This file has been cleaned of potential threats.

If you confirm that the file is coming from a trusted source, you can send the following SHA-256 hash value to your admin for the original file.

a5486565f0edfd92a7568b03aa7d416ee699f57438d25702f23c05118ac751a37

To view the reconstructed contents, please SCROLL DOWN to next page.
Developing a Cyber Counterintelligence Maturity Model for Developing Countries

Victor JAQUIRE¹, Sebastian VON SOLMS ²
¹Academy of Computer Science and Software Engineering, University of Johannesburg, South Africa.
Tel: +27 (0) 11 559 2967, Fax: +27 (0) 11 559 2138, Email: victor.jaquire@gmail.com
²Centre for Cyber Security, University of Johannesburg, South Africa.
Tel: +27 (0) 11 559 2967, Fax: +27 (0) 11 559 2138, Email: basievs@uj.ac.za

Abstract: Experience has shown that developing countries’ attempts to forthrightly adopt the frameworks and maturity models of developed nations are generally ineffective. This can be ascribed especially to the unique requirements posed by developing world constraints such as limited resources, infrastructure, technologies, skills and experience. This does not, of course, imply that existing models and frameworks are not useful to the developing countries. To design a cyber counterintelligence maturity model for developing countries it is necessary to discuss the basic concepts of frameworks and maturity models. It is further necessary to identify how they are utilised within developed countries and their general application and utilisation as part of the strategy to protect and secure cyberspace and especially national critical information infrastructure - by both government and the private sector. This, in addition to traditional cybersecurity defensive measures as part of cyber strategy within developing counties.

Keywords: cyber counterintelligence, cyber threat intelligence, defensive and offensive cybersecurity, cyber counterintelligence levels, cyber counterintelligence maturity.

1. Introduction

“It is now widely recognized that traditional approaches to cyber defence have been inadequate” [1]. The time-honoured solutions, habitually depended on to defend our milieus are no longer sufficient. Cyber-attacks are intensifying [2], and relentless breaches are progressively affecting nearly everyone. Bodmer [3] emphasises that “Just as intelligence organisations are tracking the activities of terrorist cells trying to stop them before they take action, going after the malicious attackers before they are able to commit attacks is the desired approach”. Farchi [4] stresses that “Staying vulnerable while waiting for a security patch from your software vendor is an anachronistic method that won’t survive this new world.”

2. Objectives

This paper aims to add to the promising deliberations on cyber counterintelligence (CCI) through the proposition of a CCI maturity model for developing countries. It explores the concept of frameworks and maturity models - and cybersecurity, the paper argues, can be augmented and will be more effective when incorporating a dedicated focus on defensive,
offensive, passive and active measures in a multi-disciplinary and integrated CCI approach. It deliberates on the need for cyber counterintelligence (CCI) practices in conjunction with traditional defensive and/or offensive cyber measures within both government and the private sector (business). This culminates in a discussion on a CCI maturity model within developing countries, and highlights the ideal for the establishment of a CCI maturity model that can be customised for government and private sector alike.

3. Methodology

The methodology is firstly grounded on an extensive study with regard to existing literature, and secondly on the experience of the author. The outcome is an Artefact (a Cyber Counterintelligence Maturity Model - CCIMM) which is based on the literature study and the experience of the author.

4. Frameworks and Maturity Models

There are several interpretations and comprehensions of the concepts of frameworks and maturity models. In some instances, the two concepts are utilised interchangeably and thought of as having the same underlying meaning.

The purpose of this section is not to rekindle the debate on the different meaning of the two concepts, or, whether or not they should be utilised interchangeably in the same context. With the understanding that there are various different interpretations of these two concepts, this section will express our understanding of the two notions and highlight the context in which we will utilise these two views in developing a CCI maturity model for developing countries.

The Oxford English Dictionary defines a ‘Framework’ as “an essential or underlying structure; a provisional design, an outline; a connectional scheme or system” [5]. The same dictionary describes ‘Maturity’ as “the state of being complete, perfect, or ready; fullness of development…” [6], and further refers to a ‘Model’ as “a simplified or idealised description or conception of a particular system, situation or process” [7]. Building on the Oxford English Dictionary’s definitions our interpretation with regard to these concepts is that – ‘a framework is the underlying concept and foundational dimensions on which a Maturity Model is constructed’. This is illustrated in the following figure:
As highlighted in Figure 1, a maturity model is therefore the steps, efforts and/or actions that are required to realise the basic concept or idea, as well as its corresponding foundational dimensions and / or elements, in a structured and measurable approach to ensure an optimum outcome.

There are copious different frameworks available for many different environments. Some basic dimensions of frameworks do seem to remain coherent throughout. These include elements such as the focus and sector of the business, the country or region of operation, the identification of areas to be measured and the levels of measurement - among other. These are explored further when looking at an example of a maturity model such as The Oxford Cyber Security Capability Maturity Model, within section 4.

