The GFCE-MERIDIAN Good Practice Guide

on

Critical Information Infrastructure Protection

for governmental policy-makers

FOREWORD

Critical Information Infrastructure Protection (CIIP) is a complex but important topic for nations. Societies at large critically depend on the proper functioning of their Critical Infrastructure (CI) services such as energy supply, telecommunications, financial systems, drinking water, and governmental services. In turn, these CI often critically depend on the proper functioning of Critical Information Infrastructures (CII). CII comprises both the critical information and communication infrastructures (e.g. mobile telephony and internet services) and critical information and communication systems that are part of each of the CI. These include control systems that monitor and control critical cyber-physical processes (e.g. remote operation of oil pipeline valves) as well as administrative and logistic systems.

The need for CIIP is becoming increasingly prominent. The risk to society due to insufficient protection and measures increases by the day. As information and communication infrastructures become globally interwoven, a nation's CII may be a target for malware, hackers, hacktivists and adverse state operations. At the same time, the nation's CII can become a means for attacking other nation's CII. Via the threatened CII the proper and undisturbed functioning of the CI may be at risk and through that one's society, economy, and daily life could also be at risk. Moreover, the global interconnectivity of CII means that a vulnerable CII may become the weakest link and thereby a risk to the CII of all other nations of the world.

A number of nations are on the path of Critical Infrastructure Protection (CIP) but have difficulties in progressing with CIIP. Other nations are at the very start of their combined CIP - CIIP journey. A set of nations already progressed on that path and may have experienced pitfalls and developed good practices. In order to raise the protection barriers and to progress on the CIIP path, the Meridian Process and the Global Forum on Cyber Expertise (GFCE) jointly took the initiative to develop this good practices guide on CIIP for national CI and CII policy-makers. Moreover, these good practices may be of use to nationally and internationally operating CI operators. This guide is intended to assist nations which are at the very start of their journey, but also nations whose journeys are underway. We realise that each nation has a different legal and regulatory structure, a different style of governance over CI and CII, a different adaptation level of information and communication technologies (ICT), a different culture, and so on. These good practices are not chiselled in stone. They are meant to inspire the reader. In the application of a good practice, there may be a need to tune the approach to fit each national need.

We hope that these good practices may be of help on the CI/CII protection and resilience journey, and it may be helpful to note that other nations which are further down their own path may also be able to offer help.
On behalf of the writing team, and with cooperation of Mr. Peter Burnett (Meridian Coordinator) and Mrs. Nynke Stegink (Dutch National Cyber Security Centre),

Eric Luiijf

CONTENTS

FIGURES

TABLES

1 INTRODUCTION

1.1 THE NEED FOR CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

Critical Information Infrastructure Protection (CIIP) is a complex but important topic for nations. Nations at large critically depend on Critical Infrastructure (CI) services such as energy supply, telecommunications, financial systems, drinking water, and governmental services. Critical Infrastructures (CI) are defined as: *"Those infrastructures which are essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have serious consequences"* [EC2008].

Today, the physical disruption (or even destruction) of critical elements of CI is not the only factor threatening the correct operation of CI. Information and communication technologies (ICT)-based services are becoming increasingly important for the functioning of CI. Disruption of information infrastructure is capable of causing major impact to a nation. This leads to the concept of Critical Information Infrastructure (CII) which comprises both *critical* information and (tele)communication infrastructure (e.g. mobile telephony and internet access services) and ICT and process control systems that are a *critical* part of the CI service provisioning (see Figure 1).

Disruption of CII can be caused by man-made, technical failures and disasters just as is the case with CI. The benefits of CII however (increased connectivity, remote monitoring, scalability, reliability, cost-reduction) are not always equally balanced with the possible adverse effects of malfunction of CII. CII is increasingly a critical part of CI, is the 'glue' between and within CI, and is becoming globally interconnected. At the same time, a nation's CII may be both a target for malware, hackers, hacktivists, and adverse state operations, and a means for attacking other nation's CII. A compromised or disturbed CII can jeopardise national security and stability, economic growth, citizen prosperity, and daily life, and may have far-reaching impact on other nations due to the global interconnectedness of CII. The need for effective CIIP strategies, policies and activities therefore becomes increasingly important in most nations.

1.2 PURPOSE OF THIS GOOD PRACTICE GUIDE

A number of nations are on the path of Critical Infrastructure Protection (CIP)[1] but have difficulties in progressing with CIIP. Other nations are at the very start of their combined CIP-CIIP journey. However, there are also ample examples of nations that have taken great steps in CIIP development. Their experiences, bad and good, are worth sharing. Therefore, the Meridian Process and the Global Forum on Cyber Expertise (GFCE) have taken the initiative to develop a good practices guide on CIIP development, and provide those valuable insights to nations that are in an early phase of CIIP development. This guide is primarily aimed at governmental CI and CII policy-makers, but can be of use to nationally and internationally operating CI operators as well.

1 Critical Infrastructure Protection: *"All activities aimed at ensuring the functionality, continuity and integrity of CI in order to deter, mitigate and neutralise a threat, risk or vulnerability."* [EC2008]

There are many differences between nations. Differences in cultural, legal and regulatory structures, different styles of governance over CI and CII, different political cultures, a different adaptation level of information and communication technologies (ICT), as well as other differences. The good practices described in this guide are therefore to be used in a flexible manner. They may inspire governmental CI and CII policy-makers and expedite the creation of tailored 'fit for purpose' strategies and plans while skipping approaches that have turned out to have failed elsewhere. As a nation you are not on your own as CIIP is a global issue for all nations. One may use these good practices and ask other nations about how they approach CIIP, for instance though the Meridian Process and the Global Forum on Cyber Expertise (GFCE) communities, and learn from them.

These good practices are a companion to the earlier *"Good Practices Manual for CIP Policies for policy makers in Europe"* [RECIPE]. A number of good practices from that manual are reused in the context of CIIP.

1.3 CII, CIIP AND CYBER SECURITY

Although the notion of CII was coined around 2001 (see e.g. [Bruno2002]) and not much later by the G8 [G8] and the Organisation for Economic Co-operation and Development [OECD2007, OECD2008], no widely agreed definition yet exists. A number of nations have defined their CII. Some CII example definitions from around the world are: *"Critical Cyber/ICT Infrastructure means the cyber infrastructure that is essential to vital services for public safety, economic stability, national security, international stability and for the sustainability and restoration of critical cyberspace"* [African Union], *"The ICT component of Critical Infrastructure is referred to as Critical Information Infrastructure (CII)"* [Victoria], *"Critical information Infrastructures are the subset of information assets that directly affect the achievement and continuity of state mission and the safety of society"* [Brazil], *"Critical information infrastructure (CII) may refer to any IT systems which support key assets and services within the national infrastructure"* [UK].

Based upon the set of national definitions and our understanding (see Figure 1), we developed an overarching definition of Critical Information Infrastructure which reflects the need to consider both ICT as a CI alone and the cross-CI sector aspect due to the use of the same technologies and therefore risk in most critical processes in the CI sectors:

Critical Information Infrastructure (CII): *"Those interconnected information and communication infrastructures which are essential for the maintenance of vital societal functions, (health, safety, security, economic or social well-being of people) – the disruption or destruction of which would have serious consequence"*.

Critical Information Infrastructure Protection (CIIP) is a derivative of this CII definition, and is defined as: *"All activities aimed at ensuring the functionality, continuity and integrity of CII in order to deter, mitigate and neutralise a threat, risk or vulnerability or minimise the impact of an incident"*.

There are many different definitions of the concepts discussed in this good practices guide. One may find an extensive set of national and international definitions in various languages for these notions at [CIPedia©]. In the end, however, national differences in definitions should not distract from the need for CIIP; only when making detailed arrangements with other nations, do the fine-grained differences in definitions and understandings need to be clear.

As depicted in Figure 1, the CII comprises both the CI '*information and communication critical infrastructure*' (e.g. mobile telecommunication services, internet exchange points (IXP), domain name services), and the *critical* information and communication infrastructure within each of the CI, such as critical cyber-physical systems and key administrative systems.

Cyber-physical systems are the combination of control systems that monitor and control critical physical processes for instance by remotely changing a gas or fluid flow rate through valves, starting an engine, and switch high-voltage power.[2] Examples of CII are the process control systems that monitor and control the generation of electrical power, a Global Navigation Satellite System (e.g., BeiDou, Galileo, GLONASS, GPS), the information services between banks to settle accounts, and access infrastructure to reach and use global internet services.

CI benefits from the integration with ICT for reasons of increased flexibility in business operations such as monitoring, remote access (maintenance, monitoring, and operations), integration in corporate ICT, and process adaptability [Luiijf2015]. It is essential to be aware of new dependencies and vulnerabilities in critical CI functions because of globally interconnected ICT, e.g. the use of internet, and ICT-based technologies in the monitoring and control of critical physical processes (also known as cyber-physical systems). This is a significant underpinning of CII.

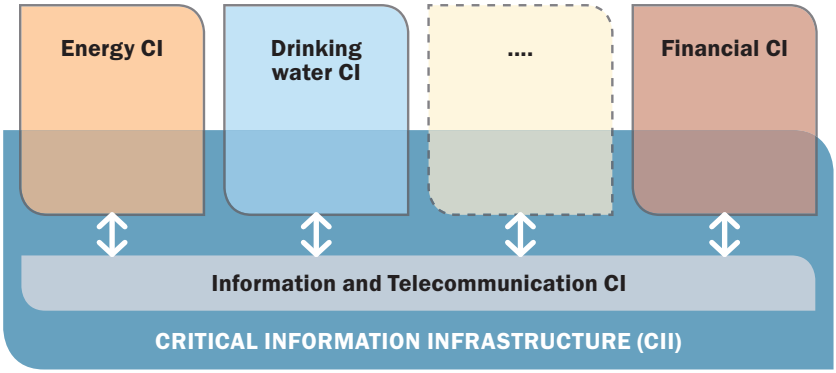

Figure 1. Relationship between Critical Information Infrastructures and Critical Infrastructures.

2 Cyber-physical systems (CPS) are defined as: *"A cyber-physical system is defined as ICT and computer systems supporting, managing and supervising physical assets"*. [ITNCS]

Cyber Security and cyber security strategies are terms that are most often not far away in media, policy documents and action plans when the topic is about infrastructure and ICT. The terms play a role with regard to CI and CIIP, but (national) interpretations differ. To gain insight and to compare, a large variety of national definitions for cyber security can be found under 'Cyber Security' in the A-Z list on the landing page of [CIPedia©][3]. In this guide, we will use the [ITU] definition:

Cyber Security: *"Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets"*.

CIIP is a vital element of cyber security and is therefore often mentioned or written about in relation to cyber security, especially with regard to National Cyber Security Strategies (NCSS) and National Cyber Security Centres (NCSC). In [Luiijf2013] the NCSS of 18 nations were analysed. Although nations aim to tackle the similar cyber security threats, there is large difference in their chosen foci and approaches. The first identified difference between the strategies is definition and scoping. Merely 44%, less than half of the nations, actually defined the notion of cyber security in their strategy; the remainder relied on descriptive text (11%) or a definition of information security (11%), or did not define the term at all (33%). The nations that did define the notion of cyber security often had a very different understanding of the concept. The way in which the definition was created also differed between nations.

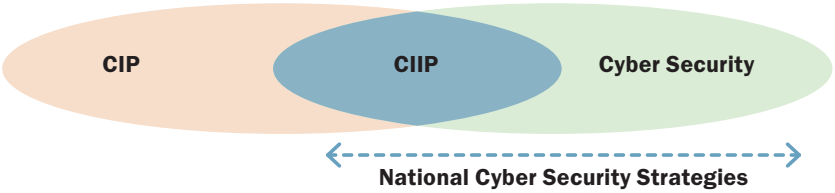

Figure 2. Relationship and coverage between CIP, CIIP, and cyber security.

The blue arrow under the elements in Figure 2 reflects the range of NCSS worldwide. Some strategies have been written from a cyber-crime perspective only or an internet-only perspective. They tend to overlook (national) disruption and crisis management for CII as well as cross-sectoral impacts. Strategies written from cyber security perspective based on a national risk assessment will adopt a broader perspective that will give room for CIP and CIIP.

NCSS with broad perspectives typically also include economic growth and freedom. Such a perspective prescribes the relations with other important stakeholders such as law enforcement agencies, other ministries and with important key private stakeholders in the CI and CII.

3 CIPedia© is a common international reference point for CIP and CIIP concepts and definitions.

Adopting a broad approach in a NCSS might sound straightforward, but a 2016 CIIP study for Latin America and the Caribbean found otherwise [Zaballos]. This study found that in general CIP-related legislation had a low level of adoption and that CIIP strategies or regulations were not present. In the cases where CIIP initiatives were found, they were mainly found because of experiences of emergency situations. Approaches to CI and CII were present in the nations studied, but identified as unsystematic and with gaps.

CIIP is thus a vital kernel of NCSS, but is not equal to cyber security and excludes ordinary cybercrime, privacy and human rights issues, and economic cyberspace matters.

For example, if CIIP were to be presented as a standalone document, its technological focus might only prescribe information security standards and safety principles, guidelines for risk management, and some sort of first response emergency planning. Such a document does not address crucial elements of regarding governance, legislation, stakeholders, incentives, regulation, and CI/CII communities.

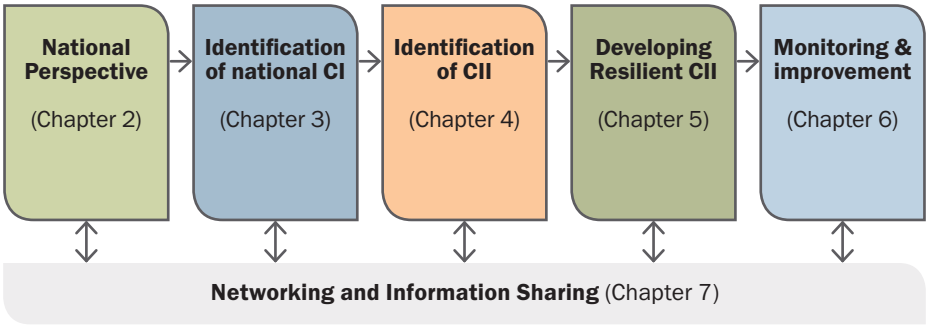

Figure 3. Visual outline of this guide.

1.4 HOW TO USE THIS GOOD PRACTICE GUIDE?

Critical information infrastructure protection is a process which follows a set of main steps underpinned by close collaboration and interactions with all relevant stakeholders. The steps shown in Figure 3 reflect the structure of this good practices guide. The networking and information sharing aspects and related good practice are described in Chapter 7. The networking and information sharing aspects of CIIP have to grow from the beginning onwards. The earlier one starts, the more commitment and collaboration is received in later stages.

