Prevention, protection and REaction to CYber attackS to critical infrastructurEs
PRECYSE

SEVENTH FRAMEWORK PROGRAMME

EUROPEAN COMMISSION

Title:	Document Version:
D 7.2 Study of EU Legislation pertinent to Security	1.1

Project Number:	Project Acronym:	Project Title:
285181	PRECYSE	Prevention, protection and reaction to cyber attacks to critical infrastructures

Contractual Delivery Date:	Actual Delivery Date:	Deliverable Type*- Security**:
March 2014	March 2014	PU R

**Type: P: Prototype; R: Report; D: Demonstrator; O: Other.*

***Security Class: PU: Public; PP: Restricted to other programme participants (including the Commission); RE: Restricted to a group defined by the consortium (including the Commission); CO: Confidential, only for members of the consortium (including the Commission). EU Restricted*

Responsible:	Organisation:	Contributing WP:
Rosi Armstrong	QUB	WP 7

Authors (organisation)
Rosi Armstrong (QUB)

Abstract:
This Deliverable provides a study of EU legislation pertinent to Critical Infrastructure systems and information security and particularly includes a description of EU Policy and Legislation for the Protection of Critical Infrastructure, and a description of other EU policy areas which are relevant to CI protection, namely EU Policy on Network and Information Security, the Directive on the Protection of Personal Data and the Directive on the Retention of Data.

Keywords:
European Union, Policy, Legislation

PROJECT REVISIONS:

Revision	Date	Description	Author (Organisation)
1.1	27/02/14	New Document	Rosi Armstrong (QUB)
Final	28/02/14	Final Document	Rosi Armstrong (QUB)

Contents

1 Introduction 5
2 Reference Material 9
3 EU Policy and Legislation for the Protection of Critical Infrastructure. 10
3.1 Introduction 10
3.2 European Programme for CI Protection 10
3.2.1 History 10
3.2.2 EPCIP goal 11
3.2.3 CI Definitions 11
3.2.4 European Critical Infrastructure Definition 12
3.2.5 CI Threat Coverage of the EPCIP 13
3.2.6 EPCIP Key Principles 13
3.2.7 Common Framework for EPCIP 14
3.2.8 EPCIP Implementation Measures 14
3.2.9 Dialogue with CI Owners, Operators and Users 16
3.2.10 Role of CI Owners, Operators and Users in EPCIP 16
3.2.11 The Role of National CI in EPCIP 17
3.2.12 Evaluation and monitoring of EPCIP 18
3.2.13 New Approach to EPCIP 19
3.3 CI Warning Information Network 23
3.4 Directive 2008/114/EC Identification and Designation of ECI and the Assessment of the Need to Improve their Protection 29
3.5 Critical Information Infrastructure Protection 38
4 EU Policy on Network and Information Security 46
4.1 COM(2000)890 Creating a Safer Information Society 46
4.2 COM(2001)298 NIS : Proposal for a European Policy Approach.. 46
4.3 Council Resolution (2002/C 43/02) Common Approach and Actions in NIS 48
4.4 Regulation (EC) No 460/2004 Establishing the European Network and Information Security Agency 49
4.5 COM(2005)229 i2010: A European Information Society for Growth and Employment 49
4.6 COM(2006)251 Strategy for a Secure Information Society 49
4.7 COM(2006)688 Fighting Spam, Spyware and Malicious Software 49
4.8 Council Resolution 2007/C68/01 Strategy for a Secure Information

Society in Europe 50
4.9 Council Resolution 2009/C 321/01 Collaborative European Approach to NIS 50
4.10 COM(2010)245 Adoption of the Digital Agenda for Europe 50
4.11 COM(2010)517 Proposal for a Directive on Attacks against Information Systems 51
4.12 COM(2013)48 Proposal for a Directive concerning Measures to Ensure a High Common Level of NIS across the Union 52
5 Directive 95/46/EC Protection of Personal Data 56
5.1 COM(2012)9 - Safeguarding Privacy in a Connected World, A European Data Protection Framework for the 21st Century................. 58
6 Directive 2006/24/EC Retention of Data 62
7 EU CI and Related Policies - Relationship to PRECYSE 65
Operator Security Plan [COM(2005)576] 67

1 Introduction

Critical Infrastructures (CI) are physical and information technology facilities, networks services and assets which are essential for the maintenance of vital societal functions, and which, if disrupted or destroyed, have a serious impact on society.

CI can be disrupted, damaged or destroyed by numerous actions, such as human error, accidents, negligence, deliberate attacks, natural disasters. CI are often controlled and monitored by Industrial control systems (ICS) including Supervisory Control and Data Acquisition (SCADA) systems. Use of commercial software in ICS products results in improved ease of use, but also increases the exposure to attacks. The introduction of Smart Grids will substantially improve control over commodity consumption and distribution, such as electricity, to the benefit of consumers, suppliers and grid operators. However, improved operations and services will come at the cost of exposing the entire commodity network to new challenges in the field of security and will open channels for attack on distribution networks. Connection of CI to intranets and communication networks increases vulnerability to computer network-based attacks.

The consequences of an attack on CI are numerous, for example, a successful attack on CI control systems could result in denial of CI services such as electricity or telecommunications, or malfunctioning of CI such as water supply networks. Any of these will, at best, cause disruption to normal life and could lead to damage to infrastructure and surrounding areas, financial loss and even loss of life.

In addition, the failure of CI in one sector could also have a cascade effect on CI in other sectors, due to a synergistic relationship between different CI, for example the relationship between energy supply CI and other CI e.g. transport. This is a particular issue for the European Union (EU), where disruption of operation of a CI of one Member State (MS) may well affect one or more other MS. Given the above, it is essential that any disruption to CI should be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of citizens and countries.

The security of CI is therefore of paramount importance. This needs to encompass CI risk and threat assessments, generation of security solutions and development of swift, coordinated and efficient responses to CI disruption. However, any CI security measures should take care to minimise any negative impact that increased security investments might have on the competitiveness of any particular CI.

The effective protection of CI will require communication, coordination and cooperation nationally and internationally among all interested parties - citizens, government and CI owners, operators and regulators.

The EU has long been cognisant of the issues surrounding the criticality and consequent necessity for protection of CI. Over the years, a CI strategy and policy regime have been developed, encompassing such themes as cooperation on CI security between MS, communication with all stakeholders, legal requirements to enhance and align MS CI protection measures, research and development of CI security methodologies and technologies and financial support for the introduction of CI policies and measures.

In particular, the EU has encouraged CI research and development in Framework Programme 7 (FP7), work programme topic - Cyber Attacks against Critical Infrastructures - by issuing a call for and financial support of projects to address this issue and enhance the protection of CI.

PRECYSE - Prevention, protection and reaction to cyber attacks to critical infrastructures - is a response to the FP7 call. This Project will define, develop and validate a methodology, an architecture and a set of technologies and tools to improve, by design, the security, reliability and resilience of the ICT systems supporting CI.

The PRECYSE Project comprises a set of specific scientific and technical objectives:

- to specify a methodology to identify CI assets, associated threats and vulnerabilities and improve the level of CI security,
- to specify and develop a CI security architecture that improves resilience and which encompasses a set of architectural principles and the tools to be instantiated into existing or to-be-created CI architectures,
- develop a set of tools and technologies for the protection of CI and the prevention of cyber attacks against them,
- develop a set of tools and technologies for the early warning of attacks on CI and the issuing of countermeasures, and
- installation of an integrated prototype of the methodologies, technologies and tools developed in the Project to evaluate PRECYSE results in realistic conditions within two demonstrations in the CI sectors of Energy and Transport.

The security of CI systems is not a stand-alone concern. It sits within a broad field of security of cyber systems and their information. There exists a set of ethical principles, set down internationally in terms of fundamental rights (e.g. privacy and protection of personal data), which is applicable to this security field. Various national legislation has also been put in place which sets out rules for the protection of these ethical principles in the context of cyber security. The security of CI therefore has to operate within this existing ethical and legal security context. In addition, there is an increasing demand for more open and interconnected CI systems and this raises new ethical and legal issues in the protection of the structure of these systems and, particularly, the information which they handle.

The PRECYSE Project comprises a Work Package, 7, specifically dedicated to Legal, Ethical, Privacy and Policy Issues relevant to CI. The main objectives of this Work Package are:

- a review of the ethical factors of systems and information security, particularly CI systems,
- an investigation of EU policy initiatives in the fields of protection of ethical principles and security of systems and information,
- a study of EU legislation, codes of practice and standards relevant to the protection of physical systems and the information of CI,
- engagement with researchers of other PRECYSE Work Packages to develop CIs system security policies and protocols which address the legal and ethical contexts, and
- interaction with EU and national policy makers to contribute to the development of strategy, policies and legislation for the protection of CI in an ethically-acceptable manner.

The PRECYSE Work Package 7 comprises a number of Deliverables, including Deliverable 7.2 - Study of EU Legislation pertinent to Security. This Deliverable entails a study of EU legislation pertinent to systems and information security including how this legislation governs CI security. This Report is the product of Deliverable 7.2.

The Report comprises a description of EU Policy and Legislation for the Protection of Critical Infrastructure, including the European Programme for CI Protection, the CI Warning Information Network, the Directive on the Identification and Designation of European Critical Infrastructures and a strategy for Critical Information Infrastructure Protection. The Report then describes other EU policy areas which are relevant to CI protection, namely EU Policy on Network and Information Security, the Directive on the Protection of Personal Data and the Directive on the Retention of Data.

2 Reference Material

The material used in the preparation of this Report, comprising EU legislation and communications, has been specified in each part of the Report and is publically available. Unless otherwise indicated, the material can be obtained from the EU EUR-Lex website, http://eur-lex.europa.eu/en/index.htm, which provides free access to EU law and other public documents. The reference documents used in this Report can be located using the search facility provided in this website.

3 EU Policy and Legislation for the Protection of Critical Infrastructure

3.1 Introduction

The essential nature of CI and the consequences of disruption thereto comprise a key issue of concern to the EU and reducing the vulnerabilities of CI is one of the major objectives of the EU. Since 2004, the EU has taken the initiative on the issue of CI protection (CIP) by working towards a common European approach in this field.

In this regard, the Council and Commission of the EU have created a strategy to strengthen the protection of CI in Europe, proposing and developing a number of specific protection measures. These include the European Programme for CI Protection, the CI Warning Information Network, the Directive on the identification and designation of European critical infrastructures and a strategy for Critical Information Infrastructure Protection. These are described in details below.

3.2 European Programme for CI Protection

The European Programme for CI Protection (EPCIP) is a package of measures established by the institutions of Europe to improve the protection of European CI - across all EU Member States and in all relevant sectors of economic activity.

3.2.1 History

EPCIP was instigated in 2004 by the European Council, as part of development of an overall strategy for CI protection (CIP) in Europe. The Council of the EU requested the European Commission to put forward measures for Europe-wide CIP and the Commission proposed the concept of the EPCIP in Communication COM(2004)702. The EPCIP concept was endorsed by the Council, and presented to relevant CI stakeholders in the Commission Communication COM(2005)576, as part of the consultation process on the establishment of EPCIP. This Communication presented the possible EPCIP policy options and requested feedback. Using the information gathered from this exercise, the Commission then set out the proposed principles, processes and instruments for the implementation of EPCIP in Communication COM(2006)786. Reviews of EPCIP were carried out from 2006, and the findings published in the EC Staff Working Documents SWD(2012)190 and SWD(2013)318.

3.2.2 EPCIP goal

The goal of EPCIP, as described in COM(2004)702 and reiterated in COM(2005)576, is to ensure that there is adequate and uniform levels of protective security for European CI, minimal points of CI failure and tested rapid reaction arrangements for CI disruption throughout the EU. EPCIP will identify European CI, analyse their vulnerability and interdependence and propose solutions to protect from and prepare for all hazards.

3.2.3 CI Definitions

To create a programme for CIP in Europe, it is first necessary to identify what is meant by the terms 'critical infrastructure' and 'critical infrastructure protection'. A definition for 'critical infrastructure' was proposed in COM(2004)702 as:

> **Critical Infrastructures** are physical and information technology facilities, networks services and assets which, if disrupted or destroyed, would have a serious impact on the health, security or economic well-being of citizens or the functioning of governments in EU countries.

