Cybersecurity in Europe – Lessons learnt from Cybersecurity Capacity Maturity Assessments

Mr Jakob Bund – Research Associate

Limassol, Cyprus

28 November 2018

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

Global Cyber Security Capacity Centre (GCSCC)

- The Global Cyber Security Capacity Centre (GCSCC) is a leading international centre for **research on efficient and effective cybersecurity capacity-building.**

- The GCSCC brings together **international expertise across multiple sectors and disciplines** to contribute to Centre's outputs.

- The GCSCC promotes an **increase in the scale, pace, quality and impact** of cybersecurity capacity-building initiatives across the world.

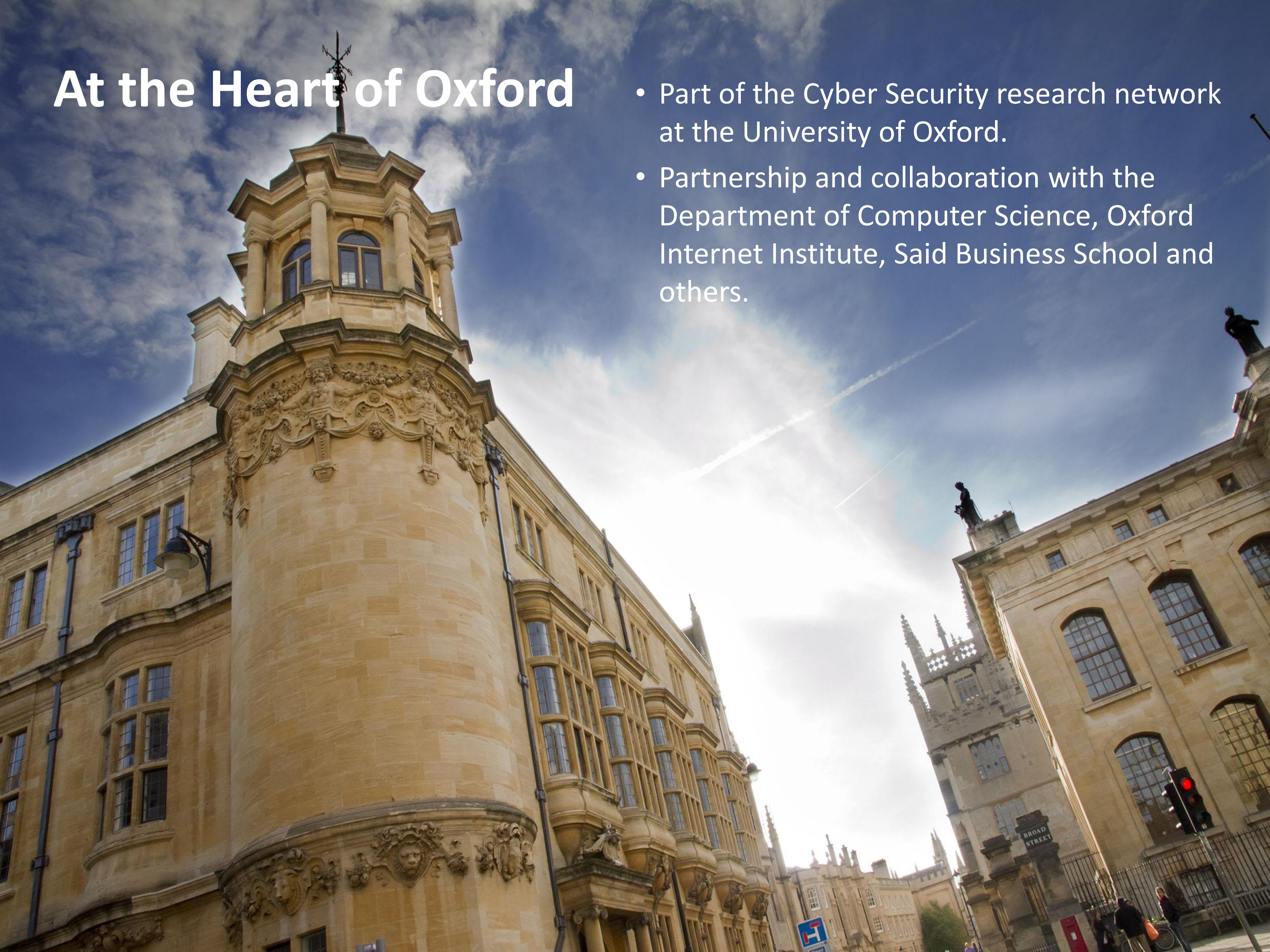
Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

At the Heart of Oxford

- Part of the Cyber Security research network at the University of Oxford.
- Partnership and collaboration with the Department of Computer Science, Oxford Internet Institute, Said Business School and others.



