Cyber security capacity building:
Digging the foundations for privacy

Chris Mitchell

www.chrismitchell.net

Data protection and cyber security

- Data protection is about protecting the privacy of the individual.
- This means that PII (Personally Identifiable Information), wherever it is collected, stored, used and communicated, needs to be protected in a variety of ways.
- That is, part of supporting data protection is about providing security …

Security underpins privacy

- Specifically, a key aspect of data protection is maintaining the:
  - confidentiality;
  - integrity; and
  - accountability

  of the collection. storage and use of PII.
- That is, data protection fundamentally depends on cyber security.
- Indeed, this is the main theme of Chapter IV of the draft data protection regulation.

An example – ISO/IEC 27018

- ISO/IEC 27018, published in 2014 (and edited by CM), is the first in a new generation of privacy-focussing 27000-series standards.
- It is concerned with the auditable services that must be provided by a cloud service provider when it acts as a PII processor.
- It builds on the Article 29 Data Protection Working Party *Opinion 05/2012 on Cloud Computing*
- It extends ISO/IEC 27002 to deal specifically with the cloud PII processor privacy issue.
- Many of the privacy-specific measures in ISO/IEC 27018 are security-focussed.

Privacy – a cultural phenomenon

- Europe has led the way in developing regulations designed to protect end user privacy.
- Around the world, nations and regions are at very different stages of developing privacy-protecting regulation and legislation.
- Partly this relates to the level of development, but partly also to cultural attitudes to privacy.
- However, many things need to be in place for effective data protection.

Privacy – building the agenda

- One key piece of the data protection puzzle is enabling effective cyber security.
- Without security, privacy cannot be effectively implemented.
- Internationally, one obstacle to providing appropriate cyber protection is lack of capability, including knowledge, skill and culture.
- This leads to main focus …

- … the UK-based *Global Cyber Security Capacity Centre* is intended to help foster development of cyber security capabilities internationally.
- In the remainder of this presentation I will summarise the main work programme of the centre, and what it has achieved so far.

Funded by UK Foreign & Commonwealth Office

- remit is to be *authoritative*, *independent* and *global*
- initial funding for 2 years (to 2015), but longer-term ambitions

Led by Sadie Creese from University of Oxford

- along with 10 other leading academics from the UK, continental Europe and Africa (including CM)

