GFCE CIIP Capacity Framework

Cybersecurity Capacity Building

GFCE

Colophon

Authors

Dr. M.H.A. Klaver
D. Molema MSc
P.E. van den Brink MSc

Input from previous versions

T.C.C. van Schie MA
Dr. T.W.J. van Ruijven

TNO

Oude Waalsdorperweg 163
2597 AK Den Haag
The Netherlands
info@tno.nl
TNO.NL

Editing and design: Waai Impact Agency

This guide has been developed in the context of the Global Forum on Cyber Expertise (GFCE), Working Group B, taskforce Critical Information Infrastructure Protection. The GFCE is a global platform that aims to strengthen cyber capacity and expertise globally through international collaboration, through practical initiatives around relevant topics.
June 2021

The development of the guide is funded by the Dutch government.

Index

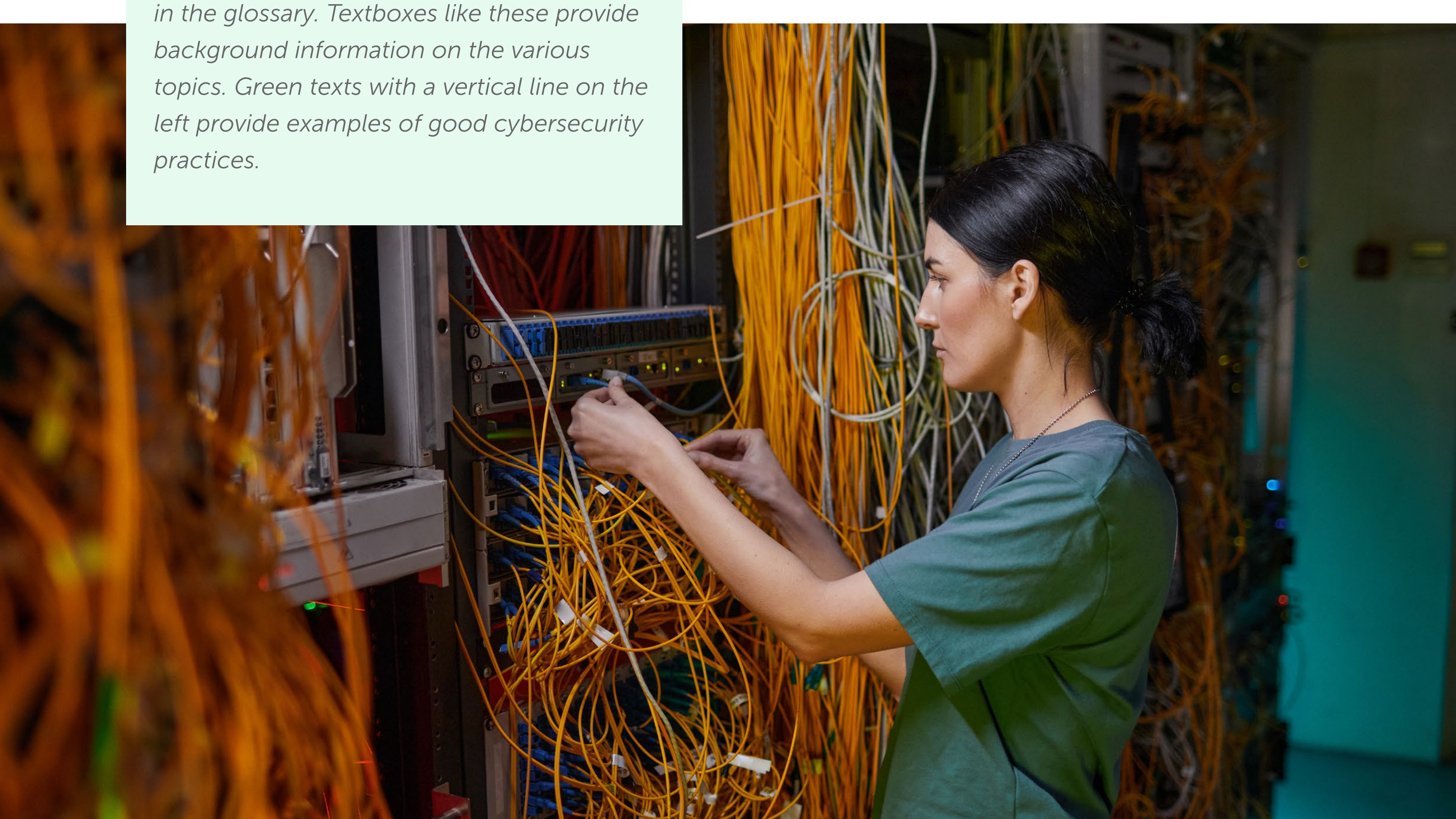
Introduction

Nations increasingly depend on Information and Communication Technology (ICT) for the proper functioning of their national Critical Infrastructure (CI) and society at large. ICT, such as Operational Technology (OT) and Information Technology (IT), can be so critical to the well-being of a nation that their disruption poses a threat to national security and results in severe economic impact. ICT that qualifies as such can be referred to as a national Critical Information Infrastructure (CII). Examples of elements that are part of CII include communication networks, data centres, industrial control systems and digital services within organisations that have been designated as critical to a nation.

To prevent or mitigate disruptions of their Critical National Information Infrastructure (CNII), nations have to incorporate measures to protect it. Such measures are commonly referred to as Critical Information Infrastructure Protection (CIIP). CIIP can be defined as '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'. The purpose of this guide is twofold. Firstly, the framework supports the discussion on CIIP and the exchange of good practices by specifying the capacities that may be part of a CIIP approach. Secondly, it provides knowledge to policymakers on how to establish and maintain sustainable and efficient efforts to protect CII by outlining the required capacities.

How to use this guide

This guide is structured in such a way that you can easily navigate between the themes in no particular order. Key terms are underscored in each theme and explained in the glossary. Textboxes like these provide background information on the various topics. Green texts with a vertical line on the left provide examples of good cybersecurity practices.



Who is this guide for?

This guide is primarily developed for policymakers who are involved in and responsible for Critical Information Infrastructure Protection on a national level. The good practices and examples provide a starting point for designing national CIIP policies. They also provide the opportunity to learn from the insights, wisdom and experiences of other countries.

Other stakeholders involved in a national CIIP may also find this guide useful as it provides an overall overview of the capacities required for the development and maintenance of an effective national CIIP. Examples of relevant stakeholders are, for instance, CI operators and policymakers in related areas such as general critical infrastructure protection.

Principles of the CIIP Capacity Framework

The CIIP Capacity Framework is based on the principle that every nation has its own set of critical infrastructures, critical information infrastructures and approach to critical information infrastructure protection. While some part of a nation's CI and CII may be similar to those of other nations, other elements may differ. This framework does not constitute a maturity model that can be used to assess national approaches to CIIP. Instead, it describes CIIP capacities in a general way to allow for the adjustment of capacities to national conditions. The framework aims to support mutual learning and to facilitate cooperation.

The GFCE

The Global Forum on Cyber Expertise (GFCE) initiative on CIIP aims to support government policymakers that are responsible for their national CIIP. By working together in a global initiative, GFCE members can leverage the knowledge, expertise, and experience on CIIP that has been developed all over the world. Moreover, the initiative enables nations worldwide to share relevant experiences and keep track of new developments.

The history of this document

The GFCE initiative on CIIP started with the development of a good practice guide on CIIP. Later, the CIIP Capacity Framework was published, providing a comprehensive overview of CIIP capacities. A companion document was published in 2017 to elaborate on important aspects of CIIP, such as definitions and the challenges pertaining to monitoring changes and continuous improvement.

The document that you are reading now, the CIIP Capacity Framework, continues to build on all three of the previously mentioned guides. By integrating the good practices with the CIIP capacities, this version of the capacity framework replaces the first version and offers an updated and integral knowledge base for critical information infrastructure protection.

What are capacities?

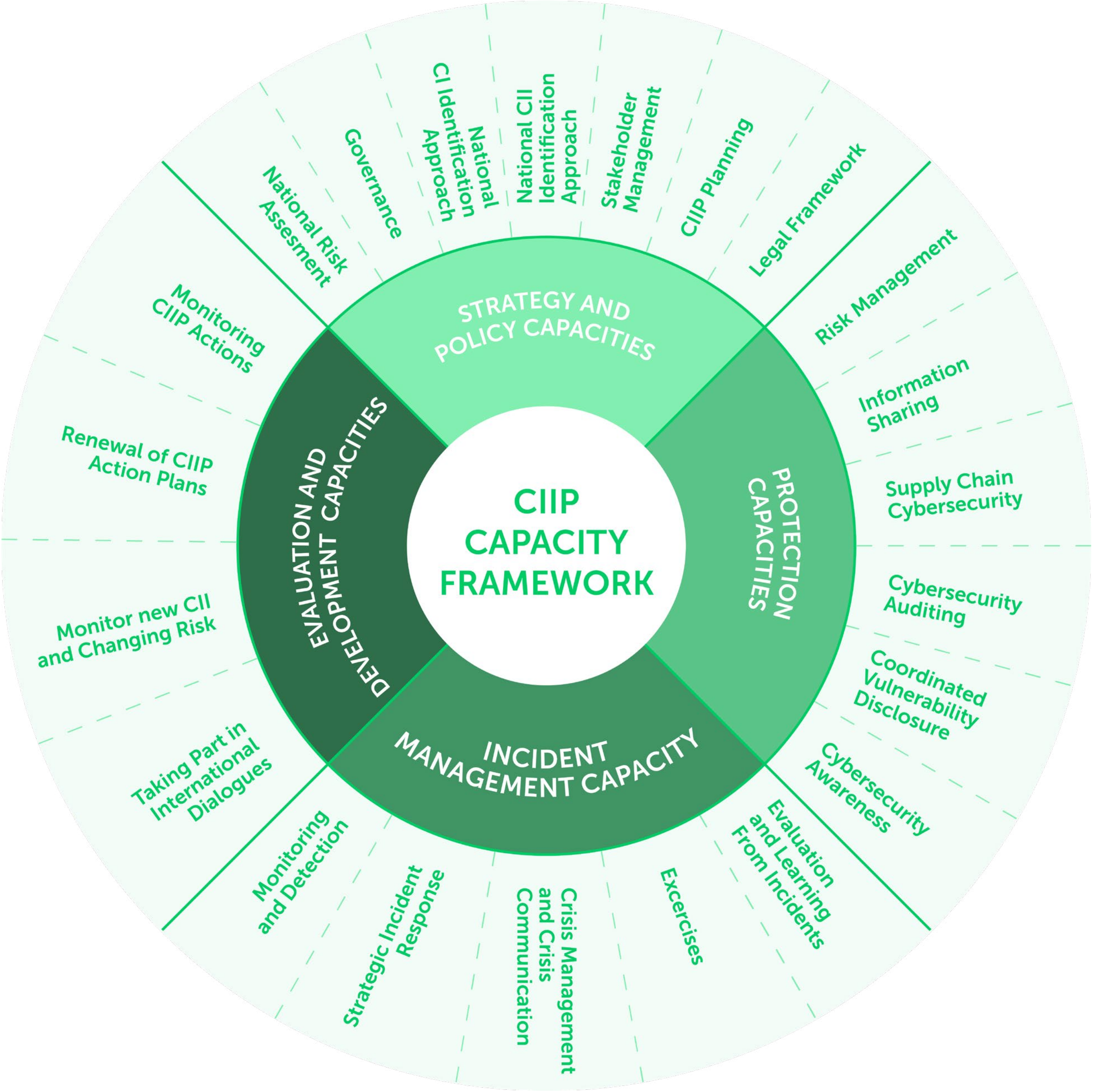
In this document, a capacity refers to 'a functioning method, tool or institution to ensure the protection of critical information infrastructures'. The terms ‘capacity’ and ‘capability’ are used interchangeably in this document. The CIIP Capacity Framework consists of four themes:

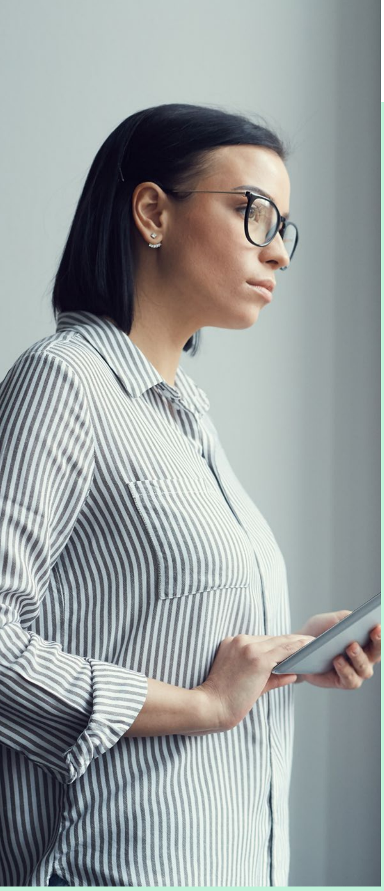
- CIIP strategy and policy
- Protection of CII
- Incident management
- Evaluation and development

For each theme, several capacities have been identified in collaboration with the GFCE community. The GFCE CIIP Capacity Framework is depicted below.

This document describes the capacities that are part of the CIIP Capacity framework. This entails:

- the four themes of the framework (dark green)
- the capacities that are part of each theme (light green), their main characteristics and the identified approaches that are used by the GFCE community to develop each capacity

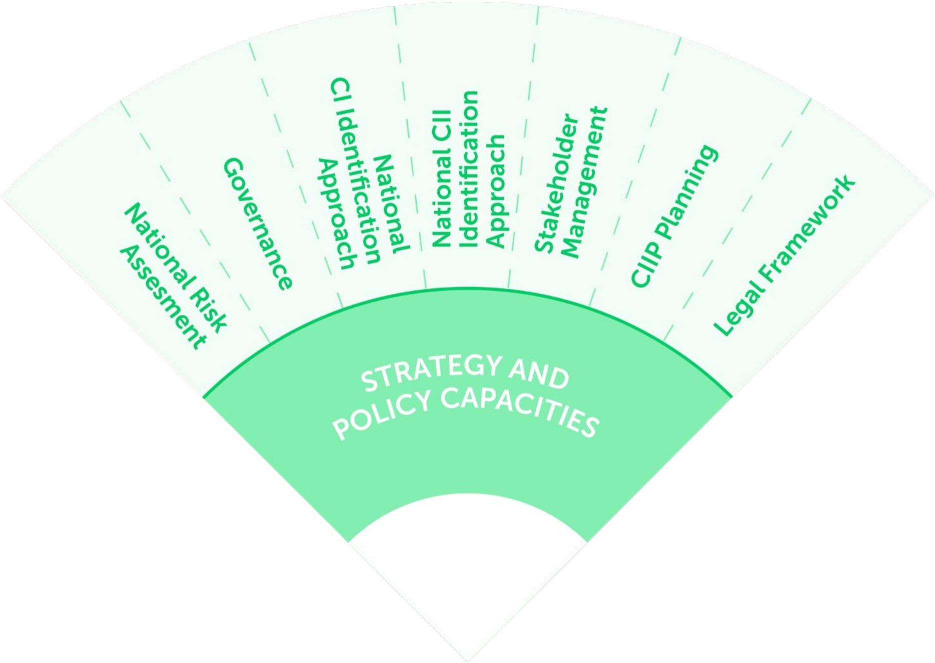

CIIP CAPACITY FRAMEWORK
STRATEGY AND POLICY CAPACITIES
PROTECTION CAPACITIES
INCIDENT MANAGEMENT CAPACITY
EVALUATION AND DEVELOPMENT CAPACITIES
National Risk Assesment
Governance
National CI Identification Approach
National CII Identification Approach
Stakeholder Management
CIIP Planning
Legal Framework
Risk Management
Information Sharing
Supply Chain Cybersecurity
Cybersecurity Auditing
Coordinated Vulnerability Disclosure
Cybersecurity Awareness
Evaluation and Learning From Incidents
Excercises
Crisis Management and Crisis Communication
Strategic Incident Response
Monitoring and Detection
Taking Part in International Dialogues
Monitor new CII and Changing Risk
Renewal of CIIP Action Plans
Monitoring CIIP Actions



Theme

Strategy and Policy Capacities

There is no single Critical Information Infrastructure Protection (CIIP) strategy that suits every nation, as the nature of the process – protecting one's critical information infrastructure – depends on a nation's specific risk profile as well as its ability to mitigate risk. These abilities and responsibilities to mitigate risk, in turn, depend on the capacities of the stakeholders involved in CIIP and the capabilities that a nation has at its disposal. These capacities determine to what extent the Critical Information Infrastructure (CII) stakeholders can work together towards desired levels of CIIP.


National Risk Assesment
Governance
National CI Identification Approach
National CII Identification Approach
Stakeholder Management
CIIP Planning
Legal Framework
STRATEGY AND POLICY CAPACITIES

National risk assessment

What constitutes a national risk assessment?

The aim of a National Risk Assessment (NRA) is to establish a common national understanding of the risks that a nation faces through a systematic assessment of threats and vulnerabilities. The outcome of a national risk assessment is typically an all-hazard overview of risks and their expected impact and likelihood of occurrence.

Identification and assessment of threats and vulnerabilities to a nation's CII are an important element of an NRA. Once identified and assessed in an NRA, risks can be managed with an integrated national approach to risk prevention, preparedness, and response. This is also known as risk management or disaster risk management.

Having an overview of these risks, and their relation to the Critical National Information Infrastructure (CNII), can be considered a requisite for the development of CII policies. Such an overview can contain, for example, an analysis of the possible impact that climate change-related risks may have on the CII.

Features

Considering the Critical Infrastructure (CI) and CII-related risks in the context of a national risk assessment will help with the development of an integrated and balanced risk management approach underpinning CIIP.

A systematic assessment of risks requires that all risks are assessed on their (potential) impact and the likelihood of occurrence using the same set of metrics. Moreover, not only current hazards (malicious and non-malicious) are to be assessed, but also expected shifts in risks should be considered—for example, risks relating to climate change and geopolitical developments.

Developing a national risk profile subset for CI and CII is a challenging task. We strongly recommend stakeholder involvement from the very start of the development of the national risk profile, as risk assessments require expert opinions and stakeholder acceptance. If your nation is developing a national risk profile for the first time, you should consider focussing on the most important risk scenarios first. Other scenarios can then be included in later stages. The prioritisation of risk scenarios can be based on information such as historical incident data, the importance of identified critical information infrastructure, or previously executed sectoral or regional risk assessments.

Good practices

Integrate risk scenarios for CI and CII in a national risk matrix

In many countries, the national risk assessment covers a variety of hazards, including pandemics, terrorist attacks and extreme weather events. In recent years, most nations have also included CI and CII risks in their national risk scenarios. A common method to visualise the results of a national risk assessment is by using a risk matrix, which shows the expected impact and likelihood of different risk scenarios. Some nations include CI and CII scenarios in an all-hazards risk matrix, other nations include these scenarios in a specific cyber risk matrix. See figure 1 for an example of an all-hazards risk matrix.

The all-hazards risk matrix in the Netherlands

The Netherlands uses an all-hazards approach for its national risk assessment. The country has developed a methodology for its NRA that incorporates assessments by subject-matter experts from the public, private and academic sectors. The methodology has been tried, tested, and improved by the Netherlands since 2007. CII scenarios are an integral part of its all-hazards risk matrix.

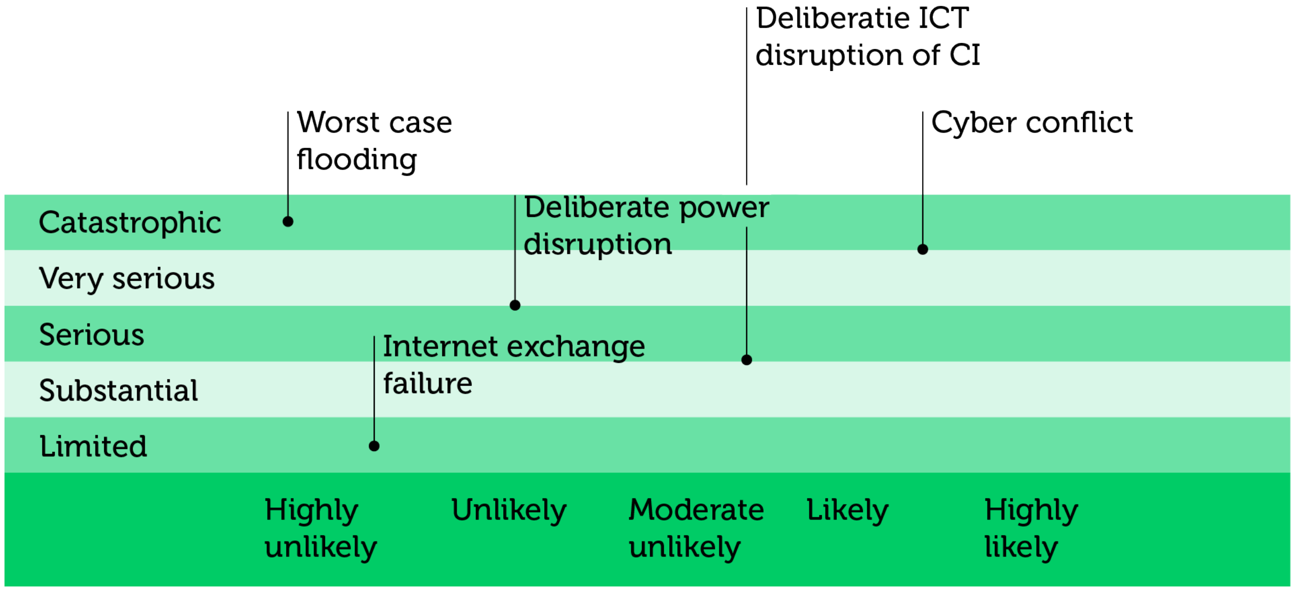


Figure 1. An example of a risk matrix

Austria’s Cyber Risk Matrix

In Austria, cyber risks at the national level were analysed using a qualitative process in collaboration with various stakeholders. The outcomes of the analysis were subsequently visualised in the Cyber Risk Matrix. The risk matrix was first developed in 2011 and has been updated in 2016. See figure 2 for the matrix of 2011.

