D7.9

Business framework conditions for the ECOSSIAN system

Project number:	607577
Project acronym:	ECOSSIAN
Project title:	ECOSSIAN: European Control System Security Incident Analysis Network
Start date of the project:	1st June, 2014
Duration:	36 months
Programme:	FP7/2007-2013

Deliverable type:	Report
Deliverable reference number:	SEC-607577 / D7.9 / 1.0
Work package contributing to the deliverable:	WP7
Due date:	MAY 2017 – M36
Actual submission date:	31st May, 2017

Responsible organisation:	INOV
Editor:	Gonçalo Cadete
Dissemination level:	PU
Revision:	1.0

Security Sensitivity Committee Review performed on:	19th April, 2017
Comments:	N/A

Abstract:	This deliverable provides a report on identified critical infrastructures, analysing the legal framework governing their businesses, including relevant procedures. It includes proposals for models for (inter-sectorial) cooperation.
Keywords:	Information sharing, cooperation, interoperability, security, privacy, governance, critical infrastructure protection

This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement n° 607577.

Editor

Gonçalo Cadete (INOV)

Contributors (ordered according to beneficiary numbers)

Barbara Gaggl, Christina Petschnigg (TEC)

Alessandra Spangaro, Giusella Finocchiaro (UNIBO)

Elisabete Carreira (INOV)

Manuel Martins (IP)

José Carlos Goncalves (IPT)

Anabela Filipe, Carlos Nunes, Sérgio Marques (PJ)

Erik Zouave, Jessica Schroers (KU Leuven)

Massimiliano Aschi (PI)

Reinhard Hutter (CESS)

Executive Summary

The purpose of this deliverable is to report on identified Critical Infrastructures (CIs), analyse the legal framework governing their businesses –including relevant procedures–, as well as to propose models for inter-sectorial cooperation, at the international and regional levels.

The ECOSSIAN System (ES) is supposed to be the first European-wide attempt to develop a holistic solution for supporting incident detection and management at the levels of individual CIs, across CI which are interdependent, as well as across borders [73].

In Chapter 2, a thorough analysis is conducted, from diverse points of view, to capture the essential systemic requirements, triggers, pain points, and gaps. This holistic analysis was performed by authors with diverse backgrounds –namely legal, organizational, and technical–, reflecting different approaches to problem analysis and solutions, thus contributing with their manifold experiences and expectations to the joint analysis effort.

In Chapter 3, the ECOSSIAN systemic enablers are proposed, based on authoritative European Union guidance, international standards, and industry best practice. Although this deliverable focus on business-related issues, the proposals do include basic Public-Private Partnership (PPP) related content. The full set of PPP recommendations, including regulatory and policy enablers, can be found in deliverable "D7.10 Partnerships: opportunities and constraints".

This work proposes a programme-based approach for implementing and developing the ES. The proposed set of models and recommendations (from Chapter 3) may be used as input for designing future ES programme initiatives and projects.

Overall, the success of future ES implementations should not be taken for granted. This work has identified significant capability and capacity gaps, in many relevant areas, adding to EU political landscape uncertainties and risks. On the other hand, it is now clearly recognized that hybrid threats are on the rise, implying that the urgency and value of effective ES-like implementations has never been higher.

Contents

Chapter 1 Introduction 1

Chapter 2 ECOSSIAN System Drivers and Needs 2

2.1 The evolving partnership context: EU, NATO, and USA 2

2.2 PPP legal and regulatory framework.. 6

2.2.1 European Union (EU).. 6

2.2.1.1 EU & PPPs for Cyber Security.. 8

2.2.1.1.1 The cPPP 11

2.2.1.1.2 EU PPP & Critical Infrastructures in the NIS Directive.. 12

2.2.2 National legislative frameworks..13

2.2.2.1 Public-Private partnerships in the Netherlands..13

2.2.2.2 Public Private Partnerships in Portugal..16

2.2.2.2.1 Scope of the 2012 PPP Law 16

2.2.2.2.2 The PPP Technical Support Unit.. 17

2.2.2.2.3 Tender preparation, evaluation and award of contract.. 18

2.2.2.2.4 Execution and Amendments to PPPs 19

2.2.2.2.5 Rules for Candidates and Exclusion Grounds 19

2.2.2.2.6 PPPs in relation to Critical Infrastructures.. 20

2.3 Principles of the European Union and their application in Cyber Security and NIS Protection.. 20

2.3.1 Conferral..21

2.3.2 Subsidiarity 22

2.3.3 Proportionality..23

2.3.4 Solidarity..23

2.3.5 Application to European Cyber & Network Information Security 24

2.4 The Challenges of a PPP for CIP.. 25

2.5 CIIP and Need for PPP 27

2.5.1 Criteria for the Criticality of CIIP 27

2.5.2 Lessons from the US Experience 29

2.5.3 PPP as enablers in CIIP..30

2.6 PPP Characteristics.. 31

2.6.1 Escalatory Factors 31

2.6.2 Inherent Limitations of PPP in CIIP 32

2.6.3 Dependence of Requirements for PPP on Levels of Impact..33

2.6.4 Need for and role of Insurance..34

2.7 ECOSSIAN-Type in CIP 35

2.7.1 The ECOSSIAN Prototype: Functions and Constraints 35

2.7.2 The European Scope of ECOSSIAN 36
2.7.3 ECOSSIAN in European CIP: Conditions for Applicability 37
2.8 Experience of the European Electronic Crime Task Force 38
2.8.1 European Electronic Crime Task Force in brief 38
2.8.2 History....39
2.8.3 Governance 39
2.8.4 Modus Operandi 40
2.8.5 Activity Lines....40
2.8.6 EECFT Permanent Members 41
2.8.8 International cooperation....42
2.8.9 Traffic Light Protocol – How Information Sharing works 42
2.8.10 EECTF Community Composition....42
2.8.11 EECTF Plenary meetings....43
2.8.12 Expert Group meetings 44
2.8.13 Example of operational activities carried out in the EECTF context: the Eurograbber case....45
2.8.14 International Projects 45
2.8.15 Priorities in Cyber Security....46
2.8.16 EECTF: an information sharing channel in support of the CERT of Poste Italiane 46
2.8.17 Conclusion and lessons learned....47
2.9 Stakeholders' survey: principles, mission, capabilities, and obstacles.... 48
2.9.1 Capability indicators w.r.t. ISO 22325:2015....48
2.9.2 Partnering objectives or mission w.r.t. ISO 22397:2014 49
2.9.3 Partnering principles or main concerns w.r.t. ISO 22397:2014 50
2.9.4 Obstacles to partnering according to ISO 22397:2014 51
Chapter 3 ECOSSIAN System Enablers.... 53
3.1 Models for promoting across-borders and inter-sectorial cooperation, interoperability, and adoption.... 53
3.1.1 A conceptual model for the ECOSSIAN Enablers 53
3.1.2 Models and methodologies for implementing the ECOSSIAN System 54
3.1.3 Models for Risk Management and Disaster Risk Management 55
3.2 A model for promoting cooperation in the European Union 58
3.3 A generic model for governance and management 58
3.4 Enabling Principles, Policies, and Frameworks 61
3.5 Enabling Processes.... 66
3.6 Enabling Organizational Structures.... 73

3.7 Enabling Culture, Ethics, and Behaviour 75

3.8 Enabling Information 76

3.9 Enabling Services, Infrastructure, and Applications 78

3.10 Enabling People, Skills, and Competencies 79

Chapter 4 Conclusion 81

Chapter 5 List of Abbreviations 82

Chapter 6 Glossary 86

Chapter 7 Bibliography 92

List of Figures

Figure 1: Model for coordination between NIS competent authorities/CERTs, law enforcement and defence, taken from [52]. 4

Figure 2: EECTF Community composition 43

Figure 3: Expert Group meetings 44

Figure 4: A conceptual model for Information System enablers, taken from [50]. 54

Figure 5: Conceptual model for implementing Information Systems' programme management, taken from [67]. 55

Figure 6: Risk management process model, taken from [3]. 56

Figure 7: Disaster Risk Management conceptual model. 57

Figure 8: Model for coordination between NIS competent authorities/CERTs, law enforcement and defence, taken from [52]. 58

Figure 9: A generic model for governance and management, taken from [50]. 59

List of Tables

Table 1: CI Disruption Impact Criteria, taken from [61]. 28

Table 2: Impacts on CI Processes, taken from [61]. 29

Table 3: Ranking of Capability Indicators. 49

Table 4: Ranking of Partnering Objectives. 50

Table 5: Ranking of Partnering Principles. 50

Table 6: Ranking of Obstacles to Partnering. 51

Table 7: Generic reference roles. 59

Table 8: BFC related to enabling Principles, Policies, and Frameworks. 61

Table 9: BFC related to enabling Processes. 67

Table 10: BFC related to enabling Organizational Structures. 73

Table 11: BFC related to enabling Culture, Ethics, and Behaviour. 75

Table 12: BFC related to enabling Information. 76

Table 13: BFC related to enabling Services, Infrastructure, and Applications. 78

Table 14: BFC related to enabling People, Skills, and Competencies. 80

Chapter 1 Introduction

To ensure success of future ECOSSIAN System (ES) implementations and developments, the technical solutions should be complemented by effective and agreed organizational concepts, as well as the implementation of novel rules, regulations, and incentives [73]. This set of environmental requirements defines what we call the Business Framework Conditions (BFC) for the ECOSSIAN System.

For addressing the high complexity of this work, a holistic approach was followed to conduct both the analysis and recommendations phases.

In Chapter 2, a thorough analysis on systemic drivers and needs is conducted, from diverse points of view, to capture the essential systemic requirements, triggers, pain points, and gaps:

- In section 2.1, the recent EU-NATO cooperation efforts are reviewed, setting the context for high-level drivers and requirements regarding European cybersecurity and cyber defense.
- The current legal and regulatory framework is then described and analyzed in sections 2.2 and 2.3, focusing on PPP legal features, as well as on European fundamental political and organizational principles.
- Major challenges, gaps, and scope issues regarding public-private partnerships (PPP) are addressed in sections 2.4 to 2.7. These sections are a sobering and stark inventory of the complexities and difficulties that need to be addressed in the ES roadmap.
- Section 2.8 changes the mood –but not the temperance–, by presenting the case study of the European Electronic Crime Task Force (EECTF), thus illustrating the challenges facing a complex information-sharing initiative, that requires the engagement of diverse public and private stakeholders –much like what is expected from the ES.
- The analysis part concludes by presenting a stakeholder's survey that was conducted with ECOSSIAN Project's stakeholders, to elicit their business motivations and concerns, assess what measures need to be implemented for the ES to be a success, and identify possible obstacles on the way.

In Chapter 3, the ECOSSIAN systemic enablers are proposed. To promote interoperability and easy adoption, the recommendations are based on widely accepted international standards and industry best practice. An agile programme-based approach is recommended for implementing and developing the ES.

Chapter 2 ECOSSIAN System Drivers and Needs

In this chapter, a thorough analysis on systemic drivers and needs is conducted, from diverse points of view, to capture the essential ES systemic requirements, triggers, pain points, and gaps.

This holistic analysis was performed by authors with diverse backgrounds –namely legal, organizational, and technical–, reflecting different approaches to problems and solutions, thus contributing with manifold experiences and expectations to the joint analysis effort.

2.1 The evolving partnership context: EU, NATO, and USA

The recent Joint EU-NATO Declaration of July 8th, 2016, established the goal to give new impetus and new substance to the EU-NATO strategic partnership [56]. The Joint Declaration framed the partnership efforts under the spirit and principles of «full mutual openness and in compliance with the decision-making autonomy and procedures of our respective organisations and without prejudice to the specific character of the security and defence policy of any of our members».

This new cooperation framework has implications for the cybersecurity and cyber defence domains, and thus for the ES in particular –as a cybersecurity early-warning and situational awareness instrument. Indeed, cyber threats and attacks are becoming more common, sophisticated and damaging, and require a new approach to international cooperation [55].

From NATO's point-of-view, eminent drivers and needs have to be addressed [55]:

- The NATO Alliance is faced with an evolving complex threat environment.
- State and non-state actors can use cyberattacks in the context of military operations.
- In recent events, cyberattacks have been part of hybrid warfare.
- NATO and its Allies rely on strong and resilient cyber defences to fulfil the Alliance's core tasks of collective defence, crisis management and cooperative security.
- NATO needs to be prepared to defend its networks and operations against the growing sophistication of the cyber threats and attacks it faces.

Some of the recent NATO cyber defence milestones and guidelines are [55]:

- In July 2016, Allies reaffirmed NATO's defensive mandate and recognised cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea.
- Allies are and remain responsible for the protection of their national networks, which need to be compatible with NATO's and with each other's.
- Allies are committed to enhancing information-sharing and mutual assistance in preventing, mitigating and recovering from cyberattacks.
- NATO also works with, among others, the European Union (EU), the United Nations (UN) and the Organization for Security and Co-operation in Europe (OSCE). The Alliance's cooperation with other international organisations is complementary and avoids unnecessary duplication of efforts.
- NATO signed a Technical Arrangement on cyber defence cooperation with the European Union (EU) in February 2016. Considering common challenges, NATO and

the EU are strengthening their cooperation on cyber defence, notably in the areas of information exchange, training, research and exercises.

- NATO is intensifying its cooperation with industry, via the NATO Industry Cyber Partnership. Through the NATO Industry Cyber Partnership (NICP), NATO and its Allies are working to reinforce their relationships with industry. This partnership relies on existing structures and includes NATO entities, national Computer Emergency Response Teams (CERTs) and NATO member countries' industry representatives. Information-sharing activities, exercises, training and education, and multinational Smart Defence projects are just a few examples of areas in which NATO and industry have been working together.
- On December 6th, 2016, NATO and the EU agreed on a series of more than 40 measures to advance how the two organisations work together – including on countering hybrid threats, cyber defence, and making their common neighbourhood more stable and secure. On cyber defence, NATO and the EU will strengthen their mutual participation in exercises, and foster research, training and information-sharing.
- On February 16th, 2017, defence ministers approved an updated Cyber Defence Plan as well as a roadmap to implement cyberspace as an operational domain. This initiative increase Allies' ability to work together, develop capabilities and share information.

In recent years, the European Commission (EC) has taken significant steps towards improving cybersecurity. An important milestone was the adoption of the EU Cybersecurity Strategy, in 2013. The strategy articulates the EU's vision of cyber-security in terms of five priorities: [52]

1) Achieving cyber resilience.
2) Drastically reducing cybercrime.
3) Developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP).
4) Developing the industrial and technological resources for cyber-security.
5) Establishing a coherent international cyberspace policy for the European Union and promoting core EU values.

Coordination and collaboration is encouraged among European agencies such as ENISA, Europol/EC3 and EDA, notably in terms of trends analysis, risk assessment, training and sharing of best practices. [52]

To address cybersecurity in a comprehensive fashion, the EC strategy recommends that activities should span across three key pillars: Network Information Security (NIS), law enforcement, and defence (see Figure 1). Therefore, it is paramount to enable interoperability between all relevant stakeholders in the areas of defence, law enforcement, and NIS, as well as to ensure cooperation between the former and industry and academia stakeholders.

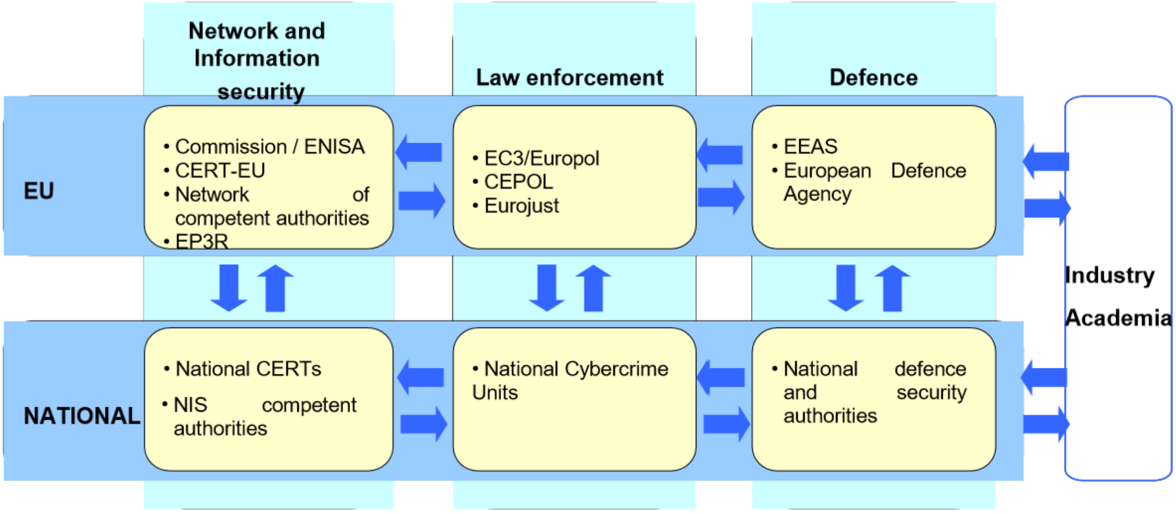

Network and Information security
Law enforcement
Defence
EU
• Commission / ENISA
• CERT-EU
• Network of competent authorities
• EP3R
• EC3/Europol
• CEPOL
• Eurojust
• EEAS
• European Defence Agency
NATIONAL
• National CERTs
• NIS competent authorities
• National Cybercrime Units
• National defence and security authorities
Industry
Academia

Figure 1: Model for coordination between NIS competent authorities/CERTs, law enforcement and defence, taken from [52].

Other major cybersecurity initiatives of the EC are: [66]

- The European Agenda on Security 2015-2020, which was adopted by the Commission in April 2015, where the EC states that cybercrime requires a coordinated response at the European level.
- The Digital Single Market Strategy, presented in May 2015, where trust and security are core objectives. The strategy includes a public-private partnership (PPP) on cybersecurity, supported by EU funds.
- The adoption of the Directive on security of network and information systems (NIS Directive) by the European Parliament, in July 2016. Member States will have 21 months to transpose the Directive into their national laws and 6 months more to identify operators of essential services. The EC is concerned that cybersecurity incidents, be they intentional or accidental, could disrupt the supply of essential services. Cybersecurity threats can have different origins - including criminal, terrorist or state-sponsored attacks, as well as natural disasters and unintentional mistakes.

Also, on an ongoing basis, the European External Action Service (EEAS), the Commission, and the Member States engage in policy dialogue with international partners and with international organisations such as the Council of Europe, the Organisation for Economic Co-operation and Development (OECD), the Organization for Security and Co-operation in Europe (OSCE), the North Atlantic Treaty Organization (NATO), and the United Nations (UN). [66]

Among the NATO members, the United States of America (USA) is an important contributor. Due to its role in the NATO Alliance, as well as the relevance of USA enterprises in the information systems, software, and hardware industries, it is important to have a good understanding of the USA cybersecurity context. Some of the main USA initiatives in the cyber security domain are:

- On February 12th, 2014, the National Institute of Standards and Technology (NIST) released the “Framework for Improving Critical Infrastructure Cybersecurity” [2], to comply with Presidential Executive Order 13636 [9]. The NIST Cybersecurity Framework is a voluntary risk-based cybersecurity framework, that proposes a set of industry standards and best practices to help organizations manage cybersecurity risks. Developed mainly for USA infrastructure, it also aims to serve as a model for international cooperation on strengthening critical infrastructure cybersecurity. [2]

- The NIST Cybersecurity Framework provides a common language for enabling communication and cooperation in cybersecurity risk management, for the Information Technology (IT) and Industrial Control Systems (ICS) environments. The Framework Core defines a set of relevant activities that help in the analysis, prioritization and implementation of cybersecurity countermeasures. Security functions are defined at the highest level of abstraction, helping to express activities for management of cybersecurity risk, and defined as follows: [2]
    - Identify: develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities;
    - Protect: develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services;
    - Detect: develop and implement the appropriate activities to identify the occurrence of a cybersecurity event;
    - Respond: develop and implement the appropriate activities to take action regarding a detected cybersecurity event; and
    - Recover: develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.
- The Presidential Policy Directive/PPD-21, issued in February 12, 2013, aimed at strengthening the security and resilience of USA critical infrastructure against both physical and cyber threats [10]. This directive identified 16 critical infrastructure sectors and designated associated Federal Sector-Specific Agencies (SSAs). SSAs are defined as Federal departments or agencies responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector. [10]

From what was presented in this section, it is paramount that the ES be aligned, at all levels –strategic, operational, and tactical–, with the ongoing developments in the cybersecurity and cyber defence domains, in both EU and NATO spaces.

The EU has set ambitious goals for partnering with NATO and its member states. To this end, the Joint Declaration calls on EU and NATO to «invest the necessary political capital and resources to make this reinforced partnership a success.».

2.2 PPP legal and regulatory framework

Public Private Partnerships (PPPs) do not have a specific legal definition.[1] The label PPP is traditionally used in the contractual relationships between governments and the private sector.[2] The cooperation can have different forms, ranging from very informal types of cooperation to more formal partnerships.[3] In the following sections, the legislative and regulatory framework regarding PPPs will be described on an EU level and in selected Member States. We will also highlight the role of PPPs in European cybersecurity policy, notably as a means to realize overarching policy goals such as the prevention of cyber incidents (and crimes), improving the resilience and protection of regionally significant assets, coordination between stakeholders within the Union and Member States, and developing industrial and technological resources.

2.2.1 European Union (EU)

At an EU level, there is no specific legal framework for PPPs.[4] PPP set-ups generally qualify as public contracts or concessions.[5] In 2004, the Commission adopted a Green Paper on Public-Private Partnerships and Community Law on Public Contracts and Concessions[6]. A debate followed and its conclusions were used in the 2005 Commission Communication.[7] Even though there is no uniform award procedure in EC law specifically designed for PPPs, it was considered negative by the stakeholders to introduce a regulatory regime covering all contractual PPPs.[8] Nonetheless, certain EU legislation can be applicable to PPPs. The main legislation on EU level applicable to PPPs is the legislation on public procurement procedures. The European Directives primarily regulate contract award procedures for public procurement, including both authorities and undertakings, from private operators. The overarching objective of the frameworks are to ensure fair awards and contracts in transboundary procurement. However, in the application of European procurement frameworks to critical infrastructures, it is important to note that there is a general exemption across all the EU directives for secrecy in the interest for national security.[9] In this regard, the main provisions of European law are found in:

- Directive 2004/17/EC[10] coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors,

[1] ENISA, Lionel Dupré, Nicole Falessi and Dimitra Liveri (eds.), Cooperative Models for Effective Public Private Partnerships - Good Practice Guide, 2011, p.6.

[2] Recipe project, Klaver, M.H.A. Luiijf, H.A.M. Nieuwenhuijsen, A.H, Good practice manual for CIP policies, 2011, p. 39.

[3] Recipe project, Klaver, M.H.A. Luiijf, H.A.M. Nieuwenhuijsen, A.H, Good practice manual for CIP policies, 2011, p. 39.

[4] Commission of the European Communities, (COM(2004) 327 final) Green paper on public private partnerships and Community Law on Public Contracts and Concessions, Brussels, 30.4.2004, COM(2004) 327 final.

[5] Commission of the European Communities (COM(2005) 569 final), Communication on Public-Private Partnerships and Community Law on Public Procurement and Concessions, , 15.11.2005, p.5.

[6] COM(2004) 327 final, 30.4.2004.

[7] COM(2005) 569 final, 15.11.2005.

[8] COM(2005) 569 final, 15.11.2005, p.5.

[9] See for example Directive 2009/81/EC of the European Parliament and of the Council on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC

[10] Directive 2004/17/EC of the European Parliament and of the Council of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors.

- Directive 2004/18[11] on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts amending Council Directive 92/50/EEC relating to the coordination of procedures for the award of public service contracts and Council Directive 93 /36/EEC coordinating procedures for the award of public supply contracts.
- Directive 2009/81/EC of the European Parliament and of the Council on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC
- As of 18 April 2016, Directive 2014/25/EU,[12] Directive 2014/24/EU[13] and Directive 24/23 EU[14] have been transposed into the domestic law of members States.

For contracts that are not subject to the provisions of the public procurement Directives, the Commission issued an interpretative communication.[15] For these contract awards, "having a sufficient connection with the functioning of the Internal Market"[16], the Internal Market rules apply. The European Court of Justice developed a set of basic standards derived from the principles of equal treatment and non-discrimination on grounds of nationality.[17] This includes the obligation of transparency, requiring the publication of an accessible advertisement prior to the award of the contract.[18] Furthermore, the impartiality of the procedure needs to be ensured, requiring a non-discriminatory description of the subject-matter of the content, equal access for economic operators from all Member States, mutual recognition of diplomas, certificates and other evidence of formal qualifications, appropriate time-limits and a transparent and objective approach.[19] The principles also apply to the contract award decision. The number of applicants may however be limited, as long as it is done in a transparent and non-discriminatory manner, e.g. considering objective factors such as the experience of the applicants. The European Commission has further noted on the importance of PPPs in improving the standards of national infrastructure. In particular, this has observed with regards to the private sector's ability to supplement much needed capital to infrastructures and as an alternate source of management for such societal resources. To that effects, the Commission has published a set of guidelines (the Guidelines) for public-

[11] Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts.

[12] Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC.

[13] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC.

[14] Directive 2014/23/EU of the European Parliament and of the Council of 26 February 2014 on the award of concession contract.

[15] Commission Interpretative Communication on the Community law applicably to contract awards not or not fully subject to the provisions of the Public Procurement Directives, 2006/C 179/02, 1.8.2006.

[16] Commission Interpretative Communication on the Community law applicably to contract awards not or not fully subject to the provisions of the Public Procurement Directives, 2006/C 179/02, 1.8.2006, p.2; e.g. in case of very modest economic interest at stake such that a contract award would be of no interest to economic operators in other Member States, the award does not need to take into account the basic standards derived from Community law.

[17] Commission Interpretative Communication on the Community law applicably to contract awards not or not fully subject to the provisions of the Public Procurement Directives, 2006/C 179/02, 1.8.2006, p.2.

[18] Commission Interpretative Communication on the Community law applicably to contract awards not or not fully subject to the provisions of the Public Procurement Directives, 2006/C 179/02, 1.8.2006, p.3.

[19] Commission Interpretative Communication on the Community law applicably to contract awards not or not fully subject to the provisions of the Public Procurement Directives, 2006/C 179/02, 1.8.2006, p.3f.

private partnerships in the Union.[20] The guidelines are not binding, nor comprehensive but rather present, *inter alia*, legal and regulatory structures to PPPs, factors for success and observed obstacles. While the Guidelines can only provide generic observations, it holds true that the EU Directives (enumerated above) also interplay with domestic bodies of law – such as in procurement, health environment, and transport to name a few – provincial and municipal regulation, and contractual concerns.[21]

2.2.1.1 EU & PPPs for Cyber Security

The laws, principles, and norms of the Union apply in the online environment as well as the physical world. Moreover, the collaboration between the public and private sector in cyber security has been informed by a much richer body of laws and policies than European procurement law. The European Union has largely recognized the significant role of the private sector in assuring these values through two strategic initiatives. The European Agenda on Security[22] entrenched the fight against cybercrime as a priority for the Union. It highlighted cybersecurity as the first line of defense against cybercrime, with an aim to give renewed emphasis to the implementation of the cybersecurity policies already in place through collaboration with the private sector and the adoption of the NIS Directive to formalize this collaboration. The Cyber Security Strategy for the European Union (*An open and Secure Cyberspace for All*),[23] seeks to outline a joint vision for the EU Member States and clarify roles and responsibilities in the domain of cybersecurity to accomplish an open and secure cyberspace. The Union's vision encompasses a democratically governed cyberspace that secures the protection of fundamental rights and freedoms and access for all. Moreover, it is widely recognized that much of the critical infrastructure and infrastructure behind the Internet and cyberspace are in private ownership and operation. The Cyber Security Strategy,[24] resultantly sets out to implement the democracy principle through a multi-stakeholder approach to governance involving non-governmental and commercial actors in the management of Internet resources and cyber security. Another basic principle to the Strategy is ensuring that all actors involved in information and communication technologies share in the responsibility and coordination to strengthen security.

These two strategies were preceded and drafted based on extensive European efforts to public-private cooperation in the area of cyber security with actions that are still running or being replicated in newer policies. The main theme through EU initiatives in this area has been to strengthen the resilience of European networks and information systems.[25] Awareness raising of network and information security has been identified as an underlying prerequisite to strengthening European cyber security, especially in the context of public-

[20] European Commission (2003). *GUIDELINES FOR SUCCESSFUL PUBLIC - PRIVATE PARTNERSHIPS.* Available: http://ec.europa.eu/regional_policy/sources/docgener/guides/ppp_en.pdf. Last accessed 06/10/2016.

