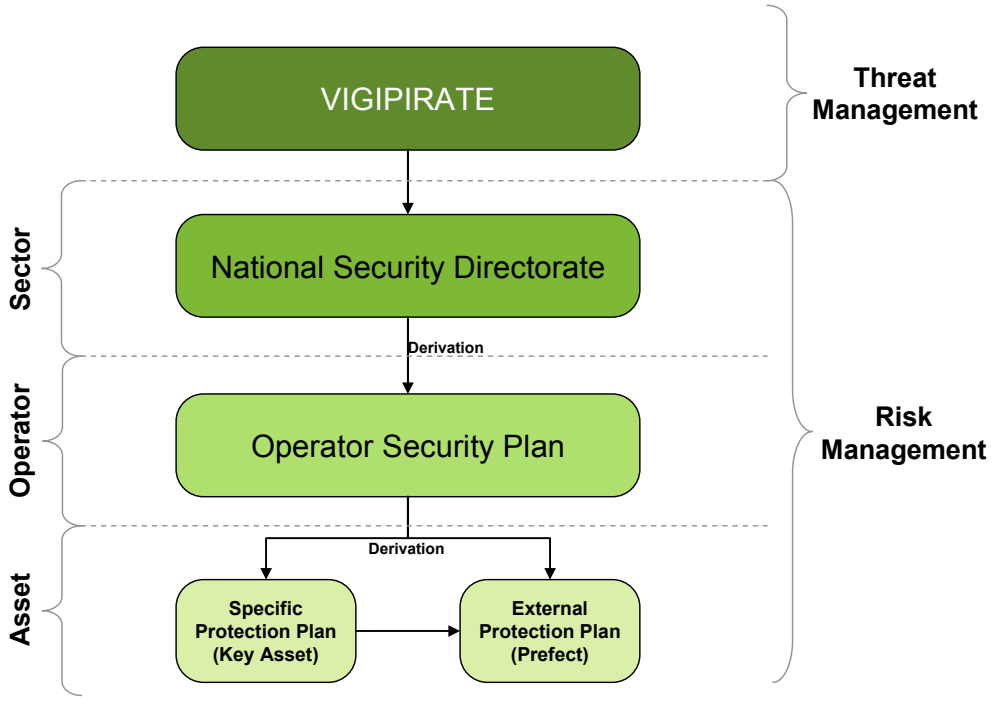


Figure 53: CIP General Architecture

The current phase of activity within the development of the VIGIPIRATE strategy employs a top-down strategy in which the government is guiding a national-level risk assessment programme for each sector. The objectives for this risk assessment were set by the SGDSN together with other ministries. These objectives were then sent to operators of vital importance (identified by SGDSN together with the ministries) that maintain services / activities of vital importance. Each ministry developed the list of vital operators for its sector of responsibility and then initiated the risk assessment process in that sector.

Once identified as a “critical operator”, the designated operators must then execute a risk assessment against the objectives and threats identified by the ministry and validated by SGDSN. The process for executing the risk assessment is in line with international best practices in the risk management field. To estimate risk levels, operators must evaluate threat scenarios and vulnerabilities to determine the likelihood of a successful attack, as well as the estimated impact. These values are used to plot individual risks on a risk heat map:

Figure 54: Example of Risk Heat Map (Illustrative)

As a result of the risk assessment, each operator must produce a list of key assets and an overall Operator Security Plan (OSP). The OSP contains, inter alia:

- Threat scenarios (mainly terrorism) including cyber-attacks
- Risk assessment and risk management
- Security targets
- Security measures (including Vigipirate measures)
- List of key assets (points of vital importance)

The responsible ministry must approve the OSP and the list of key assets, and SGDSN validates the final document. Within the OSP plan, operators also establish security liaison officers (SLOs): one overall for the company and one for each key asset. The SLO is authorized to receive classified information.

The operator then designs Specific Protection Plans (SPP) linked to Vigipirate plans for each key asset. The local prefect approves the SPP plan and creates and corresponding External Protection Plan (EPP).

Specific Protection Plan (SPP)	External Protection Plan (EPP)
▪ Local application of OSP principles ▪ Organization and relation with authorities ▪ Alert management ▪ Security meaures (including Vigipirate measures) ▪ Security management	▪ Regular surveillance ▪ Alert reponse ▪ Intervention of security forces ▪ Mitigation

Figure 55: Specific and External Protection Plans

Operators have a two-year time limit from the time at which the ministry responsible for their sector identifies them as a vital operator to submit Specific Protection Plans for their key assets. If the operator is not able to produce the SPP within this timeframe, they risk entering into a regulatory process that could potentially result in a fine. If they are still not able to produce the plan by the end of this process, the responsible prefect will intervene and create the plan on their behalf.

11.5 Public – Private Partnership & International Collaboration

The CIP strategy in France depends heavily on a cooperation model that aligns the activities of public authorities and critical infrastructure operators across all phases of a risk management life cycle (and in particular regarding security measures):

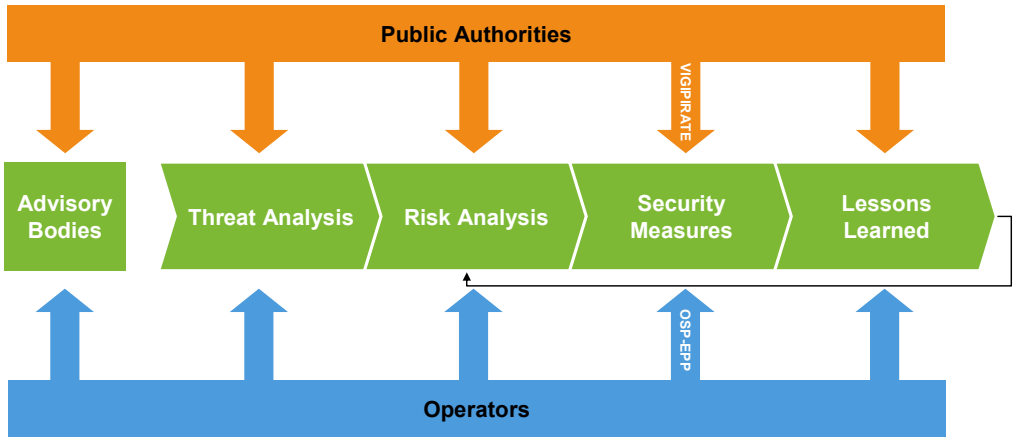


Figure 56: Specific and External Protection Plans

This "risk-managed, threat-driven" approach includes 2-3 monthly meetings between SGDSN, the SLOs identified by the operators, and the relative ministries for the sectors of the operators. There is also a yearly meeting with the chairmen of operators of vital importance.

- ***CIParis 2008 – Protection des Activitiés d'Importance Vitale*** **(Critical Infrastructure Protection)**[255]

  The French General Secretariat for Defence and National Security, organized a broad European conference on the CIP topic with two objectives:

[255] https://www.hcfdc.org/sgdn/secure/presentation.php?&lang=en

- Share and assess initial results, in particular with respect to risk analysis methods and operators security plans that enable critically important assets to be identified as well as efficiently ensure their protection
- Compare the modi operandi and procedures implemented to carry out these studies between States and operators, in various sectors

- **National Committee for Activities of Vital Importance (CNSAIV)**

  Chaired by the General Secretary for Defense and National Security, this committee gathers once a year with the CEOs of ten major operators to discuss of CIP-related issues at a strategic level.

- ***Commission Interministérielle de Coordination des Réseaux et Services de Télécommunications pour la Défense et la Sécurité Publique— (CICREST)***[256]

  CICREST is a permanent working group among the public authorities and the telecommunication operators that discusses the evolution of legal framework and is a channel that can be used to develop and/or discuss best practices or guidelines.

  Although this particular PPP is limited to the Ministry of Finance, most other ministries have similar PPP's in place.

- **European Peer Evaluation**

  In the framework of the second round of peer evaluation covering preparedness and consequence management in case of a terrorist attack, an EC-sponsored expert team made a ninth visit to France from 19 to 21 November 2008. The expert team included members from the Council General Secretariat (DG Justice and Home Affairs), European Commission (DG JLS), Europol (Serious Crime Department – Counter Terrorism), Portugal (Security Information Department), and Romania (Ministry of the Interior). The group evaluated, inter alia, the effectiveness of the VIGIPIRATE architecture and its management by SGDN.

11.6 Funding & Human Resources

Within SGDSN, there are approximately 40 staff members that work on CIP activities in addition to other security-related activities. There are only a few resources dedicated exclusively to CIP work.

In addition, each CIP-relevant Ministry has a range of 10-40 staff members working on CIP activities in addition to other activities. Within the subsidiary structure, there are seven regional zones with a few staff members each, as well as 100 prefects with at least one local CIP representative.

Overall, there are approximately 500 staff members within the entire structure working in some form on CIP activities, although the vast majority of these resources also have other responsibilities beyond their CIP-related activities.

[256] ENISA – Stock taking eCommunications Resilience - 2008

11.7 Training & Exercises

- ***The SGDSN*** prepares and leads four major exercises per year, involving the political level. Major operators participate to this exercises.
- ***The High Committee for Civil Defence,*** a non-governmental association, disseminates knowledge and good practices concerning security, organizes training sessions on CIP, especially for private operators***.***
- ***Centre de formation à la Sécurité des Systèmes d'Information, CFSSI*** **(Information Systems Security Training Center)**[257]

  The Information Systems Security Training Centres is attached to the DCSSI, and it aims to increase awareness on information systems security by training experts to design, evaluate, and make recommendations on communication security, protection against viruses, and computer security. The CFSSI also develops partnerships with higher education and further training centres.

11.8 Sector – Specific Key Players & Initiatives

NOTE: Any requests for additional detailed information or points of contact within specific sectors should be directed to the SGDSN. The SGDSN will validate all requests and then forward them to the appropriate Ministry for action.

ENERGY

Public authorities:

- ***Direction Générale de l'Énergie et du Climat, DGEC (General Directorate for Energy and Climate)***[258]

  The DGEC is part of the *Ministère de l'écologie, de l'énergie, du développement durable et de la mer)* (Ministry of Ecology, Energy, Sustainable Developpment and Sea). The mission of the DGEC is the elaboration and application of the policy related to energy, materials, climate and pollution.

NUCLEAR INDUSTRY

Public authorities:

- ***Autorité de Sureté Nucléaire, ASN (Nuclear Safety Authority)***[259]

  The Nuclear Safety Authority (ASN) is an independent administrative authority set up by law 2006-686 of 13 June 2006 concerning nuclear transparency and safety (known as the "TSN law"). It is tasked, on behalf of the State, with regulating nuclear safety and radiation protection in order to protect workers, patients, the public and the

257 http://www.ssi.gouv.fr/fr/formation/
258 http://www.industrie.gouv.fr/energie/
259 http://www.asn.fr/

environment from the risks involved in nuclear activities. It also contributes to informing the citizens.

- ***Commissariat à l'énergie atomique, CEA (Atomic Energy Commission)***[260]

  It conducts fundamental and applied research into many areas, including CBRN and the design of nuclear reactors, the manufacturing of integrated circuits, the use of radionuclides for curing illnesses, seismology and tsunami propagation and the safety of computerized systems.

INFORMATION AND COMMUNICATION TECHNOLOGY

Initiatives:

- ***Défense et Sécurité Nationale: Le Livre Blanc*** **(The Defence and National Security Whitebook**[261]**) June 2008**

  The new strategy for defence and national security includes, inter alia, the creation of a French information security agency. The mission of the agency will be to ensure the coordination of ministries in the prevention, alerting, and protection against cyber attacks, as well as cyber-crisis management.

  Within the new strategy, cyber-defence is considered a key capacity, and the cyber threat is given a high level of priority amongst the emerging threats. Early warning and detection are considered essential elements of the planned approach to protecting the Internet, which the strategy considers as a critical infrastructure.

  The Agency will report to SGDSN, which in-turn reports directly to the Prime Minister.

- ***Expression des Besoins et Identification des Objectifs de Sécurité, EBIOS (Expression of Needs and Identification of Security Objects)***[262]

  EBIOS is a methodology and free software package developed and regularly updated by the DCSSI to assess and treat risk related to information systems security. The EBIOS knowledge bases introduce and describe the types of entity, attack methods, vulnerabilities, security objectives and security requirements.

  The methodology consists of the five steps. They are directly applicable to most sectors, but they can be easily acquired and adapted to any specific context.

[260] http://www.cea.fr/
[261] http://merln.ndu.edu/whitepapers.html
[262] http://www.ssi.gouv.fr/en/confidence/ebiospresentation.html

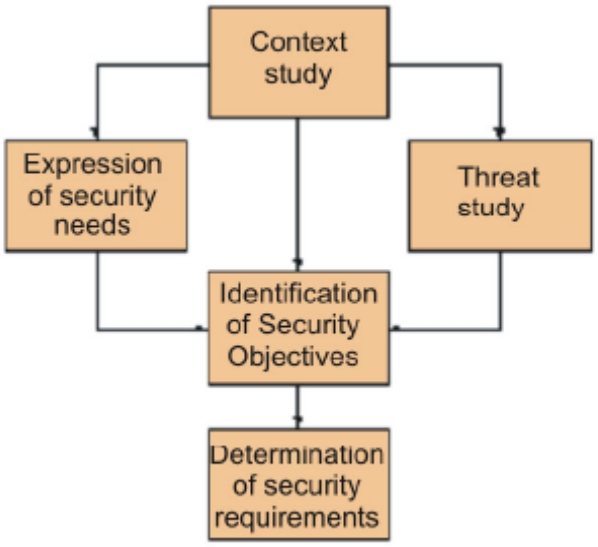


Figure 57: EBIOS Global Approach

After the first step, the environment, purpose and operation of the target system are perfectly known and the essential element and entities on which they are based are identified.

The second step contributes to risk assessment (risk estimation and definition of risk criteria). It allows the impacts to be formalized and the security needs of the essential elements to be evaluated in terms of availability, integrity and confidentiality, etc.

The third step also forms part of the risk assessment (risk analysis). It consists in identifying and describing the threats affecting the system. This is achieved by studying the attack methods and threat agents likely to use them, the exploitable vulnerabilities of the entities and the opportunities they present.

The fourth step contributes to risk evaluation and treatment. During this step, the real risks affecting the system are formalized by comparing the threats (harmful events) with the security needs (consequences). They are covered by security objectives, consistent with the assumptions, security rules, regulatory references, operating mode and identified constraints which make up the security specifications.

The fifth and last step belongs to risk treatment. It explains how to determine functional requirements allowing security objectives to be fulfilled and assurance requirements allowing the level of confidence in their fulfillment to be increased.

The methodology provides information to support decision-making (detailed descriptions, strategic stakes, detailed risks with their impact on the organization, explicit security objectives and requirements). The structured approach allows the component elements of risks to be identified (entities and vulnerabilities, attack methods and threat agents, essential elements and sensitivities, etc.). This methodical construction contributes to an exhaustive risk analysis.

In addition, selected parts of the approach can be used separately to conduct, for example, a vulnerability analysis (just the threat study) or to identify the strategic elements (context study, non-detailed expression of needs, non-detailed study of threats).

- ***Central Office for the Fight Against Hi-Tech Crime***

  The Central Office for the Fight against Cyber-Crime was founded in May 2000 by the Ministry of the Interior. It aims to control intrusions and crimes in the ICT field and it supports legal investigations in this field. The Central Office works closely with the national police and the private sector.

- ***Computer Emergency Response Teams, CERTs***

  Three different Computer Emergency Response Teams operate in France:

  The CERT-RENATER[263], for research centres and academic institutions, founded in 1993. It is dedicated to the National Network of Telecommunications for Technology, Education, and Research;

  The CERTA[264], particularly addressed to French administration services. It evaluates threats and gives advice, warnings, and information on how to prevent, respond to, and handle an attack against information systems. It is part of COSSI.

  The CERT-IST[265] (CERT-Industry, Services, and Tertiary), launched in1999 by Alcatel (a telecom company), CNES (the French Space Agency), France Telecom, and the TotalFinaElf energy group.

263 http://www.renater.fr/spip.php?rubrique19
264 http://www.certa.ssi.gouv.fr/
265 http://www.cert-ist.com/

12 Germany

Figure 58: Germany

12.1 Summary

	Organisational Model	Strategy & Policy	Methodology & Standards	Public-Private Partnership & International Collaboration	Funding & Human Resources	Training & Exercises	Sector-Specific Key Players & Initiatives
Germany	▪ Ministry of Interior (BMI) coordinates activities on CIP matters on national level ▪ CIP is handled be the relevant government departments and the Länder.*	▪ National Strategy for Critical Infrastructure Protection (CIP Strategy) ▪ National plan for Information Infrastructure Protection (NPSI ▪ Covered in Civil Protection policy	▪ Methodologies, standards, operating plans and technology regarding CIP are in place	▪ Participation in bilateral and multilateral agreements ▪ CIIP: UP Kritis working groups between CI providers, relevant associations and public authorities*	▪ No information available	▪ The BSI coordinates regular exercises on CIIP ▪ BBK performs every 2 years a national crisis management exercise (LÜKEX)	▪

In Germany, there is no dedicated, CIP-specific coordinating agency. However, the Federal Ministry of the Interior (Federal BMI) provides inter-departmental coordination of national-level CIP measures, and sectoral issues regarding CIP are dealt with at the level of the single responsible Ministry/Agency; in addition, in line with Germany's federal structure, responsibility for many infrastructure sectors lies with the *Länder* (Federal States).

Critical Infrastructures in Germany are defined as "*organizational and physical infrastructures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences.*"[266]

In Germany, critical infrastructures include:

Technical Basic Infrastructure
▪ Energy supply
▪ Information and communications technology
▪ Transport(ation)
▪ (Drinking-) water supply and sewage disposal

Socio-Economic Services Infrastructure
▪ Public health; food
▪ Emergency and rescue services; disaster control and management
▪ Parliament; government; public administration; law enforcement agencies
▪ Finance; insurance business
▪ Media; and cultural objects (cultural heritage items)

[266] National Strategy for Critical Infrastructure Protection (CIP Strategy)

12.2 Organisational Model

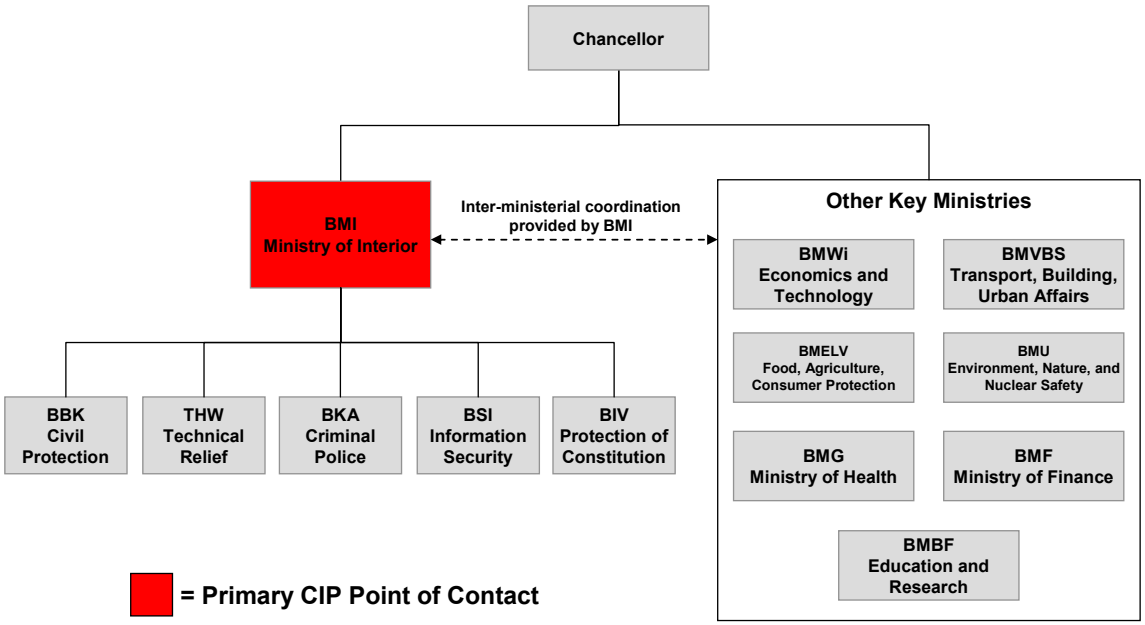


Figure 59: Organisational Chart (only CIP-related agencies shown)

Main Actors/ Responsibilities:

On principle, protection of critical infrastructure in Germany is handled by the relevant government departments; in addition, in line with Germany's federal structure, responsibility for many infrastructure sectors lies with the *Länder* (Federal States).

The overview shows the ministries and agencies/offices which, in their portfolio, cover a certain infrastructure on a political level; however, in most cases, the operators in charge are privately owned or privately organised, also on regional and/or local level.

- ***Bundesministerium des Innern* (BMI) (The Federal Ministry of the Interior)**[267]

  At the federal level, the Ministry of Interior (BMI) has the coordinating function regarding critical infrastructure protection. This derives, in particular, from the Ministry's responsibility for internal security, counter-terrorism, and civil protection/emergency management and disaster relief. The BMI sends representatives to international bodies and provides the national CIP Contact Point liaising with the European Commission.

[267] The Federal Ministry of the Interior (BMI) *Bundeministerium des Innern.* http://www.bmi.bund.de/

With regards to CIP, the management responsibility falls within the activities of the directorate general *for* crisis management and civil protection *(Abteilung Krisenmanagement und Bevölkerungsschutz),* especially in its unit dealing with Critical Infrastructure Protection.

Specific Sectoral responsibilities managed by the BMI include critical IT-Infrastructure (Ministry's CIO office), counter-terrorism, and protection / security of nuclear plants (directorate-general for public security – Abteilung für *Öffentliche Sicherheit*).

In 2002, representatives from all involved departments (Crisis Management and Civil Protection, Public Security, and the CIO) started to meet on a regular basis in order to ensure a coordinated approach towards CIP.

The BMI is supported by the following agencies within its remit:

- ***Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)*** **(Federal Office of Civil Protection and Disaster Assistance)**[268]

  BBK was established in May 2004 under the Federal Ministry of the Interior (BMI), and is the first manifestation of the new joint strategy for the protection of the population in Germany "*Neue Strategie zum Schutz der Bevölkerung in Deutschland*[269]". The responsibilities of the BBK include the support of states and communities, harmonisation of federal planning, research analysis, training of executive personnel, public information, and standardisation and quality assurance. The BBK plays a significant role in CIP matters and operates in close cooperation with the other stakeholders in the field of CIIP.

- ***Technisches Hilfswerk (THW)*** **(Federal Agency for Technical Relief)**

  THW is the operational civil protection organisation of the Federal Republic of Germany. It is a nationwide disaster relief organisation capable of responding to emergencies at the local, regional, national and global level. It assists regular fire and rescue teams in the rehabilitation of physical infrastructures after larger fires or natural disasters.

- ***Bundeskriminalamt (BKA)*** **(Federal Criminal Police Agency)**[270]

  The BKA is responsible for prosecuting crimes against the internal or external security of the Federal Republic of Germany. They are involved in crimes that entail damage to or the destruction of critical infrastructures that could result in a serious threat to life, health, or the functioning of society.

- ***Bundesamt für Sicherheit in der Informationstechnik (BSI)*** **(Federal Office for Information Security)**[271]

---

268 Federal Office of Civil Protection and Disaster Assistance (BBK) *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe* http://www.bbk.bund.de

269 http://www.bbk.bund.de/nn_402294/DE/06__Fachinformationsstelle/02__Rechtsgrundlagen/05__IMK-Beschluesse/IMK-Beschluesse__node.html__nnn=true (in German) Federal Office of Civil Protection and Disaster Assistance (BBK) *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe* http://www.bbk.bund.de

270 Federal Criminal Police Agency (BKA) *Bundeskriminalamt* http://www.bundeskriminalamt.de

271 Federal Office for Information Security (BSI) *Bundesamt für Sicherheit in der Informationstechnik* http://www.bsi.bund.de

Founded in 1991, the BSI is an independent and neutral organisation for all questions related to IT security in the information society. It works on an operative basis for the federal administration, on a co-operative basis for industry and on an informative basis for all German citizens. It is directly accountable to the Federal Ministry of the Interior and it plays a particularly significant role in CIIP. BSI works closely with critical infrastructure operators in the exchange of information, the formulation of coordinated protection strategies and joint drills and exercises on handling IT crises.

- ***Bundesamt für Verfassungsschutz*** **(BfV) (Federal Office for the Protection of the Constitution)**

  BfV is Germany's domestic intelligence agency responsible for the surveillance of anti-constitutional activities in Germany. It has been tasked with the collection and analysis of information, intelligence and other documents concerning intelligence activities and to contribute to protective security and counter-sabotage.

In addition to the BMI, several key Ministries are involved in CIP activities on the federal level. They are listed below, supplemented by subordinated agencies / offices with certain responsibilities in the field of CIP:

- ***Bundesministerium für Wirtschaft und Technologie (BMWi)*** **(Federal Ministry of Economics and Technology)**[272]

  The BMWi is responsible for economic policies and overseeing several critical sectors. It is responsible for ensuring the availability of adequate telecommunications infrastructure and services, and it also develops the framework for securing the country's energy supply.

  - *Bundesnetzagentur (BNetzA)* (Federal Network Agency)[273]

    In July 2005, the Regulatory Authority for Telecommunications and Posts was renamed the Federal Network Agency for Electricity, Gas, Telecommunications, Post, and Railway (BNetzA).

- ***Bundesministerium für Verkehr, Bauen und Stadtplanung (BMVBS)*** **(Federal Ministry of Transport, Building, and Urban Affairs)**[274]

  The areas of responsibility of the Federal Ministry of Transport, Building and Urban Affairs are closely related to the basic requirements of German citizens, namely housing, mobility, and related infrastructures. To be able, as the state, to provide optimum services for the public in these areas, the Ministry conducts departmental research to exploit all the possibilities of high-quality knowledge-based external advice, in order to help answer the numerous and diverse questions. The BMVBS is supported by the *Bundesanstalt für Verkehrswesen (BASt)*(Federal Highway Research Institute).

---

272 Federal Ministry of Economics and Technology (BMWi) *Bundesministerium für Wirtschaft und Technologie* http://www.bmwi.de

273 Federal Network Agency (BNetzA) *Bundesnetzagentur* http://www.bundesnetzagentur.de

274 http://www.bmvbs.de/en/-,1877/The-Ministry.htm

- ***Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz (BMELV)* (Federal Ministry of Food, Agriculture, and Consumer Protection)**[275]

  The BMELV's main aims include promoting a balanced, healthy diet and safe foods, ensuring that everyday goods are safe, assisting in the development of clear consumer rights, and helping to ensure that the agricultural sector is strong and able to perform the duties required of it.

  The provision of healthy food in sufficient quantities is the main condition to avoid problems within this critical infrastructure. The BMELV is supported by several institutions where parts of their work-programme are also encourage the protection of the agri-food sector:

  - *Bundesinstitut für Risikobewertung* (BfR) (Federal Institute for Risk Assessment) [276]
  - *Bundesanstalt für Verbraucherschutz und Lebensmittelsicherheit* (BVL)(The Federal Office of Consumer Protection and Food Safety)
  - *Friedrich-Loeffler-Institut* (FLI) (Federal Research Institute for Animal Health)
  - *Max Rubner-Institut* (MRI) (Federal Research Institute of Nutrition and Food)
  - *Julius Kühn-Institute* (JKI) (Federal Centre for Cultivated Plants)
  - *Bundesanstalt für Landwirtschaft und Ernährung* (BLE) (Federal Agency for Agriculture and Food)
- ***Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU)* (Federal Ministry for the Environment, Nature Conservation, and Nuclear Safety)**[277]

  The BMU has a wide range of principal functions that deal with or influence critical infrastructure:

Fundamental environmental policy issues	International cooperation
Informing and educating the public about environmental issues	Environmental remediation and development in Eastern Germany
Climate protection, environment and energy	Air quality control
Noise abatement	Conservation of groundwater, rivers, lakes and seas
Soil conservation and remediation of contaminated sites	Closed substance cycle management and waste policy
Chemicals safety, environment and health	Precautions against emergencies in industrial plants
Protection, maintenance and sustainable utilisation of biodiversity	Safety of nuclear facilities
Radiological protection	Nuclear supply and disposal

Figure 60: BMU Principal Functions

[275] http://www.bmelv.de/cln_135/EN/Ministry/ministry_node.html
[276] Federal Institute for Risk Assessment (BfR) *Bundesinstitut für Risikobewertung* http://www.bfr.bund.de
[277] http://www.bmu.de/english/the_ministry/tasks/principal_functions/doc/3094.php

- ***Bundesministerium für Gesundheit (BMG)* (Federal Ministry of Health)**[278]

  The Federal Ministry of Health is responsible for a variety of policy areas, whereby its activities focus predominantly on the drafting of bills, ordinances, and administrative regulations. Moreover, by means of prevention campaigns, the Federal Ministry of Health seeks to improve the population's health. It is supported by the *Robert Koch Institut (RKI).*

- ***Bundesministerium der Finanzen (BMF)* (Federal Ministry of Finance)**

  The BMF plays a major role in the economic growth and the financial stability of the country. It prepares the financial and fiscal framework for the country along the political guidelines of the Federal Chancellery. The ministry of finance has the important responsibility of preparing the federal budget of the country. The ministry also regulates the capital market of the country and oversees the development of the German stock and bond market. Moreover, it contributes to the European integration and worldwide globalization of financial markets. It is supported by:

  - *Bundesanstalt für Finanzdienstleistungsaufsicht* (Bafin) - The Federal Financial Supervisory Authority, which supervises banks, financial service providers, insurance companies and securities trading. Its objective is to ensure the proper functioning, stability and integrity of the German financial market. For that reason BaFin seeks to ensure that market operators comply with the relevant laws.
  - Deutsche Bundesbank - The central bank of Germany is independent of instructions from the Federal Government. The overriding aim of Bundesbank is to safeguard the stability of the general price level and the financial system. It has the following five core business areas Monetary policy, Financial and monetary system, Banking supervision (together with BaFin), Cashless payments and Cash management.

- ***The Bundesministerium für Bildung und Forschung (BMBF)* - Federal Ministry of Education and Research**[279]

  BMBF deals with subjects related to CIP that are increasingly included in their research programmes. A cross-sector approach is pursued within the framework of the National Research Programme "Research for Civil Security" (*Forschung für die zivile Sicherheit*)[280]. Under two programme lines - "Scenario-based Security Research" (Szenarienorientierte Sicherheitsforschung) and "Mixed-Technology Networks" (Technologieverbünde) - specific research projects, inter alia on transport infrastructure and supply infrastructure, have been launched; the overall security research programme, which continues until 2010 and covers various other aspects of national security, has a financial envelope of €123 million €.

278 http://www.bmg.bund.de/EN/Ministerium/ministry__node.html?__nnn=true
279 Federal Ministry of Education and Research (BMBF) *Bundesministerium für Bildung und Forschung* http://www.bmbf.de
280 http://www.bmbf.bund.de/de/11773.php

12.3 Strategy & Policy

Germany has, both nationally and internationally, actively addressed matters of critical infrastructure protection and is guided by the principle of joint action by the state, society, and business and industry. This cooperative approach was confirmed with the National Strategy for Critical Infrastructure Protection (CIP Strategy) which was approved by the Council of Ministers in June 2009.[281] The state cooperates, on a partnership basis, with other public and private actors in developing analyses and protection concepts. Either as a moderator (primarily) or by rule-making (if required), the state regulates the measures for safeguarding and securing the overall system and the system procedural flows.

Infrastructure is considered "critical" whenever it is of major importance to the functioning of modern societies and any failure or degradation would result in sustained disruptions in the overall system. An important criterium for this assessment is **criticality** as:

> *a relative measure of the importance of a given infrastructure in terms of the impact of its disruption or functional failure on the security of supply, i.e. providing society with important goods and services.*

Such criticality may be systemic and/or symbolic in nature. An infrastructure will, in particular, be of *systemic criticality* whenever - due to its structural, functional and technical position within the overall system of infrastructure sectors - it is highly relevant as regards interdependencies. Examples are the *electricity* and *information and telecommunication infrastructure.* Due to the size and density of their respective networks, they are of particular relevance as large-area and prolonged outages may lead to serious disruptions of community life and processes, as well as public safety and security.

An infrastructure may be of *symbolic criticality* if its loss might, due to its cultural significance or its important role in creating a sense of identity, emotionally unsettle a nation's society and psychologically have a lasting unbalancing effect.

Vital critical infrastructures may, with reference to their technical, structural, and functional specifics, be classified as either “technical basic infrastructure” or “socio-economic services infrastructure”. In Germany, these include:

[281] BMI, *National Strategy for Critical Infrastructure Protection (CIP),* 17 June 2009 : http://www.bmi.bund.de/cln_095/SharedDocs/Downloads/DE/Broschueren/DE/2009/kritis_englisch.html?nn=106228

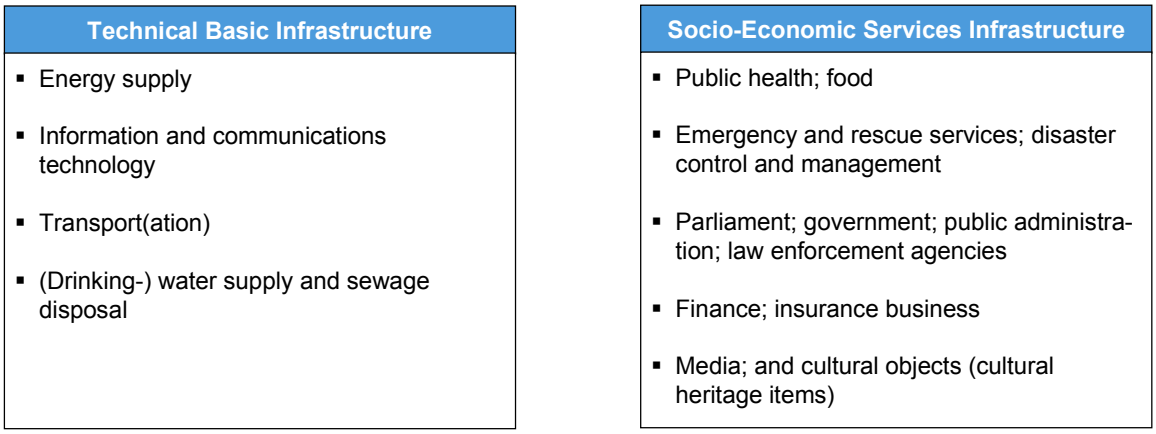


Figure 61: Critical Infrastructures in Germany

Significant interdependencies exist between these two infrastructure sectors since nearly all of the socio-economic services infrastructures largely rely on the unrestricted availability of the technical basic infrastructure. However, technical basic infrastructures, in their turn, depend on socio-economic services such as stable legal service or functioning first response, emergency medical and rescue services in the event of a crisis.

A look at the ownership structure shows that, as a rule, the various infrastructures are not state-owned facilities but that the majority of them are operated and controlled by private enterprises – part of which were privatized only recently. Increasingly, private-sector enterprises also deliver various public infrastructure services at the local government level.

As a result of this tendency towards private ownership, the responsibility for the security, reliability, and availability of such infrastructure increasingly passes to the private sector or, at least, becomes a shared responsibility. Therefore, the functions incumbent on the state and/or public authorities are primarily directed at making provisions for safeguarding and controlling the supply of goods and services in times of crisis when regular market mechanisms no longer function. Therefore, as a precaution against, and in view of coping with, serious disruptions and severe disasters/emergencies, the requirement is for institutionalized, organized cooperation between state and industry within the framework of established security partnerships.

Legal Framework

In Germany, there is no specific legal act focusing exclusively on critical infrastructure protection. It is chiefly implemented as a so-called "annexed" responsibility (i.e. an ancillary/ subsidiary preparatory or implementing task) of both general and sector-specific hazard control. Therefore, CIP measures are primarily based on sector-specific legislation introduced by the responsible ministries.

In addition to general obligations incumbent on operators, sector-specific regulations on infrastructure protection cover particular aspects such as:

- fire protection and fire-fighting
- structural measures (e.g. out-side protection)
- specific requirements to be met in terms of organization and staffing
- security of supply
- preparation of security plans
- designation of safety and security officials
- development of threat analyses and/or risk assessments.

Examples of these regulations, which in part are based on international agreements, include:

- ***Zivilschutz- und Katastrophenhilfegesetz (ZSKG*) (Act on the Federal Civil Protection and Disaster Response System)**

  Express mention is made of critical infrastructure protection in Section 18, para. 2, of the Act of 02 April 2009, under which the Federal Government - within the scope of its responsibilities - advises and supports the *Länder* on CIP matters. According to the principles of regional planning (Section 2, para. 2, no. 3, of the Federal Regional Planning Act *(Raumordnungsgesetz)*, critical infrastructure protection shall be taken into consideration at the regional planning levels.

- ***Störfallverordnung* (Major Incidents Ordinance)** or the ***Gefahrgutverordnungen Binnenschifffahrt, Eisenbahn, (See, Straße)* (Carriage of Dangerous Goods Regulations)** for the various transport modes
- ***Energiewirtschaftsgesetz (EnWG)* (Energy Industry Act)** on the Supply of Electricity and Gas
- ***Ernährungsvorsorgegesetz (EVG*) (Emergency Food Supply Act)** on the supply of agri-food products in food supply crisis situations

In addition to the *National Strategy for Critical Infrastructure Protection*, the following documents serve as key CIP references and initiatives in Germany:

- ***Schutz Kritischer Infrastrukturen – Basisschutzkonzept* (Critical Infrastructure Protection – Baseline Protection Concept)** [282]

  The guide was developed in close cooperation between the Federal Ministry of the Interior (BMI), the Federal Office of Civil Protection and Disaster Assistance (BBK),

[282] Critical Infrastructure Protection – Baseline Protection Concept http://www.bmi.bund.de/cln_012/nn_148138/Internet/Content/Broschueren/2005/Basisschutzkonzept__kritische__Infrastrukturen__en.html; http://www.bmi.bund.de/cln_012/nn_122688/Internet/Content/Common/Anlagen/Broschueren/2007/Basisschutzkonzept__kritische__Infrastrukturen__en,templateId=raw,property=publicationFile.pdf/Basisschutzkonzept_kritische_Infrastrukturen_en.pdf (PDF version)

the Federal Criminal Police Agency (BKA), and the private sector. It aims to reduce the vulnerability of critical infrastructures to natural events and accidents by providing guidance for the analysis of potential hazards such as terrorist attacks, criminal acts, and natural disasters, as well as recommendation for companies on adequate protective measures. It builds upon the trusting cooperation between the state and operators of infrastructure facilities in identifying and specifying necessary protection measures because while the state remains the guarantor for internal security and coordinates the information and communication process, only the operators, with their sufficiently detailed knowledge of their infrastructures, are in a position to implement concrete protective measures in an effective manner.

- **Protecting Critical Infrastructures- Risk and Crisis Management - A Guide for Companies and Government Authorities)**

  The CIP Baseline protection concept was complemented by a guideline *Protecting Critical Infrastructures – Risk and Crisis Management. A Guide for Companies and Government Authorities* presented in January 2008. This guideline provides methods to support the implementation of risk management and crisis management in enterprises and government organisations and offers checklists and examples.

- ***Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI)*** **(National Plan for Information Infrastructure Protection)**

  The NPSI[283], issued in 2005, is the federal government's core strategy for a comprehensive approach to the protection of IT-dependent assets. It aims to strengthen IT security and to enable rapid responses to IT-related crises.

  The NPSI strategic objectives include:

  - Prevention – protecting information infrastructures adequately
  - Preparedness – responding effectively to IT security incidents
  - Sustainability – enhancing German competence in IT security and setting international standards

  The NPSI is directed toward the whole German society but more importantly addresses public authorities and operators of critical infrastructures. The protection of the infrastructures in Germany is based on the notion that, although the government is the main responsible authority for these initiatives, 80% of critical infrastructures are run by private institutions; the involvement of private institutions is therefore paramount to mitigate the dangers of possible attacks on Germany's infrastructure system.

283 National Plan for Information Infrastructure Protection (NPSI) *Nationaler Plan zum Schutz der Informationsinfrastrukturen* (NPSI) http://www.bsi.bund.de/english/topics/kritis/veroeffentlichungen.htm#NPSI

12.4 Methodology & Standards

In the CIP field, Germany pursues an all-hazard approach, without expressly assigning any priorities. The types of hazard are, as a rule, divided into the two categories "natural hazards" and "man-made hazards"; the latter can, in their turn, be divided into technical failure or human error, on the one hand, and terrorism, crime, and war, on the other hand.

Natural events	Technical failure/ human error	Terrorism, crime, war
Extreme weather events inter alia, storms, heavy precipitation, drops in temperature, floods, heat waves, droughts	System failure inter alia, insufficient or excessive complexity of planning, defective hardware and/or software bugs	Terrorism
Forest and heathland fires	Negligence	Sabotage
Seismic events	Accidents and emergencies	Other forms of crime
Epidemics and pandemics in man, animals and plants	Failures in organization inter alia, shortcomings in risk and crisis management, inadequate co-ordination and co-operation	Civil wars and wars
Cosmic events inter alia, energy storms, meteorites and comets		

Figure 62: Natural and Man-Made Hazards in Germany[284]

Germany's efforts in the CIP field aim at ensuring and raising the level of protection by suitable measures, coordinated with the other stake-holders to improve:

Prevention

- All existing and anticipated risks will be spotted beforehand, and critical elements and processes are identified
- Severe disruption and failure of important infrastructure services will be avoided, to the extent possible, by means of comprehensive proactive (preparedness) arrangements and be minimized by an existing efficient risk and crisis management system and by providing adequate optional courses of action
- The measures taken should, whenever possible, be regularly included for testing in exercises;

Response

[284] BMI, *National Strategy for Critical Infrastructure Protection (CIP)*, 17 June 2009

- The consequences of severe disruptions and failures will be minimized to the greatest extent possible by means of effective emergency and crisis management and efficient redundancies as well as effective self-help capabilities of the entities and establishments directly affected
- All activities undertaken at the time of an incident or disaster/emergency must aim at providing a maximum of effectiveness so that regular operations can be resumed without delay, if possible

Sustainability

In addition, 'lessons learnt' regarding enhanced critical infrastructure protection must be obtained from constantly updated threat analyses and from the analyses of techno-logical and other incidents that occurred within the country or abroad, and these findings must be translated into protection standards to be developed jointly with the operators concerned and to be harmonized at the international level.

Consistent implementation of these objectives in the form of a risk management cycle for critical infrastructure will offer the necessary guarantee of a consistent protective system of sustained effectiveness, which enhances the German security competencies that are also utilized in the international exchange of experience.

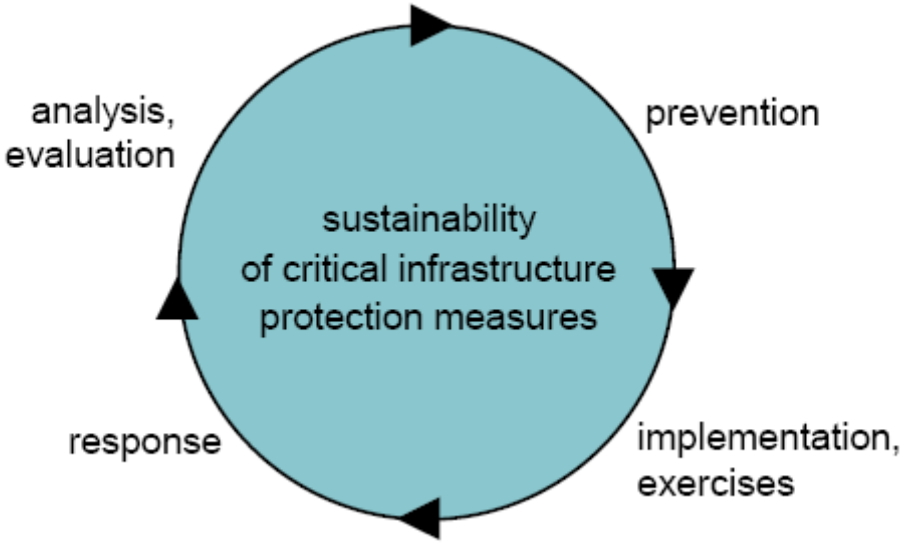


Figure 63: German CIP Risk Management Cycle

The Federation, the *Länder* and local governments are required *jointly* to enhance and implement critical infrastructure protection in their respective areas of responsibility. This purpose is served by a structured implementation procedure at these three tiers of government; this procedure is based on the cooperative approach adopted by the Federal Administration with the involvement of the other major players (i.e. operators and the relevant associations) and comprises the following work packages, which in part are implemented in parallel:

1. Definition of general protection targets
2. Analysis of threats, vulnerabilities, and management capabilities
3. Assessment of the threats involved
4. Specification of protection targets, taking account of existing protective measures; analysis of existing regulations and, where applicable, identification of additional measures contributing to goal attainment; if and where required, legislation.

These work packages are implemented primarily by the public sector with the collaboration of the companies and operators concerned. Responsibility for coordination at the federal level lies with the Federal Ministry of the Interior.

5. Implementation of goal attainment measures primarily by means of:
    - association-specific solutions and internal regulations
    - self-commitment agreements by business and industry
    - development of protection concepts by companies
6. Continuous, intensive risk communication process (dialogue on analysis findings, assessments, protection targets, and action options)

Responsibility for the implementation of work packages 5 and 6 primarily lies with the relevant companies, operators and associations, with the participation of public agencies.

For the implementation of the National Critical Infrastructure Protection Strategy, an extensive set of instruments is available in the form of:

- Programmes and plans (e.g. the National Plan for Information Infrastructure Protection *(NPSI)* and the related implementation plans as a strategic concept for IT infrastructure protection);
- Specific recommendations for action (e.g. the national Baseline Protection Concept as a basic guidance to physical critical infrastructure protection; the Risk and Crisis Management Guide for Critical Infrastructure Operators, or the national special protection concepts as detailed recommendations for action for the protection of individual CI sectors and sub-sectors);
- Standards, norms and regulations (e.g. the *BSI* Information Security Standards as a basic recommendation for action addressed to critical infrastructure operators; or the regulations of the German Gas and Water Supply Association *(DVGW)* on risk management in the field of drinking water supply).

In view of the large variety of standards, recommendations, and guides on risk management at the national and international levels, the following is only a selection of examples of general standards, cross-sectoral recommendations issued by public authorities, and sectoral standards and recommendations considered within the German CIP approach:

1. General standards

In developing or expanding a risk management scheme or parts of such a system, many critical infrastructure facilities in Germany refer to national and international

standards dealing with security issues in general or with specific aspects or measures related to risk management or business continuity, such as the Australian/New Zealand standard "AS/NZS 4360:2004 Risk Management" or the British standard "BS 25999 Business Continuity". This applies, in particular, to enterprises which come within the scope of application of the German companies act *(*Stock Corporation Act - *Aktiengesetz, AktG)* and/or of the Control and Transparency in Companies Act *(Gesetz zur Kontrolle und Transparenz im Unternehmensbereich - KonTraG)* (concerning companies limited by shares/stock corporations; and large limited liability companies) or which are placed in an international context.

Regarding IT security, the *BSI* standards on information security constitute the basic recommendation for CI providers/operators.

2. **Cross-sectoral recommendations by public authorities on risk management**

   In addition to general standards, a number of cross-sectoral recommendations by public authorities are available which, as a rule, were developed jointly with industrial actors and which can be used by CI operators/providers as a tool in developing and expanding a risk management scheme. The Guide issued by the Federal BMI on "Critical Infrastructure Protection, Risk and Crisis Management. Guide for Business/Industry and Public Authorities" *(Schutz kritischer Infrastrukturen, Risiko- und Krisenmanagement. Leitfaden für Unternehmen und Behörden)* is addressed to all critical infrastructure providers with the aim of pressing ahead with the identification and reduction of operational risks in business/industry and public authorities. Further examples of risk management recommendations made by government agencies are the Guide issued by the Federal BMI on Critical Infrastructure Protection – Baseline Security Strategy *(Schutz kritischer Infrastrukturen, Basisschutzkonzept)* and the *BSI* Emergency Management Standard (BSI Standard 100-4).

3. **Sectoral standards and criteria to be met by risk management systems**

   The general and governmental cross-sectoral standards and recommendations are supplemented by standards, sets of regulations, and recommendations which deal with the specific requirements of the various CI sectors. Thus, for the banking and insurance sectors, minimum risk management requirements have been laid down, (i.e. "minimum requirements for risk management (credit institutions)" - *MaRisk (BA)*, and "minimum requirements for risk management (insurance business)" - *MaRisk (VA)*, respectively). In the gas and water supply sector, the catalogue of rules and standards of the German Technical and Scientific Association for Gas and Water *(Deutsche Vereinigung des Gas- und Wasserfaches e.V. - DVGW)* has been supplemented by risk management instructions for water suppliers and by crisis management instructions for water and gas suppliers, respectively. As a non-binding recommendation, a Guide on Risk Management in Hospitals *(Leitfaden zum Risikomanagement in Krankenhäusern)* was published by the Federal Office of Civil Pro-tection and Disaster Assistance *(BBK)*.

Preventive security plans

Preventive security plans are developed both by government authorities (strategic-conceptual) and by business/industry (operative). The government side has developed pertinent framework strategies and plans especially for the IT sector:

- In 2005, the National CIIP Plan *(Nationaler Plan zum Schutz der Informationsinfrastrukturen – NPSI)* was issued as an overarching IT security strategy; this plan addresses three security-policy fields of activity: adequate protection of information infrastructure (prevention), effective action in case of IT security-related incidents (preparedness), and strengthening of German IT security skills/capabilities and of standardization at the international level (sustainability).
- In 2007, application of the National CIIP Plan *(NPSI)* was further detailed by the Implementation Plan for the Federal Administration *(Umsetzungsplan für die Bundesverwaltung - UP Bund)* and the CIP Implementation Plan *(Umsetzungsplan für kritische Infrastrukturen - UP KRITIS)*. The *UP KRITIS* plan was drafted in close co-operation with representatives from industry; in 2008, as a follow-up, a framework concept for "Early Detection and Mitigation of IT-related Crises" *(Früherkennung und Bewältigung von IT-Krisen)* was finalized and was published in June 2009.

In addition, specific preventive security plans and contingency plans are developed by critical infrastructure providers on their own. Such plans are, as a rule, based on sectoral regulations or on requirements stipulated in cross-sectoral legislation.

One example of sectoral regularization, including requirements to be met by security and contingency plans, can be found in Section 49 of the Energy Industry Act *(Energiewirtschaftsgesetz - EnWG)* which expressly refers to the aforementioned catalogue of rules and standards of the German Technical and Scientific Association for Gas and Water *(DVGW)* and to the obligation to comply with the recognized technical rules described in that catalogue. This also covers implementation of the Instructions for crisis management by gas suppliers *(Hinweisblatt zum Krisenmanagement durch Gasversorger)*.

Another example can be found in the transport sector where the operators of certain transport tunnels must prepare risk analyses and make the safety-related documentation available to the competent public authorities.

Methodology

The Federal Office for Information Security (BSI) has developed a specific methodology – the *Analyse Kritischer Infrastrukturen Die Methode AKIS* (Analysis of Critical Infrastructural Sector ACIS Methodology)[285] developed for identifying the processes in the economic and political context that are critical in a society.

The ACIS Methodology involves breaking down the sectors and processes in the critical infrastructural sectors and identifying their scale of criticality. A criticality matrix is used to estimate the degree of negative effects and their probability of occurrence. The

[285] Analysis of Critical Infrastructural Sector *ACIS* Methodology. http://www.bsi.de/english/topics/kritis/acis_paper_en.pdf

processes that are subsequently considered as highly critical for the whole society are assessed in terms of their dependence on Information Technology.

12.5 Public – Private Partnership & International Collaboration

- **Public-Private Partnerships**

  In the CIP field, BMI closely cooperates both with the relevant line ministries on the sectoral level and with critical infrastructure providers on the cross-sectoral level. Following the events of September 11, 2001, bilateral talks with major operators of critical infrastructure were intensified with a focus on specific objectives. These talks continue on an ad-hoc basis. In addition, cooperation activities are pursued with business and industry regarding the development of guidance documents and recommendations, as well as specific projects and research programmes. For example, a working group “Crisis Management in the Electricity Sector” has been established and takes place on a regular basis to guarantee a coordinated approach according to the existing legal framework.

  In this context, it has been possible to win the support of partners from industry for the development of the "CIP Implementation Plan“ *(Umsetzungsplan KRITIS – UP KRITIS)*. Given the focus on critical information infrastructure protection (CIIP), the participating enterprises and organizations were selected with the specific aim of including those subsectors which already experienced a high degree of IT dependency. The *UP KRITIS* was published in 2007; since then, cooperation with the *UP KRITIS* partners has been pursued in four institutionalized working groups (emergency and crisis exercises; crisis response and management; continuity of CI services; and national/international co-operation), during exercises, and in developing a network of Single Points of Contact (SPOC), so as to achieve an effective crisis response capability in case of IT-related incidents.

  Another example in the field of CIIP is CERT-Verbund, a network of German security and Computer Emergency Response Teams (CERTs) for the exchange of information (e.g. on vulnerabilities or on incidents) and for co-operation regarding critical incident management. Membership is based on non-disclosure agreements and on compliance with a "code of conduct".

- **International co-operation**

  The German CIP approach promotes bilateral and multilateral activities aimed at critical infrastructure protection, such as exchanges of information, methods, and tested procedures. To this end, Germany closely cooperates with other EU Member States and with the European Commission. In doing so, Germany will dedicate its efforts to establishing adequate protective standards within the European area and will resolutely pursue the realization of its CIP-related concepts and visions on the basis of its National Strategy.

CIP is also one important part within the Senior Civil Emergency Planning Committee (SCEPC) at NATO: Under SCEPC's direction, eight technical Planning Boards and Committees coordinate planning in various areas of civil activity.[286]

To name an example for bilateral cooperation, an agreement was signed in July 2003 between the United States Department of Homeland Security and the German Ministry of the Interior to increase the protection of computers systems and networks. The initiatives included the establishment of a joint early warning system to detect attacks on critical information infrastructure; to conduct a joint tabletop exercise to simulate the reaction to an international IT-security incident; as a result, the *International Watch and Warning Network* (IWWN) had been established, currently involving 15 participants from all continents. This bilateral initiative complements ongoing U.S. - Germany counter-terrorism efforts.

Further examples for Germany's involvement in international CIIP activities include:

IWWN: The International Watch and Warning Network

This network provides its Member States with a cooperation and coordination forum for exchanges of information and for the management of IT-related or Internet-related incidents as a CIIP input. The IWWN was established in 2004, with 15 founding members.

Group of the European Government CERTs (EGC)

This informal group of gov-CERTs aims to develop effective cooperation in the field of critical incident management, also in the light of the commonalities between their specific clients and of the problems to be taken into account in information exchanges and cooperation (e.g. handling of classified material).

G8 / G8 HTCSG

In 2003, during the G8 consultations, eleven "G8 Principles for the Protection of Critical Infrastructures" were agreed (these principles were, in January 2004, also adopted by the UN). Since then CIIP, besides other subjects, is dealt with within the G8 framework by the High-Tech Crime Sub-Group (HTCSG) of the Roma-Lyon Group. During the German G8 Presidency in 2007, the Guide on "Best practice for improving CIIP in collaboration of governmental bodies with operators of CII" was agreed, which includes seven recommendations on how nations can set up their own CIIP programme.

The Meridian Process was launched in 2005 on the basis of the activities of the G8 HTCSG in order to involve also non-G8 nations in activities aimed at the protection of critical information infrastructure.

MPSCIE (Meridian Process Control Security Information Exchange)

[286] The aim of civil emergency planning in NATO is to collect, analyse and share information on national planning activity to ensure the most effective use of civil resources for use during emergency situations, in accordance with Alliance objectives. It enables Allies and Partner nations to assist each other in preparing for and dealing with the consequences of crisis, disaster or conflict.

This Meridian Process sub-group was set up in mid-2008 for enhancing IT security in process control and monitoring systems. The mid-term and long-term aims include influencing the pertinent standardization activities.

EuroSCSIE (European SCADA and Control Systems Information Exchange)

Dealing with subjects concerning IT security in process control and SCADA systems, and developing the bases for European cooperation among government, research, and industrial actors, as well as users.

12.6 Funding & Human Resources

There is no publically available information available regarding funding and human resources of CIP-related activities in Germany.

12.7 Test, training and exercises

Training

Many universities and universities of applied science *(Fachhochschulen)* at present include CIP-related and risk management subjects or have introduced specific courses of studies on security-relevant subjects (i.e. rescue services; security and crisis management). For example, Bonn University and the Federal Office of Civil Protection and Disaster Assistance *(BBK)* jointly offer a Master's degree course which covers a broad range of subjects related to civil protection / disaster management and also deals with critical infrastructure protection[287].

The *BBK*'s academy, i.e. the Academy for Crisis Management, Emergency Planning and Civil Protection *(Akademie für Krisenmanagement, Notfallplanung und Zivilschutz - AKNZ)*, offers numerous CIP seminars, and the subject of critical infrastructure protection is included also as a subject in other seminars[288] The Academy's target audiences are representatives from federal and *Land* authorities, local government representatives, and company staff.

Sector-specific training is offered by the respective ministries.

Exercises

Many critical infrastructure providers conduct table-top, reduced-scale, and full-scale exercises in their establishments in order to review and monitor their security standard and on-site crisis management. Some operators/providers hold joint exercises of this type; for example, in May 2008, a number of banks in Frankfurt/Main

[287] http://www.uni-bonn.de/Studium/Studiengaenge_und_Abschluesse/Master/Sonstige/KaVoMa.html

[288] http://www.bbk.bund.de/cln_007/nn_402322/SharedDocs/Publikationen/Publikationen__AKNZ/AKNZ__Jhresprogramm__2009.html]

jointly conducted an evacuation exercise. In some cases, security authorities also take part in these operator-led exercises.

Every two years since 2004, the Federal Office of Civil Protection and Disaster Assistance *(BBK)* has organized and hosted the national exercise *LÜKEX (Länderübergreifende Krisen-management Exercise)*, a cross-State crisis management exercise. This exercise includes representatives from federal and *Land* authorities, as well as operators/providers of critical infrastructure. On the basis of scenarios, the existing capabilities, resources, legal regulations, and interaction of various actors in the field of civil protection/disaster management are critically reviewed and assessed. Critical infrastructure providers are increasingly interested in taking part in *LÜKEX* exercises and often combine their own internal exercises with the *LÜKEX* series.

In the field of IT infrastructure, both the Implementation Plan for the Federal Administration *(UP Bund)* and the CIP Implementation Plan *(UP KRITIS)* under the National Plan for Information Infrastructure Protection *(NPSI)* provide for regular exercises. For both implementation plans, framework concepts have been developed which lay down the types of exercises to be held and a time schedule for the development and continuation of a regular exercise scheme. The *UP KRITIS* framework concept for "IT emergency and crisis exercises in critical infrastructur. es" *(IT-Notfall- und Krisenübungen in Kritischen Infrastrukturen)* was finalized in 2008

12.8 Sector – Specific Key Players & Initiatives

See main players under Organizational Model.

13 Greece

Figure 64: Greece

13.1 Summary

	Organisational Model	Strategy & Policy	Methodology s, Standards	Public-Private Partnership & International Collaboration	Funding & Human Resources	Training & Exercises	Sector-Specific Key Players & Initiatives
Greece	▪ There is no single agency specifically dedicated to CIP ▪ General Secretariat for Civil Protection takes care of emergencies	▪ Greece is dealing in an unstructured way with CIP. ▪ CIP is mentioned as an element of the national Civil Protection plan (Xenokrates)	▪ Operating emergency plans for 21 types of risks (natural, technological, others) issued by the competent Ministries	▪ ECURIE	▪ Not Applicable	▪ Not Applicable	▪ National Emergency Plan for Nuclear, Radiological, Biological and Chemical (NRBC)

289

There is no single agency in Greece with sole responsibility for CIP. Civil Protection in Greece is organised as a co-ordinated resource system where national, regional, provincial and local authorities work together with local and public institutions and services. Each of these authorities and institutions has developed its own part of the national Civil Protection plan (*Xenokrates*), and makes its own contribution towards achieving its aims.

The overall objective of the Greek civil protection system is to ensure protection of the population, the environment and property in the event of natural or technological disasters. Specific objectives are to:

- Implement measures within a defined Government framework for the identification and mitigation of natural and technological disasters.
- Plan and lead recovery operations and responses in the event of major emergencies which threaten the population, infrastructure, property or the national inheritance.

[289] Not Applicable = Open Source Research, Web-based survey and individual interviews have not shown information/data on the given argument

13.2 Organisational Model

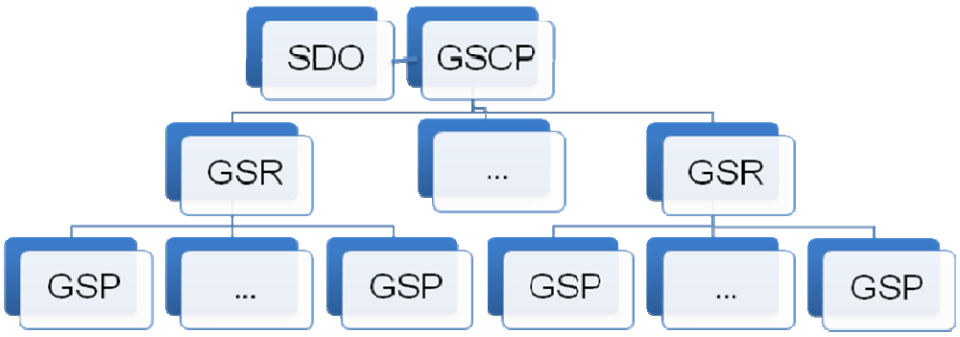


Figure 65: Organisational Chart (only CIP-related agencies shown)

Civil protection in Greece is organised in three administrative levels - national, regional and local. Geographically, Greece is divided in 13 Regions, each divided into a number of Prefectures.

In case of emergencies, the General Secretariat for Civil Protection (GSCP) carries the responsibility to rank a disaster into one of three categories, and make decisions to activate the appropriate civil protection authorities and competent services.

By law 3013/2002 natural and technological disasters are classified into one of three categories according to their expected impact on the population and infrastructures:

- general disasters;
- high or low impact regional disasters, or
- high or low impact local disasters

The management of a low impact local disaster requires activation of the competent authorities of one Prefecture, whilst a high impact local disaster involves more than one Prefecture. The management of a low impact regional disaster requires activation of the competent authorities of one Region whilst a high impact regional disaster involves more than one Region. In the case of general disasters the Minister of Interior is responsible to proclaim the State of Emergency and establish the SDO[290]. In case of regional or local disasters the General Secretary for Civil Protection carries the responsibility to proclaim a Region or a Prefecture in State of Emergency. In case of low impact local disasters the General Secretary for Civil Protection authorises the General Secretary of the Region or the Prefect to proclaim the Region or the Prefecture in State of Emergency.

Main Actors/Responsibilities:

General Secretariat for Civil Protection (GSCP)[291]

This secretariat has been established within the Ministry of the Interior. It is a new institution and manages the prevention and mitigation of natural, technological and other disasters

[290] http://www.icdo.org
[291] http://www.gscp.gr

within an integrated political framework. It is responsible for disaster prevention, relief and consequence management, implementing measures for the identification and mitigation of hazards, and the protection of the population, infrastructure, environment and property.

- ***SDO***[292]

This is an inter-ministerial co-ordination body, which has been established to look after exceptional needs in peacetime and to co-ordinate governmental action in the event of a major disaster. The role of the SDO is to reinforce, within a defined government framework, the co-ordinated activities of the GSCP in the implementation of national policy during emergency situations. The SDO is chaired by the Secretary General of the GSCP. Its members include the Secretary-Generals of the Ministries of the Interior, Public Administration and Decentralisation, Development, Public Works, Forests and Environment, Health and Welfare, Merchandise Marine, Public Order, Transportation and Communications, Media and Public Information, and the Deputy Chief of the National Defence General Staff.

According to the National Civil Protection Plan *Xenokrates,* in case of emergencies the following groups are also involved:

- Ministry of Interior (Υπουργείο Εσωτερικών)[293]
- Ministry of Environment, Physical Planning and Public Works (Υπουργός Περιβάλλοντος, Χωροταξίας και Δημοσίων Έργων)[294]
- Ministry of Development (Υπουργός Ανάπτυξης)[295]
- Ministry of Health and Social Solidarity of Greece (Υπουργός Υγείας και Κοινωνικής Αλληλεγγύης)[296]
- Ministry Employment and Social Protection (Υπουργός Απασχόλησης και Κοινωνικής Προστασίας)[297]
- Ministry of Mercantile Marine, Aegean and Island Policy (Υπουργός Εμπορικής Ναυτιλίας και Νησιωτικής Πολιτικής)[298]

13.3 Strategy & Policy

Emergency planning in Greece is organised at three levels, national, regional and local. At the national level, emergency planning is provided by the National Emergency Plan *Xenokrates*[299].

The National Emergency Plan is issued by the GSCP and includes the following:

- a glossary of civil protection definitions;

[292] http://www.icdo.org
[293] http://www.ypes.gr
[294] http://www.minenv.gr/
[295] http://www.ypan.gr/
[296] http://www.mohaw.gr/
[297] http://www.ypakp.gr/
[298] http://www.yen.gr/
[299] http://www.gaec.gr/en/index.php?fvar=html/president/_info_emergency_response

- the identification of twenty-one different types of natural, technological and other major risks;
- competent authorities for emergency planning, and
- general guidelines for emergency planning.

With the approval of GSCP, the Regions and Prefectures issue their own emergency plans at a regional and local level.

Emergency plans for the 21 different types of natural, technological and other major risks are also issued by the following Ministries:

- ***Ministry of Defence***[300]***:*** 8 plans concerning forest fires, earthquakes, floods, snowfalls, Chemical Biological Radiological Nuclear (CRBN) incidents and transport accidents.
- ***Ministry of Development***[301]***:*** 9 plans concerning earthquakes, tornados, landslides, CBRN, electric power or natural gas failures, storage of hazardous materials, industrial fires, dam failures, and mining accidents.
- ***Ministry of Environment, Physical Planning and Public Works***[302]***:*** 11 plans concerning earthquakes, floods, tornados, snowfalls, landslides, volcanic activity, storage of hazardous materials, industrial fires, environmental pollution, dam failure, and road and railway accidents.
- ***Ministry of Health and Social Solidarity of Greece***[303]***:*** 5 plans covering earthquakes, heat waves, CBRN incidents, environmental pollution and epidemic cases.
- ***Minister of Rural Development and Food***[304]***:*** 7 plans concerning forest fires, floods, snowfalls, heat waves, CBRN incidents, environmental pollution and animal and insect related hazards.
- ***Ministry of Transport and Communications***[305]***:*** 5 plans concerning tornados, CBRN incidents, telecommunication network failure, and road, railway or aircraft accidents.
- ***Ministry of Interior***[306]***:*** 16 plans covering forest fires, earthquakes, floods, tornados, snowfalls, landslides, volcanic activity, CBRN incidents, electric power failure and failure of natural gas transmission lines, storage of hazardous materials, industrial fires, environmental pollution, dam failures, mining accidents, and road, rail and aircraft accidents.
- ***Ministry of Mercantile Marine, Aegean and Island Policy***[307]***:*** 7 plans concerning earthquakes, floods, tornados, CBRN, environmental pollution, marine and aircraft air accidents.

[300] www.mod.mil.gr/
[301] http://www.ypan.gr/
[302] http://www.minenv.gr/
[303] http://www.mohaw.gr/
[304] http://www.minagric.gr/
[305] http://www.yme.gr
[306] http://www.ypes.gr/
[307] http://www.yen.gr/

13.4 Public – Private Partnership & International Collaboration

Greece is member of:

- European Union[308] (Member state)
- Council of Europe[309]
- North Atlantic Treaty Organisation (NATO)[310]
- Organisation for Economic Co-operation and Development (OECD)[311]
- World Trade Organisation (WTO)[312]
- Organisation of Black Sea Economic Cooperation (BSEAC)[313]
- European Community Urgent Radiological Information Exchange (ECURIE)[314]

13.5 Sector – Specific Key Players & Initiatives

ENERGY

Public authorities:

- ***Ministry of Development (Υπουργός Ανάπτυξης)***[315]
  The Ministry of Development deals with issues concerning industry, trade, research, technology, energy and natural resources, and tourism.

  The Department of Energy and Natural Resources is charges with the development of policy for the energy sector and exploitation of mineral resources. It also assists with the implementation of this policy and provides supervision of all bodies concerned with energy and minerals in Greece.

- ***Hellenic Transmission System Operator (HTSO)***[316]

  The HTSO manages electricity distribution in Greece. The role of HTSO is to settle the market - to act like an energy stock market that arranges on a daily basis who owns to whom.

- ***Public Power Corporation S.A. (PPC)***[317]

  The Public Power Corporation was established in 1950 to develop and implement a national energy policy. Today, PPC is the largest power generation company in Greece and the country's sole power supply company, providing electricity to approximately 7.4 million customers. PPC is also the sole company with a fully owned power transmission system in Greece. PPC owns 93% of the installed power capacity in Greece, generated by lignite, fuel oil, hydroelectric and natural gas power plants, as well as by Aeolic and solar energy parks.

[308] http://europa.eu/
[309] http://www.coe.int/
[310] http://www.nato.int/
[311] http://www.oecd.org/
[312] http://www.wto.org/
[313] http://www.bsec-organization.org/
[314] http://rem.jrc.ec.europa.eu/
[315] http://www.ypan.gr/
[316] http://www.desmie.gr/
[317] http://www.dei.gr

- ***Public Gas Corporation***[318]

  The Public Gas Corporation (DEPA) is the company that introduced natural gas to Greece, by implementing a large energy investment. The key mission of DEPA is:

  – To sell natural gas to large, mainly industrial consumers, with an annual consumption of over 10 mn cubic meters.

  – To sell natural gas to Gas Supply Companies (EPA), privately owned by more than 49%.

  – To distribute natural gas to regions where other gas supply companies have not yet been established.

  – To sell natural gas for transport purposes.

NUCLEAR INDUSTRY

Public authorities:

- ***Ministry of Development (Υπουργός Ανάπτυξης)***[319]

  The Minister of Development, through its General Secretariat of Research and Technology, is the supervisory authority of the Greek Atomic Energy Commission (GAEC) and of the "Demokritos" National Centre for Scientific Research. The Minister is responsible for the licensing and control of nuclear installations and jointly responsible with the competent Minister for the licensing of Laboratories for Nonmedical Applications.

- ***Ministry of Health and Social Solidarity of Greece (Υπουργός Υγείας και Κοινωνικής Αλληλεγγύης)***[320]

  The Minister for Health and Social Solidarity is responsible for the health of the general population. In particular, he or she is the licensing authority for laboratories for medical applications of ionisingadiation and approves medical practitioners for medical surveillance of radiation workers.

- ***Greek Atomic Energy Commission (Ελληνική Επιτροπή Ατομικής Ενέργειας ΕΕΑΕ)***[321]

  The Greek Atomic Energy Commission (GAEC) is the national competent authority responsible for nuclear safety and radiation protection issues. It is an independent public service whose primary mission is the protection of the public, workers and the environment from ionising and artificially produced non-ionising radiation. It is supervised by the General Secretariat for Research and Technology under the Ministry of Development.

  According to constitutional law and the General Plan of Civil Defence *Xenokratis* the Greek Atomic Energy Commission is responsible for the prevention, preparedness

[318] http://www.depa.gr
[319] http://www.ypan.gr/
[320] http://www.mohaw.gr/
[321] http://www.gaec.gr/

and response to radiological emergencies. In this context, GAEC works to protect Greece from terrorist attacks using radiological components, and takes the necessary precautions for the prompt and effective response to radiological emergencies. A radiological or nuclear emergency may be considered as either a:

– radioactive contamination from nuclear or radiological accident;

– radioactive contamination as a result of illegal or terrorist action, or

– radioactive sources out of control.

The Licensing and Inspections Department is responsible for the authorisation and inspection of entities who use radioactive materials or ionising radiation, to assure that they comply with the Radiation Protection Regulations.

The Environmental Radioactivity Monitoring Department coordinates the measurement of radiation and radioactivity levels throughout Greece and maintains the national database. The environmental radioactivity monitoring includes:

- The Telemetric Environmental Radioactivity Monitoring Network, which consists of 24 gamma air monitoring stations, 4 river water monitoring stations in Northern Greece and 3 aerosol monitoring stations.

- Laboratory measurements in:
  - Drinking water, air filters, soil samples
  - Rivers and lakes
  - Technically enhanced natural occurring radioactivity in materials and industrial waste
  - Imported food
  - Aerosols, milk, mixed diet, fall out
  - Imported materials belonging to the Green Catalogue of Waste

Initiatives:

The Radiation Protection Regulations of 2001, in addition to laying down provisions for radiation protection, also deal with the conditions governing the granting of licences for activities involving the use of ionising radiation.

There is no legislation dealing specifically with the prospecting for and mining of radioactive ores in Greece. These activities are therefore governed by the civil and mining codes.

The emergency plan in the event of widespread radioactive contamination or increased radiation levels is contained in the General National Emergency Plan. While the responsibility to react to natural disaster of all kinds lies with the Secretariat General for Civil Protection the GAEC plays a major role in implementing any response to radiological emergencies. GAEC participates in

- National Emergency Plan for Civil Protection *Xenokratis* for “responding to an emergency situation from important and extensive radioactivity contamination due to radiological or nuclear accidents taking place inside and outside Greece”.

- National Emergency Plan for Nuclear, Radiological, Biological and Chemical (NRBC)[322] threats by drafting and implementing the nuclear or radiological sections of the National Emergency Plan for Nuclear, Radiological, Biological and Chemical (NRBC) Threats, developed by the Athens 2004 Olympic Games Security Division.
- Greece is a Contracting Party to the 1986 Conventions on Assistance in the Case of a Nuclear Accident or Radiological Emergency and on Early Notification of a Nuclear Accident[323]

INFORMATION AND COMMUNICATION TECHNOLOGIES

Public authorities:

- ***Ministry of Transport and Communications (Υπουργός Μεταφορών και Επικοινωνιών)[324]***

  The mission of the Ministry of Transport and Communication is to plan and implement national policy and create the appropriate institutional framework at European and international level for the development of top quality telecom and postal services under conditions of healthy competition; to ensure the safety of telecommunications; and to promote the Information Society.

  The Ministry of Transport and Communications is responsible for planning the security policy of public electronic communications networks and services.

- ***National Committee of Telecommunications and Post (Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων - ΕΕΤΤ)***

  EETT is the National Regulatory Authority which supervises and regulates the telecommunications and postal services market. The Electronic Communications law 3431/2006[325] requires that the agency consults with the operators. Such consultation shall include discussion of measures that operators take to ensure the integrity of their networks and the availability of their services in extreme situations. Additionally, based on such consultations, EETT is proposing the issue of a Ministerial Decision, considering the measures that were developed with the help of this consultation.

- ***Hellenic Data Protection Authority (Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)[326]***

  The Hellenic Data Protection Authority (HDPA) is a constitutionally consolidated independent authority. The primary goal of the HDPA is the protection of citizens from the unlawful processing of their personal data, and providing assistance when it is established that their rights have been violated (in any sector - financial, health, insurance, education, public administration, transport, mass media, etc.)

- ***Hellenic Authority for Information and Communication Security and Privacy (Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών)[327]***

[322] http://www.gaec.gr/en/index.php?fvar=html/president/_info_emergency_response
[323] http://www.iaea.org/Publications/Documents/Conventions/cenna.html
[324] http://www.yme.gr
[325] http://www.eett.gr/nopencms/opencms/EETT/Electronic_Communications/GreekLaw/Laws/
[326] http://www.dpa.gr

The Hellenic Authority for Information and Communication Security and Privacy (ADAE) was established under Article 1 of Law 3115/2003, to protect the secrecy of mailing, the freedom of correspondence or communication, and the security of networks and information. The ADAE is an authority with administrative independency based in Athens, but can establish offices in other cities of Greece. ADAE is responsible to submit its decisions to the Minister of Justice. At the end of every year, all the activities performed and the actions taken by ADAE are submitted to the President of the Parliament, the Minister of Justice and the Greek parliament, and is subject to parliamentary examination.

WATER

Public authorities:

- ***Ministry of Development (Υπουργός Ανάπτυξης)***[328]

  The Ministry of Development is responsible for managing water resource until they are handed over the other institutions or specific uses, and for allocating water resources among various uses. It oversees water use in industry and energy, and in building major public water supply infrastructure (hydroelectric dams are built by the Public Power Corporation – PPC). Water resource management policy is formulated by the Interministerial Water Committee, led by the Ministry of Development.

- ***Ministry of Environment, Physical Planning and Public Works (Υπουργός Περιβάλλοντος, Χωροταξίας και Δημοσίων Έργων)***[329]

  The Ministry of Environment, Physical Planning and Public Works is empowered by law to ensure that after human usage, sufficient water is still available to meet the needs of ecosystems. It also evaluates point pollution loads, enforces compliance with quality standards and conducts licensing procedures.

FOOD

Public authorities:

- ***Minister of Rural Development and Food (Υπουργός Αγροτικής Ανάπτυξης και Τροφίμων)***[330]

  In 1910 a seventh ministry was established named the Ministry for Agriculture, Trade and Industry. It is now known as the Ministry of National Economy and is responsible for the organisation and administration of agricultural stations, wine-making, olive-growing, dairy and water management stations, and agricultural chemical factories. It oversees

  – agricultural education;

  – the constitution of agricultural chambers;

  – the rural police and the police for plant diseases;

[327] http://www.adae.gr/
[328] http://www.ypan.gr/
[329] http://www.minenv.gr/
[330] http://www.minagric.gr/

– the police of epizootic and the veterinary authority of the state, and

– the monitoring and maintenance of hedgerows, gardens, etc.

In its beginning, only one department was foreseen – agriculture, but with the Law 241/1916 the departments of Agriculture Economy, Forests, and Zootechnical and Veterinary Authority were added. The Department of Agriculture had two Offices - Administrative and Training. There were also three inspecting bodies (agriculture, plant service, vinicultural and phylloxeral).

The Ministry of Rural Development and Food promotes the development of agriculture, the competitiveness of the products, and the restructuring of the countryside. In particular, it is responsible for the planning and implementation of government policy in the following sectors: Management of the Markets of Agricultural Products, Agricultural Policy, Auditing of the Expenditure of the European Agricultural Fund, International Relations.

It also deals with matters related to the forests, the natural environment, the agricultural associations, fishing, animals, health, protection of plants and forests, water supplies. It studies the influence of the Common Agricultural Policy on the income of the Greek farmers.

- ***Hellenic Food Authority***[331]

  The Hellenic Food Authority, founded in 1999, is a governmental organisation supervised by the Ministry of Agricultural Development and Food. Its principal aim is to ensure that food produced, distributed or marketed in Greece meets the standards of food safety and hygiene as described by national and European legislation. The Authority also acts as the national contact point of the European Union for the management of the Rapid Alert System of Food (RASFF) and for the Codex Alimentarius as well as the focal point of the European Food Safety Authority (EFSA).

HEALTH

Public authorities:

- ***Ministry of Health and Social Solidarity of Greece (Υπουργός Υγείας και Κοινωνικής Αλληλεγγύης)***[332]

  The mission of the Ministry of Health and Social Solidarity is the implementation of social policy for health and welfare. This includes:

  – The promotion, protection, maintenance and restoration of the physical, mental and social robustness of the individual and society as a whole.

  – Providing the highest possible level of services and goods affecting the health and welfare, in accordance with the needs of each individual.

  – The protection of individual and social rights during the provision of health and welfare services.

[331] http://www.efet.gr
[332] http://www.mohaw.gr/

- The protection of the national environment, the control of goods and services that have influence on people's health, and application of measures for the promotion of the best possible quality of life
- All issues concerning the health and welfare professions, and those goods aiming to fulfil the needs of the society.
- Informing the society about the protection and promotion of health and healthy ways of living together, the avoidance and confrontation of illnesses and invalidities, and procedures for the restoration of individuals into society.

- ***National Health System of Greece (ESY)***[333]

  The National Health System of Greece was established in 1983 and guarantees free health care for all residents of Greece. The system covers the entire Greek population, without any special entitlement conditions, regardless of professional category or region. Health care services are also provided to EU and non-EU citizens on the basis of multilateral or bilateral agreements.

  In Greece primary health care services are provided through rural health centres and provincial surgeries in rural areas, the outpatient departments of regional and district hospitals, the polyclinics of the social insurance institutions and specialist in urban areas. Secondary care is provided by public hospitals, private for-profit hospitals and clinics or hospitals owned by social insurance funds.

FINANCIAL

Public authorities:

- ***Ministry of Economy and Finance (Υπουργός Οικονομίας και Οικονομικών)***[334]
  The mission of the Ministry is the shaping of the Greece's economic policy. The Ministry manages the national budget and overseeing the financial policies in the public sector. In achieving this, some tasks are:
  - It studies the influence of international developments on the Greek economy.
  - It cooperates with international organisations in the direction of international monetary developments.
  - It is involved in the shaping and implementation of development assistance policy and the assessment of relevant programs.
  - It follows economic developments in the European Union and participates in shaping the Common Economic Policy.
  - It leads Greece's participation in international economic organisations such as the OECD, the Council of Europe, the WTO, the UNEP, and CERN etc.
  - It is also responsible for topics related to the development assistance and technical cooperation offered to various countries by International Organisations and the European Union

[333] http://www.greeceindex.com/greece-health/greece_health_system.html
[334] http://www.mnec.gr/

– Managing issues around public property, national bequests, income tax, tax on capital, property tax, special taxes, collection of taxes in the airport, customs, salaries and pensions of public servants, public debt, and the participation of the country in the budget of the European Union

- ***Bank of Greece (Greek: Τράπεζα της Ελλάδος)***[335]

  Founded in 1927 in Geneva, the Bank of Greece is the national central bank. The Bank of Greece is a member of the European System of Central Banks (ESCB)[336] and has a staff of over 3000 employees. The primary objective of the Bank is to ensure price stability in Greece. It also supervises the private banks and acts as a treasurer and fiscal agent for the Greek government.