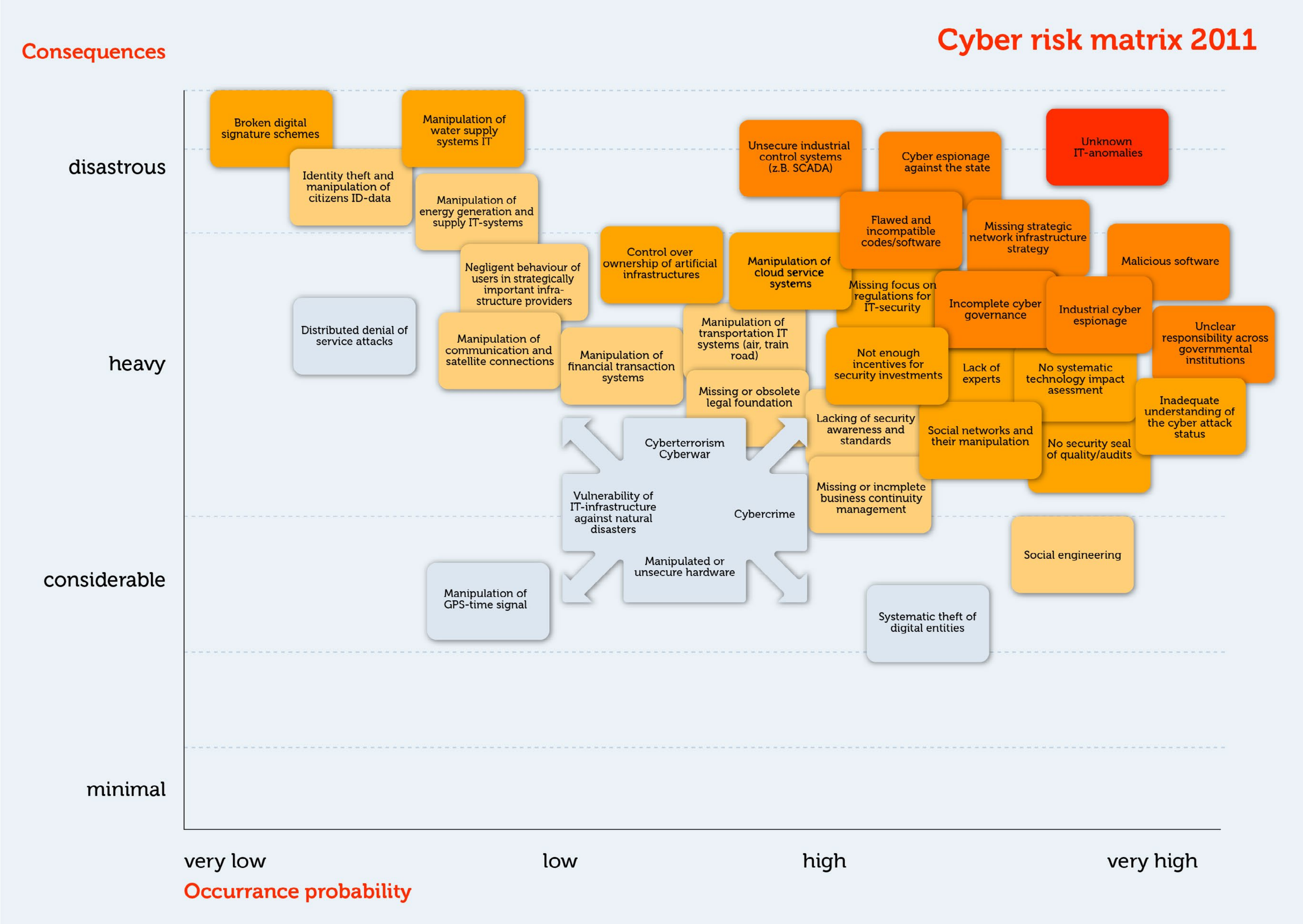


Figure 2. Austria’s Cyber Risk Matrix 2011 [1]

Governance

What constitutes governance?

Governance concerns the choices a nation makes in determining where tasks and responsibilities for CIIP reside. A nation's governance choices are reflected in the roles and responsibilities of public and private entities related to CIIP. Governance as a capacity refers to the ability of a nation to effectively and unambiguously embed CIIP-related responsibilities and mandates in the appropriate institutions within a nation.

CIIP tasks and responsibilities can be performed by both public and private bodies and can be assigned at different institutional levels: strategic, tactical, and operational (technical). At a strategic level, a governing body such as a cybersecurity council can identify strategic challenges and possible ways forward. At a tactical and operational level, such an organisation may exist in the form of a national agency, Computer Security Incident Response Team (CSIRT) or national cybersecurity centre. Such institutions can co-exist separately or reside within a single government department with well-defined areas of responsibility. Policymakers can define and influence cybersecurity strategy at both a strategic and tactical level.

Features

Within government, different departments can play a role in CIIP governance and different options for the organisational structure of CIIP can exist. Addressing the risks to the CII and the related complexity of CIIP effectively requires a multi-agency approach by the government at strategic, tactical, and operational levels. Stakeholders such as ministries (e.g. Economic Affairs, Security, Cabinet Office, Justice, and Defence), regional public bodies, agencies, and regulators have to collaborate on challenges at all levels.

At the strategic level, it is important to first establish an optimal setting to address the CI and CIIP challenges with all public stakeholders. For instance, by organising regular roundtable meetings. The strategic objectives, once formulated, will drive requirements for legal mandates, governance, organisation structure and collaborations at the tactical and operational levels.

At the tactical and operational levels, policymakers should consider cooperation with operational services in the national security, defence, and police involved in the CI and cyber domain. Some nations use coordinating structures, such as roundtables or coordinating committees, to create a collaborative atmosphere among relevant public and private stakeholders to derive a consensus on strategies for CI and CIIP challenges.

Good practices

When developing a CIIP governance policy, two important choices must be made. Firstly, which organisational structure will you choose to embed CIIP in government? Secondly, how will public-private participation be organised?

Choosing an organisational structure to embed CIIP in government

The process of setting up an organisational structure for CIIP within government is dependent on the approach that best suits both the existing and the desired form of governance. In short, this entails deciding between a more centralised approach versus a more distributed multi-agency approach. Each approach has its own benefits. The examples of Singapore and Austria show a centralised and a distributed multi-agency approach.

> ### A centralised approach in Singapore
>
> In 2015, the Cyber Security Agency of Singapore (CSA) was established as the central agency to oversee and coordinate all aspects of cybersecurity for the nation. CSA is empowered to develop and enforce cybersecurity regulations, policies, and practices. It is part of the Prime Minister's Office and is managed by the Ministry of Communications and Information.

A distributed multi-agency approach in Austria

Due to its decentralised approach, no single authority is responsible for CIIP in Austria. The main coordinative body is the Cyber Security Steering Group (CSSG). In general, the Federal Chancellery of Austria and the Federal Ministry of the Interior share responsibilities for CIP on a strategic-political level. At an operational level, the coordination structure differentiates between an Inner circle and an Outer circle. The Inner Circle includes several public agencies, the most significant of which are the Cyber Security Center, the Cyber Defense Center, GovCERT, MilCERT and the Cyber Crime Competence Center (C4). The Outer circle includes the national CSIRT and private organisations such as the sector-specific CSIRTs.

Organizing public-private interaction at the strategic level

Some nations have established high-level committees to make recommendations not only to their government, but also to their private sector. Based on the input of both public and private stakeholders, strategic challenges are identified, and advice is given on possible ways forward.

The Dutch Cyber Security Council

The Dutch Cyber Security Council (CSR) is a national and independent advisory body of the Dutch government. It works to improve cybersecurity in the Netherlands at the strategic level. The CSR is comprised of representatives of public and private organisations and the scientific community in the cybersecurity domain, including the national CII.

The mixed public, private and academic composition of the CSR enables it to analyse incidents from various angles, as well as define priorities and bottlenecks, to develop an integral vision on opportunities and threats. The CSR strives to render advice that is both theoretically substantiated and can be easily be applied.

CI identification approach

What constitutes a CI identification approach?

To identify the CII, it is important that you first identify the Critical Infrastructure (CI). Nations depend on their critical infrastructure for the functioning of their society. CI can therefore be 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 profound consequences'[2]. CI operators can be public, semi-public or private organisations. The types of goods and services provided by CI operators, the purpose for which customers use these goods and services, and the consequences of a potential disruption determine whether an infrastructure should be qualified as critical. As such, a particular infrastructure may be of vital importance to one nation but not to another. The outcome of the identification process is an overview of the CI (common examples of critical infrastructure are the water, energy and telecom sectors).

Due to the potential for disruptive consequences of malfunctioning critical infrastructure, every nation has a responsibility to identify its CI and subsequently protect it. The need for the protection of critical infrastructure activities (of which CI identification is an essential part) can also be the result of a national risk assessment. This assessment gives a nation insight into the importance of and risk to (information) infrastructures. Insight into the criticality of infrastructure and information infrastructure can also come to the surface unexpectedly. For example, an infrastructure could suddenly start to malfunction, which would expose the possibility of disruption with serious societal or economic impact. Such an unforeseen event might trigger public and private stakeholders to (re)consider the criticality of that infrastructure. Likewise, emerging new threats, such as supply chain risks, can lead to new insights concerning a nation's CII.

Third-party recommendations
Sometimes international institutions recommend nations to pay more attention to and protect their CI and CII. These recommendations can come from institutions such as:

- *regional initiatives and networks of nations (e.g. African Union (AU), Organisation of American States (OAS))*
- *networks of CII providers (e.g., Commonwealth Telecommunications Organisation (CTO))*
- *International organisations (e.g. the World Bank, G8, ITU, NATO, OECD, etc.)*

Features

When comparing the sets of CI sectors of different nations, you may find a similar base set of CI sectors but you are also likely to find major differences. A particular infrastructure might be of vital importance to one nation but not to another. Therefore, nations will have different interpretations on what should and should not be included in a national CI.

Irrespective of the national governance structure and policy options, the early involvement of public authorities, semi-public and private infrastructure operators in this identification process is important. The identification process itself often takes the form of one of three approaches:

1. The first is a **bottom-up approach**. This approach starts with looking at the sets of sectors and services defined as critical by other nations. We recommend policymakers to start looking at other nations that are similar in societal, geographical, and technical development structure. This review should result in a list of infrastructure operators of these sectors and services. A good next step would be to estimate the degree of criticality of the infrastructures from the set of avoidable impacts mentioned in the CI definition. By applying the criticality criteria to this mix of stakeholders, sectors and services, an 80 to 90 per cent completion of the set of CI sectors and services can be achieved. It is important to understand that when a certain sector is designated as a CI, this does not mean that all its underlying services are also critical.

2. A second approach is to perform an **analytical study using a methodology that contains a simple set of criteria or metrics**. Various nations have already performed evaluations of their national set of CI elements (CIPedia©)[3]. These evaluations and their methods are probably not directly applicable without taking account of national differences and specifics. However, they do provide an excellent and useful insight into the range of approaches of identification of CI that you can use for analysing your own CI set.

3. The third approach is to **start by defining fine-grained metrics**, which requires more maturity in Critical Infrastructure Protection (CIP) assessment than the other two approaches. Afterwards, by using the method outlined in the good practice below, you can determine whether an infrastructure or infrastructure service should be designated as critical or not. It must be noted that this approach has been tried by several teams from different nations, and they found that defining metrics is not an easy task.

Good practices

Use definitions of CI sectors and services of other nations

To create an initial set of CI sectors and CI services, you can use the ones defined by other nations for inspiration. Whereas definitions of 'CI' from other nations might be helpful, it should be noted that they most likely will not be directly transferable to your nation. Each nation that starts developing insight into their CI is going to identify different critical sectors and services. Comparing the CI definitions from a number of nations (e.g. you can find definitions listed under 'Critical Infrastructure' in the A-Z list on the landing page of CIPedia©[3]) may help your nation stating its own definition. We recommend choosing a definition that is similar to an already existing one.

Adopt a methodology to identify CI sectors and services systematically

The bottom-up approach offers a structured methodology for the identification of CI sectors and services in your nation. Four methodological stepping stones are briefly explained here. Together they provide a structured approach for the identification process. These steps were inspired by the 2008 European Critical Infrastructure Directive.

1. Apply sector-specific criteria

Examples of sector-specific criteria for criticality are the market share, the transport capacity, CI function, cross-border connectivity and supply of critical services to government, industry or population. Use these criteria to make a shortlist of possible CI sectors in your nation.

2. Assess criticality

The next step is to assess the criticality of the CI sectors on your shortlist based on the nation's CI definition. You need to know about the specific delivered goods and services for a given sector. It also requires that you know who are responsible for the delivery of said goods and services[4].

3. Assess dependencies

Look for critical dependencies that can lead to a cascading of outages in other infrastructures. Keep in mind that the set of CI dependencies may significantly change when the regular 24/7 functioning of elements of the CI change from a normal to, for instance, an emergency or recovery situation.

Definition of (inter)dependency

(Inter)dependencies in this context 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'*[5].

Note that in the case of CII, as many processes are digitalised, the dependencies must be viewed from a holistic point of view that takes into account both the physical dependencies and the digital ones.

4. Apply cross-cutting criteria

Cross-cutting criteria are used to assess the criticality of a CI element by comparing the possible impact of a disruption on various sectors of a society based on a set of criteria. Examples of cross-cutting criteria are:

- potential number of fatalities or injuries
- economic effects (significance of potential economic loss, degradation of services, potential environmental effects)
- public effects (impact on public confidence, level of physical suffering of the population, level of disruption of the daily life)
- dependency (potential for cascading effects on other sectors, e.g. minor, moderate or significant debilitation).

- scope of impact
  - o The affected area, for example:
    - › a local, large area with multiple sectors
    - › a single nationwide sector
    - ›an international area with multiple sectors.
  - o The size or density of the population in the affected area
- impact on service (e.g. recovery time in number of days)[6]

The optimal order in which to execute these steps depends on the information that is available to you. For example, you could be using cross-cutting criteria that are based on already available international requirements. In that case, the best order would likely be to start with the development and application of cross-cutting criteria, then assess dependencies, followed by an assessment of criticality, and end with applying sector-specific criteria.

(National and cross-border) dependency analysis

When identifying your CI, you should take national, sectoral and cross-border dependencies into account since these may expand the list of stakeholders involved in CIP. You are likely to already discover dependencies during the first steps of CI identification and risk assessments, but specific methods to draw out dependencies are also available. Apart from dependencies within the nation, you may also find dependencies between your CI and infrastructures in neighbouring nations or regions. Such dependencies may influence the criticality of a particular national infrastructure. One of the most straightforward ways to discover dependencies is by organising (regional) cross-sectoral workshops with stakeholders from different critical sectors and identify (inter) dependencies together.

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

Table 1. Examples of CI sectors and services.

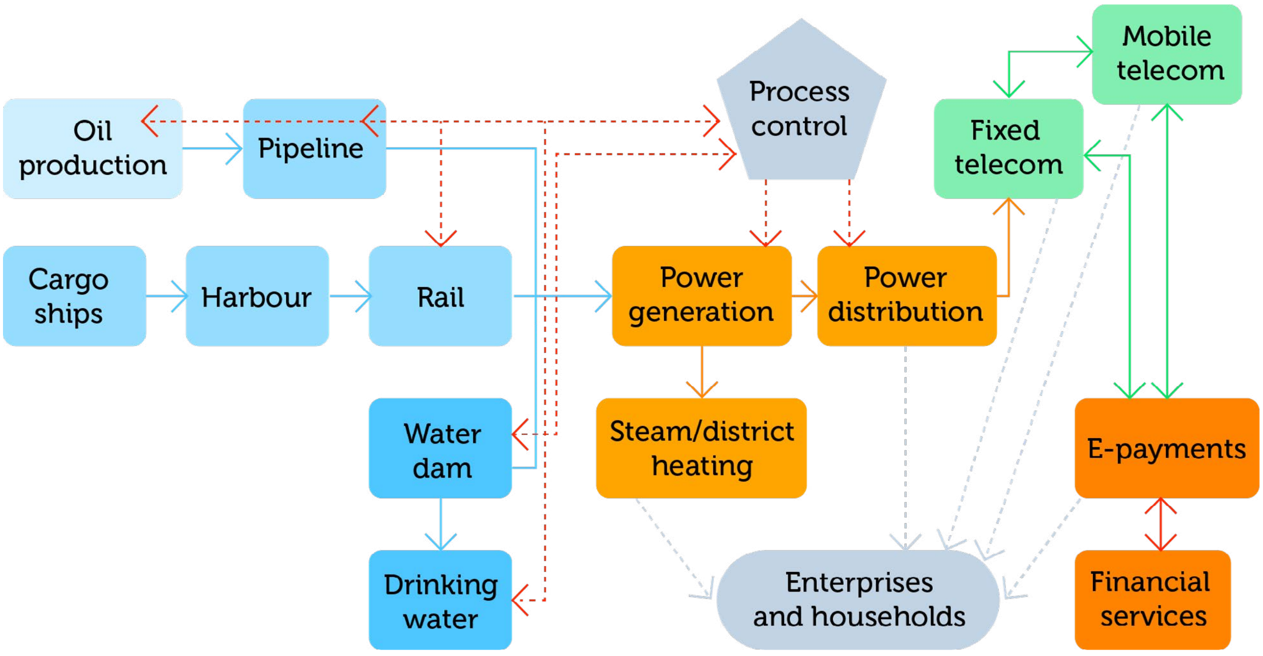


Figure 3. An example of dependencies and process control.

CII identification approach

What constitutes a CII identification approach?

Although there is no globally accepted definition of Critical Information Infrastructure (CII), it can be understood as referring to 'those interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic wellbeing of citizens, or on the effective functioning of the government or the economy'[7]. There are different approaches to the identification of CII. These different approaches are the result of the diverse nature of challenges, the different architectures of CII, and pre-existing CI identification and protection approaches.

Criteria used to identify CI may be applicable to CII. However, additional criteria are usually required to assess the importance and interconnectedness of CII. Some operators of your nation's CII may be based abroad, which can complicate the identification. The outcome of the identification process of CII is a comprehensive overview of all Information and Communication Technology (ICT) elements that are critical to the well-being of your nation.

Features

Once you have identified the national set of CI sectors, a good next step is to identify CII (note that the identification of CI and then CII can be an iterative process). The CII can be identified with steps and methods similar to the ones that are used for the identification of the CI. However, it should be noted that the identification of the CII is often more complex than the identification of the CI.

As shown in figure 4, CII has two points of focus:

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 in the CI sectors. for the delivery of said goods and services.

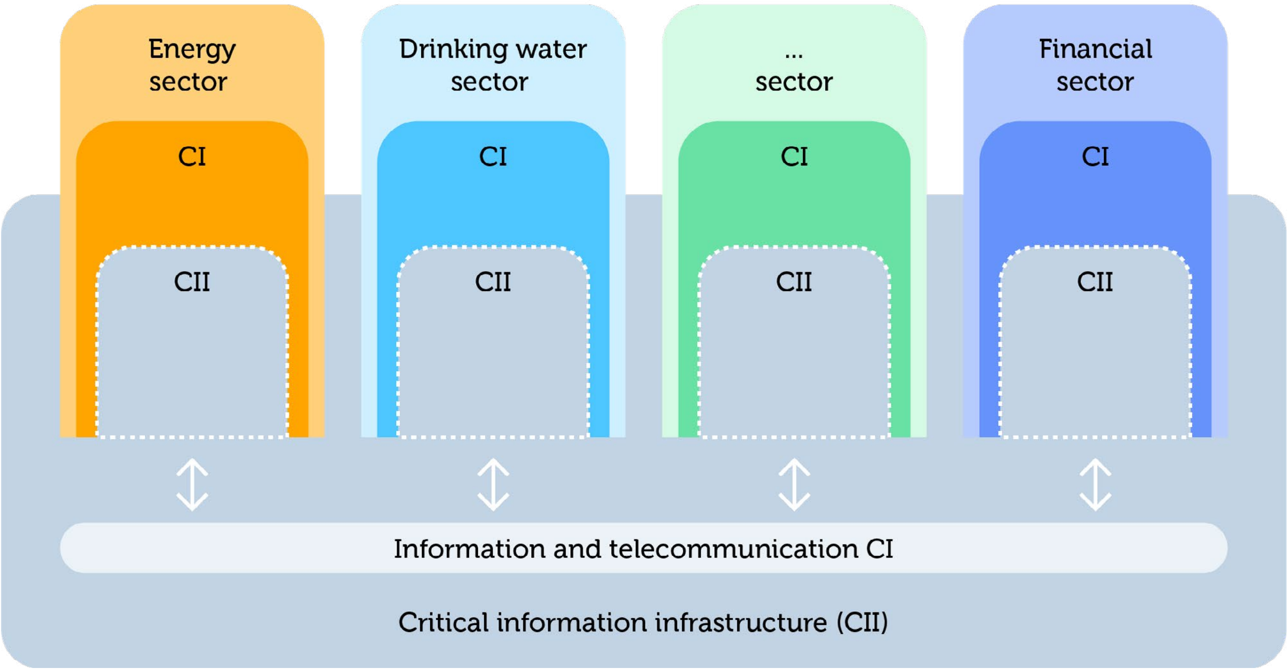


Figure 4. The CII encloses (1) the Information and Telecommunication CI, and (2) the CII components in CI (e.g. control systems).

