Companion Document to the GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers

FOREWORD

The 2016 GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers (hereafter: 2016 GPG) outlined that Critical Information Infrastructure Protection (CIIP) is a complex but important topic for nations. By nature, CIIP is a national security topic in the sense that failure, disruption or destruction of Critical Information Infrastructure (CII) may cause serious impact to the society, economy and well-being of the citizens. Societies at large, critically depend on the proper functioning of the Critical Infrastructures (CI) such as energy supply, telecommunications, financial systems, drinking water, and governmental services. In turn, these CI often critically depend on the proper functioning of CII. CII is a complex concept and includes information and communication technologies (ICT), and operational technologies (OT). OT is also known as industrial control systems and SCADA systems, that monitor and control critical cyber-physical processes. The CII comprises (1) critical ICT infrastructures (e.g. mobile telephony and internet services), (2) critical ICT and OT systems that are part of each CI, and (3) new CII services beyond these established domains.

The focus of the 2016 GPG was providing assistance to nations new to the CIIP topic. The Meridian community identified the need for more elaborate guidance and good practices for both developing and mature nations in this domain on:

- Terminology and definitions.
- Identification of Critical Information Infrastructure (CII).
- The societal uptake of Information and Communication Technology (ICT) and Operational Technology (OT) and their effects on the identification of new critical elements of the national CII.

This Companion Document provides these good practices and guidance in this domain to political leadership and governmental policy-makers in both developing and mature nations.

The writing team, with cooperation of Mr. Peter Burnett (Meridian Coordinator), Mrs. Nynke Stegink (Netherlands National Cyber Security Centre and several Meridian members trust that this Companion Document to the 2016 GPG may be of valuable help to you.

CONTENTS

FIGURES

1 INTRODUCTION

1.1 THE NEED FOR CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

The 2016 GPG [GM2016] outlined that Critical Information Infrastructure Protection (CIIP) is a complex but important topic[1] for nations. By nature, CIIP is a national security topic in the sense that failure, disruption or destruction of critical information infrastructures (CII) may cause serious impact to society, the economy, and the well-being of citizens. Societies at large and, more specifically, critical infrastructures (CI) critically depend on the proper functioning of CII.

Depending on the nation's advancement in utilising digital technologies, a national CII comprises the critical services supplied by:

1. the ICT sector (e.g. mobile telephony and internet services),
2. specific information, communication, and operational technology-based systems and networks in each of the national CI, and
3. critical services beyond the established framework of these CI.

To ease the access to this Companion Document, the notion ICT sector is used rather than explaining each of the possible national variants such as 'IT and telecommunication sector' including variants with two distinct sectors falling under different ministerial responsibilities. Chapter 2 defines and explains CII, and its increasing complexity, in more detail.

1.2 THE PURPOSE OF THIS COMPANION DOCUMENT TO THE 2016 GPG

Many nations are on the path to Critical Infrastructure Protection (CIP), but have difficulties in progressing with CIIP. Other nations are at the very start of their combined CIP-CIIP journey. There are also ample examples of nations that have taken great steps in CIIP development. Their experiences, bad and good, are worth sharing.

In 2016, the Meridian Community [Meridian] and the Global Forum on Cyber Expertise [GFCE] took the initiative to develop a good practice guide on CIIP to provide those valuable insights to nations that are in an early phase of CIIP development.

Although received very well, some readers of the 2016 GPG [GM2016] had difficulties seeing the 'whole CIIP picture' (from prevention to response, and from operational to strategic) and how the good practices fit into this picture. The Meridian community identified the need for more elaborate guidance on the CIIP concepts and terminology.

1 In the remainder of this document, the national security term is not to be confused and equated with the organisation of national security in a nation, e.g. intelligence/security services, ministry of Defence, and alike.

Moreover, the community identified three important topics, for both developing and more developed nations in the CIP/CIIP domain, that require more elaboration:

1. Definitions and terminology,
2. Identification of CII,
3. The societal uptake of ICT and OT and their effects on the identification of new elements of the national CII.

1.3 HOW TO USE THIS COMPANION DOCUMENT?

This Companion Document provides good practices and guidance to the political leadership and government policy-makers of both developing and more mature nations in this domain. In its present form, as a Companion Document,[2] the contents should be read in conjunction with the 2016 GPG. The three topics in this Companion Document deepen and add good practices to the sections 1.3 "CII, CIIP and Cyber Security", 4.2 "Good practices for the identification of CII" and 6.2 "Good practices for monitoring and continuous improvement" of the 2016 GPG.

1.4 REFERENCES AND FURTHER READING

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

[GM2016] GFCE-MERIDIAN (2016), GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers. On-line: https://www.thegfce.com/initiatives/c/critical-information-infrastructure-protection-initiative/documents/reports/2016/11/10/ciip-good-practice-guide and via https://www.tno.nl/gcciip

[Meridian] Meridian permanent website. On-line: https://www.meridianprocess.org

2 The authors have the intent to integrate both documents in due course.

2 CLEAR CIIP TERMINOLOGY

2.1 GENERAL DESCRIPTION AND MAIN CHALLENGES

Nations addressing the topic of CIIP are sometimes hampered because of their confusion and lack of clarity about the key concepts, related definitions and terminology. In the CIIP domain, such confusion is sometimes caused by the fact that a relatively small group of experts tries to convey the CIIP concept to government policy-makers in unnecessarily complex terminology.

The risk of a lack of clarity and understanding includes failure to align the whole of government with respect to a wide range of policy areas and functions involved in CIIP. CIIP, for example, relates to national security policies in the sense that failure, disruption or destruction of CII may cause a profoundly deleterious effect to society, the economy, and well-being of citizens.

Policy departments responsible for traditional infrastructures, such as energy, security, telecommunications, drinking water etc, may need to adapt their policies and regulation to cope with CIIP. CIIP also relates to the policy domains of economic development and international relations. By nature, CIIP requires multi-stakeholder governance and cooperation at strategic, tactical and operational levels: mixtures of public and private stakeholders, manufacturers, system integrators, users, and maintenance organisations involved in applying ICT and OT. National governments also need to decide on the right prioritisation and balance for CIIP in the competition for resources, e.g. against other risk factors (as in UK's National Security Risk register), and against other related topics such as cybercrime, which may appear more urgent or fashionable.

The challenge therefore is to support governmental policy departments and their tactical and operational functions and agencies in clarifying CIIP and the CIIP-related concepts and definitions. Their understanding can then be conveyed to all other stakeholders such as operators of CII.

Organisations who provide information infrastructural services which may be, or are designated as, part of the national CII, have different perspectives on the impact arising from disruption or failure of their ICT and OT infrastructure. A key challenge is getting these organisations to appreciate the difference between infrastructure that is business-critical to the organisation itself, versus infrastructure that is nationally-critical to the nation's wellbeing. Note that overlap may occur. When defining and protecting CII, one constantly needs to remind all stakeholders that CII is about the potential impact that information infrastructure has at the national level, instead of at the level of the organisation.

2.1.1 CONCEPTS AND DEFINITIONS – A SHORT BACKGROUND

A collective understanding of concepts and terminology allows people and organisations to communicate and understand each other without the need to explain and discuss a concept at length, again and again.

Once a concept is understood well, a definition can be created to share the concept and properties in precise wording[3]. Properties (or criteria), such as impact size or amount of damage after a CII disruption, are most often specified at the time of 'implementation' of the definition, e.g. in regulation or sector code. This distinction is crucial when defining the CII at the highest level of abstraction on the one hand (e.g. internet), and the set of critical services and their operators on the other hand. For example: internet access may be defined as a critical service to a nation; a single internet access operator may have over 45% of the market share in the nation, and is therefore considered to be a key operator of the CII.

2.1.2 GOOD PRACTICE: DEFINE A COHERENT SET OF CIIP-RELATED DEFINITIONS

A good practice is first and foremost to use a set of coherent definitions. Four approaches have been found:

1. Academically precise. Define the coherent set of CIIP-related definitions in an academic way. This can be a very tedious and lengthy process when one wants to straighten out all details in strict definitions. Moreover, the result may need to be changed as soon as new insights and technologies appear in this fast-moving domain.
2. A pragmatic good practice is to reuse existing definitions created by other nations or organisations.
3. Another pragmatic approach, when definitions are unavailable or unfit for the national context, is to quickly create a set of 'unpolished' definitions and refine them later when needed.
4. No definitions. Do not define the concepts, but write policy papers using the terms 'critical information infrastructure protection', 'cyber security', and others interchangeably. This is not a recommended approach as it requires that the author's own ideas about a concept align, in the end, with those of others and is likely to cause confusion.

Creating a national set of CIIP-related definitions can be done from scratch. A good practice, however, is to look for and reuse existing definitions. Such definitions can be found in international standards, or in public documents of other nations. A useful resource, which globally collects definitions on terminology in the CIP and CIIP domains, is [CIPedia].