TRANSPORT

Public authorities:

- ***Ministry of Transport and Communications (Υπουργός Μεταφορών και Επικοινωνιών)***[337]

  The mission of the Ministry of Transport and Communication is to plan and implement national transportation policy. Whilst doing so, it seeks to create an appropriate institutional framework at European and international levels for the development of top quality transport, and mass-transit. It is also responsible for ensuring the safety of transport systems.

- ***Ministry of Environment, Physical Planning and Public Works (Υπουργός Περιβάλλοντος, Χωροταξίας και Δημοσίων Έργων)***[338]

  The Ministry of Environment, Physical Planning and Public Works is responsible for the physical planning and the integration of relevant infrastructure at both national and regional levels. Such infrastructure includes harbours, roads, airports, sewage plants, dams, and flood controls etc.

- ***Hellenic Civil Aviation Authority***[339]

  The Hellenic Civil Aviation Authority (HCAA) is responsible for the development and maintenance of the Security National Program of Civil Aviation (SNPCA). It oversees the implementation of aviation security requirements by airlines. It define standards and procedures for aviation security. These responsibilities are primarily undertaken by the Authority's Airports Security Division. It also represents Greece in international meetings on air transportation security, and it collaborates with international aviation security organisations.

- ***Athens International Airport (AIA) S.A.***[340]

  Athens International Airport S.A. was established in June 1996 as a partnership between the Greek State and a private consortium led by the German company Hochtief Aktiengesellschaft. This consortium was the winner of an airport construction

335 http://www.bankofgreece.gr
336 http://www.ecb.europa.eu/
337 http://www.yme.gr
338 http://www.minenv.gr/
339 http://www.hcaa.gr/home/index.asp
340 http://www.aia.gr

tender held during 1991. The partnership managed the Eleftherios Venizelos airport for 30 years.

The main objective of Attikes Diadromes is to ensure the continuous, uninterrupted and smooth operation of the motorway (24 hours a day, 365 days a year), along with the provision of top quality services to the users.

Initiatives:

Greece is in the process of completing a programme of infrastructure projects with EU support. This program is upgrading much of the nation's transport and communication.

The Greek railway network is relatively simple, consisting of two major lines: the standard gauge line from Piraeus and Athens to northern Greece and line from Athens to Peloponnese. Almost all other lines are branch lines linking directly to these two lines. The main line of the Greek Railway System is divided into two sections: Athens to Thessaloniki, a distance of 520 kilometres and Thessaloniki to Ormenio (border with Turkey) via Alexandroupoli. According to 2007 Network Statement, the total length of the standard gauge lines was approximately 1665 km and the length of the metre gauge lines about 725 km. In addition, about 150 km of new standard gauge lines were under construction for access to Athens Airport and this became fully operational in July 2007.

The Greek motorways network comprises two main highways, Egnatia Highway (680 km), stretches east-west, linking the northwest port of Igoumenitsa to Alexandroupolis at the Turkish border via Thessaloniki, with nine vertical connections to the Balkan countries and links to five ports and eight airports and Pathe Motorway (750 km) includes the Athens ring road and stretches the north south axis from the port of Patras to the border with former Yugoslavia. The Attiki Odos is a modern motorway, extending along 65 km. It forms a ring around the greater metropolitan area of Athens and is the backbone of the road network of the entire Attica region. It is an urban-periurban motorway, with 3 traffic lanes in either direction and an emergency lane. In the centre, it has a special traffic island, reserved for the operation of the suburban railway. It constitutes a unique infrastructure project, even in European terms, since it is essentially a closed toll motorway within a metropolitan capital, where the problem of traffic congestion is really acute. The Attiki Odos forms the link which connects the PATHE road axis (Patra - Athens - Thessaloniki - Evzoni), since it links the Athens - Lamia National Road with the Athens - Corinth National Road, by-passing the centre of Athens. Being a closed motorway, it has full control of its access points and consists of two sections.

Greece has 39 international standard airports, many of which have been upgraded or rebuilt during the last few years. The next five year plan includes expansion and renovation of 21 more airports at a total cost of more than 400 mn Euro. In March 2001, the Athens International Airport was opened, following one of the biggest infrastructure projects in Greece. The airport is owned by the Greek Republic and a private consortium under the leadership of Hochtief. It has been constructed on a BOOT (Build-Own-Operate-Transfer) for a concession period of 30 years.

The 80 km of waterways system consists of three coastal canals including the Corinth Canal (6 km) and three unconnected rivers. The Corinth Canal crosses the Isthmus of Corinth connecting the Gulf of Corinth with the Saronic Gulf and shortens the sea voyage from the Adriatic to Peiraiefs (Piraeus) by 325 km.

Greece has 123 cargo or passenger ports which handle passenger ships, cruise ships and cargo. With the financing of the EU, 50 ports will be upgraded at a total expenditure of 300 mn Euro. Most of the Greek islands and many main cities of Greece are connected by air, mainly by two major airlines.

CHEMICAL INDUSTRY

Initiatives:

National Emergency Plan for Nuclear, Radiological, Biological and Chemical (NRBC)[341]

Under the National Emergency Plan for Civil Protection *Xenokratis*, the Greek Atomic Energy Commission activates Appendix P that concerns the "response to an emergency situation from important and extensive radioactivity contamination due to radiological or nuclear accidents taking place inside and outside Greece". According to the plan, the evaluation of the situation, the activation of Appendix "P" and the proposal of actions to be taken are GAEC's responsibilities. GAEC was deeply involved in drafting and implementing the nuclear or radiological part of the National Emergency Plan for Nuclear, Radiological, Biological and Chemical (NRBC) Threats, developed by the Athens 2004 Olympic Games Security Division.

RESEARCH FACILITIES

Public authorities:

- ***General Secretariat for Research and Technology (GSRT)***[342]

  The General Secretariat for Research and Technology is part of the Ministry of Development and undertakes the following:

  – Supports through its programmes, the research activities of both the country's scientific research institutes and those of industry, focussing on areas that are important for the national economy and for the improvement of the quality of life.

  – Promotes the transfer and dissemination of advanced technologies throughout the country's productive sector, ensuring early utilisation of the results of research activity.

  – Contributes to the enhancement of the country's research capabilities.

  – Represents Greece in relevant institutions of the European Union, bringing the country's research and technology activities into line with the international community.

  – Promotes cooperation with other countries and international organisations on research and technology issues.

  – Establishes new institutes and technological centres in support of the development of the Greek economy.

  – Supervises, underwrites the fixed costs of, and otherwise provides support for 21 of the country's best-known research and technological centres.

[341] http://www.gaec.gr/en/index.php?fvar=html/president/_info_emergency_response
[342] http://www.gsrt.gr/

– Aquaculture Centre of Acheloos (ACEA) encourages activities aimed at raising public awareness of research and technology issues.

14 Hungary

Figure 66: Hungary

14.1 Summary

	Organisational Model	Strategy and Policy	Methodology &, Standards	Public-Private Partnership & International Collaboration	Funding & Human Resources	Training & Exercises	Sector-Specific Key Players & Initiatives
Hungary	▪ There is no specific Agency dedicated to CIP	▪ National Program for Protection of Critical Infrastructures established by the Government in 2008	▪ National Program for Protection of Critical Infrastructures	▪ PPP Inter-Ministerial Committee ▪ NIIFI and HUNGARNET	▪ Not Applicable	▪ Not Applicable	▪ Not Applicable

343

Hungary has begun to confront CIP challenges through legislative means. It does not have an existing CIP Agency in place, but the country is responding rapidly to conform itself to European best practices in the field.

In 2008 a Hungarian Government resolution (Resolution 2080/2008 (VI.30) established the National Program for Protection of Critical Infrastructures (*Kritikus Infrastruktúra Védelem Nemzeti Programjáról – NKIV*)[344]. The legislation was approved in order to start CIP related activities, including the a proposal to incorporate critical infrastructure protection activities previously falling under different sectoral scopes into a single framework. It also considered inter-sectoral coordination reflecting the approach by the Critical Programme for Infrastructure Protection European.

[343] Not Applicable = Open Source Research, Web-bases Survey and Individual Interviews have not shown information/data on the given argument

[344] http://www.khem.gov.hu/data/cms1940264/2080_2008_KH_NCIP_angol.doc

14.2 Organisational Model

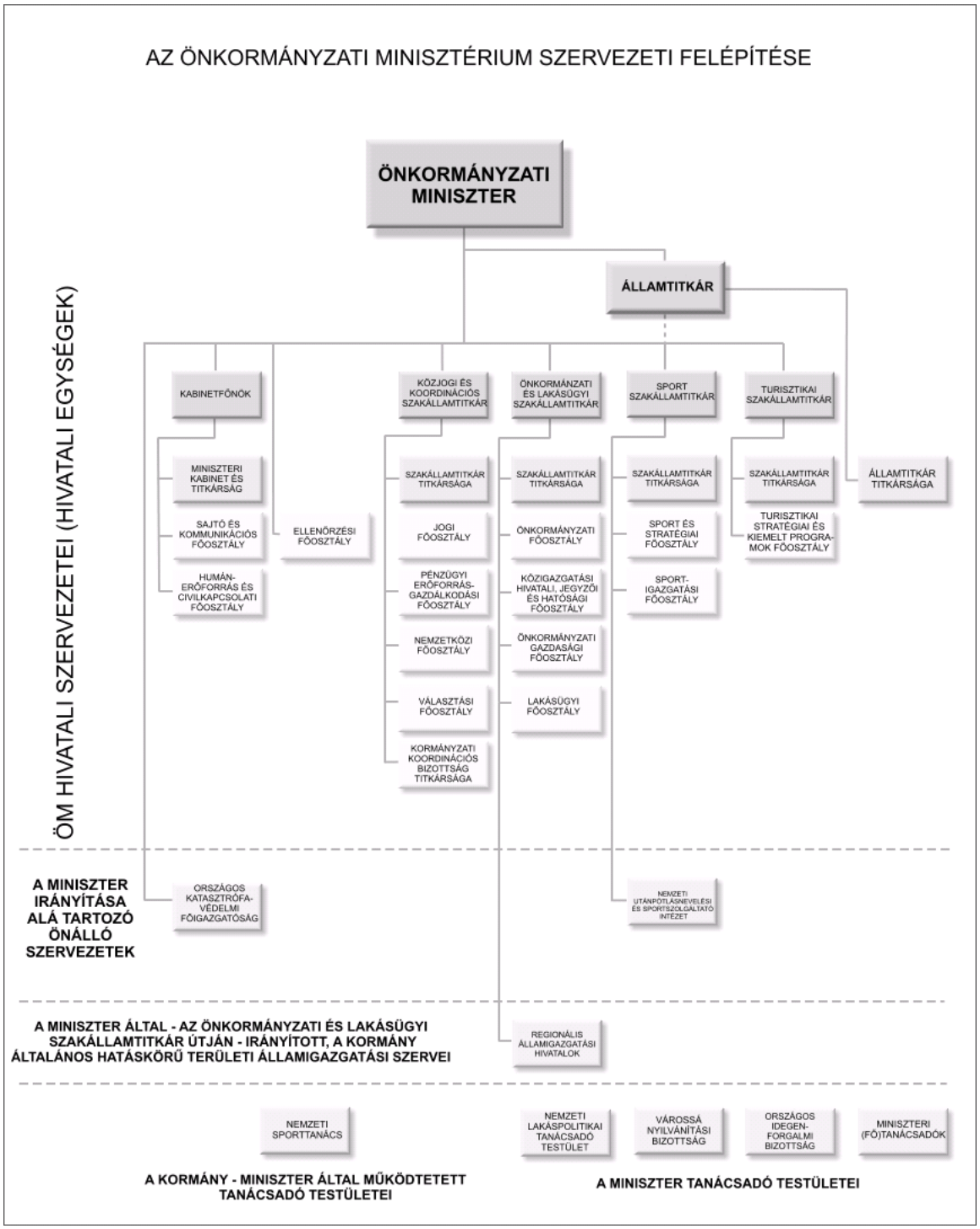


Figure 67: Organisational Chart (only CIP-related agencies shown)

Hungary does not possess a centralised organisational model for the management of CIP related issues, but acknowledges that “efficiency and coherence calls for designation of a

single coordinating agency in the legislation. The responsibilities of the coordinating agency may be fulfilled by the head of a central state administration agency designated by the Parliament or the Government (possibly the Prime Minister's Office, a ministry, a government office or government committee) or a designated government commissioner. The coordinating agency is responsible for strengthening the forms of cooperation, management and coordination facilitating NCIP implementation"[345].

Nemzetbiztonsági Kabinet (National Security Cabinet)

The National Security Cabinet coordinates policies relating to national security and prepares decisions for the protection of the state and public safety. The Cabinet is headed by the Minister of Defence, and its members are the Minister of the Interior, the Minister of Justice, the Minister of Foreign Affairs, the Minister in Charge of the Prime Minister's Office. Permanent invitees are the political state secretary of the Prime Minister's Office responsible for national security issues and the political state secretary of the Ministry of Finance. The Prime Minister's Office provides secretarial and administrative functions.

Közlekedési, Hírközlési és Energiaügyi Minisztérium (Ministry of Transport, Telecommunications and Energy - MTTE)[346]

The MTTE was created recently by the separation of the Ministry of Economy and Transport into the Ministry of Transport, Telecommunications and Energy, and Ministry of National Development and Economy[347].

The MITTE is in charge of the air, rail, road and river transport. One of the fundamental roles of the Ministry is being part of the Interministerial Public-Private Partnership Committee[348].

Many of the activities of MITTE which concern energy are conducted through the Hungarian Energy Office[349].

Honvédelmi Minisztérium – MH – (Ministry of Defence)[350]

This Ministry is responsible for national security, including the security of information. In particular, it is responsible for protecting state secrets and public data.

The main task of the Hungarian Defence Forces (a voluntary, professional army consisting of professional and contracted soldiers), is to defend the sovereignty and territorial integrity of the Republic of Hungary and to contribute to the collective defence of NATO under the North Atlantic Treaty. The Hungarian Defence Forces, in line with obligations undertaken by the Republic of Hungary, is ready to put the necessary military forces at the disposal of NATO to the extent allowed by its capacities. The HDF participates in peace support and humanitarian actions under the auspices of the UNO and other international organisations, and contributes in the recovery of serious industrial and natural disasters. In accordance with the principles of the nation's security policy, the Hungarian Defence Forces seeks to strengthen regional security and stability via bilateral and multilateral military cooperation.

Környezetvédelmi és Vízügyi Minisztérium (KVVM) (Ministry of Environmental Protection and Water Management)[351]

[345] http://www.khem.gov.hu/data/cms1940264/2080_2008_KH_NCIP_angol.doc
[346] http://www.khem.gov.hu/en
[347] For this reason, the Hungarian web-site and, particularly, English web-site are still under construction and largely incomplete.
[348] http://www.khem.gov.hu/en/en_archiv/infrastructure/logistics
[349] http://www.khem.gov.hu/en/en_archiv/liberalisation/energy/liberalisation_energy.html
[350] www.hm.hu.

The Ministry is a central governing body for environmental protection and water affairs. and undertakes expert management and regulatory tasks in the areas of environmental protection, water management and meteorology. The Ministry's responsibilities include policy development, tasks connected to governmental work and international collaboration. The Ministry's field institutions – environmental and water authorities and national park managers – attend to first degree tasks. Environmental protection second degree tasks are undertaken by the National Environment and Water Authority.

Magyar Köztársaság Külügyminisztérium – MKK – (Ministry of Foreign Affairs)[352]

Resolution No. 94/1998 (XII. 29.) of the Hungarian National Assembly on "The Basic Principles of the Security and Defence Policy of the Republic of Hungary" sets out the fundaments of the country's long term security and defence policy.

After the radical political change in Hungary, national security is intertwined with international bodies like NATO and the EU. For this reason, the MKK is essential to Hungary's security, by managing international relationships, as expected by The National Security Strategy of the Republic of Hungary.[353] Under the National Security Strategy, sector strategies for military, national security, law enforcement, economics and finance, human resource development, information systems and protection, disaster-relief, environmental security and the fight against terrorism are being developed in a co-ordinated manner.

Globalisation accelerated and brought radical changes in all areas of international relations. Especially in the fields information technologies, transport, trade and finances, as well as in public health, globalisation has reached a degree where – along with its advantages – new types of security risks have appeared. Cross-border threats are having a great impact on the international environment and the security of the Republic of Hungary: Some of these threats include:

- terrorism;
- proliferation of weapons of mass destruction;
- unstable regions, failed states;
- illegal migration;
- economic instability;
- challenges of the information society, and
- global natural, man-made and medical sources of danger.

Today, in addition to military operations, law enforcement, medical, and humanitarian activities play an increasing role in the crisis management operations undertaken by the international community. National security services help defend the country's sovereignty and constitutional order and assert its national security interests.

[351] www.kvvm.hu.
[352] http://www.kulugyminiszterium.hu/kum/en/bal/
[353] http://www.kulugyminiszterium.hu/NR/rdonlyres/61FB6933-AE67-47F8-BDD3-ECB1D9ADA7A1/0/national_security_strategy.pdf

Igazságügyi és Rendészeti Minisztérium (IRM)
(Ministry of Justice and Law Enforcement)[354]

The duties and responsibilities of this ministry include crime prevention and data protection. It controls the Public Administration and Central Electronic Public Services Office, which is the central body for all tasks relating to the provision of e-government services and the management of electronic records and documents.

Önkormányzatok Minisztérium (OM)
(Ministry of Local Government)[355]

The Ministry of Local Government is the ministry of reference for the organisation and conduct of civil protection, sport, tourism, electoral and referendum legislation, conducting elections and referendums, public administration, organisation, and responsible development[356].

Országos Katasztrófavédelmi Főigazgatóság (OKF)
(National Directorate General for Disaster Management)[357]

In the Republic of Hungary, the disaster management organisation provides assistance in case of fires, accidents, emergencies and other events threatening citizens and their property. The modern Hungarian disaster management organisation was established from the fire service and the organisations of civil protection. The merger was the result of a process intended to produce greater efficiency, and in which international experience also contributed.

Today there are about 25,000 voluntary and professional fire fighters. The Organisation of Civil Protection was established in 1935 for the purposes of air defence to reduce the risk of air raids on the civil population.

The organisation of the Disaster Management Organisation was formed on 1 January 2000. It operates at three levels - national, regional and local. The organisation is now working on the adaptation to the five-level European public administration system. It performs its tasks in close cooperation with other state organisations, services and local governments. The strategy was developed in 2003 with a careful analysis considering potential risk factors and hazardous effects. In Hungary, one needs to keep in mind several permanent risk factors, such as floods, inland waters, effects of extraordinary weather conditions, possible man-made hazards, chemicals and nuclear risks. Increasing risk factors include the transportation of hazardous materials by road, rail and air. In addition Hungary has to consider new threats such as terrorism, proliferation of weapons of mass destruction, illegal migration, and the break-down of critical infrastructure[358].

14.3 Strategy & Policy

Currently, the Republic of Hungary is preparing a Green Book on CIP. The Green Book guides the implementation of a national programme for the Protection of National Critical

[354] www.irm.gov.hu/?lang=en.
[355] www.bm.gov.hu. (Hungarian)
[356] http://www.bm.hu/web/portal.nsf/html/feladatkor.html
[357] http://www.katasztrofavedelem.hu/ (Hungarian)
[358] http://www.katasztrofavedelem.hu/tartalom.php?id=345. (English)

Infrastructure (NCIP) and the drafting of legislation which will direct government aims, considerations, and principles for NCIP.

Effective protection of critical infrastructure requires communication and cooperation among all stakeholders– owners and operators of infrastructures, authorities, specialist agencies and alliances. Therefore, another objective of the Green Book is to allow for the government to receive feedback on the potential approaches of the NCIP. This will form the basis for consultation with the private sector through the engagement of a large number of participants.

Nemzeti Információs Infrastruktúra Fejlesztési (NIIF) Program (The National Information Infrastructure Development Program)[359]

The National Information Infrastructure Development (NIIF) Program serves as a framework for the development and operation of the research network in Hungary. The Program covers the entire Hungarian academic, research and public collection community by providing them with

- an integrated computer networking infrastructure;
- a wide range of communication, information, and co-operation services;
- leading-edge environment for networking applications, and
- advanced framework for content generation and provision.

The Program is based on funding by the central state budget. The development and operation of the network and the services are executed by the NIIF Institute (NIIFI), under the supervision of the Program Committee, and with the contribution of the Technical Committee.

Nemzeti Környezetvédelmi Program

NEP relies on the most important Hungarian and international environmental policy principles, which can be classified into three main categories:

- Traditional environmental protection principles – the principles of precaution, prevention, reconstruction, liability, co-operation, information, publicity and the 'polluter pays'.
- Additional principles based on the environmental activities of developed countries - shared responsibility, transparency in planning, decision-making, financing, implementation and control, predictability in regulation and financing, accountability, clear objectives, measurable performance, partnership, subsidiarity, additionality, measures with multiple benefits.
- Taking into account the principles of sustainable development, NEP promotes the establishment of the social, economic and environmental conditions required for sustainable development. During the implementation of NEP, apart from environmental interests, non-quantifiable ethical considerations must also be taken into account. Environmental protection focusing on ethical considerations recognises the need to preserve values which supersede any economic interests.

[359] www.niif.hu/en

14.4 Methodologies & Standards

Government Resolution 2080/2008 (VI. 30.) on the National Programme for Critical Infrastructure Protection[360]

This document is essential for the adaptation of the Hungarian political infrastructure to the rules and the opportunities offered by Hungary to the European Union.

A new document about transport infrastructure development has just been published by the Ministry of Economy and Transport. The brochure contains up-to-date information about development programmes in the field of rail, road, air, inland waterway and logistics infrastructure [361].

14.5 Public – Private Partnership & International Collaboration

Public-Private Partnership (PPP) Inter-Ministerial Committee[362]

To facilitate the introduction of the PPP structure into Hungary, the Hungarian government established the PPP Inter-Ministerial Committee with its May 2003 Decree 2098/2003. At that time, the Committee's members were representatives of the Ministry of Economy and Transport, the Ministry of Finance, the Ministry of Justice, the Prime Minister's Office and the Central Statistics Office. In February 2007, Decree 2028/2007 enlarged the Committee with the inclusion of the National Development Agency, and changed the Committee's responsibilities. These changes were intended to foster better harmonisation of the governmental strategy and the use of the funds provided by the European Union. The Chairman of the Committee is the 'State Secretary with special responsibilities' of the Ministry of Economy and Transport.[363]

NIIFI (the Hungarian National Information Infrastructure Development Institute) and HUNGARNET (The HUNgarian Academic and Research NETworking Association)[364]
NIIFI and HUNGARNET maintain relationships (organisational, technical, and networking) with international organisations whose network development aims and goals are similar to those of the Hungarian research, education and public collection communities.

Puskás Tivadar Közalapítvány (The Theodore Puskas Foundation)[365]

The Theodore Puskas Foundation is a non-profit organisation whose operational arm, the Institute of International Technology, aims to disseminate advanced foreign technologies in Hungary and introduce state-of-the-art Hungarian technologies to the international market.

This work has been complemented by dedicated services which improve the competitiveness of Hungarian enterprises through consulting, technology assessment and technology audit, and the efficient use of information technologies.

In 2004, the Ministry of Informatics and Communication contracted the Foundation to operate the national Computer Emergency Response Team (CERTHungary), in consideration of its good reputation and its research experience in the field of information technology.

[360] http://www.khem.gov.hu/data/cms1940264/2080_2008_KH_NCIP_angol.doc
[361] http://www.khem.gov.hu/data/cms1057566/060810_gkm_transport_web.pdf
[362] www.khem.gov.hu
[363] http://www.khem.gov.hu/data/cms1553976/PPP_GU.pdf
[364] http://www.niif.hu/en/niif_institute/international_relations
[365] http://www.neti.hu/pta/en

14.6 Sector – Specific Key Players & Initiatives

ENERGY

Public Authorities:

- ***Magyar Energia Hivatal (The Hungarian Energy Office)***[366]

  The Hungarian Energy Office was established in 1994. The Office is a national, public administration body with independent powers and competence, acting under the control and supervision of the Minister of Economy and Transport.
  The Office plays a decisive role in operating the regulated and competitive markets, issuing operational licences for market players, regulating companies which act as natural persons or legal monopolies, the preparation decisions on prices, and supervising the market.

- ***MAVIR Magyar Villamosenergia-ipari Átviteli Rendszerirányító Zártkörűen Működő Részvénytársaság [MAVIR Hungarian Transmission System Operator Company Ltd., MAVIR ZRt.).***[367]

  MAVIR ZRt. is responsible for the operational safety and regulation of the electricity system, including the cross-border lines and network capacities. Its owner is the Hungarian state and this control is exercised by the Ministry of Economics and Transport. Today MAVIR ZRt.'s duties include:

  – To provide for the reliable, efficient and secure operation of the Hungarian power system including the required reserve capacities of generation and transmission.
  – To supervise and augment the transmission system, to perform any renewal, maintenance and development works required for a proper and reliable supply.
  – To ensure the undisturbed operation of the electricity market and access on equal terms for system users.
  – To harmonise the operation of the Hungarian power system with neighbouring systems.
  – To coordinate international co-operation.
  – To prepare the Network Development Strategy and to put forward proposals for the development of the generation pool.

NUCLEAR

Public Authorities:

- ***Országos Atomenergia Hivatal – HAEA – (Hungarian Atomic Energy Authority).***[368]

[366] http://www.eh.gov.hu/home/html/index.asp?msid=1&sid=0&lng=2&hkl=109
[367] www.mavir.hu/
[368] http://www.haea.gov.hu/web/v2/portal.nsf/index_en

The main tasks of the Hungarian Atomic Energy Authority include:

- Establishing the regulation for the safety of peaceful applications of nuclear energy, particularly for the safety of nuclear materials and facilities under both normal and irregular conditions and with nuclear emergencies. In addition, the HAEA harmonises and manages related public information activities.

- In accordance with the Atomic Energy Act, the work of the HAEA is supported by a Scientific Council. This helps ensure the scientific basis for governmental, regulatory, and emergency response measures applied to nuclear applications. This Council consists of 12 members who are nationally known professionals in the field of nuclear energy. The chairman and the members of this council are appointed by the supervising minister of the HAEA. Within its terms of reference and taking into consideration the latest scientific results, the Scientific Council is required to provide advice on the most important issues of nuclear safety, radiation protection and emergency response.[369]

- ***Magyar Tudományos Akadémia KFKI Atomenergia Kutatóintézet (AEKI) (Hungarian Academy of Sciences KFKI Atomic Energy Research Institute)***[370]
  AEKI is a research institute of the ***Hungarian Academy of Sciences*** mainly active in the field of basic and applied nuclear energy research. The activities of the institute started in the 1950s, where at that time, AEKI was part of the Central Research Institute for Physics (KFKI). AEKI became independent in 1992. AEKI has almost 200 employees of which approximately 100 are scientists. The institute operates the 10 MW ***Budapest Research Reactors***, providing the scientific community of Europe (see ***Budapest Neutron Centre*** for details) with research opportunities in neutron physics and its applications, and Hungary with radioactive isotopes, mainly for medical applications. The research reactor has been improved by the addition of a liquid hydrogen type cold neutron source, commissioned in 2000[371].

INFORMATION AND COMMUNICATION TECHNOLOGIES

Public Authorities:

- ***Nemzeti Hírközlési Hatóság (The National Communications Authority – NCA)***[372]

  Based on the Electronic Communications Act of 2003, the National Communi-cations Authority was established in 2004 as an independent regulatory body for communications. The NCA's main task is to support the development of the communications market and to ensure that every citizen has access to affordable and reliable communications services. The NCA constantly analyses the market and exchanges information with national and international experts, and adapts its capabilities, methods, and operations accordingly. The NCA is also responsible for the National Alert Service (NAS) in the postal and communication sectors, the operation of which has been outsourced to the CERT-Hungary Centre of the Theodore Puskás Foundation. The NAS relies upon the co-operation of designated

[369] http://www.haea.gov.hu/web/v2/portal.nsf/main_tasks_en
[370] http://www.kfki.hu/~aekihp/
[371] http://www.kfki.hu/~aekihp/institute.htm
[372] http://www.nhh.hu/index.php?id=hirek&mid=614&lang=en

service providers who report incidents affecting their services. The main task of NAS is to gather and distribute these reports and to co-ordinate between service providers in case of an emergency. Most frequently, these have historically been the spring floods in North-Eastern Hungary[373].

- ***Computer Emergency Response Teams – CERTs*:**
  - ***CERT-Hungary:*[374]**
    CERT-Hungary is the governmental and national CERT. It is operated by the Theodore Puskás Foundation and was established in 2005. As the Hungarian governmental CERT, it aims to improve information security for public agencies and is responsible for the technical aspects of CIIP. In order to combat high-tech crime, CERT-Hungary has developed direct communication channels to the national police force, and collaborates closely with all other agencies involved in CIIP. CERT-Hungary is an accredited member of all main CERT forums, and acts as the national contact point for incident-handling and CIIP-related issues. Furthermore, CERT-Hungary offers some free services for the public, in particular warnings about emerging threats and new vulnerabilities, and provides chargeable services for private companies, e.g., intrusion detection, security audits, or malware analysis. Finally, CERT-Hungary coordinates a SCADA working group, which is organised jointly by government agencies and the operators of SCADA networks.[375]
  - Computer Security Incidents Response Team of the National Information Infrastructure Development Program – NIIF-CSIRT[376]:
    The NIIF-CSIRT helps members of the academic networks (NIIF and HUNGARNET) to manage security incidents. The NIIF-CSIRT also disseminates important security-related information and warnings to its members.

WATER

Public Authorities:

- ***Környezetvédelmi és Vízügyi Minisztérium (KVVM)***
  (Ministry of Environmental Protection and Water Management)

  The Ministry manages the entire water cycle for the domestic, industrial and agricultural sectors through specific departments (Water and Environmental Risk Control Department, River Basin Management and Water Protection Department, Water Management Department), and is led by the State Secretary for Water Affairs.[377]

HEALTH

Public Authorities:

[373] E.M. Brunner and M. Suter, INTERNATIONAL CIIP HANDBOOK 2008-2009, Centre for Security Studies, ETH Zurich.
[374] www.cert-hungary.hu
[375] E.M. Brunner and M. Suter, INTERNATIONAL CIIP HANDBOOK 2008-2009, Centre for Security Studies, ETH Zurich.
[376] http://www.niif.hu/en/csirt.
[377] http://www.kvvm.hu/index.php?pid=3&sid=22

- ***Egészségügyi Minisztérium (Ministry of Health)***[378]

  From June 2006 the Ministry of Health is responsible for health issues. In Hungary, the first phase of the National Environmental Protection Programme (NEPP), reflecting the environmental policy, has already been accomplished. The legislation for the environmental protection law have been completed, and the establishment of an institutional system that is aligned to EU requirements has also started. Objectives were implemented most successfully in the area of nature conservation and protection of clean air, while protection of waters and human health, as well as increase of environmental safety are slightly less advanced. The second phase (NEPP-II) between 2003 and 2008 relies on the 6th Environmental Action Programme of the European Union, to be implemented until 2010. The health related tasks of NEPP-II are contained in the Environmental Health and Food Safety Action Programme.[379] Areas most affected are:
  - food safety;
  - air quality;
  - water quality, and
  - the urban environment[380]

- ***Országos Mentőszolgálat (Hungarian National Ambulance and Emergency Service)***[381]
  In Hungary, the lack of specialist emergency medicine departments in hospitals has resulted in the evolution of a highly skilled and well equipped ambulance service, which seeks to provide emergency medical care at the site of an incident. The Hungarian National Ambulance and Emergency Service (HNAES) was established in 1948 and is responsible for rescue and medical transportation all over the country. The ground rescue capability is complemented by air ambulance facilities. At the moment 203 ambulance stations have been established. 19 regional dispatch centres as well as the central dispatch centre in Budapest receive calls for assistance through the unified call number 104. Ambulances are in constant contact with the dispatch centres by a radio communication system. There are three levels of ambulance, the basic unit, the emergency unit and the mobile intensive care unit.

FINANCIAL

Public Authorities:

- ***Pénzügyminisztérium (Ministry of Finance)***[382]

  The Ministry of Finance has established the “Department of System Development of Financial Control “ to manage the risks related to financial management.[383]

- ***Gazdasági Kabinet (The Economic Cabinet)***

[378] www.eum.hu
[379] http://www.eum.hu/about-us/health-situation-in/environment-and-health
[380] http://www.rec.org/magyariroda/Documents/NKP_En.pdf
[381] http://www.mentok.hu/page.php?newmenuid=6
[382] www1.pm.gov.hu
[383] http://www1.pm.gov.hu/web/home.nsf/(menudocs)/0DE6D9C8F6233213C1256EBC/

The economic cabinet comments on conceptual issues relating to the economy, prepares economic policy decisions, and provides advice on policy issues relating to the reform of public finances. The cabinet discusses those proposals to be submitted to the Government that bear on the economy or contain budgetary commitments. The economic cabinet is headed by the Minister of Finance, and its members are the Minister without portfolio responsible for European affairs, the Minister of Employment and Labour, the Minister of Agriculture and Rural Development, the Minister of Economy and Transport, the Minister for Youth, Family, Social Affairs and Equal Opportunities, the Minister of Informatics and Communications, the Minister of Environment and Water, the Minister without portfolio responsible for regional development and convergence and the Minister in charge of the Prime Minister's Office. The Governor of the National Bank of Hungary, the chef de cabinet of the Prime Minister and the president of the Central Statistical Office are permanent invitees. The Ministry of Finance provides secretarial and administrative functions.[384]

- ***Magyar Nemzeti Bank – MNB – (Hungarian National Bank)***[385]

  The primary objective of the MNB is to maintain price stability. Without prejudice to its primary objective, the MNB also supports the economic policy of the Government using the monetary policy instruments at its disposal. In addition to performing the duties of a Central Bank, the MNB controls the monetary policy with a specific office - the Monetary Council - providing entry of Hungary in the Euro Zone[386].

RESEARCH FACILITIES

Public Authorities:

- ***Szeged Biztonságpolitikai Központ – (Szeged Centre for Security Policy)***[387]

  The Szeged Centre for Security Policy is a joint project of the Municipal Government of the City of Szeged, the Hungarian Academy of Sciences and the University of Szeged. The Centre provides a working channel of communication between international organisations (UN, OSCE, EU, WEU, NATO, WB, EBRD etc) and political, business and scientific organisations in the region.

[384] http://misc.meh.hu/letoltheto/Kiadvany-angol-0507.pdf
[385] http://english.mnb.hu/Engine.aspx
[386] http://english.mnb.hu/engine.aspx?page=mnben_monetaristanacs
[387] http://www.scsp.hu/

15 Ireland

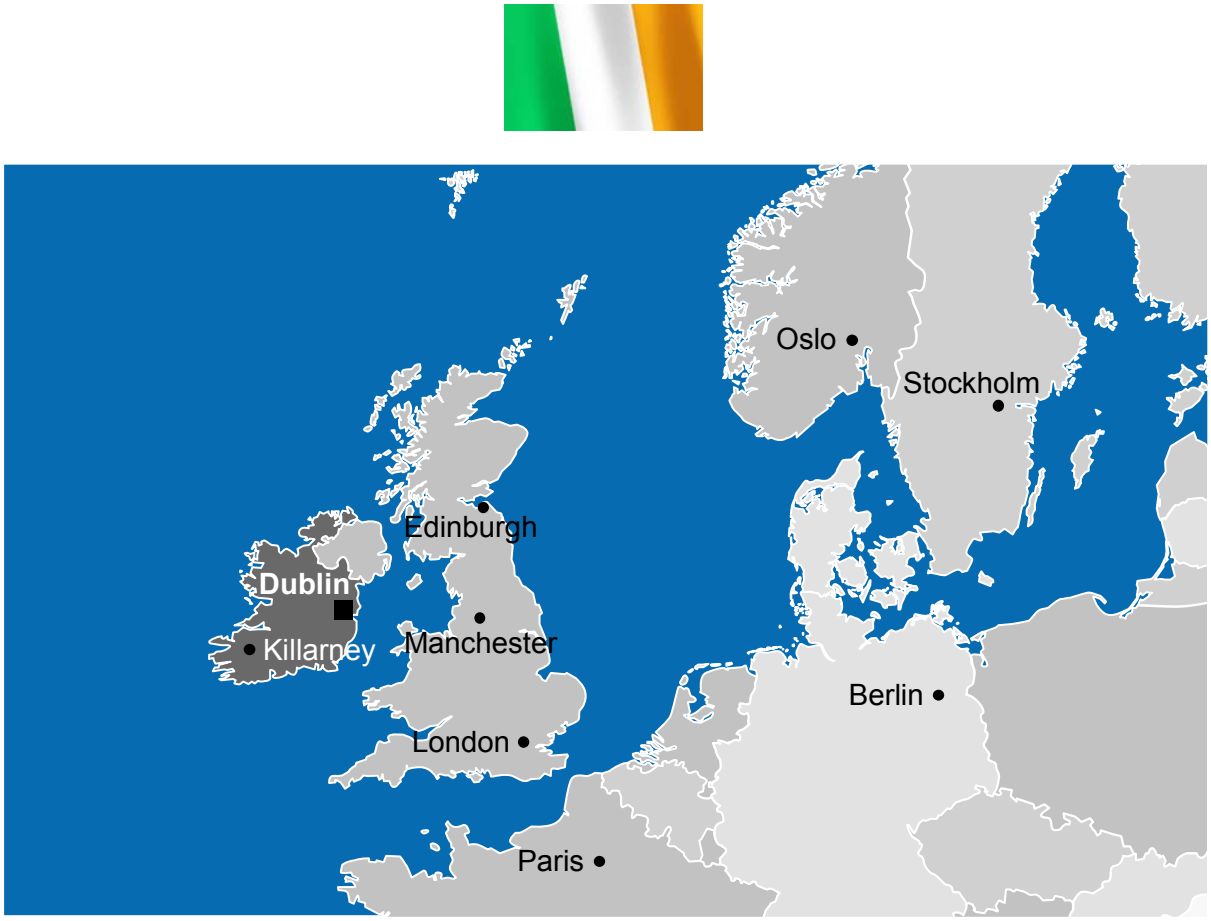


Figure 68: Ireland

15.1 Summary

	Organisational Model	Strategy & Policy	Methodology & Standards	Public-Private Partnership & International Collaboration	Norway Funding & Human Resources	Training & Exercises	Sector-Specific Key Players & Initiatives
Ireland	▪ There is no specific Agency dedicated to CIP ▪ Most appropriate department or agency is appointed on a case-by-case basis	▪ CIP is cited as a key point in the "Framework for Major Emergency Management"	▪ Not Applicable	▪ Rapid Alert System BICHAT (Biological, Chemical Attack) ▪ International Atomic Energy Agency	▪ Not Applicable	▪ Major Incident Medical Management Support (MIMMS)	▪ National Emergency Plan for Nuclear Accidents (NEPNA)

388

Ireland has adopted a decentralised approach to CIP. Responsibilities are distributed across several levels, and different government departments and agencies are responsible for specific emergency planning functions. In the event of a major emergency, the most appropriate department or agency is designated as the lead agency to co-ordinate the response to it. Government departments take the lead role in planning for emergencies in those areas in which they have statutory responsibility. Other government departments and state agencies assist the lead department as required. Emergency plans are co-ordinated at agency, local and national levels.

At a high-level, guidelines for emergency management are provided in the *Framework for Major Emergency Management*[389], where CIP is cited as a key contributor to mitigating the effect of a disaster

[388] Not Applicable = Open Source Research, Web-bases Survey and Individual Interviews have not shown information/data on the given argument

[389] http://www.emergencyplanning.ie/

15.2 Organisational Model

Emergency management is undertaken as an integral function of the Principal Response Agencies (PRA)[390]- the Ireland National Police Service (*Garda Síochána*[391]), Health Service Executive[392] and local authorities[393]. Each PRA has an individual major emergency plan, which sets out its arrangements to respond to major emergencies. These agencies' plans are in turn consistent with the arrangements set out in the *Framework for Major Emergency Management*[394]. This framework is often referred to colloquially – and somewhat misleadingly - as the 'national emergency plan'. It is in fact, not an emergency plan itself but rather the agreed protocols between the PRAs and their respective emergency plans. The Framework, primarily stated in 1984, was reviewed in-depth by the Department of the Environment, Heritage and Local Government[395] with the co-operation of, inter alia, the Department of Justice, Equality and Law Reform[396] and *An Garda Síochána* in 2006, in view of the changing nature of the PRAs generally and the increased potential for mass casualty emergencies arising from industrial, transport or terrorist incidents.

Its primary purpose is to set out arrangements for the PRAs to work together to manage large-scale events. It also facilitates other services, such as the Defence Forces and the voluntary emergency services, to work with and support the PRAs in a co-ordinated response to managing major emergencies. In particular, the Framework identifies the structured arrangements and facilities necessary to achieve effective co-ordination in a manner that is organisationally and functionally appropriate.

The Framework uses a comprehensive, five-stage systems view of emergency management, involving a continuous cycle of activity, as follows:

- hazard analysis/risk assessment;
- mitigation/risk management;
- planning and preparedness;
- co-ordinated response, and
- recovery.

The *Framework* also addresses the inter-relationship of the work of the PRAs with that of other levels of Government; in particular, it specifies requirements for clear linkages to relevant government departments.

The implementation of the new *Framework*, again led by the Department of the Environment, Heritage and Local Government with the co-operation of, inter alia, the Department of Justice, Equality and Law Reform and *An Garda Síochána*, is proceeding according to a two-year Development Programme.

[390] http://www.emergencyplanning.ie/
[391] http://www.garda.ie/
[392] http://www.hse.ie/
[393] http://www.citizensinformation.ie/
[394] http://www.emergencyplanning.ie/
[395] http://www.environ.ie
[396] http://www.justice.ie/

In 2004, the Government approved, at the proposal of the Minister for Defence[397], a *Strategic Emergency Planning Guidance* document to guide government departments in achieving effective management of the emergency planning process. The strategic guidance provides forward-looking advice that serves as a framework for action by Ministers and departments; in other words, it defines Ministerial and departmental roles in a strategic context. It is not intended to address tactical or operational aspects of emergency planning, which in all cases are carried out below departmental level by, in the 'Justice' domain, *An Garda Síochána*.

Main Actors/Responsibilities:

Government Task Force on Emergency Planning[398]

The Government Task Force on Emergency Planning, chaired by the Minister for Defence[399], provides active leadership of the emergency planning process; facilitates contact and co-ordination between Government Departments and other public authorities; and oversees all emergency planning.

Inter-Departmental Working Group on Emergency Planning[400]

The Inter-Departmental Working Group on Emergency Planning, chaired by the Office of Emergency Planning, Department of Defence[401], provides support for the policy initiatives of the Minister for Defence as chair of the Government Task Force.

Office of Emergency Planning[402]

The Office of Emergency Planning, established within the Department of Defence, supports the Minister for Defence as Chairman of the Government Task Force on Emergency Planning. The Office chairs the Inter-Departmental Working Group on Emergency Planning. The lead responsibility for specific emergency planning functions remains with the relevant Government Departments.

National Security Committee[403]

The National Security Committee ensures that the Government is advised on high-level security matters. The Committee is chaired by the Secretary General to the Government and comprises senior representatives of the Department of the Taoiseach (Prime Minister); Department of Justice, Equality and Law Reform; *An Garda Síochána*; Department of Defence, and Department of Foreign Affairs.

Government Information Service[404]

The Government Information Service (GIS) plays a key role in preparing and projecting the Government's message on emergency management and response issues. An Emergency Planning Media Unit, chaired by the GIS, promotes and co-ordinates this work. The Unit, which comprises Press and Information Officers of government departments and other key

397 http://www.defence.ie/
398 http://www.environ.ie/en/LocalGovernment/FireandEmergencyServices/EmergencyPlanning/
399 http://www.defence.ie/
400 http://www.environ.ie/en/LocalGovernment/FireandEmergencyServices/EmergencyPlanning/
401 http://www.defence.ie/
402 http://www.emergencyplanning.ie/media/docs/1SEPG.doc
403 http://www.justice.ie/en/JELR/EMWS.doc/Files/EMWS.doc
404 http://www.justice.ie/en/JELR/EMWS.doc/Files/EMWS.doc

public authorities, continues to update and co-ordinate arrangements for handling queries on emergency planning and emergency management from the media and public.

Department of Justice, Equality and Law Reform[405]

The Department of Justice, Equality and Law Reform continues to actively contribute to the work of the Government Task Force on Emergency Planning, the Inter-Departmental Working Group on Emergency Planning, the National Security Committee and the Emergency Planning Media Unit, including ensuring representation at appropriate seniority on all structures.

Having regard to the functions of the Minister for Justice, Equality and Law Reform, a major emergency arising from a terrorist attack is a scenario of particular relevance, particularly given the emergence of new forms of international terrorism.

In the case of a major emergency, the Department of Justice, Equality and Law Reform as a potential lead Department would alert the Department of the Taoiseach at an early stage in the development of the emergency.

Additionally, a support role may arise for the Department of Justice, Equality and Law Reform either as a result of it being explicitly mentioned as having support responsibilities in the lead Government Department's strategic emergency plans, with specific functions assigned to it under such plans; or as a result of the fact that non-specific assistance may be requested of the Department of Justice, Equality and Law Reform by the lead Government Department in an emergency. In this regard, the Department of Justice, Equality and Law Reform has a support role in other strategic emergency plans/activities, as National Civil Aviation Security Committee, Chemical Emergencies, and Severe Weather Emergencies.

Cabinet Secretariat[406]

Most emergency situations in Ireland are responded to and managed by area-based emergency services through their own command and control systems, with the lead government department providing a monitoring, advisory, guidance or other functional role, without any need for direct intervention by Cabinet. In a large-scale emergency, significant issues could arise for government. In the case of a major emergency, potential lead departments alert the Department of the Taoiseach at an early stage in the development of the emergency. The necessity to activate the full Cabinet to guide and assist the lead department will be a matter for the Taoiseach[407], and the Cabinet Secretariat will make the necessary arrangements.

15.3 Strategy & Policy

The *Strategic Emergency Planning Guidance*[408] document defines an emergency as "an event, incident or situation, which may present a serious threat to the welfare of the population, the environment, the political, administrative, economic stability or the security of the state, which will require the political and strategic involvement of the Government". In line

[405] http://www.justice.ie/
[406] http://www.gov.ie/en/
[407] http://www.gov.ie/en/
[408] http://www.emergencyplanning.ie/media/docs/1SEPG.doc

with the above definition, the philosophy underlying emergency planning is that it is part of general planning for each area of government activity and should be integrated into the strategic and business planning process within each department.

In the *Strategic Emergency Planning Guidance* the following principles of strategic government emergency planning are highlighted:

- A lead government department has to be identified for any emergency;
- Service delivery should take place at the lowest possible level with coordination at the most appropriate level;
- Each government department and any other public authority involved in emergency planning is responsible for:
  - carrying out its own risk assessment;
  - preparation, exercising, validation and review of its own emergency plans;
  - responding to requirements for coordination and oversight and consulting on matters affecting other government departments and public authorities;
  - ensuring that the proper resources are available, including legal powers;
  - ensuring that proper training is provided for all those involved, and
  - ensuring that performance indicators are appropriately detailed through the business planning process
- Emergency planning should be encompassed within existing governmental and departmental structures.

The lead role for planning the State's response to an emergency will rest with the functional Minister and his or her Government Department, with support from other key departments and public authorities. The functional department has the lead role in the risk assessment, prevention, mitigation, response, maintenance of public confidence and recovery, working in association with other government departments and public authorities. It is the responsibility of the lead department to work with other government departments and the providers of emergency services to ensure that their plans are sufficiently detailed and properly coordinated. It is important to address command and control issues in consultation with all the parties involved in the response and to ensure engagement in a structured exercise programme.

All government departments are prepared to act in a principal support or other support role. A government department or public authority with a principal support role is one that is explicitly mentioned as having support responsibilities in the lead government department's strategic emergency plans and has specific functions assigned to it under such plans. Other support roles include non-specific assistance, which may be requested from any government department or public authority, in an emergency. There are also a number of other departmental structures, inter-departmental structures and expert committees, which have specific functions to assist the emergency plans of the various lead government departments.

Emergency plans are coordinated at local, regional and national levels by the various lead government departments. They cater for a wide variety of situations, which include but are not confined to the following:

- There are three Departments, namely the Department of the Environment, Heritage and Local Government, the Department of Health and Children and the Department of Justice, Equality and Law Reform, with lead roles in respect of the Framework for Coordinated Response to Major Emergency
- The Department of the Environment, Heritage and Local Government has the lead role with regard to issues relating to chemical emergencies
- The Department of the Environment, Heritage and Local Government has the lead role in the National Emergency Plan for nuclear accidents and is supported by an Emergency Response Coordination Committee (ERCC)
- The Department of the Environment, Heritage and Local Government has the lead role, providing guidance to the local authorities which have responsibility for planning for severe weather emergencies
- The Department of Health and Children has the lead role for public health emergencies
- The Department of Communications, Marine and Natural Resources has the lead role for dealing with major oil spillages from vessels and all aspects of harmful substance pollution of the sea and coastal areas
- The Department of Communications, Marine and Natural Resources has the lead role for dealing with all aspects of Search and Rescue at sea
- The Department of Agriculture and Food has the lead role for dealing with exotic animal diseases

15.4 Public – Private Partnership & International Collaboration

NATO's relations with Ireland are conducted through the Partnership for Peace framework, which Ireland joined in 1999. NATO[409] and Ireland actively cooperate on humanitarian, rescue, peacekeeping and crisis management operations and have developed practical cooperation in a range of other areas, as provided for in Ireland's Individual Partnership Programme (IPP)[410].

The Department of Environment, Heritage and Local Government and the Radiological Protection Institute of Ireland participate in the work of the International Atomic Energy Agency (IAEA)[411], which includes emergency planning. The IAEA's main areas of work include safety and security, science and technology, and safeguards and verification. It helps countries to improve their nuclear safety and to prepare for and respond to emergencies. This work contributes to international conventions, standards and expert guidance, and the main aim is to protect people and the environment from harmful radiation exposure.

[409] http://www.nato.int
[410] http://www.defence.ie/WebSite.nsf/Publication+ID/0C789A43B517F3F880256C70003D9AB0?editDocument
[411] http://www.iaea.org/ -

There are two early warning notification systems used two warn of an occurrence of a nuclear or radiological accident or emergency abroad:

- ECURIE - European Community Urgent Radiological Information Exchange[412], and
- EMERCON - International Atomic Energy Agency (IAEA) warning system[413].

Alerts are passed on to the Radiological Protection Institute of Ireland (RPII), as the National Competent Authority, through *An Garda Síochána*.

There is a long tradition of mutual assistance between the emergency services from both administrations, particularly in the border counties. The agreement between the Government of Ireland and the Government of the United Kingdom of Great Britain and Northern Ireland on Police Cooperation, signed on 29th April 2002, provides for a range of cooperative measures between *An Garda Síochána* and the Police Service of Northern Ireland.

Ireland is also involved in:

- Rapid Alert System BICHAT (Biological, Chemical Attack) (RAS BICHAT)[414]
- Food Safety – RAPID Alert System[415]
- Animal Health – Office International des Épizooties (OIE), List A Diseases[416]

15.5 Training & Exercises

The Framework states that "each principal response agency should prepare and implement a staff development and training programme, designed to build the knowledge, skills and experience of staff that will fill key roles in the response to a major emergency. This programme should be revised periodically". Test, training and exercise programmes are part of the Major Emergency Management activities of PRAs.

On April 28, 2008, for example, a large scale cross border exercise took place in the coastal area of Ballykinler in County Down. The exercise was organised to test the ability of both the Northern Ireland Ambulance Service and the Republic's National Ambulance Service to respond jointly in the event of a major medical emergency in the border region. This is the first time that such an exercise has been co-ordinated in this area of the border and followed an earlier test in 2007 in the North West. The exercise involved months of preparation by the ambulance services personnel who underwent specialised, internationally recognised training in handling multiple casualty situations. This training in Major Incident Medical Management Support (MIMMS) was provided with the assistance of the Territorial Army Medical Services, the Royal Air Force and the Irish Army Air Corps.

Training for the ERU (a specialist firearms unit of *An Garda Siochana*) is carried out in the Garda's Tactical Training Unit, established in 1983 at the Garda College, Templemore. Members of the ERU have received training with the FBI's Hostage Rescue Team. In addition, ERU officers have been trained abroad in Germany, the UK and the US. ERU officers are required to qualify three times per year in all firearms being used by the unit.

[412] http://rem.jrc.ec.europa.eu/40.html
[413] http://www-ns.iaea.org/conventions/emergency.htm
[414] https://webgate.ec.europa.eu/ras-bichat/
[415] http://ec.europa.eu/food/food/rapidalert/index_en.htm
[416] http://www.oie.int/

Training consists of in-house tactical training on an ongoing basis from the ERU's own firearms instructors and refresher range practice.

15.6 Sector – Specific Key Players & Initiatives

ENERGY

Public authorities:

- ***Department of Communications, Energy and Natural Resources***[417]

  The Department of Communications, Energy and Natural Resources is a department of the Government of Ireland that is responsible for the telecommunications and broadcasting sectors and the protection and development of the natural resources of the Republic of Ireland. The head of the Department is the Minister for Communications, Energy and Natural Resources who is assisted by one Minister of State.

- ***Commission for Energy Regulation***[418]

  Established under the Electricity Regulation Act[419] 1999 as the Commission for Electricity Regulation, it was responsible for open, transparent and accountable regulatory processes for the electricity industry in Ireland. The Commission's jurisdiction expanded under the Gas (Interim) (Regulation) Act[420] 2002 to that of a broader energy regulator, incorporating both gas and electricity. The Commission has been renamed as the Commission for Energy Regulation to reflect its increased role.

- ***Electricity Supply Board (ESB)***[421]

  Founded in 1927, the Electricity Supply Board (ESB) is a statutory corporation in the Republic of Ireland. The Board includes the following sub-elements:

  – ESB Power Generation owns and operates generating stations in the Republic of Ireland with an installed capacity totalling 4651MW.

  – ESB Customer Supply & Group Services.

  – ESB Customer Supply operates as the Public Electricity Supplier offering a supply of electricity to over 2million mainly residential customer in the Republic of Ireland retail market on terms approved by the Commission for Energy Regulation (CER). Group Services is responsible for a number of unregulated activities and internal services for the various business lines within the ESB Group including the Information and Communications Technology (ICT) Group, ESB Telecoms Ltd, ESB Contracts Ltd and internal services for the ESB Group.

  – ESB Networks is the owner of the high voltage transmission system and the owner and operator of the medium and lower voltage distribution system. It provides services to all electricity customers and all generators and suppliers of electricity in the Republic of Ireland

[417] http://www.dcenr.gov.ie
[418] http://www.dcenr.gov.ie
[419] http://www.irishstatutebook.ie/
[420] http://www.irishstatutebook.ie/
[421] http://www.esb.ie

- ***EirGrid plc***[422]

  EirGrid plc is the independent electricity Transmission System Operator (TSO) in Ireland and the Market Operator in the wholesale electricity trading system. EirGrid's role is to deliver services to generators, suppliers and customers across the high voltage electricity system, and to put in place the grid infrastructure needed to support Ireland's economy. EirGrid develops, maintains and operates a safe, secure, reliable, economical and efficient transmission system. It plays a key role in the operation of the Single Electricity Market, as well as developing key infrastructural projects.

NUCLEAR

Public authorities:

- ***Department of Environment, Heritage and Local Government***[423]

  The Minister for the Environment, Heritage and Local Government exercises general responsibility for nuclear and radiological protection matters, while other ministers have specific responsibilities over certain aspects of these. The Radiological Protection Institute of Ireland is accountable to the Minister. The Minister is also empowered to give effect to European Union decisions relating to the protection of workers and the general public from ionising radiation through the mechanism of a ministerial order, issued after consultation with other ministers.

- ***Department of Agriculture, Fisheries and Food (Minister of State for Food and Horticulture)***[424]

  If there is a risk that prescribed levels of radioactivity have been exceeded, the Minister for Agriculture and Food may make regulations to control agricultural activities in a particular area. The Minister also has the power, in the event of a radiological emergency, to acquire animals, crops, food and water resources etc. [Section 32(2)]. This can only be done after consultation with the Minister for the Environment, Heritage and Local Government, the Institute and the Food Safety Authority of Ireland.

- ***Department of Communications, Energy and Natural Resources***[425]

  The Minister for Communications, Marine and Natural Resources has the power to regulate fishing and aquaculture activities in an area where levels of radioactivity activity exceed some thresholds. The Harbours Act[426], 1996 prescribes detailed provisions in relation to safety of navigation and security in harbours and provides broad statutory powers for harbour masters to give directions to ships masters including the prevention of vessel movement for safety reasons. The act specifically enjoins harbour masters from permitting entry of radioactive material (within the meaning of the IMO's International Maritime Dangerous Goods Code) without the consent of the Radiological Protection Institute of Ireland.

- ***Department of Health and Children***[427]

[422] http://www.eirgrid.com/EirgridPortal/Home.aspx
[423] http://www.environ.ie
[424] http://www.agriculture.gov.ie/
[425] http://www.dcenr.gov.ie
[426] http://www.irishstatutebook.ie/
[427] http://www.dohc.ie/

Where prescribed levels of radioactivity may have been exceeded, the Minister for Health and Children may make regulations, as prescribed by European Union Directives, controlling the importation or exportation of any food into or out of Ireland. The Minister also has certain powers in relation to the medical use of radioactive substances and irradiating apparatus. The Minister is empowered to make regulations, as prescribed by European Union Directives, to prevent hazards to the health of persons using such substances or apparatus, and may also prohibit them except in accordance with specified conditions or the granting of a licence.

- ***Department of Defence***[428]

  It is Irish policy that government departments and agencies take the lead role in planning for emergencies in the areas for which each has statutory responsibility. The responsibility for the co-ordination and oversight of government peacetime planning was conferred on the Minister for Defence by a government decision.

- ***Radiological Protection Institute of Ireland***[429]

  The Radiological Protection Institute of Ireland (RPII) is the national organisation with regulatory, monitoring and advisory responsibilities in matters pertaining to ionising radiation. In particular the RPII concerns itself with hazards to health associated with ionising radiation and with radioactive contamination in the environment. The RPII was established in 1992 under the Radiological Protection Act[430], 1991. The twelve members of the Board are appointed by the Minister for the Environment, Heritage and Local Government, six of them having been nominated by organisations with interests in various aspects of the RPII's work. The RPII is financed by grant-in-aid from the Exchequer and by income from dosimeters, product certification and other services, licence charges, and research and consultancy contracts. The Institute's responsibilities fall into the following categories:

  – Monitoring activity and ionising radiation.

  – Advising the government on radiological safety matters and on the relevant international standards.

  – Monitoring any scientific, technological, economic or other development relating to nuclear activity and keeping the government informed of such developments.

  – Carrying out or co-ordinating research.

  – Assisting in the planning and implementation of measures to deal with radiological emergencies, and giving information to the public on radiological safety.

  The act also specifies various specific functions for the Institute which it the main international point of contact for Ireland. The Institute is responsible for exchanging information and co-operating with its counterparts in other states, and for giving assistance to other states in the event of a radiological emergency.

  The RPII with support from *Met Éireann* (the Irish Meteorological Service), local authorities and the Defence Force operates a national network of permanent radiation-monitoring stations which are operational around the clock. These stations

[428] http://www.defence.ie/website.nsf/home+page?openform
[429] http://www.rpii.ie/
[430] http://www.irishstatutebook.ie/

include air samplers and gamma dose monitors. Data from the gamma monitors is continuously fed back to a central computer at RPII. While the initial warning of an accident abroad would come from the international notification systems, this network would provide the first measurements in the event of radioactivity reaching Ireland. If elevated radiation levels are detected, an alarm system is automatically triggered.

There are two independent international systems in place for rapid notification of any radiological emergencies with potential cross-border impacts. These are operated by the International Atomic Energy Agency in Vienna and the European Commission in Luxembourg. These systems operate continuously and are regularly tested and updated (communications channels for the EC system are, for example, tested daily).

- ***Food Safety Authority of Ireland (FSAI)***[431]
  With regard to radioactivity in food, it is a function of the Authority to ensure that food complies with the Radiological Protection Act[432], 1991. The Authority is responsible for monitoring the levels of radioactivity in animals, fauna, poultry, eggs, crops, animal carcasses, feeding stuffs, fish, seaweed, bottled water or water supplied intended for human consumption or any food, where specified levels of radioactivity have been or are likely to be exceeded is also specified.
- ***Emergency Response and Co-ordination Committee***[433]
  The Emergency Response and Co-ordination Committee (ERCC) is a committee established in during of emergencies under the National Emergency Plan for Nuclear Accidents (NEPNA)[434]. The members of the ERCC are
  - Department of the Environment, Heritage and Local Government (Chair)
  - RPII
  - Department of Agriculture and Food
  - Department of Defence
  - Department of Health and Children
  - Department of Communications, Marine and Natural Resources
  - Department of the Taoiseach
  - Food Safety Authority of Ireland
  - *An Garda Síochána.*

  Officials from the Nuclear Safety Section and the Fire Services and Emergency Planning Section represent the Department of the Environment.

  In the event that nuclear accident has the potential to seriously affect Ireland, the ERCC is responsible to:

  - consider the technical assessment from the RPII of the actual and potential consequences of the accident and the RPII's advice on what countermeasures

[431] http://www.fsai.ie/
[432] http://www.irishstatutebook.ie/
[433] http://www.environ.ie/en/Environment/EnvironmentalRadiation/NationalEmergencyPlan/
[434] http://www.environ.ie/en/Environment/EnvironmentalRadiation/NationalEmergencyPlan/

should be implemented by Government to minimise the radiation exposure of the public.

– provide advice to the Minister for the Environment, Heritage and Local Government and to the Committee of Ministers on the implications and practical issues associated with the recommendation of the RPII concerning any countermeasure

Initiatives:

There are no nuclear power plants, nuclear research reactors or uranium production within Ireland's territorial boundaries. Nevertheless, Ireland has developed legislation in the area of radiation protection for the purpose of protecting its people, the food supply and the environment from harmful radiation effects.

The RPII is statutorily responsible for assisting in radiological emergency planning and for the implementation of measures to deal with such emergencies. The Institute is also responsible for giving assistance to and co-operating with other states in the event of a radiological emergency.

The transport of radioactive materials in Ireland is prohibited, save under licence of the Radiological Protection Institute of Ireland. Activities involving radioactive waste products, including transport, may not be undertaken without a licence from the Institute. The licence, which may be subject to conditions, is issued for a limited period and may be revoked by the Institute if the conditions of the licence are not met.

In 2000 the Department of Environment, Heritage and Local Government developed the National Emergency Plan for Nuclear Accidents (NEPNA)[435], in accordance with the Radiological Protection Act[436], 1991.

The Department of the Environment, Heritage and Local Government has the lead role in ensuring that any nuclear emergency response operates smoothly and that the necessary precautions are taken to protect the Irish people. In the event of a nuclear emergency having the potential to affect Ireland, a Committee of Ministers will assemble to give direction on recommended countermeasures placed before it by the ERCC on the basis of advice from the RPII or, in urgent circumstances, by the RPII directly. The ERCC will consider the technical assessment from the RPII of the actual and potential consequences of the accident and the RPII's advice on what countermeasures should be taken to minimise the radiation exposure of the public. The ERCC will also provide advice to the Committee of Ministers on the implications and practical issues associated with the recommendations of the RPII.

The key role of the RPII is in information gathering and assessment, leading to recommendations on the need for countermeasures. The ERCC advises the Committee of Ministers, and based on their decision, co-ordinates the implementation of countermeasures.

INFORMATION AND COMMUNICATION TECHNOLOGIES

Public authorities:

- ***Department of Communications, Energy and Natural Resources[437]***

[435] http://www.environ.ie/en/Environment/EnvironmentalRadiation/NationalEmergencyPlan/
[436] http://www.irishstatutebook.ie/

The Department's key roles and functions in the fields of Information and Communication Technologies are:

- Communication: Ireland's telecommunications market is fully liberalised and is moving to position Ireland at the forefront of Internet developments and the e-commerce agenda. There is a large-scale programme to roll-out broadband around the country. The Department is also beginning regulatory and market reform, and is addressing the needs of national Post Office network.
- Broadcasting. The Department is creating an environment which encourages the establishment and maintenance of high quality Irish radio and television services

- ***Broadcasting Commission of Ireland***[438]
  Responsible for the licensing and regulation of the independent television and radio sector. The Commission is also responsible for licensing certain new digital television services and for the development of codes of programming and advertising standards on television and radio. The Broadcasting Complaints Commission deals with complaints relating to programme material and advertising on RTE and independent television and radio services.
- ***Commission for Communications Regulation (ComReg)***[439]
  ComReg is the statutory body responsible for the regulation of the electronic communications sector (telecommunications, radio communications and broadcasting transmission) and the postal sector. ComReg enables competition in the communications sector by facilitating market entry through a general authorisation to provide networks and services and by regulating access to networks so as to develop effective choice for consumers. In a rapidly evolving sector, both in technological and commercial terms, ComReg provides the framework for the introduction of new services such as 3G. ComReg has a wide range of responsibilities in telecommunications (or electronic communications services and networks as it is more accurately described), posts and spectrum management.
- ***Radio Telefís Éireann (RTE)***[440]
  The national public service broadcaster and a statutorily independent body, RTE operates three national television services (RTE 1, Network 2 and TG4 and four national radio services RTE 1, 2FM, Radio na Gaeltachta and Lyric FM). It produces programmes and broadcasts on television, radio and the Internet. The radio service began on 1 January 1926, while regular television broadcasts began on 31 December 1961, making it one of the oldest continuously operating public service broadcasters in the world. RTÉ is a statutory body run by an authority appointed by the Irish Government. General management of the organisation is in the hands of the Executive Board headed by the Director-General.

WATER

Public authorities:

- ***Department of Environment, Heritage and Local Government***[441]

[437] http://www.dcenr.gov.ie
[438] http://www.bci.ie/
[439] http://www.comreg.ie/
[440] http://www.rte.ie
[441] http://www.environ.ie

The Department of the Environment, Heritage and Local Government is a department of the Government of Ireland. It is led by the Minister for the Environment, Heritage and Local Government who is assisted by two Ministers of State. The aim of the Department is to promote sustainable development and improve the quality of life through protection of the environment and heritage, infrastructure provision, balanced regional development and good local government in Ireland.
Its *Statement of Strategy 2008-2010* sets out the key objectives and strategies that will be pursued by the Department in its core functional areas of environment, water, natural heritage, built heritage and planning, housing, local government, meteorological services and corporate services over the coming three years.

- ***Environmental Protection Agency (EPA)***[442]

  The EPA is at the front line of environmental protection and policing. It ensures that Ireland's environment is protected, and monitors changes in environmental trends to detect early warning signs of neglect or deterioration. The primary responsibilities of the EPA include: environmental licensing, enforcement of environmental law, environmental planning, education and guidance, monitoring, analysing and reporting on the environment, regulating Ireland's greenhouse gas emissions, environmental research development, strategic environmental assessment, and waste management

- ***Office of Public Works***[443]

  The Office of Public Works (OPW) is the lead agency for flood risk management in Ireland. The coordination and implementation of the Government's policy on the management of flood risk in Ireland, in conjunction with our responsibilities under the Arterial Drainage Acts[444], 1945-1995, form one of the four core services of the OPW.

FOOD

Public authorities:

- ***Department of Agriculture, Fisheries and Food (Minister of State for Food and Horticulture)***[445]

  The Department of Agriculture, Fisheries and Food is a department of the Government of Ireland. The mission of the Department is to lead the sustainable development of a competitive, consumer focused agro-food sector and to contribute to a vibrant rural economy and society. It is led by the Minister for Agriculture, Fisheries and Food who is assisted by two Ministers of State. The Department undertakes a variety of functions including: development and implementation of national and EU schemes in support of agriculture, food, fisheries, forestry and rural environment, monitoring and controlling aspects of food safety, control and audit of public expenditure under its control, regulation of the agriculture, fisheries, and food industries through national and EU legislation, and monitoring and controlling animal and plant health and animal welfare.

[442] http://www.epa.ie/
[443] http://www.opw.ie
[444] http://www.irishstatutebook.ie/
[445] http://www.agriculture.gov.ie/

- ***Food Safety Authority of Ireland***[446]

  The Food Safety Authority of Ireland (FSAI) was established under the Food Safety Authority of Ireland Act[447], 1998. The Act was enacted in July 1998 and came into effect on 01 January 1999.The principal function of the FSAI is to take all reasonable steps to ensure that food produced, distributed or marketed in Ireland meets appropriate standards of food safety and hygiene. The FSAI aims to ensure that food complies with legal requirements, or where appropriate with recognised codes of good practice.

HEALTH

Public authorities:

- ***Department of Health and Children***[448]

  The Department of Health and Children is a department of the Government of Ireland. The Department's mission is to improve the health and well-being of people in Ireland in a manner that promotes better health for everyone, fair access, and responsive and appropriate care delivery. The Department is led by the Minister for Health and Children who is assisted by four Ministers of State.

- ***Health Service Executive***[449]

  The Health Service Executive (HSE) is responsible for providing health and personal social services for everyone living in the Republic of Ireland. The HSE provides thousands of different services in hospitals and communities across the country. The establishment of the HSE represented the beginning of the largest programme of change ever undertaken in the Irish public service. Prior to its establishment, services were delivered through a complex structure of ten regional Health Boards, the Eastern Regional Health Authority and a number of other different agencies and organisations. The HSE replaced all of these organisations. It is now the single body responsible for ensuring that everybody can access cost effective and consistently high quality health and personal social services.

- ***Health Information and Quality Authority***[450]

  The Health Information and Quality Authority (HIQA) was established in May 2007 as part of the government's health reform programme and is committed to operating to the highest standards of corporate governance. It is an independent authority, with broad ranging functions and powers reporting to the Minister for Health. HIQA was established to drive quality, safety, accountability and the best use of resources in our health and social care services, whether delivered by public, voluntary or private bodies.

FINANCIAL

Public authorities:

446 http://www.fsai.ie/
447 http://www.irishstatutebook.ie/
448 http://www.dohc.ie/
449 http://www.hse.ie/eng/
450 http://www.hiqa.ie/

- ***Department of Finance***[451]

  The Department of Finance (*An Roinn Airgeadais*) is a department of the Government of Ireland. It is led by the Minister for Finance and is assisted by one Minister of State. The Department of Finance is responsible for the administration of the public finances of the Republic of Ireland and all powers, duties and functions connected with the same, including in particular, the collection and expenditure of the revenues of Ireland. The work of the Department of Finance is distributed between six divisions:-Taxation and Financial Services Division (TFSD), Budget, Economic and Pensions Division (BEPD), Sectoral Policy Division (SPD), Personnel and Remuneration Division (PRD), Organisation, Management and Training Division (OMTD), and Corporate Services Division (CSD).
- ***Central Bank and Financial Services Authority***[452]

  The Central Bank and Financial Services Authority (CBFSAI) has two component entities: the Central Bank, which has responsibility for monetary policy functions, financial stability, economic analysis, currency and payment systems, investment of foreign and domestic assets and the provision of central services; and the Irish Financial Services Regulatory Authority (Financial Regulator), which is an autonomous entity within the CBFSAI and has responsibility for financial sector regulation and consumer protection.

TRANSPORT

Public authorities:

- ***Department of Transport***[453]

  The Department of Transport is a department of the Government of Ireland responsible for transport policy and overseeing transport services and infrastructure. The Department is led by the Minister for Transport. Its mandate is to:
  - Deliver the national roads programme as part of the National Development Plan, and to implement the Government's roads safety strategy.
  - Provide a well functioning, integrated public transport system and ensure improved public transport provision by delivering new public transport infrastructure and facilities.
  - Ensuring that aviation practices and procedures comply with best international standards. Promote the development of a vibrant, competitive and progressively regulated aviation sector. Provide adequate airport infrastructure and competitive airport services.
  - Establish, promote, regulate and enforce maritime safety and security standards. Provide emergency response services and safeguard the maritime environment. The Department is also responsible for ports and shipping policy.

[451] http://www.finance.gov.ie/
[452] http://www.centralbank.ie
[453] http://www.transport.ie

- ***Road Safety Authority***[454]

  The Road Safety Authority (RSA) was established under the Road Safety Authority Act[455] 2006, and is charged with the task of improving safety on Irish roads.. It was established in response to the high numbers of deaths on Irish roads. Reducing this toll will involve cooperation with many stakeholders working in the area of road safety, including the *Gardai*, education sector, health sector, local authorities, the National Roads Authority, the media and the general public.

- ***Railway Procurement Agency***[456]

  Railway Procurement Agency is a state agency of the Department of Transport charged with the development of light railway and metro infrastructure. It was established in December 2001 under the Transport (Railway Infrastructure) Act[457] 2001.

- ***Irish Aviation Authority***[458]

  The Irish Aviation Authority (IAA) is a commercial state-sponsored company established in January 1994 to provide air navigation services in Irish-controlled airspace, and to regulate safety standards within the Irish civil aviation industry through: certifying and registering aircraft airworthiness, licensing personnel and organisations involved in aircraft maintenance, licensing pilots, air traffic controllers and aerodromes, approving and monitoring air carrier operating standards. Internationally set safety standards emanating from the International Civil Aviation Organisation (ICAO); European Joint Aviation Authorities (JAA); EUROCONTROL; the European Civil Aviation Conference (ECAC), the European Aviation Safety Agency (EASA) and the European Union (EU) guide the IAA in ensuring that Irish civil aviation operates to the most stringent safety standards. The IAA also utilises its capabilities and expertise to provide both technical training and aviation consultancy services worldwide.

- ***Irish Coast Guard***[459]

  The Irish Coast Guard (IRCG) is part of the Department of Transport. They are responsible for search and rescue, pollution and salvage response in the marine environment, marine communications network, marine safety awareness. The IRCG does not form part of the Irish Defence Forces, rather it operates as an agency of the Department of Transport.

- ***National Roads Authority (NRA)***[460]

  The National Roads Authority (NRA) was formally established as an independent statutory body under the Roads Act[461] , 1993 with effect from 1 January, 1994. The Authority's primary function, under the Roads Act 1993, is 'to secure the provision of a safe and efficient network of national roads'. For this purpose, it has overall responsibility for the planning and supervision of construction and maintenance works

[454] http://www.rsa.ie/
[455] http://www.irishstatutebook.ie
[456] http://www.rpa.ie/
[457] http://www.irishstatutebook.ie
[458] http://www.iaa.ie/
[459] http://www.transport.ie/marine/IRCG/index.asp?lang=ENG&loc=2029
[460] http://www.nra.ie/
[461] http://www.irishstatutebook.ie

on these roads. The NRA is responsible for the planning, maintenance and construction of National Primary Routes and National Secondary Routes as well as establishing safety measures.

- ***Dublin Airport Authority (DAA)***[462]

  Dublin Airport Authority (DAA) is the state owned airport authority in the Republic of Ireland. Headquartered at Dublin Airport, the DAA's principal activities include airport management, operation and development, domestic and international airport retail management, and airport investment

- ***Córas Iompair Éireann***[463]

  Córas Iompair Éireann (CIÉ), as a Statutory Corporation, has no issued share capital or equity invested in the company. The Irish Government is currently the sole owner of CIÉ, the Government's representatives are the Minister for Transport and his Department. For operational purposes, CIÉ has three wholly owned subsidiary limited liability companies set up under the Companies Act as provided for in the Transport (Reorganisation of Córas Iompair Éireann) Act 1986. Each of these has issued and paid up share capital.

CHEMICAL INDUSTRY

Public authorities:

- ***Petroleum Affair Division***[464]

  The Petroleum Affair Division is an element of the Department of Communications, Energy and Natural Resources. The role of the Petroleum Affairs Division is to maximise the benefits to the State from exploration for and production of indigenous oil and gas resources, while ensuring that activities are conducted safely and with due regard to their impact on the environment and other land/sea users. The Division is responsible for the promotion, regulation and monitoring of the exploration and development of oil and gas in onshore and offshore Ireland. This involves the allocation of acreage to exploration companies under various types of licences, and agreeing appropriate work programmes.

SPACE

Public authorities:

- ***The Irish ESA Delegation***

  The Irish ESA Delegation comprises representatives of the Office of Science and Technology (OST)[465] within the Department of Enterprise, Trade and Employment and representatives of Enterprise Ireland[466]. The OST maintains responsibility for policy and budgetary matters.

- ***Enterprise Ireland***[467]

[462] http://www.dublinairportauthority.com
[463] http://www.cie.ie/home/
[464] http://www.dcenr.gov.ie/Natural/Petroleum+Affairs+Division
[465] http://www.entemp.ie/science/technology/work.htm
[466] http://www.entemp.ie/
[467] http://www.enterprise-ireland.com

Enterprise Ireland, in association with the Office of Science and Technology of the Department of Enterprise, Trade and Employment, has been instrumental in developing the Irish space sector industry, by directing national space funding and providing technical and other support to participating companies. Enterprise Ireland provides a source of expertise for Irish companies in developing their space strategies as well as being a point of reference for international companies wishing to identify relevant sources of space-related expertise within Ireland.

RESEARCH FACILITIES

Public authorities:

- ***Department of Education and Science***[468]

  The Department of Education and Science is a department of the Government of Ireland. It is led by the Minister for Education and Science who is assisted by five Ministers of State. The mission of the Department of Education and Science is to provide high-quality education which will enable individuals to achieve their full potential and to participate fully as members of society, and contribute to Ireland's social, cultural and economic development. Chief among the Department's priorities are the promotion of equity and inclusion, quality outcomes and lifelong learning; planning for education that is relevant to personal, social, cultural and economic needs; enhancement of the capacity of the Department for service delivery, policy formulation, research and evaluation.

- ***Geological Survey of Ireland (GSI)***[469]

  The Geological Survey of Ireland (GSI), founded in 1845, is the national earth science agency. It is responsible for providing geological advice and information, and for the acquisition of data for this purpose. GSI produces a range of products including maps, reports and databases and acts as a knowledge centre and project partner in all aspects of Irish geology.

- ***Marine Institute***[470]

  The Marine Institute is the national agency responsible for Marine Research, Technology Development and Innovation. It seeks to assess and realise the economic potential of Ireland's 220 million acre marine resource; promote the sustainable development of marine industry through strategic funding programmes and essential scientific services; and safeguards the marine environment through research and environmental monitoring.

- ***Dublin Institute for Advanced Studies (DIAS)***[471]

  The Dublin Institute for Advanced Studies is a statutory corporation established in 1940 under the Institute for Advanced Studies Act of that year. It is a publicly-funded independent centre for research in basic disciplines. The Institute has three constituent schools: the School of Theoretical Physics, the School of Cosmic Physics and the School of Celtic studies. Each school has an independent governing board. The Institute, through the constituent schools, pursues fundamental research in

[468] http://www.education.ie/
[469] http://www.gsi.ie/
[470] http://www.marine.ie/
[471] http://www.dias.ie/

specialised branches of knowledge and trains advanced students in methods of original research. The institute is an academic publisher of monographs, books, and journals in Celtic Studies and on advanced scientific subjects.

16 Italy

Figure 69: Italy

16.1 Summary

	Organisational Model	Strategy & Policy	Methodology & Standards	Public-Private Partnership & International Collaboration	Funding & Human Resources	Training & Exercises	Sector-Specific Key Players & Initiatives
Italy	▪ Representatives from various ministries / agencies cooperate on CIP efforts through an formal national CIP working group (Tavolo PIC), but there is no dedicated national CIP agency	▪ No national-level strategic or operative plan in place ▪ Ministry of Interior initiated an activity to identify Critical Information Infrastructures	▪ No official methodology endorsed by the government	▪ AIIC - Italian Association of Critical Infrastructure Experts (Public-Private Entitiy)	▪ No CIP-specific budget assigned ▪ 5 people from Civil Protection and Office of the Military Advisory of the Prime Minister represent Italy internationally	▪ Limited university-level specialization programs ▪ MESIMEX Exercise	▪ Emergency Plan for the Electricity System (done by Terna) ▪ ISCOM released guidelines about security of TLC networks supporting critical infrastructures

Although various Ministries, government agencies, and CI operators in Italy have expressed interest and initiated activity in the CIP realm, the Italian government has not yet established an agency at the national level dedicated exclusively to CIP. Also, there is no national-level strategic or operative plan in place. CIP activities are driven by a formal working group (Tavolo PIC) containing resources from several Ministries and government agencies (no operators). This group is led by the Military Advisor to the Prime Minister.

Critical Information Infrastructure Protection has received more attention than other sectors with the establishment of a specific police force (CNAIPIC) and specific laws to fight against cyber-crimes and terrorist activities. The Ministry of Interior has also initiated an activity to identify critical information infrastructures in Italy.

The business model used by the CNAIPIC improves Public-Private Partnerships by means of bilateral agreement signed with each one of the different critical infrastructure's operators. The AIIC, a non-profit organisation that involves representative of public authorities, infrastructure owners, and CIP experts, plays a key role in this process.

