The Critical Importance of CIIP to Cybersecurity

"Without CIIP there is no Cybersecurity"

Peter Burnett

GFCE-Meridian *Coordinator*

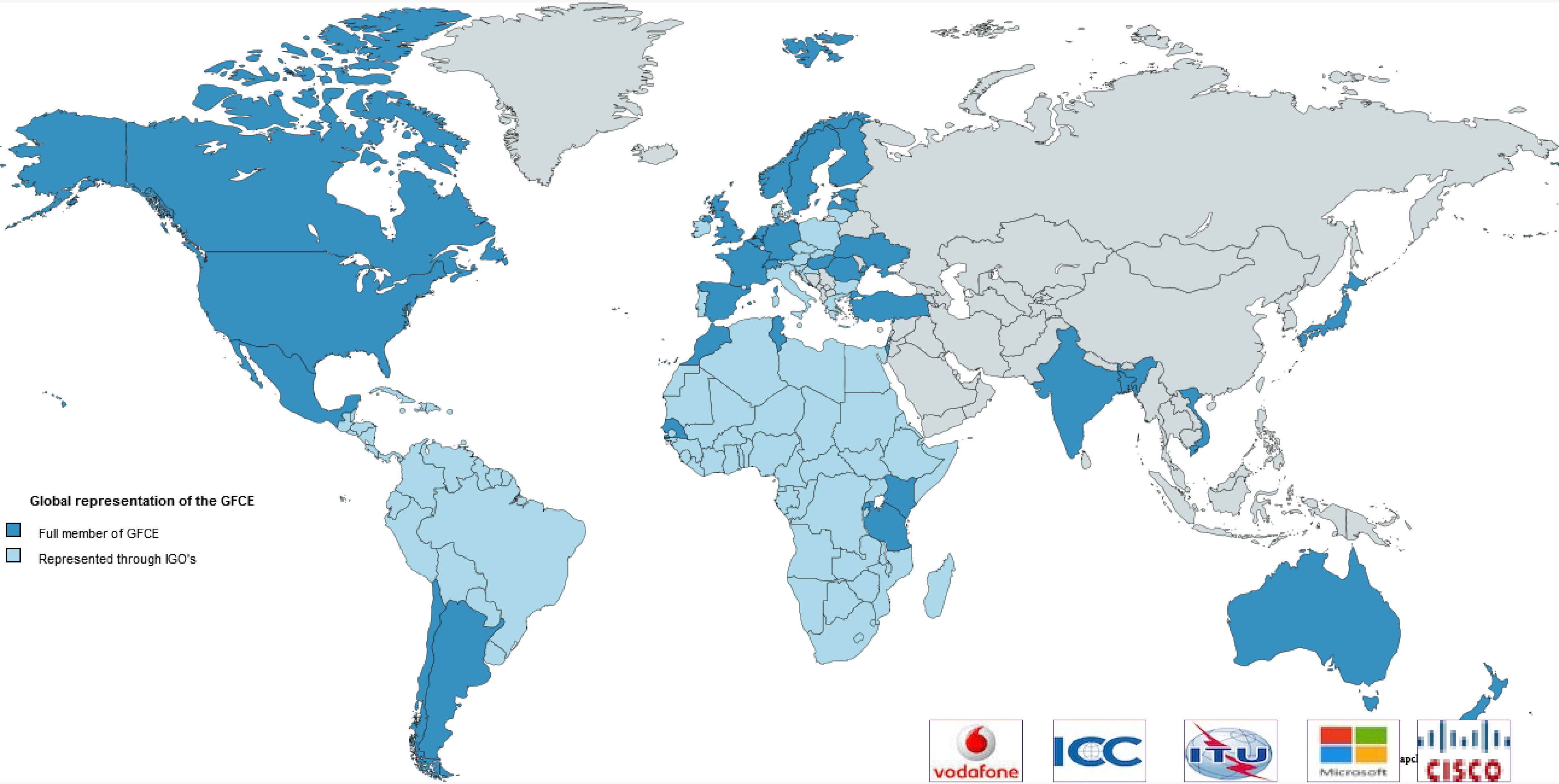
The Global Forum on Cyber Expertise

- Focus: cyber capacity building (awareness and implementation).
- Goal:
  - Identify best practices and multiply these on a global level.
  - Connecting relevant organizations.

