Cybersecurity Capacity Maturity Model for Nations (CMM)

Structure and Deployment Methodology

GFCE V-Meeting, 28 April 2020

Global Cyber Security Capacity Centre

C3SA

OCSC Oceania Cyber Security Centre

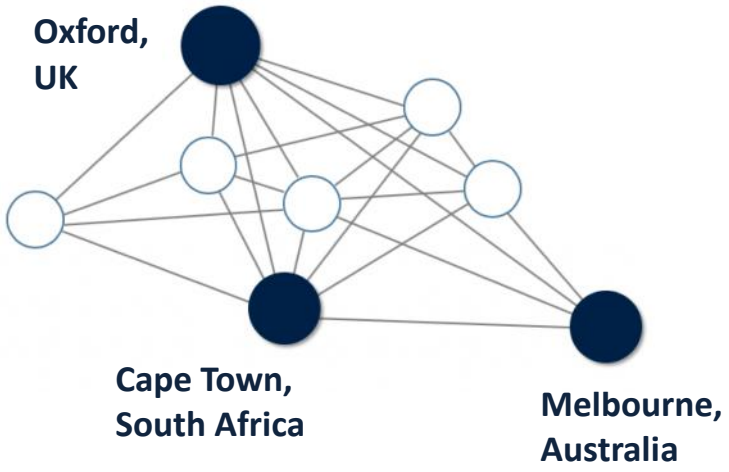
OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

Global Cyber Security Capacity Centre (GCSCC)

- A leading international **research centre in cybersecurity capacity-building** at the University of Oxford.
- Research into **what works and is effective** cybersecurity capacity development.
- The GCSCC brings together **international expertise across multiple sectors and disciplines** from across the world to contribute to its outputs.
- Promoting an **increase in the scale, pace, quality and impact** of cybersecurity capacity-building initiatives across the world.

Constellation of Regional Cybersecurity Capacity Research Centres



- Embedded in established and leading research institutions to develop a **regional body of cybersecurity research**
- Fostering **multidisciplinary research** on efficient and effective cybersecurity capacity-building worldwide
- Leading to a **deeper understanding of what constitutes national-level cybersecurity capacity** in the regions and of the context of cybersecurity
- Ensure the CMM's **regional ownership** and the **sustainable global impact**
- Drive the development of **regionally informed** cybersecurity capacity-building initiatives