[21] European Commission. (2003). *GUIDELINES FOR SUCCESSFUL PUBLIC - PRIVATE PARTNERSHIPS.* Available: http://ec.europa.eu/regional_policy/sources/docgener/guides/ppp_en.pdf. Last accessed 06/10/2016.

[22] European Commission (COM(2015) 185) *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: The European Agenda on Security*.

[23] European Commission (JOIN(2013) 1) *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.*

[24] European Commission (JOIN(2013) 1) *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*.

[25] ENISA (2016) NIS Platform (https://resilience.enisa.europa.eu) https://resilience.enisa.europa.eu/nis-platform Last accessed 14/10/2016.

private cooperation.[26] Moreover, an early policy ambition[27] was establishing a European Warning and Information System that would allow business to report attacks, alert operators and users of systems to threats and inform threat intelligence production. This warning and information system would involve Computer Emergency Response Teams (CERTs) from both public and private sectors.[28] The ambition has largely been formalized by the 2016 Network and Information Systems Directive, and aligns with the overarching objective of the ECOSSIAN project. Secondly, another long-standing action has been funding technology support and development through the Framework Research Programmes (FPs).[29] One of the core research areas of FP5 between 1998 and 2002, FP6 between 2002 and 2006,[30] Information Society Technologies included projects for the development of information security and security related technologies.[31] The Horizon 2020 Research Programme is implemented through key areas of public private partnerships[32] Similarly, ECOSSIAN was accepted as a project an FP7 SEC-2013.2.5-3 on pan-European detection and management of incidents/attacks on critical infrastructures in sectors other than the ICT sector. Finally, the Community has explored the standardization and certification of security technologies, which is also reflected in the recent contractual public-Private Partnership.[33]

[26] Commission of the European Communities (COM(2001)298) *COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Network and Information Security: Proposal for A European Policy Approach*; Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security *OJ C 43, 16.2.2002, p. 2–4;* Council Resolution of 18 February 2003 on a European approach towards a culture of network and information security *OJ C 48, 28.2.2003, p. 1–2;* Council Resolution of 22 March 2007 on a Strategy for a Secure Information Society in Europe *OJ C 68, 24.3.2007, p. 1–4* .

[27] Commission of the European Communities (COM(2001)298) *COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Network and Information Security: Proposal for A European Policy Approach*.

[28] Commission of the European Communities (COM(2001)298) *COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Network and Information Security: Proposal for A European Policy Approach*; European union (2002) *eEurope 2002*; European Union (2005) *eEurope 2005*; European Union (1999) *eEurope – An Information Society for All.*

[29] Commission of the European Communities (COM(2001)298) *COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Network and Information Security: Proposal for A European Policy Approach*;

[30] European Commission. (2015). *Information Society Technologies.*Available: https://ec.europa.eu/research/fp6/index_en.cfm?p=2. Last accessed 10/10/2016.

[31] Commission of the European Communities (COM(2001)298) *COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Network and Information Security: Proposal for A European Policy Approach;* European Commission. (2015). *EU Framework Programmes.* Available: https://ec.europa.eu/research/infrastructures/index_en.cfm?pg=framework_prog. Last accessed 10/10/2016.

[32] European Commission (C(2016) 4400) COMMISSION DECISION of 5.7.2016 *on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation*.

[33] Commission of the European Communities (COM(2001)298) *COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Network and Information Security: Proposal for A European Policy Approach;* European Commission (2016) *ANNEX 1: ANNEX CONTRACTUAL ARRANGEMENT SETTING UP A PUBLIC-PRIVATE PARTNERSHIP IN THE AREA OF CYBERSECURITY INDUSTRIAL RESEARCH AND INNOVATION BETWEEN THE EUROPEAN UNION AND THE EUROPEAN CYBERSECURITY ORGANISATION to the Commission Decision on the signing of a contractual arrangement setting up a public-private partnership in the area of cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation*.

The Programme for European Critical Infrastructure Protection (EPCIP)[34] and the Critical Infrastructure Warning Information Network (CIWIN) initiatives presented substantive investments for public-private partnerships for cyber and critical infrastructure security. The EPCIP is regarded as an "all-hazards cross-sectoral approach" to protecting critical infrastructures covering both kinetic and non-kinetic threats.[35] It laid down a framework for designating critical infrastructures which included funding for more than 100 security projects within the identified sectors, in particular for developing industrial resources for cyber security.[36]

In 2009, the Commission launched their Policy on Critical Information Infrastructure Protection (CIIPs), with an action plan specifically designed to lift the role of the private sector in threat detection, response, mitigation and recovery.[37] Com(209) 149 identified the governance of CIIs, specifically the inclusion and investment from the private sectors as a particular weakness for regional CII resilience.[38] The Commission therefore established the European Public-private Partnership for Resilience (EP3R) within ENISA to build on existing domestic PPPs for critical information infrastructure protection for the pan-European level. The EP3R closed in April 2013. The overall focus of the EP3R was to identify European good policy and industrial deployment practices.[39] Four objectives were formulated for the EP3R for these purposes:

- *Encourage information sharing and stock-taking of good policy and industrial practices to foster common understanding;*
- *Discuss public policy priorities, objectives and measures;*
- *Baseline requirements for the security and resilience in Europe;*
- *Identify and promote the adoption of good baseline practices for security and resilience.*[40]

The CIIPs policy was followed by the Resolution of June 12th, 2012 (2011/2284(INI)) supporting EU-level PPPs, including the continued work of the EP3R, and investigating industry incentives to engage in PPPs. Much of this previous work laid down in the strategies, policies and initiatives of the Union have been formalized through the adoption of

[34] Commission of the European Communities (COM(2006) 786) *COMMUNICATION FROM THE COMMISSION: on a European Programme for Critical Infrastructure Protection*.

[35] European Commission. (2016). *Critical infrastructure.* Available: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm. Last accessed 14/10/2016.

[36] European Commission. (2016). *Protection of critical infrastructure.*Available: https://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure. Last accessed 10/10/2016; Commission of the European Communities (COM(2006) 786) *COMMUNICATION FROM THE COMMISSION: on a European Programme for Critical Infrastructure Protection*.

[37] European Commission. (2013). *Policy on Critical Information Infrastructure Protection (CIIP).* Available: https://ec.europa.eu/digital-single-market/en/news/policy-critical-information-infrastructure-protection-ciip. Last accessed 14/10/2016.

[38] Commission of the European Communities (COM (2009) 149 COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" (Brussels, 30.3.2009).

[39] Commission of the European Communities (COM (2009) 149 COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" (Brussels, 30.3.2009).

[40] ENISA. (2016). *European Public Private Partnership for Resilience (EP3R).* Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ppps/public-private-partnership/european-public-private-partnership-for-resilience-ep3r. Last accessed 14/10/2016.

the NIS Directive which harmonizes formalized channels and standards for domestic and cross-border cooperation.

2.2.1.1.1 The cPPP

It is worth noting that a special public-private partnership has been set up within the EU Single Digital Market, Horizon 2020 and the Framework Programme for Research and Innovation.[41] The so-called contractual Public-Private Partnership (cPPP) was signed as a measures executing the EU Cyber Security Strategy[42] the Communication delivering on the European Agenda on Security,[43] the Joint Communication and Council Joint Framework on countering hybrid threats,[44] the NIS Directive as well as the Digital Single Market.[45] The purpose of the cPPP is to foster public-private cooperation for the innovation of cyber security solutions and services and strengthen the competitiveness of the European cyber security market.[46] While this objective is foremost oriented towards the civilian market, the European Commission expects that it will contribute to the overall security of society against cyber threats.[47] The contractual arrangement to the cPPP identifies specific areas of interest for cybersecurity innovation for essential service providers, namely health, transport, government and networks to name a few. [48] The core contractual principles of the cPPP are openness, transparency and efficiency. Competitiveness is strengthened through, inter alia, supporting technology development and exploitation on the international market, standardization, validation and testing, supporting new forms of collaboration between actors, encouraging financial investment and supporting start-ups. The Commission resolves to strengthen the innovation of the European markets in this context through financial support to disruptive innovation, support to dissemination and networking and increasing the trust and use of European certified technologies.

[41] European Commission. (2016). *Cybersecurity industry.* Available: https://ec.europa.eu/digital-single-market/en/cybersecurity-industry. Last accessed 07/10/2016.

[42] European Commission. (2013). *Communication on a Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace.* Available: https://ec.europa.eu/digital-single-market/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace. Last accessed 07/10/2016.

[43] European Commission (COM(2016) 230) *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union*.

[44] European Commission (JOIN(2016) 18) *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Joint Framework on countering hybrid threats a European Union response*.

[45] European Commission. (n.d.). *Digital Single Market.* Available: http://ec.europa.eu/priorities/digital-single-market_en. Last accessed 07/10/2016.

[46] European Commission. (2016). *Cybersecurity industry.* Available: https://ec.europa.eu/digital-single-market/en/cybersecurity-industry. Last accessed 13/10/2016; European Commission. (2016). *Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats.* Available: http://europa.eu/rapid/press-release_IP-16-2321_en.htm. Last accessed 13/10/2016.

[47] European Commission (JOIN(2016) 18 final) *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL: Joint Framework on countering hybrid threats a European Union response.*

[48] European Commission (2016) *ANNEX 1: ANNEX CONTRACTUAL ARRANGEMENT SETTING UP A PUBLIC-PRIVATE PARTNERSHIP IN THE AREA OF CYBERSECURITY INDUSTRIAL RESEARCH AND INNOVATION BETWEEN THE EUROPEAN UNION AND THE EUROPEAN CYBERSECURITY ORGANISATION to the Commission Decision on the signing of a contractual arrangement setting up a public-private partnership in the area of cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation*.

2.2.1.1.2 EU PPP & Critical Infrastructures in the NIS Directive

Already in 2013, the draft Network and Information Systems Directive (NIS Directive)[49] reiterated that cooperation between the public and private sector is essential and that market operators should also cooperate with the public sector and share information and best practices in exchange of operational support in case of incidents. The NIS Directive, which entered into force in August 2016, introduces several formal and informal proscriptions for PPPs in the area of critical infrastructure security. Rather than aiming to regulate the procurement of services from the private sector, the Directive seeks to regulate the modes, content and priorities in public-private collaboration.

One of the contributions of the NIS Directive in furthering the European cyber security PPPs is the formalization of a network of Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) including different actors across sectors throughout the Union.[50] The role of the CSIRTs under the Directive is to promote trust, confidence, and operational cooperation between the Member States.[51] The CSIRTs primary functions include supporting Member States in resolving cross-border issues of incident information exchange, coordination, and formalizing cooperation on i) categories of risks and incidents, ii) early warnings, iii) mutual assistance, and iv) modalities for coordination between Member States.[52]

While formalizing official incident notification and reporting channels via competent (public) authorities and CSIRTs,[53] the Directive also encourages operators and service providers to informal cooperation mechanisms and existing channels for collaboration.[54] The Directive recognizes that operators of essential services may be both public or private and does not exclude the possibility that digital service providers can also be public entities.[55] Moreover, the incident notifications are not restricted to the service providers themselves, but also to private bodies to whom the service providers outsources aspects of their network

[49] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48 final, Brussels, 7.2.2013. Recital 15

[50] European Commission. (2016). *Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats.* Available: http://europa.eu/rapid/press-release_IP-16-2321_en.htm. Last accessed 14/10/2016; Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union *OJ L 194, 19.7.2016, p. 1–30.* Recital 34.

[51] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union *OJ L 194, 19.7.2016, p. 1–30.* Article 1(1).

[52] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union *OJ L 194, 19.7.2016, p. 1–30.* Article 12.

[53] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union *OJ L 194, 19.7.2016, p. 1–30.* Recital 32.

[54] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union *OJ L 194, 19.7.2016, p. 1–30.* Recital 35.

[55] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union *OJ L 194, 19.7.2016, p. 1–30.* Article 4(5); DIRECTIVE (EU) 2015/1535 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification), Article 1(1).

management.[56] The Cooperation Group, which primarily facilitates strategic cooperation between states,[57] also has a specific mandate for ensuring that operators and service providers that are party to informal PPPs are not disadvantaged because of their participation in the collaboration.[58]

Article 7 of the Directive further requires all the Member States to adopt their own national strategies on NIS security formulating strategic objectives and regulatory measures for NIS security. Pursuant to Article 7, these strategies the Member States must identify the actors involved in implementing the strategies, define the respective roles of public and other actors as well as the role of PPPs in preparedness, response and recovery.

The implementation and harmonization of the NIS Directive across the territories of the Member States is further supported by a specialized platform set up by the Commission; the NIS Platform. The NIS Platform operates through Working groups in the areas of i) risk management, ii) information exchange and coordination, iii) ICT security research and innovation, to inform the Community of international best practices in these areas.[59]

2.2.2 National legislative frameworks

National states have generally the obligation to protect their population.[60] In this regard the protection of critical infrastructure is an important point. However, since due to privatization many critical infrastructures are in private hands, the concept of public private partnership is important for the protection of critical infrastructures.[61]

In the following sections, two national examples are described. In this regard, the analysis of the Netherlands focuses on the *de facto* partnerships existing in the Netherlands and how they were established, while the Portuguese analysis focuses on the legislation concerning public private partnerships.

2.2.2.1 Public-Private partnerships in the Netherlands

In the Netherlands, public-private partnerships play a crucial role in critical infrastructure protection.[62] Starting from the end of the 1990, efforts have been made to manage critical infrastructure better.[63] The main focus points were national security and ICT security. The report on 'Kwetsbaarheid op Internet – Samen werken aan meer veiligheid en

[56] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union *OJ L 194, 19.7.2016, p. 1–30.* Recital 52.

[57] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union *OJ L 194, 19.7.2016, p. 1–30.* Article 11.

[58] European Commission. (2016). *Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats.*Available: http://europa.eu/rapid/press-release_IP-16-2321_en.htm. Last accessed 17/10/2016.

[59] ENISA. (2016). *NIS Platform.* Available: https://resilience.enisa.europa.eu/nis-platform. Last accessed 17/10/2016.

[60] See P. Wiater, "On the notion of "Partnership" in Critical Infrastructure Protection", EJRR 2, 2015; and S. Brem, "Critical Infrastructure Protection from a National Perspective", EJRR 2, 2015 (referring to art. 2 Federal CPCD Law of Switzerland).

[61] P. Wiater, "On the notion of "Partnership" in Critical Infrastructure Protection", EJRR 2, 2015.

[62] Elgin M. Brunner, Manuel Suter, INTERNATIONAL CIIP HANDBOOK 2008/ 2009, available at http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-08-09.pdf, p. 283.

[63]Elgin M. Brunner, Manuel Suter, INTERNATIONAL CIIP HANDBOOK 2008/ 2009, , available at http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-08-09.pdf, p. 275.

betrouwbaarheid (KWINT)' ('Vulnerabilities on the internet – working together for more security and reliability') from 2001 mentioned that the policy measures of the report should be performed within a public-private partnership framework.[64] As a result of the report, a government-wide computer emergency response team (GOVCERT.NL) and a malware-alerting service (www.waarschuwingsdienst.nl) were founded, and additionally some tasks were given to the Platform Electronic Commerce in the Netherlands (ECP.NL), a public-private partnership platform.[65] After the KWINT program, in 2006, the Veilige Elektronische Communicatie (VEC)/Digibewust programme was set up for three years, designed as a public-private partnership under the responsibility of the Ministry of Economic Affairs.[66]

The different programs and partnerships on national and ICT security often overlap. An example was the 'Nationale Infrastructuur to combat Cybercrime' (NICC), a program with a focus on ICT/cybercrime initiated by the Ministry of Economic Affairs, Agriculture and Innovation.[67] It implemented the 'Informatieknooppunt Cybercrime' (Information node Cybercrime). NICC was in 2010 finalized, but it was decided to continue with the Informatieknooppunt Cybercrime at TNO.[68]

On the other hand, the 'Nationaal Adviescentrum Vitale Infrastructuur' (National Advisory Centre Critical Infrastructure) (NAVI) was started in 2007 to facilitate the cooperation in the field of security.[69] It was a public private partnership between government and critical infrastructure providers. The specifities were defined in the "Instellingsbesluit Nationaal Adviescentrum Vitale Infrastructuur (Instellingsbesluit NAVI)"[70].

NAVI, GOVCERT.NL and NICC have been joined as part of the National Cyber Security Centrum (NCSC).[71] The NCSC is a part of the Ministry of Security and Justice.[72] The NCSC falls under the national Coördinator Terrorismebestreiding en Veiligheid (NCTV), and there it is part of the Directie Cyber Security (DCS)[73]. Art. 53, sub c) of the Organisational decree of the Ministry of Security and Justice 2015[74] provides the tasks of the DCS. The tasks "Monitoring and Response", "Expertise and advice" and "market development and partnerships" together form the NCSC.[75] It is obvious that the promotion of public private partnerships is an important part of the work, since one of the tasks focuses on partnerships and the DCS also has as one of its tasks to provide the secretarial support/run the secretariat for public-private partnerships in the field of cyber security.

[64] CIIP handbook 2002, p. 54, referring to Ronald De Bruin, "From Research to Practice: A public-private partnership approach in the Netherlands on information infrastructure dependability". Dependability Development Support Initiative (DDSI) Workshop (28 Feb 2002).

[65] Elgin M. Brunner, Manuel Suter, INTERNATIONAL CIIP HANDBOOK 2008/ 2009, available at http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-08-09.pdf, p. 277.

[66] Elgin M. Brunner, Manuel Suter, INTERNATIONAL CIIP HANDBOOK 2008/ 2009, available at http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-08-09.pdf, p.277.

[67] see jaaroverzicht ICTU 2009, 2010 https://www.ictu.nl/jaaroverzicht2010/projecten/nationale-infrastructuur-cybercrime/

[68] https://www.rijksoverheid.nl/actueel/nieuws/2010/12/27/succesvolle-aanpak-cybercrime-voortgezet-bij-tno

[69] 2^{e} inhoudelijke analyse beschermde infrastructuur, p. 11.

[70] Overheid. (2016). *Instellingsbesluit Nationaal Adviescentrum Vitale Infrastructuur (Instellingsbesluit NAVI).* Available: http://wetten.overheid.nl/BWBR0024499/2008-09-21. Last accessed 17/10/2016.

[71] Ministrie van Veiligheid en Justitie. (n.d.). *Nationaal Cyber Security Centrum.* Available: https://www.ncsc.nl/. Last accessed 17/10/2016.

[72] Organisatiebesluit Ministerie van Veiligheid en Justitie 2015 http://www.wetten.overheid.nl/BWBR0036820/Hoofdstuk8/Artikel53/geldigheidsdatum_30-07-2015

[73] Art. 50 lid 2 sub b Organisatiebesluit Ministerie van Veiligheid en Justitie 2015.

[74] Organisatiebesluit Ministerie van Veiligheid en Justitie 2015.

[75] Art. 50 lid 3 Organisatiebesluit Ministerie van Veiligheid en Justitie 2015

Cooperation happens via different ways. In 2002, the project 'Bescherming vitale infrastructuur' (Protection critical infrastructure) was started.[76] During this project, 12 critical infrastructures in the Netherlands were identified. The goals of the project were the development and maintenance of a consistent package of measures to protect critical infrastructure, including ICT, and to anchor these measures within the operational management of public and private services. In order to do this, public and private organisations had to work together. Therefore, since 2005 special attention was given to bring together the different parties.[77] This was done by different working groups on an operational level, but also via more formal collaborations such as the 'Strategisch Overleg Vitale Infrastructuur' (Strategic consultation critical infrastructure) (SOVI) and the commissie vitaal van VNO-NCW.[78] SOVI (established in 2006) has the goal to facilitate the structural deliberation between government and the private sector within the context of critical infrastructure.[79] It was established by an official decree (Instellingsbesluit)[80] and consists at least of a chairman, one participant per critical infrastructure, one representative of the Dutch business association VNO-NCW and representatives of the ministries of interior and kingdom relations (BZK), defence and economic affairs.[81]

Additionally, there are several sector specific deliberation structures/networks (e.g. within the Telecom sector, Nationaal Coördinatie Overleg-Telecom NCO-T; within the financial sector, Platform Business Continuity Vitale Infrastructuure (BC VIF)).[82] The main focus point is that all parties know their responsibilities and assume them. The specific responsibilities are often defined by the public parties working together with the sectors. As an example, the drinking-water sector specified their concept of 'goed huisvaderschap' (good housekeeping) into specific tasks and norms, which then have been included in specific legislation (drinkwaterbesluit).[83] The drinking-water companies have furthermore joined the NICC and created within it a special information-node, the Water-ISAC.[84]

Furthermore, the 'Wet veiligheidsregios' (law on security regions)[85] established 25 different security regions in the Netherlands, the Veiligheidsberaad[86], and the 'Instituut Fysieke

[76] Vergaderjaar 2003-2004, Kst. 26643, nr. 53.

[77] 2de inhoudelijke analyse bescherming vitale infrastructuur, available at https://www.rijksoverheid.nl/documenten/rapporten/2010/02/26/analyse-bescherming-vitale-infrastructuur , p.10.

[78] 2de inhoudelijke analyse bescherming vitale infrastructuur, available at https://www.rijksoverheid.nl/documenten/rapporten/2010/02/26/analyse-bescherming-vitale-infrastructuur , p.10.

[79] Art. 3 Besluit instelling van het Strategisch Overleg Vitale Infrastructuur (Instellingsbesluit SOVI), 28 April 2006.

[80] Besluit instelling van het Strategisch Overleg Vitale Infrastructuur (Instellingsbesluit SOVI), 28 April 2006; http://wetten.overheid.nl/BWBR0019781/geldigheidsdatum_27-11-2015 .

[81] Art. 2 Besluit instelling van het Strategisch Overleg Vitale Infrastructuur (Instellingsbesluit SOVI), 28 April 2006.

[82] 2de inhoudelijke analyse bescherming vitale infrastructuur, available at https://www.rijksoverheid.nl/documenten/rapporten/2010/02/26/analyse-bescherming-vitale-infrastructuur, p.10.

[83] 2de inhoudelijke analyse bescherming vitale infrastructuur, available at https://www.rijksoverheid.nl/documenten/rapporten/2010/02/26/analyse-bescherming-vitale-infrastructuur, p.9.

[84] 2de inhoudelijke analyse bescherming vitale infrastructuur, available at https://www.rijksoverheid.nl/documenten/rapporten/2010/02/26/analyse-bescherming-vitale-infrastructuur, p.20.

[85] Wet van 11 februari 2010, houdende bepalingen over de brandweerzorg, de rampenbestrijding, de crisisbeheersing en de geneeskundige hulpverlening (Wet veiligheidsregio's) http://wetten.overheid.nl/BWBR0027466/geldigheidsdatum_27-11-2015

Veiligheid' (the Institute of Phsyical Security)[87] which has educational/research tasks. The Veiligheidsberaad developed together with sectors specific standard agreements (convenanten) to facilitate working together between the security regions and the critical infrastructure providers.[88]

As it results from the provided examples, the public and private sectors work together for the protection of critical infrastructures. This is facilitated by specific public programmes, the explicit support of public private partnerships and the existence of business organisations which speak on behalf of their members within the partnerships. Standard contractual clauses help in some regards to facilitate the partnerships between specific sectors and public services. The incentive for the private partner for working together seems to be not only the fact that businesses are responsible for the continuity of their services, but often also to have an influence on the applicable regulation.

2.2.2.2 Public Private Partnerships in Portugal

The current legal framework for Public Private Partnerships in Portugal is the result of the compromises entered by Portugal with its troika of creditors (the European Commission, the European Central Bank and the International Monetary Fund) under the Memorandum of Understanding on Specific Economic Policy Conditionality (MoU),[89] which formed part of the Economic Adjustment Programme for Portugal. Under clause 3.20 of the MoU, the Portuguese government undertook to 'put in place a strengthened legal and institutional framework (…) for assessing fiscal risks ex-ante of engaging into PPP, concessions and other public investments, as well as for monitoring their execution' before the end of the first quarter of 2012.

This resulted in the approval of the 2012 PPP Law by Decree Law no. 111/2012, of 23 May 2012, which sets out the legal framework for public-private partnerships (PPPs) in Portugal. This law should be read together with the Public Procurement Code (Decree Law no. 18/2008, of 27 April 2008, with the last amendments introduced by Decree Law no. 214-G/2015, of 2 February 2015)[90] and with specific sectorial legislation, namely Decree Law no. 185/2002, of 20 August (with the last amendments introduced by Decree Law no. 111/2012, of 23 May 2012),[91] which determines the legal regime applicable to PPPs in the health sector. In the following chapters, we will refer to and analyse the relevant provisions of the 2012 Portuguese PPP Law.

2.2.2.2.1 Scope of the 2012 PPP Law

The 2012 PPP Law establishes the general rules applicable to State intervention in the definition, design, preparation, launch, award, modification, inspection and global monitoring of PPPs.[92]

The law defines PPPs as contracts or unions of contracts through which a private partner undertakes, towards a public partner, on a long-term basis, against consideration, to ensure the performance of an activity aimed at the satisfaction of a collective need, and assumes responsibility, in whole or in part, for the investment, financing, operation and associated

[86] Consisting of the 25 chairpersons of the security regions.

[87] Art. 66 Wet Veiligheidsregios.

[88] http://www.veiligheidsberaad.nl/Pages/home.aspx see convenanten.

[89] In particular, points 3.17 to 3.21.

[90] A consolidated (Portuguese) version of the code can be accessed at http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2063&tabela=leis.

[91] A consolidated (Portuguese) version of the law can be accessed at http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1682&tabela=leis.

[92] 2012 PPP Law, Article 1(a).

risks thereof.[93] Their essential purpose is costs saving and the increased efficiency in the allocation of public resources in relation to other contracting models, as well as the qualitative and quantitative improvement of the service, spurring from effective controls that allow its continued evaluation by the public partner and by (potential) users.[94]

The expression 'public partner' covers the State, State Bodies, Autonomous Funds and Services, Public Undertakings and any other entities constituted by these to meet general interest needs.[95] The public partner is responsible for monitoring, evaluating and controlling the execution of the partnership to ensure the public interest purposes in which the PPP is based.[96]

The private partner is usually a private entity. However, for the purposes of the application of this legislation, the private partner can also be a Public Undertaking, a co-operative or a non-profit organisation.[97] The private partner is responsible for the exercise and management of the contracted activity in respect of the contract, as well as its partial or complete funding.[98]

The concept of risk-sharing between the partners is of particular relevance and must be clearly identified in the PPP contract.[99] Risks must be shared between the parties in accordance with their respective capacity to manage them,[100]and the PPP must **significantly and effectively transfer risks to the private sector**.[101] Risks that do not have a proper and duly based justification should be avoided.[102]

The contractual relationship can result from a public works concession or sub-concession, a public services concession or sub-concession, a continuous supply agreement, a service agreement, a management agreement or, in respect of the use of an already existing establishment or infrastructure owned by a party other than the public partner, a collaboration agreement.[103]

The application of the legal framework of this diploma is limited to partnerships that, cumulatively, and for the entire duration of the partnership, result in a gross expense not inferior to 10 Million Euros and an investment not inferior to 25 Million Euros (including maintenance, reparation, conservation and substitution costs). The same applies to concessions through a legal diploma granted by the State to entities with a public nature or with exclusively public capital. In these cases, only the rules concerning the purpose of the PPP, allocation of responsibilities, requirements for the use of PPP and risk-sharing apply.[104]

2.2.2.2.2 The PPP Technical Support Unit

In addition to laying down the legal regime applicable to PPPs, the 2012 PPP Law also set up a Technical Support Unit (Unidade Técnica de Acompanhamento de Projetos – UTAP). This is an autonomous administrative entity that assumes responsibilities in the preparation, development, execution and monitoring of public-private partnership procedures (PPP) and

[93] 2012 PPP Law, Article 2(1).

[94] 2012 PPP Law, Article 4(1).

[95] 2012 PPP Law, Article 2(2).

[96] 2012 PPP Law, Article 5(a).

[97] 2012 PPP Law, Article 2(3).

[98] 2012 PPP Law, Article 5(b).

[99] 2012 PPP Law, Article 7(1).

[100] 2012 PPP Law, Article 7(1)(a).

[101] 2012 PPP Law, Article 7(1)(b).

[102] 2012 PPP Law, Article 7(1)(c).

[103] 2012 PPP Law, Article 2(4).

[104] 2012 PPP Law, Article 2(5)-(7).

provides specialized technical support, notably on matters of economic, financial and legal nature (including contract management).[105]

It should be noted that the attributions granted to UTAP are without prejudice to other competences in relation to supervision, monitoring of implementation and determination of audits resulting from other laws or contracts.[106] This includes, amongst others, the supervision and control of the Portuguese Court of Auditors.