16.2 Organisational Model

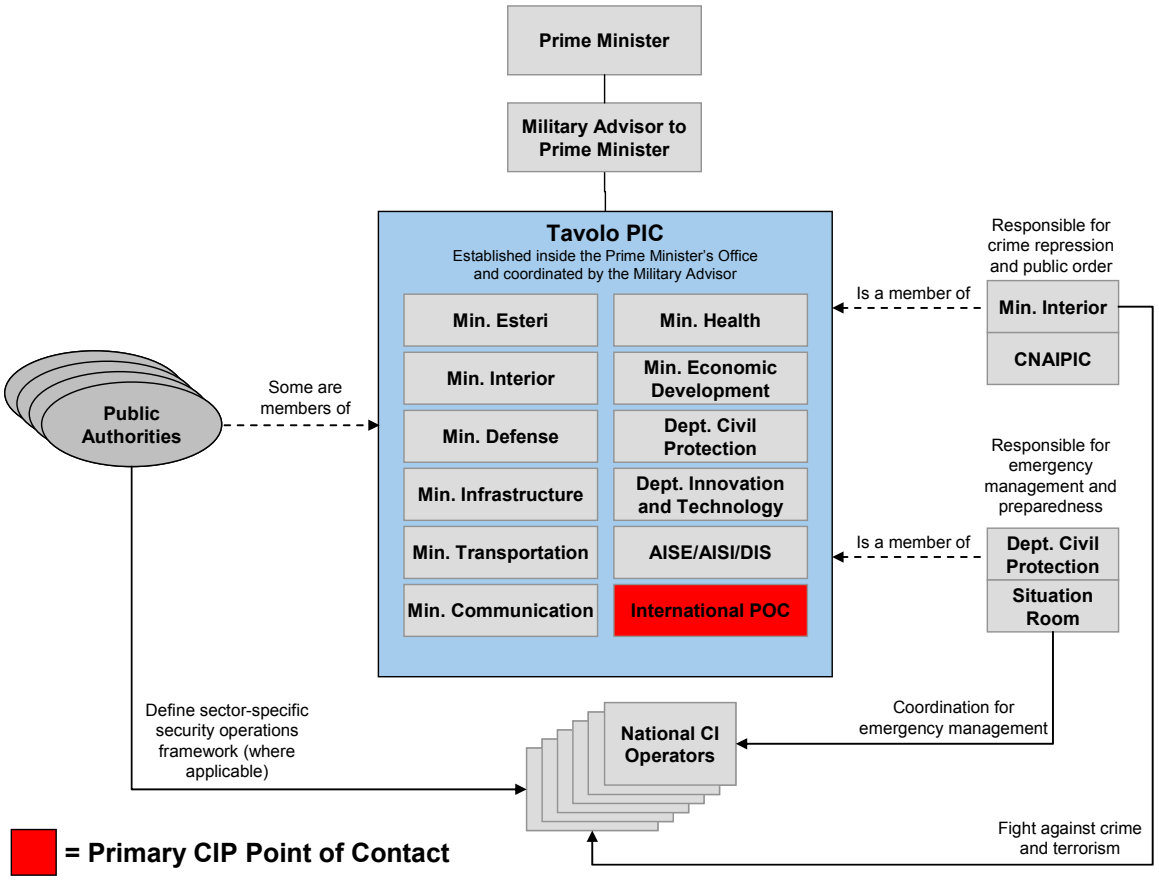


Figure 70: Organisational Chart (only CIP-related agencies shown)

Main Actors/Responsibilities:

- ***Tavolo di Indirizzo e Coordinamento per la Protezione delle Infrastrutture Critiche (Tavolo PIC)* (Critical Infrastructure Protection Working Group)**

  The Tavolo PIC is a national CIP working group. Its responsibilities include coordination between Italian activities and other international organisations (G8, UN, OCSE, EU, etc.). The Italian government established this coordination body in 2006 as part of the Nucleo Politico Militare (the advisory council to the Prime Minister for military and security issues) and it is coordinated by the Prime Minister's military advisor. The working group has delegated international POC responsibilities to the group members from the Department of Civil Protection.

- ***Ministero dell'Interno*** **(Ministry of Interior)**[472]

  The responsibility for the fight against crime and terrorism lies with the Ministry of Interior (supported by Intelligence and other police corps). The Ministry established the CNAIPC (described below) to improve the security of Critical Information Infrastructure nationwide.

- ***Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC)*** **(National Center for Electronic Crime and Critical Infrastructure Protection)**

  In 1992, the Postal Police corps established a specialized team to fight cyber crime. This unit eventually evolved into the CNAIPIC, founded in 2003 to provide timely and effective actions to prevent, contrast, and repress criminal activities against critical information infrastructures.

- ***Dipartimento Nazionale della Protezione Civile*** **(National Department of Civil Protection)**

  The Department of Civil Protection holds the responsibility for emergency management and prevention, and it operates the national situation room where public authorities and representatives of critical national infrastructures operate in close cooperation during crises. It also has the responsibility to provide operational plans for natural and man-made disasters.

16.3 Strategy & Policy

Italy has not defined a specific overall strategy for Critical Infrastructure Protection, but the responsibility for the security of infrastructures is delegated on a Sectoral basis to the respective national authorities and infrastructure stakeholders.

- ***Protezione delle Infrastrutture Critiche Informatizzate – La realtà italiana***[473] **(Critical Information Infrastructure Protection – The Italian situation)**

  In 2005, a CIP Working Group released this report that provided an assessment of the actual state of critical information infrastructures with regards to vulnerability and threat trends. The report also provided guidance on policy organisation and strategy, as well as a research agenda. Although the report initially generated a large amount of interest, its suggestions have not yet been converted into concrete activities.

- **Ministerial Decree of 9 January 2008**

  With this decree, the Ministry of Interior initiated activity to identify critical information infrastructures[474]. Specifically, it identifies information infrastructures that support central government institutions and societies operating in the field of telecommunications, energy, health, and water management as national critical information infrastructures. The owners of these national critical information

[472] http://www.interno.it/mininterno/export/sites/default/it/
[473] www.infrastrutturecritiche.it/aiic/index.php?option=com_docman&task=doc_download&gid=101&Itemid=98
[474] www.**infrastrutturecritiche**.it/aiic/index.php?option=com_docman&task=doc_download&gid=221&Itemid=58

infrastructures must stipulate a bilateral agreement with the CNAIPIC to improve their security against cyber attack.

16.4 Methodology & Standards

The Italian government has not initiated any official activities to develop standard methodologies regarding Critical Infrastructure Protection.

The responsibility for the security of each infrastructure is the responsibility of the corresponding owner or operators. For several infrastructures (i.e. electricity grid, air transportation, and rail network), sector-specific security regulations require operators to establish a security plan in accordance with prescribed guidelines. In some cases, the operators must also submit these plans to the corresponding national authority for a formal validation.

- ***UNI – Ente Nazionale Italiano di Unificazione (National Body for Standardisation)***[475]

  UNI is a private, non-profit association with more than 7,000 members including companies, freelance professionals, associations, scientific and academic institutions, and bodies connected to public administration. UNI represents Italy by participating in the activities of supranational standardisation organisations such as ISO (International Organisation for Standardisation) and CEN (Comité Européen de Normalisation).

  UNI contributes, for Italy, to the definition of the ISO TC/223 on "Societal Security" which has the goal of standardising the approaches for the "security of the critical functions of society"[476].

16.5 Public – Private Partnership & International Collaboration

- ***Associazione Italiana Esperti Infrastrutture Critiche (AIIC)*** **(Italian Association of Critical Infrastructure Experts)**[477]

  AIIC is the is the only player in the PPP field in Italy. It is a non-profit organisation which involves representatives from public authorities, critical infrastructure owners, and CIP experts. It promotes information sharing and multi-sector, multi-disciplinary approaches. It also promotes training activities on security and CIP topics, and it operates as a bridge between private sector and public authorities.

  AIIC promoted a meeting by the *Tavolo PIC* and critical infrastructure operators in March 2008, and it is involved in several EU projects related to CIP and infrastructure security (e.g. EPCIP-MS3i, DG JLS SETEC).

[475] http://www.uni.com
[476] http://www.uni.com/uni/controller/it/comunicare/articoli/2008_1/uni_ct_sicurezza.htm
[477] www.InfrastruttureCritiche.it

- **CNAIPIC Business Model**

  The CNAIPIC adopted a business model based on the presence of bilateral agreements between the Postal police and the owner of each single infrastructure. These agreements specify the modality in which CNAIPIC operates in the presence of a possible attack, what types of information the owner should provide to the police both during and after an attack, and the technical details needed to concretely contrast an attack. In this way, it is possible to better handle attacks by tailoring the police action to the specific needs of each infrastructure.

- **Project DOMINO**

  The DOMINO Project (modeling the domino effect of infrastructure collapses), submitted by the Italian Civil Protection Department, together with research institutions (Fondazione Ugo Bordoni, FORMIT) and private sector partners, was approved for funding by the EU Commission in the EPCIP program (February 2009).

  The DOMINO project aims to develop an innovative interdependency analysis methodology and an open source software tool that will support all European institutional actors in the identification of European Critical Infrastructures (ECI), according to the EU "Directive 2008/114/EC of 8 December 2008 on the identification and designation of European Critical Infrastructures (ECI) and the assessment of the need to improve their protection".

  DOMINO is meant to be a transnational project involving CIP contact points from UK, France, and Bulgaria, and having the support of contact points from other Member States, for information sharing and validation of final results. Thus, DOMINO provides a possible means to harmonize the assessment methods used in the different Member States.

Although the Italian government has not established or promoted any other specific activity with other countries on CIP topics, there are several bilateral and multilateral agreements with European and North Africa countries devoted to improve cooperation and national security that include aspects related to infrastructures.

16.6 Funding & Human Resources

FUNDING

The Italian government has not designated any specific funding or dedicated employees to Critical Infrastructure Protection programs. All CIP-related activities are funded either by the responsible government agencies or infrastructure operators.

HUMAN RESOURCES

Although there is no official CIP agency in Italy, a the Tavolo PIC represents Italy on CIP activities at the international level. The members of the Tavolo PIC hold primary, non-CIP responsibliities in the agencies that have appointed them to the Tavolo PIC, and handle their CIP responsibilities as an additional duty.

16.7 Training & Exercises

In Italy, there is currently no specific university curricula devoted to CIP, although some universities provide post-laurea master studies on security-related issues. For example, the University of Bologna launched a master in *Homeland Security* in 2008. Also, the AIIC is planning to establish a master on *Critical Infrastructure Protection* in 2009.

There are some additional initiatives promoted by universities[478] and research institutes (*inter alia* ENEA[479], Università Campus Bio-Medico, Politecnico di Milano, etc.)

The Department of Civil Protection promotes timely national and local exercises to test the capability of national structure to manage natural or man made disasters. For example, the 2006 MESIMEX exercises (Major Emergency SIMulation EXercise) was designed to evaluate the capability to evacuate the area around the Vesuvio volcano in case of an eruption. It also tested the impact that the eruption would have on electricity and TLC infrastructures. The objectives were to estimate the capability of these infrastructures to provide their service in the area of the crisis and to estimate the impact of their potential failure on the rest of nation.

16.8 Sector – Specific Key Players & Initiatives

ENERGY

Public authorities:

- **Autorità per l'Energia Elettrica e il Gas (AEEG) (Regulatory Authority for Electricity and Gas)[480]**

  The Italian Regulatory Authority for Electricity and Gas is an independent body established under Law 481 of 14 November 1995 to regulate and control the electricity and gas sectors. It is responsible for defining guidelines for the production and distribution of services, as well as monitoring the quality of electricity services

Initiatives:

After the 2003 black-out in Italy, attention surrounding the security of the electricity grid increased considerably. The government updated the national plan for the defence of the electricity system (available at www.terna.it) and the PESSE (the emergency plan for the electricity system). Moreover, Terna (grid operator) has improved its operational and organisational security with the setup of a SOC (security operation centre) and introducing several additional backup facilities.

Terna and Enel (generation, distribution) are also involved in several EU CIP-reltaed projects (e.g., EPCIP-MIA[481]).

[478] One is the master in Homeland Security organised by the University of Bologna with the Nittel (a inter-university consortium) http://www.masterhomelandsecurity.eu/
[479] http://www.progettoreti.enea.it/
[480] http://www.autorita.energia.it/

INFORMATION AND COMMUNICATION TECHNOLOGIES

Public authorities:

- ***Autorità per le Garanzie nelle Comunicazioni (AGCOM)* (Communications Regulatory Authority)**[482]

  The Communications Regulatory Authority is an independent authority responsible for the control of quality and distribution of communication services and products.

- **Postal and Communications Police**

  In 1992, the Ministry of the Interior issued a directive assigning specific responsibilities for IT and telecommunications security to the Postal and Communications Police. The Postal and Communications Police have a staff of around 2,000 highly trained officers, and manage a structure involving 19 regional departments and 76 territorial sections. The Postal and Communications Police reviews communications regulations, studies new technical investigative strategies to fight computer crime, coordinates operations and investigations for other offices, and serves as the Italian point of contact for G8 computer crime offices.

- ***Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA)* (National Centre for Information Technology in Public Administration)**[483]

  The Authority for IT in Public Administration (AIPA), founded in 1993, was transformed into the National Centre for Information Technology in Public Administration (CNIPA) in 2003. It addresses the elements responsible for IT systems in central and local administrations. CNIPA's main task is to promote modern information technologies in the Italian public administration, to establish standards and methods, to deal with security issues, and to make recommendations and technical regulations in the field of IT for public administration. CNIPA published a comprehensive guide on the protection of personal data in 2001. CNIPA also holds the responsibility for managing the SPC (*Sistema Pubblico di Connettività* – Public Connectivity System) which interconnects all Italian public administrations, as well as GovCERT.it[484], the computer emergency response team for the SPC network.

- **Computer Emergency Response Teams (CERTs)**

  GovCERT.it[485]: Managed by CNIPA and devoted to help public administrations to improve their level of ICT security by providing an early-warning service on cyber-threats.

[481] MIA is a project funded by EU Commission DG JLS in the EPCIP framework and devoted to the definition of a methodology for the assessment of mutual interdependencies between ICT and electricity generation/transmission infrastructures http://www.progettoreti.enea.it/mia/
[482] http://www.agcom.it/
[483] http://www.cnipa.gov.it/site/it-IT/
[484] http://www.govcert.it/
[485] http://www.cnipa.gov.it/site/it-it/Attivit%C3%A0/Servizi_per_la_PA/Govcert.it/.

GARR-CERT[486] assists the users of the GARR Network (the Italian Academic and Research Network) in implementing proactive measures to reduce the risk of computer security incidents and in responding to such incidents when they occur.

MoD-CERT[487] is the CERT of the Ministry of Defence that assists its users in protecting ICT networks and disseminates information about ICT security.

Initiatives:

- ***Gruppo di Lavoro sulla Protezione delle Infrastrutture Critiche Informatizzate* (CIIP Working Group)**

  The Italian government established this working group in 2003 within the Department for Innovation and Technologies of the prime Minister's Office with the participation of representatives from public authorities, infrastructure stakeholders, and academia. The Working Group was dissolved in 2006.

- ***Istituto Superiore delle Telecomunicazioni (ISCOM)* (Superior Institue of Telecommunications)**

  In 2005, the institute released a guideline for the security of telecommunication networks that support critical infrastructure[488].

WATER

Public authorities:

- ***Istituto Superiore di Sanità (ISS)* – Superior Health Institute**[489]

  The institute is the leading technical and scientific public body of the Italian National Health Service. Its activities include research, control, training and consultation in the interest of public health protection.

- ***Nucleo Anti Sofisticazioni (NAS)***[490]

  NAS is a special corps of the Carabinieri (national police) devoted to investigating food and beverage tainting and contamination.

Initiatives:

In the 2005, the ISS published a report on the prevention measures to improve the security of aqueducts against terroristic attacks[491].

FOOD

Public authorities:

[486] http://www.cert.garr.it/index-en.html.
[487] http://www.difesa.it/SMD/Staff/Reparti/II-reparto/CERT/default.htm
[488] http://www.infrastrutturecritiche.it/aiic/index.php?option=com_docman&task=cat_view&gid=75&Itemid=98&limitstart=5
[489] http://www.iss.it
[490] http://www.carabinieri.it/Internet/Cittadino/Informazioni/Tutela/Salute/01_NAS.htm
[491] http://www.iss.it/binary/aqua/cont/RappIstisan%2005%204.1204718568.pdf

- ***Istituto Superiore di Sanità (ISS)* – Superior Health Institute**[492]

  The institute is the leading technical and scientific public body of the Italian National Health Service. Its activities include research, control, training and consultation in the interest of public health protection.

- ***Nucleo Anti Sofisticazioni (NAS)***[493]

  NAS is a special corps of the Carabinieri (national police) devoted to investigating food and beverage tainting and contamination.

HEALTH

Public authorities:

- ***Istituto Superiore di Sanità (ISS)* – Superior Health Institute**[494]

  The institute is the leading technical and scientific public body of the Italian National Health Service. Its activities include research, control, training and consultation in the interest of public health protection.

FINANCIAL

Public authorities:

- ***Guardia di Finanza (Finance police*** [495]

  This police corps, under the coordination of the Ministry of the Economy, specialises in financial crimes. It established the *Nucleo Speciale Frodi Telematiche della Guardia di Finanza* (Special Unit for Eletronic Fraud).

Initiatives:

The ABI Lab is the R&D Centre for Technologies in banking, promoted by ABI to support cooperation between banks, ICT companies, and institutions. Born as a special project of ABI Technology & Security Department, in 2002 it was given the legal nature of Consortium and today it is an important centre for research and professional training on technological issues for banking.

SPACE

Public authorities:

- ***Agenzia Spaziale Italiana (ASI)* – Italian Space Agency)**

  The Italian Space Agency came into being in 1988. Its purpose was to coordinate all of Italy's efforts and investments in the space sector that had begun in the 1960s.

[492] http://www.iss.it
[493] http://www.carabinieri.it/Internet/Cittadino/Informazioni/Tutela/Salute/01_NAS.htm
[494] http://www.iss.it
[495] http://www.gdf.it/

Initiatives:

ASI launched, inside the GALILEO frame work, a program to analyse the impact of the failure of satellite communication and positioning system on the national critical infrastructures[496].

RESEARCH FACILITIES

Public Authorities:

- ***ENEA***[497]

  ENEA is a public agency operating in the fields of energy, environment, and new technologies to support Italy's competitiveness and sustainable development. This agency also focuses on CIP matters and is heavily involved in several EU-funded CIPS projects.

Initiatives:

ENEA has a strategic project on CIP titled “Progetto governo e sicurezza delle reti tecnologiche ed energetiche” (project for the governance and the security of technological and energy networks)[498]. This project aims to develop innovative tools and methodologies to improve the capability to manage and protect the different critical infrastructures taking into account their interdependencies.

[496] http://www.asi.it/it/flash/navigazione/lasi_e_il_programma_galileo
[497] http://www.enea.it
[498] http://www.progettoreti.enea.it/index.htm

17 Latvia

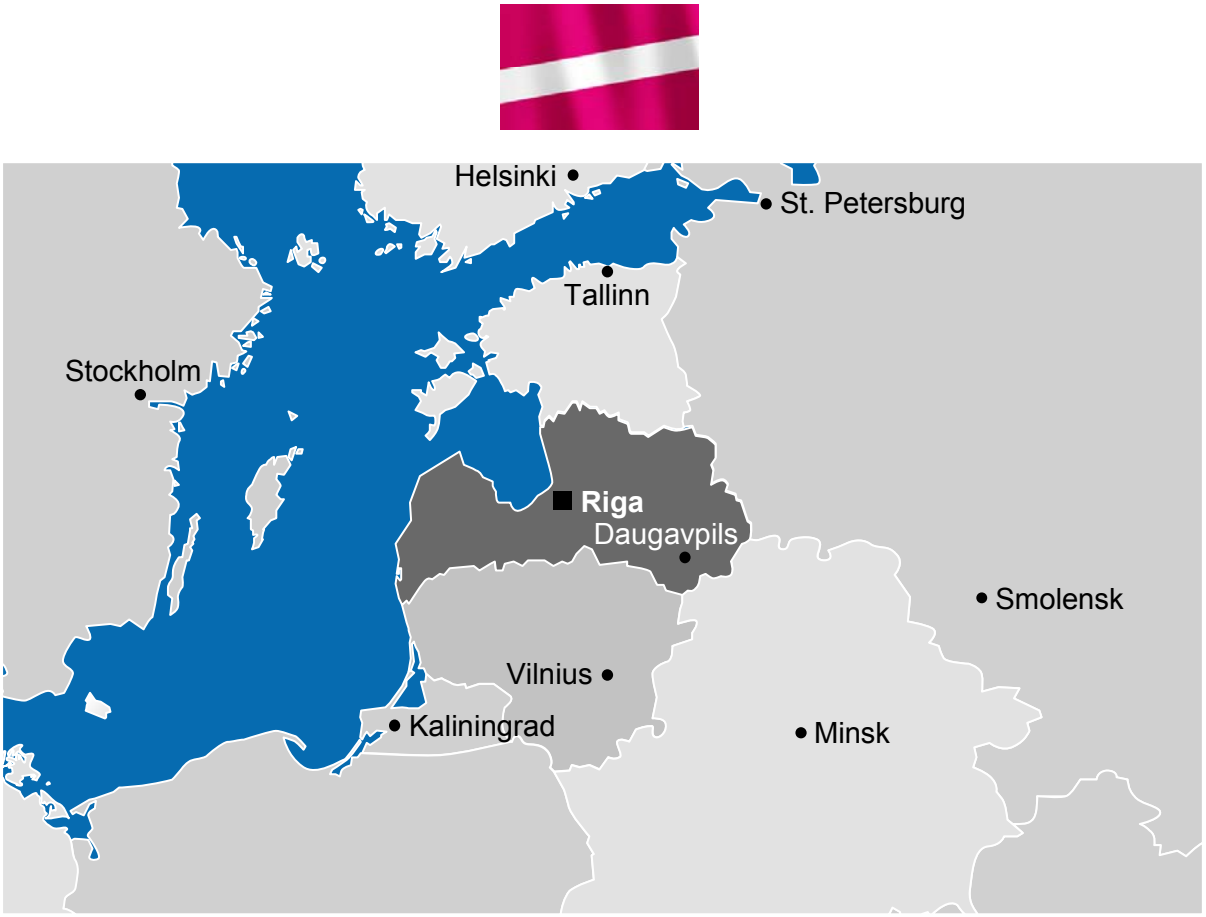


Figure 71: Latvia

17.1 Summary

	Organisational Model	Strategy & Policy	Methodology & Standards	Public-Private Partnership and International Collaboration	Funding & Human Resources	Training & Exercises	Sector-Specific Key Players & Initiatives
Latvia	▪ No specific CIP-related organisational model available	▪ Security Measures Planning and Implementation Procedure of Important Facilities for National Security in place	▪ Not Applicable	▪ NATO Senior Civil Emergency Planning Committee ▪ UNECE Convention	▪ No funding from public authorities and sources outside the country	▪ UUSIMAA 2008	▪ Not Applicable

499

The Latvian Cabinet of Ministers approved a regulation titled “Security Measures Planning and Implementation Procedure of Important Facilities for National Security”, developed by the National Security Intersectoral Commission. [500]

The implementation of this is complete, and this procedure covers all sectors strategic to CIP.[501]

[499] Not Applicable = Open Source Research, Web-based survey and individual interviews have not shown information/data on the given argument
[500] http://www.likumi.lv/doc.php?id=177273
[501] Booz & Company survey “Stock-taking of Existing Critical Infrastructure Protection Activities”

17.2 Organisational Model

Figure 72: Organisational Chart (only CIP-related agencies shown)

The Security Policy Department is one of the key agencies involved in CIP in Latvia.[502]

The structure of Latvian Civil Emergency Planning (CEP) changed radically in the summer of 1998 when amendments were made to the Civil Protection Law[503]. In particular, the main tasks of CEP were delegated to the State Fire and Rescue Service (SFRS). This law defines Civil Protection of the Republic of Latvia as a system of technical, economic, social and rescue measures created to fulfil the obligations of the State. It is aimed at protecting the civilian population, economic activities and the environment from the dangers and damages caused by potential emergencies.

The Prime Minister is responsible for the continuous function of the system and the fulfilment of its obligations. Civil protection operations are planned, coordinated, led and controlled by the SFRS, under the Ministry of the Interior. At the national level, responsibility for civil emergency planning rests with the SFRS. The local chief of Fire and Rescue Services is responsible at the municipal level. The local fire chief reports directly to the chief of SFRS.

[502] Booz & Company survey "Stock-taking of Existing Critical Infrastructure Protection Activities"
[503] http://www2.112.lv/en/content/view/233/164/

The main tasks of Latvian civil protection are:

- to provide assistance to victims;
- to reduce losses;
- to ensure economic stability in hazardous situations, and
- to ensure that State authoritative and administrative institutions, the economy and the population are prepared for situations caused by emergencies

Existing legal arrangements are concentrated on military support to civil authorities in peacetime emergencies. The formalisation of civil support to military activities is currently at an initial stage and requires further work to develop complete legal acts and regulations. The National Security Law[504] (20 December 2000) attempts to regulate such civil military cooperation. One of its important roles is to define the National Security Council and the Crisis Control Council.

National Security Council

The National Security Council[505] coordinates Latvian policy for national security, which are then implemented by state institutions and officials. It examines and reviews plans and concepts related to national security.

The members of the National Security Council are:

- The State President
- The chairperson of the Saeima
- The chairperson of the National Security Committee of the Saeima
- The chairperson of the Defence and Interior Affairs Committee of the Saeima
- The Prime Minister
- The Minister of Defence
- The Minister of Foreign Affairs
- The Minister of the Interior

Crisis Control Council

In the event of a threat to the State, the Crisis Control Council[506] coordinates civil-military co-operation and the operational activities of state administration. The legislation governing the operation of the Crisis Control Council is approved by the Cabinet of Ministers. The Council is headed by the Prime Minister and its members are the following:

- Minister of Defence
- Minister of Foreign Affairs
- Minister of Economics
- Minister of Finance

[504] http://www.mfa.gov.lv/en/security/basic/4536/
[505] http://www.am.gov.lv/en/security/basic/4536/
[506] http://www.am.gov.lv/en/security/basic/4536/

- Minister of the Interior
- Minister of Justice
- Minister of Health

The roles of the Crisis Control Council are to:

- Coordinate the operational response to national dangers;
- Coordinate the development of danger prevention plans by state administration institutions;
- Produce proposals to be submitted to the Cabinet of Ministers for changes and improvements to the national defence system;
- In case of the danger to the State, coordinate the integrated and timely implementation of political decisions in the state administration institutions.

Civil Defence Centre

The Civil Defence Centre[507] is a national level emergency management agency responsible for:

- Developing, exercising and maintaining the national emergency preparedness plan.
- Providing overall coordination of the planning process at the national and district/city level.
- Alerting, notifying and providing information to the public on the national level.
- Coordination of emergency response at the national level.
- Providing for uninterrupted and reliable functioning of the emergency communication.
- Coordination of international assistance.
- Organisation of radiation and nuclear emergency exercises at the regional and national levels, civil defence training of the population and the staff of the governmental and local authorities, enterprises and organisations.

Ministry of the Environment (Latvijas Republikas Vides Ministrija)[508]

The Ministry of Environment is a central executive institution in the area of environmental protection whose responsibilities include protection of environment and nature, maintenance and rational utilisation of natural resources, and hydrometeorology and the use of subsoil. The Ministry defines the national environmental protection policy and coordinates its implementation.

The Ministry of the Environmental Protection and Regional Development is responsible for

- early radiation warning;
- environmental radiation monitoring;
- assessment and forecasting of the metereological and radiation situation;
- recommendations of protective measures to be undertaken, and

[507] http://www2.112.lv/en/content/view/233/164/
[508] http://www.vidm.gov.lv

- exchange of information with other countries and international organizations.

Ministry of Welfare (Latvijas Republikas Labklājības Ministrijas)[509]

This Ministry of Welfare is responsible for:

- Generating proposals for new equipment for medical, emergency response and rescue services personnel.
- Development of a data base on the supplies of medical resources in health institutions and developing proposals on the necessity to change or supplement the existing state reserves of the medical materials and equipment.
- Provision of emergency and specialist medical aid to the victims of radiation and nuclear accidents.
- Coordination of the preventive stable iodine treatment and social care.
- Hygienic and epidemic control during the deployment of emergency response services personnel, casualty treatment sites, and evacuees temporary accommodation.
- Long-term population and environmental health monitoring.
- Compilation of a register of radiation and nuclear accident victims.
- Evaluation of the radiation doses received by victims.

Ministry of Health (Latvijas Republikas Veselības Ministrija)[510]

The Ministry of Health was established on 1 February 2003. Until that time the leading institution in health sector was Ministry of Welfare. Currently, the Ministry of Health is the leading governmental institution in the health sector and is responsible for public health, health care, pharmacy and legal distribution of drugs. The main task of Ministry of Health is to develop and implement state policy by ensuring public health, a healthy environment, promoting prevention, popularising healthy life style, as well as by creating conditions where the inhabitants benefit from cost effective, physically accessible, and high-quality health care services.

Ministry of Transport (Latvijas Republikas Satiksmes Ministrija)[511]

The Ministry of Communication ensures the reliable functioning of existing communications systems, provide additional communication means, coordinates the means of transportation during evacuations.

Ministry of Defence (Latvijas Republikas Aizsardzības Ministrija)[512]

The Ministry of Defence is responsible for public works, decontamination, maintenance of public order, and the safeguarding of public and private property during and after an evacuation.

Ministry of Interior (Iekslietu Ministrija)[513]

509 http://www.lm.gov.lv/
510 http://www.vm.gov.lv/
511 http://www.sam.gov.lv/satmin/content/?lng=en&cat=134
512 http://www.am.gov.lv
513 http://www.iem.gov.lv

The Ministry of Interior manages fire-fighting and rescue, maintenance of order in public places, guarding of contaminated areas, safeguarding public and private property in the course and after evacuation, registering of evacuees, decontamination, overseeing the transit of radioactive materials, and preventing the their illegal transportation.

17.3 Strategy & Policy

In 2008, the Latvian Cabinet of Ministers approved a regulation titles “Security Measures Planning and Implementation Procedure of Important Facilities for National Security”. This was developed by the National Security Intersectoral Commission and it provided guidance for sectors important to CIP.

The National Security Intersectoral Commission also prepared a list of Important Facilities for National Security[514].

The basic legal act regulating security operations during a crisis is the National Security Law[515], which contains the National Security Plan and the Civil Protection Plan. It defines the necessary competence and the responsibilities of national security entities.

In the development of a national security policy, Latvia’s governments have focused on regional co-operation and European integration. Latvia sought membership in NATO in order to add its contribution to the formation of a fully integrated Euro Atlantic security policy. At the same time, Latvia has built a special relationship with the United States in order to strengthen the trans-atlantic dimension of its security policy.

17.4 Funding & Human Resources

No explicit funding for CIP-related activities by public agencies nor by sources external to the country was identified by this study.[516]

17.5 Public – Private Partnership & International Collaboration

The State Fire and Rescue Service represents Latvia in:

- European Union institutions (in Civil Protection Committee under European Commission's Environment Directorate-General and in Civil Protection Working Group (PROCIV) of the Council of the European Union);
- NATO Senior Civil Emergency Planning Committee (SCEPC)[517] and Civil Protection Committee (CPC)[518];
- International Association of Fire and Rescue Services (CTIF)[519]

514 514Booz & Company survey “Stock-taking of Existing Critical Infrastructure Protection Activities”
515 http://www.am.gov.lv/en/security/basic/4536/

517 http://www.nato.int/issues/scepc/index.html
518 http://www.nato.int/docu/logi-en/1997/lo-1107.htm
519 http://www.ctif.org/

- UNECE Convention on Protection and Use of Transboundary Watercourses and International Lakes[520]

The Operational Department of State Fire and Rescue Service is the point of contact for:

- The European Commission Monitoring and Information Centre (MIC)[521]
- NATO Euro-Atlantic Disaster Response Co-ordination Centre (EADRCC)[522]
- United Nations[523]:
  - Office for Coordination of Humanitarian Affairs (OCHA)[524];
  - ECE Convention on the Trans boundary Effects of Industrial Accidents[525]

17.6 Training & exercises

There is no specific CIP-related training activity scheduled[526].

Latvia participates in the annual NATO Baltic Sea central region search and rescue exercise *Bold Mercy*[527]. The main aim of the exercise is to test the effectiveness of co-operation between the search and rescue co-ordination centres of Latvia (co-operation of Ministries of Defence, Interior, Transport and Health with representatives of local municipalities), and those in Great Britain, France, Poland, Lithuania, Latvia, Estonia and Sweden.

A consequence management field exercise UUSIMAA-2008[528], organised by the Euro-Atlantic Disaster Response Coordination Centre (EADRCC) in co-operation with Finland, the host nation, was conducted in Helsinki in June 2008. More than 1000 participants representing 37 nations took part in the exercise. The lead-in scenario for the exercise was flood and storm along the coastline of Gulf of Finland. Water level rose during the spring and the storm damaged some of the national critical infrastructure. Flooding caused several chemical, biological and nuclear threats to the environment and the population of the capital area. The exercise focused on consequence management and cooperation between different organisations and agencies.

17.7 Sector – Specific Key Players & Specific Initiatives

ENERGY

Public authorities:

- ***Public Utilities Commission (Sabiedrisko pakalpojumu regulēšanas komisija-SPRK)[529]***

[520] http://www.unece.org
[521] http://ec.europa.eu/environment/civil/prote/mic.htm
[522] http://www.nato.int/eadrcc/index.html
[523] http://www.un.org/index.html
[524] http://ochaonline.un.org/
[525] http://www.unece.org/env/teia/english/x1.htm
[526] Booz & Company survey "Stock-taking of Existing Critical Infrastructure Protection Activities"
[527] http://www.am.gov.lv/en/news/DomesticNews/2007/may/11-2/
[528] http://www.nato.int/eadrcc/2008/06-uusimaa/070618.htm
[529] http://www.sprk.gov.lv

The Public Utilities Commission (PUC) is an independent state institution responsible for the regulation of energy, telecommunications, post and rail in accordance with the law "On Regulators of Public Utilities" and the corresponding normative acts in the regulated sectors. Public utilities (electricity, gas, heat supply, telecommunications, water supply, sewerage and railway) are often characterised by natural monopolies. In Latvia these services are provided by historically established monopolies. Although the market of public utilities is gradually liberalised and new players enter some sectors, the large enterprises still dominate. Therefore a unified public utilities regulation system on central and local government levels was established in autumn 2001. Utilities in the state-regulated sectors, namely, energy (except heat supply), telecommunications, post and railway are regulated by the Public Utilities Regulation Commission, while household waste management, water supply, sewerage and heating industries are regulated on local government level by institutions established by the respective municipalities.

INFORMATION AND COMMUNICATION TECHNOLOGIES
Public authorities:

- ***Latvian State Department of Communications - Ministry of Transport (Latvijas Republikas Satiksmes Ministrija)***[530]

  The Latvian State Department of Communications is a branch of the Ministry of Transport, and manages electronic communications and the post.

- ***Latvijas Televīzija***[531]

  Latvijas Televīzija is the state public television broadcaster.

FINANCIAL

Public authorities:

- ***The Bank of Latvia (Latvijas Banka)***532

  The Bank of Latvia is the central bank of the Republic of Latvia. It is responsible for the nation's payment and securities settlement systems. The objectives of the Bank of Latvia's business continuity management are to identify potential threats that may affect the Bank's objectives and jeopardise the fulfilment of its tasks, and establish and implement a set of measures to ensure protection of the Bank against such threats. The Bank of Latvia has identified the functions whose forced discontinuity may cause an emergency situation and endanger the execution of the Bank's critical functions. They have also specified also the maximum permissible periods of discontinuity and the resources critical to these functions. On a regular basis, the Bank of Latvia's management reviews and assesses the list of functions and critical resources as well as the adequacy and availability of the resources for ensuring the continuity of the Bank's operations in case of emergency.

  In the field of business continuity management, the following documents have been developed at the Bank of Latvia:

530 http://www.sam.gov.lv/satmin/content/?lng=en&cat=134
531 http://www.ltv.lv
532 http://www.bank.lv

- Regulations governing the organisational procedures for the business continuity management process and the procedures for incident, emergency situation and crises management.
- Business continuity action plans that stipulate an ongoing maintenance of critical functions and availability of critical resources and provide for an execution of preventive measures to ensure an uninterrupted maintenance of critical functions
- A secondary site provision plan that stipulates the location and equipment of the secondary site for the staff involved in the implementation of critical functions, management of incidents, critical incidents and emergency situations, should their primary site be unavailable in case of incidents or critical incidents

At the Bank of Latvia, the business continuity action plans are tested and updated on a regular basis and a plan for organizing training in the field of business continuity and testing thereof has been devised for the current year.

Latvian Central Depository[533]

Latvian Central Depository (LCD) provides securities custody, clearance, settlement and information services in Latvia. LCD also maintains state funded pension system. The Latvian Central Depository (LCD) of securities has been admitted to the Euroclear international securities settlement and depository system. The LCD plans to begin actual operations within the Euroclear system soon.

TRANSPORTATION

Public authorities:

- ***Ministry of Transport (Latvijas Republikas Satiksmes Ministrija)***[534]

  The transport sector includes railways, road traffic, maritime and aviation, as well as, passenger carriage and transit branches. Road transport and traffic safety are under the responsibility of the road traffic branch.

RESEARCH FACILITIES

Public authorities:

- ***Ministry of Education and Science (Latvijas Republikas Izglītības un Zinātnes Ministrijas)***535

  The Ministry develops and implements policy in the fields of education, science, sports and language, promoting the sustainable growth of the welfare of the citizens of Latvia as educated, healthy, physically and mentally developed personalities, and integrity of the society of Latvia. The Ministry strengthens and ensures the provision of information to the public, explanation of government resolutions, and is the main link between the government and society in implementing transparent administrative process best practice.

Main operators:

[533] http://www.lcd.lv/
[534] http://www.sam.gov.lv/satmin/content/?lng=en&cat=134
[535] http://izm.izm.gov.lv/

- ***Institute of Nuclear Physics, Salaspils***536

  The Institute of Nuclear Physics was founded in 1946 as the Institute of Physics and Mathematics of the Academy of Sciences. Until 1990 the Institute was a multi-disciplinary research institution. Reorganisation took place in 1991-1993 and laboratories for solid state physics, nuclear physics, theoretical physics and mathematics were incorporated within other research institutions. Since 1994 the Institute has been a research centre specialising in problems of magnetohydrodynamics as well as heat and mass transfer.

536 http://iph.sal.lv/fi/netscape/index.htm

18 Lithuania

Figure 73: Lithuania

18.1 Summary

	Organisational Model	Strategy & Policy	Methodology & Standards	Public-Private Partnership & International Collaboration	Funding & Human Resources	Training & Exercises	Sector-Specific Key Players & Initiatives
Lituania	▪ No specific CIP-related organisational model available	▪ CIP strategy and law and currently under development ▪ Possible solutions are being developed by a working group	▪ Emergency plans available regarding Nuclear, Fire and Natural Disasters	▪ Bilateral and multilateral treaties are in place	▪ No funding from public authorities and sources outside the country	▪ Yearly trainings involving Police, Civil Protection and Private Operators	▪ No specific CIP-related initiatives in place

537

In Lithuania there is not yet a specific law on CIP. Alternative solutions are under development by a working group, but still at an early stage. One of the objects of working group is to decide how to implement CIP regulation - to integrate CIP into existing national law or to develop a new law only for CIP[538].

Lithuanian Critical Infrastructure Protection is currently managed by the armed forces as specified in the "Main Directions of the Lithuanian Defence Policy"[539]: *"… provide assistance to state and municipal institutions by responding to threats of a non-military nature – support the institutions of Interior Affairs System, protect critical infrastructure, implement search and rescue, medical evacuation tasks, de-mining of the territory of Lithuania.."*

Lithuanian Republic Law on civil protection (15th December 1998) establishes the legal and organisational principles of Lithuanian civil protection and rescue system organisation and operation, and the duties and rights of state and municipal institutions, economic entities, public organisations and residents.

[537] Not Applicable = Open Source Research, Web-based survey and individual interviews have not shown information/data on the given argument
[538] Booz & Company survey "Stock-taking of Existing Critical Infrastructure Protection Activities"
[539] http://www.kam.lt/index.php/en/188824/

18.2 Organisational Model

The Ministry of Foreign Affairs[540] is the central institution of the Republic of Lithuania implementing Lithuania's foreign policy[541] and co-ordinating the activities of other public institutions in the foreign policy field. The mission of the Ministry is to represent the legitimate interests of the Republic of Lithuania and its citizens in international organisations and worldwide.

Ministry of National Defence (The Lithuanian Armed Forces)[542]

The Ministry of National Defence is responsible for combat forces, search/rescue, and intelligence operations. (I had moved this info little bid up as Fire and rescue department is under the Ministry of Interior)

The Ministry of Interior[543] exercises public administration functions in the field of public safety, state border protection, state aid during emergencies and civil protection, control of migration processes, reform of the public administration and state governance system, development of local governance, regional development, creation of civil service system, IT and other fields attributed to the Ministry.

The mission of the Ministry is to serve the society, guarantee its safety, build an efficient and professional public administration based on information technologies, and create the conditions for sustainable regional development. Its strategic goals are:

- Implementation of public safety policy.
- Optimising the public administration system based on a professional civil service, and the development of an information and knowledge society.
- Creation of state border control and migration processes management systems in conformity with the requirements of the European Union and Schengen Treaty.
- Creation of conditions for sustainable regional development.

Subdivisions directly subordinated to the Ministry include:

- Klaipėda Police school
- Transport Service; State Enterprise "REGITRA"[544]
- State Enterprise "Infostruktūra"[545] State Institute of Information Technologies[546]
- Training Centre "Dainava" for Public and Municipal Servants

[540] http://www.urm.lt/index.php?405195998
[541] Lithuanian Foreign Policy Review http://www.lfpr.lt/index.php?id=54
[542] http://www.kam.lt/armed_forces/
[543] http://www.vrm.lt/index.php?id=124&lang=2
[544] http://www.regitra.lt/index.php?Action=en_about_us&lang=en
[545] http://www.infostruktura.lt/
[546] http://www.viti.lt/index.php?lang=en

- Lithuanian Institute of Public Administration
- Fire and Rescue Department (under the ministry of the Interior)[547]
- The State Fire and Rescue Service

The State Fire and Rescue Service

The State Fire and Rescue Service is comprised of the following bodies: the Fire and Rescue Department of the Republic of Lithuania under the Ministry of the Interior (the FRD) and its 17 subordinate services – 10 countys Fire and Rescue Boards, 3 Fire and Rescue Services for the protection of strategic establishments, the Specialised Fire and Rescue Service, the Fire-fighters Training School, the Fire Research Centre and the Emergency Response Centre.

Three Lithuanian establishments are considered to represent a high risk - *Mažeikių Nafta* (Mazeikiai oil refinery), the Lithuanian Power Plant, and the Ignalina Nuclear Power Plant. The fire and rescue services are responsible for the fire safety and fire supervision within these establishments, and are contracted for the purpose. These services are stationed close to the high-risk facilities to ensure high levels of fire safety there, and to carry out rescue operations. Their presence reduces both risks to people and damages to the infrastructure. These fire & rescue services are partly or fully financed by these companies.

Fire and Rescue Department[548]

The Fire and Rescue Department (FRD) (under the Ministry of the Interior) is responsible for the protection of people, property and the environment in case of emergencies. In addition, it is in charge of fire and emergency prevention. The FRD is responsible for:

- Determining the national policy for fire and civil protection.
- Developing strategies for its subordinate services.
- Developing fire and civil protection legislation and overseeing its enforcement.
- Undertaking the prevention and management of emergencies.
- Providing guidance to public institutions,businesses and the public in civil protection.
- Coordinating fire and civil protection training, and encourage NGO's and volunteer organisations contribute to fire protection.
- Recording fire and rescue statistics.

The FRD is in charge of responding to major accidents and rescuing people and property. The FRD administers the **Population Warning and Information System P–160**, which serves to warn the population in case of emergencies.

[547] http://www.vpgt.lt/index.php?-30969458
[548] http://www.vpgt.lt

The FRD manages civil protection exercises at national level, and the preparedness of state institutions and the community for emergencies.

The FRD manages the state stockpile of the civil protection resources. It allocates these and assists state and municipal institutions, businesses and population prepare for emergencies.

In order to gather relevant information on dangerous industrial and business enterprises in the country, the FRD maintains the **Central Database Register of Objects of State Significance and Dangerous Establishments**.

Police Department (under the Ministry of the Interior)[549]

The Police Department works for the Police Commissioner General to develop a number of strategies and manage their implementation. The Police Department is also responsible for managing local police branches. Local police branches are defined as police offices located in the community that are responsible for executing certain functions defined by the law. Special police offices are those police branches founded according to a non-territorial principle. They execute functions defined by the law for this type of police department. Educational police institutions are police training institutions established by the Police Commissioner General to ensure the continuous training and professional, in-service development of police officers.

Public Security Service[550] ().

An element of the Ministry of Interior, the tasks of the Public Security Service are:

- To ensure public order during extraordinary situations and emergencies.
- Within its sphere of competence, to eliminate the hazards to human life or health and property during extraordinary situations and emergencies.
- To transport persons detained, arrested and convicted.
- To ensure the protection of important state objects.
- To search for persons.
- To strengthen the forces of the Lithuanian police, the State Border Guard Service under the Ministry of the Interior, the Fire and Rescue Department under the Ministry of the Interior, the VIP Security Department under the Ministry of the Interior, the Financial Crime Investigation Service under the Ministry of the Interior and to assist these institutions in implementing the functions assigned to them.
- To defend the State in case of war; to perform other tasks assigned to the Service by law.

Ministry of Transport and Communications[551]

Ministry of Transport and Communications administers the nation's transportation systems (air, water, railway, and road transport), post and electronic communications, and implements State policy in these areas.

[549] http://www.policija.lt/En/
[550] http://www.vstarnyba.lt/en/index.php
[551] http://www.transp.lt/Default.aspx?Element=ViewArticles&TopicID=2&Lang=EN&UL

18.3 Strategy & Policy

In Lithuania there is not yet any specific law on CIP. Such solutions are under development by a working group, and one of the objects of the working group is to decide how to implement CIP regulation - to integrate CIP into existing national law or to develop a new law only for CIP.

This new law/policy's scope should include a series of sectors: electricity, oil, gas, transport and possibly others.

The expected timeline to begin the implementation is approximately 13-24 months and it should be completed in 5 years[552].

The Republic of Lithuania Law on the Public Security Service[553] (19 September 2006 No X-813 – Vilnius)

This Law establishes the purpose of the Public Security Service, which operates under the Republic of Lithuania Ministry of the Interior. It provides its legal basis and the principles of its activities, the tasks, functions, structure and funding of the Service, control of its activities, the general framework for co-operation with state or municipal institutions and agencies as well as other persons, powers, rights, duties and liability of Service officers as well as conditions of lawfulness of the use of coercion.

Defence Policy of Lithuania[554]

Lithuanian Defence Policy refers to the principles and provisions of national security protection described in the National Security Strategy of the Republic of Lithuania. National security protection is seen as unity of territory and the retention sovereignty, maintenance of internal security and order, maintenance of a democratic constitution, economic security, and protection of the national natural environment and cultural values.

National security is the basis of a country's welfare and prosperity. Only by ensuring national security the country can create appropriate conditions for the growth of the economic, social, and cultural potential of its society. "Secure country means prosperous society" is a saying describing the significance of national security. Among the various means of Lithuanian domestic and foreign policy for national security protection, military defence is especially important. The principal provisions for national defence are defined in the Strategy of Military Defence of Lithuania.

The purpose of Defence Policy is to create a secure international environment and prepare an effective strategy for the country's military defence, and the preplanning necessary for its implementation. Lithuania believes that cooperation is essential to ensure an effective response to threads emerging from beyond the country-borders.

[552] Booz & Company survey "Stock-taking of Existing Critical Infrastructure Protection Activities"
[553] http://www.vstarnyba.lt/en/index.php?id=128
[554] http://www.kam.lt/index.php/en/122183/

Traditionally, military defence has been understood as a nation's defensive response to the aggression of a hostile country. The essence of military defence conception remains unchanged. However, non-tradition threats, such as terrorism and natural disasters, ignore traditional country borders and demand coordination of government actions, resource pooling on an international and national scale, and the ability to employ military forces in non-traditional ways. Objectives of defence policy are to ensure:

- National defence through a readiness to defend sovereignty, territorial integrity, a democratic constitutional system of government, and human rights and liberties, in case of military assault
- Response to threats of a non-combat character by providing military assistance to government and municipal institutions, and to contribute to the effective operation of a crisis management system.
- International stability and peace by a readiness to contribute to regional and global stability operations and peace support, including participation in international operations.

Development Strategy of the Broadband Infrastructure of Lithuania for 2005-2010[555]

The strategy goals are as follows:

- to facilitate access for public administration institutions, bodies and individuals to broadband access;
- to promote market competition in Internet access provision using public and private capital investments, and
- to positively influence national social and economic growth, and
- to ensure citizens in regional areas are not excluded from gaining access.

State Programme for Road Safety for 2005–2010[556]

The State Programme for Road Safety for 2005-2010 (approved by resolution of the Government No. 759 of 8 July 2005) aims to produce a targeted long-term improvement of road traffic safety. It will do this by identifying and implementing measures to reduce road accident rates, and achieving the target set for the EU, halve the number of road accident casualties by the year 2010.

The programme also provides for improvement of driver training and examination, pedestrian and cyclists safety, traffic culture, education of motorists, traffic control, medical aid and rescue services. In the area of road infrastructure, the causes of accidents in urban and rural road sections with highest accident rates are to be eliminated and a road safety audit system is to be established.

Strategy for the Development of Lithuanian Postal Sector for 2004 – 2008 (summary)[557]

[555] http://www.transp.lt/Default.aspx?Element=ViewArticle&Lang=EN&TopicID=215&ArticleID=1936
[556] http://www.transp.lt/Default.aspx?Element=ViewArticle&Lang=EN&TopicID=215&ArticleID=1651
[557] http://www.transp.lt/Default.aspx?Element=ViewArticle&Lang=EN&TopicID=215&ArticleID=1652

The Strategy for the Development of the Lithuanian Postal Sector for 2004-2008 was developed mindful of changes in the global postal sector. The strategy establishes the main objectives and targets for the sector for a five-year period. The formulation of the strategy involved an analysis of the national postal sector and of the political, economic, social and technological factors influencing development of the sector. An analysis of development disparities between Lithuania and other EU Member States has also been undertaken.

The National Energy Strategy approved by Seimas of the Republic of Lithuania resolution[558]

The National Energy Strategy (the Strategy) defines the main targets set by the State and directions for their implementation until 2025 by fully adjusting these targets and directions to growing state needs and the most recent international requirements, having regard to the aspects of efficiency, energy security, environmental and management improvement. The Strategy specifies the ways and means of ensuring the strategic security of energy supply, reducing or neutralising the negative impact of dependence on the dominant supplier of primary energy. A fast development of Lithuania's economy, growing dependence on the import of primary energy from a single country, the envisaged decommissioning of the Ignalina Nuclear Power Plant (hereinafter referred to as the "Ignalina NPP") in 2009, substantially increased prices of fossil fuel in world markets and the tension present in them render changes in Lithuania's energy policy and updating of the National Energy Strategy as approved by Resolution of the Seimas No IX-1130 of 10 October 2002 (*Valstybės žinios*, No 99-4397, 2002).

18.4 Methodologies & Standards

Emergency plans in Lithuania are mainly related to nuclear accidents, fire and natural disasters. Some examples include:

- *Emergency Preparedness Organisation and Principles for Protection of the Public* in case of nuclear disasters (nuclear energy emergency preparedness plan)[559]
- Fire and rescue department emergency plans are publicly available on the department web site[560]
- **Ignalina** Nuclear Power Plan safety and quality policy[561]

Lithuanian Republic Law on **nuclear energy** (14th November 1996) prescribes responsibilities to relevant institutions for nuclear accident prevention and management.

Lithuanian Republic Law on **radiation protection** (12th January 1999) regulates sources of ionising radiation and radioactive waste management. It establishes the legal basis of radiation protection to safeguard people and the environment from the harmful effects of ionising radiation.

[558] http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=292522
[559] http://www.lei.lt/insc/handbook/part6.pdf
[560] http://www.vpgt.lt/index.php?59240261
[561] http://www.iae.lt/inpp_en.asp?lang=1&subsub=1

18.5 Funding & Human Resources

In the last three years (2006-2008) no funding was made available for CIP-related programmes from public authorities and sources outside the country.

At present, there are no public employees employed in CIP-related activities.

18.6 Training & Exercises

Typically, police enforcement, civil protection and private operators are involved in annual exercises.

The civil protection training and practices order is approved by Lithuanian Republic Government decision No. 111 on 1st February 2000. In the decision it describes the trainings and exercises to be undertaken, trainings and exercises planning, conduct, periodicity, duration and sponsorship.

Civil Protection Exercise: Accident at Ignalina Nuclear Power Station

On 23-24 October 2001, the Civil Protection Department conducted an exercise entitled "Evacuation of the population in case of the accident at Ignalina Nuclear Power Station". The exercise scenario was as follows:

There is an accident at the Ignalina Nuclear Power Station. Subsequently, levels of radioactivity are detected which are far in excess of the accepted safety margins. Also, accident damage has resulted in radioactive pollution spreading beyond the security zone of the nuclear power station. The exercise will involve not only the Civil Protection Department, but also officials from the Ministry of National Defence (including Deputy Ministers), Civil Protection Departments of the Districts of Utena, Vilnius, Panevëþys and Kaunas, and the Zarasai Region Municipality. Representatives from the Ministries of Environment, Transport, Health, Economy, and Agriculture will also take part, along with Fire Prevention and Rescue personnel from the Ministry of Interior, and the State Food and Veterinary Service.

The Lithuanian Great Duke Algirdas Mechanised Infantry Battalion and the Nuclear Power Safety State Inspectorate will also practise their roles during the exercise. This exercise would assist in developing the level of preparedness of central and municipal institutions with responsibility for organising and implementing evacuation of the population in case of a serious radiation accident at the nuclear power station. In particular, the exercise would be a valuable test of the effectiveness of the working relationship between the Utena District Administration with the Lithuanian Great Duke Algirdas Mechanised Infantry Battalion in case of an emergency situation. The main purpose of the exercise is to test the response of the exercise participants to the challenge of participating in joint activities, in accordance with plans for the protection of Lithuania's population in a potential accident situation at Ignalina. During the exercise, preparation for implementation of the regulations of the Decision of the Government of the Republic of Lithuania on " Procedure for evacuation of the population" would also be examined. This would also be an opportunity to rehearse the effectiveness of the Zarasai Region Municipality's evacuation plans, including the setting up of collection

points for members of the public to report to, and intermediate evacuation arrangements. Military personnel from the Algirdas Mechanised Infantry Battalion will be given the chance to examine their skills in installing and maintaining a mobile sanitary cleaning point at the intermediate evacuation point.

18.7 Sector – Specific Key Players & Initiatives

ENERGY

Main Operators:

Electricity sector:

- **Lietuvos Energija AB**[562]

  Lietuvos is the single electricity transmission system operator in Lithuania - it maintains and develops the transmission grid, ensures electricity transmission and reliable operation of the power system, and facilitates trade in electricity in an open market.

- **Rytų skirstomieji tinklai AB (Eastern Distribution Networks)**

  In the national electricity market, Rytų skirstomieji tinklai AB performs the functions of a distribution network operator and a public supplier. The company is in charge of maintenance, reliability and development of low (0.4 kV) and medium (35-10 kV) voltage electricity networks, as well as of electricity supply to the customers within the territory being served.

- **VST AB**

  VST is focused on distributing and supplying electric energy and providing services to customers in the Western and Central Lithuania. The company is the owner of the electric power distribution network, i.e. the overhead lines and cable lines of low and medium voltage, as well as the owner of more than 16,000 transformer substations. The company is responsible for power distribution networks in Kaunas, Klaipėda and Šiauliai regions, and also for safety, reliability, operation, maintenance, management and development of the network.

Gas sector:

- **AB Lietuvos Dujos**

  The company activities are natural gas purchase (import), transmission, distribution, and sales. The company owns the absolute majority of the natural gas supplies infrastructure in Lithuania.

NUCLEAR

Main Operators:

- ***State Enterprise Ignalina***[563] [564]

[562] http://www.lpc.lt/en

In 1996 and 1997 the Ignalina Nuclear Power Plant generated 85.8 and 81.3 percent of the country's electricity respectively.

INFORMATION AND COMMUNICATION TECHNOLOGIES

Public Authorities:

- ***The Communications Regulatory Authority[565] of the Republic of Lithuania***

  The Communications Regulatory Authority (RRT) is an independent national institution regulating the communication sector in Lithuania. It was established under the Law on Telecommunications and the provisions of the European Union Directives. One of the main purposes of the RRT is to promote competition in the electronic communications and postal sectors. The RRT's mission[566] is to provide a variety of technologically progressive, top quality, safe and affordable information and communications technologies (ICT) and postal services/products to Lithuanians. It also seeks to create favourable conditions for ICT and postal business development, promoting the progress of an information and knowledge rich society.
  The activities undertaken by the RRT include:

  – the promotion of competition in electronic communications and postal markets[567];
  – the regulation of the electronic communications and postal sectors;
  – management and supervision of the radio spectrum
  – surveillance of telecommunication and radio communication terminal equipment;
  – the management and supervision of telephone numbers and other identifiers of networks, and
  – the protection of consumers' rights

- ***CERT-RRT*** [568]

  The mission of CERT-RRT is to prevent and manage security incidents in Lithuania's public electronic communications networks, investigate the incidents, and coordinate their elimination. Key areas of activities include:
  – The networks of Lithuania's electronic communication operators and internet service providers

TRANSPORT

- ***Marine Transport***

  Sea routes through Klaipeda State Seaport[569] extend the road and rail lines of the east/west corridor 9B to other European seaports. Klaipeda State Seaport is one of the ice-free ports on the eastern coast of the Baltic Sea.

[563] http://www.iae.lt/inpp_en.asp?lang=1&subsub=9
[564] Ignalina Handbook http://www.lei.lt/insc/handbook/tochtml.html
[565] http://www.rrt.lt/index.php?34611049
[566] http://www.rrt.lt/index.php?1053971677
[567] http://www.rrt.lt/index.php?342437237
[568] http://www.rrt.lt/index.php?-1731099069

The Butinge Terminal is the facility situated in an all-year-round ice-free area of the Baltic Sea. The Terminal can export up to 14 million tons of crude oil a year. As an import and export terminal, it is capable of not only exporting crude oil but also accepting import cargoes.

- ***Air Transport***

  Two national companies operated in Lithuania until this year. FLY LAL Lithuanian Airlines (LAL) and Air Lithuania. Fly LAL Lithuanian Airlines ceased its operations in January, 2009. (Air Lithuania ceased its operations in 2006) There are three international airports (Vilnius[570], Kaunas[571] and Palanga[572]).

RESEARCH FACILITIES

Public authorities:

- ***The State Institute of Information Technologies***[573] has the following goals*:*
  - Development of information technologies and they implemention of experimental and theoretical research into of various engineering systems.
  - The development of information and knowledge society technologies with a priority in fiscal, nuclear safety, and IT&T security.
  - Experimental and theoretical telecommunication systems, process controls and security systems.
  - Experimental and theoretical systems research in high risk critical infrastructure such as nuclear power plants, oil pipelines, gas pipes, railways, etc.
  - Experimental and theoretical environment systems research and environmental protection technologies development.
  - Experimental and theoretical systems security research and security technologies development in IT&T sector with the priority to identification, authentication, authorisation, authorisations control.
- ***Lithuania energy institute*** has the following goals[574]:
  - To perform fundamental and applied research in the fields of thermal physics, hydrodynamics, metrology, safety and reliability of energy objects, materials engineering, hydrology, and processes management.
  - To prepare energy sector planning conceptual and methodological basis in state's policy energy sector.
  - To prepare first-class specialists for energy and scientific research related to it.
- ***The Firefighters' Training School***[575]

[569] http://www.portofklaipeda.lt/lt.php
[570] http://www.vilnius-airport.lt/index.php?lang=en
[571] http://www.kaunasair.lt/index.php?lang=2&m=1&p=110
[572] http://www.palanga-airport.lt/en/?
[573] http://www.viti.lt/index.php?lang=en
[574] http://www.lei.lt

The Firefighters' Training School is the only educational institution of this kind in Lithuania that prepares qualified and multi-skilled fire fighters and rescuers for the Lithuanian Fire and Rescue Services and Municipality Fire Brigades. Since 1992, Vilnius Gediminas Technical University has been preparing the mid-stage officers (fire engineers) for the Lithuanian Fire and Rescue Service. Under a cooperation agreement between the Fire and Rescue Department and the Main School of Fire Service in Warsaw, two officers from Lithuania are invited to study in this school annually, graduating with Bachelors and/or Masters Degrees in Fire Engineering and Safety.

- ***Klaipeda Police School***[576]

  The Klaipeda Police School is a modern, open to society training centre, responsible not only for police officers' training but also for enhancing the professional image of police force. Its policy is oriented towards training European police officers who serve the people's interests. Being the only departmental institution which trains policemen, the school applies specific entrance criteria, for the recruitment of new candidates.

  The goal of the school is to provide professional education appropriate for a police officer's profession. The task of the school is to develop personal police officer's qualities, necessary for their future career, in a society based on democratic principles. The school cooperates with M. Romeris University and police educational institutions in foreign countries. The school has contacts with Tampere Police School in Finland, Latvia State Police School, Polish Police Training Centre in Legionowo, and the Hungarian Police School.

[575] http://www.vpgt.lt/
[576] http://www.policija.lt/mokykla/

19 Luxembourg

Figure 74: Luxembourg

19.1 Summary

	Organisational Model	Strategy & Policy	Methodology & Standards	Public-Private Partnership & International Collaboration	Funding & Human Resources	Training & Exercises	Sector-Specific Key Players & Initiatives
Luxembourg	▪ Supreme Council of National Protection deals with crises and has started CIP ▪ CONATIC is still under development	▪ Luxembourg's CIP is under development, using a structured approach	▪ Directory of Emergency Services manages intervention funds and plans	▪ Directorate of Emergency Services has links with first-aid organisation in neighbouring countries	▪ Not Applicable	▪ Directorate of Emergency Services recruits and trains volunteers	▪ Not Applicable

577

Critical Infrastructure Protection in Luxembourg is managed at a government level under the supervision of the High Commission for National Protection and with the support of a National Committee on critical infrastructures. Even though it is a relatively small country, Luxembourg has a well structured approach to CIP.

[577] Not Applicable = Open Source Research, Web-based survey and individual interviews have not shown information/data on the given argument

19.2 Organisational Model

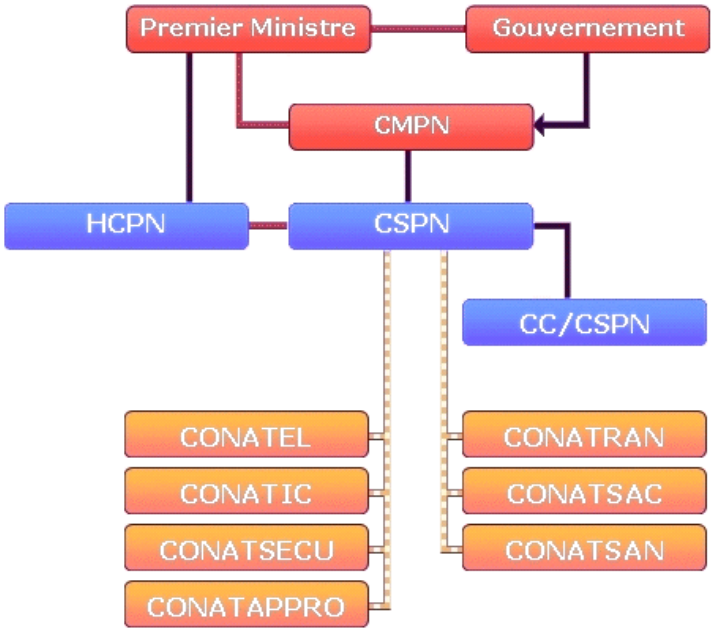


Figure 75: Organisational Chart (only CIP-related agencies shown)

***CMPN**: Conseil ministériel de la Protection nationale (Ministerial Council of National Protection)*

***CSPN**: Conseil supérieur de la Protection nationale (Supreme Council of National protection)*

***CC/CSPN**: Cellule de Crise du Conseil supérieur de la Protection nationale (Crisis cell of the Supreme Council of National protection)*

***HCPN**: Haut-commissariat à la Protection nationale (High Commission for National Protection)*

***CONATEL**: Comité national des Télécommunications (National Committee of Telecommunication)*

***CONATIC**: Comité national de l'Infrastructure critique (National Committee of Critical Infrastructure)*

***CONATSAC**: Comité national de Sûreté de l'Aviation civile (National Committee of Civil Aviation Security)*

***CONATSAN**: Comité national de la Santé (National Committee of Health)*

***CONATSECU**: Comité national de la Sécurité intérieure (National Committee of Interior Security)*

***CONATRAN**: Comité national des Transports (National Committee of Transpots)*

***CONATAPPRO**: Comité national de l'Approvisionnement (National Committee of Supply)*

Main Actors/Responsibilities:

***Ministère de l'Intérieur et de l'Aménagement du territoire (Ministry of the Interior and Territorial Management)*[578]**

The Ministry of the Interior and Territorial Management was created in 2004[579]. It is divided in the Department for the Interior and the Department of Territorial Management. The responsibilities of the Ministry are:

- managing and overseeing local authorities and their activities;
- undertaking the program of international and interregional policies for the management of the territory;
- coordination of governmental action to enable sustainable management and the protection of natural resources, and
- coordination of the emergency services.

***Haut-Commissariat à la Protection Nationale, HCPN (High Commission for National Protection)*[580]**

The HCPN was created after the Second World War, as a civil authority reporting to the Prime Minister. It was dormant after the end of the Cold War, but was reactivated after the events of the 11th of September 2001.

The main responsibility of the HCPN is the co-ordination of the security and protection planning and training of all government bodies and agencies, whether directed at a crisis, emergency or war. It also represents Luxembourg in international meetings dealing with security and emergency issues. Some of its key responsibilities include:[581]

- The identification and analysis of threats.
- Coordination of the national protection function and the evaluation of national capabilities.
- The maintenance of governmental functions during a crisis.
- The protection of essential national infrastructure.
- The preparation and maintenance of national operational capacity for national protection, including warning systems and protection.

[578] http://www.miat.public.lu/
[579] Arrêté grand-ducal of the 7 of August 2004 for the constitution of the Ministries
[580] http://www.hcpn.public.lu/protection_nationale/concept/index.html
[581] http://www.hcpn.public.lu/protection_nationale/concept/missions_nat/index.html

- The identification of critical infrastructure vulnerable to identified threats and the priority of their protection, establishing and maintaining the map of national vital points whether they are state-owned or private.
- The development of plans for the response to national crisis and emergencies.
- The authority for the HCPN's decision is the Conseil Ministériel de la Protection Nationale, CMPN (Ministerial Council of National Protection).

The planning and coordination structure is headed by a permanent forum, named *Conseil supérieur de la Protection nationale*, CSPN (Supreme Council of National Protection), that operates under the HCPN. The CSPN is responsible for national planning, but the specific planning in each domain is task of the *Comités nationaux,* CONAT (National Committees) of consultation. They are responsible for inter-ministerial and civil-military coordination and planning in the domains of health, telecommunications, transports, interior security, etc.

The HCPN has the role of coordinating all the elements operating under the framework of national protection to ensure they align their reparation, planning and procedures.

Comité national de l'Infrastructure critique – CONATIC (National Committee of Critical Infrastructure)

The legal basis of this Committee is still being developed under the Règlement grand-ducal and at the moment there is only a workgroup at the CSPN level working on protection of critical infrastructures.

In the future, this Committee will be established under the CSPN, and compose a group of experts delegated by the Ministries and the administrations for the protection of Critical Infrastructures.

This committee will be responsible for:

Establishing a list of the National Critical Infrastructure and their interdependencies.

- Determining the vulnerability of each piece of infrastructure, and the priority of its protection depending upon the level of risk.
- Establishing a national concept for Critical Infrastructure Protection
- Validating the plans and procedures through simulations and exercises

Direction des Services de secours (Directorate of Emergency Services)[582]

The Directorate of Emergency Services is attached to the Ministry of the Interior and Territorial Management. The main responsibilities of the Directorate are:

coordinating civil protection under the direct authority of the government, and

Providing services for fire and rescue depending on local authorities.

In the event of a catastrophe, the Directorate for Emergency Services leads rescue operations and reports to the Minister of the Interior.

[582] http://www.miat.public.lu/services_secours/index.html, http://www.112.public.lu/index.html

19.3 Strategy & Policy

Before the creation of the CSPN, if a crisis occurred the Government designated a Leading Minister, crisis unit, or an interministerial committee. Currently these tasks have been taken over by the CSPN, under the authority of the CMPN.

In the case of a crisis each ministry is still responsible for reviewing its own area of activity and undertaking the measures necessary to maintain government continuity, the protection of the population, maintenance of economic activity, and civilian support for military activities.

19.4 Public – Private Partnership & International Collaboration

The Directorate of Emergency Services develops links with first-aid organisations in neighbouring countries and helps to implement plans and directives arising from the mutual assistance agreements made between Luxembourg and Belgium, Germany and France.

19.5 Training & Exercises

The Directorate of Emergency Services is qualified to recruit and train the volunteer instructors of the assistance units.

The mechanism for civil-military cooperation in case of a crisis or emergency situation is tested in national and international exercises.

19.6 Sector – Specific Key Players & Initiatives

TRANSPORT

Public authorities:

Direction de l'Aviation Civile, DAC (Directorate of Civil Aviation) 583

The DAC was created as a part of the Ministry of Transport. The staff of the DAC is composed of officials and employees engaged in accordance with Article 19 of this Act. The Branch may be assisted temporarily by foreign experts as needed. Some CIP related responsibilities include:

- ensuring the safety and security of all civil aviation activities in Luxembourg;
- maintenance and improvement of aviation security and safety, and
- management of airport facilities and coordinating and controlling the activities of various operators on the airport.

Main operators :

[583] http://www.dac.public.lu/

Société Nationale des Chemins de Fer Luxembourgeois, CFL (Luxembourg Railways)[584]

CFL is the national railway company of Luxembourg. In 2005, the company carried approximately 14.1 million passengers and 11.7 million tonnes of goods. It employs 3,090 people, making CFL the country's seventh-largest corporate employer. The Luxembourgeois rail system comprises 275 kilometres of track, of which 140 km is double track and 135 km single track.

[584] http://www.cfl.lu/CFLInternet/Espaces/01EspaceVoyageurs

20 Malta

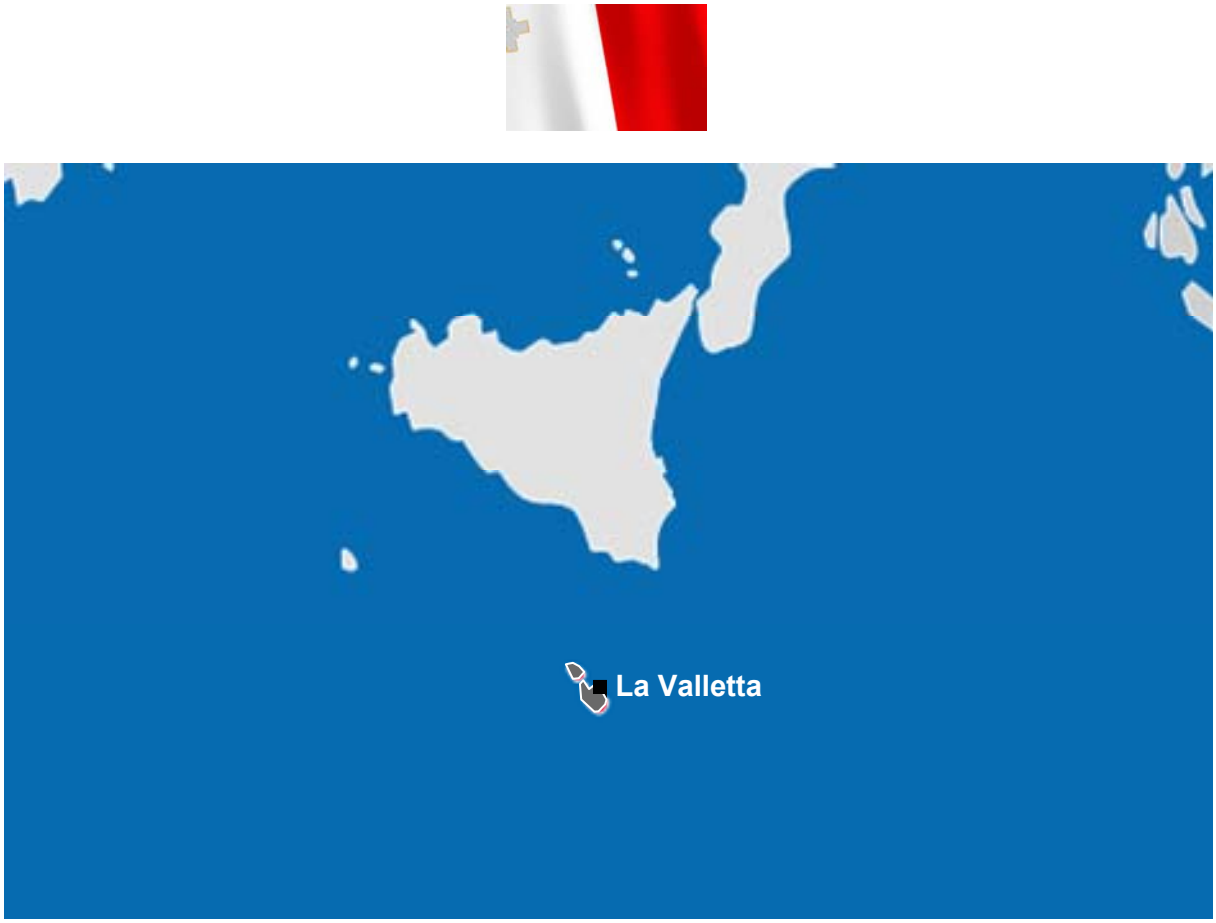


Figure 76: Malta

20.1 Summary

	Organisational Model	Strategy & Policy	Methodology & Standards	Public-Private Partnership & International Collaboration	Funding & Human Resources	Training & Exercises	Sector-Specific Key Players & Initiatives
Malta	▪ There is no specific Agency dedicated to CIP	▪ Malta is dealing in an unstructured way with CIP	▪ Malta Standards Authority deals with official Maltese standards	▪ ESPD ▪ 5+5 Defence Initiative	▪ Not Applicable	▪ Phoenix Espress Exercise ▪ Exercise Canale (Malta and Italy)	▪ Data Protection Twinning Light Project

585

Malta currently maintains a decentralised approach to CIP. There is no single agency with sole responsibility for the issue.

585 Not Applicable = Open Source Research, Web-based survey and individual interviews have not shown information/data on the given argument

20.2 Organisational Model

The Office of the Prime Minister[586]

The Prime Minister of Malta is both the head of government and a minister in his own right, with portfolio responsibilities for strategic matters such as the Public Service, defence, and EU matters including the management of EU pre-accession and structural funds. Most of these portfolio responsibilities are administered through the Office of the Prime Minister, commonly known as OPM or *Kastilja*. OPM's mission is to support the Prime Minister in providing leadership and direction for a stable and effective government.

The Main Permanent Secretaries, Authorities and Boards of the OPM include:

- Permanent Secretary for Infrastructure, Transports and Communications
- Permanent Secretary for Resources and Rural Affairs
- Permanent Secretary for Finance, Economy and Investment
- Permanent Secretary for Justice and Home Affairs
- Permanent Secretary for Tourism and Sustainable Development
- Principal Permanent Secretary (Armed Forces of Malta)
- Malta Environment and Planning Authority – MEPA
- Malta Councilfor Economic and Social Development
- The Defence Matters Directorate

Defence Matters Directorate

The Defence Matters Directorate was established in May 2003 within the Office of the Prime Minister to upgrade, consolidate and formalise the defence function of the OPM (a function which has exercised since 1964). The main responsibilities of the Directorate are:

- To provide objective technical and policy advice as well as timely analysis of military matters affecting the Government's defence policy.
- To monitor and analyse the implementation of Cabinet decisions and government policies on defence matters and to report on the extent to which policy and performance targets are met.
- To develop new policy initiatives and concepts on all Armed Forces of Malta (AFM) matters with a view to improving the operational, logistic and administrative effectiveness of the AFM.
- In co-ordination with other stakeholders within OPM, and in liaison with the Ministry of Foreign Affairs, conduct defence diplomacy and manage bilateral and multilateral defence relations with other countries and international organisations[587]

Ministry for Infrastructure, Transport and Communications – MITC [588]

[586] http://opm.gov.mt/
[587] http://www.gov.mt/frame.asp?l=2&url=http://www.opm.gov.mt/Annual_Report_2008.pdf.
[588] https://secure2.gov.mt/mitc/

The MITC has a broad and diversified portfolio that includes:

- Civil Aviation
- Malta Maritime Authority
- Malta Freeport Corporation
- Malta Transport Authority
- Malta Communications Authority
- Information and Communications Technology Strategy
- National Identity Management (Public Registry, Land Registry, Civil Registration, ID Cards, Passports)
- Coordination of Urban Development Projects (including Smart City, Grand Harbour and Marsamxett Regeneration)
- Coordination of Road Building, Maintenance and Landscaping; Water Services Corporation
- Enemalta Corporation
- Malta Shipyards[589]

Ministry of Foreign Affairs – MFA[590]

The main objectives and role of the ministry is ensuring that Malta's foreign policy objectives on European Union, bilateral, regional and global issues are pursued. The Ministry also coordinates the negotiation and conclusion of bilateral agreements[591]

Department of Information – DOI – of the OPM [592]

The Department of Information (DOI) provides the public with up-to-date, comprehensive and meaningful information on government policies, services and activities as well as on matters of public interest[593]. The Government Information Service provides members of the general public with information and material relevant to government services and activities[594].

The Malta Environment and Planning Authority – MEPA[595]

MEPA is the national agency responsible for environmental regulation in Malta. It was established under the Environment Protection Act (2001)[596] and the Development Planning Act (2001)[597] of the Laws of Malta[598].

Armed Forces of Malta[599]

[589] http://www.gov.mt/frame.asp?l=2&url=http://www.doi.gov.mt/en/ministries_and_departments/portfolio08.asp
[590] www.foreign.gov.mt/
[591] http://www.foreign.gov.mt/default.aspx?MLEV=51&MDIS=520
[592] http://www.doi.gov.mt/
[593] https://opm.gov.mt/dipartiment-informazzjoni?l=1
[594] http://www.doi.gov.mt/about_doi.asp
[595] http://www.mepa.gov.mt/main.aspx?
[596] http://doi.gov.mt/en/parliamentacts/2001/default.asp
[597] http://doi.gov.mt/en/parliamentacts/2001/default.asp
[598] http://www.gov.mt/frame.asp?l=2&url=http://www.opm.gov.mt/
[599] http://www.gov.mt/frame.asp?l=2&url=http://www.opm.gov.mt/Annual_Report_2008.pdf.

With the Force restructuring of 2006/7 the AFM focused on developing its operational capabilities and on enhancing its international presence. In 2008, the AFM participated for the first time in EU-led missions, reactivated its membership in NATO's Partnership for Peace, and increased its efforts to engage neighbouring countries, particularly through the 5+5 Initiative and Blue Border Control. Locally, the AFM's primary role is maintaining the territorial integrity of the Maltese Islands and safeguarding national interests. In part, it achieves this through constant surveillance on land, in the air and at sea by both physical and electronic means. Specifically, AFM perform two defence roles:

- The AFM is responsible for the external security and integrity of the Maltese Islands in peacetime and in crisis. Missions undertaken to achieve this role include:
  - Maintaining territorial integrity, particularly at the Malta International Airport and other sensitive locations.
  - Maintaining the integrity of Maltese waters, including employing physical and electronic surveillance against smuggling, illegal trafficking of immigrants and law-breaking at sea.
  - Providing surveillance of Maltese airspace.
  - Providing a search and rescue service in Malta and its Search and Rescue Region
  - Provide Explosive Ordnance Disposal (EOD) and Improvised Explosive Device Disposal (IEDD) services.
  - Contributing to international peace and stability by participating in the EU-led Peace Support.
- The AFM provides military support in specified areas to the Police Force on a regular basis and to other government departments when required. The demands placed on the AFM by this roles include:
  - Providing military assistance to government departments and the civil community.
  - Providing civil emergency protection support (explosives, marine pollution, floods and other disasters).
  - Providing military aid to the Police and Security Services (internal security, anti-narcotic patrols and vehicles check-points).
  - Underaking state ceremonial and other public duties.

Ministry for Justice and Home Affairs – MJHA –[600]

The portfolio of Ministry includes:

- Courts of Justice
- Attorney General's Office
- Police; Immigration
- Airport Security
- Correctional Services
- Civil Protection
- Data Protection[601]

Moreover, the MJHA operates in several Boards and Committees, among other:

[600] www.mjha.gov.mt
[601] http://www.doi.gov.mt/EN/ministries_and_departments/ministry_justice_home1.asp

- Aviation Security Committee
- Civil Protection Council
- Civil Protection Scientific Committee
- Explosives Committee
- Health and Safety Monitoring Board
- Immigration Appeals Board
- Police Academy Board
- Police Board
- Weapons Board
- Data Protection Appeals Tribunal[602]

Ministry for Resources and Rural Affairs – MRRA[603]

Malta is a small island and the sustainable management of its resources is crucial. The integrated coordination of agricultural and fisheries production, resources management, and the environment are an important responsibility. This is even more so in the context of European Union and other international obligations604, 605 Inter-alia, the portfolio of the MRRA includes:

- Malta Resources Authority
- Climate Change Policy
- Development of Alternative Energy Sources
- Oil Exploration
- National Parks, afforestation and the countryside
- Waste Management Strategy Implementation
- Building Industry Consultative Council
- Manufacturing and Servicing; Construction and Maintenance
- Science and Technology Policy
- Research and Innovation; Rural Development
- Agriculture
- Horticulture
- Fisheries
- Aquaculture
- Veterinary Services

[602] http://www.mjha.gov.mt/boards/boards.html
[603] http://mrra.gov.mt/
[604] http://mrra.gov.mt/theministry.asp
[605] http://mrra.gov.mt/thecurrentministry.asp

- Animal Welfare[606]

***Malta Resources Authority*[607]**

The Malta Resources Authority (MCA) is a public corporate body with regulatory responsibilities for the water, energy and mineral resources in the Maltese Islands. It was established by the Maltese Parliament through the Malta Resources Authority Act of 2000.

The MRA has wide ranging responsibilities including the regulation of water and energy utilities, industrial enterprises exploiting resources such as oil exploration, quarry operators and private abstractors of groundwater, retailers, operators and tradesmen in the regulated sectors. The Authority falls under Ministry for Resources and Rural Affairs[608]. Article 4 of the MRA Act establishes the functions of the Authority and gives it wide responsibilities for the regulation of practices, operations and activities on energy, water and minerals sectors. This includes the regulation of:

- The national utilities and service providers for energy and water namely Enemalta Corporation and the Water Services Corporation and their subsidiary companies.
- Industrial enterprises exploiting resources such as oil exploration, quarry owners and groundwater extraction.
- Retailers and operators in the regulated sectors including operators of petrol stations, gas and kerosene delivery entities, offshore bunkering companies, private operators of desalination plants, and operators of road tankers[609].