Hosted by Oxford Martin School

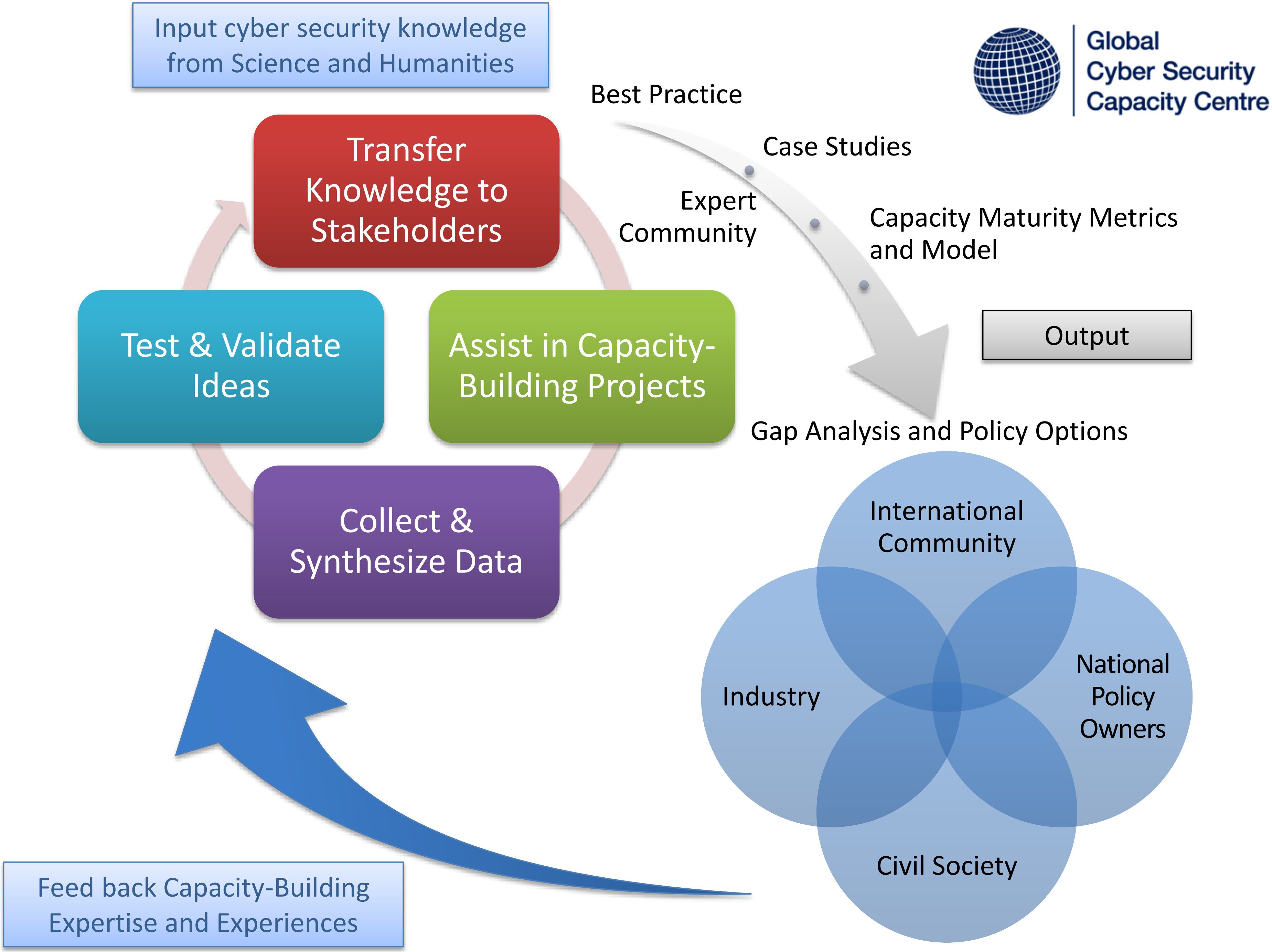
Motivation

- Desire to increase the scale, pace and impact of global cyber-security capacity-building …
  - all countries need the capacity to tackle online threats and reduce harm, and are interdependent upon each other for success
  - while ensuring that cyberspace supports innovation, economic growth and social benefits, and respects individual privacy
  - global nature of cyberspace and interdependencies between regions make collaboration necessary
- … but little consensus on what constitutes good practice
  - need to be able to measure status and progress
  - require scientific basis for policy and development

Objectives

- develop the framework within which to measure and understand national capacity in cyber security
- creating and maintaining a critical guide to global expertise on cyber security
- setting out what needs to be done to close gaps in the global response
  - analysis of priorities, identification of gaps
- identifying what works, what doesn’t, and why
- promote and so increase the supply of effective capacity building

Global
Cyber Security
Capacity Centre



Input cyber security knowledge from Science and Humanities

Transfer Knowledge to Stakeholders

Test & Validate Ideas

Assist in Capacity-Building Projects

Collect & Synthesize Data

Best Practice

Case Studies

Expert Community

Capacity Maturity Metrics and Model

Output

Gap Analysis and Policy Options

International Community

Industry

National Policy Owners

Civil Society

Feed back Capacity-Building Expertise and Experiences

Need to measure current state and establish priorities

- science requires measurement
  - or we’re just shooting in the dark
- main effort is devoted to devising a model against which countries (or regions) can measure themselves
- drawing on, not competing with, other similar efforts
  - ITU Global Cybersecurity Index
  - WEF Global Information Technology Report
  - ENISA Guidelines
  - …