We suggest starting with the national perspective. What is the primary reason to work on CIIP? What is the balance with all other policy and political issues a nation is facing? A national risk assessment and profile approach may be a possible help, as is described in Section 2.1.1. As one cannot really start with CIIP without understanding what one's CI looks like, a short set of steps and supporting good practices and reference material are provided in Chapter 3 on the Identification of National Critical Infrastructure. Only after identifying the

CI can one start identifying one's CII. This is a complex task, as CII covers two focus areas: one of critical information and (tele)communication CI; and one of ICT embedded within the CI itself. Chapter 4 on the Identification of Critical Information Infrastructure describes the process steps and related good practices. The next step is towards adequately protecting the CII in balance with the risk, as outlined in Chapter 5 on Developing Critical Information Infrastructure Protection (CIIP). Chapter 6 is describes continuous Monitoring and continuous improvement when needed, e.g. because of a revised risk assessment or major technology changes. Each of these chapters contains a good practices section and a section with literature references and pointers for further reading.

This guide is intended to be accessible to all governmental CIIP policymakers irrespective of such differences. However, these good practices may require adjustments to local national needs.

Moreover, not all good practices are suitable for implementation by every nation. Like the [RECIPE] good practice manual on CIP, it is the reader who creates the national CIIP policies, action plans, collaboration of all relevant stakeholders, and stimulates activities.

1.5 REFERENCES AND FURTHER READING

[African Union] African Union, African Union Convention on Cyber Security and Personal Data Protection, LC12490, 27th June 2014. On-line: http://pages.au.int/sites/default/files/en_AU%20Convention%20on%20CyberSecurity%20Pers%20Data%20Protec%20AUCyC%20adopted%20Malabo.pdf

[Brazil] GUIA DE REFERÊNCIA PARA A SEGURANÇA DAS INFRAESTRUTURAS CRÍTICAS DA INFORMAÇÃO Versão 01 (Nov. 2010)/ Portaria Nº 34, de 5 de agosto de 2009. Conselho de Defesa Nacional, Secretaria Executiva, 2009. On-line: http://dsic.planalto.gov.br/documentos/publicacoes/2_Guia_SICI.pdf

[Bruno2002] S. Bruno and M. Dunn, Critical Information Infrastructure Protection: An Inventory of Protection Policies in Eight Countries, ETH, Zürich, Switzerland, 2002. On-line: http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP_Handbook_2002.pdf

[CIPedia©] CIPedia©: a common international reference point for CIP and CIIP concepts and definitions. On-line: http://www.cipedia.eu and https://publicwiki-01.fraunhofer.de/CIPedia/index.php/CIPedia%C2%A9_Main_Page

[EC2008] European Council, 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 (Text with EEA relevance). On-line: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008L0114

[G8] G8, G8 Principles for Protecting Critical Information Infrastructures, 2003. On-line: http://www.cybersecuritycooperation.org/documents/G8_CIIP_Principles.pdf

[GFCE] Global Forum on Cyber Expertise website, https://www.thegfce.com

[ITNCS] Presidency of the Council of Ministers, National strategic framework for cyberspace security, Rome, Italy (December 2013). On line: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf

[ITU] ITU Security in Telecommunications and Information Technology: An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications, ITU-T, Geneva (2012) - ITU-T X.1205. On-line: http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

[Luiijf2013] H.A.M. Luiijf, K. Besseling, P. de Graaf, Nineteen National Cyber Security Strategies, International Journal on Critical Infrastructures (IJCIS), V9 N1/2, 2013, pp.3-31.

[Luiijf2015] H.A.M. Luiijf, B-J. te Paske, GCCS: Cyber Security of Industrial Control Systems, TNO, 2015. On line: http://publications.tno.nl/publication/34616507/KkrxeU/luiijf-2015-cyber.pdf

[Meridian] Meridian Process website, https://www.meridianprocess.org

[OECD2007] OECD Working Party on Information Security and Privacy, Development of Policies for Protection of Critical Information Infrastructures: Ministerial Background Report DSTI/ICCP/REG(2007)20/FINAL, OECD, 2007. On-line: http://www.oecd.org/sti/40761118.pdf

[OECD2008] OECD ICCP Committee and the Working Party on Information Security and Privacy, OECD Recommendation on the Protection of Critical Information Infrastructures [C(2008)35], 2008, OECD. On-line: http://www.oecd.org/sti/40825404.pdf

[RECIPE] M. Klaver, E. Luiijf, A. Nieuwenhuijs, Good Practices Manual for CIP Policies for policy makers in Europe, TNO, 2011. On line: http://www.tno.nl/recipereport

[UK] Cyber Security in the UK, Postnote Number 389, September 201. On-line: http://www.parliament.uk/documents/post/postpn389_cyber-security-in-the-UK.pdf

[Victoria] Victorian Government CIO Council, Critical Information Infrastructure Risk Management, Victoria, Australia, 2012. On-line: http://www.digital.vic.gov.au/wp-content/uploads/2014/07/SEC-STD-02-Critical-Information-Infrastructure-Risk-Management1.pdf

[Zaballos2016] A.G. Zaballos and I. Jeun, Best Practices for Critical Information Infrastructure Protection (CIIP): Experiences from Latin America and the Caribbean and Selected Countries, 2016. On-line: https://publications.iadb.org/handle/11319/7848

2 NATIONAL PERSPECTIVE

There is no single CIIP strategy that suits every nation. The nature of the process to CIIP depends upon a nation's risk profile and the need and ability to mitigate risk. The ability but also the responsibilities to mitigate risk depend on the capabilities of the stakeholders involved in CIIP, and the capabilities that a nation has at its disposal, to make the CII stakeholders work in a collaborative way towards desired levels of CIIP. This approach aligns with the basic principles for CIIP stated in [NISC.JP2014].

2.1 GENERAL DESCRIPTION AND MAIN CHALLENGES

2.1.1 START DEVELOPING A NATIONAL RISK PROFILE REGARDING FAILURE OF CI/CII

Protection of CI and CII may start with the development of a risk profile of a nation as a whole. The primary intent of a national risk profile is to establish a common national understanding of the risk factors that a nation faces through systematic assessment of the threats towards a nation and its vulnerabilities (impact and frequency). The result of a risk assessment is an overview of risk factors and their relative positions with respect to impact and frequency of occurrence. Each risk that is addressed in a national risk profile may form the basis of an integrated national approach to risk prevention, preparedness and response. Considering the CI and CII related risk in the context of a nation's risk profile may help to develop an integrated and balanced risk management approach underpinning CIIP.

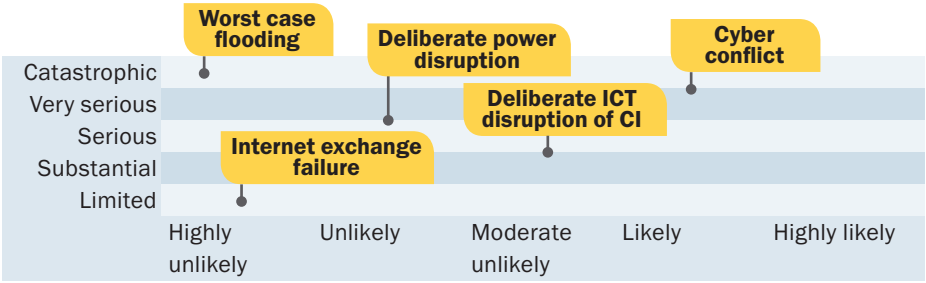

Figure 4. A risk profile example (derived from [NLNRA2014]).

The systematic assessment of the threats implies that all threats are assessed on basis of their impact and likelihood of occurrence using the same set of metrics. Moreover, not only current hazards, malicious and non-malicious, can be assessed including the shift in threats and impacts due to for instance climate change and geopolitical developments.
Developing a national risk profile subset for CI and CII is a challenging task for which we provide a few guidelines in Section 2.2.1. We strongly recommend stakeholder involvement from the very beginning of the development of a national risk profile since risk assessment is not a purely rational process and stakeholder acceptance is vital. In practice, nations that develop a national risk profile for the first time may consider concentrating on the most important risk scenarios and including other scenarios in a second stage or in later stages.

Table 1. A non-exhaustive listing of CII stakeholders.

- CIIP coordinating ministries, e.g. Interior, Justice, Defence, Prime Minister's Office
- Ministries responsible for ICT, e.g. Communications, Media, ICT departments
- Ministries responsible for specific CI, e.g. Economic Affairs, Energy, Health departments
- Regulators for specific CI Domains
- Law enforcement and other public agencies
- CI and CII operators / utilities
- Politicians and Parliament
- Manufacturers, system integrators, and 3rd party maintenance companies
- Cross-sector (branch) organisations
- Computer Security Incident Response Teams (CSIRT)
- National Cyber Security Centre
- Academics and Research and Development ('Triple Helix')

2.1.2 START IDENTIFYING STAKEHOLDERS

Protection of CI and CII requires insight into the governance and ownership structure of a nation's CI and CII and the type of stakeholders (see inset) that are involved. This means that the stakeholders have to be categorised as public, semi-public or private, and as regionally, nationally or internationally operating. There are many methods and tools available for stakeholder analysis, e.g. [Mitchell1997] and [Yang2011], but a basic approach suffices to gain a general understanding of the sort of stakeholders involved in CI and CII. In many nations, a diverse mix of stakeholders will need to be involved in CIIP. Table 2 may be useful to create a first set of relevant CI and CII stakeholders.

Table 2. Table to assist in stakeholder analysis. (some examples)

	Public	**Semi-public**	**Private**
International	OECD		Multinational software vendor, SCADA manufacturer
National	Municipal utility	National gas transport services	Telephony provider; Internet service provider; national internet exchange
Regional	Air Traffic Control	Coastal pilot services	Internet exchange

2.1.3 IDENTIFYING POLICY OPTIONS

National authorities may consider a broad range of policy options to enhance CIIP. Which policy options are fit-for-purpose depends on many factors including the type of threats a nation and its CII faces, the type of stakeholders involved in the protection of the CII and the history and culture of public policy in the nation. Policy options range from:

- self-regulation;
- voluntary compliance;
- voluntary government programmes;
- market mechanisms and incentives;
- legal and regulatory frameworks.

Whether a nation makes use of voluntary programmes, incentives ('carrots and sticks') or regulatory and legal frameworks depends on the type of stakeholders involved in CII, its culture, established practices, goals and ambitions with regard to CIIP. Many nations have adopted a risk and responsibility driven approach that sets baselines for CIIP and leaves the details of how to protect CII to more technologically advanced CI/CII operators. When multinationals operate part(s) of CII, one should take into account arrangements they have made in other nations.

Nations should realise that situations in which part(s) of CII are operated by multinationals present specific opportunities and challenges. On the one hand, nations can benefit from the CIIP experiences multinationals had in other nations. On the other hand, it can also be more difficult to influence multinationals to alter their CIIP activities in one's nation because of the arrangements they have made with other nations and the resulting need for cross-border cooperation and uniform internal processes.

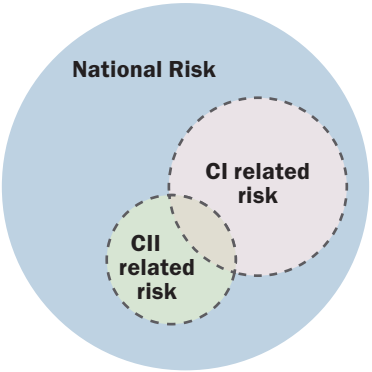

Figure 5. CII risk within the context of national risk.

To support these challenges, the following good practices are described in the next section:
- Develop a national risk profile.
- The CII challenges for developing nations.
- Building public-private partnerships as a policy option.
- Adopt a multi-agency approach and start information exchanges.

2.2 GOOD PRACTICES REGARDING THE NATIONAL PERSPECTIVE

2.2.1 GOOD PRACTICE: DEVELOP A NATIONAL RISK PROFILE

Developing effective CIIP policies starts with the development of a nation's risk profile and understanding of the consequences of failure of CI and CII. We therefore recommend nations to develop a National Risk Profile that includes the risk of failure of CI and CII. Developing a National Risk Profile is a substantial and challenging task and the scope of this good practice guide does not allow us to go into detail about the processes involved. The EU Risk Management Capability Assessment Guidelines [EC2015] may support national authorities

that aim to develop a National Risk Profile. The purpose of this Guideline is to provide nations with a comprehensive and flexible methodology that fosters understanding of the elements required for a national risk assessment and the development of a National Risk Profile including the determination of what comprises their CI and CII.

The EU Guidelines include topics like the selection of a risk assessment framework, coordinating the risk assessment, involving the right stakeholders and expertise, applying the right methodology and ICT tooling, and planning and financing the risk assessment. For each topic, a set of questions that helps to develop the risk management capability is provided. We further recommend the National-level Risk Assessments analysis report from ENISA that provides guidelines and good practices on developing a national risk profile [ENISA2013].

Finland's National Risk Assessment 2015 [Finland2015] provides an example of how the failure of CI and CII can be incorporated into a national risk profile, and makes a distinction between wide ranging events affecting society and serious regional incidents. Disruption of CII is considered under the risk factors in the cyber domain that are grouped under the wide ranging events affecting society. The NRA describes how disruption of CII causes disruption of CI and other vital processes in society that may result in material damage and the loss of life. Some other national risk assessments are [Cabinet2010], [DSB02014], [NLNRA2009], and [MSB2012].

2.2.2 GOOD PRACTICE: THE CII CHALLENGES FOR DEVELOPING NATIONS

During workshops organised by the Commonwealth Telecommunication Organisation on CIIP in 2015, a set of challenges for CIIP has been mentioned [CTO]:

1. Cost and lack of financial investment: funds required to establish a CIIP strategic framework can be a hindrance as well as limited human and institutional resources.
2. Technical complexity in deploying CIIP: one needs to understand dependencies and vulnerabilities *(Section 3.2.3 of this document may be of help)*.
3. Limited knowledge on how to identify and classify CI: need to consider business value, scope of population and technical dependencies *(Chapter 3 of this document may be of help)*.
4. Need for cyber security education and culture re-think: create awareness on importance of cyber security and CIIP as well as create a cyber security culture that can promote trust and confidence.
5. Lack of relevant CIIP strategies, policies and framework *(these good practices and its references may be of help)*.
6. Lack of information sharing and knowledge transfer *(Chapter 7 and [Luiijf2015] may be of help)*.

These CII challenges and lessons learned are at least to be acknowledged during one's national CIIP development. If CI and CII in one's nation have been privatised, challenges such as the ones stated above can be managed by working with private partners by establishing form of public-private partnership (PPP), see next section and Chapter 7.

2.2.3 GOOD PRACTICE: BUILDING PUBLIC-PRIVATE PARTNERSHIPS AS A POLICY OPTION

The protection of CI/CII is part of the national security of many nations but most cyber security-related decisions are made by the CII operators. To make sure that the individual CII stakeholders take the national security risk of CII failure into account during their decision-making, cooperation between national authorities and CII operators is often necessary. When CII is operated by private stakeholders, such cooperation may require the establishment of public-private partnerships (PPP). With PPP we mean *collaboration between a government agency and private entities with, in the case of CIP/CIIP, the purpose of ensuring the correct functioning of the CII services*. PPP is about the mind-set how one approaches relations, responsibilities, and cooperation with their stakeholders regardless whether they are public or private. The same mind-set can be used when CI and CII are operated by public entities.