Global Cyber Security Capacity Centre

C3SA
Cybersecurity Capacity Centre for Southern Africa

OCSC
Oceania Cyber Security Centre

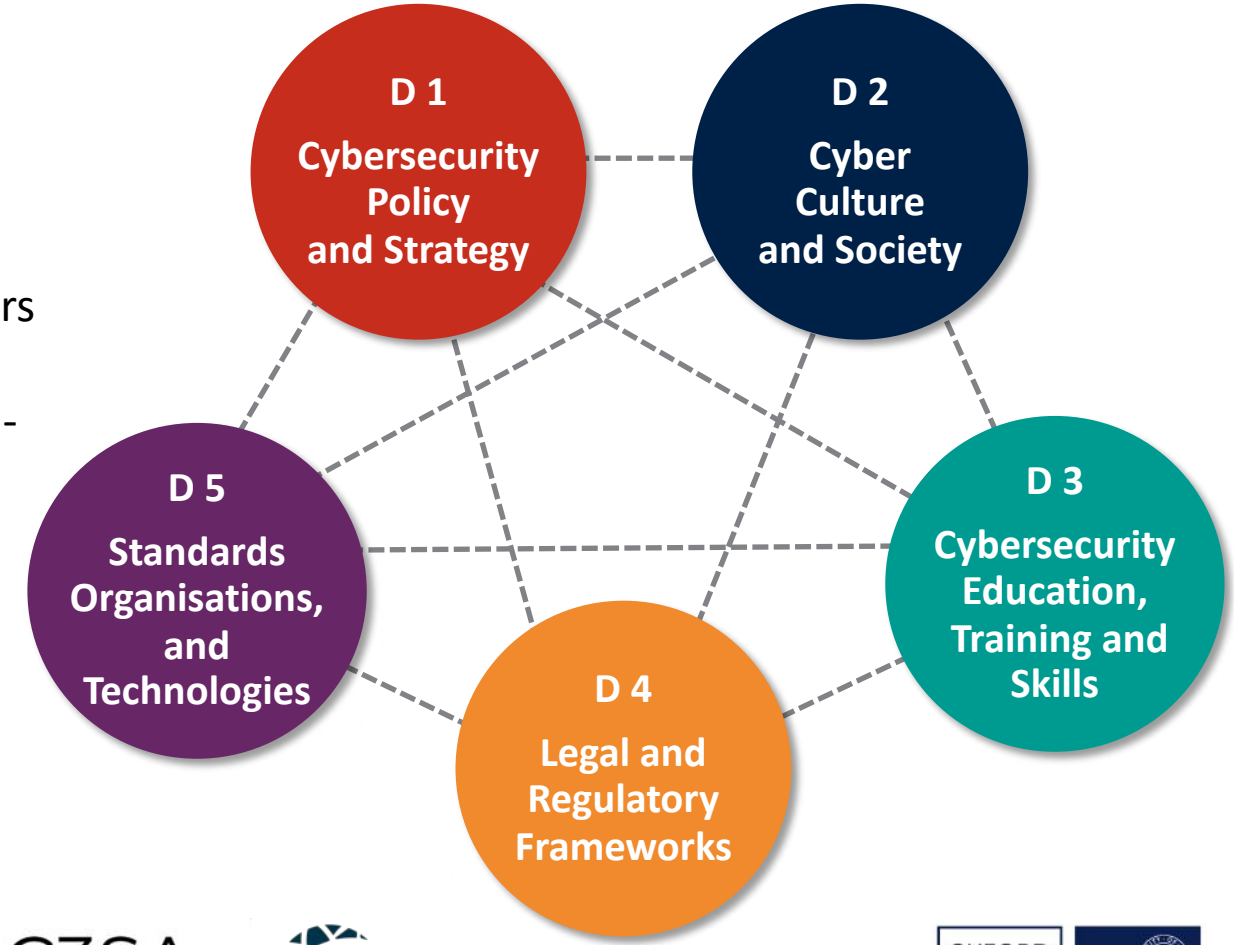
OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

Cybersecurity Capacity Maturity Model for Nations (CMM)

https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20revised%20edition_09022017_1.pdf

- a model suitable for self-assessment of current capacity, spanning five dimensions and 24 Factors including over 200 indicators
- developed in a global multi-stakeholder consultation process
- creating a comprehensive benchmark of current position and how to increase maturity.