GFCE

Global Forum on Cyber Expertise

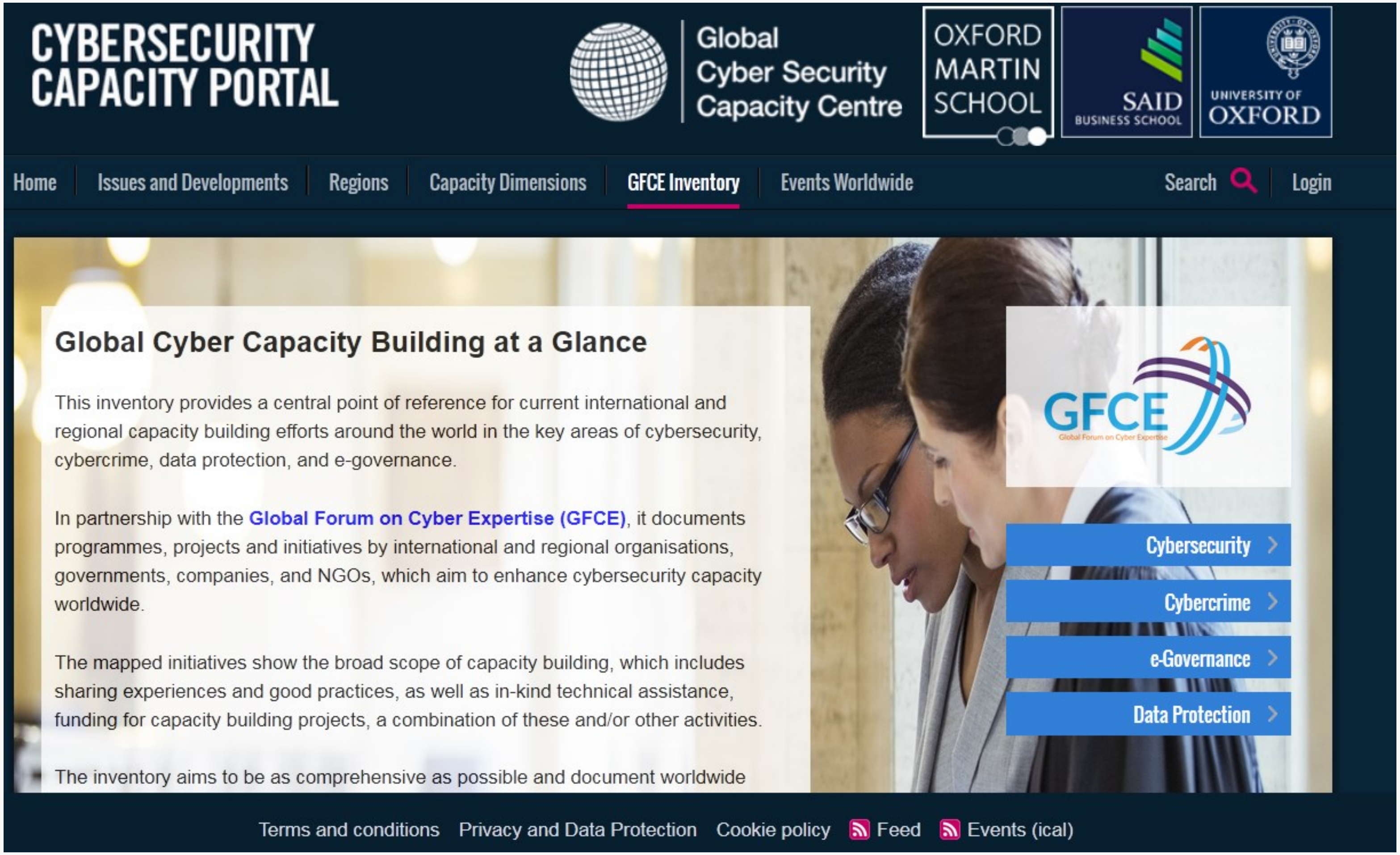
GFCE Members


Global representation of the GFCE
■ Full member of GFCE
□ Represented through IGO's

54 members: countries (36), private organizations (9), intergovernmental organizations (IGOs) (9)

IGOs are for example: AU, EC, OAS, ICC, ITU, Europol

GFCE Inventory at the Oxford Global Cyber Security Capacity Centre



Global Cyber Capacity Building at a Glance

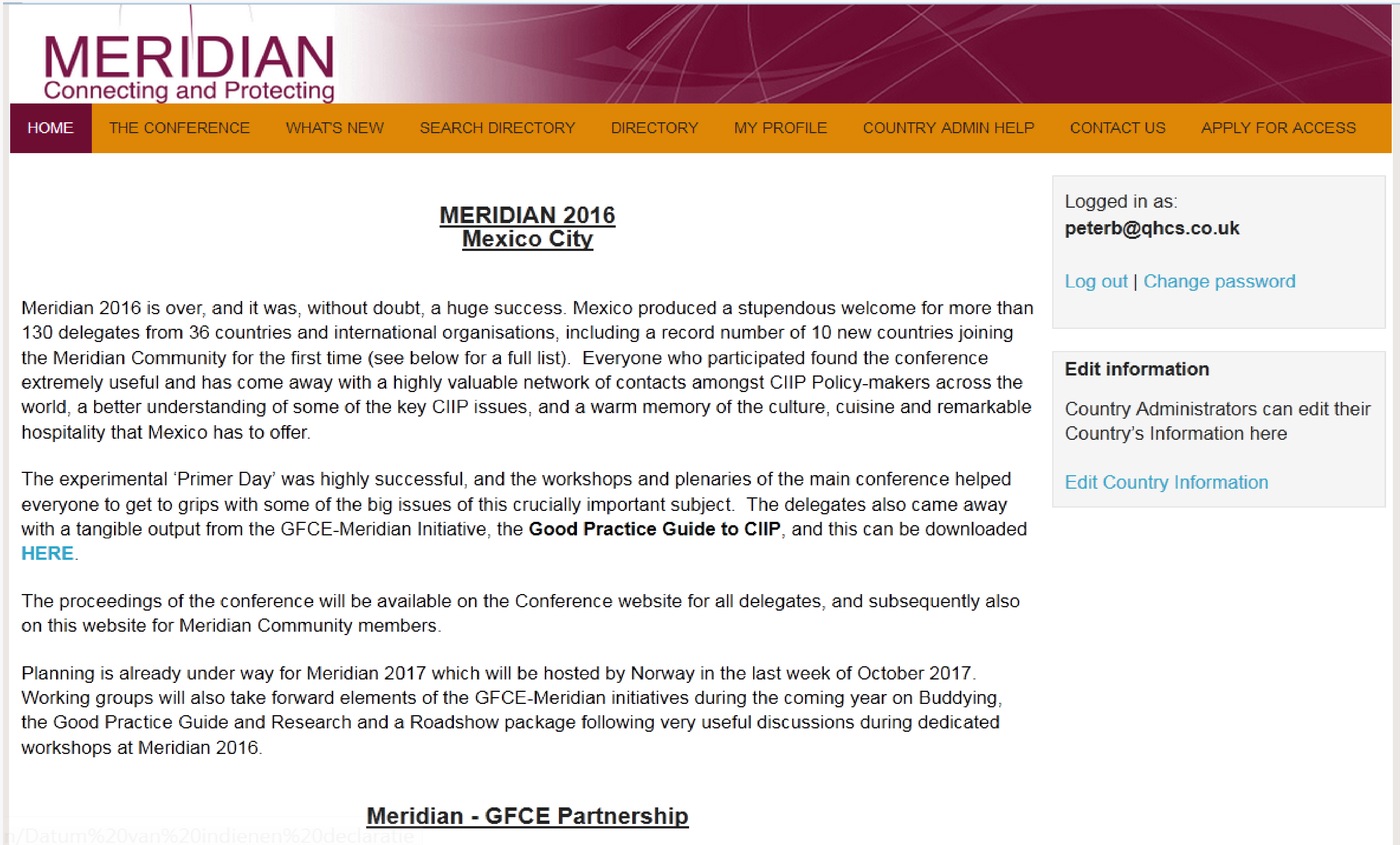
This inventory provides a central point of reference for current international and regional capacity building efforts around the world in the key areas of cybersecurity, cybercrime, data protection, and e-governance.