2.2.2.2.3 Tender preparation, evaluation and award of contract

As mentioned, PPPs' aims at costs savings, an increased efficiency in the allocation of public resources and the improvement of the provided service. The launching and the award of a PPP contract is subject to several requirements:

I) The use of this model of contracting must result in benefits to the public sector in relation to alternative ways of reaching the same objective(s) and, simultaneously, result in the private partner having a prospect of obtaining an adequate remuneration to the invested quantities and to the type and degree of risks it assumes.[107]

II) A prior analysis of predictable budgetary impacts and their affordability, as well as their sensitivity assessments in relation to the existing demand and the macroeconomic evaluation is required.[108]

III) It must comply with the law, including the rules concerning multiannual financial programming that are part of the Budgetary Framework Law.[109]

IV) Obtaining the required authorizations, licenses and legal opinions, so that the execution risks are –or may be– adequately transferred to the private partner.[110]

V) The objectives of the PPP for the public sector must be made clear, including the intended results and the associated advantages, from the perspective of a cost-benefit analysis, as well as the results that the private partner must achieve.[111]

VI) The term of the PPP must be adequate to the circumstances and characteristics of each project.[112]

VII) The PPP model and contractual structure must avoid or minimize to the possible extent the possibility of unilateral contract modifications by the public partner or that result from any facts or circumstances that generate or enhance obligations to restore the financial balance of the contract.[113]

VIII) The PPP model and contractual structure must guarantee that the financial effort of the public partner is shared appropriately in respect of budgetary affordability, allowing for the maintenance of the interest of the private partner in every circumstance and during the entire term of the PPP.[114]

IX) During a pre-contractual phase, all the diligences and appropriate requirements to reach an economically competitive economical result must be adopted.[115]

[105] 2012 PPP Law, Articles 34 to 36

[106] 2012 PPP Law, Article 31

[107] 2012 PPP Law, Article 6(1)(a).

[108] 2012 PPP Law, Article 6(1)(b).

[109] 2012 PPP Law, Article 6(1)(c)-(d).

[110] 2012 PPP Law, Article 6(1)(e).

[111] 2012 PPP Law, Article 6(1)(f)-(g).

[112] 2012 PPP Law, Article 6(1)(h).

[113] 2012 PPP Law, Article 6(1)(i).

[114] 2012 PPP Law, Article 6(1)(j).

[115] 2012 PPP Law, Article 6(1)(k).

X) The detailed breakdown of all the risks incurred by each party and an adequate assignment of responsibilities and risk sharing between the public and private partners must be disclosed.[116]

XI) The situations that during the contract duration can result in benefit-sharing between the parties and/or result in the allocation to the public partner of all the benefits must be identified.[117]

XII) The public entity responsible for any existing payments as well as the reasoned identification of the origin of the respective funds must be identified.[118]

XIII) The public entity responsible for managing the contract must be identified.[119]

Whenever one potential public partner intends to initiate the study and preparation of the launch of a PPP, it must present a dully grounded proposal to the Minister describing the object of the PPP, its objectives, its economic rationality and its financial viability.[120] If the minister decides to initiate the study and preparation of the PPP, he establishes a project team together with the Minister of Finance, and the PPP Technical Support Unit.[121] The project team will develop the preparatory works necessary for launching the PPP tender and assess the verification of all the requirements for the PPP tender preparation and award of contract.[122] The choice of the procedure for entering into a PPP contract shall obey the provisions of the Public Procurement Code.[123] The procedure for awarding the PPP contract is conducted by a jury, appointed by a joint decree issued by the Minister of Finance and the Minister whose portfolio covers the area of the project. Within thirty days from the reports issued by the jury, a PPP contract can be awarded by a joint decree issued by the Minister of Finance and the Minister whose portfolio covers the area of the project.[124]

2.2.2.2.4 Execution and Amendments to PPPs

The execution of the PPP shall obey to what is established in the contract. Whenever the complexity, associated values or public interest of the PPP justify it, the Minister of Finance and the Minister whose portfolio covers the area of the project can determine the constitution of a team to follow the initial execution of the contract.[125] The procedures amending a contract through the course of its execution are regulated in the law and require negotiations with the public party, the approval of the Ministers and the intervention of the PPP Technical Support Unit.[126]

2.2.2.2.5 Rules for Candidates and Exclusion Grounds

The rules for participation of entities as candidates in Public Procurement procedures are determined in articles 52 to 55 of the Public Procurement Code. Under these provisions, single or legal entities, either by themselves or as a consortium, are allowed to participate in Public Procurement procedures.

Article 55 of the Public Procurement Code contains the list of causes for exclusion of candidates from public procurement procedures. These include: insolvency and bankruptcy; conviction in relation to crimes that affect one’s professional conduct or in relation to

[116] 2012 PPP Law, Articles 6(1)(l)-(m) and 7.
[117] 2012 PPP Law, Article 6(1)(n).
[118] 2012 PPP Law, Article 6(1)(o).
[119] 2012 PPP Law, Article 6(1)(p).
[120] 2012 PPP Law, article 9(1).
[121] 2012 PPP Law, articles 9(2)-(3) and 10.
[122] 2012 PPP Law, article 12(1)-(2).
[123] 2012 PPP Law, article 15.
[124] 2012 PPP Law, article 18(1).
[125] 2012 PPP Law, article 19.
[126] 2012 PPP Law, articles 20 to 23.

participation in a criminal organization activity, corruption, fraud or money laundering by single persons, or in respect of legal persons, by the holders of their governing, management or administration bodies; administrative sanctions for serious breach of professional conduct applied to single persons, or in respect of legal persons, to the holders of their governing, management or administration bodies; lack of payment of social security contributions or taxes in Portugal or in the State of which they are nationals or in which they are established.

2.2.2.2.6 PPPs in relation to Critical Infrastructures

To the best of our knowledge, the Portuguese Law (namely, the 2012 PPP Law, the Public Procurement Code and Decree Law no. 62/2011, of 9 May 2011, which implements in Portugal the 2008 Directive on European Critical Infrastructures) does not contain any direct reference to PPPs in relation to Critical Infrastructures. However, the Public Procurement Code allows the use of direct awards in Public Procurement independently of the object of the contract when, under the applicable law, the contract is declared to be secret or its execution must be made with special security measures, as well as whenever the defence of essential interests of the State require it.[127]

On the other hand, the area of security is one of the areas where there is an ongoing PPP. This relates to a Digital System for the Emergency and Security Network, which was awarded by the Portuguese Government to a consortium that then gave origin to SIRESP - Redes Digitais de Segurança e Emergência, S.A. (the operator).[128] The 'SIRESP' (Integrated System of Portugal's Emergency and Security Networks) aims at providing an inter-agency voice and data communications to users in the police, fire and ambulance services. It resulted in the implementation of a digital two-way radio network with improved national coverage, increased security and voice quality and packet data capability and in the adaption of the business processes followed by the various government agencies.

2.3 Principles of the European Union and their application in Cyber Security and NIS Protection

The European Union was founded through a series of historic agreements; the 1951 Treaty of Paris and the creation of the European Coal and Steel Community, the 1957 Treaties of Rome and the European Economic Community and European Atomic Energy Community, the 1967 Merger Treaty and the establishment of European Community institutions, the 1985 Schengen Agreement, the 1985 Single European Act and the 1992 Maastricht Treaty. Today, the Union finds its basis in the Treaty of the European Union (TEU)[129] and the Treaty on the Functioning of the European Union (TFEU),[130] aligning all the areas where the Union enjoys legislative competence to the foundational values and principles of the Union. These values and principles apply to physical and digital realities alike.[131] Not surprisingly then, one

[127] Public Procurement Code, article 24(1)(f).

[128] See SIRESP. (2009). *SIRESP.* Available: http://www.siresp.com/. Last accessed 17/10/2016. The PPP contract and other non-confidential documentation related to this PPP are publicly available at the PPP Technical Support Unit website – Segurança. (n.d.). *Segurança.* Available: http://www.utap.pt/seguranca.htm. Last accessed 17/10/2016.

[129] Consolidated version of the Treaty on European Union *OJ C 326, 26.10.2012, p. 13–390*

[130] Consolidated version of the Treaty on the Functioning of the European Union OJ C 326, 26.10.2012, p. 47–390

[131] European Commission (COM(2015) 185) *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: The European Agenda on Security;* European Commission (JOIN(2013) 1) JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL

of the strategic objectives of EU policy and law in this realm is the protection of its fundamental values; human dignity, freedom, democracy, equality, the rule of law and respect for human rights.[132] European cyber and Network Information Security has developed as a matter of strategy, policy and law over time and across the competences of the Union, e.g. ensuring freedom, security and justice (Title V TFEU), as matter of common security and defense policy (Title I), in view of achieving the operation of the Common Market (Article 308 TEU) and to approximate laws concerning health, safety, environmental protection and consumer protection (Article 114 TFEU). This text focuses specifically on the fundamental principles of the European Union, including the principles ensuring the sovereignty of the Members States - *conferral*, *subsidiarity, and proportionality,* enshrined in Article 5 TEU - and how they have been applied to European cyber and Network Information Security.

2.3.1 Conferral

> *Under the principle of conferral, the Union shall act only within the limits of the competences conferred upon it by the Member States in the Treaties to attain the objectives set out therein. Competences not conferred upon the Union in the Treaties remain with the Member States.*

The principle of conferral is set out by Article 4 and 5 (above) TEU. The principle relates to the distribution of competences between regional and domestic institutions within the Union.[133] The principle essentially constricts the powers of the Union to ensure the sovereignty of the states and that the Union only acts according to its areas of competence: [134]

Exclusive. Article 3 TFEU determines that the Union has exclusive competence in the areas of the customs union, monetary policy, marine biology conservation, or common commercial policy.

Shared. Article 4 TFEU determines that the shared competences between the Union and Member States are the internal market, social policy, economic, social and territorial cohesion, consumer protection, trans-European networks, energy, freedom, security and justice, common safety and public health to name a few.

Coordinated. Article 5 TFEU sets out a mandate to coordinate certain economic policies relating to the employment and social policy.

Support, coordinated or supplemented. Article 6 TFEU allows the Union to support, coordinate or supplement Member State action in the fields of protection and improvement of, inter alia, human health, civil protection and administrative cooperation.

COMMITTEE AND THE COMMITTEE OF THE REGIONS: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (Brussels, 7.2.2013)S

[132] Consolidated version of the Treaty on European Union *OJ C 326, 26.10.2012, p. 13–390,* Article 2; *The European Agenda on Security;* European Commission (JOIN(2013) 1) JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (Brussels, 7.2.2013)

[133] Eurlex. (n.d.). *Distribution of competences.* Available: http://eur-lex.europa.eu/summary/glossary/competences.html. Last accessed 07/11/2016.

[134] See European Commission. (2016). *FAQ on the EU competences and the European Commission powers.* Available: http://ec.europa.eu/citizens-initiative/public/competences/faq#q1. Last accessed 07/11/2016

2.3.2 Subsidiarity

> *Under the principle of subsidiarity, in areas which do not fall within its exclusive competence, the Union shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level.*
>
> *The institutions of the Union shall apply the principle of subsidiarity as laid down in the Protocol on the application of the principles of subsidiarity and proportionality. National Parliaments ensure compliance with the principle of subsidiarity in accordance with the procedure set out in that Protocol.*

Subsidiarity is one of the foundational principles of the European Community and was codified already in the Single European Act as and the Maastricht Treaty. It is regulated by Article 5 TEU (above) and Protocol No 2 to the Treaty on the European Union.[135] It exists to anchor powers and decisions as close to the citizens as possible[136] and to cement the sovereignty of the Member States in areas of policy and law that are not exclusive competences to the Union. Conversely, the principle provides for a limited mandate of Union involvement to situations where the scale or effects of proposed action make Union interventions better placed to achieve an action.[137] The effect of these dual objectives is a balance of power between institutions.[138] Three criteria for subsidiarity have been condensed from Article 5 by the European Parliament:

The non-exclusivity of competence. The area of policy or law must not rest within the Union's *exclusive spheres of competence* as determined by Article 3 TFEU, i.e. the customs union, monetary policy, marine biology conservation, or common commercial policy.[139] The Union actions must fall under the competences that are *shared* between the Union and Member States under Article 4 TFEU, *coordinated* polices under Article 5, or actions to *support, coordinate or supplement* the actions of Member States under article 6 TFEU.[140]

Necessity. The actions would not be sufficiently achieved by the individual Member States.

Added value. The actions will be more successful when implemented by Union institutions because of the scale or effects of the action.

The principle applies to the Union legislature on the one hand[141] and to the Union Institutions on the other hand.[142] The principle is enforced by means of legislative consultations and

[135] 2. PROTOCOL ON THE APPLICATION OF THE PRINCIPLES OF SUBSIDIARITY AND PROPORTIONALITY (C 310/207)

[136] 2. PROTOCOL ON THE APPLICATION OF THE PRINCIPLES OF SUBSIDIARITY AND PROPORTIONALITY (C 310/207)

[137] Eurlex. (n.d.). *Subsidiarity.* Available: http://eur-lex.europa.eu/summary/glossary/subsidiarity.html. Last accessed 07/11/2016; European Parliament. (2016). *THE PRINCIPLE OF SUBSIDIARITY.* Available: http://www.europarl.europa.eu/ftu/pdf/en/FTU_1.2.2.pdf. Last accessed 07/11/2016.

[138] European Parliament. (2016). *THE PRINCIPLE OF SUBSIDIARITY.* Available: http://www.europarl.europa.eu/ftu/pdf/en/FTU_1.2.2.pdf. Last accessed 07/11/2016.

[139] See European Commission. (2016). *FAQ on the EU competences and the European Commission powers.* Available: http://ec.europa.eu/citizens-initiative/public/competences/faq#q1. Last accessed 07/11/2016

[140] See European Commission. (2016). *FAQ on the EU competences and the European Commission powers.* Available: http://ec.europa.eu/citizens-initiative/public/competences/faq#q1. Last accessed 07/11/2016

[141] 2. PROTOCOL ON THE APPLICATION OF THE PRINCIPLES OF SUBSIDIARITY AND PROPORTIONALITY (C 310/207), Article 2.

other procedural requirements on the Commission and Parliament set out by Protocol No 2 and through domestic parliamentary compliance monitoring according to Articles 5(3) and 12(b) TEU. Additionally, the Court of Justice of the European Union has jurisdictions to rule on matters relating to the principle.[143]

2.3.3 Proportionality

> *Under the principle of proportionality, the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties.*
>
> *The institutions of the Union shall apply the principle of proportionality as laid down in the Protocol on the application of the principles of subsidiarity and proportionality.*

Much like the principles of conferral and subsidiarity, the principle of proportionality in Article 5 (above) limits the powers of the European regional vis-à-vis the Member States and the citizens of states within the Union.[144] The actions of the Union must be adequate for the objective and not exceed what is necessary to achieve objectives. Proportionality also balances rights and principles, especially the rights of the individual against interferences from Union actions through its implementation in case law in the Court of Justice of the European Union and the European Court of Human Rights.[145] Like the principle of subsidiarity, the enforcement of the principle is controlled through the procedures in Protocol No2 TEU.

2.3.4 Solidarity

The principle of solidarity, Enshrined in Article 3 TEU, facilitates Union cohesion as it ensures that the Member States share equally, or at least reciprocally, in the benefits and burdens of collaboration.[146] Solidarity featured already in the 1951 Treaty Establishing the European Coal and Steel Community Treaty, stating in the preamble that “Europe can be built only through real practical achievements which will first of all create real solidarity, and through the establishment of common bases for economic development.” Moreover, Article 122 of the Lisbon Treaty reaffirms the importance of solidarity as a mechanism of collaboration in the context of disasters within the Member States:

The Union and its Member States shall act jointly in a spirit of solidarity if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster. The Union shall mobilise all the instruments at its disposal, including the military resources made available by the Member States

[142] 2. PROTOCOL ON THE APPLICATION OF THE PRINCIPLES OF SUBSIDIARITY AND PROPORTIONALITY (C 310/207), Article 1.

[143] 2. PROTOCOL ON THE APPLICATION OF THE PRINCIPLES OF SUBSIDIARITY AND PROPORTIONALITY (C 310/207), Article 8.

[144] Eurlex. (n.d.). *Proportionality principle.* Available: http://eur-lex.europa.eu/summary/glossary/proportionality.html. Last accessed 07/11/2016.

[145] Her Majesty's Government of the United Kingdom. (2014). *Review of the Balance of Competences between the United Kingdom and the European Union Subsidiarity and Proportionality.* Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/388852/BoCSubAndPro_acc.pdf. Last accessed 07/11/2016.

[146] Europfound. (2011). *Solidarity principle.* Available: https://www.eurofound.europa.eu/observatories/eurwork/industrial-relations-dictionary/solidarity-principle. Last accessed 28/03/2017; Jérôme Vignon. (2011). *Solidarity and responsibility in the European Union.* Available: http://www.institutdelors.eu/media/bref27_jvignon_en.pdf?pdf=ok. Last accessed 28/03/2017; Andrea Sangiovanni. (2013). Solidarity in the European Union. *Oxford Journal of Legal Studies*. 33 (2), 213-241.

It is noteworthy that in cases of disasters, Article 122 of the Lisbon Treaty specifically seeks to enable solidarity through prevention, protection, assistance, and coordination.

2.3.5 Application to European Cyber & Network Information Security

It should be noted that all the principles of the European Union apply to European cyber and network information security (NIS). However, not all the principles relevant to sovereignty and cooperation have codified overtly into this field of Union actions. Among the former three the two principles regulated by Protocol No 2, subsidiarity and proportionality, are foremost reflected in this area of policy and law. Similarly, complementarity is the favored principle among the three Union tenets for cooperation. The principles ensure state sovereignty and Union cooperation became explicit to European cyber and NIS security in COM(2006) 786 and the European Programme for Critical Infrastructure Protection (EPCIP). The principle of subsidiarity has meant that the Union competence over critical infrastructure concerns the infrastructures that are important to the EU.[147] The EU implemented this focus substantively through key policy enablers of the principles; i) the identification and designation of European Critical Infrastructures and ii) an assessment of the need to improve their protection,[148] iii) a Critical Infrastructure Warning Information Network (CIWIN) for threats that are common to the Member States,[149] and iv) collaboration between Member States on evaluating the socioeconomic impact of network security incidents and collaboration between CERTs. These initiatives all targeted infrastructures and threats that are shared between states. Within the EPCIP framework, it was also determined that proportionality would mean that Union actions only respond to gaps in the security of critical infrastructures and that the measures are in proportion to the seriousness of the threat. In 2016, the European Union adopted Directive (EU) 2016/1148 (the NIS Directive) in accordance with the subsidiarity principle.[150] The Union reasoned that the effects of high common level of security of network and information systems across the Union cannot be achieved by the individual Member States, but only through Union intervention.[151] The Union also considered the NIS Directive to be limited to measures necessary for achieving the objective (*proportionality*) of a high common level of security.[152] Moreover, the NIS Directive also conferred powers to the Commission to lay down procedural arrangements for the transnational bodies established by the Directive.[153] It should further be recognized that the European cyber and NIS initiatives generally reflect attempts at improving prevention, protection and coordination in line with the solidarity principle. As such these policy initiatives and regulations are attempts at structuring enablers for solidarity in cybersecurity incidents, crises and disasters.

[147] European Parliament. (2006). *The European Programme for Critical Infrastructure Protection (EPCIP) (MEMO/06/477).* Available: europa.eu/rapid/press-release_MEMO-06-477_en.pdf. Last accessed 07/11/2016; Commission of the European Communities (COM(2006) 786) COMMUNICATION FROM THE COMMISSION:

[148] 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 [2008] OJ L345/75.

[149] Commission of the European Communities (COM(2008) 676) Proposal for a COUNCIL DECISION on a Critical Infrastructure Warning Information Network (CIWIN) (Brussels, 27.10.2008)

[150] Council Resolution (2009/C 321/01) on a collaborative European approach to Network and Information Security

[151] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Recital 74

[152] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Recital 74

[153] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Recital 74; See also Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

2.4 The Challenges of a PPP for CIP

CIs have become one of the most vulnerable and valuable targets of different causes of disruption, in higher developed societies. Increasing numbers of CI incidents with political or even strategic dimension are demanding new security concepts. Terms like Cyber War, Hybrid Treats (NATO), Unconventional or Non-Linear Warfare have entered the political discussion (see e.g. [14]).

There are numerous PPPs but little in CIP let alone fully working role models on PPPs for CIP/ CIIP. Awareness at the political level in the USA was developed as early as 1997 [11]: **"The only sure path to protected infrastructures in the years ahead is through a real partnership between infrastructure owners and operators and the government"**. This requires a culture of trust and confidence, and the cognizance that both, infrastructure providers and governments need to produce a **win-win strategy,** if the worst should be avoided in the event of critical or catastrophic incidents.

In Europe, awareness started much later and –in many nations–, there is still the tendency of scepticism on the industry side, and of desire to over-regulate on the government side. In Germany, e.g. the parliament passed the IT-Sicherheitsgesetz" (law on IT security). It basically tries to put the burden of obligations on the infrastructure providers and even exempts the public sector from these obligations [13].

When thinking about introducing instruments of the EPCIP in general, of PPPs in particular, and especially a toolset such as the ECOSSIAN System (ES), the basic prerequisite for success will be the **willingness of cooperation of all to the benefit of all**.

It is important to recognize the following drivers, needs, triggers, and issues:

1. Major CI incidents may have catastrophic impacts on societies, with significant strategic and political dimensions;
2. The degree of severity of risks is growing;
3. Effective preparedness and response can only be addressed in an environment of cooperation between the private sector and governmental institutions (and increasingly by engaging other societal organizations, communities, and individuals);
4. PPPs have a tradition in sectors where the public-private cooperation has historically grown (e.g. in healthcare or aviation);
5. ICT security standards and implementations often chronically lag behind the technical possibilities and behind required security levels;
6. For ensuring success, the EU may contribute with a clearly cooperative strategy and execution, aligned with the principles of subsidiarity and solidarity;
7. A system such as ECOSSIAN can effectively work only under well-defined PPP agreements which include the three "tiers": EU, national governments and industry. This makes PPP even more difficult than pure national PPPs.

Also, regarding the scope and purpose of the ES, the following issues need to be addressed:

1. The scope of ECOSSIAN is **European**. I.e. it will serve to cope with incidents that require more than local responses. Most incidents that require national, transnational or European-wide responses will require one way or another cooperation between governmental and non-governmental (primarily industrial) actors. Note, however, that even local incidents may be better addressed by engaging help from cooperating organizations, for the purposes of improved situational awareness, response, recover, as well as sharing of best practices.

2. The design of an ECOSSIAN System will not be confined to minor/local incidents, but should also support national, multinational or European responses to incidents that would/could endanger states and societies at large.
3. PPP is understood to include organizational structures, methods for establishing and operating PPP, procedures and rules for cooperation between public and private actors in preparing for and responding to security incidents. For ECOSSIAN this needs to include cooperation between national organizations and enterprises.
4. The criticality of PPP requirements varies with areas of concern. It is particularly strong in areas like public transport, traffic, energy, communication and under extreme crisis conditions (international conflict, strategic terrorism). It also varies between Member States (MS) w.r.t. vulnerabilities (e.g. different degrees of industrial digitalization), preparedness levels, risk exposures, potentials for PP synergies and emerging new challenges. But also, "every day" incidents, information exchange and coordination need to be regulated.
5. **Increasing interdependencies** resulting from progressing industrial digitalization and the **widening range of risks and attackers** will combine to increase the needs and requirements of ECOSSIAN. It will tend to change the role of state authorities and to enlarge the role of enterprises along with an increasing need for cooperation not only between public and private actors, but also between enterprises and organizations in different branches.
6. Given the increasing importance of hybrid threats, the range of scenarios will need to be broadened to include roles for ECOSSIAN in complex crises and conflicts with non-state adversary actors and, more importantly still, future state-actors who arguably will possess more devastating means for cyber-attacks.
7. ECOSSIAN thus should be designed not only with regards to challenges as they exist at the presumed time of its operation, but in view of **plausible changes** throughout its life-time and in view of **future needs** and requirements.
8. In this vein, the ECOSSIAN project is an important initial step, the more so if it succeeds to become relevant on EU level. But then PPP itself becomes mandatory.
9. In particular, in view of the European level **comparative country assessments** of state-enterprise arrangements and of the varying scope for synergies, **standardization and harmonization of national efforts** on the EU level are indispensable.
10. Since ECOSSIAN is expected not to be confined to enhanced capacities for cyber effects, system studies are needed to understand current and future functionalities within critical configurations of actors, in varying risk and threat scenarios. In particular, the benefits from PPP for public and private actors, for crisis management and for the viability of societies at large need to be analysed and realised.

Finally, addressing the challenges of PPPs for the ES entails pondering the factors:

1. The ECOSSIAN project is expected to develop a prototype-system to support CIP in Europe on all levels: individual, national/regional and European levels. **Its European scope will be the most demanding objective**: it requires effective solutions on lower levels, but as a three tiers-system it needs to work w.r.t. the variety of divergent national CI systems as well as the additional complexity on national, transnational and European levels (three tier situation). It needs to meet the challenges of the European ecosystem of cooperation and interdependencies of CIs and multiple types of existing and needed types of public-private cooperation.

2. **Given inherent tensions and constraints in public-private cooperation**, a holistic system embracing these three tiers requires types of institutionalized and contractual cooperation, i.e. of public-private partnership (PPP), to become effective.
3. While national approaches to **risk and threat assessments in part differ widely**, responses on European levels need to be **harmonized to the extent possible,** as they are uniquely indispensable in case of serious-to-catastrophic incidents with major transnational and Europe-wide consequences.
4. ECOSSIAN is expected to develop a prototype that will demonstrate the feasibility of solutions for information-sharing and coordination under threatening conditions for CIP. This system will be successful only if the technical solutions will be complemented by an effective and agreed organizational framework and the implementation of novel rules and regulations [73]. To become effective on all levels –namely on the European level–, embedding an ECOSSIAN-type system into the European ecosystem of cooperation and interdependencies in CIP will require complex and innovative work on national and European levels. Establishing institutionalized public-private partnerships that enable **effective information-sharing and coordination of responses** also on European levels will be a prerequisite.
5. Work on applicability of the ECOSSIAN system to that end, namely including coordination of responses, will require far more preparatory conceptual, organizational and legal study. Some important stocktaking, definitional and conceptual preparatory work has been undertaken by ENISA [37]. ENISA's work pertains to the risks of cyberattacks on CIIP and on the requirements for governance and adaptability for PPP to ensure both the security of IT-based governmental activities and for sustainable Digital Single Market ecosystem in Europe.[154]

2.5 CIIP and Need for PPP

This section presents and discusses criteria for the criticality of CIIP, lessons from the USA experience, and the role of PPP in CIIP.

2.5.1 Criteria for the Criticality of CIIP

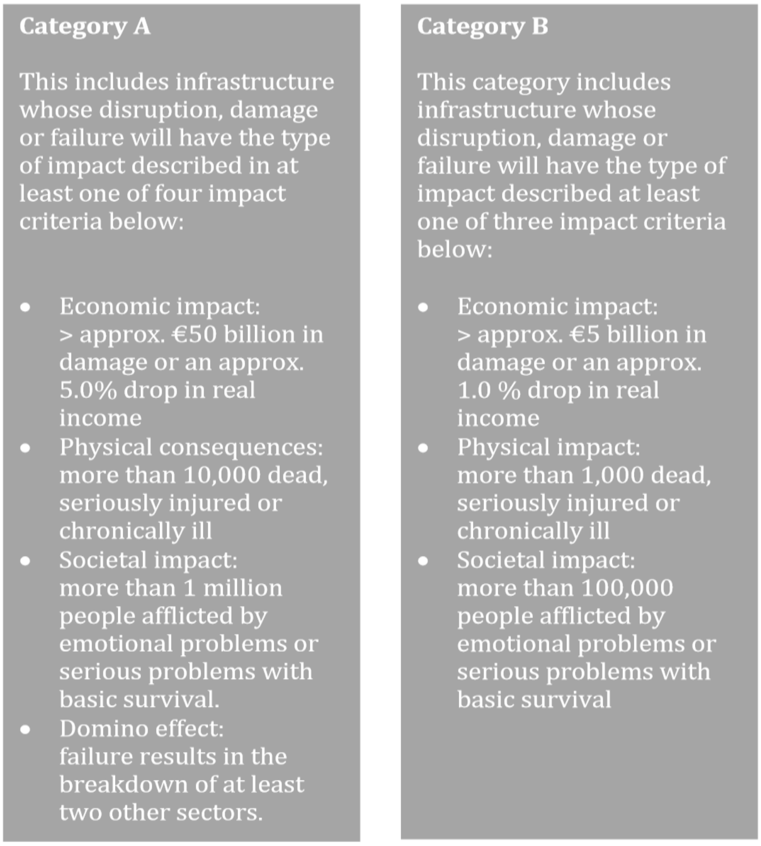
On all levels - i.e. local, corporate (like hubs that tend to spread disruptive effects), regional, governmental, national and up to transnational, Europe-wide and increasingly global-, the vulnerabilities and risk exposures of advanced societies would suggest an increasing frequency and impact of disruptive incidents and actions than is actually the case. On the other hand, given the damage in more severe cases, it is important to recognize the resilience of societies, economies and governmental structures, to anticipate severe disruptions and their consequences and get prepared for them.