Typical CI includes energy installations and networks, communications and information technology, finance, health care, food, water, transport, production, storage and management of dangerous goods, government. In COM(2005)576, three types of infrastructure assets were identified, namely : public, private and governmental infrastructure assets and interdependent cyber and physical networks; procedures and, where relevant, individuals that exert control over CI functions; objects having cultural or political significance as well as 'soft targets' which include mass events (i.e. sports, leisure and cultural).

COM(2005)576 suggests an indicative list of CI sectors, as given in Annex 1.

COM(2005)576 further proposed a definition for critical infrastructure protection as:

> **Critical Infrastructure Protection** is the ability to prepare for, protect against, mitigate, respond to, and recover from critical infrastructure disruptions or destruction.

Various other definitions relevant to the issue of CIP in Europe were set down in communication COM(2005)576, as described in the table below:

Alert - notification that a potential disaster situation will occur, exists or has occurred.

Contingency Plan - a plan used by a Member State (MS) and critical infrastructure owners/operators to decide how to respond to a specific systems failure or disruption of essential service.

Essential Service - applied to utilities (water, gas, electricity, etc.), standby power systems, environmental control systems, communication networks which, if interrupted, presents a risk to public safety and confidence, threatens economic security, or impedes the continuity of a MS government and its services.

Impact - the total sum of the different effects of an incident, such as geographic scope and severity.

Interdependency - identified connections or lack thereof between and within CI sectors.

Prevention - a range of tasks and activities required to build, sustain, and improve the operational capability of a CI, to prevent, protect against, respond to, and recover from an incident.

Occurrence - an event (either human caused or by natural phenomena) that requires a serious emergency response to protect life or property or puts at risk public safety and confidence, seriously disrupts the economy, or impedes the continuity of a MS government and its services.

Response - activities that address the short-term direct effects of a CI incident.

Risk - the possibility of loss, damage or injury due to a CI incident.

Threat - any indication, circumstance, or event with the potential to disrupt or destroy critical infrastructure, or any element thereof.

Vulnerability - a characteristic of an element of a CI's design, implementation or operation that renders it susceptible to destruction or incapacitation by a threat.

3.2.4 European Critical Infrastructure Definition

In addition to the above, in order to create a programme for the protection of European CI, it is necessary to define what is meant by a 'European Critical Infrastructure (ECI)'. This was described in COM(2005)576 as:

European Critical Infrastructures include those physical resources, services, and information technology facilities, networks and infrastructure assets, which, if disrupted or destroyed would have a serious impact on the health, safety, security, economic or social well-being of two or more European Union Member States.

To decide if a CI is a ECI, several factors should be taken into account including the cross border effect of the CI, which ascertains whether an incident could have a serious impact beyond its MS national territory or two or more MS national territories, and the interdependencies between MS CI, in particular to identify which MS would be affected by a major CI incident.

The procedure for the identification and designation of ECI and a common approach to the assessment of the needs to improve the protection of such infrastructures has been established by means of an EU Directive (see below).

3.2.5 CI Threat Coverage of the EPCIP

There are many types of threats which endanger ECI. In Communication COM(2005)576 feedback was sought as to whether the EPCIP should seek to tackle all intentional and unintentional threats, or all threats with a priority on terrorist attacks, or just terrorist-initiated threats. An assessment of the responses indicated that, whilst recognising threats from terrorism as a priority, the protection of CI in the EPCIP should be based on an all hazards approach (COM(2006)786).

3.2.6 EPCIP Key Principles

A number of key principles which should be addressed by EPCIP was laid down in COM(2005)576 and developed in COM(2006)786. These included:

- Subsidiarity - the prime responsibility for CIP lies with individual EU MS and CI owners/operators, the EU should focus on aspects of CIP which have a cross border effect, i.e. on ECI rather than national or regional CI,
- Complementarity - the EPCIP framework should be complementary to existing CIP measures and avoid duplicating existing EU, national or regional CIP measures where these have proven to be effective,
- Confidentiality - CIP information should be shared in a confidential manner and should be classified at EU and MS levels,
- Stakeholder Cooperation - all stakeholders have a role to play in CIP and should contribute to the development and implementation of EPCIP,
- Proportionality - CIP strategies and measures should be proportional to the level of risk, taking account of the threat, relative criticality, cost-

benefit ratio and necessary level of protection. CIP measures should only be proposed where a gap in existing CI security has been identified, and

- Sector-by-sector approach – since various sectors possess particular CIP experience expertise and requirements, EPCIP will be developed on a sector-by-sector basis and implemented following an agreed list of CIP sectors.

3.2.7 Common Framework for EPCIP

A common framework for CIP in Europe is appropriate because damage or loss of a CI in one MS may have negative effects on one or more other MS and on the European economy as a whole. The common EU level framework for CIP in Europe set out in EPCIP ensures that each MS is providing adequate and equal levels of CIP.

The common EPCIP framework seeks:

- to define the competence and responsibilities of all CIP stakeholders,
- set down the basis for sector-specific protection,
- complement existing measures at EU and MS levels,
- set out a common list of CIP definitions and CI sectors,
- describe sector-by-sector CIP criteria; comprise common CIP principles and objectives,
- comprise commonly-agreed methodologies and codes/standards,
- exchange best practices; define CIP priority areas, and
- elucidate agreed benchmarks.

The common framework could be voluntary or mandatory, although only a legal framework would provide a strong and enforceable basis for a coherent and uniform implementation of EU-wide CIP.

3.2.8 EPCIP Implementation Measures

Communication COM(2005)576 identified a number of areas where differences in MS practice could lead to inconsistencies and difficulties in European CIP and the proposed EPCIP implementation and supporting measures to address these. For example, different MS have different alert levels corresponding to different CI incidents. This may make it difficult for trans-national companies to prioritise their expenditure on CIP measures. It is therefore beneficial to harmonise different alert levels and for MS to work with a common methodology of identifying and classifying CI threats, capabilities, risks, and vulnerabilities and drawing conclusions about the possibility, probability, and degree of severity posed by a threat.

A number of measures were proposed by the Commission in COM(2006)786 to facilitate the implementation of EPCIP and to further EU level work on CIP. These included the EPCIP Action Plan, the use of CIP expert groups at EU level, CIP information sharing processes and the identification and analysis of interdependencies.

i) EPCIP Action Plan

This sets out the actions to be achieved along with relevant deadlines, takes into account sector specificities, involves, as appropriate, other stakeholders and is updated regularly based on the progress made.

The Action Plan organises CIP related activities around three 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 ECI and is implemented at a sectorial level, and
- work stream 3 supports MS in their activities concerning National Critical Infrastructures.

ii) CIP Information Sharing Process

CIP information exchange will facilitate:

- improved and accurate information and understanding about CI interdependencies, threats, vulnerabilities, security incidents, counter measures and best practices,
- increased awareness of CI issues,
- stakeholder dialogue, and
- better focused training, research and development.

However it is recognised that the CIP information sharing process among relevant stakeholders requires a relationship of trust, such that proprietary, sensitive or personal information that has been shared voluntarily will not be publicly disclosed and sensitive data is adequately protected. Care must be taken to respect privacy rights. CIP information will not be used other than for the purpose of protecting CI and any personnel handling classified information will have an appropriate level of security vetting by their MS.

iii) Identification and Analysis of CI Interdependencies

The identification and analysis of CI interdependencies, both geographic and sectorial in nature, is an important element of improving CIP in Europe. This ongoing process will feed into the assessment of vulnerabilities, threats and risks concerning ECI.

CI interdependencies will extend beyond the EU and consequently, enhancing

CIP cooperation outside Europe through such measures as sector-specific memoranda of understanding and encouraging the raising of CIP standards outside of the EU should therefore be an important element of EPCIP.

3.2.9 Dialogue with CI Owners, Operators and Users

The success of any CI protection programme depends on the cooperation and level of involvement that can be achieved with the CI owners and operators. EPCIP should therefore engage the owners and operators of CI in partnerships. A common approach to bring together all stakeholders in the CI public and private sphere would provide each MS, the Commission and the CI industry with an important platform through which to communicate. Where relevant, the Commission could encourage the creation of European CIP related industry/business associations.

3.2.10 Role of CI Owners, Operators and Users in EPCIP

Designation of an infrastructure as a MS CI or an ECI implies certain responsibilities for its owners, operators and users. Communication COM(2005)576 recognises this and describes what these responsibilities might involve. Four particular responsibilities are envisaged:

- notification to a relevant MS CIP body of the fact that an infrastructure may be of a critical nature,
- designation of a senior representative(s) to act as Security Liaison Officer (SLO) between the owner/operator and the relevant MS CIP authority,
- establishment, implementation and updating of an Operator Security Plan (OSP), and
- participation in the development of a contingency plan relative to the CI with relevant MS civil protection and law enforcement authorities where requested.

The OSP is intended to present a vehicle for a bottom up approach in regulating MS and European CIP, that gives leeway and responsibility to the private sector in the development of CIP measures.

It is suggested that the Operator Security Plan (OSP) would identify the owner/operator CI assets and establish relevant security solutions for their protection. The OSP should describe methods and procedures which are to be followed to ensure compliance with EPCIP, National CIP Programmes and relevant sector-specific CIP programmes and identify the critical points of a CI on which security protective measures could be concentrated.

The OSP could contain security measures arranged around two headings:

- permanent security measures, which would identify indispensable security procedures and investment, for which the owner/operator would maintain alertness against potential threats, and
- graduated security measures, which could be activated according to varying threat levels.

Submit for approval to the relevant MS CIP sector authority which would guarantee the consistency of security measures taken by specific owners and operators and the relevant sectors in general. In return owners and operators could be given relevant feedback and support as to relevant threats, development of best practices and where appropriate help in assessing interdependencies and vulnerabilities.

A suggested OSP template is shown in Annex 2.

3.2.11 The Role of National CI in EPCIP

In COM (2005)576 it is suggested that, in the interests of MS and the EU, each MS protects its national CI (NCI) under a common framework so that owners/operators throughout Europe benefit from a uniform CIP approach. National CIP programmes for NCI could be based on the common framework provided by EPCIP.

To achieve efficiency and coherency it is suggested that it is a necessity to designate a single CI body in each MS to deal with the overall implementation of EPCIP. Specific competences of the MS CI body could include:

- coordination, monitoring and overseeing of the overall implementation of EPCIP in a MS,
- serving as the main institutional contact point on CIP matters with the Commission, other MS and CI owners and operators,
- participation in the designation of ECI,
- taking the legal decision on designation of an infrastructure under its jurisdiction as a NCI,
- serve as an authority of legal recourse for owners/operators who do not agree that their infrastructure is a CI.

COM(2006)786 further developed the envisaged role of NCI in EPCIP. It is suggested that the responsibility for protecting NCI falls on the NCI owners/operators and on the MS, with due regard to existing European Community competences. The Commission will support the MS in these efforts where requested to do so. The measures proposed by the Commission to facilitate the implementation of EPCIP and to further EU level work on CIP include support for MS concerning NCI.

With a view to improving the protection of NCI, each MS is encouraged to establish a National CIP Programme. The objective of such programmes would be to set out each MS approach to the protection of NCI located within its territory. Such programmes would at a minimum address the following issues:

- the identification and designation by the MS of NCI according to predefined national criteria, these criteria would be developed by each MS taking into account as a minimum the following qualitative and quantitative effects of the disruption or destruction of a particular infrastructure:
    - scope - the disruption or destruction of a particular CI will be rated by the extent of the geographic area which could be affected by its loss or unavailability,
    - severity - the consequences of the disruption or destruction of a particular infrastructure will be assessed on the basis of public effect (number of population affected), economic effect (significance of economic loss and/or degradation of products or services), environmental effect, political effects, psychological effects, and public health consequences,
- the establishment of a dialogue with CIP owners/operators,
- identification of geographic and sectorial interdependencies,
- drawing-up NCI related contingency plans where deemed relevant, and
- each MS is encouraged to base its National CIP Programme on the common list of CI sectors established for ECI.

The introduction of similar approaches to the protection of NCI in the MS would contribute to ensuring that CI stakeholders throughout Europe benefit from not being subjected to varying frameworks resulting in additional costs and that the Internal Market is not distorted.

3.2.12 Evaluation and monitoring of EPCIP

It is recognised throughout the development and implementation process of EPCIP that evaluation and monitoring is essential.