The elements of CII

The focal points of CII described in figure 4 align with the 2008 understanding of the OECD of CII: "CII {...} typically include one or more of the following:

- *Information components supporting CI.*
- *Information infrastructures supporting essential components of government business.*
- *Information infrastructures essential to the national economy."* [8]

Good practices

Adopt a layered approach for the identification of CII

The identification of critical sectors is often a good starting point for CIP and CIIP, as sectors are clearly delineated and cover a range of (critical) processes and systems. A good practice for the identification of CII is to adopt a layered approach. A layered approach means using multiple levels of analysis to describe, analyse and identify elements of your nation's CII. Layers of CII that are frequently mentioned in the literature are:

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

A layered approach will help you identify and structure elements of your national CII. Within each critical sector, core functions can be distinguished. These core functions describe the critical parts within a sector that you should focus on. Within core functions, critical resources (such as specific assets and components) can be distinguished to further narrow the scope and focus of CIIP. These levels of analysis – from sector to component – allow researchers and policymakers to distinguish the critical elements from information infrastructures on different levels.

At the intra-sector level, dependencies between sectors should be analysed to assess the criticality of specific sectors. Also, threats to critical resources that are used in multiple sectors can be analysed to assess any common vulnerabilities of multiple sectors combined.

Another advantage of a layered approach is that it incentivises the development of criticality criteria. Many nations have developed criteria and identified CI and CII at a sectoral level (e.g. Austria, Germany, India, the United States and Sweden). However, identification of core functions or critical resources is less common. Analyses at the level of the intra-sector layer and the sector layer are generally the domain of the national authorities that focus on the criticality of individual sectors and cross-sector dependencies regarding societal well-being and national security. On the other hand, core functions and critical resources should, in general, be jointly identified by national authorities and the CII operators.

Estonia's layered CIIP approach

A great example of a CIIP policy that used a layered approach to identify CII can be found in Estonia. Estonia has identified its CII using a multi-layered, stepwise approach. Estonia's CI sectors have been identified as part of Estonia's CIP policy. For each CI sector, a 'service organiser' (also known as the relevant ministry) was selected, who determined the criteria and thresholds used to identify critical service providers within that sector (this resembles the core functions or critical sub-sector layer). After they had been identified, the critical service providers each performed a risk analysis, listed critical resources, and drafted risk mitigation and business continuity plans. The Estonian Information System Authority (RIA) validated these lists of critical resources and risk mitigation plans. The RIA has composed a national list of elements of the CII, based on the combined list of critical resources of all critical service providers. This list resembles the intra-sector layer approach to identifying CII.[9]

Critical information infrastructure elements of other CI sectors

It is a good practice to clearly communicate and draw the distinction between critical elements of the ICT sector on the one hand and CII elements of other CI sectors on the other. Doing so will also help with the development of suitable criticality criteria for all elements of CII.

Critical elements of the ICT sector can be Internet Service Providers (ISP), Internet Exchanges (IE), 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 are, for example, specific communication networks, information systems, or Industrial Control Systems (ICS). Elements of the CII can be located both in the ICT sector and in the other CI sectors and they may even 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.

Japan's CII sectors identification

Based upon analysis, the Japanese Cybersecurity Policy for Critical Infrastructures Protection*, defines the set of 13 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 service*
- *petroleum industries*

Incorporate a dependency analysis in the criticality assessment of information infrastructure

In some cases, an information infrastructure needs to be classified as CII due to the dependency of other critical systems on this information infrastructure. These dependent systems are either part of CI or CII. Both the dependency of other CI elements and CII elements should be part of the criticality assessment of information infrastructure (as seen in the capacity of identifying CI). If a layered approach is adopted, dependencies within the 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 the CII (cross-sector dependencies).

Assessing dependencies can be done in several ways. Most often, assessments are based on either expert opinion or modelling and simulation. During the analysis of dependencies, special attention should be paid to information infrastructure elements that serve multiple elements of CI or CII. Disruption of such elements will cause multiple elements of CI or CII to fail simultaneously, which amplifies the disruptive effects. In figure 5, a visualisation of such a dependency analysis is displayed.

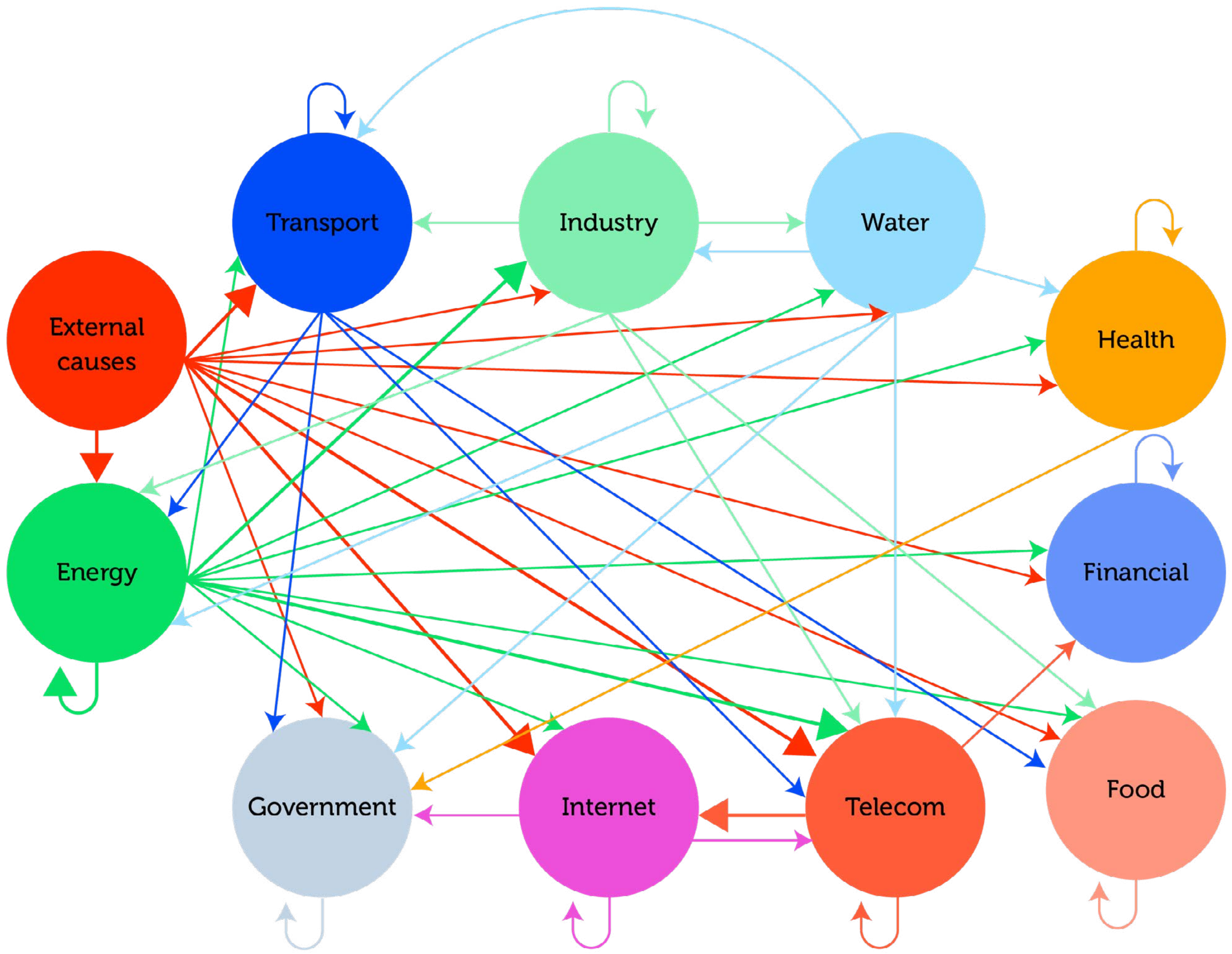


Figure 5. CI cascading disruptions through dependencies in Europe (2005-2009). Note: relative size of external causes is divided by five.

VPN as potential CII element

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

Use specific and objective criticality criteria to identify critical resources

Assessment of potentially critical information infrastructures can only be done properly when specific and objective criticality criteria are used. The criticality criteria specify which properties an information infrastructure must have to qualify as an element of CII. When a layered approach is used (see the first good practice for CII identification) criticality criteria need to be defined 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 can be part of a CIP policy or a specific feature of CIIP.

The UK's criticality scales

The UK has created an overview of criticality scales that serve as a categorisation of the level of criticality of its infrastructures. Such a scaling system offers a systematic indication of what infrastructures could be earmarked as CI or CII while also providing an indication of the degree of their criticality. See Table 2 underneath.

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 fell within this category. The impact of loss of these *sets 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).

Table 2. Example: Criticality Scale for national infrastructure.[10]

Assess criticality with support of surveys and data

Criticality assessment is often based on expert judgment. If possible, you should strive to support the criticality assessment with surveys taken from CI operators and (potential) CII operators. In CI and CII sectors with many stakeholders, surveys may provide more elaborate insight into the overall or average criticality of potential CII elements than (just) the judgement of experts. Data on dependencies and consequences of failures from CI and CII operators can provide even more insight. When collecting this data, make sure to pay proper attention to confidentiality and the handling of potentially sensitive information.

A survey to increase insights in cross-border CII dependencies

A study on regulating cross-border dependencies of CII provides a good example of a survey used to increase insight into CI dependencies on information infrastructure beyond national borders – i.e. cross-border dependencies of CII.[11] The study addresses both 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 overall energy, finance and transportation were found to be most dependent on cross-border CII.

The study concludes that there are only a 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. We believe the results of this study are informative for governmental policymakers and regulators as they provide a good insight into cross-border dependencies of CII and the associated legal, policy and strategic issues.

Look at other nations for inspiration, but remain sensitive to national particularities

Any governmental policymaker studying the body of knowledge on CIIP will encounter a multitude of approaches for identifying their nation's CII to choose from. We recommend compiling a portfolio of approaches to assess CII rather than pick one as a one-size-fits-all. Input for such a portfolio can be found in the CIIP policies and practices of other nations. However, policymakers should tailor their CIIP policy to the specific conditions of their nation, being the degree of digitalisation or other particularities like unique CI or specific dependencies on specific ICT and OT. Moreover, because of the global trend of increasing digitalisation, it is prudent to regularly reassess the need to step up efforts on CIIP.

Stakeholder management

What constitutes stakeholder management?

Stakeholder management entails all activities conducted by responsible authorities to involve relevant actors in the protection of their CII. This may include fostering relations with other public organisations, as well as with private organisations. In many nations, the largest part of CI and CII is operated by private organisations. Government intervention can take place in the form of collaborative agreements between public and private sectors. You may choose to limit the role of government and opt purely for market provision for CII.[12] If your nation's CII is mostly operated by private entities, the government can support information sharing, facilitate and stimulate cooperation, and perform control and oversight through legal and regulatory instruments. Public-private partnerships (PPPs) are often employed to structure the relationships between government and private operators. Such partnerships can lead to reduced risks and lower costs for the organisations involved because of improved collaboration. It is important, however, that actors involved advocate clear roles and responsibilities, irrespective of the chosen approach to structure stakeholder relations. Finally, exercises can play an important role in support of stakeholder management. Assembling stakeholders in one room and running an exercise is an effective method the authorities responsible for CIIP can use to manage stakeholder relationships, engage stakeholders and generate stakeholder commitment (see the capacity on exercises for more information).

Features

Protection of a CI and CII requires insight into their governance and ownership structures and the type of stakeholders that are involved. Different types of stakeholders exist. Stakeholders can 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, but a basic method of listing the CII elements seems to suffice to gain a general understanding of the sort of stakeholders involved in a nation's CI and CII. A diverse mix of stakeholders will likely need to be involved in CIIP. After initial alignment between public stakeholders, CII operators and other key stakeholders (from private industry, chambers of commerce, academics and research & development, and others) should be brought in to jointly address CIIP challenges. In practice, this requires a gradual, continuous, and iterative process of stakeholder management.

As a policymaker, you can either engage with specific stakeholders or start broad dialogues with multiple stakeholders. The goal is to build partnerships. Establishing partnerships with a mix of stakeholders can be an effective method to develop a shared vision on critical information infrastructure resilience and will help create broad support for policy measures. At the strategic level, this stakeholder engagement and building of partnerships can be used for high-level discussions and building consensus on strategic decisions. At the tactical level, stakeholder engagement efforts can be aimed at policymakers of involved organisations to share risk management assessments or insights and prepare for collaboration during incidents. Some examples of CII stakeholders are:

- 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 a specific element of CI (e.g. Economic Affairs, Energy, Health departments)
- regulators for specific CI Domains
- law enforcement and other public agencies
- CI and CII operators (e.g. energy plants, hospitals, internet providers)
- politicians and parliament
- manufacturers, system integrators, and third-party maintenance companies
- intra-sectoral or cross-sectoral (branch) organisations
- Computer Security Incident Response Teams (CSIRTs)
- the national cyber security centre
- academics and research and development ('triple helix')

Good practices

Building public-private partnerships

Even though in many nations the protection of CI and CII is part of the national security policy, most cybersecurity-related decisions on CIIP are made by the CII operators. Cooperation between national authorities and CII stakeholders is necessary to ensure that the various CII stakeholders take the national security risks of CII failure into account during their decision-making. When CII is operated by private stakeholders, such cooperation may require the establishment of public-private partnerships (PPP). PPP in the contexts of CIP and CIIP refers to any collaboration between a government agency and private entities for the purpose of ensuring the correct functioning of the CII services. From a policymaker's perspective, PPP should be about fostering a collaborative mindset on how to manage relationships, responsibilities, and cooperation with stakeholders regardless of whether they are public or private. Most likely, a diverse mix of stakeholders will need to be involved in your nation's CIIP. Table 3 offers a template to create your initial set of relevant CI and CII stakeholders.

A survey to increase insights in cross-border CII dependencies

In Germany, UP KRITIS is a national initiative between the state and critical infrastructure operators for the protection of critical information infrastructures. UP KRITIS consists of more than 450 associates. Since ICT has become an important element for all critical processes, the protection of information infrastructure is of particular importance to UP KRITIS. The organisations involved cooperate on the basis of mutual trust. They exchange ideas and experiences and help each other learn how to best protect the critical (information) infrastructure.

	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

Table 3. Table to assist in stakeholder analysis (some examples)

CIIP Action Planning

What constitutes CIIP action planning?

CIIP action planning is aimed at providing an overview of all objectives and the required actions to achieve these objectives in the context of protecting CII. This overview often translates into a clear action plan. In many cases, CII is important for several policy domains that fall under different parts of the government (e.g. the Ministry of Economic Affairs and the Ministry of Security). A cross-domain CIIP action plan will help you cover all relevant aspects and balance different policy perspectives for your nation's CII. This, in turn, can help you with putting the topic of CIIP on the agenda of other government policymakers. A national CIIP action plan can be either part of a (new) national (cyber) security plan or drafted as a separate document. An action plan typically includes objectives, a mission and vision statement, budgetary planning, responsibilities, ambitions, planning (long- and short-term) and actions.

Features

You may want to consider a broad range of policy options as part of your nation's plans to enhance the national CIIP. Which policy options are best fit for purpose depends on many factors, including the type of threats your nation and its CII face, the types of stakeholders involved in the protection of the CII, and the history and culture of public policy in the nation. Policy options include, but are not limited to:

- self-regulation by organisations involved with CI and CII
- voluntary compliance
- voluntary government programmes
- market mechanisms and incentives
- legal and regulatory frameworks

Whether your nation uses voluntary programmes for CII operators to participate in, incentives ('carrots and sticks') or regulatory and legal frameworks depends on various factors, such as the type of stakeholders involved in the CII, the nation's culture, its established practices or goals and ambitions with regards to CIIP. Many nations have adopted a risk and responsibility-driven approach that sets a baseline for their CIIP and leaves the specifics on how to protect its CII to the CI and CII operators, who inherently have more technological expertise. If multinationals operate in a part of the national CII, you should consider the arrangements they have made in other nations. Be aware that situations in which a part of the CII is operated by multinationals, present specific opportunities and challenges. On the one hand, nations can benefit from the experience multinationals have gained with CIIP in other nations. On the other hand, it can also be more difficult to influence multinationals to align their CIIP activities in your nation because of the arrangements they have made with other nations and the resulting need for cross-border cooperation and uniform internal processes.

Good practices

National CIIP action plan

A national, cross-sectoral action plan on CIIP is an all-encompassing tool that will help you with CIIP planning. As stated in the explanatory paragraph on CIIP planning, the action plan outlines strategic objectives and activities over a long-term period, which enables all identified stakeholders to collaborate in a joint national vision on the protection of critical (information) infrastructure.

Canada's action plan for critical infrastructure

Canada has created a Blueprint *to implement its National Strategy for Critical Infrastructure. The National Cross Sector Forum 2021-2023 Action Plan for Critical Infrastructure (the Action Plan) sets out tangible initiatives that promote a collaborative approach among governments and critical infrastructure sectors to identify and manage risks before they lead to disruptions. The National Strategy is based on the principles outlined under the Emergency Management Framework for Canada, which recognises the roles that various stakeholders must play in Canada's emergency management system to enhance the safety of Canadians. The Action Plan sets out concrete activities under each of these three strategic objectives and takes a close look at the risks that the critical infrastructure community faces today, and those it might face in the upcoming years. It also considers accomplishments resulting from previous and ongoing collaborative efforts among all levels of government and critical infrastructure sectors.*

Legal framework

What constitutes a legal framework?

Legal and regulatory frameworks are key governmental instruments to structure the protection of CII. Nations may use national law and regulation to assign responsibilities to operators of CII, for example, to meet cybersecurity standards. Many nations have to deal with a patchwork of global, regional and national level legal and regulatory frameworks in relation to CIIP. Every nation also has its own unique legal and regulatory structure. Legal frameworks are included in the CIIP Capacity Framework as they constitute a key component of any approach to CIIP.

Features

Adopting a broad CIIP approach in a national legal framework or national cybersecurity strategy may sound straightforward. However, a 2016 CIIP study for Latin America and the Caribbean found that 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 mainly existed because of past emergency situations. Approaches to CI and CII were present in the nations studied but were identified as unsystematic and containing gaps.

Moreover, governance through legislation has proven to be a challenge in the rapidly evolving cyberspace. Where possible, legislation relating to the identification and protection of CII should be drafted in such a way that additional legislation will not be 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/from the list of elements comprising the national CII with minimal delay. To effectively arrange the governance of new elements of CII, you can also look for alternatives to legislation and regulation.

Good practices

Specific cybersecurity legislation

Despite the challenges of creating effective and durable cybersecurity legislation, having a legal framework in place specifically for the cybersecurity domain can prove to be very valuable. For instance, such a framework can provide clarity on important principles of cybersecurity, on security requirements, and on where responsibilities lie in case of incidents. Moreover, it can facilitate a clear outline of a larger cybersecurity policy perspective or of critical information infrastructure protection in particular.

Estonia's Cybersecurity Act

Estonia has a specific law on cybersecurity that provides the requirements for the maintenance of network and information systems essential for the functioning of network and information systems for society and state and local authorities. The law also covers liability and supervision, as well as the legal basis for the prevention and resolution of cyber incidents.