Our Funding Partners

Foreign &
Commonwealth
Office

Government of Victoria, Australia

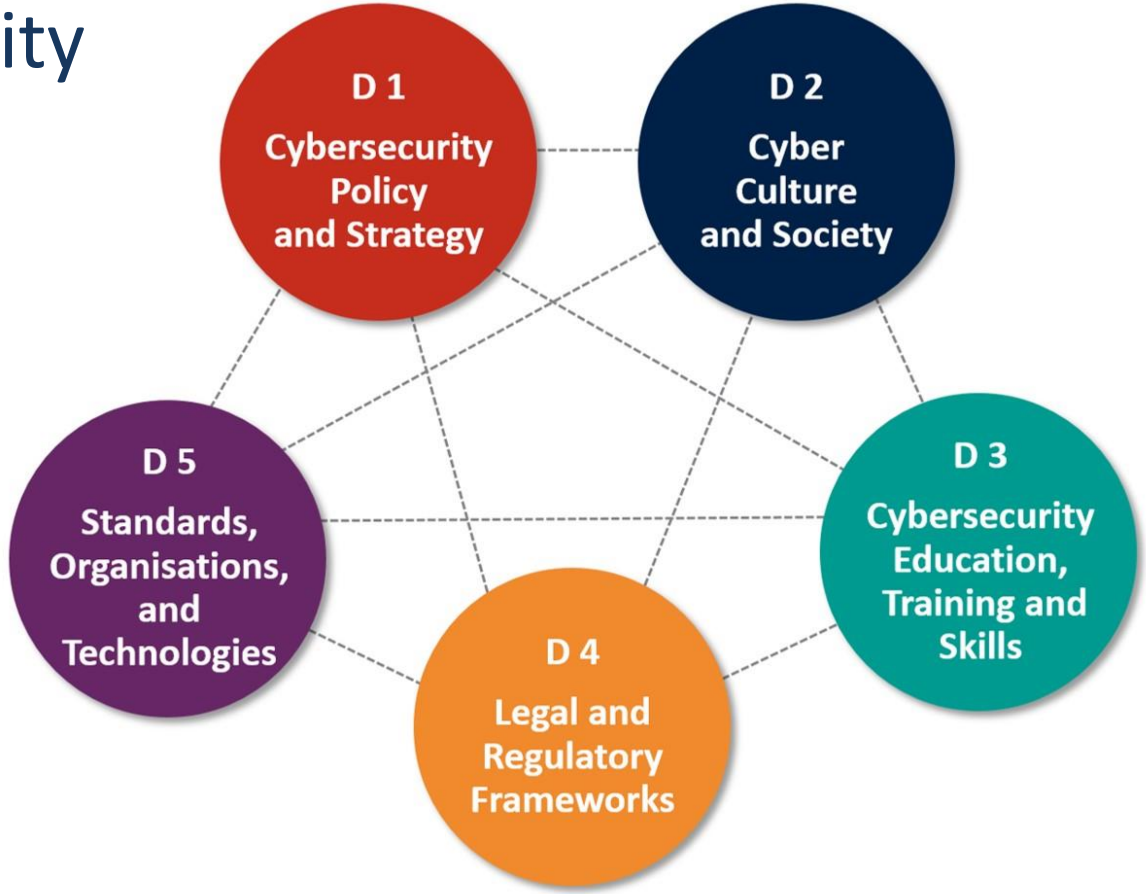
Previous funders:

GFCE
Global Forum on Cyber Expertise

Ministry of Foreign Affairs of Norway

Cybersecurity Capacity Maturity Model for Nations (CMM)