It is suggested that evaluation and monitoring of the implementation of EPCIP should comprise a multi-level process which requires the involvement of all stakeholders:

- at EU level, a peer evaluation mechanism could be established, in which MS and the Commission would work together on assessing the overall level of implementation of EPCIP in each MS, Commission annual progress reports concerning the implementation of EPCIP could be prepared,

- the Commission would report progress to MS and other institutions each calendar year in a Commission staff working paper,
- at MS level, the overall EPCIP implementation should be monitored ensuring compliance with National CIP Programme(s) and sector-specific CIP programmes, through yearly reports to the Council and Commission.

Specific evaluation and monitoring reports on the implementation of EPCIP were produced as Commission Staff Working Documents SWD(2012)190 and SWD(2013)318. In SWD(2012)190, it was recognised that the sector approach of EPCIP represented challenges to a number of MS, as the usual practice in the analysis of criticalities is not restricted by sectorial boundaries and follows a system or service approach. In SWD(2013)318, after evaluation of the experience gained from EPCIP implementation since 2006, it was decided that a new approach to EPCIP was required. In parallel with this new approach, MS and the private sector should continue their efforts of identifying ECI, building on their work so far and on the results of the projects already pursued under EPCIP.

3.2.13 New Approach to EPCIP

SWD(2013)318 describes the new approach as a result of a comprehensive review of EPCIP conducted in close cooperation with MS and CI stakeholders. The reshaped EU CIP approach builds upon the existing EPCIP framework by focusing on its strengths and addressing the gaps identified in the review process.

One such gap is the recognition and cognisance of interdependencies between CI, industry, and MS actors. Threats to a single CI can have a very significant impact on a broad range of actors in different infrastructures. The effects of these interdependencies are not limited to single countries; many CI have a cross border dimension. In addition to interdependencies between sectors, there are also many interdependencies within the same sector spanning a number of MS. One such example is the European high-voltage electricity grid, composed of the interconnected national high-voltage electricity grids.
It is therefore necessary to study the extent to which impact of one CI on another is taken into account in current CIP planning and how consideration of interdependencies can be improved.

This will be achieved by selecting and working with four CI having a European dimension – Eurocontrol (EU Air Traffic Management (ATM) Network Manager), Galileo (European programme for a global satellite navigation system), the Electricity Transmission Grid and the Gas Transmission Network - in order to optimise their protection and resilience. The four European CI were selected on the basis of their European nature due to their cross-border dimension, both physically (i.e. the infrastructures are located in the territory of more than one MS) and at the level of the service provided (i.e. a disruption of service in one MS can affect several other MS) and their representativeness, the selected CI cover the transport, space and energy sectors.

The first stage of the new EPCIP approach will be to work with the four European CI to ensure a comprehensive understanding of their CIP measures to date, in each of prevention, preparedness and response. This will include examining how interdependencies and cascading effects feed into their CIP planning. Common factors will be identified and ways in which CIP and resilience measures can be improved considered.

I. Prevention

The work done so far will be reviewed in order to provide an update on the progress in CI security measures and the evolving interdependences within sectors (ICT, water, etc.).

The Commission will then work with the selected European CI to set up tools for risk assessment and risk management, taking account of existing research and innovation activities. These include the Environment Theme of FP7, in particular the development of hazard risk assessment methodologies, and the EU Cybersecurity Strategy, which identifies actions that will further contribute to the cyber resilience and security of infrastructures covered by EPCIP. Where appropriate, knowledge among the selected European CI will be shared to identify opportunities to strengthen existing protection plans. Dialogue between the CI operators and the actors upon whom they rely will be encouraged along with exchanges of best practices and the development of scenario exercises, guidelines and recommendations. The Commission will play a supporting and facilitating role, developing guidelines, methodological tools, and other support tools to contribute to the overall assessment of CI dependencies and criticalities.

II. Preparedness

The Commission will then support the development of preparedness strategies based around contingency planning, stress tests, awareness raising, training, joint courses, exercises and staff exchange. The establishment of such structures can also be supported by promoting incident reporting, which can be encouraged as a means to improve the level of knowledge on the performance of CI during a disruptive event (e.g. the extent of cascading effects, overall impact, etc.). Work will be carried out to develop further a picture of what is useful at European level.

The Commission will again promote and facilitate dialogue between the operators of the selected European CI and those who rely upon them. The aim is to increase consideration by the MS and other actors reliant upon CI of how they can prepare a response to events affecting ECI.

III. Response

Having facilitated dialogue on preparedness, the Commission can then help identified actors think about their response to CI events. The aim is to strengthen the links between the CI community and early warning systems, as early warning tools for natural disasters can point to potential threats to CI.

Mechanisms for long-term recovery of critical services will be considered, for example promotion of the use of recovery specialists deployed at the request of MS. The Commission and the selected European CI will work on establishing specific CIP modules within the mechanisms, or including the required CIP expertise in existing modules.

In terms of the new approach to EPCIP, the pilot phase will start immediately, establishing a roadmap, setting out the aims to be completed by the second half of 2014, after which time the Commission will report back on progress and the way ahead.

MS and other stakeholders (such as operators' associations), will be invited to have an active role in all stages of the pilot phase. The benefits of this will be three-fold: an increased understanding of how actors in the MS (both public and private sector) rely on the selected European CI; greater access to the tools and best practice identified in the study of these CI; the opportunity to contribute to the discussion on how CI can best benefit from EU structures to improve their protection.

This new approach to EPCIP provides the opportunity to make CIP planning in Europe more cohesive and helps ensure that each MS has an optimum CIP plan. By fostering dialogue between CI sectors and involving MS in the dialogue, best practice can be disseminated.

Following the pilot phase, the Commission anticipates that the new EPCIP approach could lead in the following directions. The application of the work with the selected European CI should provide the necessary indicators to allow for the shaping of an EU approach towards CIP. This would be based on the results achieved and the gaps identified, and seek to provide useful tools for improving CI protection and resilience, including strengthened risk mitigation, preparedness and response measures. The approach could be implemented in regions where MS are interested in cooperating with each other, for example a resilience concept for the overall critical transport infrastructure around the Baltic Sea and a programme for supply chain criticalities in the Danube region.

The new EPCIP approach could thus encourage and nurture the development of CIP at all levels, from local and national to European and international, making the EU more secure and better prepared for threats to its CI, and improving overall resilience if disruptions occur.

3.3 CI Warning Information Network

The CI Warning Information Network (CIWIN) was proposed by the Commission as part of the development of an overall strategy for CIP in Europe and, in particular, as a supporting measure for the implementation of EPCIP. The intention of CIWIN is to provide a multi-level communication system for exchanging CIP related ideas, studies and good practices, and serve as a repository for such information.

In COM (2005)576, the Commission suggested creating CIWIN to stimulate the development of appropriate protection measures by facilitating an exchange of best practices in a secure manner, as well as being a vehicle for transmission of immediate threats and alerts, and put forward three options for the development of CIWIN:

- CIWIN would be in the shape of a forum limited to the exchange of CIP ideas and best practices in support of CI owners and operators; such a forum could take the form of a network of experts and an electronic platform for the exchange of relevant information in a secure environment; the Commission would play an important role in gathering and disseminating such information,
- CIWIN would be a rapid alert system (RAS) linking MS with the Commission, this option would increase the security of CI by providing warnings limited to immediate threats and alerts; the objective would be to facilitate a rapid exchange of information about potential threats to CI owners and operators,
- CIWIN would be a multi-level communication/alert system composed of two distinct functions: a) a RAS linking MS with the Commission and b) a forum for the exchange of CIP ideas and best practices.

A study was launched to determine the scope and technical specifications necessary for CIWIN and its interface with the MS.

In COM(2006)786, it was decided that CIWIN should be set up through a separate Commission proposal, which was issued in the form of a proposal for a Council Decision COM(2008)676, described below.

The CIWIN initiative is part of EPCIP, being concerned specifically with the information-sharing process between EU MS and an information technology system to support that process. CI in the EU is subjected to a varying puzzle of protective measures and obligations, with no minimum standards being applied horizontally. Addressing the exchange of information between MS is a complex area that requires a well-considered approach. It is important to prevent duplications of activities resulting from insufficient information on similar situations in other MS. Furthermore, there is a fear of exchanging sensitive information among CI stakeholders. If information is to be exchanged efficiently, an environment of trust and flexibility has to be established.

No provisions on the exchange of information and alerts in the field of CI protection currently exist in the EU. A number of sectorial RAS exist in the EU. The main difference between CIWIN and the existing RAS is the cross sectorial nature of CIWIN, none of the existing RAS provide a horizontal and cross sectorial functionality that would be accessible to a wider range of stakeholders.

The CIWIN proposal is fully consistent with the objectives of the EU. It is consistent with other policies as it does not aim to replace existing measures, but to complement them with a view to improving ECI protection.

All relevant stakeholders have been consulted on CIWIN through and within the consultation on EPCIP. The responses to EPCIP and ongoing discussions with all stakeholders have had a major impact in shaping the proposal for CIWIN and the final concept of CIWIN is the result of these discussions.

The Commission carried out an impact assessment regarding various different policy options for CIWIN. It was concluded that the policy option of CIWIN as a secure voluntary/opt-in multi-level communication/alert system with two distinct functions: a rapid alert system and an electronic forum for the exchange of CIP ideas and best practices clearly showed the most advantageous ratio between benefits and drawbacks.

A Council Decision is proposed as the instrument for the implementation of CIWIN, as, in order for the CIWIN prototype to become fully functional and available to all EU MS, a legal basis is needed. As the subject addressed by this legal instrument is specific and not general in scope, a Council Decision is best suited to achieve this goal, and at the same time oblige the users of the system (MS and the Commission) to respect the potential confidentiality of the information exchanged.

The main provisions of the Proposal for a Council Decision on CIWIN are given below.

Article 1 Subject-matter

This Decision sets up a secure information, communication and alert system with the aim of assisting MS to exchange information on shared threats, vulnerabilities and appropriate measures and strategies to mitigate risks related to CIP.

Article 2 Definitions

For the purpose of this Decision, the following definitions shall apply:

“Critical Infrastructure” shall mean those assets, systems or parts thereof located in MS which are essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a MS as a result of the failure to maintain those functions.

"Participating Member State" shall mean the MS having signed a Memorandum of understanding with the Commission.

"CIWIN Executive" shall mean the CIWIN contact point in a relevant MS or the Commission that ensures adequate use of CIWIN and compliance with the user guidelines within the relevant MS or the Commission.

"Threat” shall mean any indication, circumstance, or event with the potential to disrupt or destroy CI, or any element thereof.

Article 3 Participation

Participation in and use of CIWIN is open to all MS. The participation in CIWIN shall be conditional upon the signature of a Memorandum of understanding that contains technical and security requirements applicable to CIWIN, and information on the sites to be connected to CIWIN.

Article 4 Functionalities

(1) The CIWIN shall consist of the two following functionalities:

  (a) an electronic forum for CIP related information exchange;

  (b) a rapid alert functionality that shall enable participating MS and the Commission to post alerts on immediate risks and threats to CI.

(2) The electronic forum shall be composed of fixed areas and dynamic areas. Fixed areas shall include MS Areas, Sector Areas e.g. Energy, Transport and Water, CIWIN Executive Area, EU External Co-operation Area, Contact Directory. Dynamic areas shall include Expert Working Group Area, Project Area, Alert Areas, Special Topics Area.

Article 5 Role of the Member States

(1) Participating MS shall designate a CIWIN Executive and notify the Commission thereof. The CIWIN Executive shall be responsible for granting or denying access rights to the CIWIN within the relevant MS.

(2) Participating MS shall provide access to the CIWIN in compliance with the guidelines adopted by the Commission.

(3) Participating MS shall provide and regularly update relevant CIP information of common EU interest.

Article 6 Role of the Commission

(1) The Commission shall be responsible for:

(a) the technical development and management of the CIWIN, including the IT structure thereof and the elements for information exchange;

(b) laying down guidelines on the terms of use of the system, including confidentiality, transmission, storage, filing and deletion of information. The Commission shall also establish the terms and procedures for granting full or selective access to the CIWIN.

(2) The Commission shall appoint the CIWIN Executive, responsible for granting or denying access rights to the CIWIN within the Commission.

(3) The Commission shall provide and regularly update relevant CIP information of common EU interest.

Article 7 Security

(1) The CIWIN shall be established as a secure classified system, and shall be capable of handling information up to the level of RESTREINT UE. The Commission shall decide on the most appropriate technological platform for CIWIN and users shall meet the technical requirements established by the Commission. The security classification of the CIWIN shall be upgraded as appropriate.