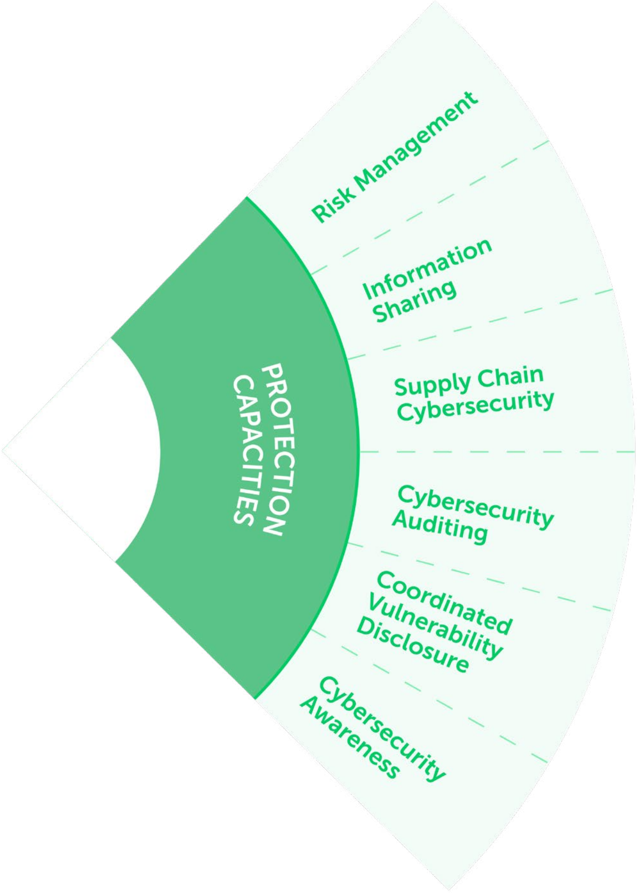
References Strategy and policy

1. Federal Chancellery of the Republic of Austria, Austrian Cyber Security Strategy, 2013. Online
2. 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). Online
3. CIPedia© is a Wikipedia-like online community service focusing on Critical Infrastructure Protection (CIP) and Critical Infrastructure Resilience (CIR)-related issues, developed by the EU FP7 project CIPRNet and continued by volunteers.
4. For more information on this topic, see for example:
   - European Council Directive 2008/114/EC
   - S. Gnatyuk, Y. Polishchuk, V. Sydorenko and Y. Sotnichenko, "Determining the Level of Importance for Critical Information Infrastructure Objects," 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), 2019, pp. 829-834, doi: 10.1109/PICST47496.2019.9061390. Online
   - O. Potii and Y. Tsyplinsky, "Methods of Classification and Assessment of Critical Information Infrastructure Objects," 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), 2020, pp. 389-393, doi: 10.1109/DESSERT50317.2020.9125028. Online
5. 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.
6. 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). Online
7. 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. Online
8. 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. Online
9. Mattioli, R., & Levy-Bencheton, C. (2014). Methodologies for the identification of Critical Information Infrastructure assets and services. ENISA Report–2014–43. Online
10. Cabinet Office, Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure from Natural Hazards, March 2010. Online
11. Kaska, K. and Trinberg, L. (2015). Regulating cross-border dependencies of Critical Information Infrastructures, NATO Cooperative Cyber Defence Centre of Excellence (CCD-COE), Tallinn. Online
12. Assaf, F. (2008). Models of critical information infrastructure protection. International Journal of Critical Infrastructure Protection 6(14). Online

Theme

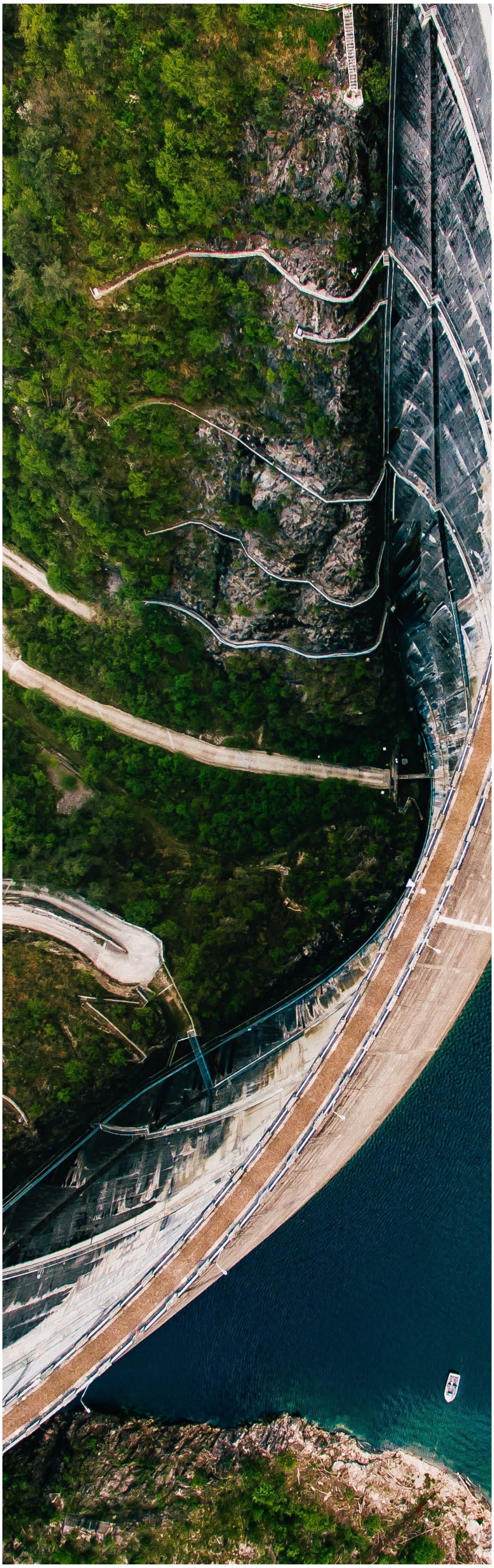
Protection Capacities

Protection of the Critical National Information Infrastructure (CNII) encompasses 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. The protection of a nation's CII is not only a technical concern; organisational and human aspects are equally important. Awareness of Critical Information Infrastructure Protection (CIIP) risk management may ensure a balanced approach to cover the full cyber incident response cycle. Regular use of a risk assessment will help you strengthen established CIIP efforts to match actual risks.



Recommendations for CII operators

Unlike recommendations in the other themes, which are primarily aimed at policymakers, risk management and protection measures in this theme should be understood as practices to be employed by individual CII operators or a sector-specific set of CII operators. For instance, information sharing on a sectoral basis can strengthen the overall level of protection of a CI sector.



Risk management

What constitutes risk management?

Critical Information Infrastructure (CII) operators can use risk management to determine the measures needed to protect their operations. Risk management typically involves C-level decision-making. Governmental policymakers may provide tools and guidelines to support the use of risk management. They can also provide information on cybersecurity threats to a nation and its industries. Key factors to take into account for CII risk management are:

- the assessment of the vulnerability of CII systems
- critical dependencies with other sectors and services
- the assessment of the overall impact of disruptions
- the current cyber threat landscape
- the use of a balanced approach to cover the full cyber incident response cycle (proactive, pre-emption, prevention, preparation, incident response, recovery, aftercare and follow up) in order to mitigate risks.

Features

Risk management by CII operators is an important aspect of CIIP. For example, the EU NIS directive promotes a culture of risk management, involving risk assessment and the implementation of security measures appropriate to the risks faced.

Risk management efforts can be used to 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 risks that arise from critical dependencies with other sectors, an aspect of impact that may supersede the direct interests of a CII operator.

There are many nations that have developed risk management guidelines and tools. Although these differ considerably between nations, they have some elements in common:

- An understanding of the context in which the analysis is conducted.
- Identification of potential risks.
- Assessment of threats, vulnerabilities (sometimes integrated into the determination of threats) and impacts.
- Determination of ensuing risk factors (and analysing them).
- Determination of appropriate measures.

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

In addition to risk management by individual Critical Infrastructure (CI) or CII operators, collective approaches to risk management can be applied. Be aware that a cross-sectoral risk analysis requires a more structured and managed approach. Such an analysis can be organised by an association (companies or sector), or in cooperation with one or more governmental agencies. These types of risk assessments can be supported by scenario-based approaches and discussions. In comparison to more technically focused risk analysis, scenarios can incorporate a broader narrative (going beyond mere technical risks and include for example external shocks or other contextual information). Scenario-based risk analyses within a sector can help stakeholders to imagine conditions under which information infrastructure elements may fail. It may also help stakeholders assess the criticality of different elements of CII on a national level. Moreover, a scenario-based risk analysis with a broad scope (process, people, technology) can shed light on the importance of Information and Communication Technology (ICT) and Operational Technology (OT) – which are not directly related to the critical process but are also important elements – and new developments, so they can be incorporated into CIIP policy.

Good practices

Providing tools and risk information to CII operators

Policymakers can stimulate CII operators to conduct risk management by providing tools and guidelines. Providing tools and input may encourage the use of risk management and enhance the applicability of the assessment. A good practice for policymakers is to freely offer risk analysis tools and information to organisations and companies. There are many nations that have developed risk management guidelines and tools. For instance, some nations offer guides that provide an overview of the risk management steps that need to be taken, and some nations offer self-assessment tools that can be used to identify risks for the CII operator.

The USA's Cyber Resilience Review

An example of a voluntary, no-cost risk analysis assessment is the US Cyber Resilience Review (CRR). The CRR can evaluate an organisation's operational resilience and cybersecurity practices in terms of critical services of CI sectors, organisational size, and maturity. The CCR is comprised of ten resource guides. Each guide can be used on its own. Others may prefer to use the full set of CCR resource guides as a coherent approach. The Cyber Resilience Review Resources guides are:

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

An overview of risk management approaches by ENISA

Another extensive guide for risk management approaches is found in the ENISA publication of 'Inventory of Risk Management methods and tools'[1]. For CIIP, a number of risk management methods can be used. Although these methods differ in both the actual steps that need to be taken and the tools that can be used to apply those steps, most risk management methods still rely on a common structure. The ENISA publication provides a structure of common elements in most risk management methods, such as the assessment of the risks and decisions on how to treat those risks, see figure 6.

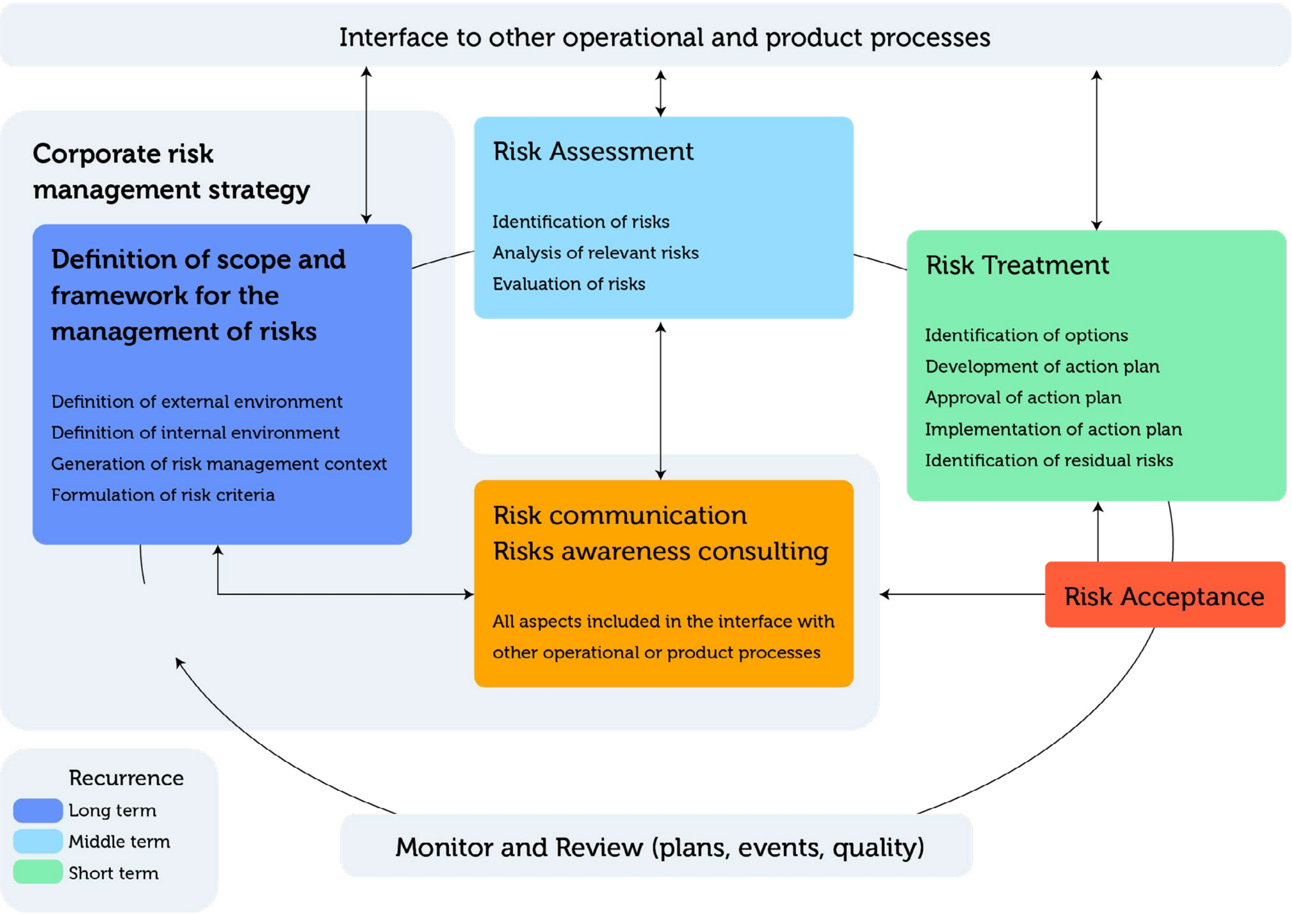

Interface to other operational and product processes
Corporate risk management strategy
Definition of scope and framework for the management of risks
Definition of external environment
Definition of internal environment
Generation of risk management context
Formulation of risk criteria
Risk Assessment
Identification of risks
Analysis of relevant risks
Evaluation of risks
Risk Treatment
Identification of options
Development of action plan
Approval of action plan
Implementation of action plan
Identification of residual risks
Risk communication
Risks awareness consulting
All aspects included in the interface with other operational or product processes
Risk Acceptance
Monitor and Review (plans, events, quality)
Recurrence
Long term
Middle term
Short term

Figure 6. Common elements in risk management methods

Information sharing

What constitutes information sharing?

The interconnectedness of CII requires organisations to collaborate to ensure and maintain the protection of the CII. Information sharing is a key element of such collaboration. Information sharing within or between public and private organisations provides a basis for a collective understanding of threats, risk, vulnerabilities, dependencies, and shared knowledge on protective measures. It allows for stronger protection of CII, both at the national and international level. For example, sharing cyber intelligence or information about incidents can contribute to greater situational awareness.

Features

Building strong, trusted networks between CIIP stakeholders and enabling the sharing of information are important conditions to safeguard society. Timely and speedy sharing of cybersecurity-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 cybersecurity challenges of CII operators. As the nature of cybersecurity has and will continue to evolve rapidly over time, information sharing efforts should also evolve to keep pace with changes in the cybersecurity landscape. A benefit of sharing information is the opportunity to leverage knowledge, awareness, understanding and experiences across a broader community. For example, other countries may have valuable experiences to share from previous CIIP efforts.

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. Therefore, information sharing (in this context) is usually performed among a group of carefully chosen people with a mutual goal: keeping abreast of new and emerging threats and vulnerabilities, and related issues. This group meets regularly, develops personal trust, and shares sensitive information about incidents, threats, vulnerabilities, good practices, and solutions. Information sharing can be conducted in a traditional face-to-face setting as well as remotely. In both cases, the information sharing environment should be confidential, meaning that group members should not be likely to disclose the details or the originators of the information while using use of the information to protect their own systems.

Policymakers can assist in the creation of such an essential confidential environment. The location of the environment, either explicitly outside or inside a particular ministry, affects the approach of information sharing chosen by public and private stakeholders (for instance, there is a major difference of setting within a ministry of defence or secret service compared to within a ministry of economic affairs). The environment may also be influenced by how information exchange takes place (regular, regulated, formal or informal rules) and how previous efforts of public bodies to create such an environment were perceived by relevant stakeholders. Establishing an environment of trust and value takes time and commitment by all participants, but the added value of information exchange greatly outweighs the cost of these efforts.

Good practices

Stimulate the sharing of cybersecurity-related information within critical sectors

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 because it ensures that information on new risk factors is available more quickly to stakeholders. The CII protection measures may be adapted accordingly. If major CII disruption occurs, the existence of a trusted network with common interest and experience helps to address the incident effectively and collaboratively. Information sharing is therefore an effective approach in support of managing the collaborative CII risk in a domain where the threat landscape is continuously changing.

Experiences of successful voluntary information sharing initiatives show that trust is the key success factor. A cornerstone of this trust is an agreement on how stakeholders may use exchanged information within their own organisation. Information sharing, however, is a multi-faceted notion with many related policy issues, both on the public and the private side. For more information, see a picture of some of the building blocks starting from green (relatively simple) to red (major effort) in figure 7[2]. for the CII operator.

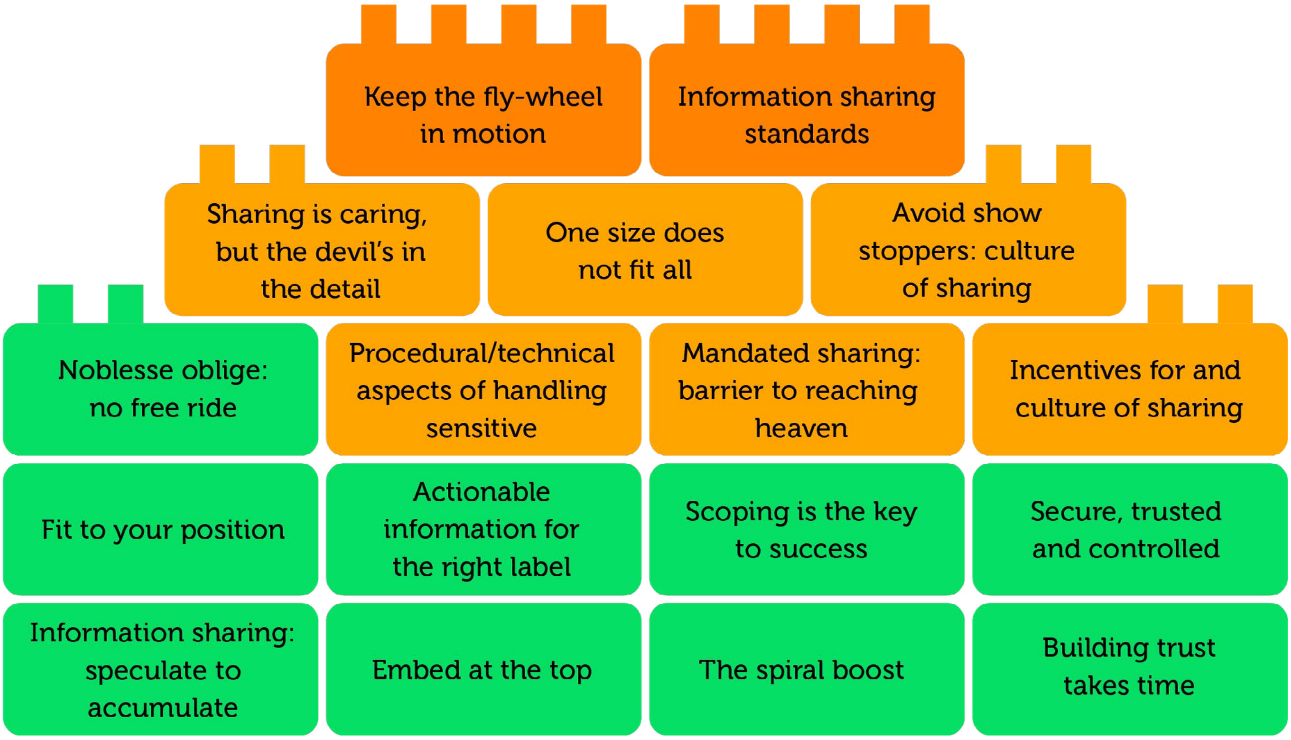

Keep the fly-wheel in motion
Information sharing standards
Sharing is caring, but the devil's in the detail
One size does not fit all
Avoid show stoppers: culture of sharing
Noblesse oblige: no free ride
Procedural/technical aspects of handling sensitive
Mandated sharing: barrier to reaching heaven
Incentives for and culture of sharing
Fit to your position
Actionable information for the right label
Scoping is the key to success
Secure, trusted and controlled
Information sharing: speculate to accumulate
Embed at the top
The spiral boost
Building trust takes time

Figure 7. Building blocks for information sharing[2].

By law or through regulation, you can mandate information sharing by CII operators about (cyber) security breaches and CII disruptions. However, experience learns that in such cases, it is often hard to guarantee the quality of the exchanged information, as laws and regulations do not instil an intrinsically motivated exchange; they are a stick, not a carrot. Even mandated approaches therefore require trust and a spirit of voluntary cooperation.

In an international environment, it has proven to be even more difficult to build the trust needed for effective information sharing due to logistic challenges when organising face-to-face meetings, language barriers, cultural differences, regulatory disparities, and competitive hurdles. However, some nations have established cross-border communities that share CIIP information, like the Financial Services Information Sharing and Analysis Center (FS-ISAC).

Information Sharing and Analysis Centres (ISAC)

An Information Sharing and Analysis Centre (ISAC) is a platform for deliberation concerning cybersecurity issues that are relevant for a specific sector. ISACs generally include a network of ICT and cybersecurity specialists and aim to facilitate the sharing of sensitive or confidential information about cyber incidents, threats, vulnerabilities, and measures. By discussing the experiences of various organisations in a sectorial ISAC, participants learn a lot from each other. Policymakers can play a role in the world of ISACs by, for example, organising meetings within and between ISACs, or by sharing guidelines for starting or joining an ISAC.

Traffic Light Protocol (TLP)

In order to establish the level of trust needed for information sharing between public and private organisations, you will need procedures on how to deal with sensitive information in a trusted manner. The Traffic Light Protocol (TLP) provides a very simple method for establishing the required level of confidentiality for the information exchanged. One of the key principles of the TLP is that whoever shares sensitive information also establishes if and how widely the information can be circulated.
The originator of the information can label a piece of information with one of four colours:

RED – Not for disclosure, restricted to participants only. Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED information should be exchanged verbally or in person.

AMBER – Limited disclosure, restricted to participants' organisations. Sources may use TLP:AMBER when information requires support to be effectively acted upon yet carries risks to privacy, reputation, or operations if shared outside of the organisations involved. Recipients may only share TLP:AMBER information with members of their own organisation, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing and these must be adhered to.

GREEN – Limited disclosure, restricted to the community. Sources may use TLP:GREEN when information is useful for the awareness of all participating organisations and peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organisations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

WHITE – Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Stimulate information sharing with a broader community

In order to enhance the critical information infrastructure protection capacity, policymakers can benefit from having a broad scope of potential organisations and other entities that could be involved in the information sharing process. Given the interconnectivity and interdependencies in the information infrastructure, it is in the interest of cybersecurity to look beyond the critical sectors and governing bodies for information sharing. A good way to generate a collective understanding of threats, risk, dependencies, and shared knowledge on protective measures is to set up a network of information sharing nodes. In this network, each organisation has its own network of stakeholders with whom it can share relevant cybersecurity information. The linking pins in these separate networks (e.g. CERTs) are connected with each other and possibly a (governmental) cybersecurity linking pin (e.g. an nCSIRT) to ensure that relevant information can be distributed between them and a wide range of potentially relevant stakeholders. As a policymaker, you can both stimulate the establishment of such a broad information sharing network as well as facilitate its practice with tools such as guidelines for collaboration and information sharing.

