UCD Forensics and
Security Research Group

UCD
DUBLIN

Proceedings of the 16th European Conference on Cyber Warfare and Security

University College Dublin
Ireland
29-30 June 2017

Edited by

Dr. Mark Scanlon and Dr. Nhien-An Le-Khac

University College Dublin

acpi

A conference managed by ACPI, UK

Cultivating a Cyber Counterintelligence Maturity Model

Victor Jaquire[1] and Sebastiaan von Solms[2]
[1]Academy of Computer Science and Software Engineering, University of Johannesburg, South Africa
[2]Centre for Cyber Security, University of Johannesburg, South Africa
jaquire@gmail.com
basievs@uj.ac.za

Abstract: Just as the utilisation of cyberspace became more mainstream, intricate and advanced during the past decade, so did the intricacy and advancement of threats mature - paralleling the conveniences and essentials that cyberspace provide. It is now vigorously recognised that traditional approaches to cyber defence have become deficient [Heckman et al, 2012]. The respected solutions that we loyally hanged on to throughout the decades, trusting them to defend our environments are no longer sufficient. Unyielding breaches and cyber-attacks are relentlessly intensifying and becoming the order of the day [PWC, 2015]. Farchi [2016] argues that "Staying vulnerable while waiting for a security patch from your software vendor is an anachronistic method that won't survive this new world". This notion corresponds with Bodmer [2012] who stresses 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". This article flows from, and builds on previous discussions and publications with regard to the concept of a maturity model for cyber counterintelligence (CCI). It aims to also resonate with and add to previous publications and maturing debates through the proposition of cultivating and implementing such model. It explores the notion of a CCI maturity model and argues that cybersecurity can be intensified - 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. The article provides a brief look at the benefits that the implementation of such a model hold for both government and the private sector. 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). It also discusses the ideal for the establishment of such a maturity model that can be customised, in a similar way, for organisations (public and private sector), and crowns in discussions on implementation and control.

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

1. Introduction

The recent expression of possible interference in the processes and affairs of sovereign states, such as the USA presidential election, casts renewed focus on the need for vigilance and innovative thinking in cyber defensive measures [ICA, 2017]. Although reports on offensive actions do seem to highlight such actions against government environments and nation states, it is clear that not only government are at risk from such attacks and actions. As much of a country's critical information, infrastructure and systems rest within the private sector, logic dictates that the private sector is just as vulnerable, if not more so.

Kenneth [2016] underlines this interconnection between government and business within cyberspace, stressing that "highly motivated (and potentially state-sponsored) hackers potentially will direct their most sophisticated attacks at private-sector operators when they are searching for national-security information". He notes that the mere fact that environments are part of business and the private sector, instead of government entities, does not constitute a "free pass". He emphasises further the acknowledgement that "absolute security is an unattainable goal" and that "it isn't even realistic to try to keep pace with hackers--let alone a step ahead".

The ICA [2017] report highlights the multi-faceted approaches utilised by adversaries throughout their efforts and campaigns. In order to address the need to prosper and remain attentive in a continually transmuting cyber world, the thinking and approach towards being secure in cyberspace need to evolve and mature accordingly.

The successes in combining conventional defensive 'and/or offensive' cyber security measures with practices generally attributed to traditional intelligence related environments are extensively deliberated [Ferguson, 2012]. Specifically with regard to the gathering of appropriate intelligence information, both reactively and pre-emptively throughout counterintelligence operations, the essence of cyber counterintelligence. In line with the deliberation above 'signifying the ineffectiveness of defensive only measures', it can be argued that effective cybersecurity for both government and the private sector cannot be achieved without a dedicated focus on both defensive and offensive measures in a multidisciplinary and integrated cyber counterintelligence approach.

For this to be achieved successfully, governments and private business requires an efficient maturity model which can be utilised by both of these environments respectively to mature their existing traditional defensive-only environment, or their newly-envisaged Cyber Counterintelligence (CCI) environment over a set period of time into a fully functional cyber counterintelligence function. This is a critical need to adapt in line with the continued evolution towards cyberfication of business and government.

This article provides the rudimentary concept and motivation for a cyber counterintelligence maturity model (CCIMM). The complete breakdown of the CCIMM can be obtained from the University of Johannesburg, at the website indicated within the acknowledgement at its conclusion.

Within the following sections, the article highlights the benefits derived from a CCIMM, deliberates various considerations during the creation of the model, and lastly emphases some reflections during implementation and control of the CCIMM.