(2) Users' rights to access documents shall be on a “need to know” basis and must at all times respect the author’s specific instructions on the protection and distribution of a document.

(3) MS and the Commission shall take the necessary security measures:

(a) to prevent any unauthorised person from having access to the CIWIN;

(b) to guarantee that, when using CIWIN, authorised persons have access only to data which are within their sphere of competence;

(c) to prevent information on the system from being read, copied, modified or erased by unauthorised persons.

(4) The uploading of information onto CIWIN shall not affect the ownership of the information concerned. Authorised users shall remain solely responsible for the information they provide and shall ensure that its contents are fully compliant with existing Community and national law.

Article 8 User guidelines

The Commission shall develop and regularly update User guidelines containing full details of CIWIN's functionalities and roles.

Article 9 Costs

The costs incurred in connection with the operation, maintenance and central functioning of the CIWIN shall be borne by the Community budget. Costs related to users' access to CIWIN within participating Member States shall be borne by participating Member States.

Article 10 Reviewing

The Commission shall review and evaluate the operation of the CIWIN every three years, and shall submit regular reports to the MS.

Annexes to the proposal for the Council Decision for CIWIN set out the mechanisms to be used for evaluation and monitoring of CIWIN. The following indicators of progress are to be used in order to assess progress being made by CIWIN:

- number of MS participating in the CIWIN system (at least 20 MS should use it regularly in order for the system to be deemed successful),
- the level of confidentiality of the information exchanged (are MS uploading only non-classified information or is classified information uploaded as well), and
- are CIP experts group using CIWIN as a main tool for the exchange of opinions in order to achieve their objectives (e.g. definition of the criteria to identify critical infrastructure in specific sectors).

After the conclusion of the testing period (CIWIN pilot project) in 2009, the Commission proposed assessing the satisfaction of MS with the CIWIN system and verification of whether it contributes to the general objectives of the CIWIN initiative. Measures taken following an intermediate/ex-post evaluation include a review by the Commission every 3 years. The Commission based its review on MS opinions obtained at the regular CIP Contact Points meetings.

In SWD(2013)318, the progress of CIWIN was described. CIWIN was moved into the production phase in October 2012 and has been operational since

January 2013. In the first months of operation, positive developments were observed, including an increase in usage statistics and the use of the dedicated CIWIN area for national purposes. The Commission expects that CIWIN will continue to improve, serving as an important interactive tool for the development of the EU approach to CIP.

3.4 Directive 2008/114/EC Identification and Designation of ECI and the Assessment of the Need to Improve their Protection

The Directive forms part of the Commission's overall strategy for the protection of CI in Europe and is a key element in the implementation of EPCIP. COM(2006)787 set out a proposal for the Directive, presenting the measures that the Commission recommended for the identification and designation of ECI and the assessment of improvement of their protection.

This Communication identified the need for a common framework for ECI, as only this can provide the necessary basis for a coherent and uniform implementation of measures to enhance the protection of ECI, as well as defining clearly the respective responsibilities of relevant stakeholders. An ECI identification and designation procedure, and a common approach to the assessment of ECI protection can only be established by way of a directive in order to ensure:

- adequate levels of protection concerning ECI,
- all ECI stakeholders are subjected to similar rights and obligations, and
- the stability of the Internal Market is maintained.

Effective protection requires communication, coordination, and cooperation nationally and at EU level involving all relevant stakeholders. Full involvement of the private sector is important as most critical infrastructure is privately owned and operated.

All relevant stakeholders have been consulted concerning the development of EPCIP, through the EPCIP Green Paper (COM(2005)576), CIP seminars hosted by the Commission, informal meetings of CIP Contact Points, and informal meetings with private sector representatives. Available expertise was collected through various meetings and seminars. An EPCIP Impact Assessment was also carried out.

The MS have varying approaches to CIP and different legal systems. A Directive is therefore best suited to create a common procedure for the identification and designation of ECI, and a common approach to the assessment of the needs to improve the protection of such infrastructures.

The key ideas put forward by the proposal for the Directive include:

- the creation of a basic EU level coordination mechanism,
- putting an obligation on MS to identify their CI,
- implementation of a set of basic security measures for CI, and

- the identification and designation of key ECI.

Directive 2008/114/EC, as enacted, largely mirrors its proposal as set out in COM(2006)787. The CI sectors used for the implementation of the Directive are to be the energy and transport sectors.

Directive 2008/114/EC comprises the following Articles:

ARTICLE 1
Subject matter
This Directive establishes a procedure for the identification and designation of European critical infrastructures ('ECIs'), and a common approach to the assessment of the need to improve the protection of such infrastructures in order to contribute to the protection of people.

ARTICLE 2
Definitions
For the purpose of this Directive:
(a) 'critical infrastructure' means an asset, system or part thereof located in MS which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a MS as a result of the failure to maintain those functions;
(b) 'European critical infrastructure' or 'ECI' meansCI located in MS the disruption or destruction of which would have a significant impact on at least two MS. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure;
(c) 'risk analysis' means consideration of relevant threat scenarios, in order to assess the vulnerability and the potential impact of disruption or destruction of critical infrastructure;
(d) 'sensitive CIP related information' means facts about aCI, which if disclosed could be used to plan and act with a view to causing disruption or destruction of CI installations;
(e) 'protection' means all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralise a threat, risk or vulnerability;
(f) 'owners/operators of ECIs' means those entities responsible for investments in, and/or day-to-day operation of, a particular asset, system or part thereof designated as an ECI under this Directive.

ARTICLE 3

Identification of ECIs

1. Each MS shall identify potential ECIs which both satisfy the cross-cutting and sectorial criteria and meet the definitions set out in Article 2(a) and (b).

The Commission may assist MS at their request to identify potential ECIs.

The Commission may draw the attention of the relevant MS to the existence of potential CI which may be deemed to satisfy the requirements for designation as an ECI.

Each MS and the Commission shall continue on an ongoing basis the process of identifying potential ECIs.

2. The cross-cutting criteria referred to in paragraph 1 shall comprise the following:

(a) casualties criterion (assessed in terms of the potential number of fatalities or injuries);

(b) economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects);

(c) public effects criterion (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life; including the loss of essential services).

The cross-cutting criteria thresholds shall be based on the severity of the impact of the disruption or destruction of a particular infrastructure. The precise thresholds applicable to the cross-cutting criteria shall be determined on a case-by-case basis by the MS concerned by a particular critical infrastructure. Each MS shall inform the Commission on an annual basis of the number of infrastructures per sector for which discussions were held concerning the cross-cutting criteria thresholds.

The sectorial criteria shall take into account the characteristics of individual ECI sectors.

The Commission together with the MS shall develop guidelines for the application of the cross-cutting and sectorial criteria and approximate thresholds to be used to identify ECIs.

The criteria shall be classified. The use of such guidelines shall be optional for the MS.

3. The sectors to be used for the purposes of implementing this Directive shall be the energy and transport sectors. The subsectors are identified in Annex I.

If deemed appropriate and in conjunction with the review of this Directive as laid down in Article 11, subsequent sectors to be used for the purpose of implementing this Directive may be identified. Priority shall be given to the ICT sector.

ARTICLE 4

Designation of ECIs

1. Each MS shall inform the other MS which may be significantly affected by a potential ECI about its identity and the reasons for designating it as a potential ECI.

2. Each MS on whose territory a potential ECI is located shall engage in bilateral and/or multilateral discussions with the other MS which may be significantly affected by the potential ECI. The Commission may participate in these discussions but shall not have access to detailed information which would allow for the unequivocal identification of a particular infrastructure.

A MS that has reason to believe that it may be significantly affected by the potential ECI, but has not been identified as such by the MS on whose territory the potential ECI is located, may inform the Commission about its wish to be engaged in bilateral and/or multilateral discussions on this issue. The Commission shall without delay communicate this wish to the MS on whose territory the potential ECI is located and endeavour to facilitate agreement between the parties.

3. The MS on whose territory a potential ECI is located shall designate it as an ECI following an agreement between that MS and those MS that may be significantly affected. The acceptance of the MS State on whose territory the infrastructure to be designated as an ECI is located, shall be required.

4. The MS on whose territory a designated ECI is located shall inform the Commission on an annual basis of the number of designated ECIs per sector and of the number of MS dependent on each designated ECI. Only those MS that may be significantly affected by an ECI shall know its identity.

5. The MS on whose territory an ECI is located shall inform the owner/operator of the infrastructure concerning its designation as an ECI. Information concerning the designation of an infrastructure as an ECI shall be classified at an appropriate level.

6. The process of identifying and designating ECIs pursuant to Article 3 and this Article shall be completed by 12 January 2011 and reviewed on a regular basis.

ARTICLE 5

Operator security plans

1. The OSP procedure shall identify the CI assets of the ECI and which security solutions exist or are being implemented for their protection.

2. Each MS shall assess whether each designated ECI located on its territory possesses an OSP or has in place equivalent measures. If a MS finds that such an OSP or equivalent exists and is updated regularly, no further implementation action shall be necessary.

3. If a MS finds that such an OSP or equivalent has not been prepared, it shall ensure by any measures deemed appropriate, that the OSP or equivalent is prepared. Each MS shall ensure that the OSP or equivalent is in place and is reviewed regularly within one year following designation of the CI as an ECI. This period may be extended in exceptional circumstances, by agreement with the MS authority and with a notification to the Commission.

4. In a case where supervisory or oversight arrangements already exist in relation to an ECI such arrangements are not affected by this Article and the relevant MS authority referred to in this Article shall be the supervisor under those existing arrangements.

5. Compliance with measures including Community measures which in a particular sector require, or refer to a need to have, a plan similar or equivalent to an OSP and oversight by the relevant authority of such a plan, is deemed to satisfy all the requirements of MS under, or adopted pursuant to, this Article. The guidelines for application referred to in Article 3(2) shall contain an indicative list of such measures.

ARTICLE 6

Security Liaison Officers

1. The SLO shall function as the point of contact for security related issues between the owner/operator of the ECI and the relevant MS authority.

2. Each MS shall assess whether each designated ECI located on its territory possesses a SLO or equivalent. If a MS finds that such a Security Liaison Officer is in place or an equivalent exists, no further implementation action shall be necessary.

3. If a MS finds that a Security Liaison Officer or equivalent does not exist in relation to a designated ECI, it shall ensure by any measures deemed appropriate, that such a SLO or equivalent is designated.

4. Each MS shall implement an appropriate communication mechanism between the relevant MS authority and the SLO or equivalent with the objective of exchanging relevant information concerning identified risks and threats in relation to the ECI concerned. This communication mechanism shall be without prejudice to national requirements concerning access to sensitive and classified information.

5. Compliance with measures including Community measures which in a particular sector require, or refer to a need to have, a SLO or equivalent, is deemed to satisfy all the requirements of MS in, or adopted pursuant to, this Article. The guidelines for application referred to in Article 3(2) shall contain an indicative list of such measures.

ARTICLE 7

Reporting

1. Each MS shall conduct a threat assessment in relation to ECI subsectors within one year following the designation of CI on its territory as an ECI within those subsectors.

2. Each MS shall report every two years to the Commission generic data on a summary basis on the types of risks, threats and vulnerabilities encountered per ECI sector in which an ECI has been designated pursuant to Article 4 and is located on its territory. A common template for these reports may be developed by the Commission in cooperation with the MS. Each report shall be classified at an appropriate level as deemed necessary by the originating MS.

3. Based on the reports referred to in paragraph 2, the Commission and the MS shall assess on a sectorial basis whether further protection measures at Community level should be considered for ECIs. This process shall be undertaken in conjunction with the review of this Directive as laid down in Article 11.

4. Common methodological guidelines for carrying out risk analyses in respect of ECIs may be developed by the Commission in cooperation with the MS. The use of such guidelines shall be optional for the MS.

ARTICLE 8

Commission support for ECIs

The Commission shall support, through the relevant MS authority, the owners/operators of designated ECIs by providing access to available best practices and methodologies as well as support training and the exchange of information on new technical developments related to CIP.

ARTICLE 9

Sensitive European critical infrastructure protection-related information

1. Any person handling classified information pursuant to this Directive on behalf of a MS or the Commission shall have an appropriate level of security vetting. MS, the Commission and relevant supervisory bodies shall ensure that sensitive ECI protection-related information submitted to the MS or to the Commission is not used for any purpose other than CIP.

2. This Article shall also apply to non-written information exchanged during meetings at which sensitive subjects are discussed.