In partnership with the **Global Forum on Cyber Expertise (GFCE)**, it documents programmes, projects and initiatives by international and regional organisations, governments, companies, and NGOs, which aim to enhance cybersecurity capacity worldwide.

The mapped initiatives show the broad scope of capacity building, which includes sharing experiences and good practices, as well as in-kind technical assistance, funding for capacity building projects, a combination of these and/or other activities.

The inventory aims to be as comprehensive as possible and document worldwide

MERIDIAN



MERIDIAN 2016
Mexico City

Meridian 2016 is over, and it was, without doubt, a huge success. Mexico produced a stupendous welcome for more than 130 delegates from 36 countries and international organisations, including a record number of 10 new countries joining the Meridian Community for the first time (see below for a full list). Everyone who participated found the conference extremely useful and has come away with a highly valuable network of contacts amongst CIIP Policy-makers across the world, a better understanding of some of the key CIIP issues, and a warm memory of the culture, cuisine and remarkable hospitality that Mexico has to offer.

The experimental ‘Primer Day’ was highly successful, and the workshops and plenaries of the main conference helped everyone to get to grips with some of the big issues of this crucially important subject. The delegates also came away with a tangible output from the GFCE-Meridian Initiative, the **Good Practice Guide to CIIP**, and this can be downloaded **HERE**.

The proceedings of the conference will be available on the Conference website for all delegates, and subsequently also on this website for Meridian Community members.

Planning is already under way for Meridian 2017 which will be hosted by Norway in the last week of October 2017. Working groups will also take forward elements of the GFCE-Meridian initiatives during the coming year on Buddying, the Good Practice Guide and Research and a Roadshow package following very useful discussions during dedicated workshops at Meridian 2016.

Meridian - GFCE Partnership

Logged in as:
peterb@qhcs.co.uk

Log out | Change password

Edit information

Country Administrators can edit their Country’s Information here

Edit Country Information

n/Datum%20van%20indienen%20declaratie

The Meridian Process

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

- The Meridian Process seeks to create a community of senior government policymakers in CIIP by fostering ongoing collaboration. The Meridian Process recognizes that it is only by working together that we can each advance our national CIIP goals and objectives.