When a nation's CII is privately owned and operated, it is important that public, semi-public and private CII operators work together in a co-ordinated way in the protection of CII. It should be realised that PPP in CIIP can be much more than a delegation of public tasks to private stakeholders. A broader concept of collaboration embraces the pooling of resources, mutual support, and joint decision-making. PPP do not only involve contracting-out schemes but also inter-organisational networks of collaboration. PPP specifics and good practices can be found in Chapter 7.

To involve private stakeholders, the government may provide reliable expert knowledge on infrastructure and CIP/CIIP to public and private stakeholders. The added value for the private partners is rooted in the fact that the government independently visits many companies, and reaches an all-encompassing view of the protection status of an infrastructure sector or multiple sectors. When an overview of the cyber security posture is combined with threat information from intelligence, this can be translated into operational information that can be acted upon. In this way the government can become a valued partner for CI operators.

2.2.4 GOOD PRACTICE: ADOPT A MULTI-AGENCY APPROACH AND START INFORMATION SHARING

Addressing the risk to CII and the related complexity of CIIP effectively requires a multi-agency approach by the government at strategic, tactical and operational/technical levels. Stakeholders such as ministries (e.g. Communications, ICT, Economic Affairs, Security, Cabinet Office, Justice, and Defence), regional public bodies, agencies, or regulators have to collaborate on the challenges both at the strategic, tactical, and operational/technical levels. It is important to first establish an optimal setting with all public stakeholders to address the CI and CIIP challenges at the strategic level. This might take the form of regular round-table meetings. The strategic objectives should ideally drive subsequent requirements such as legal mandates, and a governance and organisation structure as well as collaborations at the tactical and operational/technical levels. At the tactical and operational levels, one should consider cooperation with operational services in the national security, defence, and police involved in the CI and cyber domain. At the technical level, a national Computer Security Emergency Response Team will usually have a role in CIIP (see Section 5.2.2).

Even when certain public bodies are designated (and thus responsible) for the CI and CII identification and CIIP process, one should realise that a wider community of public stakeholders may be directly and indirectly involved in CIIP planning and execution. After initial alignment between all public stakeholders, the CII operators and other key stakeholders from private industry, chambers of commerce, academics and research & development, and others have to be brought around the table to jointly address the CIIP challenges.

Public bodies can stimulate or facilitate information sharing between CIIP stakeholders [Luiijf2015]. If favourable conditions for information sharing are established for CIIP stakeholders, public and private organisations such as governmental security organisations, CII operators, key manufacturers, system integrators, and third party maintenance parties might start sharing information on CIIP topics. The participation of public stakeholders may influence the willingness of private stakeholders to share information. More on building collaboration networks and information sharing can be found in Chapter 7 on Networking and information sharing.

2.3 REFERENCES AND FURTHER READING

[Cabinet2010] Cabinet Office, Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure from Natural Hazards, March 2010. On-line: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62504/strategic-framework.pdf

[CTO] Commonwealth Telecommunication Organisation, Critical Information Infrastructure Protection (CIIP) workshops, 2015. On-line: http://www.slideshare.net/CandiceTang1/cto-ciipgaborone-workshoppresentationfinal18mar2015compressed

[Denmark2013] Danish Emergency Management Agency, National Risk Profile (NRP), April 2013. On-line: https://brs.dk/viden/publikationer/Documents/National_Risk_Profile_(NRP)_-_English-language_version.pdf

[DSB2014] National Risk Analysis 2014: Disasters that may affect Norwegian Society, Norwegian Directorate for Civil Protection (DSB), 2014. On-line: https://www.dsb.no/globalassets/dokumenter/rapporter/nrb_2014_english.pdf

[EC2015] European Commission, Commission Notice: Risk Management Capability Assessment Guidelines (2015/C 261/03). On line: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015XC0808(01)

[ENISA2013] ENISA, National-level Risk Assessments: An analysis report (2013). On-line: https://www.enisa.europa.eu/publications/nlra-analysis-report

[Finland2015] Ministry of the Interior, Finland, National Risk Assessment 2015, Ministry of the Interior Publication 4/2016. On-line: https://www.intermin.fi/download/65647_julkaisu_042016.pdf

[Klimburg2012] Klimburg, National Cyber Security Framework Manual, NATO CCD-COE Publications, December 2012. On-line: https://ccdcoe.org/publications/books/-NationalCyberSecurityFrameworkManual.pdf

[Luiijf2015] Luiijf, H.A.M., Kernkamp, A., GCCS: Sharing Cyber Security Information, TNO, 2015. On line: http://publications.tno.nl/publication/34616508/oLyfG9/luiijf-2015-sharing.pdf

[Mitchel1997] Mitchell, R. K., Agle, B. R., & Wood, D. J. (1997). Toward a theory of stakeholder identification and salience: Defining the principle of who and what really counts. Academy of management review, 22(4), 853-886.

[MSB2012] Swedish National Risk Assessment 2012, Swedish Civil Contingencies Agency (MSB), Sweden, 2012. On-line: https://www.msb.se/RibData/Filer/pdf/26621.pdf

[NISC.JP2014] The Basic Policy of Critical Information Infrastructure Protection (3rd Edition) – tentative translation, Japan, 2014. On-line: http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3.pdf

[NLNRA2009] Ministry of the Interior and Kingdom Relations, Working with scenarios, risk assessment and capabilities in the National Safety and Security Strategy of the Netherlands, The Hague, The Netherlands, October 2009. On-line: http://www.preventionweb.net/files/26422_guidancemethodologynationalsafetyan.pdf

[NLNRA2014] Analistennetwerk Nationale Veiligheid, M. G. Mennen (ed), Nationale Risicobeoordeling 6, Rijksinstituut voor Volksgezondheid en Milieu (RIVM), 2014. On-line: https://www.nctv.nl/binaries/nat.risicobeoordeling-6-definitief_tcm31-32706.pdf

[Yang2011] Yang, J., Shen, G. Q., Bourne, L., Ho, C. M. F., & Xue, X. (2011). A typology of operational approaches for stakeholder analysis and engagement. Construction management and economics, 29(2), 145-162.

3 IDENTIFICATION OF NATIONAL CRITICAL INFRASTRUCTURE

3.1 GENERAL DESCRIPTION AND MAIN CHALLENGES

3.1.1 THE NEED TO IDENTIFY CI

When comparing the sets of CI sectors of different nations, one may find a similar base set of CI but also major differences. A particular infrastructure might be of vital importance to one nation, but not to another nation. Thus, interpretations of nations differ with regard to what is considered to be included in their national CI. A clear example and comparison of differences and related discussions between a group of nations is found in [PSC2014]: *"[…] there have been significant shifts in the global security environment that have caused each of the members to approach infrastructure security and resilience in new ways"*. [Mattioli2015; table 1] came to the same conclusion when comparing the CI sector sets of 17 EU nations.

From the definition of CI in Section 1.3, it is clear that nations have a responsibility to identify their CI and to take actions to properly protect these CI. On top of that, pressure for CIP activities can come from different places. From an international perspective, regional initiatives and networks of nations (e.g. African Union (AU), Organization of American States (OAS)), networks of CII providers (e.g., Commonwealth Telecommunications Organisation [CTO]), as well as international organisations (World Bank, G8, ITU, NATO, OECD), may recommend or even pressure nations to give (more) attention to CI and CII. The need for CIP activities may also be the result of a national risk assessment (see Section 2.1.1) that gives a nation insight into the importance of and risk to infrastructures and information infrastructures. Insight into the criticality of infrastructure and information infrastructure might also come to the surface unexpectedly. Infrastructure could suddenly start to malfunction which might lead to disruption with a serious societal and/or economic impact. Such an unforeseen event might trigger public and private stakeholders to consider or reconsider the criticality of that infrastructure.

Traditionally, CI operations such as power, gas, postal and telecommunication services were public services operated by the government, public agencies, states/provinces, or municipalities. In many nations, liberalisation and privatisation took place for many CI services, meaning that semi-public and private organisations are now responsible for and operate the 'utilities' and provide their infrastructure services. With such privatisation, the security and safety of supply of these critical services largely lies with the semi-public and private industry.

The first step in CIP is the actual identification of criticality of national infrastructure. Different nations have different understandings of what is critical to their nation. This good practice guide therefore does not mention numbers and strict indicators but a general overview of the possibilities in how to approach this process.

Irrespective of the national governance structure and policy options, the early involvement of public authorities, semi-public and/or private infrastructure operators in this identification process is important. Depending on the type of governance of infrastructures influences the process of identification of CI, see [RECIPE] and Section 3.1.2 on 'Start identifying CI sectors'.

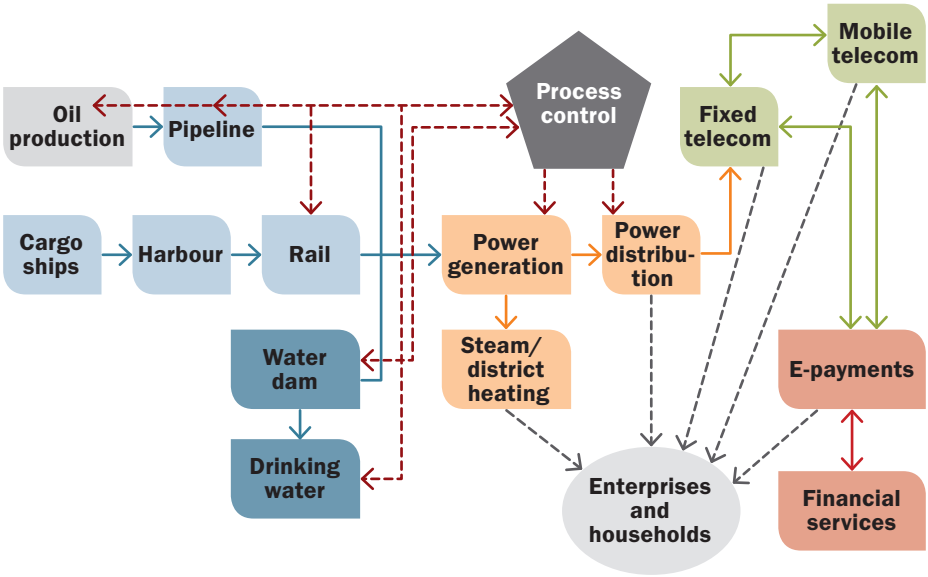

Figure 6. Example of dependencies and process control.

3.1.2 START IDENTIFYING CI SECTORS

Public, semi-public and private CI operators provide goods and services. It is the sort of goods and services provided by these operators and the type of use by their customers that determines whether an infrastructure service is critical. Table 3 provides examples of CI sectors and their services. More examples from critical services can be found under the entry 'Critical Infrastructure Sector' in the A-Z list on the landing page of [CIPedia©] and [Mattioli2015; table 1].

Table 3. Examples of CI sectors and services.

Sector	Services
Communications	Fixed, Mobile, Satellite communications, Navigation
Energy	Electricity, Oil, Gas, District heating
Health	Hospitals, Medicine
Transport	Air, Rail, Road, Inland Shipping, Ocean and short-sea shipping and ports
Water	Drinking water, Wastewater/Sewage
...	

Established approaches by other nations can be followed to identify one's CI can be followed. However, one may use a short-cut approach. Three steps are only briefly mentioned here and will be outlined later in the good practices in Section 3.2.2:

1. The bottom-up approach is to start looking at the sets of sectors and services defined as critical by other nations. One may start to look at other nations in the world that are similar in societal, geographical, and technical development structure (see Section 3.2.1). This results in a list of infrastructure operators of these services.
   A next step would be to define the feeling about 'criticality' of the infrastructures identified as potentially critical, from the set of avoidable impacts mentioned in the CI definition. Applying the criticality criteria onto this mix of stakeholders, sectors and services will bring an 80 to 90 percent completeness of the set of CI sectors and services.
   It is important to understand that when a certain sector is designated as a CI, this does not mean that all underlying services are critical. For example, in the critical energy sector, for instance, a 'district heating service' does not need to be designated as critical at national level, whereas the delivery of electrical power is.
   Two pathways exist after having established a completeness of 80 to 90%. The first pathway is to start Identifying the CII (Chapter 5). The other pathway is to identify all relevant stakeholders such as CI operators within this provisional set of CI sectors and CI services (see Chapter 7). Thereafter, collaboratively refine the set of critical sectors and services by analysing CI dependencies (Section 3.2.3).
2. A second approach is to do an analytical study using a methodology that contains a simple set of criteria and/or metrics. Various other nations have already performed evaluations of their national set of CI [CIPedia©]. These evaluations and their methods are probably not directly applicable without taking account of national differences and specifics. However, they provide an excellent and useful insight into the range of approaches of identification of CI one may use for analysing one's own national set of CI.
3. The third approach is to define fine-grained metrics first, which requires more maturity in CIP assessment. Thereafter, using the method outlined in Good Practice 3.2.2, one can determine whether an infrastructure or infrastructure service should be designated as critical or not. It must be noted that this approach was tried by several nations already. They found that defining metrics is not an easy task.

3.2 GOOD PRACTICES FOR THE IDENTIFICATION OF NATIONAL CRITICAL INFRASTRUCTURE

This section will provide you with good practices for the identification of CI sectors and services:

- adopt definitions of CI sectors and services from other nations;
- adopt a methodology to identify CI sectors and services systematically;
- (national and cross-border) dependency analysis.

3.2.1 GOOD PRACTICE: GRASP DEFINITIONS OF CI SECTORS AND SERVICES FROM OTHER NATIONS

Definitions from other nations may be helpful inspiration, but they will not be directly transferable. Comparing the CI definitions from all the nations (listed under 'Critical Infrastructure' in the A-Z list on the landing page of [CIPedia©]) may guide nations in stating their own definition, preferably one that equals an already existing one. Each nation that starts developing insight into their CI is going to identify different critical sectors and services. Regardless of the diversities, the goal remains the same: the CI and CII of a nation have to keep functioning in an undisturbed way as much as possible.

To create an initial set of CI sectors and CI services one may be inspired by the sets of CI sectors and services defined by other nations. The entry 'Critical Infrastructure Sector' in the A-Z list on the landing page of [CIPedia©] lists both critical sectors, and in a number of cases the critical services too.

3.2.2 GOOD PRACTICE: ADOPT A METHODOLOGY TO IDENTIFY CI SECTORS AND SERVICES SYSTEMATICALLY

How does one approach the identification of CI sectors and services? The four methodological stepping stones explained in [RECIPE2011] are briefly explained here. They provide a structured approach to the identification process. These steps were inspired by the European Critical Infrastructure Directive [EC2008] which starts bottom-up from within a sector that potentially may be critical:

1. Apply sector-specific criteria
2. Assess criticality
3. Assess dependencies
4. Apply cross-cutting criteria.

The most useful order of these steps depends on the information that is available to national policy-makers. In some cases, it is possible to start with the development and application of cross-cutting criteria, assess dependencies, assess criticality, and end with applying sector-specific criteria.