The **5 DIMENSIONS** of Cybersecurity Capacity



D 1

Cybersecurity Policy and Strategy

D 2

Cyber Culture and Society

D 3

Cybersecurity Education, Training and Skills

D 4

Legal and Regulatory Frameworks

D 5

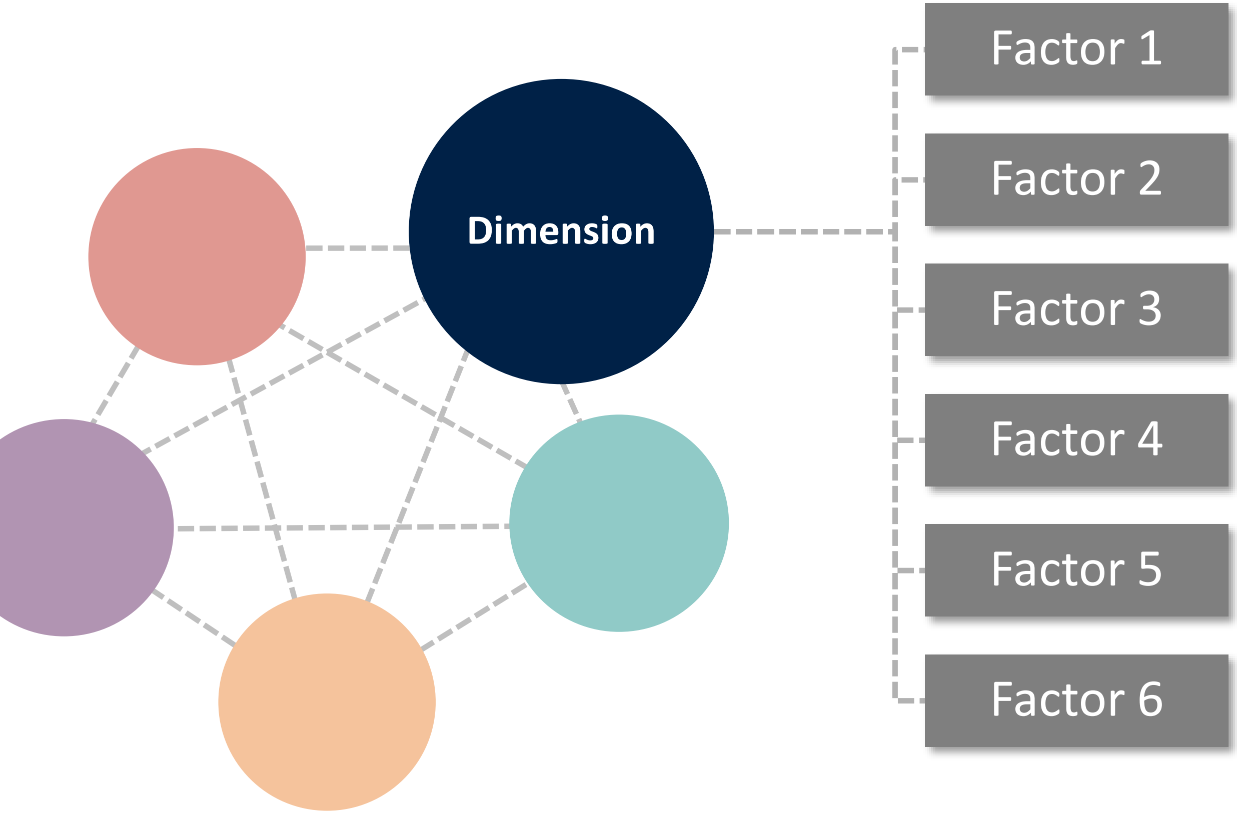
Standards, Organisations, and Technologies

Global Cyber Security Capacity Centre

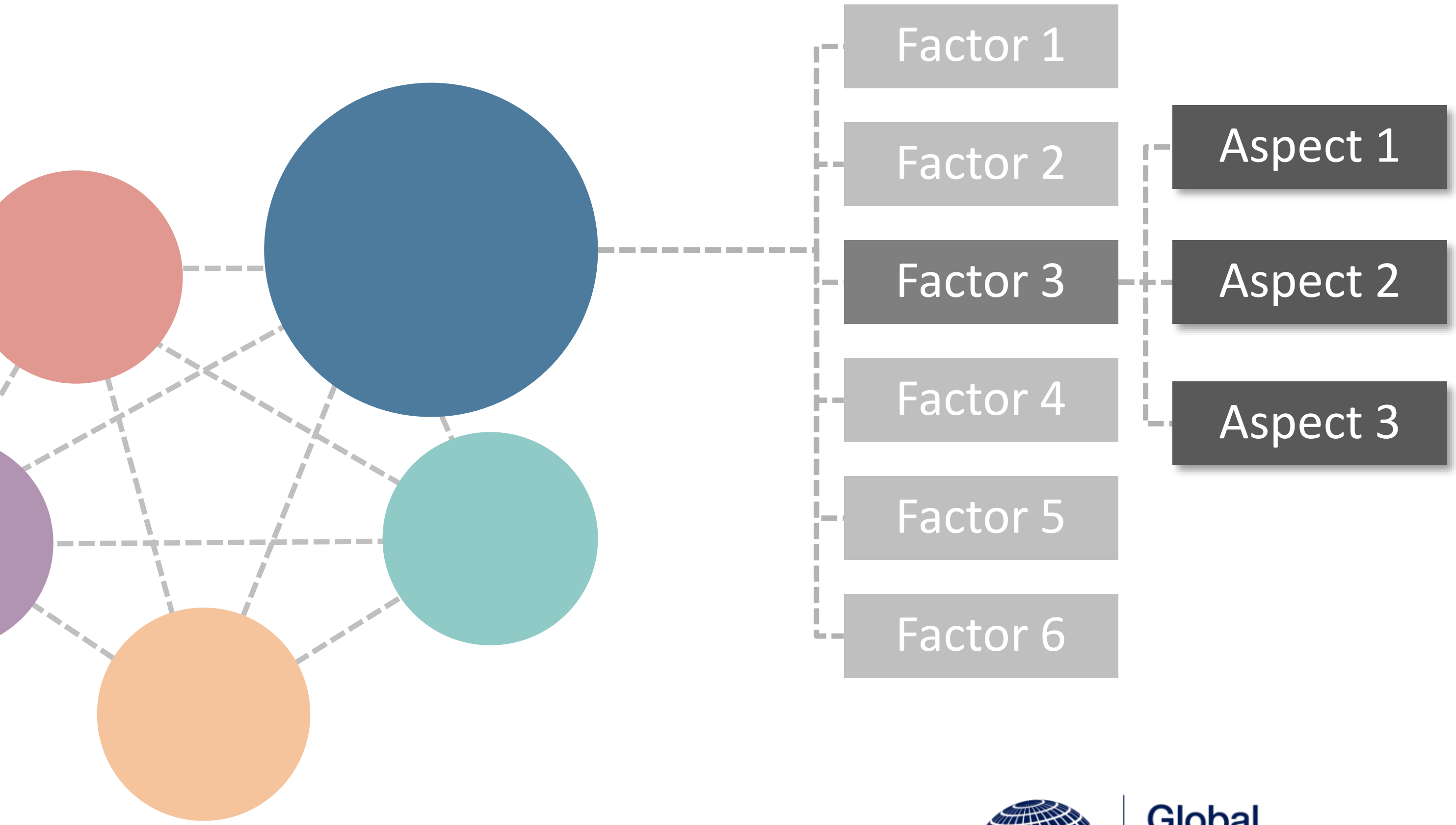
OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