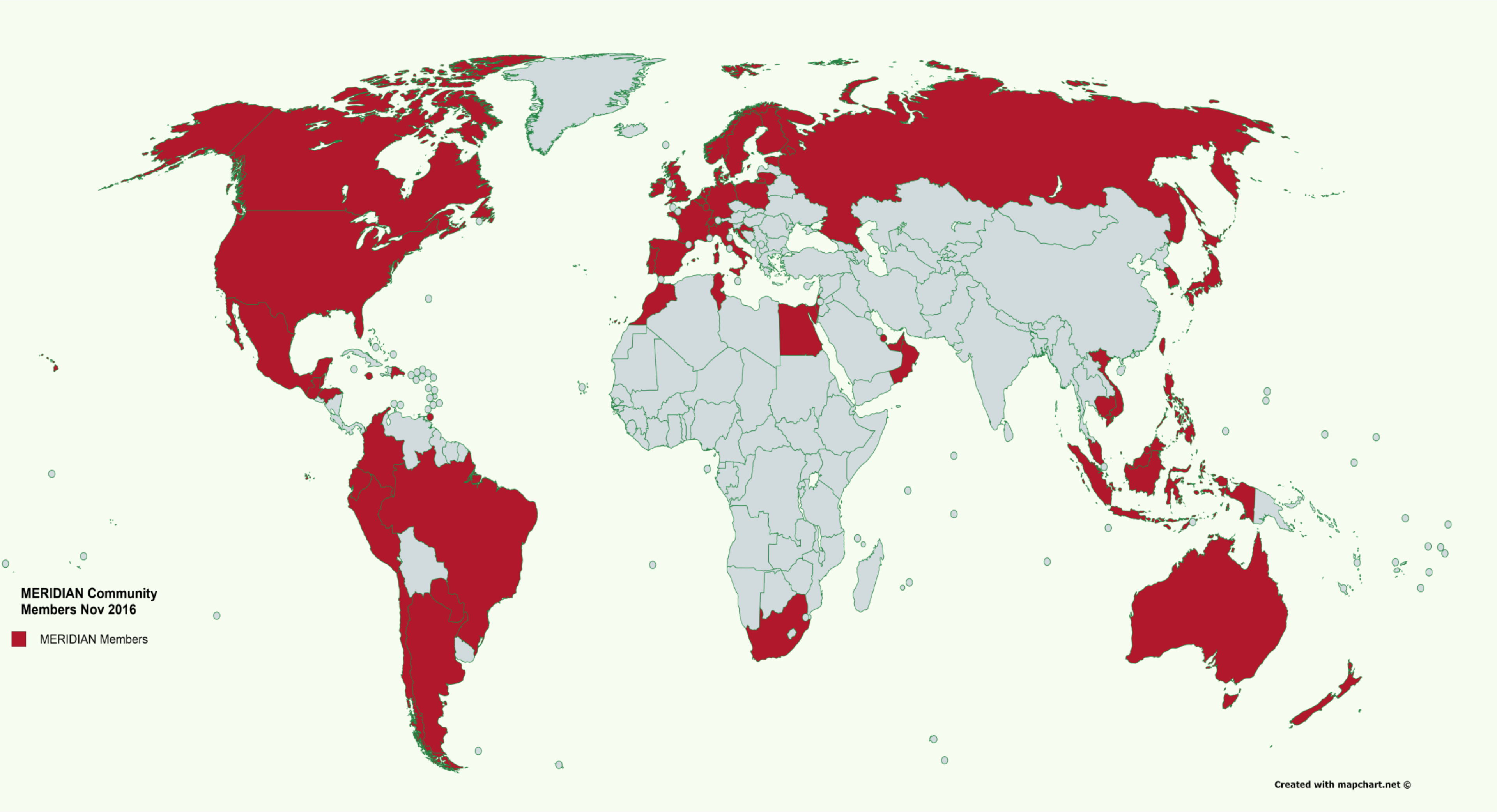
- Participation in the Meridian Process is open to all countries/economies and is aimed at senior government policy-makers involved in CIIP-related issues. Every country/economy is invited to take part in the Meridian Process, and is encouraged to attend the annual Meridian Conference.