2. The benefits of a CCI maturity model (CCIMM)

Utilising a model can assist an organisation (either government or private sector) to realise its objectives effectively, efficiently and methodically during the formation, implementation and maturity of efforts - such as functions, processes, capabilities, strategy or operations.

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” [APMG International, 2016].

There are several different types of maturity models on offer to nearly every sector. APMG International [2016] the certification and examination institute, in a comprehensive discussion advocates the advantages of a maturity model. The APMG report advances “Maturity” as being signified by affording a distinct "Maturity Level". The report signifies a “known Maturity Level, with precise recommendations on how to improve”. APMG further points to the adeptness 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:

- Significant enhancement in self-assessment
- Consistence in questionnaires and scoring
- Independent verification and certification
- Independent benchmarks

As a pertinent example, the Oxford Cyber Security Capability Maturity Model (CMM), founded in 2014, serves as an illustration of such an effective maturity model [Oxford, 2014]. The successful worldwide consumption of this model to identify and guide cyber security capability maturity, reiterate the benefits of applying a maturity model. Its gradual evolution since 2014, pronounces the need for a maturity model itself to mature through time to ensure that it remains relevant. This will also be key for the evolution of our maturity model.

The Oxford model offers several aspects / characteristics useful to the building of a cyber counterintelligence maturity model (CCIMM). These include attributes such as the model layout and the usage / standardisation of certain vocabulary and descriptive words such as ‘Dimension, Sub-Dimension and Category'. This provides us with the prospect 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.

One of the main business benefits of this CCIMM is that it recognises the distinctive situation within each different organisation and sector. It tolerates and Inspires customisation, such as the following:

- Encourages 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 permits such environments the opportunity to develop a CCI maturity strategy (guided by the CCI maturity model) in line with their own capabilities, strategy and realities.

3. Creating a CCI maturity model (CCIMM)

As identified in previous publications in this regard, it is ascertained that the notion of cyber counterintelligence (CCI), as is the case with its parent concept (counterintelligence) is investigated in two main areas, namely Denial and Deception (the latter of which also including 'counter-deception') [Heckman et al, 2012]. 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 demand 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 this, we can then utilise the original counterintelligence concept as described by Sims [Sims, 2009] and championed by Duvenage & von Solms [2015], to progress into a fundamental framework that will be more suited to our cyber counterintelligence needs. This principal framework is depicted as follows:

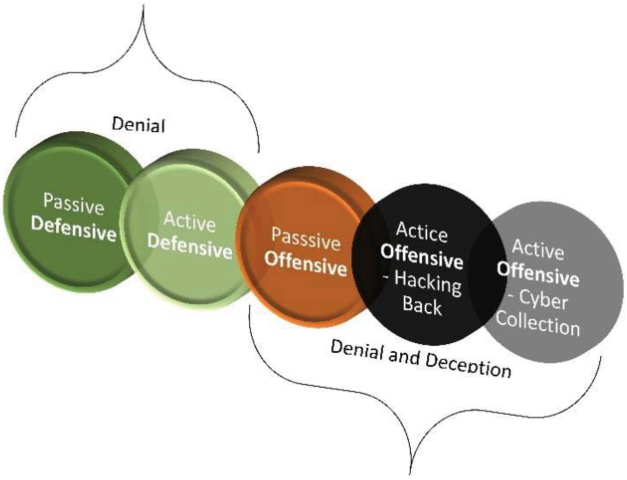

Figure 1: The fundamental elements of cyber counterintelligence – Adapted from Sims 2009; (Duvenage & von Solms 2015)

This fundamental framework combines four dimensions (A - D) under the identified two main areas of denial and deception. Dimension A and B applies the area of denial, and dimension C and D applies both areas of denial and deception. The fourth dimension (D) is further divided in two sections. These form two distinctive focus areas within the active offensive dimension which effectually divides (dimension D) into two, namely (Dimension D1 and D2).

Although the ultimate goal of dimension D remains a dedicated focus on active offensive, dividing it in two allows Dimension D1 to focus on hacking back (D1), and dimension 2 to focus on cyber collection efforts (D2). This enables and organisation to choose how dimension D will be utilised for its purposes in line with its area of business and strategy. It can choose to either focus on Dimension D1 or Dimension D2, or focus on Dimension D in its entirety to concentrate on both hacking back and cyber collection. This division of Dimension D is therefore done intentionally to allow for customisation later on within the maturity model based on an organisations area of business and profile (government, private sector etc.). Based on these possible variations, the CCI framework then effectively consists of five dimensions.

