Towards a National Cybersecurity Capability Development Model

P.C. Jacobs[1,2], Prof. S.H. von Solms[2], Prof. M.M. Grobler[1,2]
[1] Council for Scientific and Industrial Research, Pretoria, South Africa
[2] University of Johannesburg, Johannesburg, South Africa
pjacobs@csir.co.za
basievs@uj.ac.za
mgrobler1@csir.co.za

Abstract: Nations need to develop cybersecurity capabilities at national level in order to facilitate the requirements expressed through national authoritative and normative documents. These national cybersecurity capabilities typically consist of people, processes and technology or tools. From the research conducted, no publicly available models or frameworks for national cybersecurity capability development could be found. In this paper, the authors identify and compare existing military capability development models and propose a national cybersecurity capability development model based on these models. Military capability development frameworks are a comprehensive way to define work deliverables and work standards, and provides a way to measure the work deliverables (eWorks Moodle, 2016). The use of such a national cybersecurity capability development model is advantageous during the planning phase of the national cybersecurity capability. For example, the using of a model allows for a capability to be broken down into its components, a model serves as a blueprint to ensure that those building the capability considers all components, allows for cost estimation and facilitates the evaluation of trade-offs. One national cybersecurity capability - the incident management cybersecurity capability - is selected to illustrate the application of the national cybersecurity capability development model. This model was developed as part of previous research, and is called the Embryonic Cyberdefence Monitoring and Incident Response Center (E-CMIRC) (P. Jacobs; S.H. von Solms & M.M. Grobler, 2016). The characteristics of national incident management cybersecurity incidents have to be determined, as these would affect each component of the military-based national cybersecurity capability development model.

Once the national cybersecurity capability components are identified using the military-based cybersecurity capability development model, it also has to be operated. To achieve this requirement, available organisational operational models are identified and compared, and one operating model is selected to augment the national cybersecurity capability development model. The fusion of the military-based national cybersecurity capability development model with the operations models results in the national military-based cybersecurity capability development model. This paper has three outcomes in mind: firstly to determine the characteristics of national cybersecurity incidents, secondly, the development of the national cybersecurity capability development model, and thirdly, the development of a national cybersecurity capability operational model. This paper describes the methodology followed in describing the E-CMIRC structure using a capability development framework, and organisational operational models. The national cybersecurity capability development model – using a military capability development framework - and the national cybersecurity capability operational models derived from existing organisational frameworks, are presented as a single, integrated model.

Keywords: Cybersecurity capability development model, cybersecurity operational model,
National cybersecurity capabilities, national cybersecurity incident characteristics, POSTEDFIT-B

1. Introduction

Considering the prominence of recent national cybersecurity incidents – specifically during the American elections (Diamond, 2016), and cybercrimes at national level (Ed Vaizey, 2016), (White, 2016) it is necessary for countries to establish cybersecurity services at national level. These services could be offered in the cyber offensive or cyber defensive domains (NATO Cooperative Cyber Defence Centre of Excellence, 2012).

In this paper, the authors propose three contributions. Firstly, the authors propose the characteristics of national cybersecurity incidents. Secondly, a model for the development of national cybersecurity capabilities, of which the E-CMIRC structure is an example, is proposed. This model is called the E-CMIRC Capability Development Model (CDM) and uses the POSTEDFIT-B military capability development framework. Thirdly, a model, which could be used to facilitate the operations of the E-CMIRC is, proposed, leveraging of the eTOM Business Process Framework. This model is called the E-CMIRC Operations Model (OM). The ECMIRC CDM and E-CMIRC OM are presented as a singular, combined model to describe the E-CMIRC structure.

Section 2 provides background on national cybersecurity capabilities, while Section 3 considers the concept of cybersecurity incident handling, and defines what constitutes cybersecurity incidents at national level. This culminates into the identification of the characteristics of national cybersecurity incidents. This is important since the characteristics of national cybersecurity incidents has an influence on how they are detected and managed. This ultimately influences the E-CMIRC CDM.

Section 4 provides background on capability development frameworks, and identifies the prominent military capability development frameworks. These military capability development frameworks are compared with each other, and a military capability development framework is selected and motivated to develop the model. In Section 5, the E-CMIRC operational model is presented, while Section 6 presents the E-CMIRC integrated model. Section 7 proposes future work. The paper is concluded in Section 8.