Meridian Community
International Organisations

- EU
- ENISA
- EEAS
- ITU
- WEF
- WB
- OAS
- GFCE

- International Organisations that have attended Meridian Conferences

Meridian Community Countries

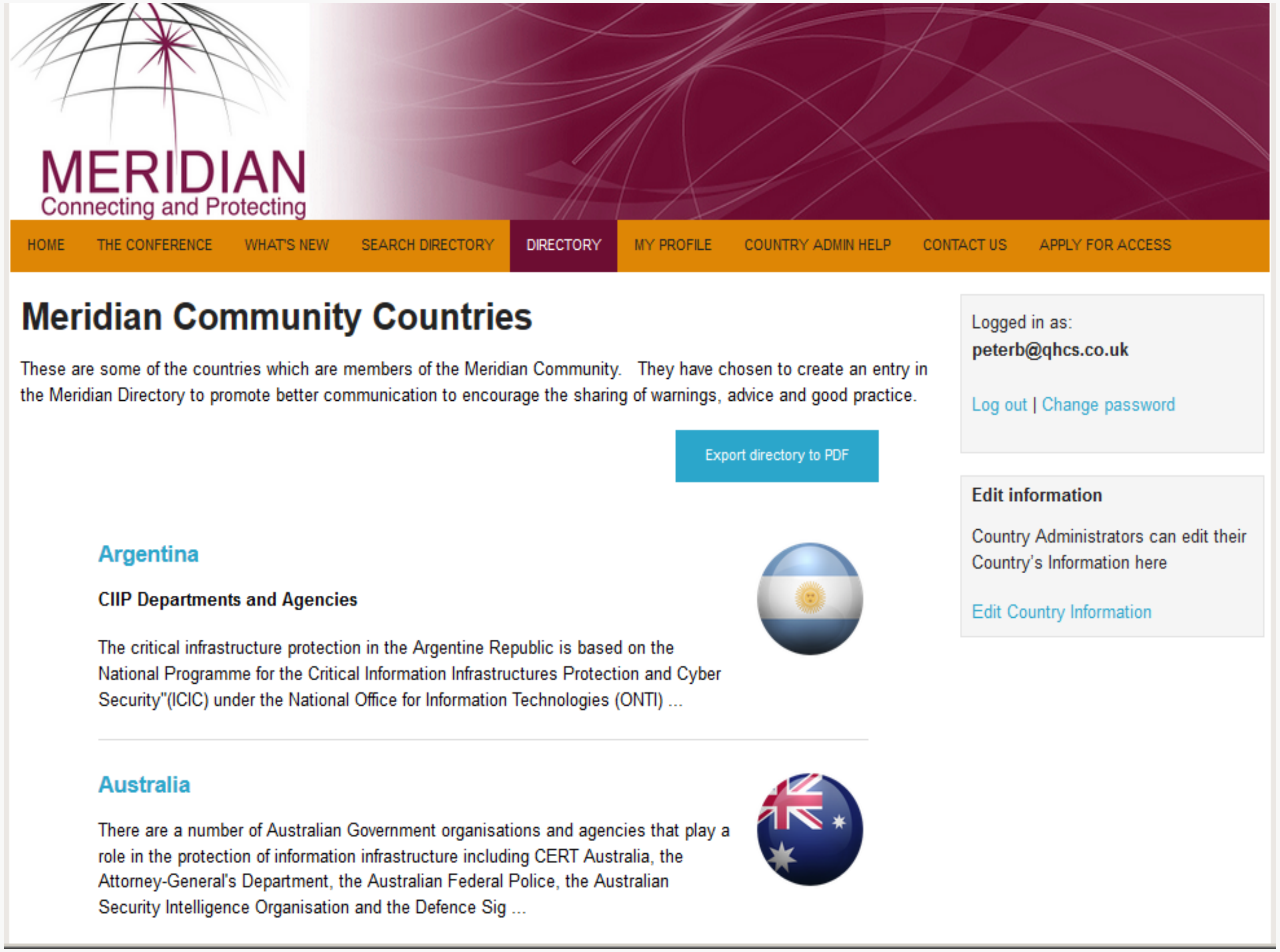


Meridian Community Member Countries

Argentina, Australia, Austria, Belgium, Belize, Brazil, Brunei, Cambodia, Canada, Chile, Colombia, Costa Rica, Croatia, Czech Republic, Denmark, Dominican Republic, Ecuador, Egypt, Estonia, Finland, France, Germany, Guatemala, Honduras, Hungary, Indonesia, Ireland, Israel, Italy, Jamaica, Japan, Lithuania, Luxembourg, Malaysia, Malta, Mexico, Morocco, Netherlands, New Zealand, Norway, Oman, Paraguay, Peru, Philippines, Poland, Portugal, Qatar, Republic of Korea, Russia, Singapore, Slovak Republic, South Africa, Spain, Sweden, Switzerland, Taiwan, Trinidad and Tobago, Tunisia, United Arab Emirates, United Kingdom, United States of America, Uruguay, Vietnam

63 Countries; 10 New members in November 2016

The Meridian CIIP Directory



Meridian Community Countries

These are some of the countries which are members of the Meridian Community. They have chosen to create an entry in the Meridian Directory to promote better communication to encourage the sharing of warnings, advice and good practice.

Argentina

CIIP Departments and Agencies

The critical infrastructure protection in the Argentine Republic is based on the National Programme for the Critical Information Infrastructures Protection and Cyber Security"(ICIC) under the National Office for Information Technologies (ONTI) ...

Australia

There are a number of Australian Government organisations and agencies that play a role in the protection of information infrastructure including CERT Australia, the Attorney-General's Department, the Australian Federal Police, the Australian Security Intelligence Organisation and the Defence Sig ...

Logged in as:
peterb@qhcs.co.uk

Edit information

Country Administrators can edit their Country's Information here

Cybersecurity, CIIP and CIP

- “Sometimes it’s hard to see the wood for the trees”
- ‘The Wood’ = the Forest or the Rainforest Canopy

By Tim35 - Own work, Public Domain, https://commons.wikimedia.org/w/index.php?curid=6853197

Cybersecurity, CIIP and CIP

- Cybersecurity is like a canopy – it covers everything to do with Cyber
- Now it’s hard to see the trees for the wood.
- CIIP = the trees
- CIP = the roots

By The original uploader was Adz at English Wikipedia - Transferred from en.wikipedia to Commons., CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=2250531

Cyber Security and CIIP

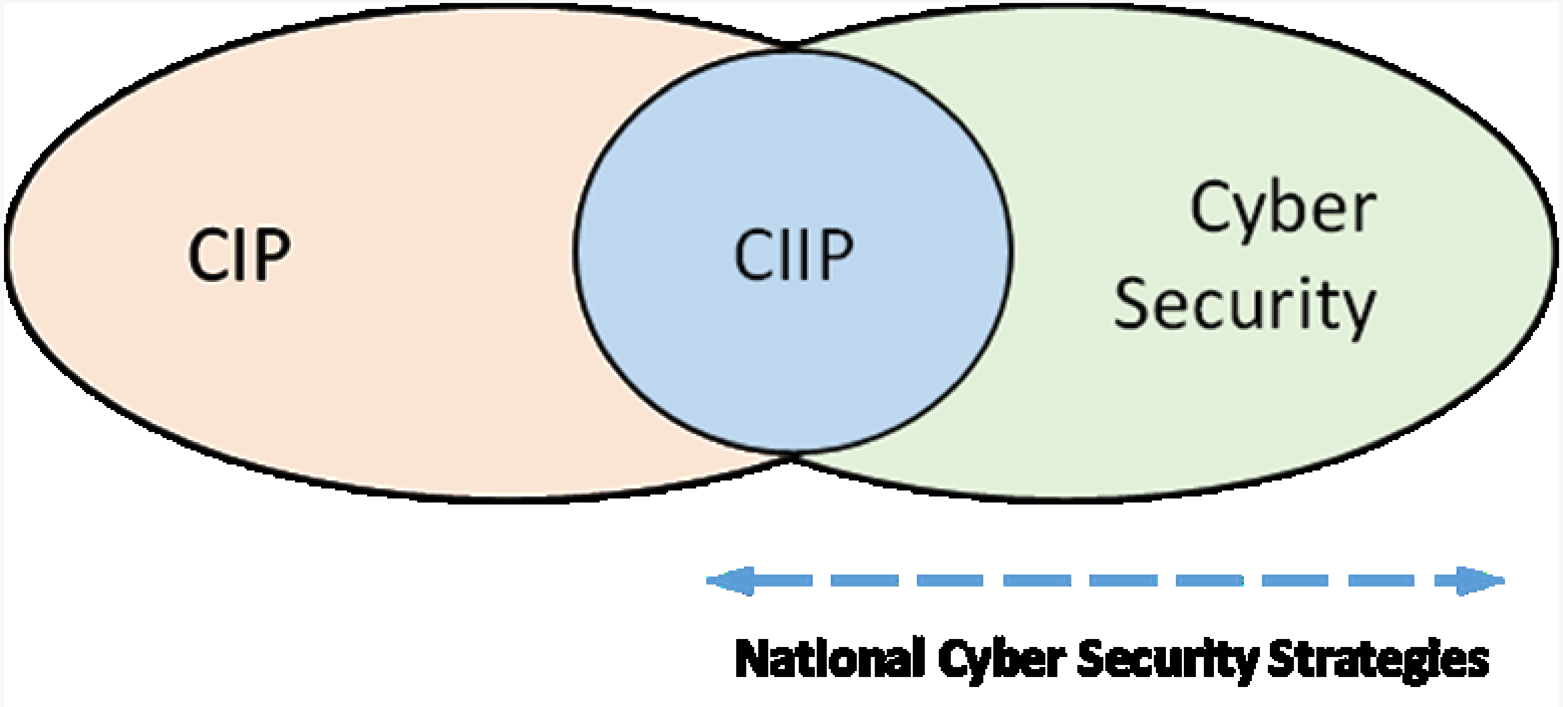
Key Drivers for a Culture of Security in Some Countries