5. The benefit of a Maturity Model

In line with our deliberation with regard to frameworks in section 3, the same situation is prevalent with regard to maturity models. There are numerous diverse maturity models on offer to almost every sector. Utilising a model can assist a government or organisation to attain its goals successfully, efficiently and systematically during the establishment, implementation and maturity of efforts - such as a process, capability, function, strategy or operation.

A maturity model further assists an organisation in enabling it to follow a clear road map and guidelines with clear deliverables towards defined ends. A good maturity model should allow for some level of flexibility to permit different organisations to utilise the same model in dissimilar ways to attain its own definable ambitions and realities in line with its strategy, ethos and capabilities. Likewise, it can also be utilised by organisations to have its “methods and processes assessed according to management best practice, against a clear set of external benchmarks” [8].

Figure 1: The Relation between a Framework and a Maturity Model – (Created by the Author)
In a comprehensive discussion, the certification and examination institute, APMG International, espouses the advantages of a maturity model [8]. The APMG report posits “Maturity” as being indicated by the award of a particular "Maturity Level". The latter denotes a “known Maturity Level, with precise recommendations on how to improve”. APMG further points to the proficiency a maturity model affords an organisation to “compare their maturity level with other organisations, or other parts of their own organisation”, thereby enhancing and/or ensuring, among other, the following:

- “A big improvement on self-assessments”
- “A consistent set of questionnaires and scoring”
- “Independently verified and certified”
- “An independently held set of "benchmarks"”

The Oxford Cyber Security Capability Maturity Model (CMM) as established in 2014 serves as an example of such an effective maturity model [9]. The successful utilisation of this model worldwide to identify and guide cyber security capability maturity, reaffirm the benefits of utilising a maturity model. It progressed through a few iterations thus affirming that a maturity model itself has to mature through time to ensure that it remains relevant – an aspect that will also be essential for our maturity model.

Even though the Oxford model is not a cyber counterintelligence maturity model, it offers several aspects useful to the latter’s’ construction. These aspects include (a) the model layout and (b) the usage as well as the standardisation of certain vocabulary and descriptive words such as ‘Dimension, Sub-Dimension and Category'. This provides us, during the development of our CCI maturity model, with the opportunity to assist in the effort to standardise some of these concepts, use of vocabulary and naming conventions within maturity models, by resonating this throughout our CCI maturity model for developing countries.

6. Developing our CCI Maturity Model for Developing Countries - (CCIMM)

Within an underlying framework for CCI, the CCI concept is explored in two areas, namely Denial and Deception (with the understanding that the concept of ‘deception’ also includes the concept of ‘counter-deception’) [10]. Heckman highlights the evolution of cyber security, by describing it as being at a “critical juncture”, as “Computer network defence (CND) has reached the limits of what traditional perimeter defences such as boundary controllers and firewalls, as well as intrusion detection systems, can do to increase an organisation’s overall security posture”. There is a call for more advanced techniques that can “not merely monitor, detect, and block intrusions, but would actively engage adversaries and study their tactics, techniques, and procedures (TTPs) and craft customized responses and mitigation strategies”.

Considering these perspectives, we can then modify the original counterintelligence postures as described by Sims [11] and espoused by Duvenage & von Solms [12], to evolve into a framework that will be more suited to CCI. Graphically our adaption of the matrix for purposes of the CCI maturity model can be depicted as follows:
Within this adapted framework, it is possible to retain the initial four quadrants of counterintelligence. All four of these quadrants / dimensions (A, B, C and D) are then combined with the concept of denial and deception. Dimension A and B focusses on denial, and dimension C and D focuses on both denial and deception. The last dimension (D) is then also further split in two, to allow for two unique focus areas within the active offensive dimension. This effectively splits the one dimension (dimension D) into two dimensions (Dimension D1 and D2), focussing either on hacking back (D1), or on cyber collection efforts (D2) - or on both of these areas (D1 and D2). This is done purposefully to allow for customisation later on within the maturity model based on an organisations area of business and profile (government, private sector etc.). In line with these modifications, the CCI framework then effectively consists of five dimensions.

From the discussion thus far, it is apparent that an effective CCI maturity model (CCIMM) will have to cater for both a government and private sector environment. Furthermore, we need to address all five dimensions of the adapted CCI framework and attend to the three levels (sub-dimensions) within an organisation, namely strategic, operational and tactical/technical.

As the focus of the CCIMM is centred on attaining maturity, there should be different levels of compliance (or goals) in order to identify, plan and execute different actions to attain different intensities of maturity in line with an organisations strategy, sector of business, area of operation and risk profile. The CCIMM should be scalable and customisable with clear guidance towards the achievement of goals and the attainment of outcomes.