***Civil Protection Department*[610]**

The Civil Protection (CP) Department has been in operation for four years, but continues to develop. The Department undertakes roles previously undertaken by the the AFM and the Police Force. The main functions of the Department are:

- To develop contingency plans for the protection of life, property and economic resources in the case of natural and technological disasters which may impact the Maltese Islands.
- To muster civil protection services by co-ordinating the resources and services of Ministries and other Departments such as the Police, the AFM and the Health Authorities (including also voluntary organisations) which could be called upon to respond in a national or regional disaster or in an emergency.
- To undertake vulnerability and risk assessment studies.
- To promote public awareness of civil protection issues.
- To maintain an Assistance and Rescue Force.
- To prepare regulations under the Civil Protection Act and under the Emergency Powers Act.
- To organise and co-ordinate training to employees of the Department of Civil Protection and other Government entities, and to carry out exercises on a regular basis.

606 http://www.doi.gov.mt/EN/ministries_and_departments/ministry_rural_affairs1.asp
607 www.mca.org.mt/
608 http://www.doi.gov.mt/EN/bodies/authorities/malta_resource.asp
609 http://www.mra.org.mt/aboutus2.shtml
610 http://www.gov.mt/newsletterarticle.asp?a=115&l=2

The Assistance and Rescue Force

Established under the Civil Protection Department, the Assistance and Rescue Force is responsible for fire-fighting and rescue on land and fire-fighting and pollution control at sea. Its main functions are to maintain an adequate service for prompt intervention in case of fire and rescue on land, flooding, sea salvage, rescue and anti-pollution support at sea, or any other natural or man-made disaster situation which requires the immediate assistance of a public force or special equipment, and to intervene in any emergency or disaster.

This Force is equipped with not less than twenty-seven fire-fighting vehicles donated by the Italian Government under the IV Financial protocol, together with two rescue launches and two fire-fighting and pollution vessels also donated under the same Financial Protocol.

Training of personnel is carried out on a regular basis both in Malta and abroad, the latter mostly under the auspices of the Italian Government and Euro-Med Pilot Project on Civil Protection.

A Civil Protection Operation Centre has been set up with modern sophisticated equipment also donated by the Italian Government.

20.3 Strategy & Policy

Malta does not currently possess an overarching strategy regarding CIP, although in the ICT domain, some actions have been performed.

In January 2003, Malta became part of the European Union (EU) Mechanism for Civil Protection. Through this Memorandum of Understanding, all EU countries are expected to assist each other in case of disasters. This assistance may also be extended to other countries, according to the directives of the Presidency.

The Smart Island Strategy [611]

The origin of the 2010 vision of The Smart Island is the 2004 National ICT Strategy which mapped out the country's approach to exploiting the global ICT revolution. The Smart Island Strategy seeks to pro-actively address the major challenges which the country's development in this sector shall inevitably face. Primary amongst these are the need to identify and address the 'new' digital divides which will emerge in the coming years, the successful application of technologies in the enhancement of our quality of life, and the constantly moving target of becoming and remaining a leading ICT industry in the region. The Smart Island strategy is a complex web of inter-twined initiatives constructed through a 'hub-and-spoke' model, with the vision serving as the hub and seven inter-related strategic streams as spokes:

- Robust ICT environment and next generation infrastructure
- A connected society – bridging the last and the new miles
- Develop human potential into a smart workforce

[611] https://secure2.gov.mt/SmartIsland/Pages/Home.aspx

- e for everything – enhancing our citizens' quality of life through ICTs
- Re-inventing government – transformation and open government
- Taking care of (e) business
- Developing a world-leading ICT industry

Each stream features key strategic targets and is composed of a series of supporting spokes. The deployment of the spokes is supported by a structured set of strategic programmes and initiatives.

Information Security Organisation Policy[612]

The Information Security Organisation Policy is a policy document of the OPM whose purpose is to specify organisational requirements for the management of the Public Service Information Security Framework (ISF). The Policy includes the definition, roles and responsibilities to be adopted to promote information security in the Public Service.

The Public Service of the Government of Malta is to establish an organisational capacity to manage the ISF within the Public Service. The ISF organisational capacity is three tiered. At the corporate level capacity will reside within the National Security Authority (NSA) of Malta Security Service (MSS), InfoSec Authority of the Central Information Management Unit (CIMU) and the Cabinet Office in terms of Security Accreditation and management of EU Classified Information. A Public Service ICT Security Committee (PSISC) will act as corporate consultative and advisory body to CIMU.

20.4 Public – Private Partnership & International Collaboration

European Security and Defence Policy – ESDP

Over the past twelve months, there were significant developments in Malta's involvement in European Defence matters, the ESDP in particular. The Malta Quota Post on the EU's Military Staff was taken up for the first time in April. Moreover, the AFM's participation in the EU's missions in Georgia and in the Gulf of Aden demonstrates the commitment Malta has in furthering ESDP[613].

NATO Partnership for Peace

On 3 April 2008, NATO formally accepted Malta's application to reactivate its participation in Partnership for Peace (PfP). Following this acceptance, the process of accreditation involving the "Agreement on the Security of Information with NATO" and associated code of conduct was initiated. Following a certification visit to Malta by the NATO Office of Security in July, Malta was certified to receive and handle NATO/PfP released classified information. Work on the Individual Partnership Programme is in progress[614].

United Nations

[612] http://ictpolicies.gov.mt/docs/infosec_policy.pdf
[613] http://www.gov.mt/frame.asp?l=2&url=http://www.opm.gov.mt/Annual_Report_2008.pdf.
[614] http://www.gov.mt/frame.asp?l=2&url=http://www.opm.gov.mt/Annual_Report_2008.pdf.

In 2008, Malta participated for the first time in a UN mission. This was achieved with the support of the Italian Ministry of Defence who allowed an AFM officer to be deployed as part of the Italian contingent in Lebanon where he was employed in the Civil-Military Co-operation (CIMIC) branch. The experience gained on this mission was essential for the officer's preparation to take up Malta's quota post on the EU's military staff later on in the year[615].

Organisation for Security and Co-operation in Europe – OSCE

The AFM regularly contributes to OSCE by sending qualified personnel as part of inspection teams in accordance with the Dayton Peace Agreement and other confidence building measures undertaken by the this organisation[616].

5 + 5 Defence Initiative

Malta's participation in the 5+5 Defence Initiative goes back to December 2004 when, together with the other Western Mediterranean Littoral Countries, it signed the Declaration of Intent which established this initiative. The Defence Initiative provides a framework for security dialogue and co-operation between member states. Throughout 2008, the 5+5 was under Libyan presidency and Malta participated in 13 activities that were organised as part of the 2008 Action Plan, including meetings, seminars and training exercises[617].

20.5 Methodologies & Standards

***Malta Standards Authority*[618]**

The Malta Standards Authority (MSA) was established in 2000 by virtue of Chapter 419 of the Revised Edition of the Laws of Malta. Its mission is to co-ordinate standardisation and related activities to meet the needs of the Maltese community.[619]. This Authority falls under the Ministry of Finance, the Economy and Investment.

20.6 Training & Exercises

For the first time, in 2008 the AFM participated in Exercise PHOENIX EXPRESS, an annual multilateral maritime exercise held in the Central Mediterranean region. The aim of this exercise is to improve interoperability between navies in the region – in particular with regard to law enforcement and interdiction. The search and rescue component of this exercise was introduced by the Maltese co-ordinators. Malta also hosted the operational headquarters for this exercise which was stationed at Luqa Barracks and included two AFM officers.

The 2008 Exercise CANALE, a bilateral maritime exercise organised between Malta and Italy and to which all 5+5 Initiative countries are invited, was held in Maltese waters between 30 May and 7 June. The aim of this exercise is to train personnel in joint search and rescue, law

[615] http://www.gov.mt/frame.asp?l=2&url=http://www.opm.gov.mt/Annual_Report_2008.pdf.
[616] http://www.gov.mt/frame.asp?l=2&url=http://www.opm.gov.mt/Annual_Report_2008.pdf.
[617] http://www.gov.mt/frame.asp?l=2&url=http://www.opm.gov.mt/Annual_Report_2008.pdf.
[618] www.msa.org.mt
[619] http://www.msa.org.mt/directorates.htm

enforcement operations at sea and explosive ordnance disposal. This year's participants included all 5+5 member countries with the exception of Libya.

Exercise TERRA FERMA 2008 was once again organised in two phases. In the first phase, Italian and Maltese troops exercised together in Malta while the second phase consisted of training at the Italian Army training facility in Torre di Nebbia, Italy. The aim of this exercise is to train Italian and Maltese troops in joint peace support operations and to test the interoperability of the two Forces[620].

Besides training its personnel overseas, the AFM seeks to organise its own courses. Relevant courses held in 2008 include the Key Point Protection and VIP Escort courses, and a course for officers who will be employed as arms verification inspectors in the Balkans. Some of these courses were held by the AFM on its own while others were organised with the assistance of the Italian Military Mission in Malta or by mobile training teams which were brought from abroad for this purpose.

The AFM Search and Rescue Training Centre has been operating for the last three years and offers specialised training in search and rescue operations. The centre is operated by the AFM and funded by the US Coast Guard and organises courses for both Maltese and foreign Search and Rescue operators. In 2008, the Centre organised a number of courses which, apart from Maltese students, included students from Saudi Arabia, Egypt, Montenegro, Algeria, Libya and the United Kingdom. The courses offered have been diversified to fit the requirements of participants and further developments are envisioned for 2009[621].

20.7 Sector – Specific Key Players & Initiatives

ENERGY

Main Operators:

- ***Enemalta Corporation – EMC[622]***

  The Maltese national electricity grid is isolated and is not connected to any other electrical network. Therefore, all the electrical energy that is required is generated in Malta. This is carried out by Enemalta Corporation (EMC). At present EMC operates two power stations with a total combined nominal installed capacity of 571MW, which supply all the electrical power needs of the Islands of Malta and Gozo. These stations are interconnected by means of the existing grid. Malta has no indigenous primary energy resources and therefore EMC relies entirely on imported fuels, mainly heavy fuel oil and light distillate.[623]

  The Petroleum Division is responsible for the programming, importation, storage and distribution of all petroleum products and liquid petroleum gas in Malta. The Fuel Procurement Committee of Enemalta is responsible for the acquisition of these products and the chartering of vessels and tankers for their transportation to Malta.

[620] http://www.gov.mt/frame.asp?l=2&url=http://www.opm.gov.mt/Annual_Report_2008.pdf.
[621] http://www.gov.mt/frame.asp?l=2&url=http://www.opm.gov.mt/Annual_Report_2008.pdf.
[622] http://www.enemalta.com.mt/page.asp?p=925&l=1
[623] http://www.enemalta.com.mt/page.asp?p=926&l=1

INFORMATION AND COMMUNICATION TECHNOLOGIES

Public Authorities:

- ***Malta Communications Authority – MCA[624]***

  The MCA is the national agency responsible for the regulation of the electronic communications sector (telecommunications, radio communications and broadcasting transmission), e-commerce and the postal sector, and was established on the 1st January 2001. The MCA is the National Regulatory Authority for these sectors in accordance with EU law which is subsequently transposed into Maltese legislation. The MCA is responsible for promoting competition, for protecting consumers and for encouraging innovation. The MCA enables competition in the communications sector by facilitating market entry through a general authorisation to provide networks and services and by regulating access to networks so as to develop effective choice for consumers. In a rapidly evolving sector, both in technological and commercial terms, the MCA provides the framework for the introduction of new services[625].

- ***Information Management Unit[626]***

  The Information Management Unit (IMU) is the primary ICT business driver at the OPM, providing advice and support to all OPM departments and authorities. The main IMU business functions include drawing up of OPM ICT strategic plans; the management of ICT project design, procurement and financing; management of information systems policy; application development and open source/standards research; management of hardware inventories; authorisation and provision of information services; liaison with suppliers providing information technology services including MITTS; management of data centre facilities; and providing first-hand operational support on infrastructure[627].

- ***Operation and Programme Implementation Directorate – OPI[628]***

  Data protection compliance in the public service is the primary corporate initiative under the responsibility of the Directorate. By means of this project, the OPM Data Protection Team (composed of OPI and MITTS personnel) offers advice and assistance to ministries and departments in the field of data protection. It also provides advisory support to departments in case of queries received from the Data Protection Commissioner and acts as intermediary between the Office of the DP Commissioner and the relevant departments.

Initiatives:

- ***Data Protection - Twinning Light Project***

  The *Twinning Light* project[629] - data protection training in the Malta Public Service, was successfully undertaken during 2008 in conjunction with German

[624] www.mca.org.mt/
[625] http://www.mca.org.mt/corporateprofile/openarticle.asp?id=13
[626] http://www.gov.mt/frame.asp?l=2&url=http://www.opm.gov.mt/Annual_Report_2008.pdf.
[627] http://www.gov.mt/frame.asp?l=2&url=http://www.opm.gov.mt/Annual_Report_2008.pdf.
[628] http://www.gov.mt/frame.asp?l=2&url=http://www.opm.gov.mt/Annual_Report_2008.pdf
[629] http://www.gov.mt/frame.asp?l=2&url=http://www.opm.gov.mt/Annual_Report_2008.pdf.

partners. The project, was financed by the EU 2005 Transition Facility Programme for Malta, to provide training in data protection to a large number of public officers. The project which was led by the Independent Centre for Privacy Protection in Kiel of Schleswig-Holstein, Germany, together with the Operations and Programme Implementation Directorate, was implemented between January and July. Besides enhancing data protection skills and practices across the public service, the training activities organised improved the data protection general awareness of participants, both as users of personal data and also as data subjects themselves. Data protection issues were also covered in specific sectors that process significant volumes of personal data in the public service (health, education, police, social welfare, among others).

WATER

Public Authorities:

- ***Water Services Corporation***[630]

  The Water Services Corporation (WSC) was established in 1993 to produce and distribute potable water in the Maltese Islands. Some 31 mn cubic meters of good quality water are produced annually to cater for the needs of Malta's 400,000 inhabitants as well as the over 1 mn tourists who visit every year. Approximately 57% of this water is produced at the Corporation's three reverse osmosis plants - Pembroke, Cirkewwa and Ghar Lapsi. The remaining water is groundwater produced from boreholes and pumping stations. In October 2003, the former Drainage Section, now known as the Wastewater Section, was incorporated within the WSC. The Wastewater Section of the WSC is responsible for the treatment and safe disposal of wastewater in the Maltese Islands. Apart from extensive upgrading works and the building of new wastewater treatment plants, the Section also carries out routine maintenance such as the cleaning of approximately 400km of sewer every year[631].As such, the Corporation is now wholly responsible for the complete water cycle from production to its safe disposal[632].

  In 2006-07 just under 17 million cubic metres of water was produced by reverse-osmosis plants. This blend is stored in the 24 reservoirs in Malta, Gozo and Comino which have a total capacity of 400,000 cubic metres. All the production, transfer and storage of water is controlled and monitored in real time by remote sensing from the control room at Luqa.[633].

FOOD

Public Authorities:

- ***Food Safety Commission***[634]

630 www.wsc.com.mt/
631 http://www.wsc.com.mt/(S(kkb45p55igpy4bf2chktln55))/default.aspx?MLEV=15&MDIS=20
632 http://www.wsc.com.mt/(S(kkb45p55igpy4bf2chktln55))/default.aspx?MLEV=4&MDIS=12
633 http://www.wsc.com.mt/(S(kkb45p55igpy4bf2chktln55))/default.aspx?MLEV=14&MDIS=76
634 http://www.health.gov.mt/fsc/fschome.htm

Established by Article 5 of the Food Safety Act, 2002[635]. The principal function of the Food Safety Commission (FSC) is to ensure that food produced, distributed or marketed in Malta meets the highest standards of food safety and hygiene reasonably available and to ensure that food complies with legal requirements, or where appropriate with recognised codes of good practice.

FINANCIAL

Public Authorities:

- ***Ministry of Finance, The Economy and Investment – MFIN[636]***

  The role of MFIN is to promote policies and programmes that support Malta's financial and fiscal well being and to contribute to the sustainability of such initiatives. Its main areas of responsibility include :

  – Formulating advice on revenue and expenditure policy
  – Evaluating individual spending programmes
  – Carrying out research and compiling policy submissions for consideration
  – Contributing to better financial management in the public service by carrying out an ongoing review of relevant policies and procedures

  Core Functions :

  – Providing ad hoc reports on financial policy issues in response to specific requests at Ministry level
  – Identifying focus areas for evaluation with a view to appraising consistency with overall Government policy
  – Facilitating better financial management via continuous updating of policies and procedures and contributing to their sustainability through a service-wide outreach programme
  – Evaluating the financial implications of new conditions of employment in the public service and ensuring that existing conditions of service are being implemented in accordance with approved parameters
  – Reviewing developments relating to the Public Private Partnership Programme with a view to contributing to the success of this initiative and its extension to other areas of activity
  – Monitoring the progress of efficiency review programmes in selected areas of activity across the public service[637]

  The main purpose of the Economic Policy Division is to serve as the strategic arm of the Ministry. It is responsible for strategic planning and policy co-ordination across the Ministry. Policy co-ordination is also undertaken with other Ministries, particularly where effective handling of specific issues calls for close inter-

[635] http://docs.justice.gov.mt/lom/legislation/english/leg/vol_14/chapt449.pdf
[636] http://mfin.gov.mt
[637] http://finance.gov.mt/page.aspx?site=MFIN&page=finance

Ministerial collaboration. It is also responsible for the national economic strategy and matters related to international economic relations[638].

- ***Central Bank of Malta***[639]

  The Central Bank of Malta is an independent institution which seeks to carry out its statutory responsibilities in the public interest. As a member of the Eurosystem, the Bank's primary objective is to maintain price stability, thereby contributing to sustainable economic development. Its objectives are:

  – promoting price stability;
  – contributing to the stability of the financial system;
  – promoting, regulating and overseeing sound and efficient payment and securities settlement systems;
  – supporting the development of financial markets;
  – providing and promoting efficient currency services;
  – optimising the returns on financial assets through prudent investment practices;
  – collecting, compiling, disseminating and publishing statistics, and
  – Advising the government generally on financial and economic matters[640]

TRANSPORT

Public Authorithies:

- ***Malta Maritime Authority***[641]

  The Malta Maritime Authority (MMA) was established as a distinct and autonomous corporate body to supervise the the primary maritime services. It was established in 1991 as a Government Agency to enable ports, merchant shipping and yachting centres to operate within centralised framework. The Authority operates as a commercially driven organisation, committed to excellence in the provision of services that are both effective and competitive. The Malta Maritime Authority's principal role is to create a climate that further enhances Malta's maritime standing and associated business activity[642].

- ***The Malta Transport Authority – MTA***[643]

  The Malta Transport Authority comprises two boards appointed by the Minister for Transport, Infrastructure and Communications. The legal functions of Authority are to plan, secure and promote the provision of, a properly integrated, safe, economical and efficient transport system.

- ***Department of Civil Aviation of Malta – DCA***[644]

[638] http://finance.gov.mt/page.aspx?site=MFIN&page=economic
[639] www.centralbankmalta.org/site/
[640] http://www.centralbankmalta.org/site/about2.html
[641] http://www.mma.gov.mt/
[642] http://www.mma.gov.mt/org_setup.htm
[643] http://www.maltatransport.com/en/#
[644] http://www.dca.gov.mt/

The Department of Civil Aviation, which forms part of the Ministry for Infrastructure, Transport and Communications, functions as the regulator of all aviation activities in Malta. Its ensures that such activities are carried out in compliance with those international standards which Malta has adopted as a result of its membership in organisations such as the International Civil Aviation Organisation (ICAO), the European Civil Aviation Conference (ECAC), EUROCONTROL and the Joint Aviation Authorities of Europe (JAA). The Department is thus responsible for the safety oversight of aircraft, aircraft and aerodrome operators and air navigation service providers, the licensing of aeronautical personnel and the conclusion of international air services agreements[645].

[645] http://www.dca.gov.mt/about/index.asp

21 The Netherlands

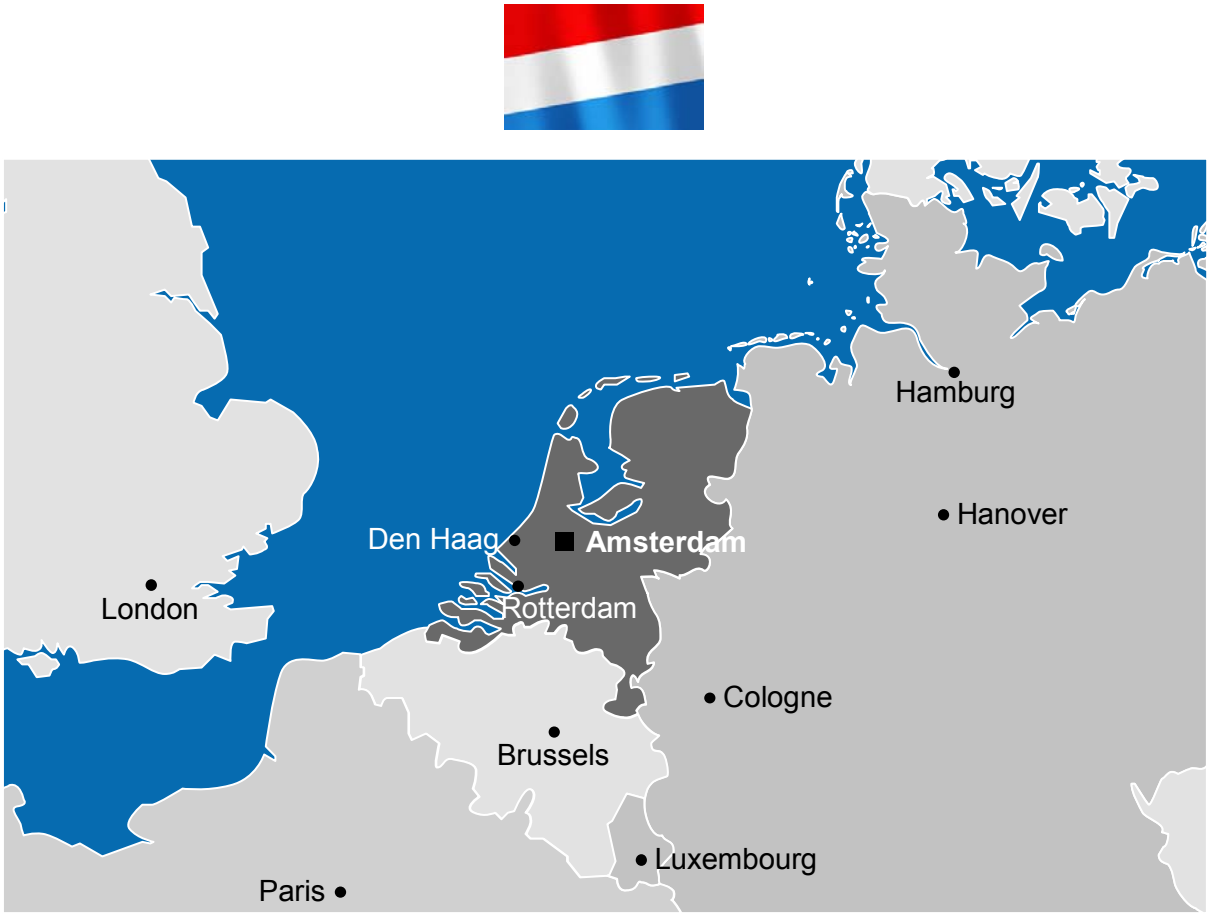


Figure 77: The Netherlands

21.1 Summary

	Organisational Model	*Strategy & Policy*	*Methodology & Standards*	*Public-Private Partnership & International Collaboration*	*Funding & Human Resources*	*Training & Exercises*	*Sector-Specific Key Players & Initiatives*
The Netherlands	▪ Ministry of the Interior and Kingdom Relations, Directorate of National Security leads an informal, inter-ministerial CIP working group	▪ CIP programs fall under national security strategy ▪ Activities involve national government, CI operators, and safety regions	▪ National Security: strategy and work programme 2007-2008 ▪ The Dutch CIP Methodology	▪ Some bilateral (floods) and multilateral (ICT) agreements in place ▪ PPPs in place for CIP (SOVI and NAVI)	▪ Core CIP group has 9 staff members ▪ Main support agency has approximately 20 staff members	▪ "Shift-Control" exercise on ICT attack ▪ Voyager (2007) ▪ Waterproof (2008)	Specific CIP-related initiatives across all sectors, including some sectors not identified by the EC as "critical

The Netherlands manages CIP through a semi-centralized approach. Efforts are lead by the Ministry of the Interior and Kingdom Relations, Directorate of National Security, through an inter-ministerial CIP working group. However, there is no CIP-specific law for the formation of this group or assigning the lead role to the Ministry of the Interior and Kingdom Relations. The Dutch CIP program is realized through cooperation rather than legislative measures.

The all-hazards approach is based on the National Security Strategy. Cooperation between national government, critical infrastructure operators, and the safety regions is key to the success of the program.

The Dutch government has defined 12 critical sectors and 33 critical services and products. Initiatives across all sectors include a vulnerability analysis.

21.2 Organisational Model

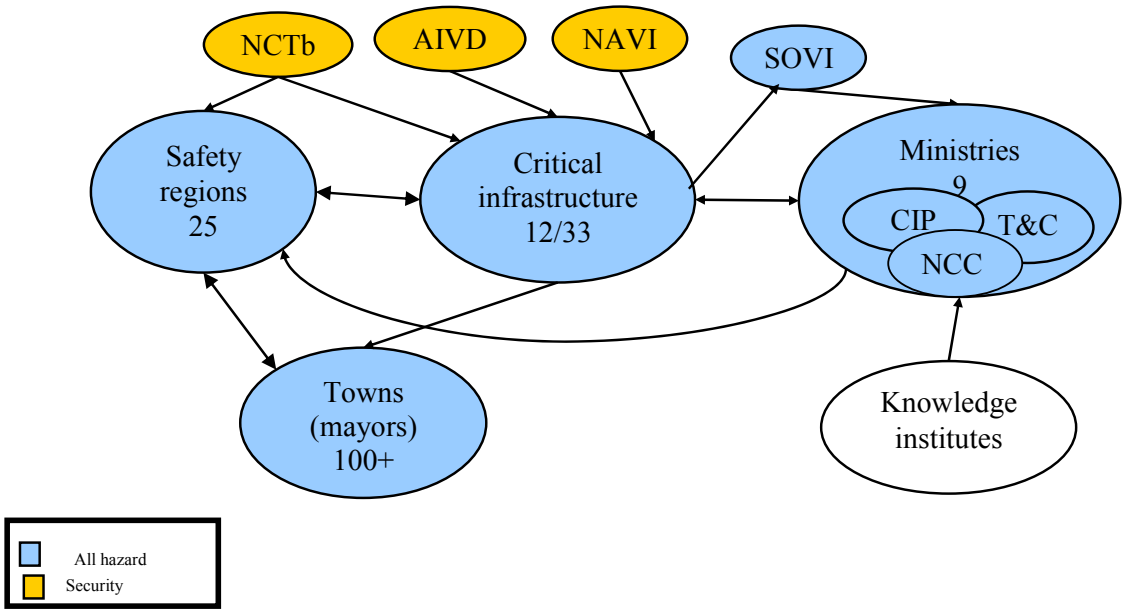


Figure 78: Organisational Chart (only CIP-related agencies shown)

The Ministry of the Interior and Kingdom Relations, Directorate of National Security, leads a national-level inter-ministerial working group with nine other ministries to form an integrated CIP program. This group drives CIP activity in the Netherlands. In addition to the CIP program, this group is also closely linked to the interdepartmental programme "Threats & Capacities" which is responsible for the National Risk Assessment (NRA) and capacity building measures, as well as to the National Crisis Centre (NCC).

Safety regions (geographically divided) are responsible for CIP and crisis response at the regional level, while Mayors are responsible for public order and for crisis response at the local (municipality) level. All levels of government work together with critical infrastructure owners/operators to ensure a sufficient level of protection at their respective levels.

Main Actors/Responsibilities:

THE INTER-MINISTERIAL WORKING GROUP

This groups consists of a DG-level steering committee that focuses on the policy areas of National Security Strategy, CIP, and National Crisis Management. The group also contains a CIP working group with representatives from each ministry that meets on a monthly basis to discuss CIP activities and exchange information. This group is lead by the Ministry of the

Interior and Kingdom Relations and operates in a cooperative nature (not based on any specific legislation).

Ministries	Sectors
Ministry of Transport, Public Works and Water Management (V&W)	Transport Stemming and Managing Surface Water
Economic Affairs (EZ)	Energy Telecommunications/ICT
Agriculture, Nature and Food Quality (LNV)	Food
Finance	Financial
Justice	Legal Order
Housing, Spatial Planning and the Environment (VROM)	Drinking Water Chemical and Nuclear
Health, Welfare and Sport (VWS)	Health
Interior and Kingdom Relations (BZK) (and Defence (Defensie) and Foreign Affairs (BUZA))	Public Order and Safety Public Administration

Figure 79: Ministries and Sectors of Responsibility

- ***Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*** **(The Dutch Ministry of the Interior and Kingdom Relations[646])**
  The ministry of the Interior and Kingdom Relations (BZK) is one of the thirteen ministries of Dutch central government. The Directorate of National Security leads the Inter-Ministerial workgroup and the Netherlands CIP program. In addition to its lead role in the working group, the Ministry also holds a second operational role in relation to its mission to: uphold the Constitution; guarantee the democratic rule of law; ensure an effective and efficient public administration; coordinate urban policy; promote public order and safety and provide centralised management of the countries police forces; promote the quality of the civil service and coordinate management and personnel policy for all civil servants; coordinate cooperation with Aruba and the Netherlands Antilles.
- ***Ministerie van Verkeer en Waterstaat; V&W*** **(The Dutch Ministry of Transport, Public Works and Water Management[647])**
  This Ministry is responsible for the Dutch system of water management, public and private transport and infrastructure. The ministry has two main responsibilities: regulation and management of transportation of people and goods via roads, trains, boats and airplanes; Water management by water works, such as dikes, polders and channels.
- ***Ministerie van Economische Zaken*** **(The Dutch Ministry of Economic Affairs[648])**

646 **http://** www.minbzk.nl
647 **http://***www.verkeerenwaterstaat.nl*
648 **http://***www.ez.nl*

The mission of the Ministry is to promote sustainable economic growth in the Netherlands. The political responsible of the ministry is in hands of the Minister of Economic Affairs, who is part of the Dutch Cabinet.

- ***Ministerie van Landbouw, Natuurbeheer en Voedselkwaliteit; LNV*** **(The Dutch Ministry of Agriculture, Nature and Food Quality[649])**
  The Ministry is responsible for four fields of policy: agriculture and *fisheries;* natural conservation, open air recreation and national parks; food safety; rural development.
- ***Ministerie van Financiën; Fin*** **(The Dutch Ministry of Finance[650])**

  The Ministry is occupied with the national budget, taxation and financial economic policy, including supervision of financial markets.
- ***Ministerie van Justitie; Jus (The Dutch Ministry of Justice[651])***

  The Ministry has the legal miss*ion to: provide workabl*e legislation for citizens, government and the courts; prevent crime, in order to build a safer society; protect youth and children; enforcement the law, in order to build a safer society; provide independent, accessible and effective administration of justice and legal aid; provide support to the victims of crime; provide fair, consistent and effective enforcement of punishment and other sanctions; regulate immigration into the Netherlands. It is also responsible for the coordination of anti-terrorism policy.
- ***Ministerie van Volkshuisvesting, Ruimtelijke Ordening en Milieu – VROM*** **(The Dutch Ministry of Housing, Spatial Planning and the Environment[652])**
  This Ministry is responsible for policies on public housing, spatial planning, the environment, and the housing of national government agencies.
- ***Ministerie van Volksgezondheid, Welzijn en Sport*****; VWS (The Dutch Ministry of Health, Welfare and Sports[653])**
  It is the public health authority of the Netherlands. The ministry is responsible for three policy areas: public health and health care, welfare and social-cultural work, sports.
- ***Ministerie van Defensie; Def (The Dutch Ministry of Defence[654])***

  It coordinates the military of the Netherlands. The ministry has the responsibility for: protecting the territory of the Netherlands and her allies, including the Dutch Antilles and Aruba; protecting and enhancing the international legal system and stability; supporting civil authorities in maintaining order, in case of emergencies and in giving humanitarian aid, both national and international.

OTHER KEY AGENCIES (NOT PART OF INTER-MINISTERIAL WORKING GROUP)

- ***Nationaal Coördinator Terrorismebestrijding (NCTb)[655]*** **(National Coordinator for Counterterrorism)**

649 **http://***www.minlnv.nl*
650 **http://**www.minfin.nl/en/home
651 http://*www.justitie.nl/*
652 http://www. vrom.nl
653 http://*www.minvws.nl*
654 http://www.defensie.nl/

In the field of security various actors play a part in CIP. The NCTb[656] coordinates counterterrorism policy.

1. Analysing intelligence and other information
2. Policy development
3. Coordinating anti-terrorist security measures

Combining these tasks increases the effectiveness of the government's efforts to combat terrorism. The office of the NCTb and its staff fall under the responsibility of two ministers: the Minister of Justice (the lead minister for counterterrorism) and the Minister of the Interior and Kingdom Relations. In terms of organisation and management, the office of the NCTb falls under the Ministry of Justice, in a similar way to a directorate-general.

- ***Binnenlandse Veiligheidsdienst, Domestic Security Service (Dutch Intelligence Service. Algemene Inlichtingen- en Veiligheidsdienst (AIVD[657]), formerly known as the BVD)***

  It is the General Intelligence and Security Service of the Netherlands. The AIVD focuses mostly on domestic non-military threats to Dutch National security, whereas the Military Intelligence and Security Service (MIVD[658]) focuses on international threats, specifically military and government-sponsored threats such as espionage. The AIVD, unlike its predecessor BVD, is charged with collecting intelligence and assisting in combating both domestic and foreign threats to national security.

- ***Nationaal Adviescentrum Vitale Infrastructuur (NAVI)[659]* (National Advisory Centre for Critical Infrastructure)**

  The NAVI assists and advises both public and private partners in critical sectors in developing security management. Its three core activities are:

  1. Advice on security protection
  2. Knowledge and information exchange
  3. Networking

  The first sectoral analysis in 2005 showed that malicious disruption as a cause of failure of critical infrastructure needed more attention in the Netherlands. Measures focused on the security of the critical infrastructure had to be intensified. In this light, NAVI has been founded. NAVI was set up through public-partnership in 2007 to help the Dutch government intensify security protection in the critical sectors. This involves more parties than just government. Most business enterprises in the critical sectors are responsible for their own security protection and business continuity.

- ***Strategisch Overleg Vitale Infrastructuur (SOVI)* (Strategic Council for Critical Infrastructure Protection)**

  The SOVI is public-private partnership on CIP at an executive level. Due to the fact that, the intersectoral connections determine, to a large extent at least, critical infrastructure

655 www.nctb.nl
656 www.nctb.nl
657 http://www.aidv.nl
658 http://www.defensie.nl/
659 www.navi-online.nl

vulnerability, it is important for the sectors to be able to hold one another accountable in terms of performance. An initiative to do so was launched in consultation with the VNO-NCW employers' organisation in 2006. There was ample support for establishing the SOVI. Both government and business are represented in this group, which has a dual function:

1. For consultations between government and business
2. For consultations between the critical sectors

The SOVI offers a platform for coordinating, strategic topics that affect all parties. The SOVI is not a formal, decision-making body. Participants represent the executive levels of business and government, overseen by an independent chairperson.

There are several knowledge institutes in the Netherlands that contribute to the CIP program with commissioned research. TNO is a frequent partner.

Organizational Impact of EU Legislation

On 12 January 2009, the European Directive on protection of critical infrastructure and the associated (non-binding) guidelines entered into force. The Netherlands has chosen to implement in its entirety through policy. A key area for each sectoral ministry concerned is whether the obligations for an OSP (operator security plan) and an SLO (Security Liaison Officer) for each potential ECI (European Critical Infrastructure) will be fulfilled. This could potentially lead to an amendment of the sectoral legislation by the responsible ministries. This will only come into play if one or more ECI's are designated in the Netherlands. Furthermore, this situation is different for each critical infrastructure.

The Dutch CIP contact point will play a crucial role in the process of identifying and designating ECI's. The strength of maintaining an interdepartmental joint committee as the "CIP contact point" is that it will have a crosscutting approach and impact. This also fits in with the range of thought of the directive. From this viewpoint, the CIP contact point has been set up as a priority, so that the actual implementation of the directive can be channelled through the CIP contact point. In this regard, the necessary collaboration between the ministries, as well as with business, will be reinforced.

The CIP contact point has developed the following implementation plan:

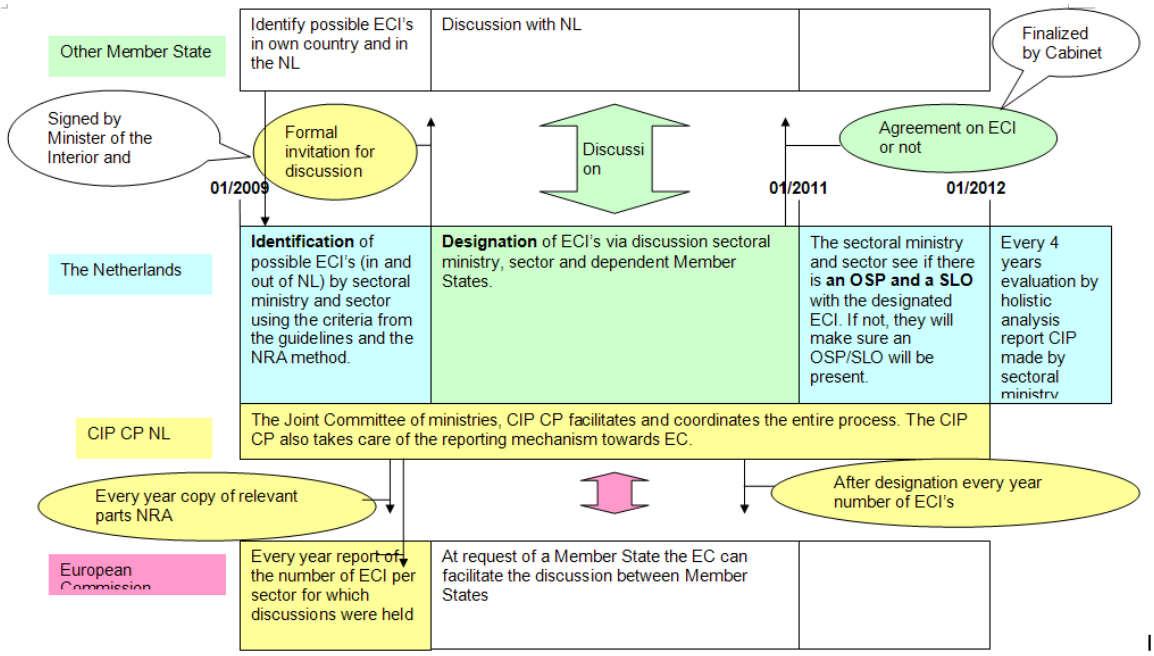


Figure 80: Dutch Implementation Plan for EU CIP Directive

1. Identification

The responsible ministry and the sector, supported by the CIP contact point, will examine which infrastructure in the Netherlands could potentially be an ECI. The responsible ministry and the sector will also look at infrastructures located abroad on which the Netherlands is dependent, which should be considered as an ECI. They will do this by using the criteria from the guidelines, supplemented with the method of the Dutch National Risk Analysis.

2. Information

By way of the interdepartmental joint committee and the CIP contact point, the impacted countries (Member States which are dependent on an infrastructure situated in the Netherlands) will be informed by a formal letter and invited to consult with the responsible Dutch ministry and the sector. This letter will be signed by the coordinating minister of the Ministry of the Interior and Kingdom Relations (BZK) and the responsible minister.

3. Designation

It will be agreed jointly (impacted countries and the Netherlands) whether the infrastructure concerned is an ECI or not. If requested, the European Commission may play a mediating role in this process. The decision whether an infrastructure in the Netherlands is critical at a European level will be taken in the Council of Ministers.

In addition:

4. Each year, the CIP contact point will send a copy of the relevant parts of the NRA (National Risk Analysis) to the European Commission.

5. Every four years, each responsible ministry shall also consider the impact on, and from, other countries in the integral analysis of CIP.

6. The CIP contact point is a joint committee of the various ministries (explicitly not under the sole responsibility of the Ministry of the Interior and Kingdom Relations), and handles process management, support, archiving and coordination. In process terms, the CIP contact point comes under the BZK Ministry, National Security Directorate.

The contact point is positioned as the Dutch contact and coordination point for EPCIP matters. The contact point will be characterised by approachability, dependability, coordination and expertise.

Composition of the contact point

For the execution of EPCIP, various parties are involved, which may have a role in the contact point based on their responsibility, expertise or the interests they represent. In order for the contact point to work properly, it is desirable to bring together the right parties in a joint committee.

In practice it means that the contact point consists of representatives of:

- The Ministry of the Interior and Kingdom Relations as the supervisor and contact point with the European Commission;
- The Ministry of Economic Affairs as being responsible for the energy sector;
- The Ministry of Transport, Public Works and Water Management as being responsible for the transport sector;
- The Ministry of Housing, Spatial Planning and the Environment as being responsible for the energy sector (nuclear and pipelines);
- The Ministry of Justice as being responsible for air transport security;

Advisory and knowledge centres such as the NAVI could be involved by the CIP contact point because of their knowledge of security and contacts with the sectors. The Ministry of Foreign Affairs will be informed regularly about the activities of the CIP contact point regarding establishing contacts with other Member States. The Ministry of Foreign Affairs can play a mediating role if this is desired.

21.3 Strategy & Policy

National Security Strategy

CIP is an integrated part of the national security strategy of the Ministry of the Interior and Kingdom Relations. In this CIP-policy programme, nine ministries, coordinated by the Ministry of the Interior and Kingdom Relations, cooperate to ensure a sufficient level of protection. The scope of the policy program is all-hazards. Since 80% of the Dutch critical infrastructure is owned or operated by private companies, it is imperative for public and private sector to work together closely to ensure a sufficient level of protection.

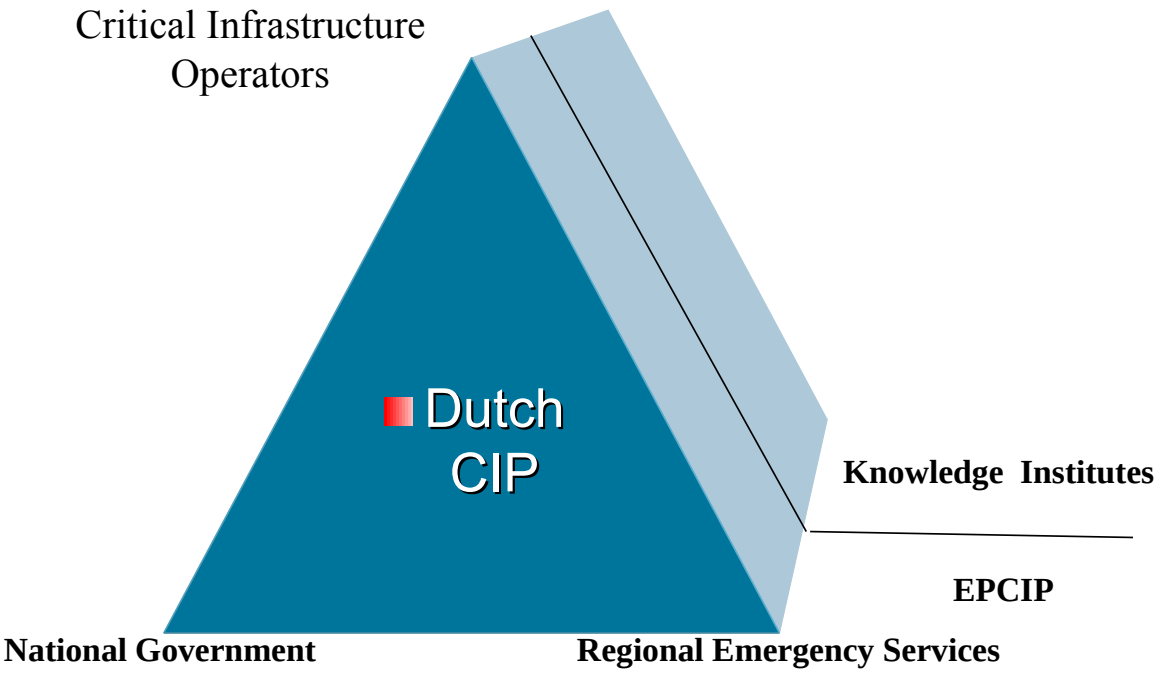


Figure 81: Dutch Approach to CIP

In this strategy a mechanism has been identified which consists of risk assessment, capacity building and policy arrangements which also include crisis response. In this regard, CIP is a specific area of interest.

The Ministry of the Interior and Kingdom Relations produces the National Risk Analysis on a yearly basis. In the assessment, threats to national security are identified and classified on the criteria of 'high/low impact' and 'high/low probability'. The threats to national security which score the highest in the National Risk Analysis (NRA) are used in the CIP programme as input for capacity building measures (protection/prevention/crisis response) in the various critical sectors of society. In the NRA of 2008, pandemic flu, worst imaginable flood from sea, and major blackout/failure of ICT were the highest scoring threats. Graphically, the national security strategy is presented as follows:

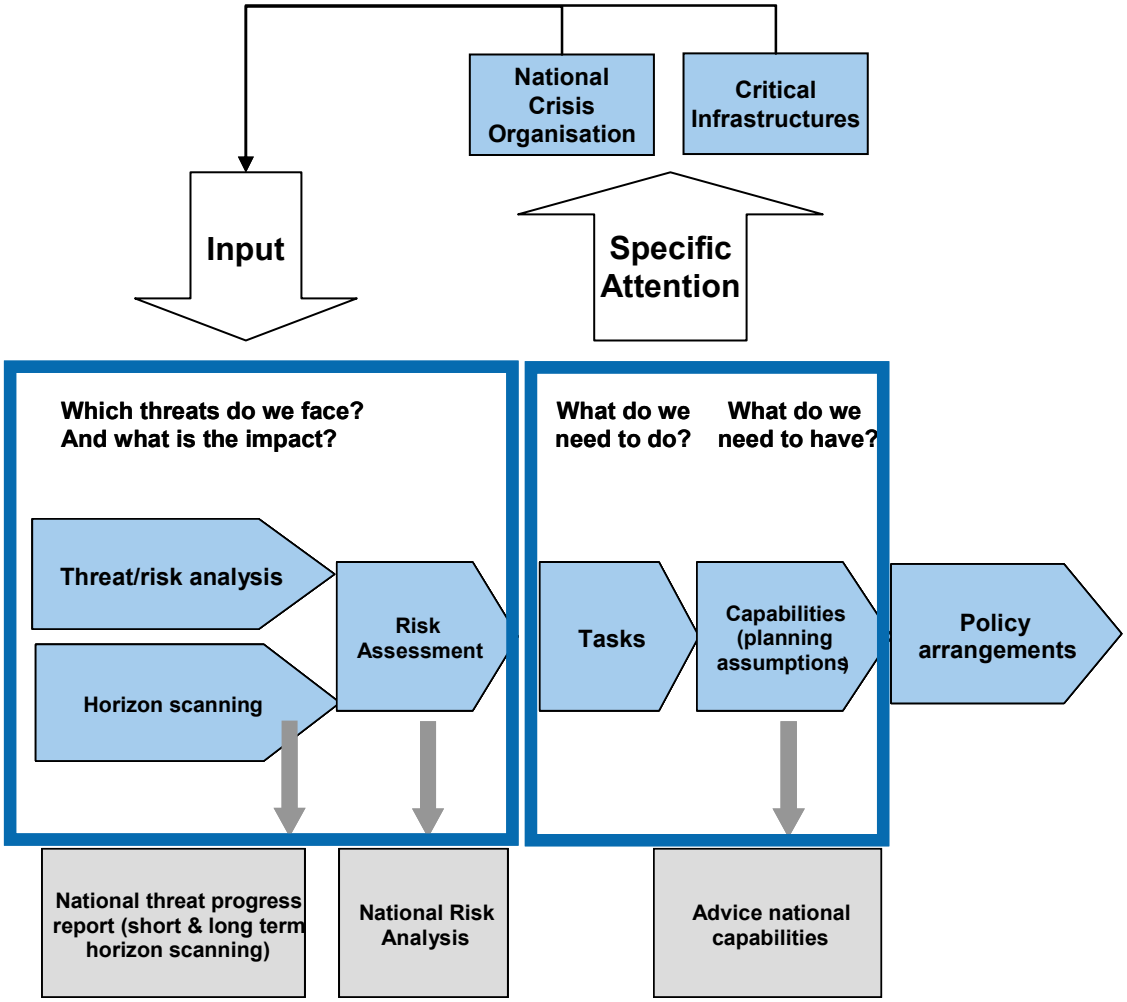


Figure 82: National Security Strategy

The resulting CIP system is based on the principle of responsibility within each sector, and the successful implementation of this approach requires close coordination between the national government, critical infrastructure owners/operators, and the safety regions.

The system is set up as shown below, with a set of expectations that are defined for the government and the critical infrastructure owners/operators. It is based on the belief that the incentive to preserve business continuity is a more effective tool than legislation to realize a high level of protection. Therefore, being part of a critical infrastructure requires participation in this system. On the other hand, in a crisis situation, critical infrastructure has priority attention of the government.

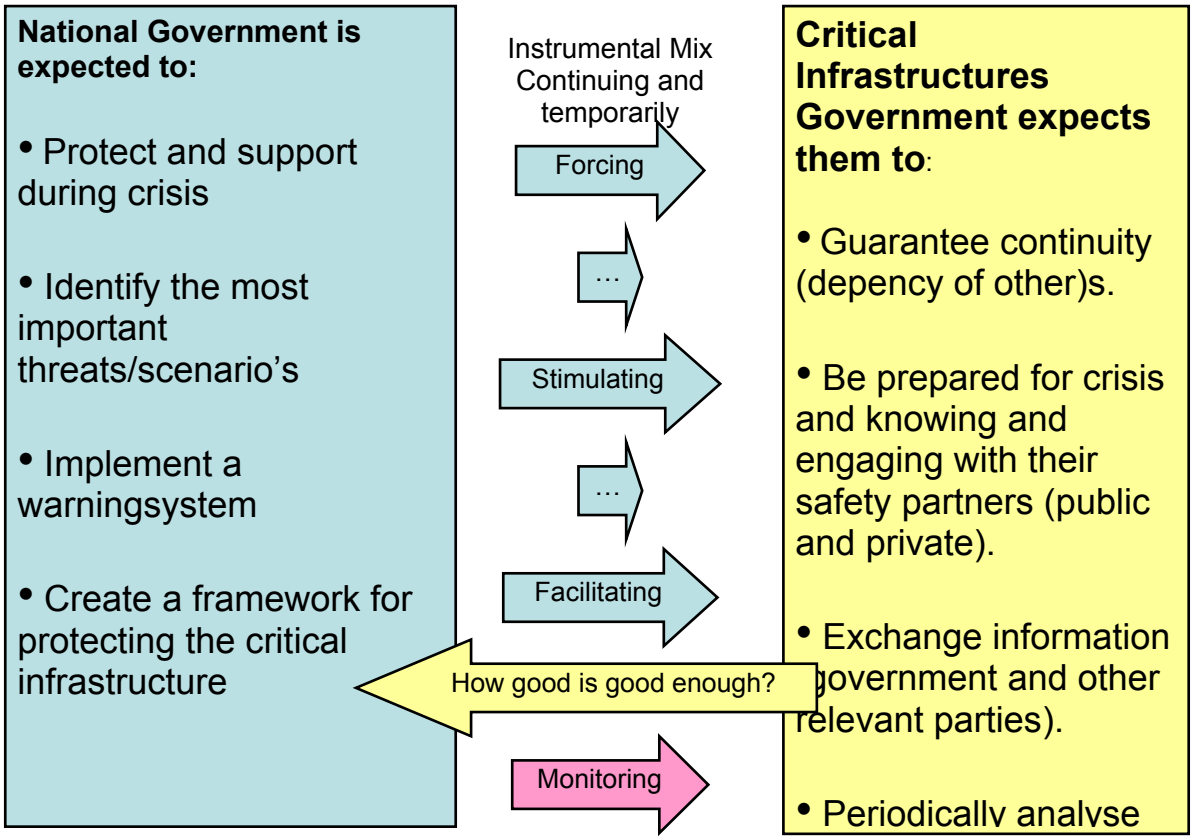


Figure 83: The CIP System and Expectations

The Dutch government has identified 33 products and services such as electricity, drinking water, dams, and banks as critical for society. [660] If one of these critical products or services fails, Dutch society could be significantly impacted.. To prevent failure of these types of critical products and services, the Dutch government initiated the CIP program in 2002. Nine Dutch ministries are involved in this policy program (refer to list above that outlines actors), coordinated by the ministry of Interior and Kingdom Relations. Within this program, the government works together with the public and private owners of critical infrastructure and with the largest Dutch employers' organization (VNO-NCW). Protection of critical infrastructure demands an intensive collaboration of private and public parties. The program's aim is threefold:

1. to prevent large scale failure or disruption as much as possible
2. to ensure public and private sectors are adequately prepared for the consequences of failure or disruption
3. To allow effective repressive measures to be taken in order to minimise damage caused by failure or disruption

The Netherlands have identified the following 12 critical sectors and 33 critical products or services.

[660] See www.nationale-veiligheid.nl

Sector	Product of Service
Energy	1. electricity 2. natural gas 3. oil
Telecommunication/ICT	4. fixed telecommunication services 5. mobile telecommunication services 6. radio communication and navigation 7. satellite communication 8. broad casting 9. internet access 10. postal services
Drinking water	11. drinking water services
Food	12. food service and safety
Health	13. emergency management 14. medicine 15. sera and vaccines 16. nuclear medicine
Financial	17. financial system 18. financial transfer government
Stemming and managing surface water	19. water quality management 20. stemming and management water quantity
Public Order and Safety	21. enforcement public order 22. enforcement public safety
Legal Order	23. dispensation of justice and detention 24. maintenance of law and order
Public Administration	25. diplomatic communication 26. government information handling 27. military order 28. public administration decision-making
Transport	29. main port Schiphol 30. main port Rotterdam 31. National infrastructure (main roads and rivers) 32. railway system
Chemical and nuclear industry	33. transportation, storage and production / handling of chemical and nuclear substances

Figure 84: Critical Sectors, Products, and Services

Although, some of these critical sectors are owned by the government, such as the management of surface water and public order and safety, about 80 percent of the critical infrastructure is owned by private parties. Therefore, the protection of critical infrastructures always demands public-private cooperation to be effective.

Cross-sector initiatives

Interdependencies

The Dutch CIP strategy recognizes that interdependencies are one of the key cross-sector issues in CIP and that critical sectors are also dependent on the continuation of other critical sectors. A key component of this strategy therefore revolves around knowing which inter-sectoral dependencies exist in order to enable critical sectors to prepare and take precautionary steps. In 2008, with all relevant public and private parties held joint workshops in order to enhance the knowledge and awareness of interdependencies. The national threats identified by the National Risk Analysis were the starting point.

Connection to crisis response organizations

In addition to preventing failure in critical sectors, the Dutch strategy also recognizes the importance of being ready if a failure occurs or if the probability of failure increases during crisis periods. In this regard, the national government finds it important that all relevant parties, from critical sectors to local crisis management services, are quickly alerted about upcoming threats. To help achieve this goal, the current alerting system for counterterrorism will be extended with some of the threats identified by the National Risk Analysis.

Policy

Although the various components of the Dutch CIP strategy are not based on legislation, the following key documents published by the Ministry of the Interior and Kingdom Relations establish the national CIP framework and processes:

- ***Critical Infrastructure Protection in the Netherlands: Quick-scan on Critical Products and Services***[661] ***(2003)***

  This report gave an overview on current Dutch CIP policy at the time. Written at the conclusion of the first phase of the CIP project, it contains the results of a Quick Scan on critical products and services in the Netherlands, as well as a background on the origin of the project and its foreseen future.

  In April 2002, the intergovernmental project on Critical Infrastructure Protection was set up to implement this action point. The first step of this comprehensive project comprised mapping out the Netherlands' critical products and services. Experts broadly representing industry and government helped to coherently investigate the range and interrelationship of their critical products and services. This yielded a clear

[661] http://www.minbzk.nl/bzk2006uk/subjects/public-safety/publications/5241/critical

picture as to which sectors, products, and services comprise the Netherlands' Critical Infrastructure and gave a preliminary view of possible negative consequences of their breakdown or disruption.

The conclusions of the Quick Scan phase can be summarized in the following five points:

1. In consultation with the government and industry, it was determined that the Netherlands' Critical Infrastructure comprises 11 sectors and 31 products and services. An up to date list of the critical sectors and product (expanded since then) is available on the BZK web site.
2. The Quick Scan gave the government and industry a clear understanding of the interdependencies of critical products and services and underlined the need for integrated protection. Critical business processes proved far more dependent on one another than the sectors had previously perceived.
3. The approach taken generated a systematic view of all forms of damage that may arise from the disruption, malfunctioning, or breakdown of a critical product or service (damage impact). There is a high degree of complexity, and there are many interdependencies. The disruption, malfunctioning, or breakdown of a vital product or service may generate cascading effects that could have a substantial impact on Dutch society, and that of its neighbouring countries, if no contingency or other protection measures are taken.
4. Those responsible for the contingency of critical business processes had a limited understanding of their interdependence and of the extent of this dependence. Therefore, protecting availability and integrity can only be accomplished by taking into account the supply chains as a whole.
5. In preventing and preparing for possible disasters, it is essential to recognise the differences in the breakdown and recovery characteristics of products and services that are part of a larger chain. The Quick Scan contributed to this effort by inventorying them.

- ***Critical Infrastructure Protection in the Netherlands***[662] ***(2005)***

The second report on Critical Infrastructure Protection (CIP) in the Netherlands and it gives a more comprehensive overview of the Dutch CIP approach. In the report, the backgrounds of the project are explained, the distinguished starting points are highlighted, and a description of how the Netherlands have organised CIP is included.

This next phase is elaborated into three sub-projects:

1. Identifying critical junctions (also in terms of geographic location) between critical sectors and services.
2. Mapping out the vulnerability of sectors and junctions, as well as obtaining insight into protective measures already implemented.
3. Developing a cohesive set of protective measures, including any additional protective measures, and embedding the measures to protect critical

[662] http://www.minbzk.nl//bzk2006uk/subjects/public-safety/publications/10447/critical_0

infrastructures within the standard business operations of the government and business community.

These sub-projects are explained in the report as well. Finally, this document discusses the state of affairs of the project. The first sub-project is already underway. In March 2004, a list announcing the junctions between critical sectors and services (also in terms of geography) was presented to the Parliament. The Parliament is informed that this list of junctions is neither exhaustive nor definitive.

Refining of the list will continue during the implementation of the vulnerability analysis. The Parliament is notified as well that involved parties gained a clear understanding of the complexity of the subject. Accordingly, there is a broad consensus around the fact that the protection of critical infrastructure isn't a once-only activity. CIP needs continuous attention, and it must be seen as a cyclical policy-process. This means that, although the project ended in June 2004, the ministries involved will continue to work on finalising and maintaining the set of measures.

- ***National Security: strategy and work programme 2007-2008***[663]

  In order to be optimally prepared for various threats, the Cabinet has drawn up a national security strategy. It puts the roles and responsibilities of all parties involved in a coherent framework. An integrated, whole-of-government approach to Dutch national security is a central component of this strategy.

- ***Final report: National Safety & Security. Responding to risks to citizens, communities and the nation***[664] ***(2008)***

  The report identified three key themes. The first is the need to follow a process of identification, assessment, and mobilisation in any crisis situation. The second key theme was that the "novelty" factor should be reduced as far as possible, and there should be no surprises. Finally, creating the right political structure is key; making sure that someone is in power who can actually drive this agenda forward. If the leadership is not legitimised, it will be hard to achieve common goals.

- **Trend report/2009: Insight into cyber crime: trends & figures**[665]

  This report is about the current state of affairs in cyber crime and information security in the Netherlands, and it contains information about the latest technical advances made by internet criminals and the impact on end users, government, and industry.

21.4 Methodologies & Standards

- ***"National Security: strategy and work programme 2007-2008"***

  The National Security Strategy is a working method that better enables the Dutch Cabinet to determine which threats endanger Dutch national security and how to anticipate those threats, irrespective of their origin or nature. In addition, the method helps the Cabinet view these choices in regards to their relationships with each other.

663 http://www.minbzk.nl/bzk2006uk/subjects/public-safety/publications/106955/national-security
664 http://www.minbzk.nl//bzk2006uk/subjects/public-safety/national-security/publications/115984/final-report
665 http://www.govcert.nl/download.html?f=115

While new, the working method makes use of existing, sector-oriented processes; these come together in the working method, thus enriching information and insights and increasing knowledge. From 2009 onwards, the working method will be applied across the full range of national security issues. The period up to 2009 was used to roll out the working method. The introduction in stages is described in the 2007-2008 work programme.

The working method will generate a strategic (long-term) foresight report every two years, the yearly selection of threat themes requiring in-depth analysis, and a twice-a-year government-wide horizon scan of shorter-term threats. This scan will result in the “Threat Assessment Netherlands” report. Moreover, annual results of the national risk assessment will be presented in the “Risk Assessment Netherlands” report.

In order to accomplish this goal, the working method starts by analysing the threats facing the Netherlands, assessing those threats in terms of risks to the vital interests, and positioning these risks vis-à-vis each other: the national risk assessment.

The Dutch Cabinet will then decide which risks will be prioritised for detailed treatment in the strategic planning stage. At that stage, the method will determine which capabilities the government would require to deal with the prioritised risks and which capabilities it already possesses and/or can expect from external parties such as the business community, social organisations, and international organisations. The Cabinet will then decide if, where, and how national security must be strengthened. The political/administrative choices will then be translated into policy, legislation, and concrete measures. The development of the choices made by the Cabinet is not only in the hands of the national government: other public authorities, the business community, and social organisations also play a role.

In order to enable an integral approach, all parties involved must know and respect each other's role in strengthening national security, follow a shared doctrine, align their working methods, and be connected to the same communication network.

As many threats to national security do not originate in the Netherlands, but can have consequences there, a purely national approach is not sufficient for realization of the complete Dutch strategy. International cooperation, both at bilateral and multilateral level, is vital for reinforcing national security. The Cabinet is going to put security topics that require an international approach on the agenda. Wherever relevant, it will work in an international context to generate the capabilities deemed necessary to withstand threats. European programmes will also be leveraged to this aim. The goal of the Cabinet is to intensify the relationships with countries that use similar working methods to guarantee national security.

The goal of the strategy for national security is to protect the vital interests of the Netherlands in order to prevent societal disruption. These interests are also explicitly used in the risk assessment method. The five vital interests are: territorial security, economic security, ecological security, physical security and social and political stability.

The working method looks beyond threats: planning and policy are no longer based on specific (known) threats, and instead the degree in which national security is or can be threatened is taken as the point of departure. “Looking beyond threats”

presumes an approach whereby the borders between sub-areas of national security (which have been demarcated between ministries, local governments, and other organisations) become blurred, thus preventing that topics are dealt with twice over or, worse still, end up not being discussed at all.

- ***The Dutch CIP methodology***

  The first step of the phased plan of the CIP project involved a Quick Scan on critical products and services with the objective to:

  1. Give an overall view of the essential products and services that comprise the Netherlands' Critical Infrastructure
  2. Determine their (inter)dependencies, and
  3. Give a preliminary view of the negative consequences as a result of their possible breakdown

  After the Quick Scan phase, the Dutch government identified the following three main sub-projects to achieve the final results in a more effective manner:

  Identifying critical junctions (also in terms of geographic location) between critical sectors and services. Part of the network of industrial and policy processes, junctions occur at the crossroads of critical products or services which are either completely or largely interdependent. This level of dependence is described in the Quick Scan report. Geographic junctions involve spatial groupings of critical products and services. Identification is necessary as a starting point for the determination of junctions between critical sectors and services. This list of junctions must offer a clear view of the critical sectors and services involved, the vulnerability of which at the very least must be investigated.

  Mapping out the vulnerability of sectors and junctions. The objective is to obtain insight into protective measures already implemented. Scenarios are used to identify and map out vulnerabilities. In this process, the critical sectors and junctions will at least be assessed in terms of vulnerabilities that are the result of: technical or organisational problems (i.e. a wide range of human and material factors that play an essential role in the continuity of critical products and services); deliberate or accidental human action; natural disasters.

  The ministries perform the vulnerability analysis as an extension of sub-project 1. Because the circumstances in each sector differ significantly, it is difficult to develop a uniform, project-wide approach. Therefore, the manner in which the vulnerability analysis will be implemented is determined on a sector-by-sector basis. It is essential that the scenarios will be applicable in as broad a manner as possible. They must be tailored in order to reveal as many of the sectors' vulnerabilities as possible. In addition, the scenarios must reflect the nature of the sector itself as much as possible in order to generate a solid understanding of the sector's possible vulnerabilities.

  Developing a cohesive set of protective measures, including any additional protective measures and embedding the measures to protect critical infrastructures within the standard business operations of the government and

business community. To facilitate the decision-making process for the Dutch Cabinet, the ministries will elaborate solutions for any shortfalls in consultation with the other tiers of government involved, social partners, and the business community. These solutions will be based on the Dutch Cabinet's assessment and with due consideration of the vision of the Parliament regarding the findings of the CIP project. An integral component of the ministerial proposal is the division of responsibilities and authority regarding the protection of critical infrastructures and financing the measures (including additional measures) to be taken.

21.5 Public – Private Partnership & International Collaboration

- ***Strategisch Overleg Vitale Infrastructuur, SOVI (Strategic Board for CIP)***

  The Strategic Board for CIP was established in September 2006 as a dedicated public-private partner-ship for critical infrastructure protection. All critical sectors are represented in the strategic board, which meets two or three times a year. In 2007, the SOVI initiated a study on the electric power dependency of the various critical sectors and their resilience and ability to cope with longer duration power outages. It investigated issues such as secondary dependencies (e.g., dependency of various sectors on diesel oil for back-up generators) and the way in which these are prioritized amongst the critical sectors. It also studied the question of which related arrangements already exist or have yet to be made.

- ***Nationaal Adviescentrum Vitale Infrastructuur (NAVI) (The National Advisory Centre for the Critical Infrastructure)***

  Although NAVI is not an official Public-Private Partnership, the Dutch government intends to make this formal distinction during upcoming development. NAVI has knowledge and expertise about the security of critical infrastructures and aims to exchange these with the critical sectors, critical sector enterprises, and government agencies. It builds upon its links within the government and critical sectors, such as current information provided by the AIVD and the Dutch National Coordinator for Counterterrorism (NCTb). NAVI offers various services to its constituency such as support for risk analysis as well as security advice. NAVI's modus operandi is derived from the (physical security aspect) of the UK's Centre for the Protection of National Infrastructure (CPNI). It has established sector-specific information exchanges between critical sectors and government functions. NAVI offers various services such as a front office and advisory function for critical infrastructure enterprises, good practices, and an international contact desk (information and good practices exchange with other nations and the EU). NAVI offers products such as risk analyses and risk methodologies, critical sector-specific threat scenarios, security methodologies, and advice.

Regarding activities outside of The Netherlands, international cooperation enables the Netherlands to influence developments over which it otherwise has no control. This is possible by means of bilateral (e.g. in the case of flood risk) or multilateral (e.g. in the case of ICT security) agreements. The Netherlands can also provide

substantive inputs into the (national and international) security-relevant policy of international organisations. The Netherlands underscores the importance of international cooperation and utilises all possibilities it offers. It will take an active stance in international organisations and forums. As a member state of, interalia, the European Union (EU), the United Nations (UN), the North Atlantic Treaty Organisation (NATO), and the Organisation for Security and Cooperation in Europe (OSCE), the Netherlands is aligned with and agrees with the security strategies of these organisations. Said strategies particularly describe the possibilities of international cooperation and the role that international organisations play therein, and leave scope for the member states in the realisation of their own national policy to reinforce security.

21.6 Funding & Human Resources

Although there is no official funding program for CIP activities, each ministry is responsible for funding the activities within its sector through normal operating budgets.

There are currently nine staff members within the Ministry of the Interior and Kingdom Relations, Directorate for National Security, working exclusively on CIP-related topics. In addition, there are approximately twenty dedicted staff members working in NAVI.

21.7 Training & Exercises

- ***Waterproef (November 2008)***

  In November 2008, a three-day large scale exercise on flooding took place. Its aim was to establish whether councils, provincial administrations, and government agencies would be able to operate in an efficient, integrated manner in the face of the worst imaginable flood disaster.

  The emergency scenario involved a severe storm in the North Sea, coupled with high spring tides, high seas, massive waves, and rivers bursting their banks. Exercises on an unexpected breach in a dyke also formed part of the drill and afterwards elements such as crisis communication and how to deal with all the issues following the crisis in order to return back to normalcy were discussed.

- ***Voyager (October 2007)***

  The large-scale national, multi-disciplinary crisis decision-making exercise code-named Voyager took place on 3 October in The Hague and Rotterdam. This exercise involved a collision between a container ship and a passenger ship, along with a threatened terrorist attack.

- ***Shift Control Exercise (2007)***

  The “Shift-Control” exercise, organized and implemented by the government in June 2007 consist of a large-scale ICT-attack with socially disruptive consequences was simulated within the “Shift-Control” exercise. The Dutch government took part in this exercise up to ministerial level, where various parties from the public and private

sectors, including GOVCERT.NL provided support: this was a well planned exercise. There was also an international exercise. At the start of 2008 a delegation from GOVCERT.NL took part as an observer during the Cyber Storm II12 exercise in the United States. This was not a full participation, but rather the chance to follow activities from close up and to talk to participating organisations. The visit confirmed how important exercises are. The preparations alone, which took approximately 18 months in the case of Cyber Storm II, give the participating organisations numerous leads for improvements that they can implement themselves to be better prepared for a digital attack.

- ***Bonfire exercise[666] (April 2005)***

  This large multidisciplinary exercise, codenamed Bonfire was held in the ArenA (the Netherlands largest stadium) in Amsterdam. During this exercise, a mock terrorist attack was carried out during a concert, in the presence of a large number of spectators. The Bonfire exercise was organised by the Dutch Ministry of the Interior and Kingdom Relations and the municipality of Amsterdam. Along with various ministries, the participants included the province of North Holland, the Amsterdam ArenA, the municipality of Amsterdam and the emergency services, including those with dedicated tasks such as safety and security, information, backup and communications. Some 2,000 persons in public administrative positions, civil servants and emergency workers took part. In addition, several thousand people played the roles of the victims and the public.

- ***National Nuclear Crisis Management staff exercise (2005)***

  Carried out on 25 May 2005 in cooperation with the nuclear plant in Borssele. Representatives from many of the CIP sectors were involved. The security agreements for nuclear installations between company and local triangle are provided for in the so-called IBO/EBO system (Internal and External Safety Organisation).

21.8 Sector – Specific Key Players & Initiatives

ENERGY

Public Authorities:

- ***Ministerie van Economische Zaken* (The Dutch Ministry of Economic Affairs[667])**

  The mission of the Ministry is to promote sustainable economic growth in the Netherlands. The political responsible of the ministry is in hands of the Minister of Economic Affairs, who is part of the Dutch Cabinet.

Initiatives:

- ***Vulnerability analysis and findings***

666 www.minbzk.nl//bzk2006uk/subjects/public-safety/publications/53955/what_can_be_learned
667 **http://***www.ez.nl*

A vulnerability analysis of the interconnections within the energy sector was conducted using an extensive collection of realistic possible scenarios and causes of problems that are the most relevant for the critical energy sub-sector in question. The analysis led to a classification of the vital interconnections to residual risk, to allow, for example, a distinction to be made between oil, gas and electricity, and between the different regions. It also indicated that the energy sector is, to a significant degree, already fortified against threats. There is an extremely high level of continuity and supply guarantee in The Netherlands.

Nevertheless, a few problem areas were also identified. In order to eliminate these in the future, preventative as well as repressive measures were assessed. These are measures that must be taken either by the public sector or the private sector, or both. Problem areas and measures were compiled in a list of areas of improvement. On the preventative side, this included, but was not limited to:

1. the harmonisation of the overall safety and security policy in all sectors;
2. overall safety and security policy as regards the energy sector;
3. access granted to outside parties as a result of outsourcing;
4. overall safety and security of objects;
5. personnel and hiring policies;
6. and the freedom of movement around critical interconnections.

On the repressive side, this included:

1. powers and responsibilities of the parties involved; provision of information;
2. mutual preparation;
3. and means of communication.

NUCLEAR

Public Authorities:

- ***Ministerie van Volkshuisvesting, Ruimtelijke Ordening en Milieu – VROM*** **(The Dutch Ministry of Housing, Spatial Planning and the Environment[668])**
  This Ministry is responsible for policies on public housing, spatial planning, the environment, and the housing of national government agencies.

Initiatives:

The Netherlands has a small nuclear programme. The country currently has only one nuclear power plant (NPP), located in Borssele and operated by the Electricity Generating Company for the Southern Netherlands (EPZ). Moreover The Netherlands has three research reactors in operation.

Nuclear supervision is exercised by several (mainly governmental) organisations. These are staffed by only a very small number of people: a reflection of the small scale of the country's nuclear programme. Plants operate under licence, awarded after a safety

668 http://www. vrom.nl

assessment has been carried out. This is based on the Safety Requirements and Safety Guides[669] in IAEA Safety Series 50, as amended for application in the Netherlands. The licence is granted under the Nuclear Energy Act. The current government, in office since the start of 2007, has decided that during their term of office, no (additional) nuclear power plants will be built[670].

INFORMATION AND COMMUNICATION TECHNOLOGY

Public Authorities:

- ***Ministerie van Economische Zaken* (The Dutch Ministry of Economic Affairs[671])**

  The mission of the Ministry is to promote sustainable economic growth in the Netherlands. The political responsible of the ministry is in hands of the Minister of Economic Affairs, who is part of the Dutch Cabinet.

Initiatives:

- ***Vulnerability analysis and findings***

  Studies and vulnerability analyses that were conducted revealed that many services, processes and underlying infrastructure are highly dependent on the ICT sector. Failure or disruption of these critical services can form a huge risk, regardless if caused by intentional human actions, technical failures, or natural disasters.

  Telecommunication service providers have a clear responsibility to ensure proper continuity. Specifically, this means that they actively take measures where necessary. Consequently, the interests on the part of the providers match public interest to a significant degree. Parties have already made many arrangements among themselves in order to confine possible damage to systems.

DRINKING WATER

Public Authorities:

- ***Ministerie van Volkshuisvesting, Ruimtelijke Ordening en Milieu – VROM* (The Dutch Ministry of Housing, Spatial Planning and the Environment[672])**
  This Ministry is responsible for policies on public housing, spatial planning, the environment, and the housing of national government agencies.

Initiatives:

669 Since the introduction of IAEA Safety Series No. 50 as the basis for the Dutch regulations, the nomenclature of the 'Codes' of the IAEA NUSS programme has been changed to 'Standards'. For this reason, the terms 'Code' and 'Standard' are both used in this report.

670 Convention on Nuclear Safety, National Report of The Kingdom of the Netherlands Fourth Review Meeting (April 2008)

671 **http://***www.ez.nl*

672 http://www. vrom.nl

Drinking water supply continuity and quality have been well organised for years. The water companies' supply plans serve as the policy framework, and in practice any long-term disruptions to the supply of drinking water seldom occur. In 2002, the project Netherlands' Water Sector Security (Beveiliging Nederlandse Watersector - Benewater) began. An initiative of two water companies, the Association of Dutch Water Companies (VEWIN) and the central government (VROM and BZK), and the General Intelligence and Security Service (AIVD), the project was prompted by the events that took place on 11 September 2001. As a result, the sector has reached agreements on a basic level of security. As part of the Critical Infrastructure Protection project, an assessment was made to determine whether the supply plans and the agreed level of security adequately cover the drinking water supply.

- ***Vulnerability analysis and findings***

  The sector has been evaluated in terms of natural disasters, technical-organisational failures, and intentional human action, as well as inter-sectoral dependencies. The sector is well prepared for the first two start events mentioned, and improvements will be made on preparations for responding to intentional human action. Deliberate human action in this case refers to a simple or complex threat to or actual contamination of drinking water at regional or national level, which could cause widespread panic and result in people being afraid to drink or use drinking water, and at the same time the water companies being unable to offer an absolute guarantee regarding the safety of the drinking water.

STEMMING AND MANAGEMENT OF SURFACE WATER

Public Authorities:

- ***Ministerie van Verkeer en Waterstaat; V&W*** **(The Dutch Ministry of Transport, Public Works and Water Management[673])**
  This Ministry is responsible for the Dutch system of water management, public and private transport and infrastructure. The Motto of the ministry is "familiar with water, progressive with connections" to be updated. The ministry has two main responsibilities: regulation and management of transportation of people and goods via roads, trains, boats and airplanes; Water management by water works, such as dikes, polders and channels.

Initiatives:

An important concern of the government is the protection against flooding and the supply of clean and adequate water for all users. Protection against flooding is achieved by building and maintaining dikes. These are classified according to four categories:

1. primary dikes: protection against flooding from the major rivers, IJsselmeer, Markermeer and the sea;
2. regional dikes: protection against flooding from regional waters;

673 **http://***www.verkeerenwaterstaat.nl*

3. drainage: draining hinterlands for the sake of providing protection against flooding;
4. water quality: preventing large-scale pollution of surface water.

An object is considered critical when failure would result in damages exceeding 5 billion euros, or in large numbers of casualties. Critical characteristics of the surface water stemming and management sector Inventories and workshops were used to map out the vitality of the surface water stemming and management sector. A distinction was made among the four categories mentioned.

An analysis of the categories led to the following conclusions:

- Primary dikes: the majority of the primary dikes (ca 75%) are considered critical.
- Regional dikes: a small percentage of the regional dikes (ca 10%) are considered critical.
- Drains: only a small number (10 maximum) of drains should be considered critical.
- Water quality: is not considered critical.

- ***Vulnerability analysis and findings***

  The water-stemming sector is first and foremost vulnerable to natural disasters: the entire system of dikes is designed to prevent flooding from extremely high water, whether or not in combination with a severe storm. There is a slight chance that a dike will burst on account of a greater amount of stress than the dike is legally required to accommodate. Other causes, including intentional human action as well as technical or organisational, cannot be ruled out entirely. Managers are confronted regularly with vandalism. And a terrorist attack is not completely unthinkable. However, this would only have an effect in a situation involving high water, which occurs very rarely. Due to the necessary combination of deliberate sabotage with natural conditions, the odds of a terrorist disturbance that has critical consequences are considered slim. Overdue maintenance and construction and design errors are possible causes, and have already garnered the sector's attention. Quality guarantee has already been built into the normal management processes. The chances of technical failures with critical consequences are considered small.

FOOD

Public Authorities:

- ***Ministerie van Landbouw, Natuurbeheer en Voedselkwaliteit; LNV*** **(The Dutch Ministry of Agriculture, Nature and Food Quality[674])**
  The Ministry is responsible for four fields of policy: agriculture and *fisheries;* natural conservation, open air recreation and national parks; food safety; rural development.

[674] **http://***www.minlnv.nl*

Initiatives:

- ***Vulnerability analysis and findings***

  The geographic distribution of elements that contribute to securing the food supply, such as food production and distribution, seems to indicate that specific measures are not necessary. In the event that the largest production location should fail, the food supply would not be in danger in any branch. Also, other foods could substitute for many types of food in case of emergency. However, a special point of attention here is the relationship between food supply and food safety. The vulnerability of the food sector lies primarily in unsafe food eaten by many people, which could cause major social disturbance.

  Many branches in the food sector are highly dependent on the same critical products and services, with drinking water, energy and road transport being the most important. Large-scale failure of these critical products and services pose the greatest risk, regardless of the underlying cause. The second group of start events that could have a significant impact consist of intentional human action in the form of a terrorist attack or sabotage intended to contaminate food or foodstuffs.

HEALTH

Public Authorities:

- ***Ministerie van Volksgezondheid, Welzijn en Sport*; VWS (The Dutch Ministry of Health, Welfare and Sports[675])**
  It is the public health authority of the Netherlands. The ministry is responsible for three policy areas: public health and health care, welfare and social-cultural work, sports.

Initiatives:

- ***Vulnerability analysis and findings***

  Although disruptions in health care do not directly affect other sectors at the “critical” level, health care is important in a social sense. Therefore, additional security measures, among others, are being taken.

  Medical assistance is distributed across a vast number of private enterprises and professionals, such as hospitals and general practitioners. Consequently, the loss of one institution or a number of medical professionals can be sufficiently covered within the sector, thanks to the quantity and distribution. The institutions themselves are primarily responsible for risk management at their company. As a rule, large-scale disruption to emergency medical assistance and other hospital care will be the result of (partial) failure of another critical sector.

  The most significant vulnerability is the dependence on other sectors such as energy (electricity and oil), drinking water, and the availability of sufficient (personnel for) relief for large numbers of victims. Whether the existing measures are adequate depends on

675 http://*www.minvws.nl*

the nature and scope of the disaster, the degree of exposure, and alternative arrangements.

FINANCIAL

Public Authorities:

- ***Ministerie van Financiën; Fin*** **(The Dutch Ministry of Finance[676])**

  The Ministry is occupied with the national budget, taxation and financial economic policy, including supervision of financial markets.

Initiatives:

A working group chaired by the Ministry of Finance's Financial Markets Directorate was appointed for the study of critical infrastructure in the financial sector. This working group conducted an analysis that involved examining this sector's dependencies, vulnerabilities and protective measures.

The financial sector comprises four critical services: counter payments, mass giro transfers, the large-value payment systems, and securities transactions. The (partial) failure of counter payment traffic immediately causes social disturbance, due to the fact that payments either cannot be made or incur delays. Moreover, when transactions cannot take place, financial-economic damage occurs in the form of turnover loss among businesses. However, a high degree of substitution typifies the system of counter payments, and, generally speaking, in the event of a short term disruption involving one means of payment, another means of payment can be used as a substitute fairly easily.

