# GFCE Global Good Practices

## Critical Information Infrastructure Protection (CIIP)

GFCE
Global Forum on Cyber Expertise

# Preface

The unprecedented uptake of ICT worldwide leads to a growing dependency of economic sectors, public institutions and societies as a whole. Multiple recent outbreaks of hostage-taking software (ransomware) have shown the criticality of ICT for sectors such as transport and healthcare. Attention for the security and continuity of critical ICT is crucial to the well-being of modern societies.
Some elements of ICT have become critical for national security. These elements form the Critical Information Infrastructure (CII) of a nation. Protection of CII (CIIP) has obtained worldwide attention which has, for example, resulted in a OECD high-level policy framework (2008) containing recommendations on the Protection of Critical Information Infrastructure.

This Global Good Practice document on CIIP builds forth on these efforts by providing policy-makers and political leaders with essential but concise knowledge. This knowledge helps policy-makers in defining sustainable and efficient efforts to protect national Critical Information Infrastructure (CII). The benefits and risk of the gradual and unstoppable uptake of Information and Communications Technologies (ICT) are experienced by all nations. Effective national policy on CIIP requires regular updates and alignment with international developments. This document provides a set of good practices to develop an effective national CIIP policy (from identification of CII, to development of CIIP and handling of the inevitable dynamics).

The process of establishing a CIIP policy and living up to it in the long term should preferably be performed on basis of evidences and experiences from others. Resources and guiding information are often scarce. The good practices in this document are based on previous research, the GFCE-Meridian CIIP meeting in Mexico (2016), literature and experience elicitation from interviews.

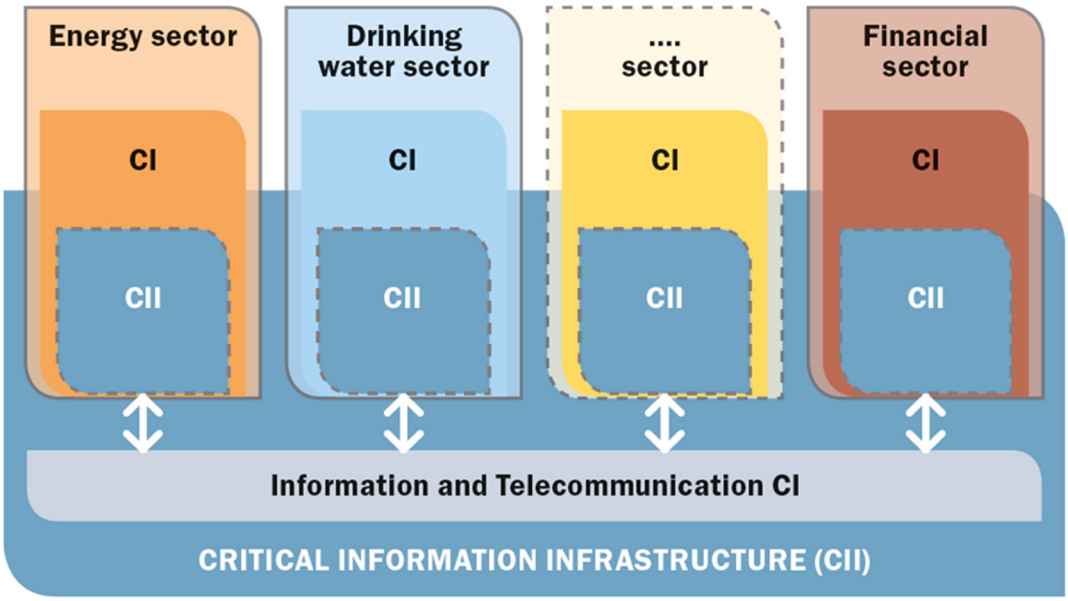
Preface ..... 3
1. Introduction ..... 5
What is Critical Information Infrastructure Protection? ..... 5
Why should one adopt a CIIP policy? ..... 6
Basic steps to establish and implement a CIIP policy ..... 6
2. Good practices ..... 7
Make CIIP a national security priority ..... 7
Identify CII ..... 7
Develop CIIP ..... 9
Handle CIIP dynamics ..... 10
3. Key challenges ..... 13
Key challenge 1: Aligning a CIIP policy with a national risk profile and/or CIP policy ..... 13
Key challenge 2: Separating what is critical from what is important ..... 13
Key challenge 3: Getting many heterogenous stakeholders involved ..... 13
Key challenge 4: Identifying and assessing CII dependencies between (Information) Infrastructures ..... 14
Key challenge 5: Involving organisations related to physical security ..... 14
Key challenge 6: Maintaining attention for CII (frequent reviewing) in absence of public and/or private turmoil ..... 14
Annex: sources on CIIP ..... 15