⍰

Two main drivers which support the development of a culture of security at the national level:

1. Implementation of e-Government applications and services

2. Protection of national critical information infrastructures (CII)


CIP
CIIP
Cyber Security
National Cyber Security Strategies

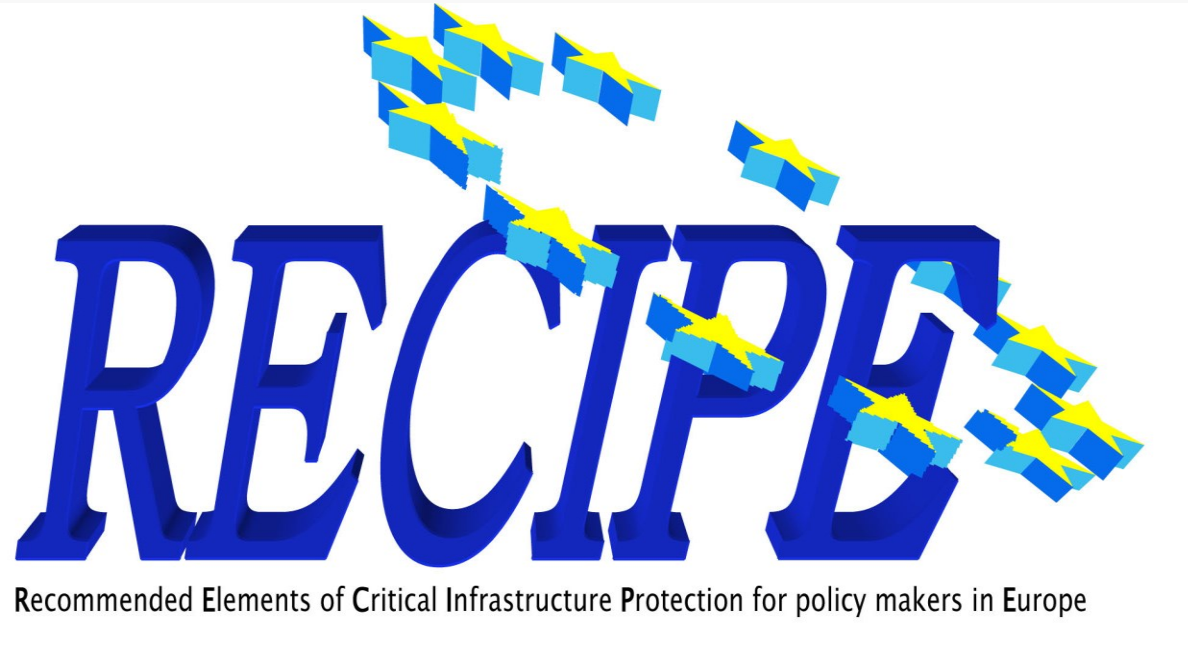
Critical **I**nfrastructure **P**rotection

- Decide what Services and Functions are Critical to your nation
- Identify how those services are delivered
- Consider the threats and vulnerabilities
- What protection and mitigation can you put in place
- Critical Infrastructure Sectors
- Criticality Criteria