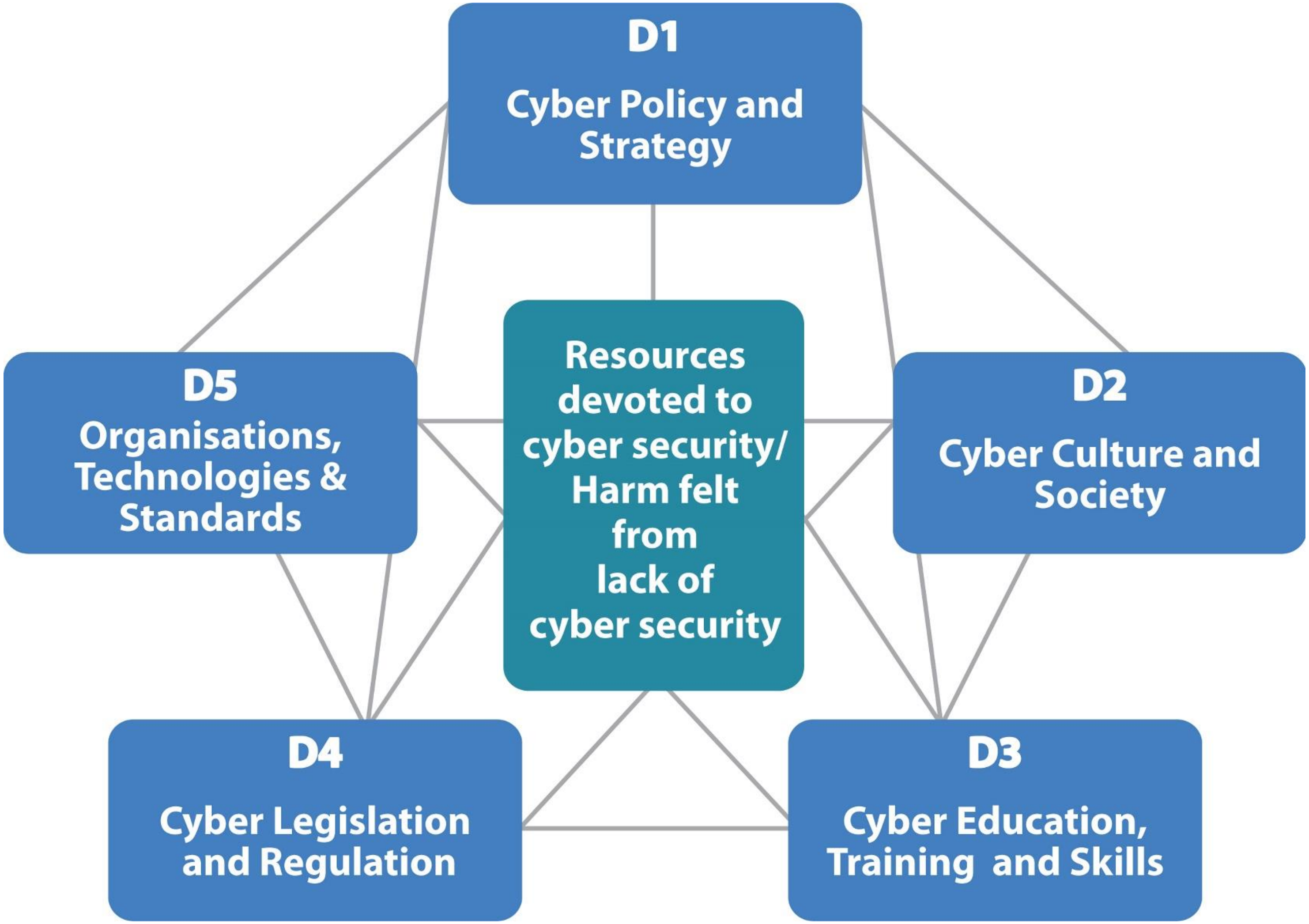
Five complementary dimensions of cyber security capacity:

1. devising national cyber policy and cyber defence
2. encouraging responsible cyber culture within society
3. building cyber skills into the workforce and leadership
4. creating effective legal and regulatory frameworks
5. controlling risks through technology and processes