Identifying relevant stakeholders for information sharing initiatives

The good practice of identifying relevant stakeholders for information sharing initiatives is among the first steps you should take as a policymaker when starting out with CIIP information sharing endeavours. Policymakers can facilitate the establishment of new sharing initiatives by approaching partnerships or networks that are already in place but do not yet share their information. For example, sectoral or regionally connected organisations may have formed associations (such as an association for municipalities or a trade association) that already have a network infrastructure in place. You could approach a frontrunner in these existing networks that could assist in developing a cyber information sharing capacity within the partnership. Moreover, through the individual organisations in these associations, a more elaborate network to other stakeholders (such as suppliers or clients) can be used to distribute relevant information even outside of the network. Lastly, you may benefit from creating a priority list of sectors or other domains in which you would like to facilitate such an information sharing initiative based on the importance of the sector or impact sensitivity.

Examples of stakeholders involved in information sharing initiatives are:

- The Forum for Incident Response and Security Teams (FIRST)
- The European Government CERT Group (ECG)
- Infragard
- Several ISACs in the US
- The UK Cyber-Security Information Sharing Partnership (CiSP)
- The German UP KRITIS
- CPNI Information Exchanges in the UK
- National Cyber Security Center (previously known as MELANI) in Switzerland
- The ISACs in the Netherlands

In many of these initiatives, CIIP stakeholders come together and actively share information about threats, incidents, vulnerabilities, and good practices.

The Swiss National Cyber Security Centre (previously known as MELANI)

The Swiss NCSC serves two groups of constituents. The first one is the public customer group that includes private computer and internet users, and small and medium-sized enterprises (SMEs) in Switzerland.

The second is a closed customer group that comprises selected operators of the CI (e.g. energy suppliers, telecommunication companies, and banks). It is the NCSC'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 aim of the NCSC is to ensure that network and system interruptions as well as abuse are rare, of short duration, controllable, and have minimal impact. The NCSC can only achieve this task through close partnerships and cooperation with these CII operators. Within this partnership, the Swiss NCSC focusses on sharing knowledge and resources that are available only to the government and which are not otherwise accessible to the private sector. For example, information of intelligence services (e.g. countering industrial espionage), the Computer Emergency Response Teams (CERTs) in the nation and law enforcement.

Supply chain cybersecurity

What constitutes supply chain cybersecurity?

Supply chain cybersecurity refers to the efforts that enhance the security of all elements in the supply chain of a CI or CII. In today's interconnected world, the functioning of critical (information) infrastructures is often dependent on entities other than any individual CI or CII operator. A supply chain attack seeks to damage an organisation by targeting vulnerable elements in the supply chain information network, such as compromised networks or software vulnerabilities. Attacks can be carried out through malware inserted into software or hardware, or through counterfeit hardware. In the context of CI(I)P, supply chain cybersecurity refers to the secure design and manufacturing of ICT elements and the assurance that these elements are adequately secured throughout their entire lifecycle. Supply chain cybersecurity aims to ensure the correct functioning of all systems within a supply chain that are critical for either a CI or CII.

Multiple stakeholders play a role in ensuring the trustworthiness, reliability, integrity, and continuity of critical ICT elements in the supply chain that are critical to the operations of the CII. Acquiring organisations must ensure that they define appropriate security requirements and that they only acquire products and services that fit those requirements. Suppliers, on the other hand, have a responsibility to provide secure products and services.

Policymakers also carry a responsibility for the security of critical services. Policymakers who want to improve the cybersecurity of a CI or CII supply chain should create an overview of the most critical parts of the supply chain, provide security requirements for parts of the chain, and provide incentives and tools to support all organisations involved.

Approaches to supply chain cybersecurity

There are three perspectives on supply chain cybersecurity that can be distinguished:

- *The acquirer-based approach focusses on the responsibilities of the organisation that acquires products and services (i.e. CI operators) to ensure adequate security of their own hardware, software and services, and those acquired from suppliers.*
- *The supplier-based approach focusses on the responsibilities of the vendor organisations to supply secure products and services.*
- *The supply chain approach tries to assess and ensure the security of the overall chain. This perspective takes all relations in the entire supply chain into consideration as it presumes that cyber risks cannot be sufficiently managed by a single organisation.*

Features

Societies at large not only use but also rely strongly on the safe and secure functioning of critical (ICT) products and services. Over the years, there has been a trend for supply chain cybersecurity to become increasingly complex. Because, as interdependencies grow, CI and CII tend to rely more and more on third parties and small incidents are likely to affect many stakeholders. Managing direct suppliers has in many cases already proven to be a challenge, but, nowadays, supply chain cybersecurity also includes the management of third parties in an increasingly globalised setting. The ICT market is run by a few large global suppliers, who are not easily swayed to cater to the needs of individual organisations for their CII operations. At present, there is a need for a harmonised set of cybersecurity requirements and measures, as well as adequate regulation to act on (or overall vision on how to deal with) supply chain cybersecurity. This need stems from the existing fragmentation of national requirements, measures, and regulations. As supply chains are constantly changing, it is often difficult for organisations to identify CI or CII supply chains, let alone recognise that they belong to such a supply chain and act on it (both within and outside the organisational boundaries). It has also become increasingly difficult for organisations to ensure the trustworthiness, standardisation, reliability, integrity, and continuity of ICT elements of all of their main suppliers. This makes organisations vulnerable to attacks and disruptions through the weak links in their supply chain. As a policymaker, you can help mitigate these risks and vulnerabilities through various activities, such as the following:

- Stimulating supply chain cybersecurity by selecting a mix of appropriate governance approaches. When preparing for new policies, policymakers need to determine what form of governance is adequate, effective, and feasible. They must decide whether an increase in supply chain security should be secured through law, (self-)regulation, or softer policy measures. One way to increase supply chain cybersecurity is by stimulating the harmonisation of requirements or standards of supply. Another would be to focus on stimulating transparency for requirements that are already in place for both operators and vendors.
- Enforcing or stimulating the cybersecurity in supply chains of CI operators and vendors by focussing on (sufficient) levels of security. Policymakers can balance different approaches on how to facilitate the process of mandatory and voluntary auditing requirements, how to enforce or incentivise these requirements, and how to help the industry in understanding cybersecurity policies and standards. Policymakers should also appropriately motivate organisations to comply.
- Facilitating and stimulating dialogue between organisations in supply chains to create more awareness and security. This is not only a good way to stress the importance of supply chain cybersecurity to operators, vendors and other organisations, but also helps foster mutual understanding. Furthermore, it is a starting point to identify other potentially relevant stakeholders for the supply chain.
- Stimulating the development of measures and guidelines for supply chain assurance from CI and CII operators on a global level. For instance, assurance frameworks for CI and CII operators, certification requirements or guidelines for supply chain risk management (e.g. access rules for manufacturers for updating the firmware) or the reliability of services that reside outside national borders – for instance, the providers of transnational services (e.g. GPS or certificate authorities).

Good practices

Provide an overview of existing tools

Policymakers can support operators and vendors by providing an overview of existing tools such as frameworks, regulations, requirements, or guidelines that can be used to manage cybersecurity risks in supply chains. Creating these overviews can help achieve alignment and mutual understanding of what is needed to manage supply chain cybersecurity risks. It can also be an important step in the development of standardisation and regulations.

Supply Chain Security Guidance by the UK NCSC

The UK NCSC has developed the 'Supply chain security guidance' consisting of 12 principles that help organisations gain and maintain the necessary level of control over supply chains. This guide may help your nation in deciding on the level of detail of its own guideline, how such a guideline should be communicated and what kind of tools are to be provided.
The guidance provides a list of some frameworks and standards for managing supply chain cybersecurity, such as:

- *Cybersecurity Framework Manufacturing Profile*
- *Framework Improving Critical Infrastructure Cybersecurity*
- *MITRE's Supply chain attack framework and attack patterns (2014) & resiliency mitigations (2017)*
- *MITIGATE: a dynamic supply chain cyber risk assessment methodology*
- *Supply chain risk management practices for federal information systems and organisations*
- *ISO 28001: Security management systems for the supply chain*
- *ISO/IEC 27005: information security risk management (2018)*
- *ISO 31000: risk management (2019)*

Stimulate harmonisation of cybersecurity requirements

Suppliers often struggle with security requirements for their products and services for CII. Even when suppliers feel the need to provide cybersecurity for their products and services, it is not always clear to them which security requirements they have to fulfil. In other cases, multiple requirements between organisations and countries exist. Complying with specific security requirements for each organisation that relies on its products or services can be a serious challenge for suppliers. Policymakers can support the harmonisation of requirements across organisations, sectors or even nations. Different approaches exist, ranging from setting up dialogues between suppliers and acquiring organisations to harmonise requirements and publicly sharing information on the security ratings for products, to defining requirements through regulations. Keep in mind that regulation will not always be effective, and the global nature of the challenge calls for international collaboration to harmonise requirements.

Smart meter cybersecurity harmonisation in Europe

The European Smart Metering Industry Group (ESMIG) worked on harmonising requirements for secure smart metering across Europe. The group represents multiple European smart energy solution providers.

CISA taskforce for ICT supply chain risk management

The US Cybersecurity and Infrastructure Security Agency (CISA) has set up a task force to specifically focus on ICT supply chain risk management. The task force is the United States' pre-eminent public-private supply chain risk management partnership. Its mission is to identify and develop consensus on strategies to enhance ICT supply chain security.

Facilitate relationships between suppliers, operators, and other partners

Establishing relationships and building trust within a supply chain network can be an exhaustive and intensive process. To achieve the goal of adequate cybersecurity in a supply chain, we recommend taking a step-by-step approach. The primary role of the policymaker in this process is to facilitate and stimulate the actors in the steps they are taking. This requires policymakers to keep track of the maturity of a given sector's supply chain. This, in turn, will allow for stimulating measures targeted at the relevant stakeholders. Facilitation of relationships can be done in four steps:

1. Identify critical supply chains. The first step is to identify supply chains and make organisations recognise they are part of a supply chain. One of the ways to start the identification process is by conducting triage: which organisations are most important or closely linked to critical infrastructure and are therefore most important to its supply chain? From there, the network can grow. An example of a stimulus in this phase of the process is to inform organisations on the importance and workings of a supply chain in CI.

2. Stimulate dialogue between organisations in supply chains that have been identified. Provided that these organisations have an understanding of their position in the overarching supply chain of critical infrastructure (as well as in their own supply chain), stimulating dialogue between them can help create a better understanding of each other's role in the supply chain. Furthermore, a select number of organisations that already have insight into their supply chain dependencies can initiate a dialogue to gain a deeper insight into possible additional dependencies or a potential supply chain goal. For an example of stimulating dialogue, see Norway's National Cyber Security Strategy. They included initiating this type of dialogue as a recommendation in their list of measures.

3. Stimulate information sharing within supply chains. Information sharing between organisations in a supply chain can nurture the insight that there is a common supply chain challenge that – willingly or unwillingly – connects organisations with each other and that the security of the supply chain cannot be ensured by one organisation on its own. Information sharing may help organisations gain insights in: the criticality of specific elements, shared dependencies, and lessons learned from incidents. Policymakers can stimulate information sharing by catering to the infrastructural needs in the network of information sharing. A good example of information sharing in practice is within Information Sharing and Analysis Centres (ISACS) and Information Sharing and Analysis Organisations (ISAOs), where lessons learned and other information are shared on Industrial Control Systems.

4. Stimulate or facilitate collaborative risk analyses within supply chains. Organisations in a supply chain can also be brought together to perform a collective cybersecurity supply chain risk analysis in addition to individual risk analyses. Doing so might reveal unknown risks as well as opportunities to share responsibilities in the mitigation of risks. This may lead to organisations collaboratively deciding to influence manufacturing processes or diversification of common suppliers. A great way to do this is by organising a cross-organisational risk assessment with a collaborative perspective[3].

What constitutes cybersecurity auditing?

Auditing can be used to assess the cybersecurity of an organisation or specific ICT element. A cybersecurity audit is an evaluation of the level of security within an organisation. The audit assesses how well an organisation complies with a set of established criteria. When government organisations or a CI sector require CII operators to adopt specific cybersecurity measures, auditing can be used to gather evidence of compliance. It is not uncommon to delegate the auditing process to a third-party organisation. The auditing organisation can be an audit firm (specialised in a specific audit framework and standard) or a government agency, such as a regulator.

Features

Government organisations are looking for effective ways to ensure the security of their CII. As a policymaker, you can promote the use of audits according to common frameworks by CI operators or use auditing to ensure compliance with your national cybersecurity regulation.

Different techniques can be used during an audit, such as personal interviews, document analysis, and penetration tests. It is important that auditing organisations have adequate cybersecurity skills to ensure adequate results. In recent years, many traditional auditing firms have expanded their services in this area. For some auditing organisations, especially in government, cybersecurity audits are still a relatively new topic. Some of those audit organisations mention limitations in cyber-related skills and difficulties in evaluating progress in cybersecurity as one of the main challenges to cybersecurity auditing. Finding the right mix of skills at the auditing organisations is therefore important.

Since the auditing process requires a lot of effort from the audited operator, it can be worthwhile to use existing frameworks or standards to verify compliance. An advantage of using a well-known standard, such as ISO 27001, is that the certification process is already well-established and that there is an approval process that ascertains the quality of audit firms. Furthermore, the certificate is internationally recognised.

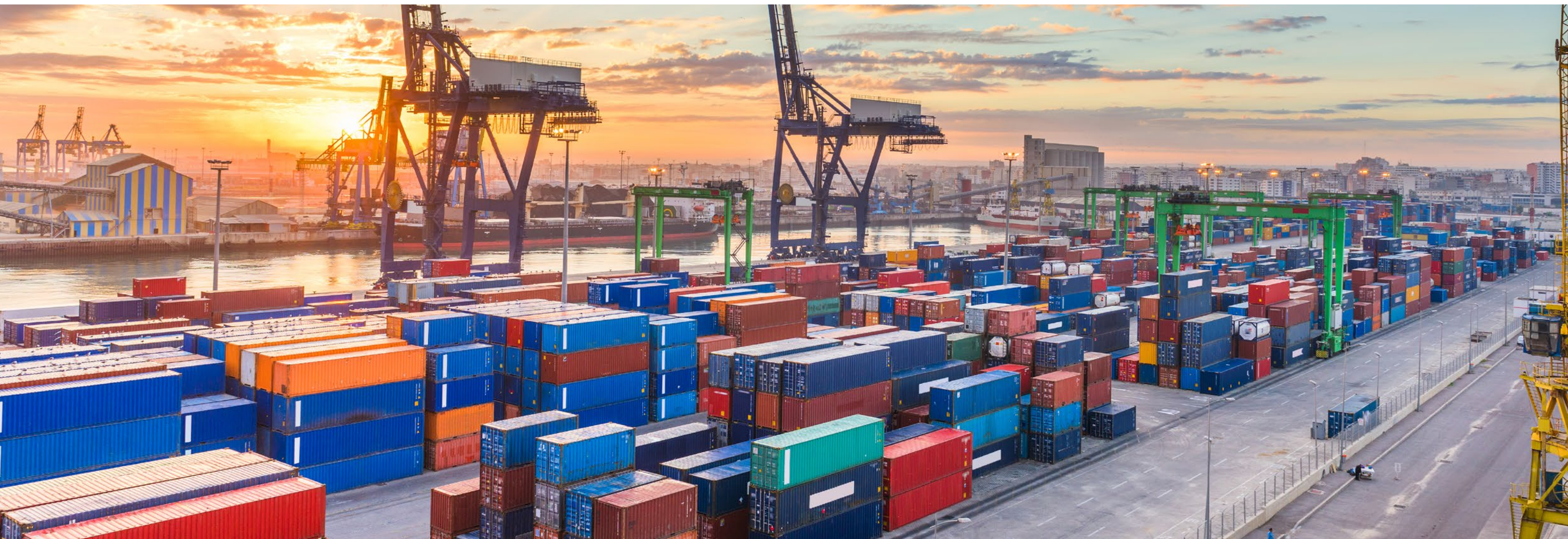
Good practices

Verify regulatory compliance with auditing

Auditing can be an important instrument to verify compliance with new cybersecurity regulation. One of the primary goals of the audit is to assess the design and effectiveness of the implemented organisational and technical controls.

Audit guidelines by CSA (Singapore)

The Cyber Security Agency of Singapore (CSA) has developed guidelines for auditing critical information infrastructures. Auditing is used to verify the compliance of CII operators with requirements of the Singapore Cyber Security Act, and to assess the adequacy and effectiveness of controls and measures put in place to meet these requirements.



Promote auditing based on existing frameworks and standards

CI operators can use auditing to assess their own level of security based on existing frameworks or standards. One of the well-known standards in this area is ISO 27001. Many companies and government agencies across the world use ISO 27001 to acquire certification for compliance. The certification is granted by certified audit firms.

Guidelines by ENISA on auditing NIS requirements

ENISA has published guidelines on assessing the compliance of CI and CII with the NIS Directive requirements (the NIS Directive is the first piece of EU-wide cybersecurity legislation [see EU 2016/1148]). The ENISA guidelines outline audit and self-assessment and management frameworks that can be applied to CI or CII operators, or the regulator.

Audits based on known standards, with additional requirements

Germany considers certifications based on ISO 27001 one of the options critical operators can use to document their compliance with the German Cybersecurity Act. A valid ISO 27001 certificate can be used as part of the documentation of compliance, as long as some basic conditions are met. In addition to an ISO 27001 certification, some other requirements are put on the scope of the audit. To be used for compliance, the scope of the documentation of compliance must fully cover the critical infrastructure or the essential service. Furthermore, the audit should assess the continuity of the essential services, focussing on the measures taken to avoid supply shortages for the population.

Coordinated vulnerability disclosure

What constitutes coordinated vulnerability disclosure?

Security researchers may attempt to breach, exploit, and manipulate CII systems to help uncover security flaws in systems and software. To facilitate the notification of vulnerabilities, a Coordinated Vulnerability Disclosure (CVD) program can be adopted. This should be done under strict conditions by trusted organisations for isolated subsystems. CVD can be defined as 'revealing ICT vulnerabilities in a responsible manner in joint consultation between discloser and organisation based on a responsible disclosure policy set by organisation'[4].

Features of coordinated vulnerability disclosure

Attempts to breach, exploit, and manipulate CII systems and their software occur all the time. Flaws in ICT security are exploited, unauthorised attempts to access systems happen, and CII operations might be interfered with because of such attempts. One way or the other, ICT-related incidents will happen. That is why it is important for organisations to facilitate notification efforts from benevolent individuals (such as ethical hackers).

CVD pertains to the mechanisms by which vulnerabilities are shared and disclosed in a controlled manner. Through CVD, knowledge of vulnerabilities is shared with one or more potentially vulnerable organisations to arrive at a solution for a found vulnerability in collaboration with the reporting party.

Policymakers may stimulate the use of CVD and provide information to organisations on how to set up their own CVD policies. Organisations can indicate via a CVD policy that they are open to receiving external vulnerability reports, describe their preconditions, and make promises through a non-persecution clause or by offering a reward for reporting the vulnerability. A CVD policy provides clarity and creates a safe environment for reporting parties to investigate and report vulnerabilities without taking legal action.

Good practices

Promote a policy for CVD

A good practice is to promote organisations' efforts of notifying security flaws in ICT security with a policy for CVD (sometimes also referred to as Responsible Disclosure). Governments, major banks, international organisations, and other private parties often have a CVD policy in place. The CVD policy ensures that they will not prosecute an individual for disclosing a security flaw if certain requirements are met. Through these policies, organisations guarantee anonymity to the disclosing party and guarantee to fix the issue they were notified of.

A CVD policy should cover at the very least the following elements:

- contact method for secure communication
- preconditions for reporting parties
- clear expectations for handling a report
- methods for rewarding a report

Coordinated Vulnerability Disclosure Guideline by NCSC

The Netherlands Cyber Security Centre has developed guidelines for setting up a CVD policy. For CVD to work, all parties must comply with agreements on how to report a vulnerability and how the vulnerability should be dealt with. It helps if an organisation publishes its preconditions for CVD, such as which systems are within the scope and what kind of research can be conducted. One important precondition is that the organisation will not report the reporting party or take other legal steps if the investigation and reporting are carried out within the conditions set. The NCSC's CVD guideline provides organisations with guidance in drawing up their own policy to embody the principles of CVD. Other useful resources on the subject are the website of the FIRST Special Interest Group on Multi-Party Coordination and Disclosure and the OECD guidelines on how policymakers can help address digital security vulnerabilities.

Cybersecurity awareness in the context of CII

What constitutes cybersecurity awareness?

Protection of the CII requires awareness from all stakeholders (e.g. infrastructure operators, authorities, suppliers, and contractors) about the importance of CII and the risk of CII disruptions. National cybersecurity awareness campaigns, conferences, regular communication and (national) exercises between CI and CII operators and authorities will contribute to this awareness. Cybersecurity awareness is about informing stakeholders of the importance of cybersecurity and CIIP, as well as creating a collective understanding among stakeholders that promotes trust and confidence. As a policymaker, you can promote this by showing leadership, and extensive participation and involvement in CIIP. An increase in cybersecurity awareness within a nation can lead to a heightened priority for security planning and management among stakeholders, as well as an increased understanding of the need for security.

Features

Cybersecurity awareness in the context of CIIP is mainly focused on raising awareness of cybersecurity risks for CII-related organisations. Organisations who concern themselves with critical infrastructure, either directly or indirectly, should be aware of their role in the larger CIIP landscape. They need to understand how their cybersecurity policies and efforts can affect not only their own operations but also whole supply chains. As a policymaker, you can raise awareness of CII risks by engaging in activities such as:

- encouraging organisations to review their use of technology
- sharing risk-related information about new types of cyberattacks
- sharing information on security measures and general good practices

Incident analysis and the publication of the outcomes of such analysis can also raise the cybersecurity awareness of CIIP stakeholders. Furthermore, it will contribute to an improved collective understanding of cybersecurity in the context of CIIP. Another course of action that could increase cybersecurity awareness in organisations is by promoting cyber capacity skills training, especially when aimed at professionals who support a critical service.