Apply sector-specific criteria

A first selection of CI and CI services within a sector can be made based on sector-specific criteria. Such criteria may be the market share, the transport capacity (e.g. m^3 per second gas flow, CI function which is a single point of failure), cross-border connectivity (import and/or export), supply of critical services to government, industry or population. This first step results in a CI short-list from within a particular sector. This step also narrows down the number of potential CI operators in the case where the sector has multiple operators. Be awere that sector-specific criteria may be treated as classified information by some nations as they could reveal dependencies, vulnerabilities and sensitivities. This leads to a short-list of CI from which further deliberations are to be made. This method clearly favours objective, quantifiable criteria rather than subjective, qualitative criteria.

Table 4. Example: Criticality Scale for national infrastructure [Cabinet2010].

Criticality Scale	Description
Cat. 5	This is infrastructure the loss of which would have a catastrophic impact on the UK. These assets will be of unique national importance whose loss would have national long-term effects and may impact across a number of sectors. Relatively few are expected to meet the Cat 5 criteria.
Cat. 4	Infrastructure of the highest importance to the sectors should fall within this category. The impact of loss of these assets on essential services would be severe and may impact provision of essential services across the UK or to millions of citizens.
Cat. 3	Infrastructure of substantial importance to the sectors and the delivery of essential services, the loss of which could affect a large geographic region or many hundreds of thousands of people.
Cat. 2	Infrastructure whose loss would have a significant impact on the delivery of essential services leading to loss, or disruption, of service to tens of thousands of people or affecting whole counties or equivalents.
Cat. 1	Infrastructure whose loss could cause moderate disruption to service delivery, most likely on a localised basis and affecting thousands of citizens.
Cat. 0	Infrastructure the impact of the loss of which would be minor (on national scale).

Assess criticality

The second step is to assess criticality of the short-list from the previous step based on the nation's CI definition. This requires knowledge about specific delivered goods and services from a sector as well as the answer to the question who or what is responsible for it. An example is that for the energy sector, criticality might only lie within the provision of electricity and gas. For the ICT sector, a nation might only find the accessibility of their national emergency number a critical service, although this kind of service falls under the telecom sector. It is thus good to stress that a transplantation of other examples is suitable for the first steps in finding sectors and services, but that national differences and interpretations of criticality apply.

Assess dependencies

The third step is to identify CI dependencies. (Inter)dependencies are defined as follows:

- A **dependency** is *"the relationship between two products or services in which one product or service is required for the generation of the other product or service"*.
- An **interdependency** is *"the mutual dependency of products or services"*. [Luiijf2009]

CI sectors and their critical services have dependencies with other CI sectors and their critical services. Empirical data suggest that interdependencies between sectors rarely occur [VEeten2011]. This means that dependencies between sectors and services have never been as critical and thus never led to major disruptions of nations in the past.

It is more worthwhile to find the critical dependencies that may carry forward outages in a cascading way. Moreover, the set of CI dependencies may significantly change when the normal 24/7 CI's functioning changes from normal operations to, for instance, an emergency or recovery situation. A hospital might not use fuels during normal operations, but needs diesel to operate their emergency generators when the external power supply fails. Assessment of such 'mode of operation' shifts in dependencies is hard to perform [Nieuwh2008].

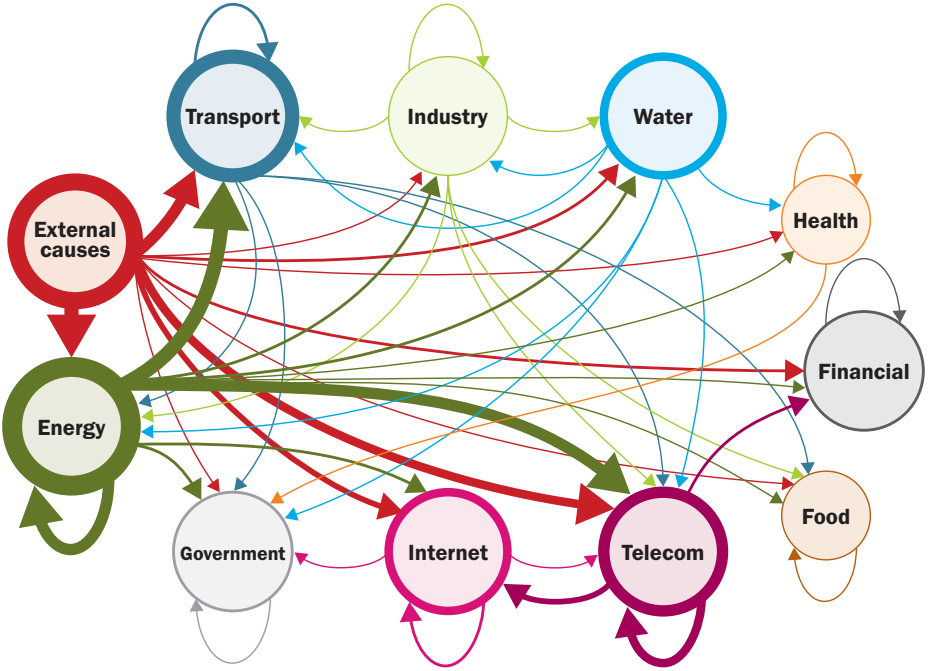

Figure 7. CI cascading disruptions through dependencies in Europe (2005-2009). Note: relative size of external causes is divided by five.

The set of CI identified is likely to be extended after the identification of CI dependencies. CI sectors and services are a critical part of service and supply chains that are increasingly becoming longer and entangled. The use of ICT amplified this trend. For example, a disruption at an external infrastructure supplier such as a telecommunication backbone provider could potentially result in disruptions through dependencies in a whole set of CI processes, e.g. the functioning of a hospital, and the inability to control the flow to a sewage processing plant.

Assess cross-cutting criteria

Cross-cutting criteria may underpin the criticality of certain infrastructure services to a nation, both under normal circumstances and during emergencies. Cross-cutting criteria can be found in [Qatar2014] and [EC2008], for instance:

– casualties criterion (potential number of fatalities or injuries);

- economic effects criterion (significance of potential economic loss and/or degradation of services, potential environment effects);
- public effects criterion (impact on public confidence, level of physical suffering of the population, level of disruption of the daily life);
- dependency criterion (e.g. potential for cascading effects on other sectors, e.g. minor, moderate, significant, debilitation);
- scope of impact criterion (affected area: e.g. local, large area or multiple sectors (partially), nationwide or single sector (full), international or multiple sectors (full); size of population affected and/or density of the population in the affected area);
- service impact (e.g. recovery times in number of days).

One may refer to [RECIPE2011], [EC2008], [Mattioli2015] and [Qatar2014] for further reading.

3.2.3 GOOD PRACTICE: (NATIONAL AND CROSS-BORDER) DEPENDENCY ANALYSIS

Dependencies will already come to the surface during the first steps of CI identification and risk assessments, but specific methods to draw out decencies are at hand. Apart from dependencies within a nation, nations might also find dependencies between national CI and infrastructures in neighbouring nations and regions. Such dependencies may influence the criticality of a particular national infrastructure, for instance when the national economy depends heavily on exporting or importing. The most accessible method is to organise workshops with stakeholders from different critical sectors.

3.3 REFERENCES AND FURTHER READING

[Brunner2009] E.M. Brunner and M. Sauer, International CIIP Handbook 2008/2009: An Inventory of 25 national and 7 international Critical Infrastructure Protection Policies, ETH, Zürich, Switzerland, 2009. On-line: http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-08-09.pdf

[Bruno2002] S. Bruno and M. Dunn, Critical Information Infrastructure Protection: An Inventory of Protection Policies in Eight Countries, ETH, Zürich, Switzerland, 2002. On-line: http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP_Handbook_2002.pdf

[Cabinet2010] Cabinet Office, Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure from Natural Hazards, March 2010. On-line: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62504/strategic-framework.pdf

[CTO] Commonwealth Telecommunication Organisation, Critical Information Infrastructure Protection (CIIP) workshops, 2015. On-line: http://www.cto.int/strategic-goals/cybersecurity/ciip-workshops/

[EC2008] European Council, 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 (Text with EEA relevance). On line: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008L0114

[Hyslop] Maitland Hyslop, Critical Information Infrastructures: Resilience and Protection, Springer, 2007.

[Luiijf2009] Luiijf, E, Nieuwenhuijs, A., Klaver, M., Eeten, M. van., Cruz, E., Empirical Findings on Critical Infrastructure Dependencies. In: R. Setola, S. Geretshuber (eds), Critical Information Infrastructure Security, Lecture Notes in Computer Science (LNCS) 5508, Springer, 2009, pp. 302-310.

[Macaulay2008] Macaulay, T., Critical Infrastructure: understanding its component parts, vulnerabilities, operating risk, and interdependencies, CRC press, Canada, 2008.

[Mattioli2015] R. Mattioli, C. Levy-Bencheton, Methodologies for the identification of Critical Information Infrastructure assets and services, ENISA, February 2015. On-line: https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis/at_download/fullReport

[Nieuwh2008] Nieuwenhuijs, A.H., Luiijf, H.A.M., Klaver M.H.A., 'Modeling Critical Infrastructure Dependencies', in: IFIP International Federation for Information Processing, Volume 290, Critical Infrastructure Protection II, eds. P. Mauricio and S. Shenoi, (Boston: Springer), October 2008, pp. 205-214, ISBN 978-0-387-88522-3.

[PSC2014] Public Safety Canada/Sécurité publique Canada, Critical Infrastructure Policy, Forging a Common Understanding for Critical Infrastructure. March 2014. On line: https://www.dhs.gov/sites/default/files/publications/critical-five-shared-narrative-critical-infrastructure-2014-508.pdf

[Qatar2014] Qatar Ministry of Information and Communications Technology, Qatar National Cyber Security Strategy (السيبراني للأمن الوطنية الاستراتيجية), May 2014. On-line: http://www.motc.gov.qa/sites/default/files/national_cyber_security_strategy.pdf

[RECIPE2011] M. Klaver, E. Luiijf, A. Nieuwenhuijs, Good Practices Manual for CIP Policies for policy makers in Europe, TNO, 2011. On line: http://www.tno.nl/recipereport

[VEeten2011] M. van Eeten, A. Nieuwenhuijs, E. Luiijf, M. Klaver, E. Cruz, The State and the Threat of Cascading Failure across Critical Infrastructures: The Implications of Empirical Evidence from Media Incident Reports, Public Administration, Vol. 89, No. 2, 2011, (381-400).

4 IDENTIFICATION OF CRITICAL INFORMATION INFRASTRUCTURE

A second step after the identification of the national set of CI, is to identify the CII. Similar steps as in the previous chapter can be used, although the identification of CII is often more complex than the identification of CI as will be explained below.

4.1 GENERAL DESCRIPTION AND MAIN CHALLENGES

The identification of the set of CII is a demanding process. However, if it is done in a structured way with use of good practices, one might get grip on the process.

4.1.1 START DETERMINING THE SET OF POSSIBLE CII

As shown in Figure 8, the CII has two foci:

1. The critical ICT infrastructure services used by CI (e.g. mobile telecommunication, internet access);
2. The critical information, communication, and control system technologies that are used in and across the CI processes of the CI sectors.

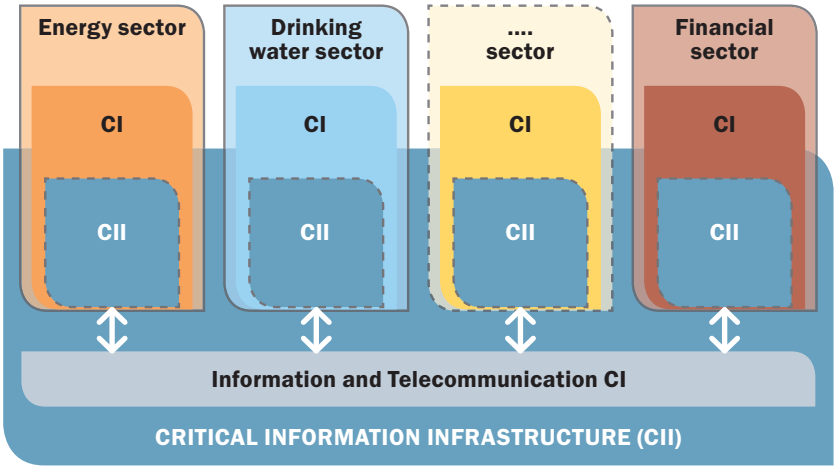

Figure 8. The CII encloses (1) the Information and Telecommunication CI, and (2) the CII components in CI (e.g. control systems).

This aligns with the 2008 understanding of the OECD of CII [OECD2008]: *"National CII {...} typically include one or more of the following:*

- *information components supporting CI; and/or*
- *information infrastructures supporting essential components of government business; and/or*
- *information infrastructures essential to the national economy".*

A lot of the classical and current CII/CIIP literature concentrates on the first focal point. In other words, they concentrate on the Information and Telecommunication CI and the CI-interconnection arrows depicted in Figure 1. The intersection of the CII with the various CI services is sometimes overlooked.

The critical information, communication, and control system technologies that are used in and across the CI processes of the CI sectors:

1. Control systems that monitor and control critical parts of specific CI sectors and/or services (e.g. specific control systems in the production, transport and distribution of natural gas). The reasons to regard them as part of the CII are:
   - CII control system technologies are increasingly becoming non-sector specific, commercial-off-the-shelf, and internet protocol ('TCP/IP') enabled.
   - Business requirements may request CI operators their critical control systems to the internal business networks and thus indirectly to public networks including the internet.
   - At the same time, complex multi-operator CI operations may require interconnectivity of the critical CI systems of different operators.
   - Manufacturers, maintenance companies and system integrators may require remote access 24/7 to the control systems and controlled cyber-physical systems to optimise processes and to look for wear and tear within the installation, e.g. a power plant.
2. Similarly, other critical elements such as financial and logistic systems in other CI of various CI operators are increasingly interconnected in collaboratively delivering critical end-to-end services and are part of international service backbones, e.g. the SWIFT inter-banking services.

Based upon analysis, [NISC.JP2014] defined the set of 13 Japanese CII sectors as:
- information and communication services
- financial services
- aviation services
- railway services
- electric power supply services
- gas supply services
- government and administrative services (including municipal utilities)
- medical services
- water services
- logistics services
- chemical industries
- credit card services; and
- petroleum industries.

Many new pieces of equipment only operate with ICT and may require connectivity with public networks, if not the internet. This trend has introduced both desired and unexpected dependencies for critical processes in CI.

An increasing proportion of functions are being outsourced to third parties. Such third parties might also operate outside national borders. This is also the reason why private stakeholders often have some kind of role in CI, as stated earlier in this guide. Therefore, the CII identification is a process that requires flexibility and regular reassessments over time.