Global Cyber Security Capacity Centre

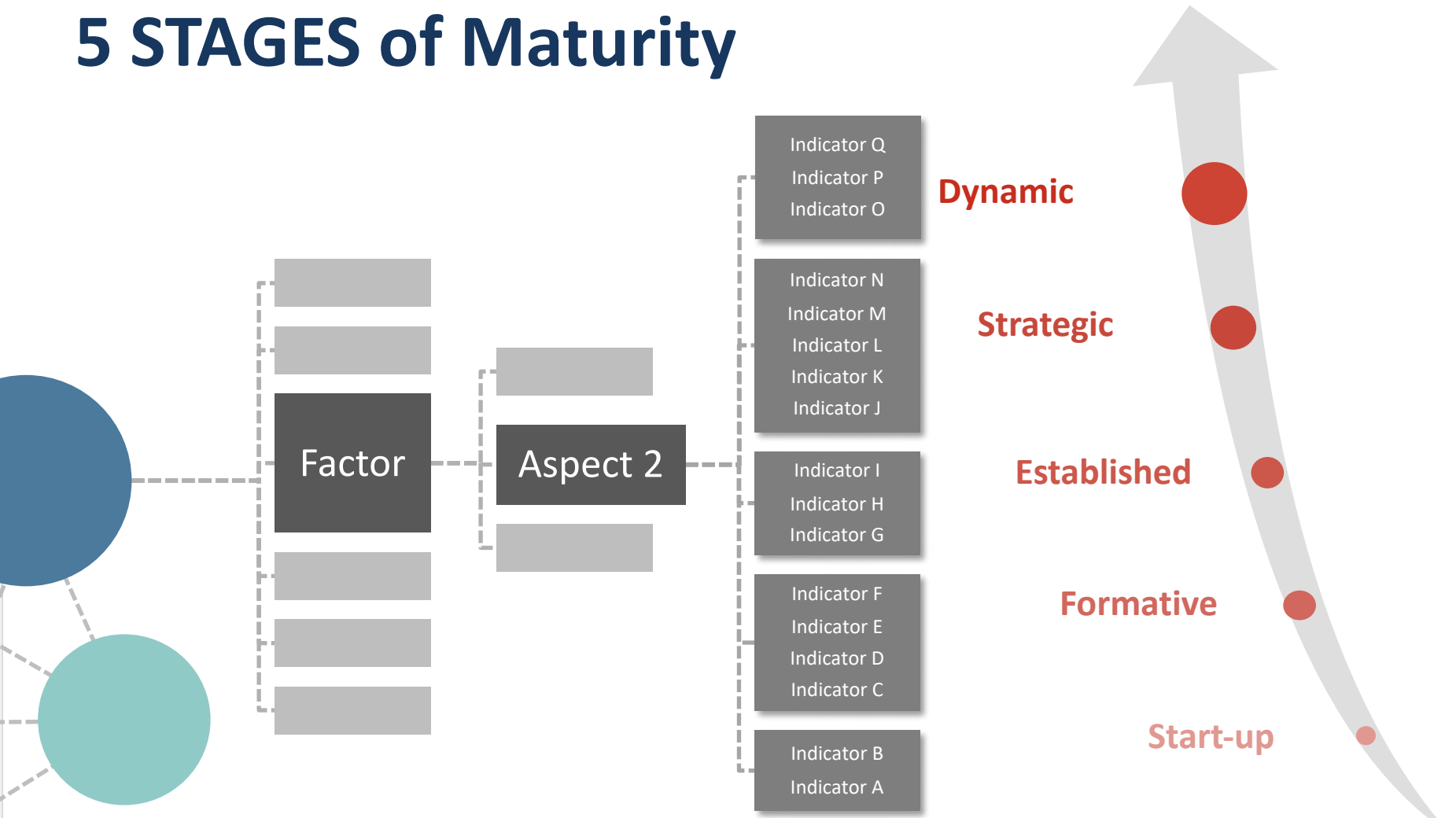
C3SA Cybersecurity Capacity Centre for Southern Africa

OCSC Oceania Cyber Security Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

5 STAGES of Maturity



Example:
LEGAL AND REGULATORY FRAMEWORKS

Dimension 4

D4 FACTOR
D4.1 Legal Frameworks

D4.1 ASPECT
Legislative Framework for ICT Security

Aspect INDICACTORS

Start-up	Formative	Established	Strategic	Dynamic
Legislation relating to ICT security does not yet exist. Efforts to draw attention to the need to create a legal framework on cybersecurity have been made and may have resulted in a gap analysis.	Experienced stakeholders from all sectors may have been consulted to support the establishment of a legal and regulatory framework. Key priorities for creating cybersecurity legal frameworks have been identified through multi-stakeholder consultation, potentially resulting in draft legislation, but legislation has not yet been adopted	Comprehensive ICT legislative and regulatory frameworks addressing cybersecurity have been adopted. Laws address the protection of critical information infrastructure, e-transactions, liability of Internet Service Providers and, potentially, cyber incident reporting obligations.	The country reviews existing legal and regulatory mechanisms for ICT security, identifies where gaps and overlaps exist, and amends laws accordingly or enacts new laws. Monitoring of enforcement of legislative frameworks informs resource allocation and legal reform	Mechanisms are in place for continuously harmonising ICT legal frameworks with national cybersecurity-related ICT policies, international law, standards and good practices. Participation in the development of regional or international cybersecurity cooperation agreements and treaties is a priority. Efforts are in place to exceed minimal baselines specified in these treaties where appropriate.