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD



D1

Cyber Policy and Strategy

D2

Cyber Culture and Society

D3

Cyber Education, Training and Skills

D4

Cyber Legislation and Regulation

D5

Organisations, Technologies & Standards

Resources devoted to cyber security/ Harm felt from lack of cyber security

GCSCC – organisation

- each dimension chaired by two academics
  - ensuring availability and diversity of viewpoint
- backed by broader Working Group
  - drawn from academia, industry, governmental and trans-governmental bodies
  - *pro bono* contributions, only limited expenses
- dedicated staff
  - three Research Fellows shared among dimensions
  - one knowledge-transfer professional
  - a number of graduate interns over both summers
  - secretariat and logistic support from Martin School

Key Output: Capability Maturity Model

- derive science-based, evidence-driven metrics
- gather best-practice from around the world …
- … along with what has been shown not to work
- in order to facilitate:
  - bench-marking nations and regions
  - identifying policy options for capacity growth
  - understand impact of policy across different areas of capacity

Capability Maturity Model – factors:

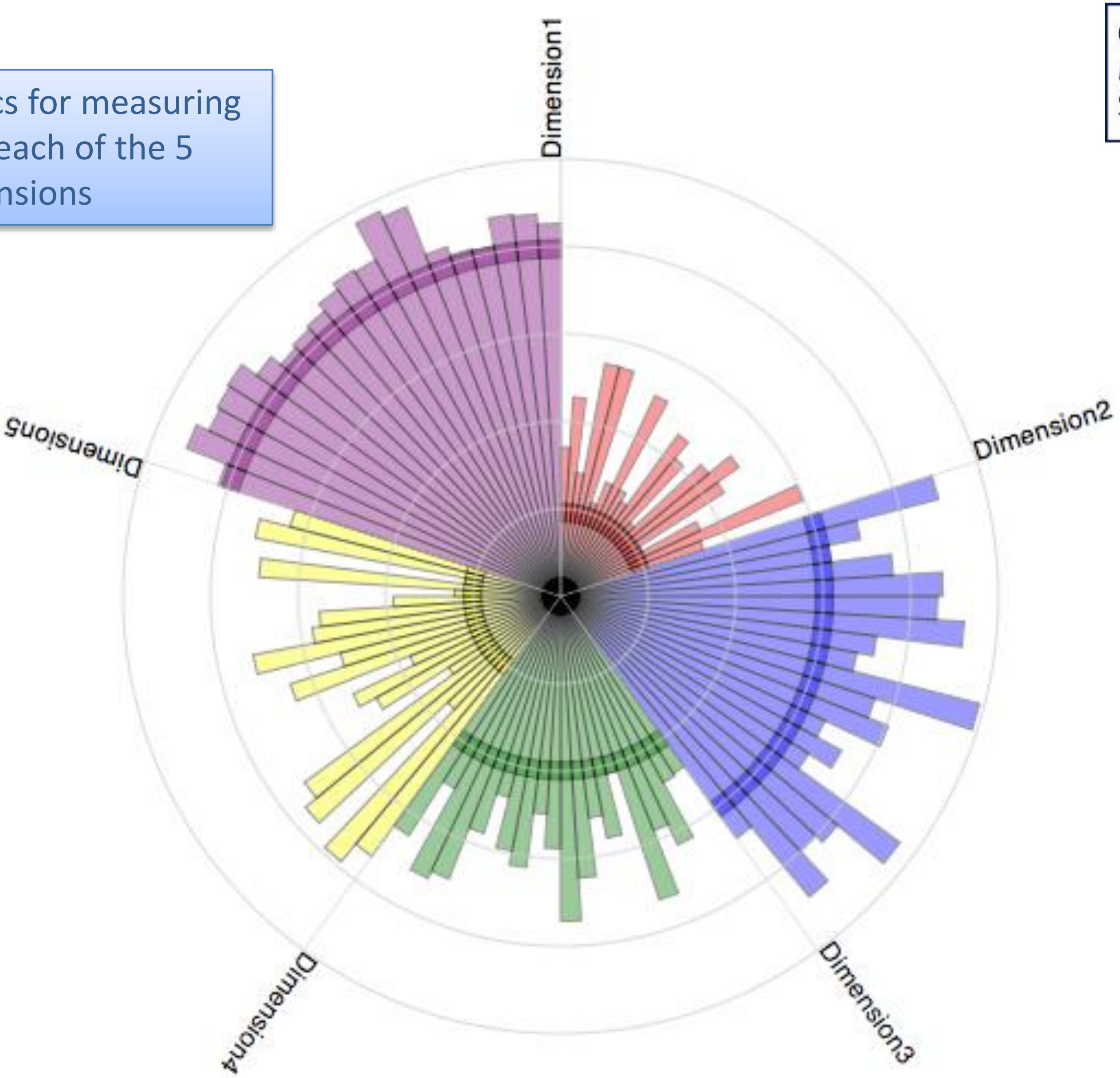
- within each of the five dimensions, a series of key *factors* have been identified
- these key topics capture the state of development of cyber security within each dimension
- by measuring level of development for each factor, we get a picture of overall maturity level for cyber security within the country/region/domain.