Good practices

Information campaign

One of the most fundamental activities to raise cybersecurity awareness is organising an information campaign. These campaigns can take many different forms, such as broadcasting public service announcements, organising workshops, or sharing cybersecurity toolkits. In all cases, successful communication will help foster an understanding of the cybersecurity topics that require attention. It will contribute to a heightened awareness among stakeholders of the potential risks for their own organisation, the broader supply chain and for the operability of critical functions that affect society.

India's Cyber Surakshit Bharat

The Ministry of Electronics and Information Technology in India has launched a programme called the Cyber Surakshit Bharat*. It is set to leverage the expertise of the IT industry in cybersecurity as it aims to ensure awareness about cybercrime and adequate safety measures for Chief Information Security Officers (CISOs) and frontline IT staff across all government departments. It includes an awareness programme on the importance of cybersecurity and a series of workshops on best practices and enablement of the officials with cybersecurity health tool kits to manage and mitigate cyber threats. The initiative focuses on topics such as the fundamental building blocks of a secure critical infrastructure, the role of a CISO in IT risk management, and analysing a department's cyber health. This programme also conducts training sessions for CISOs and technical officials.*

Singapore's Cyber Security Awareness Alliance

In Singapore, the government has supported the establishment of a public-private Cyber Security Awareness Alliance. The alliance comprises representatives from government, private enterprises, trade associations, and non-profit organisations. The goal of the alliance is to promote and enhance awareness and adoption of good cybersecurity practices among members of the public and enterprises in Singapore.

France's Etalab 2.0

In France, the current awareness and information sharing initiatives contain a wide array of tools and manuals, developed by ANSSI (Agence nationale la sécurité des systèmes d'information) in collaboration with public and private partners. For individuals and professionals, they developed a knowledge toolkit called Etalab 2.0. In this toolkit, the most important cybersecurity risks are explained and described in videos, articles, action points, and memos. The aim of Etalab 2.0 is to promote both preventative measures and reactive measures. Moreover, victims of cyber-attacks can seek contact with cybersecurity professionals on the Etalab 2.0 platform who can assist them. Lastly, the consortium also organises workshops and cybersecurity knowledge seminars.

References Protection Capacities

[1] ENISA, CIIP Governance in the European Union Member States (Annex), 2016, ENISA.
Online: Stocktaking, Analysis and Recommendations on the protection of CIIs (europa.eu)

[2] 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.

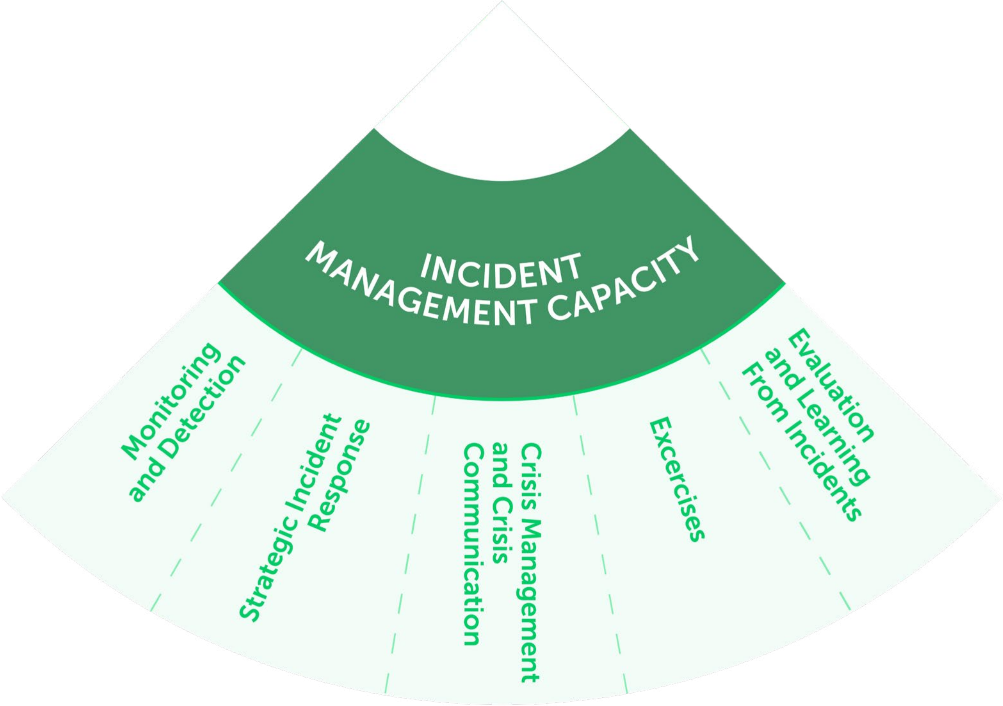
[3] National Institute of Standards and Technology (NIST), Best Practices in Cyber Supply Chain Risk Management, Conference Materials, 2015, NIST. Online

[4] NCSC-NL, Coordinated Vulnerability Disclosure: the Guideline, 2018, NCSC-NL. Online:

Theme

Incident Management Capacities

Even with protection capacities for Critical Information Infrastructure (CII) in place, cyber incidents will keep occurring. Incident management for CII aims to detect and respond quickly to cyber incidents in the Critical National Information Infrastructure (CNII), manage the required actions, and reduce the impact of cyber incidents involving the CII. The insights gained from analysing cyber incidents can be used to reduce the chances of new cyber incidents occurring in the future.


INCIDENT MANAGEMENT CAPACITY
Monitoring and Detection
Strategic Incident Response
Crisis Management and Crisis Communication
Excercises
Evaluation and Learning From Incidents

Monitoring and detection

What constitutes monitoring and detection?

Most organisations that are a part of the Critical Infrastructure (CI) or CII monitor their networks closely to detect intrusions of their networks and systems at an early stage. Some nations provide organisations with instruments in support of monitoring and detection. Different models exist. Some nations support their critical operators by providing a secure and confidential system for exchanging threat information. This system allows participating organisations to detect cybersecurity risks more quickly. Other nations (that monitor large scale systems and networks that are of critical importance) ask local telecom and internet service providers to help them. This approach may include the implementation of detection systems at their CII operators. These activities require maintaining a balance between respecting the responsibility of CII operators, the legal framework, and the protection of civil rights.

Features

Policymakers face the following challenges:

- Sharing classified information in a secure way. CI operators use the monitoring of their networks as a means to detect anomalies and possible attacks on their networks in a timely manner. Some CI sectors are a target for highly sophisticated (state-sponsored) attacks that may be hard to detect. The sharing of threat information by government agencies may enhance their capabilities to detect those types of attacks in an early stage. Collaboration with the government may in this case include the sharing of classified or other confidential cyber threat information (e.g. in the form of Indicators of Compromise (IoCs)).
- Stimulating mutual exchange of detection data. In systems that share threat and detection information, the information tends to flow only one way. Government agencies provide threat intelligence, but only a limited number of participants from private organisations share monitoring and detection information on attacks on their computer networks. Previous experiences show that it takes time to build the level of trust necessary for this two-way flow.

Good practices

Enhance monitoring and detection by sharing IoCs

Sharing indicators of compromise between organisations may help CII operators to defend themselves against similar incidents. Due to the highly sensitive nature of this information, it is important to establish a highly trusted environment for sharing this type of classified information.

Sharing indicators of compromise in the Netherlands

The National Detection Network (NDN) in the Netherlands is aimed at sharing IoCs between government agencies and organisations that are part of the national critical infrastructure and sectorial CSIRTs.

Within the NDN, the National Cyber Security Centre and intelligence agencies share information about cyber threats and make this information available. Organisations that participate in the NDN provide anonymous information as well. This way, other participants can determine whether they are facing a digital attack and implement suitable measures. knowledge seminars.

Providing sensor systems to CI operators in Sweden

In Sweden, a government agency offers CII operators the possibility of connecting to a sensor system. The sensor system provides connected actors with an expanded capability to discover and protect themselves from serious cyberattacks. The system is aimed to be a complement to commercial products and is designed with a high level of security and integrity protection.

Strategic incident response process

What constitutes strategic incident response?

To protect information and critical information infrastructure, a strategic incident response process can be developed and implemented to counteract any adverse cyber incident. This entails both an ex-ante and an ex-post process. The ex-ante strategic incident response process may include setting up predefined plans, roles, training, communications, and management oversight. The ex-post process entails engaging in mitigation and recovery by cybersecurity entities (e.g. Cis, SOCs and CSIRTs).

Ex-ante vs post ante

Strategic incident response actions can be divided into two categories based on the phase in which the actions take place: the ex-ante and the ex-post phase. Ex-ante strategic incident response entails the preparatory actions that can be taken to facilitate and improve the response when an incident occurs. Ex-post strategic incident response, on the other hand, entails the responsive actions that take place after the occurrence of an incident, which are aimed at controlling and mitigating damage.

At the operational level CI operators and Computer Security Incident Response Teams (CSIRTs) can execute procedures such as:

- accepting and analysing cybersecurity incident reports
- establishing an incident-specific response plan
- applying ad-hoc (containment) measures
- returning all systems back to normal operation

At the national level, governments (e.g. through a national CSIRT) can support the mitigation and recovery process by:

- initiating an investigation
- facilitating coordination
- sharing information
- obligating other CI operators to install preventive measures

Both the ex-ante and ex-post processes are aimed at achieving a quick restoration of the integrity of the networks and systems, thus effectively restricting damage to any critical information infrastructure.

Features

Entities responsible for performing incident management actions must recognise that they do not operate in isolation and that communication and interaction with all relevant parties is key – both internally with the CII community and with other external contacts. A notable challenge for policymakers is to facilitate the establishment of such a network of stakeholders and to encourage solid information exchange between all the nodes in this strategic incident response network. CSIRTs or Computer Emergency Response Teams (CERTs) are vital components of such a network, as their purpose is to provide services and support to stakeholders in the community to prevent, manage and respond to information security incidents. These teams are usually comprised of multidisciplinary specialists who act according to predefined procedures and policies to ensure a quick and effective response to security incidents as well as mitigate the risk of cyberattacks. They can serve different communities, e.g. critical infrastructure sectors, financial institutions, the government and its agencies, municipalities, product manufacturers, the cyber industry, and other types of organisations.

Establish a national CSIRT

An important trend in recent years has been the institutionalisation and creation of nCSIRTs. An nCSIRT's primary goal is to enhance the country's resilience in terms of digital safety, security and protection. An nCSIRT can be seen as a capacity that provides a wide range of cyber activities and services (both technical and non-technical) to relevant stakeholders in order to fulfil this goal. This entails for example activities aimed at preventing and resolving cybersecurity incidents, presenting lessons learnt in the process, operationally coordinating with stakeholders on countering cyber threats and incidents, collaborating with other CSIRTs, (often as a national point of contact) and generating situational awareness about cybersecurity risk. Although in practice many nCSIRTs are part of their respective government, nCSIRTs may also be operated by an independent third party. In either case, the nCSIRT will be tied to the national crisis management structure. What makes an nCSIRT national is that it has a formal mandate to fulfil a national responsibility.

An nCSIRT helps coordinate incident response at a national and an international level. They monitor, alert, warn, and give support during cyber incidents to their constituency. Some act as a default operational response team that national and international stakeholders can turn to when there is no other known contact in a country. Establishing an nCSIRT, therefore, is a core component of a nation's overall strategy to secure and maintain the services and infrastructures that are vital to national security and economic growth. Their services are vital in helping constituents during an attack or incident.

The institutional embedding of an nCSIRT, as well as its mandate, authority, responsibility, services, and funding, varies from country to country. Some national CSIRTs reside in government agencies, others reside outside of government structures. JPCERT/CC in Japan and Sri Lanka CERT, for example, are non-governmental organisations. Despite these two examples, the majority of nCSIRTs are part of a government structure.

As nCSIRTs focus on incident response, they need information and thus thrive under close cooperation and information exchanges. An operational body like a CSIRT may have strong ties with an entity that coordinates Critical Information Infrastructure Protection (CIIP) at the tactical level. In the case of privatisation, CI and CII operators may have already established a CSIRT to keep their element of the CII cyber secure. In such cases, it may be beneficial for the public bodies to interact or form an alliance with those private CSIRTs.

So, regardless of which organisation could take the lead in the strategic response effort, they will always need input from both CI and CII operators to assess the potential impact on the various elements of the Critical National Infrastructure (CNI). In addition, organisations will have to rely on international public, private and academic networks to gain the latest insights.

Singapore's nCSIRT

The Singapore Computer Emergency Response Team (SingCERT) responds to cybersecurity incidents for its Singapore constituents. Singapore's national CSIRT (SingCERT) was developed by the Infocomm Development Authority of Singapore in cooperation with the National University of Singapore in 1997. It has since become a part of the Cyber Security Agency of Singapore. SingCERT was designed as a one-stop centre for incident response; facilitating the detection, resolution, and prevention of security-related incidents on the Internet. SingCERT provides technical assistance and coordinates response to cybersecurity incidents, identifies, and follows cyber intrusion trends, disseminates threat information timely, and coordinates with other security agencies to resolve computer security incidents. SingCERT has also been active in organising and hosting Association of South-East Asian Nations (ASEAN) and Asia Pacific Computer Emergency Response Team (APCERT) exercises. Additionally, Singapore hosts seven Forum of Incident Response and Security Teams (FIRST) members.

AfricaCERT

AfricaCERT is a non-profit organisation that includes eleven African countries and provides a forum for cooperation among African CSIRTS to handle computer security incidents, assisting in the establishment of CSIRTs in countries that currently lack incident response capabilities, fostering and supporting incident prevention and educational outreach programs in ICT security, encouraging information sharing, and promoting best practices for cybersecurity.

Pratical guides and resources for setting up a national CSIRT

More information on how to set up a (n)CSIRT and assess its maturity can be found in the following documents:

- Best practices for establishing a national CSIRT – USCERT
- Global CSIRT Maturity Framework (GFCE)
- GFCE Good Practice Guide for National Computer Security Incident Response Teams for CII
- Getting started with a national CSIRT (GFCE)

(n)CSIRT information exchange

To facilitate the information exchange within a critical information infrastructure community (and possible adjacent organisations), it is important to establish contact between the relevant incident response teams. An nCSIRT could act as a linking pin within these networks. It can develop and sustain information exchange between the relevant CSIRTS and national partners as well as create an international network with other nCSIRTS. Already existing CSIRTs could thus be connected by building trust and providing reliable arrangements for optimal information exchange. This requires close collaboration and a multi-stakeholder approach. Moreover, the nCSIRT could use its expertise to stimulate and assist in the establishment of other CSIRTs and Information Sharing and Analysis Centres (ISACs) by providing tools, guidance and good practices, expertise, and organising joint exercises. In that way, the national CSIRT capacity can be extended by sharing the capacities of other CSIRTs.

Nationwide Coverage System

The Dutch 'Landelijk Dekkend Stelsel' (Nationwide Coverage System) is a system that allows various parties from the public and private sectors, such as CSIRTs, sectoral and regional partnerships, the Dutch National Cybersecurity Center (NCSC) and the Digital Trust Center (DTC) to share information and knowledge. The NCSC functions like a central information hub in a web of relevant stakeholders. The NCSC designates CSIRTs and other organisations as 'having an objectively recognisable task'. This means they have the explicit duty to inform other organisations or the public about cyber threats and incidents that are relevant to them. The information sharing could take place in a partnership alliance within a sector, a region or a supply chain. These alliances can also be designated as 'having an objectively recognisable task', which allows the NCSC to share valuable information on vulnerabilities or threats with its members. The CSIRTS and organisations in the alliance can subsequently inform their constituents and other relevant entities.

Crisis management and communications

What constitutes crisis management and communications?

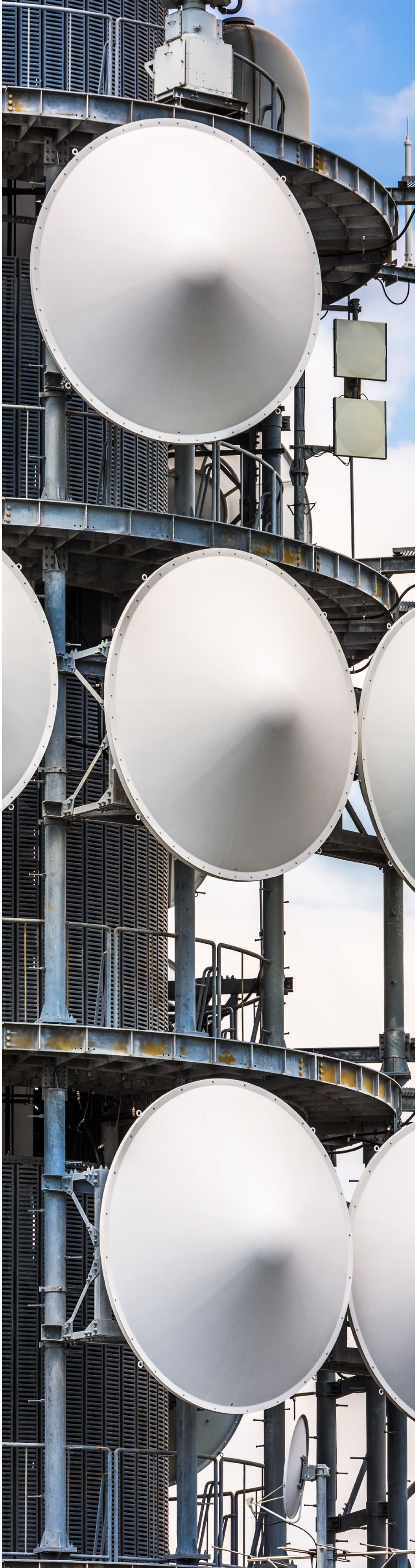
A large-scale incident can lead to a crisis. A crisis entails a situation with a high level of uncertainty that disrupts core activities to such an extent that it poses a threat to critical societal functions and therefore requires urgent action. Urgent action is what constitutes crisis management, which is designed to protect the organisation, stakeholders and society, and aims to mitigate the damage as much as possible. To achieve this as quickly as possible, the usual line of command is often temporarily changed for the duration of the emergency. The temporary change in command should facilitate the coordination process and facilitate a high situational awareness of all activities and statuses of the entities that are affected or that are taking part in the response.

An essential feature of crisis management is crisis communication. At the strategic level, this involves the enactment of control (at least in appearance) in the face of high uncertainty to win external audiences' confidence. At the operational level, crisis communication entails the collecting and processing of information for crisis team decision-making along with the creation and dissemination of crisis messages to stakeholders.

The dissemination of relevant information can take place through various communication channels, including the media. Regardless of the channel, relevant information must be distributed timely and accurately to those either responsible for taking part in the response or requiring to be kept informed about the progress and current status of the crisis management efforts. Hence, an important objective of crisis communication is effective stakeholder engagement.

Features

National crisis management organises and manages all roles, responsibilities and resources to deal with serious incidents, emergencies, and crises at a national level. Good crisis management



at a national level, as well as at international and regional levels, takes CII into account as part of its preparedness, response, and recovery phases since the consequences of a CII disruption can be severe. Therefore, national crisis management needs to prepare for the disruption of the CII.

Prevention of CII disruption and proper incident management is a primary task of the CII operator. Although there are many ways to try to prevent disruptive events from happening, there is no way that prevention can eliminate all risks related to the CII. Therefore, national crisis management also needs to plan for dealing with the impact of CII disruptions. Cross-sector exercises may increase the preparedness of both governmental and CII operators to a large extent. For crisis management organisations, the continuity of some CII services may be crucial to the effectiveness of their operations.

From the above, it should be clear that effective and efficient crisis management requires in-depth knowledge of the CII, its operations and its dependencies. Close cooperation and mutual understanding with the CI and CII operators are required during incident response planning, emergency preparedness (e.g. joint training and cross-CII exercises), crisis response and restoration A coordinating CIIP body, such as an nCSIRT, might streamline these efforts (see also the section on Strategic incident response).