The financial sector is dependent on the following critical infrastructure: electricity, fixed telecom, mobile telecom, Internet and post and courier services. The most important dependencies in the financial sector are electricity (for payment transactions) and fixed telecom (for all processes in the financial sector). The 'mass giro transfer' system is the most sensitive to disruptions in other sectors. The system is affected by disruptions in virtually every underlying infrastructure. Counter payment transactions are also highly dependent on other infrastructure. Premium inter-bank transactions and securities transactions have fewer dependencies; these services rely mainly on fixed telecom. Power failures will have an impact primarily on consumers and businesses; practically every institution in the financial sector is fitted out with no-break equipment. However, telecom outages could have major consequences for the financial sector.

For the financial sector, the risk of falling victim to terrorism is becoming increasingly important. Experiences in the United States, Turkey and Spain have shown that financial sector can serve as a serious target for terrorists. A major terrorist attack in the Netherlands will likely have an extremely severe impact on Dutch society. The major blow to the financial sector will be if the attack were to result in loss of personnel. Terrorist attacks can also affect (confidence in) the economy, and consequently also affect the financial sector.

676 **http://**www.minfin.nl/en/home

TRANSPORT

Public Authorities:

- ***Ministerie van Verkeer en Waterstaat; V&W*** **(The Dutch Ministry of Transport, Public Works and Water Management[677])**
  This Ministry is responsible for the Dutch system of water management, public and private transport and infrastructure. The Motto of the ministry is "familiar with water, progressive with connections". The ministry has two main responsibilities: regulation and management of transportation of people and goods via roads, trains, boats and airplanes; Water management by water works, such as dikes, polders and channels.

Initiatives:

In general, transport is not considered vulnerable: the existence of dense networks and different modes of transportation make it hard to imagine that disruption could occur across the board. Although the disruption of a few links in the chain would initially create a significant obstacle, alternatives would quickly become available for specific transport channels for critical functions.

Nevertheless, four specific elements in the transport system demand special attention in the context of Critical infrastructure Protection:

1. Main port Schiphol
2. Main port Rotterdam
3. Main road network and main waterway network, managed by Rijkswaterstaat (the Directorate-General for Public Works and Water Management).

These form the backbone of the landside transport system. Within these, specific links can be distinguished that could give rise to “critical”-scale disruption. National infrastructure with a damming function is included in the same context.

4. Railway: although the railway system’s part in the transport sector is indeed limited, “critical”-scale disruption is conceivable, given the inherent accessibility and concentration of people.

In general, the CIP project encompasses a permanent route with many parties involved. In order to prevent the project from losing its effectiveness due to the fact that so many are involved, the sectors will have to develop a framework with the Ministry of the Interior and Kingdom Relations. Special attention is especially required for both main ports for the regional approach in addition to the sectoral approach presently in place.

- ***Main port Schiphol***
  Schiphol serves a pivotal role in the air transport of passengers, high quality and perishable goods, and other key goods. The economic activity that this generates in the surrounding commercial and (high-grade) industry is of vital importance to the

[677] **http://***www.verkeerenwaterstaat.nl*

Dutch economy. The economic spin-off of the Main port can be directly related to the unimpeded continuation of a number of critical services and processes. The scope of the CIP project for the Main port includes:

- The aviation industry, including (ground) handling of air traffic, handling passengers and cargo, along with the accompanying logistic processes.
- The critical business processes and services of air traffic control (Luchtverkeersleiding - LVNL) and KLM/Air France in and around Schiphol and accompanying infrastructure.
- The other critical activity and accompanying infrastructure in and around Schiphol such as a number of critical office buildings and fuel distribution locations.

A critical relationship exists with the access infrastructure in and around Schiphol such as the State, provincial and municipal road system, the railway and the (international) air routes.

- ***Main port Rotterdam***
  Main port Rotterdam is an international seaport that plays a key role in foreign trade. This key role is of vital importance not only for the Dutch economy, but also for a considerable part of the European hinterlands and global flows of goods. In addition to serving as a logistic interconnection, which includes trade and distribution centres, the Main port Rotterdam is also an important (petro)chemical / industrial complex. An estimated 80% of the oil for the EU market passes through Rotterdam, more than 50% of the strategic European oil reserves are located in the main port area, and 18% of the American oil imports come from Rotterdam.
- ***Main roads and waterways (national infrastructure)***
  With national infrastructure forming the backbone, roads and waterways make up an intricate system in the Netherlands. Generally speaking, this system is well protected against large-scale disruption on a critical scale, thanks to the large number of alternative routes available. A specific analysis is advisable due to the concentration of critical functions around both main ports and the dependence on transport connections.
- ***Railway***
  As sub-sector, the railway has been grouped within the critical sector Transport on account of its proven (social) vulnerability in the wake of the attacks in Madrid on 11 March 2004.

  For the purpose of contributing to the CIP project, the Dutch government formed a “Railway Security Platform” (Platform Security Spoor) comprising representatives from the Ministries of Transport, Public Works and Water Management, Justice, and the Interior and Kingdom Relations, as well as the railway sector (NS and ProRail) and the AIVD. The platform will continue to meet regularly, not only in connection with the CIP project.

CHEMICAL

Public Authorities:

- ***Ministerie van Volkshuisvesting, Ruimtelijke Ordening en Milieu – VROM*** **(The Dutch Ministry of Housing, Spatial Planning and the Environment[678])**
  This Ministry is responsible for policies on public housing, spatial planning, the environment, and the housing of national government agencies.

Initiatives:

- ***Vulnerability analysis and findings***

  The Major Accidents Risks Decree (Besluit risico's zware ongevallen - BRZO) provides for external safety ("safety") and with that technical-organisational errors. Intentional human action ("security") took priority in the risk analysis. The vulnerability analysis revealed that the chances of terrorists targeting the chemical sector for an attack are extremely slim. The resistance capacity of the regular external security policy is more than enough, but offers insufficient guarantees in the event of a terrorist attack such as in London in July 2005.

  Should terrorists nevertheless decide to carry out an attack, a number of risks with disastrous effects are conceivable. It involves businesses with installations and storage tanks, transports of hazardous materials by rail, road or inland shipping, and theft of chemicals that could be used to make explosives. Other groups that could pose a potential threat include hackers, vandals, and company employees. The acts involved include cyber crime, vandalism to railroad tracks, shunting-yards and parking areas, or sabotage to a chemical installation bya company employee.

ADDITIONAL SECTORS IDENTIFIED BY THE NETHERLANDS (BUT NOT BY THE EUROPEAN COMMISSION) AS CRITICAL

PUBLIC ORDER AND SAFETY

Public Authorities:

- ***Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*** **(The Dutch Ministry of the Interior and Kingdom Relations[679])**
  The ministry of the Interior and Kingdom Relations (BZK) is one of the thirteen ministries of Dutch central government. The Directorate of National Security leads the Inter-Ministerial workgroup and the Netherlands CIP program. In addition to its lead role in the working group, the Ministry also holds a second operational role in relation to its mission to: uphold the Constitution; guarantee the democratic rule of law; ensure an effective and efficient public administration; coordinate urban policy; promote public order and safety and provide centralised management of the countries police forces; promote the quality of the civil service and coordinate management and personnel policy for all civil servants; coordinate cooperation with Aruba and the Netherlands Antilles.

678 http://www. vrom.nl
679 **http://** www.minbzk.nl

Initiatives:

Introduction

The disciplines that are involved with upholding Public Order and Safety (fire brigade, police, and medical assistance) are designed to respond to incidents and to minimise the harmful effects of these incidents. The operational and administrative direction (local, regional, provincial and national) in upholding Public Order and Safety is set forth in various legislation, including the Police Act 1993, the Fire Services Act 1985 and the Disasters and Major Accidents. The main task of the Public Order and Safety (POS) sector is to preserve public order, provide help in emergency situations, and be in charge of safety and security in the Netherlands. Large-scale and long-term disruption in the sector or parts thereof could lead to the collapse of Dutch society. Alternatives for these services that are available for the long term and on a large scale are limited. For these reasons, the POS sector is regarded as critical.

Critical aspects

In order to be able to perform its duties properly, the POS sector depends on three main critical aspects:

- Manpower (use of POS personnel).
- Equipment (vessels, vehicles and airplanes, and the facilities that support operations).
- Communication facilities (incident rooms, including the information and communication systems used in the incident rooms, such as C2000, GMS, emergency number 112 and telephones, WAS and OMS).

POS sector vulnerability

Most importantly, the POS sector must perform optimally under circumstances caused by disruptions in critical components of society. Accordingly, this was explicitly taken into consideration when evaluating the vulnerability of the POS sector. Furthermore, unlike any other sector, the POS sector has been educated and trained to be able to find ways to function as best possible under extreme conditions. A list of start events drawn up among departments was used as the blueprint for assessing vulnerability.

Organisational and technical causes

There is no identifiable organisational reason that would shut down an important part of the POS sector. Although the high degree of organisation in the sector does make going on strike a possibility on a large-scale, under no circumstance would this hinder the deployment of major portions of the POS sector in the event of a demonstrable emergency. Therefore, no additional measures are required to prevent this.

Furthermore, scaling up agreements make the POS sector vulnerable, especially where ambiguity exists as to the manner of scaling up with other sectors and the accompanying (temporary) use of equipment. Consequently, it is important that scaling up scenarios are well attuned to other sectors, such as the Ministry of Health, Welfare and Sport's health care sector. Aside from sound alignment, no additional measures are necessary here, either.

The steering role played by Public Administration (PA) is crucial to POS sector operations, both under normal and extraordinary circumstances, such as a crisis. Nevertheless, theoretically speaking, disruption to this PA sector will not severely hinder POS sector operations under such circumstances, although the lack of steering will have an effect in the long run. The geographical distribution renders the equipment immune to disruptions. Technical failures, however, do pose a threat to the incident room and its systems.

LEGAL ORDER

Public Authorities:

- ***Ministerie van Justitie; Jus (The Dutch Ministry of Justice[680])***

  The Ministry has the legal mission to: provide workable legislation for citizens, government and the courts; prevent crime, in order to build a safer society; protect youth and children; enforcement the law, in order to build a safer society; provide independent, accessible and effective administration of justice and legal aid; provide support to the victims of crime; provide fair, consistent and effective enforcement of punishment and other sanctions; regulate immigration into the Netherlands. It is also responsible for the coordination of anti-terrorism policy.

Initiatives:

Introduction

In the event of a disaster, a legal responsibility exists to ensure that the judicial process can continue properly, and that 'closed' institutions do not turn out to be 'somewhat open' after all. Analysis efforts focused specifically on three sub-sectors of the legal order sector:

1. the Public Prosecutor (Openbaar Ministerie - OM)
2. the Council for the Administration of Justice
3. the Custodial Institutions Service (Dienst Justitiële Inrichtingen - DJI).

Public Prosecutor

The Public Prosecutor is a national organisation with offices throughout the Netherlands. There are 19 district public prosecutor's offices, where public prosecutors review over 100,000 cases every year, with the help of administrative and judicial specialists. Cases that are appealed are transferred to one of the five public prosecutor's offices at the Court of Appeal. The offices are supervised by chief public prosecutors and chief advocates general. The Board of Procurators General in The Hague is responsible for the national administration of the OM. The Minister of Justice is politically responsible for the OM.

The Council for the Administration of Justice

In order to continue functioning properly, the Council for the Administration of Justice depends primarily on the critical sectors energy, telecommunications, and drinking water.

680 http://*www.justitie.nl/*

Here, this concerns the Public Prosecutor, the Custodial Institutions Service (whose duties include bringing people and files to and from the courts), and the (court) police. These dependencies are particularly important in relation to criminal cases. Furthermore, depending on the type of case, there are dependencies on advocates, bailiffs, notaries, interpreters, and last but not least, the parties involved. Both the parties involved and the court officials all depend on the transport sector in order to show up in court.

The Custodial Institutions Service

The critical importance of the Custodial Institutions Service (DJI) is that the breakdown of custodial institutions would cause major social disturbances. A segment of the prison population poses a danger to Dutch society, and these individuals can cause major problems if they are not incarcerated. A number of processes are critical, and were analysed. The conclusion was that many measures have already been taken, and that consequences do not qualify as "critical." Vulnerability is limited. Each location within the DJI must be prepared for incidents; this is in accordance with zoning permit regulations. They need to have a company relief organisation and the accompanying emergency procedures, an emergency response plan, an evacuation plan and other similar precautions. Institutions must have a back-up power supply for at least three days.

PUBLIC ADMINISTRATION

Public Authorities:

- ***Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*** **(The Dutch Ministry of the Interior and Kingdom Relations[681])**
  The ministry of the Interior and Kingdom Relations (BZK) is one of the thirteen ministries of Dutch central government. The Directorate of National Security leads the Inter-Ministerial workgroup and the Netherlands CIP program. In addition to its lead role in the working group, the Ministry also holds a second operational role in relation to its mission to: uphold the Constitution; guarantee the democratic rule of law; ensure an effective and efficient public administration; coordinate urban policy; promote public order and safety and provide centralised management of the countries police forces; promote the quality of the civil service and coordinate management and personnel policy for all civil servants; coordinate cooperation with Aruba and the Netherlands Antilles.
- ***Ministerie van Defensie; Def (The Dutch Ministry of Defence[682])***

  It coordinates the military of the Netherlands. The ministry has the responsibility for: protecting the territory of the Netherlands and her allies, including the Dutch Antilles and Aruba; protecting and enhancing the international legal system and stability; supporting civil authorities in maintaining order, in case of emergencies and in giving humanitarian aid, both national and international.

  Ministry of Foreign Affairs is also involved for diplomatic communication.

Initiatives:

681 **http://** www.minbzk.nl
682 http://www.defensie.nl/

Introduction

Public Administration plays a special role in the Critical Infrastructure Protection project. In the event of major disasters such as catastrophic terrorist attacks, and natural and industrial disasters, the government – in this case Public Administration – has the integral responsibility for Public Order and Safety. This means that the effects of a disruption in any one critical sector by definition become the responsibility of Public Administration. Given the fact that in practically every disaster there is a direct relationship with Public Administration and/or Public Order and Safety, harmonisation with the (line) Minister of the Interior and Kingdom Relations is always necessary.

Critical Public Administration means:

- the protection of policymaking continuity during the response to and restoration of critical infrastructure in the event of disruption;
- the protection of means of communication for the essential exchange of information between governments and for communicating with the population during (the threat of) severe disasters.

Clearly, the continuity of the democratic state depends on the protection of Public Administration. The competences and power relationships that have been stipulated must – certainly in the Dutch risk society – be able to continue functioning, which is something that must be made known in the event of a serious threat or, even worse, an actual crisis situation.

Critical Public Administration consists of four key components:

1. Administrators: officials with national political-administrative responsibility and competencies, such as Cabinet members, members of the States General, the Royal Family, the Council of States, and local authorities;
2. Administrative crisis centres (national crisis centres, local crisis centres);
3. Internal government communication: communication links between officials and national/regional/local crisis centres (fixed and mobile telephone service, internet, e-mail)
4. Government communication with the population: communication links with the officials mentioned and the public (television, radio, national, regional and local newspapers).

The sector report makes a correlation between the components mentioned and the vulnerabilities inherent to the start events that have been identified. For example, although the temporary absence of one or several administrative decision-makers need not be considered critical, in the event of a serious disaster, the availability of Public Administration is critical. After all, it is at that very moment when decision-making and communication with the population must be immediate. Visible Public Administration must serve to channel any public unrest and collective stress. This report inventories the existing vulnerabilities across the entire scope of Public Administration. This is the first time that an integral approach has been taken, and consequently this sector report also serves as a zero measurement for the state of affairs at Public Administration. In continuation of the Critical Infrastructure project, more depth will be sought as regards the vulnerabilities that have been identified.

Defence sub-sector

The CIP project aims to render society's critical sectors less vulnerable. The Ministry of Defence fulfils its role in CIP as part of Public Administration. Clearly, protecting Public Administration is critical for the continuity of the democratic rule of law. Although Defence is indispensable as a whole, as well as often unique in the individual areas for the functioning of society, it is not vulnerable and therefore is not regarded as critical.

The relationship between Defence and CIP

The Netherlands' armed forces have three main duties:

1. To protect the integrity of its own territory, as well as that of its allies;
2. To promote international law and order and stability;
3. To support civil authorities in law enforcement, disaster relief, and humanitarian aid, nationally as well as internationally.

The armed forces' national CIP duties stem from part of the first key responsibility (protecting the integrity of territory) and the third key responsibility (supporting civil authorities). In principle, this covers all of the tasks that the Dutch armed forces carry out in their own territory in consultation with, or for the sake of, supporting national civil authorities, both in the Netherlands and the Netherlands Antilles and Aruba. Subsequently, in the area of national security, Defence is involved in national safety security affairs, including the protection of critical infrastructure.

Foreign Affairs sub-sector

The Ministry of Foreign Affairs fulfils its role in the public administration sector in the CIP project. This entails diplomatic communication and communication with other countries and international organisations (including NATO, UN, and COREU/ESDP) through the network of diplomatic posts. The ministry realised new data communication connections by signing a contract with a telecom provider that offers extremely high availability guarantees. In the event of an emergency, these connections will also enable spoken communications conducted through the Ministry of Foreign Affairs' incident room, 24 hours a day, 7 days a week. The ministry is in constant contact with the provider to discuss possibilities for further improving and optimising the connections.

22 Norway

Figure 85: Norway

22.1 Summary

	Organisational Model	Strategy & Policy	Methodology & Standards	Public-Private Partnership & International Collaboration	Funding & Human Resources	Training & Exercises	Sector-Specific Key Players & Initiatives
	▪ No structured CIP entity, but a decentralized structure based on Ministries	▪ Report on Protection of Critical Infrastructures and Critical Societal Functions	▪ Creation of a new digital communication network for emergency and public safety services	▪ NorCert and NorSIS	▪ Funding from Ministries	▪ Exercises to tackle catastrophes and terror scenarios in place	▪ National Post and Telecommunication Authority is responsible for contingency planning in the electronic communications infrastructure

Regarding CIP strategy in Norway, the Norwegian Committee on 'A Vulnerable Society' established in 1999-2000 laid an important foundation for the protection of critical infrastructures and in particular emphasizing ICT vulnerability[683] It gave basis for national emergency planning and assessing priorities and debate on vulnerabilities. The findings included establishing the definition of critical infrastructures acknowledging the need for a flexible definition considering the present technical, economic and social developments occurring in society.

According to a report submitted to the Ministry of Justice and the Police in April 2006 by the Committee for the Protection of Critical Infrastructures in Norway (the CIP-Committee), a definition for Critical infrastructures and its sectors was proposed[684]. This definition was later finalized in the Communication to the parliament nr. 22 (2007-2008) Societal Security. Critical infrastructures were also distinguished from critical societal functions- which are in themselves dependent on critical infrastructures. The CIP- Committee identified the following sectors as Critical Infrastructures: electrical power, electronic communication, water supply and sewage, transport, oil and gas, satellite-based infrastructure and critical societal functions as banking and finance, food supply, health services, social services, and social security, police services, emergency and rescue services, crisis management, parliament and government, judiciary, defence, environment surveillance, waste treatment.

683 http://www.regjeringen.no/Rpub/NOU/20002000/024/PDFA/NOU200020000024000DDDPDFA.pdf (in Norwegian)

684 http://www.regjeringen.no/upload/JD/Vedlegg/Norwegian_CIP_Commision_Report_NOU_2006_No_6_English_summary.pdf

22.2 Organisational Model

In Norway, the principle of liability applies to all public and private activities, and forms the basis for the assessment of the division of responsibility between different public authorities (the sector principle). In addition to this, the Ministry of Justice and the Police has been given a more distinct coordinating role in the work on safety and security of society. The coordinating role implies that the Ministry of Justice and the Police should take the necessary steps to clarify areas of responsibility. The Ministry of Justice and the Police is also responsible for the civilian overall coordination of CIP activities.

The military CIP coordination falls under the responsibility of the Ministry of Defence and the protection of ICT infrastructures under the Ministry of Government Administration and Reform. They are all responsible for the emergency preparedness and protection of critical infrastructures in times of peace and in times of unrest.

Main Actors/Responsibilities:

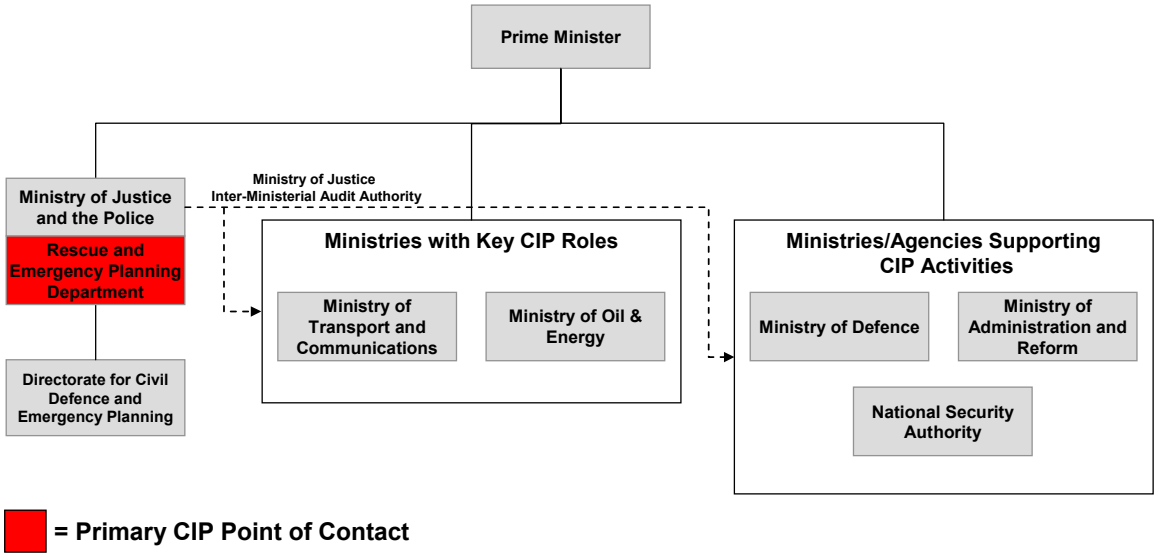


Figure 86: Organisational Chart (only CIP-related agencies shown)

- ***Justis- og Politidepartementet* (Ministry of Justice and the Police)**[685]

  Justis- og Politidepartementet has the main purpose to provide for the maintenance and development of the basic guarantees of the rule of law and with the overriding task of ensuring the security of its society and citizens.

- ***Rednings- og Beredskapsavdelingen* (Rescue and Emergency Planning Department)**[686]

685 http://www.regjeringen.no/en/dep/jd

Rednings- og Beredskapsavdelingen, a department within the Ministry of Justice and the Police, is the superior authority to the Directorate for Civil Protection and Emergency Planning. It is responsible for coordinating the Norwegian Rescue service and has the administrative responsibility for the main rescue coordination centre. This department also coordinates CIP efforts in Norway.

This inter-ministerial coordinating role also includes auditing other ministries to determine the effectiveness of CIP processes within each Ministry (results are not evaluated). Audit points include basic questions such as:

Has a risk assessment been performed?

Are contingency plans in place?

The department provides audit results to the Ministry of Justice, as well as the audited Ministry, with recommendations for improvement.

- ***Direktoratet for Samfunnssikkerhet og Beredskap (DSB)*** **(Directorate for Civil Protection and Emergency Planning)**[687]

  The Directorate for Civil Protection and Emergency Planning was established on 1 September 2003, and is subordinate to the Ministry of Justice and the Police. It replaces the former Directorate for Civil Defence and Emergency Planning and the Directorate for Fire and Electrical Safety. Regarding CIP related matters; the DSB is responsible for the actual implementation of emergency contingency preparedness and response measures on behalf of the government. In the context of CIIP, the DSB coordinates and carries out research on vulnerabilities and the protection of critical assets in cooperation with other actors.

- ***Samferdselsdepartementet*** **(Ministry of Transport and Communications)**[688]

  The Ministry of Transport and Communications has responsibility for the framework conditions for postal and telecommunications activities, for the civil aviation, public roads and rail transport sector and for ferry services forming part of the national road system. It is thus responsible for protection of infrastructures involved in these sectors.

- ***Olje-og Energidepartemetet*** **(Ministry of Oil and Energy)**[689]

  The principal responsibility of the Ministry of Oil and Energy is to achieve a coordinated and integrated energy policy through the efficient management of its energy resources.

- **Forsvarsdepartementet (Ministry of Defence)**[690]

  The Ministry of Defence is responsible for the formation and implementation of Norwegian security and defence policy. It is also responsible for the overall management and control of the Armed Forces and subordinate agencies.

- ***Nasjonal Sikkerhetsmyndighet – NSM – (National Security Authority)***[691]

686 http://www.regjeringen.no/en/dep/jd.
687 http://www.dsb.no
688 http://www.regjeringen.no/en/dep/sd
689 http://www.regjeringen.no/en/dep/oed
690 http://www.regjeringen.no/en/dep/fd

NSM is a Norwegian National Security Authority administratively governed and funded by the Ministry of Defence and also accountable to the Ministry of Justice and the Police in civilian matters. NSM is a cross-sectoral professional and supervisory authority within the protective security services in Norway. The main task of the NSM is to coordinate and control protective measures against national security threats such as espionage, sabotage or acts of terrorism. In CIP, NSM recommends protective security measures on physical objects as well as collaborates with experts on computer security and data encryption. It moreover hosts *SERTIT* the public Certification Authority for IT Security in Norway, and operates NorCERT.

***Fornyings- og Administrasjonsdepartementet* (Ministry of Government Administration and Reform)[692]**

The ministry is responsible for the Government's administration and personnel policy, competition policy, national policy for development and coordination of the use of information technology and measures. The ministry is also responsible for establishing measures for the protection of ICT infrastructures.

22.3 Strategy & Policy

- **Communication No. 17 to the Parliament (2001-2002) Statement on Safety and Security of Society**

  Communication No. 17 was presented to the Parliament by the Norwegian Ministry of Justice and police on April 5, 2002. The report, henceforth called the White Paper, is a comprehensive statement on the government's proposals to reduce the vulnerability of modern society and how to increase safety and security in the years to come. The Parliament's recommendations on the White Paper form the basis for the government's process of initiating measures.

- **Protection of critical infrastructures and critical societal functions in Norway – Report NOU 2006:6**

  The *Report on the Protection of Critical Infrastructures and Critical Societal Functions* in Norway was issued in April 2006 and lays the foundation for CIP and CIIP policies in Norway. It assesses the protection mechanisms of critical infrastructure and critical societal functions in Norway[693]. The Ministry of Government Administration and Reform issued the report *'An Information Society for All'* in December 2006. The report clarified responsibilities among ministries in relation to preventive security work during a crisis as well as showing the state of affairs in the ICT sector.[694]

- **Communication to the Parliament nr. 22 (2007-2008) Societal Security**

691 http://www.nsm.stat.no
692 http://www.regjeringen.no/nn/dep/fad
693 Brunner M. Elgin and Suter, Manuel. "*Germany". International CIIP Handbook 2008/2009- An Inventory of 25 National and International Critical Information Infrastructure Protection Policies.* p. 313
694 Brunner M. Elgin and Suter, Manuel. "*Germany". International CIIP Handbook 2008/2009- An Inventory of 25 National and International Critical Information Infrastructure Protection Policies.* p. 313-314

In the Communication to the Parliament nr. 22 (2007-2008) Societal Security, the Ministry of Justice and the Police considers the CIP-committees proposals in NOU 2006:6. Several of the proposed measures from NOU 2006:6 are accepted in Communication nr. 22 (2007-2008).

- **Norwegian Security Act**[695]

  The object of the Norwegian Security Act is to reduce risks related to threats of espionage, sabotage, or acts of terrorism through protective security measures. According to the Act, the enterprise concerned has a duty to identify information and assets that the enterprise owns or otherwise controls or supervises that need special protection due to their importance to national security, national sovereignty, and other interest that are considered vital to the nation. In addition, the Act also establishes that once an object has been identified as "critical", certain restrictions may apply to the object. These restrictions are still being defined by the related lawmaking authorities.

  Work on protective security in accordance with the law implies taking the necessary protective security measures to protect sensitive information and critical assets from activities that pose a threat to security – such as terrorism, sabotage or espionage. The Act is considered an important measure for CIP.

22.4 Methodology & Standards

According to the Norwegian CIP approach, the challenges related to "a vulnerable society" are as present today as they were in 2000. "New" challenges to Norwegian safety and security such as terrorism and the consequences of climate change relate to the society as a whole and constitute a particular challenge to enterprises that are responsible for critical infrastructures and critical societal functions. Those enterprises must be able to deal with both new and old challenges to safety and security, whether they are caused by antagonistic or non-antagonistic threats.

The choice of public ownership as an instrument to ensure that the interests of national security (and other interests that are considered vital to the nation) are safeguarded must be based on comprehensive assessments. Still, the high degree of complexity and dependency on critical infrastructures and critical societal functions makes it difficult to predict what can go wrong, and what the consequences of disruption in these infrastructures and functions are. In this perspective, the consequences of what can go wrong must be emphasized more than the likelihood of the incident happening. Therefore, measures for the protection of critical infrastructures and critical societal functions require the highest priority and thorough preparation, even if the theoretical probabilities of incidents happening are low.

In order to protect critical infrastructures and critical societal functions, legal requirements given by the supervisory authorities to businesses must be clear and the supervision and control that is carried out must be as efficient as possible. At the same time, businesses need to be aware of their own responsibilities. The work on protection of critical

695 Protection of critical infrastructures and critical societal functions in Norway – Report NOU 2006:6

infrastructures and critical societal functions in Norway is about protecting those services that are necessary for the basic needs of society, and to maintain the feeling of safety and security.

The committee for the protection of critical infrastructure in Norway (the CIP- committee) was established by Royal Decree in October 2004. The CIP-committee's report[696] is a comprehensive assessment on how critical infrastructures and critical societal functions are protected, including what effects exposure to competition, reorganization, rapid shifts in ownership, etc., has had on this work. This is further discussed in the Communication to the Parliament nr. 22 (2007-2008) Societal Security

In the initial phase of the work the CIP-committee identified critical infrastructure and critical societal functions. This task was first addressed by establishing a definition of "critical infrastructure" followed by a set of guidelines to be used in the identification process.

The definition of critical infrastructure

Critical infrastructures are those constructions and systems that are essential in order to uphold society's critical functions, which in time safeguard society's basic needs and the feeling of safety and security in the general public.

Collectively, critical infrastructures and critical societal functions contribute to ensuring the interests of national security and other interests that are considered vital to the nation. In order to be more specific on what critical infrastructure is, the CIP-committee distinguished between critical infrastructures and critical societal functions. This methodology is confirmed in the Communication to the Parliament nr. 22 (2007-2008) Societal Security.

The CIP-committee identified critical infrastructures using a method based on three criteria. The method is not intended to give an accurate assessment of the level of criticality of the infrastructure, just "yes" or "no". The criteria used are:

- ***Dependability***, i.e. high degree of dependability implies criticality.
- ***Alternatives***, i.e. few or no alternatives imply criticality.
- ***Tight coupling***, i.e. high degree of tight coupling (linkage) in a network implies criticality.

This method can be illustrated as follows:

[696] Protection of critical infrastructures and critical societal functions in Norway – Report NOU 2006:6

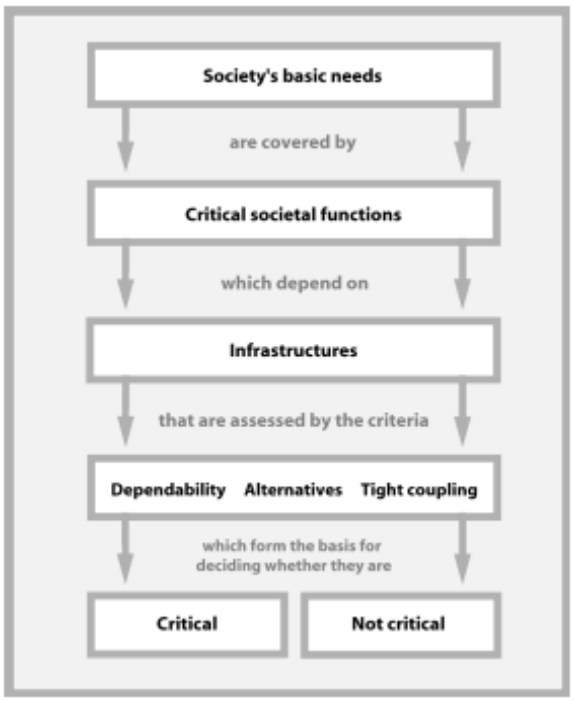


Figure 87: Norwegian Methodology for Identifying Critical Infrastructure

By using this method and assessing the different infrastructures within each sector, some common infrastructures will appear. Infrastructures that many parts of society depend on. If these infrastructures are disrupted in any way, it can have devastating effects on society. Based on this, the Norwegian CIP-committee was of the opinion that *critical infrastructures* shall be limited to those installations and systems that support electrical power, electronic communication, water supply and sewage, transport, oil and gas, and satellite communication and surveillance.

The table below gives an overview of the critical infrastructures and critical societal functions the Norwegian CIP-committee has identified:

Critical infrastructures	Critical societal functions
Electrical power	Banking and finance
Electronic communication	Food supply
Water supply and sewage	Health services, social services and social security benefit
Transport	The Police
Oil and gas	Emergency and rescue services
Satellite-based infrastructure	Crisis management
	Parliament and government
	The judiciary
	Defence
	Environmental surveillance
	Waste treatment

Figure 88: Critical Infrastructures and Societal Functions in Norway

In its report the CIP-committee did not explicitly assess the critical societal functions below the dotted line. It is emphasized that the list of critical infrastructures and critical societal functions is not intended to be a final and objective list. The purpose of this particular list has been to form a basis for assessing instruments for the protection of critical infrastructures and critical societal functions. Hence, the list is of a general nature.

After identifying critical infrastructures and societal functions, various instruments can be applied to ensure their protection. The Norwegian CIP-committee has categorized these instruments as follows:

- ***Juridical instruments -*** Laws, regulations, concessions, price regulations, etc.
- ***Organisational instruments -*** Outsourcing, company formation, the establishment of inspectorates, etc.
- ***Economic instruments -*** Subsidies, purchasing of goods and services, tax levy, etc.
- ***Pedagogical instruments -*** Planning, exercises, etc.
- ***Ownership -*** Public ownership as an instrument.

The Norwegian CIP-committee has given several recommendations concerning the overall use of these five categories of instruments. The recommendations is further discussed in the Communication to the Parliament nr. 22 (2007-2008) Societal Security.

22.5 Public – Private Partnership & International Collaboration

Public-Private initiatives for critical infrastructural protection were strengthened particularly after the findings of the 'A Vulnerable Society' report establishing the need for early warning capabilities such as NorCERT and NorSIS. The Norwegian Computer Emergency Response Team (NorCERT) was established in January 2006 as an operational department of the *Nasjonal Sikkerhetsmyndighet (NSM) National Security Authority* and is the national CERT for Norway[697].

22.6 Funding & Human Resources

Funding is provided for through the national budget and distinctively through the respective ministries. Specific CIP-related funding amounts are not publically available.

There is no dedicated CIP agency in Norway. CIP matters are coordinated by the staff of the Rescue and Emergency Planning Department as an integrated part of their normal work.

22.7 Training & Exercises

- ***Øvelse Oslo 2006 Exercise Oslo 2006***

  The *Øvelse Oslo 2006 Exercise Oslo 2006* initiative[698] was a significant and comprehensive exercise that aimed to train and develop society's ability to tackle extensive terror scenarios and catastrophes. The Norwegian Ministry of Justice and the Police delegated the administrative responsibility for the planning and leadership of exercises in emergency preparedness to the *Direktoratet for Samfunnssikkerhet og Beredskap (DSB)* (Directorate for Civil Protection and Emergency Planning). The Norwegian Police Directorate, the Directorate for Health and Social Affairs, the City of Oslo, and the County Governor of Oslo and Akershus constituted the exercise leadership together with DSB. A number of other public agencies and institutions were also significant in the planning process and the execution of the exercise. All functions, from operative personnel to strategic decision-makers at the ministerial l level and were held on 17 and 18 October 2006. The purpose of Exercise Oslo 2006 was to train and improve society's ability and capacity at all levels in dealing with the consequences of an extreme terrorist attack and other extensive catastrophes. During the exercise the following major elements were focused upon:

  - Co-operation and co-ordination between local, regional and central crisis management
  - Activation of information strategy at several levels (local, regional and central)

697 http://www.nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/

698 http://www.dsb.no/article.asp?articleid=1864&Framework=engelsk&leftmenu=v_ovelse_oslo&rank=7&oppslag=1

- Activation and co-ordination of society's total search and rescue resources – including private companies and voluntary organisations
- Measure the ability and capacity to deal with several parallel high risk scenes of damage simultaneously
- Test efforts and priorities at the scene of damage
- Receipt and treatment of mass injuries/many patients

- **ICT 08 Exercise (19 March 2008)**

  The exercise focused on Information and Communications Technologies (ICT) in Critical Infrastructures (CI). This was the first exercise of this nature in Norway and was a cooperative effort among about 30 participants under the sponsorship of the DSB and NSM. This distributed, multi-location table top exercise included important actors from private and public sectors including banking and finance, electric power supply, oil and gas, telecommunications, and justice and police.

22.8 Sector – Specific Key Players & Initiatives

CRITICAL INFRASTRUCTURES

ELECTRICAL POWER

Public Authorities:

- ***Olje-og Energidepartemetet* (Ministry of Oil and Energy)**[699]

  The principal responsibility of the Ministry of Oil and Energy is to achieve a coordinated and integrated energy policy through the efficient management of its energy resources.

- ***Norges vassdrags- og energidirektorat – NVE – (Norwegian Water Resources and Energy Directorate)***[700]

  NVE is a directorate under the Norwegian Ministry of Petroleum and Energy, with responsibility for managing the country's water and energy resources. NVE's mandate is to ensure integrated and environmentally friendly management of the country's watercourses, to promote efficient power market and cost-effective energy systems and to work to achieve a more efficient use of energy. NVE has a central role in flood prevention work and the work to prevent accidents in watercourses, and has the overall responsibility for maintaining national power supplies.

Initiatives:

699 http://www.regjeringen.no/en/dep/oed
700 http://www.nve.no

- **Reversion of ownership to hydroelectric power plants**

  Public ownership of the hydroelectric power plants has been ensured by an arrangement of reversion to the state. This means that the power plant is handed over to the state, free of charge, after a fixed concessionary period. From a security and emergency preparedness perspective, the Norwegian CIP-committee strongly recommended that the arrangement of reversion of ownership to the state is continued so that today's public, national ownership of power resources is not weakened in the long run.

- **Solutions for emergency power supply**

  The power grid in Norway is constructed in such a way that it is difficult to prioritize the supply of electric power to individual enterprises. Nevertheless, the Norwegian CIP-committee proposed that the authorities should conduct further assessments in order to establish a solution for the rationing of electric power. At the same time, it should be considered how power supply to critical societal functions can be secured through a more extensive use of emergency power supply units. Special requirements regarding alternative power supply should also be assessed.

- **Economic instruments in the electrical power sector**

  Analyses made on the power industry's adaptation to the KILE requirement ("Quality adjusted income in case of undelivered power") suggest that the requirement influences the companies' decisions regarding investments and maintenance. KILE is primarily a long-term instrument to stimulate investments and maintenance, and it can have beneficial socioeconomic effects regarding the security of supply, if the arrangement is appropriately modeled. It should be assessed to what degree a framework that regulates income can be used as an instrument to maintain competence and to impose continuous review of the data on the networks.

ELECTRONIC COMMUNICATION

Public Authorities:

- ***Samferdselsdepartementet* (Ministry of Transport and Communications)[701]**

  The Ministry of Transport and Communications has responsibility for the framework conditions for postal and telecommunications activities, for the civil aviation, public roads and rail transport sector and for ferry services forming part of the national road system. It is thus responsible for protection of infrastructures involved in these sectors.

- ***Post -og teletilsynet* (Norwegian Post and Telecommunications Authority (NPT))[702]**

[701] http://www.regjeringen.no/en/dep/sd
[702] http://www.npt.no

The Norwegian Post and Telecommunications Authority is under the Norwegian Ministry of Transport and Communications and is an autonomous administrative agency which has monitoring and regulatory responsibilities for the postal and electronic communications markets in Norway. With regards to the protection of its critical infrastructures, the NPT is responsible for contingency planning in the electronic communications infrastructure.

- ***Fornyings- og Administrasjonsdepartementet* (Ministry of Government Administration and Reform)**[703]
  The ministry is responsible for the Government's administration and personnel policy, competition policy, national policy for development and coordination of the use of information technology and measures. Primarily the Department of IT Policy which is under this ministry is responsible for establishing measures for the protection of ICT infrastructures.
- ***Avdeling for IKT og fornying* (Department of ICT policy and Public Sector Reform)**[704]
  This department, subordinate to the Ministry of Government Administration and Reform, is responsible for working on the development of a strategy and policy associated with an integrated policy for the Information Society, including the eNorway plans. The department is responsible for the policy related to the development of broadband coverage and for making broadband available throughout the country. It also has the responsibility for taking initiatives and coordinating the development of an electronic administration where access to public services is a major issue. In this work, further development of the Public Web Portal MinSide (My Page) constitutes an important instrument. The goal is to create an open administration available to the general public.
- **The *Norsk Senter for Informasjonssikring (NorSIS)* (Norwegian Centre for Information Security)**[705]
  NorSIS, under the Ministry of Government Administration and Reform, is responsible for coordinating activities related to ICT security in Norway. The centre receives reports about security related incidents from companies and departments, and is working on obtaining an overall impression of threats towards Norwegian ICT systems. The establishment of the centre was part of a strategy for reducing the society's vulnerability to information and communication technology (ICT) recommended by The Vulnerability Committee in June 2000.

Initiatives:

- ***Koordineringsutvalget for Forebyggende Informasjonssikkerhet (KIS) (Information Security Coordination Council)***[706]

  The Information Security Coordination Council was established in 2004 by the *Ministry of Government Administration and Reform*. KIS has a central role in the implementation of the national guidelines to strengthen information security by

703 http://www.regjeringen.no/nn/dep/fad
704 http://www.regjeringen.no/en/dep/fad
705 http://www.norsis.no
706 http://www.nsm.stat.no/kis/

identifying cross-sectoral challenges in information assurance and in maintaining dialogue with the private sector and the government that could have impact on the measures for CIIP. KIS has no authority to make decisions but provides a platform for discussions and advises ministries and government agencies in topics related to ICT security, national security (interests), critical information infrastructure, common standards, working methods for ICT security, risks, and vulnerabilities. Its main tasks include coordinating and developing regulations, provide recommendations and advise in relation to implementation of national strategies all within information security.

- **Responsibility for IT-security on the national level**

  The Norwegian CIP-committee recommended that the number of ministries with overall responsibility for IT-security on the national level must be reviewed. This was proposed in an assessment conducted by The Office of the Auditor General in Norway. Ideally, this responsibility should be assigned to one ministry. Based on this, the CIP-committee proposed a coordination of the responsibilities for IT-security on the national level assigned to the Ministry of Transport and Communications and the Ministry of Government Administration and Reform. The CIP-committee's proposal was accepted in Communication to the Parliament nr. 17 (2006-2007) ICT Security and the Communication to the Parliament nr. 22 (2007-2008) Societal Security

WATER SUPPLY AND SEWAGE

Public Authorities:

- ***Norges vassdrags- og energidirektorat – NVE – (Norwegian Water Resources and Energy Directorate)***[707]

  NVE is a directorate under the Norwegian Ministry of Petroleum and Energy, with responsibility for managing the country's water and energy resources. NVE's mandate is to ensure integrated and environmentally friendly management of the country's watercourses,

- **Mattilsynet - The Norwegian Food Safety Authority (NFSA)**

  The Norwegian Food Safety Authority (NFSA) reports to three different ministries: The Ministry of Agriculture and Food, The Ministry of Health and Care Services and The Ministry of Fisheries and Coastal Affairs. NFSA keeps the waterworks under supervision regarding contingency planning.

- **Municipalities**

  The water supply and sewage sector is characterized by the strong synergy between the activities related to the infrastructure (technical installations) and water supply and sewage services. This synergy favors vertical integration of

[707] http://www.nve.no

these activities. Therefore, the municipalities maintain the lead roles in protecting the infrastructure required to deliver these services.

From a security and emergency preparedness perspective, the Norwegian CIP-committee recommended that the water supply and sewage enterprises should remain in public ownership. Exposing certain activities to competition, as well as organizing water supply and sewage enterprises in private co-operatives must still be permitted, provided that security and emergency preparedness is adequately safeguarded. The proposal is considered in Communication nr. 22 (2007-2008) Societal Security.

Initiatives:

- **The government's role in the water supply and sewage sector**

  The Norwegian CIP-committee recommended the establishment of a coordinating group for the water supply sector, with appropriate representation, sufficient resources, and tasks that include coordinating the work on regulations and supervision, conducting risk assessments, evaluating the level of security, and identifying CIP-measures.

  It was the Norwegian CIP-committee's opinion that the Norwegian Food Safety Authority needed to increase its efforts within this field, in order to ensure compliance with the requirements for quality as well as to safety and security. The Norwegian Food Safety Authority must give priority to implementing measures in the action plan to ensure a more secure water supply.

  The Norwegian CIP-committee also found that it was important that the Norwegian Food Safety Authority monitor developments in laboratories, and that government funding is provided if this is considered necessary.

- **Competence within the water supply and sewage sector**

  The Norwegian CIP-committee recommended that a study be carried out as to how more resilient organizations within the sector can be established, including measures to ensure a necessary level of competence. In this study the need for minimum standards of competence and manning should also be assessed. Furthermore, the recruitment situation in the sector should be evaluated.

- **Emergency preparedness in the water supply and sewage sector**

  An emergency in the water supply sector will normally have localized effects and be handled by the emergency managers in the municipalities, waterworks, and the Food Safety Authority, possibly in cooperation with other local emergency units. The Norwegian CIP-committee considers the crisis management unit in Sweden to be a useful model and proposed that a similar unit be established in Norway. This unit should assist the individual waterworks in a crisis situation.

- **Economic instruments in the water supply and sewage sector**

  The Norwegian CIP-committee warned against moving away from the current economic regime of full cost coverage in the sector, and into a system based on

regulation of income, without thorough assessments of the long-term consequences such a change can have on the safety and security in the sector.

TRANSPORT

Public Authorities:

- ***Samferdselsdepartementet* (Ministry of Transport and Communications)**[708]

  The Ministry of Transport and Communications has responsibility for the framework conditions for postal and telecommunications activities, for the civil aviation, public roads and rail transport sector and for ferry services forming part of the national road system. It is thus responsible for protection of infrastructures involved in these sectors.

- ***Jernbaneverket* (National Rail Administration)**[709]

  Under the Ministry of Transport and Communications, *Jernbaneverket* is the national railway authority responsible for the management and maintenance of the national railway network.

- ***Statens Jernbanetilsyn* (Norwegian Railway Inspectorate)**[710]

  Under the Ministry of Transport and Communications, *Statens Jernbanetilsyn* is a Norwegian government agency responsible for control and supervision of rail transport in Norway, including railways, tramways, rapid transits, heritage railways and side tracks.

- ***Statens Havarikommisjon for Transport* (Accident Investigation Board)**[711]

  Under the Ministry of Transport and Communications, *Statens Havarikommisjon for Transport* is a Norwegian government agency responsible for investigating accidents and incidents within aviation, railway (including tram and rapid transit) and road transport.

- ***Luftfartstilsynet* (Norwegian Civil Aviation Authority)**[712]

  Under the Ministry of Transport and Communications, *Luftfartstilsynet* is the Norwegian inspectorate responsible for civil aviation, airport and air traffic management operator in Norway.

- ***Norges Statsbaner (NSB)* (Norwegian State Railways)**[713]

  Under the Ministry of Transport and Communications, NSB is a Norwegian transport company. Owned by the Government of Norway, it is the largest passenger railway company and, through the subsidiary Nettbuss, bus company in Norway.

- ***Statens Vegvesen* (Norwegian Public Roads Administration)**[714]

708 http://www.regjeringen.no/en/dep/sd
709 http://www.jernbaneverket.no/
710 http://www.sjt.no/
711 http://www.aibn.no
712
713 http://www.nsb.no/

Under the Ministry of Transport and Communications, *Statens Vegvesen* is a Norwegian government agency responsible for the state and county public roads in the country. This includes planning, construction and operation of the state and county road networks, driver training and licensing, vehicle inspection and subsidies to car ferries. In 2010, portions of this responsibility will shift to the counties.

- ***Fiskeri- og kystdepartementet* (Ministry of Fisheries and Coastal Affairs)**[715]

  Fiskeri- og kystdepartementet has the responsibility for the fisheries and aquaculture industries, seafood safety, and fish health and welfare, harbours, infrastructures for sea transport and emergency preparedness for pollution incidents.

- ***Kystverket (NCA)* (The Norwegian Coastal Administration)**[716]

  Under the Ministry of Fisheries and Coastal Affairs, the Norwegian Coastal Administration is the Norwegian national agency for coastal management, marine safety and communication.

- **Ministry of Trade and Industry**
  The Ministry of Trade and Industry's responsibility for industrial policy spans many sectors since there are numerous areas that factor into industrial policy – such as tax, labour market, energy, and competition. The transportation sector also plays a key role in developing industrial policy.

- ***Sjøfartsdirektoratet (Norwegian Maritime Directorate)***[717]

  Under the Ministry of Trade and Industry, *Sjøfartsdirektoratet* has jurisdiction over ships registered in Norway and foreign ships arriving Norwegian ports. The directorate's main goals are to prevent accidents and to achieve a high level of safety for lives, health, vessels, and the environment.

Initiatives:

The Norwegian CIP-committee has emphasized the need to integrate the core security and emergency preparedness activities within the day-to-day management of an enterprise. The CIP-committee believes this to be a precondition for ensuring an adequate level of safety and security.

The CIP-committee recommended that the Ministry of Transport and Communications, the Ministry of Trade and Industry, the Ministry of Fisheries and Coastal Affairs and the Ministry of Justice and the Police co-operate in order to emphasize the importance of transporting hazardous goods as safely as possible. The proposal is considered in Communication nr. 22 (2007-2008) Societal Security.

714 http://www.vegvesen.no/
715 http://www.regjeringen.no/nn/dep/fkd.html?id=257.
716 http://www.kystverket.no/?did=9103236
717 http://www.regjeringen.no/nn/dep/nhd/Om-departementet/Underliggjande-etatar/the-norwegian-maritime-directorate.html?id=435117

OIL AND GAS

Public Authorities:

- ***Olje-og Energidepartemetet* (Ministry of Oil and Energy)**[718]

  The principal responsibility of the Ministry of Oil and Energy is to achieve a coordinated and integrated energy policy through the efficient management of its energy resources. The Ministry's tasks include regulation of the upstream gas network (Gassled) and oil pipelines.

- **Oljedirektoratet – OD – (The Norwegian Petroleum Directorate)**

  OD is subordinated to the Ministry of Petroleum and Energy, and is responsible for the administration of Norway's petroleum resources. Its goals are to contribute to creating the highest possible values for society from oil and gas activities, founded on a sound management of resources, safety and environment.

- **Arbeids- og inkluderingsdepartementet (Ministry of Labour and Social Inclusion)**
  The Ministry is responsible for Labour market policy, Working Environment and Safety, Poverty and Welfare, Integration and Diversity, Sami and Minority Affaires and Migration.

- **Petroleumstilsynet (Petroleum Safety Authority Norway (PSA))**

  PSA is the regulatory authority for technical and operational safety, including emergency preparedness, and for the working environment.The regulatory role covers all phases of the industry, from planning and design through construction and operation to possible ultimate removal. "Safety" covers a broad range in the terminology and embraces three categories of loss – human life, health and welfare, the natural environment, and financial investment and operational regularity.

- **Public ownership in the oil and gas sector**

  A significant part of the petroleum activity on the Norwegian continental shelf in operated by privately owned and/or foreign enterprises. It is therefore necessary to have an effective regulatory regime for security and emergency preparedness, with sufficiently strong sanctions. Such instruments are available in today's legal framework.

  Public ownership is, according to the CIP-committee, at best a partial instrument for ensuring national security and other interests that are considered vital to the nation, and will be less important if these oil and gas regulations are effective and are properly enforced.

SATELLITE-BASED INFRASTRUCTURE

Public Authorities:

[718] http://www.regjeringen.no/en/dep/oed

- ***Samferdselsdepartementet*** **(Ministry of Transport and Communications)**[719]

  The Ministry of Transport and Communications has responsibility for the framework conditions for postal and telecommunications activities, for the civil aviation, public roads and rail transport sector and for ferry services forming part of the national road system. It is thus responsible for protection of infrastructures involved in these sectors.

Initiatives:

The Galileo-system is best achieved through active participation in committees, working groups, and permanent staffed organizations in the European Union and the European Space Agency. Such participation also provides the possibility to influence solutions.

Norway considered joining the Public Regulated Service (PRS) of the Galileo-system, as civilian public users will not be granted access to equivalent information through the Global Positioning System (GPS) in the future, and because Galileo PRS will have more resilient signals. Participation in Galileo PRS requires government control mechanisms.

If Galileo ground infrastructure should be placed in Norway (i.e. on Svalbard) it will be important to determine which measures should be implemented in order to protect this infrastructure.

CRITICAL SOCIETAL FUNCTIONS

BANKING AND FINANCE

The Norwegian CIP-committee has primarily looked at instruments to protect the critical infrastructures, which in turn will have an effect on the protection of critical societal functions.

The CIP-committee emphasizes the importance of conducting risk and vulnerability analyses in the banking and finance sector, including risks and vulnerabilities related to the high degree of interdependencies between critical infrastructures and critical societal functions.

FOOD SUPPLY

Norwegians should expect a certain level of food stocks in each household, so that individuals are capable of taking care of themselves for a few days without government intervention. In connection with Y2K, the former Directorate for Civil Defence and Emergency Planning produced a brochure with advice on what food and other basic necessities a household should keep in case of emergency.

719 http://www.regjeringen.no/en/dep/sd

From a security and emergency preparedness perspective, the Norwegian CIP-committee emphasizes the importance of upholding an adequate level of food production in Norway.

The Norwegian CIP-committee recommended a strengthening of the efforts made by the Ministry of Trade and Industry in cooperation with the major distributors of food to identify vulnerabilities in the critical infrastructures on which food supply depends. In this way, the weaknesses can be communicated to the appropriate authorities and minimized, as far as possible.

HEALTH SERVICES, SOCIAL SERVICES, AND SOCIAL SECURITY BENEFIT

Hospitals must establish dialogue with their suppliers of critical goods and services in order to secure their supplies and to ensure that relief efforts are prioritized in case of interruptions to delivery. Hospitals must develop crisis response plans for emergencies related to failures of the water supply, the power supply, and electronic communication.

- **Supply of medicines**

  Vaccines and medicines can be scarce commodities during serious epidemics and pandemics. Faced with an imminent threat, the distribution of vaccines and medicines must be considered a very important task for the health services and other relevant authorities. The Norwegian CIP-committee recommended that critical infrastructures and critical societal functions should be given priority in these cases, thus avoiding the escalation of a potential crisis.

  A working group consisting of representatives from the Directorate of Health and Social Welfare, the Norwegian Medicines Agency, and the Norwegian Institute of Public Health has worked on ways to ensure the delivery of medicines. The object of the work is to reduce vulnerability in situations where there are limited supplies of medicines produced outside Norway.

THE POLICE

The Norwegian CIP-committee has no specific recommendations regarding the safeguarding of the critical societal functions provided by the Police. It is pointed out that the critical functions of the Police are primarily safeguarded by the protection of critical infrastructures. For example, their capabilities will be severely reduced in case of lapse in electronic communications or power supply. Nevertheless, the CIP-committee addressed two important matters related to the Police.

- **Private security services**

  It is necessary to look closer at the strong growth in private security services. Among other things, these firms use force on civilians, carry out undercover investigations at workplaces, and investigate criminal activity. The main objection is that private security services are not subject to the same strict democratic control as the Police. These firms carry out important functions in society, but it is considered that the Police in accordance with the Police Act should carry out these tasks. The Norwegian CIP-committee questioned whether personnel without the professional skills of the Police should carry out tasks that include use of force on civilians, undercover investigations at workplaces, and investigation of

criminal activity. The CIP-committee recommended that the Ministry of Justice and the Police conduct a thorough assessment on this matter.

- **The Police Reserve and the Home Guard**

  The CIP-committee recommended a review of the division of tasks and responsibilities between the Police Reserve and the Home Guard. This included responsibilities for armed protection of critical infrastructures and critical societal functions.

EMERGENCY AND RESCUE SERVICES

- **The "principle of cooperation" in the Norwegian rescue service**

  The Norwegian CIP-committee emphasized the importance of maintaining and developing the so-called "principle of cooperation" in the Norwegian rescue service. This is particularly important during the process of reorganization and reform that is going on in public enterprises, as the principle does not apply for private enterprises. This aspect has therefore been included in the CIP-committee's recommendations on ensuring security and emergency preparedness during the process of reform and reorganization.

- **The ability to handle large-scale emergencies and rescue operations**

  In November 2005, the Directorate for Civil Protection and Emergency Planning presented a proposal for strengthening the ability to handle large-scale emergencies and rescue operations that demand extraordinary resources from emergency and rescue services. The proposal was based on a comprehensive assessment done in cooperation with relevant parties. The proposal implied further development and modernization of the operative forces in the Civil Defence. The CIP-committee supported this proposal.

CRISIS MANAGEMENT

- **The crisis management system**

  The Norwegian CIP-committee recommended that:

  1. The direction and priority given to the crisis management system must not be downgraded because national crisis situation occur relatively infrequently and must be maintained at all times.
  2. The crisis management system must be sufficiently flexible to handle all kinds of scenarios. The same system should be used irrespectively of the extent of the crisis (except in case of war). This implies that the relationship between the Government Crisis Management Council and other strategic councils that may become operational during a crisis must be assessed.
  3. The Government's Crisis Management Unit should be responsible for ensuring the development and strengthening of competence as a day-to-day task, including maintaining national and international networks for crisis management. Tasks related to crisis management in other authorities should be coordinated with the tasks and responsibilities assigned to the Crisis Management Unit. The seconding of personnel from these authorities can facilitate this.

4. Efficient and well-established routines are necessary for the transfer of overall crisis management command between the ministries and the Ministry of Justice and the Police. Based on assessments and exercises related to potential crisis scenarios, the crisis management command structure should be assigned in advance. This could form the basis for the development of a national crisis response plan.
5. During larger crises, it is especially important to coordinate crisis management. To be able to do this effectively, it is necessary to coordinate the different emergency plans. Therefore, the CIP-committee pointed out that it is necessary to standardize the emergency plans in the various ministries.
6. The emergency preparedness duties and responsibilities concerning crisis management in the county administrations should be more clearly defined. This includes powers to requisition resources and to ration critical goods and services if necessary.
7. Important parts of the government administration must have modern and functional means of communication in crisis management, enabling secure communication of information classified up to SECRET.
8. Regular exercises need to be carried out in order to test and further develop national emergency preparedness in relation to potential crises in critical infrastructure and critical societal functions. The exercises must be followed by evaluations leading to continuous improvements in crisis response plans. Existing plans should be used as part of the exercises.
9. The municipalities must be given a general duty to conduct emergency planning.

- **The role of the religious communities in the prevention and management of crises**

  The Norwegian CIP-committee recommended that a permanent advisory council consisting of representatives from different religious communities should be established and linked to the Ministry of Justice and Police. This will enable the government to use existing expertise in the various religious communities. The advisory council should be assigned the following tasks:

  - Give advice on how to manage insecurity and suspicion towards or between different religious communities, in crises where Norwegian interests are involved.
  - Give advice on how to prevent and manage religious extremism.
  - Give advice on how the different religious communities can contribute to post-trauma counseling after a crisis.

  The CIP-committee emphasized the importance of giving the council sufficient time to develop a common platform for its work. The CIP-committee also emphasized the importance of representation from different denominations in the council. As a first step, the CIP-committee proposed the establishment of a working group consisting of representatives from some of the central religious communities in Norway.

- **Warning and information to the population**

  The Norwegian Broadcasting Corporation (NRK) has an important function with regard to emergency preparedness, as it is responsible for broadcasting government information bulletins during national crises and catastrophes, using the radio channel NRK P1. NRK P1 covers the entire nation, and together with the warning system administered by Civil Defence (sirens) it is the best platform for rapidly warning and delivering information to the general population. The CIP-committee referred to the agreements between the various authorities and NRK and recommended the following:

  1. That agreements and arrangements should be adapted to today's challenges to safety and security. The CIP-committee recommended a review of the roles and responsibilities on the government level regarding warning and informing the general population.
  2. The CIP-committee recommended a review of the financial support provided by the government for emergency preparedness in this field, in order to increase effectiveness and strengthen emergency preparedness in the media.
  3. The CIP-committee recommended that the FM network can only be switched off once a new network has the same coverage as today's network. It must be made clear that the warning function assigned to NRK P1 continues in the digital audio broadcasting (DAB) network.

23 Poland

Figure 89: Poland

23.1 Summary

	Organisational Model	Strategy & Policy	Methodology & Standards	Public-Private Partnership & International Collaboration	Funding & Human Resources	Training & Exercises	Sector-Specific Key Players & Initiatives
Poland	▪ Security agency with CIP responsibilities reporting directly to Prime Minister	▪ CI and CIP defined in Crisis Management Acts of 2007 and 2009	▪ Will be addressed in the National CIP Program which will replace the National CIP Plan through amendments to the CMA, effective Sep 19 2009.	▪ Public Administration / CI Owners Public-Private Forum	▪ Dedicated CIP staff within cross-functional agency (GCS)	▪ This will be prepared after the process of selecting CI will be concluded	▪ CERT Polska ▪ CERT GOV PL ▪ ARAKIS-GOV

The CIP program in Poland is tightly interwoven with the overall Crisis Management activities.

The body responsible for coordinating the national CIP effort is the Government Centre for Security (GCS), which also acts as the national contact point for European Union institutions and Member States in the field of Critical Infrastructure Protection. The GCS is directly subordinate to the Prime Minister. The responsibility for the protection of systems identified as Critical Infrastructure will fall under the appropriate Ministers or Heads of Central Offices.

The terms Critical Infrastructure (CI) and Critical Infrastructure Protection (CIP) are defined in the Crisis Management Act of 26th April 2007 (CMA) and include the following systems (based on criteria a list of CI is currently being developed. It will be ready in march 2010 – according to the new amendments to the CMA):

- Energy and fuel supply systems
- Communication and tele-information network systems
- Financial systems
- Water and food supply systems
- Health protection systems
- Transportation and communication systems
- Rescue systems
- Systems ensuring the continuity of public administration activities
- Systems of production, storing and use of chemical and radioactive substances, including pipelines for dangerous substances

23.2 Organisational model

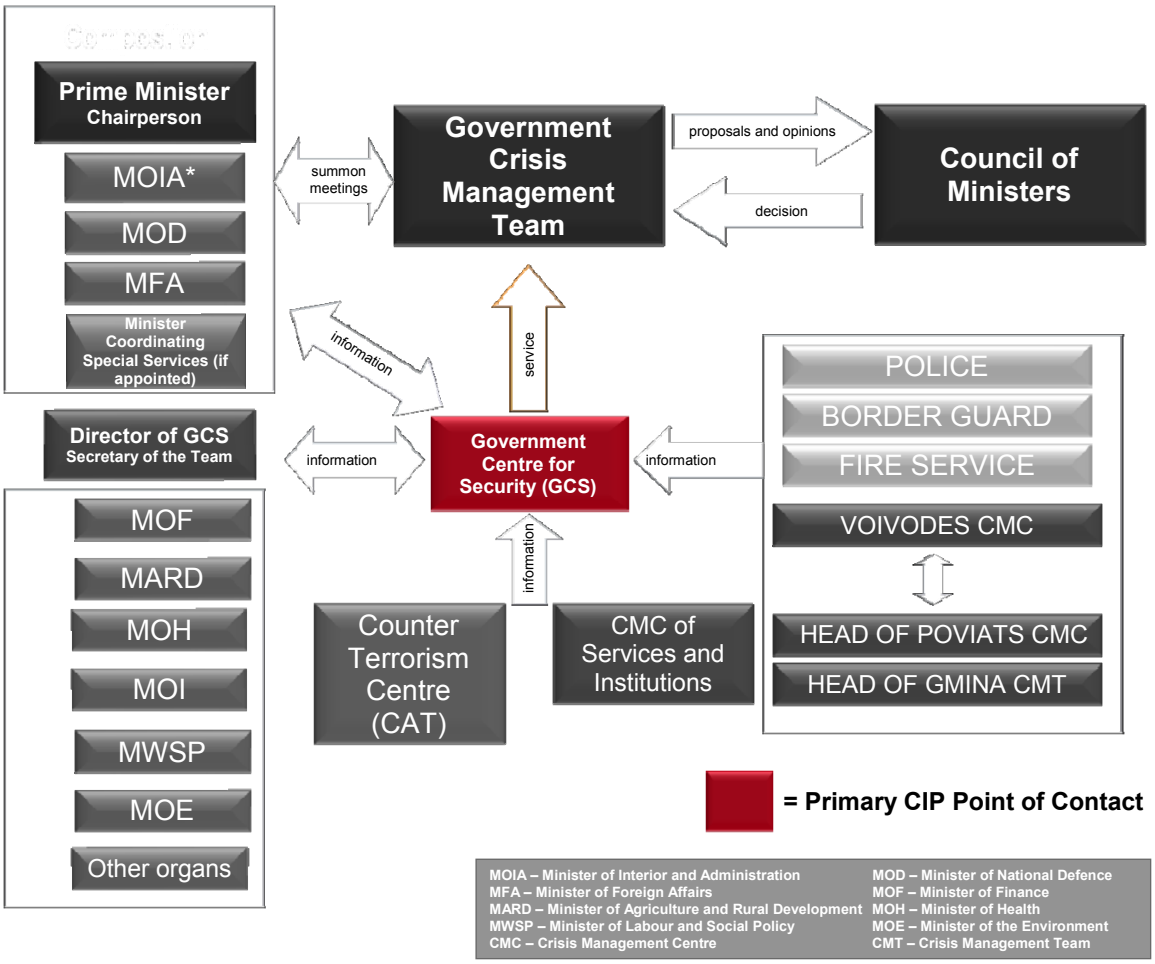


Figure 90: Organisational Chart showing the place of the Government Centre for Security within the public administration

Main Actors/Responsibilities:

- **Council of Ministers**[720]

  According to the Crisis Management Act, the Council of Ministers shall be responsible for crisis management on the territory of the Republic of Poland. However, in an urgent situation, Crisis Management shall be undertaken by the Minister responsible for internal affairs, who shall in turn inform the Prime Minister of his actions.

- **Government Crisis Management Team**[721]

720 Booz & Co EU CIP Stocktaking Web-Based Survey, 2009
721 Place and Role of the Government Centre for Security in the Polish Crisis Management System

The GCMT is an advisory and opinion body to the Council of Ministers in matters dealing with initiation and coordination of activities related to crisis management including:

- Development of the proposals to use capabilities and resources necessary to restore control over emergency situations;
- Provision of advice in the field of coordination of activities of government administration, state institutions and services in emergency situations;
- Giving opinion on final reports on activities taken in relationship with crisis management;
- Giving opinion on needs in the scope of reconstructing infrastructure or restoring its previous state;
- Giving opinion on the National Crisis Management Plan and presenting it to the Council of Ministers for approval;

The Team shall be composed of:

1) Prime Minister as the chairperson;
2) Minister of Defence and minister competent for internal affairs as deputy chairpersons;
3) Minister of Foreign Affairs;
4) Minister Coordinating Special Services – if appointed.

The following government administration authorities shall participate, if necessary, in the Team meetings, as members:

1) Ministers heading the government administration sections:
   a) Public administration;
   b) Construction, spatial and housing planning and economy ;
   c) Public finance;
   d) Economy;
   e) Maritime economy;
   f) Water economy;
   g) Financial institutions;
   h) IT development;
   i) Culture and protection of national heritage;
   j) Communications;
   k) Education;
   l) Agriculture;
   m) Justice;
   n) Natural environment;

o) Transport;

p) Health;

r) Labour and social security;

s) State Treasury

2) Chief Geodetic Inspector of Poland;
3) Chief Sanitary Inspector;
4) Chief Veterinary Officer;
5) Chief Commandant of the State Fire Service;
6) Commander in Chief of Police;
7) Chief Commander of Border Guard
8) Head of the National Atomic Energy Agency
9) Head of the Civil Aviation Office;
10) Head of the Internal Security Agency;
11) Head of the Foreign Intelligence Agency;
12) Head of the National Civil Defence;
13) Head of the Military Counter-Intelligence Service;
14) Head of the Military Intelligence Service.

- **Government Centre for Security**[722]

  The body responsible for coordinating the national CIP effort is the Government Centre for Security (GCS), which also acts as the national contact point for European Union institutions and Member States in the field of Critical Infrastructure Protection. The GCS is directly subordinate to the Prime Minister.

[722] Booz & Co EU CIP Stocktaking Web-Based Survey, 2009

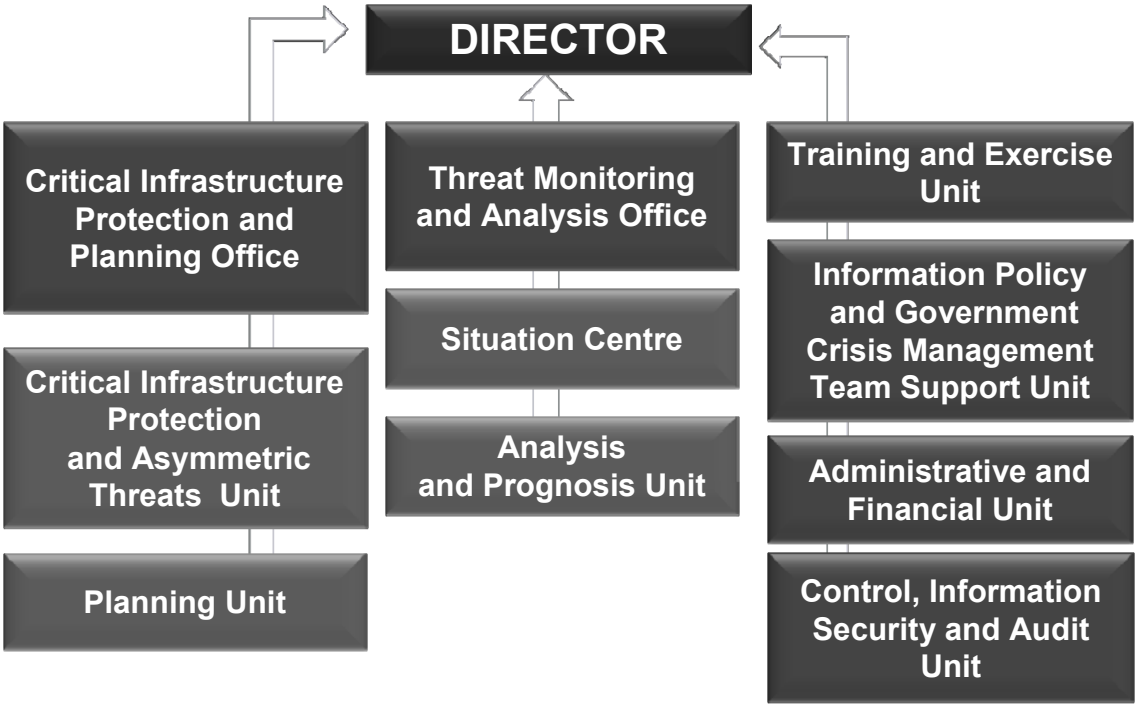


Figure 91: Organisational Chart – Government Centre for Security

The tasks of the GCS include:

- Provides the Council of Ministers, the Prime Minister and the Government Crisis Management Team with support in the area of crisis management
- Civil Planning
- Critical Infrastructure Protection
- Threats Monitoring
- Organizing exercises
- Conducting trainings
- International Cooperation

The responsibility for the protection of Critical Infrastructure within specific systems will fall under the appropriate Ministers or Heads of Central Offices.

23.3 Strategy & Policy

The approach to Crisis Management, and in turn CIP, in Poland is based on a hierarchical crisis management structure with a territorial perspective:

Figure 92: Territorial Perspective of Crisis Management in Poland

- **Crisis Management Act (CMA) of 26 April 2007**[723]

  The term Critical Infrastructure (CI) and CIP are defined in the Crisis Management Act of 26th April 2007 (CMA).

  CI are systems and mutually bound functional objects contained therein. This includes constructions, facilities, installations, and services of key importance for the security of the state and its citizens, as well as the efficient functioning of public administration authorities, institutions, and enterprises.

  CI includes the following systems:

  - Energy and fuel supply systems
  - Communication and tele-information network systems
  - Financial systems

[723] Booz & Co EU CIP Stocktaking Web Survey, 2009

- Water and food supply systems
- Health protection systems
- Transportation and communication systems
- Rescue systems
- Systems ensuring the continuity of public administration activities
- Systems of production, storing and use of chemical and radioactive substances, including pipelines for dangerous substances

CIP is defined as a set of organisational guidelines implemented with the aim of ensuring the functionality, continuity of functioning and integrity of critical infrastructure in order to mitigate threat, risks and weak points and to minimize and neutralize its effect and fast recovery in case of failures, attacks and other events disrupting its appropriate functioning.

An important element of the CIP system is setting up cooperation between the CI owners and the administration. The CMA obliges the owners of CI to nominate persons responsible for maintaining contacts with public administration in the field of critical infrastructure protection.

- **Organization and Operating Model of the Government Centre for Security**[724]

  This regulation from the Prime Minister established the composition of the Centre, as well as the responsibility and authority of the director. Tasks in the scope of counteracting, prevention, and elimination of consequences of terrorist acts shall be performed by the Centre in cooperation with the competent government organisations responsible for the counteracting, prevention and elimination of consequences of terrorist acts, in particular with the Head of the Internal Security Agency.

- **Organization and Operating Model of the Government Crisis Management Team**[725]

  This Order from the Prime Minister defines when and where the team would meet, protocol for invitations to join the team, and methodology for decision making.

- **Revised Crisis Management Act of 2009**[726]

  The primary revision in law resulting from the new amendment to the CMA is the lack of critical infrastructure protection plans on the national and voivodship levels. Also, a new National Critical Infrastructure Protection Program (NCIPP) was introduced. The aim of the NCIPP is to prepare a framework which will improve the security of Critical Infrastructure. The NCIPP will outline:
  - national priorities, goals, standards, which will ensure the adequate functioning of CI;
  - ministers and heads of central offices responsible for the particular CI systems introduced in the CMA;
  - criteria for determining critical infrastructure in each of the systems introduced in the CMA.

724 Journal of Laws No. 128 – 7016 – Item 821
725 Monitor Polski No. 61 – 2471 – Item 538
726 Act of 17th July 2009 on the change of the Crisis Managment Act

The operational issues dealing CIP will now be a part of crisis management plans prepared at the national, voivodship, poviat and gmina levels.

23.4 Methodology & Standards

Under the current CMA , the national government defined critical infrastructure systems. Currently, the criteria for selecting CI are being finished in collaboration with the help of government experts, industry, and the science community.

In addition, CI operators are required to submit a Critical Infrastructure Protection plans directly to the GCS. Many of these operators are state-owned.

- **Critical Infrastructure Protection Plans**

Critical Infrastructure Protection Plans (CIPP) exist on the operator level. CI operators are required to prepare and implement, as appropriate for the occurring threat, their own critical infrastructure protection plans. Operators must also hold their own reserve systems ensuring security and maintaining the functioning of the critical infrastructure until it is fully recovered. In addition, operators must indicate persons responsible for maintaining contacts with public administration in the scope of critical infrastructure protection.

23.5 Public – Private Partnership & International Collaboration

- **Public Administration / CI Owners Private-Public Forum**[727]

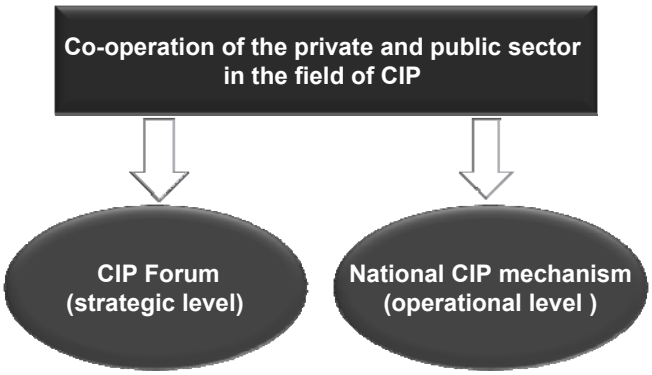


Figure 93: Public – Private Partnership Structure in Poland

To facilitate good cooperation between the public administration and the CI owners a private-public CIP Forum is being set up. The Director of GCS is the chairman of the

[727] Booz & Co EU CIP Stocktaking Web-Based Survey, 2009

forum. The aim of the forum is to bring together experts from the private and public sectors to talk together about the most important CIP issues, get to know each other, and build trust among members (crucial when working on security issues). This will include support for activities required to implement and sustain the national CI protection effort.

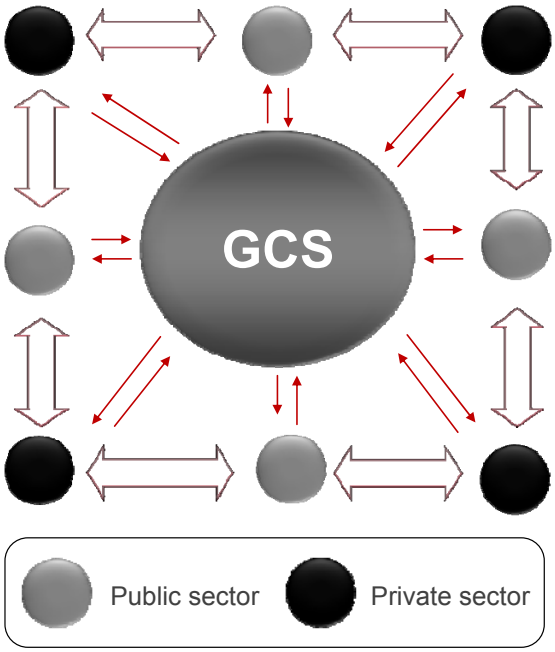


Figure 94: Functioning of Public – Private CIP Forum in Poland

One of the elements of this cooperation will be a rapid alert system which will enable to send information on threats that might affect a certain CI.

This Forum mechanism is already being used on work on sectoral criteria which will enable the public authorities to prepare the CI list.

- ***CERT Polska (Polish Computer Emergency and Response Team)***[728]

  The Polish Computer Security Response Team (CERT Polska), a part of the NASK organisation, is very much engaged in information infrastructure protection and security issues[729]. It was established in March 1996 (formerly known as CERT NASK). Its goals include:

  – To provide a single trusted point of contact in Poland for the community of NASK customers and other networks in Poland to deal with network security incidents and their prevention

  – To respond to security incidents in networks connected to NASK and networks connected to other Polish providers reporting security incidents

  – To provide security information and warning of possible attacks in cooperation with other incident response teams all over the world.

[728] www.cert.pl.
[729] http://www.nask.pl/run/n/Who_we_are

The CERT Polska team registers all requests, alerts, and incoming and outgoing information and provides statistical data and reports on registered incidents. It also provides help for sites that have security problems, and supplies current information about security problems and solutions for dealing with them[730]. CERT Polska itself points out that the creation and maintenance of a computer security and incident response team benefits the government in many respects. Four of its areas of activities in particular contribute to critical infrastructure protection: Early warning and alerting, centralized security management, security response, and auditing. CERT Polska signed a cooperation agreement on IT security with the Information Security Department of the Polish Internal Security Agency in July 2004.[731]

It also organizes a highly respected annual conference under the auspices of NASK. The SECURE conference series, organized since 1997, brings together company and IT managers; specialists in information system, network, and database security; and telecommunications and data network users who are interested in security issues. Co-sponsored by ISSE (Information Security Solutions Europe), ENISA (European Network and Information Security Agency) and the Polish Ministry of the Interior and Administration, SECURE is Europe's largest conference on data communications safety[732].

- **CERT GOV PL.**

  On 1 February 2008, the Internal Security Agency established the government's computer incident response team (CERT GOV PL). Its goals include ensuring and developing the ability of public administration units to defend themselves against cyber-threats, in particular against attacks on the infrastructure consisting of IT systems and networks, the disruption or destruction of which might to a large extent threaten the life and health of people, national heritage, and the environment, or result in considerable financial losses and disrupt the operation of the state.

  The goals of the CERT GOV PL include[733]:

  – Creating a policy concerning cyber-defence
  – Coordination of the information workflow among the above-mentioned entities with reference to cyber-threats
  – Detection and recognition of and response to cyber-threats
  – International cooperation concerning cyber defence
  – Playing an oversight role in relation to all national institutions, organisations, and units within governmental departments concerning cyber-defence

  The main objectives of the CERT GOV PL are:

  – Collecting information concerning the current security status and threats to the critical IT infrastructure

[730] http://www.cert.pl/index3.html?id=24
[731] Elgin M. Brunner and Manuel Suter, INTERNATIONAL CIIP HANDBOOK 2008-2009, Centre for Security Studies, ETH Zurich.
[732] http://www.naska.pl/newsID/id/431.
[733] Elgin M. Brunner and Manuel Suter, INTERNATIONAL CIIP HANDBOOK 2008-2009, Centre for Security Studies, ETH Zurich.

- Responding to IT security incidents, in particular the ones concerning the national critical IT infrastructure
- Post-incident computer forensics
- Establishing the policy for defence of the cyberspace of the Republic of Poland
- Training sessions and raising awareness of the topic
- Consulting and advising with reference to cyber-security

- ***ARAKIS-Gov***[734]

  In 2004, ARAKIS-gov, a distributed internet-based early-warning system developed and maintained by CERT Polska (NASK) in cooperation with the Information Security Department of the Polish Internal Security Agency, was accepted as the most important system for ensuring the protection of the Polish critical information infrastructure.