Capability Maturity Model – maturity levels

- designed to serve as a self-assessment tool to underpin needs assessment and strategy
- will also enable richer benchmarking than currently available – qualitative and quantitative
- increase levels of cyber capacity across the five dimensions using five levels of maturity:

Start-Up / Formative / Established / Strategic / Dynamic

Multiple metrics for measuring maturity in each of the 5 dimensions



5 levels of maturity, solid bands indicating minimum level across all metrics for any particular dimension

Oxford Centre Capacity Dimensions

Dimension 1

Cyber Security Policy and Strategy

D1-1: National Cyber Security Strategy

D1-2: Incident Response

D1-3: Critical National Infrastructure (CNI) Protection

D1-4: Crisis Management

D1-5: Cyber Defence Consideration

D1-6: Digital Redundancy

Dimension 2

Cyber culture and society

D2-1: Cyber Security Mind-set

D2-2: Cyber security Awareness

D2-3: Confidence and trust on the Internet

D2-4: Privacy online

Dimension 3

Cyber security education, training and skills

D3-1: National availability of cyber education and training

D3 -2: National development of cyber security education

D3-3: Corporate training and educational initiatives within companies

D3-4: Corporate Governance, Knowledge and Standards

Dimension 4

Legal and regulatory frameworks

D4-1: Cyber security legal frameworks

D4-2: Legal investigation

D4-3: Responsible Disclosure

Dimension 5

Standards, organisations, and technologies

D5-1: Adherence to standards

D5-2: Cyber security coordinating organisations

D5-3: Cyber Security marketplace

D5-4: National Infrastructure Resilience

Not Simply a Classification Scheme

- the CMM looks deeper into causes and core issues
  - for example, there is no ‘Cyber Crime’ dimension, because Cyber Crime is an effect, not a cause
- the CMM will help governments and organisations
  - to engage across the variety of stakeholders involved
    - breaking down silos
  - to develop policies that create long-lasting impact
    - by tackling underlying root causes

No Intellectual-Property Restrictions

- anyone can use the CMM for free
  - outputs will be published on the centre website
- neither the Centre nor Oxford ‘own’ it
  - rather, by working collaboratively and open-sourcing its findings along the way the GCSCC hopes to make contribute something valuable to the international cyber security community

Developing the model – methodology

Aim

- To pilot the CMM and understand the application process, with a view to improve the tool for self assessment.

Tool

- The application tool used for the collection of data is premised and reflects the indicators of the Model.

Stakeholders

- Stakeholders from: across government, law enforcement, private sector, business, academia and the technical community

Capability Maturity Model – status

- initial selection of factors finalised
- first version of model now being used in series of pilots arranged jointly with high-profile collaborative partners:
  - Organization of American States (OAS);
  - World Bank.