# 1. Introduction

## What is Critical Information Infrastructure Protection?

Nations critically depend on Critical Infrastructures (CI) such as energy supply, telecommunications, financial systems, drinking water, and governmental services. One definition of Critical Infrastructure (CI) is: "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" (CIPedia). CI is increasingly dependent on information and communication technologies (ICT). Therefore, a disruption of such ICT with critical functions and services may cause a major impact to a nation.

The set of "all interconnected information and communication infrastructures which are essential for the maintenance of vital societal functions, (health, safety, security, economic or social well-being of people), the disruption, or destruction of which would have serious consequence" is called the Critical Information Infrastructure (or CII).[1]




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

Protecting CI and CII is key to national security. Critical Information Infrastructure Protection (CIIP) can be defined as "all activities aimed at ensuring the functionality, continuity and integrity of CII to

[1] Some nations use the notion 'essential information services' for CII. Definition (GFCE-Meridian).

deter, mitigate and neutralise a threat, risk or vulnerability or minimise the impact of an incident" (GFCE-Meridian). CIIP is seemingly straightforward but involves a substantial number of stakeholders such as CII operators, hard- and software vendors, government agencies, ministries and, ultimately the public. These stakeholders are diverse in nature and have conflicting interests.

## Why should one adopt a CIIP policy?

CII forms a 'glue' between and within CI and is becoming interconnected on a global scale. Increasing connectedness may introduce unexpected and unprecedented (cascading) effects. Compromised or interrupted CII can jeopardise national security and stability, economic growth, citizen prosperity, and daily life. The benefits of using CII (increased connectivity, remote monitoring, scalability, reliability, cost-reduction) must exceed the risk of malfunction and disruption of CII. Implementing and following up on adequate CIIP contributes to reduce this risk. Therefore, the need for effective CIIP strategies, policies and activities becomes increasingly important to all.

Despite this need, CIIP is a challenging topic. For a nation to separate what information infrastructure services are critical from what services are 'merely' important is difficult because of the complexity and entanglements of infrastructural systems and the services they provide. Such separation is however quintessential for the development of an effective national security policy and the identification of those critical elements in cyberspace which require specific protection.

## Basic steps to establish and implement a CIIP policy

Working towards a CIIP policy requires to go (at least) through a few basic steps. Having a National Risk Profile (NRP) and a CII embedded within a National Cyber Security Strategy greatly facilitate the process of developing an effective CIIP policy now, and in the future. The basic steps of developing and maintaining a current CIIP policy are:[2]

Step 1. Make CIIP a national priority

Step 2. Identification of Critical Information Infrastructure

Step 3. Development of a Critical Information Infrastructure Protection policy including:

- 3a. a risk-based approach (in comparison to an ad-hoc approach)
- 3b. embedding of CII(P) in national crisis management
- 3c. support for networking and information sharing

Step 4. Monitoring and continuous improvement

[2] For a more elaborate stepwise approach, see the GFCE-Meridian Good Practice Guide on Critical Information Infrastructure Protection.

# 2. Good practices

## Make CIIP a national security priority

CIIP is primarily a matter of national security and should therefore be embedded in the national security strategy.

A good practice is giving CIIP prominence in the national cyber security strategy. Moreover, a high-ranking committee responsible for ICT developments in the nation can promote CIIP issues to be placed on the national security agenda. Changes in the national security landscape must be taken along, also from CII operators that do not reside in the public domain.
An example of a high-ranking committee is the Dutch Cyber Security Council (Dutch Cyber Security Raad (CSR)). The CSR is the national independent advisory body at the strategic level for the Dutch government on Cyber Security and CII. The CSR comprises representatives of public and private organisations and the scientific community.