4.1.2 IDENTIFY CII OPERATORS (PUBLIC, PUBLIC-PRIVATE, PRIVATE)

Previous chapters stated the differences between nations with regard to CI. In some nations, CI is in the hands of the public sector itself, whilst in other nations private companies are responsible for CI. Drinking water companies are an example of this variation. In some nations, drinking water work companies are privatised, while in other nations the supply of drinking water is the sole responsibility of a national, state or municipal water agency. However, even if governments did not privatise their critical services, they still dependent on the correct functioning of CII. For many nations, ICT is becoming more important for the proper functioning of society (both in terms of critical processes as in normal daily life), therefore public and private CI operators become increasingly involved with national and international CII operators. These factors might make the identification of CII operators difficult, as they cut through old processes and introduce new ICT-based services and dependencies. The network building as described in Chapter 7 is a means to involve all relevant stakeholders in this process early as possible.

4.1.3 IDENTIFY CII DEPENDENCIES AND INFORMATION SUPPLY CHAINS

Many, if not all, CI are directly or indirectly influenced by control systems[4]. Crucial processes in most CI and of many other organisations rely businesswise on the correct and undisturbed functioning of control systems and control system networks. Control systems are very often semi-autonomous and perform automatic tasks in the background (monitoring, handling routine tasks) and therefore have usually been designed and built to operate in an isolated and remote operated environment 24 hours per day, 7 days a week. For efficiency and flexibility reasons, control systems are increasingly connected to networks external to its systems and networks it operates in. Often control systems networks have connectivity with networks including the internet.

A failure of a control system may cause (critical) service disruptions and a safety risk to people and the environment. Therefore, the cyber security of control systems is of utmost importance to utilities and other CI operators, and to all organisations which use control systems and thereby potentially to society as a whole. A subset of control systems in CI monitors and controls critical processes of the CI (e.g., purification, production and distribution of drinking water). For those control systems it will be obvious that they are part of its associated CII.

4 Control Systems perform the 24/7 monitoring and control part of cyber-physical systems, e.g. generation of electric power, the production processes of a refinery, and signaling and control of switches of railways. There exists a wide variety of notions for '*Control Systems*': Industrial Control Systems (ICS), Industrial Automation and Control Systems (IACS), Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Process Control Systems (PCS), and more. Although there are slight differences, for the purpose of this guide we use the notion Control Systems.

ICT has been the engine of communication systems since the beginning, but ICT is now implemented, embraced and adopted in different but prominent non-ICT environments. For example, control systems now operate and monitor systems that used to be operated manually, e.g. the control of railway signalling, points, and barriers. This poses new challenges because ICT will suddenly become a factor to consider when trying to secure 24/7 continuity of production or services. Another important aspect is that ICT has often been introduced into business environments without awareness of ICT-security or potential vulnerabilities. The result of this might be that malfunctioning IT in back office environments might proceed to cause damage in local and remote production environments.

4.1.4 CRUCIAL INSIGHT INTO UNCONTROLLABLE DEPENDENCIES

The focus on dependencies, CI operators and stakeholders requires a wider perspective. Global communication takes place over the internet and CII possibly uses that same infrastructure for critical communication. A nation's connectivity to the global internet might greatly depend on Internet Exchange Points and communication hubs nationally and internationally.

The dependency on linked systems and services (and underlying technologies) over which one has no direct control is nowadays unavoidable. It is therefore essential to obtain insight in the extent of such uncontrollable dependencies and possible negative effects during failure or outage. If the impact of these effects is deemed unacceptable, stakeholders affected by malfunctioning of critical processes must take action to either prevent this, or substitute the critical process.

Elements that may require attention are: certificate authorities (CA), satellite communication, worldwide hosting platforms (e.g. cloud services), internet exchange points (IX), domain name services (DNS), hardware manufacturers, and more to come [Luiijf2015a]. The uncontrollable dependencies are a unique dimension to take care of. This dimension is unique to ICT due to its complex global connectivity which could disrupt international systems that for example rely on ICT huge distances away.

Dependencies might also be introduced when old technology is replaced by new. One might suddenly depend on new technologies that are vulnerable to for manipulation, disruption and malfunction due to cyber threats. The trade-off between increased efficiency and cost-reduction must be carefully observed.

4.2 GOOD PRACTICES FOR THE IDENTIFICATION OF CII

Good practices for the identification of CII are the following:

- G8 Principles for Protecting Critical Information Infrastructures;
- identification of CII;
- keep ahead of CII technology developments and shifting dependencies.

4.2.1 GOOD PRACTICE: G8 PRINCIPLES FOR PROTECTING CRITICAL INFORMATION INFRASTRUCTURES

In 2003, the G8 observed that information infrastructures increasingly form an essential part of CI [G8]. The G8 concluded that nations should protect their CII from damage and secure them against attack. Effective CIIP includes identifying threats, reducing vulnerabilities, minimising damage and recovery time, identifying the cause of disruption, and analysis by experts andor investigation by law enforcement. Effective CIP also requires communication, coordination, and cooperation nationally and internationally among all stakeholders with due regard for the security of information and applicable law concerning mutual legal assistance and privacy protection. To further these goals, the G8 adopted and promoted the following *principles for CIIP*:

1. Nations should have emergency warning networks regarding cyber vulnerabilities, threats, and incidents.
2. Nations should raise awareness to facilitate stakeholders' understanding of the nature and extent of their CII, and the role each must play in protecting them.
3. Nations should examine their infrastructures and identify dependencies among them, thereby enhancing protection of such infrastructures.
4. Nations should promote partnerships among stakeholders, both public and private, to share and analyse critical infrastructure information in order to prevent, investigate, and respond to damage to or attacks on such infrastructures.
5. Nations should create and maintain crisis communication networks and test them to ensure that they will remain secure and stable in emergency situations.
6. Nations should ensure that data availability policies take into account the need to protect CII.
7. Nations should facilitate tracing attacks on CII and, where appropriate, the disclosure of tracing information to other nations.
8. Nations should conduct training and exercises to enhance their response capabilities and to test continuity and contingency plans in the event of an information infrastructure attack and should encourage stakeholders to engage in similar activities.
9. Nations should ensure that they have adequate substantive and procedural laws, such as those outlined in the Council of Europe Cybercrime Convention of 23 November 2001, and trained personnel to enable them to investigate and prosecute attacks on CII, and to coordinate such investigations with other nations as appropriate.
10. Nations should engage in international cooperation, when appropriate, to secure CII, including by developing and coordinating emergency warning systems, sharing and analysing information regarding vulnerabilities, threats, and incidents, and coordinating investigations of attacks on such infrastructures in accordance with domestic laws.
11. Nations should promote national and international research and development and encourage the application of security technologies that are certified according to international standards.

These principles were subsequently revisited and adopted by the OECD.

4.2.2 GOOD PRACTICE: IDENTIFICATION OF CII

A methodology to perform an in-depth analyses and identification of CII is documented by ENISA in [Mattioli2015] and largely aligns with the 'Good Practice: Adopt a methodology to identify CI sectors and services systematically' (Section 3.2.2). However, this approach only considers the first CII focus outlined in Section 4.1.1 above. After the identification of CI sectors, the methodology describes the identification of critical services as a two-step process:

1. Identification of critical services – can be done either by a government-based approach or a CI operator driven approach, and
2. The identification of CI assets (applications) supporting critical services.

Determining the second focus of CII identification outlined in Section 4.1 above, the cross-CI-sector infrastructure and critical technologies, is much harder to achieve. This requires confidence building and close co-operation (see Chapter 7) with each of the CI sectors, and the supply chain of the critical elements of CI (manufacturers, vendors, system integrators, turn-key providers, third party maintenance companies).

4.2.3 GOOD PRACTICE: KEEP AHEAD OF CII TECHNOLOGY DEVELOPMENTS AND SHIFTING DEPENDENCIES

Keeping CII safe and secure is not a onetime activity. On the one hand, the threat landscape of the current install base constantly changes; on the other hand, new technologies are regularly being deployed in CII. Therefore it is important to create functionality at national level that keeps up with new threats and vulnerabilities. Moreover, such functionality should assess the short and long term CII security and resilience implications of the introduction of new technologies in CII. These insights need to be shared between the CII policy-makers and national CII operators [Luiijf2015].

For the current threats and vulnerabilities it is important to establish a process to identify relevant information sources, to process the intelligence gathered, to assess potential impact and to release relevant and accurate fact sheets, advisories etc. (see Chapter 7).

4.3 REFERENCES AND FURTHER READING

[CIPedia©] CIPedia©: a common international reference point for CIP and CIIP concepts and definitions. On-line: http://www.cipedia.eu

[G8] G8 Principles for Protecting Critical Information Infrastructures, G8, 2003. On-line: http://www.cybersecuritycooperation.org/documents/G8_CIIP_Principles.pdf

[Luiijf2015] E. Luiijf, M. Klaver, Symposium on Critical Infrastructures: Risk, Responsibility and Liability. Governing Critical ICT: Elements that Require Attention, European Journal of Risk Regulation, Vol. 6, Issue 2 (2015), pp. 263-270

[Mattioli2015] R. Mattioli, C. Levy-Bencheton, Methodologies for the identification of Critical Information Infrastructure assets and services, ENISA, February 2015. On-line: https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis/at_download/fullReport

[NISC.JP2014] The Basic Policy of Critical Information Infrastructure Protection (3rd Edition) – tentative translation, Japan, 2014. On-line: http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3.pdf

[OECD2008] OECD ICCP Committee and the Working Party on Information Security and Privacy, OECD Recommendation on the Protection of Critical Information Infrastructures [C(2008)35], 2008, OECD. On-line: http://www.oecd.org/sti/40825404.pdf

[Willke2007] B.J. Willke, A Critical Information Infrastructure Protection Approach to Multinational Cyber Security Events (presentation slides), ENISA, September 2007. On-line: https://www.enisa.europa.eu/topics/national-csirt-network/files/event-files/ENISA_best_practices_for_ciip_Willke.pdf

5 DEVELOPING CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

5.1 GENERAL DESCRIPTION AND MAIN ISSUES

CIIP is not only a technical concern. Non-technical organisational aspects are equally important. Awareness of CIIP risk management may ensure a balanced approach to cover the full cyber incident response cycle (proactive, pre-emption, prevention, preparation, incident response, recovery, aftercare/ follow up); see e.g. Chapter 4: Organisational Structures & Considerations in [Klimburg2012]. After an initial start, regular use of risk assessment may strengthen current CIIP efforts to match actual risk. In comparison to the national risk profile as mentioned in chapter 2, risk management in this chapter is understood as a practice for individual CII operators (or a sector-specific set of CII operators). Crisis exercises are a crucial element for CIIP, because they combine both technical aspects of CIIP and the cross-organisational aspects of the incident response cycle.

5.1.1 RISK MANAGEMENT

CIIP risk management actions can be performed by CII operators. If an information infrastructure is identified as critical, providing tools and guidelines for risk management may encourage its use and enhance the inclusiveness and applicability of the assessment. Risk management efforts can establish a common framework of what parts of the CII are analysed, and what terms, definitions, criteria, metrics are used. Proper CII risk management takes into account the risk that arises from critical dependencies with other sectors; an aspect of impact that may supersede the direct interests of the CII operator.

During the first phases of CIIP, such a risk management perspective remains dependent on what is deemed possible within and across sectors. Figure 9 illustrates the relationship between various risk management concepts.

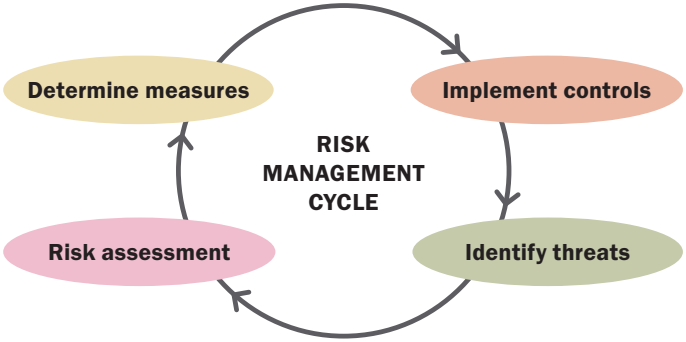

Figure 9. Relationship between risk assessment and risk management.

There are a large number of nations who have developed risk management guidelines and tools (e.g., [VanMill2006], [Habegger, 2008]). Although these differ considerably, they have some elements in common that contribute to their success:

1. determination of the context of the analysis;
2. identification of potential risk;
3. assessment of threats, vulnerabilities (sometimes integrated into determination of threats) and impacts;
4. determination of ensuing risk factors (and analysing them).

In order to identify and make sense of risk one needs information about threats, effect(s) of impact(s), and a common understanding of definitions and metrics. Note that private CII operators may already have applied own risk management methodologies which may cause friction if government mandates another risk management method for CII.

More on the topic of risk management and some good practices for the CI/CII domain can be found in Chapter 7 of [RECIPE] and in [Habegger, 2008].

5.1.2 NATIONAL CRISIS MANAGEMENT NEEDS TO PREPARE FOR CII CRISES

Although there are many ways to try to prevent disruptive events from happening, there is no way that prevention can eliminate all risk related to CII to nations and their citizens. National crisis management organises and manages all roles, responsibilities and resources to deal with serious incidents, emergencies, and crises at national level. Good crisis management at the national level, as well as at international and regional levels, takes CII into account as part of its preparedness, response, and recovery phases on the following grounds:

- By definition, the consequences of a CII disruption may be severe. Prevention of CII disruption and proper incident management is a primary task of the CII operator. However, national crisis management needs to plan for dealing with CII disruptions and impact. Joint, cross-sector exercises may enhance the preparedness of both governmental and CII operators to a large extent.
- For crisis management organisations, the continuity of CII services may be crucial to the effectiveness of their operations (see e.g. [Luiijf2009]).

From the above, it is clear that effective and efficient crisis management requires in-depth knowledge of CII, their operations and their dependencies. Close co-operation and mutual understanding with the CI/CII operators is required during incident response planning, emergency preparedness (e.g. joint training and cross-CII exercises), crisis response and restoration (see: Chapter 8 of [RECIPE]). A coordinating CIIP body might streamline the efforts; see Section 5.2.2 on Good Practice: Start a coordinating body for CIIP.

5.2 GOOD PRACTICES FOR DEVELOPING CIIP

5.2.1 GOOD PRACTICE: INVOLVEMENT OF CII EXPERTISE AS SUPPORT FUNCTION TO NATIONAL CRISIS MANAGEMENT

For effective decision-making, crisis management coordination at the national level needs to take into account the consequences of CII disruption in a certain area including its cascading effects. Help for national crisis management decision-making can be obtained from CIIP) experts who understand threats to CI and the CII, their critical dependencies, their disruption and restoration characteristics, and potential cascading effects. The responsibilities for crisis management and CIIP may be assigned to different parts of the same public and/or private organisation. Bridging them may be essential. Close co-ordination with the CIIP entities may shorten the recovery and restoration process but common understanding is not a given. This involvement of the CII stakeholders is similar to the involvement of CI stakeholders as described in [RECIPE] pages 77-82.