Capability Maturity Model – collaborations - OAS

- OAS are mapping Cyber Security capacity across the Latin Americas and Caribbean region, in a joint project with the Inter-American Development Bank.
- they have chosen to work with the CMM, and the GCSCC has collaborated to develop an application tool (essentially a survey) specifically for their membership.
- OAS have taken ownership of this tool and are driving the roll out of the CMM.
- publicly available report of the OAS study will be published in the third quarter of 2015.

Capability Maturity Model – collaborations – World Bank (WB)

- WB are working with GCSCC to pilot the CMM across countries they are engaged with using an application tool tailored for the WB members.
- The GCSCC is leading on the assessments/data collection as well as both the government and academic outputs
- The goal of the WB is to establish their own capacity to measure Cyber security (using the GCSCC model), so in future they can independently carry out maturity assessments, with remote support from GCSCC

Capability Maturity Model – pilots

- pilots with Organisation of American States
  - **Jamaica**: 22/23 January 2015;
  - **Columbia**: 29/30 January 2015;
  - on-line remote self-assessment roll out to all OAS member states later in 2015
- pilots with World Bank
  - **Armenia**: 2/3/4 February 2015;
  - **Kosovo**: 9/10/11 February 2015;

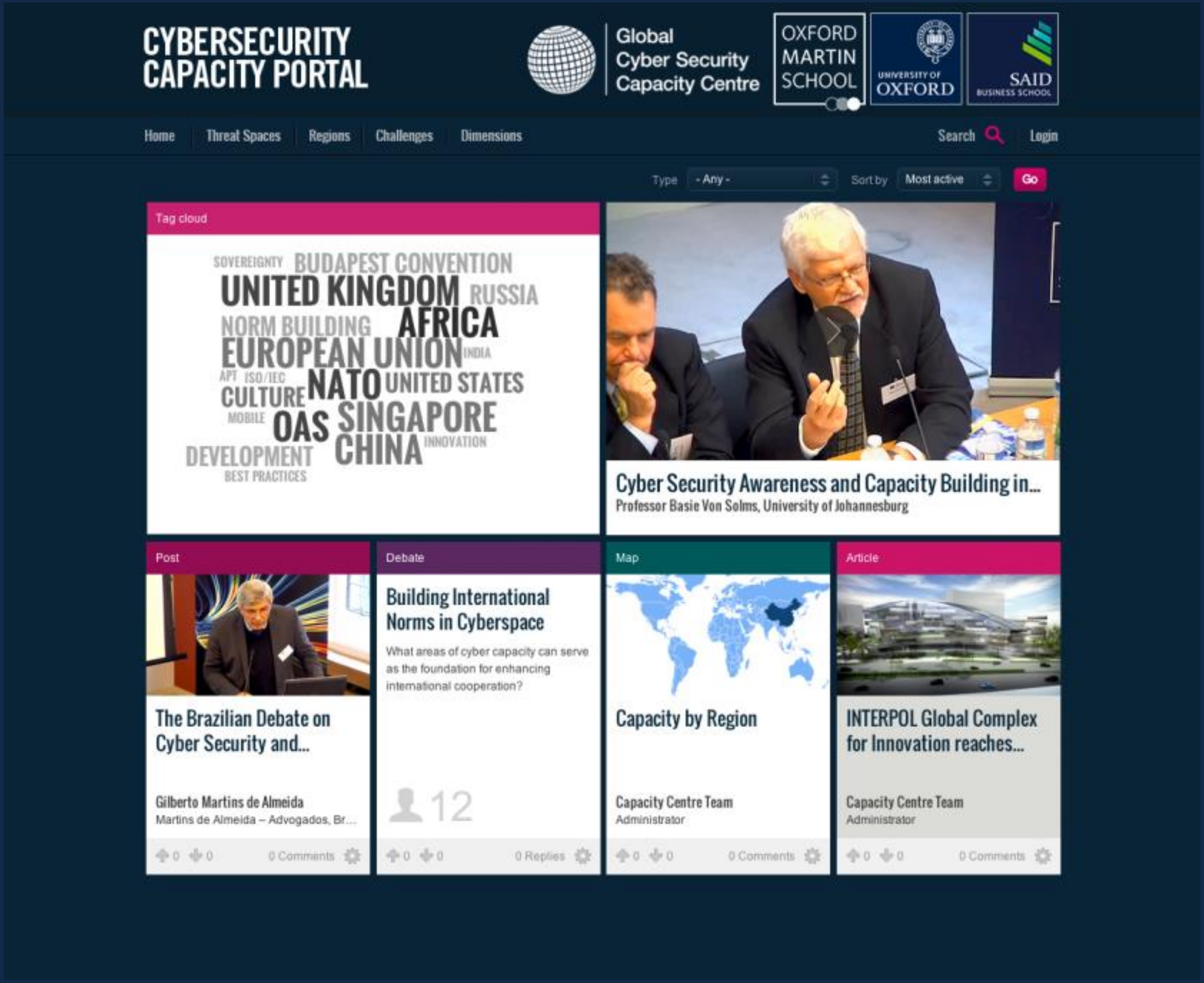
  - more to follow.