ARTICLE 10

ECI protection contact points

1. Each MS shall appoint a ECI protection contact point (‘ECIP contact point’).

2. ECIP contact points shall coordinate ECIP issues within the MS, with other MS nad with the Commission. The appointment of an ECIP contact point does not preclude other authorities in a MS from being involved in ECIP issues.

ECI OSP PROCEDURE

The OSP will identify CI assets and which security solutions exist or are being implemented for their protection. The ECI OSP procedure will cover at least:

1. identification of important assets;

2. conducting a risk analysis based on major threat scenarios, vulnerability of each asset, and potential impact; and

3. identification, selection and prioritisation of counter-measures and procedures with a distinction between:

- permanent security measures, which identify indispensable security investments and means which are relevant to be employed at all times. This heading will include information concerning general measures such as technical measures (including installation of detection, access control, protection and prevention means); organisational measures (including procedures for alerts and crisis management); control and verification measures; communication; awareness raising and training; and security of information systems,
- graduated security measures, which can be activated according to varying risk and threat levels.

Procedure for the identification by the MS of CI which may be designated as an ECI pursuant to Article 3

Article 3 requires each MS to identify the CI which may be designated as an ECI. This procedure shall be implemented by each MS through the following series of consecutive steps.

A potential ECI which does not satisfy the requirements of one of the following sequential steps is considered to be 'non-ECI' and is excluded from the procedure. A potential ECI which does satisfy the requirements shall be subjected to the next steps of this procedure.

<u>Step 1</u>

Each MS shall apply the sectorial criteria in order to make a first selection of CI within a sector.

<u>Step 2</u>

Each MS shall apply the definition of critical infrastructure pursuant to Article 2(a) to the potential ECI identified under step 1. The significance of the impact will be determined either by using national methods for identifying CI or with reference to the cross-cutting criteria, at an appropriate national level. For infrastructure providing an essential service, the availability of alternatives, and the duration of disruption/recovery will be taken into account.

Step 3

Each MS shall apply the transboundary element of the definition of ECI pursuant to Article 2(b) to the potential ECI that has passed the first two steps of this procedure. A potential ECI which does satisfy the definition will follow the next step of the procedure. For infrastructure providing an essential service, the availability of alternatives, and the duration of disruption/recovery will be taken into account.

Step 4

Each MS shall apply the cross-cutting criteria to the remaining potential ECIs. The cross-cutting criteria shall take into account: the severity of impact; and, for infrastructure providing an essential service, the availability of alternatives; and the duration of disruption/recovery. A potential ECI which does not satisfy the cross-cutting criteria will not be considered to be an ECI. A potential ECI which has passed through this procedure shall only be communicated to the MS which may be significantly affected by the potential ECI.

It is a requirement of Directive 2008/114/EC (Article 11) that a review of the Directive be carried out. An evaluation study on the implementation and application of the Directive was launched in 2011 and delivered final results in 2012, set out in SWD(2012)190.

It was found that the majority of MS implemented the provisions of the Directive by incorporating them into their national legislation and regulatory frameworks, using approaches such as new laws, amendments to existing laws, procedural changes to existing CIP-related activities. Some MS concluded that no legislative changes were required to implement the Directive and, instead, made procedural changes within their existing national CIP frameworks. No major difficulties were reported by MS in implementing the Directive, although some MS indicated that the sector-focused approach of the Directive produced some challenges.

In the identification of ECI, the Directive lays down steps to be followed and most MS have used these, with a few making adjustments and adaptations to align them with an existing national approach. Almost all MS started the process of identifying ECI with a list of their NCI – they considered the latter to be the 'whole set' from which the 'sub-set' of ECI was to be identified. This could lead to overlooking potential ECI not already identified as NCI.

The Directive further lays down steps for the designation of NCI as ECI. The

ECI designation process between MS has been managed using the ECI points of contact, appointed by each MS, as channels of communication to establish, mainly, bilateral agreements.

The impact of the Directive as perceived by the MS varied depending on the maturity of the MS national CIP programme. There was a strong perception that implementation of the Directive did not result in sufficiently clear and tangible improvements to ECI security levels, but that it had increased general CIP awareness and cooperation in the EU.

Further review of Directive 2008/114/EC was carried out and reported in SWD(2013)318. Whilst all MS have implemented the Directive by establishing a process to identify and designate ECI in the energy and transport sectors, less than 20 ECI have been designated and consequently very few new Operator Security Plans have been produced. Some clear CI of European dimension, such as main energy transmission networks, are not included. Despite having helped foster European cooperation in the CIP process, the Directive has mainly encouraged bilateral engagement of MS instead of a real European forum for cooperation.

The sector-focused approach of the Directive likewise represents a challenge to a number of Member States, as in practice the analysis of criticalities is not confined to sectorial boundaries and follows rather a ‘system’ or ‘service’ approach (e.g. hospitals, financial services).

The Directive was considered to be essential by a majority of stakeholders. The majority of the CIP community expects that the benefits brought by the current Directive, notably in raising awareness, will continue to increase.

It was proposed that by keeping the current Directive, consolidating the work done so far, and developing a cross sectorial approach to EPCIP, the shortcomings of the current approach can be addressed without losing the benefits of the current legal framework. Through this approach, an environment of trust and common goals can continue to be fostered.

3.5 Critical Information Infrastructure Protection

The EU has identified ICT systems as being of particular importance in the policy area of CI. In COM(2005)576, the concept of Critical Information Infrastructure (CII) was introduced and defined as:

> Critical Information Infrastructures are ICT systems that are critical infrastructures themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.).

The Communication further defined Critical Information Infrastructure Protection (CIIP) as:

> Critical Information Infrastructures Protection is the programs and activities of infrastructure owners, operators, manufacturers, users, and regulatory authorities which aim at keeping the performance of critical information infrastructures in case of failures, attacks or accidents above a defined minimum level of services and aim at minimising the recovery time and damage.

CIIP should be viewed as a cross-sector phenomenon rather than being limited to specific sectors.

In 2009, the Commission adopted a Communication, COM(2009)149, specifically addressing the issue of CIIP with the aim to protect Europe from large scale cyber-attacks and disruptions by enhancing preparedness, security and resilience. The Communication sets out a plan (the 'CIIP action plan') to strengthen the security and resilience of vital ICT infrastructures. The aim was to stimulate and support the development of a high level of preparedness, security and resilience capabilities both at national and European level, which approach was broadly endorsed by the European Council. The CIIP action plan details the work to be done in CIIP by the Commission, the MS and/or industry, with the support of the European Network and Information Security Agency (ENISA).

ICT systems, services, networks and infrastructures form a vital part of European economy and society, either providing essential goods and services or constituting the underpinning platform of other CI. They are typically regarded as CII as their disruption or destruction would have a serious impact on vital societal functions. The high dependence on CII, their cross-border interconnectedness and interdependencies with other infrastructures, as well as the vulnerabilities and threats they face raise the need to address their security and resilience in a systemic perspective as the frontline of defence against failures and attacks.

The Communication focused on prevention, preparedness and awareness and defines a plan of immediate actions to strengthen the security and resilience of CII. This is consistent with the debate launched at the request of the Council and the European Parliament to address the challenges and priorities for network and information security (NIS) policy.

The activities described in this Communication are conducted under and in parallel to the European Programme for Critical Infrastructure Protection (EPCIP) and Directive 2008/114/EC on the identification and designation of ECI, which identifies the ICT sector as a future priority sector.

A European effort is needed to bring added value to national policies and programmes by fostering the development of awareness and common understanding of the challenges, stimulating the adoption of shared policy objectives and priorities, reinforcing cooperation between MS and integrating national policies in a more European and global dimension. An integrated EU approach to enhance the security and resilience of CII would complement and add value to national programmes as well as to the existing bilateral and multilateral cooperation schemes between MS.

Five pillars are proposed:

(1) preparedness and prevention: to ensure preparedness at all levels,
(2) detection and response: to provide adequate early warning mechanisms,
(3) mitigation and recovery: to reinforce EU defence mechanisms for CII,
(4) international cooperation: to promote EU priorities internationally, and
(5) criteria for the ICT sector: to support the implementation of the Directive 2008/114/EC.

1. Preparedness and prevention:

<u>Baseline of capabilities and services for European cooperation</u>

The Commission invites Member States and concerned stakeholders to:

- define a minimum level of capabilities and services for National/Governmental Computer Emergency Response Teams (CERTs) and incident response operations in support to pan-European cooperation,
- make sure National/Governmental CERTs act as the key component of national capability for preparedness, information sharing, coordination and response.

European Public Private Partnership for Resilience (EP3R)

The Commission will

- foster the cooperation between the public and the private sector on security and resilience objectives, baseline requirements, good policy practices and measures. The primary focus of the EP3R would be on the European dimension from strategic (e.g. good policy practices) and tactical/operational (e.g. industrial deployment) perspectives. EP3R should build upon and complement existing national initiatives and the operational activities.

European Forum for information sharing between Member States

The Commission will

- establish a European Forum for Member States to share information and good policy practices on security and resilience of CIIs. This would benefit from the results of the activities of other organisations, in particular ENISA.

2. Detection and response:

European Information Sharing and Alert System (EISAS)

The Commission supports the development and deployment of EISAS, reaching out to citizens and SMEs and being based on national and private sector information and alert sharing systems. The Commission financially supports two complementary prototyping projects.

3. Mitigation and recovery:

National contingency planning and exercises

The Commission invites Member States to

- develop national contingency plans and organise regular exercises for large scale networks security incident response and disaster recovery, as a step towards closer pan-European coordination. National/Governmental CERTs/CSIRTs may be tasked to lead national contingency planning exercises and testing, involving private and public sector stakeholders. The involvement of ENISA is called upon to support the exchange of good practices between Member States.

Pan-European exercises on large-scale network security incidents

The Commission will

- financially support the development of pan-European exercises on Internet security incidents, which may also constitute the operational platform for pan-European participation in international network security incidents exercises, like the US Cyber Storm.

Reinforced cooperation between National/Governmental CERTs

The Commission invites Member States to

- strengthen the cooperation between National/Governmental CERTs, also by leveraging and expanding existing cooperation mechanisms like the EGC. The active role of ENISA is called upon to stimulate and support pan-European cooperation between National/Governmental CERTs that should lead to enhanced preparedness; reinforced European capacity to react and respond to incidents; pan-European (and/or regional) exercises.

4. International cooperation:

Internet resilience and stability

Three complementary activities are envisaged

- European priorities on long term Internet resilience and stability. The Commission will drive a Europe-wide debate, involving all relevant public and private stakeholders, to define EU priorities for the long term resilience and stability of the Internet.
- Principles and guidelines for Internet resilience and stability (European level). The Commission will work with MS to define guidelines for the resilience and stability of the Internet, focusing *inter alia* on regional remedial actions, mutual assistance agreements, coordinated recovery and continuity strategies, geographical distribution of critical Internet resources, technological safeguards in the architecture and protocols of the Internet, replication and diversity of services and data. The Commission is already funding a task force for DNS resiliency that, together with other relevant projects, will help build the consensus.
- Principles and guidelines for Internet resilience and stability (global level). The Commission will work with MS on a roadmap to promote principles and guidelines at the global level. Strategic cooperation with third countries will be developed, notably in Information Society dialogues, as a vehicle to build global consensus.

Global exercises on recovery and mitigation of large scale Internet incidents

The Commission invites European stakeholders to

- reflect on a practical way to extend at the global level the exercises being conducted under the mitigation and recovery pillar, building upon regional contingency plans and capabilities.

5. Criteria for ECI in the ICT sector:

ICT sector specific criteria

By building on the initial activity carried out in 2008, the Commission will

- continue to develop, in cooperation with Member States and all relevant stakeholders, the criteria for identifying ECI for the ICT sector. To this end, relevant information will be drawn from a specific study being launched.

Security and resilience of CII are the frontline of defence against failures and attacks. Their enhancement across the EU is essential to reap the full benefits of the information society. To achieve this objective an action plan is proposed to reinforce the tactical and operational cooperation at the European level. The success of these actions depends on their effectiveness to build upon and benefit public and private sector's activities, on the commitment and full participation of MS, European Institutions and stakeholders.

In 2011, the Commission adopted a further CIIP Communication, COM(2011)163, focusing on the ‘Achievements and next steps: towards global cyber-security’.

