YEARLY LEGAL REPORT ON CRITICAL INFRASTRUCTURES (CIs) AND CRITICAL INFORMATION INFRASTRUCTURES (CIIs)

October 14, 2009

Contents

Chapter 1

Introduction

Critical Infrastructures (CI) are complex and highly interconnected systems (transportation systems, power plants, financial facilities, hospitals, defence systems, etc.) that are crucial for the well-being of the society [1]. According to the European Commission, Critical Infrastructures consist of "those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States"[2]. On the other hand, the United States consider Critical Infrastructures as "those systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters"[3].

But not only the infrastructures are considered critical. Information and Communication Technologies (ICTs) are increasingly intertwined in our daily activities. Some of these ICT systems, services, networks and infrastructures form a vital part of the world economy and society, either providing essential goods and services or constituting the underpinning platform of other critical infrastructures. They are typically regarded as critical information infrastructures (CIIs) as their disruption or destruction would have a serious impact on vital societal functions. Recent examples include the large-scale cyber-attacks targeting Estonia in 2007 and the breaks of transcontinental cables in 2008.

Not only the potential risk of existing threats is of importance, it is also significant to measure whether a certain infrastructure is more critical than others. For the EU, the selection criteria of what infrastructures are critical and their different degrees of criticality depends on the following three factors:

- *Scope*: The loss of a critical infrastructure element is rated by the extent of the geographic area, which could be affected by its loss or unavailability.
- *Magnitude*: The degree of the impact or loss can be assessed according to the following criteria: public impact (population affected), economic (significance of economic loss, present and future), environmental (impact

on the location), interdependency (between other critical infrastructures), and political (regarding the confidence on the government).

- *Time*: This criterion ascertains at what point the loss of an element could have a serious impact, and at what point it would be possible to recover the functionality of that element.

The risks to CIIs due to man-made attacks, natural disasters or technical failures are often not fully understood and/or sufficiently analysed. Consequently, the level of awareness across stakeholders is insufficient to devise effective safeguards and countermeasures. Cyber-attacks have risen to an unprecedented level of sophistication. The recent large scale cyber-attacks on Estonia, Lithuania and Georgia are the most widely covered examples of a general trend. The huge number of viruses, worms and other forms of malware, the expansion of botnets and the continuous rise of spam confirm the severity of the problem.

The protection of critical infrastructures is a priority for homeland and corporate security. The development of the information society has caused a vast majority of such infrastructures to critically depend on the correct operation of the information systems that control them. Indeed, the interruption of such an operation or, even worse, the destruction of those information systems as a consequence of an accident or a terrorist attack can result in huge financial, material or even human losses [4]. So, the high dependence on CIIs, 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. Due to the seriousness of the consequences, the protection of the critical (information) infrastructures (CII) must have the highest priority [5].

Chapter 2

SOME CHALLENGES TO BE ADDRRESSED IN ORDER TO STRENGTHEN THE SECURITY AND RESILIENCE OF CIs AND CIIs

2.1 Uneven and uncoordinated national approaches.

Although there are commonalities among the challenges and the issues faced, measures and regimes to ensure the security and resilience of CIs, as well as the level of expertise and preparedness, differ across states. A purely national approach runs the risk of producing a fragmentation and inefficiency across the world. Differences in national approaches and the lack of systematic cross-border cooperation substantially reduce the effectiveness of domestic countermeasures, inter alia because, due to the interconnectedness of CIs, a low level of security and resilience of CIs in a country has the potential to increase vulnerabilities and risks in other ones.

2.2 Need for a new governance model

Enhancing the security and the resilience of CIs poses peculiar governance challenges. While states remain ultimately responsible for defining CI-related policies, their implementation depends on the involvement of the private sector, which owns or controls a large number of CIs. On the other hand, markets do not always provide sufficient incentives for the private sector to invest in the protection of CIs at the level that governments would normally demand.

2.3 Limited early warning and incident response capability

The third challenge consists in that governance mechanisms will be truly effective only if all participants have reliable information to act upon. This is particularly relevant for governments that have the ultimate responsibility to ensure the security and well-being of citizens. However, processes and practices for monitoring and reporting network security incidents differ significantly. Some countries do not have a reference organisation as a monitoring point. More importantly, cooperation and information sharing between states of reliable and actionable data on security incidents appears underdeveloped, being either informal or limited to bilateral or limitedly multilateral exchanges. In addition, simulating incidents and running exercises to test response capabilities are strategic in enhancing the security and resilience of CIs, in particular by focusing on flexible strategies and processes for dealing with the unpredictability of potential crises.

Chapter 3

PRIVACY CHALLENGE

A critical infrastructure should ensure that the data collected on individuals (e.g. passenger tracking in an airport, patient monitoring in a hospital, credit card data in a financial infrastructure, surveillance data collected by intrusion detection systems, etc.) will not lead to violation of individual privacy.