Criticality Criteria

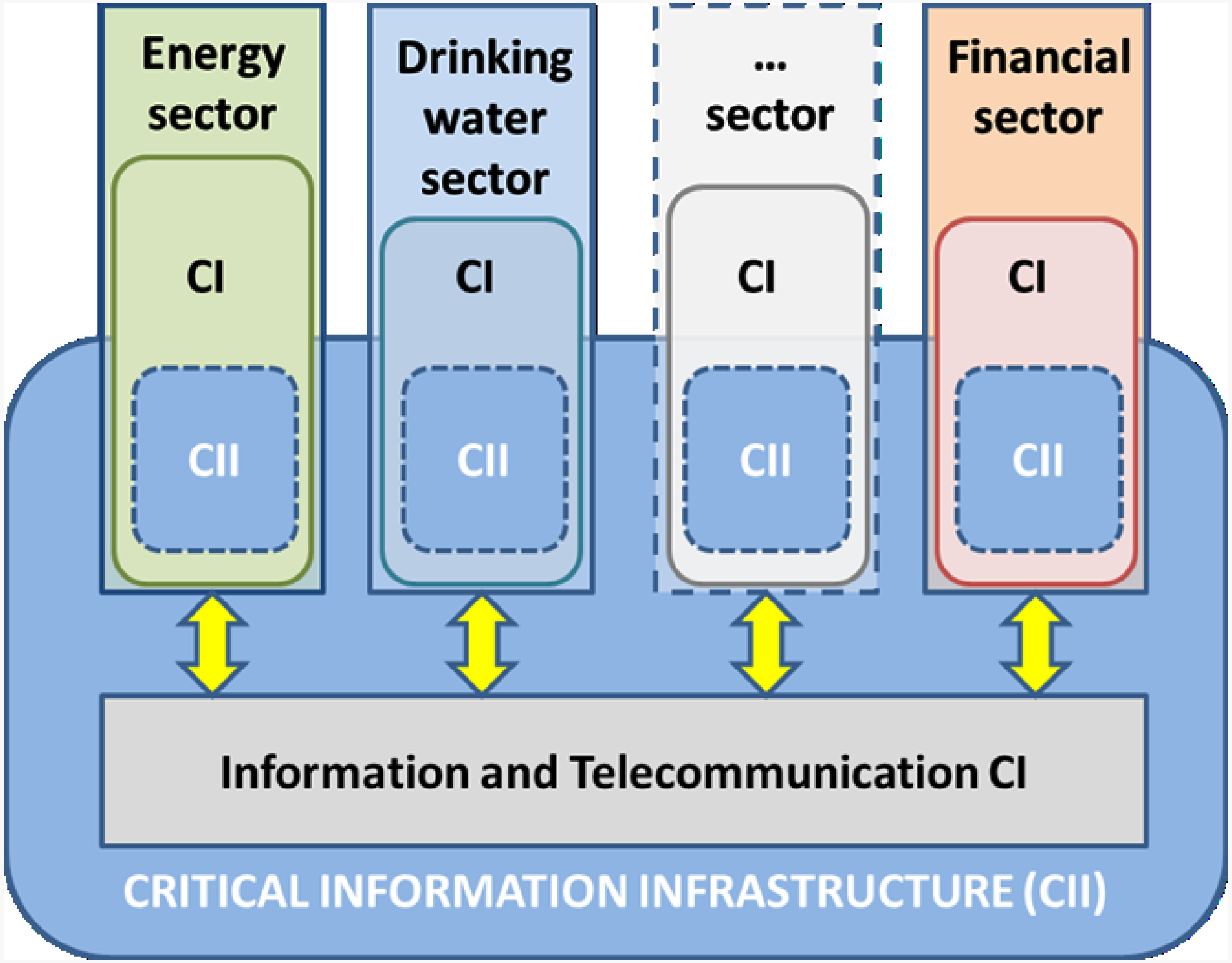
Criticality Scale	Description
Cat. 5	This is infrastructure the loss of which would have a catastrophic impact on the UK. These assets will be of unique national importance whose loss would have national long-term effects and may impact across a number of sectors. Relatively few are expected to meet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

CIP Guidance


RECIPE
Recommended Elements of Critical Infrastructure Protection for policy makers in Europe