2. Background

From literature such as the North Atlantic Treaty Organisation's (NATO) National Cyber Security Framework Manual (NATO Cooperative Cyber Defence Centre of Excellence, 2012), the International Telecommunications Union (ITU) National Cybersecurity Strategy Guide (F. Wamala, 2012), the United Kingdom's Cyber Security Capability Maturity Model (CMM) (T. Roberts, 2014) and the Cybersecurity Capability Maturity Model (C2M2) developed by the United States Department of Homeland Security (J. D. Christopher, 2014) – thirteen national cybersecurity capabilities were identified. These are:

- Military Cyber / Cyber Warfare
- Cybercrime / Investigations / Digital Forensics
- Research and Development (R&D), Education and Awareness
- Critical Information Infrastructure Protection (CIIP)
- Cryptography
- E-Identity
- Incident Response
- Monitoring and Evaluation of ICT
- Internal Coordination
- External Stakeholder Engagement
- National Policy and Strategy Development
- National Regulations Development
- National Strategic Risk and Threat Assessment

One of these identified national cybersecurity capabilities - incident response - were selected to illustrate the application and usage of the E-CMIRC Capability Development Model (CDM) model. The rationale for the selection of the national cybersecurity capability of incident response, is that the authors have extensive experience in this domain of cybersecurity – both at a national, and enterprise level.

The purpose of the E-CMIRC model is to provide nations with an effective and efficient way of addressing national cybersecurity incident. The E-CMIRC CDM and E-CMIRC OM describe a national cybersecurity structure called the E-CMIRC structure. The E-CMIRC structure was developed by fusing the services offered by Security Operation Centers (SOCs) and Computer Security Incident Response Teams (CSIRTs) (P. Jacobs; S.H. von Solms & M.M. Grobler, 2016).

A model is a representation which can be used to mimic the operation of a service (Jacobs P., 2015). A service provides a function, and consists of capabilities (T. Graves, 2012), while a capability is made up of people, processes and technology (R. Heffner, 2010). *Figure 1* as taken from Graves, 2012 illustrates this concept.

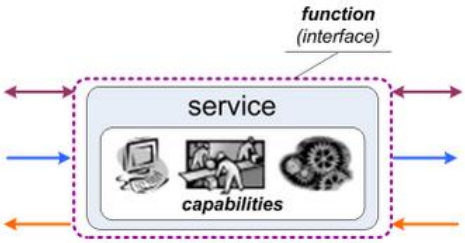

Figure 1: Relationship between Service, Function and Capability (T. Graves, 2012)

3. Cybersecurity Incident Handling Capability

The Software Engineering Institute at the Carnegie Mellon University recommends that organisations need to define cybersecurity incidents for their specific environments (NATO Cooperative Cyber Defence Centre of Excellence, 2016), (Software Engineering Institute, 2016). It is the experience of the authors that this recommendation is equally applicable to nation states defining cybersecurity incidents at national level. This implies that the definition of the term cybersecurity incident is something intimate, and organisational or country specific. The definition of cybersecurity incidents must be done keeping in mind the unique conditions and requirements of the organisation or nation state that they are being developed for. The characteristics of national cybersecurity incidents will directly influence all components of the E-CMIRC CDM.

3.1 National Cybersecurity Incident Definitions

To determine the characteristics of cybersecurity incidents at national level, it is necessary to consider existing definitions by nation states for national cybersecurity incidents, as well as standards, frameworks and best practices. Some of the most common national cybersecurity incident definitions are listed in Table 1 as taken verbatim from NATO Cooperative Cyber Defence Centre of Excellence, 2016.

Table 1: National Cybersecurity Incident Definitions (NATO Cooperative Cyber Defence Centre of Excellence, 2016)

Country	Definition
United States of America (NIST-IR)	*Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein* (Kissel, 2013).
Czech Republic	*Cyber security incident means a cyber security event during which security of information in information systems breach or security of services or security and integrity of electronic communication networks breach occurred* (Republic, 2014)
Lithuania	*Incident shall mean an event, act or omission which gives rise or may give rise to an unauthorized access to an information system or electronic communications network, disruption or change of the operation (including takeover of control) of an information system or electronic communications network, destruction, damage, deletion or the change of electronic information, removal or limiting of the possibility to use electronic information and, also, which gives rise or may give rise to the appropriation, publication, dissemination or any other use of non-public electronic information by persons unauthorized to do so* (R. Simansius, 2011)

3.2 Standards and Frameworks Cybersecurity Incident Definitions

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) in ISO/IEC 27035:2011 standard on Information technology - Security techniques - Information security incident management, define an information security event as an *"identified occurrence of a system, service or network state indicating a possible breach of information security, policy or failure of controls, or a previously unknown situation that may be security relevant"* (ISO/IEC, 2011).

The National Institute of Standards and Technology (NIST) Special Publication 800-61 "Computer Security Incident Handling Guide" Cichonski; Millar; Grance & Scarfone, (2012b) also defines cybersecurity incidents, and together with ISO/IEC 27035:2011 they emerge as the main standard (ISO/IEC 27035:2011) and guideline

(NIST SP 800-61) associated with cybersecurity incident management (Tøndel, Line, & Jaatun, 2014). Their definitions for cybersecurity incidents together with other standards and frameworks are summarised verbatim in Table 2.