FACTORS: What it means to possess cybersecurity



ASPECTS: Structure the Factor’s content into more concise parts

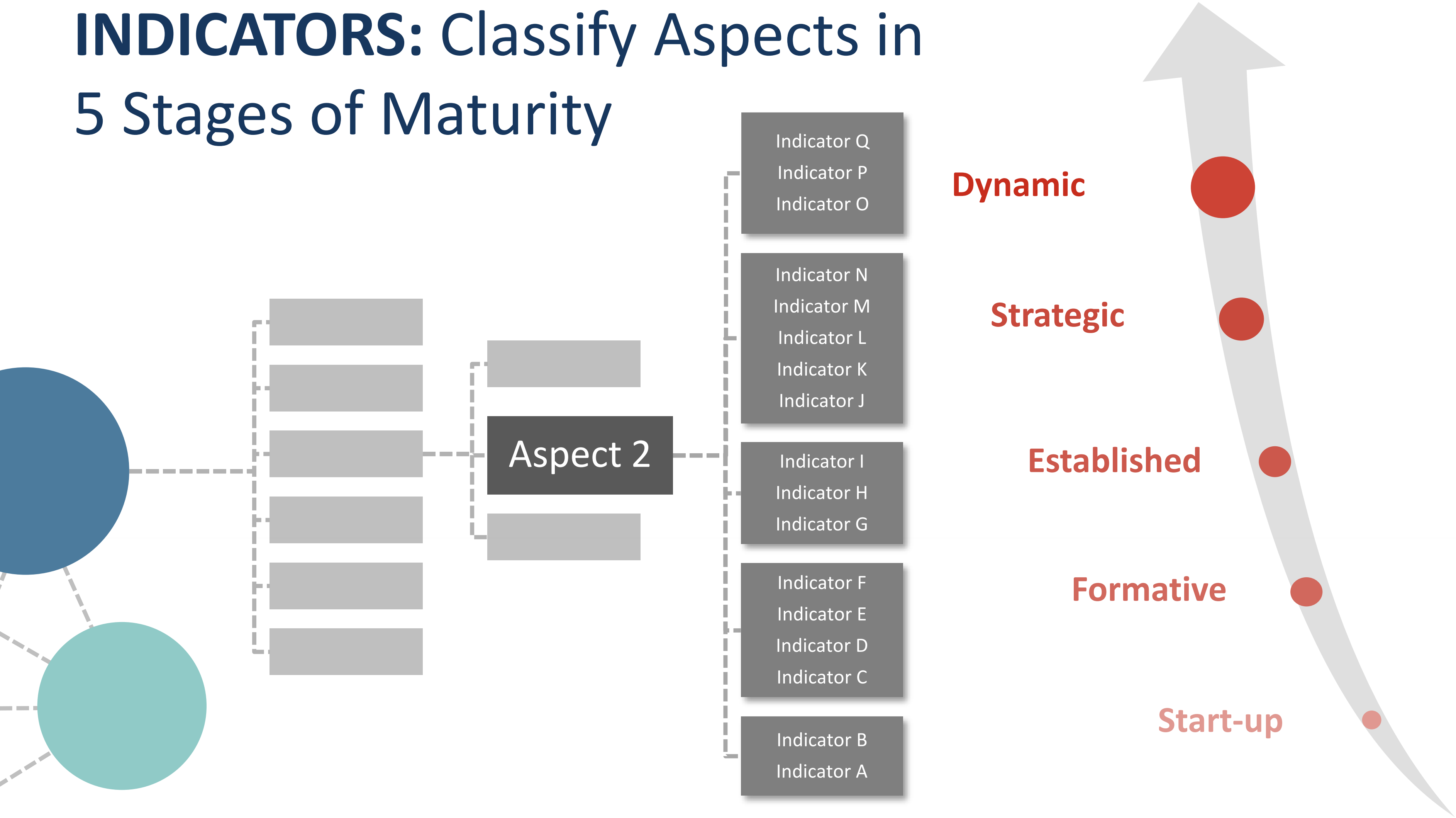


Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

INDICATORS: Classify Aspects in 5 Stages of Maturity

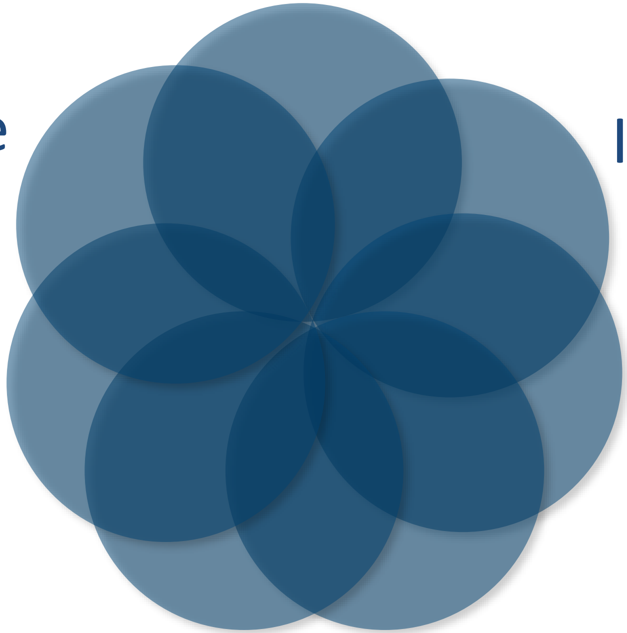


Deploying the CMM

Methodology

- In-country focus group discussions with key stakeholders
- 10 sessions over 3 days
- Research team from the GCSCC
- Interactive deployment tool makes it possible to identify current stage of maturity according to the CMM