This Communication takes stock of the results achieved since the adoption of the CIIP action plan in 2009. It describes the next steps planned for each pillar of the action plan at both European and international level. It also highlights the global dimension of the challenges and the importance of boosting cooperation among MS and the private sector at national, European and international level, in order to address global interdependencies.

The main points from the report of the achievements and next steps of the CIIP action plan follow.

1. Preparedness and prevention:

The European Forum of Member States (EFMS) has made significant progress in fostering discussion and exchanges between relevant authorities on good policy practices related to security and resilience of ICT infrastructures. EFMS is acknowledged by MS to be an important platform for discussions and exchange of good policy practices. Its future activities will focus on cooperation among National/Governmental CERTs, identifying economic and regulatory incentives for security and resilience, evaluating the state of cyber security health in Europe, driving pan-European exercises, as well as discussing priorities for international outreach on security and resilience.

The European Public-Private Partnership for Resilience (EP3R) was launched as a Europe-wide governance framework for the resilience of ICT infrastructures and serves as a platform for international outreach on public policy, economic and market matters relevant to security and resilience, in particular to strengthen the global risk management of ICT infrastructures.

The minimum set of baseline capabilities and services and related policy recommendations for National/Governmental CERTs to function effectively and act as the key component of national capability for preparedness, information sharing, coordination and response have been developed. These will be a building block to establish a network of CERTs in all MS. Such a network will be the backbone of the European Information Sharing and Alert System (EISAS) for citizens and SMEs, to be built with national resources and capabilities.

2. Detection and response

ENISA devised a high-level roadmap for the development of an EISAS, building upon the implementation of basic services at the level of National/Governmental CERTs and of interoperability services for national information and sharing alert systems to be integrated in EISAS. Appropriate protection of personal data will be one of the key elements of this activity.

3. Mitigation and recovery

So far only 12 Member States have organised exercises for large-scale network security incident response and disaster recovery. ENISA has developed a good practice guide on national exercises as well as policy recommendations on the development of national strategies to support MS activities, which should be intensified.

The first pan-European exercise on large-scale network security incidents took place in 2010 with the involvement of all MS. Future pan-European cyber exercises would undoubtedly benefit from a common framework that builds upon and interlinks national contingency plans, thus providing baseline mechanisms and procedures for communications and cooperation between MS.

4. International cooperation

European principles and guidelines for the resilience and stability of the Internet were discussed and developed in the context of EFMS. The Commission will discuss and promote these principles with relevant stakeholders, in particular the private sector (via EP3R), bilaterally with key international partners, in particular the US, as well as multilaterally. The objective is to make these principles and guidelines a shared framework for international collective engagement on the long-term resilience and stability of the Internet.

5. Criteria for ECI in the ICT sector

The technical discussion in EFMS led to a first draft of the ICT sector-specific criteria for identifying ECI, with a focus on fixed and mobile communications and the Internet. The technical discussion will continue and benefit from the consultations on the draft criteria, at national and European (via EP3R) level, with the private sector.

The implementation of the CIIP action plan is marked by positive achievements, in particular regarding recognition that a cooperative approach to network and information security, involving all stakeholders, is needed. It is also broadly in line with the milestones and the timeline set out in 2009.

Promotion of a global culture of risk management is required. The focus should be on promoting coordinated actions to prevent, detect, mitigate and react to all kinds of disruptions, whether man-made or natural, as well as to prosecute related cyber-crimes. This includes conducting targeted actions against security threats and computer-based crime.

To this end, the Commission will:

- promote principles for the resilience and stability of the Internet,
- build strategic international partnerships, and
- develop trust in the cloud.

Since security is a shared responsibility of everyone, all MS have to ensure that their national measures and efforts will collectively contribute towards a coordinated European approach to prevent, detect, mitigate and react to all kinds of cyber disruptions and attacks. In this respect, the MS should commit to:

- enhance EU preparedness by establishing a network of well functioning National/Governmental CERTs by 2012,
- a European cyber incident contingency plan by 2012 and regular pan-European cyber exercises, and
- European coordinated efforts in international fora and discussions on enhancing security and resilience of the Internet.

Experience shows that purely national or regional approaches to tackle the security and resilience challenges are not enough. European cooperation has developed significantly since 2009 with encouraging achievements. However, Europe should continue its efforts to build a coherent and cooperative approach across the EU.

European efforts, in order to be successful, have to be embedded in a coordinated approach at global level. To this end, the Commission will promote discussions on cyber-security in all appropriate international fora.

In 2012 the European Parliament produced a Resolution on CIIP, TA(2012)0237, looking at the achievements in this sector to date and the next steps towards global cyber security. In the Resolution, the European Parliament broadly endorsed the findings of the Commission Communication COM(2011)163 and sets out its opinion on the various CIIP and CIP initiatives, providing comment and recommendations.

The European Parliament:

1. Welcomes the MS implementation of the European Programme for CIIP, including the setting-up of CIWIN.
2. Considers that the CIIP efforts will not only enhance the overall security of citizens but also improve citizens' perception of security and their trust in measures adopted by government to protect them.
3. Acknowledged the main achievements of the CIIP policy, i.e. establishment of the EFMS and the E3PR, carrying out of pan-European CIIP exercises and adoption of a minimum set of baseline capabilities and services and related policy recommendations for CERTs to function effectively.
4. Acknowledges that the Commission is considering revising Council Directive 2008/114/EC and calls for evidence to be provided of the effectiveness and impact of the directive before further steps are taken.
5. Calls on the Commission, in cooperation with MS, to assess the implementation of the CIIP action plan, urges the Member States to establish well-functioning national/governmental CERTs, develop national cyber security strategies, organise regular national and pan-European cyber incident exercises, develop national cyber incident contingency plans and contribute to the development of a European cyber incident contingency plan.
6. In view of the inter-connected and highly interdependent, sensitive, strategic and vulnerable nature of national and European CII, calls for the regular updating of minimum resilience standards for preparedness and reaction against disruptions, incidents, destruction attempts or attacks.
7. Recommends that operator security plans or equivalent measures be put in place for all European CII, and that security liaison officers be appointed.
8. Recommends that the Commission propose binding measures designed to impose minimum standards on security and resilience and improve coordination among national CERTs.
9. Calls on the Commission to propose an EU framework for the notification of security breaches in critical sectors such as energy, transport, water and food supply, as well as in the ICT and financial services sectors, to ensure that relevant MS authorities and users are notified of cyber incidents, attacks or disruptions.

4 EU Policy on Network and Information Security

The majority of CI will comprise information networks and this policy area of the EU is therefore relevant to the security of CI and is discussed in this Report.

A review of EU network and information security (NIS) policy from 2000 to 2010 has been carried out and the principal features and objectives of the major policy documents is presented.

4.1 COM(2000)890 Creating a Safer Information Society

The success of the information society is important for Europe's growth, but also opens up new opportunities for criminal activities. In the Feira European Council, 2000 a comprehensive eEurope action plan was adopted which highlighted the importance of NIS and the fight against cybercrime, and this Communication discusses the need for a policy initiative for improving NIS and combating cybercrime. Recommendations included legislative measures to approximate MS national provisions on cybercrime and high tech crime, the setting up of an EU Forum to raise awareness of, promote best practice in and develop security tools for, fighting cybercrime, and the promotion of research and development to understand and reduce vulnerabilities to cybercrime.

4.2 COM(2001)298 NIS : Proposal for a European Policy Approach

In 2001, the Council of the EU together with the Commission decided on the necessity of developing a comprehensive strategy and practical implementing actions for the security of networks. The Commission undertook to design the strategy and this is set out in this communication.

A definition for NIS was first proposed:

> Network and Information Security is the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems.

The Communication went on to identify NIS as a key priority because communication and information have become a key factor in economic and societal development. It was noted that concerns about NIS have been growing along with the rapid increase in the number of network users and the value of their transactions. NIS is now a prerequisite for further growth of electronic business and the functioning of the whole economy.

Generic security requirements in networks and information systems consist of availability, authentication, integrity and confidentiality. Security incidents can be grouped as: interception, unauthorised access, attacks, malicious software, misrepresentation, software and hardware failure, human error, natural disasters.

Finding an adequate NIS policy response is becoming an increasingly complex task. The situation in which such a policy must operate is changing considerably due to developments in this field e.g. liberalism (networks are increasingly privately owned), convergence (networks and information systems are becoming more interconnected) and globalisation (communications are increasingly cross border). These developments constrain the ability of governments to influence the level of NIS for its citizens.

The context of any NIS policy includes:

- legislation: in order to ensure a minimum level of security a substantial body of legislation as part of the telecommunications framework and data protection law has been put in place, this legislation has specific implications for NIS, e.g. security requirement imposed on ISPs, and
- market: many security risks remain unsolved or solutions are slow coming to the market as a result of certain market imperfections, e.g. prices do not accurately reflect security investment costs and benefits.

Proposed NIS policy measures have to be seen in the context of the existing telecommunications, data protection and cyber-crime policies.

Legal provisions at an EU level need to be applied effectively and need to evolve which needs a common understanding of NIS issues. As market forces do not drive sufficient investment in NIS, specific policy measures addressing market imperfections can reinforce the market process and improve the legal framework. Due to the cross border nature of communications and information services, an EU policy approach is needed to ensure the Internal Market for these services.

The Commission is to develop a comprehensive strategy on security of electronic networks, including practical implementing action. Proposed measures include:

- awareness raising - public information and education campaign, security courses,
- EU warning and information system - MS to strengthen their CERTs to provide a CERT network,
- technology support - NIS will be included in the 6th Framework research programme and focus on addressing key security challenges and the need to secure the rights of individuals and communities,
- standardisation and certification support - EU standardisation bodies are invited to accelerate work on interoperable and secure products and services,
- legal framework - the Commission will propose a legislative measure to approximate national criminal laws relating to attacks against computer systems including hacking and DoS attacks,
- security in government use - develop a culture of security in public organisations and organisational security policies,
- international cooperation - the EU will reinforce the dialogue with international organisations and partners.

4.3 Council Resolution (2002/C 43/02) Common Approach and Actions in NIS

The Council of the EU:

- asks MS to launch or strengthen NIS information and education campaigns, promote NIS best practice, promote NIS in education and training, review effectiveness of computer emergency response arrangements, promote the use of common criteria standard, take significant steps towards interoperable security measures, cooperate on electronic and biometric identification systems, exchange NIS information,
- welcomes the intention of the Commission to facilitate awareness actions best practice, reinforce dialogue with international organisations, improve the process by which products are evaluated, establish a cyber-security task force,
- welcomes the increased focus on NIS research and stresses the need for more research activities interoperability, network reliability and protection, advanced cryptography, privacy enhancing technologies and wireless communications security, and
- calls upon suppliers and service providers to strengthen NIS as an integral part of product and service offerings, the EU private sector suppliers and representative groups to participate more actively in international standardisation activities.

4.4 Regulation (EC) No 460/2004 Establishing the European Network and Information Security Agency

In this legislation, the EU establishes European Network and Information Security Agency (ENISA) to advise the Commission and MS on NIS and coordinate the measures being taken to secure their networks and information systems. The main objective of ENISA is to enhance the capability of the Commission, MS and the business community to prevent, address and respond to NIS problems.

4.5 COM(2005)229 i2010: A European Information Society for Growth and Employment

This Communication describes i2010 which is a comprehensive strategy for modernising and deploying all EU policy instruments to encourage the development of the digital economy. The aim is to provide a coherent regulatory framework for Europe's digital economy that is market-oriented, flexible and future-proof and to boost the digital economy by combining regulatory tools, research and public-private partnerships to foster ICT growth and jobs. Creating a Single European Information Space will provide an open and competitive digital economy single market. Technological convergence must be supported with policy convergence: efficient spectrum management policy (2005), modernisation of audiovisual media services rules (2005), ecommunications regulatory framework update (2006), secure information society strategy (2006), interoperable DRM (2006/7).

4.6 COM(2006)251 Strategy for a Secure Information Society

The purpose of this Communication is to revitalise EU policy on NIS by identifying current challenges and proposing measures to tackle them, including multi stakeholder dialogue, partnership between stakeholders, MS and the Commission and empowerment of stakeholders to improve their NIS.

4.7 COM(2006)688 Fighting Spam, Spyware and Malicious Software

This Communication addresses the evolution of spam and threats such as spyware and malicious software. It takes stock of the efforts so far to fight these threats and identifies further actions that can be taken, such as strengthening EU law, law enforcement, cooperation between MS, industry initiatives and research and development.