  The goal formulated for this project is to create a real early-warning system that can detect a new threat, analyze the exploit, and create a description of a new attack. Therefore, data from various sources, such as firewalls, darknets, honeypots, and anti-virus systems are correlated in order to detect emerging threats against the Polish network (also, notably, against governmental institutions), to detect new attack patterns, to monitor differences between attacks observed in Poland and in other countries, to gather statistical data, and to aid in general incident-handling activities.

  ARAKIS also provides a public dashboard showing a snapshot of network activity observed by the system. In the form of a polar chart, the alerts as generated by the ARAKIS system over the last 24 hours are plotted.

23.6 Funding & Human Resources

There are currently six staff members in the CIP and Asymmetric Threats Unit of the Government Centre for Security focusing on CIP activities in Poland.

Within the ministries, there are no dedicated CIP staff members. CIP responsibilities are carried out in addition to regular duties. Funds for CIP-related activities within each Ministry are planned in each Ministry's budget in accordance with its role in the Crisis Management system.

23.7 Training & Exercises

This will be prepared after the process of selecting CI will be concluded.

[734] http://arakis.cert.pl/en/index.html.

23.8 Sector-Specific Key Players & Initiatives

Any inquiries regarding sector-specific activities and responsible Ministries should be directed to the Government Centre for Security.

24 Portugal

Figure 95: Portugal

24.1 Summary

	Organisational Model	Strategy & Policy	Methodology & Standards	Public-Private Partnership & International Collaboration	Funding & Human Resources	Training & Exercises	Sector-Specific Key Players & Initiatives
Portugal	▪ There is no specific organisation dealing with CIP	▪ Portugal currently maintains a decentralised approach to CIP. ▪ Portugal has no specific strategies for CIP	▪ Generic Civil Protection Emergency plans	▪ NATO ▪ Eurodefence Portugal	▪ Not Applicable	▪ Not Applicable	▪ Crutial Project ▪ FOREVER Program

735

Portugal currently maintains a decentralised approach to CIP. There is no single agency with sole responsibility for the issue.

[735] Not Applicable = Open Source Research, Web-based survey and individual interviews have not shown information/data on the given argument

24.2 Organisational Model

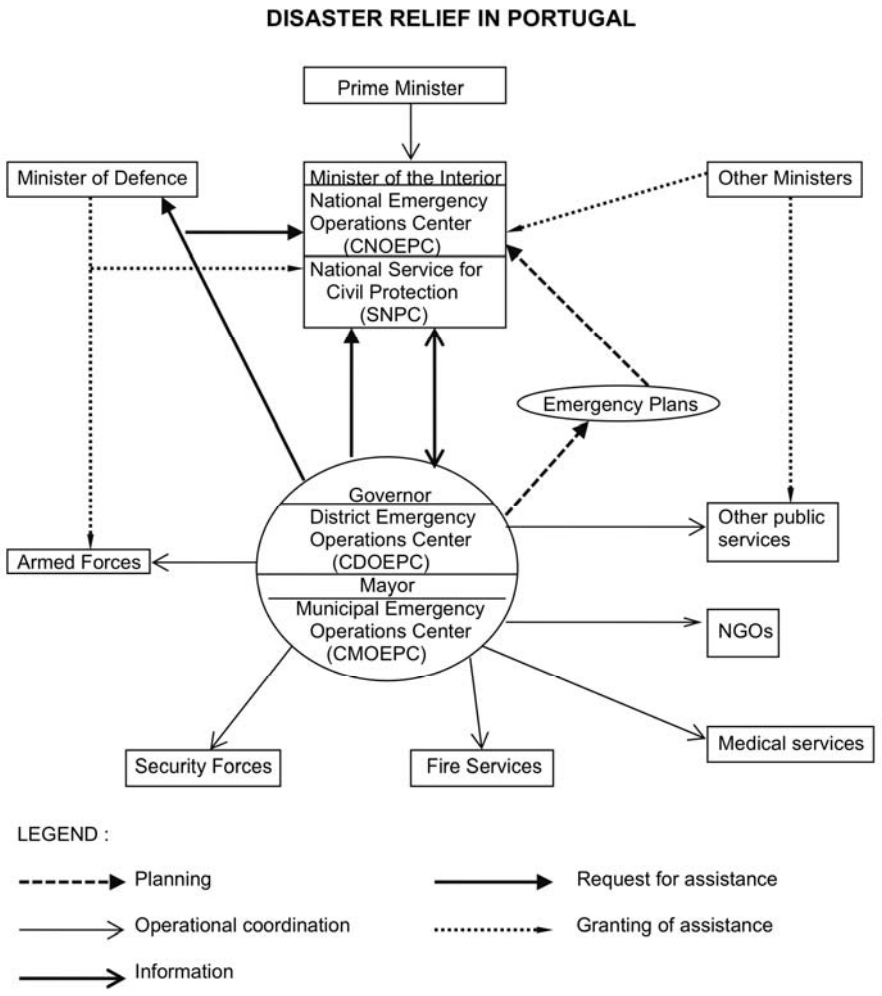


Figure 96: Organisational Chart (only CIP-related agencies shown)

Ministry of Interior[736]

The Ministry of the Interior is responsible for managing any civil protection and emergency preparedness response in the event of a national disaster.

Ministry for Finance Public Administration[737]

The Ministry for Finance Public Administration (MFAP) is the government department whose mission is to define and implement the financial policy of the state. In doing this it complies with public administration policies, and promotes the rational management of public

[736] http://www.mai.gov.pt
[737] http://www.min-financas.pt

resources, an increases the efficiency in its systems and procedures. In the pursuit of its mission, the MFAP has the responsibility to:

- Define, coordinate and evaluate the human resources policies in the civil service, in particular with regard to the regimes of public employment and professional qualification and development.
- Define, coordinate and apply policies relative to the civil service, in particular in the areas of organisation and management of services, with a view to increasing efficacy and efficiency, the rationalisation of the administrative activity and the promotion of quality in the public sectors.
- Manage the health subsystem of the civil service.
- Assure complementary social actions for civil employees.

Ministry for National Defence[738]

The Ministry of National Defence (MDN) prepares and implements national defence policy, under the powers conferred upon it by the Law on National Defence and Armed Forces. The MDN supervises the administration of the Armed Forces and other departments and agencies taking part in National Defence. The MDN is also responsible to develop an integrated policy for maritime affairs, in conjunction with the other relevant government authorities. The MDN also:

- participates in defining national defence policy and developing and implementing the policy of its military component;
- oversees the administration of the Armed Forces;
- promotes and fosters the study, research, technology development and dissemination of materials of interest to National Defence;
- provides technical and administrative support to the High Council of National Defence and the Prime Minister in the exercise of their functions on national defence and the Armed Forces.

The Ministry of Public Works, Transport and Communications (MOPTC)[739]

The government agency whose mission is to define, coordinate and implement national policy in the fields of construction and public works, air, maritime, river and land transport, and communications. MOPTC Tasks include:

- Developing the legal and regulatory framework for construction and public works, and the real estate sector.
- Developing the legal and regulatory framework for air, sea, river and land transportation.
- Coordinating and promoting the management and modernisation of airport infrastructure and air navigation, roads, rail and ports.
- Developing and regulating communications.

[738] http://www.mdn.gov.pt/mdn/pt/
[739] http://www.moptc.pt/

- Ensuring the coordination of the transport sector and stimulate the integration of its various modes and its competitiveness in order to better meet the users.
- Promoting business logistics and efficient competition.

The National Service for Civil Protection[740]

The National Service for Civil Protection works to prevent natural or man made hazards such as major accidents or disasters, to mitigate losses and damages for the population, material resources and environment, and to provide emergency relief during emergencies.

The civil protection system integrates the National Service for Civil Protection (SNPC), the Regional Service for Civil Protection (SRPC) and the Municipal Service for Civil Protection (SMPC). In accordance with the Portuguese Administrative Organisation, Portugal has 18 districts with a SNPC delegation in each district. The Ministry of the Interior is responsible for directing the civil protection and emergency preparedness response in case of disaster at national level. This responsibility belongs to the Presidents of the Azores and Madeira Autonomous Regions and to the Governors of each of the 18 districts in the mainland. At local level, responsibility belongs to the mayors.

Civil Protection is organised into the National Emergency Operations Centre Organisation (CNOEPC) and the National Disaster Emergency Response Office (NDERO).

- CNOEPC is activated by the SNPC to coordinate and control relief operations and logistics support at national level, as soon as it is realised a major disaster cannot be solved within Municipality or the District where it takes place.
- NDERO works 24 hours a day in the SNPC to control and manage the situation. At regional and local levels, Emergency Operations Centres in Districts (CDOEPC) and Municipalities (CMOEPC) are activated every time a major incident occurs inside those administrative areas.

Fire and Civil Protection National Service[741]

The Portuguese Service for Fire & Civil Protection (SNBPC) is the result of the merger in 2003 of three existing services – the National Service for Civil Protection, the National Commission for Wildfires, and the National Service for Fire and Fire-fighters. Its missions include:

- To coordinate and supervise all the operational activities undertaken by Portuguese fire-fighters.
- To assess infrastructure projects and plans with respect to their fire safety, and verify and inspect their observance.
- To coordinate emergency response activities at national and district level

24.3 Strategy & Policy

Portugal has no national strategy specifically devoted to critical infrastructure protection. It does however have a number of well developed strategies for the welfare and protection of Portugal's citizens and national interest.

[740] **http://www.snbpc.pt**
[741] **http://www.snbpc.pt**

24.4 Methodologies & Standards

Emergency Plans are organised as: National Emergency Plan; District Emergency Plans; Municipal Emergency Plans; Special National Plan.

National Special Emergency Plans are related to: Forest Fires; Floods; Earthquakes; Heat waves; Nuclear accidents; Droughts; Radiological accidents; Cold waves; Road transport of hazardous materials; Rail transport of hazardous materials.

People involved in Civil Protection and Emergency plan are (total of approximately 70 people): President of the National Service for Civil Protection; Deputies; Head of Service; Head of Division; specialists and employees.

The ***main civil protection agents*** are the Fire National Service (SNB), the security forces (Police and National Guards), the Armed Forces, the Maritime and Aeronautics Authorities, and the National Institute for Medical Emergency (INEM). The league of volunteer firemen, health services, social security institutions, NGOs and other volunteer organisations, public services responsible for forest and natural reserves, industry and energy, transport, communications, water resources and environment, security and relief services belonging to private and public companies, seaports and airports, have the duty to cooperate with civil protection agents already mentioned. Several scientific and technological institutions and organisations are commonly assigned for cooperation with SNPC and are important contributors into the civil protection system. These include those related to meteorology and geophysics, engineering, industrial technology, geology, forestry, nuclear protection and natural resources.

24.5 Public – Private Partnership & International Collaboration

- ***NATO***

Portugal is a founding member of NATO (1949), the OECD (1961) and EFTA (1960); it left the latter in 1986 to join the European Economic Community which become the European Union in 1993. In 1996 it co-founded the Community of Portuguese Language Countries (CPLP). The country is a member state of the United Nations since 1955.

- ***Eurodefence-Portugal***[742]

The EuroDefense association was created in March 1994 in order to promote a European security and defence identity, contribute to the development of a sense of European defence through specific initiatives, establish and reinforce the links with fellow associations in each WEU country. The first national associations were in France, Germany, then it Italy, Spain, Belgium, the Netherlands, the UK, Portugal, Austria, Luxembourg, Greece, Hungary and Romania. It was decided that each national association would have the name EuroDefense followed by the name of the country in the national language.

2001 marked the creation of a EURODEFENSE bringing together all the national associations and governed by a Memorandum of Understanding. All associations are driven by a common belief in the importance of a strong common defence and share the same belief that *"It is not possible to have defence without Europe nor Europe without defence"*.

[742] http://eurodefense.aip.pt/

The associations have as their mission *"to pursue the search for a united and effective European defence"*.

24.6 Training & Exercises

There are no organic disaster response units, nor schools for civil protection. The training of civil protection agents lies down under their commands/directions that have schools and training centres for such purpose. However, the SNPC is responsible for a systemic public awareness. information and education campaign, through the dissemination of security and self-protective measures to be adopted by the population in case of a situation of risk.

24.7 Sector – Specific Key Players & Initiatives

ENERGY

The Directorate General for Energy and Geology (DGEG) is the organisation responsible for the conception, promotion and evaluation of policies for geological resources, with a view toward sustainable development and the security of the energy supply. The DGEG is the licensed entity overseeing the installation of the means of extraction, storage and transport of natural gas. The Regional Directorates of the Economy (DREs) are responsible for the licensing of the supply networks for natural gas (under concession or licensing).

DGEG is also responsible for licensing the facilities intended for fuel extraction, processing, refining, storage, transport, distribution and supply, without prejudice to the authority of Municipalities and the Regional Directorates of the Economy (DREs). It is also responsible for monitoring the compliance of Portuguese and international regulations regarding mandatory fuel reserves, and the collation of statistics for production, import, consumption and export of fuel.

Initiatives:

- ***Crutial project*[743]**

  The Crutial project is introducing new networked ICT systems to manage the electric power grid. CRUTIAL's innovative approach includes modelling interdependent infrastructures and building new architectures, resilient to both accidental failures and malicious attacks. The objectives of the project include the investigation of scalable and open models and architectures, the analysis of critical scenarios in which faults in the information infrastructure could lead to serious impacts on the electric power infrastructure; the investigation of distributed architectures which enable dependable control and management of the power grid.

INFORMATION AND COMMUNICATION TECHNOLOGY

Public Authorities:

- ***CERT.PT*[744]'**

[743] http://crutial.cesiricerca.it/

The roles of the CERT.PT include:

– Offering technical support to computer users in resolving security incidents, advising on best-practices, analysing artefacts, and coordinating actions with the parties involved.

– Gathering and disseminating information about security vulnerabilities and recommended solutions.

– Gathering from accredited sources information related to security vulnerabilities, and working with the community to minimise their impact at the National level

– Promoting the creation of new CERT/CSIRTs in Portugal, and raising awareness of security issues for computer users.

- ***Autoridade Nacional de Comunicações (ANACOM)[745]***

The regulatory authority for electronic communications and postal services in Portugal. ANACOM also represents Portugal at relevant international fora and has several functions with respect to electronic commerce. It has been active since 1989. Its main objectives are to promote competition, transparency in prices and conditions of use, and the development of communication networks and markets. ANACOM also works to defend the interests of citizens, in particular the users of communications. This work involves ensuring access to the global services through both electronic communications and postal services.

RESEARCH

Initiatives:

- ***ReSIST: Resilience for Survivability in IST[746].***

ReSIST is an Network of Excellence in Information Systems Technology security that addresses the strategic objective “Towards a global dependability and security framework” and responds to the stated “need for resilience, self-healing, dynamic content and volatile environments”.

The network will integrate leading researchers active in the multidisciplinary domains of dependability, security, and human factors, to provide Europe with a well-focused coherent set of research activities. These are aimed at ensuring that future “ubiquitous computing systems”, the immense systems of ever-evolving networks of computers and mobile devices which are needed to support and provide Ambient Intelligence (AmI), have the necessary resilience and survivability.

- ***HIDENETS***

HIDENETS (HIghly DEpendable IP-based NETworks and Services)[747] is a targeted research project funded by the European Union under the Information Society Sixth

[744] http://www.cert.pt
[745] http://www.anacom.pt/index.jsp?categoryId=2958
[746] http://www2.laas.fr/RESIST/index.html

Framework Programme. The project was started in January 2006 and has a duration of three years.

The aim of HIDENETS is to develop and analyse end-to-end resilience solutions for distributed applications and mobility-aware services in ubiquitous communication scenarios. Technical solutions will be developed for applications with critical dependability requirements, such as car-to-car communication infrastructure service support.

- ***FOREVER: Fault/intrusiOn REmoVal through Evolution & Recovery***[748]

FOREVER is a one-year research project (Jan-Dec 2008) funded by the European Union through the ReSIST Network of Excellence. The goal of the project is to develop a Fault/intrusiOn REmoVal through Evolution & Recovery (FOREVER) service. This service can be used to enhance the resilience of replicated systems, namely those that can be affected by malicious attacks. FOREVER addresses three of the research gaps identified in ReSIST D13 deliverable, namely: GE1 – Evolution of Threats, GA3 – Dependability Cases, and GD1 – Diversity for Security. In order to achieve the project goal, the work is divided into three main tasks: definition of the FOREVER service architecture; analysis of how diversity can be managed; evaluation of the FOREVER service and development of a dependability case.

- ***Health Early Warning System***[749] [750]

HEWS is a project by the Portugese Instituto Nacional de Saúde and Tekever S.A[751]. HEWS will enable timely detection and tracking of emerging threats to public health and safety via satellite.

[747] http://www.hidenets.aau.dk/
[748] http://forever.di.fc.ul.pt/
[749] http://ec.europa.eu/research/infocentre/article_en.cfm?id=/research/headlines/news/article_09_01_09_en.html&item=Infocentre&artid=9553
[750] http://www.esa.int/esaCP/SEMZ00V681F_index_0.html
[751] http://www.tekever.com

25 Romania

Figure 97: Romania

25.1 Summary

	Organisational Model	Strategy & Policy	Methodology & Standards	Public-Private Partnership & International Collaboration	Funding & Human Resources	Training & Exercises	Sector-Specific Key Players & Initiatives
Romania	▪ There is no specific organisation dealing with CIP	▪ Romania is dealing in an unstructured way with CIP ▪ Romania has no specific strategies for CIP	▪ Not Applicable	▪ Collaboration in the develop-ment of the Mutual Support Integrated Operational System	▪ Not Applicable	▪ Not Applicable	▪ Not Applicable

752

Romania currently maintains a decentralised approach to CIP. There is no single agency with sole responsibility for the issue. Responsibilities for the handling of critical situations are distributed across various agencies and structures.

Romania has an Emergency Situations Management System (ESMS) that includes the General Inspectorate for Emergency Situations, Inspectorates, committees, units, sub-units and other groups. The head of the ESMS is the Prime Minister, through the Ministry of Administration and Interior.

The Minister of Administration and Interior, in turn, has a General Inspectorate for Emergency Situations as a specialised body for the general co-ordination of Emergency Situations.

At the local level, the Prefects of the counties and the Mayors in the local public administrations are responsible for civil security and emergency management[753].

[752] Not Applicable = Open Source Research, Web-based survey and individual interviews have not shown information/data on the given argument

[753] International CEP Handbook 2006, OCB The Swedish Emergency Management Agency

25.2 Organisational Model

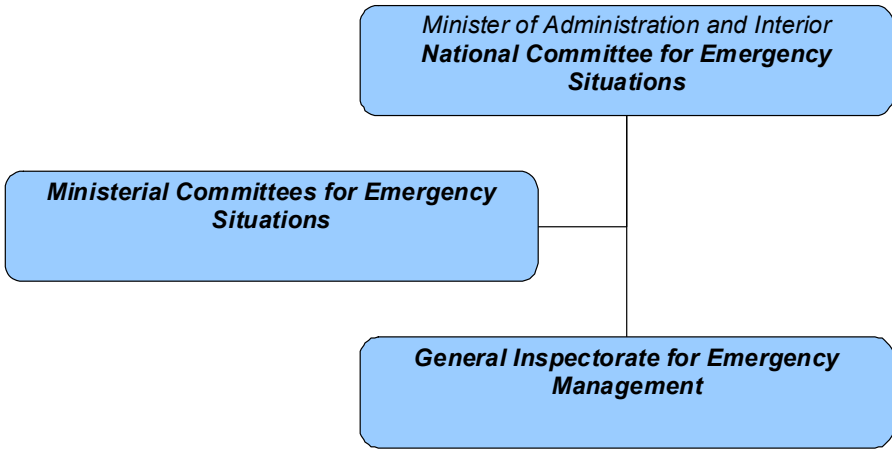


Figure 98: Organisational Chart (only CIP-related agencies shown)

Main Actors/Responsibilities

Inspectoratul General pentru Situații de Urgență (Romanian General Inspectorate for Emergency Situations, GIES)[754]

The Romanian General Inspectorate for Emergency Situations (GIES) was founded by merging of Civil Protection Command (*Comandamentul Protecției Civile*) and General Inspectorate of Military Fire Corps (*Inspectoratul General al Corpului Pompierilor Militari*), as a specialised element of the Romanian Ministry of Administration and Interior. At the national level the GIES is responsible for the coordination of the organisations involved in emergency management.

Ministerul Administrației şi Internelor (Ministry of Administration and Interior)[755]

The Ministry of Administration and Interior of Romania is responsible for Romanian public administration, order and safety. Its main tasks are:

- Establishing measures for defending human rights and liberties, and for defending public and private property.
- The organisation and development, through specialised structures, of activities for preventing and countering terrorism, organised crime, the trafficking and consumption of illicit drugs, trafficking in persons, illegal migration, computer crime, as well as other crimes and antisocial deeds.
- Monitoring the reform and restructuring of the central and local public administration, in compliance with the European Union standards and the domestic legislation.

[754] http://www.igsu.ro/
[755] http://www.mai.gov.ro/engleza/Home_eng/english.htm

- Guiding and controlling the activity of the Prefectures in their fulfilment of the federal governing programme.

25.3 Strategy & Policy

The Gov. Decision21/2004–art. 1(2) constituted the National Emergency Management System, so that "it is composed of a network of structures tasked within the emergency situation management, on levels and areas of competence, having the necessary resources and infrastructure to carry out their tasks."

The National Emergency Management System organises Romanian efforts for the prevention and management of emergency situations, and the provision and coordination of human, material and financial resources.

The General Inspectorate for Emergency Situations is part of the National Emergency Management System and is a component of the National Defence System.

25.4 Public – Private Partnership & International Collaboration

The GIES is involved in NATO exercises, and collaborates as part of the Mutual Support Integrated Operational System for the relief of undesirable effects caused by natural or technological disasters and terrorist activities within the South-Eastern Europe region.

25.5 Sector – Specific Key Players & Initiatives

NUCLEAR

Romania currently has one active nuclear power plant, with two reactors, which provide approximately 18 % of the national power generation capacity of the country.

Public authorities

- ***National Agency for Atomic Energy*** [756]

  The Romanian National Agency for Atomic Energy (ANEA) has a technical and research role in the nuclear sector.

- ***Romanian Nuclear Activities Authority***[757]

  The Romanian Nuclear Activities Authority (RAAN) operates the *Triga* research reactor and undertakes research and development on safety, nuclear fuel, radiation protection, reactor systems, and radioactive waste management. It also operates a heavy water plant.

- ***National Commission for Nuclear Activities Control***[758]

  The National Commission for Nuclear Activities Control (CNCAN) is the regulator established under the Nuclear Act 1996 to ensure nuclear safety and to licence

[756] http://www.mct.ro/anea/anea.htm
[757] http://www.raan.ro/
[758] http://cncan.ro/ro/default.php

nuclear sites and operations. It is also responsible for safeguards and international liaison, ensuring conformity with IAEA standards, as well as radiation protection.

INFORMATION AND COMMUNICATION TECHNOLOGIES

Public authorities

- ***Ministerul Comunicațiilor şi Societății Informaționale (Ministry of Communications and Information Society)***[759]

  The Ministry of Communications and Information Technology has the mission to guide Romania's transition to an Information Society. The main responsibilities of the Ministry are:

  – Improvement of the services to citizens to provide broader access to information
  – The reduction of bureaucracy
  – Faster economic growth and higher economic competitiveness for the Romanian economy.

WATER

Public authorities

- ***Ministerul Mediului şi Dezvoltării Durabile (Ministry of the Environment and Sustainable Development)***[760]

  The Ministry of Environment and Sustainable Development promotes a unitary, coherent environmental policy, and its main objectives are:

  – Integration of the environmental requirements in the sectorial strategies.
  – Supplying drinking water to the population, purifying waste waters, protecting the population against the dangerous effects of noise, closing waste disposal sites that do not comply with current requirements, renewing the technology of central heating systems and increasing their energy efficiency, promoting renewable sources of energy, and the ecological rehabilitation of the historically polluted areas or coastal erosion
  – Preventing environment damage caused by economic growth.
  – Guarding biodiversity.
  – Monitoring and reducing climate change risks.
  – Risk management and prevention of flood-associated disasters.
  – Implementing the "polluter pays" principle.
  – Financing projects related to the environment
  – Raising public awareness and strengthening cooperation with environmental non-governmental associations.

HEALTH

[759] http://www.mcti.ro/index.php?L=1
[760] http://www.mmediu.ro/

Public authorities

- ***Ministerul Sănătății Publice (Ministry of Public Health)***[761]

  The Ministry of Public Health (MoPH) is responsible for developing national health policy and dealing with public health issues. The MoPH plays a major role in the decision-making process in health policy and it is responsible for setting organisational and operational standards for public health institutions, developing and financing national public health programmes, data collection, empowering public health officials and producing regular reports on the population's health status. The Ministry is responsible for providing preventive services at both the individual and population level.

FINANCIAL

Public authorities

- ***Ministerul Economiei şi Finanțelor (Ministry of Economy and Finance)***[762]

  The Ministry of Economy and Finance of Romania is one of the fifteen ministries of the Government of Romania. The following agencies are subordinated to the Minister:

  – National Agency for Fiscal Administration (Agenția Națională de Administrare Fiscală)
  – National Customs Authority (Autoritatea Națională a Vămilor)
  – Financial Guard (Garda Financiară)
  – 40 Public Finances County General Directorates (Direcții generale ale finanțelor publice județene), the Public Finances General Directorate of Bucharest (Direcția Generală a Finanțelor Publice a Municipiului Bucureşti) and the General Directorate for the Administration of Big Taxpayers (Direcția generală de administrare a marilor contribuabili)

- ***Banca Națională a României, BNR (National Bank of Romania)*** [763]

  The National Bank of Romania, established in April 1880, is the central bank of Romania. The main tasks of the National Bank of Romania are:

  – To define and implement monetary and exchange rate policy.
  – To conduct the authorisation, regulation and prudential supervision of credit institutions and to promote and oversee the smooth operation of the payment system with a view to ensuring financial stability.
  – To issue banknotes and coins as legal tender on the territory of Romania.
  – To set the exchange rate regime and to supervise its observance.
  – To manage the official reserves of Romania.

TRANSPORT

[761] http://www.ms.ro/
[762] http://www.minind.ro/
[763] http://www.nbr.ro/

Public authorities

- ***Ministerul Transportutilor şi Infrastructurii (Ministry of Transport and Infrastructure)***[764]

  The Ministry of Transport and Infrastructure is responsible for establishing general transport strategy and policy, defining transport network needs, communicating with international organisations and organising the transport sector through licensing of operators and promulgating rules and regulations.

RESEARCH FACILITIES

Public authorities

- ***Ministerul Educației şi Cercetării, MEdC (Ministry of Education and Research)***[765]

  The Ministry of Education and Research of Romania is empowered by the Government with the management of the national system of education and research: it coordinates and controls the national education and research system, plans, elaborates and implements government policies regarding education, is responsible for research, technology and innovation. The Ministry is divided into several departments that are responsible for different tasks and education levels and some of the responsibilities of the ministry are exercised through agencies, services and specialised offices under its authority.

[764] http://www.mt.ro/engleza/index_eng.html
[765] http://www.edu.ro/

26 Slovakia

Figure 99: Slovakia

26.1 Summary

	Organisational Model	Strategy & Policy	Methodology & Standards	Public-Private Partnership & International Collaboration	Funding & Human Resources	Training & Exercises	Sector-Specific Key Players & Initiatives
Slovakia	▪ CIP is covered by Crisis Management and Civil Protection under the Ministry of Interior	▪ Slovakia is dealing in a structured way with CIP - involving all sectors considered strategic by the Government	▪ Specific CIP-technology tools: CECIS, ECURIE, RAPEX, RASFF	▪ The Ministry of Interior has recently established a dialogue with all relevant key players and held preliminary discussions	▪ No CIP-specific budget known ▪ Approx. 1-10 public employees working on CIP	▪ Some universities offer CIP-related degrees ▪ Sporadic CIP-related exercises are performed	▪ No specific CIP-related initiatives available

766

Slovakia is tackling CIP in a structured way. A national set of actions has been approved and is being further developed. The Ministry of the Interior approved a resolution for National CIP Programme, and an Act on CIP is under development. CIP is covered by the Crisis Management and Civil Protection departments under the Ministry of Interior.

The Ministry of Interior of the Slovak Republic (SR) defines CIP as “a new concept in the field of security and civil protection[767]”. Critical infrastructure is defined as that infrastructure (selected organisations and institutions, buildings, facilities, services and systems), which in case of threats can cause destruction to or disablement of the political and economic management of the country, or threats to the life and health of the population[768]. This may occur because of major natural or technological disasters, terrorist attacks, the effects of extreme weather, or for other reasons.

766 Not Applicable = Open Source Research, Web-based survey and individual interviews have not shown information/data on the given argument

767

768

26.2 Organisational Model

Main Actors/Responsibilities:

Ministerstvo vnútra Slovenskej republiky, MV SR (Ministry of Interior of the Slovak Republic)[769]

The main responsibilities of the SR Ministry of Interior are:

- Protection of the government, public order, security of persons and property, documents, the integrated rescue system, civil protection and protection against fires.
- General administration, including internal affairs and the territorial administrative functions of the Slovak Republic.
- Police force and fire and rescue corps.
- Coordinating staff training in the municipalities and higher territorial units.

The SR Ministry of Interior is the central authority for the administration of civil protection measures financed from the state budget.

Ministerstvo obrany, MoD SR (Ministry of Defence of the Slovak Republic)[770]

The Ministry of Defence of the Slovak Republic is the central state administration of the with responsibility for defence. It begun its work 1st of January 1993. The main responsibilities of the Ministry are:

- defence of the Slovak Republic;
- building and commanding Army of the SR;
- co-ordination of the activities of the state administration and institutions aimed at preparation of the defence of the SR;
- safeguarding Slovak air space;
- co-ordinating military air traffic with civil air traffic;
- commanding military intelligence, and
- managing military facilities and military forests.

Ministry of Transport and Telecommunications[771]

This Ministry is involved in the management of CIP activities in the fields of ICT and Transport (Road, Rail, Air)[772].

Ministry of Economy[773]

This Ministry is involved in the management of CIP activities in the fields of Energy.

[769] http://www.minv.sk/
[770] http://www.mosr.sk/index.php?ID=149
[771] www.telecom.gov.sk
[772] Booz & Company Survey “Stock-taking of Existing Critical Infrastructure Protection Activities”
[773] www.economy.gov.sk

26.3 Strategy & Policy

The Ministry of the Interior approved a resolution for a National Programme on CIP, and the development of an Act on CIP is under development[774]. This Act will focus on a series of sectors that are considered critical for the country, namely:

- Water
- Food
- Health (Medicines, Serums, Vaccines and Pharmaceuticals)
- Energy (Electricity, Oil, Gas)
- Nuclear energy
- Information and Communication Technology (Fixed & Mobile TLC, Internet, Networks, Radio, Satellite Communications, Broadcasting)
- Transport (Rail, Road, Air, River)
- Industry (Pharmaceutical, Metallurgy, Chemical, Defence)
- Financial (Regulated Markets, Payment and Securities clearing)
- Post

The development of the Act has begun, and is expected to be completed in approximately one year.

Some steps are have already been completed, namely:

- The development of the CIP policy has been assigned to the Crisis Management and Civil Protection department.
- A public-private round table has been organised.[775]

The CIP Strategy includes a definition of what is considered “Critical Infrastructure” for the Slovakian Government. The steps already performed include:

- the definition of detailed measurable criteria for designating infrastructure as “critical”;
- the definition of a list of critical infrastructure, and
- the mapping of critical infrastructure throughout the country.

There are multiple internal and external preventive security plans for the critical infrastructure, each related to a specific risk. These are submitted to the Ministry of Interior.

The Government of the Slovak Republic annually evaluates the capabilities of the key state bodies to respond in a timely and efficient way to the threat of terrorist attacks, and makes an assessment of the likely consequences of these attacks.

In the *National Plan of Action on Combating Terrorism*[776], the government is directed to define the measures necessary to improve its preparedness to adopt any necessary measure to predict and avert the threat of a terrorist attack and to manage its consequences.

[774] Booz & Company Survey “Stock-taking of Existing Critical Infrastructure Protection Activities”
[775] Booz & Company Survey “Stock-taking of Existing Critical Infrastructure Protection Activities”
[776] http://www-8.vlada.gov.sk/1788/

This program reflects changes in the development and structure of crime, new conditions and options of fighting against crime in the period of SR's membership in European and transatlantic structures, changes in criminal law regulations, changes in the forms and methods of crime detection and investigation, as well as in the police instruments and procedures applied.

The Slovak Government is planning to prepare a draft law on combating terrorism. It will create appropriate mechanisms to improve co-ordination, cooperation and interoperation among intelligence services, the police and other relevant services. In combating terrorism and organised crime, specialised units and services perform important tasks. The Government will continue supporting their activities.

The Government plans to enhance civil protection for the population. In the event of natural disaster, accident, or emergency, the nation's civil protection capabilities must be ready to undertake:

- operational responses;
- flexible analysis and assessment of the extent of threat;
- timely and undistorted notification and warning of the population, and
- efficient steps to protect the population.

The Government will continue modernising the civil protection warning and notification network. In order to better face emergency situations, the Slovak Government plans to complete the integrated rescue system, in particular completing its communication and information infrastructure.

Some of the acts and laws important for the civil security of Slovakia are:

- Act of the National Council of Slovak Republic No. 42/1994 Coll. on Civil Protection of the Population (and later amendments)
- Act of the National Council of Slovak Republic No. 129/2002 Coll. on Integrated Rescue Systems
- Act of the National Council of Slovak Republic No. 387/2002 Coll. on Crisis Management of the State in War and Warfare
- Act of the National Council of Slovak Republic No. 261/2002 Coll. on the Prevention of Major Industrial Accidents and on the amendments of some acts.
- Constitutional Act No. 227/2002 Coll. on the Security of the State in Times of War, Warfare and State of Emergency
- Order No. 75/1995 Coll. on the Provision of Evacuation
- Order No. 303/1996 Coll. on the Provision of Training for Civil Protection
- Order No. 348/1998 Coll. on the Provision of the Technical and Operational Conditions of the Civil Protection Information System

- Order No. 201/2002 Coll. on the Provision of the Organisation of the Civil Protection Units and the Rescue, Containment and Elimination Operations[777]

26.4 Methodologies & Standards

Slovakia uses a number of European technology tools to aid its CIP activities:

- Common Emergency Communication and Information System (CECIS). CECIS facilitates communication between the European MIC with National Authorities, making response to disasters faster and more effective.
- European Community Urgent Radiological Information Exchange (ECURIE).
- RAPEX, the EU rapid alert system for all dangerous consumer products.
- Rapid Alert System for Food and Feed (RASFF).

Other information sharing and emergency response tools are available, usually developed and funded publically[778].

26.5 Funding & Human Resources

There are approximately 1-10 public employees working specificly on CIP related activities, but there is no evidence of a dedicated budget, if it exists[779].

26.6 Training & Exercises

There are some specific CIP-related degree programmes at general Universities that are attended by Public Authorities and Private Operators.

Sporadically CIP-related exercises are held, involving Police, Civil Protection and Private Operators[780].

26.7 Sector – Specific Key Players & Initiatives

ENERGY

Public authorities:

- **Ministerstvo hospodárstva SR (Ministry of Economy)**

  The Ministry of Economy is the state administration responsible for:

  – Industry, with the exception of the food industry, construction products and the manufacture of construction materials.

  – Power generation, inclusive of nuclear fuel management and the storage of nuclear waste.

[777] Swedish Emergency Management Agency, *International CEP Handbook 2006: Civil Emergency Planning in the NATO/EAPC Countries*
[778] Booz & Company Survey "Stock-taking of Existing Critical Infrastructure Protection Activities"
[779] Booz & Company Survey "Stock-taking of Existing Critical Infrastructure Protection Activities"
[780] Booz & Company Survey "Stock-taking of Existing Critical Infrastructure Protection Activities"

- Heat generation and gas manufacture.
- Exploitation and treatment of solid fuels, exploitation of oil and natural gas, exploitation of core and non-metallic resources, and searching, survey and exploitation of radioactive materials.
- Support of small and medium-size businesses.
- The creation and support of a good business environment.
- Domestic trade, foreign trade, tourism and consumer protection.
- Protection and the use of mineral resources, including the supervision of the protection and the use of mineral deposits.
- Supervision of health and safety protection in work places, safety in mining, activities performed in productive mines, and at the use of explosives.
- Enforcement of the ban on the development, manufacture, storage, use and trade of chemical weapons and their precursors.
- The coordination and guidance of economic mobilisation.
- The privatisation of state property and the administration of state property in the business environment.

The Ministry is also responsible for some defence issues and for creating conditions favourable for defence and security preparations.

The Ministry is also responsible for some international agreements and treaties, and to develop bilateral contacts and relations between countries. It exercises due diligence in legal matters subjected to the extent of its competence, and it develops Bills and drafts of other general binding legal regulations.

- ***Slovenská inovačná a energetická agentúra, SIEA (Slovak Innovation and Energy Agency, SIEA)***[781]

The main tasks of the SIEA are:

- Fulfilling the tasks of the Slovak Ministry of Economy within the the energy sector.
- Reviewing options for the more effective use of energy, renewable energy sources, and combined electricity and heat production.
- Cooperating with the Ministry and other central state authorities in the development of legal and economical instruments to influence effective and environmentally friendly use of energy.
- Cooperating in the certification and assessment of the energy efficiency of appliances and devices.

[781] http://www.sea.gov.sk/english/index.htm

- Providing expert advice on the level of energy usage, the efficiency of investment in energy sector, the level of organisation and management of energy sector, and energy consumers.
- Issuing grants resolving problems in energy sector.
- Coordinating energy advisory centres and energy auditors.
- Cooperating with local government bodies and with other NGOs in promoting energy efficiency.

NUCLEAR INDUSTRY

Public authorities:

- ***Úrad jadrového dozoru Slovenskej republiky, UJD (Slovak Nuclear Regulatory Authority)***[782]

  The UJD is an independent government body established in January 1993. The mission of the UJD is to ensure public health and safety are protected during the peaceful use of nuclear energy and to ensure the safety of nuclear installations in Slovakia.

  The main tasks of the UJD are to regulate the safety of nuclear installations, develop safeguards and controls for nuclear materials, oversee the whole nuclear fuel cycle, and provide quality assurance programmes in the nuclear industry.

  It has regulatory functions in:

  – establishing standards and regulations;
  – issuing licenses for nuclear facility operators, selected personnel, and users of nuclear materials, and
  – inspecting nuclear facilities and users of nuclear materials.

HEALTH

Public authorities:

- ***Ministerstvo zdravotníctva SR (Ministry of Public Health)***[783]

  The Ministry of Public Health (MOPH) is responsible for developing national health policy and managing with public health issues. The MoPH plays a major role in the decision-making process in health policy and it is responsible for setting organisational and operational standards for public health institutions, developing and financing national public health programmes, data collection, empowering public health officials and producing regular reports on the population's health status. The Ministry is responsible for providing preventive services at both the individual and whole-of-population level.

FINANCIAL

[782] http://www.ujd.gov.sk/AMIS/www/ujd.nsf/indexEn?OpenPage
[783] http://www.ms.ro/

Public authorities:

- ***Ministerstvo financií Slovenskej republiky (Ministry of Finance of the Slovak Republic)***[784]

- ***Národná banka Slovenska, NBS (National Bank of Slovakia)*** [785]
  Authorised by the Slovak Government, the Bank represents Slovakia in international financial institutions and in international money market transactions related to monetary policy performance.

TRANSPORT

Main operators:

- ***Železnice Slovenskej republiky, ŽSR (Slovak Republic Railways)***[786]

  ŽSR is the state-owned railway infrastructure operator in Slovakia. It was founded in 1993 as the successor of the Československé státní drahy. Until 1996 it had formal, and since then a de facto, monopoly on rail transportation in the country.

  In 2002 a law divided the company into ŽSR for infrastructure maintenance, and Železničná spoločnosť (ZSSK)[787] for transport. In 2005 this new company was further split into Železničná spoločnosť Slovensko (ZSSK) providing passenger services and Železničná spoločnosť Cargo Slovakia (ZSSK Cargo/ZSCS) providing freight services.

RESEARCH FACILITIES

Public authorities:

- ***Ministerstvo školstva Slovenskej republiky (Ministry of Education)***[788]

  The Ministry of Education of the Slovak Republic is the central body of the state administration of the Slovak Republic responsible for elementary, secondary and higher education, educational facilities, lifelong learning, science and for the state's support for sports and youth.

  It administers the network of school and school facilities in the Slovak Republic through generally binding rules, and by providing vocational guidance to operators. It typically does this through regional school authorities.

  The Ministry is also responsible for sport, science and research.

[784] http://www.finance.gov.sk
[785] http://www.nbs.sk/en/home
[786] http://www.zsr.sk/anglicky.html?page_id=124
[787] http://www.zssk.sk/en
[788] http://www.minedu.sk/index.php?lang=en

27 Slovenia

Figure 100: Slovenia

27.1 Summary

	Organisational Model	Strategy & Policy	Methodology & Standards	Public-Private Partnership & International Collaboration	Funding & Human Resources	Training & Exercises	Sector-Specific Key Players & Initiatives
Slovenia	Inter-ministerial working group on critical infrastructure in Slovenia, chaired by Ministry of Defence	▪ Slovenia is dealing in an unstructured way with CIP ▪ No specific CIP-related strategy and policy in place	▪ General Emergency and Relief Plans	▪ Bilateral agreement with Austria on the tunnel Karavanke	▪ No CIP-specific budget ▪ Some public employees working on CIP, embedded in the different Ministries	▪ Training Centre for Civil Protection and Disaster Relief of the Republic of Slovenia	▪ ECURIE ▪ ZARE Communication System ▪ Research Project on CIP

The Republic of Slovenia currently maintains a decentralised. Although explicit CIP strategies have not yet been developed or implemented, there is a inter-ministerial working group on critical infrastructure, chaired by Ministry of Defence and co-chaired by Ministry of Interior (started 2006). In September 2009, the Government received the third CIP from this group, and future tasks depend upon the guidance of this group.

27.2 Organisational Model

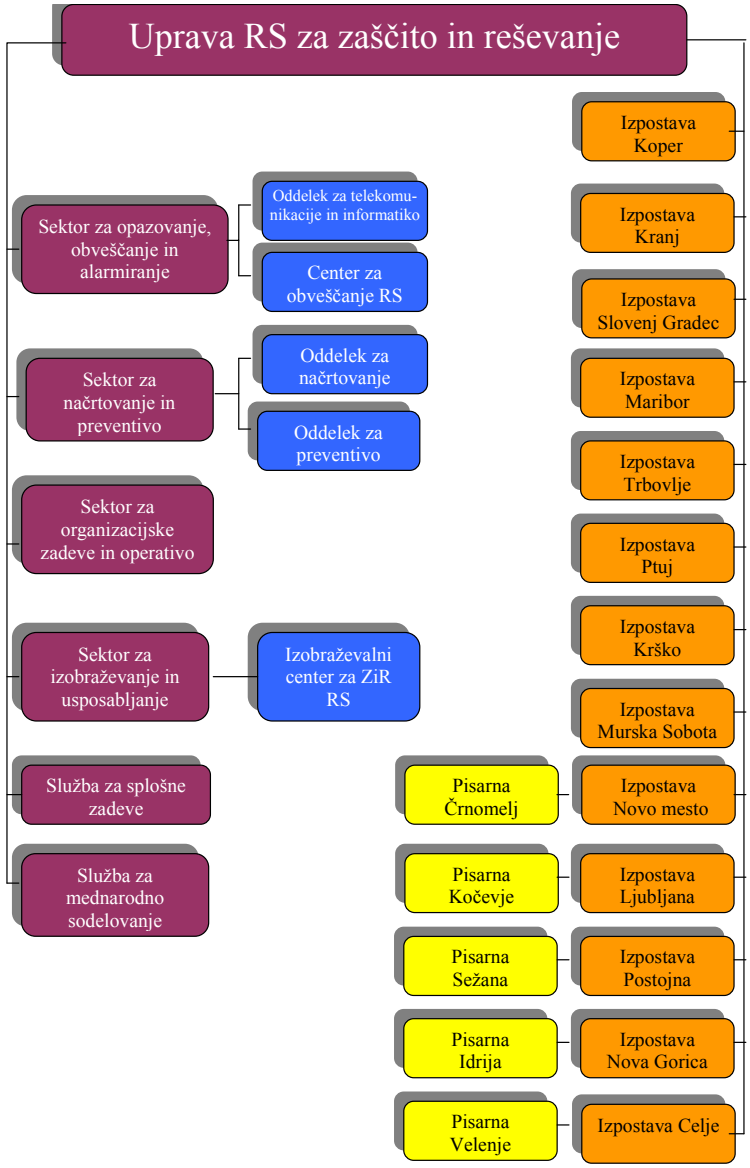


Figure 101: Organisational Chart (only CIP-related agencies shown)

Main Actors/Responsibilities

Ministrstvo za Obrambo Slovenska Vojska (Ministry of Defence)[789]

The Ministry of Defence carries out administrative and professional tasks related to the national defence plan; the development, organisation, equipping, and command and control

[789] http://www.slovenskavojska.si/

of the Slovenian Armed Forces; preparation of civil defence; administrative communications and cryptographic protection within the defence system; military schools; organisation, preparation and implementation of the system for civil protection and disaster relief, and the rights and duties of citizens with respect to defence, civil protection and disaster relief[790].

The General Staff of the Slovenian Armed Forces (SAF)

The SAF is the highest professional military body in Slovenia, performing professional military tasks related to the activities and development of the Slovenian Armed Forces in peace and in war. It commands and controls the Slovenian Armed Forces at the strategic level. Under its authority are the commands of the Armed Forces, military units, and institutes linked to the General Staff.

Uprava za zaščito in reševanje (Administration for Civil Protection and Disaster Relief – ACPDR)[791]

Administration of the Republic of Slovenia for Civil Protection and Disaster Relief (ACPDR) is a constituent body of the Ministry of Defence. It performs administrative and professional protection, rescue and relief tasks as well as other tasks contributing to protection against natural and other disasters. The ACPDR is divided into six internal organisational units (four sectors and two services) based in Ljubljana as well as 13 other ACPDR branches operating throughout Slovenia. Within each branch there is a regional notification centre that performs a 24-hour service. Altogether, 300 people are employed at ACPDR branches and notification centres.

The disaster management system is one of the three pillars of the Slovenian national-security system, and it encompasses protection, rescue and relief activities. The aim of the system is to reduce the number of disasters and to reduce the number of casualties and other consequences of such disasters. Due to Slovenia's geographic characteristics, natural disasters, especially floods, summer storms, fires and earthquakes, are common. The risk posed by environmental disasters is increasing due to urbanisation and industrialisation; however contemporary threats of terrorism and the occurrence of contagious diseases also pose significant risk.[792].

Ministrstvo za notranje zadeve* (*Ministry of Interior)[793]

The mission of the Ministry is to provide the highest possible level of security in the state through the preventive, rather than repressive, action of law enforcement agencies. The Ministry is responsible for public security and police, internal administrative affairs and migrations. The Ministry of the Interior, together with the Police and Internal Affairs Inspectorate as autonomous bodies within its framework, performs tasks defined by law in the following fields of activity:

- internal administrative affairs;
- tasks in the field of migration and integration;
- police and security, and

[790] http://www.vlada.si/en/about_the_government/who_is_who/ministries/ministry_of_defence/
[791] http://www.sos112.si/eng/index.php
[792] http://www.sos112.si/eng/clanek.php?catid=27
[793] http://www.inz.gov.si/en/

- the Inspectorate for Interior Affairs[794]

The Ministry is also responsible for the coordination of European affairs and international cooperation in the field of security.

The Internal Affairs Inspectorate is a body within the Ministry of the Interior, and performs tasks in the following areas:

- Overseeing the implementation of the regulations for the private protection and detective industry.
- Overseeing the implementation of regulations for weapons and ammunition.
- Overseeing the implementation of regulations governing the roadworthiness of motor vehicles.
- Overseeing the implementation of regulations for the public service.
- Administrative inspection[795]

Ministrstvo za Finance (Ministry of Finance)[796]
In accordance with the State Administration Act the Ministry of Finance performs tasks in the areas of the treasury, public accounting, budgets, public contracts, the tax and customs systems, general government revenue and the system of finance, the prevention and detection of money laundering, the regulation of gaming activities, state aid, macroeconomic analyses and forecasts, and international cooperation with foreign financial institutions[797].

Ministrstvo za Gospodarstvo (Ministry of Economy)[798]
The Ministry of the Economy is divided into six directorates covering the internal market, enterprise and competition, foreign economic relations, tourism, and energy and electronic communications. There are also Ministry bodies performing tasks in the areas of intellectual property, consumer protection, protection of competition, economic promotion and promotion of foreign investment, market inspection, inspection of electronic communications and mail, and the energy sector.

- The Energy Directorate manages the energy supply, particularly electricity and natural gas It works to ensure the proper functioning of the energy market, the reliable and economical supply of energy in normal and extraordinary circumstances, and the sustainable development of energy systems. It performs in-depth economic analyses of the energy sector. It works for the development of energy legislation and for the implementation of administrative procedures in the area of energy supply. The directorate assists in managing and privatising state property in state-owned energy sector companies. It also covers energy issues in international relations. The Energy Directorate actively cooperates with the Energy Agency and with non-governmental organisations operating in the energy sector.
- The Electronic Communications Directorate manages legislation and regulation in the area of post, electronic communications, digital signatures and related areas. Development strategies are being prepared to improve the level of competitiveness in the electronic communications markets. Development projects are being managed to

[794] http://www.vlada.si/en/about_the_government/who_is_who/ministries/notranjezadeve/
[795] http://www.vlada.si/en/about_the_government/who_is_who/ministries/notranjezadeve/
[796] http://www.mf.gov.si/slov/index.htm
[797] http://www.vlada.si/en/about_the_government/who_is_who/ministries/finance/
[798] http://www.mg.gov.si/en/

promote the development of e-communication and projects are being implemented with Structural Funds support. Special attention is focused on monitoring European legislation and its transposition into Slovenia's legal order. The Electronic Communications Directorate is responsible for managing the companies Telekom Slovenije and Pošta "the Post Office". It works closely with the Agency for Post and Electronic Communications, which is the independent national regulator for electronic communications and the postal service.799

Ministrstvo za Javno Upravo (Ministry of Public Administration)[800]
The Ministry of Public Administration performs tasks in the following areas:

- the organisation of public administration and staff;
- the public sector salaries system;
- E-government and related administrative processes;
- investments, real estate and joint state administration services, and
- the coordination and guidance of local administrative units.

27.3 Strategy & Policy

The ***Doctrine on Protection, Rescue and Relief***[801] is an important document adopted by the Government of the Republic of Slovenia on 30 May 2002, and is based on Article 93 of Law on Protection against Natural and Other Disasters (RS Official Gazette, no. 64/94, 33/00, and 87/01[802]). The Doctrine provides common principles and professional and operational guidance for the organisation and conduct of protection, rescue and relief efforts in the event of natural and other disasters. The use of common principles provides for a functionally unified and harmonised approach to disaster preparation as well as harmonising and interlinking the operations of those who carry out protection, rescue and relief efforts. The Doctrine takes into account that protection against natural and other disasters is part of the internal security of Slovenia, and that protection and rescue is, organisationally and functionally, an independent and unified subsystem of Slovenia's national security. It includes and integrates all rescue activities, services, and other tasks involved in protection, rescue and relief efforts so that they may make use of common telecommunication and information systems and other infrastructure.

- Article 2 of the Doctrine establishes starting points for planning, organising and conducting protection, rescue and relief. The main sources of dangers and threats are pollution, military threats, terrorism, and other non-military sources of threat.

In the context of the integration of Slovenia into the international economic community, significant population migrations, and the increase of organised crime, security threats such as terrorism and other forms of violence and non-military threats are increasing. Their forms are diverse and more difficult to predict.[803]

[799] http://www.vlada.si/en/about_the_government/who_is_who/ministries/ministry_of_the_economy/
[800] http://www.mju.gov.si/en/
[801] http://www.sos112.si/db/priloga/p4359.pdf
[802] http://odlocitve.us-rs.si/usrs/us-odl.nsf/o/E117D3C348F9C0D7C125717200280B2A
[803] http://www.sos112.si/db/priloga/p4359.pdf

Article 4 establishes the goals and missions of protection, relief and rescue operations. These are to protect people, animals, material and other goods, and the environment against disasters or destruction, damage and other consequences of disasters and to alleviate the consequences. These basic goals is implemented through:

- preventive activities;
- the establishment and maintenance of preparedness for action;
- monitoring, notification and warning systems;
- protection, rescue and disaster relief operations, and
- the alleviation of the aftermath of disasters

Article 6 of the ***Doctrine on Protection, Rescue and Relief*** lays down general rules for intervention strategies for civil protection. Protection, rescue and relief forces are assigned to conduct protection, rescue and relief activities and missions in the event of natural and other disasters. They are organised as units, services and other structures. They are organised by local communities, governments and particular enterprises, institutes and other organisations. Local communities and governments organise them with regard to the level of threat to their area; enterprises, institutes and other organisations do the same in accordance with risks related to the activities which they perform. When organising protection, rescue and relief forces, priority, if possible, is given to volunteer forces. With regard to the integration and cooperation of citizens, these are divided into:

- Volunteer forces which are organised according to the principles of nongovernmental voluntary service, in particular, humanitarian organisations.
- Professional forces which are organised as units or services and conduct their missions on a professional basis, such as public institutes and administrative organisations.
- Compulsory forces which are organised within units, services and bodies of the Civil Protection units and based on citizen responsibilities.

Protection, rescue and relief forces are comprised of rapid reaction forces, general rescue forces and services, special rescue forces and services, and units, services and bodies of Civil Protection. The police and the Slovenian Armed Forces cooperate in conducting protection, rescue and relief efforts.[804]

27.4 Methodologies & Standards

The National Assembly of the Republic of Slovenia, during its session on 3 May 2006 endorsed the officially revised text of the *Act on the Protection against Natural and other Disasters*.[805] This Act regulates the protection of people, animals, property, cultural heritage and environment against natural and other disasters. The state, municipalities and other self-governed local communities are responsible for organising protection against natural and other disasters as part of a unified and integral national system. The protection system comprises the planning, organisation, implementation, supervision, and financing of measures and activities for the protection against natural and other disasters.

[804] http://www.sos112.si/db/priloga/p4359.pdf
[805] http://www.sos112.si/db/priloga/p4360.pdf

National protection and rescue plans are developed by the government, and local community plans by mayors. The body responsible for national plans is the Administration of the Republic of Slovenia for Civil Protection and Disaster Relief, and municipal administrations are responsible for municipal plans. Protection and rescue measures to be deployed in the event of a disaster are laid down in the protection and rescue plans which must be drawn up for each individual type of disaster by state bodies, local communities, public institutions (schools, institutions caring for special groups of people, medical institutions, institutions for the protection of cultural heritage, etc.), and those commercial companies whose activity presents a threat to nearby residents or the environment, and a number of other organisations.[806]

27.5 Public – Private Partnership and International Collaboration

A bilateral agreement has been signed with Austria, for the joint management and protection of the approximately 7 km long Karavanke tunnel which joins Austria and Slovenia[807].

The core purpose of Slovenian international cooperation in the military area is the implementation of activities which support the efforts of the Republic of Slovenia as a partner and full member of NATO and the EU. Since 29 March 2004, when Slovenia joined the North-Atlantic Alliance, the Slovenian Armed Forces have taken an active role in supporting international peace. Their activities also include the participation of the Slovenian Armed Forces in peace support operations and humanitarian activities[808].

27.6 Funding & Human Resources

In Slovenia there is no specific annual budget from public authorities specifically for CIP related programmes, even though there are some research projects related to this topic.

There are some government employees working on CIP issues, but they are not centrally organised, and their activities are sponsored by each Ministry depending on the sector.[809]

27.7 Training & Exercises

Basic theoretical and practical knowledge about natural and other disasters, and means to protect against them are taught during primary school education. During vocational, high school and university education, topics related to protection against natural and other disasters are taught in accordance with the guidelines of individual education programs.

Training for the population in personal and collective protection and implementing obligatory protective measures is organised by local communities and the government, according to security risks. Protection and rescue plans are also used as noncompulsory training forms. Initial measures to be taken for personal and collective protection in the event of disasters are disseminated. The training of a professional protection, rescue and relief cadre is carried out through the regular education system and with various forms of functional education.

[806] http://www.sos112.si/eng/page.php?src=na1.htm
[807] Booz & Company Survey “Stock-taking of Existing Critical Infrastructure Protection Activities”
[808] http://www.slovenskavojska.si/en/international-cooperation/
[809] Booz & Company Survey “Stock-taking of Existing Critical Infrastructure Protection Activities”

Only the training of professional fire-fighters is carried out through a special education program. Training of protection, rescue and relief force members based on programs determined by the minister responsible for protection against natural and other disasters. The training of protection, rescue and relief force members is organised by the individual units, services and other operational structures. It is also undertaken by the *Training Centre for Protection and Relief Efforts of the RS Administration for Protection, Rescue and Relief Efforts*[810], the responsible training organisation and organisations and other non-governmental organisations[811].

The training of protection, rescue and relief force members comprises introductory, basic and supplementary training and exercises. Supplementary forms of training and exercises are usually attended by entire units and other operational structures and their leadership. The purpose of exercises is to examine the training and the readiness of the system of protection against natural and other disasters as a whole or its individual parts and components. The exercises also examine the concept of protection and rescue which has been elaborated in plans. Exercises can be of local or state significance, individual or staff, command, territorial or collective protection or defence protection.

All exercises must be planned carefully. Exercises designed for examining readiness in the event of disasters involving hazardous material are generally conducted every three years, in the event of nuclear disasters every five years and for other major types of disaster every five to ten years[812].

***Izobraževalnega centra za zaščito in reševanje v Republiki Sloveniji (Training Centre for Civil Protection and Disaster Relief of the Republic of Slovenia)*[813]**

The *Training Centre for Civil Protection and Disaster Relief of the Republic of Slovenia* in Ig near Ljubljana provides education and training programs for units, services and individuals of the protection, rescue and relief system. Some of the Centre's fire-fighter training is undertaken at the Centre's training unit, based in Sežana. The Centre is responsible for the development and evaluation of training programs and the preparation of training materials. In addition, it organises training to be undertaken in conjunction with international organisations such as NATO, the UN and the Stability Pact for South Eastern Europe. It provides professional publishing support for the Ujma national magazine, which addresses issues on disaster management.

From 24th till 27th of September, International Exercise on Post-earthquake Damage Assessment was conducted in Ljubljana, Ig and Čezsoča pri Bovcu, within the boundaries of STEP Project - Strategies and Tools for Early Post-Earthquake Assessment[814].

27.8 Sector – Specific Key Players & Initiatives

ENERGY

[810] *www.sos112.si/eng/tdocs/iczr_ang.pps*
[811] http://www.sos112.si/db/priloga/p4359.pdf
[812] http://www.sos112.si/db/priloga/p4359.pdf
[813] http://www.sos112.si/eng/page.php?src=iz1.htm
[814] http://www.sos112.si/eng/clanek.php?catid=2&id=2649

Public authorities:

- ***Agency for Energy***[815]
  The Energy Agency has been operating since 2001. It was established with the aim of helping to create suitable conditions for the opening of the market for electricity and natural gas in the Republic of Slovenia, and to control these significant changes. As of 1 July 2007 both markets have been fully opened. As a national regulatory body, the Energy Agency has the double aims of working towards Slovenia's national interests, while at the same time contributing to the development of the common European energy market[816].

NUCLEAR INDUSTRY

Public authorities:

- ***Slovenian Radiation Protection Administration***[817]

  The Slovenian Radiation Protection Administration (SRPA) performs tasks in the fields of radiation protection, including the safe use of radiation sources in medicine and veterinary care, radiation protection of the general population, the inspection of living and working environments, monitoring of food and drinking water, the control of harmful health effects due to exposure to non-ionising radiation, and the authorisation of approved radiation protection experts.

- ***Slovenian Nuclear Safety Administration (SNSA)***[818]

  The Slovenian Nuclear Safety Administration's (SNSA) include the regulation of:
  – Nuclear and radiological safety of nuclear facilities, nuclear trade, the transport and handling of nuclear and radioactive materials, the accountability and control of nuclear materials
  – Physical protection of nuclear facilities and nuclear materials
  – The professional qualifications of personnel operating in nuclear facilities and their training.
  – Quality assurance in the nuclear field.
  – Radiological monitoring of the environment.
  – Early notification in the event of a nuclear or radiological accident.
  – International co-operation in nuclear issues.

Initiatives:

The Slovenian early warning network (MZO)[819] is an automatic system to detect and warn of elevated radiation levels in the environment, established at the beginning of the last decade. The system is designed for immediate detection of raised levels of radiation and is one of the key elements of the response to an emergency. When radioactive release occurs, the levels of external radiation and concentrations of radioactive particles in the air are higher, since the air, ground, drinking water, food and fodder may be contaminated by the fallout. The warning systems are managed by the SNSA, the Krško NPP, the EARS and each of the Slovenian

[815] http://www.agen-rs.si/en/
[816] http://www.agen-rs.si/en/informacija.asp?id_meta_type=27&id_informacija=634
[817] http://www.uvps.gov.si/en/
[818] http://www.ursjv.gov.si/en/
[819] http://www.ursjv.gov.si/en/monitoring/mzo/

thermal power plants. The SNSA collects, analyses and archives data which is also presented on-line on the SNSA web pages.

In the year 2007 there were no high radioactivity events. On June 4, 2008, the European Commission set off an EU wide alarm through the European Community Urgent Radiological Information Exchange (ECURIE). The power plant was safely shut down to a secure mode after a small leak in the cooling circuit. The leak was immediately located and treated. According to the SNSA, no radioactive release into the environment occurred and none is expected. The event did not affect employees, the nearby population or the environment. According to nuclear expertise groups, national entities within the European Union, such as the ASN in France, this incident was wrongly reported to ECURIE. ECURIE, when receiving a notification, has an obligation to forward it to all parties. In this particular situation, the notification turned out to be a false alarm. These type of incidents (a small leakage on primary pumps) are not a rare occurrence in nuclear power plants, but an incorrect form was used to report this incident to the other states in Europe.

ROKO (the name derives from the Slovenian for Radioactivity in the Environment)[820] is a database which contains measurements of radioactivity in the Republic of Slovenia. The program monitors levels of radioactivity in the environment as a consequence of global contamination due to nuclear bomb tests and the Chernobyl acciden. In addition to the data on levels of radioactive contamination of the environment, the SNSA has also gathered data from the Krško NPP, the ŽirovskiVrh Mine, the Low and Intermediate Level Waste Depository and the Reactor Centre at Brinje.

INFORMATION AND COMMUNICATION TECHNOLOGIES
Public authorities:

- ***Post and Electronic Communications Agency[821]***

  This Agency is a professionally, politically, and financially independent national regulatory agency for media. It was established in 2001 as the Telecommunications, Broadcasting, and Post Agency of the Republic of Slovenia (ATRP). It was renamed the Post and Electronic Communications Agency of the Republic of Slovenia in 2004. Its mission is to regulate the electronic communications and postal market to ensure competitiveness and to provide high-quality, modern and affordable services and radio and television programmes in the Slovenia. The Agency aims to ensure equality for operators of communication networks, service providers and providers of postal services. It also manages the radio frequency spectrum and number range, monitors the content of radio and television programmes and protects the rights of users in both the Republic of Slovenia and the European Union. The Agency's objective is to offer user-oriented services, a regulated and standardised European market, equal rights to those of other citizens of the European Union, and variety in the cultural, linguistic and programme content of radio and television programmes.
- ***RadiotelevizijaSlovenija[822]***

  RadiotelevizijaSlovenija or RTV Slovenija is the national public broadcasting organisation of Slovenia. It is the only network in Slovenia with both radio and television stations.

[820] http://www.ursjv.gov.si/en/monitoring/radioactivity_in_the_environment/
[821] http://www.apek.si/
[822] http://www.rtvslo.s

Initiatives:

A uniform autonomous system of radio communications (ZARE) is used during protection, rescue and relief operations in Slovenia. The Administration of the Republic of Slovenia for Civil Protection and Disaster Relief manages its technical aspects and ensures the disturbance-free operation of the system. The system is used by all rescue services in the country. The system's communication centres are located in regional notification centres, where radio traffic is managed and used to connect users to public and functional telecommunications systems. The ZARE system guarantees 95% coverage of the territory by radio signal from a stationary network, and complete territorial coverage by means of mobile repeaters. The ZARE communications system is the largest single professional system of radio links in the country. Its network consists of 40 repeaters of the high network and 56 digital base stations of the lower network. In terms of its functions, the system is divided into a sub-system of radio links and of personal calls. The radio link sub-system allows for direct and indirect radio links to be established between users of radio stations and direct links with regional notification centres. The personal call sub-system enables the transmission of short, 245-character-long texts to users of personal call receivers. The system is designed to work in both ordinary and emergency circumstances. The collapse of an individual part of the system cannot bring the whole system down. The system administrator guarantees the immediate repair or replacement of defective system parts and, in emergencies, may also strengthen the radio network with mobile repeaters in areas where there is an immediate need. The personal identification of radio station users is regulated by means of a uniform radio directory. Regional notification centres may also send messages to the holders of personal call receivers inside the home region, while the National Notification Centre can do so across the entire territory of the state[823].

WATER

Public authorities:

- ***Health Inspectorate of the Republic of Slovenia[824]***

  The Health Inspectorate of the Republic of Slovenia (HIRS) is a constituent body of the Ministry of Health[825]. HIRS is an enforcement body which monitors the implementation of laws and other regulations governing communicable diseases, wholesomeness and safety of food, drinking water, mineral waters, food packaging articles and materials, alcohol consumption, cosmetic products, toys, tobacco products, bathing waters, health and hygiene. It also oversees safety in the fields of health care, child care, schooling, education, hygiene care, social care and general product safety, exclusive of chemicals, medicinal products and sources of radiation.

- ***Ministrstvo za Okolje in Prostor (Ministry of Environment and Spatial Planning)[826]***

[823] http://www.sos112.si/eng/page.php?src=pr12.htm
[824] http://www.zi.gov.si/en/
[825] http://www.mz.gov.si/
[826] http://www.mop.gov.si/en/

The Ministry of Environment and Spatial Planning is responsible for water resources, water quality, and the sustainable management of surface, underground and seawater. The Ministry ensures that development in Slovenia is undertaken in such a way as to minimise the impact of natural disasters. It also establishes solidarity mechanisms for natural disaster relief. It ensures that environmental costs are included in the economic costs of business and the national economy. The key strategically important long-term environmental protection directions and goals of the Ministry are aimed at preventing or mitigating adverse impacts presenting a threat to sustainable development. The *Environmental Protection Act* [827] is the regulatory framework for the environment in Slovenia. Moreover, the Resolution on the National Environmental Protection Programme discusses climate change, nature and biodiversity, quality of life, and waste and industrial pollution.[828]

- ***The Environmental Agency***[829]

The Environmental Agency is an agency of Ministry of Environment and Spatial Planning and performs expert, analytical, regulatory and administrative tasks in the area of the environment at the national level. Its mission is to monitor, analyse and predict natural phenomena and processes in the environment, and to reduce the danger to people and their property from them. Their range of duties in this area includes the national services for meteorology, hydrology and seismology. The Agency also monitors environmental pollution and ensures the quality of public environmental data. To this end, it operates a measurements network and laboratories. The Agency contributes to the minimisation of environmental problems by implementing environmental legislation. It fulfils the administrative procedures with those liable to pay environmental contributions: water rates, water burden taxes, taxes for burdening the air with carbon dioxide emissions, and taxes for burdening the environment through waste disposal.

FOOD

Public authorities:

- ***Health Inspectorate of the Republic of Slovenia***[830]

The Health Inspectorate operates as the national contact point within the EU Rapid Alert System for Food and Feed (RASFF).[831]

- ***Agency for Agricultural Markets and Rural Developments***[832]

Among the different tasks of the Agency is the responsibility to coordinate relief efforts for agricultural natural disasters.

- ***The Inspectorate for Agricultural, Forestry and Food***[833]

The inspectorate supervises the implementation of acts and regulations on agriculture, the quality and labelling of agricultural products and food, the quality of

[827] http://odlocitve.us-rs.si/usrs/us-odl.nsf/o/EDDF8F5A8A2D6706C125720A00325AAB
[828] http://www.mop.gov.si/en/areas_of_work/
[829] http://www.arso.gov.si/en/
[830] http://www.zi.gov.si/en/
[831] http://ec.europa.eu/food/food/rapidalert/index_en.htm
[832] www.arsktrp.gov.si/en
[833] http://www.mkgp.gov.si/en/bodies_of_the_ministry/inspectorate_of_the_republic_of_slovenia_for_agriculture_forestry_and_food/

mineral fertilisers, plant protection products, seeds, propagating material, plant health, animal feed, wine, and the safety, organisation and exploitation of agricultural land, financing, and other matters relating to arable farming[834].

Phitosanitary Administration of the Republic of Slovenia – PARS[835]

PARS performs administrative, professional and development tasks in the fields of the protection of plants, plant products and of regulated articles from harmful organisms; the protection and registration of varieties of plants (property rights); the production, processing and marketing of agricultural seed and propagating material; conservation of agricultural plant genetic resources; the registration, marketing and use of plant protection products; the technical requirements for the equipment for the application of plant protection products; the quality of mineral fertilisers; the professional training of the relevant persons; and information dissemination to the public.

Veterinary Administration of the Republic of Slovenia[836]

The Veterinary Administration (VARS) carries out the administrative tasks, and inspection and control activities in the veterinary sector. The most important administrative tasks include:

- providing for the implementation of and organising the monitoring of residues in foodstuffs, animals, animal products and in animal feed;
- preparing risk assessments for risks posed to public and animal health and effects on the environment,
- organising and managing actions to prevent, suppress and eradicate animal diseases and zoonoses;
- carrying out preparations for the defence, protection and operation of veterinary services in time of war, or other catastrophes and emergencies;
- carrying out the training of veterinary first aid units and civil defence units;
- monitoring programmes,
- harmonising work and defining measures for the implementation of programmes of control and the prevention of the spread of certain animal diseases and epidemics;
- monitoring and reporting on the movement of certain animal diseases in the RS and abroad.[837]

Initiatives:

The planning of Ministry of Health activities in the area of prevention and health improvement understands that health is something of value both to individuals and to society as a whole, and is a precondition for the successful economic and social development of the country. In the field of food safety, the Ministry proposed a national policy in the Slovenian Food and Nutrition Action Plan 2005 - 2010[838].[839]

[834] http://www.vlada.si/en/about_the_government/who_is_who/ministries/ministry_of_agriculture_forestry_and_food/

[835] http://www.furs.si/en/index.asp

[836] http://www.vurs.gov.si/en/

[837] http://www.vlada.si/en/about_the_government/who_is_who/ministries/ministry_of_agriculture_forestry_and_food/

[838] http://www.mz.gov.si/fileadmin/mz.gov.si/pageuploads/mz_dokumenti/delovna_podrocja/javno_zdravje/national_programme_of_food_and_nutrition.pdf

[839] http://www.mz.gov.si/

HEALTH

Public authorities:

- ***Ministrstvo za Zdravje – MZ – (The Ministry of Health)***[840]

  The Ministry of Health deals with matters relating to healthcare and health insurance. These include: healthcare activities at the primary, secondary and tertiary levels, monitoring of the nation's state of health and the preparation and implementation of health improvement programmes; economic relations in healthcare and tasks relating to the founding of public healthcare institutions in line with the law; health measures to be taken in the event of natural and other disasters; protection of the population against addiction-related health problems; protection of the population against infectious diseases and HIV infection; food safety and the nutritional quality and hygiene of food and drinking water with a view to preventing chemical, biological and radiological pollution and conducting a general policy on nutrition; the production of, trade in and supply of medicines and medical products; the production of and trade in poisonous substances and drugs; the safety of products intended for general use; health and ecological issues relating to the environment, where a direct impact on human beings is involved; problems related to drinking water, bathing waters, air, soil and vibrations; waste management from the health protection aspect; protection against ionising and non-ionising radiation in residential and work environments; conditions relating to the removal and transplantation of human organs; the formulation and implementation of international agreements on social security.

- ***The Health Inspectorate***[841]

  As for water, the Health Inspectorate has a role in the inspection and supervision of food safety.

Initiatives:

Health care is a public service provided through the public health service network. This network also includes, on an equal basis, other institutions, private physicians and other private service providers. With relatively limited public funds available for this purpose, the level of health care in Slovenia is comparable with the level of health care in the advanced countries of Europe. Primary health care services are organised locally, such that they are equally accessible to all people without discrimination. Everyone must be assured continuously accessible urgent medical attention and emergency services. In Slovenia the system of health insurance is divided into compulsory health insurance, voluntary health insurance for additional coverage, and insurance for services that are not a constituent part of compulsory insurance. Compulsory health insurance is mandatory for all citizens with permanent residence in Slovenia. Compulsory insurance does not, however, ensure the coverage of all costs that arise in treatment. Complete coverage of costs is provided only for children, school children and for certain illnesses and conditions.

[840] http://www.mz.gov.si/en/
[841] http://www.zi.gov.si/en/

FINANCIAL

Public authorities:

- ***Bank of Slovenia***[842]

  The Bank of Slovenia is the central bank of the Republic of Slovenia. It was established on 25 June 1991 by the adoption of the Bank of Slovenia Act (BoSA).It is a legal entity governed by public law. The Bank of Slovenia and the members of its decision-making bodies are independent and, pursuant to the BoSA, are not bound to any decisions, positions or instructions of the state agencies or any other bodies. Since the introduction of the Euro in 2007 the Bank of Slovenia, in carrying out its tasks, fully abides by the provisions of the ESCB[843] and ECB[844] Statutes. As a member of the ESCB, in line with the Treaty establishing the European Community and the two statutes just mentioned, the Bank of Slovenia carries out the following tasks:

  – implementation of the common monetary policy
  – co-management of the official foreign reserves of the Member States in accordance with the treaty on establishing the European Community, and
  – facilitation of the smooth operation of the payment system.

- ***Ministry of Finance***[845]

  The Ministry of Finance manages the budget and state finances, monetary funds and national debts, and has a regulatory role in the financial system. In accordance with the Organisation and Competence of Ministries Act, it is charged with tasks in the following areas: the monetary, banking and foreign exchange systems; financial relationships with foreign countries; the system of taxes, contributions, duties, customs duties and other types of public income; the systems of insurance, securities, funds and other financial organisations; the system of gaming activities; the public expenditure system and the budget, including public procurement and the system of accountancy, auditing and financial operation, as well as joint tasks of the country's administrative bodies and governmental services in conducting financial and accountancy services.

TRANSPORT

Public authorities:

- ***Ministry of Transport***[846]

  The Ministry of Transport performs tasks in the field of rail, air, maritime and inland waterway and road transport (with the exception of road transport safety control), as well as tasks in the field of transport infrastructure and cableway installations. The Ministry is structured into offices that include the Transport Directorate, International Affairs Directorate, Roads Directorate, Railways and

[842] http://www.bsi.si
[843] http://www.ecb.int/ecb/orga/escb/html/index.en.html
[844] http://www.ecb.int/
[845] http://www.mf.gov.si/angl/predstavitev/del_podr.htm
[846] http://www.mzp.gov.si/

Cableways Directorate, Civil Aviation Directorate, Maritime Directorate. Bodies under the responsibility of the Ministry perform operational tasks, whereas Inspectorates carry out control tasks.

- ***The Maritime Administration***[847]
  An element of the Ministry of Transport responsible for the development of port infrastructure owned by the RS and the management of the radio watch services. The Maritime Administration performs administrative and professional tasks in the area of maritime transport, port securit, navigation safety, the operation of maritime transport and the maintenance of structures for safe navigation and navigation channels. It oversees the implementation of regulations in the area of maritime transport and port infrastructure, and the implementation of regulations governing inland navigation.
- ***Slovenian Roads Agency*** [848]

  The Slovenian Roads Agency is an element of the Ministry of Transport that performs expert, technical, organisational and developmental tasks relating to: the construction, maintenance and care for public roads; control of the state of the roads; cargo and passenger road transport; the keeping of records on public roads and traffic levels, and management duties concerning safety measures for public roads and the traffic on them.
- ***Agency for the Management of Public Railway Infrastructure Investment*** [849]

  An agency of the Ministry of Transport responsible for the organisation, handling, and management of investments in public rail infrastructure. In addition, it revises project documentation, and concludes public service contracts on railway services, the management of the public railway infrastructure, and the management of railway stations, and supervises both the implementation thereof and the manager's other tasks.
- ***DARS, Motorway Company***[850]

  DARS d.d. is in charge of financial engineering, preparing, organising and managing construction and maintenance of the motorway network, and is responsible for the management of motorways in the Republic of Slovenia.

CHEMICAL INDUSTRY

Public authorities:

- ***Chemicals Office of the Republic of Slovenia***[851]

  The Chemicals Office of the Republic of Slovenia (CORS) is a body within the Ministry of Health operating under the Chemicals Act, the Biocidal Products Act, the Act of Strategic Goods of Special Significance for Safety and Health, Illicit Drug Prevention Act, and the Cosmetic Products Act. The Chemicals Office is responsible for performing tasks pertaining to: trade in chemicals and biocidal

[847] http://www.up.gov.si/en
[848] http://www.dc.gov.si/en/
[849] http://www.dzi.si/index.php?option=com_content&view=category&layout=blog&id=20&Itemid=29
[850] http://www.dars.si/
[851] http://www.uk.gov.si/en/

products, measures aimed at human health and environment protection against harmful effects of chemicals and biocidal products, participation in registration procedures of plant protection products, production, trade and use of substances that could be precursors for manufacturing illicit drugs with the aim of preventing their abuse and use for illicit purposes, obligations, bans and limitations pertaining to products of strategic significance for safety and health, requirements to be met by cosmetic products, drafting and implementing of the National Programme for Safe Chemicals Management[852],cooperation with international organisations and participation in international projects cooperation with other competent authorities in Slovenia and abroad, conducting education in relation to chemical safety, monitoring of trade and use of chemicals, biocidal products and monitoring their degradation products and traces in the environment and living organisms, monitoring progress in science and technology related to impacts and hazards on human health and environment related risk factors, interministerial coordination and the Committee for Safe Chemicals Management[853],information support for chemicals, and carrying out inspections.

SPACE

Public authorities:

- ***Ministry of Higher Education, Science and Technology[854]***

  The Ministry of Higher Education, Science and Technology performs tasks in the field of higher education, research, technology, metrology and promotion of the information society in the areas not covered by other ministries. The ministry also co-ordinates work in the field of the information society.

RESEARCH FACILITIES

Public authorities:

- ***Ministry of Higher Education, Science and Technology[855]***

The Ministry of Higher Education, Science and Technology performs tasks in the field of professional higher and university education, and research by means of the Directorate for Science and Higher Education. For implementation of these tasks, the Directorate is divided to the Department for Science, and the Department for Higher Education. The Department for Higher Education performs tasks enabling planning, directing and financing of higher education activities, residential facilities for students and higher education libraries. The Department for Science provides advice on government research policy. It drafts laws and implements regulations on research activities. It manages a system of comprehensive analysis and monitoring of research, develops new tools for attaining research policy goals, and plans the financing of research activities.

852 http://www.kemijskovaren.si/program/kazalo.htm
853 http://www.kemijskovaren.si/
854 http://www.mvzt.gov.si/
855 http://www.mvzt.gov.si/

***Initiatives*:**

Slovenia has undertakan a cross-sector research project on CIP titled Project "Definition and protection of the critical infrastructure in Republic Slovenia".[856] The project includes the conceptualisation of critical infrastructure, the analysis of CIP in other countries, cross-sector synthesis, and the development of recommendations for improving mechanisms in the field of CIP. Sectors included in the project include electricity, oil, gas, nuclear energy, ICT, transportation, health, food, and the financial system. The Faculty of Social Science, University of Ljubljana, respective ministries and other institutions are involved[857]

[856] Booz & Company Survey "Stock-taking of Existing Critical Infrastructure Protection Activities"
[857] www.fdv.uni-lj.si

28 Spain

Figure 102: Spain

28.1 Summary

	Organisational Model	Strategy & Policy	Methodology & Standards	Public-Private Partnership & International Collaboration	Funding & Human Resources	Training & Exercises	Sector-Specific Key Players & Initiatives
Spain	▪ CIP National Centre ▪ Assistance organized through the Directorate General for Civil Protection	▪ Structured approach to tackle CIP issues	▪ Creation of a National Plan for CIP	▪ Based on bilateral relations (with France, Portugal, South-American Countries) ▪ Participation to CNPIC	▪ Over 100 public employees dedicated to CIP ▪ Funding from Ministries and EU	▪ Escuela Nacional de Protección Civil forms experts in security and emergency	▪ CCN-Cert becoming the National Alert Centre ▪ University of Alcalà de Henares involved in CIP-related research

Spain is dealing with CIP using a structured approach. Established in November 2007, the National Centre for Critical Infrastructure Protection Centre provides 24 hour-a-day monitoring of more than 3,500 security-sensitive facilities such as roads, power or water supply and food, included in the Strategic Infrastructure Catalogue of. The new Centre is part of the common security policy of the European Union, which provides emergency plans in all EU countries.

Spain is actively involved in designing its national security strategy and critical infrastructure protection strategy.

In 2003 Spain reviewed its National Security strategy producing the white paper Strategic Defence Review[858], [859].

This document is the result of the development process of the “STRATEGIC DEFENCE REVIEW”, directed by the Secretariat General for Defence Policy. In particular the document describes “The Context of the Strategic Review” and the “National Security Interests”. The Context of the Strategic Review includes a specific examination of strategic and military innovations, changes in present-day values, and the new reality of globalisation; all of which affect the evolution of our country in a timeframe that extends through the year 2015. The “National Security Interests” describes each of these interests both within and outside Spanish borders, while also analysing other traditional elements of strategic conception, such as risks and theatres of action.

[858] http://www.mde.es/descarga/RED_Ingles_vol_1.pdf
[859] http://www.mde.es/descarga/RED_Ingles_vol_2.pdf

28.2 Organisational model

Ministerio del Interior[860] (Ministry of the Interior)

The Ministry of the Interior is the supreme authority in civil protection matters and is responsible for intervening in cases of catastrophe and for drawing up plans of intervention. The Ministry of Interior is divided into two branches: the General Direction of the Police and the Civil Guard (both conduct investigations nationwide; the National Police Force are responsible for identity documents, control on foreigners and public security; the Civil Guard patrols rural areas, borders, the coast and highways) and the General Direction of Civil Protection and Emergencies.