Definitions that are reused can be tweaked for one's own national understanding, but preferably should be used without changes, as that helps in international discussions and understanding. Moreover, it should be noted that some nations, e.g. Spain, approach the CI

3 A definition is "a statement which captures the meaning, the use, the function and the essence of a term or a concept." From: V. Veerasamy (2013), The Importance of Good Definitions (Or: How To Think Clearly). On-line: https://www.referralcandy.com/blog/importance-of-good-definitions/

topic in a holistic way. They do not make any distinction between CI and CII and apply the concept of integral physical and cyber security to CI.

Although CIIP is inherently a national security topic in the sense that failure, disruption or destruction of CII causes serious impact to society, the economy, and the well-being of citizens, one needs to realize before reusing a definition of another nation that some nations have created CIIP-related definitions from another perspective rather than a strategic view on national security, e.g. an anti-cybercrime view.

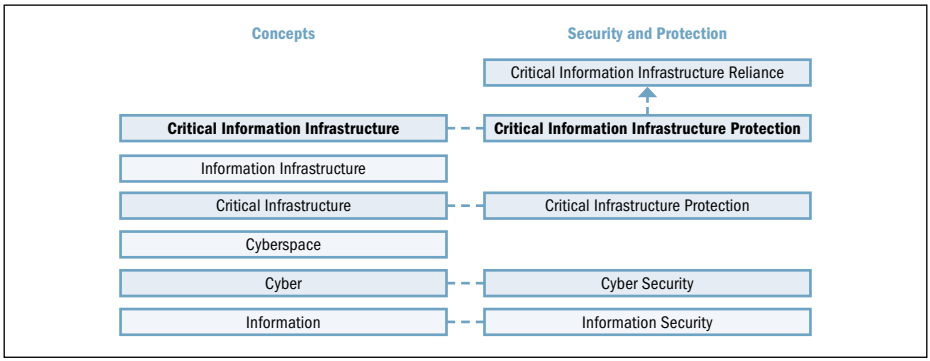

Figure 1: Stack of security and protection definitions related to concepts

To ease the understanding of CIIP and related concepts, Figure 1 shows a selection of key concepts on the left side and the terms which relate to their security and protection on the right. Below, these concepts and definitions are discussed with the focus on the terms that are depicted in bold (CI, CIP, CII, CIIP).

CONCEPT: INFORMATION

Information is defined by the Oxford dictionary as "what is conveyed or represented by a particular arrangement or sequence of things." In the cyberspace realm, information equates to a "representation of things in a way that it can be transmitted, processed, and stored for later (re)use."

PROTECTION: INFORMATION SECURITY

Information Security is defined by the International Organization for Standardization (ISO) in a very concise way as a set of information-related properties that have to be preserved: "Preservation of confidentiality, integrity and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved." (ISO/IEC 27000, 2014).

The US National Institute of Standards and Technology (NIST) has defined information security from a protection angle: "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to

provide confidentiality, integrity, and availability." [NIST2013]. These and similar national and international definitions describe security properties closely related to information and the systems that process, store and transmit information; but not cyber security which is a broader concept than information security.

CONCEPT: CYBER

Cyber is a prefix nowadays used to describe a "person, thing, or idea as part of the computer and information age."[4] The notion of cyber was derived from *κυβερνήτης* or kybernetes which is the Greek word for "steersman" or "governor". The term was first used in the book title "Cybernetics: Or Control and Communication in the Animal and the Machine" by Norbert Wiener in 1948.

PROTECTION: CYBER SECURITY

Cyber Security is a broader concept than information security as it refers to organisational aspects, processes, practices, and human factor aspects in dealing with general risk in cyberspace and the taking of a wide range of mitigating measures to reduce that risk. For example, Hungary defines cyber security as: "Cyber security is the continuous and planned taking of political, legal, economic, educational, awareness-raising and technical measures to manage risks in cyberspace that transforms the cyberspace into a reliable environment for the smooth functioning and operation of societal and economic processes by ensuring an acceptable level of risks in cyberspace".

Sometimes, the risk to minimise is referred to as well, e.g. the Austrian definition of cyber security states: "Cyber security describes the protection of a key legal asset through constitutional means against actor-related, technical, organisational and natural dangers posing a risk to the security of cyberspace (including infrastructure and data security) as well as the security of the users in cyberspace." And last, but not least, the ITU defines cyber security as: "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." [ITU2009]

Cyber Security is therefore much broader than Information Security, but also from CIIP as the latter only concerns risk at the level of national security through (the chance of) serious disruption or destruction of a critical designated information infrastructure.

CONCEPT: CYBERSPACE

A wide range of definitions for 'cyberspace' exists. Some definitions only consider internetworked technology, whereas others define cyberspace as the total sphere of computer hardware, software, networks, information, processes and humans (as operators/ end users).

4 Derived from: http://searchmicroservices.techtarget.com/definition/cyber

An example of the first type of definition is Australia's "Cyber space is the virtual space of all IT systems interconnected at data level on a global scale", which is close to defining the internet. The broader concept of cyberspace includes embedded processors, sensors, smartcards, internet-of-things (IoT), industrial internet-of-things (IIoT), operational technology (OT) and any "new computerised-technology" to come. India's definition of cyberspace is an example, although OT is not explicitly mentioned: "Cyberspace is a complex environment consisting of interactions between people, software and services, supported by worldwide distribution of Information and Communication Technology (ICT), devices and networks." In the context of both current and future CII, the use of a broader, holistic cyberspace definition is recommended.

CONCEPT: CRITICAL INFRASTRUCTURE (CI)

There exist many national definitions for the concept of Critical Infrastructure, see e.g. [CIPedia]. Kenya, for example, defines CI as "assets that are essential for the functioning of a society and economy. (e.g., electrical grid, telecommunications, water supply). Spain defines CI as: "strategic infrastructures (that is, those that supply essential services) the functioning of which is necessary and does not allow alternative solutions, reason why their disruption or destruction would have serious impact on essential services" and India as "those facilities, systems, or functions, whose incapacity or destruction would cause a debilitating impact on national security, governance, economy and social well-being of a nation." Most of these definitions contain elements of criticality and impact to avoid, for example: "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]

PROTECTION: CRITICAL INFRASTRUCTURE PROTECTION (CIP)

A smaller number of formal definitions for Critical Infrastructure Protection exist, as the objective of protecting the unwanted impact is quite clear by itself. Amongst the formal definitions you may find in [CIPedia], we can point at EU's definition for CIP: "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]

CONCEPT: INFORMATION INFRASTRUCTURE

Information infrastructure is a relatively ambiguous concept. Definitions range from technical to almost political-oriented concepts. Below we will use Information infrastructure in the sense of the Finnish definition "the structures and functions behind information systems that electronically transmit, transfer, receive, store or otherwise process information (data)". Our understanding aligns with this definition which reflects the wider perspective of cyberspace above.

CONCEPT: CRITICAL INFORMATION INFRASTRUCTURE (CII)

Critical Information Infrastructure (CII) is defined by a large set of international bodies and nations, e.g. the OECD defines CII in [OECD2008] as: "those interconnected information and

communication infrastructures, the disruption or destruction of which would have serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy." Japan, as another example, defines CII as: "Critical Information Infrastructure (CII) is the backbone of national life and economic activities formed by businesses providing services that are extremely difficult to be substituted. If the function of these services is suspended, deteriorates or becomes unavailable, it could have a significant impact on the national life and economic activities."

Key components of the various definitions are: (1) it concerns the information infrastructure, (2) which is critical, vital, essential or another specific explanation of 'criticality' (depending on national choice of terminology), (3) given threats against availability, reliability and resilience seriously impacting the nation.

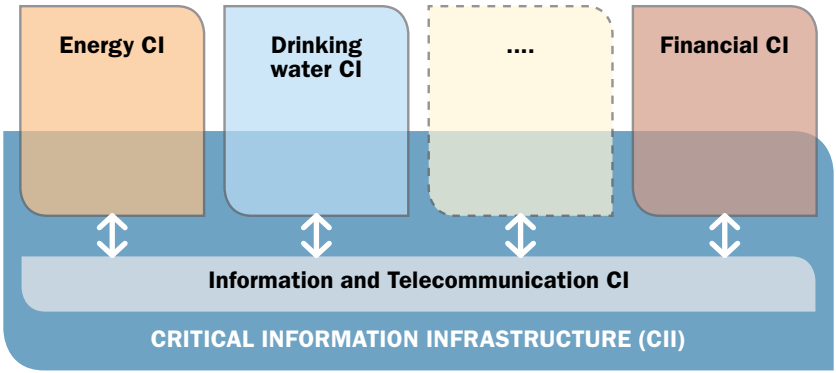

Figure 2: Critical Information Infrastructure (CII). Based on [GM2016]

Most CII definitions struggle in clearly understanding and defining the information infrastructure component. Obviously, this is complex as the critical ICT-based and OT-based functions and other services hide themselves in the (vertical) CI, the ICT CI, and even beyond these established domains. As is shown in Figure 2, depending on the maturity and critical use of digital technologies the CII subsequently comprises:

1. Critical elements and services of the 'ICT sector'.
   This may be mobile telecommunication data services, internet exchange points (IXP), domain name services, certificate infrastructure and Global Navigation Satellite Systems (BeiDou, Galileo, GLONASS, GPS);
2. Critical information and communication infrastructure elements in each of the CI.
   This may include e.g. critical financial transaction systems in the financial sector, critical logistical information chains, OT monitoring and controlling critical cyber-physical systems such as in power transmission, gas transport, harbours, railways, healthcare and refineries;

3. The products and services of manufacturers, vendors and system integrators which are used across multiple CI sectors, nationally and internationally, whose vulnerability or common failure may negatively impact the proper functioning of CII and the CI that they are a critical element of.