CMM Deployment Methodology

- In-country **focus-group discussions** with key stakeholders from multiple sectors
- Usually 10 sessions over 3 days, each covering 2 Dimensions
- Research team from the GCSCC or its partners who have undergone detailed training on the methodology
- An interactive deployment tool makes it possible to identify current stage of maturity according to the CMM

Global Cyber Security Capacity Centre

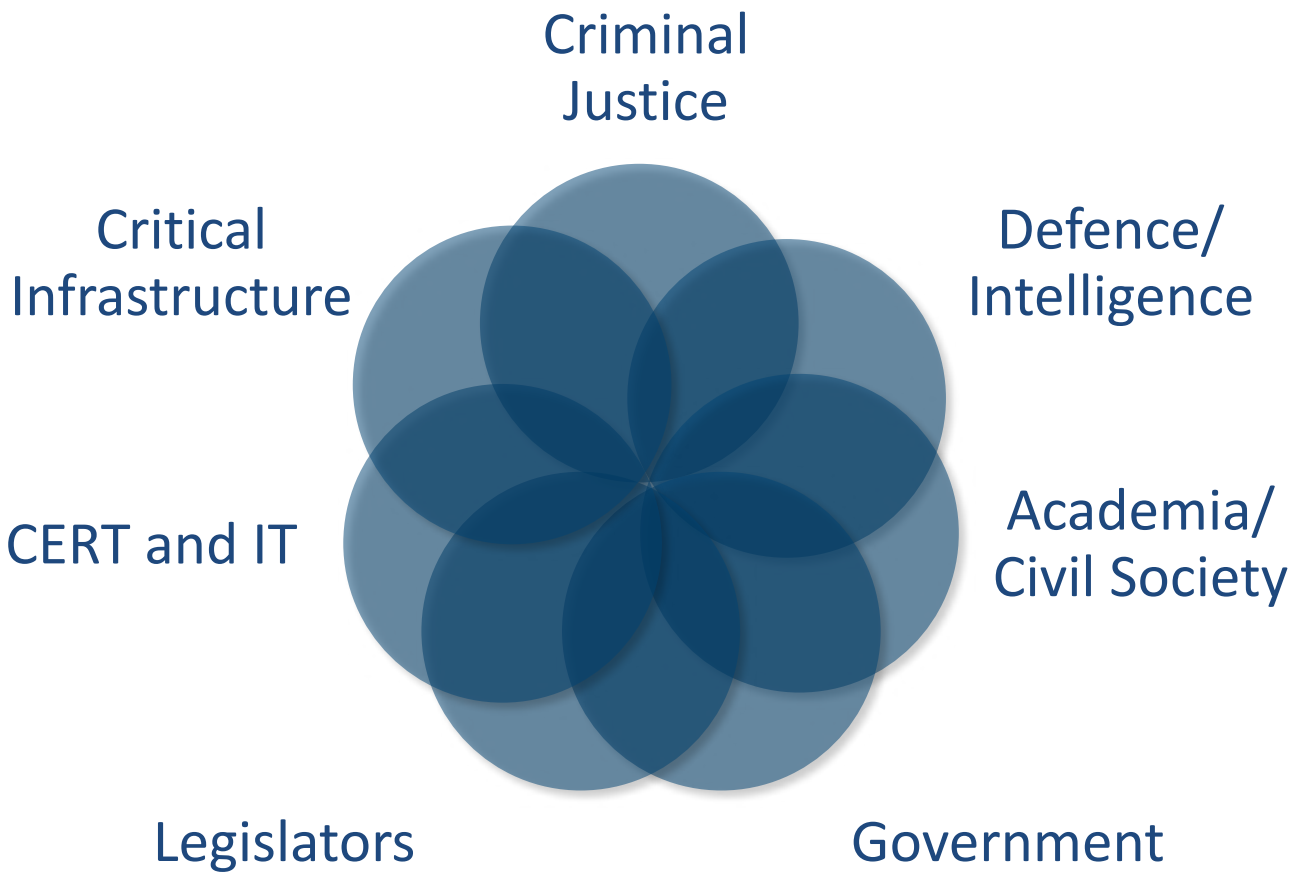
C3SA
Cybersecurity Capacity Centre for Southern Africa