Centro Nacional de Protección de Infraestructuras Críticas, CNPIC (The National Centre for Protection of Critical Infrastructures)[861]

This Centre reports to the State Secretariat for Security (SES, within the Ministry of the Interior - Ministerio del Interior). This unit was founded in November 2007 and has eleven full-time staff. Five experts deal with physical security, and one expert addresses IT-security, resilience and the dependability of public e-communication networks. The creation of the CNPIC is related to European Union initiatives. The agency is responsible for leading, coordinating and supervising the protection of the national critical infrastructure. Moreover, the State Secretariat for Security is responsible for the application of the *National Plan for the Protection of the Critical Infrastructures*, the coordination of Spain's policies with the requirements of the EU, and the drawing up of consistent best practice procedures. More specifically, the tasks of CNPIC include[862]:

- The maintenance and updating of the national security plan for critical infrastructure and of the Strategic Infrastructure Catalogue.
- The collection, integration, evaluation and analysis of relevant information provided by public institutions, police forces and relevant actors related to strategic sectors.
- Threat assessment and risks analysis of strategic infrastructure.
- The design and establishment of information, communication, and alert mechanisms.
- The coordination with the respective programs of the EU.

Dirección General de Protección Civil y Emergencias[863]
(General Direction for Civil Protection)

The General Direction for Civil Protection and Emergencies, part of the Ministry of the Interior, is the national body responsible for developing national the emergency intervention programs. The Spanish system is based on preliminary planning and cooperation between agencies who maintain emergency management resources. One of its characteristic features is the use of existing resources and not those allocated specifically to civil protection. The system seeks early agreement between all relevant participants and those who have

[860] http://www.mir.es/
[861] ENISA – Stock taking eCommunications Resilience - 2008
[862] ETH Zurich – CIIP Handbook 2008
[863] http://www.proteccioncivil.org

resources at their disposal. The system is decentralised and allows the nationwide distribution of resources to cope with an emergency. It is through the Directorate-General for Civil Protection that requests for international assistance or the intervention of Spanish assistance outside Spanish borders are organised.

Ministerio de Industria, Turismo y Comercio[864]
(Ministry of Industry, Tourism and Trade)

The department within the Spanish general administration responsible for proposing and carrying out government policy in the areas of industrial development and innovation, trade policy, small and medium sized enterprises, energy and mining, tourism, telecommunications, audiovisual media and the development of the Information Society.

Guardia Civil[865] ***(The Spanish Civil Guard)***

An armed service of a military nature that is part of the Security Forces of the State. As a law enforcement agency, the Constitution provides it a primary mission of protecting the free exercise of the rights and freedoms of Spaniards and ensuring public safety. The Spanish Civil Guard has a dual dependence. It is responsive to the Ministry of the Interior in services, salaries, assignments and resources, and to Defence for promotions and military missions.

Cuerpo Nacional de Policía (National Police Force)

An armed force of a civil nature that is part of the Security Forces of the State. It depends from the judicial authorities. It has five branches: judiciary police, intelligence, scientific police, public order and documentation and foreigners.

28.3 Strategy & Policy

Spain is actively involved in designing its national security and critical infrastructure protection strategies. The CIP strategy seeks to tackle the protection of critical infrastructures in a structured way, and includes the creation of a National Centre for Critical Infrastructure Protection.

The main national instruments for national defence, civil protection, and welfare are the following:

National Defence Directive 1/2004[866]

The legislation concerning civil protection[867]***, includes:***

- Royal decree No. 1547 dated 24 July 1980 concerning the reorganisation of civil protection
- Royal decree No. 692 dated 27 March 1981 concerning coordination of the assistance required to repair damage or to relieve the areas affected by an emergency or natural disaster.

[864] http://www.mityc.es/
[865] http://www.guardiacivil.org/quesomos/index.jsp
[866] http://www.mde.es/descarga/ddn_2004_en.pdf
[867] http:// www.icdo.org/pdf/struc/spain-en.pdf and http://www.proteccioncivil.org

- Ordinances dated 2 November 1981, 30 November 1984 and 23 October 1985, as well as Royal decree No. 881 dated 5 March 1982, concerning the response to a road or rail accident involving dangerous substances
- Ordinance dated 17 June 1982 for the basic plan to fight forest fires; Law No. 2 dated 21 January 1985 defining the functions and general organisation of civil protection
- Royal decree No. 1378 dated 1 August 1985 concerning the resources to be provided for managing serious risks, disasters or public calamities.
- Royal decree No. 888 dated 21 March 1986 setting out the composition, organisation and functioning of the National Commission for Civil protection.
- Royal decree No. 886 dated 15 July 1988 concerning the prevention of major accidents in certain industrial activities.
- Royal decree No. 952 dated 29 June 1990 amending and complementing the arrangements concerning the prevention of major accidents in certain industrial activities.
- Royal decree dated 26 October 1990 establishing the Special Committee of the International Decade for Reducing Natural Disasters.
- Resolution of the Council of Ministers dated 30 January 1991 approving the basic standards for developing special plans for the chemical sector in a harmonised manner.
- Royal decree No. 407 dated 24 April 1992 approving the Basic Standards of Civil protection.
- Statement made at the Global Platform for Disaster Risk Reduction (2007)[868] - Spain (Intervención de la Delegación Española en la Primera Reunión de la Plataforma Global para la Reducción de Desastres): A statement made by Mr. Juan Pedro Lahore, Representative of the Spanish Committee for Disaster Reduction, Conseiller Technique, Civil Protection, Ministry of Interior and Representative of the Spanish Committee for Disaster Reduction, Spain, in the first session of the Global Platform for Disaster Risk Reduction, June 2007

The aim of the ***National Defence Directive*** is to establish the guidelines for the Spanish defence policy and its development, with the objective of ensuring the defence of the homeland, the security of the Spanish people, and promoting international peace, security and stability.

The ***Civil Protection*** mission is adapting and improving disaster reduction programs to lessen the risks of natural and technological catastrophes:

- Identification and establishment of special maps of dangerous zones, and evaluation of the vulnerability of buildings and other constructions.
- Training courses for the staff of the intervention services and programs of public education and awareness
- Developing appropriate systems for emergency interventions, coordination of alerting networks and aid in case of emergency.

[868] http://www.preventionweb.net/files/2266_SpainStatementGP07.pdf

- Organisation and control of a transmission network for use in emergencies
- Development of disaster plans in order to ensure a state of readiness for sure and swift intervention, designate command arrangements for emergency services to avoid improvisation and confusion, and ensure concerted action by all existing intervention services.
- Aftermath programs of recovery and resilience.
- Statutory provisions facilitating the planning of efficient operations.

28.4 Methodology & Standards

Plan Nacional para la Protección de Infraestructuras Críticas

This plan has been developed by the Secretariat of State for Security, at the Ministry of the Interior. The general objective of the Plan is establishing the criteria and guidelines needed to mobilise Spain's operational capabilities and articulating the integrated measures and responses needed for the permanent and homogeneous protection of the nation's strategic infrastructure system against both generic and specific threats[869]

This is achieved by the following four activities:

Establishing programmes and articulating sectoral and territorial prevention and protection measures in order to provide adequate security for strategic infrastructure, especially against terror and criminal attacks.

Articulating actions which will minimise risks and the damage following crisis situations, and cooperating to adequately manage these.

Cooperation in the development of appropriate mechanisms in order to swiftly recover the infrastructure.

Establishing permanent coordination mechanisms with infrastructure operators and their respective security and emergency plans

National Defence Directive 1/2004[870]

The aim of this Directive is to establish the guidelines for defence policy and for its development, with the objective of ensuring the defence of the Spanish homeland, contributing to the security of the Spanish people, and promoting international peace, security and stability.

Spanish defence policy includes the following priorities and observations:

1. The strengthening of the role of the Armed Forces is a relevant factor in the external actions of the Spanish State.
2. The dynamic and constant reform of the Armed Forces so as to adapt them to the circumstances and needs arising from the strategic situation existing at any given time.

[869] Booz & Company survey "Stock-taking of Existing Critical Infrastructure Protection Activities"
[870] http://www.mde.es/descarga/ddn_2004_en.pdf

3. The implementation, in concert with our partners and allies, of our commitments in the area of shared security and collective defence.
4. Firm and resolute support for an effective multilateral system as a means of resolving conflicts, with full respect for the resolutions of the United Nations Security Council
5. The active participation of Parliament in the discussion of major issues of defence policy and the seeking of parliamentary support for government decisions regarding the involvement of Spanish Armed Forces in operations abroad

Civil Protection operating plans

The Basic Standard[871][872] lays down the requirements for civil protection plans. It sets out the criteria for coordination between the plans of various administrations and the general framework for developing the competencies of these administrations. Cooperation between the three administrations (central, autonomous, local) made it possible to develop standards derived from the Basic Standard. It is primarily within the framework of the National Commission on Civil Protection that this cooperation has developed.

Each administration can organise and manage its civil protection systems with complete autonomy but must respect the principles of inter-territorial complementarity, subsidiarity and solidarity. The first two principles mean that the local administration is responsible (in principle) for coping with an emergency. The autonomous community level takes over if the local administration is unable to cope with the problem. The central level plays a similar role for the autonomous communities. The principle of inter-territorial solidarity ensures that the resources available outside the territory where the emergency happens can be used, and this is the case with the intervention of resources available in the autonomous community plan outside the local territory, and intervention with resources provided for in the State plan for resources outside the territory of the autonomous community. In case of a national emergency, the national government may assume the general direction of relief operations. National emergencies are:

- Situations in which it is necessary to declare a state of alarm, of emergency or of siege, in agreement with the Basic Law of 1981, to ensure the security of persons and of goods.
- Situations in which the coordination of several administrations must be taken into account, or when the disaster extends beyond one single autonomous community, or which require the mobilisation of resources beyond the community level.
- Finally, situations which, by their actual or forecast size, require national direction of the affected public administrations

The Basic Standard establishes two types of plan: the territorial plan and the special plan. The first, intended to cope with general cases, can be a guideline plan which defines the general framework for allowing access to territorial plans at a local level. The special plan involves the implementation of methodologies and technical and scientific resources specific to each type of risk. This plan can relate to:

- Nuclear incidents

[871] Resolution of the Council of Ministers dated 30 January 1991 approving the basic standards for setting up special plans for the chemical sector in a harmonized way
[872] *Royal* decree No. 407 dated 24 April 1992 approving the basic standards of civil protection.

- Situations of war
- Floods
- Seismic activity
- Chemicals
- Transport of dangerous substances
- Forest fires
- Volcanic activity

The first two are of national interest but the other administrations can be involved, both at the resource level (sanitary installations, logistics, et cetera) and at the planning level (municipal emergency plans in the event of a nuclear accident). The national government being responsible for the coordination and direction of civil protection, approves the Basic Plans and specific plans of national interest as well as the Basic Guidelines, after these have been examined by the National Commission for Civil protection. The autonomous communities, on the other hand, approve those territorial and specific plans related to their own territories.

Riesgos y Catástrofes: Actitudes y conductas en la sociedad española (Risk and Disaster: Attitudes and Behaviours in Spanish society)[873]

This study aims to achieve an understanding of the attitudes of the Spanish people to catastrophes, disasters, emergencies or situations of risk. In all these cases, situations have the characteristic of being:

- harmful to the life, health or general well-being (individual or collective);
- uncommon, i.e. they are outside everyday and do not usually occur, or
- applicants for protection or security measures that prevent, limit or offset.

28.5 Public – Private Partnership & International Collaboration

As a member of NATO since 1982, Spain has become a major participant in multilateral international security activities. Spain's EU membership is an important part of its foreign policy.

Spain also has many bilateral relations:

With France: The police of Spain and France cooperate to suppress the terrorist group ETA.

With Portugal: Portugal and Spain cooperate in the fight against drug trafficking and in tackling forest fires (common in the Iberian Peninsula in summers).

With Latin American countries: Mexico, Venezuela, Cuba, Colombia, Dominican Republic, Brazil, Argentina, Chile, Bolivia and several Central American countries.

[873] http://www.proteccioncivil.org/es/publicaciones_recientes.html

FEPIC

European Forum for Critical Infrastructure Protection (pending of approval for funding by EC). It is a forum for cooperation among established EU national CIP Centres and public-private-partnerships. It is a focused group discussion on specific topics.

Two seminars are foreseen for the first year of existence of the Forum. In the second seminar, sectoral workshops identified in the first seminar will be organised, involving public and private experts.

28.6 Funding & Human Resources

CIP funding in Spain is provided by the Ministry of Treasury, the Ministry of Interior, EU Civil Protection Financial Instruments and other EU financing instruments on Critical Infrastructure Protection.

There are over 100 public employees involved in CIP related activities in Spain. Eleven of them work in the CNPIC.Their main tasks are developing plans and implementing countermeasures[874].

28.7 Training & Exercises

The **National School of Civil Protection *(Escuela Nacional de Protección Civil)***[875] is responsible for theoretical and practical education on the risks and emergencies management. The school is an organism of the General Direction of Civil Defence and Emergencies (Ministry of Interior) and has the following functions:

Training of commanders and staff from various departments and organisations involved in protecting people and property in case of emergency.

Acting as a forum for meetings of technicians and specialists in various disciplines related to risk and emergency management through Technical Seminars, Conferences and Congresses.

The School provides its training activities not only nationally but also internationally, particularly for the European Union, Latin America and the Mediterranean.

28.8 Sector - Specific Key Players & Initiatives

ENERGY

Main Operators:

- ***Equipos Nucleares***

  Spain has 8 working nuclear plans connected to the grid[876]. The main Spanish Nuclear Steam Supply System (NSSS) manufacturer is Equipos Nucleares, S.A[877].

[874] Booz & Company survey “Stock-taking of Existing Critical Infrastructure Protection Activities”
[875] http://www.proteccioncivil.org/es/ENPC/ and https://enpc.proteccioncivil.es/
[876] http://www.nea.fr
[877] http://www.ensa.es/

(ENSA), which designs, produces and inspects nuclear power plants primary circuit equipment and components.

INFORMATION AND COMMUNICATION TECHNOLOGY

Public Authorities:

- ***Network Information Security (NIS)***

  In Spain there is no single agency responsible for NIS. The Ministry of Industry, Tourism and Commerce has overall responsibility for developing and implementing national information security policy. Responsibility for implementing and ensuring compliance with electronic communications legislation is held by the Directorate General of Telecommunications, which is part of the Ministry of Industry, Tourism and Commerce. The Ministry of Interior has overall responsibility for critical infrastructure protection (CIP/CIIP). Within the Ministry, the State Secretariat for Security is responsible for development of the National Critical Infrastructure Protection Plan. The National Cryptology Centre (CCN) acts as a certification body, and runs the government CERT, which has a co-ordinatory role and acts a main point of contact with international organisations.

- ***National Cryptology Centre***[878]

  The CCN is responsible for providing ICT security for the public administration and functions also an information security certification body. CCN is part of the National Intelligence Centre, which is associated with the Ministry of Defence.

- ***CCN-CERT***[879]

  It is the Spanish governmental CERT. Its mission is to become the National Alert Centre, to cooperate and assist public administration in giving a quick and efficient response to information security incidents and to actively face new threats to which they are currently exposed.

  CCN-CERT offers its services through the following:

  - Support and coordination for the resolution of incidents suffered by national, provincial or local administrations.
  - Research and dissemination of best practices on information security among the public administrations. The CCN-STIC offers standards, instructions, guidelines and recommendations to ensure the security of state ICT systems.
  - Training through courses in the area of ICT security aimed at specialised public administration staff.

  The CCN-CERT provides the information and tools necessary for different administrations to develop their own CERTs, allowing CCN-CERT to act as a coordinator. CCN-CERT is part of the National Cryptology Centre.

- ***National Institute of Communication Technologies (INTECO)***[880]

  INTECO is a platform for the development of the “knowledge society” through projects in the area of innovation and technology. INTECO is promoted by the Ministry of

[878] http://www.ccn.cni.es/
[879] https://www.ccn-cert.cni.es/english/
[880] http://www.inteco.es

Industry, Tourism and Trade. INTECO's goal is to promote and develop Information and Communication Technologies (ICT) innovation projects which will improve the position of Spain and increase its competitiveness. The institute is tasked with developing, among other things, initiatives on technological security, accessibility and inclusion in the digital society, and communications solutions for companies and individuals. In the area of security, INTECO runs the following projects, with the aim of delivering a service to citizens and SMEs:

- Computer Emergency Response Team for SMEs and Citizens
- Information Security Observatory
- Security Technologies Show-Room for SMEs

- ***IRIS-CERT***[881]

  IRIS-CERT is the security service of RedIRIS, the national academic and research network. RedIRIS has more than 300 affiliated institutions, mainly universities and public research centres. IRIS-CERT is part of the Ministry of Industry, Tourism and Trade.

HEALTH

Public Authorities:

- ***The National Health System***[882]

  The National Health System (NHS) is made up of both the central government and autonomous communities public health care managements working in coordination to cover the health care duties and services for which public authorities are legally responsible. The central government's areas of respon-sibilities include general health care coordination and legislation; international health and international health relations and agreements; pharmaceutical policy.

FINANCIAL

- ***Banco de Espana***[883]
  Since January 1st, 1999 the Banco de España has been performing the following basic functions attributed to the ESCB:

  – Defining and implementing the Eurosystem's monetary policy ,with the principal aim of maintaining price stability.

  – Conducting currency exchange operations consistent with the provisions of Article 111 of the Treaty on European Union, and holding and managing the States' official currency reserves.

  – Promoting the sound working of payment systems.

  – Issuing legal tender banknotes and the placement in circulation of coins and the performance, on behalf of the State, of all such other functions entrusted to it in this connection.

  – The holding and management of currency and precious metal reserves not transferred to the European Central Bank.

[881] http://www.rediris.es/cert/
[882] http://www.msc.es/en/estadEstudios/estadisticas/docs/LIBRO-BAJA-INGLES.PDF
[883] http://www.bde.es

– The promotion of the sound working and stability of the financial system and, without prejudice to the functions of the ECB, of national payment systems.
– The supervision of the solvency and compliance with specific rules of credit institutions, other entities and financial markets, for which it has been assigned supervisory responsibility.
– Preparation and publication of statistics relating to its functions, and assisting the ECB in the compilation of the necessary statistical information
– Provision of treasury services and acting as the financial agent for government debt.

RESEARCH

Public Authorities:

- ***Spanish National Research Council***[884]

  The Spanish National Research Council (CSIC) is Spain's largest and most important public research organisation. With 126 centres and 145 associated units, it is present in all of Spain's Autonomous Regions. The CSIC's mission is to promote, coordinate, develop, and disseminate multidisciplinary scientific and technological research in order to contribute to economic, social, and cultural development and the progress of knowledge. Furthermore, it aims to train research personnel and provide advice to public and private institutions on subjects within its areas of expertise.

- ***General Military Academy***[885]

  The aim of the AGM is training future Army Officers from the Arms General Corps and the Civil Guard, from the Armed Forces Common Corps, from the Army Specialists Corps and from the Army Polytechnic Engineering Corps. Likewise, it offers complementary training for the diploma required to join the Service Corps.

- ***University of Alcalà de Henares***

  The University of Alcalà de Henares is involved in CIP-related research in Spain[886]

[884] http://www.csic.es/
[885] http://www.ejercito.mde.es/ingles/personal/centros/agm.html
[886] Booz & Company survey "Stock-taking of Existing Critical Infrastructure Protection Activities"

29 Sweden

Figure 103: Sweden

29.1 Summary

	Organizational Model	Strategy and Policy	Funding and Human Resources	Public-Private Partnership and international collaboration	Test, training and exercises	Methods, standards, operating plans and technology	Sector-specific initiatives
Sweden	▪ CIP is managed by the SCCA ▪ Ministries deal with CIP issues on a case-by-case basis	▪ Sweden is dealing in an informal way with CIP	▪ Funding partially assigned from Central Government and from the involved entity	▪ Svenskt Näringsliv Industry Security Delegation promotes cooperation between enterprises on vulnerability issues	▪ Coordination exercises will be performed	▪ RAKEL standard is being introduced to secure commu-nications	▪ Committee on Electronics Communication focuses on a more secure electronics communication s infrastructure

Sweden does not yet have an official definition of CIP in place; the most significant initiative that laid the foundation for defence and emergency preparedness planning in Sweden is the ***Commission on Vulnerability and Security***. The Commission was established to analyze and submit proposals for a more integrated approach to civil defence and emergency preparedness planning; its findings were presented in May 2001.

The commission had suggested several strategic measures for the development of critical infrastructure protection, such as: proposing measures designed to enhance information assurance and improve protection against information operations; for the Swedish government to assume key responsibility in these areas also by providing the necessary functions and facilities that exceed the financial capabilities of other sectors in society; and emphasized that all managers and system owners are responsible for securing their own systems.

Swedish preparedness consists of a network of authorities on all levels of society with various areas of responsibility and roles. In the event of accidents, they must be able to cooperate in order to ensure more efficient coordination. Both the public and private sectors in society needs to strengthen its own capacity in handling a sudden malfunction of critical infrastructures.[887]

The various agencies and organisations in charge of CIP are under the heading of the ministry they are affiliated with, including the Ministry of Defence; the Ministry of Industry, Employment and Communication; and the Department of Justice.

[887] *Krisberedskapsmynigheten* SEMA Swedish Emergency Management Agency www.krisberedskapsmynigheten.se

29.2 Organisational model

Organisational Chart:

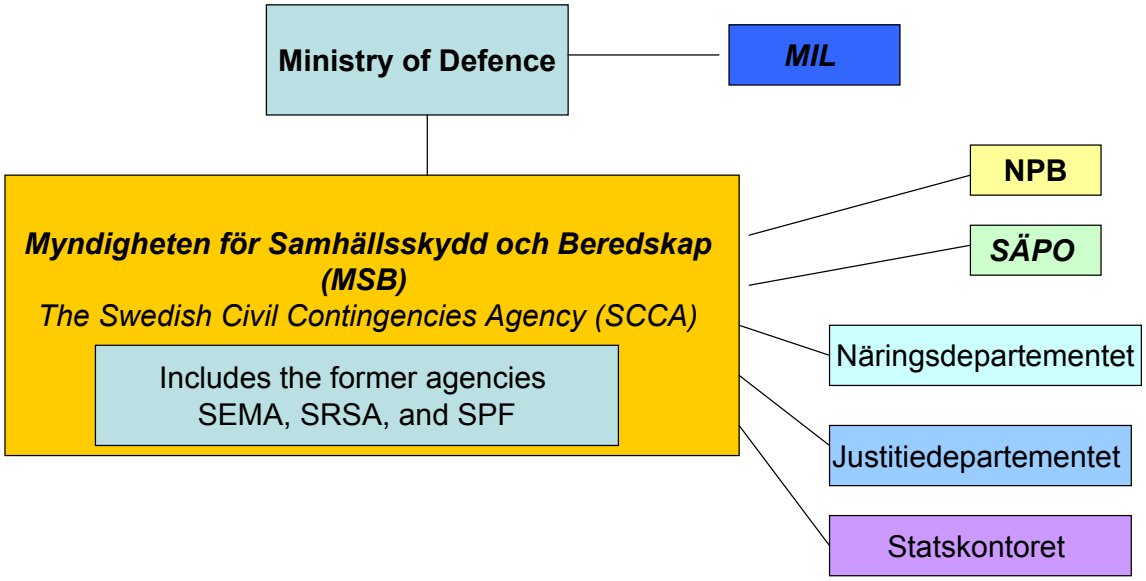


Figure 104: Organisational Chart (only CIP-related agencies shown)

Main Actors/Responsibilities

- ***Försvarsmyndigheten*** (**Ministry of Defence**)[888] is responsible for the overall defence policy, protection, preparedness against accidents, and preparedness for severe peacetime emergencies. Swedish defence is currently in the process of transformation and is based under the Government Bill – 'The New Defence' presented in November 18, 1999. It includes a more modern, flexible and mobile operational defence system entailing changes in the size, training and management of the organisation, and particularly towards a more network based on information and communications technology.

- ***Myndigheten för Samhällsskydd och Beredskap (MSB) – The Swedish Civil Contingencies Agency (SCCA)***[889] is the new national government agency established as of 1 January 2009 being formed from three existing national government authorities, namely *Swedish Emergency Management Agency (SEMA)*, the *Swedish Rescue Services Agency (SRSA)*, and the *National Board*

888 *Försvarsmyndigheten Ministry of Defence* www.sweden.gov.se
889 *Myndigheten för Samhällsskydd och Beredskap (MSB) – The Swedish Civil Contingencies Agency (SCCA)* www.msbmyndigheten.se

of Psychological Defence (SPF). The Agency has the all-encompassing task with regard to civil contingencies covering the whole spectrum of contingencies from serious emergencies such as bomb threats, hostile attacks, epidemics, natural disasters, and war to everyday road traffic accidents, fires, chemical emergencies, power cuts, and other technical failures. The responsibilities of this new agency will include information security. SEMA's current work on CIIP will be expanded, and the new agency will be given the authority to issue binding regulations.

Since the Swedish Emergency Management Agency (SEMA) had the overall governmental responsibility for information assurance in Sweden, *The Swedish Civil Contingencies Agency (SCCA)* will thus take over and be in charge of the co-ordination of national information assurance at the policy level. Its tasks will include analyzing the development of information society and the interdependency of critical societal functions. The agency will moreover promote interaction between the public and private sector and coordinate research and development in the area of emergency management. The *Information Assurance and Analysis Department* at SEMA previously managed the following tasks:

- Maintaining an overall picture of society's information security in terms of threats, vulnerabilities, protective measures, and risks
- Hosting various forums in order to develop a common national culture of information assurance
- Developing public-private partnerships
- Gathering, analyzing, and disseminating open-source information related to information assurance
- The development of preventive IT security recommendations (consistent with ISO / IEC 17799) to support the IT security activities of other organisations
- Initiating research and development in the area of different important societal systems and summarizing the respective risk and vulnerability assessments
- Managing the Board of Information Assurance
- Participating as a member in several international forums

SCCA will work in a preventive capacity with IT security issues; it will conduct IT security analyses and give advice and recommendations to safeguard these IT systems. SEMA supports and co-ordinates the communication protection operation within Sweden's civil defence. The purpose of communication protection is to give authorities and companies who run critical information infrastructure the ability to protect classified information from access by unauthorized parties during information exchanges.

- ***Försvarsmakten – MIL* – (The Swedish Armed Force)**[890]
  is developed according to the concept of network-based defence, with its armed forces able to quickly respond to different types of threats and risks. The

[890] *Försvarsmakten (MIL) the Swedish Armed Forces* www.mil.se

protection of information infrastructure is thus highly significant; the armed forces are heavily involved in research and development in areas such as IT security and information infrastructures. The Swedish Military Intelligence and Security Service handle operational IT security in the armed forces during peacetime. In addition, the National Communications Security Group (TSA) offers advice and inspections of cryptographic systems to Swedish defence organisations and industries.

- ***Rikspolisstyrelsen – NPB* – (The Swedish National Police Board)**[891]

  The NPB is the central administrative and supervisory authority of the police service. The NPB administers the National Criminal Police and the Swedish Security Service. Within the NPB, the IT Crime Squad has expert knowledge in investigating IT crime. This group supports the local Swedish police departments in IT crime investigations, participates in the education of parts of the judicial system, and assembles and communicates information about IT crime. The Internet Reconnaissance Unit is linked to this squad.

- ***Säkerhetspolisen – SÄPO* – (The Swedish Security Service)**[892]

  SÄPO has the fundamental duty of preventing and detecting crimes against the Swedish security, and protects the government. SÄPO is engaged in four main fields: protective security (including personal protection), counter-espionage, counter-terrorism, and protection of the constitution.

- ***Näringsdepartementet* (Ministry of Enterprise, Energy and Communications)**[893]

  This ministry is responsible for issues relating to business development, energy, transport and particularly in issues concerning the Information and communications technology ensuring the protection of critical infrastructures.

- ***Justitiedepartementet* (Ministry of Justice)**[894]

  The Ministry of Justice is responsible for the overall judicial, criminal and security matters.

- ***Statskontoret* (The Swedish Agency for Public Management)**[895]

  The Swedish Agency for Public Management conducts studies and evaluations, develops administrative policy with the application of ICT, and ensures that the electronic infrastructure in the public sector is open and secure.

891 *Rikspolisstyrelsen (NPB)* The Swedish National Police Board www.polisen.se
892 *Säkerhetspolisen (SÄPO) The Swedish Security Service* www.sakerhetspolisen.se
893 *Näringsdepartementet* Ministry of Enterprise, Energy and Communications www.sweden.gov.se
894 *Justitiedepartementet* Ministry of Justice www.sweden.gov.se
895 *Statskontoret The Swedish Agency for Public Management* www.statskontoret.se

29.3 Strategy & Policy

Cross-sectoral work with CIP in Sweden

The Swedish Civil Contingency Agency (former SEMA and SRSA) is responsible for the national coordination of cross sectoral CIP issues and development, including the ongoing work and coordination of EPCIP. It inherited these issues from the Swedish Emergency Management Agency (SEMA) when the new authority was activated in January 2009: Apart from participating in the preplanning for EPCIP, SEMA did define 11 areas which were considered as Critical Societal Functions and also settled a definition for that matter. In addition, SEMA did benchmarking, especially in Europe, regarding CIP and the need for a national strategy or policy regarding CIP which Sweden did not have.

SEMA did also conduct some research regarding the need for public-private partnerships and raising awareness of interdependencies, and tools to identify dependencies between businesses and organisations to reduce risk exposure.

The main reason for not implementing a national strategy or policy for CIP was fundamentally based the Swedish Crisis Management System. This system is based on voluntarism and cooperation and a bottom – up perspective rather than regulations and supervision. There are no strong "national" resources in place, even for crisis management. Counties and central agencies held responsibility for coordinating individual regions (muni, counties), currently at various levels of development and maturity. SCCA is trying to improve the coordination of these efforts.

Additionally, each sector in Sweden is responsible for CIP-related work and have rather sophisticated risk reduction programs. The final major point was that CIP, as it was approached in several European countries, was considered too limited to ensure a robust society. Therefore, instead of focusing on CIP, Sweden has used the term "Critical Societal Functions", more about resilience than protection and a broader perspective than CIP.

However; mirroring the EPCIP programme and the implementation of the directive, the Swedish Authority has the national responsibility to develop the work with protecting vital societal functions and Critical Infrastructure and aiming to establish a National Strategy for CIP. At the moment there are two parallel studies to define the national needs and gaps, and based on these studies Sweden will settle a plan for the national approach, including CIP.

The key documents establishing the measures for the Swedish security framework and that have major implications on CIP are:

- ***Starkt Krisberedskap för Säkerhets skull*** **(The Bill on Swedish security and Preparedness Policy) –** ***Regerings proposition 2007/08:92***[896]

  This Bill contains changes of tasks and responsibilities for the actors within Swedish crisis preparedness; some changes include that in 2009, the *Krisberedskapsmyndigheten Swedish Emergency Management Agency (SEMA)* – and other agencies involved in CIP initiatives will be replaced by a new agency called

[896] *Bill on Swedish security and Preparedness Policy "Starkt Krisberedskap för Säkerhets skull"* http://www.regeringen.se/content/1/c6/10/11/51/45e238c5.pdf (in Swedish) / www.krisberedskapsmyndigheten.se

the *Myndigheten för Samhällsskydd och Beredskap Swedish Civil Contingencies Agency (SCCA)* that will report to the Ministry of Defence. The objective to obtain a holistic view of the issues and then decide how much change, if any, is needed.

- ***Commission on Vulnerability and Security***

  Based largely on the findings and proposals of the *Commission on Vulnerability and Security*, the government presented its first bill in March 2001 on Swedish security and preparedness policy. The findings and proposals of the bill has been the most significant step toward the implementation of a new planning system to prepare for major societal crises and activities related to potential threats to war: The bill further presenting an account of the structural crisis management structure would be strengthened such as establishing a new organisational structure for information assurance and improve protection against information operations; these accordingly having implications to CIP and CIIP.

Based on the strategy defined in these references, critical functions comply with one or both of the following conditions:

1. A shutdown or severe disruption in the function, single handedly or in combination with other similar events, can rapidly lead to a serious emergency in society.

2. The societal function is important or essential for responding to an existing serious emergency and minimising the damage.

SEMA has produced criteria that help identify these functions. Criteria that govern preventive work are *impact criteria* – what happens when a certain function is disrupted? Criteria that govern response are *capability criteria* - what significance does a function have for society's emergency response capabilities?

The following lists some examples of the sectors and the critical functions – essential assets, services and system – in each of these sectors:

Sector	Functions
Energy supply	Production and distribution of electricity, district heating, fossil fuels and vehicle fuels.
Information and communication	Telephone services, Internet, radio and TV broadcasts, postal services, production and distribution of newspapers, radio and TV.
Financial services	Money transmission, cash access, private insurance and securities trading.
Social insurances	Payment of sickness and unemployment benefits and the national pension system.
Public health and medical services, and special social services	Emergency hospitals, primary care, psychiatry, pharmaceutical supplies, infectious disease control, and special social services for children, disabled persons and the elderly.
Protection, security and safety	Rescue services, police, courts, correctional institutions and SOS Alarm, military, coast guard, and customs, border and immigration control.
Transport	Road, rail, sea and air transport, and transport infrastructure management.
Municipal services	Drinking water, sewage treatment, street-cleaning, public meeting places, refuse collection and roads.
Food	Agriculture and the production, distribution and control of food.
Trade and industry	Retail, IT operations and service, construction and contract work, guard and security services and the manufacturing industry.
Public administration • governance • support functions • service sector	National management, regional management and local management, diplomatic and consular services, inspection and permit services, expert and analytical services, detection and laboratory services, collection and provision of population data, meteorological services, training services and burial services.

Figure 105: Critical Sectors and Functions in Sweden

29.4 Methodology & Standards

RAKEL (*Radiocommunication for Efficient Command*) is a new radio communication system for public safety authorities which will be constructed by the Swedish Civil Contingencies Agency (SCCA). RAKEL will replace the more than 200 different systems that are currently in use and will be primarily used by the police, local civil protection, emergency and ambulance personnel, and national defence authorities. Other actors will also be able to access the system in events of accidents of a wider scale. The RAKEL system will function nationwide and will be developed in the years 2005-2010. It will help to streamline and secure communications - from small scale accidents to serious crises from electricity cut downs to telecommunication breakdown. RAKEL will offer a variety of new features; for instance it will be possible to encrypt sensitive information and to quickly form optional caller groups. The system can be used both for speech and data transmission[897].

29.5 Public – Private Partnership & International Collaboration

- ***Public-Private Partnerships***

  The public-private partnership initiatives in Sweden currently include the following SCCA (previously by SEMA) efforts to promote interaction between the public and the private sector:

  – ***Svenskt Näringsliv* (Industry Security Delegation) *(NSD)***[898] is a delegation within the Confederation of Swedish Enterprise whose objective is to increase cooperation between companies, organisations and authorities; and promote comprehensive views on vulnerability and security issues. The overall goal of this network structure is to enhance security risk awareness within the general public and the companies, and the Swedish Information Processing Society (DFS). The *Private Sector Partnership Advisory Council* and the *Board of Information Assurance*, part of SCCAs public-private partnership forum, has however not yet established how the CIP public-private partnership will be institutionalized.

    There are two advisory councils connected to SEMA: the Private Sector Partnership Advisory Council and the Board of Information Assurance. SEMA has two forums for sharing information between private and public actors in the area of information assurance. The two established forums in the area of Supervisory Control and Data Acquisition (SCADA) and the financial sector. In these forums, the actors share information about threats and vulnerabilities in order to learn from each other. This concept is largely based on the British model for Information Exchange (IE).

  - ***The Dataföreningen Swedish Information Processing Society (DFS)***[899]

[897] SEMA http://www.krisberedskapsmyndigheten.se/templates/EntryPage____1217.aspx
[898] *Krisberedskapsmynigheten* SEMA Swedish Emergency Management Agency www.krisberedskapsmyndigheten.se
[899] *Dataföreningen* Swedish Information Processing Society (DFS) www.dfs.se

The Swedish Information Processing Society (DFS) is an independent organisation for IT professionals with 32,000 members. The DFS owns the *SårBarhetsAnalys* SBA *Vulnerability Assessment* brand of security products which are focused on risk analysis and information security. SBA is regarded as the de-facto a Swedish standard.

- ***PTS/The Swedish IT Incident Centre (SITIC)***[900]

  The Swedish IT Incident Centre (SITIC) officially established on 1 January 2003 and can be considered to be the Swedish government CERT. SITIC supports national activities for protection against IT incidents by:

  – Operating a system for information exchange on IT incidents between both public and private organisations and SITIC

  – Rapidly communicating to the public information on new problems that can disrupt IT systems

  – Providing information and advice on preventive measures

  – Compiling and publishing incident statistics as input to the continuing improvements of preventive measures.

29.6 Funding & Human Resources

The Central Government continues to have primary responsibilities for funding the measures taken in critical infrastructure protection, particularly in events entailing very serous and far-reaching consequences. The *'Responsibility measure'* is still applicable wherein the cost of physical protection should be to a large extent financed by the owner/operator itself whenever possible. Funding and planning of crisis management activities that are conducted by public authorities can be financed by taxes, charges, and self-funding[901].

SCCA also injects funding into system for the development of crisis management functions (not prevention, CIP, etc). SCCA is currently considering expanding its funding opportunities.

29.7 Training & Exercises

One of the tasks of the Swedish Civil Contingencies Agency (SCCA) will be to initiate and conduct exercises in order to strengthen the emergency preparedness. It will be responsible for planning and coordinating the preparations in cooperation with the affected authorities, agencies and organisations.

900 PTS/The Swedish IT Incident Centre (SITIC) www.sitic.se

901 The Swedish Commission on Vulnerability and Security 2001:41 "*Vulnerability and security in a New Era- A Summary"* p.10-12

SCCA is the responsible authority that coordinated exercises every year, varying formats, participants, geographic areas, and scope. In these exercises, participating actors exercise coordination through cooperation with focus on the main threats facing Swedish society today. Examples of scenarios include: Transport, Spreading of Infectious Agents, Toxic Chemicals and Radioactive Materials and Protection, Rescue and Care.[902]

29.8 Sector - Specific Key Players & Initiatives

ENERGY

Public Authorities:

- ***Näringsdepartementet Ministry of Enterprise, Energy and Communications***[903]

  Näringsdepartementet is responsible for handling the overall government business in the energy, transport, electronic communications, IT, business development and competition, R&D sector.

- ***Finansdepartementet (Ministry of Finance9***[904]
  The Ministry of Finance is responsible for the central government budget, taxes, banks, securities and insurance.

- ***Miljödepartementet (Ministry of Environment)***[905]

  The Ministry of Environment is responsible for initiatives on the environment, energy and climate change, housing and construction, water and seas, chemical and sustainable development policies.

- ***Energimyndigheten* (*Swedish Energy Agency)***[906]

  Energimyndigheten works towards transforming the Swedish energy system into an ecological and economically sustainable system through securing access to electricity and other energy resources by collaborating with trade and industry, energy companies, municipalities and the research community. The Swedish Energy Agency supervises net companies in accordance with electricity regulations as well as supervising the natural gas market. They monitor and analyze the electric market and play an expert role in issues relating to the sale of electricity. The Agency is also the authority responsible in times of emergency in oil, coal and gas.

- ***Strålsäkerhetsmyndigheten* (*Swedish Radiation Safety Authority)***[907]

---

902 *Myndigheten för Samhällsskydd och Beredskap (MSB)* – The Swedish Civil Contingencies Agency (SCCA) www.msbmyndigheten.se
903 *Näringsdepartementet* Ministry of Enterprise, Energy and Communications www.sweden.gov.se
904 *Finansdepartementet* Ministry of Finance www.sweden.gov.se
905 *Miljödepartementet* Ministry of Environment www.sweden.gov.se
906 *Energimyndigheten* Swedish Energy Agency www.swedishenergyagency.se
907 *Strålsäkerhetsmyndigheten* Swedish Radiation Safety Authority www.stralsakerhetsmyndigheten.se

Strålsäkerhetsmyndigheten is a managing authority under the Ministry of the Environment since 1 July 2008, with national collective security responsibility within the areas of radiation protection and nuclear safety.

Main Operators:

- ***Vattenfall***[908]

  Vattenfall provides around 50% of Sweden's electricity production, mostly from nuclear and hydro-power sources.

- ***E.ON Sverige***[909]

  E.On Sverige is formerly known as Sydkraft and is Sweden's second largest energy utility company. E.On Sverige produces and supplies energy – electricity, gas, heating, freezing and waste disposal services, and energy related services.

- ***Svenska Kraftnät*** [910]

  Svenska kraftnät is a state utility that administers and runs the national electrical grid. Since July 2005, Svenska Kraftnät also has the system responsibility for the national supply of natural gas.

- ***Elsäkerhetsverket Swedish National Electrical Safety Board***[911]

  Elsäkerhetsverket is the supervisory authority for electrical safety and electromagnetic compatibility (EMC). It aims to prevent injury to persons and damage to property caused by electricity, maintain and further develop a high level of safety for high voltage electrical installations and electrical equipment, and prevent interference caused by EMC through regulations, authorisation, co-operation for standardisation, supervision and information initiatives.

INFORMATION AND COMMUNICATION TECHNOLOGY

Public Authorities:

- ***Post och Telestyrelsen (PTS) Swedish Post and Telecom Agency***[912]

  PTS monitors the electronic communications – telephones, the Internet and radio, as well as the postal sectors in Sweden.

- ***Försvarets Materielverks (FMV) The Swedish Defence Materiel Administration***[913] and the *(CSEC)* Swedish *Certification Body for IT Security*. The FMV is the procurement agency for the armed forces involved in the area of IT

908 Vattenfall www.vattenfall.com
909 E.ON Sverige www.eon.se
910 Svenska kraftnät www.svk.se
911 Elsäkerhetsverket www.elsakerhetsverket.se
912 *Post och Telestyrelsen (PTS)* Swedish Post and Telecom Agency www.pts.se
913 *Försvarets Materielverks (FMV) The Swedish Defence Materiel Administration* www.fmv.se

security evaluations performing in-house evaluations of equipment intended for use by the armed forces. In the summer of 2002, the FMV was tasked by the government with establishing a national scheme for the evaluation and certification of IT security products to be used within Swedish governmental organisations. The certification body CSEC is now established as an independent entity within the FMV and is responsible for the establishment, operation and administration of a system for evaluating and certifying IT security products and systems.

- ***Försvarets Radioanstalt (FRA)* the *Swedish National Defence Radio Establishment***[914]

  FRA is the Swedish national authority for signals intelligence. It is a civilian agency directly subordinated to the Ministry of Defence. FRA is also engaged in Information Assurance and supports government authorities and state-owned companies regarding current IT threats as well as general advice to improve security. The Information Security Technical Support Team is associated with the FRA and consists of 20 experts in the field of IT security. The team is intended to support the national crisis management entity where IT-security qualifications are required, and in the identification of individuals and organisations involved in IT-related threats against critical systems. The team supports the Swedish authorities, agencies, and state-owned corporations that are responsible for critical functions in Swedish society with IT-security expertise and services. The customized services consist of penetration tests, forensic computer investigations, source code analysis, audits, risk analyses, etc. The team co-operates on a regular basis with the national and international IT security community.

- ***Forskningsinstitut för Försvar, Säkerhet och Teknikutveckling (FOI) The Swedish Defence Research Agency***[915]

  FOI focuses on research and development in the fields of applied natural sciences and political sciences, such as security policy analysis. The Critical Infrastructure Studies Unit (CISU), which is part of the Division of Defence Analysis, is a research group that carries out long-term research programs on CIP sponsored by SEMA, in cooperation with Systems Analysis and IT Security - another FOI department. This department has acquired a deep knowledge of commercial and military IT systems and applications.

- ***Kommunikationsmyndigheten (PTS) The Swedish National Post and Telecom Agency***[916]

  The Swedish National Post and Telecom Agency (PTS) is a government authority that reports to the Ministry of Industry, Employment and Communications that monitors all issues relating to Information communications Technology (ICT) and postal services in Sweden. One of its key tasks is to ensure the development of functioning postal and telecom markets. The Department of Network Security

914 *Försvarets Radioanstalt (FRA)* the *Swedish National Defense Radio Establishment* www.fra.se
915 *Forskningsinstitut för Försvar, Säkerhet och Teknikutveckling (FOI*) The Swedish Defence Research Agency www.foi.se
916 *Kommunikationsmyndigheten (PTS)* The Swedish National Post and Telecom Agency www.pts.se

within the PTS is responsible for monitoring developments concerning security issues and implementing measures to reduce the threats to ICT from sabotage and terrorism. Emergency measures are planned following consultation with the ICT operators, the Swedish Armed Forces and other agencies. The *Department of Network Security* within this PTS is tasked with monitoring developments related to security issues and with implementing measures to reduce the threats to ICT from sabotage and terrorism. Emergency measures are planned in consultation with the ICT operators, the Swedish armed forces, and other agencies. As an example, critical nodes in the ICT structures are hardened, ad all nodes that are crucial for running the ".se" domain autonomously have been installed within Sweden's borders.

- ***Sveriges IT Incident Centrum (SITIC) Swedish IT Incident Centre***[917]

  The Swedish IT Incident Centre is associated with this department is an independent organisation that supports the society against threats within the IT security area. SITIC is a part of the National Post and Telecom Agency (PTS) and continuously assesses and informs about threats against the IT security that involves risks against public authorities, county councils, municipalities and companies. SITIC provides a function for information exchange about IT-incidents among society's organisations and disseminates information in the society about new problems that can disturb IT systems.

Main Operators:

- ***TeliaSonera AB***[918]

  TeliaSonera AB is the dominant telephone company and mobile network in Sweden that also provides telecommunication services in the Nordic and Baltic countries, in Spain and the emerging markets of Eurasia, including Russia and Turkey

- ***Tele2***[919]

  Tele2 is one of Europe and Sweden's leading telecommunications operators serving as a fixed-line telephone operator, cable television provider, mobile phone operator, internet service provider.

- ***ERICSSON***[920]

  Ericsson is one of the largest fixed and mobile technologies service provider.

***Initiatives*:**

- ***Committee on Electronic Communications***

[917] *Sveriges IT Incident Centrum (SITIC)* Swedish IT Incident Center www.sitic.se
[918] Telia Sonera AB www.teliasonera.com
[919] TELE2 www.tele2.se
[920] Ericsson www.ericsson.com

This bill presented through a decision in 19 April 2001, established the Committee on Electronics Communication with tasks of reviewing policy objectives towards a more coordinated regulation of the whole area of electronic communications infrastructure and services. The new formulations of its policy prioritized among others, a more secure electronics communications infrastructure.

- ***'An Information Society for All'***

  The Government bill "An Information society for All" defined the Swedish overall IT policy objectives focusing on regulatory systems, education and training and infrastructure.

- ***Information Security Policy proposals by the Committee on Information Assurance***

  The Swedish government on 11 July 2002 instituted the Committee on Information Assurance in Swedish Society with an objective to present an assessment of information protection requirements in critical sectors of society, and to make a proposal on organisational matters of the Swedish signals protection service and to develop a national strategy on information assurance.

- ***SEMA action plan for information security***

  The Swedish Emergency Management Agency (SEMA) was commissioned in January 2007 by the government to prepare a proposal for a plan of action to implement and administer the nation's strategy for information security. The plan consists of proposed measures covering the following four areas as priorities.

  Improved sector-wide and cross-sectoral work is needed for civil information security. All-embracing directives for the field of information security applying to all government agencies should be prepared. At the same time, by clarifying sector-specific responsibility must be clarified and opportunities for providing practical recommendations to other civil sectors;

  Establishing a fundamental security level must be for information security for securing the information assets that have become increasingly fundamental for both trade and industry and the public sector;

  An operative national coordinating function should therefore be established for society to be able to deal with extensive IT-related disturbances and emergencies.

FINANCIAL SERVICES

Public Authorities:

- ***Finansdepartementet Ministry of Finance*** [921]

[921] *Finansdepartementet* Ministry of Finance www.sweden.gov.se

The Ministry of Finance is responsible for handling government business in the central government budget, taxes, bank securities and insurance, international economic and financial cooperation.

- ***Riksbank Sweden's Central Bank*** [922]

  Riksbank is Sweden's central bank and is responsible for monetary policy with the objective to maintain price stability. The bank has also been given the task to promote a safe and efficient payment system.

- ***Finansinspektionen (FI) Swedish Financial Supervisory Authority***[923]

  The FI supervises and monitors companies operating in financial markets. Companies offering financial services in Sweden require permits issued by the Financial Supervisory Authority.

- ***Skatteverket Swedish Tax Agency***[924]

  The Swedish tax Agency is a government agency in Sweden responsible for national tax and population registers related issues.

- ***Ekonomistryning (ESV) Swedish National Financial Management Authority***[925]

  ESV has the overall responsibility to develop and implement financial management.

- ***Kammarkollegiet Legal, Financial and Administrative Services Agency***[926]

  Kammarkollegiet is a public authority that also operates commercial undertakings mainly involve activities that require qualified legal and economic expertise. The role of the agency in capital administration is to provide a state-run alternative for the public sector in the broad sense.

- ***Skandinaviska Enskilda Banken AB (SEB)***[927]

  SEB is Sweden's largest bank, occupying a leading position among large corporations and private banking customers.

- ***Tullverket Swedish Customs***[928]

  Swedish Customs manages the flow of goods, ensure competitive neutrality in trade and contribute to a safe and secure trade flow.

- ***Riksgälden Swedish National Debt Office***[929]

922 *Riksbank* Sweden's Central Bank www.riksbank.com
923 *Finansinspektionen (FI)* Swedish Financial Supervisory Authority www.fi.se
924 *Skatteverket* Swedish Tax Agency www.skattevverket.se
925 *Ekonomistryning (ESV)* Swedish National Financial Management Authority www.esv.se
926 *Kammarkollegiet* Legal, Financial and Administrative Services Agency www.kammarkollegiet.se
927 *Skandinaviska Enskilda Banken AB (SEB)* www.seb.se
928 *Tullverket* Swedish Customs www.tullverket.se
929 *Riksgälden* Swedish National Debt Office www.riksgalden.se

is the central government financial manager, providing state cash's management, managing and finance central government debt and providing state guarantees.

HEALTH

Public Authorities:

- ***Socialdepartementet Ministry of Health and Social Affairs*** [930]

  The Ministry of Health and Social Affairs covers basic welfare issues and a broad policy field - economic security, social services, health and medical care, public health and the rights of children and people with disabilities.

- ***Statens Folkhälsoinstitutet (FHI) Swedish National Institute of Public Health***[931]

  The FHI is a state agency under the Ministry of Health and Social Affairs and is responsible for monitoring and coordinating the implementation of national public health policy and is the national centre of knowledge for the development and dissemination methods and strategies in the field of public health.

- ***Smittskyddsinstitutet (SMI) Swedish Institute for Infectious Disease Control***[932]

  The SMI is a governmental expert agency that monitors the epidemiological situation for infectious diseases in humans. It is also responsible for promoting protection against such diseases.

- ***Social Styrelsen National Board of Health and Welfare***[933]

  Social Styrelsen is a government agency under the Ministry of Health and Social Affairs, with duties within the fields of social services, health and medical services, environmental health, communicable disease prevention and control and epidemiology.

TRANSPORT

Public Authorities:

- ***Järnvägsstyrelsen (JVS) Swedish Rail Agency***[934]

  JVS is the regulatory body responsible for matters concerning safety in the railway, underground and tram systems. The agency will also see to it that the markets for rail services function efficiently and competitively.

930 *Socialdepartementet* Ministry of Health and Social Affairs www.sweden.gov.se
931 *Statens Folkhälsoinstitutet (FHI)* Swedish National Institute of Public Health www.fhi.se
932 *Smittskyddsinstitutet (SMI)* Swedish Institute for Infectious Disease Control www.smittskyddsinstitutet.se
933 *Social Styrelsen* National Board of Health and Welfare www.socialstyrelsen.se
934 *Järnvägsstyrelsen (JVS)* Swedish Rail Agency www.jvs.se

- ***Vägverket (VV) Swedish Road Administration***[935]

  VV is the national authority assigned the overall responsibility for the entire road transport system. The SRA is also responsible for drawing up and applying road transport regulations and for the planning, construction, operation and maintenance of the state roads.

- ***Banverket Sweden's Rail Administration*** [936]

  Banverket has the overall responsibility for the rail transport system in Sweden that covers conventional railways, underground railways and light rail systems. It leads and follows developments in the rail sector and assists the Government and Parliament on issues that concern the entire rail transport system.

- ***Statens Järnvägar AB (SJ) Swedish State Railways***[937]

  SJ is a government-owned passenger train operator.

- ***Sjöfartsverket Swedish Maritime Administration***[938]

  Sjöfartsverket is a Swedish government agency that provides the transport sector by keeping the sea lanes open and safe. The Administration provides services in pilotage, fairways, icebreaking, hydrographics, maritime search and rescue and maritime safety inspection. The Swedish Maritime Administration's primary tasks include responsibility for providing infrastructural services in the form of safe and accessible fairways to meet the needs of shipping.

- ***Luftfartstyrelsen Swedish Civil Aviation Authority (SCAA)***[939]

  Luftfartstyrelsen is responsible for regulations and inspections within Swedish civil aviation and shall supervise, analyze and evaluate the development of the civil aviation sector as well as provide expertise in issues including physical planning, the environment, emergency planning and contingency planning. The SCAA is also responsible for the Search and Rescue Services.

- ***Statens Institution för Kommunikationsanalys (SIKA) Swedish Institute for Transport and Communications Analysis***[940]

  SIKA has three main areas of responsibility in the transport and communications sector: to carry out studies for the Government, to develop forecasts and planning methods and to be the responsible authority for official statistics.

- ***Transportstyrelsen Swedish Transport Agency***[941]

935 *Vägverket (VV)* Swedish Road Administration www.vv.se
936 *Banverket* Sweden's Rail Administration www.banverket.se
937 *Statens Järnvägar AB (SJ)* Swedish State Railways www.sj.se
938 *Sjöfartsverket* Swedish Maritime Administration www.sjofartsverket.se
939 *Luftfartstyrelsen* Swedish Civil Aviation Authority (SCAA) www.luftfartsstyrelsen.se
940 *Statens Institution för Kommunikationsanalys (SIKA)* Swedish Institute for Transport and Communications Analysis www.sika-institute.se
941 *Transportstyrelsen* Swedish Transport Agencywww.transportstyrelsen.se

Has the overall responsibility for drawing up regulations and ensuring that authorities, companies, organisations and citizens abide by them. They work to ensure accessibility and for a secure rail, sea and road transport.

- ***Kustbevakningen Swedish Coast Guard***[942]

  is responsible for implementing maritime surveillance, marine environment and other supervision tasks and protection.

FOOD

Public Authorities:

- ***Jordbruksdepartementet Ministry of Agriculture***[943]

  The Ministry of Agriculture is responsible over agricultural and environmental issues relating to among others agriculture, fisheries, animal welfare, foodstuffs, forestry as well as research in the field of agricultural sciences.

- ***Livsmedelsverket (SLV) National Food Administration***[944]

  SLV is the central supervisory authority for matters relating to food, including drinking-water.

WATER

Public Authorities:

- ***Social Styrelsen National Board of Health and Welfare***[945]

  The National Board of Health and Welfare is a government agency under the *Socialdepartementet* Ministry of Health and Social Affairs, with duties within the fields of social services, health and medical services, environmental health, communicable disease prevention and control and epidemiology.

- ***Svenska Miljöinstitutet (IVL) Swedish Environmental Research Institute***[946]

  IVL is an independent research body that is involved in the development of solutions to environmental problems on behalf of the business sector and the community. IVL deals with environmental issues from a holistic perspective with the aim of contributing to sustainable growth.

- ***Svensktvatten (SWWA) Swedish Water & Wastewater Association***[947]

  The SWWA is responsible for the coordination, research and providing expertise on water and wastewater related activities.

942 *Kustbevakningen* Swedish Coast Guard www.kustbevakningen.se
943 *Jordbruksdepartementet* Ministry of Agriculture www.sweden.gov.se
944 *Livsmedelsverket (SLV)* National Food Administration www.slv.se
945 *Social Styrelsen* National Board of Health and Welfare www.socialstyrelsen.se
946 *Svenska Miljöinstitutet (IVL)* Swedish Environmental Research Institute www.ivl.se
947 *Svensktvatten (SWWA)* Swedish Water & Wastewater Association www.svensktvatten.se

30 United Kingdom

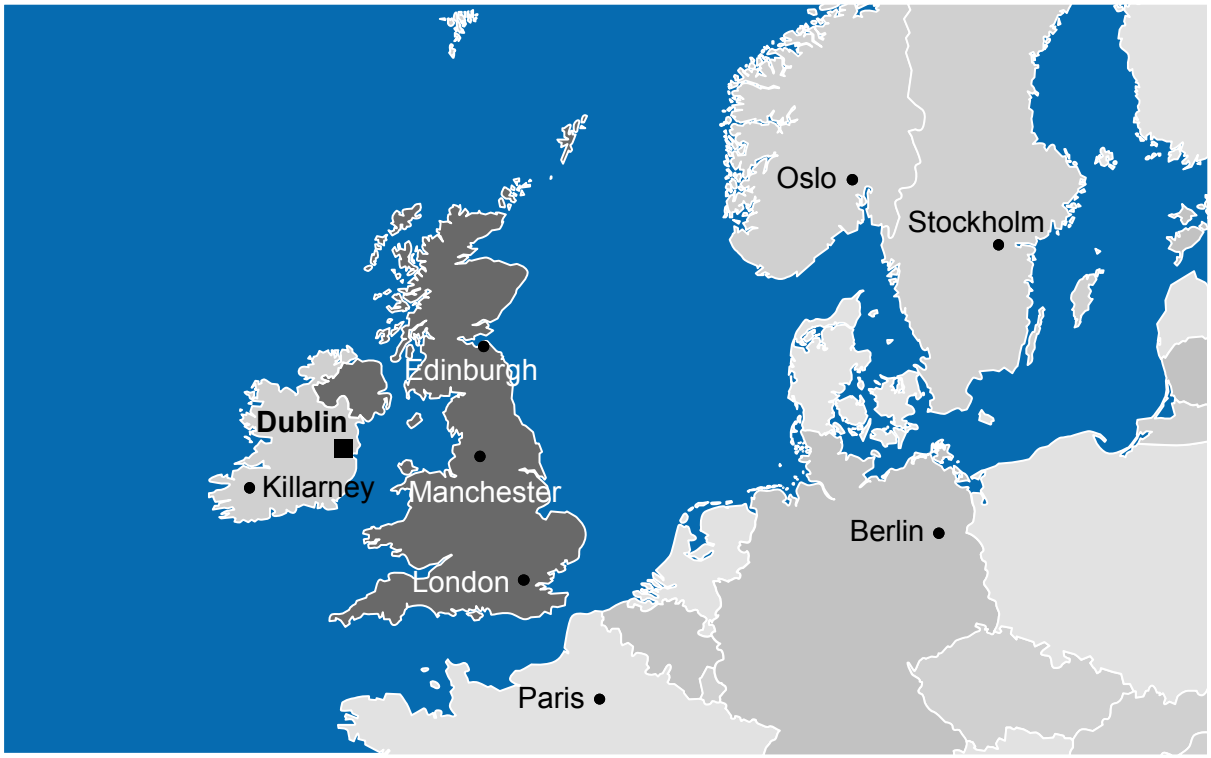


Figure 106: UK

30.1 Summary

	Organisational Model	Strategy & Policy	Methodology & Standards	Public-Private Partnership & International Collaboration	Funding & Human Resources	Training & Exercises	Sector-Specific Key Players & Initiatives
UK	▪ There is a dedicated government authority (CPNI) for delivering advice to the national infrastructure	▪ No single strategy covering all hazards ▪ National strategies are in place for security, counter-terrorism, and cyber security	▪ Methdology and plans published and recommended, but not mandated, by CPNI ▪ National Risk Register ▪ National Risk Assessment	▪ Information Exchanges and WARPs drive information sharing between public and private entities	▪ No information available	▪ Three national scale exercises every year	▪ Multiple activities across many sectors

CPNI is the Government authority that provides security advice to businesses and organisations across the national infrastructure. CPNI is an interdepartmental organisation, with resources from a number of Government departments, agencies, industry and academia. It provides integrated advice covering physical, information and personnel security.

CPNI advice is targeted primarily at the critical national infrastructure (CNI) - those key elements of the national infrastructure which are crucial to the continued delivery of essential services to the UK. Without these key elements, the essential services could not be delivered and the UK could suffer serious consequences, including severe economic damage, grave social disruption, or large-scale loss of life. According to CPNI, there are nine sectors in the national infrastructure providing essential services: communications, emergency services, energy, finance, food, government, health, transport, and water. The UK government aims to ensure that the UK is protected against attacks by terrorists or other national security threats.

In August 2008 the Government published the National Risk Register to provide an assessment of the most significant emergencies which the UK and its citizens could face over the next five years. The purpose is to help organisations, businesses, community groups and individuals to prepare to emergency situations and to encourage debate on security. The register is categorised into natural events and accidents, malicious acts and attacks.

30.2 Organisational Model

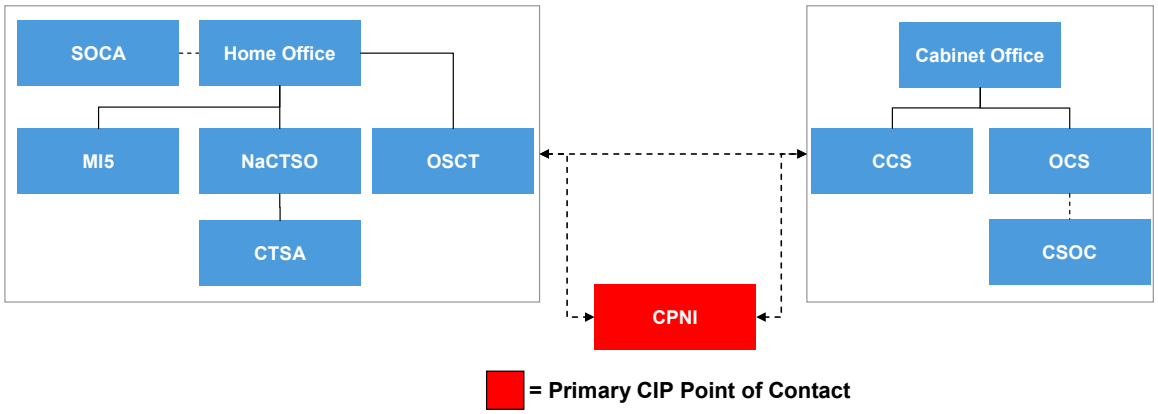


Figure 107: Organisational Chart (only CIP-related agencies shown)

Main Actors/Responsibilities:

- ***Cabinet Office (CO)***

  The Cabinet Office sits at the very centre of government and, together with the Treasury, provides the 'head office' of government.

- ***Office of Cyber Security (OCS)***[948]

  In 2009, the Cyber Security Strategy set out the Government's plans to establish this new organisation, which will be established in September 2009, and will be operational by the end of March 2010. The Office of Cyber Security (OCS) will provide strategic leadership for and coherence across Government. The OCS will establish and oversee a cross-government programme to address priority areas in pursuit of the UK's strategic cyber security objectives.

- ***Cyber Security Operations Center (CSOC)***

  In 2009, the Cyber Security Strategy set out the Government's plans to establish this new organisation, which will be established in September 2009, and will be operational by the end of March 2010. The Cyber Security Operations Centre (CSOC) will bring together existing functions: to actively monitor the health of cyber space and co-ordinate incident response; to enable better understanding of attacks against UK networks and users; and to provide better advice and information about the risks to business and the public.

- ***Civil Contingencies Secretariat (CCS)***[949]

948 http://www.cabinetoffice.gov.uk/reports/cyber_security.aspx
949 http://www.cabinetoffice.gov.uk/secretariats/civil_contingencies.aspx

The Civil Contingencies Secretariat was created in July 2001. It is the department of the British Cabinet Office responsible for ensuring the United Kingdom's resilience against disruptive challenge and it reports to the prime minister through the prime minister's security adviser. Until its creation in 2001, emergency planning in Britain was the responsibility of the Home Office. The CCS works in partnership with government departments, the devolved administrations of Scotland and Wales, and key stakeholders to enhance the preparedness to prevent and respond to emergencies. CCS has three divisions in London: horizon-scanning and response; capabilities; local response. It also has an Emergency Planning College lovated near York. It has also recently created a Natural Hazards Team responsible for work to reduce the vulnerability of critical national infrastructure to natural hazards, following the recommendations of Sir Michael Pitt following the 2007 floods.

The current objectives of CCS are:

- Ensuring to government the functioning and the delivering of services during a crisis and working with departments and the wider Cabinet Office to ensure that plans and systems cover the full range of potential disruption;
- Ensuring improved resilience of the government and the public sector, and supporting policy makers;
- Leading activities for the identification of potential threats, also with sharing of best practices with other organisations and countries;
- Improving the preparedness to respond and manage potential crisis of all levels of government, the wider public sector, and the private and voluntary sectors.

Like all Cabinet Office Secretariats, the CCS supports ministers collectively. In times of national crisis, it supports the Civil Contingencies Committee, which manages and exercises arrangements to handle national crises in the Cabinet Office Briefing Room (COBR) to deliver an integrated government response.

CCS maintains the UK Resilience website[950] with useful information and guidance (including an explanation about the roles of other Government Departments in emergencies) and also provides the public with practical information about preparing for emergencies[951].

- ***Home Office (Ministry of Interior)***[952]

  The Home Office has the overall responsibility for the counter-terrorism policy of the UK. One of the fundamental roles for the government is ensuring continuity in times of crisis. The aims are, amongst others, to protect the UK National Infrastructure and to render it more resistant to disruption and quicker able to recover without economic damage, social disruption, or large scale loss of life.

- ***Serious Organised Crime Agency (SOCA)***[953]

950 http://www.ukresilience.gov.uk/
951 http://www.preparingforemergencies.gov.uk/
952 http://www.homeoffice.gov.uk/
953 http://www.soca.gov.uk/index.html

The Serious Organised Crime Agency (SOCA) is an Executive Non-Departmental Public Body sponsored by the Home Office, but operationally independent.

SOCA is an intelligence-led agency with law enforcement powers and harm reduction responsibilities. Harm in this context is the damage caused to people and communities by serious organised crime.

The Home Secretary may set SOCA strategic priorities and will judge the success of its efforts. Within that framework, SOCA plans its priorities, including how it will exercise the functions given to it by statute, and what performance measures it will adopt.

- ***Office for Security and Counter-Terrorism (OSCT)***[954]

  The Office for Security and Counter-Terrorism leads the work under the Home Office on counter-terrorism in the UK, working closely with the police and security services. It provides advice to ministers, and develops policy and security measures to combat the threat of terrorism.

  After the attacks in the US on September 11, 2001, the number of stakeholders and partners increased and more information is made available to the public.

  The main responsibilities of the OSCT are:

  - Exercising the UK's response to a terrorist incident
  - Developing legislation on terrorism
  - Providing security measures and protection packages for public figures
  - Ensuring that the UK's critical national infrastructure is protected from attack (including electronic attack)
  - Ensuring the UK is prepared to deal with a chemical, biological, or nuclear release
  - Liaising with government and emergency services during terrorist incidents or counter-terrorism operations

- ***Centre for the Protection of National Infrastructure (CPNI)***[955]

  CPNI was born in February 2007, from the merger of the National Infrastructure Security Co-ordination Centre (NISCC) and the National Security Advice Centre (NSAC).

  The aim of CPNI is to reduce the vulnerability of the national infrastructure to terrorism and other threats, keeping the UK's essential services (delivered by the communications, emergency services, energy, finance, food, government, health, transport and water sectors) safer. The primary flow of advice out of the CPNI is directed toward operators and includes information on how best to protect the critical national infrastructure (CNI) against threats to national security infrastructure. If parts of this infrastructure were to be disrupted, the UK could suffer serious consequences,

954 http://security.homeoffice.gov.uk/
955 http://www.cpni.gov.uk/default.aspx

including severe economic damage, grave social disruption, or even large scale loss of life.

CPNI is an interdepartmental organisation, with resources from the Security Service (MI5), CESG (the UK's Government's National Technical Authority for Information Assurance) and other Government departments and agencies. It is accountable to the Director General MI5 and operates under the Security Service Act of 1989.

CPNI bases its advice from the expertise, knowledge, and information of the organisations which contribute to its work. It sponsors research and works in partnership with academia, other government agencies, research institutions, and the private sector.

CPNI advice is provided to national infrastructure businesses and organisations in a variety of ways, including face-to-face advice through teams of sector based and specialist, highly experienced advisers, training, online information, and written advisory products.

- ***Security Service (MI5)***[956]

  The Security Service (MI5) is the UK's security intelligence agency; it is responsible for protecting the United Kingdom against threats to national security (terrorism, espionage and the proliferation of weapons of mass destruction). It provides security advice to a range of other organisations, helping them reduce their vulnerability to the threats.

  The aims are therefore to:

  - Frustrate terrorism
  - Prevent damage to the UK from foreign espionage and other covert foreign state activity
  - Frustrate procurement by proliferating countries of material, technology, or expertise relating to weapons of mass destruction
  - Watch out for new or re-emerging types of threats
  - Protect Government's sensitive information and assets, and the Critical National Infrastructure (CNI)
  - Assist the Secret Intelligence Service (SIS) and the Government Communications Headquarters (GCHQ) in the discharge of their statutory functions
  - Build service capability and resilience

- ***National Counter Terrorism Security Office (NaCTSO)***[957]

  The National Counter Terrorism Security Office (NaCTSO) is a police unit co-located with the Centre for the Protection of the National Infrastructure (CPNI). It is funded by and report to the Association of Chief Police Officers (ACPO). NaCTSO contributes to

956 http://www.mi5.gov.uk/output/uk-home-page.html
957 http://www.nactso.gov.uk/

the UK government's counter terrorism strategy (CONTEST) by supporting the Protect and Prepare strands of that strategy.

30.3 Strategy & Policy

- ***Counter Terrorism Strategy (CONTEST)***[958]

  CONTEST is the UK Government's counter terrorism strategy. The key aim of the counter-terrorism strategy is to reduce the risk from international terrorism so that people can go about their business freely and with confidence. In this regard, the UK government has developed the Counter Terrorism Strategy framework, a long term strategy launched in 2003 for countering international terrorism. This strategy has four principal strands:

  Prevent

  The Prevent strand is concerned with tackling the radicalisation of individuals, both in the UK and elsewhere, which sustains the international terrorist threat.

  Pursue

  The Pursue strand is concerned with reducing the terrorist threat to the UK and to UK interests overseas by disrupting terrorists and their operations.

  Protect

  The Protect strand is concerned with reducing the vulnerability of the UK and UK interests overseas to a terrorist attack. This covers a range of issues including:

  - protecting key utilities by working with the private sector
  - strengthening border security, so that terrorists and those who inspire them can be prevented from travelling here and we can get better intelligence about suspects who travel, including improving our identity management
  - reducing the risk and impact of attacks on the transport system through security and technological advances
  - protecting people going about their daily lives in crowded places

  Prepare

  The Prepare strand is concerned with ensuring that the UK is as ready as it can be for the consequences of a terrorist attack.

- ***Cyber Security Strategy (June 2009)***[959]

  As the UK's dependence on cyber space grows, so the security of cyber space becomes ever more critical to the health of the nation. Cyber space cuts across almost all of the threats and drivers outlined in the National Security Strategy: it

958 http://security.homeoffice.gov.uk/counter-terrorism-strategy/
959 http://www.cabinetoffice.gov.uk/reports/cyber_security.aspx

affects everyone, it reaches across international borders, it is largely anonymous, and the technology that underpins it continues to develop at a rapid pace.

The threats to those who use cyber space range from phishing to enable credit-card fraud through to corporate espionage. These activities can affect organisations, individuals, critical infrastructure, and the business of government.

This Cyber Security Strategy recognises the challenges of cyber security and the need to address them. It stresses that the UK needs a coherent approach to cyber security, and one in which the Government, organisations across all sectors, the public, and international partners all have a part to play. The Strategy outlines the Government's approach and puts in place the structures that the UK needs in order to weave together new and existing work to move towards its vision:

Citizens, business and government can enjoy the full benefits of a safe, secure and resilient cyber space: working together, at home and overseas, to understand and address the risks, to reduce the benefits to criminals and terrorists, and to seize opportunities in cyber space to enhance the UK's overall security and resilience.

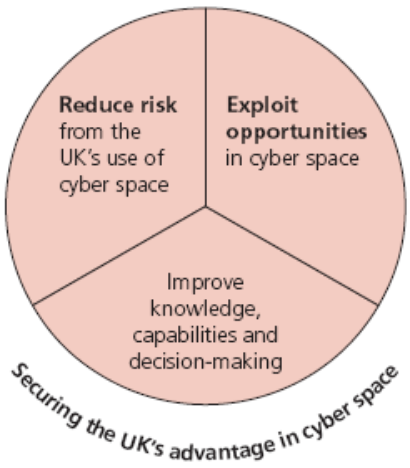


Figure 108: UK Cyber Security Strategy Objectives

The Strategy highlights the need for Government, organisations across all sectors, international partners and the public to work together to meet the UK's strategic objectives of reducing risk and exploiting opportunities by improving knowledge, capabilities and decision-making in order to secure the UK's advantage in cyber space.

Figure 109: Securing the UK's Advantage in Cyber Space

The Government, in conjunction with industry, already undertakes a range of high quality activity in the field of cyber security. However, the challenges are such – and cyber security is so important – that this needs to be developed further. One of the principal aims of this Strategy is to bring greater coherence to the UK's cyber security work, by setting up two new organisations that will bring together the expertise and advice to meet this objective.

Figure 110: Addressing the UK's Cyber Security Challenges

- ***CNI Protection in the United Kingdom, Framework and Guidance***

  CPNI's Framework and Guidance document sets out the UK's approach for protective security of critical national infrastructure. The framework covers the definitions and criteria used to distinguish between 'critical' infrastructure and wider national infrastructure; the national approach to managing risks and prioritising effort; and the roles and responsibilities of different government bodies. It is intended to provide clarity and a common foundation for activity by all those in government involved in national infrastructure protection.

  The framework sets out what is meant by the terms 'national infrastructure' and 'critical national infrastructure' (CNI) as they relate to the UK. In the context of the UK's response to security threats, its understanding of national infrastructure is focused around the concept of essential services. The national infrastructure is viewed as comprising those facilities, systems, sites, and networks necessary for the delivery of the essential services upon which daily life in the UK depends and which ensure the country continues to functions socially and economically. There are nine national infrastructure sectors which provide these essential services. The UK's infrastructure protection effort is organized into these nine sector streams. Activity may also be driven forward on cross-cutting themes such as 'space' wherein there may be infrastructure which supports the delivery of essential services across a number of sectors, or 'personal security' which will be important to improving security across all of the sectors, but these are not recognised as national infrastructure sectors in their own right. The nine national infrastructure sectors are further broken down into sub-sectors as follows:

National Infrastructure Sector	Sub Sector	Whitehall Sector Sponsor Dept
Communications	Telecommunications	BIS
	Postal Services	BIS
	Broadcast	DCMS
Emergency Services	Ambulance	DH
	Fire & Rescue	DCLG
	Marine	DfT
	Police	HO
Energy	Electricity	DECC
	Gas	DECC
	Fuel	DECC
Finance	Payment, Clearing, & Settlement Systems	HMT
	Markets & Exchanges	HMT
	Public Finances	HMT
Food	Production	DEFRA & FSA
	Processing	
	Import	
	Distribution	
	Retail	
Government	Central Government	CO
	Devolved Administrations/ Functions:	
	Regional & Local government	DCLG
	Parliament	Palace of Westminster
Health	Health & Social Care	DH
Transport	Aviation	DfT
	Maritime	DfT
	Land	DfT
Water	Potable Water Supply	DEFRA
	Waste Water Services	
	Dams	

Figure 111: UK National Infrastructure Sectors and Sub-Sectors

30.4 Methodology & Standards

- **National Risk Register**[960]

  In August 2008 the Government published the National Risk Register to provide an assessment of the most significant emergencies which the UK and its citizens could face over the next five years. It is set out in categories relating to natural events and accidents, malicious acts and attacks and its purpose is to help businesses, organisations, community groups and individuals prepare for emergencies as well as encouraging public debate on security.

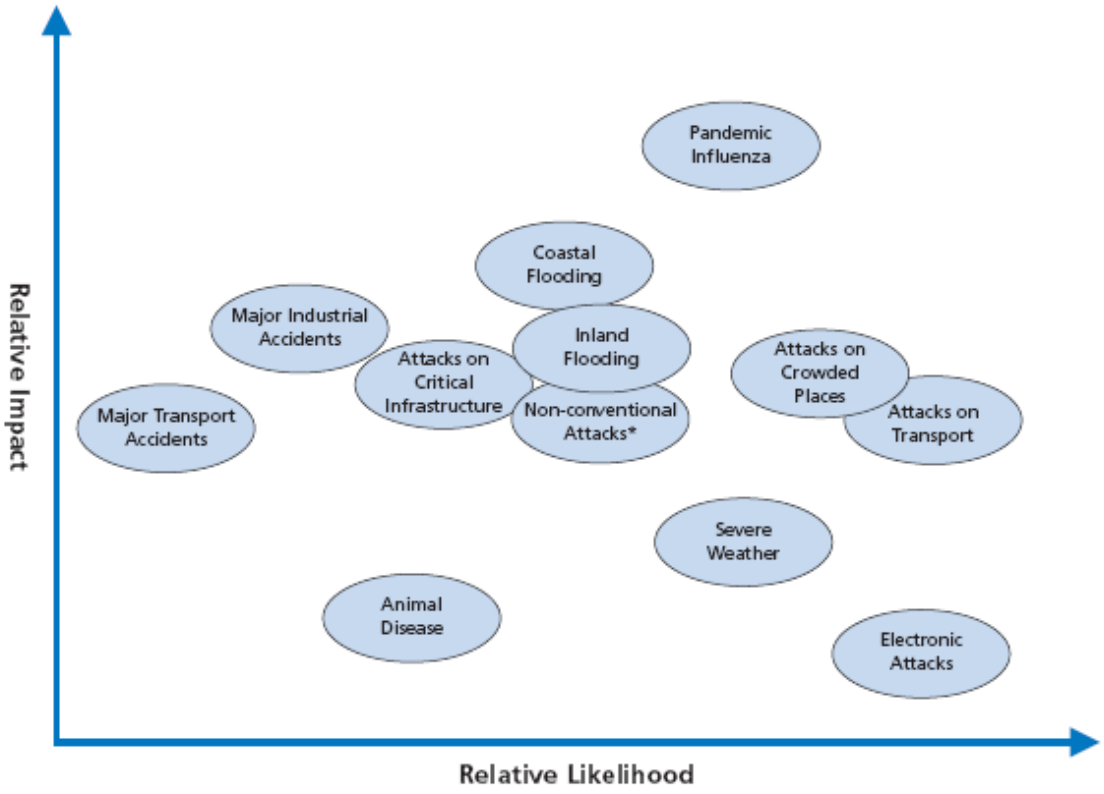
  It provides a national picture of the risks the UK faces, and is designed to complement Community Risk Registers, already produced and published locally by emergency planners. The driver for this work is the Civil Contingencies Act 2004, which also defines emergencies, and what responsibilities are placed on emergency responders in order to prepare for them.

  Understanding the risks and determining their relative significance in terms of potential impact is the starting point for emergency planning. The key to turning this into useful planning information is remembering that it is not the risks themselves that people have to deal with when things go wrong, but their consequences. In an increasingly complex and interdependent society, emergencies can have increasingly complex knock-on effects. The Register identifies both direct and indirect consequences, many of which are common to several risks, and provides information on how to prepare for them.

  Figure 3 gives an indication of the relative likelihood and impact of the high consequence risks that are outlined in the National Risk Register. Due to the nature of the risks contained within each grouping, it is not possible to represent an exact comparison but only to give an idea of the position of each group of risks relative to the others, in terms of likelihood and impact.

  It is also important to highlight that the risks shown in Figure 3 are not the full range of possible risks to the UK, from the insignificant to the catastrophic. They are those risks that are deemed significant enough for inclusion due to their likelihood or impact or both.

960 http://www.cabinetoffice.gov.uk/reports/national_risk_register.aspx



* The use of some chemical, biological, radiological and nuclear (CBRN) materials has the potential to have very serious and widespread consequences. An example would be the use of a nuclear device. There is no historical precedent for this type of terrorist attack which is excluded from the non-conventional grouping on the diagram.

Figure 112: Illustration of the High Consequence Risks Facing the UK

The UK Government does not expect individuals or communities to tackle any of the risks described in the Register on their own. In all cases, the Government is working to reduce the risks to the UK from civil emergencies, ranging from a flu pandemic and serious flooding, to international terrorism. It also aims to provide an effective response where emergencies cannot be prevented from happening.

The National Risk Register is for those who may want to improve their own preparedness:

Chapter Two of the Register provides a summarised assessment of the groups of risks, based on those contained within the National Risk Assessment. Each risk grouping includes a section on further information sources for anyone who wants to find out more about a particular risk and what can be done do to prepare for it.

Chapter Three of the Register provides further guidance for organisations in the public, private and voluntary sectors interested in business continuity planning. This sets out business continuity planning considerations which are designed to complement business continuity planning under the British Standard (BS 25999).

Chapter Four of the Register provides suggestions for members of the public interested in individual, family or community based emergency preparedness.

Chapter Five illustrates how the Government carries out risk assessment, and how the National Risk Assessment is created.

- **National Risk Assessment**

Since 2005, the UK Government has carried out a classified assessment of the risks facing the United Kingdom: this is the National Risk Assessment (NRA), and it is the basis for the public National Risk Register.

The NRA process uses historical and scientific data and the professional judgements of experts to analyse the risks to the UK. There are three stages to this analysis:

- identification of risks;
- assessment of the likelihood of the risks occurring and their impact if they do;
- and comparison of the risks.

Identifying risks

The first stage in the National Risk Assessment process is to identify the risks. This is done by consulting a wide range experts across government, so as to ensure a comprehensive picture of the potential accidents, natural events (hazards) and malicious attacks (threats) that could cause significant harm and disruption to the UK.