Good practices

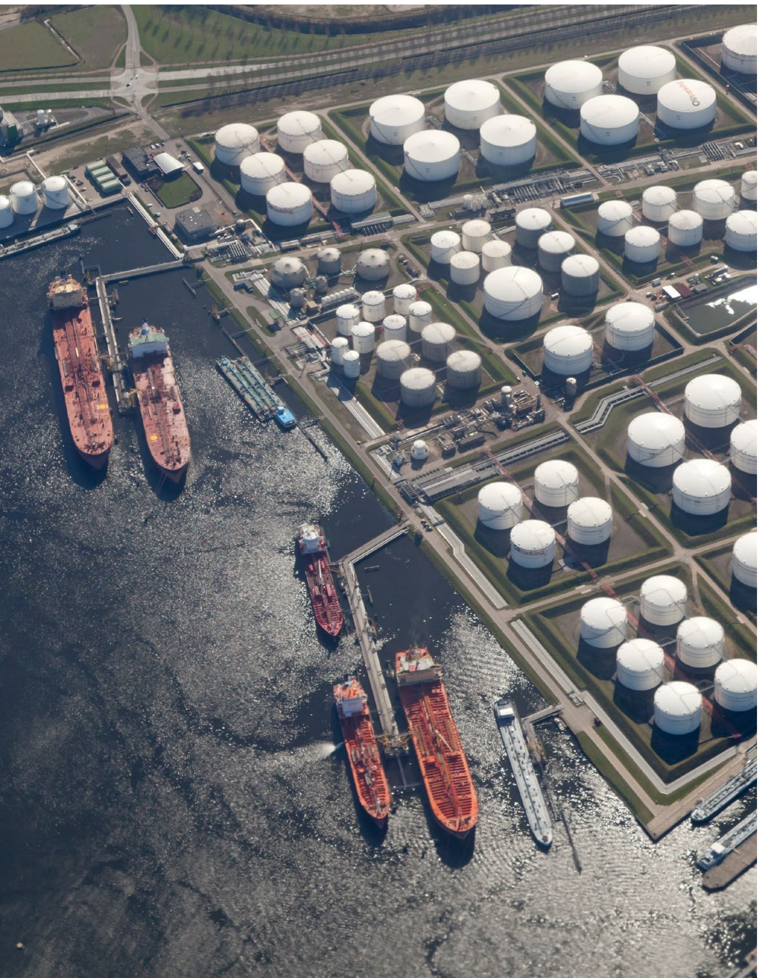
For effective decision-making, crisis management coordination at a national level needs to take into account the scope of consequences of disruptions to an element of CII for a given area, including its cascading effects. Help for national crisis management decision-making can be obtained from CIIP experts who understand threats to CI and CII, their critical dependencies, their disruption and restoration characteristics, and potential cascading effects. The responsibilities for crisis management on the one hand and CIIP on the other can be assigned to different parts of the same public or private organisation. If this is the case, close coordination is essential. For instance, close coordination with the CIIP entities can shorten the recovery and restoration process in the wake of a crisis. However, close coordination does not ensure that there is a common understanding.

Dutch ICT Response Board (IRB)

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 elements of CII that could affect or actively affects national security, the Council of Ministers takes decisions based on advice provided by both the NCSC and the IRB. After a thorough analysis of the situation at hand and the available response options, the IRB provides tactical level advice to the strategic and political level decision-makers. They may also provide 'horizontal' advice to the other private IRB organisations, such as the CII operators. Membership of the IRB currently comprises several CI sectors (drinking water, energy, financial, government, and telecom (including ISP)), the Dutch CERT community, as well as academic and other experts (IRB).

Create a strategic digital crisis plan

A digital crisis often affects a large number of staff members both inside and outside an organisation. It is therefore important that a plan exists for how different entities involved interact with each other, so that CII incidents or crises can be handled in a smooth and timely manner. Due to the speed of events in the digital arena, it is important to have a crisis plan in place that identifies possible events, relevant stakeholders, decision-making processes, and possible actions that need to be taken.



Dutch National Digital Crisisplan

The Dutch National Digital Crisisplan (NCP-Digital) is a guideline that allows for a quick overview of the main existing arrangements concerning digital crisis management at the national level. It covers incidents in network and information systems with considerable societal consequences. The plan broadly describes the crisis management approach at the national level. It also states how the cooperation and connections with involved public and private partners and networks are arranged at the international and regional level. So, the NCP-Digital provides a framework and an overarching plan for all the individual – more operationally established – crisis plans and scenarios of the involved actors and organisations. Therefore, it explicitly does not replace the existing plans of individual organisations or the existing arrangements between organisations. However, when relevant, these individual plans do need to align with the NCP-Digital.

NCP-Digital includes a roadmap that assists in finding the answers to the following three questions:

1. *What are the most important potential (in) direct consequences and effects of the incident/crisis?*
2. *What mitigating measures are necessary to prevent, mitigate or control these consequences and effects?*
3. *What parties are involved or need to be involved in an adequate crisis management approach?*

Exercises

What constitutes exercises in CIIP?

Organising cyber exercises can help nations prepare for incident response and crisis management. Exercises can be used to test the cyber incident response plans and procedures. They can be designed for different target groups, e.g. on the operational, tactical or strategic level and different geographical levels, e.g. on a regional, national or international level. Running exercises can be a good way for operational incident response units and decision-makers to practice their skills and procedures. In addition, they encourage collaboration between different organisations, experts and nations.

Exercises at the national level can be used to build networks and stimulate collaboration between stakeholders, including the national CSIRT, representatives from relevant CI sectors, Information and Communication Technology (ICT) experts and policymakers. Exercises can also be used to collaboratively explore the right procedures to respond to a large-scale cyber incident.

As globalisation and digitalisation increases, so does the importance of international exercises (e.g. by the International Watch and Warning Network or IWWN) and cross-border exercises. Internationally organised exercises may support the development of internationally coordinated procedures, stimulate cross-border cooperation, and establish an international network of experts and incident response organisations.

Features

To increase the effectiveness of exercises, policymakers may consider the following actions:

- Stimulating exercises at different levels. Exercises can be used to test the cyber incident response plans and procedures at the national or international level. An adequate level of preparedness to manage large scale cyber incidents requires well-known procedures and networks of organisations that can collaborate closely even under high pressure. Simulation exercises at the strategic, tactical or operational level can help enhance the level of preparedness for a specific type of incident. They can lead to a better understanding of the procedures, roles and responsibilities of all organisations involved.
- Encouraging participation from both the government and CI operators. Responding to large scale cyber incidents affecting the CII requires action from a variety of organisations, both government organisations and CII operators. CII operators can be asked to participate in (national) cyber exercises to involve them in the implementation of CIIP policies or to test their performance on CIIP capacities. By performing joint exercises, participants learn (often the hard way) about each other's roles, responsibilities, decision-making cycles, capabilities, abilities, and terminology. Last but not least, 'getting to know each other' is an often-mentioned key factor in diminishing friction between groups and facilitating cooperation.
- Identifying and following up on lessons learned. For exercises that are used to optimise incident response procedures, a crucial part of each exercise is to assess the course of the scenario and actions taken, and identify lessons learned. Cyber exercises may cover important elements of responding to incidents, such as technical actions, incident response procedures, and decision-making processes. Assessing the actions taken and decisions made by different participants during the exercise may lead to a number of lessons learned, for example, on the effectiveness of procedures for contingency planning and crisis management. It is important to follow up on these lessons learned and implement (wherever feasible) the findings and lessons learned into response policies and procedures.

Good practices

Design exercises at different levels with government organisations and CI operators

Joint public-private regional, national and cross-border exercises create the right level of preparedness for large scale cyber incidents with key stakeholders, such as cybersecurity incidents response teams (both within government and CII operators), crisis management organisations, and decision-makers. Exercises can be held at the operational, tactical, and strategic level or span multiple levels. Increasingly, nations involve CII operators as key partners in cybersecurity exercises. Joint, cross-sector exercises increase the preparedness of both government and CII operators. Be aware that organising exercises with a broad set of participants require a sharp definition of the exercise objectives for each of the target groups that participate.

A handbook for organising tabletop exercises

The Czech organisation Nukib organises different types of exercises throughout the year, ranging from local or sector-based exercises to exercises with international partners. In support of organising cyber exercises, Nukib wrote a handbook on how to develop a cybersecurity tabletop exercise*. The handbook is intended for those responsible for protecting and operating CII, important information systems, or any type of high-value assets. The handbook describes how cyber exercises may be designed to effectively educate and train different target groups, ranging from technical personnel to executives and political leaders.*

Participating in international exercises

Cyber incidents do not stop at international borders. Therefore, international collaboration is an important element in the management of large-scale cyber incidents. Participation in international exercises can help your nation to test and align internationally coordinated response procedures. It will also help you build an international network of response organisations and experts.

Annual cyber defence exercises between ASEAN members

Since 2013, Japan has organised cyber exercises in collaboration with international partners. The exercise *consists of a remote exercise and a tabletop exercise. The remote exercise aims to establish communication procedures between the governments of the ASEAN member states and Japan in the event of a cyberattack, whereas the tabletop exercise – conducted since 2016 – exists to discuss national policies and measures that can be implemented in the event of a cyberattack. The scenarios used for the exercises are agreed upon by Japan and the ASEAN member states.*

In June 2020, Japan organised a cyber defence exercise (co-hosted by Vietnam) with 10 ASEAN countries participating. The exercise scenario contained a cyberattack on CI systems, such as power grids and waterworks and required sharing information both within the Japanese government and with international partners.

Cyber Europe

Since 2010, the EU has organised cross-border cyber exercises to protect EU infrastructures against coordinated cyberattacks. The bi-annual Cyber Europe *exercises bring together cybersecurity experts, CII operators and policymakers from across Europe. The exercise starts with real-life inspired technical incidents that may build up during the scenario to a crisis at a local, organisational, national, or European level.*

Evaluation and learning from incidents

What constitutes evaluation and learning from incidents?

Organisations analyse and evaluate cyber incidents to learn about the cause and then use that knowledge to improve their protection and response measures. In recent years, some organisations have been sharing the underlying causes of cyber incidents and the lessons learned from those incidents. In addition to these voluntary sharing initiatives, some nations and, for example, the European Union, have developed more formal national and international incident reporting schemes to create more transparency about cyber incidents. These schemes focus on large impact cyber incidents that affect the critical infrastructure and critical information infrastructure. These schemes can be organised both on either a voluntary or a mandatory basis. Based on the restricted detailed incident reports, some nations and organisations provide periodic reports with aggregated data on the number and types of incidents. Sharing incidents and lessons learned on an international basis as well as creating and maintaining expertise networks are important factors in becoming more resilient for upcoming and greater threats.

Features

Victims of cyber incidents are often reluctant to share information on these incidents. A lack of information makes it hard for both government and CI operators to determine if cyber incidents are increasing in frequency and/or impact. Policymakers can stimulate the sharing of information on cyber incidents through a voluntary or mandatory approach. For both approaches, it is important that you share the results of the incident reporting and disseminate the lessons learned with stakeholders while protecting the confidentiality of the information (e.g. by anonymising the victim organisation or the used modes of operation). Approaches for policymakers to incentivise information sharing and learning include the following:

- Establishing regulations on cyber incident reporting. Organisations that are hit by a cyber incident are not always willing to share information on the incident. To stimulate information sharing on cyber incidents, some nations have included incident reporting in their legal framework. For instance, the EU includes incident reporting in their NIS directive and requires operators of critical services to report cyber incidents which significantly impact the continuity of an essential service. The threshold for mandatory incident reporting covers, for example, the number of users affected, the duration of the incident, and the geographical spread of the incident.
- Analysing cyber incident reports and sharing trends in an aggregated form. By collecting cyber incident reports and analysing patterns in, for instance, the number of cyber incidents, their impact and their cause, trends can be identified and shared. Government organisations may use the analysis of cyber incident reports to identify trends in the number or cause of attacks and use that information to assess the need for additional guidelines or policy measures. CI operators may use the analysis of cyber incident reports as a starting point for assessing the adequacy of their measures.
- Stimulating information sharing on detailed incident analyses. In addition to sharing information on trends, organisations can be stimulated to share lessons learned from more detailed incident analyses. These detailed analyses are sometimes performed by the victim of the incident or by government agencies that took part in the incident response. The number of details shared varies per incident. Sometimes, when incidents have already received a lot of media attention, organisations that are affected are more willing to share details about the attack and lessons learned (if necessary, this can be done under the TLP sharing system). In other cases, details of the attack are anonymised at the request of the victim organisation or to prevent the spread of sensitive information on the methods used.

Good practices

Sharing trends in cyber incidents

Sharing trends on the frequency and impact of cyber incidents on, for example, a national or sectoral basis, helps organisations to get an overview of the current level of threat and trends. Both government organisations and CI operators may use the analysis of cyber incident reports as a starting point for assessing the adequacy of their security measures.

> **ENISA**
>
> *ENISA shares information on the statistics of incidents in the telecommunications sector. In the EU, telecom operators and trust service providers have to notify their national regulators about security incidents that have a significant impact. At the end of every year, nations send summary reports about these incidents to ENISA. ENISA aggregates, anonymises, and analyses this data and shares the results on their website.*

Creating a deeper understanding of the root causes

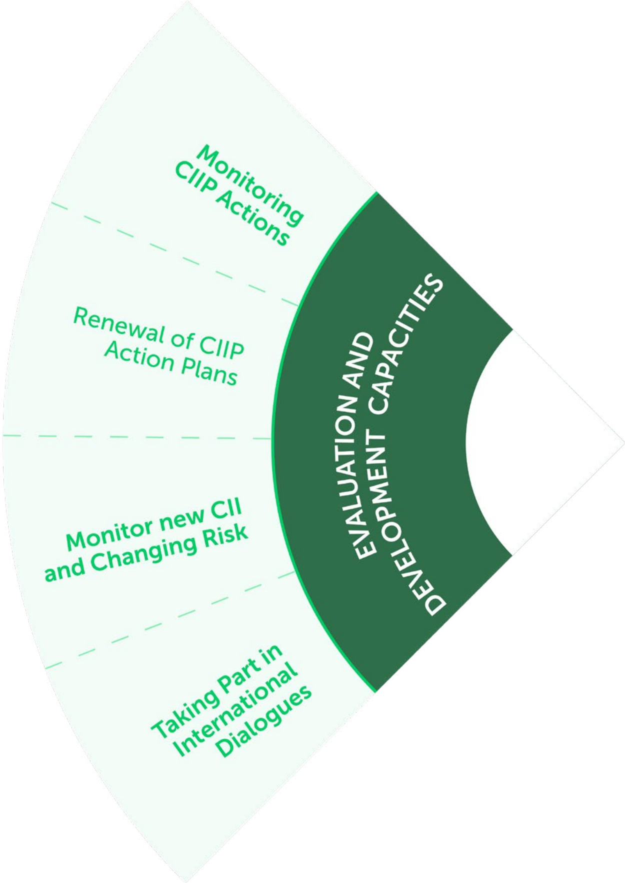
Technological complexity can make it difficult to imagine what can go wrong within information infrastructures and what combinations of events can trigger disruptions. Analysing incidents and their impacts can help stakeholders understand how disruptions are triggered and prevent future CII disruptions. A way to stimulate information sharing of more detailed analyses is by suggesting anonymised sharing as this might lower the barrier for those involved. In that case, incidents can be anonymised and shared as a more generally applicable case study on what might go wrong in a critical infrastructure. When a cyber incident has already received a lot of media attention, victim organisations are more inclined to share details of the incident and lessons learned.

Interesting examples are anonymized case studies on incidents with Industrial Control Systems and the impact and response of the NotPetya incident with Maersk in 2017.

Theme

Evaluation and Development Capacities

Nations should regularly reassess risk factors and possible changes in Critical National Information Infrastructure (CNII) vulnerabilities. The evaluation of Critical Information Infrastructure Protection (CIIP) policies and the review of the risk landscape (and the corresponding changes in CII vulnerabilities) can be used to develop a roadmap or action plan that covers the necessary steps to keep CIIP at the desired level. Although these reassessments can be time-consuming, regular evaluation and updating of a CIIP plan ultimately ensure the adequate functioning of a nation's CIIP.


Monitoring CIIP Actions
Renewal of CIIP Action Plans
Monitor new CII and Changing Risk
Taking Part in International Dialogues
EVALUATION AND DEVELOPMENT CAPACITIES

Monitoring CIIP actions and CIIP action plans renewal

ⓘ The 'monitoring CIIP actions' capacity and the 'CIIP actions plans renewal' capacity are closely intertwined and are therefore combined in this chapter.

What constitutes monitoring of CIIP actions?

Sharing trends on the frequency and impact of cyber incidents on, for example, a national or sectoral basis, helps organisations to get an overview of the current level of threat and trends. Both government organisations and CI operators may use the analysis of cyber incident reports as a starting point for assessing the adequacy of their security measures.

CIIP policies can include a broad range of actions (e.g. regulations, stakeholder management, information sharing, and awareness campaigns). Keeping track of the implementation of these actions and their impact allows for a continuous CIIP improvement cycle. The continuous updating of actions will help you to create the most secure, efficient, and effective CIIP possible (see also the capacity on planning).

You can track progress on CIIP actions through progress assessment, (scenario-based) exercises, and auditing. Progress assessment requires clearly defined policy intentions and objectives. Exercises (either within a single organisation or together with sector partners) allow for evaluation of the actual actions taken by organisations in the event of a disruption of the CII and are a good way to check if these actions result in the desired outcomes. Doing these exercises on a regular basis will help to develop experience with the execution of these actions and allows for a deeper understanding of the functionality and impact of certain actions. Cybersecurity auditing can be used to check if organisations have the required action plans in place and can deliver on them.

Cybersecurity auditing can be done by an auditing agency, a government body, or another party, depending on which aspect of a CIIP plan is being audited (see the capacity on auditing for more information).

What constitutes renewal of CIIP action plans?

Over time, any action plan requires updating. The government body is chiefly responsible for the action plan and should determine whether a plan is still adequate or if refinement is necessary. Additionally, external organisations can signal that an evaluation is necessary (e.g. the EU, through its NIS Directive on cybersecurity). If so, the CIIP-related objectives, mission and vision statements, responsibilities, ambitions, and planning should be reviewed. In any case, your country should have some monitoring activities in place to identify if plans need to be renewed. Also, be mindful of the effort required in bringing involved parties together over a longer period of time to discuss the pre-determined objectives and missions. Keep in mind that it can often be a challenge to reach shared goals and understanding, because over time, the goals of involved parties can change, and this, in turn, can affect the CIIP plans in place.

Features

Once a CIIP strategy or policy has been developed, you should keep monitoring its implementation and effectiveness. Your policies need to have clearly defined intentions and objectives, so you can effectively monitor the implementation of CIIP actions. The CIIP activities should be defined in a Specific, Measurable, Achievable, Realistic and Timely (SMART) manner. Even without SMART defined objectives, it is still wise to monitor the progress that is made towards the implementation of CIIP policies and action plans.

Continuous monitoring of the CIIP activities' implementation enables you to make adjustments in a timely manner. It also allows you to take heed of lessons learned, observe improvements in the CIIP, and notify others when a renewal of plans is necessary. Finally, continuous monitoring makes it possible for the stakeholders responsible for CIIP to swiftly improve on elements of the CIIP action plan that are outdated. Apart from keeping track of your nation's CIIP actions and planning, it is also essential to keep up to date with the constantly evolving threat landscape. A cycle of continuous CIIP improvement will help you keep a close eye on this changing landscape.

Good practices

Define SMART objectives

Define Specific, Measurable, Achievable, Realistic and Timely (SMART) objectives for monitoring CIIP actions. SMART objectives allow a national parliament to perform their oversight role and the responsible ministry (or ministries) or agencies to monitor the progress of CIIP action lines.

The Canada-United States Infrastructure Protection Framework for Cooperation

The Joint CIP Framework of Canada and the United States is an initiative that aims to align strategic objectives for both governments, based on the 'Smart Border Declaration and Action Plan'. Its objectives are based on compatible protective and response strategies and programmes for shared critical infrastructure. A good example of such a programme is the electric grid security and resilience strategy, one of its aims being continuous development and learning.

Organise exercises to learn and evaluate the implementation of CIIP actions

Organising exercises with others is a great way to learn (see the capacity on exercises for more information). Often risks and vulnerabilities that exist at one organisation can potentially harm others. That is why it is so important to share threat information and lessons learned from these incidents. A good next step would be putting these lessons learned into exercises and discussing with a broad range of participants each other's evaluation and monitoring results.

Pan European CIIP exercises

Since 2010, the first Pan European exercise was held on Critical Information Infrastructure Protection. These exercises help the exchange of information on how member states of the European Union handle ICT incidents at a national level.

Embed monitoring activities in existing security practices

A good way to spot if a security strategy or plan is up for renewal, is by adding monitoring activities to the day-to-day security practices. This allows for a proactive method to gather information on any element of a strategy in need of change. It will also offer you plenty of time to organise any changes in CIIP actions. Furthermore, it can be a good way to gather relevant information which you can share with other organisations and policymakers.

ENISA's Evaluation Framework for cybersecurity strategies

ENISA has worked on an evaluation framework for national cybersecurity strategies that can aid policy experts and governments with the design, implementation and evaluation of policies. It focuses on key performance indicators (see good practices on SMART objectives) and the logic of recurring components of a national cybersecurity strategy. It also offers an evaluation model that can be used for CIIP action plans.

Monitoring for new elements of CII and changing risks

What constitutes monitoring for new elements of CII and changing risks?

Monitoring for new elements of Critical Information Infrastructure (CII) and changing risks is about keeping a close eye on the CII(P) developments. The CIIP landscape tends to evolve rapidly. Sophisticated new threats constantly target CIIs. Also, dependencies shift due to unforeseen uptakes or failure of (apparent) traditional or unimportant information infrastructure technology, causing other information infrastructure services to become critical to a nation. The overview of identified CII elements within your nation should be reviewed and (re-)assessed to keep on par with this dynamic environment. The same holds true for the risks related to your CII (see the capacities on Identifying CII and National Risk Assessment on methods for both).

Features

The threat landscape changes constantly. New threats arise, and the impact of threats can increase (or decrease) due to new actors, new technology, or a change in the political climate. The adoption of new technologies in CII can create new vulnerabilities through which the CII can be disrupted. This is why keeping the CII safe and secure is not a one-time activity but requires continuous monitoring of new elements of CII and risks. Each actor in a cybersecurity supply chain of the CII should be aware of this changing landscape and actively monitor threats and risks. Furthermore, some threats and vulnerabilities can impact multiple actors. This is why it is important to create a functionality at a national level that keeps up with new threats and vulnerabilities. Such a functionality can advocate the importance of continually monitoring threats and vulnerabilities as well as the necessity for actors to analyse the impact of specific risks on their own organisation. Also, this functionality should assess both the short- and long-term CII security and resilience implications of adopting new technologies in the CII. Furthermore, these insights should be shared with CII policymakers and national CII operators.