Stakeholder Clusters



Criminal Justice

Defence/ Intelligence

Academia/ Civil Society

Government

Legislators

CERT and IT

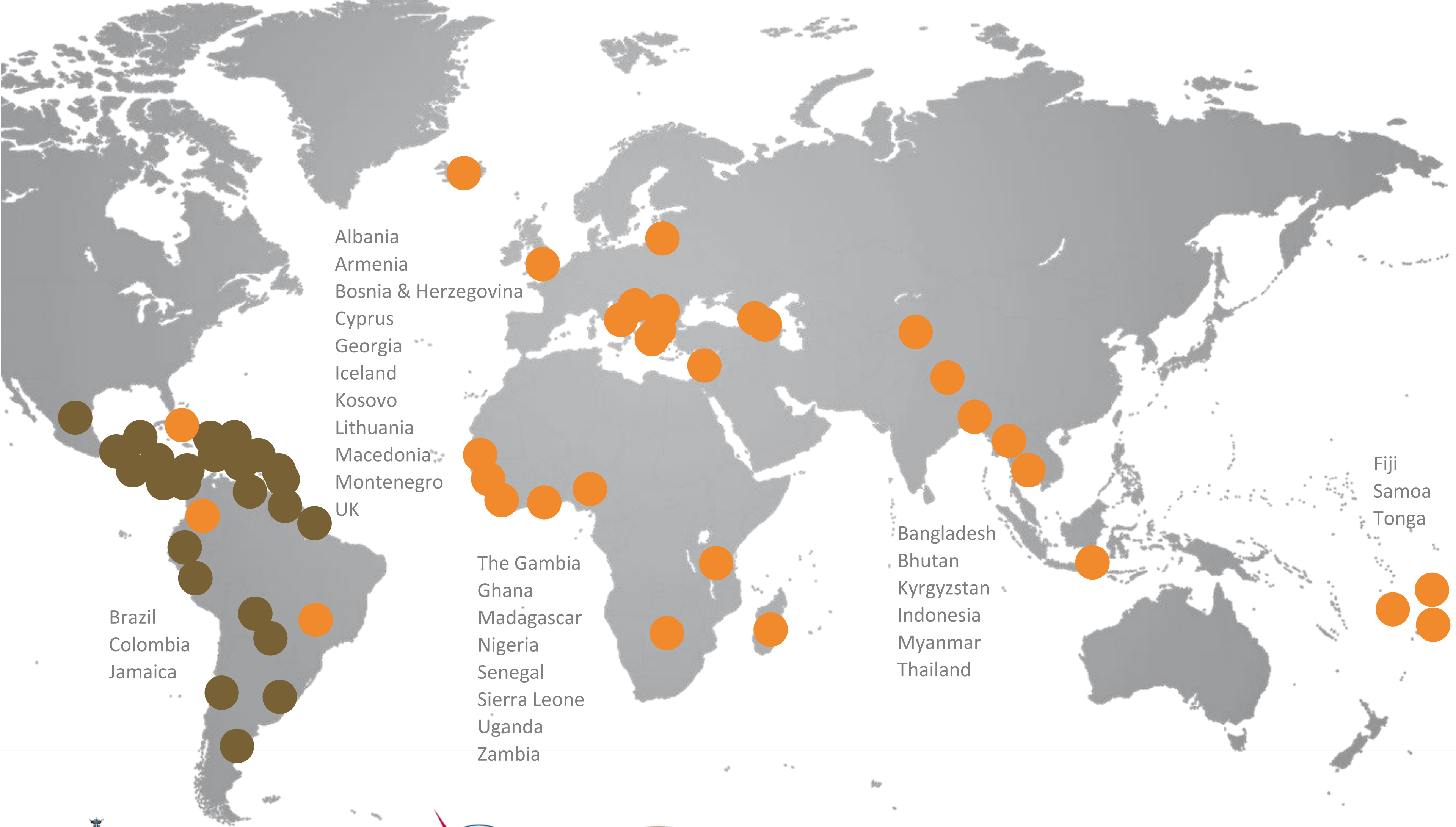
Critical Infrastructure

“All models are wrong but some are useful.”
-- *George Box*

Added-value of CMM Deployments

- Facilitation of direct conversations with stakeholders in-country
- Organic awareness raising through stakeholder exchanges
- Nationally owned process, supported by neutral external evaluation
- Qualitative and quantitative benchmarking
- Assisted self-assessment
- Coordinated recommendations to guide investment priorities

Status: November 2018



CTO COMMONWEALTH TELECOMMUNICATIONS ORGANISATION

ITU

Organization of American States

THE WORLD BANK IBRD • IDA | WORLD BANK GROUP

OCSC Oceania Cyber Security Centre

NRD Cyber Security

NUPI Norwegian Institute of International Affairs

Implementation & Strategic Partners

CTO COMMONWEALTH TELECOMMUNICATIONS ORGANISATION

ITU

Organization of American States

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

NRD Cyber Security

NUPI Norwegian Institute of International Affairs

Ministry of Foreign Affairs of the Netherlands
Ministry of Foreign Affairs of Norway

UK Cabinet Office
Global Forum on Cyber Expertise

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

Feedback

- Countries found the reviews informative and helpful in identifying previously under-considered capacity gaps
- Diverse stakeholder groups enables comprehensive picture in report development
- Review itself as capacity-building exercise and allowed discussions among different stakeholders
- Various lessons learned across all five dimensions of cybersecurity capacity

Observations & Lessons Learnt

Lessons Learnt

- **Policy and Strategy:** Misperception of the role of the CSIRT
- **Culture and Society:** Lack of awareness and of understanding of the relationship between trust/confidence and security
- **Education and Training:** Disconnect between educational offerings and industry needs
- **Legal Frameworks:** Question whether new cybercrime/cybersecurity legislation is needed or adapting existing law is sufficient