   Examples:
   – an exploited vulnerability within routers of the top-5 manufacturers in the world affecting a large part of the internet infrastructure,
   – a major exploitable risk to OT in power generation and transmission, drinking water production and transport, as well as rail (train, metro) and harbour systems, or
   – a 'deeply-buried systemic weakness' in the chip set of credit and debit cards.

With ongoing digitisation, CII tends to increasingly extend beyond the established CI domains. Governmental policy makers should anticipate the existence of CII elements:
1. which are operated by organisations outside the classical ministerial supervision and/or regulation,
2. which are physically located outside the nation,
3. and/or are operated by foreign operators.

PROTECTION: CRITICAL INFORMATION INFRASTRUCTURE PROTECTION (CIIP)

Only a limited number of nations have defined Critical Information Infrastructure Protection as is shown by a collected set of definitions [CIPedia]. Nations like the Czech Republic and Spain consider CIIP to be an integral part of CIP. Estonia shows both an all-hazard approach and a minimum service level to maintain in their definition: "trouble-free functioning of the country's essential information and communication systems under ordinary circumstances and to ensure their continuity on a minimum level during critical situations."

The key objective of CIIP is "protection" against all hazards, of the CII, by all means; in other words: avoiding the occurrence of serious impact incidents. Protection activities should therefore balance and unite a broad range of people, processes and technology-related activities. An example definition of Critical Information Infrastructure Protection therefore builds on the CII definitions described above and a global understanding of CIP definitions [CIPedia]: "Critical Information Infrastructure Protection (CIIP) is all activities aimed at ensuring the functionality, continuity and integrity of CII to deter, mitigate and neutralise a threat, risk or vulnerability or minimise the impact of an incident".

As stated earlier, CIIP is a national security topic. Therefore, CIIP should be a core element of the National Cyber Security Strategy (NCSS) and or the CIP-related part of the national security / civil emergency planning strategy.
All CIIP stakeholders need to understand that the CIIP objectives are not equivalent to business continuity and protecting business critical processes, although both types of protection activities may coincide. Moreover, CIIP is distinct from cyber security objectives

which, amongst other things, address ordinary cybercrime, privacy and human rights issues, and economic cyberspace matters, although cyber security measures may contribute to CIIP.

CIIP-activities include protection measures such as developing operator security plans, physical security, electromagnetic security, screening and training of personnel, inter-organisational collaboration (e.g. joint protection of CII resources in a CI supply chain), collecting threat intelligence, information sharing, trust building, and cyber security. It will be clear that both internal and external multi-stakeholder aspects form a major proportion of the CIIP-related activities.

PROTECTION: CRITICAL INFORMATION INFRASTRUCTURE RESILIENCE (CIIR)

Increasing attention is given in academia, business, organisations, and in context of smart cities, to the "resilience" concept. The UN International Strategy for Disaster Reduction (ISDR)[5] has defined resilience as "the ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions." The US National Infrastructure Advisory Council (NIAC) has defined infrastructure resilience as: "the ability to reduce the magnitude and/or duration of disruptive events." [NIAC2009]

As the term Critical Information Infrastructure Resilience (CIIR) starts to appear in literature, we add the term to this list. What is important under CIIR is that the impact and duration of a CII incident are reduced as much as possible. This is especially relevant as the complexity of cyber space is making it increasingly difficult to protect CII and prevent incidents. CIIR is different from CIIP, which objective is to protect against the risk of a critical incident occurring in the first place. Resilience focuses on preparation, incident response, recovery, and after-incident activities.[6] The activities of "pro-action" and "prevention" (the first elements of the incident response cycle) make of course a valuable contribution to CIIR.
From a national security perspective and the risk to CII, one may argue that the focus of a nation's activities should be on CIIP: prevent incidents from occurring. From that perspective, CIIR could only be a secondary objective.
Critical information infrastructure resilience (CIIR) therefore can be defined as: "The ability to reduce the magnitude and/or duration of the impact of disruptive events in CII".

5 See: https://www.unisdr.org/we/inform/terminology
6 The full cyber incident response cycle comprises: pro-action, pre-emption, prevention, preparation, incident response, recovery, aftercare/ follow up). See e.g. Chapter 4: Organisational Structures & Considerations of [Klimburg2012].

2.2 REFERENCES AND FURTHER READING

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

[GM2016] GFCE-MERIDIAN (2016). GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers. On-line: https://www.thegfce.com/initiatives/c/critical-information-infrastructure-protection-initiative/documents/reports/2016/11/10/ciip-good-practice-guide or via https://www.tno.nl/gcciip

[ISO/IEC 27000] ISO (2014). ISO/IEC 27000:2014 Information technology – Security techniques – Information security management systems – Overview and vocabulary.

[ITU2009] ITU (2009), ITU X.1205: Overview of cybersecurity. On-line: https://www.itu.int/rec/T-REC-X.1205-200804-I

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

[NIAC2009] US Homeland Security/National Infrastructure Advisory Council (2009), Critical Infrastructure Resilience Final Report and Recommendations., page 8. On-line: https://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf

[NIST2013] NIST (2013). Glossary of Key Information Security Terms, NISTIR 7298 rev 2. On-line: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

[OECD2008] OECD (2008), OECD Recommendation of the Council on the Protection of Critical Information Infrastructures C(2008)35. On-line: http://www.oecd.org/sti/40825404.pdf

3 IDENTIFICATION OF CII

Many nations – including some nations with an established CIIP policy – lack a mature and structured approach to the identification of CII [ENISA2014]. Much academic work has been done in the past on the identification of CI and CII that is still useful to improve CIIP policies worldwide. The main challenge for many nations is not to develop a new or better methodology, but to adopt and implement an effective methodology with the support of existing methods.

In this chapter, we use available insights and methodology in the body of knowledge on CIIP (and CIP), in combination with insights from recent research and contemporary examples, to provide several good practices for the identification of CII. This chapter elaborates on chapter 4 "Identification of Critical Information Infrastructure" of the 2016 GPG.

3.1 GENERAL DESCRIPTION AND MAIN CHALLENGES

3.1.1 THE IMPORTANCE OF IDENTIFYING CII

Disruption of information infrastructures can have a severe impact on the well-being of a nation, in terms of economic costs as well as through indirect physical damage or societal unrest. To reduce the risk of disruption of information infrastructures, a key issue is to identify which information infrastructure elements are critical to the nation and which information infrastructure elements are merely 'very important'. Separating critical elements from other elements of information infrastructures enables nations to focus protective efforts on those critical elements and to maintain national security effectively.

Identifying CII is relevant and challenging for both developing and more mature nations because continual changes in information infrastructures and their use inevitably alter what is critical and what is not. Identifying CII is therefore not a one-time but a continuous effort. Continuous attention to the identification of CII is required for a nation to address the CII-related aspects of the risk to national security effectively.

3.1.2 THE MAIN CHALLENGES OF IDENTIFYING CII

The challenges of the identification of CII stem from the complexity of Information and Communication Technology (ICT) and Operational Technology (OT) and its embeddedness in Critical Infrastructures. The main challenges of identifying CII are:

– CIIP is sometimes perceived as a subset of CIP. Nations following that approach may underestimate the risk related to ICT and OT to their nation. However, nations in an early adaptation phase of ICT, may start defining their CII as consisting of one or more critical ICT-sector services. The use of ICT and OT in critical processes within CI sectors (if defined) can then be perceived as a CI sector specific responsibility.
  More advanced use of digital technologies by nations, however, requires a cross-CI sector approach as the risk related to ICT and OT in critical processes need to be mitigated.
  For example, certain malware may target OT systems of the power and gas grids, drinking

water and chemical plants. The same CI industries may be targeted by denial-of-service attacks via critical ICT-sector services.
As explained in section 2.1.2, more matured nations have to consider the criticality of new information infrastructure services beyond the established CI domains.