## Identify CII

### Good practice 1: Understand definitions of CII sectors and services from other nations

CIIP is complex and so is its terminology. Clear terminology is crucial both for understanding a CIIP policy, as well as for clear and coherent national and international dialogues. Definitions from other nations provide helpful inspiration to nations in defining their CIIP approach. Such definitions can be found under 'Critical Information Infrastructure' on the landing page of (CIPedia). If possible, adopt an already existing definition or base the national definition of CIIP on an existing definition.
Every nation that starts to develop insight into their CII will identify critical CII sectors and services that are different than other countries.[3] Regardless of these differences, the goal of CIIP remains the same: the CII of a nation must continuously operate in an undisturbed way as much as possible. Terminology can therefore be similar between nations at an aggregate level, deviating only at the level of differences in critical use of information infrastructure for instance due to different technologies or type of use of ICT services.

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

**Good practice 2: Adopt criteria to systematically identify CII sectors and operators**

Identification of CII can be done on basis of four methodological stepping stones that are also used for the identification of CI in (RECIPE2011[4]). The four stepping stones are: (1) apply sector-specific criteria, (2) assess criticality, (3) assess dependencies, and (4) apply cross-cutting criteria.

The most useful order for these steps depends on the information that is available to national policy-makers (for more elaborate instructions, see GFCE-Meridian reference in the annex).

Cross-cutting criteria (such as the number of casualties or social and economic impact of disruption) underpin the assessment of the criticality of information infrastructure sectors to a nation, both under normal circumstances and during emergencies. Applying cross-cutting criteria helps to identify information infrastructure sectors that are crucial to a nation, both in general or because of their importance to specific CI. Sector specific criteria (such as market share or capacity) are used to specify CII operators and services. Assessment of dependencies is necessary to determine the criticality of specific CII elements and services.

**Good practice 3: Assess dependencies and identify CII services**

CI(I) dependencies can be defined as "the relationship between two products or services in which one product or service is required for the generation of the other product or service" (Luiijf2009). CII sectors and their critical services have dependencies with other CII sectors and their critical services. To identify critical CII services, it is necessary to find critical dependencies that may trigger outages in a cascading way. Note that the set of critical dependencies may significantly change when the daily functioning changes to a non-normal mode of operation (e.g. due to an emergency such as a natural disaster). It is not easy to identify the full set of critical dependencies taking such 'mode of operation' shifts into account. Yet it is crucial to understand them (Klaver, M., Luiijf, H., Nieuwenhuijs, A. et al).

A stepwise process for identifying CII with illustrating cases can also be found in the Best Practices for Critical Information Infrastructure Protection (CIIP) by (Zaballos and Jeun).

[4] The four stepping stones provide a structured approach to the identification process. The steps are inspired by the European Critical Infrastructure Directive (EC2008) which starts bottom-up from within a potentially critical sector.

## Develop CIIP

### Good practice 1: Make us of existing CIIP principles

In 2003, the G8 concluded that nations should protect their CII from damage and secure them against attacks (G8). Effective protection of CII, according to the G8, includes identifying threats, reducing vulnerabilities, minimising damage and recovery time, identifying the cause of disruption, and analysis by experts and or investigation by law enforcement. Effective CIIP also requires communication, coordination, and cooperation nationally and internationally among all stakeholders. In this way, the security of information and applicable law concerning mutual legal assistance and privacy protection are taken into regard. To further these goals, the G8 adopted and promoted eleven principles for CIIP. These principles have been adopted by the OECD (OECD).

### Good practice 2: Involve CII expertise as support function to national crisis management

For effective crisis decision-making, national crisis management coordination needs to consider the consequences of CII disruption, including possible cascading effects. National crisis management decision-making can be strengthened and made effective by involving CII experts who deeply understand the threats to CI and the CII, their critical dependencies, their disruption and restoration characteristics, and potential cascading effects. The responsibilities for national crisis management and CIIP may be assigned to different (parts of) public and/or private organisations. Therefore, bridging national crisis management and CIIP is essential for effective response to (potential) CII disruptions (see (RECIPE) pages 77-82).