Assessing risks

The next stage is to assess the likelihood and impact of each risk. To assess the likelihood of hazards, historical, statistical and scientific data are used. Where possible, the assessment looks forward to take account of known or probable developments over the next five years that would affect the likelihood.

The likelihood of terrorist or other malicious attacks is assessed more subjectively. The willingness of individuals or groups to carry out attacks is balanced against an objective assessment of their capacity – now and, as far as possible, over the next five years – and the vulnerability of their intended targets.

In each case, the question being asked is: how likely is it that this type of emergency will happen, somewhere in the country, sometime over the next five years. The NRA does not calculate the chances of these events happening in one particular place, or to one particular community or individual.

In terms of impact, the National Risk Assessment takes account of the following effects:

- **The number of fatalities** that are directly attributable to the emergency

- **Human illness or injury**, over a period following the onset of an emergency
- **Social disruption** – the disruption to people's daily lives. Ten different types of disruption are taken into account, from an inability to gain access to healthcare or schools, to interruptions in supplies of essential services like electricity or water, to the need for evacuation of individuals from an area.
- **Economic damage** – the effect on the economy overall, rather than the cost of repairs.

In addition, the National Risk Assessment (but not – at present at least – Community Risk Registers) also attempts to estimate the psychological impact that emergencies may have. This includes the anxiety, loss of confidence or outrage that may be felt by communities throughout the country as a result of an emergency, or widespread changes to patterns of behaviour.

Comparison of the risks

In planning for emergencies, local responders have to decide what types of risk, and what levels of consequence, to plan for. Putting a lot of effort into preparing for risks that are either very unlikely to happen, or are likely to cause relatively minor damage, is unlikely to be the best use of the time available to prepare. Priority is instead given to high risks: risks that are both relatively likely and could have a serious impact.

Apart from identifying the highest risks, the Government also provides guidance at national level and to LRFs called planning assumptions, on the range and type of damage and disruption that might result from a selection of the higher risks. This ensures that planning is mostly non-specific and can be adapted to different scenarios when necessary.

Different types of planning assumptions are needed by different groups. • For emergency responders, and regional and local Government, to help them plan for and carry out their duties in an emergency. Planning assumptions are issued to provide information, for example on the numbers of casualties that might need treating, or how many people might need to be evacuated or found shelter. These are on a restricted distribution because some of the information they contain is classified for national security reasons.

- ***CPNI Good Practices Guidelines and Archive***[961]

A key CPNI objective is to promote best practice among operators of the national infrastructure. CPNI encourages improving technical standards - and increasing protection against electronic attack - by looking at the experience of others and drawing from their lessons. Guidance can also be enhanced by the findings of research work, as well as the general day-to-day experiences of professionals in the field. The Good Practices publications therefor include guidelines produced by CPNI experts, in collaboration with, for example, members of Information Exchanges.

961 http://www.cpni.gov.uk/Products/guidelines.aspx

CPNI also offers other products and services for the protection of the operators of the national infrastructure including:

- CSIRTUK Advisories
- General Protective Security publications
- InfoSec Technical Notes
- InfoSec vulnerability disclosures
- Good practice guidelines
- Viewpoints
- Information Exchanges

- ***CPNI Security Planning***[962]

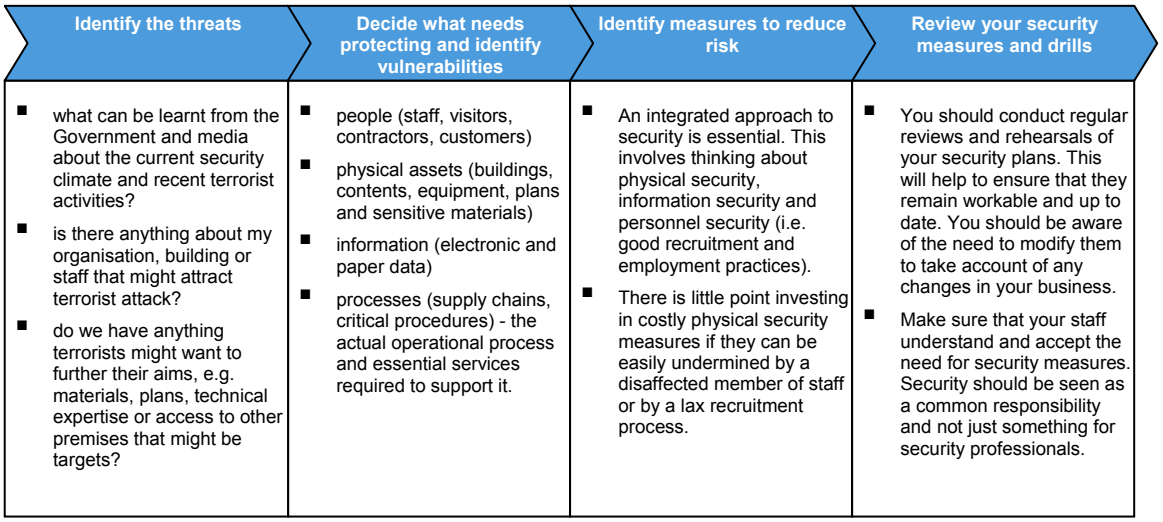
  CPNI has published a series of guides devoted to security planning that contain information on how to protect organisations including:

  - Why security planning is important
  - Risk assessment
  - Creating security plans
  - Handling bomb threats
  - Search planning
  - Mail and deliveries
  - Evacuation planning
  - Business continuity planning

  For example, the Risk Assessment guide[963] helps organisations decide on the threats they might be facing and their likelihood, identify vulnerabilities, and evaluate the potential impact of exploitation.

  The steps identified include:

962 http://www.cpni.gov.uk/securityplanning.aspx
963 http://www.cpni.gov.uk/SecurityPlanning/3305.aspx



Identify the threats	Decide what needs protecting and identify vulnerabilities	Identify measures to reduce risk	Review your security measures and drills
▪ what can be learnt from the Government and media about the current security climate and recent terrorist activities? ▪ is there anything about my organisation, building or staff that might attract terrorist attack? ▪ do we have anything terrorists might want to further their aims, e.g. materials, plans, technical expertise or access to other premises that might be targets?	▪ people (staff, visitors, contractors, customers) ▪ physical assets (buildings, contents, equipment, plans and sensitive materials) ▪ information (electronic and paper data) ▪ processes (supply chains, critical procedures) - the actual operational process and essential services required to support it.	▪ An integrated approach to security is essential. This involves thinking about physical security, information security and personnel security (i.e. good recruitment and employment practices). ▪ There is little point investing in costly physical security measures if they can be easily undermined by a disaffected member of staff or by a lax recruitment process.	▪ You should conduct regular reviews and rehearsals of your security plans. This will help to ensure that they remain workable and up to date. You should be aware of the need to modify them to take account of any changes in your business. ▪ Make sure that your staff understand and accept the need for security measures. Security should be seen as a common responsibility and not just something for security professionals.

Figure 113: Selected Text from Risk Assessment Guide

30.5 Public – Private Partnership & International Collaboration

- ***Information Exchanges***[964]

  The sharing of information about the risks facing networks is self evidently beneficial to both government and industry. If a mechanism can exist through which one company can learn from the experiences, mistakes, and successes of another, without fear of exposing company sensitivities to competitors and the media, then every participant can improve their level of assurance.

  Information Exchanges are based upon the personal trust of representatives, sharing information in a confidential meeting, run under a version of the Chatham House Rule. Trust is built up slowly; representatives at Information Exchanges are expected to attend all meetings, which are held every two months. Meeting face-to-face, we are building up a trusted, relatively small community with a common interest. Each organisation can put forward a maximum of two representatives, and cannot send substitutes to attend; a stranger turning up at a meeting would inhibit the sharing of sensitive information.

  Information Exchanges utilize the following basic structure:

  - Trusted group of industry and government representatives
  - Discuss security incidents and vulnerabilities
  - Rules of membership
  - No cost to members
  - Members per organisation
  - Cannot delegate

964 http://www.cpni.gov.uk/Products/information.aspx

- Information sharing protocol

The current portfolio of Information Exchanges includes:

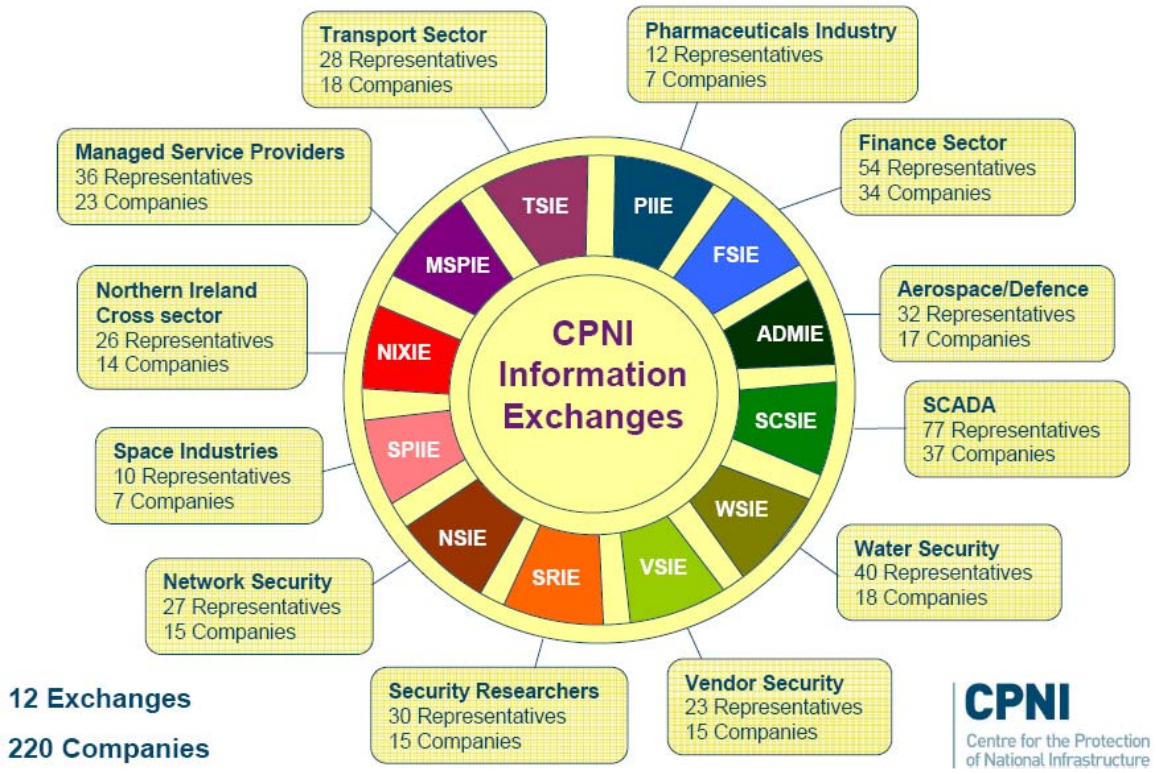


Figure 114: Current Portfolio of Information Exchanges

In addition to the Information Exchanges facilitated by CPNI, other exchanges will be set up, both in the UK and internationally. CPNI is creating channels through which information in one Information Exchange is passed to others; a channel exists between the UK and US Network Security Information Exchanges.

- ***Warning, Advice, and Reporting Point (WARP)*** [965]

  A WARP is a small, not-for-profit, community-based service where members can receive and share up-to-date advice on information security threats, incidents and solutions. A WARP is set up to provide a service to members of a community. It is run by a WARP operator who understands the information security needs of its members. The operator will typically:

  - filter relevant information and deliver it to the community

965 http://www.warp.gov.uk/index.htm

- facilitate the sharing of advice and best practice within the members of that community. This will help build trust within the community thereby encouraging members to report incidents to each other
- anonymise these reports and may share them with other WARPs

There will usually be between 20 and 100 members belonging to a *community* (small businesses, local government, service providers, interest groups etc etc).

The operator uses a website, email, telephone, SMS, and occasional meetings (where possible) to send a personalised service of warnings and advice to the members. This will be mainly IT security advice, but can include other material (other threats, e-crime, contingency planning etc) as well.

The Operator also taps into the knowledge of the members themselves to help out other members using a bulletin board, meetings and general communication skills.

A successful WARP will build up enough trust to encourage members to talk about their own incidents & problems, anonymously, for the benefit of the rest.

- ***Combined Security Incident Response Team (CSIRT)*** [966]

The Combined Security Incident Response Team (CSIRTUK) is a CERT for CPNI partners in the private sector who operate in the national infrastructure. This service advises how to manage the response to incidents and produces advisories on security matters.

An important part of security risk management is to learn from the experiences of others. Accordingly, via CSIRTUK, CPNI aims to hear about potential security vulnerabilities, incidents or events, whether in the electronic, physical or personnel security spheres from national infrastructure organisations. This information will be treated as confidential, and if necessary, particulars that would identify individuals or organisations will be removed so the information can be incorporated into generic security advice. In this way, valuable experience can be shared to help others.

By enhancing the traditional CERT role to cover holistic advice - covering physical, personnel and electronic issues - CSIRTUK provides a central point for reporting security incidents and for receiving advice and guidance.

- ***Meridian Process*** [967]

The Meridian process, launched by the UK, aims to provide governments worldwide with a means by which they can discuss how to work together at the policy level on critical information infrastructure protection (CIIP). An annual conference and interim activities is held each year to help build trust and establish international relations within the membership to facilitate sharing of experiences and good practices on CIIP from around the world. Participation in the Meridian process is open to all countries and aimed at senior government policy-makers. The Meridian process is founded on the G8 principles that provide a basic framework for understanding and implementing

966 http://www.cpni.gov.uk/Products/advisories.aspx
967 http://meridianprocess.org/

CIIP measures. As new challenges of connectivity and dependencies arise beyond national borders, Meridian enables Governments to explore the benefits and opportunities of cooperation with the private sector, and exchange of information and good practices in CIIP between governments internationally. Tools to raise awareness and share information include the CIIP Directory to facilitate intergovernmental contacts and the Traffic Light Protocol to facilitate distribution of information.

30.6 Funding & Human Resources

There is no publicly available information regarding CPNI funding and human resource data.

30.7 Training & Exercises

- ***CPNI Products and Services***[968]

  CPNI offers a wide range of internal and external training opportunities. Their products and services also include a variety of instruments aimed at sharing knowledge and raising the general awareness level in the UK around Critical Infrastructure Protection issues:

  CSIRTUK Advisories: advisories that contain details of potential security problems that should be acted upon accordingly

  General Protective Security Publications: CPNI publishes a range of documents designed to provide clear and concise advice

  InfoSec Briefings: CPNI's information security briefings comprise a range of general interest documents which highlight risks faced by the national infrastructure

  InfoSec Technical Notes: CPNI's technical notes offer practical advice on dealing with topical issues, aimed at information security professionals

  InfoSec Vulnerability Disclosures: CPNI undertakes research into computer vulnerabilities to determine the threats, identify problems, and work with vendors to provide software patches

  Good Practice Guidelines: CPNI promotes best practice amond operators of the national infrastructure, reflecting its commitment to information sharing

  Viewpoints: CPNI's Viewpoint papers provide an overview of emerging technologies and other issues facing the IT sector

  Information Exchanges: Sharing information about the risks facing networks is beneficial to both government and industry

968 http://www.cpni.gov.uk/productsServices.aspx

- ***Defence Science and Technology Laboratory (DSTL)*** [969].

  The DSTL (agency of the Ministry of Defence) supplies scientific and technical research and advice to the Ministry of Defence to ensure that the best science and technology solutions are available to underpin the UK's defence and security capability.

- ***The Home Office National Counter-Terrorism Exercise Programme***[970].

  To manage and practice handling potential crises (including terrorism, natural disaster and other major accidents), the government and emergency services organizations regularly practice the Counter-Terrorism Exercises. The aims of this programme are to test UK's ability to respond to terrorist incidents and to identify ways of improving the response.

  The programme includes:

  - Three annual large-scale live exercises, involving police forces and other government departments and agencies
  - Strategic-level decision-making by senior government officials
  - Paper exercises where decisions are explored, rather than played out

  During exercises participants respond to a scenario as though the events are really happening: they are given no warning of what the scenario will be before it begins. Exercises (especially live exercises) take months of planning to ensure the situation is as realistic and challenging as possible.

  Government departments, emergency services, the military, local authorities and health providers, scientists and technical specialists can be involved in each exercise.

- ***Cyber Storm 2***[971]

  In March 2008, the US Department of Homeland Security's National Cyber Security Division (NCSD) sponsored its second large-scale national cyber exercise, Cyber Storm II. Planned in close coordination with and driven by its stakeholders and participants, the exercise centered on a cyber-focused scenario that escalated to the level of a cyber incident requiring a coordinated Federal response. Cyber Storm II is part of Homeland Security's ongoing risk-based management effort to use exercises to enhance government and private sector response to a cyber incident, promote public awareness, and reduce cyber risk within all levels of government and the private sector.

  Cyber Storm II included 18 federal departments and agencies, nine US states, four other countries - Australia, Canada, New Zealand, and the UK - and more than 40

969 http://www.dstl.gov.uk/
970 http://security.homeoffice.gov.uk/responding-terrorist-incident/national-response/exercise-programme/
971 http://www.us-cert.gov/reading_room/infosheet_CyberStormII.pdf

private companies. These include ABB, Air Products, Cisco, Dow Chemical Company, Harris Corporation, Juniper Networks, McAfee, Microsoft, NeuStar, PPG Industries and Wachovia.

30.8 Sector – Specific Key Players & Initiatives

COMMUNICATIONS

Public authorities:

- **Department for Business, Innovation and Skills (BIS)**[972]

  The Department for Business, Enterprise and Regulatory Reform is a UK government department created on 28 June 2007 on the disbanding of the Department of Trade and Industry (DTI). The main responsibilities are Company Law, Trade, Business Growth, Employment Law, Regional Economic Development, and Consumer Law. The principal machinery of government changes affecting the department on creation were the removal of the Office of Science and Innovation to the new Department for Innovation, Universities and Skills and the arrival of the Better Regulation Executive from the Cabinet Office. Subsequently, in October 2008, responsibility for energy policy was removed to the new Department of Energy and Climate Change.

- **Department for Culture, Media, and Sport (DCMS)**[973]

  The DCMS aims to maintain, support, and protect a dynamic media, extending the benefits of the digital revolution to all UK citizens and promoting strong public service broadcasting.

  It strives to take account of the views and interests of the UK citizen in its decision-making as the Government Department with responsibility for the BBC Charter review, the self regulation of the press, and - jointly with the Department for Business, Innovation and Skills (BIS) - for digital TV switchover.

Initiatives:

- **Cyber Security Strategy 2009**[974]

  The Government has published its first national Cyber Security Strategy alongside the annual update of the National Security Strategy.

  The Cyber Security Strategy refers to cross-Government partnership with business, international partners and the public on cyber security and announces the establishment of an Office of Cyber Security and a Cyber Security Operations Centre.

  CPNI is highlighted in the strategy as one of the organisations that interface on cyber security and as an example of partnership working with industry.

972 http://www.berr.gov.uk/whatwedo/energy/index.html
973 http://www.culture.gov.uk/about_us/default.aspx
974 http://www.cabinetoffice.gov.uk/reports/cyber_security.aspx

- ***Information Assurance Advisory Council (IAAC)***[975]

  IAAC is a public-private forum that brings together corporate leaders, public policy makers, law enforcement and the research community to address the challenges of information infrastructure protection. It develops policy recommendations to government and corporate leaders at the highest levels. The recommendations are influential because IAAC's Sponsors and Members comprise leading commercial end-users, government policy makers and the research community.

  IAAC aims to work for the creation of a safe and secure Information Society. It is a unique, not for profit body with high level support from government and industry backed by world class research expertise.

- ***National Information Assurance Strategy***[976]

  The National Information Assurance Strategy was produced by Information Security and Assurance (IS&A), a unit within the Cabinet Office The objective of this strategy is to provide ongoing assurance to the government that the risks to information systems and the information they hold are appropriately managed.

  Other partner organisations, in collaboration with the IS&A, collaborate to deliver strategy's recommendations, and the IS&A coordinates and sponsor work programs.

  The IS&A has a lead role in helping governments to improve Information Assurance. This is possible through enabling the government to deliver public services through the appropriate use of ICT, protecting information systems from risks, improving economic and social well-being realising the full benefits of ICT by governments, businesses and citizens.

- ***Government Data Security***[977]

  A number of recommendations on data handling procedures have been accepted by the government after a data security incident in November 2007, when the prime minister asked the Cabinet Office to review procedures in all departments.

  The aim of the present and future recommendation is to enhance transparency, increase monitoring, improve guidance and mandatory training.

  A number of other reviews are being commissioned across the UK government that will have an effect on data.

- ***NSIE***

  The UK Network Security Information Exchange (UK-NSIE) was formed in April 2003 to share sensitive information in the information and communications technologies sector. It currently includes IP providers; core mobile operators; and traditional telecommunications providers, as well as CPNI. Participating

975 http://www.iaac.org.uk/
976 http://www.cabinetoffice.gov.uk/csia/national_ia_strategy.aspx
977 International CIIP Handbook 2008/2009, Elgin M. Brunner and Manuel Suter

companies now cover over 80% of the telecommunications market in the UK. It is linked to NSIE in USA, of which BT is a member. BT acts as the channel for information between the two Exchanges. Under the aegis of the NSIE, a number of working groups have been established, and several guidance documents and technical papers have been produced. These include: a guide to the procurement of resilient telecoms; best practice guidance on the secure implementation of BGP.

- ***PITCOM (Parliamentary Information Technology Committee)***[978]

  PITCOM was founded in 1981 to provide a bridge between Parliament and the IT industry. The Committee is an associate Parliamentary Group, complying with House of Commons rules for all-party groups. Its administration is funded by members' annual subscriptions. PITCOM addresses the public policy issues generated by ICT and their application across the public and private sectors of the UK economy.

- **VSIE**

  The Vendor Security Information Exchange (VSIE) was formed in January 2005 to share confidentially mutually beneficial information regarding electronic security threats among the major companies involved in the ICT industry. The VSIE comprises members of major international companies in the ICT sector.

EMERGENCY SERVICES

Public authorities:

- **Department of Health (DH)**

  The Department of Health is responsible for health protection, health improvement, and health inequalities issues in the UK, including pandemic influenza, seasonal flu, patient safety, tobacco, obesity, drugs, sexual health, and international health. It provides health and social care policy, guidance and publications for NHS and social care professionals.

- **Department of Communities and Local Government (DCLG)**

  DCLG works with local fire and rescue authorities to help prevent deaths, injuries, and damage to property. They also work in partnership with the Fire and Rescue Service and other agencies to build the resilience and capability to deal with major emergencies, including terror attacks and natural disasters.

- **Department for Transport (DfT)**

  The Department for Transport provides leadership across the transport sector to achieve its objectives, working with regional, local and private sector partners to deliver many of the services. The Maritime and Coast Guard Agency's responsibility includes co-ordinating search and rescue at sea through Her Majesty's Coastguard, and checking that ships meet UK and international safety

978 http://www.pitcom.org.uk

rules. It works to prevent the loss of lives at the coast and at sea, to ensure that ships are safe, and to prevent coastal pollution.

- **Home Office (HO)**

  The Home Office has the overall responsibility for the counter-terrorism policy of the UK. One of the fundamental roles for the government is ensuring continuity in times of crisis. The aims are, amongst others, to protect the UK National Infrastructure and to render it more resistant to disruption and quicker able to recover without economic damage, social disruption, or large scale loss of life.

ENERGY

Public authorities:

- **Department for Energy and Climate Change (DECC)**[979]

  The Department for Energy and Climate Change is a UK government department created on 28 June 2007 on the disbanding of the Department of Trade and Industry (DTI). The main responsibilities are Company Law, Trade, Business Growth, Employment Law, Regional Economic Development, and Consumer Law. The principal machinery of government changes affecting the department on creation were the removal of the Office of Science and Innovation to the new Department for Innovation, Universities and Skills and the arrival of the Better Regulation Executive from the Cabinet Office. Subsequently, in October 2008, responsibility for energy policy was removed to the new Department of Energy and Climate Change.

Initiatives:

- ***SCSIE*** [980]

  The SCADA and Control Systems Information Exchange, facilitated by CPNI, are for those companies that are dependent upon SCADA (Supervisory Control and Data Acquisition) or other process control or telemetry systems. Formed in October 2003, it shares confidential and mutually beneficial information regarding electronic security threats, vulnerabilities, incidents and solutions in the SCADA and process control environment. The SCSIE includes members from UK-based energy, transport and water companies. It has produced and is currently working on good practice guidance. Completed guidance includes: Implement secure architecture, understanding business risk, firewall deployment for SCADA, process control networks, and others.

FINANCE

Public authorities:

- ***Her Majesty's Treasury (HMT)***[981]

979 http://www.berr.gov.uk/whatwedo/energy/index.html
980 http://www.cpni.gov.uk/Products/information.aspx

HM Treasury, in full Her Majesty's Treasury, is the United Kingdom government department responsible for developing and executing the British government's public finance policy and economic policy.

Initiatives:

- ***FSIE***

  The UK Financial Services Information Exchange was formed in February 2003, to share confidentially mutually beneficial information regarding electronic security threats, vulnerabilities, incidents and solutions in the UK financial sector. The FSIE includes members from UK-based financial organisations including banking, insurance, securities, service providers, exchanges and CPNI.

FOOD

Public authorities:

- ***Department for Environment, Food and Rural Affairs (DEFRA)***[982]

  The Department for Environment, Food and Rural Affairs is a UK Government Department that aims to secure a healthy environment.

  Defra helps people to adapt to changes, deals with environmental risks and makes the most of the opportunity we now have to secure a sustainable society and a healthy environment.

- ***Food Standards Agency (FSA)***[983]

  The Food Standards Agency is a non-ministerial government department of the Government of the UK created in 2000. It is responsible for protecting public health in relation to food throughout the United Kingdom and is led by an appointed board that is intended to act in the public interest. The Meat Hygiene Service and, more recently, the Wine Standards Board are branches of the Food Standards Agency.

GOVERNMENT

Public authorities:

- ***Cabinet Office (co)***

  The Cabinet Office sits at the very centre of government and, together with the Treasury, provides the 'head office' of government.

- **Department of Communities and Local Government (DCLG)**

  DCLG works with local fire and rescue authorities to help prevent deaths, injuries, and damage to property. They also work in partnership with the Fire and Rescue

981 http://www.hm-treasury.gov.uk/
982 http://www.defra.gov.uk/
983 http://www.food.gov.uk/

Service and other agencies to build the resilience and capability to deal with major emergencies, including terror attacks and natural disasters.

HEALTH

Public authorities:

- ***Department of Health (DH)***[984]

  The Department of Health (DH) is a department of the United Kingdom government with responsibility for government policy for England on health, social care and the National Health Service (NHS). It is led by the Secretary of State for Health with two Ministers of State and three Parliamentary Under-Secretaries of State.

  In the other countries of the United Kingdom, responsibility for health and the management of their National Health Services falls under the jurisdiction of the devolved governments, namely:

  - The Department of Health, Social Services and Public Safety of the Northern Ireland Executive
  - The Scottish Government Health and Wellbeing Directorate
  - The Welsh Assembly Government

TRANSPORT

Public authorities:

- **Department for Transport (DfT)**

  The Department for Transport provides leadership across the transport sector to achieve its objectives, working with regional, local and private sector partners to deliver many of the services.

Initiatives:

- ***ADMIE***

  The Aerospace and Defence Manufacturer's Information Exchange was formed in December 2006, to share confidentially mutually beneficial information regarding electronic security threats in the aerospace and defence sector. The ADMIE comprises UK-based organisations involved in this sector.

- ***TSIE***

  The Transport Sector Information Exchange was formed in September 2006 and expanded coverage of the aviation sector Information Exchange to include other major transport methods.

984 http://www.dh.gov.uk/en/index.htm

WATER

Public authorities:

- ***Department for Environment, Food and Rural Affairs (DEFRA)***[985]

  The Department for Environment, Food and Rural Affairs is a UK Government Department that aims to secure a healthy environment.

  Defra helps people to adapt to changes, deals with environmental risks and makes the most of the opportunity we now have to secure a sustainable society and a healthy environment.

985 http://www.defra.gov.uk/

31 Worldwide CIP Research Report

31.1 R&D ACTIVITIES OUTSIDE EU COUNTRIES

31.1.1 Summary

This chapter describes some of the CIP Research and Development (R&D) activities being undertaken outside the EU. It seeks to identify which are the main institutions that are supporting R&D activities in the CIP framework, the strategic plans developed by different governments where they exist, the most active research groups, and the most significant projects being undertaken.

Specific attentions has been given to the following topics playing key roles in the development of the EPCIP programme:

- early warning;
- information sharing;
- sectoral interdependencies, and
- modelling and simulation.

These, in many regards, are considered the areas where innovation is most likely to lead to significant improvement in CI protection. However, the analysis has not been limited exclusively to these topics, and also includes other relevant CIP research activities.

Specifically, the analysis emphasised the global interest in studying interdependencies. This “new” phenomena is generally studied using simulation approaches as these methods are considered best suited for managing the huge complexity of the subject. There is also the need to improve the interoperability of simulation platforms initially developed for the study of like types of infrastructure. Of note, is that inter-dependent impact analysis has been accepted as a mandatory task in several countries during the planning of CIP recovery, contingency, and emergency preparedness strategies.

Another topic of interest is cyber-security, with a specific focus on early-warning systems, information sharing, and on the protection of Supervisory, Control and Data Acquisition (SCADA) systems.

Another active field of research is the prevention and detection of Chemical, Biological, Radiological-Nuclear and Explosive (CBRNE) threats. The focus of this research includes the development of instruments and methodologies to detect such agents, to design infrastructure which is more robust against these types of attack, and to improve the responsiveness of the capabilities who react to such attacks.

The final section summarises a range of authoritative academic journals and conferences, the monitoring of which could provide useful insights into R&D trends and results.

It is important to stress that the research described in this report is not an exhaustive survey of the R&D activities performed in the different countries, but a selection of those

that appear the most aligned with the goals of the project and the development of the EPCIP programme.

31.1.2 United States

The United States is undertaking many programs to improve research activities in the field of international security, and for CIP specifically.

The ***Homeland Security Advanced Research Project Agency (HSARPA)***[986] engages industry, academia, government, and other sectors in innovative research and sponsors development, rapid prototyping, and technology transfer to meet operational needs. HSARPA is funded by the Department of Homeland Security(DHS).[987]

These activities are complemented by those sponsored by the National Science Foundation (NSF)[988]. With an annual budget of approximately US$6 billion (fiscal year 2008), the NSF funds approximately 20 percent of all federally-supported basic research conducted by the United States' colleges and universities.

The **Critical Infrastructure Protection Directive (PDD-63)**[989] of May 22, 1998, calls for a national effort to ensure the security of the vulnerable and increasingly interconnected infrastructure of the United States. Such infrastructures include telecommunications, banking and finance, energy, transportation, and essential government services. The directive requires immediate federal government action, including risk assessment and planning to reduce exposure to attack. It stresses the critical importance of cooperation between the government and the private sector, and seeks to link designated agencies with private sector representatives.

The ***National Plan for Research and Development In Support of Critical Infrastructure Protection***[990] was released in 2004 by the Office of Science and Technology Policy and the DHS Science and Technology Directorate. It identifies several priorities:

- *Improve Sensor Performance* – Develop improved physical and cyber monitoring and detection systems that will include enhancements in speed, fewer false-positive readings, reduced power requirements, increased durability, and lower cost.
- *Advance Risk Modelling, Simulation, and Analysis for Decision Support* – Improved capabilities in this area will address all critical infrastructure sectors and their interdependencies. Create computer models and algorithms accessible to owners and operators of critical infrastructure that are interoperable and use common inputs and assumptions.
- *Improve Cyber Security* - Develop new methods for protection from, automated detection of, response to, and recovery from attacks on critical information infrastructure systems

[986] http://www.dhs.gov/xres/grants/gc_1247254578009.shtm
[987] www.dhs.gov
[988] www.nsf.gov
[989] http://www.usdoj.gov/criminal/cybercrime/white_pr.htm
[990] http://www.dhs.gov/xlibrary/assets/ST_2004_NCIP_RD_PlanFINALApr05.pdf

- *Improve Prevention and Protection* – Develop new, low-cost physical perimeter and area defence systems for critical infrastructure sectors, including systems to mitigate high explosive blast, projectile, and fire threats.
- *Better Address the Insider Threat* – Improve technologies such as intent determination and anomalous behaviour monitoring for insider threat detection, covering physical and cyber infrastructures.
- *Improve Large-scale Situational Awareness for Critical Infrastructure* - Define the communication and computing system architecture required to create a national Common Operating Picture (COP) of the nation's critical infrastructures.
- *Develop Next-Generation Designs and Architecture for Devices and Systems* – Develop next-generation infrastructural concepts, architectures and systems, both physical and cyber, to include designed-in and built-in security.
- *Develop a Human-Technology Interface that Allows Better Comprehension and Decisions* - Develop improved systems and processes that address the interface that necessarily occurs between people and technology.

A new Bill of July 10, 2009[991], has been introduced in the Senate, which encourages the Secretary of State to work with other governments to further cooperation on cyber-security and report to Congress on those efforts. Specifically the legislation states the Secretary should work with other governments to:

- develop cooperative activities;
- encourage international cooperation for improving cyber-security, and
- develop safeguards for privacy, freedom of speech and commercial transactions to be included in any agreements or other activities designed to safeguard cyberspace.

The review recommended that the government develop a view on an international cyber-security policy framework and strengthen its international partnerships related to cyber-security.

Projects

- ***Institute for Information Infrastructure Protection*** [992]

  The Institute for Information Infrastructure Protection (I3P) is a consortium of leading national cyber security institutions, including academic research centres, government laboratories and non-profit organisations, managed by Dartmouth College. It was founded after September 2001 to help meet the need for improved R&D to protect the United States' information infrastructure against catastrophic failures. The Institute's main role is to coordinate a national cyber security R&D program and help build relationships between academia, industry and government. The I3P continues to work toward identifying and addressing critical research problems in information

[991] http://thomas.loc.gov/cgi-bin/query/z?c111:S.1438:
[992] http://www.thei3p.org/

infrastructure protection and opening information channels among researchers, policymakers and infrastructure operators.

More than 100 I3P researchers from dozens of disciplines and backgrounds are collaborating to understand and mitigate critical challenges in the field of cyber security. Five multi-institutional I3P teams are currently investigating the following topics:

- survivability and recovery of process control systems;
- business rationale for cyber security;
- safeguarding digital identity;
- human behaviour, insider threat and awareness, and
- security incentives through risk pricing.

Protected Critical Infrastructure Information Program[993]

The Protected Critical Infrastructure Information Program (PCIIP) aims to protect certain information shared by the private sector from being disclosed under the federal Freedom of Information Act. Under this program, only people who are trained and certified as PCII-compliant can receive protected critical infrastructure information. The program's goal is to encourage private-sector companies to voluntarily share information so that the DHS and other federal, state, and local agencies can analyse and secure critical infrastructure and protected systems, identify vulnerabilities, develop risk assessments, and enhance recovery preparedness measures.

National Infrastructure Simulation and Analysis Center[994]

The National Infrastructure Simulation and Analysis Center (NISAC) is a modelling, simulation, and analysis program within the DHS comprising personnel in the Washington, D.C., area, as well as from Sandia National Laboratories (SNL) and Los Alamos National Laboratory (LANL). NISAC prepares and shares analyses of Critical Infrastructure and Key Resources (CIKR), including their interdependencies, vulnerabilities, consequences, and other complexities, under the direction of the Office of Infrastructure Protection, Infrastructure Analysis and Strategy Division (IASD).

NISAC provides strategic, multi-disciplinary analyses of interdependencies and the consequences of infrastructure disruptions across all 18 critical infrastructure sectors at national, regional, and local levels. NISAC experts have developed and are employing simulation tools to better understand the complexities of interdependent national infrastructures, including process-based systems dynamics models, mathematical network optimisation models, physics-based models of existing infrastructures, and high-fidelity agent-based simulations of systems.

Domestic Nuclear Detection Office[995]

[993] http://www.dhs.gov/files/programs/editorial_0404.shtm
[994] http://www.sandia.gov/nisac/
[995] http://www.dhs.gov/xabout/structure/editorial_0766.shtm

The Domestic Nuclear Detection Office (DNDO) was established in April 2005, as a jointly staffed office that aims to improve the nation's capability to detect and report unauthorised attempts to import, possess, store, develop, or transport nuclear or radiological material. The strategic objectives of the project include:

- develop a global nuclear detection and reporting architecture;
- develop, acquire, and support the domestic nuclear detection and reporting system;
- fully characterise detector system performance prior to its deployment;
- establish situational awareness through information sharing and analysis;
- establish operation protocols to ensure detection leads to effective response;
- conduct a transformational R&D program, and
- establish the National Technical Nuclear Forensics Center to provide planning, integration, and improvements to US government nuclear forensics capabilities

Critical Infrastructure Protection Decision Support System (CIPDSS) Project[996]

The main objective of the CIP research, promoted by the DHS Science and Technology Directorate, is to carry out a comprehensive evaluation of risks extending across multiple infrastructures, and to ensure that information that can support the decision-making process in times of emergency is provided as quickly as possible.

The objectives of the CIP project are:

- calculating the extent of potential damage to those critical infrastructures with certain designated risks
- creating a basic interdependency model for critical infrastructures
- calculating the effect of natural disasters on critical infrastructures
- evaluating the efficacy of damage mitigation measures
- providing practical support measures on region wide and area-wide scales.

National SCADA Test Bed [997]

SCADA systems and distributed control systems (DCS) are computerised control systems that support the efficient production and distribution of commodities such as electricity, oil, and gas. If unprotected, they are vulnerable to malicious cyber-attacks that could produce potentially catastrophic disruptions to the critical national infrastructures.

[996] www.sandia.gov/nisac/docs/UncertaintyAnalysis.doc
[997] http://www.oe.energy.gov/nstb.htm

The National SCADA Test Bed is a Department of Energy[998] multi-laboratory program that addresses the security challenges of control systems in the energy sector through:

- control systems testing;
- advanced technology development;
- control systems requirements development, and
- industry outreach.

The National SCADA Test Bed is jointly managed and executed by Idaho National Laboratory (INL) and SNL. Other partners include the Pacific Northwest National Laboratory, Argonne National Laboratory, the National Institute of Standards and Technology, and contractors.

Using the testing facilities within the National SCADA Test Bed, researchers have made significant accomplishments in securing control systems for the energy sector.

National Information Exchange Model[999]

The US governments launched the National Information Exchange Model (NIEM) project in February 2005, as a response to the apparent lack of coordination surrounding 9/11. It is a federal, state, local and tribal interagency initiative providing the foundation for seamless information exchange. NIEM was launched through a partnership agreement between the Department of Justice and the DHS.

NIEM is a framework to:

- Bring stakeholders and communities-of-interest together to identify information sharing requirements in routine, operational and emergency situations.
- Develop standards, a common lexicon, and an on-line repository of information exchange package documents to support information sharing.
- Provide technical tools to support the development, discovery, dissemination and re-use of exchange documents.
- Provide training, technical assistance and implementation support services for enterprise-wide information exchange.

Intellipedia

Intellipedia is an online system for collaborative data sharing used by the United States Intelligence Community (US IC). It is a project of the Office of the Director of National Intelligence (ODNI)[1000] Intelligence Community Enterprise Services (ICES). It was established as a pilot project in late 2005 and consists of three wikis running on JWICS, SIPRNet, and Intelink-U. They are used by individuals with appropriate clearances from the 16 agencies of

[998] www.doe.gov
[999] http://www.niem.gov/
[1000] http://www.dni.gov/

the US IC and other national-security related organisations, including the Combatant Commands and other federal departments. It was created to share information on some of the most difficult subjects facing the US IC, bringing emergent technologies into play. It also allows information to be assembled and reviewed by a wide variety of sources and agencies. A number of projects are under way to explore the use of the Intellipedia for the creation of traditional intelligence products. The wikis are not open to the public.

31.1.3 Canada

The Canadian ***Defence S&T Strategy***[1001] was released by the Department of National Defence (DND)[1002] in December 2006, as Canada's first-ever pan-departmental guidance on defence science and technology.

The *Defence S&T Strategy* provides guidance to ensure that the Departmental science and technology investment is appropriately aligned with the priorities of the Canadian Forces (CF).

The ***Defence Research & Development Canada (DRDC)***[1003], an agency of the DND, aims to respond to the scientific and technological needs of the CF. DRDC has an annual budget of C$300 million and employs about 1500 people. The agency is comprised of seven research centres, each focusing on a particular set of scientific and operational requirements. They include:

- DRDC Suffield - expertise in military engineering, autonomous intelligent systems, and defence against chemical and biological agents.
- DRDC Toronto - centre of excellence for human effectiveness science and technology in the defence and national security environment.
- DRDC Ottawa - the DND's lead authority and centre of expertise for radiofrequency communications, sensing, electronic warfare, network security and information operations technologies and systems, radiation effects, space systems, synthetic environments and modelling and simulation.
- DRDC Centre for Security Sciences (DRDC CSS) - a joint endeavour with Public Safety Canada, provides science and technology services and support to address national public safety and security objectives.
- DRDC Valcartier – provides world-leading expertise in optronic systems, information systems, and combat systems.
- DRDC Atlantic - provides world-leading expertise in antisubmarine warfare, mine and torpedo defence, air and naval platform technology, the modelling and simulation of ship and combat systems, shipboard command and control, maritime information and knowledge management, emerging materials, power sources, and signature management.

[1001] http://www.drdc-rddc.gc.ca/sciences/strat/intro-eng.asp
[1002] http://www.forces.gc.ca/site/home-accueil-eng.asp
[1003] http://www.drdc-rddc.gc.ca/

- DRDC Centre for Operational Research and Analysis (DRDC CORA) - providing scientific rigour to decision support and option analysis to the DND, CF, and Canadian security partners.

The ***Government of Canada Position Paper on a National Strategy for Critical Infrastructure Protection***[1004] of November 2004, identifies a number of R&D agencies, in addition to DRDC, which have CIP responsibilities. These include:

- The Communications Security Establishment Canada (CSEC)[1005], which provides to the Canadian Government foreign signals intelligence in support of defence and foreign policy, and the protection of electronic information and communication.
- Industry Canada (IC)[1006], whose program areas include developing industry and technology capability, fostering scientific research, setting telecommunications policy, promoting investment and trade, promoting tourism and small business development, and setting rules and services that support the effective operation of the marketplace.
- The National Research Council Canada (NRCC)[1007], which focuses on health and wellness, sustainable energy and the environment, and providing support for broad-spectrum research and development.
- Public Safety and Emergency Preparedness Canada (PSEPC)[1008], which provides coordination across all federal departments and agencies responsible for national security and the safety of Canadians, from natural disasters, crime and terrorism
- The Royal Canadian Mounted Police (RCMP)[1009], is the Canadian national police service and an agency of the Ministry of Public Safety Canada.

Projects

Canada's Public Security Technical Program[1010]

The Public Security Technical Program (PSTP) program is a federally funded science and technology program involving 21 federal government departments and agencies that play a role in public safety and security. PSTP consists of four thematic areas:

- CBRNE threats;
- critical infrastructure protection;
- surveillance, intelligence, and interdiction, and
- emergency management and systems interoperability.

The majority of funding is allocated to projects within the CBRNE theme. The PSTP is managed by the DRDC Centre for Security Science (CSS).

[1004] http://www.acpa-ports.net/advocacy/pdfs/nscip_e.pdf
[1005] http://www.cse-cst.gc.ca/index-eng.html
[1006] http://www.ic.gc.ca/ic_wp-pa.htm
[1007] http://www.nrc-cnrc.gc.ca/eng/index.html
[1008] http://www.publicsafety.gc.ca/index-eng.aspx
[1009] http://www.rcmp-grc.gc.ca/index-eng.htm
[1010] http://www.css.drdc-rddc.gc.ca/pstp/index-eng.asp

Chemical, Biological, Radiological-Nuclear and Explosives Research and Technology Initiative[1011]

The CBRNE Research and Technology Initiative (CRTI) of the DRDC CSS funds science and technology projects that will strengthen Canada's preparedness for, prevention of, and response to, potential CBRNE threats, including terrorist and criminal acts, accidents and natural disasters.

This initiative is a component of the PSTP[1012]. It was launched on the 10th of May 2002, as part of the federal government's security agenda, and it began as a $170-million, five-year project as part of the $7.7 billion investment the Government of Canada announced in Budget 2001 to improve Canadian security and counter-terrorism efforts. In those five years, a total of $134.2 million was allocated to 136 projects through an annual competitive project selection process. An additional $150 million was leveraged through in-kind and other contributions from partners in academia, industry and other government departments. CRTI is now an effective model for bringing together Canada's national science and technology and security communities and applying their collective knowledge and capabilities towards common goals.

In October 2006, CRTI's mandate was extended for an additional five years, receiving more than $175 million in funding. Since this renewal, the CRTI has provided over $79 million in funding to 49 projects. In 2009 24 new research projects, worth more than $35 million were sponsored.

The research projects cover the following themes[1013]:

- Research and technology development projects: aiming to enhance the capabilities and capacities of the science and technology and operational communities to effectively respond to CBRNE incidents.
- Technology acceleration projects: aiming to more rapidly commercialise technologies that are already in development
- Technology demonstration projects: involve the participation of the operational community to ensure that the science and technology capacity is being developed responsive to their needs. These projects aim to test new technologies in an operational setting and to provide the end-user with a capability which allows them to permanently integrate the knowledge and technology acquired into their daily operations.

Integrated Threat Assessment Centre[1014]

The Integrated Threat Assessment Centre (ITAC) is a cooperative initiative, housed at the Canadian Security Intelligence Service (CSIS)[1015], to facilitate intelligence information sharing and analysis within Canada's intelligence community, and with

[1011] http://www.css.drdc-rddc.gc.ca/crti/index-eng.asp
[1012] http://www.css.drdc-rddc.gc.ca/pstp/index-eng.asp
[1013] The complete project list for 2009 is available at http://www.forces.gc.ca/site/news-nouvelles/view-news-afficher-nouvelles-eng.asp?id=2886.
[1014] http://www.itac-ciem.gc.ca/index-eng.asp
[1015] http://www.csis-scrs.gc.ca/index-eng.asp

first responders, such as law enforcement. The ITAC also shares and receives security assessments from its international partners.

Such assessments, focused on events and trends related to domestic and international terrorism, are aimed at assisting the government of Canada to coordinate activities in response to specific threats more effectively, and to prevent or mitigate risks to public safety.

HOT Admin: Human, organization and technology centred improvement of the IT security administration[1016]

The goals of this project, managed by the Laboratory for Education and Research in Secure Systems Engineering[1017], are to make the first significant strides to understand and improve the management of security and privacy in IT settings by:

- studying security administrators within organisations;
- understanding and modelling their tasks and the effectiveness and usability of the tools they currently use to perform these tasks;
- developing models, theories, and guidelines for security administration that can aid developers and planners in evaluating and improving these tools, and
- refining and validating these findings by developing new tools, and testing them with real administrators in real settings using established principles of human-computer interaction.

The project's novel approach considers the problem as the interaction of three main factors: Humans, Organisations, and Technologies (HOT). Within this project, field studies of security administrators in real, complex organisations are undertaken to characterise their roles, responsibilities, interactions with others, the tasks they perform, and the tools they use.

The desired effect will be better security administration systems that address the needs of organisations, the people who set security policies, and those who implement them. This will enhance the overall level of trust in the complex information systems that form the foundation of modern organisations.

Biometrics User-Centric Secure Networks[1018]

The aim of this project, managed by the NSERC (Natural Sciences and Engineering Research Council of Canada)[1019], is to develop an integrated security architecture to secure and protect sensitive information and data within the domain of a care enterprise such as wireless health care and homecare applications and services. The project addresses the need for secure communication and authentication of personal information to provide enhanced privacy and confidentiality. The proposed security architecture, named "Biometrics User Centric Secure Networks (BUSNet)" will implement novel biometrics-based security solutions and technologies that can be effectively integrated into a wide-range of wireless infrastructures.

[1016] https://lersse.ece.ubc.ca/tiki-index.php?page=Project_HOT-Admin
[1017] https://lersse.ece.ubc.ca/tiki-index.php
[1018] http://www.comm.toronto.edu/~dimitris/research/busnet.doc
[1019] http://www.nserc-crsng.gc.ca/index_eng.asp

Visual analytics for safety and security[1020]

Visual analytics (VA) is the science of analytical reasoning facilitated by interactive visual interfaces. The Canadian Network of Visual Analytics Centres (CNVAC) is undertaking a project whose goals are:

- extending interaction science methods to address VA applications and situations, using tools and environments developed by industry partners;
- working with partner companies to build proof-of-concept prototypes of VA applications, and
- extending the functionality of applications developed in university labs to enhance their commercialisation potential in VA applications.

Internetworked systems security network (ISSNet)[1021]

The aim of the ISSNet is to better understand the emerging threats to Internet usability, security and stability, and to devise techniques and mechanisms to better protect against them. It has been funded by a five year grant from the NSERC, with support from industry and government partners. NSERC's Strategic Networks Grants program awarded ISSNet $5 million in research funds for 2008. An additional 20 percent of its funds come from direct industrial contributions.

It is focused on collaboration among researchers. Participants include leading Canadian researchers from nine universities that are world-class experts in network-oriented, software systems-oriented and human-oriented security, supplemented by government and industrial partners.

The Network's expected outcomes are:

- innovative methods to enhance the usability and security in human-computer interaction;
- the development of Canadian expertise to address attacks to software-based networks, including expanded expertise among university researchers and a mentoring program for the next generation of highly qualified personnel;
- the transfer of knowledge to Canadian industries as a result of the network's collaborative research focus and the flow of trained graduate students into industry;
- industry partners obtaining new, cutting-edge tools and expertise needed to secure vital information systems;
- significant benefits to Canada's economy and society by providing collaborative research that will enhance industry products and business prospects, and
- the dissemination of the Network's results and technology transfer to appropriate organisations.

[1020] http://www.cnvac.ca/
[1021] http://www.issnet.ca/

31.1.4 Japan

In Japan, the ***Disaster Countermeasure Basic Act*** provides a basic plan for disaster prevention and management. Together with the ***Civil Protection Act***, it establishes the roles and responsibilities of national and local government, and relevant stakeholders in the public and private sector. The Disaster Countermeasure Basic Act provides specifically for the management of major disasters, and the Civil Protection Act manages the deployment of task forces during Emergency Response and armed attack situations.

In the main though, CI are owned and operated by private companies, (designated as Public Corporations by the Acts), who are responsible for taking measures to protect them. These Acts mandate countermeasures for risks and disaster, establish the mechanisms for cooperation between the public and private sector, and stress the necessity of information sharing among the stakeholders.

A number of projects[1022][1023] on the theme of CIP are funded by the Japan Science and Technology Agency (JST)[1024] under the Evolution Science and Technology (CREST) Program[1025].

Projects

Capabilities for Engineering of Protection, Technical Operation, Analysis, and Response (CEPTOAR)

The CEPTOAR project was established to improve cooperation between the national government and private enterprises.

The First National Strategy on Information Security and the Action Plan on Security Measures for CI mandated the implementation of CEPTOAR within each CI sector.

The CEPTOAR receive information from the Cabinet Secretariat (via the presiding ministries and agencies) and provide this information to corporate members that operate critical infrastructures.

In order to enable this public-private information sharing, the NIPC issued a “traffic light” protocol for information sharing.

The research on disaster reduction using crisis-adaptive information sharing technologies[1026]

A field test conducted between July 2004 and March 2007, the “research on disaster reduction using crisis-adaptive information sharing technologies” joint project included a range of contributors including government, national research institutes, universities, lifeline corporations, a non-profit organisation and a private company.

[1022] *Hada Y., Kodama N., Suzuki, T. and Meguro, K.,* Road Information Sharing using Probe Vehicle Data in Disasters*, Proc. 14th World Conf. Earthq. Eng., Beijing, 2008*

[1023] *Suzuki, T. and Yozo, Goto,* Joint Research Project on the Disaster Mitigating Information Sharing Platform and its Application to a Test Field, *Proc. 14th World Conf. Earthq. Eng., Beijing, 2008.*

[1024] http://www.jst.go.jp/EN/index.html

[1025] http://www.jst.go.jp/kisoken/crest/en/about/what.html

[1026] *T. Suzuki & Y. Hada*, Development of the framework for disaster mitigating information sharing platform and its application to a local government, *Risk Analysis VI Simulation and Hazard Mitigation (2008)*

The project aimed to achieve effective disaster response in case of disasters and improved information sharing among organisations in charge of disaster reduction.

The project was funded by the Ministry of Education, Culture, Sports, Science and Technology. The National Research Institute for Earth Science and Disaster Prevention (NIED) was in charge of the project.

The project developed a disaster-mitigation information sharing platform, predominantly for local governments, as a framework to enable information sharing in disasters. A prototype of the platform was built by integrating an individual system and tool. Then, it was applied to actual local governments and it proved to be effective.

Researchers who participated in this project have established an incorporated non-profit organisation named as ADMiRe (Agency for Promoting Disaster Mitigation and Damage Reduction)[1027] in order to continue the development and deployment of the platform.

31.1.5 Brazil

Brazil is developing a long-term program focused on Critical Telecommunication Infrastructure Protection (CTIP). Its objectives are:

- to identify the critical points of Brazil's telecom infrastructure;
- to propose recommendations to prevent security incidents and to guarantee service and operations continuity if they occur;
- to develop strategies and policies to protect Brazil's telecom infrastructure, and
- to analyse interdependencies among different infrastructure elements.

The CTIP project is based upon four main elements:

- contextualisation;
- a protection strategy;
- a set of methodologies, and
- software tools to support them.

This program is being conducted by Anatel, the Brazilian telecom regulator, and by CPqD, a private R&D telecom centre. It is sponsored by Fundo para o Desenvolvimento Tecnológico das Telecomunicações (Funttel).

31.1.6 Australia

In the last few years, the Australian Government has made significant effort to address critical infrastructures threats and vulnerabilities through R&D initiatives. It has established CIP as a national research priority.

[1027] http://admire.jpn.org/ (Japanese)

In 2002 a set of national priorities to guide Australia's future research and development activities were announced. The purpose of one of these priorities, ***Safeguarding Australia***, is to enhance Australia's capacity to anticipate and manage critical threats to society and relevant strategic areas. This priority includes R&D initiatives to protect Australia's CI, economy and society from terrorism and crime, and to develop transformational technologies for the defence and national security sectors.

Within this broad policy context, a number of Australian Government projects and initiatives that stimulate R&D in the CIP domain have emerged. In particular, two initiatives are managed by the Department of Prime Minister and Cabinet designed to stimulate R&D in the CIP arena:

- The National Security Science & Technology (NSST)[1028] Unit was established with responsibility for coordinating science, engineering and technology to support Australia's counter-terrorism needs. It provides a national focus area for science and technology for counter-terrorism, maintains and develops knowledge of the science and technology research providers supporting counter-terrorism, and manages international links and collaborative programs of research.
- The Publicly-funded Agencies Collaborative Counter-Terrorism (PACCT) initiative aims of harness the collective R&D expertise held by Australia's publicly funded research agencies. It seeks to collaboratively progress science and technology for counterterrorism in the fields of chemical, biological and radiological detection and response, information and communications technologies and systems, and the modelling of the interdependencies of CI networks.

Projects

Trusted Information Sharing Network (TISN)[1029]

The TISN is a forum that allows the owners and operators of CI to share information on the security issues that affect them. It provides a safe environment where industry and government can share vital information on CIP and organisational resilience. The TISN has established a truly collaborative relationship between business and government, based on trust, which is helping to build a more resilient Australia.

The TISN is made up of nine different sectoral groups, called 'Infrastructure Assurance Advisory Groups', overseen by the Critical Infrastructure Advisory Council. It gives CI owners and operators a way of communicating with the Australian Government at a high level. It also feeds into Australia's counter-terrorism arrangements. The Council has set up two permanent Expert Advisory Groups—one for IT security and the other looking at issues likely to affect CIP in the future. It can establish other Expert Advisory Groups to provide advice as required. The TISN has also formed 'communities of interest', which bring together members from different sectors to work on common issues in relation to SCADA systems, pandemic planning and business resilience.

[1028] http://www.pmc.gov.au/nsst/
[1029] http://www.tisn.gov.au/

Australian Government's Critical Infrastructure Protection Modelling and Analysis Program (CIPMA)[1030]

The CIPMA program is a world-leading computer modelling program. It is a key component of the Australian Government's efforts to enhance CIP and is a major national security initiative.

CIPMA helps strengthen Australia's economic and social resilience by providing 'virtual insight' into disruptions to services whether caused by natural or human disasters. Owners and operators of CI can use this information to plan how to prepare, prevent, respond and recover from an adverse event. CIPMA also helps governments shape their policies on national security and critical infrastructure protection.

CIPMA has achieved good coverage of the banking and finance, communications and energy sectors and is progressing coverage of the water sector. Engagement with the transport sector has commenced and inclusion of other key sectors in the CIPMA capability will occur over time.

CIPMA's primary purpose is to strengthen national security and better protect Australia's CI. It does this through a computer based capability which uses a vast array of data and information from a range of sources (including the owners and operators of CI) to model and simulate behaviour and dependency relationships of critical infrastructure.

The capability includes a series of 'impact models' to analyse the effects of a disruption to critical infrastructure services. The impact models assess the flow-on effects of a critical infrastructure service disruption within and across sectors, how the economy and population will be affected, how long the disruption is likely to last, the area affected and how the various infrastructure systems will behave as a result of the service interruption.

CIPMA is an 'all hazards' program, that delivers strategic support to government and business decision makers involved in critical infrastructure protection, counter-terrorism and emergency management, especially with regard to prevention, preparedness and planning, and recovery.

CIPMA supports this decision-making by helping to:

- identify connections between critical infrastructure nodes and facilities within sectors and across sectors;
- provide insights into the behaviour of complex networks;
- analyse relationships, dependencies and interdependencies;
- examine the flow-on effects of infrastructure failure, and
- identify choke points, single points of failure, and other vulnerabilities.

The program was launched and is managed by the Australian Federal Government's Attorney-General's Department. Geoscience Australia and the Commonwealth

[1030] http://www.csiro.au/partnerships/CIPMA.html

Scientific and Industrial Research Organisation(CSIRO) work closely together to construct its technical components.

Computer Network Vulnerability Assessment (CNVA)[1031]

Set up by the Australian Government, the CNVA Program helps organisations that own or manage critical infrastructure test the security of their computer networks and systems. The CNVA program gives dollar-for-dollar funding to eligible organisations from the private sector or government business enterprises to conduct vulnerability assessments. The program is managed by GovCERT.au[1032] —the Australian Government Computer Emergency Readiness Team—which is part of the Attorney-General's Department.

e-Security National Agenda (ESNA)[1033]

The ESNA was established in 2001 by the Australian Government to create a secure and trusted electronic operating environment for both the public and private sectors, recognising the increasing reliance of government, business and home users on information and communications technologies.

Online attacks potentially come from a number of sources, including organised crime, foreign intelligence services, and politically motivated groups. They potentially pose a risk to the:

- continuity of government;
- reliable delivery of critical services by both the public and private sector, and
- identity and financial information of home users and small to medium-sized enterprises.

In 2006, the Government announced a review of the ESNA to ensure that its policies were keeping up to date with changing security needs. The review found that because the online environment is highly interconnected, e-security threats to different segments of the Australian economy cannot be addressed in isolation. This key finding saw the development of three new priorities to address concerns and to assist in achieving the original objective of ESNA. They are to:

- reduce the e-Security risk to Australian Government information and communications systems;
- reduce the e-Security risk to Australia's national CI, and
- enhance the protection of home users and small to medium enterprises from electronic attacks and fraud.

Research Network for a Secure Australia[1034]

The Research Network for a Secure Australia (RNSA) is a multi-disciplinary collaboration, funded by the Australian Research Council for a period of five years It

1031 http://www.tisn.gov.au/www/tisn/tisn.nsf/Page/CIPPrograms_ComputerNetworkVulnerabilityAssessment(CNVA)Program
1032 http://www.ag.gov.au/govcert
1033 http://www.tisn.gov.au/www/tisn/tisn.nsf/Page/e-Security#National_Agenda
1034 http://www.secureaustralia.org/

was established to strengthen Australia's research capacity to enhance the protection of the nation's CI from natural, deliberate, or accidental disasters, and terrorist acts.

The RNSA facilitates a knowledge-sharing network for research organisations, government and the private sector to help them develop research tools and methods to mitigate emerging CI safety and security issues. The network will integrate complementary, yet diverse, research areas including physical and information infrastructure security, and surveillance and intelligent systems. The RNSA has identified the majority of Australia's leading researchers, Commonwealth and state officers and industry leaders involved in CIP. This includes more than 300 researchers and professionals from 25 Australian research organisations, 15 government organisations, and an industry consortium.

The network will identify and facilitate the integration of research programs and collaboration in CIP. The RNSA will encourage and support:

- Open exchange of information and sharing of resources across disciplinary, organisational, institutional and geographical boundaries by organising workshops, focus groups and an annual conference.
- Development and implementation of cohesive and integrated research plans among researchers by bringing them together and encouraging communication opportunities for cross-disciplinary research collaboration.
- Nurturing the careers of young investigators and research students through incentives, such as attending an annual summer retreat, as well as opportunities to participate in international and inter-institutional exchange programs.
- Links with actual and potential end-users, and the broader community through an advisory board composed of recognised key stakeholders in Australian CIP.

31.2 Academic forums

CIP/CIIP is a strong, multi-disciplinary, but still immature field of research[1035]. There are several specialised communities of experts that operate in this field, including cyber-security, modelling, risk, control system experts, and those with expertise in the security management of CI. These communities use largely their own languages, vocabularies and scientific networks, with the consequence that results are dispersed and difficult to retrieve and merge.

Only in the last few years have attempts been undertaken to create common scientific forums specifically devoted to CIP/CIIP. Listed below are a number of these fora, generally considered as the most authoritative.

International Journal of Critical Infrastructures (IJCIS)[1036].

[1035] S. Bologna, E. Luiijf, and R. Setola, “R&D activities in Europe on Critical Information Infrastructure Protection (CIIP)”, Int. Journal of System of Systems Engineering (IJSSE), Vol. 1, N. 1/2 , pp. 257 – 270, 2008.

[1036] http://www.inderscience.com/browse/index.php?journalID=58

This scientific journal is published in four issues per year by Inderscience Publishers. It has a technical focus, and aims to provide a professional and scholarly forum for information exchange between different scientific and technological disciplines, and between societal and managerial disciplines in the area of CI. Its goal is to provide an authoritative source of information in the field of risk and vulnerability assessment, and the management of vital societal systems exposed to both man-made and natural threats.

International Journal of Critical Infrastructure Protection (IJCIP)[1037].

This journal was launched in 2008 by Elsevier, to publish high quality scientific and policy papers in all areas of CIP. Of particular interest are articles that weave science, technology and policy to craft sophisticated yet practical solutions that will secure information, computer and network assets in the various critical infrastructure sectors. It is linked with the IFIP Working Group 11.10 on CIP.[1038]

International Journal of System of Systems in Engineering (IJSSE).[1039]

This scientific journal, published in four issues per year by Inderscience Publishers, approaches CIP from a system-of-systems perspective. It considers CIP, and other more general security issues, in terms of the integration and cooperation of several technological, organisational, and cyber systems. In this framework, the journal is more devoted to supporting the design/analysis phase of such complex systems.

Journal of Homeland Security and Emergency Management [1040].

This journal publishes articles describing research or practice in the fields of homeland security and emergency management. It was created in 2004 by Berkeley Electronic Press to provide high-quality, peer-reviewed content in the realm of homeland security and to discuss the relationships between emergency management (for natural, technological, industrial, and terrorism events) and the new field of homeland security. It is an electronic journal which publishes one issue per year, updated continuously.

Journal of Contingencies and Crisis Management[1041].

This scientific journal is published four times a year by Blackwell Publishing. It focuses on all aspects of contingency planning, scenario analysis, and crisis management in both the corporate and public sectors, and seeks to provide analysis of the opportunities and threats facing organisations. It presents case studies of crisis prevention, crisis planning, recovery, and change management.

ECN – European CIIP Newsletter [1042]

This newsletter provides coverage of CIIP issues with a particular European focus. It is sponsored by the EU project IRRIIS.

Two conferences have been recognised as the most important for the CIP/CIIP topic. These are CRITIS and those arranged by the IFIP[1043] WG 11.10. The first is a European

[1037] http://www.elsevier.com/wps/find/journaldescription.cws_home/713691/description#description
[1038] http://ifip1110.org/
[1039] http://www.inderscience.com/browse/index.php?journalID=184#objectives
[1040] http://www.bepress.com/jhsem/
[1041] http://www.wiley.com/bw/journal.asp?ref=0966-0879
[1042] http://www.irriis.org/?lang=en&nav=289
[1043] International Federation for Information Processing

conference, while the second is held in USA. They cooperate strongly and they have built what appears to be the most important scientific community in the field of CIP/CIIP.

CRITIS (Critical Information Infrastructures Security)

Although this conference was originally specifically devoted to CIIP, it has evolved to include topics about CIP. This conference has now been held on four occasions - Samos Island (Greece) 2006[1044], Malaga (Spain) 2007[1045], Roma (Italy) 2008[1046], Bonn (Germany) 2009. Its proceedings are published by Springer in the Lecture Notes on Computer Science series[1047].

IFIP WG 11.10 International Conference on Critical Infrastructure Protection[1048]

The IFIP Working Group 11.10 on Critical Infrastructure Protection[1049] is an active international community of researchers, infrastructure operators and policy-makers dedicated to applying scientific principles, engineering techniques and public policy to address current and future problems in information infrastructure protection. This conference has been held on three occasions - Hanover, New Hampshire, 2007, Arlington Virginia, 2008, Hanover, New Hampshire, 2009. Its proceedings are published by Springer in the Critical Infrastructure Protection series[1050].

[1044] http://critis08.dia.uniroma3.it/archive/2006/index.html
[1045] http://critis08.dia.uniroma3.it/archive/2007/index.html
[1046] http://critis08.dia.uniroma3.it/
[1047] http://www.springer.com/computer/communications/book/978-3-642-03551-7
[1048] http://ifip1110.org/Conferences/
[1049] http://ifip1110.org/
[1050] http://www.ifip1110.org/Publications/

32 Annex: Member State Summary Report[1051]

	Organizational Model	Strategy & Policy	Methodology & Standards	Public-Private Partnerhsip & International Collaboration	Funding & Human Resources	Training & Exercises	Sector-Specific Key-Players and Initiatives
Austria	▪ No single national CIP organisation in place ▪ Federal Alarm Centre coordinates information in case of emergency	▪ Government resolution on CIP approved and under implementation ▪ Voluntary relief services integrated into Civil Protection system at regional level	▪ Government Resolution and Master Plan for CIP under implementation	▪ Bilateral Disaster Assistance Agreements in place with main confining states ▪ PPPs regarding ICT (A-SIT and CIRCA)	▪ € 5-10 Mn budget in 2008 aimed at CIP programs	▪ Basic and advanced training for relief workers available ▪ Special training available at Universities	▪ Central European Gas Hub ▪ Adoption of a Transport Master Plan
Belgium	▪ There is no single specific agency dedicated to CIP ▪ Presence of a Crisis Centre, but not specifically dealing with CIP	▪ Belgium has a decentralised approach to CIP ▪ Each Ministry is responsible for its own competence area	▪ Not Applicable	▪ Participation in alert networks (Ecurie, BICHAT, MIC, etc…)	▪ Not Applicable	▪ Not Applicable	▪ No specific CIP-related initiatives available
Bulgaria	▪ There is no single agency dedicated to CIP ▪ Ministry of State Policy for Disasters and Accidents created in 2006, and is on a developmental path to fully deal with CIP	▪ Bulgaria does not presently have a single centralised strategy to deal with CIP ▪ Each Ministry is responsible for their competence area in case of crisis	▪ Not Applicable	▪ National Fire Safety and Protection of Population Service collaborate with peers in the Balkans and in several countries over the world	▪ Not Applicable	▪ General training and education on civil protection available	▪ Summit on Natural Gas For Europe Security And Partnership
Cyprus	▪ There is no single agency specifically dedicated to CIP ▪ CIP is managed under the same arrangements as any other emergency situations by the existing Civil Defence arrangements	▪ Cyprus dealing in an unstruc-tured way with CIP	▪ Not Applicable	▪ International Search and Rescue Advisory Group (INSARAG)	▪ International Urban Search and Rescue Exercise	▪ In the ICT industry, ISO27001 is a standard commonly used	▪ Not Applicable

[1051] Not Applicable = Open source research, web-based surveys and individual interviews have not provided information/data on this data point

	Organizational Model	Strategy & Policy	Methodology & Standards	Public-Private Partnerhsip & International Collaboration	Funding & Human Resources	Training & Exercises	Sector-Specific Key-Players and Initiatives
Czech Republic	▪ There is no specific Agency dedicated to CIP ▪ CIP-related issues are addressed by the Civil Emergency Planning Committee	▪ CIP is addressed in the "Security Strategy Document of the Czech Republic" document - but in an unstructured way	▪ Integrated Rescue System (rescue and clean-up operations)	▪ Cooperation with Austria on radiation emergency	▪ Managed within operators and agencies as an additional duty	▪ Nuclear safety Exercise "Zone 2008"	▪ No specific CIP-related initiatives available
Denmark	▪ Emergency Management Agency (DEMA) with CIP responsibility reporting to Ministry of Defence ▪ Formal CIP working group (KG/KI)	▪ CIP activities guided by the Danish Preparedness Act	▪ DEMA RVA model defines methodology for defining Responsibility, Threats, Assessment, and Profile	▪ DSIS hosts a cross-sectoral public-private contact group	▪ No CIP-specific budget, integrated into Preparedness activities ▪ Approx. 30 government employees have secondary CIP responsibilities	▪ National KRISOV excerise on emergency mgmt ▪ Exercise Secretariat within DEMA to track exercises nationwide	▪ BERIT Forum for communi-cation infra-structures
Estonia	▪ There is no specific Agency dedicated to CIP ▪ Ministry of Interior leads CIP working group	▪ CIP is addressed as "continuation of vital services" in the Emergency Act of 15 June 2009	▪ Emergency Act establishes risk assessment and continuous operation plan methodology	▪ Cooperative Cyber Defence Centre of Excellence	▪ Not available	▪ Pandora Exercise on pandemic crisis	▪ Refer to Ministry of Interior
EU	▪ CPI is dealt with at the EU Commission Level	▪ EU is dealing in a structured way with CIP ▪ Directives, Communications, Regulations and Green Papers are in place	▪ No Methods, standards, operating plans and technology regarding CIP	▪ No PPP and international collaboration on CIP	▪ No CIP-specific budget and headcount known ▪ Funding provided partially by European Commission	▪ Exercises, simulations and trainings are performed are performed	▪ Initiative is in place in the ICT (CI^2RCO) ▪ Rapid Alert System for Food and Feed (RASFF)
Finland	▪ There is no specific Agency dedicated to CIP	▪ CIP approach explained in "The Strategy for Securing the Functions Vital to Society" document	▪ Implementation of the Govern-ment Report on Security and Defence Policy	▪ NBED and NESC ▪ CIVPRO Network (risk management) ▪ Bilateral Agreements with Sweden and Norway	▪ Not Applicable	▪ UUSIMAA 2008 Exercise (consequence management field exercise)	▪ Not Applicable

	Organizational Model	Strategy & Policy	Methodology & Standards	Public-Private Partnerhsip & International Collaboration	Funding & Human Resources	Training & Exercises	Sector-Specific Key-Players and Initiatives
France	▪ Defence and national security agency (SGDN) with CIP responsibility reporting to Prime Minister	▪ CI Sectors and objectives defined (Decree No. 2006-212)	▪ EBIOS for CIIP ▪ Specific Methodolog and Tool for Risk Analysis for CIP	▪ CIParis 2008 ▪ National committee for CIP ▪ Security liaison officers meetings ▪ CSTI (Strategic Advisory Board on Information Technologies)	▪ Approximately 500 people across all levels of government have additional duties related to CIP	▪ CFSSI (Training Centres on systems security) ▪ National exercises at governme nt level, with private operators	▪ Multiple initiatives identified for ICT sector
Germany	▪ Ministry of Interior (BMI) coordinates activities on CIP matters on national level ▪ CIP is handled be the relevant government departments and the Länder.*	▪ National Strategy for Critical Infrastructure Protection (CIP Strategy) ▪ National plan for Information Infrastructure Protection (NPSI ▪ Covered in Civil Protection policy	▪ Methodologies , standards, operating plans and technology regarding CIP are in place	▪ Participation in bilateral and multilateral agreements ▪ CIIP: UP Kritis working groups between CI providers, relevant associations and public authorities*	▪ No information available	▪ The BSI coordinates regular exercises on CIIP ▪ BBK performs every 2 years a national crisis managem ent exercise (LÜKEX)	
Greece	▪ There is no single agency specifically dedicated to CIP ▪ General Secretariat for Civil Protection takes care of emergencies	▪ Greece is dealing in an unstructured way with CIP. ▪ CIP is mentioned as an element of the national Civil Protection plan (Xenokrates)	▪ Operating emergency plans for 21 types of risks (natural, technological, others) issued by the competent Ministries	▪ ECURIE	▪ Not Applicable	▪ Not Applicable	▪ National Emergency Plan for Nuclear, Radiological, Biological and Chemical (NRBC)
Hungary	▪ There is no specific Agency dedicated to CIP	▪ National Program for Protection of Critical Infrastructure s established by the Government in 2008	▪ National Program for Protection of Critical Infrastructure s	▪ PPP Inter-Ministerial Committee ▪ NIIFI and HUNGARNET	▪ Not Applicable	▪ Not Applicable	▪ Not Applicable
Ireland	▪ There is no specific Agency dedicated to CIP ▪ Most appropriate department or agency is appointed on a case-by-case basis	▪ CIP is cited as a key point in the "Framework for Major Emergency Management	▪ Not Applicable	▪ Rapid Alert System BICHAT (Biological, Chemical Attack) ▪ International Atomic Energy Agency	▪ Not Applicable	▪ Major Incident Medical Managem ent Support (MIMMS)	▪ National Emergency Plan for Nuclear Accidents (NEPNA)

	Organizational Model	Strategy & Policy	Methodology & Standards	Public-Private Partnerhsip & International Collaboration	Funding & Human Resources	Training & Exercises	Sector-Specific Key-Players and Initiatives
Italy	▪ Representatives from various ministries / agencies cooperate on CIP efforts through an formal national CIP working group (Tavolo PIC), but there is no dedicated national CIP agency	▪ No national-level strategic or operative plan in place ▪ Ministry of Interior initiated an activity to identify Critical Information Infrastructures	▪ No official methodology endorsed by the government	▪ AIIC - Italian Association of Critical Infrastructure Experts (Public-Private Entitiy)	▪ No CIP-specific budget assigned ▪ 5 people from Civil Protection and Office of the Military Advisory of the Prime Minister represent Italy internationally	▪ Limited university-level specialization programs ▪ MESIMEX Exercise	▪ Emergency Plan for the Electricity System (done by Terna) ▪ ISCOM released guidelines about security of TLC networks supporting critical infrastructures
Latvia	▪ No specific CIP-related organisational model available	▪ Security Measures Planning and Implementation Procedure of Important Facilities for National Security in place	▪ Not Applicable	▪ NATO Senior Civil Emergency Planning Committee ▪ UNECE Convention	▪ No funding from public authorities and sources outside the country	▪ UUSIMAA 2008	▪ Not Applicable
Lithuania	▪ No specific CIP-related organisational model available	▪ CIP strategy and law and currently under development ▪ Possible solutions are being developed by a working group	▪ Emergency plans available regarding Nuclear, Fire and Natural Disasters	▪ Bilateral and multilateral treaties are in place	▪ No funding from public authorities and sources outside the country	▪ Yearly trainings involving Police, Civil Protection and Private Operators	▪ No specific CIP-related initiatives in place
Luxembourg	▪ Supreme Council of National Protection deals with crises and has started CIP ▪ CONATIC is still under development	▪ Luxembourg's CIP is under development, using a structured approach	▪ Directory of Emergency Services manages intervention funds and plans	▪ Directorate of Emergency Services has links with first-aid organisation in neighbouring countries	▪ Not Applicable	▪ Directorate of Emergency Services recruits and trains volunteers	▪ Not Applicable
Malta	▪ There is no specific Agency dedicated to CIP	▪ Malta is dealing in an unstructured way with CIP	▪ Malta Standards Authority deals with official Maltese standards	▪ ESPD ▪ 5+5 Defence Initiative	▪ Not Applicable	▪ Phoenix Espress Exercise ▪ Exercise Canale (Malta and Italy)	▪ Data Protection Twinning Light Project
The Netherlands	▪ Ministry of the Interior and Kingdom Relations, Directorate of National Security leads an informal, inter-ministerial CIP working group	▪ CIP programs fall under national security strategy ▪ Activities involve national government, CI operators, and safety regions	▪ National Security: strategy and work programme 2007-2008 ▪ The Dutch CIP Methodology	▪ Some bilateral (floods) and multilateral (ICT) agreements in place ▪ PPPs in place for CIP (SOVI and NAVI)	▪ Core CIP group has 9 staff members ▪ Main support agency has approximately 20 staff members	▪ "Shift-Control" exercise on ICT attack ▪ Voyager (2007) ▪ Waterproof (2008)	Specific CIP-related initiatives across all sectors, including some sectors not identified by the EC as "critical

	Organizational Model	Strategy & Policy	Methodology & Standards	Public-Private Partnerhsip & International Collaboration	Funding & Human Resources	Training & Exercises	Sector-Specific Key-Players and Initiatives
Norway	▪ No structured CIP entity, but a decentralized structure based on Ministries	▪ Report on Protection of Critical Infrastructures and Critical Societal Functions	▪ Creation of a new digital communication network for emergency and public safety services	▪ NorCert and NorSIS	▪ Funding from Ministries	▪ Exercises to tackle catastrophes and terror scenarios in place	▪ National Post and Telecommunication Authority is responsible for contingency planning in the electronic communications infrastructure
Poland	▪ Security agency with CIP responsibilities reporting directly to Prime Minister	▪ CI and CIP defined in Crisis Management Acts of 2007 and 2009	▪ Will be addressed in the National CIP Program which will replace the National CIP Plan through amendments to the CMA, effective Sep 19 2009.	▪ Public Administration / CI Owners Public-Private Forum	▪ Dedicated CIP staff within cross-functional agency (GCS)	▪ This will be prepared after the process of selecting CI will be concluded	▪ CERT Polska ▪ CERT GOV PL ▪ ARAKIS-GOV
Portugal	▪ There is no specific organisation dealing with CIP	▪ Portugal currently maintains a decentralised approach to CIP. ▪ Portugal has no specific strategies for CIP	▪ Generic Civil Protection Emergency plans	▪ NATO ▪ Eurodefence Portugal	▪ Not Applicable	▪ Not Applicable	▪ Crutial Project ▪ FOREVER Program
Romania	▪ There is no specific organisation dealing with CIP	▪ Romania is dealing in an unstructured way with CIP ▪ Romania has no specific strategies for CIP	▪ Not Applicable	▪ Collaboration in the develop-ment of the Mutual Support Integrated Operational System	▪ Not Applicable	▪ Not Applicable	▪ Not Applicable
Slovakia	▪ CIP is covered by Crisis Management and Civil Protection under the Ministry of Interior	▪ Slovakia is dealing in a structured way with CIP - involving all sectors considered strategic by the Government	▪ Specific CIP-technology tools: CECIS, ECURIE, RAPEX, RASFF	▪ The Ministry of Interior has recently established a dialogue with all relevant key players and held preliminary discussions	▪ No CIP-specific budget known ▪ Approx. 1-10 public employees working on CIP	▪ Some universities offer CIP-related degrees ▪ Sporadic CIP-related exercises are performed	▪ No specific CIP-related initiatives available
Slovenia	Inter-ministerial working group on critical infrastructure in Slovenia, chaired by Ministry of Defence	▪ Slovenia is dealing in an unstructured way with CIP ▪ No specific CIP-related strategy and policy in place	▪ General Emergency and Relief Plans	▪ Bilateral agreement with Austria on the tunnel Karavanke	▪ No CIP-specific budget ▪ Some public employees working on CIP, embedded in the different Ministries	▪ Training Centre for Civil Protection and Disaster Relief of the Republic of Slovenia	▪ ECURIE ▪ ZARE Communication System ▪ Research Project on CIP

	Organizational Model	Strategy & Policy	Methodology & Standards	Public-Private Partnerhsip & International Collaboration	Funding & Human Resources	Training & Exercises	Sector-Specific Key-Players and Initiatives
Spain	▪ CIP National Centre ▪ Assistance organized through the Directorate General for Civil Protection	▪ Structured approach to tackle CIP issues	▪ Creation of a National Plan for CIP	▪ Based on bilateral relations (with France, Portugal, South-American Countries) ▪ Participation to CNPIC	▪ Over 100 public employees dedicated to CIP ▪ Funding from Ministries and EU	▪ Escuela Nacional de Protección Civil forms experts in security and emergency	▪ CCN-Cert becoming the National Alert Centre ▪ University of Alcalà de Henares involved in CIP-related research
Sweden	▪ CIP is managed by the SCCA ▪ Ministries deal with CIP issues on a case-by-case basis	▪ Sweden is dealing in an informal way with CIP	▪ Funding partially assigned from Central Government and from the involved entity	▪ Svenskt Näringsliv Industry Security Delegation promotes cooperation between enterprises on vulnerability issues	▪ Coordination exercises will be performed	▪ RAKEL standard is being introduced to secure commu-nications	▪ Committee on Electronics Communication focuses on a more secure electronics communications infrastructure
UK	▪ There is a dedicated government authority (CPNI) for delivering advice to the national infrastructure	▪ No single strategy covering all hazards ▪ National strategies are in place for security, counter-terrorism, and cyber security	▪ Methdology and plans published and recommended, but not mandated, by CPNI ▪ National Risk Register ▪ National Risk Assessment	▪ Information Exchanges and WARPs drive information sharing between public and private entities	▪ No information available	▪ Three national scale exercises every year	▪ Multiple activities across many sectors