Capability Maturity Model – pilot outcomes

- Two distinct outputs expected from pilots:
  - report for relevant government outlining their cyber security maturity, and recommendations for moving forward
  - an academic output, describing our greater understanding of the interdependencies of Cyber Capacity building, and how to increase its pace, impact and sustainability

Cyber Security Capacity Portal

- aimed at both recipients and suppliers of capacity building in cyber security
- connects to knowledge and experience around the global community – linked into the CMM
- built on platform developed by SBS for education
- http://www.sbs.ox.ac.uk/cybersecurity-capacity/explore/home



CYBERSECURITY CAPACITY PORTAL

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

SAID BUSINESS SCHOOL

Home | Threat Spaces | Regions | Challenges | Dimensions | Search | Login

Type: - Any - | Sort by: Most active | Go

Tag cloud

SOVEREIGNTY BUDAPEST CONVENTION UNITED KINGDOM RUSSIA NORM BUILDING AFRICA EUROPEAN UNION INDIA APT ISO/IEC CULTURE NATO UNITED STATES MOBILE OAS SINGAPORE DEVELOPMENT CHINA INNOVATION BEST PRACTICES

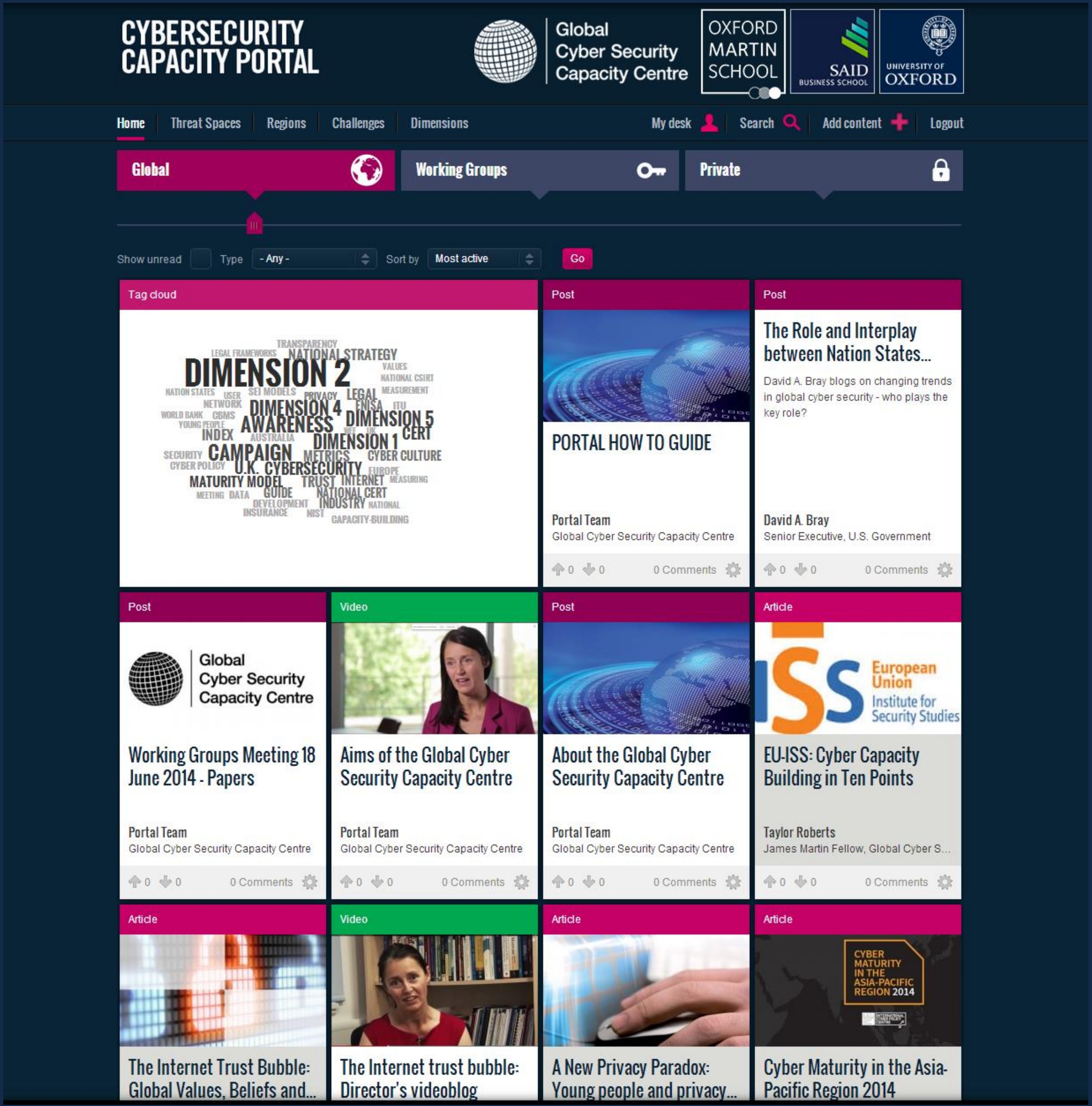
Cyber Security Awareness and Capacity Building in...
Professor Basie Von Solms, University of Johannesburg

Post
The Brazilian Debate on Cyber Security and...
Gilberto Martins de Almeida
Martins de Almeida – Advogados, Br...
0 0 · 0 Comments

Debate
Building International Norms in Cyberspace