4.8 Council Resolution 2007/C68/01 Strategy for a Secure Information Society in Europe

NIS is an essential part in the creation of a European Information Space as part of the i2010 initiative. The Council invites MS to:

- support NIS training programmes and general awareness,
- strengthen the contribution to security-related research and development,
- give due attention to the need to prevent and fight new and existing security threats,
- encourage the continuous improvement of the national CERTs, and
- continue a strategic discussion and cooperation in i2010,

4.9 Council Resolution 2009/C 321/01 Collaborative European Approach to NIS

This Resolution of the Council of the EU invites MS to:

- organise national NIS exercises and participate in European NIS exercises,
- create CERTS and reinforce cooperation between national CERTs,
- increase efforts in NIS education, training and research, and
- jointly react to cross border NIS incidents.

The Resolution invites the Commission to:

- initiate an awareness campaign regarding appropriate management of NIS risks,
- encourage and improve multi stakeholder NIS models, and
- present a holistic strategy for NIS in Europe.

4.10 COM(2010)245 Adoption of the Digital Agenda for Europe

This Communication is the first flagship initiative adopted under the Europe 2020 strategy. It presents priority areas for action including:

- creating a digital single market,
- improvement the framework conditions for interoperability between ICT products and services,
- boosting Internet trust and security,
- provision of faster Internet access,
- encouraging investment in relevant research and development,
- enhancing digital literacy, skills and inclusion, and
- applying ICT to address social challenges, e.g. climate change.

Key NIS actions identified in the Communication are the presentation by the

Commission of measures aimed at a reinforced and high level NIS security policy and legislative initiatives to combat cyber attacks against information systems. Other actions include establishing a European cyber crime platform, examining the feasibility of a European cybercrime centre and supporting EU wide cyber security preparedness exercises.

The Communication suggests that MS should:

- establish a network of CERTs at national level to cover all of Europe,
- carry out large scale attack simulation and test mitigation strategies, and
- set up or adapt national alert platforms to the Europol cybercrime platform.

4.11 COM(2010)517 Proposal for a Directive on Attacks against Information Systems

Consultation on the existing EU NIS policy revealed key areas where action was required, including the need for the EU to act in this field to update policies to meet emerging threats, the need to crimilise new forms of offences in particular new methods of cyber attack such as botnets and the need to eliminate obstacles to investigation and prosecution in cross border cases.

To address these issues, it was proposed to strengthen the efforts to counter attacks against information systems using both non legislative and legislative means, in particular the proposal of comprehensive EU legislation against cybercrime in the form of a new Directive.

The Directive retains the current provisions and introduces new elements:

- maintains provisions concerning illegal access to information systems, illegal system interference and illegal data interference,
- penalises the production, use, sale, procurement for use, import and distribution of devices/tools used for committing cyber offences,
- includes aggravating circumstances such as the large scale aspect of attacks and concealment of perpetrator identity,
- introduces illegal interception as a crime,
- introduces measures to improve European criminal justice cooperation, and
- addresses the need to provide statistical data on cybercrimes by making the recording of offence data obligatory.

4.12 COM(2013)48 Proposal for a Directive concerning Measures to Ensure a High Common Level of NIS across the Union

The aim of the proposed Directive is to ensure a high common level of NIS. This means improving the security of the Internet and the private networks and information systems underpinning the functioning of our societies and economies. This will be achieved by requiring the MS to increase their preparedness and improve their cooperation with each other, and by requiring operators of CI, such as energy, transport, and key providers of information society services (e-commerce platforms, social networks, etc), as well as public administrations to adopt appropriate steps to manage security risks and report serious incidents to the national competent authorities.

The current situation in the EU, reflecting the purely voluntary approach followed so far, does not provide sufficient protection against NIS incidents and risks across the EU. Existing NIS capabilities and mechanisms are simply insufficient to keep pace with the fast-changing landscape of threats and to ensure a common high level of protection in all the MS.

Despite the initiatives undertaken, the MS have very different levels of capabilities and preparedness, leading to fragmented approaches across the EU. As networks and systems are interconnected, the overall NIS of the EU is weakened by those MS with an insufficient level of protection. This situation also hinders the creation of trust among peers, which is a prerequisite for cooperation and information sharing. As a result, there is cooperation only among a minority of MS with a high level of capabilities. Therefore, there is currently no effective mechanism at EU level for effective cooperation and collaboration and for trusted information sharing on NIS incidents and risks among the MS.

The current regulatory framework requires only telecommunication companies to adopt risk management steps and to report serious NIS incidents. The players managing CI or providing services essential to the functioning of our societies are not under appropriate obligations to adopt risk management measures and exchange information with relevant authorities.

A step-change is therefore needed in the way NIS is dealt with in the EU. Regulatory obligations are required to create a level playing field and close existing legislative loopholes. To address these problems and increase the level of NIS within the European Union, the objectives of the proposed Directive are as follows:

- the proposal requires all the MS to ensure that they have in place a minimum level of national capabilities by establishing competent authorities for NIS, setting up CERTs, and adopting national NIS strategies and national NIS cooperation plans,
- the national competent authorities should cooperate within a network enabling secure and effective coordination, including coordinated information exchange as well as detection and response at EU level, and
- to ensure that a culture of risk management develops and that information is shared between the private and public sectors.

The main provisions of the proposed Directive are:

- the Directive lays down measures to ensure a high common level of network and information security (hereinafter referred to as "NIS") within the Union,
- obligations for all MS concerning the prevention, the handling of and the response to risks and incidents affecting networks and information systems,
- a cooperation mechanism between MS in order to ensure a uniform application of this Directive within the Union and, where necessary, a coordinated and efficient handling of and response to risks and incidents affecting network and information systems,
- security requirements for market operators and public administrations,
- MS shall ensure a high level of security of the network and information systems in their territories in accordance with this Directive,
- MS shall adopt a national NIS strategy defining the strategic objectives and concrete policy and regulatory measures to achieve and maintain a high level of network and information security. The national NIS strategy shall address in particular the following issues
    - the definition of the objectives and priorities of the strategy based on an up-to-date risk and incident analysis,
    - a governance framework to achieve the strategy objectives and priorities, including a clear definition of the roles and responsibilities of the government bodies and the other relevant actors,
    - the identification of the general measures on preparedness, response and recovery, including cooperation mechanisms between the public and private sectors,
    - an indication of the education, awareness raising and training programmes,
    - research and development plans and a description of how these plans reflect the identified priorities.

- the national NIS strategy shall include a national NIS cooperation plan complying at least with the following requirements:
    - a risk assessment plan to identify risks and assess the impacts of potential incidents,
    - the definition of the roles and responsibilities of the various actors involved in the implementation of the plan,
    - the definition of cooperation and communication processes ensuring prevention, detection, response, repair and recovery, and modulated according to the alert level
    - a roadmap for NIS exercises and training to reinforce, validate, and test the plan. Lessons learned to be documented and incorporated into updates to the plan,
- the national NIS strategy and the national NIS cooperation plan shall be communicated to the Commission within one month from their adoption,
- MS shall designate a national competent authority on the security of network and information systems (the "competent authority"),
- MS shall set up a Computer Emergency Response Team responsible for handling incidents and risks according to a well-defined process,
- the competent authorities and the Commission shall form a network ("cooperation network") to cooperate against risks and incidents affecting network and information systems,
- the exchange of sensitive and confidential information within the cooperation network shall take place through a secure infrastructure,
- the competent authorities or the Commission shall provide early warnings within the cooperation network on those risks and incidents that fulfil at least one of the following conditions: they grow rapidly or may grow rapidly in scale; they exceed or may exceed national response capacity; they affect or may affect more than one Member State,
- following an early warning the competent authorities shall, after assessing the relevant information, agree on a coordinated response in accordance with a Union NIS cooperation plan,
- MS shall ensure that public administrations and market operators take appropriate technical and organisational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations, having regard to the state of the art, these measures shall guarantee a level of security appropriate to the risk presented and in particular, measures shall be taken to prevent and minimise the impact of incidents affecting their network and information system on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems,

- MS shall ensure that public administrations and market operators notify to the competent authority incidents having a significant impact on the security of the core services they provide.

At the time of writing, the Directive has yet to be brought into force in the EU.

5 Directive 95/46/EC Protection of Personal Data

In the current age, many complex systems, such as CI, cannot operate without the collection and processing of personal data. Such CI in Europe will have to comply with the European legislation in place for the protection of personal data and make provision for such protection in the configuration and operation of their component systems and networks. In particular, these CI will have to comply with the requirement to protect personal data from unauthorised access.

The right to privacy is a recognised human right, and extends to the right to protection of personal data. The EU has provided for such protection by the setting up of a regulatory framework, in the form of Directive 95/46/EC, which seeks to strike a balance between a high level of protection of privacy of individuals' personal data and free movement of personal data within the EU.

The Directive applies to personal data processed by automatic means (e.g. computer databases), but does not apply to personal data rendered anonymous in such a way that the data subject is no longer identifiable.

Personal data is any information relating to a natural person (called a data subject) who can be identified, e.g. with reference to an identification number or factors specific to his physical, physiological, mental, economic, cultural or social identity. Personal data also includes sound and image data relating to natural persons. Processing of data means any operation which is performed on personal data, such as collection, storage, alteration, consultation, use, disclosure by transmission, dissemination, blocking , erasure or destruction.

The Directive sets out principles relating to data quality:

- personal data must be processed fairly and lawfully,
- personal data must be collected for explicit and legitimate purposes and not further processed in a way incompatible with those purposes,
- the purposes for which personal data is collected must be specified at the time of collection,
- personal data must be adequate, relevant and not excessive in relation to the purposes for which it is collected,
- personal data must be accurate and kept up to date, inaccurate or incomplete data should be erased or rectified, and
- personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected.

The controller of the personal data must make sure that the above criteria are complied with

The Directive sets out criteria for making data processing legitimate:

- personal data may be processed only if the data subject gives consent (freely given, specific and informed indication of the data subject's wishes, by which he gives his agreement to processing of his personal data),

or

- processing is necessary for the performance of a contract of the data subject,
- processing is necessary for compliance with a legal obligation of the data controller,
- processing is necessary to protect the vital interests of the data subject,
- processing is necessary for a task carried out in the public interest,
- processing is necessary for the exercise of official authority given to the data controller,
- processing is necessary for legitimate interests of the data controller provided that the rights and freedoms of the data subject are not overriding.

MS can determine the circumstances in which personal data may be used or disclosed to a third party for legitimate business purposes such as marketing, e.g. allowing data subjects to object to processing of their data for such purposes.

Principles are set out for the processing of data which, by its nature, is capable of infringing fundamental freedoms or privacy:

- processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and concerning health and sex life is prohibited,

unless

- the data subject has given explicit consent,
- processing is necessary for the data controller to comply with employment law,
- processing is necessary to protect the vital interests of a data subject,
- processing of members' personal data by associations such as trade unions or political parties,
- the personal data is in the public domain,
- processing is necessary for a data subject's health,

- processing is for journalism and the need for freedom of information outweighs that for privacy.

Every data subject has the right to obtain from the controller of their personal data: confirmation of whether or not data concerning the data subject is being processed, the purpose of the processing, the categories of data being processed and recipients of the data; the data itself and any information on its source; the rectification, erasure or blocking of data the processing of which does not comply with this Directive; notification to third parties of such rectification, erasure or blocking of data. MS may restrict the rights of access and information: in the interest of the data subject or others; in order to safeguard national security, defence, public safety and important economic interests; to prosecute criminal offences.

Data subjects must be provided with the right to object, on compelling legitimate grounds, to processing of their data and specifically to object to processing which is anticipated to lead to direct marketing by the data controller or to disclosure of data to third parties for direct marketing.

A data controller (and any processor appointed by the controller) must implement appropriate technical and organisational measures to protect personal data against: unlawful destruction; accidental destruction, loss or alteration; unauthorised disclosure or access, particularly when processing involves transmission over a network; other unlawful forms of processing. A data controller generally needs to notify an appointed national data protection authority if he is processing personal data.

Transfer of personal data from a MS to a country outside the EU is allowed if the country has an adequate level of protection for such data or if safeguards are in place.

5.1 COM(2012)9 - Safeguarding Privacy in a Connected World, A European Data Protection Framework for the 21st Century

In 2012, the Commission proposed a comprehensive reform of the EU's 1995 data protection rules to strengthen online privacy rights and boost Europe's digital economy.