In the Netherlands, a public-private ICT Response Board (IRB) has been established which is hosted by the Dutch National Cyber Security Centre (NCSC). During a major cyber threat or cyber crisis involving the CII that could affect or actively affects the national security, the Council of Ministers takes decisions based upon advices by both the NCSC and the IRB. After thorough analysis of the actual situation and the available response options, the IRB provides tactical level advice to the strategic and political level decision-makers. They also may provide 'horizontal' advice to the other private IRB organisations such as the CII operators. Membership of the IRB currently comprises the CI sectors drinking water, energy, financial, government, and telecom (including ISP), the Dutch CERT community, as well as academic and other experts [IRB].

5.2.2 GOOD PRACTICE: START A COORDINATING BODY FOR CIIP

The efforts for CIIP can be supported by a coordinating public body. Such a body (or set of bodies) can operate at the strategic or tactical level, but also on a technical/operational level (see: chapter 4 in [Klimburg2012]). There are certain benefits in combining some of these levels with regard to CIIP. The tactical and strategic levels – mostly initiated because of political will – could for example be active in crafting CIIP strategies, establishing international connections (at strategic, tactical, operational/technical levels) and to start taking part in international dialogues with networks of public and private CII(P) stakeholders (see Chapter 7).

An operational/technical level in CIIP could be public and private Computer Security Incident Response Teams (CSIRT), also known as Computer Emergency Response Teams (CERT). CSIRT often have an important role in developing technical incident response capability for CII. To do so, CSIRT monitor, alert, warn and give support during cyber incidents to their constituency. As they focus on incident response, they need information and thus thrive under close cooperation and information exchanges (e.g. [SEIa], [SEIb]). An operational/technical body like a CSIRT may have strong ties with an entity that coordinates CIIP at the tactical level. In the case of privatisation, CI/CII operators might already have established

a CSIRT to keep their CII cyber secure. In such cases, it might be beneficial for the public bodies to interact or form an alliance with those private CSIRT.

In recent years, several nations have established a National Cyber Security Centre (NCSC) in which CSIRT or CSIRT capabilities are a core element. Such a centre may combine and coordinate the efforts of the public stakeholders with regard to CIIP (CI/CII identification, risk assessment, monitoring, and international cooperation). When we observe NCSC around the world, it is identified that they are coordinating bodies that actively involve CIIP stakeholders. Some NCSC deliver their services to public and private stakeholders. They may act as a trusted broker (no business model). Establishing a NCSC is not appropriate during the first steps of CIIP, but it might be very helpful in supporting further steps in maturity ([NCSC2015]).

How this functionality will look like will vary per nation. Where there is a National Cyber Security Centre, a national CERT/CSIRT or a similar initiative, this organisation could take the lead in this effort, but will always need the input from CI(I) operators to assess the potential impact on the various CI and an international public, private and academic network to gain the most up to date insights.

5.2.3 GOOD PRACTICE: JOINT PUBLIC-PRIVATE CRISIS MANAGEMENT EXERCISES INVOLVING CII SECTORS/OPERATORS

CII operators can be made part of (national) crisis exercises to involve them in the implementation of CIIP policies or to test their performance on (parts of) CIIP capacities. There is a discrepancy in intended goals of performing exercises for a wide range of hazards and emergencies at public authorities and CII operators. CII operators make sure their business continuity of production, processes and services is tested in support of their customers. Public participants have different objectives in crisis management exercises.

Rather than dealing with CII operators in an ad hoc manner, there are many reasons for establishing a clear understanding and framework for addressing incidents, emergencies and crises. Lacking this, a straightforward incident may evolve into a major crisis. By performing exercises, one learns (often the hard way) about each other's roles, responsibilities, decision-making cycles, capabilities, abilities, and terminology. Last but not least, the 'getting to know each other' is a much quoted important factor in diminishing friction between groups and facilitating co-operation.

Joint public-private, (regional), national and cross-border exercises create the right level of preparedness for emergencies of CM and CII operators. Exercises can be held at operational, tactical, and strategic levels and/or span multiple levels. Increasingly, nations involve CII operators as key partners in regional, national and international exercises.

CII involvement in regional and national exercises can be organised in different ways:
- Some nations oblige their CII operators to take part in regional and national CM exercises.
- Other nations expect their CII operators to voluntary play their role in regional and national exercises.
- A minority of nations contract CI/CII operators to take part in their national exercises.

In Europe, some nations organise major national exercises that involve CII and the possibility of disruption of CI/CII with cascading effects. Examples of international CM-CII exercises are the worldwide series of Cyber Storm exercises exercises organised in the US, and Cyber Europe which was organised by ENISA.

Experiences/lessons learned
- A prerequisite to an exercise is to define the exercise objectives. A 'making errors is allowed – no consequences' policy yields most lessons to be learned for the improvement of CM-CII cooperation.
- One result of exercises is diminishing the chances of friction and misunderstanding during the 'fog of a real crisis'.
- Exchange of sensitive private company data to CM during exercises requires data security safeguards by the CM environment (see Section 7 on Information sharing).

5.3 REFERENCES AND FURTHER READING

[CIPedia©] CIPedia©: a common international reference point for CIP and CIIP concepts and definitions. On-line: http://www.cipedia.eu

[CSA] Cyber Security Agency Singapore, Ministry of Communications and Information. On-line: https://www.csa.gov.sg/

[FICORA] Finnish Communications Regulatory Authority. On-line: https://www.viestintavirasto.fi/en/cybersecurity.html

[Habegger2008] B. Habegger, International Handbook on Risk Analysis and Management: Professional experiences, ETH, Zurich, Switzerland, 2008. On-line: https://www.files.ethz.ch/isn/47029/HB_RiskAnalysis&Management.pdf

[IRB] NCSC web site on 'ICT Response Board (IRB)'. On-line: https://www.ncsc.nl/english/Cooperation/ict-response-board.html

[Klimburg2012] Klimburg, National Cyber Security Framework Manual, NATO CCD-COE Publications, December 2012. On-line: https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

[Luiijf2009] E. Luiijf, M. Klaver, 'Insufficient Situational Awareness about Critical Infrastructures by Emergency Management', paper 10 in: Proceedings Symposium on 'C3I for crisis, emergency and consequence management', Bucharest 11-12 May 2009, NATO RTA: Paris, France. RTO-MP-IST-086.

[NCSC2015] CSIRT Maturity Kit: A step-by-step guide towards enhancing CSIRT Maturity, NCSC, The Hague, The Netherlands, 2015. On-line: https://check.ncsc.nl/static/CSIRT_MK_guide.pdf

[NCSC-UK] Website of the National Cyber Security Centre, United Kingdom. On-line: https://www.ncsc.gov.uk/

[SEIa] CERT division, Software Engineering Institute, Carnegie Mellon Institute, Create a CSIRT web page. On-line: http://www.cert.org/incident-management/products-services/creating-a-csirt.cfm

[SEIb] CERT division, Software Engineering Institute, Carnegie Mellon Institute, Action List for Developing a CSIRT web page. On-line: http://www.cert.org/incident-management/csirt-development/action-list.cfm

[VanMill2006] B.P.A. van Mil, A.E. Dijkzeul, R.M.A. van der Pennen, A view on Risk: Risk Modelling Handbook - Selection of models and methods for conducting risk analyses, Delft. On-line: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/-rapporten/¬2006/09/18/a-view-on-risks/handbook-risk-modelling.pdf

6 MONITORING AND CONTINUOUS IMPROVEMENT

6.1 GENERAL DESCRIPTION AND MAIN ISSUES

With an up to date view on the risk factors and changing CII vulnerabilities a nation faces, national governments can assess whether changes to CIIP policies are required. Ideally, the assessment of CIIP policies and the review of the risk landscape and changes in vulnerabilities results in a roadmap of policy changes to be implemented in order to keep CIIP at a desired level.

6.1.1 START TO MONITOR ACTIONS AND CONTINUOUS IMPROVEMENT

Once a CIIP strategy or policy has been developed, it remains important to monitor their implementation and effectiveness, as well as to develop a continuous cycle of CIIP improvement. To be able to monitor the implementation of CIIP actions, it is desirable that policies have clearly defined intentions and objectives, and that activities are defined in a Specific, Measurable, Achievable, Realistic and Timely/time-bound [SMART] way. SMARTness allows for instance a National parliament to perform their oversight role and the responsible ministry (or ministries) or agencies to monitor the progress of CIIP action lines. Even without SMART defined objectives, it is wise to monitor the progress that is made towards the implementation of CIIP policies and action plans.

Continuous monitoring of the CIIP activities' implementation makes it possible to make adjustments along the way. Also, it provides the possibility for the stakeholders responsible for CIIP to swiftly take action in areas of the CIIP actions where progress lags. Apart from keeping track of one's own actions and planning, it is also essential to keep up to date with constantly evolving threat landscape, or a landscape that changed due to incidents. A cycle of continuous CIIP improvement might keep the changing landscape observed effectively.

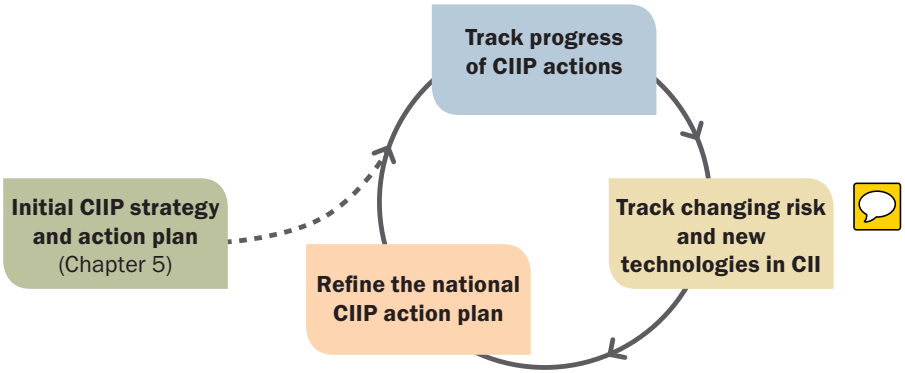

Figure 10. Continuous CIIP improvement cycle.

The perspectives of the CIIP improvement cycle are:

- *Review*: evaluate the progress made in the implementation of CIIP policies and action plans.
- *Adjust*: track the CII-related risk profile in order to:
  - assess changes in risk to CII
  - assess changes in the vulnerabilities of CII.
- *Refine*: the national CIIP action plan.

***Review*: Keep track of CIIP actions**

CIIP policies may include a broad range of measures including policy and legal frameworks, self-regulatory schemes of specific CI sectors, or the voluntary or mandatory adoption of specific protective measures. Keeping track of the implementation of such policies can be done through progress research, auditing, self-reporting of incidents and near misses by CII operators and operational agencies.

Oversight of CIIP related policies is often a task of authorities or agencies working on broader topics like boosting the use of ICT and cyber security. Some nations may choose to appoint a special authority or agency for monitoring, coordination and pushing for progress on CIIP. A good practice to be part of international dialogues to verify and reflect on one's own CIIP actions, and identify gaps (see good practice 6.2.1).

***Adjust*: Keep track of a changing risk landscape and CII vulnerabilities**

CIIP activities and action plans cannot be effective if they do not take the changing risk landscape of a nation and the evolution of vulnerabilities in CII into account. Keeping track of the changing risk landscape starts by reviewing changes of the risk to the nation. Reviewing risk should ideally be done with regard to all identified CII and the components and systems comprising these CII ways to do so are for instance: periodical reviews, through a risk management process (see Section 5.1.1), auditing, incidents, and lessons identified in CII exercises (see e.g. section 3.1.2 of [NISCJP]).

As with the risk to a nation, the vulnerabilities of CII also evolve over time. Vulnerabilities can, for example, stem from aging information infrastructure, overload, or technical vulnerabilities such as outdated software and lack of maintenance. There are several international institutions and national agencies that provide information and reports on ICT vulnerabilities (Mitre's Common Vulnerabilities and Exposures [CVE], European Governments CERT group [EGC], [US CERT], [ICS-CERT], TF-CSIRT, manufactures of CI/CII and cyber security companies, and software vendors. To be more aware of voluntary notification of vulnerabilities, see the coordinated vulnerability disclosure good practice (6.2.2).

Where possible, it is desirable to try to align the national CIIP improvement cycle with the cycles of subnational authorities and private stakeholders as well as the cycles followed by international institutions where they exist. Because the outcomes of evaluations at these levels and the publishing of new subnational or international CIIP policies often provide input for CIIP policies at the national level.

***Refine*: The national CIIP action plan**
This continuous improvement cycle aligns with the Plan-[Do-Check]-Action (PCDA) cycle one finds in literature, e.g. [NISC.JP2014].

6.1.2 LONG-TERM VIEW: FROM PROTECTION TO RESILIENCE

Nations that start to develop policies and practices regarding the security of CII are advised to start with CIIP first. However, the notion 'resilience' is mentioned very often in strategies, policies, and initiatives. Therefore the notion is briefly explained here.

Critical information infrastructure resilience (CIIR) points to the wider incident response cycle: pro-action, prevention, preparation, incident response, and recovery and after-incident activities. Although the literature on resilience offers little consensus about the definition and nature of the concept [HOSS2016], a useful definition of resilience in the context of CII is provided by the National Infrastructure Advisory Council [NIAC]: *"The ability to reduce the magnitude and/or duration of disruptive events in CII. The effectiveness of a resilient CII depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event"*. Resilience frameworks stress the fact that resilience includes all aspects of security and continuity of the incident response cycle [e.g. LABAKA2015, MARU2016].

Nations that start initiatives on CIIP may benefit from the insight that CIIP is often followed by CIIR by incorporating the possibility in CIIP policies to include aspects of CIIR in later stages or by adopting a CIIR perspective right away.

6.2 GOOD PRACTICES FOR MONITORING AND CONTINUOUS IMPROVEMENT

6.2.1 GOOD PRACTICE: TAKE PART IN INTERNATIONAL DIALOGUES

To keep track of changes in the risk to CII and vulnerabilities it is useful to reach out to international communities and fora. There are several international communities and organisations with different objectives. Organisations at a tactical/strategic level are, e.g. Europol (EC3), the ITU, OAS, African Union, G8, Global Cyber Security Capacity Centre [GCSCC]. Forums with operational/technical objectives are, e.g. TF-CSIRT, Forum of Incident Response Security Teams [FIRST], public outreach by CERTs worldwide, [ICS-CERT], [EGC], and [US CERT].

Other examples are the Meridian Process and the Global Forum on Cyber Expertise (GFCE). The Meridian Process aims to exchange ideas and initiate actions for the cooperation of governmental bodies on Critical Information Infrastructure Protection (CIIP) issues globally. It explores the benefits and opportunities of cooperation between governments and provides an opportunity to share best practices from around the world.