Data ought to be collected at the lowest possible granularity level compatible with the security of the critical infrastructure (e.g. cloak passenger locations in an airport into cells if exact passenger locations are not needed). Strict access control policies to those data should be enforced: only employees with appropriate clearance should have access to private individual data. This includes developing schemes whereby low-clearance employees can operate the CI with a minimum knowledge of confidential information.

Chapter 4

EUROPEAN LEGAL INSTRUMENTS ON CRITICAL INFRAESTRUCTURE PROTECTION

4.1 Background

In June 2004 the European Council asked for the preparation of an overall strategy to protect critical infrastructures. In response, on 20 October 2004, the Commission adopted a Communication on critical infrastructure protection in the fight against terrorism (COM (2004) 702 final) which put forward suggestions as to what would enhance European prevention of, preparedness for and response to terrorist attacks involving critical infrastructures.

On 17 November 2005 the Commission adopted a Green Paper on a European programme for critical infrastructure protection (COM (2005) 576 final) which provided policy options on the establishment of the programme and the Critical Infrastructure Warning Information Network (CIWIN). The Green Paper on the European Programme for Critical Infrastructure Protection clearly foresees a number of funding sources for activities related to the protection of critical infrastructures in Europe. The Commission is prepared to participate in the funding of CIP-related measures including relevant studies and the development of specific methodologies. Funding for concrete hardware updates, however, would have to be found from other sources. The responses received to the Green Paper emphasised the added value of a Community framework concerning critical infrastructure protection. The need to increase the critical

infrastructure protection capability in Europe and to help reduce vulnerabilities concerning critical infrastructures was acknowledged. The importance of the key principles of subsidiarity, proportionality and complementarity, as well as of stakeholder dialogue was emphasised.

4.2 The European Programme for Critical Infrastructure Protection (EPCIP)

In December 2005 the Justice and Home Affairs Council called upon the Commission to make a proposal for a European programme for critical infrastructure protection (EPCIP) in which it reiterated that it was the ultimate responsibility of the Member States to manage arrangements for the protection of critical infrastructures within their national borders while welcoming the efforts of the Commission to develop a European procedure for the identification and designation of European critical infrastructures ('ECIs') and the assessment of the need to improve their protection. The European Programme demands that the Commission produces an annual communication to take stock of progress made and challenges ahead. This will integrate the various analyses and measures across the different sectors of the economy. Member-state governments would continue to develop and maintain databases of significant critical infrastructure on a national basis and would be responsible for developing, validating and auditing relevant plans to ensure continuity of services in case of an attack under their jurisdictions.

4.3 The Critical Infrastructure Warning Information Network (CIWIN)

In October of 2008, the European Commission (EC) proposed legislation to create the Critical Infrastructure Warning Information Network (CIWIN), a system designed to strengthen information sharing on critical infrastructure protection (CIP) between EU Member States (see COM(2008) 676 final).

CIWIN will bring together member-state CIP specialists to assist the Commission in drawing up programmes to facilitate exchange of information on shared threats and vulnerabilities and appropriate counter-measures and strategies. The USA has a similar system known as Critical infrastructure Warning Information Network (CWIN), operational since 2003.

The CIWIN consists of the two following functionalities (article 4):

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

(b) a rapid alert functionality that shall enable participating Member States and the Commission to post alerts on immediate risks and threats to critical infrastructure.

The electronic forum shall be composed of fixed areas and dynamic areas.

Fixed areas shall be included in the system on a permanent basis. While their content may be adjusted, the areas may not be removed, renamed or new areas added. The Fixed areas shall be comprised of the following:

(1) Member State Areas, offering each participating Member State the possibility to create its own area in the CIWIN portal. The organisation, administration and the content of this area will be the sole responsibility of Member States. The area will be accessible exclusively to users from the respective Member State.

(2) Sector Areas, with 11 separate sectors: Chemical Industry; Energy; Financial; Food; Health; ICT; Nuclear fuel-cycle industry; Research facilities, Space, Transport; and Water. There will also be a cross-sector sub-area for generic topics and issues of relevance to multiple sectors.

(3) CIWIN Executive Area, serving as a strategic coordination and cooperation platform designed to promote and enhance the work and communication as far as Critical Infrastructure Protection is concerned. This area will be accessible to CIWIN Executives exclusively.

(4) EU External Co-operation Area, focusing on raising awareness of external cooperation in Critical Infrastructure Protection and of Critical Infrastructure Protection standards outside the EU.

(5) Contact Directory, to facilitate the search for contact details of other CIWIN users or Critical Infrastructure Protection experts.