Monitoring for new elements of CII and risks is an important practice for organisations. It requires an established process that identifies threats and vulnerabilities and translates these into risks. At the very least, such a process should encompass the following actions:

- identifying relevant information sources (open and (semi-)closed data)
- processing the gathered intelligence.
- assessing the impact of threats to a specific CII or organisation.
- sharing relevant and accurate information on threat impacts with relevant parties

Sharing information on identified vulnerabilities or risks with other stakeholders benefits CII, as it will create more awareness among stakeholders on common risks.

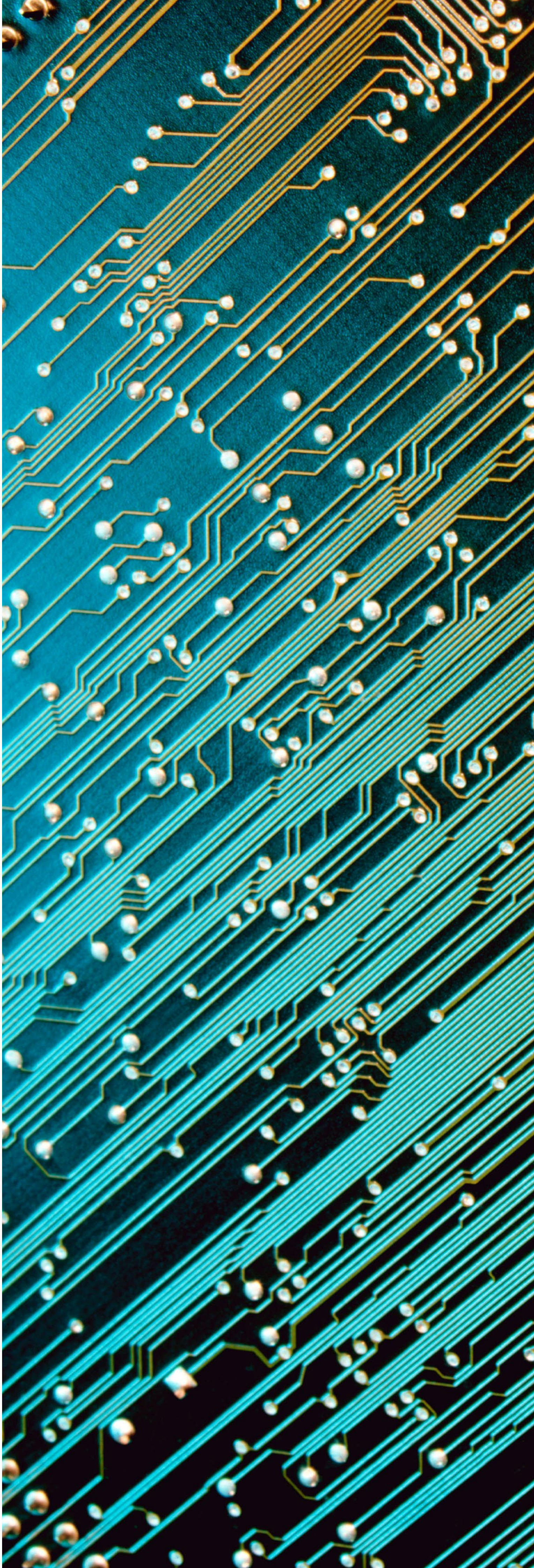
Good practices

Perform and support regular horizon scanning

Setting up regular horizon scanning is a good way to identify new elements of CII and potential risks. At its core, horizon scanning is a systematic process of detecting early signs of potentially important developments based on early signals, trends, wild cards, problems, risks, or threats. It is about determining what is constant, what may change, and what is constantly changing. Ultimately, the goal of horizon scanning is to be more aware of and prepared for what is coming. Horizon scanning strengthens CIIP policy as it enables nations to proactively signal and assess developments in technology, so they can assess which new technologies have matured enough to potentially become part of the CII. Horizon scanning will help you grasp the developments that will influence the current and coming state of affairs in CIIP. Each organisation that is connected to the CII can translate these developments into potential risks or opportunities for their organisation. Regular collaborative horizon scanning can help build a relationship between governmental policymakers and relevant national and international stakeholders. This in turn can be a starting point for further cooperation and bring about a shared understanding of the factors that influence the CII and the subsequent need for CIIP. Horizon scanning is particularly insightful when the perspectives of different stakeholders are incorporated. A good practice is to invite key stakeholders that comprise the set of potential CII elements in a nation to perform a horizon scan together. The different perspectives gathered this way can lead to a valuable understanding of dependencies across technologies and organisations.

Horizon scans on emerging technology

Most horizon scans have a broad scope and many exist that investigate threats to and vulnerabilities in cybersecurity as a whole. Often the importance of critical infrastructure and the protection of CII is covered in these scans. For instance, the Information Security Forum *has produced a horizon scan for 2021, in which they analysed technological developments that have the potential to alter the functions on which a society is critically dependent. The opportunities created by new technologies are great. However, they can also give rise to new threats to the CII. For CI, growing digital connectivity can expose it to new threats, like parasitic malware that can infect CII. The* World Economic Forum *undertakes activities that look into emerging technologies and systemic risk for cybersecurity, providing both opportunities and uncovering potential new threats for critical infrastructures. Finally, ENISA has been developing* threat landscapes *on different* threats *and reports on each of these threats. Threats like information leakages, identity theft, physical manipulation, damage, theft and loss, cyberespionage, or data breach. Another report by ENISA focusses on emerging trends in cybersecurity that can produce a threat. It is wise to take these* emerging trends *into account when performing a horizon scan for CIIP.*



Taking part in international dialogues

What constitutes taking part in international dialogues?

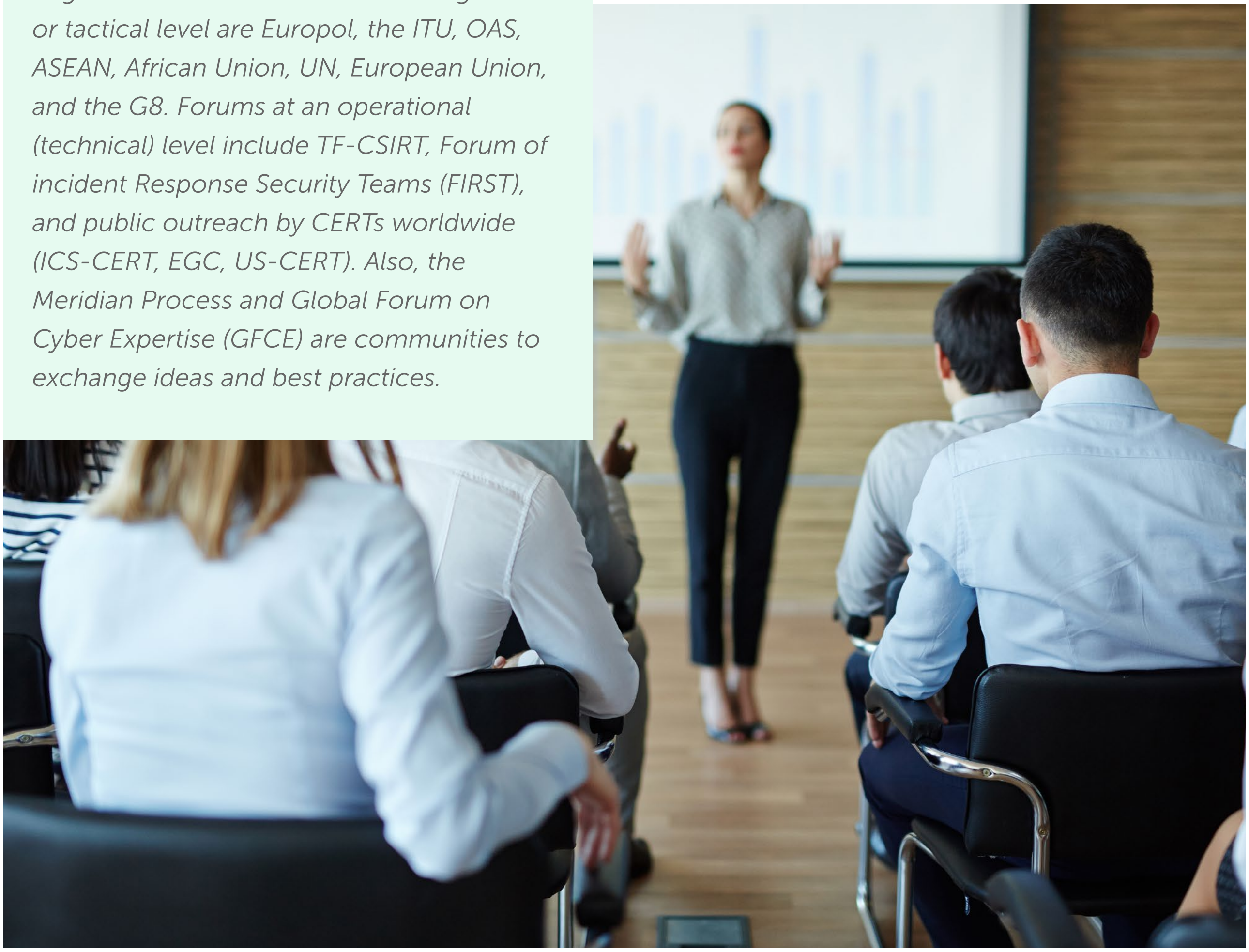
Reaching out to international communities can help nations to keep track of changes in risk and vulnerabilities of their CII and can contribute to international policy developments in the cybersecurity domain. Regardless of national differences in CIIP, your nation can learn from others, ask, and receive help, and discuss different policy options. Furthermore, taking part in international dialogues provides you with an opportunity to participate and shape decision making processes on an international level. There are many international communities and organisations you can reach out to.

Features of taking part in international dialogues

As CIIP is of utmost importance to every single nation, many organisations in different countries take steps to learn as much as possible about changes in risks and vulnerabilities. Setting up international dialogues can be challenging, especially when objectives and goals differ between countries and organisations. However, without taking part in international dialogues, it is hard to integrate necessary information such as best practices, knowledge on vulnerabilities or lessons learned from incidents, into your own CIIP action plans. Combining efforts and sharing information on risks and vulnerabilities also enables you to make your own CIIP efforts more efficient and effective.

International organisations to get in touch with

Organisations to consider at a strategic or tactical level are Europol, the ITU, OAS, ASEAN, African Union, UN, European Union, and the G8. Forums at an operational (technical) level include TF-CSIRT, Forum of incident Response Security Teams (FIRST), and public outreach by CERTs worldwide (ICS-CERT, EGC, US-CERT). Also, the Meridian Process and Global Forum on Cyber Expertise (GFCE) are communities to exchange ideas and best practices.



Good practices

Engaging with international communities on CIIP

A good practice constitutes taking part in international dialogue via community platforms that were designed to promote dialogue on matters concerning CIIP. In the boxes on this page we describe two of these communities.

Community: the Meridian Process

The The Meridian Process aims to exchange ideas and initiate actions for the cooperation of governmental bodies on 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. It also seeks to create a community of senior government policymakers in CIIP by fostering ongoing collaboration.

Community: Global Forum on Cyber Expertise

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

The buddy system

You can benefit from reaching out to and coordinating with nations that have different CIIP policies and capabilities. Nations with well-developed CIIP policies and capabilities often choose to pair up with nations that have just started on the path of CIIP to support them in their development – they become 'buddies'. Usually, these initiatives are not specifically focused on CIIP, nor do they tend to rely on a pre-set, coordinated approach. They grow organically instead.

You might want to consider a close bilateral or multi-lateral buddying relationship, mostly because your nation (if it has less developed policies and activities) can be provided with resources and knowledge, thereby fast-tracking the increase of CIIP. Through the buddy system, nations can learn about valuable organisational methods or process-wise approaches and learn about pitfalls to avoid.

Offering to be a guide nation (a nation with more developed CIIP policies) has its own benefits. The starting nation may ask CIIP questions which the guide nation has not yet considered and thereby help increase its own CIIP. Moreover, a strengthened CIIP in the buddy nation creates a safer CII node in cyberspace.

Before selecting a buddy nation, it is worth considering whether there is a match between the nations. You will have to bridge any differences in legal and other governance structures, language, etc. When seeking a potential buddy, make sure that the guide nation has undertaken all necessary coordination and authorisation with the relevant ministries and agencies in their nation. We recommend that you start with informal buddying discussions to establish compatibility and mutual interests, as a preliminary move before deciding to develop a more formal buddying relationship.

Further reading

Strategy and policy

National risk assessments

- OECD, National Risk Assessments: A Cross Country Perspective, 2018, OECD. Online: https://doi.org/10.1787/9789264287532-en.

Governance

- ENISA, CIIP Governance in the European Union Member States (Annex), 2016, ENISA. Online: Stocktaking, Analysis and Recommendations on the protection of CIIs (europa.eu)

CI Identification approach

- CIPedia©: a common international reference point for CIP and CIIP concepts and definitions. Online: http://www.cipedia.eu
- 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). Online: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008L0114
- Klaver, M., Luiijf, E. & A. Nieuwenhuijs, Good Practices Manual for CIP Policies for policymakers in Europe, TNO, 2011. Online: http://www.tno.nl/recipereport
- Mattioli, R., Levy-Bencheton, C. Methodologies for the identification of Critical Information Infrastructure assets and services, ENISA, February 2015. Online: https://www.enisa.europa.eu/publications/methodologies-for-the-identificationof-ciis/at_download/fullReport
- Qatar Ministry of Information and Communications Technology, Qatar National Cyber Security Strategy, May 2014. Online: http://www.motc.gov.qa/sites/default/files/national_cyber_security_strategy.pdf

CII identification approach

- Brunner, E.M. and Sauer, M. International CIIP Handbook 2008/2009: An Inventory of 25 national and 7 international Critical Infrastructure Protection Policies, ETH, Zürich, Switzerland, 2009. Online: http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-08-09.pdf
- Fekete, A. (2011). Common criteria for the assessment of critical infrastructures. International Journal of Disaster Risk Science, 2(1), 15-24. Online: https://link.springer.com/article/10.1007/s13753-011-0002-y
- 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), First International Conference on IEEE (pp. 1-3).
- Mattioli, R., & Levy-Bencheton, C. (2014). Methodologies for the identification of Critical Information Infrastructure assets and services. ENISA Report–2014–43. Online: https://www.enisa.europa.eu/publications/methodologies-for-theidentification-of-ciis/at_download/fullReport
- Theoharidou, M., Kotzanikolaou, P., & Gritzalis, D. (2010). A multi-layer criticality assessment methodology based on interdependencies. Computers & Security, 29(6), 643-658. Online: https://doi.org/10.1016/j.cose.2010.02.003

Protection

Information sharing

- Luiijf, H.A.M., Kernkamp, A. GCCS: Sharing Cyber Security Information, TNO, 2015. Online: http://publications.tno.nl/publication/34616508/oLyfG9/luiijf-2015-sharing.pdf
- Klaver, M., Luiijf, E., & A. Nieuwenhuijs. Good Practices Manual for CIP Policies for policy makers in Europe, TNO, 2011. Online: http://www.tno.nl/recipereport

Auditing

- BSI, Orientation guide to documentation of compliance according to Section 8a (3) BSIG, Version 1.1 of 21/08/2020. Online: BSI - Homepage - Orientation guide to documentation of compliance according to Section 8a (3) BSIG (bund.de)
- CSA, Guidelines for auditing critical information infrastructure, 2020. Online: Guidelines for Auditing Critical Information Infrastructure (csa.gov.sg)
- ENISA, Guidelines on assessing DSP and OES compliance to the NISD security requirements; Information Security Audit and Self – Assessment/ Management Frameworks, 2018. Online: Guidelines on assessing DSP security and OES compliance with the NISD security requirements — ENISA (europa.eu)

CVD

- NCSC, Coordinated Vulnerability Disclosure: the Guideline, 2018. Online: Coordinated Vulnerability Disclosure: the Guideline | Publication | National Cyber Security Centre (ncsc.nl)

Incident management

- Chapter 8 of RECIPE: Klaver, M., Luiijf, E., Nieuwenhuijs, A. Good Practices Manual for CIP Policies for policy makers in Europe, TNO, 2011. Online: http://www.tno.nl/recipereport
- ENISA, Strategies for Incident Response and Cyber Crisis Cooperation, 2016. Online: Strategies for incident response and cyber crisis cooperation — ENISA (europa.eu)
- 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.

Evaluation and development capacities

- Cuhls, K., Van der Giessen, A., & Toivanen, H. (2015). Models of horizon scanning. How to integrate Horizon scanning into European research and innovation policies. Brussels: Report to the European Commission (end report of the European Commission, A 6, Study on Horizon Scanning).
- Curry. A & Hodgson, A. (2018). Seeing in multiple horizons: connecting futures to strategy. Journal of Futures Studies 13(1). Online: https://www.researchgate.net/publication/253444667_Seeing_in_Multiple_Horizons_Connecting_Futures_to_Strategy
- GFCE-MERIDIAN, GFCE-MERIDIAN Good Practice Guide on Critical Informatiopolicymakersure Protection for governmental policy-makers, 2017, GFCE. Online: https://thegfce.org/initiatives/critical-information-infrastructure-protection-initiative/
- Luiijf, H.A.M., Kernkamp, A., GCCS: Sharing Cyber Security Information, TNO, 2015. Online: http://publications.tno.nl/publication/34616508/oLyfG9/luiijf-2015-sharing.pdf
- OECD, Netherlands 2016: Foundations for the Future, Reviews of National Policies for Education, 2016, OECD. Online: https://doi.org/10.1787/9789264257658-en

CIIP General

- NCTV, Dutch National Risk Assessment, 2019. Online: Dutch National Risk Assessment | Publication | National Coordinator for Security and Counterterrorism (nctv.nl)
- GCSCC, Cybersecurity Capacity Maturity Model for Nations (CMM), 2016. Online: cmmrevisededition090220171pdf (ox.ac.uk)
- 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. Online: http://www.oecd.org/sti/40825404.pdf
- Saalman, L., Integrating Cybersecurity and Critical Infrastructure, SIPRI, 2018. Online: Integrating Cybersecurity and Critical Infrastructure: National, Regional and International Approaches | SIPRI

Glossary

Capacity

In broad terms, capacity building in the cyber domain is aimed at building functioning and accountable institutions in order to respond effectively to cybercrime and to enhance countries' cyber resilience. In the CIIP domain, a capacity refers to a functioning method, tool or institution to ensure the protection of Critical Information Infrastructures (CII).

CERT

Computer Emergency Response Team. It is a registered mark licensed to Carnegie Mellon University. CSIRTs have to contact the Carnegie Mellon University CERT Division to use the CERT® mark.

CSIRT Constituency

Who the CSIRT functions are aimed at, the "clients" of the CSIRT.

Critical National (Information) Infrastructure

When talking about critical (information) infrastructure in the context of cybersecurity, the terms CI and CII can refer to a variety of levels (e.g. sectoral, national, regional, and international). Critical National (Information) Infrastructure (CN[I]I) refers specifically to the critical infrastructure of a nation.

Critical infrastructure (CI)

System and assets, whether physical or virtual, so vital to society that the incapacity or destruction of such systems and assets would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters.

Critical infrastructure Protection (CIP)

All activities aimed at ensuring the functionality, continuity, and integrity of critical infrastructure (CI) to deter, mitigate, and neutralise a threat, risk or vulnerability, or minimise the impact of an incident.

Critical information infrastructure (CII)

Those interconnected information and communication infrastructures which are essential for the maintenance of vital societal functions (e.g., health, safety, security, economic, or social well-being of people) – of which the disruption or destruction would have serious consequences.

Critical information infrastructure protection (CIIP)

All activities aimed at ensuring the functionality, continuity, and integrity of critical information infrastructure (CII) to deter, mitigate, and neutralise a threat, risk or vulnerability, or minimise the impact of an incident.

CSIRT

Computer Security Incident Response Team. A CSIRT supports a particular target audience (i.e. the CSIRT's constituency) in preventing as well as responding to computer security incidents. There are different types of CSIRTs, often defined by the type of constituency they serve.

Cybersecurity

Cybersecurity is the combination of people, policies, processes, and technologies employed by an enterprise to protect its cyber assets. Cybersecurity is optimised to levels that business leaders define, balancing the resources required with usability/manageability and the amount of risk offset. Subsets of cybersecurity include IT security, IoT security, information security, and OT security.

Indicators of compromise (IoCs)

An Indicator of Compromise (IoC) is information that can help with identifying specific malicious behaviour on a system or within a network.

Information Sharing and Analysis Centres (ISACs)

Information Sharing and Analysis Centers (ISACs) are non-profit organizations that provide a central resource for gathering information on cyber threats (in many cases to critical infrastructure).

Information technology (IT)

'IT' is the common term for the entire spectrum of technologies for information processing, including software, hardware, communications technologies, and related services. In general, IT does not include embedded technologies that do not generate data for enterprise use.

IT incident management

IT incident management is the process followed by an IT support organisation to restore its IT service to normal as quickly as possible. Organisations use IT incident management processes after a disruption to minimise its impact on business operations and meet service-level agreements.

ISO (International Organization for Standardization)

A voluntary, non-treaty organisation established in 1949, as a technical agency of the United Nations, to promote international standardisation in a broad range of industries. ISO's Open Systems Interconnection (OSI) Reference Model establishes guidelines for network architectures.

Operational Technology (OT)

Operational technology (OT) is hardware and software that detects or causes a change through the direct monitoring or control of industrial equipment, assets, processes, and events.

Supply chain

Supply chain is a group of functions and processes focused on optimising the flow of products, services, and related information from sources of supply to customers or points of demand. It stretches across multiple tiers in the supplier network to customers and to customers of those customers. It includes supply chain planning, sourcing and procurement, manufacturing, distribution, transportation, and services within a company and its ecosystem of partners.