In part this also derives from the specificity of intentions and circumstances that result in disruptive events. Technological, organizational, as well as educational measures of preparedness thus are indispensable. But the more advanced the societies and the greater their complexity, the greater the need for enhanced security, but also the likelihood that security measures may fail or be insufficient. Prioritized risk reduction tends to suffer if complete security is the overriding goal.

[154] The evolving efforts towards Industry 4.0 have speeded the Commission's activities towards PPP. See the Commission's proposed PPP on cybersecurity that followed the launch of the Digital Single Market plan.

On all levels interdependencies exist between sectoral processes. They are critical to the extent disruption in one sector or process has the potential to impact on much larger scales on societies, economies and/or governmental structures.

Table 1: CI Disruption Impact Criteria, taken from [61].

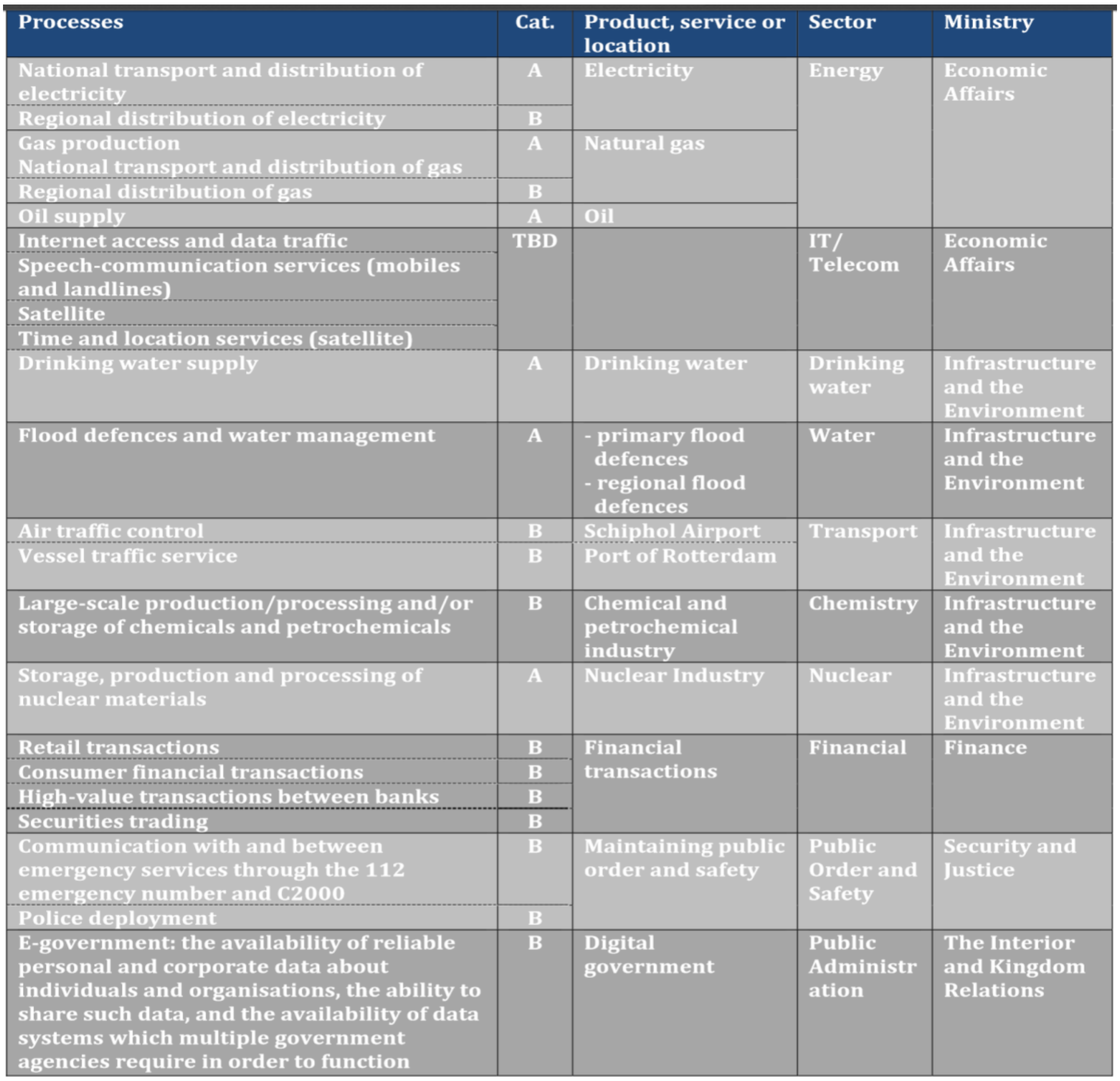


Category A	**Category B**
This includes infrastructure whose disruption, damage or failure will have the type of impact described in at least one of four impact criteria below:	This category includes infrastructure whose disruption, damage or failure will have the type of impact described at least one of three impact criteria below:
• Economic impact: > approx. €50 billion in damage or an approx. 5.0% drop in real income • Physical consequences: more than 10,000 dead, seriously injured or chronically ill • Societal impact: more than 1 million people afflicted by emotional problems or serious problems with basic survival. • Domino effect: failure results in the breakdown of at least two other sectors.	• Economic impact: > approx. €5 billion in damage or an approx. 1.0 % drop in real income • Physical impact: more than 1,000 dead, seriously injured or chronically ill • Societal impact: more than 100,000 people afflicted by emotional problems or serious problems with basic survival

Criteria for the criticality of infrastructures vary though. The National Strategy for Critical Infrastructure Protection issued by the German Federal Government defines CIs as "organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences." In 2013 the Dutch government has undertaken a review that relates criticality to processes instead of sectors and it has introduced a list of CIs that distinguishes two categories of CIs (see Table 1) in order to ease prioritization and the selection of arrangements for enhancing resilience[155]. Table 2 shows a summary of critical processes, the related CIs and the responsible ministries in the Netherlands.

[155] For the resulting list of CIs see Table 2.

Table 2: Impacts on CI Processes, taken from [61].



Processes	Cat.	Product, service or location	Sector	Ministry
National transport and distribution of electricity	A	Electricity	Energy	Economic Affairs
Regional distribution of electricity	B			
Gas production National transport and distribution of gas	A	Natural gas		
Regional distribution of gas	B			
Oil supply	A	Oil		
Internet access and data traffic	TBD		IT/ Telecom	Economic Affairs
Speech-communication services (mobiles and landlines)				
Satellite				
Time and location services (satellite)				
Drinking water supply	A	Drinking water	Drinking water	Infrastructure and the Environment
Flood defences and water management	A	- primary flood defences - regional flood defences	Water	Infrastructure and the Environment
Air traffic control	B	Schiphol Airport	Transport	Infrastructure and the Environment
Vessel traffic service	B	Port of Rotterdam		
Large-scale production/processing and/or storage of chemicals and petrochemicals	B	Chemical and petrochemical industry	Chemistry	Infrastructure and the Environment
Storage, production and processing of nuclear materials	A	Nuclear Industry	Nuclear	Infrastructure and the Environment
Retail transactions	B	Financial transactions	Financial	Finance
Consumer financial transactions	B			
High-value transactions between banks	B			
Securities trading	B			
Communication with and between emergency services through the 112 emergency number and C2000	B	Maintaining public order and safety	Public Order and Safety	Security and Justice
Police deployment	B			
E-government: the availability of reliable personal and corporate data about individuals and organisations, the ability to share such data, and the availability of data systems which multiple government agencies require in order to function	B	Digital government	Public Administration	The Interior and Kingdom Relations

2.5.2 Lessons from the US Experience

With Europe lagging behind US developments in CIP, the US experience provides essential guidance for European solutions. Given existing interdependencies, the vulnerability of electric power grids became a top priority. The lessons learned from US experience are useful and sobering for Europe as these characteristics suggest:

- Industry runs around 80% of US electricity supply.
- Governments are unable to act as a similar provider.
- Industry tends to prefer self-control.
- Governmental expertise is, however, superior in security, in particular risk assessments and situational awareness and supporting computing technology.
- Both government agencies and industry consider information sharing a priority, but their definitions of what constitutes priority differ.
- Information-sharing needs to be a two-way street, but industry is slow in view of its concerns over liability and proprietary-based reservations, whereas public

services, such as intelligence and military services, need information sharing typically in real time.

- Edison Electric Institute has launched an initiative to enable near-real-time-machine-to-machine information (CRISP = Cyber Risk Information Sharing Program), but private initiatives face hurdles on both sides: In 2015 CRISP was shared by the government and 15 companies, i.e. 15 out of around 3000 US companies. The expectation was to double that until 2016, but the need would be to deploy CRISP across the entire industry.
- Competing assessments notwithstanding, the likelihood of a US national power grid being knocked out is widely considered high, although it would take capabilities only sophisticated attackers would possess.
- Given these uncertainties of a successful cyber-attack against a power grid to happen, withholding investment funds to prevent a crisis that may not happen tends to become a key factor in slowing CRISP's development.
- Short of an escalating crisis, the tension between privacy and security will prevail, even if, in one observer's words, "in the face of mounting cyber threats, businesses are slowly, painfully setting aside some of their concerns and considering a closer collaboration with federal agencies."
- At this point the distinction between vulnerability analysis and threat analysis gets critical. While both US government and industry address the question of whose interests could be served by a successful cyber-attack against a power grid, intelligence does not rule out that enemy malware is already sitting in the national grid waiting for a moment where strategic leverage from disruption of the national power grids pays off.
- Local distribution of electricity has been considered a possible way to enhance security and resilience (following similar logic of decentralization that led to the internet), but local distributors and smart grid architectures are no longer subject to federal/central regulatory standards and they lack the resources of large corporations. They are thus more vulnerable, however also less attractive targets.
- Given the rapid digitalization of both governmental and industrial processes, there evolves a typical race between efficiency and security which gap for the foreseeable future is widening unless the IT security industry provides CIIP solutions that reduce vulnerabilities and increase the requirements for successful cyber-attacks.
- This in turn is bound to change the conditions for government-industry cooperation in CIIP: The need for governmental investments is increasing and innovative industrial capacities need to grow and thus will become ever more self-controlled and self-sustainable.

Given the dependence of all other sectors, the vulnerability of the US power grid extends to US national security at large.

2.5.3 PPP as enablers in CIIP

Cooperation between governmental bodies and industry has a history that dates back to the 19th century, depending on economic and social framework conditions in Europe and the US. It typically served specific purposes such as cost-saving, control or efficiency. In the 1980s it was originally introduced in the US to enhance governmental processes, along with growing awareness of the vulnerabilities of electronic networks, public-private partnership came to be seen as a method to enhance security.

The rise of the internet and the exploding dependency of all societal sectors on ICT triggered two developments: Governments sought above all outsourcing of services, privatization and cost sharing, whereas rapidly increasing interdependencies of governmental bodies and industry made vulnerability of networks a key security concern. The growing awareness of vulnerabilities of sectors on which national security and the viability of societies at large depend made security of critical information infrastructures a high priority challenge.

Ever since the Report of the Presidential Commission on Critical Infrastructure Protection (USA) in 1997, Public-Private Partnership (PPP) [11] has been considered a method to ensure the viability of critical infrastructures. It was followed by Presidential Directives and National Infrastructure Plans that established a framework for developing contractual partnerships between government and industry for the security and resilience of critical infrastructures.

PPP as a method to enhance ICT security was induced by the rapid development of critical information infrastructures in the US. It was followed in Europe, in particular by the UK, NL and to some extent in Germany. In 2003, the EU Commission issued Guidelines for successful PPP projects. But concerns over information-sharing also became a retarding factor, in particular in areas such as finance.

2.6 PPP Characteristics

This section presents and discusses relevant PPP characteristics such as escalatory factors, limitations, impacts, and insurance.

2.6.1 Escalatory Factors

Within the ecosystem of multiple interdependencies each CI is embedded in a net of other CIs it depends on. The criticality of interdependent CIs depends on i) the sectors at stake, ii) on the preparedness level of these CIs, iii) their vulnerabilities, iv) on the nature of the attack or disruptive impact, and v) the level and crisis management phase of those:

- Disruptive effects can cause instant large-scale damage such as electric outages with major effects on society, economy and possibly on governmental sovereignty. That would be a regional or national security matter, i.e. involve governmental agents from the outset: It would affect governmental functionalities and require CI mitigation and governmental responses.
- Levels of national security could also be reached by escalatory processes that originate from local incidents that failed to get contained. This can happen in case of distributed operational facilities like hubs, ports, central railway stations, persons and goods, of physical processes such as CBRN[156] effects or because of shortcomings in subsidiary sequences of responses.
- Escalatory potential of local incidents may or may not be met by CI-internal preparedness levels. Given the initial uncertainties and the possibility of multiple incidents, information-sharing and coordination with higher levels will always be required. But the more escalatory processes progress to higher levels, the greater the complexity of interdependencies. And the higher the level of impacts, the more governmental agents will get directly involved and need to be connected.

[156] CBRN is acronym for Chemical, Biological, Radiological, and Nuclear.

2.6.2 Inherent Limitations of PPP in CIIP

Industries lack the contextual knowledge on a crisis that is about to unfold, but they have a basic interest not to share sensitive information with potential or actual competitors within the same domain or in fact other domains on which they critically depend. This is even more so if the crisis is under control, but sensitive information has been released. Governmental operators, on the other side, are extremely reluctant to share critical information even within governments, among agencies with divergent functions, let alone with private operators who often own the bulk of the CIs and who are supposed to provide first-hand information.

Industrial stakeholders share the objective of securing competitive economic advantages which often also limits the readiness to cooperate. Governmental stakeholders are expected to prioritize national security, although in extreme situations this too can become a critical part of international competitiveness. Given different country-specific states of state-industry relationships and ownership arrangements in Europe, the distinction between private and public is ambiguous. In some CIs there exist evolving trends to consider business security a potential constituent part of business development, i.e. a new source of competitive advantage:

- Governmental agencies and industry may both recognize a risk or a threat, but apply different definitions and assessments of the repercussions and the notions of what to prioritize.
- Similarly, government agencies may be extremely reluctant to share crisis information, even though industrial crisis management is indispensable and beyond what governments can do.
- Releasing classified information will further constrain information-sharing or even serve as an excuse for withholding.
- Moreover, in the absence of an acute crisis, tensions between privacy and security are often more likely to be resolved through political tradeoffs in favor of the former thus hampering what is needed to enhance preparedness. By the same token, governmental action is likely to be led by assignments and procedures that are not unlikely to be bypassed in a severe crisis. In fact, the "crisis free circumstances" of governmental responsiveness will be restricted by legal and organizational constraints that may not dominate in a severe crisis. With centralized governmental structures these obstacles will be less critical than in federal structures.

In Europe, the diversity of national systems and the absence of a European framework for cooperation between industrial and governmental stakeholders poses an even more complex structural problem than the United States need to cope with. And in the US, there is a consensus since 1997 that, all constraints notwithstanding, "the only sure path to protect infrastructures in the years ahead is through a real partnership between the infrastructure owners and operators and the government." [11].

Above all, in Europe there exists no equivalent to what the United States has basically agreed upon as "national security". Within the European "ecosystem" of interdependent critical infrastructures prioritizing public-private partnerships thus is of overriding importance: Without it information-sharing and coordination through ECOSSIAN-type systems and capabilities may not provide the protection and resilience it is designed for. The other way around, a working ECOSSIAN-type system could serve to facilitate governmental-industrial cooperation and support efforts to eliminate the above constraints, although those constraints may turn out to prevail even with an effective ECOSSIAN-type system in place.

2.6.3 Dependence of Requirements for PPP on Levels of Impact

The criticality of infrastructures thus relates to three types of expected impacts and respective consequences:

1. Near-instant impacts and large-scale effects like electric outages,
2. Processes that render containment the more difficult, the more they are progressing, e.g. CBRN and cyber-based disasters or attacks,
3. Local incidents involving infrastructures that have been designed for physical distributions such as aviation hubs, ports, main railway stations.

The first type, the "near-instant impacts" addresses networks across large areas, the second type chains of effects, and the third one, local events within an operational environment that may or may not be prevented from effects spreading ("escalatory processes"):

- In case of local events with the potential for cascading effects, the internal security management is decisive. With the possible exception of intentional decentralization of distribution systems, common governmental standards are usually absent. In local events, units dominate that face trade-offs between security and efficiency (and respective costs).
- The risks of spreading effects relate to interdependencies, and risk management would require degrees of preparedness for inter-service cooperation.
- In case of complex units like airports (hubs) contractual partnerships often do exist within the wider operational environments.

The feasibility and requirements for PPP differ w.r.t. the level of impact: For the national level, near-instant impacts require cooperation on all levels including near-instant coordination on national levels, whereas escalatory processes require real-time information and coordination bottom up and in accordance with obligatory procedures for meeting subsidiarity, i.e. here on the national level, complexity of interdependencies is even larger, but there is likely to exist more response time.

Given that national disasters are likely to spread effects across borders or throughout Europe at large, Europe faces an even far more complex challenge than the US in view of lacking convergence of standards and central coordination capacity. E.g. in the US thousands of power distribution systems are by now interconnected within three US grids. Cooperation is alleviated by common technologies such as SCADA systems most of which are manufactured by a small number of companies and display relevant similarities in structure and programming.

The initial impact may not allow instant assessments of its escalatory potential, yet for the same reason it necessitates information-sharing at the earliest possible stage. Its criticality (see e.g. the Dutch A and B categories, Table 1), is thus measured in terms of expected damage, i.e. after the initial incident and possibly after the crisis at large.

The inherent constraints on both governmental and corporate readiness to instantly share information, if not common operational pictures (COP), thus are likely to be exacerbated in view of unavoidable scenarios-dependence in early damage assessments. PPP in CIP matters will always require a common framework, particularly on higher levels and respective needs for multi-level coordination. But this will hardly suffice to meet all operational needs, one crucial reason being, that on different levels the range and specifics of partners vary.

The European network of interdependencies between operators is further constrained by the fact that so far internal security remains a national responsibility, although transnational cooperation is a basic feature of the existing network of interdependencies and a multitude of transnational and even Europe-wide systems of dependencies and interactions does exist (as indicated by the scenarios chosen for ECOSSIAN). Further, within the EPCIP, based on the Directive 2008/114/EC a process is on-going which develops criteria for the definition of national vs. "European" CI (ECI[157]) for which we assume certain EU responsibilities in preparedness and response to develop. Cross-cutting criteria on casualties, economic and public effects have been developed as well as sectoral criteria[158] for transport and energy sectors. Further elements to be regarded in a future PPP include National Contact Points (NCP), national Operator Security Plans (OSP), the Critical Infrastructure Warning and Information Network (CIWIN), the European Reference Network for Critical Infrastructure Protection (ERN-CIP) and further numerous supporting projects.

To assess the potential impact of ECOSSIAN on interactions among different operators within the European ecosystem of cooperation, the state of internal preparedness for security management thus needs to be taken into account. The readiness of CI operators to share information and engage in cooperation is limited.

For information-sharing and coordination to function and to provide situational awareness and coordination of responses does require that the internal preparedness of operators for security management is sufficiently in place. It is, however, still inadequate in a large variety of operating units in all sectors and on all levels of operation. Moreover, security requirements differ widely among European states.

Disasters or attacks on CIs can impact on local structures or processes with subsequent chains of effects that may or may not be contained. They could hit structures such as hubs (like airports, ports or railway stations) or facilities (like power stations) with near-instant spread of large scale effects. And they could cause near instant disruptive effects like blackouts that can have consequences on transnational and even trans-Continental scales.

2.6.4 Need for and role of Insurance

There are all kinds of insurance models for all kinds of limited up to catastrophic risks. The basis for risk insurance is historical information and forecasting on that basis. The main criteria being expected are (a) frequency and likelihood of malicious incidents, combined with (b) the related amount of damages, and some extrapolation into the future of both, from past information and by experts' analysis of what may happen in the future.

The problem in CIP with the focus on cyber[159] vulnerability and threat, is that the history data base is weak because (e.g. compared to hurricanes), we have only one or two decades with fast changing threat and vulnerability environments, and a serious forecast of what may happen in the coming decades is almost impossible, least highly unreliable. Therefore, insurances and reinsurances are highly reluctant in calculating and offering CIP insurance tariffs at reasonable cost (whatever "reasonable" may mean).

Insurance experts have stressed this fact in dialogue with governments stating that covering high to catastrophic risks resulting from cyber-based threats to CIs can only reasonably or even completely be covered in a strong partnership –e.g. in the form of PPPs– where the government helps to limit the risk for insurances.

[157] ...means critical infrastructure located in Member States the destruction or disruption of which would have a significant impact on at least two Member States

[158] Confidential.

[159] which is the focus of ECOSSIAN.

2.7 ECOSSIAN-Type in CIP

2.7.1 The ECOSSIAN Prototype: Functions and Constraints

The ECOSSIAN project will develop and test a prototype of a European early warning system for critical infrastructures with focus on cyber-related threats. As a cross-border system it is designed to connect local/sub-state SOCs (O-SOCs), national SOCs (N-SOC) and transnational SOCs with inclusion of member state SOCs. It is intended to provide eventually a European SOC (E-SOC) for information-sharing and coordination on all levels and EU-level agencies in the CIIP area.

As a three-tier system it will be required to work in case of transnational or EU-wide impacts of failure and/or attacks that result in sustained supply shortages, significant disruption of safety and security and other potentially serious to catastrophic consequences.

An ECOSSIAN-type system will be effective in significant crises only if the technical solutions will work within an agreed and effective ecosystem of interdependencies and cooperation on national and transnational levels. To be effective in crisis management, it needs to be taken into account also in efforts to ensure high preparedness levels.

The basic architecture of an ECOSSIAN-type system will be the same for all SOC levels, but requirements and constraints and respective implementations and technologies will differ between the three tiers.

As outlined in D1.5 [78] ECOSSIAN "will provide tools and services to the CIs of Europe that allow for situational awareness and early warning in the ecosystem of international cooperation.". These infrastructures are "distributed among Europe and directly cooperate together, creating deep chains of dependencies" which arise from distributed supply chains and nets and from cross-sector and cross-border services and operational facilities. Within this ecosystem of multiple interdependencies each CI is embedded in a net of other CIs it depends on.

Above a certain escalation level, the ecosystem of interdependent CIs thus always does involve private-public relationships. Moreover, the higher the impact and response level, the more coordination between private and governmental operators will be involved and needed. However, this is far from being an organic relationship:

- Needed services may get outsourced by governmental agents.
- Assessments and respective criteria may differ between industry and government w.r.t. e.g. objectives, risk awareness, cost-sharing, conflicting priorities, etc.
- Public and/or private operators may entertain conflicting views on what is necessary.
- In cases involving several CI sectors, private responses may be difficult to coordinate because governments may lack the authority, and/or operators in different sectors concerned may have different lines of communications with governmental agents, and/or governmental structures may lack the capacity for effective coordination.
- Business also tends to be concerned about disclosure of vulnerabilities and of incidents, as prerequisites for an efficient of PPP.
- Underlying these concerns is the fear of surrendering privacy and proprietary information to the government and its security and intelligence agencies.
- There is a systemic conflict potential between the need and obligations of governments to regulate security matters and the resistance of industries against any type of regulations or even patronizing by the government.

Public-private (PP) or governmental-industrial relations in security matters thus are distributed among the "ecosystem of interdependencies", although with widely varying degrees of cooperativeness. Given that internal preparedness for enhancing CIs' security often is far from sufficient for both governmental and corporate operators, cooperation between these requires specific efforts and arrangements. Moreover, information sharing is conditioning all other activities between governmental and industrial operators and stakeholders, but have intrinsic reasons for limiting information sharing, in particular if near real-time information-sharing is required as in cases of cyber-attacks.

The larger the impact and the more demanding the requirements for response and resilience, the more such relationships will proliferate and the more complex they will need to be.

PP relations in the CIP area are pivotal for the whole ecosystem of cooperation. In case of failure or disruption all other sectors will face secondary effects. Depending on the role and function of public and private agents in case of significant impacts, the PP relationships will be critical. In particular, private agents can be indispensable because they own the facility at stake and/or have the most dependable first-hand knowledge of the origin of failures and/or disruptive events. But they often lack the organization and rules needed for firm PP relations. Public agents, on the other hand, tend to have broader contextual knowledge which is needed to assess the scope and dynamics of a disaster or crisis and its impact on society. The larger the impact the more complex interagency processes and transnational information-sharing and coordination will become.

PP relations that are considered necessary for CIP and respective incident handling and crisis management will need to be effective, institutionalized and contractual. However only 56% of the 17 MSs examined by ENISA have institutionalized forms of cooperation in forms of PP partnerships.

2.7.2 The European Scope of ECOSSIAN

As discussed in section 2.4:

- The scope of ECOSSIAN is European, i.e. it should serve to cope with incidents that require more than local responses. Most incidents that require national, transnational or European-wide responses will require one way or another cooperation between governmental and non-governmental (primarily industrial) actors. The design of an ECOSSIAN system will not be confined to minor/local incidents, but should also support national, multinational or European responses to incidents that would/could endanger states and societies at large.
- An ECOSSIAN PPP thus should be designed not only with regard to challenges as they exist at the presumed time of its introduction, but in view of plausible changes throughout its life-time and in view of future needs.
- Also, given the diminishing divides between "war" and "peace", the range of scenarios will need to be broadened to include roles for ECOSSIAN in complex crises and conflicts caused by non-state actors and, more importantly still, future state-actors (who arguably will possess more devastating means for cyber-attacks).

Cooperation at all threat and escalation levels and in particular, responses on "catastrophic" levels will require an agreed and effective framework for PPP including organization, procedures and sets of rules, contractual frameworks and standards.

PPP is understood to include structures, procedures and rules for information exchange and cooperation between public and private actors in preparing for and responding to major security incidents. For ECOSSIAN this needs to include cooperation and coordination between national organizations and enterprises.

The criticality of PPP requirements varies with areas of concern. It is particularly strong in areas like public transport, traffic, energy, communication and under extreme crisis conditions (international conflict, strategic terrorism). it substantially varies between different CI sectors. It also varies between MSs w.r.t. vulnerabilities (e.g. different degrees of industrial digitalization), preparedness levels, risk exposures, potentials for PP synergies and emerging new challenges.

Increasing interdependencies resulting from progressing industrial digitalization and the widening range of risks and attackers will combine to increase the need and requirements of ECOSSIAN. This will tend to narrow the differential between MSs, to change the role of state authorities and to enlarge the role of enterprises (including cooperation not only between public and private actors, but between different enterprises in same and different sector). And it will ask for a dedicated coordination role at EU level.

In this vein. the ECOSSIAN project is an important initial step, the more so if it succeeds to become relevant on EU level. But w.r.t. to critical cooperation requirements, PPP itself needs to be developed: at the present stage of developing these PPP principles, neither models for analyzing interdependencies and assessing their effects, nor sufficient data nor scenarios that allow to evaluate choices do exist.

2.7.3 ECOSSIAN in European CIP: Conditions for Applicability

ECOSSIAN is an attempt to provide a functionality for early warning, disaster response coordination and crisis management support, across CI-, national- and EU-levels. There are two ways to approach that: 1) to start from CI level upwards to identify, install and demonstrate functions on national and EU-levels or 2) to start from EU-level in view of supportive functions on lower levels.

The first –bottom up approach– tends to get confined to command and control functions and its approach may fail to reach effectively the EU-level, because it tends to be focused on narrow incidents that do seldom call for EU-level interaction.

The second –top-down– tends to envisage a wider range of responsibilities in terms of widening the functionalities of existing EU-level entities –which in reality still have limited roles in CIP.

In the end, a mixture of both may develop, driven by common interest and mutual understanding of divergences.

ECOSSIAN builds on more than 10 years of EU-supported work on CIP. Besides EPCIP, there have been a number of activities, e.g. at ENISA and Joint Research Centre (JRC), and research projects that were focused on E-level functionalities, although with limited applicability, e.g. the project CATO [58] on CBRN, CIRAS [60] on tools for risk assessment or PULSE [59] on healthcare.

PPPs do play a role in all areas of ECOSSIAN applications, the more so, the higher the level, but by the same token the more complex, the higher the level.

PPPs are not a panacea, but an essential prerequisite. A PPP will be required if a system such as the ES is ever implemented and the other way around, a "3-tier" PPP matters because in many CIP sectors PPPs exist –if at all– primarily on a national level. The issue for ES is above all how to endow, improve or supplement existing PPPs in the interaction of O-SOCs, N-SOCs and an E-SOC.

Arguably, an extension of PPP functionalities to E-level could both reduce the workloads on lower levels in view of improved information sharing, common standards, trust etc. and it would ease the establishment of PPP networks on lower levels for partly the same reason.