OCSC
Oceania Cyber Security Centre

OXFORD MARTIN SCHOOL

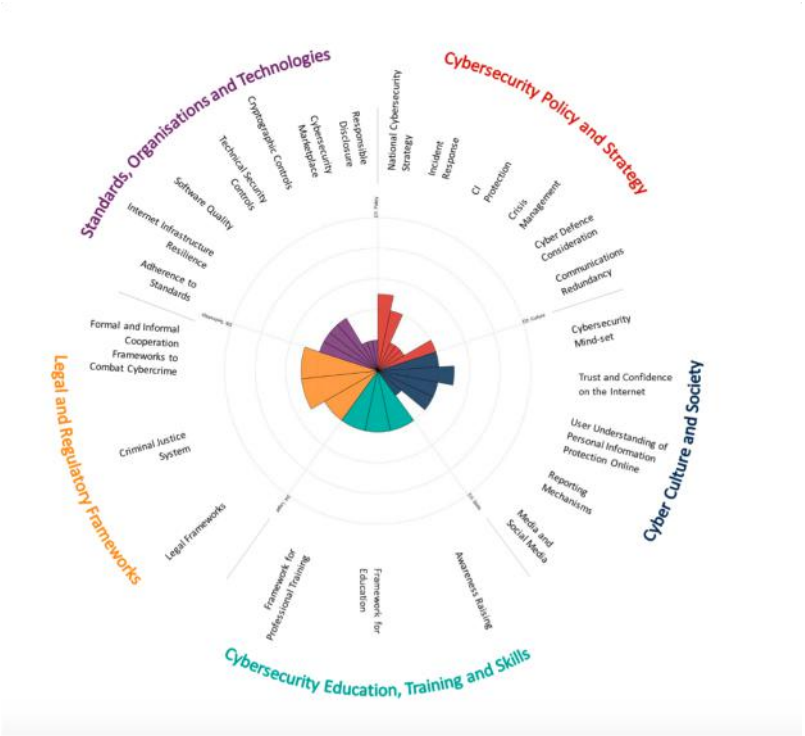
UNIVERSITY OF OXFORD

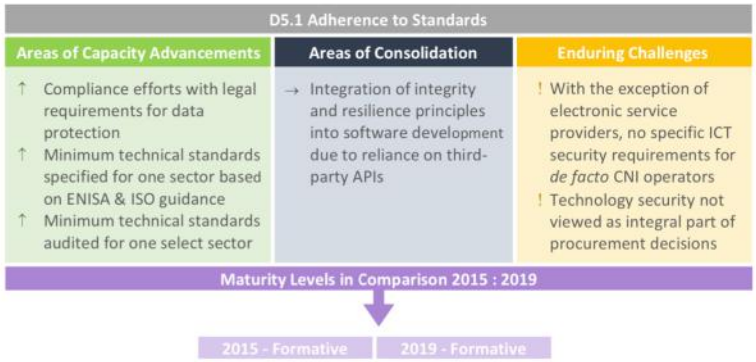
Stakeholder Clusters



Output and Benefits

- Review of cybersecurity capacity across five dimensions
- Stage of maturity per factor (not one single score for a country, no ranking)
- Ownership of review lies with country
- Self-assessment to point out needs and next steps
- Qualitative and quantitative benchmarking
- Detailed CMM review report with recommendations