– The criticality assessment of information infrastructure elements requires a collective understanding of the term critical. However, what is critical is often in the eye of the beholder. Setting objective criteria for criticality is an analytical challenge and can reveal conflicting interests in which some sectors or stakeholders are looking to be labelled as 'critical' while others try to avoid it. An incentive for the first approach may be for the government to pay for additional security measures. On the other side, some sectors or organisations may try to avoid additional regulations, inspections and the obligation to invest in additional security measures.
– To assess the criticality of CII, expertise from within the potentially critical sectors is required. This implies that identification of CII is a joint endeavour between sector experts and national security experts. National security experts may be confused by sector-specific information and sector-specific terminology which they may have difficulty evaluating. Therefore, they may experience difficulties in identifying those insights that are relevant from the national security and public policy perspective. On the other hand, sector experts may lack the broad overview and objectivity of national security experts.
– Large scale and prolonged disruption of CII is generally a high-impact, low-probability event. Real-world examples of such CII disruptions are scarce. Therefore, dependencies and cascading effects must often be deduced by expert judgement instead of being based on real cases and data.
– Many methods for the identification of CII originate from specific CI sectors and from the generic risk analysis domain – with limited attention to dependencies and cascading effects between sectors. There is a selection of methodologies available for criticality assessment [CIIP2008, ENISA2014]. Nations may have difficulties finding the right method and sufficiently accommodating dependencies between sectors.

3.2 GOOD PRACTICES FOR THE IDENTIFICATION OF CII

This section contains several good practices for the identification of CII. The good practices are derived from the academic literature and suggestions from experts within and outside the Meridian community.

3.2.1 GOOD PRACTICE: ADOPT A LAYERED APPROACH FOR THE IDENTIFICATION OF CII

The identification of (critical) sectors layer is often the point of departure for CIP and CIIP as sectors are clearly delineated and cover a range of (critical) processes and systems. A good practice is to adopt a layered approach for the identification of CII. A layered approach means using multiple levels of analysis to describe, analyse and identify CII. The academic literature provides several models or frameworks that help distinguish between levels of analysis [CIIP2008, Theoh2010].

Layers of CII that are frequently mentioned in the literature are:

1. the intra-sector layer,
2. the (critical) sector layer,
3. the core functions layer(e.g. individual systems or operators),
4. the critical resources layer (assets, technical components).

A layered approach helps to identify and structure elements of CII. Within each critical sector, core functions can be distinguished to focus on critical parts of a sector instead of the whole sector. Within core functions, critical resources can be distinguished to narrow the reach and focus of CIIP to specific assets and components. These levels of analysis – from sector to component – enable researchers and policy-makers to set critical elements apart from information infrastructures as a whole. Beyond each critical sector, at the intra-sector level, dependencies between sectors can be analysed, which is necessary to assess the criticality of specific sectors. Also, threats to critical resources that are used in multiple sectors can be analysed, which is necessary to assess the common vulnerability of multiple sectors combined.

A layered approach supports the development of criticality criteria. Many nations have developed criteria and identified CI(I) at a sectoral level (e.g., Austria, Germany, India, the United States, Sweden). Identification of core functions or critical resources is less common [ENISA2014]. The intra-sector or national layer and the sector layer are generally the domain of national authorities that may focus on the criticality of individual sectors and cross-sector dependencies regarding societal well-being and national security.[7] Core functions and critical resources must generally be jointly identified by national authorities and the CII operators.

An example of a CIIP policy that includes a layered approach to CII can be found in Estonia. Estonia has identified CII using a multi-layered, stepwise approach [ENISA2014]. The CI sectors of Estonia have been identified as part of Estonia's CIP policy. For each CI sector, a 'service organiser' (the relevant ministry) is selected that determines criteria and thresholds to identify critical service providers within the sector (this resembles the core functions or critical sub-sector level). The identified critical service providers performed a risk analysis, listed critical resources, and drafted risk mitigation and business continuity plans (this resembles the critical resources level). The Estonian Information System Authority (RIA) checked these lists of critical resources and risk mitigation plans. On basis of the combined list of critical resources of all critical service providers, RIA has composed a national list of CII. This list resembles the intra-sector level approach to identifying CII.

7 National security in the sense that failure, disruption or destruction of CII may cause serious impact to the society, economy and well-being of the citizens.

3.2.2 GOOD PRACTICE: IDENTIFY CRITICAL ELEMENTS OF THE ICT SECTOR AND CRITICAL INFORMATION INFRASTRUCTURE ELEMENTS OF OTHER CI SECTORS

Making a distinction between critical elements of the ICT sector[8] and CII elements for other CI sectors is a good practice to communicate clearly about CIIP and to develop suitable criticality criteria for all elements of CII. Critical elements of the ICT sector may be Internet Service Providers, Internet Exchanges or major cloud service providers. Disruption of the operations of these actors, and the systems they operate, may directly affect the well-being of a nation and pose a threat to national security. CII elements for other CI sectors may be specific communication networks, information systems or Industrial Control Systems.

The relation between the two is depicted in Figure 2. The figure and accompanying text makes clear that CII is located in both the ICT sector and within the other CI sectors, and even may exist beyond those established CI domains. Moreover, attention must be paid to the critical aspects of the vulnerabilities stemming from the use of software and hardware (globally) produced by a limited set of OT and ICT manufacturers, vendors and system integrators. Their products, systems and services are used across sectors and in multiple nations.

A challenge is the fact that government structures often have a ministry or department (vertically) responsible for one or more CI, and another ministry or department responsible for the ICT sector. A holistic CII identification and governance approach to all aspects of CII may result in turf battles. However, the dispersion of critical ICT and OT outside the classical vertical CI structures is an on-going development (chapter 4 addresses this issue). Keeping oversight of CII and maintaining consistency in the identification of CII requires a coordinated approach between all government actors involved, instead of distinct CIIP initiatives within each CI.

3.2.3 GOOD PRACTICE: INCORPORATE DEPENDENCY ANALYSIS IN THE CRITICALITY ASSESSMENT OF INFORMATION INFRASTRUCTURE

An information infrastructure may need to be classified as CII due to dependency of other critical systems upon this information infrastructure. These dependent systems may either be part of CI or CII. Both the dependency of other CI and CII should be part of the criticality assessment of information infrastructure. If a layered approach is adopted (see section 3.2.1), dependencies between CII at distinct layers (from critical resources, to core functions, to critical sectors) must be addressed as well as dependencies of CI on various levels of CII (cross-sector dependencies).

Assessing dependencies can be done in several ways [Nieuwenhuis2008]. Most often, it is done on basis of expert opinion or modelling and simulation. During the analysis of dependencies, special attention is required for information infrastructure elements that serve multiple CI(I). Disruption of such elements will cause multiple C(I)I to fail simultaneously which amplifies the disruptive effects.

8 To ease the access to this Companion Document, we will use the notion ICT sector rather than explaining each of the possible national variants such as 'IT and telecommunication sector' including variants with two distinct sectors falling under different ministerial responsibilities.

An example of a potential CII is a Virtual Private Network (VPN) service that can be used to secure the confidentiality of communications while using the Internet as a transmission service. VPN connections are used by CII operators in the ICT sector as well as CI operators such as energy or financial institutions. Specific VPN services may become an element of CII when CI and CII rely on the availability and functioning of a particular VPN service.

3.2.4 GOOD PRACTICE: USE SPECIFIC AND OBJECTIVE CRITICALITY CRITERIA TO IDENTIFY CRITICAL RESOURCES

Assessment of potentially critical information infrastructures can only be done well with support of specific and objective criticality criteria [Fekete2011, Theoh2009]. The criticality criteria specific which properties an information infrastructure must have to qualify as a CII (see section 2.1.1). When a layered approach is used (see the good practice in section 3.2.1), criticality criteria are required for each layer (critical sectors, core functions, and critical resources).

Sectoral criticality criteria are generally part of a national or multinational CIP policy. Identification of core functions may also be part of a CIP policy or a specific feature of CIIP. In both situations, specific criteria to assess the criticality of core functions are required. An effective CIIP policy also requires the identification of critical resources. This includes resources in the ICT sector and the information infrastructure elements of CI.

To identify critical resources, it is also necessary to incorporate dependencies into the criticality criteria because it is often not the immediate, first-order impact of disruption of resources that makes them critical, but the effect of disruption on other C(I)I elements. The criticality of resources that are used across multiple CI sectors and of which failure disrupts the functioning of CII and the CI they are a critical element of, can only be assessed when dependencies are known. By incorporating dependencies (see good practice in section 3.2.3), the debilitating effects of disruption of critical information infrastructure elements on the national well-being remains the crucial point of reference.

3.2.5 GOOD PRACTICE: ASSESS CRITICALITY WITH SUPPORT OF SURVEYS AND DATA

Criticality assessment is often based on expert judgment. If possible, nations should strive to extend the criticality assessment with surveys involving CI operators and (potential) CII operators. In CI(I) sectors with many stakeholders, surveys may provide more elaborate insight into the overall or average criticality of potential CII than the judgement of experts. Data on dependencies and consequences of failures from CI and CII operators may provide even more and reliable insight although sufficient attention must be paid to confidentiality and possibly sensitive information.