The Meridian Process seeks to create a community of senior government policymakers in CIIP by fostering ongoing collaboration. Participation in the Meridian Process is open to all countries/economies and is aimed at senior government policy-makers involved in CIIP-related issues. Every nation/economy is invited to take part in the Meridian Process, and is encouraged to attend the annual Meridian Conference. The Meridian Conference provides all participants, regardless their maturity in CIIP, with the opportunity to learn from others, exchange ideas and to partner with other nations.

The Global Forum on Cyber Expertise (GFCE) is a global platform for countries, international organisations and private companies to exchange best practices and expertise on cyber capacity building. The aim is to identify successful policies, practices and ideas and multiply these on a global level. Together with partners from Non-Governmental Organisations (NGO), the technology community and academia GFCE members develop practical initiatives to build cyber capacity.

The GFCE has combined with Meridian specifically to take forward CIIP initiatives, but is also responsible for many related activities on CSIRTs and various aspects cyber security.

6.2.2 GOOD PRACTICE: BE RECEPTIVE TO COORDINATED VULNERABILITY DISCLOSURE

Attempts to breach, exploit and manipulate CII systems and software take place constantly. Flaws in ICT security are exploited, unauthorised attempts to access systems happen, and CII operation might be interfered with because of such attempts. One way or the other, ICT-related incidents will take place. It is important however to facilitate notification efforts from benevolent individuals.

Regardless if flaws in ICT systems are found actively or not, they will remain present if the owner is not notified. There are individuals around the world that deliberately try to find security flaws in systems and software in order to make the world a safer place. These benevolent individuals are called ethical hackers. On the other hand, there are also people and groups that have malicious intentions to exploiting or breaching ICT systems. Ethical hackers or individuals that have unexpectedly found a security flaw in an ICT system have often found it difficult and dangerous to notify the owner of the system with information about the flaws. This is firstly because they were unable to send their findings to the right people, and secondly because notifying such flaws could result in them being prosecuted.

A good practice to deal with efforts of notification about security flaws in ICT security is to formulate and implement a policy of ‘coordinated vulnerability disclosure’ (sometimes also referred to as Responsible Disclosure) [GFCE]. Governments, major banks, international organisations and other private parties have already implemented a coordinated vulnerability disclosure policy [Microsoft]. The effect of the implementation is that they do not prosecute the individual if certain requirements are met, and they guarantee anonymity and also to fix the issue they were notified of. Security incidents will occur and this is an example good practice to help mitigate their effects.

6.3 REFERENCES AND FURTHER READING

[CVE] Mitre, web page on 'Common Vulnerabilities and Exposures (CVE)'. On-line: https://cve.mitre.org

[EGC] Web page European Government CERTs (EGC). On-line: http://www.egc-group.org

[GCSCS] Web page Global Cyber Security Capacity Centre. On-line: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/front

[GFCE] Web page on 'Coordinated Vulnerability Disclosure'. On-line: https://www.thegfce.com/initiatives/r/responsible-disclosure-initiative-ethical-hacking

[HOSS2016] Hosseini, S., Barker, K., & Ramirez-Marquez, J. E. (2016). A review of definitions and measures of system resilience. Reliability Engineering & System Safety, 145, 47-61.

[ICS-CERT] Web page The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). On-line: https://ics-cert.us-cert.gov

[LABAKA2015] Labaka, L., Hernantes, J., & Sarriegi, J. M. (2016). A holistic framework for building critical infrastructure resilience. Technological Forecasting and Social Change, 103, 21-33.

[MARU2016] Maruyama, H. (2016). Taxonomy and general strategies for resilience. In Urban Resilience (pp. 3-21). Springer International Publishing.

[Microsoft] Web page Microsoft Tech Center on 'Report a Computer Security Vulnerability'. On line: https://technet.microsoft.com/nl-nl/security/ff852094

[NIAC] Homeland Security (DHS)/National Infrastructure Advisory Council (NIAC), Critical Infrastructure Resilience Final Report and Recommendations. On-line: https://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf

[SMART] Web page on SMART Objectives. On-line: http://www.nationalacademies.org/hmd/About-IOM/Making-a-Difference/Community-Outreach/Smart-Bites-Toolkit/~/media/17F1CD0E451449538025EBFE5B1441D3.pdf

[US CERT] Web page US Computer Emergency Readiness Team (US CERT). On-line: https://www.us-cert.gov

7 NETWORKING AND INFORMATION SHARING

7.1 GENERAL DESCRIPTION AND MAIN ISSUES

Building strong trusted networks between CIIP stakeholders and enable the sharing of information are important conditions to safeguard society. Timely and speedy sharing of cyber security related information between the CII stakeholders – within the government, within critical sectors, across sectors, between public and private organisations, nationally and internationally – is widely perceived as an effective measure to address some of the cyber security challenges of CII operators.

Information sharing, in this context, is usually performed amongst a group of carefully chosen people with a mutual goal: keeping abreast of new and emerging threats and vulnerabilities, and related issues. It is important to choose people with a similar level of technical knowledge, at similar levels of authority and autonomy and with similar risk appetites [ENISA]. These people share information in order to be able to take appropriate risk mitigating measures in advance, during incidents but also in the aftermaths of incidents. They will meet regularly, develop personal trust, and share sensitive information about incidents, threats, vulnerabilities, good practices and solutions. They typically do this in a confidential environment where they all undertake to not disclose the details or the originators of the information, but they can use it to protect their own systems. There are many variations on this model, as discussed below.

Key factors for a successful information exchange are trust and value [Luiijf2015]. To initiate and maintain the sharing of knowledge and information, CIIP stakeholders need an environment in which a basis of trust can be established and sustained in an efficient and effective way. The physical environment might influence the experience and feeling about the information exchange. An 'environment' explicitly outside or inside a ministry might influence the approach of public and private stakeholders (for instance there is a major difference of setting within a ministry of defence or secret service or within a ministry of economic affairs). The 'environment' might also be influenced based on how the information exchange takes place (regular, regulated, formal or informal rules) and how previous efforts of public bodies were received by relevant stakeholders.

To establish an environment of trust and value takes time and commitment by all participants, but the added-value of improved and trusted exchanged information far outweighs these necessary efforts.

Sharing information particularly helps those actors that manage and mitigate cyber security risk at an operational level. By being able to talk about vulnerabilities and incidents freely and, in an atmosphere of absolute trust, public, semi-public, and private organisations obtain a better overview of potential threats, vulnerabilities, and impact on their organisation,

sector, or across sectors. The nature of cyber security has and will continue to evolve very quick over time. Information sharing efforts should also evolve to keep pace with changes in the cyber security landscape. A benefit of information sharing is the opportunity to leverage knowledge, awareness, understanding and experiences across a broader community.
Other countries might have valuable experiences about previous CIIP efforts. To exchange experiences, the GFCE-Meridian initiative is introducing a 'Buddy Initiative'. The initiative is mentioned as a good practice, in addition to other good practices in Networking and information sharing. References to further reading material and good practices are presented in Section 7.2:

- stimulate the sharing of cyber security related information;
- establish clear roles in CIIP in Sharing Initiatives;
- be informed about Information Sharing Standards;
- take note of the Guide to Cyber Threat Information Sharing;
- the buddying system;
- various organisational forms of Public-Private Partnerships for CIP/CIIP;
- Cyber Security Council at the national level;
- Traffic Light Protocol (TLP).

7.2 GOOD PRACTICES FOR NETWORKING AND INFORMATION SHARING

For many CII stakeholders it is abundantly clear that no single organisation can address the full spectrum of its CIIP alone, as organisations are increasingly globally interconnected and exposed to the same global security threats. The purpose of networking and sharing cyber security related information is to reduce uncertainty with regards to the performance and business continuity of CII at an individual CI operator, in a whole CI sector, and/or across CI service chains spanning multiple organisations. The following sections provide several good practices on this topic. More practices can be found in the references.

7.2.1 GOOD PRACTICE: STIMULATE THE SHARING OF CYBER SECURITY RELATED INFORMATION

Information sharing provides a basis for the common understanding of threats, vulnerabilities, dependencies, and shared knowledge of possible countermeasures. Information sharing improves the quality of risk management (see Section 5.1.1) because information on new risk factors might be available more quickly. The CII protection measures may be adapted accordingly.

When major CII disruption occurs, existence of a trusted network with common interest and experience helps to effectively and collaboratively address the incident. Information sharing is therefore an effective approach in support of managing the collaborative CII risk in a domain where the threat landscape is changing continuously.

Experiences of successful *voluntary* information sharing initiatives show that **trust** is the main key success factor. In support of that is an agreement on how one may use exchanged information in one's own organisation. In many nations, the Traffic Light Protocol (TLP; see

Section 7.2.8) is a proven approach to enable information sharing between private, semi-public and public organisations. Information sharing, however, is a multi-faceted notion with many related policy issues, both from the public and the private side. A discussion on all topics and a set of Good Practices can be found in [Luiijf2015]; a picture of some of the building blocks starting from green (relatively simple) to red (major effort) can be found in Figure 11.

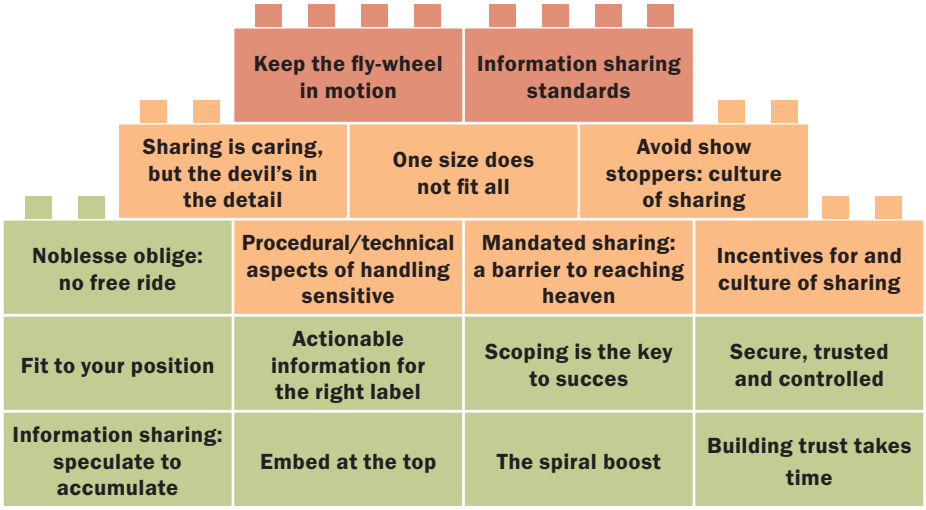

Figure 11. Building blocks for Information Sharing in [Luiijf2015].

By law and/or regulation, nations may mandate information sharing by CII operators of (cyber) security breaches and CII disruptions. In such a case it is often hard to guarantee the quality of the exchanged information, as the motivation is a stick, not a carrot. Even mandated approaches therefore emphasise that a key to the success of sharing with CII operators is still to build trust and a spirit of voluntary co-operation.

In an international environment, it proves to be more difficult to build the trust needed for effective information sharing due to the problems of organising regular face-to-face meetings, and the language, cultural, regulatory and competitive barriers. However, some nations have established cross-border communities that share CIIP information like the Financial Services Information Sharing and Analysis Center (FS-ISAC). Similarly, information sharing on a specific CIIP topic, such as control system security and others, takes place between nations and CII operators (e.g. the [EUROSCSIE] and the Japanese CIIP policy [NISC.JP2014]).

7.2.2 GOOD PRACTICE: ESTABLISH CLEAR ROLES IN CIIP IN SHARING INITIATIVES

There are examples of good practices around the world where stakeholders in CIP/CIIP are involved in information sharing initiatives at a regional, national or international level. Some of these initiatives are government to government (G2G), others business to business (B2B)

but also many public-private initiatives are in place. Examples the Forum for Incident Response and Security Teams [FIRST], the European Government CERT group [EGC], Infragard [Infragard], several ISACs in the US, the UK Cyber-Security Information Sharing Partnership (CiSP), the German UP KRITIS [UP-KRITIS], CPNI Information Exchanges in the UK [CPNI IE], Reporting and Analysis Centre for Information Assurance MELANI in Switzerland [MELANI], and the NCSC's ISACs in the Netherlands [NCSC]. In many of these initiatives CIIP stakeholders come together and actively share information about threats, incidents, vulnerabilities and good practices. An example is highlighted below.

MELANI - SWITZERLAND

MELANI serves two customer groups. The first one is the open customer group which includes private computer and Internet users, and small and medium-sized enterprises (SMEs) in Switzerland. MELANI offers this first group:

- Information on threats and measures for dealing with modern information and communication technologies (e.g., internet, e-banking) in the form of factsheets.
- Reporting the most important trends and developments relating to incidents and events in information and communication technologies.
- A registration form to report incidents.

The second, closed customer group comprises selected operators of the national CI (e.g. energy suppliers, telecommunication companies, banks, etc.). It is MELANI's responsibility to protect these CI, especially where they critically depend on the functioning of information and communication infrastructures, in other words: the CII. The goal is that network and system interruptions as well as abuses should be rare, of short duration, controllable, and have minimal impact. MELANI can only achieve this task through close partnership and cooperation with these CII operators. In this partnership, MELANI focuses on sharing knowledge and resources that are available only to the government and which are not otherwise accessible to the private sector, especially information of intelligence services (e.g., countering industrial espionage), the National Computer Emergency Response Teams (CERTs) and law enforcement.

7.2.3 GOOD PRACTICE: BE INFORMED ABOUT INFORMATION SHARING STANDARDS

The Information Sharing and Analysis Organization (ISAO) Standards Organization [ISAO] is a US based non-governmental organisation established October 1, 2015 that has the mission to improve the US' cyber security posture by identifying standards and guidelines for robust and effective information sharing and analysis related to cyber security risk, incidents, and best practices.

ISAO SO works with existing information sharing organisations, owners and operators of CI, relevant agencies, and other public and private-sector stakeholders through a voluntary consensus standards development process to identify a common set of voluntary standards

and guidelines for the creation and functioning of information sharing and analysis organisations. These standards address, but are not be limited to, contractual agreements, business processes, operating procedures, technical specifications, and privacy protections.

A recently released document is 'ISAO 300-1: Introduction to Information Sharing' [ISAO300-1] that provides an introduction to cyber security information sharing. This document describes a conceptual framework for information sharing, information sharing concepts, the types of cyber security information an organisation may want to share, ways an organisation can facilitate information sharing, as well as privacy and security concerns to be considered.

7.2.4 GOOD PRACTICE: TAKE NOTE OF THE GUIDE TO CYBER THREAT INFORMATION SHARING

The National Institute of Standards and Technology has published the NIST Special Publication 800-150 Guide to Cyber Threat Information Sharing [Johnson2016]. Cyber threat information is any information that can help an organisation identify, assess, monitor, and respond to cyber threats. Cyber threat information includes indicators of compromise; tactics, techniques, and procedures used by threat actors; suggested actions to detect, contain, or prevent attacks; and the findings from the analyses of incidents. Organisations that share cyber threat information can improve their own security postures as well as those of other organisations.