Obviously, subsidiarity applies, i.e. except for enabling and supporting functions on lower levels, entities on E-levels come into play in case of major incidents with transnational and

Europe-wide and potentially existential consequences. At this stage, illustrative cases are rare.

Analyzing the consequences of catastrophic events is beyond routine work, even more so demonstrations, training and exercising typical scenarios. But it is in those cases that subsidiarity comes into play, i.e. the interaction between E-level, N-level and O-level SOCs. A top-down approach would require sufficient knowledge of pre-existing distributions of SOC entities on lower levels, and in particular of governmental and corporate entities ready for PPP arrangements. Also, some assumptions on the (future) existence and empowerment of an appropriate EU-level organization need to be made.

Severe to catastrophic threats and incidents thus are or should be a driving consideration for a future PPP concept. Naturally cascading and cross-sector consequences are most difficult and complex to handle, the more so if E-level capacities are still unclear to some extent. They will need to assume widening time-horizons with potentially growing numbers and types of agents, of endangered sectors, of plausible escalatory chains, with differing risk exposure of MSs and regions. The need for such a three-level-type PPP has been derived here from the perspective of major disastrous CI incidents with impact on national security and with the need for coordination at EU level. Nevertheless, it must be clear that a future PPP also needs to regulate all information exchange and cooperation and coordination functions for less intensive threats and for every day monitoring and situation assessment.

2.8 Experience of the European Electronic Crime Task Force

In this section, the European Electronic Crime Task Force (EECTF) case study is presented, as an illustration of the challenges facing a complex information-sharing initiative, that requires the engagement of diverse public and private stakeholders.

Many aspects of this collaborative enterprise are described, with relevance for the future implementation and development of the ES, such as:

- Public and private stakeholders;
- Engagement of US agencies;
- Engagement of law Enforcement, financial sector, academia, international institutions, as well as ICT security vendors;
- Engagement with many high-profile institutional stakeholders that share the enterprise’s purposes.
- The EECTF itself is an effective cooperation mechanisms for strengthening the Public Private Partnership, that is considered essential for an overall advancement of the sector.
- The importance of establishing common language artefacts (e.g. taxonomies), to facilitate the communications among different countries, sectors and legal jurisdictions.

The section concludes with additional remarks concerning lessons learned.

2.8.1 European Electronic Crime Task Force in brief[160]

The European Electronic Crime Task Force (EECTF) is an information-sharing initiative, started in 2009 by an agreement between the United States Secret Service, the Italian

[160] Some contents in this section are similar to the contents of the Wikipedia page for EECTF (as of May 10th 2017), which is co-edited by Poste Italiane.

Ministry of Internal Affairs and Poste Italiane, and whose mission is to support the analysis and the development of best practices against cybercrime in European countries, through the creation of a strategic alliance between public and private sectors, including Law Enforcement, financial sector, academia, international institutions and ICT security vendors.

Accordingly, the EECTF aims to help the cyber security community by:

- Strengthening relationships between the different players;
- Training and supporting members through sharing expertise and knowledge;
- Enabling an effective communication channel for information exchange;
- Maintaining co-operation on a technical and operational level.

2.8.2 History[161]

The EECTF was established on the June 30th, 2009 by an agreement between the United States Secret Service, the Italian Ministry of Internal Affairs and Poste Italiane, on the basis of the successful experiences of analogous ECTFs founded in the USA by the Secret Service.

The United States Secret Service participates through the Rome Office, the Italian Ministry of Interior participates through the Service of Postal and Telecommunications Police and Poste Italiane participates through the Information Security Department.

Initially restricted to the Founder Members only, the EECTF was opened thereafter to the main stakeholders in cybercrime sector, who expressed the will to contribute to a proactive sharing of relevant information. A Permanent Members Group was started, which gathers to analyze emerging trends in cyber-crime and discuss methodologies and techniques to combat them.

2.8.3 Governance[162]

The EECTF is not a legal entity, it is a working group, created on a voluntary basis, which since its creation has been governed by the EECTF Board, composed of the three Founding Members: the United States Secret Service, represented by the Special Agent in Charge of the Rome Office, the Postal and Telecommunications Police, represented by the Head of Service and Poste Italiane, represented by the CEO.

Poste Italiane has been chairing the EECTF Board since its birth. Administrative and operational activities are in charge of the EECTF Technical Secretariat, held by Poste Italiane.

The EECTF Constituency is composed of:

- **3 Founding Members** – Poste Italiane, the United States Secret Service and the Postal and Telecommunications Police;
- **19 Permanent Members** – ABI Lab, American Express, Bulgarian Police, CA, Citibank, Consip, Global Cyber Security Center, Italian Ministry of Economy and Finance, Kaspersky, Mastercard, NTTData, Romanian Police, RSA, Selex ES, Symantec, VISA Europe, Unicredit, UNICRI, and Verizon.
- **1 Community of around 500 professionals**, evenly distributed between public sector, financial institutions, LEAs, international organizations, research & academia and ICT vendors.

[161] Idem.

[162] Idem.

The possibility to acquire information from a cross-sectorial base of expertise made the EECTF an acknowledged reference to have a comprehensive picture of the current scenario also at the institutional level. To mention one, significant example, it has also been officially called to participate to a public hearing on the state of network and information security held at the Chamber of Deputies of the Italian Parliament in 2011.

2.8.4 Modus Operandi[163]

The EECTF is managed by means of monthly meetings involving a selected group of Permanent Members, quarterly open events extended to a wide Community of selected experts and continuous sharing of relevant information to the cybercrime scenario, and also through dedicated specific tools.

To obtain the active status of Permanent Member, the applying organization must agree on the EECTF modus operandi, which has been conceived on the basis of three pillars:

- pro-activity in bringing knowledge, expertise and proposals to the Group;
- non-disclosure of sensitive information, in accordance to a Traffic Light Protocol, undersigned by each Permanent Member;
- non-competition among counterparts commercially active in the same business domain.

Permanent Members are internationally acknowledged organizations, both private and public, with a broad view on prevention, analysis and contrast of electronic crimes at European level, whose competencies might represent instances coming from whole domains of interest.

Permanent Members formally commit to proactively share information with other Members of the Group in a non-competitive environment, according to a non-disclosure agreement, as well as to actively contribute to the EECTF life, taking part to meetings and supporting the EECTF development.

Additionally, to make the most out of the competencies of the whole EECTF community, an Expert Group has been established, which gathers on a periodic basis and is restricted to Permanent Members only, focusing on technical information sharing about new threats and possible countermeasures.

In this framework, a qualified assembly was created, bringing together highly representative of professionals active in the cyber security field, with the aim to strengthen cross-sectorial collaboration between public entities and private organizations. The objective is to create a homogeneous and unique group of response, analysis and prevention against the most significant and emerging forms of electronic crime.

Relying upon the voluntary contributions regularly provided by participants, the Task Force also launched a project oriented to the establishment of a European center of excellence (high-powered even by private sector entities) for the enhancement of the exchange of technical and operational information, for the assessment of risks and the evolution of threats related to the continuing evolution of the *electronic crime* phenomena.

2.8.5 Activity Lines

Currently, the EECTF activities are organized along three priority lines, summarized as follows:

[163] Idem.

- **ANALYSIS:** with reference to the development of insights focused on new threats, identified by partners in their respective areas of competence and operation. These insights are developed either with a joint approach on specific common initiatives or with a view to share studies carried out internally. This context also sets the background for the participation of Poste Italiane as an EECTF representative to several projects funded from the European Union in the field of Information Security and inter-sectorial collaboration.
- **NETWORK:** concerning the construction of a network of collaborations and information exchange more and more thick and effective, either with institutional partners at a national level or in the context of wider initiatives. An example of this activity is the participation to an ENISA group called FI-ISAC, Financial Institutions Information Sharing and Analysis Center, that brings together representatives from financial institutions, national CERTs, European CERTs and Law Enforcement Agencies with the aim to facilitate the information exchange about the security of banking services and fraud prevention.
- **COMMUNICATION:** regarding the realization of communication initiatives, either dedicated to a limited audience, as in the case of technical meetings denominated Expert Group, or addressed to a wider audience, as in the case of the three annual Plenary Meetings, or the CyberNews newsletter.

2.8.6 EECFT Permanent Members

Under the coordination of the Founding Members - chaired by Poste Italiane, which plays the role of Chairman of the Task Force - the following stakeholders are members of the Permanent Group:

- **Law Enforcement sector**: Bulgarian Police, Romanian Police, in addition to the founding members Postal and Telecommunications Police and United States Secret Service;
- **Research and Institutional Bodies sector:** GCSEC Foundation, Italian Ministry of Economy and Finances (UCAMP), UNICRI (United Nations Interregional Crime and Justice Research Institute);
- **Finance sector:** American Express, Citibank, Mastercard, Unicredit, VISA Europe;
- **Security sector:** SelexElsag, representing the Finmeccanica Group;
- **ICT sector:** CA Technologies, Kaspersky, RSA, Symantec, Verizon.

2.8.7 Institutional cooperation

By virtue of a very consistent representation of stakeholders involved in countering cybercrime at national level, the EECTF has established relevant and consolidated institutional relationships with public counterparts of utmost importance:

- **The Ministry of Interior**, not only through the continual operational cooperation with the Postal and Telecommunications Police, but also through the participation in the community of representatives of Law Enforcement;
- **The Ministry of Economy and Finance**, establishing a collaboration with both UCAMP (Anti-crime Center for payment systems) and Consip, whose Security Operation Center is considered as a national best practice;
- **The Ministry of Economic Development**, through the ISCOM (Higher Institute for Communications and Information Technology), which contributes through a supporting role to the definition of the Italian Digital Agenda;
- **The Authority for the Protection of Personal Data;**

- **Bank of Italy**;
- **Italian Banking Association**, by means of ABI Lab, Permanent Member of the EECTF.

2.8.8 International cooperation

International cooperation is another important action line of the Task Force, which significantly contributes to the creation of added value to benefit of the members.

Several permanent contacts were established with many high-profile institutional stakeholders that share the purposes of EECTF:

- **ENISA**, through specific working groups like FI-ISAC (Financial Institutions Information Sharing and Analysis Center, where Poste Italiane formally participates) and EP3R (European Public-Private-Partnership for Resilience);
- **Europol**, with reference to the establishment of the European Cyber Crime Center (EC3) and the possibility to activate an operational collaboration channel about e-crime issues;
- the **European Payments Council**;
- **CERT-EU**;
- **EuroJust**;
- the **AntiPhishing Working Group**;
- the **Digital Crimes Consortium**;
- additional, restricted-access groups composed of highly qualified and vendor-independent stakeholders, which allowed to build working relationships with security centers of important private organizations over the years. Examples in this context are the active contact with the main European and National CERTs, as well as with the US-CERT and the Australian CERT.

2.8.9 Traffic Light Protocol – How Information Sharing works

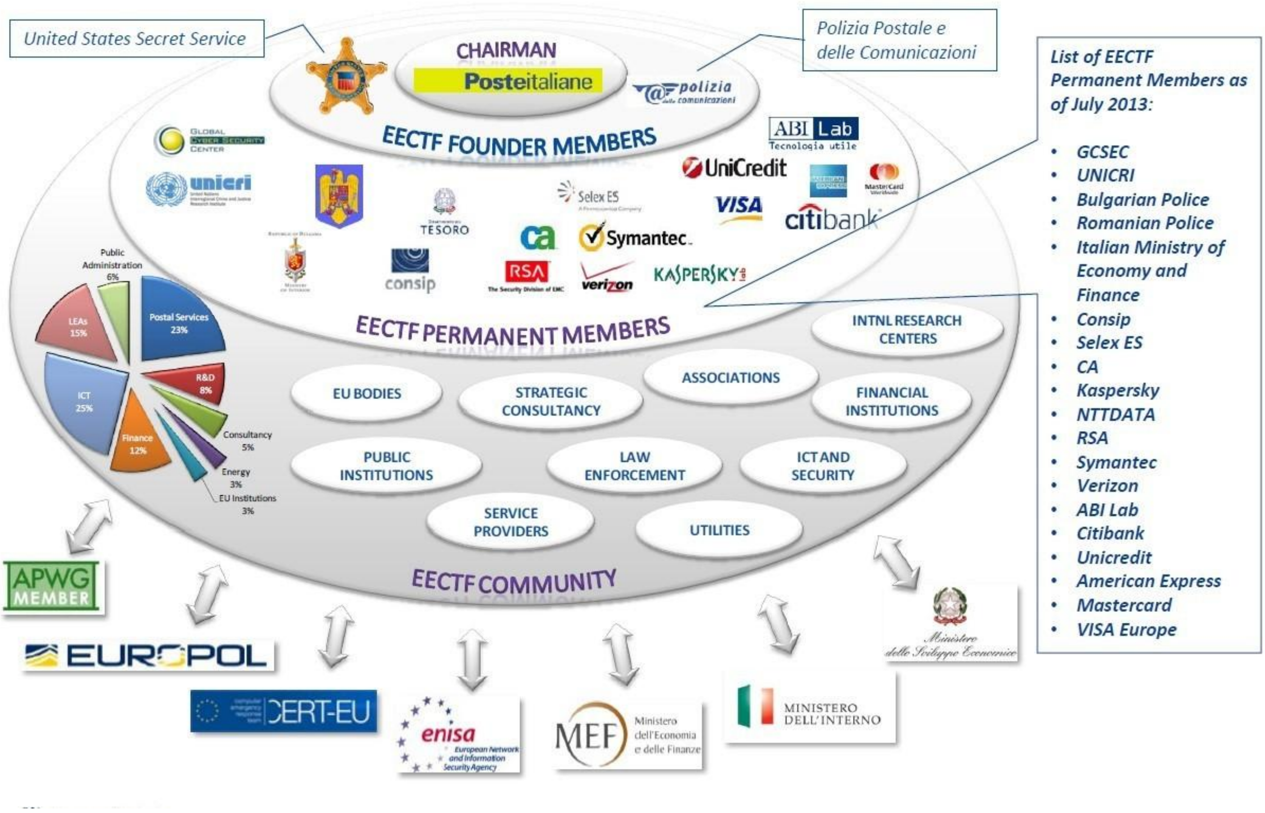
Each member of the Permanent Task Force is invited to give its consent on an information exchange protocol that identifies four levels of confidentiality:

- **RED Code:** cannot be disclosed neither orally nor in writing. During each Expert Group meeting, a red code information exchange session takes place, during which each participant can share comments and formulate requests for particularly significant phenomena or threats that insist on its domain of expertise.
- **AMBER Code:** information to be disclosed only for operational purposes within the permanent member organizations with the opportunity to discuss the findings in the context of the Expert Group.
- **GREEN Code:** information to be disclosed only within the entire Community of EECTF, also by means of the monthly newsletter.
- **WHITE Code:** no level of confidentiality, information can be disclosed even outside the Community and/or publicly.

2.8.10 EECTF Community Composition

The current composition of EECTF Community is well represented by the registrations performed during the last plenary meeting: 10 different countries were represented, about 150 professionals coming from financial institutions, Law Enforcement Agencies, ICT providers, University and Research, Public Administration, European Institutions and other supranational entities.

It is important to highlight the homogeneous distribution among representatives of public entities (about 60 %) and private organizations (about 40 %). The EECTF also wants to be a context of privileged cooperation for strengthening the Public Private Partnership, that is considered essential for an overall advancement of the sector.



List of EECTF Permanent Members as of July 2013:

- *GCSEC*
- *UNICRI*
- *Bulgarian Police*
- *Romanian Police*
- *Italian Ministry of Economy and Finance*
- *Consip*
- *Selex ES*
- *CA*
- *Kaspersky*
- *NTTDATA*
- *RSA*
- *Symantec*
- *Verizon*
- *ABI Lab*
- *Citibank*
- *Unicredit*
- *American Express*
- *Mastercard*
- *VISA Europe*

Figure 2: EECTF Community composition

2.8.11 EECTF Plenary meetings

All the members of the Community are invited to join the Plenary Meetings and quarterly meetings aimed to gather insights on specific themes of interest. During the last Plenary meetings, the following topics were discussed:

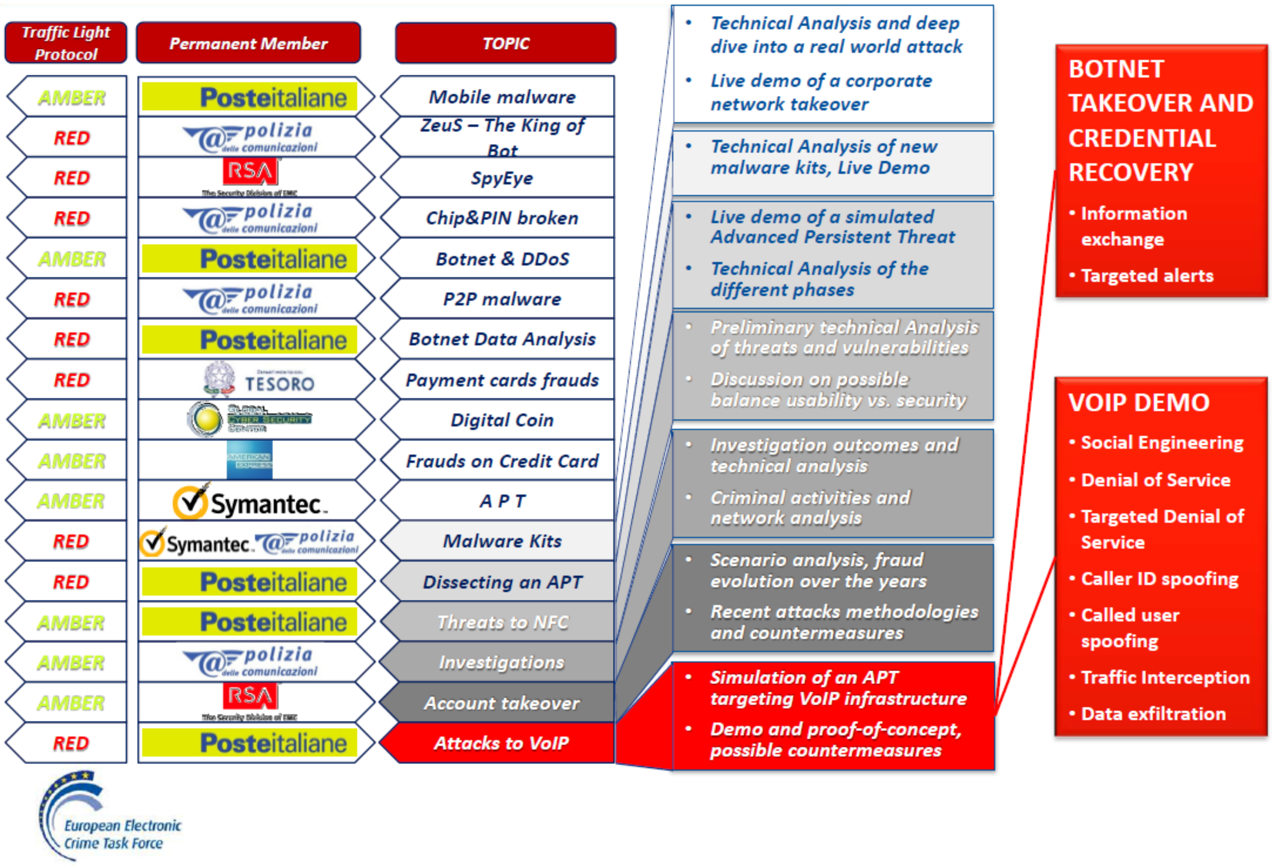
- **The Advanced Persistent Threats,** with reference to attacks specifically forged for individual companies or organizations, which aim to take over the keys of access to systems, applications and resources, collecting critical information in a silent and protracted mode and realizing sophisticated cyber espionage techniques;
- **Secure Management of e-Identity in Cyber Space**, with reference to the initiatives launched in both the public and private sector to ensure the safety and security of personal information for digital users, and the main trend relating to cybercrime in Europe;
- **Security of Innovative Payment Systems**, with reference to the identification of the main trends taking place in the EU context, considering the current acceleration of the overall framework of enabling technologies, delivery channels, regulatory reference and information sharing about protection strategies and monitoring of ongoing threats.

2.8.12 Expert Group meetings

As already mentioned in Section 4, the exchange of information among the Permanent Members takes place through regular meetings, dedicated to issues of significant relevance based on proposals made by the partners.

Below it follows a sample list of Expert Group meetings organized during the last years:

- **Advanced Persistent Threats:** Analysis Techniques and detailed report on a real attack;
- **Web Exploit Kit:** Live Demo of a botnet control;
- **Advanced Persistent Threats:** APT Live Demo and detailed report on the attack phases;
- **Vulnerability of NFC systems**: preliminary technical analysis of threats and vulnerabilities;
- **Investigation Report** on successfully closed cases;
- **Attacks on VoIP protocol:** Technical Analysis and Live Demo.



Traffic Light Protocol	Permanent Member	TOPIC
AMBER	Posteitaliane	Mobile malware
RED	polizia delle comunicazioni	ZeuS – The King of Bot
RED	RSA The Security Division of EMC	SpyEye
RED	polizia delle comunicazioni	Chip&PIN broken
AMBER	Posteitaliane	Botnet & DDoS
RED	polizia delle comunicazioni	P2P malware
RED	Posteitaliane	Botnet Data Analysis
RED	TESORO	Payment cards frauds
AMBER	Global Cyber Security Center	Digital Coin
AMBER	American Express	Frauds on Credit Card
AMBER	Symantec	A P T
RED	Symantec polizia delle comunicazioni	Malware Kits
RED	Posteitaliane	Dissecting an APT
AMBER	Posteitaliane	Threats to NFC
AMBER	polizia delle comunicazioni	Investigations
AMBER	RSA The Security Division of EMC	Account takeover
RED	Posteitaliane	Attacks to VoIP

- Technical Analysis and deep dive into a real world attack
- Live demo of a corporate network takeover

- Technical Analysis of new malware kits, Live Demo

- Live demo of a simulated Advanced Persistent Threat
- Technical Analysis of the different phases

- Preliminary technical Analysis of threats and vulnerabilities
- Discussion on possible balance usability vs. security

- Investigation outcomes and technical analysis
- Criminal activities and network analysis

- Scenario analysis, fraud evolution over the years
- Recent attacks methodologies and countermeasures

- Simulation of an APT targeting VoIP infrastructure
- Demo and proof-of-concept, possible countermeasures

BOTNET TAKEOVER AND CREDENTIAL RECOVERY

- Information exchange
- Targeted alerts

VOIP DEMO

- Social Engineering
- Denial of Service
- Targeted Denial of Service
- Caller ID spoofing
- Called user spoofing
- Traffic Interception
- Data exfiltration

European Electronic Crime Task Force

Figure 3: Expert Group meetings

2.8.13 Example of operational activities carried out in the EECTF context: the Eurograbber case

A relevant example can be mentioned to underline the value of the EECTF activities for the overall advancement of preventions and reaction systems against e-crime.

In December 2012, the mainstream press reported about a new attack, called Eurograbber, which caused the theft of approximately 30,000 credentials through a joint infection of both PCs and mobile phones belonging to users of home banking services offered by several Italian banks. The report referred as the main information source identified the total value of successful frauds for a total amount of about 36 million of euro.

The reported attacks were linked to Windows malware belonging to the Zeus family, able to inject malicious code on the compromised PC and ask the user to enter his/her phone number and the model of his/her mobile phone. The victim then received a text message on his/her mobile phone with a link that invites him/her to log on in order to download a security update. The link actually started the download of a malicious code (for Android, Symbian and Blackberry) that enabled the complete control of the device, including the retrieval of the authentication credentials related to the home banking service.

By performing a more accurate analysis of the confidential sources gathered from the EECTF channels, it was possible to estimate with reasonable accuracy that the amount reported actually corresponded to the aggregate availability on all accounts accessible through the use of the stolen credentials. In addition, it was confirmed by the CERT of the leading financial institutions at European level, that the estimate was made taking into account all the infected clients, even those with a partial infection where the mobile device was not compromised at all.

In brief, the in-depth analysis performed by the EECTF resulted in the determination that **the actual economic damage was much lower than the amount specified in the report by the vendor**.

In the context of the EECTF Expert Group it was also possible to get information regarding the configuration files related to the malware, identifying the target of attacks and **triggering an information notice to the Police and the banks involved**.

2.8.14 International Projects

In terms of international cooperation, the EECTF is currently involved in three research projects:

- Definition of a **Global Taxonomy about Electronic Crime** – initiative coordinated by the AntiPhishing Working Group. A first step concerned the shared definition of an eCrime-o-pedia, which contains a categorization and a definition of everything that refers to the universe of Electronic Crime. The overall purpose of the activity is to produce a document containing a coherent and universally accepted classification of all forms of Electronic Crime. This deliverable facilitates the communications among different countries, sectors and legal jurisdictions.
- Another significant project under the operational profile relates to the activation of an **Advanced Cyber Defence Center** funded in the context of the European Commission research projects. The aim is to create a network for prevention, protection and punishment of the Phenomenon botnets. The consortium is very large and well structured, with several EU member states representatives, and Poste Italiane is part of the Advisory Board in quality of chairman of the EECTF.
- The "Cyber Crime Policies" project, result of a partnership with UNICRI and GCSEC Foundation, aims to define a reference framework of information sharing initiatives on cybercrime and international cooperation among the National CERTs and CERTs

owned by private organizations, with the objective to identify the most fruitful ways to collaborate and the critical issues to address.

2.8.15 Priorities in Cyber Security

The privileged context offered by EECTF in terms of aggregation and information allows to keep the major trends constantly under review and, therefore, to highlight the priority actions to be addressed to ensure a better response as European system as well. Three developments are deemed to have the greatest impact in the near future:

- The development of a coherent regulatory framework can provide effective tools for prevention and repression in line with the modification of the threat scenario and to facilitate the cross-national collaboration among the initiatives of individual actors. This will achieve a more rapid management of emergencies that nowadays very rarely have a dimension limited to national borders;
- International cooperation among qualified organizations able to represent instances of multiple sectors related to a single geographical area of responsibility (i.e. the activation of national CERTs, which is considered one of the top priorities in the cyber security strategy by the European Commission) or more organizations belonging to a single area of interest (e.g. industry associations, specialized European agencies, etc.)
- The approach to security as a strategic driver for the evolution of business and the implementation of the so-called security-by-design, with reference to the integration of the security requirements already in the planning phase of business processes and to the technological tools to support their execution.

2.8.16 EECTF: an information sharing channel in support of the CERT of Poste Italiane

The indications coming from the European Institutions –the Commission in the first instance– claim for the creation of one single operational infrastructure for international collaboration, able to develop a strong level of cooperation and mutual interaction.

The information sharing activities in the context of the EECTF match these intentions and integrate into the synergies that Poste Italiane is activating in this period. The CERT in Poste Italiane is a point of synthesis and central coordination for prevention and incident response, through integrated management of information flows coming from different security areas within Poste Italiane, ensuring externally a single user interface for security information sharing activities.

The CERT of Poste Italiane is featured by a federated approach to operational management of security at service level.

By virtue of the highly widespread and deeply rooted presence of Poste Italiane throughout the national territory, another distinctive characteristic of the CERT is the ability to act as a unified connection point with respect to potentially emerging critical issues in specific regions of the country.

Thanks to the channels activated in the context of the EECTF, the CERT of Poste Italiane integrates with already existent and equivalent operational security structures both at national and international level, with particular reference to National CERTs owned by other countries, the Italian Public Administration and the European institutions, becoming part of the major global security network.

In the overall roadmap of evolution of digital services provided by the Public Administration, therefore, the CERT of Poste Italiane is acting as a reference player also to provide operational support to the national strategy for cyber security of the Italian Government.

To follow-up to the indications given by the European Commission in the European Digital Agenda, the National CERT was activated, which acts as a collector of operational initiatives implemented by single subjects in the Italian context, either public institutions or private companies.

Therefore, the national response center to security emergencies (National CERT) strongly benefits from the interaction with the CERT of Poste Italiane, in terms of both immediate availability of a qualified network and comprehensive support to the management of information security incidents, as well as in terms of ability to exploit privileged channel of information sharing.

The CERT of Poste Italiane raises targets that can be easily included in those of the national CERT, with reference to:

- creating a single point of interface with the outside world for operational security aspects which will increase the capacity to react, escalate and manage critical issues, leading to the development of processes encoded for federated security management at application level, also scalable to external stakeholders;
- participating to the most relevant national and international security communities (e.g. FIRST certification), for an increase in the level of protection of the system of each Country through an overall increase in the security culture;
- ensuring greater protection of digital services and encourage the qualification of innovative delivery channels, with the ultimate goal to increase citizen’s security and protection;
- ensure maximum visibility of the developed content, through periodic reports, statistics, surveys and timely analysis that the CERT makes available to the outside world, also through dedicated events.