### Good practice 3: Joint public-private crisis management exercises involving CII sectors/operators

Without a clear framework and previous experience in addressing cyber security incidents, a straightforward incident involving CII may evolve into a major crisis. Public and private CII operators should therefore perform joint crisis exercises. Exercises (stress)-test the performance of CIIP capacities and reveal unknown and unexpected consequences and dependencies.

The mutual effort parties invest in performing exercises can kick-start or strengthen relationships (insight in each other's roles, procedures, effectiveness, decision making cycles and failures). This strengthens CII protection in the short and long run by creating trust, and engages CI/CII operators for potential future implementation of national CIIP policies.[5]

[5] For more on this good practice, see "The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers", pages 40-41.

**Good practice 4: Start a coordinating body for CIIP**

CIIP efforts should be supported by a coordinating public body. One must carefully think about where such a body is embedded and what its mandate is. A body (or set of bodies) can operate at the strategic or tactical level, and provide guidance to programmes and taskforces at the technical/operational level (see: chapter 4 in (Klimburg2012)). A combination of coordinating bodies at several levels may provide most added value for stakeholders involved in CIIP. A (cyber) security council involving high-level representatives may function as a coordinating body at the strategic level. At the tactical level, coordination can be done by a national agency (such as the Cyber Security Agency of Singapore).[6] Coordination at the tactical level involves for example the alignment of government and/or public-private cyber security programs or support and guidance for the implementation of regulation by CII operators. At the operational level, coordination is often done by a national CERT (e.g. US CERT or govCERT.dk) which supports CII operators and other stakeholders with threat intelligence and incident response.

## Handle CIIP dynamics

**Good practice 1: Keep ahead of CII developments, uptake and trends**

To uphold national security, it is important to keep constant attention for CIIP because of its inherent dynamic character. This requires an organisational functionality at the national level, which can keep track (overarching vision) and which can also act accordingly (flexible). The landscape evolves rapidly over time. There is a constant stream of sophisticated new threats which target CII. Dependencies shift unexpectedly due to unforeseen uptakes or failure of (apparent) traditional or unimportant information infrastructure technology causing other information infrastructure services to become critical to the nation.

An overarching vision is derived from short, and long-term (risk) assessments and support from CIIP policy-makers and experts (national CII operators and academia). A culture of information exchange on cybersecurity stimulates and supports public and private actors to better prepare for possible essential organisational changes, threats, and governance changes.[7]

6 For more information, see: https://www.csa.gov.sg/

7 See chapter 6 in the GFCE-Meridian Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers".

**Good practice 2: Take part in international dialogues**

It is highly recommended to keep track of changes in the risk to CII and new vulnerabilities of CII by reaching out to international communities. Regardless of national differences in CIIP, one can learn from others and receive help. At the same time, one needs to offer help when possible.[8] Besides gathering information on changes and threats to CII, reaching out and taking part in international dialogues provides an opportunity to participate and shape decision making processes.

There are many international communities and organisations that provide platforms for such dialogues, each having a different scope and objectives. The table below is not exhaustive, but gives a good indication in the broad set of actors providing different sorts of guidance for CIIP efforts.

<table>
<tr>
<td>International intergovernmental organisations<br>- United Nations<br>- International Telecommunications Union<br>- G8<br>- Interpol<br>- Etc.<br><br>Regional departments of aforementioned organisations<br>- United Nations Southeast Asia and Pacific<br>- Caribbean Telecommunications Union<br>- Etc.</td>
<td>Private, technical, and non-governmental organisations<br>- FIRST (Forum for Incident Response and Security Teams)<br>- Internet Corporation for Assigned Names and Numbers ICANN<br>- The Global Forum on Cyber Expertise GFCE<br>- Meridian Process<br>- Asia Pacific Computer Emergency Response Teams - APCERT<br>- knowledge institutes, research institutes<br>- CERT.org<br>- Internet Society<br>- Internet Governance Forum IGF<br>- TF-CSIRT<br>- Etc.</td>
</tr>
<tr>
<td>Intergovernmental organisations<br>- African Union<br>- Organization of American States<br>- Association of Southeast Asian Nations ASEAN<br>- Etc.</td>
<td>Regional intergovernmental organisations<br>- European Union<br>- Europol<br>- Economic Community of West African States ECOWAS, etc.<br>- Etc.</td>
</tr>
</table>

[8] See GCCS2015 Good Practice: Sharing Cyber Security Information (Luiijf and Kernkamp): “Noblesse Oblige: No Free Ride”.