- **Standards:** Standards adoption (particularly ISO standards) mostly ad-hoc

- **Overall:** Lack of cooperation and information-sharing; resources; data collection challenges

Observations

- Improvements in government cybersecurity mind-set drive development of national cybersecurity strategy
- No measure of cooperation at the operational level can substitute for institutionalized coordination
- NIS Directive, GDPR function as capacity building instruments (toolkit of best practices)
- Standards and certificates become educational backbone in absence of cybersecurity curriculum/ degree programs
- Informal cooperation facilitates capability advances with greater flexibility and speed …
- …. BUT also creates single points of failure

Impact Examples of CMM Deployments in Europe

FYROM Around 70% of the CMM recommendations got incorporated into the NCS (adopted July 2018); the remaining ones will likely become part of the Action Plan (currently in the making).

Kyrgyz Republic Workshop with over 60 representatives of public sector and academia, topics incl. incident response and security teams, global cyber incident trends, cyber incidents in the finance sector; WB delivering targeted cybersecurity technical assistance for the Digital CASA-Kyrgyz Republic Project Implementation Unit.

Lithuania CMM results/recommendations were considered during the NCS drafting process and some of the recommendations turned into actions; national cybersecurity status report 2018 mentioned and gave reference to CMM assessment.

Cyprus Research collaboration of National Cyber Risk Management, start October 2018; signing of a Memorandum of Understanding on 15th October; we have identified and are in the process of arranging interviews with four people (all involved in Cyprus's risk assessment); Cyprus has shared their national risk-assessment methodology.

Going Forward

- Development of Cyber Harm Framework to assess and measure direct and indirect harms caused by cyber incidents
- Joint deployment of CMM and Cyber Harm Framework

  → results to facilitate **prioritisation of capacity investments** towards harm reduction
- CMM data analysis
- Consultation on CMM revision