Dynamic areas shall be created upon demand, and shall serve a specific purpose. Their existence shall be terminated upon fulfilment of their initial purpose. The dynamic areas shall be the following:

(1) Expert Working Group Area, to provide support to the work of CIP Expert groups;

(2) Project Area, containing information on projects financed by the Commission;

(3) Alert Areas, which may be created in the event of an alert being triggered in the RAS, and will constitute the channel of communication during CIP-related activities;

(4) Special Topics Area, to focus on specific topics.

The CIWIN shall be established as a secure classified system, and shall be capable of handling information up to the level of RESTREINT UE (article 7) 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. 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.

Member States 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 the 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.

The uploading of information onto the 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.

Finally, the Commission shall review and evaluate the operation of the CIWIN every three years, and shall submit regular reports to the Member States (article 10). The first report, which shall be submitted within three years after the entry into force of this Decision, shall, in particular, identify those elements of the Community network which should be improved or adapted. It shall also include any proposal that the Commission considers necessary for the amendment or adaptation of this Decision.

4.4 EU New Directive 2008/114/EC

The Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection constitutes a first step in a step-by-step approach to identify and designate ECIs and assess the need to improve their protection. As such, this Directive concentrates on the energy and transport sectors and should be reviewed with a view to assessing its impact and the need to include other sectors within its scope, inter alia, the information and communication technology ('ICT') sector. The primary and ultimate responsibility for protecting ECIs falls on the Member States and the owners/operators of such infrastructures. There are a certain number of critical infrastructures in the Community, the disruption or destruction of which would have significant cross-border impacts. This may include transboundary cross-sector effects resulting from interdependencies between interconnected infrastructures. Such ECIs should be identified and designated by means of a common procedure. The evaluation of security requirements for such infrastructures should be done under a common minimum approach. Bilateral schemes for cooperation between Member States in the field of critical infrastructure protection constitute

a well established and efficient means of dealing with transboundary critical infrastructures. EPCIP should build on such cooperation. Information pertaining to the designation of a particular infrastructure as an ECI should be classified at an appropriate level in accordance with existing Community and Member State legislation.

4.4.1 Identification of ECIs (article 3)

The Directive requires Member States to identify and designate European Critical Infrastructure (ECI) providers. To qualify as critical, disruption of the infrastructure has to have a cross-border dimension. The Commission has identified an indicative list of priority sectors. ECI designation is also subject to a severity test and the comitology procedure.

The cross-cutting criteria shall comprise the following:

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

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

(3) 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 Member States concerned by a particular critical infrastructure. Each Member State 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 sectoral criteria shall take in into account the characteristics of individual ECI sectors. The Commission together with the Member States shall develop guidelines for the application of the cross-cutting and sectoral 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 Member States.

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.

ENERGY

1. Electricity: Infrastructures and facilities for generation and transmission of electricity in respect of supply electricity.

2. Oil: Oil production, refining, treatment, storage and transmission by pipelines

2.Gas: Gas production, refining, treatment, storage and transmission by pipelines and LNG terminals

TRANSPORT
4. Road transport
5. Rail transport
6. Air transport
7. Inland waterways transport
8. Ocean and short-sea shipping and ports

Therefore the list of ECI sectors in itself does not generate a generic obligation to designate an ECI in each sector.

4.4.2 Designation of ECIs (article 4)

Each Member State shall inform the other Member States hich may be significantly affected by a potential ECI about its dentity and the reasons for designating it as a potential ECI. Each Member State on whose territory a potential ECI is located shall engage in bilateral and/or multilateral discussions with the other Member States which may be significantly affected by the potential ECI.

A Member State that has reason to believe that it may be significantly affected by the potential ECI, but has not been identified as such by the Member State 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 Member State on whose territory the potential ECI is located and endeavour to facilitate agreement between the parties.

4.4.3 Operator security plan (article 5)

Once identified and designated, a common approach will be applied to assessing how the protection of the infrastructure should be improved. The proposed common approach requires the owner or operator of the relevant infrastructure to establish an Operator Security Plan (OSP) and to review this plan against the Directive methodology within two years after the Directive comes into force. More detailed European Union sector specific requirements may be adopted by comitology. Member States must ensure adequate and regular supervision of each OSP and its implementation, in line with the risk and threat assessment.

Annex 2 of the ECI Directive provides the minimum contents of such OSPs including:

(a) identification of important assets;

(b) a risk analysis based on major threat scenarios, vulnerability of each asset, and potential impact shall be conducted.

(c) identification, selection and prioritisation of counter-measures and procedures with a distinction between:

- Permanent security measures, which identify indispensable security investments and means which cannot be installed by the owner/operator

at short notice. This heading will include information concerning general measures; technical measures (including installation of detection, access control, protection and prevention means); organizational 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 are activated according to varying risk and threat levels.