It is noted from the discussion so far that an effective CCI maturity model (CCIMM) will have to cater for most environments and sector, irrespective if it is a government or private sector environment. We also need to address all five dimensions of the principle CCI framework and attend to the identified three main sub-dimensions within an organisation, namely strategic, operational and tactical/technical.

With focus of the CCIMM concentrated on realizing maturity, different levels of compliance (or goals) there should be observed to identify, plan and implement dissimilar activities to achieve distinct intensities of maturity in line with an organisations strategy, area of business, sector of operation and risk profile. The CCIMM should be scalable and customisable with well-defined guidance towards the attainment of objectives and the realisation of outcomes. This concept can be depicted in the following figure as an example:

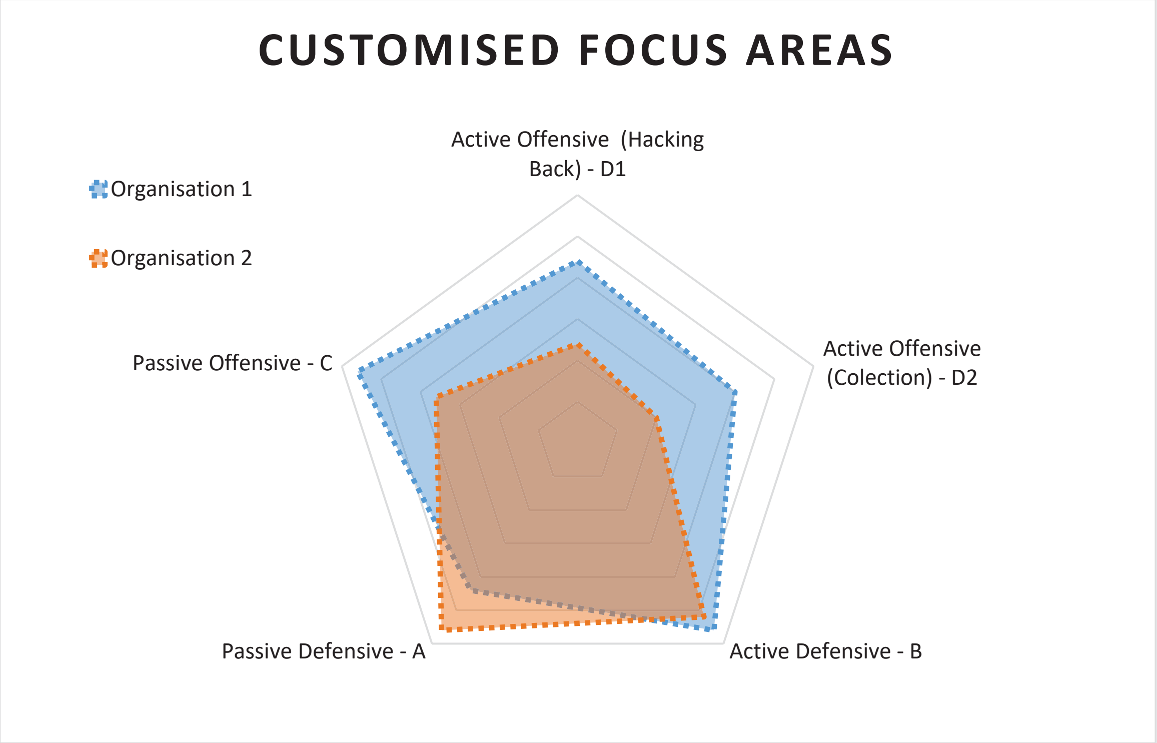

Figure 2: A graphical depiction of the CCIMM focus areas for two different organisations

In Figure 2, we can highlight how two different organisations can utilise the same cyber counterintelligence maturity model (CCIMM) in order to establish and mature its cyber counterintelligence (CCI) programme.

In this example, Organisation 1 has an extensive focus on most of the five dimensions, with an intensive focus on both the Active Defensive and Passive Offensive dimensions. Organisation 2, on the other hand, has a more conservative focus on Passive offensive, hacking back and cyber collection, with a more dedicated focus on both the Passive and Active Defensive dimensions. In this example, both organisations will implement all five dimensions of the maturity model, however, the level of focus for each dimension will be different for each of the two organisations.

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. The dimensions are further broken down into sub-dimensions and categories as depicted in figure 3.

As indicated in Figure 3, each of the five dimensions are broken down into three sub-dimensions, namely:

- Strategic,
- Operational,
- Tactical/Technical.