An example of a survey to increase insight in CI dependencies on information infrastructure beyond national borders – i.e. cross-border dependencies of CII – can be found in a study on regulating cross-border dependencies of CII [Kaska2015]. The study addresses similarities and differences between CIP and CIIP in twelve nations and assesses the dependency of each nation on cross-border CII. Dependencies varied between nations but energy, finance and

transportation were found to be most dependent on cross-border CII in all nations. The study concludes that, in general, there are few measures that nations can take to directly deal with cross-border dependencies. Only three respondents (Spain, Estonia and Hungary) reported specific legal obligations to assess and mitigate cross-border dependencies on CII. The study results are informative to all governmental policy-makers and regulators as they provide general insight in cross-border dependencies of CII and the associated legal, policy and strategic issues.

3.2.6 GOOD PRACTICE: CONSIDER THE VALUE OF CRITICALITY CRITERIA UNDER DIFFERENT CONDITIONS

The impact of disruption of CII is often assessed during 'normal' operational conditions in the sense that the effects of a disruption is estimated on basis of the assumption that all other things remain equal. Disruption of a telecommunications network, for example, is generally assessed in isolation and not in combination with disruptions in other critical sectors or specific circumstances. Disruption of CII might be the effect of a crisis condition such as disrupted energy supply, flooding, extreme weather, or a large-scale cyber-attack. Under specific circumstances, specific information infrastructures, for instance those information infrastructures used for crisis response or satellite communication links as backup to general communication links, can be considered as CII. Under normal operational conditions, these systems are not considered to be CII. [Nieuwenhuijs2008]. A practical example of the incorporation of different conditions is to include seasonal dependencies for regions in which the population alters significantly during specific seasons, e.g. tourist areas. Telecommunication networks in such areas may not satisfy criticality criteria during winter as their disruption does not affect effect enough people or cause a significant economic impact while the effects do pass the threshold during summer.

3.2.7 GOOD PRACTICE: LOOK AT OTHER NATIONS FOR INSPIRATION BUT REMAIN SENSITIVE TO NATIONAL PARTICULARITIES

Looking at the body of knowledge on CIIP, governmental policy-makers have a multitude of approaches for identifying CII to choose from. In line with ENISA (2014), a good practice for nations is to choose a portfolio of approaches to assess CII rather than pick one as a one-size-fits-all. ENISA also concludes that only nations that are ranked high on the World Economic Forum Network Readiness Index (WEF NRI) tend to have a structured approach to CIIP. This indicates that willingness to invest the necessary resources for a structured approach to CIIP comes with far reaching digitisation.

Having a well-established CIIP policy is vital to the security of a nation. Governmental policy-makers should tailor their CIIP policy to the specific conditions of the nation, being the degree of digitisation or other particularities like unique CI or specific dependencies on specific ICT and OT. Because of the global trend of increasing digitisation, government policy-makers should regularly reassess the need to step-up their efforts on CIIP.

3.3 REFERENCES AND FURTHER READING

[Kaska2015] Kaska, K. and Trinberg, L. (2015). Regulating cross-border dependencies of Critical Information Infrastructures, NATO Cooperative Cyber Defence Centre of Excellence (CCD-COE), Tallinn. On-line: https://ccdcoe.org/sites/default/files/multimedia/pdf/CII_dependencies_2015.pdf

[CIIP2008] Brunner, E. M., & Suter, M. (2008). International CIIP handbook 2008/2009, Center for Security Studies, ETH Zurich. On-line: http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-08-09.pdf

[ENISA2014] Mattioli, R., & Levy-Bencheton, C. (2014). Methodologies for the identification of Critical Information Infrastructure assets and services. ENISA Report–2014–43. On-line: https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis/at_download/fullReport

[Fekete2011] Fekete, A. (2011). Common criteria for the assessment of critical infrastructures. International Journal of Disaster Risk Science, 2(1), 15-24. On-line: https://link.springer.com/article/10.1007/s13753-011-0002-y

[GM2016] GFCE-MERIDIAN (2016), GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers. On-line: https://www.thegfce.com/initiatives/c/critical-information-infrastructure-protection-initiative/documents/reports/2016/11/10/ciip-good-practice-guide or via https://www.tno.nl/gcciip

[Katina2013] Katina, P. F., & Hester, P. T. (2013). Systemic determination of infrastructure criticality. In: International journal of critical infrastructures, 9(3), 211-225. On-line: https://doi.org/10.1504/IJCIS.2013.054980

[Nieuwh2008] Luiijf, H. A. M., Nieuwenhuijs, A. H., & Klaver, M. H. A. (2008). Critical infrastructure dependencies 1-0-1. In Infrastructure Systems and Services: Building Networks for a Brighter Future (INFRA), 2008 First International Conference on (pp. 1-3). IEEE.

[Theoh2010] Theoharidou, M., Kotzanikolaou, P., & Gritzalis, D. (2010). A multi-layer criticality assessment methodology based on interdependencies. Computers & Security, 29(6), 643-658. On-line: https://doi.org/10.1016/j.cose.2010.02.003

[Theoh2009] Theoharidou, M., Kotzanikolaou, P., & Gritzalis, D. (2009). Risk-based criticality analysis. Critical Infrastructure Protection III, 35-49. On-line: https://doi.org/10.1007/978-3-642-04798-5_3

4 TECHNOLOGICAL DEVELOPMENTS AND THE IDENTIFICATION OF NEW CII

CIIP is an ongoing challenge for governmental policy-makers and political leadership. Effective CIIP requires a constant outlook to the future. Developments in ICT and OT continuously alter the nature of CI and CII. The increasing use of ICT and (embedded) OT to monitor and control critical and complex cyber-physical systems means that many CI have a CII component or are slowly transforming into CII. This has already happened within the financial sector in many nations. Smart grid technologies are also fundamentally changing the energy sector and may introduce new CII elements. Continuous developments in digital technology require nations to keep track of the changing risk landscape and to review CIIP policy accordingly, as was pointed at by chapter 6 of the 2016 GPG [GM2016].

This chapter identifies challenges that developments in technology and its use pose to CIIP policy-makers. Several good practices for signalling and monitoring developments and their implications for CIIP are provided.

4.1 GENERAL DESCRIPTION AND MAIN CHALLENGES

4.1.1 THE CHALLENGE OF UNDERSTANDING DEVELOPMENTS IN TECHNOLOGY

Assessing what is critical in an information infrastructure is notoriously difficult. This is especially the case with new technology and developments in the use of technology. With a well-established CIIP policy, a nation is ready to tackle recognised changes and developments. However, developments in technology are rarely fully known. The use of emerging technologies and the critical dependencies of the nation upon them may appear as a relative surprise.

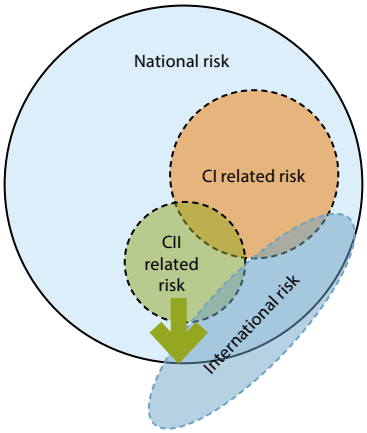

Figure 3: National and international risk includes the CI risk and CII risk

The hyper-connectivity of modern technology contributes to the difficulties in seeing developments in the criticality of information infrastructures. Complexity is created by linking to, or even outsourcing services elsewhere in cyberspace. The increasing number of connections between systems is also altering existing dependencies and introducing new dependencies within CII and between CII and CI. Dependencies may shift in unforeseen ways due to unanticipated adoption of traditional or seemingly unimportant information infrastructure elements. Such changes may cause other information infrastructure services to become critical to the nation.

As discussed in previous chapters, CII is only partly embedded in the traditional vertical governance structures of CI and the ICT-sector. Apart from the critical ICT and OT elements within specific CI, and the critical services of the ICT-sector, CII elements outside these areas are increasingly more difficult to identify and manage (see Figure 3). New information infrastructure elements that may form a risk to a nation may find their origins in relatively unknown and unregulated territory such as international cyberspace (e.g. cloud services used for CI operations).

Mass adoption and integration of new technology is, besides changing the nature of CI and CII, also increasing the cyberattack risk to CII. Developments such as the Internet of Things (IoT), blockchain technology, artificial intelligence (autonomous vehicles, machine learning, robotics etc.), and Industrial Internet of Things (IIoT) provide tremendous opportunities for economic growth. The downside is that the multi-millions of devices, when not well-secured, provide new attack platforms to CII. Such changes in risk increases the necessity of having an effective national CIIP policy on the one hand, and to understand the new risk to one's CII in time.