With the intention of being multi-disciplined, the CCIMM should also allow for the integration of existing cyber related defensive and/or offensive structures and efforts within an organisation. Each of the five dimensions are therefore broken down accordingly into three sub-dimensions, namely:
- Strategic,
- Operational,
- Tactical/Technical.

Each one of the sub-dimensions are then further broken down in six areas of compliance (further described as categories), namely:

- Structures,
- People,
- Processes,
- Technologies,
- Legal / Policies,
- Training / Skills Development.

These six categories are identified as the main compliance focus areas, from the onset, that would be applicable to most environments irrespective if it is a government department or private sector business. This does however not dictate that these are the only categories that can, or should be utilised. Further categories can be identified and added based on the organisation’s needs, nature of business and risk profile. Therefore, the level of adherence to each of the categories within a specific sub-dimension will be different to each organisation depending on the profile of the organisation (private sector business, government structure and so on). Accordingly, the intensity of adherence to the sub-dimensions within each of the five specific dimensions will also differ from organisation to organisation.

Each of the six categories within the sub-dimensions are then allocated four levels of maturity, ranging from level 0 (indicating that nothing is in place) to Level 3 (the highest level of maturity). Every one of these maturity levels can be specified according to the need of the organisation, stemming from a defined baseline that is set for either a government environment or a private sector business environment. An organisation can then decide which level of maturity (level 0 - 3) it wishes to attain for each of the six categories within each sub-dimension for all five of the dimensions. This decision can be based on matters such as organisational strategy, risk profile and/or risk appetite, availability of funding, and so on.

For all three sub-dimensions (under the five main dimensions), the six categories (as specified above) are the same, as each of these will need to comply with specific goals within each of the six categories. This also assists in aligning the corresponding categories within each of the three sub-dimensions throughout the five dimensions. The alignment is firstly done within each specific sub-dimension and then secondly between the five different dimensions to ensure that the five dimensions align with each other, as highlighted in the figure below.
This alignment is done intentionally. It allows every different organisation to do the following in line with the underlying framework and CCI maturity model (CCIMM):

- Ensure general synergy within a specific dimension, and/or between dimensions,
- Ensure synergy on each specific sub-dimension (strategic - (between all dimensions), operational - (between all dimensions) and Technical/Tactical - (between all dimensions)),
- Ensure a complete view, integrated multi-disciplinary approach and dedicated focus on each of the three sub-dimensions, as well as each of the six categories within a specific dimension,
- Ensure a complete view, integrated multi-disciplinary approach and dedicated focus on each of the three sub-dimensions, each of the six categories and each dimension between all dimensions,
- Minimise the possibilities for “silo” thinking, “silo” implementation and “silo” operationalisation.

To ensure effective implementation and monitoring of this CCIMM, each of the three areas (strategic, operational and technical/tactical), as well as each of the six areas of compliance and their corresponding levels of maturity need to be specified in a matrix, outlining (among other) the following:
- What each area is about (consists of)
- What is the aim or the need to be addressed?
- What is the desired outcome?
- How will the organisation know when the desired outcome and level of maturity is reached,
- What is the timeframe for review to ensure continued applicability, effectiveness and required adjustment? (This can also state the criteria for each of these review items).

All this information can then be captured within a dashboard (CCIMM-SAT-D) to graphically display the current status of the CCI maturity effort, areas of concern and areas that require either more or less prioritisation or focus.

### 7. Business Benefits

One of the main benefits of this CCI maturity model is that it acknowledges the unique situation within developing countries.

- It allows a government and/or private sector business to utilise its existing investment within defensive and/or offensive cyber as a basis to develop and mature an effective cyber counterintelligence focus.
- It further allows these environments to develop a CCI maturity strategy (guided by the CCI maturity model) in line with their own capabilities, strategy and realities.

### 8. Conclusions

It is widely comprehended that conventional methodologies to cyber defence have become inadequate, and that the time-honoured defensive solutions, habitually depended on to defend our environments are no longer sufficient.

The mere adoption of maturity models of developed nations by developing countries will not always be effective, due to the unique requirements and realities within developing worlds.

A cyber counterintelligence maturity model, specifically formulated for developing countries (in line with international best practice), will assist governments and the private sector to develop a customised CCI maturity strategy - in line with the CCI maturity model. It will further assist to establish and mature an effective cyber counterintelligence focus in line with their own capabilities, strategy and realities.

### Acknowledgment

The research presented in this paper forms part of a project at the Centre for Cyber Security (Academy for Computer Science and Software Engineering, University of Johannesburg) aimed at formalising CCI as a multi-disciplinary field of academic inquiry in the South African context. Those interested are invited to contact the authors and/or view more detail at - http://adam.uj.ac.za/csi/CyberCounterintelligence.html
References