Global Cyber Security Capacity Centre

C3SA Cybersecurity Capacity Centre for Southern Africa

OCSC Oceania Cyber Security Centre

OXFORD MARTIN SCHOOL

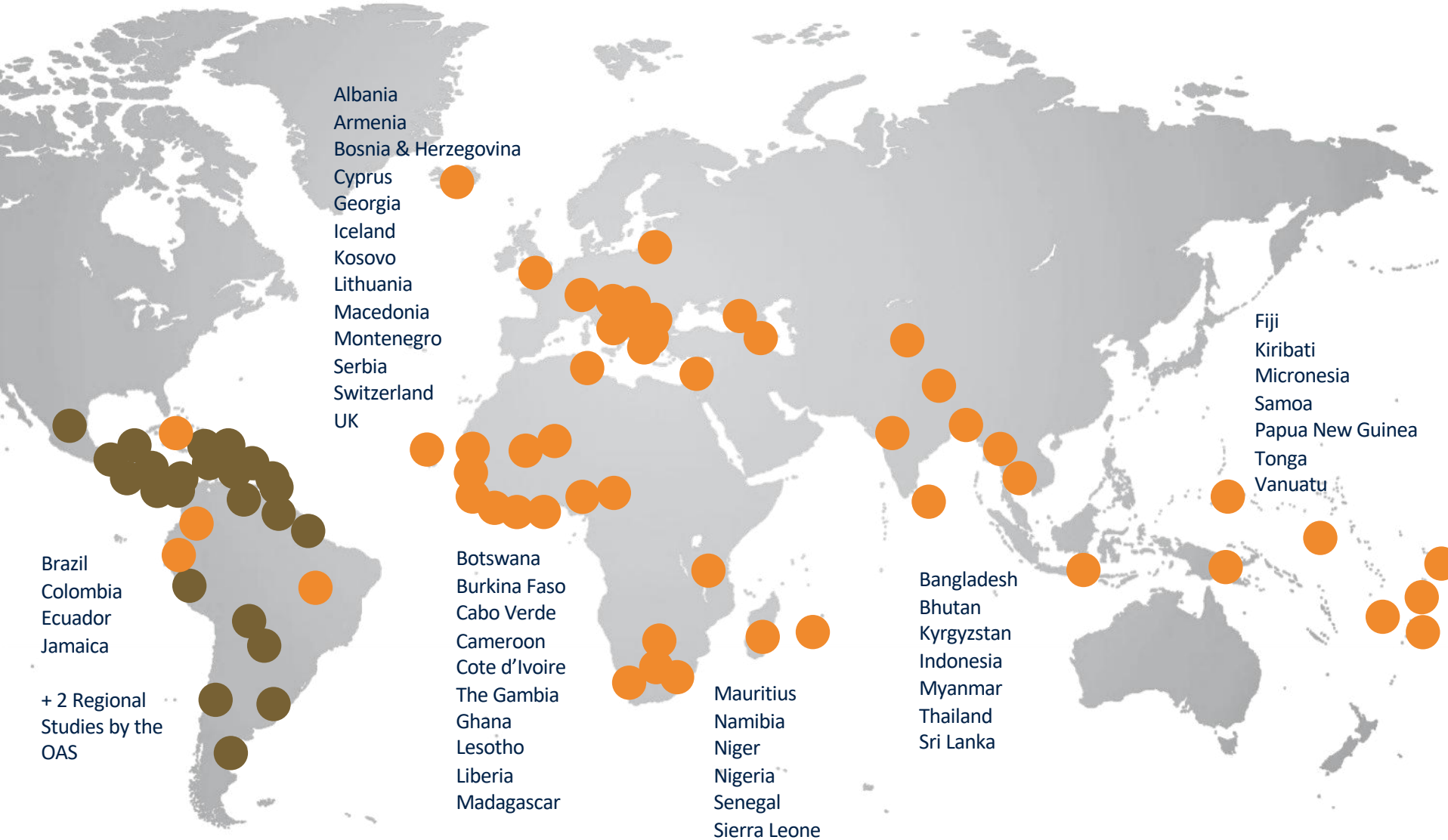
UNIVERSITY OF OXFORD

End-user Value and Capacity-building Impact

- A CMM review drives enhanced awareness and capacity-building in the area of cybersecurity
- Countries have cited the CMM as foundational to their NCS
- A review enhances internal credibility of cybersecurity agenda within governments
- Helps define roles and responsibilities within government
- Has resulted increased funding for cybersecurity capacity-building

GCSCC Strategic & Implementation Partners

Over 80 National Cybersecurity Capacity Reviews



Status: January 2020