4.1.2 NEW TECHNOLOGY INTRODUCES NEW STAKEHOLDERS

New forms of information and operational technology may be developed and/or integrated in national critical services by organisations other than those already involved in CIIP (or CIP). As shown by Luiijf and Klaver [Luiijf2015a], six technological and organisational areas should be watched when, on the one hand, considering new information infrastructures to become CII, and on the other hand, revealing new risk to the (existing) CII, nationally and internationally. The protection of CII is strengthened when developments in these six areas are anticipated and new CII and critical changes in existing CII are identified in time.

The six elements of CII that need to be monitored by governmental policy-makers and political leadership:

1. Top manufacturers: when their products fail (e.g. zero-day vulnerability in all OT of one key supplier), this may affect the availability and integrity of CII.
2. Technological and organisational changes in the ICT-sector.
3. Major technological changes in the (embedded) ICT and OT in the 'traditional CI' as discussed above. Technology changes in this area may cause shifts in the set of CII, e.g. cryptocurrency and blockchain infrastructures may become CII soon.

4. Critical services provided by third parties to the ICT sector such as name and address services, certificate infrastructures, etc. which are critical to the operations of the CII (and CI). Both technological and organisational changes in this area may (silently) cause shifts in the set of CII.
5. Mass market/consumer ICT. Major virus outbreaks, failing (major) cloud, social media, movie and email services/servers as well as smart appliances and Internet of Things (IoT) may create societal disruptions nearing the criticality level.
6. Mass market products with embedded (inter)connected ICT and OT which determines the functionality of the product. Think of IoT, modern (automatic) vehicles and the like. The risk of cyber-attacks to CII needs to be considered and managed now, and certainly in the future, by all stakeholders. This risk includes major malware outbreaks, exploited zero-day vulnerabilities, and, increasingly, the misuse of multi-millions of IoT devices as cyberattack platform.

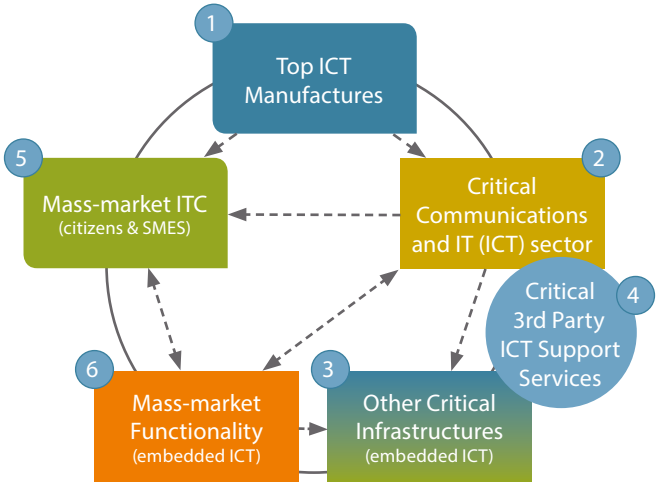

Figure 4: Division of the CII in six elements

The (new) stakeholders in these six areas that can be considered as (potential) key players in CII and the protection thereof, need to be involved in the governance of CIIP.
The first challenge for nations is to determine sufficiently early, that such new services are part of the CII. This means that nations need to keep track of technological developments as part of the CII identification process.
Second, the obligations of CII stakeholders need to be applied to new stakeholders as well. This can be difficult because new entrants might be reluctant to become part of the existing CIIP community. Small companies that operate CII elements may be unwilling to bear the costs of increased protection. Long-term trust based CII operator communities may be reluctant to admit 'fast rising' but not long-term proven newly assigned CII-operators. Some CI/CII operators may also lose their criticality status as their systems are no longer deemed critical, and may be reluctant to give up their position.

When new CII technology is operated by multinational enterprises, individual nations may experience difficulties in making these influential stakeholders comply with national standards and regulation. There may also be national security implications of foreign ownership of CII elements which will need to be overcome. [AUSGov2015] [ISF2011]

4.1.3 TRACKING OF ORGANISATIONAL CHANGES THAT MAKE STAKEHOLDERS PART OF CII

Cyberspace is dynamic and so are the changes in ownership. Changes in ownership can directly and indirectly alter criticality of information infrastructure, as well as introduce or diminish dependencies. Bankruptcy, mergers, acquisitions, outsourcing, and off-shoring influence the ownership and responsibility for information infrastructure. Such changes may cause information infrastructure services to become critical to a nation. For instance, over time a merger of two CII operators may cause the technical services to integrate, reducing options for redundancy of contracted critical services. Another example is the acquisition of a CII operator by a foreign company. Will the foreign company protect the nations' CII as before, or might priorities change and result in less reliable critical services?

Organisational changes can also occur in the supporting supply chain of a company. Cloud adoption is increasing for both data-storage and delivery and functionality of software (Software as a Service) [CloudPro2017]. Various acquisitions in the cloud industry happened in 2017, which further consolidated the number of cloud providers internationally. Individual cloud services might become incorporated into bigger operators, which increases the chance of single-point failures of major cloud services.

Organisational changes also come to the surface when companies decide to host and manage software in other countries, where ownership might be the same, but where responsibility, integrity and security of data cannot be sufficiently managed.
The consequences of failing to accommodate this issue can be severe [Anderson2017].
Safe and secure outsourcing of data and/or services by respected companies or public sector remains the responsibility of the operator in charge (which can be either public or private entity). The duty of care can be considered and ensured on paper, but might not be completely clear in practical terms to the owner and user of the data or service. Moreover, the effects of a breach or disruption might be unforeseen (because of outsourcing, supply chain mergers or acquisitions).
Managing CII in other countries introduces unexpected difficulties such as lack of supervision, accessibility, legal and regulatory challenges and distance to travel to the location.
Unforeseen breaches or disruptions reveal a lack of awareness which can result in contractual requirements that omit requirements on how to manage organisational changes.

4.2 GOOD PRACTICES REGARDING DEVELOPMENTS IN TECHNOLOGY AND IDENTIFICATION OF NEW CII

This section contains a list of potential good practices for monitoring and understanding developments in technology and the identification of new CII.

4.2.1 GOOD PRACTICE: PERFORM AND SUPPORT REGULAR HORIZON SCANNING

A good practice is regular horizon scanning. Horizon scanning strengthens CIIP policy as it enables nations to proactively signal and assess developments in technology, and to act when new technology reaches the potential to become part of the national CII. Horizon scanning helps to grasp the developments that will influence the current state of affairs in CIIP.

> Cuhls et al. describe horizon scanning as:
> Horizon Scanning is the systematic outlook to detect early signs of potentially important developments. These can be weak (or early) signals, trends, wild cards or other developments, persistent problems, risks and threats, including matters at the margins of current thinking that challenge past assumptions. Horizon Scanning can be completely explorative and open or be a limited search for information in a specific field based on the objectives of the respective projects or tasks. It seeks to determine what is constant, what may change, and what is constantly changing in the time horizon under analysis. A set of criteria is used in the searching and/ or filtering process. The time horizon can be short-, medium- or long-term.

Regular collaborative horizon scanning can foster a relationship between governmental policymakers and relevant national and international stakeholders. This can create a basis for further cooperation and mutual understanding of what influences or changes CII and the need for CIIP (for example inviting new stakeholders for joint crisis management exercises or CIIP information sharing [Luiijf2015b]).

Horizon scanning is particularly useful when perspectives from different stakeholders are incorporated. A good practice is to invite key stakeholders in a nation that make up the set of potential CII elements (see Figure 4). The different perspectives can lead to an understanding of dependencies across technologies and organisations.

Future technology watches are relevant, however technological developments must be assessed with regard to the wider scope of (possible) dynamics, development and dependencies they introduce to CI and CII.

More information on horizon scanning can be found in [Curry2008] and [OECD2016].

4.2.2 GOOD PRACTICE: (SCENARIO-BASED) RISK ANALYSIS

National security experts, analysts and CII operators should regularly engage in joint risk analysis. This may provide input to a reassessment of the set of identified CII and the recognition of shifts in criticality. A good practice for a government is to freely offer risk analysis tools and information to organisations and companies. Risk analysis might be mandatory but information infrastructure providers might also want to gain a holistic insight in their products' and services' resilience and criticality.

An example of a voluntary, no-cost risk analysis assessment is the US Cyber Resilience Review (CRR). The CRR can evaluate the resilience capabilities in terms of critical services of CI sectors, organisational size and maturity [US-CERTnd]. The CCR is comprised of ten resource guides – see the inset below. Each guide can be used on its own. Others may prefer to use the full set of CCR resource guides as a coherent approach.
Another extensive guide for risk management approaches is found in the ENISA publication of "Inventory of Risk Management methods and tools" [ENISA2016].