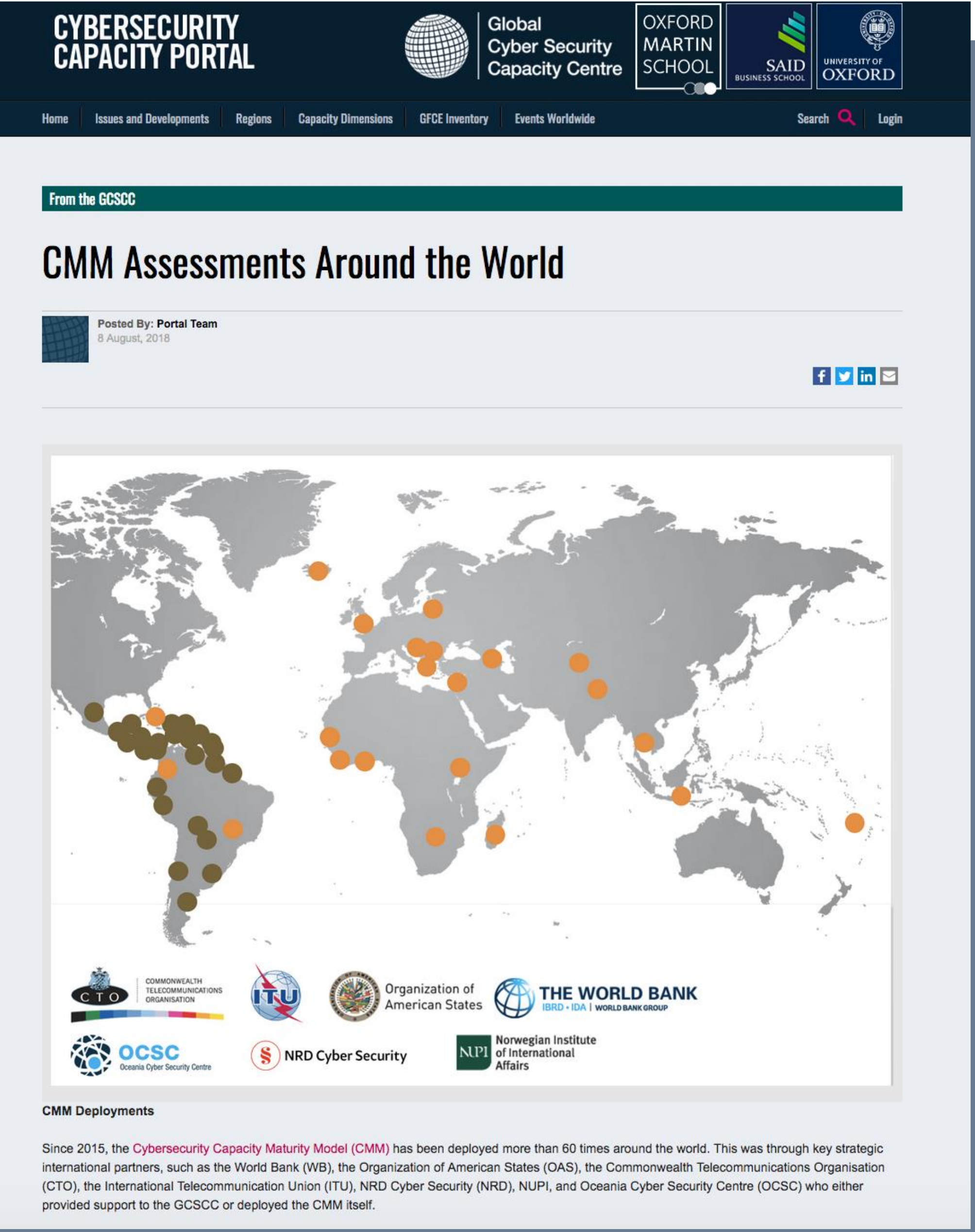
Annex

Cyber Harm Framework (CHF) - Overview

- Additionally, the Capacity Centre is developing a robust methodology for the measurement of harm in/from cyberspace.

- The **CHF** would expand the existing CMM with a methodological underpinning, backed up by a data collection framework, for relating cybersecurity capacity indicators to the areas in which harm might be reduced.

- The results shall facilitate **prioritisation of capacity investments** towards harm reduction.


CYBERSECURITY CAPACITY PORTAL
Global Cyber Security Capacity Centre
OXFORD MARTIN SCHOOL
SAID BUSINESS SCHOOL
UNIVERSITY OF OXFORD
Home
Issues and Developments
Regions
Capacity Dimensions
GFCE Inventory
Events Worldwide
Search
Login
COMMONWEALTH TELECOMMUNICATIONS ORGANISATION
CTO
ITU
Organization of American States
THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP
OCSC
Oceania Cyber Security Centre
NRD Cyber Security
NUPI
Norwegian Institute of International Affairs

From the GCSCC

CMM Assessments Around the World

Posted By: Portal Team
8 August, 2018

CMM Deployments

Since 2015, the Cybersecurity Capacity Maturity Model (CMM) has been deployed more than 60 times around the world. This was through key strategic international partners, such as the World Bank (WB), the Organization of American States (OAS), the Commonwealth Telecommunications Organisation (CTO), the International Telecommunication Union (ITU), NRD Cyber Security (NRD), NUPI, and Oceania Cyber Security Centre (OCSC) who either provided support to the GCSCC or deployed the CMM itself.

CMM Reports

Over 60 CMM reviews completed

31 single country reports by GCSCC completed or in progress:

2 Regional Reports completed or in progress by the OAS

Recent publications:

From the GCSCC

Sierra Leone: Cybersecurity Capacity...

From the GCSCC

FYR Macedonia: Cybersecurity Capacity...