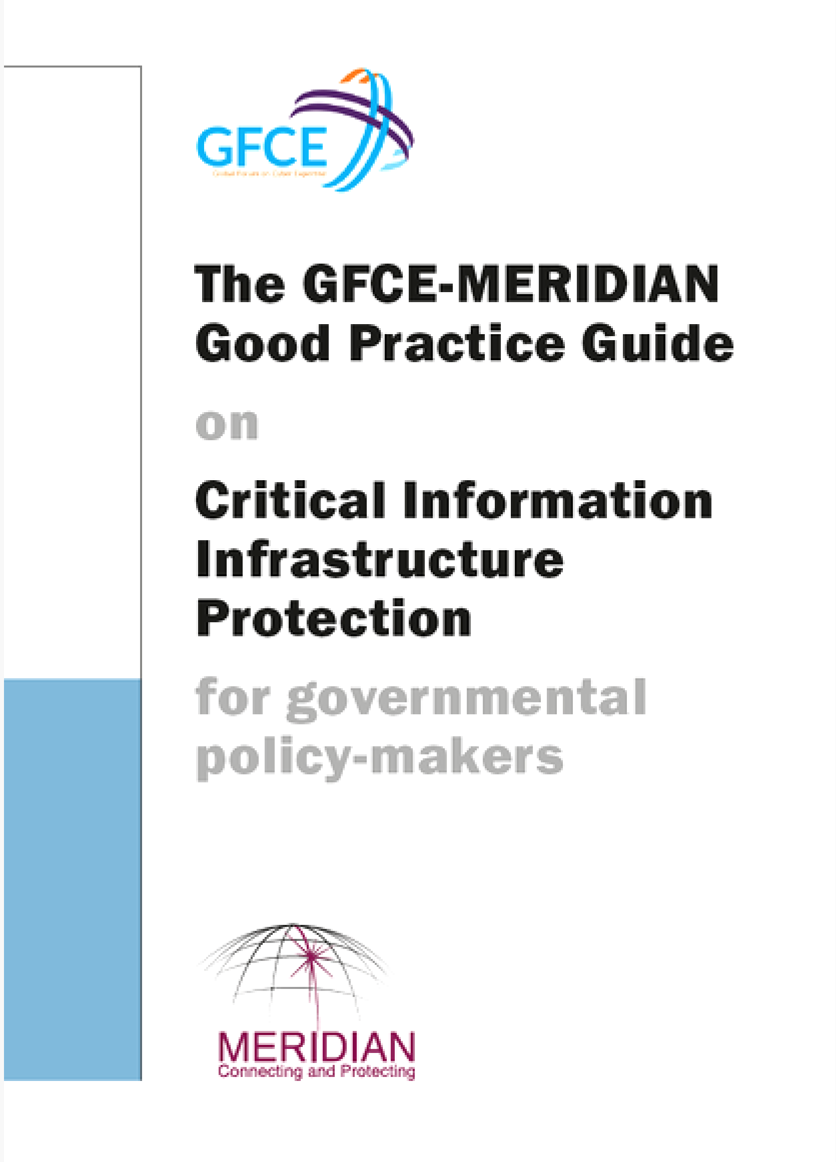
https://www.tno.nl/recipereport//

CI and CII


Energy sector
CI
CII
Drinking water sector
CI
CII
… sector
CI
CII
Financial sector
CI
CII
Information and Telecommunication CI
CRITICAL INFORMATION INFRASTRUCTURE (CII)

CIIP

- *When you’ve Protected your CI ………*
- Identify your CII
- ICT components of CI systems
- Industrial Control Systems (ICS) and SCADA
- Trans-CI functions and systems
- Dependencies
- Dependencies on systems beyond your control
- Protect or mitigate and Crisis Management
- Monitor, Review, Improve ………. continuously
- Test and Exercise
- Information Sharing



GFCE

Global Forum on Cyber Expertise

The GFCE-MERIDIAN Good Practice Guide

on

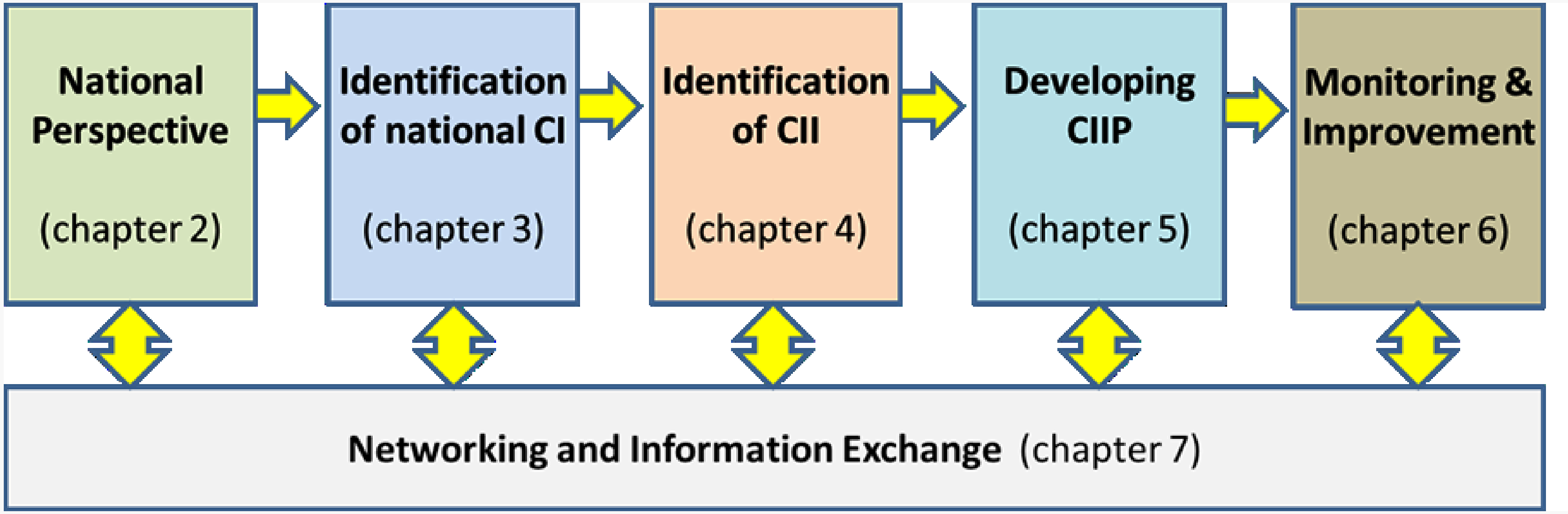
Critical Information Infrastructure Protection

for governmental policy-makers

MERIDIAN

Connecting and Protecting

https://www.meridianprocess.org/



National Perspective (chapter 2)

Identification of national CI (chapter 3)

Identification of CII (chapter 4)

Developing CIIP (chapter 5)

Monitoring & Improvement (chapter 6)

Networking and Information Exchange (chapter 7)

Everybody needs to protect their CI

GFCE

The GFCE-MERIDIAN Good Practice Guide

on

Critical Information Infrastructure Protection

for governmental policy-makers

MERIDIAN
Connecting and Protecting

Cybersecurity

- When you’ve done CIP
- And you’ve done CIIP
- Now you’re ready for Cybersecurity

Thank you

www.meridianprocess.org
www.thegfce.org
https://www.sbs.ox.ac.uk/cybersecurity-capacity/explore/gfce

enquiries@ meridianciip.net