The ten Cyber Resilience Review (CRR) Resource Guides downloadable via [USCERTnd] are:

- Asset Management: The Asset Management guide focuses on the processes used to identify, document, and manage the organization's assets.
- Controls Management: The Controls Management guide focuses on the processes used to define, analyse, assess, and manage the organization's controls.
- Configuration and Change Management: The Configuration and Change Management Guide focuses on the processes used to ensure the integrity of an organization's assets.
- Vulnerability Management: The Vulnerability Management Guide focuses on the processes used to identify, analyse, and manage vulnerabilities within the organization's operating environment.
- Incident Management: The Incident Management Guide focuses on the processes used to identify and analyse events, declare incidents, determine a response and improve an organization's incident management capability.
- Service Continuity Management: The Service Continuity Management Guide focuses on processes used to ensure the continuity of an organization's essential services.
- Risk Management: The Risk Management Guide focuses on process used to identify, analyse, and manage risks to an organization's critical services.
- External Dependencies Management: The External Dependencies Management Guide focuses on processes used to establish an appropriate level of controls to manage the risks that are related to the critical service's dependence on the actions of external entities.
- Training and Awareness: The Training and Awareness Guide focuses on processes used to develop skills and promote awareness for people with roles that support the critical service.
- Situational Awareness: The Situational Awareness Guide focuses on processes used to discover and analyse information related to the immediate operational stability of the organization's critical services and to coordinate such information across the enterprise.

Cross-sectoral or supply chain risk analysis requires a more structured and managed approach. Such an activity can be provided by an association (companies or sector), and/or provided in cooperation with one more governmental agencies.

A good practice for governmental policy makers is to appoint an agency or multiple agencies to perform a cross-sectoral or supply chain risk assessment, especially in countries where responsibility for CIIP is diffuse.

Risk analysis can also be performed and supported by scenario-based discussions.
In comparison to technical risk analysis, scenarios can incorporate a broader narrative. Scenario-based risk analysis helps stakeholders to imagine conditions under which information infrastructure elements may fail, and assess the criticality of different elements for the nation at large, under similar conditions. Moreover, a scenario-based risk analysis with a broad perspective (process, people, technology) can shed light on the importance of ICT and OT which are not directly related to the critical process, but are also important stakeholders and new developments, to incorporate (in near the future) into CIIP policy.

4.2.3 GOOD PRACTICE: DEEPER UNDERSTANDING THROUGH INCIDENT ANALYSIS

Technological complexity can make it difficult to imagine what can go wrong within information infrastructures and what combinations of events can trigger disruptions. Analysing incidents and their impacts can help to understand how disruptions are triggered and prevent future CII disruptions. Incident analysis and publication of outcomes may also help to raise the security awareness of CIIP stakeholders.

There are several examples of incidents from which lessons can be drawn.

CRITICAL DEPENDENCIES

National CII might be dependent on the stability of the global internet infrastructure or international services. The reliability and integrity of these infrastructures and services has proven to be important for products and services used all over the world. The Border Gateway Protocol (BGP) manages the most efficient route between internet exchange points. Exchange points are connected by cables. These cables, which connect continents, are placed and installed by private companies and managed by not-for-profit internet exchange organisations. Disruptions to undersea cables caused problems in the northern part of Argentina. Five million people were affected [Eldiario242012], [Lanaction2012]. Australia and Jersey also suffered domestic problems to millions of customers of a national internet service provider due to problems in undersea cables. [Dailymail2016], [TheRegister2016].

Analysis of such specific key infrastructure incidents and of the wider set of CI/CII disruption incidents (see e.g. Figure 5) may also help nations to identify their CII and to manage critical dependencies of their CII services.

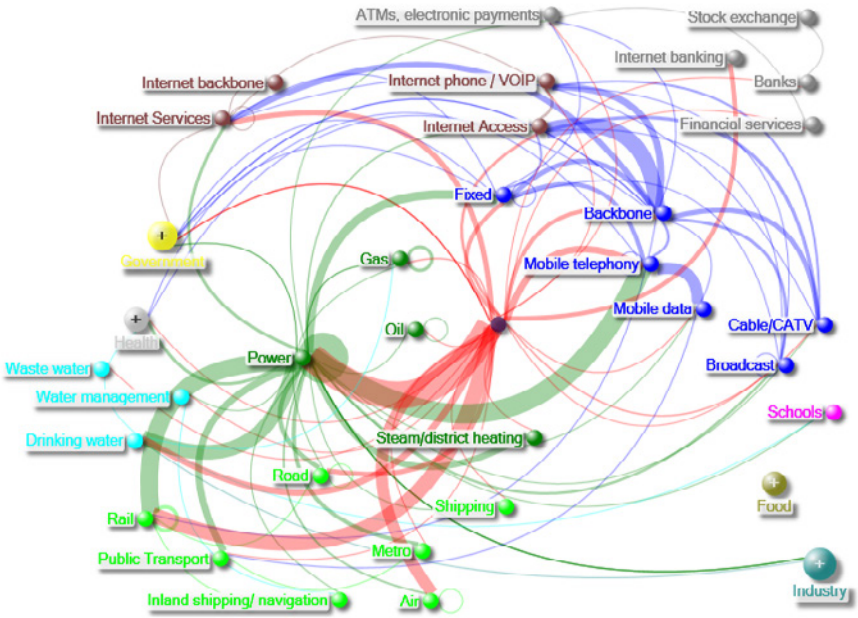

Figure 5: Example view on CI service dependencies based on TNO's data set with CI/CII disruption incidents which were reported in public news sources and occurred in Europe between 2005 and 2017 (figure by TNO)

CAPACITY SHORTAGE

There are several examples of incidents where connected devices collectively attempt to reconnect or restart. In 2013, Dutch mobile phones from one particular carrier were unable to connect to foreign networks in Belgium, France, Monaco and Ethiopia [Tweakers.net2013]. Because of the holiday season, many Dutch customers were traveling and generated more requests to connect to foreign mobile phone carrier networks. In New Zealand, mobile phones overloaded a radio network controller on a massive scale because customer devices attempted to reconnect due to an outage in another radio network [Lightr2010]. Analysis of such incidents has helped to understand and overcome capacity shortages in CII.

DEPENDENCY ON REMOTE CONNECTIVITY

It is expected that the number of 5G connected devices will surpass the number of devices connected over current network infrastructures. The numbers of IIoT and IoT devices that require external connections (remote control, command, maintenance) are on a rapid rise and already reveals small and large-scale problems due to disruptions in the required external connections. Problems have been caused by malfunctioning updates, patches, loss of contact with manufacturer. An example is a fire in Samsung's headquarters. This caused worldwide error messages across smartphones, tablets, and smart TVs. [COMPW2014]

[FOCUS2014] Connected thermostats have also found to be unable to function without connectivity. [Motley2016] [ARSTECHNICA2017]

Moreover, the sheer number of devices connected can be exploited (e.g. by non-patchable or unknown vulnerabilities) in order to strengthen and function as attack platform against CII (e.g. in the form of denial-of-service attacks). Nations may monitor the dependency on remote connectivity by examining such incidents.

4.2.4 GOOD PRACTICE: PROACTIVE DESIGN OF GOVERNANCE FOR NEW CII

Developments in technology bring new stakeholders into the focus of CIIP. These stakeholders need to be involved in CIIP as soon as possible to assess the criticality of their technology and services and to make them aware of the responsibilities that are attached to the operation of CII.

A good practice for well-informed, balanced and proactive governance for new CII can be found in Singapore. Singapore's Cyber Security Strategy encourages the national government, sector regulators and owners of CII to work closely together to identify new CII. Singapore is drafting a new formal procedure as part of the 2018 Cybersecurity Bill (TBA) to designate new CII. The Ministry of Communications and Information (MCI) and the Cyber Security Agency of Singapore (CSA) have explicitly invited stakeholders to provide feedback on the proposed Cybersecurity Bill.

Governance through legislation is a challenge in the quickly evolving cyberspace. Where possible, legislation relating to the identification of CII should be drafted in such a way that new legislation is not required when new CII components are identified. CII components should be listed independently from legislation, and it should be possible to add or remove operators and systems to the list of CII with minimal delay. To effectively arrange the governance of new CII, nations may look for alternatives to legislation and regulation.
New stakeholders can be involved in the governance of CII by:

- Inclusion in the government information sharing community on CIIP making available relevant trend reports, threat intelligence information, factsheets, and whitepapers,
- Invitation to standard-setting communities and government consultations,
- Invitation to information sharing platforms.

CIIP policy might hamper the adoption of emerging techniques and products as CIIP generally introduces additional security requirements. Emerging technologies may be of great importance to businesses, consumers and citizens. Restrictions to operators, manufacturers or companies incorporating or producing technologies must be carefully balanced against the potential benefits. Being identified as CII might introduce responsibilities for CII operators. A collaborative approach and transparency about the responsibilities stemming from CIIP policy is a good practice for proactive governance.