What areas of cyber capacity can serve as the foundation for enhancing international cooperation?
12
0 0 · 0 Replies

Map
Capacity by Region
Capacity Centre Team
Administrator
0 0 · 0 Comments

Article
INTERPOL Global Complex for Innovation reaches...
Capacity Centre Team
Administrator
0 0 · 0 Comments



Show unread □ Type - Any - Sort by Most active

Tag cloud

Post

PORTAL HOW TO GUIDE

Portal Team
Global Cyber Security Capacity Centre

0 0 0 Comments

Post

The Role and Interplay between Nation States...

David A. Bray blogs on changing trends in global cyber security - who plays the key role?

David A. Bray
Senior Executive, U.S. Government

0 0 0 Comments

Post

Working Groups Meeting 18 June 2014 - Papers

Portal Team
Global Cyber Security Capacity Centre

0 0 0 Comments

Video

Aims of the Global Cyber Security Capacity Centre

Portal Team
Global Cyber Security Capacity Centre

0 0 0 Comments

Post

About the Global Cyber Security Capacity Centre

Portal Team
Global Cyber Security Capacity Centre

0 0 0 Comments

Article

EU-ISS: Cyber Capacity Building in Ten Points

Taylor Roberts
James Martin Fellow, Global Cyber S...

0 0 0 Comments

Article

The Internet Trust Bubble: Global Values, Beliefs and...

Video

The Internet trust bubble: Director's videoblog

Article

A New Privacy Paradox: Young people and privacy...

Article

Cyber Maturity in the Asia-Pacific Region 2014

Cyber security capacity building

Chris Mitchell

www.chrismitchell.net