2.8.17 Conclusion and lessons learned

The overall picture of the security of networks at national level is rapidly evolving, in terms of both attacks and law enforcement processes and related enabling technologies.

The EECTF is an information sharing environment that has been developed over time in response to the growing, cross-sector and cross-national demand to counter all forms of electronic crime. This privileged point allows to identify several fundamental priorities for the development of a synergistic action to be pursued with all the stakeholders involved in enforcement, prevention and repression activities against electronic crime:

- Identification of a process of construction of a national Identity Provider.
- Development of a continuous awareness campaign targeted to end-users, via activation of specific communication initiatives.
- Harmonization of the regulatory framework in data and information security, both in comparison with other European countries and comparing to areas not yet covered.
- Strengthening of information sharing activities in the field of security by means of an overall coordination among the actions taken by both the public and private sectors.

The strong commitment guaranteed by its Permanent Members to the promotion and strengthening of information sharing actions enables the EECTF to act as an operational support for the implementation of the National Strategic Plan on cyber security.

2.9 Stakeholders' survey: principles, mission, capabilities, and obstacles

The ECOSSIAN Project DoW [73] mandates developing an understanding of stakeholders' ES-related mission, expectations, as well the needs to preserve their business and their customers.

To help accomplish this task, nine ES stakeholders were invited to participate in a questionnaire to elicit their motivations and concerns, assess what measures need to be implemented for the ES to be a success, and identify potential obstacles on the way.

2.9.1 Capability indicators w.r.t. ISO 22325:2015

The most important capability indicators with respect to ISO 22325:2015 are summarized below.

The numbers in column “Importance for Partners” mean how many partners out of the nine that were interviewed, envisioned this indicator as important.

Table 3: Ranking of Capability Indicators.

Importance for partners	Capability indicator
8	Incident response
7	Coordination and Cooperation
5	Information and Communication
4	Emergency response planning
2	Risk assessment
1	Exercise
0	Leadership and Competence
0	Resource management

The most important capability indicator for the partners who have filled in the questionnaire is the **incident response**, as a common and consistent incident management process is one of the chief goals of ECOSSIAN. ECOSSIAN should enable coordinated incident response throughout Europe. It is important to mitigate any threats as fast as possible. Incident response will, for example, allow PJ to improve their law enforcement agency (LEA) skills.

Also, CCG considers incident response as an important role as the information provided by ECOSSIAN enables and improves the incident response on all levels. As EADSUK's tool is an incident response capability it must comply with the correct ISO.

Coordination and cooperation is also perceived as an important capability indicator by most of the stakeholders. ECOSSIAN is built specifically to provide a secure forum for Critical Infrastructures to cooperate and coordinate a common systematic approach. Furthermore, it will allow a better and faster reply and it is crucial for securing CIs in future. In a connected world, the coordination and cooperation of the activities on the national level is key to effective and successful incident response.

Information and communication is the third most important capability indicator since information exchange is a vital factor for the success of ECOSSIAN. It is important to let stakeholders know issues in timely fashion. For CCG, for instance, information and communication is important, because every management process relies on the validated and appropriate information and communication.

Emergency response planning is perceived as rather important by several partners, because it is envisaged that the platform will be included for use during an emergency response. It is crucial to have pre-determined action plans at hand. ECOSSIAN should be providing useful inputs to the response teams in case of an emergency.

Also, a credible **risk assessment** process is vital for ECOSSIAN as well as **exercises** to hold drills and tests for readiness.

2.9.2 Partnering objectives or mission w.r.t. ISO 22397:2014

The major partnering objectives and missions according to ISO 22397:2014 are summarized below. The numbers mark, how many partners out of the 9 that were asked, envisioned this objective as important.

Table 4: Ranking of Partnering Objectives.

Importance for partners	Partnering objectives
7	Continuity of operations
6	Protection of assets
3	Saving lives and protecting properties
3	Protection of image and reputation
1	Protection of the environment

It is obvious that for the partners who have filled in the questionnaire, **continuity of operations** and the protection of assets are the major partnering objectives and missions.

The reason why the protection of assets is crucial is the fact that the platform will be used post incident to attempt to protect assets from future incidents. The ECOSSIAN mission is to protect national and European critical assets; and to fight against crime.

The continuity of operations is also one of the major partnering objectives for most of the stakeholders, because the additional information provided by the ECOSSIAN platform enhances their ability to prevent incidents interrupting operations. Quick analysis post incident will also allow the business to maintain their image and reputation. ECOSSIAN should help ensuring **continuous access to vital infrastructures** to the European citizens. For GAIS for instance, it is important to keep energy supply available for customers.

Also, the protection of **image and reputation** is crucial as it is the foundation of every successful business. Furthermore, incident response capability with quick analysis will allow the business to maintain their image and reputation.

Saving lives and protecting properties is considered as another major partnering objective by EADSUK and PJ, because the platform will be used to identify evidential sources, which could potentially save lives. Also, GAIS considers saving lives and protecting properties crucial as safety of customers and the public is most important.

2.9.3 Partnering principles or main concerns w.r.t. ISO 22397:2014

Main partnering principles and concerns according to ISO 22397:2014 are summarized below. The numbers mark, how many partners out of the 9 that were asked, envisioned this principle as important.

Table 5: Ranking of Partnering Principles.

Importance for partners	Partnering principles
4	Accountability
3	Compliance
2	Transparency
2	Competence
1	Fairness

The main partnering principles are **accountability**, **compliance**, **competence** and **transparency**.

Transparency is fundamental to ensure fairness and is seen as an important partnering principle, because the focus on **transparency will allow the effectiveness and efficiency**

in information sharing. Transparency between participating partners is considered important and key to make the system really work and **benefit all partners equally**.

Also, **competence** is important, as the **objective of partnering is to complement own's capabilities**.

Moreover, **compliance with the NIS Directive** for critical infrastructure is a core principle.

2.9.4 Obstacles to partnering according to ISO 22397:2014

Main partnering obstacles according to ISO 22397:2014 are summarized below. The numbers mark, how many partners out of the 9 that were asked, envisioned this obstacle as relevant.

Table 6: Ranking of Obstacles to Partnering.

Importance for partners	Obstacles to partnering
5	Confidentiality obstacles
4	Non-commitment obstacles
3	Non-responsiveness obstacles
2	Self-interest obstacles
2	Self-review obstacles
2	Management obstacles
2	Technical/technological obstacles
1	Contractual obstacles
1	Organizational obstacles
1	Familiarity obstacles
1	Intimidation obstacles
1	Communication obstacles
1	Interoperability obstacles
0	Exclusion obstacles
0	Logistical obstacles

The major obstacle for most of the partners is **confidentiality**. Confidentiality issues could compromise the very essence of ECOSSIAN that implies information sharing. The main concern is directed towards access to personal and business related data. ECOSSIAN has primarily aimed at tackling this issue by providing appropriate security mechanisms (e.g. ABE). It must also be ensured that no customer identifiable data is disclosed.

Non-commitment obstacles are the second most often indicated obstacles. It may be a problem to make all joining partners share information in an equal way. If one or more partners are under-committed and share too little information this could undermine the overall effectiveness of ECOSSIAN. Moreover, it is important that the application to the private sector allows the team to foresee some difficulty in promoting a common vision.

Another primary concern is **non-responsiveness**. Finding out if an incident has really happened, and especially finding the cause for it is very time-consuming and needs very deep skills, which makes responding in time difficult. Resources available within a SOC are typically proportional to the sole activity of critical incident handling. This could possibly mean that the operators might not be capable of adding relevant information to be shared within an appropriate time span.

Self-interest might be a particular case of the general non-commitment obstacle, which is considered by several partners. In a cooperation system like ECOSSIAN it is important that partners share information. However, it is very difficult to build this kind of **trusted relationships between CIs**.

Another relevant obstacle is **self-review**. Some partners might want to hide their own mistakes related to some incidents they can deal with internally. This way, interesting and important lessons learned will not be shared.

Furthermore, **familiarity** and trust are pivotal obstacles, which ECOSSIAN has aimed to tackle by providing appropriate security mechanisms.

Technical obstacles should not be forgotten, as they may constitute a major risk, especially in the ICS environment. It is also important to ensure that vendor warranty is not voided by ECOSSIAN sensors on production network.

Contractual obstacles might also be relevant, because multi-party contracts to build an end-to-end incident management eco-system could be an obstacle to the partnering.

I**nteroperability obstacles** may also be an issue, as it is difficult to account for all types of data that will be processed by the platform during an incident.

To conclude the questionnaire, partners were asked to define the enabling/required factors to establish a successful ECOSSIAN partnership.

Here, **confidentiality** is being considered as very important. It is challenging to keep one's own data confidential while receiving information out of the partnership that adds value to the own operations.

Another crucial factor is **trust between joining partners**. They need to meet each other in person and discuss things together. Of course, it also needs strong agreements, but to make the system really work requires also the **personal relationship built on trust**.

Another fundamental requirement in order to establish a successful ECOSSIAN partnership is **strong project leadership and direction**.

Besides that, **transparency and information sharing** are essential to make the ECOSSIAN System a success. It is also important to develop and implement mechanisms that combat the obstacles that have been identified by the partners.

Another key enabling factor is to have a **full and variegated representation of the most critical actors**, which might be positively affected by the project results at all relevant levels: organizational, national and European. This would increase the effectiveness of the ECOSSIAN solutions and with respect to cooperation and partners' responsiveness.

Another driving factor is to reach **high levels of interoperability** between the many bricks of the ECOSSIAN system. Moreover, it is important to attempt to understand the **types of data** that may be required to be dealt with during an incident and the **legal aspects around forensic acquisition/analysis in different countries**.

Chapter 3 ECOSSIAN System Enablers

Following the analysis performed in Chapter 2, in this chapter we'll propose the ECOSSIAN System Enablers, i.e. the set of business framework conditions (BFC) that facilitate the successful implementation, development, and operation of a future ECOSSIAN-like system.

The guiding principles for proposing the ES enablers are the following:

1) To facilitate interoperability and adoption, the proposed ECOSSIAN systemic enablers are based on authoritative European Union guidance, international standards, and industry best practice.
2) To facilitate inter-sectorial cooperation, the proposals are sector-neutral. However, given that the ES is an information and communication system, industry best practice from the information and communications technology (ICT) sector is extensively used.

The proposed BFC encompass two generic requirement areas:

a) **Effective and agreed organizational concepts**: a three-tier E-SOC, N-SOC, and O-SOC is assumed as a high-level organizational conceptualization. However, each of these tiers will be implemented in quite different settings, with diverse national and corporate cultures, as well as practices, capability levels, and capacity levels. To be effective, the ES enterprise will require consistent and competent governance and management, i.e. one that is capable of building trust, maximize value, and be adaptive and resilient in a challenging political environment.
b) **The implementation of novel rules, regulations, and incentives**: in order so succeed, the ES enterprise should active and adaptive, both in terms of self-adaptation (e.g. through legal and regulatory compliance), as well as in terms of adapting the environment (e.g. promoting legal and regulatory improvement). This requirement is extremely difficult to realize, as legal and regulatory change has a hard time trying to cope with the Internet-speed pace of change.

The consideration of these design principles entails that the proposed business framework conditions are to be taken as generic reference models and reference proposals, for the purposes of facilitating the implementation and development of future ES-related initiatives.

3.1 Models for promoting across-borders and inter-sectorial cooperation, interoperability, and adoption

Interoperability is key for enabling communication, cooperation, and coordination among the diverse ES stakeholders, as well as to maximize the value of ES-initiatives, i.e. maximize benefits, minimize costs, and control risk.

Note that additional national-specific standards, industry-specific standards, organization-specific best practice, as well as proprietary solutions need not to be discouraged; however, care should be taken to maximize value from ES-related investments, in any case avoiding severe hindrances to interoperability and adoption throughout the ES life cycle.

3.1.1 A conceptual model for the ECOSSIAN Enablers

Enabling success of ES-related initiatives is a complex task, requiring a systemic and holistic approach. Enablers are factors that, individually and collectively, influence whether something will work [50] –in this case, governance and management of the ES enterprise.

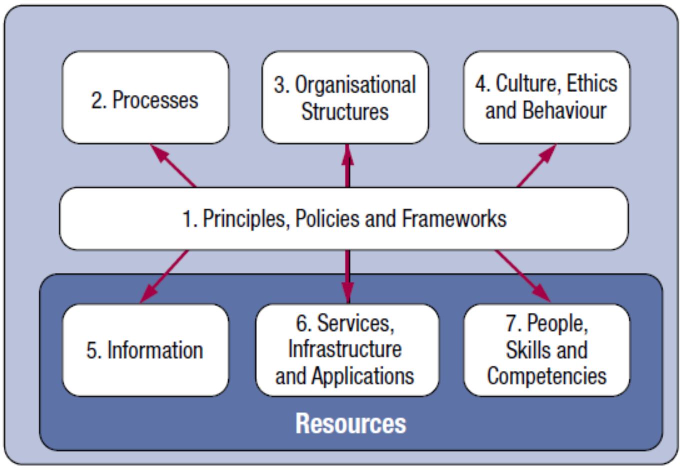

2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour
1. Principles, Policies and Frameworks
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies
Resources

Figure 4: A conceptual model for Information System enablers, taken from [50].

The proposed sector-neutral conceptual model (see Figure 4) is a systemic and holistic model for the governance and management of the ES. It covers seven categories of enablers [50]:

- **Principles, policies and frameworks** are the means to translate the desired culture, ethics, and behaviour into guidance for day-to-day management. They provide practical discernment criteria for other enablers.
- **Processes** describe an organised set of practices and activities to achieve certain objectives, in a certain area of concern.
- **Organisational structures** are the key decision-making entities in the ES enterprise.
- **Culture, ethics and behaviour** of individuals and of organisations are key to enabling solidarity, information-sharing, communication, cooperation, and coordination.
- **Information** includes all information produced and used by the ES enterprise. Information and information-sharing are required for operational excellence, as well as keeping the organisation running and well governed.
- **Services, infrastructure and applications** include the ES infrastructure, technology and applications.
- **People, skills and competencies** are required for successful completion of all activities and for making correct decisions and taking corrective actions.

3.1.2 Models and methodologies for implementing the ECOSSIAN System

The implementation of a future ES should not be understood as a one-shot short term project. Instead, due to the high complexity, fast pace of political and technological change, as well as the evolving hybrid threat scenario, a programme approach to implementing and developing the system should be adopted.

Programme agility is also required, to enable frequent observation and control points, to cope with changing requirements. This programme approach should maximize the return on investment by allowing for several implementation stages, aiming at maximizing benefits, minimizing costs, and controlling risks.

The proposed conceptual model for programme management is shown in Figure 5. It covers and aligns management phases, change enablement phases, and a continual improvement life cycle.

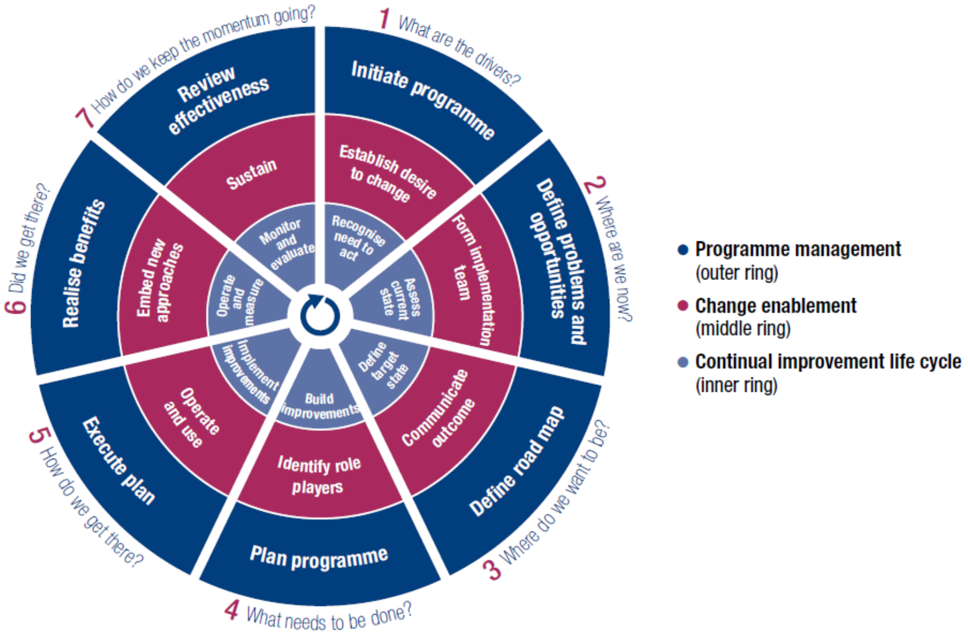


Figure 5: Conceptual model for implementing Information Systems' programme management, taken from [67].

This deliverable aims at providing help for the first three stages of a future ES implementation programme. The proposed set of models and recommendations may be used as input for planning future ES implementation programme initiatives.

The cyclical model should be run as many times as is prudently required, in an agile fashion, to cope with the fast change of political and technological change.

Excellence of change enablement if key for implementing the ES system, especially if significant obstacles to partnering are to be overcome (see Table 6):

- Confidentiality obstacles;
- Non-commitment and non-responsiveness obstacles;
- Self-interest obstacles;
- Self-review obstacles;
- Management obstacles.

3.1.3 Models for Risk Management and Disaster Risk Management

The proposed generic risk management model (see Figure 6) is taken from the ISO 31000 standard.

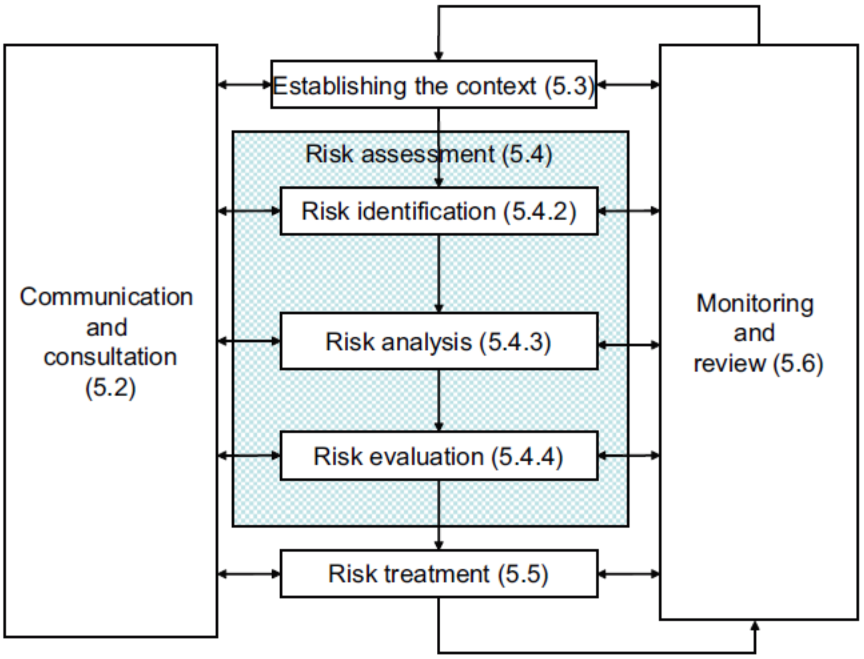

Establishing the context (5.3)
Risk assessment (5.4)
Risk identification (5.4.2)
Risk analysis (5.4.3)
Risk evaluation (5.4.4)
Risk treatment (5.5)
Communication and consultation (5.2)
Monitoring and review (5.6)

Figure 6: Risk management process model, taken from [3].

Tailoring of this model to the complex multi-stakeholder and multi-layered structure (i.e. E-SOC, N-SOC, O-SOC) of the ES requires the following considerations, regarding ES operational challenges:

1) **Achieve a common risk context understanding**: all ES stakeholders should work towards achieving a common understanding of the risk context, namely concerning political. social, economic, technological, and regulatory factors, as well as threats and vulnerabilities. This requirement is also an information-sharing challenge.
2) **Align risk assessment**: work towards achieving a common understanding of risks and towards using common methodologies. In particular, all ES stakeholders should align, as much as possible, the risk assessment methodologies and techniques (see e.g. ISO 31010). Note that organizations participating in the ES need not, necessarily, expose or change their internal risk-related processes; however, for the purposes of collaboration in the ES ecosystem, alignment, transparency, and consistency of ES processes and artifacts are key to operational excellence.
3) **Align risk treatment**: all ES layers should align, as much as possible, the risk treatment strategies, operations, and tactics, albeit each according to their values, goals, capabilities, and capacities.
4) **Understanding the diverse stakeholder values and decision processes**: risk management should be an integral part of value management and thus inform the decision processes. Therefore, all ES stakeholders should strive to understand each other’s values (at risk) and goals, as well as each other’s decision processes. This understanding is important for building partnership trust.

Alignment in the above areas is key to achieve operational excellence, avoid decision-making based on unrealistic assumptions, as well as build partnership trust and commitment throughout the entire ES ecosystem.

Relational mechanisms such as communication, consultation, monitoring, and review activities (see Figure 6) are important to achieve adequate risk management capability.

Regarding the disaster risk management reference model (see Figure 7), the following process areas are proposed:

1) **Identify**: develop the organizational understanding to manage cybersecurity risk to CI services, CI systems, CI assets, CI data, and CI capabilities; [2]
2) **Protect**: develop and implement the appropriate safeguards to ensure delivery of CI services; [2]
3) **Detect**: develop and implement the appropriate activities to identify the occurrence of a CI cybersecurity event; [2]
4) **Respond**: develop and implement the appropriate activities to act regarding a detected CI cybersecurity event; [2]
5) **Recover**: develop and implement the appropriate activities to maintain plans for CI resilience and to restore any capabilities or services that were impaired due to a CI cybersecurity event; [2]
6) **Risk Management**: this area should be aligned with the reference risk process model (see Figure 6), and cover the above areas (identify, protect, detect, respond, and recover); and
7) **Enable**: other processes, structures, and relational mechanisms that support and complement the above key process areas. Risk management of these areas should also be performed.

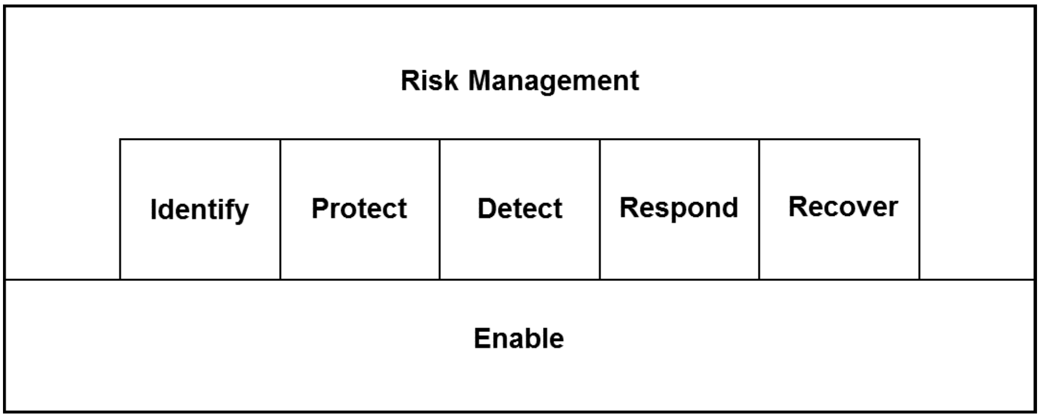


Figure 7: Disaster Risk Management conceptual model.

3.2 A model for promoting cooperation in the European Union

As presented in section 2.1, the EC strategy recommends that activities addressing cybersecurity in a comprehensive fashion should span across three key pillars: network and information security (NIS), law enforcement, and defence (see Figure 8).

Therefore, it is paramount to enable interoperability between all relevant stakeholders in the areas of defence, law enforcement, and NIS, as well as to ensure cooperation between the former and industry and academia stakeholders.

Given the recent NATO-EU Joint Declaration [56], the defence pillar should now include NATO relations, both at the National level (i.e. NATO Member States) and at the EU level.

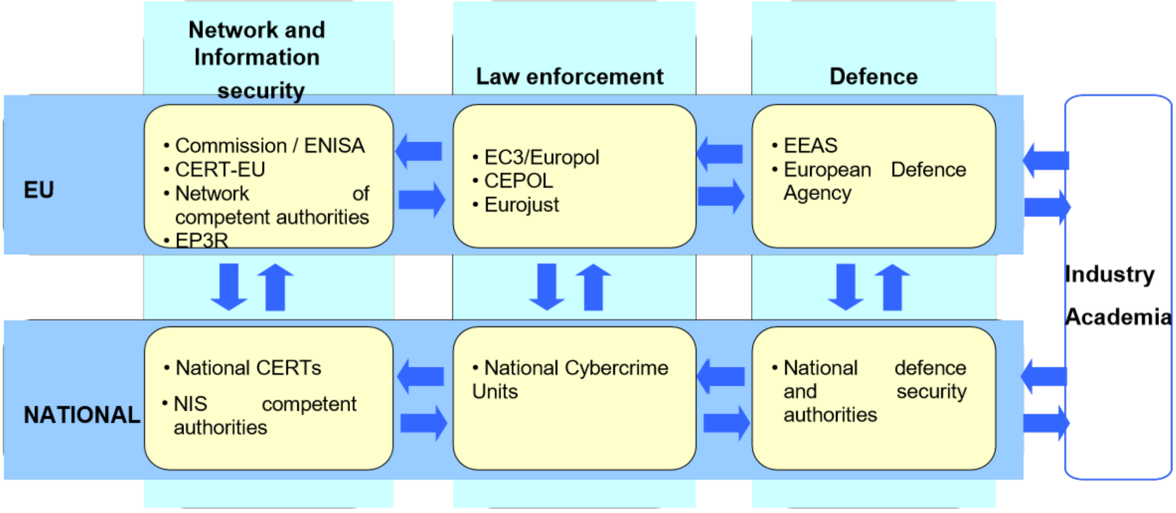

Network and Information security
Law enforcement
Defence
EU
NATIONAL
• Commission / ENISA
• CERT-EU
• Network of competent authorities
• EP3R
• EC3/Europol
• CEPOL
• Eurojust
• EEAS
• European Defence Agency
• National CERTs
• NIS competent authorities
• National Cybercrime Units
• National defence and security authorities
Industry
Academia

Figure 8: Model for coordination between NIS competent authorities/CERTs, law enforcement and defence, taken from [52].

Also, given the recent –and still ongoing– developments regarding the United Kingdom's (UK) role in the EU, we should bear in mind that the proposed model may need to be clarified and updated. In any future political configuration, the UK is essential to Europe's, EU, and NATO cybersecurity and cyber defence.

Regarding law enforcement, the model in Figure 8 should also include, at the National level, counter-terrorism units, as well as anti-corruption units. Figure 1

3.3 A generic model for governance and management

Currently, no specific organization has been assigned with the accountability and responsibility of implementing, developing, or coordinating a European-wide network of ES instances –following the completion of the ECOSSIAN Project.

For the purposes of this work, we'll refer to such a hypothetical enterprise as the ECOSSIAN System Governance and Management Organization (ESGMO).

In practice, the abstract concept of a ESGMO need not be implemented as a single legal entity. Also, it need not be either a new or dedicated organization, as its mission and responsibilities might be carried out by existing organizational structures. Furthermore, note that the ESGMO may cut across responsibilities in the military, law enforcement, and critical infrastructure domains.

According to the model proposed in Figure 9, the ESGMO is responsible for the following key areas:

- Governance: direct, evaluate, and monitor;
- Management: plan, build, run, and monitor.

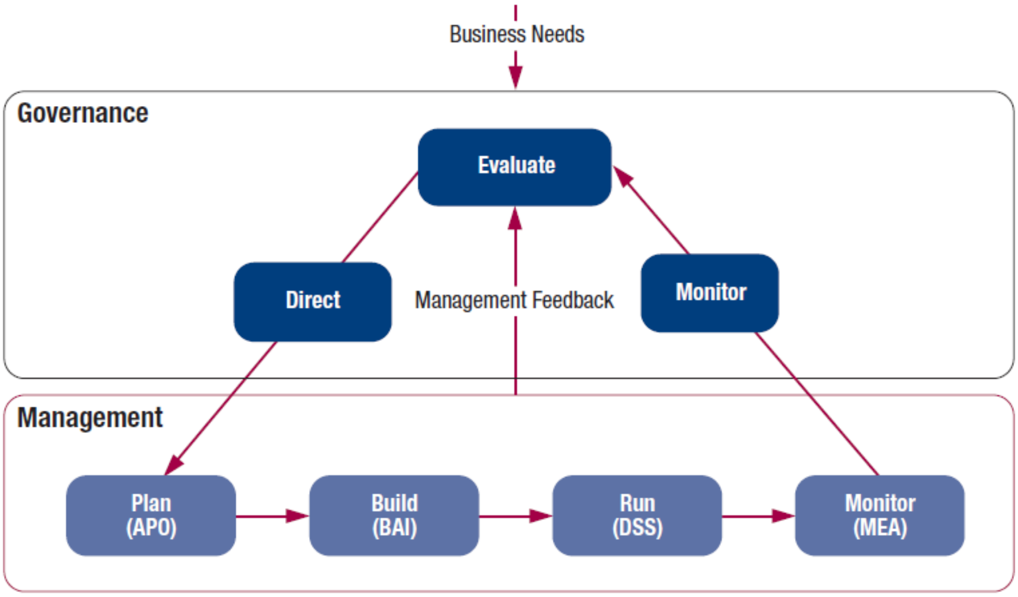


Figure 9: A generic model for governance and management, taken from [50].