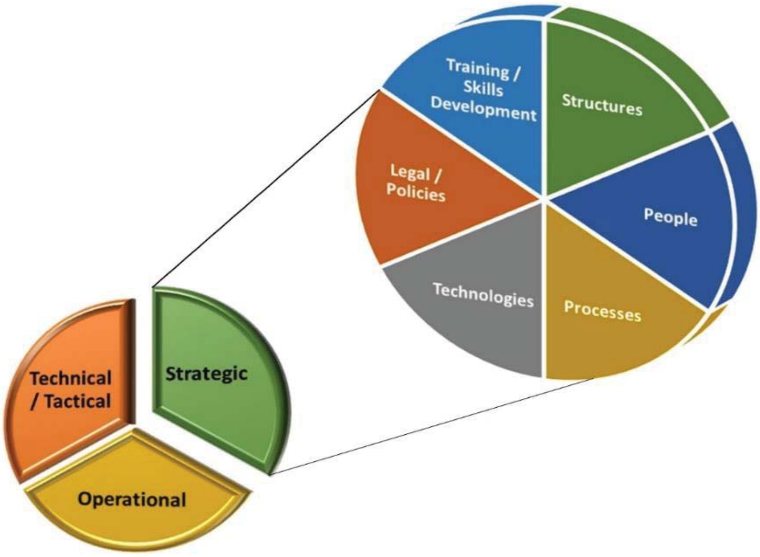

Figure 3: The sub-dimensions and categories within each of the five dimensions of the CCIMM

Each sub-dimension concentrates on (an initially identified) six areas of compliance (further described as categories), such as:

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

The six categories as sampled above are featured as the initial focus areas applicable to most environments irrespective if it is a government department or private sector business. Further focus areas can be identified and added based on the organisation's needs, nature of business and risk profile. The level of adherence to each of the focus areas within each specific sub-dimension will therefore be different to each organisation depending on the profile of the organisation (private sector business, government structure etc.). In consequence, the level 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 further allocated four levels of maturity, varying from level 0 (indicating that either nothing, or the bare minimum is in place) to Level 3 (the highest aim of maturity). This can be indicated in Figure 4.

Each maturity level can be customised and reflected in line with the need of the organisation, aligning with a defined baseline that is set for either a government environment or a private sector business environment. An organisation can then determine the level of maturity (level 0 - 3) it wishes to attain for each of the categories within each sub-dimension for all five of the dimensions. This determination will further align with organisations unique composition, grounded on issues such as strategy, risk profile and/or risk appetite and funding model, to name but a few.

In the CCIMM the categories that are identified under all three sub-dimensions (within the five main dimensions) are identical. Each category needs to comply with specific goals within each sub-dimensions. This allows for effective alignment and control of corresponding categories within each of the three sub-dimensions throughout the five dimensions during and after implementation of the model. 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.

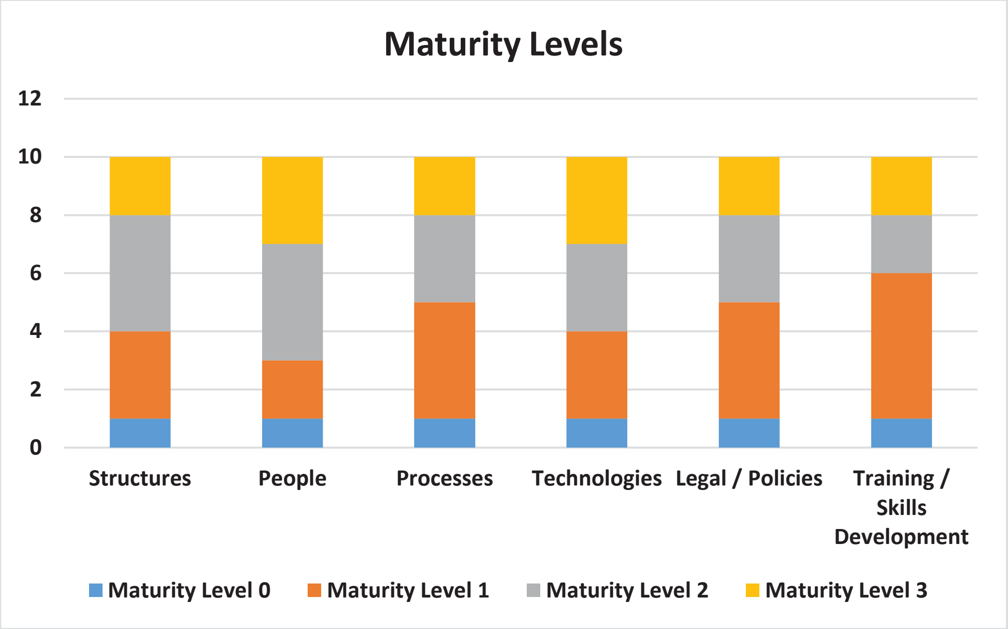

Figure 4: The maturity levels for each category, within each sub-dimension, for every dimension of the CCIMM