The rapid pace of technological change and globalisation have profoundly transformed the way in which an ever-increasing volume of personal data is collected, accessed, used and transferred. New ways of sharing information through social networks and storing large amounts of data remotely have become part of life for many of Europe's 250 million Internet users. At the same time, personal data has become an asset for many businesses. Collecting, aggregating and analysing the data of potential customers is often an important part of their economic activities. In this new digital environment, individuals have the right to enjoy effective control over their personal information.

The EU's 1995 Data Protection Directive was adopted 17 years ago when the Internet was in its infancy. In addition, the MS have implemented the 1995 Directive differently, resulting in divergences in enforcement. A single law will do away with the current fragmentation and costly administrative burdens. In today's new, challenging digital environment, existing rules provide neither the degree of harmonisation required, nor the necessary efficiency to ensure the right to personal data protection. The Commission is therefore proposing a fundamental reform of the EU's data protection framework.

To prepare the reform of the EU's data protection framework in a transparent manner, the Commission has, since 2009, launched public consultations on data protection and engaged in intensive dialogue with stakeholders. These discussions made clear that both citizens and businesses wanted the Commission to reform EU data protection rules in a comprehensive manner. After assessing the impacts of different policy options, the Commission proposes a strong and consistent legislative framework across Union policies, enhancing individuals' rights, the Single Market dimension of data protection and cutting red tape for businesses.

The Commission proposes that the new framework should consist of:

- a Regulation (replacing Directive 95/46/EC) setting out a general EU framework for data protection, and
- a Directive setting out rules on the protection of personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities.

The Commission is proposing new rules which will provide the following.

Improve individuals' ability to control their data, by:

- ensuring that, when their consent is required, it is given explicitly, meaning that it is based either on a statement or on a clear affirmative action by the person concerned and is freely given,

- equipping Internet users with an effective right to be forgotten in the online environment, the right to have their data deleted if they withdraw their consent and if there are no other legitimate grounds for retaining the data,
- guaranteeing easy access to one's own data and a right to data portability, a right to obtain a copy of the stored data from the controller and the freedom to move it from one service provider to another, without hindrance, and
- reinforcing the right to information so that individuals fully understand how their personal data is handled, particularly when the processing activities concern children.

Improve the means for individuals to exercise their rights, by:

- strengthening national data protection authorities' independence and powers, so that they are properly equipped to deal effectively with complaints, with powers to carry out effective investigations, take binding decisions and impose effective and dissuasive sanctions, and
- enhancing administrative and judicial remedies when data protection rights are violated. In particular, qualified associations will be able to bring actions to court on behalf of the individual.

Reinforce data security, by:

- encouraging the use of privacy-enhancing technologies (technologies which protect the privacy of information by minimising the storage of personal data), privacy-friendly default settings and privacy certification schemes, and
- introducing a general obligation for data controllers to notify data breaches without undue delay to both data protection authorities (which, where feasible, should be within 24 hours) and the individuals concerned.

Enhance the accountability of those processing data, in particular by:

- requiring data controllers to designate a Data Protection Officer in companies with more than 250 employees and in firms which are involved in processing operations which, by virtue of their nature, their scope or their purposes, present specific risks to the rights and freedoms of individuals ("risky processing"),
- introducing the "Privacy by Design" principle to make sure that data protection safeguards are taken into account at the planning stage of procedures and systems, and

- introducing the obligation to carry out Data Protection Impact Assessments for organisations involved in risky processing.

The new EU data protection policy and legislation is, at the time of producing this Report, still in the review stage.

6 Directive 2006/24/EC Retention of Data

For telecommunications CI, the provisions of this Directive will have to be complied with.

Telecommunication service providers or operators store clients' personal data for the purposes of transmitting communications, invoices, and interconnection payments, marketing and certain other value-added services. Because of the value of these data in preventing danger and investigating criminal activity, the EU sought to ensure that they are made available to law enforcement authorities.

MS adopted varying legislation for the retention and availability of such data which presented obstacles to the internal market for electronic communications, given the importance of traffic and location data for detection of crime and for security.

The aim of this Directive was to harmonise MS provisions concerning the obligations of providers of publicly available electronic communications services or networks to retain data generated or processed in the process of supplying their communications services, in order to ensure that the data are available for the investigation, detection and prosecution of serious crime as defined by each MS.

The provisions of the Directive apply to traffic and location data on natural persons and legal entities; they do not apply to content of electronic communications. Data retained in accordance with this Directive shall be provided only to competent national authorities in specific cases.

The data that shall be retained is:

- data necessary to trace and identify the source of a communication comprising for fixed and mobile telephony, the calling telephone number, the name and address of the service subscriber, for Internet access, e mail and telephony, the allocated user ID(s), the user ID and telephone number allocated to any communication entering the public telephone network, the name and address of the subscriber of the IP address, user ID or telephone number,
- data necessary to identify the destination of a communication comprising for fixed and mobile telephony, the number(s) dialled and to which the call is routed, the name and address of the service subscriber, for Internet e mail and telephony, the user ID or telephone number of the intended

recipient of a call, the name and address of the subscriber and user ID of the intended recipient of the communication,

- data necessary to identify the date, time and duration of a communication comprising for fixed and mobile telephony, the data and time of the start and end of the communication, for Internet access, e mail and telephony, the data and time of the log in and log off of the Internet access service, IP address allocated to the service user and the user ID of the subscriber, the data and time of the log in and log off of the Internet e mail service or telephony service,
- data necessary to identify the type of communication comprising for fixed and mobile telephony, the telephone service used, for Internet e mail and telephony, the Internet service used,
- data necessary to identify user's communication equipment comprising for fixed telephony, the calling and called telephone numbers, for mobile telephony, the calling and called telephone numbers, for Internet access, e mail and telephony, the calling telephone number for dial up access, the DSL or other end point of the originator of the communication, and
- data necessary for location of mobile communication equipment comprising the location label (cell ID) at the start of the communication, data identifying the geographic location of cells by reference to their cell IDs during the period for which communications data are retained.

No data revealing the content of a communication may be retained.

Data shall be retained for not less than 6 months and not longer than 2 years. Retained data shall be destroyed at the end of the period of retention.

Retained data shall be of the same quality and subject to the same security and protection as data on the network. Retained data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure, and to ensure access by specially authorised personnel only. Retained data shall be stored in such a way that it can be transmitted upon request to the competent authority without undue delay.

The Directive was issued in 2006 and ratified by the MS. Law enforcement authorities in most EU MS reported that retained data played a central role in their criminal investigations. However, the application of the data retention Directive was uneven, with a diversity of approaches, in terms of limitations to the use of data, data storage periods and other aspects. This presented considerable difficulties for the telecommunications industry. Furthermore, it was recognised that there was a need to strengthen the protection of personal data and to minimise the risk of breaches of privacy during storage, access and use.

In 2011 the Commission adopted an evaluation report of the Data Retention Directive outlining the lessons learned since its adoption in 2006. The report concludes that retained telecommunications data play an important role in the protection of the public against the harm caused by serious crime, but that the transposition of the Directive has been uneven. The Directive also does not in itself guarantee that data are stored, retrieved and used in full compliance with the right to privacy and protection of personal data, and this has led courts to annul the legislation transposing the Directive in some Member States. It was decided that the Commission should review the current data retention rules, in consultation with the police and the judiciary, industry, data protection authorities, and civil society with a view to proposing an improved legal framework. In 2013, the Commission set up an experts group to advise on best practice in the implementation of the Data Retention Directive. The Commission intends to propose changes to EU data retention, although there is no precise timetable at the time of writing.

7 EU CI and Related Policies - Relationship to PRECYSE

It is the overall objective of the PRECYSE Project to provide methodology and architecture tools that can be implemented in CI ICT systems to improve their security, reliability and resilience. Such tools should take into account the EU CI and related policies described in this Report, and particularly should enable legal requirements to be addressed.

These requirements include:

- enabling the operator of a CI to decide if the CI should be designated as a ECI,
- notification of the ECI designation to a relevant MS CIP authority,
- designation within a CI operator of a Security Liaison Officer to act as liaison between the operator and the relevant MS CIP authority,
- establishment and implementation by a CI operator of an Operator Security Plan,
- compliance with the requirements of the Data Protection Directive, particularly the principles relating to data quality and the implementation of appropriate technical and organisational measures to protect personal data, and
- when a CI is a publicly available electronic communications service or network, compliance with the requirements of the Data Retention Directive to retain data for the investigation, detection and prosecution of serious crime.

In addition, the PRECYSE tools should comply with the new NIS Directive when this is enacted and with the proposed revisions to the data protection and data retention policies.

This challenge will be specifically addressed in the upcoming Work Package 7 Deliverable, 7.4, which will set out protocols for the implementation of PRECYSE CI security tools in a manner compliant with ethical expectations and legal requirements.

Annex 1

Indicative list of Critical infrastructure sectors			
Sector		Product or service	
I	Energy	1	Oil and gas production, refining, treatment and storage, including pipelines
		2	Electricity generation
		3	Transmission of electricity, gas and oil
		4	Distribution of electricity, gas and oil
II	Information, Communication Technologies, ICT	5	Information system and network protection
		6	Instrumentation automation and control systems (SCADA etc.)
		7	Internet
		8	Provision of fixed telecommunications
		9	Provision of mobile telecommunications
		10	Radio communication and navigation
		11	Satellite communication
		12	Broadcasting
III	Water	13	Provision of drinking water
		14	Control of water quality
		15	Stemming and control of water quantity
IV	Food	16	Provision of food and safeguarding food safety and security
V	Health	17	Medical and hospital care
		18	Medicines, serums, vaccines and pharmaceuticals
		19	Bio-laboratories and bio-agents
VI	Financial	20	Payment services/payment structures (private)
		21	Government financial assignment
VII	Public & Legal Order and Safety	22	Maintaining public & legal order, safety and security
		23	Administration of justice and detention
VIII	Civil administration	24	Government functions
		25	Armed forces
		26	Civil administration services
		27	Emergency services
		28	Postal and courier services
IX	Transport	29	Road transport
		30	Rail transport
		31	Air traffic
		32	Inland waterways transport
		33	Ocean and short-sea shipping
X	Chemical and nuclear industry	34	Production and storage/processing of chemical and nuclear substances
		35	Pipelines of dangerous goods (chemical substances)
XI	Space and Research	36	Space
		37	Research

[COM(2005)576]

Annex 2

OPERATOR SECURITY PLAN [COM(2005)576]

Introduction

Contains information concerning the pursued objectives and the main organisational and protection principles.

***Detailed part** (classified)*

Presentation of the operator

Description of the operator's activities, organisation, connections with public authorities and details of the operator's Security Liaison Officer (SLO).

Legal context

Requirements of the National CIP Programme and any sector-specific CIP programmes.

Description of the criticality of the infrastructure

Description of the critical services/products provided and how particular elements of the CI come together to create an end-product. Details should be provided concerning:

- material elements;
- non-material elements (sensors, command, information systems);
- human elements (decision-maker, expert);
- access to information (databases, reference systems);
- dependence on other systems (energy, telecoms);
- specific procedures (organisation, management of malfunctions, etc.).

Formalisation of security requirements

Identification of the critical points in the CI, which could not be easily replaced and whose destruction or malfunction could significantly disrupt the operation of the CI or seriously endanger the safety of users, customers or employees or result in essential public needs not being satisfied. The security of these critical points is then addressed.

Identification by the owners, operators and users ('users' being defined as organisations that exploit and use the CI for business and service provision purposes) of the CI of the critical points of their CI, which would be deemed restricted areas. Access to restricted areas should be monitored in order to ensure that no unauthorised persons and vehicles enter such areas. Access would only be granted to security cleared personnel. The relevant background security checks (if deemed necessary by a MS CIP sector authority) should be carried out by the MS in which the CI is located.

Risk analysis and management

The operator conducts a risk analysis of each identified critical point.

Security measures

The operator presents the security measures arranged around two headings:

- Permanent security measures, which will identify indispensable security procedures and investment for which the owner/operator would maintain alertness against potential threats. This heading will include information concerning general measures; technical measures (including installation of detection, access control, protection and prevention means);

- organisational measures (including procedures for alerts and crisis management); control and verification measures; communication; awareness raising and training; and security of information systems.
- Graduated security measures, which may be activated according to varying threat levels.

Presentation and application

The operator will prepare detailed information sheets and instructions on how to react to various situations.

Monitoring and updating

The operator sets out the relevant monitoring and update mechanisms which will be used.