To provide adequate coverage of relevant ESGMO roles, we'll define the following generic reference roles:

Table 7: Generic reference roles.

Acronym	Generic reference role
ES-Board	Board
ES-CEO	Chief Executive Officer
ES-CFO	Chief Financial Officer
ES-COO	Chief Operating Officer
ES-BizExec	Business Executives
ES-BPO	Business Process Owners
ES-SEC	Strategy Executive Committee
ES-SPC	Steering (Programmes/Projects) Committee
ES-PMO	Project Management Office
ES-VMO	Value Management Office
ES-CRO	Chief Risk Officer
ES-CISO	Chief Information Security Officer
ES-ArchBoard	Architecture Board

Acronym	Generic reference role
ES-ERC	Enterprise Risk Committee
ES-HR	Head Human Resources
ES-Compliance	Compliance
ES-Audit	Audit
ES-CIO	Chief Information Officer
ES-Arch	Head Architect
ES-Dev	Head Development
ES-ITOps	Head IT Operations
ES-ITAdmin	Head IT Administration
ES-Service	Service Manager
ES-InfoSec	Information Security Manager
ES-BCM	Business Continuity Manager
ES-DPO	Data Protection Officer / Privacy Officer

In practice, these generic roles are intended to be mapped to future real-world role/actor instances of the ESGMO organization. This enumeration includes roles relevant to the governance and management of information systems –such as the ES–, according to industry best practice; however, it is not intended to be complete, i.e. neither necessary nor sufficient.

For the purposes of this work, we will designate the group of relevant government regulatory agencies, for the cybersecurity and ICT domains, as Regulatory Agencies (RA). This concept encompasses both European and national agencies.

3.4 Enabling Principles, Policies, and Frameworks

Principles, policies and frameworks are the means to translate the desired culture, ethics, and behaviour into guidance for day-to-day management.

They provide practical discernment criteria for other enablers.

In the following table, the business framework conditions are rated according to their relative impact levels and implementation priority.

Table 8: BFC related to enabling Principles, Policies, and Frameworks.

ID	Description	Impact	Priority
PPF.BFC.01	The ES implementation and development should be embodied as a PPP-based enterprise (see also section 3.3). Currently, no specific organization has been assigned with the accountability and responsibility of implementing, developing, or coordinating a European-wide network of ES instances –following the completion of the ECOSSIAN Project. For the purposes of this work, we'll refer to such a hypothetical enterprise as the ECOSSIAN System Governance and Management Organization (ESGMO). In practice, the abstract concept of a ESGMO need not be implemented as a single legal entity. Also, it need not be either a new or dedicated organization, as its mission and responsibilities might be carried out by existing organizational structures. Furthermore, note that the ESGMO may cut across responsibilities in the military, law enforcement, and critical infrastructure domains.	High	High
PPF.BFC.02	The ES implementation and development should be realized using an agile programme approach. The implementation of a future ES should not be understood as a one-shot short-term project. Instead, due to the high complexity, fast pace of political and technological change, as well as the evolving hybrid threat scenario, a programme approach to implementing and developing the system should be adopted. Programme agility is also required, to enable frequent observation and control points, to cope with changing requirements. This programme approach should maximize the return on investment by allowing for several implementation stages, aiming at maximizing benefits, minimizing costs, and controlling risks. The proposed conceptual model for programme management is shown in Figure 5. It covers and aligns management phases, change enablement phases, and a continual improvement life cycle.	High	High

ID	Description	Impact	Priority
PPF.BFC.03	Committed leadership and sufficient funding should be provided for implementing the ES, both at the European and national government levels. Adoption may be severely hampered if critical infrastructure operators are faced with high implementation costs and risks, interoperability and integration problems, as well as unsurmountable partnering obstacles. Situational awareness and early warning are to be understood as national and European security and defence missions. A narrow focus on operator compliance and regulatory requirements may endanger the ES enterprise success.	High	High
PPF.BFC.04	Regarding crisis level criteria and crisis level management, it is important to clarify the discernment criteria for achieving the correct balance between privacy, confidentiality, and timely action. Also, the “need to know” principle should be balanced by the “need to share” principle, pondering the specific crisis management scenario.	High	Med.
PPF.BFC.05	A security vetting/clearance should be put in place, both for ES partner organizations and people engaged in managing and operating the ES. This requirement is important for helping build trust and confidence in the partnership.	Med.	Med.
PPF.BFC.06	An all-hazards approach is required, especially to cope with emerging hybrid threats. Risk management should follow an all-hazards approach. The ESGMO should engage representatives (e.g. through liaison officers) from all concerned security and defence areas, including: • Armed forces; • Law enforcement; • Intelligence agencies.	High	Med.
PPF.BFC.07	The insurance market for cyber security is relevant and should be developed. Information-sharing brings benefits, but also risks (reputational, competitive, liability, unintended privacy and confidentiality breaches). The ESGMO may offer insurance as a partnership benefit, to foster adoption.	Med.	Med.

ID	Description	Impact	Priority
PPF.BFC.08	A common reference model for ES governance and management should be adopted. Each ES partner should map their existing (and maybe proprietary) governance and management model to the ES model, for interoperability purposes. The reference governance principles are: • Meet ES stakeholder's drivers and needs; • Cover the ES enterprise end-to-end and enable a holistic approach; • Integrate and align the stakeholder's frameworks; • Separate governance from management. Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives. Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives. [70]	Med.	Med.
PPF.BFC.09	A common reference model for ES risk management and disaster risk management should be adopted. Each ES partner should map their existing (and maybe proprietary) risk management models to the ES models, for interoperability purposes.	High	Med.
PPF.BFC.10	The ESGMO mission and purpose focuses on enhancing the following high priority capabilities: • Incident response. • Coordination and Cooperation. • Information and Communication. • Emergency response planning. • Risk assessment. • Exercise. Care should be taken to ensure that these capabilities integrate seamlessly in the broader cybersecurity and cyber defence capability portfolio.	High	High
PPF.BFC.11	The ESGMO mission and purpose focuses on enabling the following partnering objectives: • Continuity of operations. • Protection of assets. • Saving lives and protecting properties. • Protection of image and reputation. • Protection of the environment.	High	High

ID	Description	Impact	Priority
PPF.BFC.12	The ESGMO should foster the following partnering principles: • Accountability. • Compliance. • Transparency. • Competence. • Fairness.	High	Med.
PPF.BFC.13	The ESGMO should work to overcome the following partnering obstacles: • Confidentiality obstacles. • Non-commitment obstacles. • Non-responsiveness obstacles. • Self-interest obstacles. • Self-review obstacles. • Management obstacles. • Technical/technological obstacles. • Contractual obstacles. • Organizational obstacles. • Familiarity obstacles. • Intimidation obstacles. • Communication obstacles. • Interoperability obstacles.	High	High

ID	Description	Impact	Priority
PPF.BFC.14	The ESGMO should provide a ES policy framework [70], including: • Information security principles. These principles should cover the areas: ○ Support and defend the business. ○ Promote responsible information security behaviour. • Information security policy, consisting of high-level direction on information security. Examples of policies are: ○ Information security policy ○ Access control policy ○ Personnel information security policy ○ Physical and environmental information security policy ○ Incident management policy ○ Business continuity and disaster recovery policy ○ Asset management policy ○ Rules of behaviour (acceptable use) ○ Information systems acquisition, software development and maintenance policy ○ Vendor management policy ○ Communications and operation management policy ○ Compliance policy, including data protection ○ Risk management policy • Specific information security policies: these policies provide subsidiary tactical guidance. • Information security procedures, standard operating procedures, requirements, and documentation: to be consulted first in case of an operational issue. The ES policy framework needs to define the: • Approvers of the enterprise policies. • Consequences of failing to comply with the policy. • Means for handling exceptions. • Manner in which compliance with the policy will be checked and measured.	High	Med.

3.5 Enabling Processes

Processes describe an organised set of practices and activities to achieve certain objectives, in a certain area of concern.

The proposed ESGMO critical processes, for which high capability levels should be achieved, are the following [50]:

- Manage Human Resources
- Manage Relationships
- Manage Suppliers
- Manage Risk
- Manage Security
- Manage Organisational Change Enablement
- Manage Changes
- Manage Change Acceptance and Transitioning
- Manage Configuration
- Manage Operations
- Manage Service Requests and Incidents
- Manage Problems
- Manage Continuity
- Manage Security Services
- Monitor, Evaluate and Assess Compliance with External Requirements

The proposed ESGMO process areas of concern, for which goal achievement and metrics control is especially important, are the following [50]:

- Ensure Benefits Delivery
- Ensure Risk Optimisation
- Ensure Stakeholder Transparency
- Manage Strategy
- Manage Enterprise Architecture
- Manage Innovation
- Manage Solutions Identification and Build
- Manage Availability and Capacity

The ESGMO, besides ensuring its own process capability levels, should also help ECOSSIAN partners achieve a minimal common level of information security operational excellence, thereby helping to ensure the partnering principles of accountability, compliance, transparency, competence, and fairness. Additional guidance may be found in COBIT5 references [50][68][70][71][72].

In the following table, the business framework conditions are rated according to their relative impact levels and implementation priority.

Unless otherwise specified, the term “enterprise” refers to both the ESGMO organization and the ES enterprise (i.e. implementation, development, management).

Table 9: BFC related to enabling Processes.

ID	Description	Impact	Priority
PRO.BFC.01	Process Area: Ensure Benefits Delivery. Optimise the value contribution to the ES ecosystem from ES services and ES assets resulting from investments made, at acceptable costs. Goals: Benefits, costs and risk of ES investments are balanced and managed and contribute optimal value.	Med.	Med.
PRO.BFC.02	Process Area: Ensure Risk Optimisation. Ensure that the ESGMO and ES partners’ risk appetite and tolerance are understood, articulated and communicated, and that risk to enterprise value related to the use of the ES is identified and managed. Goals: Information risk management is part of overall ES ecosystem’s risk management.	High	Med.
PRO.BFC.03	Process Area: Ensure Stakeholder Transparency. Ensure that ESGMO and ES performance and conformance measurement and reporting are transparent, with stakeholders approving the goals and metrics and the necessary remedial actions. Goals: Information security reporting is established and is complete, timely and accurate. Stakeholders are informed of the current status of information security and information risk across the ES enterprise.	High	Med.
PRO.BFC.04	Process Area: Manage Strategy. The European political landscape is changing at a fast pace. The ESGMO needs to provide a holistic view of the current environment, the future direction, and the initiatives required to migrate to the desired future environment. It should leverage enterprise architecture building blocks and components, including externally provided services and related capabilities to enable reliable and efficient response to strategic objectives. Goals: An information security policy framework is defined and maintained. A comprehensive information security strategy is in place and is aligned with the overall ES enterprise and ESGMO strategy. The information security strategy is cost-effective, appropriate, realistic, achievable, enterprise-focussed and balanced. The information security strategy is aligned with long-term cyber security and cyber defence strategic goals and objectives.	High	Med.

ID	Description	Impact	Priority
PRO.BFC.05	Process Area: Manage Enterprise Architecture (EA). Establish a common architecture consisting of business process, information, data, application and technology architecture layers for effectively and efficiently realising ES strategies by creating key models and practices that describe the baseline and target architectures. Define requirements for taxonomy, standards, guidelines, procedures, templates and tools, and provide a linkage for these components. Improve alignment, increase agility, improve quality of information and generate potential cost savings through initiatives such as reuse of building block components. Goals: Information security requirements are embedded within the enterprise architecture and translated into a formal information security architecture. Information security architecture is understood as part of the overall enterprise architecture. Information security architecture is aligned and evolves with changes to the enterprise architecture. An information security architecture framework and methodology are used to enable reuse of information security components across the enterprise.	High	High
PRO.BFC.06	Process Area: Manage Innovation. The cybersecurity and cyber defence technologies are evolving at a fast pace. Maintain an awareness of information technology and related service trends, identify innovation opportunities, and plan how to benefit from innovation in relation to ES needs. Analyse what opportunities for business innovation or improvement can be created by emerging technologies, services or IT-enabled business innovation, as well as through existing established technologies and by business and IT process innovation. Influence strategic planning and enterprise architecture decisions. Goals: Innovation is promoted within the information security programme. Information security requirements are taken into account when innovation is enabled.	Med.	Med.
PRO.BFC.07	Critical Process Area: Manage Human Resources (HR). Provide a structured approach to ensure optimal structuring, placement, decision rights and skills of human resources. This includes communicating the defined roles and responsibilities, learning and growth plans, and performance expectations, supported with competent and motivated people. Goals: HR capabilities and processes are aligned with information security requirements.	High	High
PRO.BFC.08	Critical Process Area: Manage Relationships. Manage the relationships between the ES stakeholders in a formalised and transparent way that ensures a focus on achieving a common and shared goal of successful enterprise outcomes in support of strategic goals and within the constraint of budgets and risk tolerance. Base the relationship on mutual trust, using open and understandable terms and common language and a willingness to take ownership and accountability for key decisions. Goals: Co-ordination, communication and a liaison structure are established between the information security function and various other stakeholders. Stakeholders recognise information security as a business enabler.	High	High

ID	Description	Impact	Priority
PRO.BFC.09	Critical Process Area: Manage Suppliers. Manage ES-related services provided by all types of suppliers to meet enterprise requirements, including the selection of suppliers, management of relationships, management of contracts, and reviewing and monitoring of supplier performance for effectiveness and compliance. Goals: Suppliers and contracts are assessed regularly and appropriate risk mitigation plans are provided. Suppliers recognise information security as an important business enabler.	High	High
PRO.BFC.10	Critical Process Area: Manage Risk. (see also section 3.1.3) Continually identify, assess and reduce ES-related risk within levels of tolerance set by enterprise executive management. Goals: A current and complete information risk profile exists for technology, applications and infrastructure within the enterprise. Information security incident response is integrated with the overall risk management process to provide the capability to update the risk management portfolio. Tailoring the risk management reference model to the complex multi-stakeholder and multi-layered structure (i.e. E-SOC, N-SOC, O-SOC) of the ES requires the following considerations, regarding ES operational challenges: 1) Achieve a common risk context understanding: all ES stakeholders should work towards achieving a common understanding of the risk context, namely concerning political. social, economic, technological, and regulatory factors, as well as threats and vulnerabilities. This requirement is also an information-sharing challenge. 2) Align risk assessment: work towards achieving a common understanding of risks and towards using common methodologies. In particular, all ES stakeholders should align, as much as possible, the risk assessment methodologies and techniques (see e.g. ISO 31010). Note that organizations participating in the ES need not, necessarily, expose or change their internal risk-related processes; however, for the purposes of collaboration in the ES ecosystem, alignment, transparency, and consistency of ES processes and artifacts are key to operational excellence. 3) Align risk treatment: all ES layers should align, as much as possible, the risk treatment strategies, operations, and tactics, albeit each according to their values, goals, capabilities, and capacities. 4) Understanding the diverse stakeholder values and decision processes: risk management should be an integral part of value management and thus inform the decision processes. Therefore, all ES stakeholders should strive to understand each other's values (at risk) and goals, as well as each other's decision processes. This understanding is important for building partnership trust. Alignment in the above areas is key to achieve operational excellence, avoid decision-making based on unrealistic assumptions, as well as build partnership trust and commitment throughout the entire ES ecosystem. Relational mechanisms such as communication, consultation, monitoring, and review activities (see Figure 6) are important to achieve adequate risk management capability.	High	High

ID	Description	Impact	Priority
	Regarding the disaster risk management reference model, the following process areas are proposed: 1) Identify: develop the organizational understanding to manage cybersecurity risk to CI services, CI systems, CI assets, CI data, and CI capabilities; 2) Protect: develop and implement the appropriate safeguards to ensure delivery of CI services; 3) Detect: develop and implement the appropriate activities to identify the occurrence of a CI cybersecurity event; 4) Respond: develop and implement the appropriate activities to act regarding a detected CI cybersecurity event; 5) Recover: develop and implement the appropriate activities to maintain plans for CI resilience and to restore any capabilities or services that were impaired due to a CI cybersecurity event; 6) Risk Management: this area should be aligned with the reference risk process model, and cover the above areas (identify, protect, detect, respond, and recover); and 7) Enable: other processes, structures, and relational mechanisms that support and complement the above key process areas. Risk management of these areas should also be performed.		
PRO.BFC.11	Critical Process Area: Manage Security. Define, operate and monitor a system for information security management. Goals: A system is in place that considers and effectively addresses enterprise information security requirements. A security plan has been established, accepted and communicated throughout the enterprise. Information security solutions are implemented and operated consistently throughout the enterprise.	High	High
PRO.BFC.12	Critical Process Area: Manage Programmes and Projects. (see also section 3.1.2) The ESGMO should manage all programmes and projects from the investment portfolio in alignment with enterprise strategy and in a co-ordinated way. Initiate, plan, control, and execute programmes and projects, and close with a post-implementation review. Goals: Information security requirements are considered and incorporated in all programmes and projects. The implementation of a future ES should not be understood as a one-shot short term project. Instead, due to the high complexity, fast pace of political and technological change, as well as the evolving hybrid threat scenario, a programme approach to implementing and developing the system should be adopted. Programme agility is also required, to enable frequent observation and control points, to cope with changing requirements. This programme approach should maximize the return on investment by allowing for several implementation stages, aiming at maximizing benefits, minimizing costs, and controlling risks. The proposed conceptual model for programme management is shown in Figure 5. It covers and aligns management phases, change enablement phases, and a continual improvement life cycle.	High	High

ID	Description	Impact	Priority
PRO.BFC.13	Process Area: Manage Solutions Identification and Build. Establish and maintain identified solutions in line with enterprise requirements covering design, development, procurement/sourcing and partnering with suppliers/vendors. Manage configuration, test preparation, testing, requirements management and maintenance of business processes, applications, information/data, infrastructure and services. Goals: Information security measures are embedded in the solution and effectively support enterprise strategic and operational objectives. Information security solutions are accepted and have been successfully tested. Changes to information security requirements are correctly incorporated in the solution.	High	High
PRO.BFC.14	Process Area: Manage Availability and Capacity. Balance current and future needs for availability, performance and capacity with cost-effective service provision. Include assessment of current capabilities, forecasting of future needs based on business requirements, analysis of business impacts, and assessment of risk to plan and implement actions to meet the identified requirements. Goals: Information security requirements are included in the availability, performance and capacity management plans. Information security impact on availability, performance and capacity is monitored and optimised.	High	Med.
PRO.BFC.15	Critical Process Area: Manage Organisational Change Enablement. Maximise the likelihood of successfully implementing sustainable enterprise-wide organisational change quickly and with reduced risk, covering the complete life cycle of the change and all affected ES stakeholders. Goals: Information security alerts and trends are used effectively to enable change in the enterprise and influence the enterprise's culture on information security culture. Information security protocols are revised and refined as the enterprise changes through information security awareness.	Med.	High
PRO.BFC.16	Critical Process Area: Manage Changes. Manage all changes in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure. This includes change standards and procedures, impact assessment, prioritisation and authorisation, emergency changes, tracking, reporting, closure and documentation. Goals: Information security requirements are incorporated during impact assessments of processes, applications and infrastructure changes. Emergency changes take into account the necessary information security requirements.	High	High
PRO.BFC.17	Process Area: Manage Change Acceptance and Transitioning. Formally accept and make operational new solutions, including implementation planning, system and data conversion, acceptance testing, communication, release preparation, promotion to production of new or changed processes and ES services, early production support, and a post-implementation review. Goals: Information security testing is an integral part of acceptance testing. Information security improvements identified are incorporated in future releases.	Med.	Med.

ID	Description	Impact	Priority
PRO.BFC.18	Critical Process Area: Manage Configuration. Define and maintain descriptions and relationships between key resources and capabilities required to deliver ES-enabled services, including collecting configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository. Goals: Information security configuration baselines are approved, implemented and maintained across the enterprise.	High	Med.
PRO.BFC.19	Critical Process Area: Manage Operations. Co-ordinate and execute the activities and operational procedures required to deliver internal and outsourced IT services, including the execution of predefined standard operating procedures and the required monitoring activities. Goals: Information security operations are performed according to an information security operational plan in line with the information security strategy. Applicable information security standards are identified and met.	High	Med.
PRO.BFC.20	Critical Process Area: Manage Service Requests and Incidents. Provide timely and effective response to user requests and resolution of all types of incidents. Restore normal service; record and fulfil user requests; and record, investigate, diagnose, escalate and resolve incidents. Goals: An effective information security incident response programme is established and maintained.	High	High
PRO.BFC.21	Critical Process Area: Manage Problems. Identify and classify problems and their root causes and provide timely resolution to prevent recurring incidents. Provide recommendations for improvements. Goals: Information security problems are solved in a sustainable way.	High	High
PRO.BFC.21	Critical Process Area: Manage Continuity. Establish and maintain a plan to enable the enterprise to respond to incidents and disruptions in order to continue operation of critical business processes and required IT services and maintain availability of information at a level acceptable to the enterprise. Goals: Information risk is properly identified and addressed in the information and communications technology (ICT) continuity plan.	Med.	Med.
PRO.BFC.22	Critical Process Area: Manage Security Services. Protect enterprise information to maintain the level of information security risk acceptable to the enterprise in accordance with the security policy. Establish and maintain information security roles and access privileges and perform security monitoring. Goals: Network and communication security meet business needs. Information processed on, stored on and transmitted by endpoint devices is protected. All users are uniquely identifiable and have access rights in accordance with their business roles. Physical measures have been implemented to protect information from unauthorised access, damage and interference when being processed, stored or transmitted. Electronic information is properly secured when stored, transmitted or destroyed.	High	High

ID	Description	Impact	Priority
PRO.BFC.23	Critical Process Area: Monitor, Evaluate and Assess Compliance with External Requirements Evaluate that ESGMO/ES processes and ES-supported business processes are compliant with laws, regulations and contractual requirements. Obtain assurance that the requirements have been identified and complied with, and integrate ES compliance with overall enterprise compliance. Goals: Information security and information risk practices conform to external compliance requirements. Monitoring is conducted for new or revised external requirements with an impact on information security, resilience, and privacy.	Med.	Med.

3.6 Enabling Organizational Structures

Organisational structures are the key decision-making entities in the ES enterprise.

In the following table, the business framework conditions are rated according to their relative impact levels and implementation priority.

Table 10: BFC related to enabling Organizational Structures.

ID	Description	Impact	Priority
ORG.BFC.01	An ESGMO should be created for managing the ES implementation and development programme. (see also section 3.3)	High	High
ORG.BFC.02	The ESGMO should be sufficiently funded and empowered, to accomplish its mission and purpose.	High	High
ORG.BFC.03	The ESGMO should be adequately staffed, pondering: • People, skills and competencies (see section 3.10) requirements. • The reference ESGMO core roles (see section 3.3) • Liaison officers: the ESGMO may engage representatives from all concerned security and defence areas, including: ○ Armed forces; ○ Law enforcement; ○ Intelligence agencies; ○ CIWIN – DG HOME; ○ EPCIP initiatives; ○ ERNCIP Project Platform - JRC; ○ NIST; ○ United Kingdom's peer cybersecurity and cyber defence stakeholders.	High	High
ORG.BFC.04	Clarify the organizational and operational consequences of the terms "critical infrastructure", "European critical infrastructure", and "operator of essential services", as well as the relation between these terms.	Med.	Med.

ID	Description	Impact	Priority
ORG.BFC.05	In the US, Presidential Policy Directive/PPD-21 defined 16 critical infrastructure sectors and designated associated Federal Sector-Specific Agencies (SSAs). On the other hand, the EU situation has not reached such a clear and complete conceptual and operational definition –although the recent NIS Directive provides some definitions in this area. Clear and transparent alignment/mapping should be achieved between the US and EU, regarding the identification of CI infrastructure sectors, to enable seamless collaboration.	High	High

3.7 Enabling Culture, Ethics, and Behaviour

Culture, ethics and behaviour of individuals and of organisations are key to enabling solidarity, information-sharing, communication, cooperation, and coordination.

In the following table, the business framework conditions are rated according to their relative impact levels and implementation priority.

Table 11: BFC related to enabling Culture, Ethics, and Behaviour.

ID	Description	Impact	Priority
CEB.BFC.01	European foundational values, principles, and objectives should be promoted and embedded in ES policy framework supporting artifacts (see also PPF.BFC.14 and section 2.3).	High	Med.
CEB.BFC.02	A significant effort should be made by the ESGMO, to promote the Solidarity principle. (see also CEB.BFC.01)	High	Med.
CEB.BFC.03	A crucial factor is trust between joining partners. They need to meet each other in person and discuss things together. (see section 2.9) The ESGMO should ensure enough funding and empowerment is made available for trust-building activities.	High	Med.

3.8 Enabling Information

Information includes all information produced and used by the ES enterprise. Information and information-sharing are required for operational excellence, as well as keeping the organisation running and well governed.

In the following table, the business framework conditions are rated according to their relative impact levels and implementation priority.

Table 12: BFC related to enabling Information.

ID	Description	Impact	Priority
INF.BFC.01	Promote interoperability between all relevant partners, by establishing a common informational and knowledge understanding, regarding terminology, taxonomies, and ontologies. Goal: provide semantic bridges to enable communication, cooperation, and coordination between the parties engaged in CD/CS missions. As an example, some of the main sources for reference terminology are: • EU sources, namely ENISA glossaries and the NIS Directive, representing European cybersecurity concerns; • NATO official sources, representing NATO cyber defence concerns; • NIST official documents, representing USA cybersecurity concerns; • ISACA sources, representing information assurance concerns, as well as IS/IT industry governance and management best practice. Note that these sources often refer to ISO standards.	High	High
INF.BFC.02	Define the Levels of Cyber Occurrences, regarding common terminology and operational consequence, across the EU and NATO domains. Although the NATO Cyber Defense Taxonomy provides high level definitions for levels of occurrences, significant future work is needed for defining and operationalizing these concepts. Also, EU and NATO terminology should be aligned, as much as possible, to enable effective and efficient coordination of operational processes and activities.	High	High
INF.BFC.03	Clarify the classification of Incidents and Events. Future work is needed for improving interoperability in this classification area. The “Common Taxonomy for Law Enforcement and the National Network of CSIRTs” [57], approved by Europol and ENISA, is proposed as a starting point for this endeavour.	High	High

ID	Description	Impact	Priority
INF.BFC.04	Clarify CS and CD concepts with high political and operational impact. Some CS and CD terms have high political and operational significance, but have contested definitions e.g. “cyberterrorism”. In such cases, further work is needed to reach consensus and formal approval.	High	Med.
INF.BFC.05	(see also PPF.BFC.14) The ESGMO should manage the life cycle of the informational artifacts related to the ES policy framework, including: • Information security principles. These principles should cover the areas: • Information security policy, consisting of high-level direction on information security. Examples of policies are: ○ Information security policy ○ Access control policy ○ Personnel information security policy ○ Physical and environmental information security policy ○ Incident management policy ○ Business continuity and disaster recovery policy ○ Asset management policy ○ Rules of behaviour (acceptable use) ○ Information systems acquisition, software development and maintenance policy ○ Vendor management policy ○ Communications and operation management policy ○ Compliance policy ○ Risk management policy • Specific information security policies: these policies provide subsidiary tactical guidance. • Information security procedures, standard operating procedures, requirements, and documentation: to be consulted first in case of an operational issue.	High	Med.

3.9 Enabling Services, Infrastructure, and Applications

Services, infrastructure and applications include the ES infrastructure, technology and applications.

In the following table, the business framework conditions are rated according to their relative impact levels and implementation priority.

Table 13: BFC related to enabling Services, Infrastructure, and Applications.

ID	Description	Impact	Priority
SIA.BFC.01	Secure Identity Management services should be made available and enforced for users of the ES. These services should be: • Responsive, rapid, and agile; • Secure and resilient, both to natural and man-made disasters; • Audited. Trust and confidence between stakeholders should be ensured and enforced. • Integrate with the adequate security vetting/clearance processes and procedures.	High	Med.
SIA.BFC.01	The ESGMO should help the SOCs develop their service catalogue, by sharing best practice and promoting peer-to-peer collaboration. As an example, the service catalogue may include the following services: [82] • Reactive Services: ○ Alerts and Warning ○ Incident handling ○ Incident analysis ○ Incident response on site ○ Incident response support ○ Incident response coordination ○ Vulnerability handling ○ Vulnerability analysis ○ Vulnerability response ○ Vulnerability response coordination ○ Artefact handling ○ Artefact analysis ○ Artefact response ○ Artefact response coordination • Proactive Services: ○ Announcements ○ Technology watch ○ Security Audits or Assessments ○ Configuration and Maintenance of Security Tools, Applications, and Infrastructures ○ Development of Security Tools ○ Intrusion Detection Services	Med.	Med.