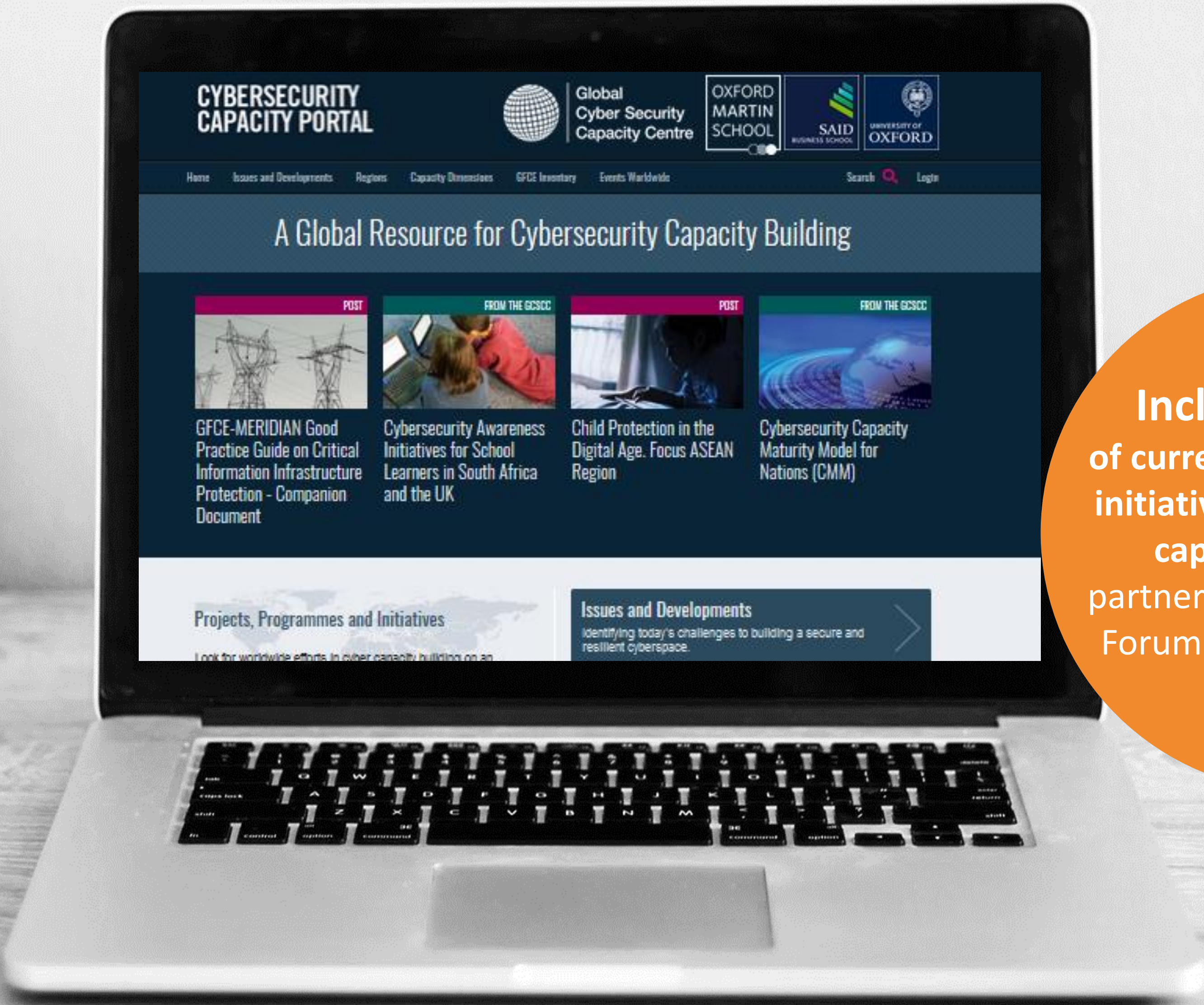
From the GCSCC

Iceland: Cybersecurity Capacity Review 2017

Visit: www.sbs.ox.ac.uk/cybersecurity-capacity to read the published reports

Cybersecurity Capacity Portal –
a global knowledge resource for Cybersecurity Capacity Building

www.sbs.ox.ac.uk/cybersecurity-capacity



CYBERSECURITY CAPACITY PORTAL

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

SAID BUSINESS SCHOOL

UNIVERSITY OF OXFORD

Home | Issues and Developments | Regions | Capacity Dimensions | GFCE Inventory | Events Worldwide | Search | Login

A Global Resource for Cybersecurity Capacity Building

POST
GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection - Companion Document

FROM THE GCSCC
Cybersecurity Awareness Initiatives for School Learners in South Africa and the UK

POST
Child Protection in the Digital Age. Focus ASEAN Region

FROM THE GCSCC
Cybersecurity Capacity Maturity Model for Nations (CMM)

Projects, Programmes and Initiatives

Look for worldwide efforts in cyber capacity building on an

Issues and Developments

Identifying today's challenges to building a secure and resilient cyberspace.

Incl an Inventory
of current intl and regional initiatives in cybersecurity capacity building –
partnership with the Global Forum on Cyber Expertise (GFCE)

Thank you!

Global
Cyber Security
Capacity Centre

www.oxfordmartin.ox.ac.uk/cybersecurity

@CapacityCentre

https://www.linkedin.com/company/
global-cyber-security-capacity-centre/