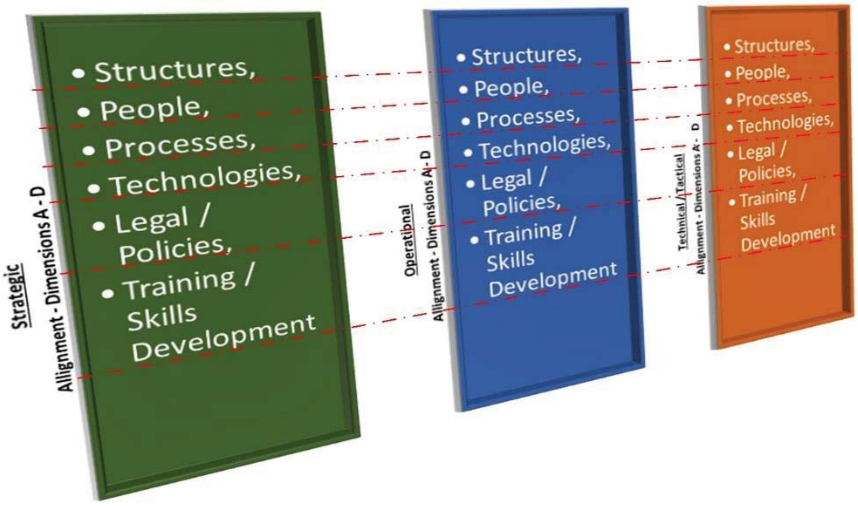

Figure 5: Horizontal and vertical alignment of the dimensions within the CCIMM

This alignment is therefore done intentionally. It allows every unique organisation to do the following, in line with the principle CCI framework and CCI maturity model (CCIMM):

- Facilitate general synergy within a specific dimension, and/or between dimensions,
- Allow for synergy on each specific sub-dimension (strategic - (between all dimensions), operational - (between all dimensions) and Technical/Tactical - (between all dimensions)),
- Provide a comprehensive view and 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,
- Provide an all-embracing view and 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,
- Diminish the likelihood for “silo” thinking, “silo” implementation and “silo” operationalisation.

4. Implementation and control of the CCIMM

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 consists of
- The aim
- The desired outcome
- The control objectives
- The timeframe for review to ensure sustained applicability and usefulness

This information can then be captured within a dashboard (CCIMM-SAT-D) to graphically display the status of the CCI maturity effort, areas of concern and areas that require either more or less prioritisation or focus. The dashboard further provides a graphical representation of the progress, maturity status and trend of maturity development at any given time during, before and after implementation as indicated in figure 6:

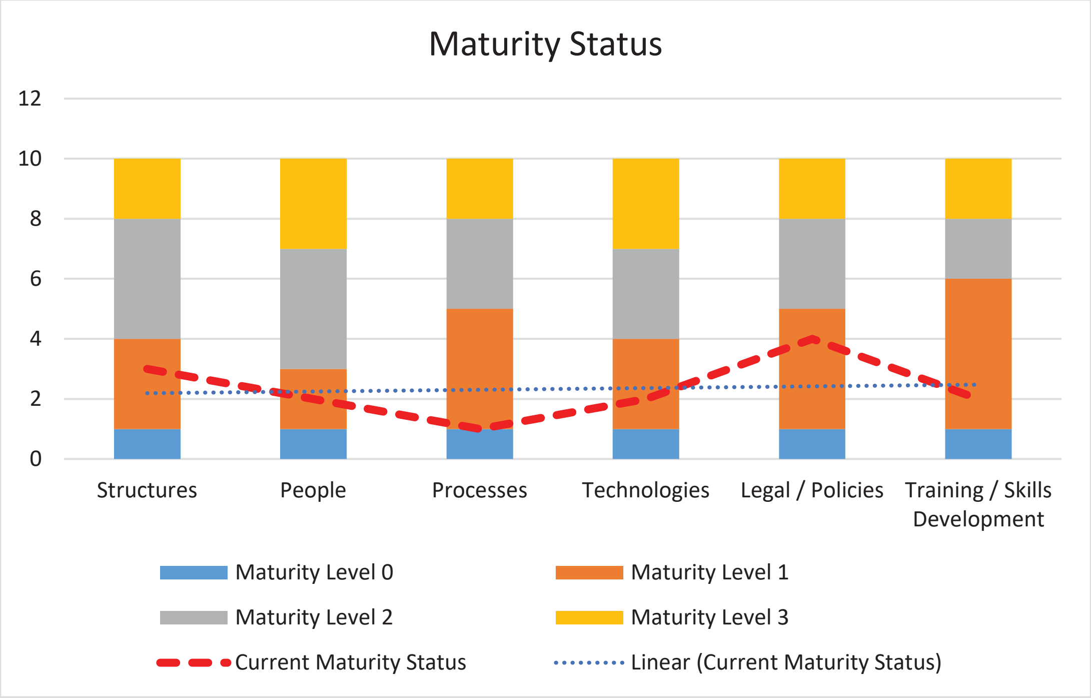

Figure 6: The maturity status as measured continually - before, during and after the implementation process for each category throughout the sub-dimensions and dimensions of the CCIMM

This graphical representation will then allow decision makers to adapt implementation strategies, processes and funding models etc. to address any changes required within the maturity process in line with strategic requirements.

5. Conclusion

Traditionally, CCI is utilised within governments as a subset of counterintelligence activities, as well as within some large private sector organisation. Traditional defensive cyber solutions are no longer sufficient on their own to safeguard our environments. Cyber Counterintelligence can and should be utilised successfully within government and private sector organisations to deal with the advanced and ever persistent cyber threats. To this end, an effective cyber counterintelligence maturity model (CCIMM) is essential to ensure a structured and effective implementation of CCI.

A CCIMM should align with a principle CCI framework to ensure that it addresses all areas of focus within the CCI concept and at the same time address all three main focus areas within an organisation, namely the strategic, operational and technical / tactical level.

It is further imperative to align the elements within the maturity model in such a way that it stimulates adherence to a multi-disciplinary approach, leverage on existing defensive and/or offensive cyber capabilities within an organisation and discourage polarised implementation or a silo approach.

An effective CCI maturity model is central to transition an ineffective defensive-only environment into a fully functional multi-disciplinary cyber counterintelligence function, capable of addressing the level of cyber threats that is faced globally. Such model enables an organisation by, (a) indicating the process and activities to progress from the present status towards a more mature status and, (b) accurately gaging progression towards such a fully functional CCI approach.

Acknowledgments

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

APMG International, 2016, http://www.apmg-international.com/en/consulting/what-maturity-model.aspx, Accessed 31 October 2016

Bodmer, Kilger, Carpenter & Jones (2012). *Reverse deception–Organized cyber threat counter- exploitation*, McGraw-Hill, New York.

Duvenage, P. C. & von Solms. S.H., (2015), 'Cyber Counterintelligence: Back to the Future', Journal of Information Warfare, Vol 13, Issue 4. http://adam.uj.ac.za/csi/CyberCounterintelligence.html

Ferguson, (2012), Increasing Effectiveness of U.S. Counterintelligence: Domestic and International Micro-Restructuring Initiatives to Mitigate, Monterey, California: Naval Postgraduate School, June 2012.

Farchi, (2016) Offensive Counter-Intelligence and Cyberwarfare - A Paradigm Shift in Information Security, http://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=261, Accessed 18 Feb 2016

Heckman et al, (2012), Cyber Denial, Deception and Counter Deception, A Framework for Supporting Active Cyber Defence, Springer.

ICA 2017, Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution, ICA 2017-01D, 6 January 2017

Oxford, 2014, Cybersecurity Capability Maturity Model (CMM) – V1.2, The Oxford Martin School, Global Cyber security Capacity Centre, University of Oxford

PWC, (2015), GYB Report https:// www .pwc .com /us /en /private – company – services /publications /assets /pwc-gyb-cybersecurity.pdf, Accessed 20 May 2016

Sims, J. E., (2009), "Twenty-first-Century Counterintelligence" in Sims, J. E. and Gerber, B. (eds.), Vaults, mirrors, and masks: Rediscovering U.S. counterintelligence, Twenty-first-Century Counterintelligence: The Theoretical Basis for Reform, Washington, D.C, Georgetown University Press, pp 21-22.