**Good practice 3: Stimulate the sharing cyber security related information**

Cyber security information sharing is the basis for a collective understanding of threats, vulnerabilities, dependencies, and mitigation measures. It is worthwhile to invest in such a relationship in initial stages of CIIP and to commit to it in the long run. Information sharing is crucial across governmental agencies and highly important to private actors. In a hyperconnected society, interactive exchange of information between public and private actors is beneficial to all parties involved.[9] One way to start structured and trusted information sharing is by abiding to the "Traffic Light Protocol" (TLP), which is used by both technical and non-technical communities that are active in the cyber security domain.[10]

In case of CII disruptions or crisis, the relationship that the government and CII operators established strengthens the common interest to effectively and collaboratively address the incident. Information sharing is a relative low investment but a very effective approach of managing the collaborative CII risk in a domain that is in constant flux, and builds trust.

Voluntary information sharing could be at odds with law and regulation. Various nations have mandated information sharing in case of data leaks, disruptions and malfunctioning due to CII failure. The relationship is key: proposing mandatory information sharing after mandated information sharing due to a crisis does not stimulate the intended trusted relationship. When the process, structure and relationship for information sharing are introduced and maintained properly, mandated information sharing is just a minor part of the voluntary information sharing, as the motivation is the carrot, and not the stick. [11]

9 GCCS2015 Good Practice: Sharing Cyber Security Information (Luiijf and Kernkamp)
10 See: TLP guidelines on the FIRST website. On-line: https://www.first.org/tlp
11 See GCCS2015 Good Practice: Sharing Cyber Security Information (Luiijf and Kernkamp)

# 3. Key challenges

Hurdles are evident while developing a CIIP policy with many different stakeholders. However, some hurdles are already experienced by others. In this paragraph, six key challenges are highlighted.

### Key challenge 1: Aligning a CIIP policy with a national risk profile and/or CIP policy

A national risk profile, a CIP policy and a CIIP policy are all elements that help a nation focus its national security efforts on issues that are critical to the well-being of the nation. A CIIP policy should ideally take notice of relevant elements of a CIP policy. Both the CIP and CIIP policies should focus on the risk identified in a national risk profile and follow the directions set in a national security strategy. However, in many cases, these elements are developed within different timeframes, with different experts and stakeholders involved. This may provide a tremendous challenge to policy makers. For an effective approach to national security, it is necessary that a national risk profile, CIP policy and CIIP policy – and the national security strategy, if present – are aligned.

### Key challenge 2: Separating what is critical from what is important

The essence of adopting a CIIP policy is focusing security efforts on those parts of the (information) infrastructure that, when being disrupted, pose a threat to national security, in other words; critical elements. It can be a major challenge to make the distinction between critical elements and elements that, when being disrupted, cause major harm or substantial damage yet not at the level of national security, in other words: important elements. Such distinction, however, plays a major role in times of crisis when triage-based decisions are required and in the aftermath of incidents, when elements may appear more important than they objectively are.

### Key challenge 3: Getting many heterogenous stakeholders involved

It is a challenge to accommodate parties to get involved in CIIP despite different interests in protecting CII. Actors involved originate from different disciplines, sectors and (institutional) histories. Upholding national security might be an overarching goal that suffices to get many stakeholders engaged in the beginning, but CI and CII operators, regulators or sector-organisations have different day-to-day challenges. The added value of involvement must be clear. Ensuring that all parties bring something to the table can also fortify that the point on the horizon (CIIP) is an appreciated and efficient mutual effort.