How to promote effective and voluntary activities by CII operators when drafting CIIP policy? A good practice is contained in Japan's Action plan for CIIP [NISC2014]:

- Realistic content of an CIIP action plan that is achievable for first movers.
- Basic items should be articulated in the Basic Policy so that executives and senior managers in the business community who hold the key to ensure information security at CII operators can understand the need for the implementation of the Basic Policy.
- Since both experts as well as non-experts are likely to read the Basic Policy, the Plan should be something easy to comprehend for any relevant parties so that each party understands what kind of measures are required to take under the Basic Policy.
- Clarify the PDCA cycle for maintenance and enhancement of protective capability for CII, particularly vis-à-vis small- and medium-sized CII operators as well as those operators still in the process of developing such capability, which will contribute to promoting effective and voluntary measures by those operators.
- Explain in detail the importance of risk management and the need for introducing such risk management by CII operators to address environmental changes in a flexible manner.
- Compile regulations across various layers which CII operators are required to understand into a certain kind of package in a way that such package can easily be shared and handed over to successors among relevant parties despite high turnover.
- Further promote public relations activities so that even after the Basic Policy is released, appropriate response will be made to address ever-changing environment and collection and provision of relevant information will be continuously carried out.

4.3 REFERENCES AND FURTHER READING

[Anderson2017] New York Times (2017), Swedish Government Scrambles to Contain Damage From Data Breach, On-line: https://www.nytimes.com/2017/07/25/world/europe/ibm-sweden-data-outsourcing.html

[ATECHNICA2017] ARSTECHNICA, 2017. IoT garage door opener maker bricks customer's product after bad review | Ars Technica. On-line: https://arstechnica.com/information-technology/2017/04/iot-garage-door-opener-maker-bricks-customers-product-after-bad-review/

[AUSGov2015] Australian Government (2015). Information Security Management Guidelines:. Risk management of outsourced ICT arrangements (including Cloud), version 1.1. On-line: www.protectivesecurity.gov.au/informationsecurity/Documents/AustralianGovernmentInformationSecurityManagementGuidelines.pdf

[CLOUDPRO2017] CloudPro. (2015). SaaS and cloud M&A on the up in 2017. On-line: http://www.cloudpro.co.uk/cloud-essentials/public-cloud/6992/saas-and-cloud-ma-on-the-up-in-2017.

[COMPW2014] COMPUTERWELT, 2014. Feuer bei Samsung lässt Smart-TVs ausfallen. On-line: http://www.computerwelt.at/news/wirtschaft-politik/unternehmen/detail/artikel/103307-feuer-bei-samsung-laesst-smart-tvs-ausfallen/,/

[Curry2008] Curry, A. and Hodgson, A. (2008). Seeing in Multiple Horizons: Connecting Futures to Strategy, Journal of Futures Studies, 13(1): 1 – 20. On-line: http://jfsdigital.org/articles-and-essays/2008-2/vol-13-no-1-august/ articles/seeing-in-multiple-horizons-connecting-futures-to-strategy/

[Cuhls2015] Cuhls, K., Van der Giessen, A., Toivanen, H. (2015). Models of Horizon Scanning - How to integrate Horizon Scanning into European Research and Innovation Policies, Technical Report. DOI: 10.13140/RG.2.1.1938.7766

[Dailymail2016] Daily Mail Online, 2012. Telstra outage hits customers AGAIN five days after 8m users left without service. On-line: http://www.dailymail.co.uk/news/article-3503708/Telstra-customers-complain-outage-just-five-days-eight-million-users-went-without-service.html?ITO=1490&ns_mchannel=rss&ns_campaign=1490.

[Eldiario2012] ElDiario24.com. Gigantesco apagón informático en todo el norte argentine. On-line: http://www.eldiario24.com/nota/256476/gigantesco-apagon-informatico-en-todo-el-norte-argentino.html

[ENISA2016] European Network and Information Security Agency. (2015). Inventory of Risk Management methods and tools. On-line: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/introduction

[FOCUS2014] FOCUS Online, 2014. Samsung: Brand in Korea ärgert Samsung-Nutzer in aller Welt. On-line: http://www.focus.de/digital/samsung-brand-in-korea-aergert-samsung-nutzer-in-aller-welt_id_3788162.html

[Motley2016] The Motley Fool, 2016. Google's Nest Proves the Internet of Things Still Has a Long Way to Go – The Motley Fool. On-line: https://www.fool.com/investing/general/2016/01/19/googles-nest-proves-the-internet-of-things-still-h.aspx

[GM2016] GFCE-MERIDIAN (2016), GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers. On-line: https://www.thegfce.com/initiatives/c/critical-information-infrastructure-protection-initiative/documents/reports/2016/11/10/ciip-good-practice-guide and via https://www.tno.nl/gcciip

[ISF2011] Information Security Forum (2011). Driving out the seven deadly sins of cloud computing: Information Security Forum. On-line: https://www.securityforum.org/uploads/2015/03/isf_cloud_computing_es.pdf.

[LaNacion] La Nacion, 2012. Un apagón de Telecom afectó a medio país. On-line: http://www.lanacion.com.ar/1481581-un-apagon-de-telecom-afecto-a-medio-pais

[Lightr2010] LightReading, 2010. New Zealand's 3G Network Nightmare. On-line: http://www.lightreading.com/mobile/3g-hspa/new-zealands-3g-network-nightmare/d/d-id/674871

[Luiijf2015a] Luiijf, E., Klaver, M. (2015). Governing Critical ICT: Elements that Require Attention, European Journal of Risk Regulation, Symposium on Critical Infrastructures: Risk, Responsibility and Liability, Vol. 6, Issue 2 pp. 263 – 270.

[Luiijf2015b] Luiijf, E. and Kernkamp, A. (2015). GCCS2015 Good Practice: Sharing Cyber Security Information, TNO. Retrieved from: DOI: 10.13140/RG.2.1.4321.7442 https://repository.tudelft.nl/view/tno/uuid:1eeb81c7-4328-459f-944d-f55c52e31fb1/

[NISC2014] National Information Security Center NISC, 2014. The Basic Policy of Critical Information Infrastructure Protection (3rd Edition). On-line: https://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3.pdf

[OECD2016] OECD (2016). Preparing governments for long term threats and complex challenges. On-line: http://www.oecd.org/gov/Preparing-governments-for-long-threats-and-complex-challenges.pdf

[TheRegister2016] The Register, 2016. Jersey sore: Anchor rips into island's undersea cables, sinks net access. On-line: https://www.theregister.co.uk/2016/11/30/jersey_submarine_cable/

[Tweakers.net2013] Tweakers.net, 2013. Deel KPN-klanten in buitenland weer offline door mislukken herstelactie - Tablets en telefoons. On-line: https://tweakers.net/nieuws/90365/deel-kpn-klanten-in-buitenland-weer-offline-door-mislukken-herstelactie.html

[US-CERTnd] US-CERT (not dated). Assessments: Cyber Resilience Review (CRR) | US-CERT. On-line: https://www.us-cert.gov/ccubedvp/assessments.

5 LIST OF ABBREVIATIONS

BGP	Border Gateway Protocol
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
ENISA	European Union Agency for Network and Information Security
GFCE	Global Forum on Cyber Expertise
GNSS	Global Navigation Satellite System
GPG	Good Practice Guide
ICT	Information and Communication Technologies
IIoT	Industrial Internet of Things
IoT	Internet of Things
ISO	International Organization for Standardization[9]
ISO/IEC	ISO's International Electrotechnical Commission
IT	Information Technology/Technologies
ITU	United Nations specialized agency for information and communication technologies – ICTs
NCSC-NL	Netherlands National Cyber Security Centre
NCSS	National Cyber Security Strategy
NGO	Non-Governmental Organisation
NIST	(USA) National Institute of Standards and Technology
NRI	Network Readiness Index
OECD	Organisation for Economic Co-operation and Development
OT	Operational Technology/Technologies
PDCA	Plan, Do, Check, Act (cycle)
RIA	Riigi Infosüsteemi Amet (Estonian Information System Authority)
SCADA	Supervisory Control and Data Acquisition
VPN	Virtual Private Network
WEF	World Economic Forum

9 ISO is a description rather than an abbreviation, see www.iso.org

COLOPHON

AUTHORS

Mr. Eric Luiijf
Mr. Tom van Schie
Mr. Theo van Ruijven

TNO

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

With contributions by Mr. Peter Burnett (Meridian Coordinator), Mrs. Nynke Stegink (NCSC-NL) and Meridian members from Singapore, the United States, Japan, Korea, Switzerland, Spain, and the Organization of American States (OAS).

This Companion Document to the 2016 GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers was instigated by GFCE-Meridian. The digital version of the 2016 GPG is available for download at: https://www.thegfce.com/initiatives/c/critical-information-infrastructure-protection-initiative/documents/reports/ 2016/11/10/ciip-good-practice-guide and via https://www.tno.nl/gcciip. This Companion Document is also available for download from https://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 good 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 good practices and expertise on cyber capacity building. The aim is to identify successful policies, practices and ideas, and to 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].

October 2017

This document was funded by the Dutch government.