Cyber security capacity governance

Professor Basie von Solms
Centre for Cyber Security
University of Johannesburg, South Africa

Professor David Upton
American Standard Companies Professor of Operations Management
Saïd Business School
University of Oxford, United Kingdom

Keywords
Cyber Security, Capacity Building, Maturity Model, Global Cyber Security Capacity Centre, Oxford

Extended Abstract

1. Introduction

There are many definitions and approaches to Cyber (Security) Capacity Building (CCB) and in general it is agreed that such capacity goes far beyond merely building technical cyber security capacity. It is also important: '*cyber capacity building is not only about security – it impacts on social and economic development worldwide*' (European Union, 2014).

CCB is a multi-disciplinary concept which impacts economic, social, legal and regulatory developments involving different stakeholders from Government, private sector, academia and civil society - is therefore much more than creating a group of technical oriented cyber security professionals.

'*Capacity building in cyberspace should follow a multi-level governance process encompassing (efforts) across government departments, private actors, and civil society*'. (European Union, 2013).

'*The importance of capacity building in cyberspace is increasingly acknowledged by governments, international organizations and the private sector*' (European Union, 2014).

The International Telecommunications Union (ITU) of the UN has included Cyber Capacity Building as one of the core pillars of its Global Cybersecurity Agenda (GCA), and emphasises its integration with the other core pillars (ITU, 2007). The ITU defines this pillar as ' *the development of a global strategy to facilitate human and institutional capacity building to enhance knowledge and know-how across the sectors and amongst the players.* '

Figure 1 below indicates this integration.

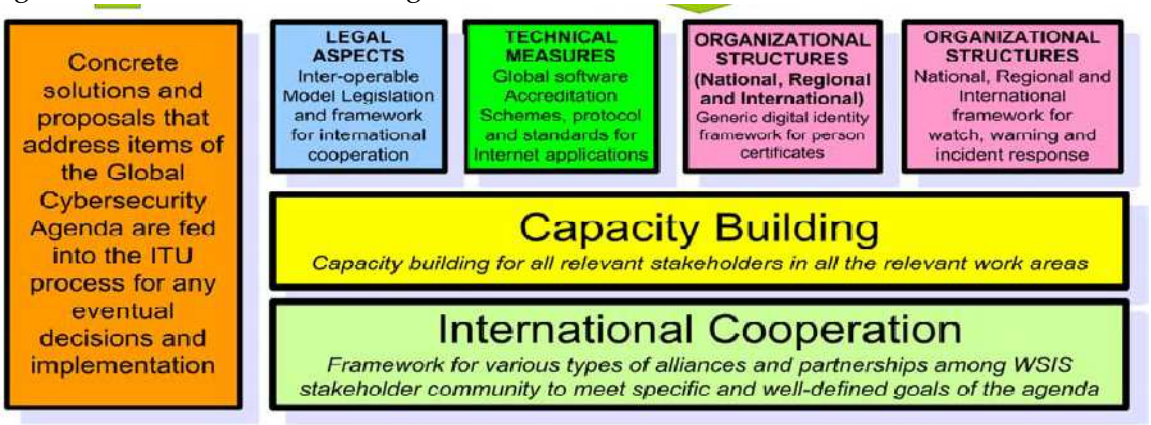


Figure 1

From Figure 1 it is clear that Capacity Building forms the foundation of the pillars of Legal aspects, Technical Measures and Organizational Structures.

Cyber (Security) Capacity Governance is the way in which Cyber Security Capacity Building (CCB) is managed and governed in a country. Of course, as in any governance process, for Cyber (Security) Capacity Governance the concept of measurement, metrics and compliance enforcement as far as CCB is concerned, is crucial. Some mechanism is therefore needed to establish the level of maturity of CCB in a specific country. Determining and measuring how far the CCB process has advanced and what measures are needed to move to the next level is core to the idea of Cyber (Security) Capacity Governance.

Presently there are a number of measurement tools/mechanisms available to determine the status of a country's CCB, and without such a determination, proper Cyber Capacity Building Governance is not possible. However, they are generally not comprehensive, and are focused on a particular element. They are also not progressive – in the sense that they do not establish the degree of maturity, and identify the next level that a country might strive for.

The Cybersecurity Capacity Maturity Model (CMM) of the Global Cybersecurity Capacity Centre (GCSCC) of the University of Oxford [GCSCC, 2016)] is a powerful measurement approach and is therefore extremely valuable as far as Cyber (Security) Capacity Governance is concerned. It draws on much of the extant work, as well as a worldwide panel of experts and stakeholders to inform the model.