## Key challenge 4: Identifying and assessing CII dependencies between (Information) Infrastructures

Insight into dependencies is essential and a key challenge remains on how to encounter for uncontrollable dependencies. There are two sorts of uncontrollable dependencies. Ones that are a given (e.g. Internet Exchange Points, Domain Name Services, GPS, etc.), and other ones that come to the surface unexpectedly due to shifting panes during a crisis (e.g. sudden uptake in satellite telephony, exponential increase in mobile network usage, emergency telephone number overload, certificate hijacking, etc.). Getting and maintaining insight in dependencies between and within CII is a profound challenge.

## Key challenge 5: Involving organisations related to physical security

Adequately aligning CIIP challenges and expertise into or alongside the responsibilities, scope and mandate of traditional CIP organisations is a major challenge. Some nations merge organisations responsible for CIP and CIIP, while others keep separate entities. Institutional stovepipes and rationales remain a major challenge; stakeholders work, think, mitigate and protect differently. Calculating and preparing for the effects of flooding combined with electricity outage is very different than calculating the impact of a malfunctioning server. Measures for mitigation are also completely different. What is undisputed is that physical security remains relevant; one needs to renew and update national risk profiles considering physical risks. However, because CII cuts through old (and introduces new) processes, dependencies and networks, protecting CI now needs to consider new risks and challenges.

## Key challenge 6: Maintaining attention for CII (frequent reviewing) in absence of public and/or private turmoil

Attention for CII should be continuous and enduring. Dynamics in CII require continuous attention and reviewing of the related risk. In various nations, CIIP only became important after incidents happened. Incidents increase the sense of urgency and kick-start CIIP activities. However, such activities do not necessarily lead to the durable attention it requires. Because of the dynamic nature of CII and CII operators and the interconnectedness worldwide, it is essential yet highly challenging to maintain political and governmental attention for CIIP, even in absence of incidents that cause societal turmoil.

# Annex: sources on CIIP

The following sources were used to draft this Global Good Practice. These sources can also be used for local policy development and implementation by individual governments and/or critical (information) infrastructure operators and other stakeholders.


CIPedia© (2017), CIPedia is a web resource on international CIP and CIIP related definitions and abbreviations by the EU CIPRNet project. Retrieved from: http://cipedia.eu.

ENISA (European Union Agency for Network and Information Security) (2015). Good Practice Guide on Vulnerability Disclosure. Retrieved from: https://www.enisa.europa.eu/publications/vulnerability-disclosure/at_download/fullReport

ENISA (European Union Agency for Network and Information Security) (2014). Methodologies for the identification of Critical Information Infrastructure assets and services; guidelines for charting electronic data communication networks. To be retrieved from: https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis/at_download/fullReport

G8, G8 Principles for Protecting Critical Information Infrastructures, 2003. Retrieved from: http://www.cybersecuritycooperation.org/documents/G8_CIIP_Principles.pdf

Klaver, M., Luiijf, H., Nieuwenhuijs, A. et al., (2011). RECIPE Good Practices Manual for CIP Policies, The Hague. Retrieved from: https://www.tno.nl/recipereport/

Luiijf, H., van Schie, T., van Ruijven, T., Huistra, A. (2016). The GFCE-Meridian Good Practice Guide 1.0 on Critical Information Infrastructure Protection for governmental policy-makers, TNO. Retrieved from: https://www.tno.nl/media/8578/gpg_criticalinformationinfrastructureprotection.pdf

Luiijf, H., van Schie, T., van Ruijven. (2017). Compendium Document to the GFCE-Meridian Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers, TNO. Retrieved from: https://www.tno.nl/media/10425/companiondocument_gpg_ciip.pdf.

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

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

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

Zaballos A.C. and Jeun, I. (2016), Best Practices for Critical Information Infrastructure Protection (CIIP): Experiences from Latin America and the Caribbean and Selected Countries. Retrieved from: http://www.andi.com.co/camarabpo/Documents/Documentos%20de%20Interes/Best%20practices%20for%20information%20BID.pdf

This document was drafted and developed in cooperation with TNO for the Global Conference on Cyberspace GCCS in India (2017). Many thanks to all others, especially those from the CIIP community, who participated in the realisation of this document.

GFCE
Global Forum on Cyber Expertise