This publication provides guidelines for establishing and participating in cyber threat information sharing relationships. This guidance helps organisations establish information sharing goals, identify cyber threat information sources, scope information sharing activities, develop rules that control the publication and distribution of threat information, engage with existing sharing communities, and make effective use of threat information in support of the organisation's overall cyber security practices.

7.2.5 GOOD PRACTICE: THE BUDDYING SYSTEM

Nations with well-developed CIIP policies and capabilities may have contacts with other nations who have just started on the path of CIIP. Such outreach, however, is not always specifically focused on CIIP, or coordinated. A closer bilateral or multi-lateral buddying relationship may be beneficial to consider. The nation with less developed policies and activities may be offered resources and knowledge, and may learn from the buddy nation about valuable organisational or process-wise approaches and about pitfalls to avoid. In this way, their CIIP journey may be faster than going on the path alone. Before selecting a buddy nation, it is worth considering whether there exists a 'match' between the nations, bridging the differences in legal and other governance structures, language, etc.

Offering to be a guide nation, when a nation is ahead of other nations on the CIIP path, brings benefits as well. The buddy nation may ask CIIP questions which the guide nation has not yet considered. Moreover, a strengthened CIIP in the buddy nation creates a safer CII node in cyberspace. At the same time, guide nations should ensure that all necessary coordination and authorisation has been undertaken with the relevant ministries and agencies in their

nations before making approaches to a potential buddy. It is however possible to begin with informal buddying discussions to establish compatibility and mutual interests, before each nation decides to develop a more formal buddying relationship.

The Meridian process [Meridian] has announced a buddying proposal whereby a nation may consider engaging as a buddy nation (or a guide nation). The annual Meridian conference is designed to facilitate the early informal stages of buddying by creating a confidential environment for nations from across the world to meet and explore their similarities and goals. By creating an informal stage of buddying it may so happen that two nations are considering a closer and more formal buddying relationship in a later stage. However, bilateral or multi-national buddying approaches to CIIP, e.g. by regional collaboration on CIIP, may work as well. Moreover, there is no reason why a country should not develop more than one buddy, to help with different aspects of CIIP development, or to provide a choice of advice and experience. Current cyber security strategy development arrangements like the ones by e.g. the African Union (AU) and the Organization of American States (OAS) may be used as a stepping stone.

7.2.6 GOOD PRACTICE: VARIOUS ORGANISATIONAL FORMS OF PUBLIC-PRIVATE PARTNERSHIPS FOR CIP/CIIP

PPP function in many different forms, varying from very informal types of co operation to more formal partnerships. The degree of formality is often associated with the amount of control the governmental bodies aim to exert. This spectrum is illustrated in Figure 12: Degree of control in PPP.

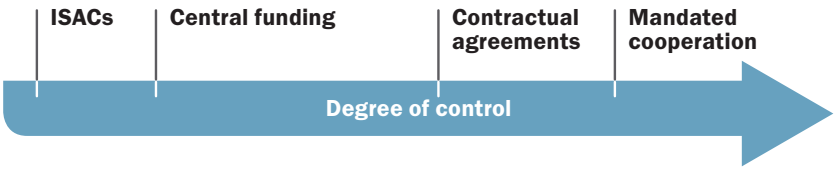

Figure 12. Degree of control in PPP (source: [RECIPE]).

Some of the benefits PPP can bring to CIP/CIIP are:

1. Stronger PPP will positively influence the capability of CI/CII operators participating to manage the consequences of disaster.
2. Improvements in the resilience of CI/CII will positively improve supply chain resilience.
3. A higher capacity to maintain business continuity, resulting in higher levels of service and trust between service providers and clients.
4. A higher level of understanding of how dependencies among sectors affect responses to emergencies, leads to better levels of preparation and response to disruptions, and shortens the duration till full recovery.
5. Co-operation can lead to reduced risk for all organisations involved.
6. Co-operation can lead to lower costs for all organisations involved.

Whilst there is no guaranteed format for success in establishing a PPP, there are certain factors that are of the utmost importance for a successful PPP. These factors are:

- Trust: as PPP in CIP/CIIP often concern touchy subjects (commercially, in terms of reputation, security wise, shifting responsibilities), it is essential to create an atmosphere of trust in which all organisations show awareness of each other's need for discretion and consistently act accordingly. Clear membership guidelines of operating rules may support the building of trust, e.g. [FS-ISAC].
- Value: Participation in a PPP must produce benefits otherwise the enthusiasm to participate will quickly fade.
- Respect: all organisations have to recognise and respect the added value the other organisations bring to the collaboration. This can be reached by 'selling' your own added value (in your partner's terminology) while actively looking for the added value of your partners.
- Code of conduct: it is necessary to have clear, specific and predictable rules that do not provide scope for discretion and prevent any conflict of interest.
- Awareness of each other's possibilities and restrictions: this prevents conflict through misjudgement of the cause of a negative response and allows for an optimum return on the efforts of the alliance. This implies that both organisations should know each other's business. A good way to attain this is to have worked together for a long period of time, preferably years.
- Realistic expectations: all organisations have to take into consideration affordability of resources, development budget, etcetera, to be able to form realistic expectations of the PPP.

7.2.7 GOOD PRACTICE: CYBER SECURITY COUNCIL AT THE NATIONAL LEVEL

Some nations have established high level committees to make recommendations to governments but also to the private sector. An example is the Dutch Cyber Security Council (Nederlandse Cyber Security Raad, [CSR]). The Cyber Security Council is a national and independent advisory body at the strategic level of the Dutch government and comprises representatives of public and private organisations and the scientific community in the cyber security domain including the CII. The CSR works to raise cyber security in the Netherlands on the strategic level.

Due to the unique composition of the Council (private-public-scientific), it is able to consider priorities, bottlenecks and incidents from various angles and to develop an integral vision on opportunities and threats. The CSR strives to render advice that is theoretically substantiated and practicable.

The Council has been charged with the following duties:

- To provide solicited and unsolicited advice to the government and private parties on relevant cyber security developments. The Council advises the government on the implementation and execution of the National Cyber Security Strategy.

- To propose priority themes on the topic of cyber security, for purposes of, inter alia, attuning government research programmes to one another and, wherever possible, to those of scientific research centres and the business sector. To contribute to the National Cyber Security Research Agenda.
- To contribute to safeguarding public-private cooperation.
- To advise the Dutch emergency response organisation in case of large-scale incidents.

The participation of private stakeholders in the CSR is not essential in order to establish such a high level body on CIIP/cyber security at a national level, although it does reflect a PPP mind-set and is a good example of the benefits of PPP and the variety of ways of implementing it.

7.2.8 GOOD PRACTICE: TRAFFIC LIGHT PROTOCOL (TLP)

In order to establish the level of trust needed for information sharing between public and private organisations, it is necessary to establish procedures on how to deal with sensitive information in a trusted way.

The Traffic Light Protocol (TLP) provides a very easy method for establishing the required level of confidentiality for the information exchanged. One of the key principles of the TLP is that whoever contributes sensitive information also establishes if and how widely the information can be circulated.

The originator of the information can label the information with one of four colours.

- **RED – personal for named recipients only.** In the context of a meeting, for example, RED information is limited to those present at the meeting. In most circumstances, RED information will be passed verbally or in person.
- **AMBER – limited distribution.** The recipient may share AMBER information with others within their organisation, but only on a 'need-to-know' basis. The originator may be expected to specify the intended limits of that sharing.
- **GREEN – community wide.** Information in this category can be circulated widely within a particular community. However, the information may not be published or posted publicly on the Internet, nor released outside of the community.
- **WHITE – unlimited.** Subject to standard copyright rules, WHITE information may be distributed freely, without restriction.

The TLP is used widely, both by nations and by multinational working groups. Its strength is that it is very easy to use and that the responsibility of both the originator and receiver of the information are very clear. Point of attention is that a Freedom of Information Act (FOIA) law or regulation can defeat TLP (see [Luiijf2015]).

The Forum of Incident Response and Security Teams [FIRST] announced the release of version 1.0 of its consolidated Traffic Light Protocol (TLP).

The FIRST TLP addresses some criticisms that users had with prior version, and ensures international sharing can happen without mismatched expectations. It is currently used by various types of CSIRTs, operational trust communities, information sharing analysis organisations, government agencies, and private researchers, and has achieved 'de facto' international standard status.

The FIRST community, in consultation with other security information sharing communities, has established a Standards Special Interest Group (SIG) for TLP. The TLP SIG has drafted a common standardised set of definitions for all TLP colours, along with clear usage guidance explaining how, when and where it should be used [FIRST].

7.3 REFERENCES AND FURTHER READING

[CiSP] UK NCSC web site on 'Cyber-Security Information Sharing Partnership (CiSP)'. On line: https://www.ncsc.gov.uk/cisp

[CPNI IE] UK CPNI Information Exchanges webpage. On-line: http://www.cpni.gov.uk/about/Who-we-work-with/Information-exchanges/

[CSR] NCSC, web page on the Dutch 'Cyber Security Council'. On-line: https://www.ncsc.nl/english/Cooperation/cyber-security-council.html

[EGC] Web page European Government CERTs (EGC). On-line: http://www.egc-group.org

[ENISA] L. Dupré, M. Falessi, D. Liveri, Good Practice Guide on Cooperatve Models for Effective PPPs, ENISA 2011. On-line: www.enisa.europa.eu/publications/good-practice-guide-on-cooperatve-models-for-effective-ppps

[EuroSCSIE] Webpage of European SCADA and Control Systems Information Exchange (EuroSCSIE): https://espace.cern.ch/EuroSCSIE/default.aspx

[FIRST] Web site 'Forum for Incident Response and Security Teams'. On-line: https://www.first.org/tlp

[FS-ISAC] Financial Services Information Sharing & Analysis Center (FS-ISAC) Operating Rules June, 2016, On-line: https://www.fsisac.com/sites/default/files/FS-ISAC_OperatingRules_June2016.pdf

[ICS-CERT] Web page The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). On-line: https://ics-cert.us-cert.gov

[Infraguard] Web site Infraguard (PPP of CI and FBI). On-line: https://www.infragard.org/

[ISAO] The ISAO Standards Organization is a non-governmental organisation. On-line: https://www.isao.org/

[ISAO300-1] ISAO 300-1: Introduction to Information Sharing, ISAO, September 2016. On-line: https://www.isao.org/wp-content/uploads/2016/10/ISAO-300-1-Introduction-to-Information-Sharing-v1-01_Final.pdf

[Johnson2016] C. Johnson, L. Badger, D. Waltermire, J. Snyder, C. Skorupka, NIST Special Publication 800-150 Guide to Cyber Threat Information Sharing, National Institute for Standards and Technology, October 2016. On-line: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

[Luiijf2015] Luiijf, H.A.M., Kernkamp, A., GCCS: Sharing Cyber Security Information, TNO, 2015. On-line: http://publications.tno.nl/publication/34616508/oLyfG9/luiijf-2015-sharing.pdf

[MELANI] Confédération Suisse, Reporting and Analysis Centre for Information Assurance MELANI. On-line: https://www.melani.admin.ch/melani/en/home.html

[NCSC] NCS webpage on Information Sharing and Analysis Centres (ISACS). On-line: https://www.ncsc.nl/english/Cooperation/isacs.html

[NISC.JP2014] The Basic Policy of Critical Information Infrastructure Protection (3rd Edition) – tentative translation, Japan, 2014. On-line: http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3.pdf

[RECIPE] M. Klaver, E. Luiijf, A. Nieuwenhuijs, Good Practices Manual for CIP Policies for policy makers in Europe, TNO, 2011. On line: http://www.tno.nl/recipereport

[UP KRITIS] German PPP UP KRITIS 'Industrie und Kritische Infrastrukturen'. On-line: https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Aktivitaeten/UP_KRITIS/up_kritis_node.html

[US CERT] Web page US Computer Emergency Readiness Team (US CERT). On-line: https://www.us-cert.gov

8 LIST OF ABBREVIATIONS

AU	African Union
B2B	Business to business
CA	Certificate Authority
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CIIR	Critical Information Infrastructure Resilience
CIP	Critical Infrastructure Protection
CIR	Critical Infrastructure Resilience
CPS	Cyber-Physical System
CSIRT	Computer Security Incident Response Team
CSISP	Cyber-Security Information Sharing Partnership
CTO	Commonwealth Telecommunication Organisation
CVE	Common Vulnerabilities and Exposures
DCS	Distributed Control System
EGC	European Governments CERTs
ENISA	European Union Agency for Network and Information Security
FIRST	Forum for Incident Response and Security Teams
FOIA	Freedom of Information Act
G2G	Government to government
GFCE	Global Forum on Cyber Expertise
GLONASS	Globalnaya Navigatsionnaya Sputnikovaya Sistema
GPS	Global positioning system
IACS	Industrial Automation and Control Systems
ICS	Industrial Control System
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ICT	Information and Communication Technologies
ITU	United Nations specialized agency for information and communication technologies – ICTs
IX(P)	Internet Exchange (Points)
NCSC	National Cyber Security Centre
NCSS	National Cyber Security Strategy
NGO	Non-Governmental Organisation
NIAC	National Infrastructure Advisory Council
OAS	Organization of American States
OECD	Organisation for Economic Co-operation and Development
PCDA	Plan-Do-Check-Action
PCS	Process Control System
PPP	Public-Private Partnership
SCADA	Supervisory Control and Data Acquisition
TLP	Traffic Light Protocol

COLOPHON

AUTHORS

Eric Luiijf
Tom van Schie
Theo van Ruijven
Auke Huistra

TNO

Lange Kleiweg 137
2288 GJ Rijswijk
Netherlands
eric.luiijf@tno.nl
TNO.NL

With contributions by Peter Burnett (Meridian Coordinator) and Nynke Stegink (Dutch NCSC), and Martijn Neef (TNO).

This good practice guide was instigated by GFCE-Meridian. A digital version of this good practice guide is available for download at: www.tno.nl/gcciip

MERIDIAN

The Meridian Process aims to exchange ideas and initiate actions for the cooperation of governmental bodies on Critical Information Infrastructure Protection (CIIP) issues globally. It explores the benefits and opportunities of cooperation between governments and provides an opportunity to share best practices from around the world. The Meridian Process seeks to create a community of senior government policymakers in CIIP by fostering ongoing collaboration.

The Meridian Process recognises that it is only by working together that we can each advance our national CIIP goals and objectives. Participation in the Meridian Process is open to all nations/economies and is aimed at senior government policy-makers involved in CIIP-related issues. Every nation/economy is invited to take part in the Meridian Process, and is encouraged to attend the annual Meridian Conference. [www.meridianprocess.org].

GFCE

The Global Forum on Cyber Expertise (GFCE) is a global platform for nations, international organisations and private companies to exchange best practices and expertise on cyber capacity building. The aim is to identify successful policies, practices and ideas and multiply these on a global level. Together with partners from NGOs, the tech community and academia GFCE members develop practical initiatives to build cyber capacity [www.thegfce.com/].

November 2016