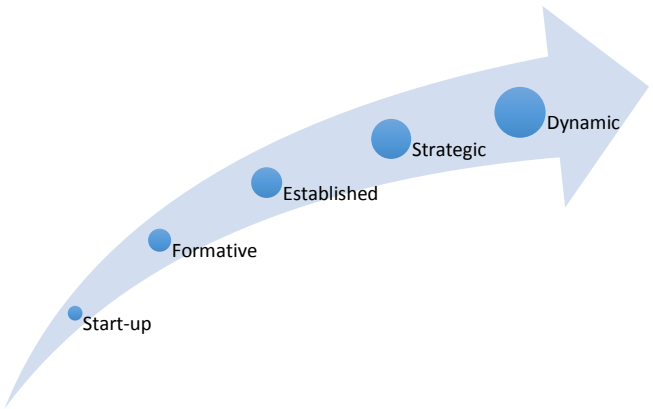
It is designed to serve as a (self)-assesment tool to underpin needs assessment and strategy, to enable richer benchmarking (both qualitative and quantitative) and ultimately to increase levels of cyber capacity across the five dimensions described below.

2. The Cyber Security Capacity Maturity Model (CMM) of the Global Cybersecurity Capacity Centre (GSCCC) of the University of Oxford

The Cybersecurity Capacity Maturity Model (CMM) of the Global Cybersecurity Capacity Centre (GCSCC) of the University of Oxford is a measurement approach which evaluates the cyber security capacity building status of a country over 5 different dimensions. Within each Dimension the status can be one of 5 maturity levels (see Figure 2). These 5 maturity levels are:

Maturity Level 1 : Start up
Maturity Level 2 : Formative
Maturity Level 3 : Established
Maturity Level 4 : Strategic
Maturity Level 5 : Dynamic

The progressive nature of the model assumes that lower levels have been achieved before moving to the next.



The GCSCC's CMM currently considers cyber security capacity as being comprised of the following five Dimensions:

Dimension 1 : Devising cyber policy and strategy
Dimension 2 : Encouraging responsible cyber culture within society
Dimension 3 : Building cybersecurity knowledge across the country
Dimension 4 : Creating effective legal and regulatory frameworks
Dimension 5 : Controlling risks through organization, standards and technology

These five dimensions link well with the ITU's GCA.

Every Dimension consists of a number of Factors which can be seen as sub-dimensions of the specific Dimension.

Every Factor (sub-dimension) consists of a number of Categories, which represents the 'things' which are to be measured and for which a maturity level status is to be determined.

For every Category, for every Maturity level for that Category, there are a number of Indicators which indicate what must be satisfied for the specific Category to be on the specific Maturity Level.

An example is shown in Figure 3

Dimension 3: Building Cybersecurity Knowledge across the country

D3-1: Awareness Raising					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Awareness Programme	The need for awareness of cybersecurity threats and vulnerabilities across all sectors is not recognised, or is only at initial stages of discussion.	Awareness raising programmes, courses, seminars and online resources are available for target demographics from public, private, academic, and/or civil sources, but no coordination or scaling efforts have been conducted. National awareness raising programmes may be informed by international initiatives but are not linked to national strategy.	A national programme for cybersecurity awareness raising led by a designated organisation (from any sector) is established, which addresses a wide range of demographics and issues, but no metrics for effectiveness have been applied. Consultation with stakeholders from all sectors informs the creation and utilisation of programmes and materials. A single online portal linking to appropriate cybersecurity information exists	The national awareness raising programme is coordinated and integrated with sector-specific, tailored awareness raising programmes, such as those focusing on government, industry, academia, civil society, and/or children. Metrics for effectiveness are established and evidence of application and lessons learnt are fed into future programmes. The evolution of the programme	Awareness raising programmes are adapted in response to performance evidenced by monitoring which results in the redistribution of resources and future investments. Metrics contribute toward national cybersecurity strategy revision processes. Awareness programme planning gives explicit consideration to national demand from

D3-1: Awareness Raising					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
			and is disseminated.	is supported by the adaptation of existing materials and resources, involving clear methods for obtaining a measure of suitability and quality. Programmes contribute toward expanding and enhancing international awareness raising good practice and capacity-building efforts	the stakeholde communicatio (in the widest sense), so that campaigns continue to impact the entire society.

Figure 3 (from [4])

Figure 2 represents part of the first Factor D3-1 'Awareness Raising' of Dimension 3 (D3) 'Knowledge Development'. Only the first Category of D3-1 'Awareness Programmes' is displayed.

Awareness Programmes will be measured to be on Maturity Level Start-up if the Indicator

'*The need for awareness of cybersecurity threats and vulnerabilities across all sectors is not recognised, or is only at initial stages of discussion*'

is determined to be true. This level has only this one Indicator.