Once an OSP has been created, each ECI owner/operator should submit it to the relevant Member State authority. Each Member State will setup a supervisory system concerning OSPs which will ensure that sufficient feedback is given to the ECI owner/operator concerning the quality of the OSP and in particular the adequacy of the risk and threat assessment.

4.4.4 Security Liaison Officer (SLO)

The second obligation imposes on the owners/operators of those critical infrastructures consists in the designation of a Security Liaison Officer (SLO). Article 6 of the ECI Directive requires all CI owners/operators designated as ECI to appoint an SLO. The SLO would function as the point of contact for security issues between the ECI and the relevant CIP authorities in the Member States. The SLO would therefore receive all relevant CIP related information from the Member State authorities and would be responsible for providing relevant information from the ECI to the Member State.

4.4.5 Reporting (article 7)

Member States must conduct an industry wide risk and threat assessment in relation to their critical infrastructure and report to the Commission on the types of vulnerabilities, threats and risks in each sector using a common template. The Commission will then assess on a sectoral basis where additional measures are needed, and may develop, on the basis of comitology, common methodologies for assessing risks

4.5 Air traffic control

Security of Aircraft in the Future European Environment (the SAFEE project) was begun in 2004 with the aim of improving security on commercial aircraft. It addresses classic hijacking situations, September 11-type scenarios and futuristic scenarios involving electronic jamming and hacking of computer systems. Subprojects will address technical issues such as onboard-threat detection, threat assessment and response management plus flight protection.

4.6 The maritime sector

The International Ship and Port Facility Security, ISPS code, was introduced in July 2004. It requires ports and vessels to show that they have put adequate security systems in place - and vessels to show that they have been calling only at certified ports. The purpose of the code is to provide a standardised, consistent framework for evaluating risk.

4.7 The Critical Information Infrastructure Protection Policy (CIIP)

In april 2009, the EC created a Critical Information Infrastructure Protection policy, which focuses security efforts on information technology and communications systems. The Critical Information Infrastructure Protection (CIIP) policy proposed by the Commission focuses on prevention, preparedness and awareness and defines a plan for immediate actions to strengthen the security and resilience of CIIs (see COM/2009/0149 final) The proposed actions complement existing measures in the area of police and judicial cooperation to prevent, fight and prosecute criminal and terrorist activities targeting CIIs. These proposals are also reflected in the EU research efforts in the field of network and information security and are in line with the international initiatives in this area. To achieve an enhanced level of awareness and preparedness throughout the EU, the Commission proposes the following set of actions:

(1) **Preparedness and prevention**: to ensure preparedness by defining a baseline of capabilities and services of national/governmental Computer Emergency Response Teams, creating a European Public-Private Partnership for Resilience and a European Forum of Member States to share information and good policy and operational practices.

(2) **Detection and response**: to provide adequate early warning mechanisms, by supporting the development and deployment of a European Information Sharing and Alert System, reaching out to citizens and SMEs and being based on national and private sector information and alert sharing systems.

(3) **Mitigation and recovery**: to reinforce EU defence mechanisms for CII, via the development by Member States of national contingency plans and the organisation of regular exercises for large scale networks security incident response and disaster recovery, as a step towards closer pan-European coordination, and by strengthening the cooperation between national/governmental Computer Emergency Response Teams.

(4) **International and EU wide cooperation**: to promote EU priorities internationally, by driving 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, by working with Member States to define guidelines for the resilience and stability of the Internet and by working on a roadmap to promote principles and guidelines at the global level, possibly leveraging strategic cooperation with third countries.

(5) **Criteria for the ICT sector**: to support future implementation of EPCIP, by continuing to develop, in cooperation with Member States and all relevant stakeholders, the criteria to identify the European critical infrastructures in the ICT sector.

Bibliography

[1] Metzger, J.: The Concept of Critical Infrastructure Protection (CIP). In: Business and Security: Public-Private Sector Relationships in a New Security Environment, pp. 197– 209. Oxford University Press, Oxford, 2004

[2] Commission of the European Communities: Communication from the Commission to the Council and the European Parliament: Critical Infrastructure Protection in the Fight Against Terrorism, COM (2004) 702 final, Brussels (2004)

[3] Congress of the United States of America: USA PATRIOT ACT. Public Law, 107–156, Washington, D.C., 2001

[4] Javier Lopez, Cristina Alcaraz, Rodrigo Roman. /"*On the Protection and Technologies of Critical Information Infrastructures*"/. On Foundations of Security Analysis and Design IV, LNCS 4677, pp 160-182, Springer.

[5] Dunn, M., Abele-Wigert, I.: The International CIIP Handbook 2006: An Inventory of Protection Policies in 20 Countries and 6 International Organizations (Vol. I) (Zurich, Center for Security Studies, 2006)