ID	Description	Impact	Priority
	○ Security-Related Information Dissemination • Security Quality Management Services: ○ Risk Analysis ○ Business Continuity and ○ Disaster Recovery Planning ○ Security Consulting ○ Awareness Building ○ Education/Training ○ Product Evaluation or Certification		

3.10 Enabling People, Skills, and Competencies

People, skills and competencies are required for successful completion of all activities and for making correct decisions and taking corrective actions.

In the following table, the business framework conditions are rated according to their relative impact levels and implementation priority.

Table 14: BFC related to enabling People, Skills, and Competencies.

ID	Description	Impact	Priority
PSC.BFC.01	The ESGMO should address the current cybersecurity and cyber defence human resources shortage, from both the capacity and capability point-of-views, enabling the ES partners to build adequate capability and capacity for managing and operating the ES instances and interfaces. Highlights: ○ Cyber curricula planning and execution should ensure alignment and practical cooperation with the ongoing efforts in NATO and the US (e.g. NICE, see http://csrc.nist.gov/nice/), as well as those ongoing in the Member States. ○ Cyber curricula should be aligned with culture, ethics, and behaviour enablers (see chapter 7). ○ Cyber curricula should encompass a mix of ethical, legal, organizational, and technical aspects, as well an adequate mix of civil, law enforcement, and military concepts and contents – depending on the job/training profile.	High	Low
PSC.BFC.02	The ESGMO should provide training guidance and promote exercise events, to enhance readiness and foster operational excellence, as well as build trust between partners. The actual execution of training and exercise events may be outsourced or executed using partner resources. Engagement and participations in other exercise events (e.g. national, EU, NATO) may also be promoted.	High	High

Chapter 4 Conclusion

The success of future ES implementations should not be taken for granted. This work has identified significant capability and capacity gaps, in many areas, regarding ES business framework conditions, including PPP aspects.

Furthermore, the European political, security, and defence context has changed in fundamental ways, since the inception of the ECOSSIAN Project, adding to the difficulty and complexity of future ES-related initiatives. As we write these lines, the future mission and political configuration of the European Union is a subject of high profile debate; the political landscape is changing in several Member States (MS); and major changes are taking place in the United Kingdom. Most significantly, support for the Solidarity principle in wavering, challenging the European Union's foundations and creating uncertainty for ES-related initiatives –which are critically dependent on the stakeholder's will to communicate, cooperate, and coordinate their efforts, as well as on EU/MS drive, leadership, and funding. Therefore, if steadfast trust is to be aimed at, much work needs to be done regarding culture, ethics, behaviour, principles, and policies.

On the other hand, it is now clearly recognized that hybrid threats are on the rise, implying that the value of effective ES-like implementations is also increasing. Also, in 2016 major steps have been taken to foster EU-NATO cooperation, opening new possibilities for enhancing and integrating situational awareness and early warning capabilities.

The analysis performed in Chapter 2 soberly demonstrates the complexities and difficulties of implementing successful ES-like solutions.

However, Chapter 3 proposes an enabling path towards such a success, based on an agile programme-based approach for implementing and developing the ES. Furthermore, the proposed ECOSSIAN systemic enablers are based on authoritative European Union guidance, international standards, and industry best practice, thus facilitating interoperability –and, ultimately, widespread adoption.

Chapter 5 List of Abbreviations

Abbreviation	Description
AACM	Aggregation Analysis Correlation Module
ANSI	American National Standards Institute
API	Application Programming Interface
APT	Advanced Persistent Threat
CERT	Computer Emergency Response Team
CFR	Charter of Fundamental Rights of the European Union
CI	Critical Infrastructure
C-I-A	Confidentiality, Integrity, and Availability
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
CIWIN	Critical Infrastructure Warning Information Network
CIRT	Computer Incident Response Team
CM	Correlation Module
CNIL	Commission Nationale de l'Informatique et des Libertés
CNPD	Comissão Nacional de Protecção de Dados *(Portuguese Data Protection Authority)*
COBIT	Control Objectives for Information Technology
COP	Common Operational Picture
COTS	Commercial-Off-The-Shelf (products)
CRISP	Cyber Risk Information Sharing Program
CD	Cyber Defense (EU and NATO scope)
CS	cybersecurity (EU and NATO scope)
CSIRT	Computer Security Incident Response Team
CSF	Cyber Security Framework (NIST)
DAE	Digital Agenda for Europe
DHS	Department of Homeland Security
DoD	US Department of Defence
DoW	Description of Work
DPA	Data Protection Act / Authority
DSM	(European) Digital Single Market

Abbreviation	Description
ECI	European Critical Infrastructure
ECOSSIAN	European Control System Security Incident Analysis Network
EDA	European Defence Agency
EPCIP	European Program on Critical Infrastructure Protection
ES	ECOSSIAN System
ESGMO	ECOSSIAN System Governance and Management Organization
ES-Arch	Head Architect (ESGMO role)
ES-ArchBoard	Architecture Board (ESGMO role)
ES-Audit	Audit (ESGMO role)
ES-BCM	Business Continuity Manager (ESGMO role)
ES-BizExec	Business Executives (ESGMO role)
ES-Board	ECOSSIAN System Board (ESGMO role)
ES-BPO	Business Process Owners (ESGMO role)
ES-CEO	Chief Executive Officer (ESGMO role)
ES-CFO	Chief Financial Officer (ESGMO role)
ES-CIO	Chief Information Officer (ESGMO role)
ES-CISO	Chief Information Security Officer (ESGMO role)
ES-Compliance	Compliance (ESGMO role)
ES-COO	Chief Operating Officer (ESGMO role)
ES-CRO	Chief Risk Officer (ESGMO role)
ES-Dev	Head Development (ESGMO role)
ES-DPO	Data Protection Officer / Privacy Officer (ESGMO role)
ES-ERC	Enterprise Risk Committee (ESGMO role)
ES-HR	Head Human Resources (ESGMO role)
ES-InfoSec	Information Security Manager (ESGMO role)
ES-ITAdmin	Head IT Administration (ESGMO role)
ES-ITOps	Head IT Operations (ESGMO role)
ES-PMO	Project Management Office (ESGMO role)
ES-SEC	Strategy Executive Committee (ESGMO role)
ES-Service	Service Manager (ESGMO role)
E-SOC	European Security Operations Center
ES-SPC	Steering (Programmes/Projects) Committee (ESGMO role)
ES-VMO	Value Management Office (ESGMO role)
EU	European Union
ECHR	European Convention on Human Rights

Abbreviation	Description
EGE	European Group on Ethics in Science and New Technologies to the European Commission
ENISA	European Network and Information Security Agency
EPCIP	European Programme for Critical Infrastructure Protection
FEMA	Federal Emergency Management Agency
GDPR	General Data Protection Regulation
ICS	Industrial Control Systems
ICT	Information and Communication Technologies
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IMM	Incident Management Module
IPS	Intrusion Protection System
ISACA	(previously known as the) Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO	International Organisation for Standardisation
ISP	Internet Service Provider
ITIL	Information Technology Infrastructure Library
LEA	Law Enforcement Agency
MS	(EU) Member State
NATO	North Atlantic Treaty Organisation
NCIA	NATO Communications and Information Agency
NCIRC	NATO Computer Incident Response Capability
NGO	Non-governmental organization
NICP	NATO Industry Cyber Partnership
NIDS	Network Intrusion Detection Systems
NIPP	(USA) National Infrastructure Protection Plan
NIS	Network Information Security
NIST	National Institute of Standards and Technology
N-SOC	National Security Operations Center
OSINT	Open Source Intelligence
O-SOC	Operator’s Security Operations Center
PII	Personally Identifiable Information
PLC	Programmable Logic Controller
PMO	PPP Management (and administration) Organization

Abbreviation	Description
PP	Public-Private
PPD-21	(US) Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience
PPP	Public-Private Partnership
RA	Regulatory Agencies, the set of all relevant government regulatory agencies, for the cybersecurity and ICT domains
RAM	Risk Assessment Module
RS	Reporting System
SA	Situational Awareness
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information Event Monitoring
SLA	Service Level Agreement
SME	Small- and Medium-sized Enterprises
SOC	Security Operation Centre
SWOT	Strengths, Weaknesses, Opportunities, and Threats
TDM	Threat Detection Module
TEU	Treaty on European Union
TFEU	Treaty of Lisbon on the Functioning of the European Union
TMM	Threat Mitigation Module
UNISDR	United Nations Office for Disaster Risk Reduction
US, USA	United States of America
USCYBERCOM	United States Cyber Command
VM	Visualisation Module
VPN	Virtual Private Network

Chapter 6 Glossary

Term (and context)	Definition(s) and source(s)
Critical Infrastructure	Means an asset, system or part thereof located in Member States 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 Member State as a result of the failure to maintain those functions. (Source: Council Directive 2008/114/EC) Systems whose incapacity or destruction would have a debilitating effect on the economic security of an enterprise, community or nation. (Source: ISACA Glossary of Terms, 2015) 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. (Source: USA Patriot Act of 2001)
Crisis	Situation with high level of uncertainty that disrupts the core activities and/or credibility of an organization and requires urgent action. (Source: ISO 22300:2012)
Disaster	Situation where widespread human, material, economic or environmental losses have occurred which exceeded the ability of the affected organization, community or society to respond and recover using its own resources. (Source: ISO 22300:2012) A serious disruption of the functioning of a community or a society involving widespread human, material, economic or environmental losses and impacts, which exceeds the ability of the affected community or society to cope using its own resources. (Source: UNISDR, 2009) 1. A sudden, unplanned calamitous event causing great damage or loss. Any event that creates an inability on an enterprise's part to provide critical business functions for some predetermined period of time. Similar terms are business interruption, outage and catastrophe. 2. The period when enterprise management decides to divert

Term (and context)	Definition(s) and source(s)
	from normal production responses and exercises its disaster recovery plan (DRP). It typically signifies the beginning of a move from a primary location to an alternate location. (Source: ISACA Glossary of Terms, 2015)
electronic communications network	Means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed. (Source: Directive 2002/21/EC)
Enterprise	Means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity. (Source: GDPR) A group of individuals working together for a common purpose, typically within the context of an organizational form such as a corporation, public agency, charity or trust. (Source: ISACA Glossary of Terms, 2015)
European critical infrastructure	Means critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. 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. (Source: Council Directive 2008/114/EC)
Hazard	Source of potential harm. (Source: ISO Guide 73, ISO 22300:2012) A dangerous phenomenon, substance, human activity or condition that may cause loss of life, injury or other health impacts, property damage, loss of livelihoods and services, social and economic disruption, or environmental damage. (Source: UNISDR, 2009) Natural or manmade source or cause of harm or difficulty. (Source: DHS Lexicon, 2010)
Incident	Situation that might be, or could lead to, a disruption, loss, emergency or crisis. (Source: ISO 22300:2012) Means any event having an actual adverse effect on the

Term (and context)	Definition(s) and source(s)
	security of network and information systems. (Source: NIS Directive) Any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service. (Source: ISACA Glossary of Terms, 2015) An occurrence, caused by either human action or natural phenomenon, that may cause harm and require action, which can include major disasters, emergencies, terrorist attacks, terrorist threats, wild and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, cyberattacks, cyber failure/accident, and other occurrences requiring an emergency response. (Source: DHS Lexicon, 2010)
Interoperability	Ability of diverse systems and organizations to work together i.e. to inter-operate. (Source: ISO 22397:2014)
Network and information system	Means: (a) an electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC; (b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or (c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance. (Source: NIS Directive)
NIS Directive	Same as: Directive(EU) 2016/1148 of the European Parliament and of the Council, of 6 July 2016.
Operator of essential services	Article 4(4): Means a public or private entity of a type referred to in Annex II, which meets the criteria laid down in Article 5(2). Article 5(2): The criteria for the identification of the operators of essential services, as referred to in point (4) of Article 4, shall be as follows: (a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities; (b) the provision of that service depends on network and information systems; and (c) an incident would have significant disruptive effects on the provision of that service. (Source: NIS Directive)

Term (and context)	Definition(s) and source(s)
Partnering	Association with others in an activity or area of common interest in order to achieve individual and collective objectives. (Source: ISO 22397:2014) *(See also: Partnership, Public-Private Partnership)*
Partnership	Organized relationship between two bodies (public-public, private-public, private-private) which establishes the scope, roles, procedures and tools to prevent and manage any incident impacting on societal security with respect to related laws. (Source: ISO 22300:2012) *(See also: Partnering, Public-Private Partnership)*
Personal data	Means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. (Source: GDPR)
Processing	Means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. (Source: GDPR)
Profiling	Means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. (Source: GDPR)
Pseudonymisation	Means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. (Source: GDPR)
Public-Private Partnership	An organised relationship between public and private organisations, which establishes common scope and objectives and uses defined roles and work methodology to achieve shared goals. (Source: ENISA, Cooperative Models for Effective Public

Term (and context)	Definition(s) and source(s)
	Private Partnerships, Good Practice Guide, 2011) *(See also: Partnering, Partnership)*
Resilience	The ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions. (Source: UNISDR, 2009) The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions; includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. (Source: PPD-21, 2013) Adaptive capacity of an organization in a complex and changing environment. (Source: ISO Guide 73, ISO 22300:2012)
Risk	Means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems. (Source: NIS Directive) Effect of uncertainty on objectives. Note 1 to entry: An effect is a deviation from the expected: positive and/or negative. Note 2 to entry: Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process). Note 3 to entry: Risk is often characterized by reference to potential events, and consequences, or a combination of these. Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence. Note 5 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood. (Source: ISO Guide 73) A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Term (and context)	Definition(s) and source(s)
	Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. (Source: NIST SP800-53 Revision 4)

Chapter 7 Bibliography

[1]. The Council of the European Union, “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,” Official Journal of the European Union, 2008

[2]. NIST, "Framework for Improving Critical Infrastructure Cybersecurity - Version 1.0," NIST - National Institute of Standards and Technology, 2014.

[3]. ISO, ISO 31000:2009 - Risk management — Principles and guidelines, 2009.

[4]. ISO, ISO Guide 73:2009 - Risk Management — Vocabulary, 2009.

[5]. ISO, ISO/IEC 31010:2009 – Risk management – Risk assessment techniques, 2009.

[6]. CIPRNet, Official website for the CIPRNet - The Critical Infrastructure Preparedness and Resilience Research Network.

[7]. The ERNCIP Project Platform, Official website for the ERNCIP Project Platform - European Reference Network for Critical Infrastructure Protection, JRC - Joint Research Centre, European Commission.

[8]. European Commission, "Risk Assessment and Mapping Guidelines for Disaster Management. SEC(2010) 1626 final," Brussels, 2010.

[9]. T. P. o. t. U. S. o. America, “Executive Order 13636 - Improving Critical Infrastructure Cybersecurity,” Federal Register, 2013.

[10]. T. P. o. t. U. S. o. America, Presidential Policy Directive / PPD-21 - Critical Infrastructure Security and Resilience, 2013.

[11]. President’s Commission on Critical Infrastructure Protection, “Critical Foundations - Protecting America’s Infrastructures, The Report of the President’s Commission on Critical Infrastructure Protection,” Washington, DC, 1997.

[12]. Barbara Schmickler, Bundestag debated draft, tagesschau.de, 2015.

[13]. Deutscher Bundestag, “Draft law to increase security of IT systems (Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme – IT-Sicherheitsgesetz),” 2015.

[14]. D. H. Gunneriusson, “Nothing is Taken Serious Until it Gets Serious: Countering Hybrid Threats,” Defence Against Terrorism Review, vol. 4, no. 1, pp. 47-70, 2012.

[15]. T. Maurer, “Public-Private Partnerships for Critical Infrastructure Protection,” CSIS - Centre for Strategic & International Studies, Washington, DC, 2013.

[16]. “Official website for the FSSCC - Financial Services Sector Coordinating Council,” [Online]. Available: https://www.fsscc.org/.

[17]. M. D. Cavelty, Cybersecurity in Switzerland, Zurich: Springer, 2014.

[18]. M. D. Cavelty and M. Suter, “Public–Private Partnerships are no silver bullet...,” International Journal of Critical Infrastructure Protection, vol. 4, no. 2, pp. 179-187, 2009.

[19]. Complex Interactive Processes (CIP) Institute, How to deal with crises? - 2nd International CIP Event, Amsterdam, 2015.

[20]. National Cyber Security Centre (NCSC), “Cyber Security Assessment Netherlands - Official website,” National Cyber Security Centre (NCSC) of the Ministry of Security and Justice, [Online]. Available: https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands.

[21]. “European Union procedures and resources for crisis management,” International Peacekeeping, vol. 11, no. 3, pp. 404-421, 2004.

[22]. FIRST - Forum of Incident Response and Security Teams, “Official website of FIRST - Forum of Incident Response and Security Teams,” [Online]. Available: https://www.first.org.

[23]. Commission of the European Communities, “Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM(2006) 786 final,” Brussels, 2006.

[24]. JRC - Joint Research Centre, European Commission, “Official website of The ERNCIP Project Platform - European Reference Network for Critical Infrastructure Protection,” [Online]. Available: https://erncip-project.jrc.ec.europa.eu/.

[25]. DG HOME, European Commission, “Critical Infrastructure Warning Information Network (CIWIN),” [Online]. Available: http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network/index_en.htm.

[26]. FCC - Federal Communications Commission, “Disaster Information Reporting System (DIRS),” [Online]. Available: https://www.fcc.gov/general/disaster-information-reporting-system-dirs-0.

[27]. NATIONAL Y2K INFORMATION COORDINATION CENTER, “Best Practices and Lessons Learned,” 2000.

[28]. Software Engineering Institute (SEI), “Officil website of the CERT Division of the Software Engineering Institute (SEI),” [Online]. Available: http://www.cert.org.

[29]. M. J. West-Brown, D. Stikvoort, K.-P. Kossakowski, G. Killcrece, R. Ruefle and M. Zajicek, Handbook for Computer Security Incident Response Teams (CSIRTs), Hanscom AFB, MA: Software Engineering Institute (SEI), Carnegie Mellon, 2003.

[30]. FIRST - Forum of Incident Response and Security Teams, “FIRST Policies”.

[31]. European Government CERTs (EGC) group, “Webpage of the CERTs (EGC) group”.

[32]. European PPP Expertise Centre, “Offical website of the European PPP Expertise Centre (EPEC),” [Online]. Available: http://www.eib.org/epec/.

[33]. EPEC - European PPP Expertise Centre, “A Programme Approach to PPPs - Lessons from the European experience,” Luxembourg, 2015.

[34]. European Commission, “Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM(2016) 410 final,” Brussels, 2016.

[35]. “Position of the Council on the adoption of a Directive of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union, COM(2016) 363 final,” Brussels, 2016.

[36]. The European Parliment and the Council of the European Union, “Directive (EU) 2016/1148 of the European Parliment and the Council, of 6 July 2016, concerning measures for a high common level of security of network and information systems across the Union,” Official Journal of the European Union, 2016.

[37]. ENISA - European Network and Information Security Agency, “Cooperative Models for Effective Public Private Partnerships, Desktop Research Report,” ENISA, 2011.

[38]. ENISA - European Network and Information Security Agency, “Cooperative Models for Effective Public Private Partnerships, Good Practice Guide,” ENISA, 2011.

[39]. ENISA - European Union Agency for Network and Information Security, “EP3R 2010-2013, Four Years of Pan-European Public Private Cooperation,” ENISA, 2014.

[40]. ISO - International Organization for Standardization, ISO 22397:2014(E) – Societal security — Guidelines for establishing partnering arrangements, ISO, 2014.

[41]. THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, “REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR),” Official Journal of the European Union, pp. L 119/1 - L 119/88, 4 5 2016.

[42]. THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, “DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, on the protection of natural persons with regard to the processing of personal data by competent authorities,” Official Journal of the European Union, pp. L 119/89 - L 119/131, 4 5 2016.

[43]. ISO, ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements, ISO, 2013.

[44]. NIST - National Institute of Standards and Technology, NIST Special Publication 800-53 Revision 4 - Security and Privacy Controls for Federal Information Systems, NIST - U.S. Department of Commerce, 2015.

[45]. NSO - NATO Standardization Office, NATO GLOSSARY OF TERMS AND DEFINITIONS (ENGLISH AND FRENCH), AAP-06 Edition 2015, NATO, 2015.

[46]. ISACA, “ISACA Glossary of Terms, 2015,” 2015.

[47]. DHS Risk Steering Committee, “DHS Risk Lexicon - 2010 Edition,” DHS - Department of Homeland Security, 2010.

[48]. United Nations Office for Disaster Risk Reduction (UNISDR), “2009 UNISDR Terminology on Disaster Risk Reduction,” Geneva, 2009.

[49]. ISO - International Organization for Standardization, “ISO 22300:2012 Societal security — Terminology,” ISO, 2012.

[50]. ISACA, COBIT 5: A Business Framework for the Governance and Management of Enterprise IT, Rolling Meadows, IL, USA: ISACA, 2012.

[51]. ENISA Threat Landscape: Overview of current and emerging cyberthreats, December 2014.

[52]. European Commission, JOIN(2013) 1 final, “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace”, Brussels, February 7th 2013.

[53]. Roberta Wohlstetter: Warning and Decision. Stanford, Cal. 1962, p. 70 and Wohlstetter: Warning and Decision, loc.cit., pp. 385

[54]. Michael Briggs, Charlie Edwards: The business of security has shifted from protecting companies from risks, to being the new source of competitive advantage. DEMOS 2006

[55]. NATO news article “Cyber defence”, February 17th 2017. Available: http://www.nato.int/cps/en/natohq/topics_78170.htm .

[56]. NATO-EU Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, July 8th 2016.

[57]. Europol, Common Taxonomy for Law Enforcement and the National Network of CSIRTs. Available: https://www.europol.europa.eu/publications-documents/common-taxonomy-for-national-network-of-csirts .

[58]. CBRN Crisis Management Architecture, Technologies and Operational procedures. Available: http://driver-project.eu/content/cato , http://www.cato-project.eu .

[59]. Platform for European Medical Support during major emergencies. Available: http://www.pulse-fp7.eu .

[60]. Critical Infrastructure Risk Assessment Support. Available: http://www.cirasproject.eu .

[61]. Sven Hamelink, Jaroen Mutsaers,CIP: From Protection to resilience, in CIIP Newsletter, Volume 9, Number 3 (issue22), October 2015.

[62]. Ted Koppel, Lights Out, Crown Publishing, New York, USA, 2015.

[63]. Commission of the European Communities, Green Paper on public-private partnerships and Community law on public contracts and concessions (presented by the Commission), COM(2004) 327 final, Brussels, 30.4.2004 .

[64]. Directive 2013/40/EU of the European Parliament and of the Council, of 12 August 2013,on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

[65]. 2012 PPP Law by Decree Law no. 111/2012, Ministry of Finance, Portugal, of 23 May 2012, in Diário da República, 1.ª série — N.º 100 — 23 de maio de 2012.

[66]. European Commission, "EU cybersecurity initiatives: working towards a more secure online environment" factsheet, January 18th 2017.

[67]. ISACA, COBIT 5 Implementation, Rolling Meadows, IL, USA, ISACA, 2012.

[68]. ISACA, COBIT 5 Enabling Processes, Rolling Meadows, IL, USA, ISACA, 2012.

[69]. ISACA, COBIT 5 Enabling Information, Rolling Meadows, IL, USA, ISACA, 2013.

[70]. ISACA, COBIT 5 for Information Security, Rolling Meadows, IL, USA, ISACA, 2012.

[71]. ISACA, COBIT 5 for Risk, Rolling Meadows, IL, USA, ISACA, 2013.

[72]. ISACA, COBIT 5 Process Assessment Model (PAM): Using COBIT 5, Rolling Meadows, IL, USA, ISACA, 2013.

[73]. ECOSSIAN Description of Work (DoW), European Control System Security Incident Analysis Network, FP7-SEC-2013-1, Grant agreement no: 607577, European Union's Seventh Framework Programme.

[74]. D1.1 State of the Art Report, ECOSSIAN Project deliverable, 2014.

[75]. D1.2 Requirements report, ECOSSIAN Project deliverable, 2015.

[76]. D1.3 General Architectural Framework, ECOSSIAN Project deliverable, 2015.

[77]. D1.4 Gap Analysis Report, ECOSSIAN Project deliverable, 2015.

[78]. D1.5 Use Case Scenario Report, ECOSSIAN Project deliverable, 2015.

[79]. D1.6 Security Methodologies, ECOSSIAN Project deliverable, 2015.

[80]. D1.7 Architecture Specifications, ECOSSIAN Project deliverable, 2015.

[81]. D2.1 Architectural Design of Secure Real-time Monitoring and Attack Detection, ECOSSIAN Project deliverable, 2016.

[82]. D2.2 Architectural Design of SOCs, ECOSSIAN Project deliverable, 2017.

[83]. D3.1 Study on Data Collection, Fusion and Sharing Mechanisms for Pan-European Cyber Defence, ECOSSIAN Project deliverable, 2015.

[84]. D3.2 Incident Information Sharing, Analysis, Correlation, and Visualization System Concept , ECOSSIAN Project deliverable, 2016.

[85]. D3.3 Incident Information Sharing, Analysis,Correlation, and Visualization System Implementation, ECOSSIAN Project deliverable, 2016.

[86]. D4.1 Continuity plan for ECOSSIAN infrastructure, ECOSSIAN Project deliverable, 2016.

[87]. D4.2 Threat mitigation and incident management in CI use cases of ECOSSIAN, ECOSSIAN Project deliverable, 2016.

[88]. D4.3 Cyber Forensics Toolset, ECOSSIAN Project deliverable, 2017.

[89]. D4.4 CI incident impacts and interdependencies, ECOSSIAN Project deliverable, 2017.

[90]. D5.1 Evaluation methodology, ECOSSIAN Project deliverable, 2016.

[91]. D5.2 Preliminary interface integration report, ECOSSIAN Project deliverable, 2016.

[92]. D5.3 Demonstration scenario definition, ECOSSIAN Project deliverable, 2016.

[93]. D5.4 Secure Gateways, ECOSSIAN Project deliverable, 2016.

[94]. D5.5 Integrated system prototype, ECOSSIAN Project deliverable, 2016.

[95]. D5.6 Integration test report, ECOSSIAN Project deliverable, 2017.

[96]. D5.7 Technical Scenarios Preparation Report, ECOSSIAN Project deliverable, 2017.

[97]. D5.8 Evaluation report and recommendations, ECOSSIAN Project deliverable, 2017.

[98]. D6.1 Demonstration support materials, ECOSSIAN Project deliverable, 2017.

[99]. D6.2 Demonstration speech, ECOSSIAN Project deliverable, 2017.

[100]. D6.3 Demonstrations, ECOSSIAN Project deliverable, 2017.

[101]. D6.4 Questionnaires, ECOSSIAN Project deliverable, 2017.

[102]. D7.1 Analysis of the applicable legal framework, ECOSSIAN Project deliverable, 2014.

[103]. D7.2 Legal requirements, ECOSSIAN Project deliverable, 2015.

[104]. D7.3 Information sharing policies in disaster situations - Version 1, ECOSSIAN Project deliverable, 2015.

[105]. D7.4 Report by External Ethical Advisor - Version 1, ECOSSIAN Project deliverable, 2015.

[106]. D7.5 Report by External Ethical Advisor - Version 2, ECOSSIAN Project deliverable, 2016.

[107]. D7.6 Legal evaluation of the ECOSSIAN system and recommendations, ECOSSIAN Project deliverable, 2017.

[108]. D7.7 Information sharing policies in disaster situations - Version 2, ECOSSIAN Project deliverable, 2017.

[109]. D7.8 Report by External Ethical Advisor - Version 2, ECOSSIAN Project deliverable, 2017.

[110]. D7.10 Partnerships: opportunities and constraints, ECOSSIAN Project deliverable, 2017.

[111]. D7.11 Societal and ethical impact analysis, ECOSSIAN Project deliverable, 2017.

[112]. D8.5 Exploitation and Standardization Plan, ECOSSIAN Project deliverable, 2016.

[113]. D8.6 Dissemination Report, ECOSSIAN Project deliverable, 2017.

[114]. D8.7 Exploitation and Standardization Report, ECOSSIAN Project deliverable, 2017.

[115]. D9.7 Compliance with Ethical Issues, ECOSSIAN Project deliverable, 2016.

[116]. European Commission. (2003). Guidelines for Successful Public-Private Partnerships.