To be on the Maturity Level Formative, the two relevant Indicators must be satisfied.

As can be seen in Figure 2, the number of Indicators may differ between Maturity Levels. The full CMM can be found in (GCSCC, 2016).

3. Applying the CMM

The first version of the CMM was finalized in 2013. So far the CMM had only been applied on the national level (rather than the organizational level), and 42 countries have been fully evaluated through engagement and collaboration with the host country. The *process* by which a country is assessed is as important as the model itself, and the implementation/measurment approach is one of the key outputs of this ongoing project.

After an initial discussion with key stakeholders in the country, a sponsor is identified. A team from the GCSCC then visits the country and holds interviews with relevant stakeholders over as wide a spectrum as practicable. The interviews usually take about 2 to 3 days, and result in a comprehensive report to the country indicating the relevant Maturity Level for all Factors in all Dimensions. A comprehensive set of recommendations is also provided to indicate to the country how to improve the different Maturity Levels.

An example of the activity and collaboration partners of the Centre between February and November 2005 is as follows:

Jamaica and Colombia (with the Organization of American States)

Armenia, Kosovo, Bhutan and Montenegro (with the World Bank)

Uganda and Fiji (with the Connonwealth Telecommunications Organisation)

Indonesia (with the Ministry of Information and Communications Technology and Telekom University)

United Kingdom (with the Cabinet Office)

More recently, Senegal was reviewed in January 2016, in conjunction with the Government of the Netherlands. Publication of the results is at the discretion of the country. Senegal chose to publish. The second version of the CMM is presently being finalized, based on the learnings from the deployment of the first model.

It is envisaged that the CMM can also be applicable to private corporations and organizations. This more fine-grained model has now been developed, and is currently under review by experts in the field. Eventually, a self-assessment process may be developed, though this is a contentitious issue because any lack of impartiality would undermine both the model and its results.

An important (and concurrent) next step is the development of "Harm Model" to understand the various aspects of harm that results from a lack of cybersecurity (crime, privacy, psychological well-being, destruction of national infrastructure for example). Its development follows a similar engagement approach to the one used for the CMM iitself. In conjunction with the CMM is will provide the ability for countries (and organizations) to focus their limited resources on the aspects of cybersecurity which are least advanced, and which are likely to cause most harm. This will of course be contingtent on the particular circumstances of each country.

Sustainability has been a key underpinning of the endeavour. The Vision 2020 sub-project outlines the future development and deployment of the model. As part of this, the development of Regional Satellite centres has begun (because of the need for expertise and labour beyond the Oxford team). The first example of this is the Regional Centre for Cybersecurity Capacity launched with the Government of Victoria in 2016. This will be a key focus area for the Oceania region, and brings together eight universities from Victoria, as well as the Melbourne-based Defence Sciences Institute and major private sector partners. The centres will work in close collaboration with the Oxford team to ensure ongoing consistency in the use of the model, and to avoid "forking"the project into multiple versions (which would diminish its utility).

4. Summary

The GCSCC's CMM is a very powerful tool/mechanism to evaluate the status of CCB in a country, which is essential for proper Cyber (Security) Capacity Governance in that country. It is the first of its kind in its breadth, ranging across all areas crucial to the development of cybercapacity building. It was built in collaboration with international stakeholder from all relevant sectors, and uses academia to provide a comprehensive analysis of in-country cybersecurty capacity, with the objective of informing future actions rather than ranking. The engagement process is an important element of the research, in that any model is likely to languish without a clear understanding of the process by which it is used. The over-arching principle is to work alongside the country and its stakeholder so that there is a sense of ownership and investment in the results. This process will thus provide a platform from which further development of cybersecurity capacity can be embraced as an objective.

References

European Union, 2013, 'Capacity building in cyber space : taking stock', European Union, 2013, http://www.iss.europa.eu/uploads/media/EUISS_Cyber_Task_Force_Report.pdf, (retrieved on 28 March 2016)
European Union, 2014, 'Cyber Capacity Building in Ten Points. European Union, 2014, http://www.iss.europa.eu/uploads/media/EUISS_Conference-Capacity_building_in_ten_points-0414.pdf. (retrieved on 28 March 2016)
ITU, 2007, 'ITU Global Cybersecurity Agenda (GCA)', http://www.ifap.ru/library/book169.pdf, 2007, (retrieved on 27 March 2016)
GCSCC, 2016, Global Cyber Security Capacity Centre, 2016, https://www.sbs.ox.ac.uk/cybersecurity-capacity/explore/home, retrieved on 27 March 2016