Table 2: Standards and Frameworks Cybersecurity Incident Definitions

Standards and Guidelines	Definition
ISO/IEC 27035:2011	*"single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security"* (ISO/IEC, 2011)
NIST SP 800-61	*"A computer security incident is a violation or imminent threat of violation1 of computer security policies, acceptable use policies, or standard security practices"* (P. Cichonski; T. Millar; T. Grance & K. Scarfone, 2012b)
ITIL v3	*"An Incident is defined as an unplanned interruption or reduction in quality of an IT service (a Service Interruption)."* (ITIL, 2011)
ISO/IEC 27001:2005	*"a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security."* (A. Segovia, 2015)
ITU-T Rec E.409	*"Information and Communication Networks (ICN) security incident: Any real or suspected adverse event in relation to the security of ICN. This includes:* *• Intrusion into ICN computer systems via the network;* *• Occurrence of computer viruses;* *• Probes for vulnerabilities via the network into a range of computer systems;* *• PABX call leak-through;* *• Any other undesired events arising from unauthorized internal or external actions."* (ITU-T, 2004)
IETF RFC 2350	*"A computer security incident is any event which compromises some aspect of computer or network security."* (N. Brownlee & E. Guttman, 1998)

These definitions indicate that cyber incidents imply an activity that has a negative impact on services or service quality. Examples of incidents are distributed denial of service attacks to networks, or where a user leaks sensitive organisational information through file sharing services (V. Agrasala, 2010). Considering the definition as expressed in NIST SP 800-61 (P. Cichonski; T. Millar; T. Grance & K. Scarfone, 2012a), ITIL (Office of Government Commerce, 2000), ISO/IEC 27000 (Praxiom Research Group, 2016) and ITU-T Rec E.409 (ITU-T, 2004), the following can be listed as characteristics of organisational cybersecurity incidents:

- It is an unplanned event
- It threatens the confidentiality, availability and integrity of organisational cyber assets and Infrastructure
- It has a negative impact or consequence at organisational level
- It is operational in nature.

3.3 National Cybersecurity Incident Characteristics

The British Government Communications Headquarters (GCHQ) defines national cybersecurity incidents as *"state-sponsored attacks on critical national infrastructure or defence capabilities"*. The definition was adopted by industry, and is used to describe organisational information security incidents (J. Creasey, 2013). GCHQ serves as a United Kingdom (UK) security agency alongside Military Intelligence, Section 5 (MI5) and the Secret

Intelligence Service (Military Intelligence Section 6 ((MI6)). They are responsible to protect the UK's communications and electronic data from actors wishing to do them harm (GCHQ, 2016).
The NATO National Cybersecurity Framework Manual ascribes three characteristics to cybersecurity incidents at national level (NATO Cooperative Cyber Defence Centre of Excellence, 2012). The characteristics are repeated in the UK's Cyber Security Strategy document (Office, 2011).

From experience, the authors would like to add a fourth characteristic. The fourth characteristic is that more than one organisation in an industry is suffering from the same, or different cybersecurity incidents from similar sources. This characteristic would not be applicable to critical infrastructure as singular entities. The characteristics of cybersecurity incidents at national level are:

- Cybersecurity attack originates from various actors
- Aimed against national cyber assets
- It must affect MORE than one organisation in the sector or industry
- Could spawn effects or incidents identical to kinetic attacks

4. Capability Development Frameworks

The Merriam-Webster dictionary defines the concept of a model as *"a description or analogy used to help visualize something (as an atom) that cannot be directly observed"* (Merriam-Webster, 2016). The E-CMIRC will be represented by means of a model. The E-CMIRC Capability Development Model will be an abstract, visual model. The value that a model can provide in representing a system is as follows (SEBoK, 2016):

- It allows for the documentation of E-CMIRC requirements and functions
- Enables assessment of the performance of the E-CMIRC structure
- Enables cost estimation
- Allows for the evaluation of trade-offs
- Aids in performance management, decreases risk and manages cost.

The E-CMIRC is a structure like a CSIRT or a SOC. When planning and building the E-CMIRC to facilitate the incident handling capability and monitoring capability, a capability development model specific to the E-CMIRC structure needs to be followed. Following a capability development model allows the E-CMIRC structure to be broken down into its components. It also serves as a blueprint to assist those building the structure to make sure that all components are considered and catered for (eWorks Moodle, 2016).

The E-CMIRC is a structure to enable the incident handling and monitoring capabilities at national level. In developing capabilities at national level, capabilities can be seen as being made up of Personnel, Organisation, Sustainment, Training, Equipment, Doctrine, Facilities, Information, Technology and Budget (POSTEDFIT-B) (C. Gildenhuys, 2013), (Oosthuizen & Roodt, 2008). The South African Department of Defence (SA DOD) uses POSTEDFIT-B in the development of military capabilities.

Other capability development frameworks are Training, Equipment, Personnel, Infrastructure, Doctrine and concepts, Organization, Information, Logistics (TEPID-OIL) used by the UK Ministry of Defence (UK MOD) (C. Kerr; R. Phaal & D. Probert, 2003). The United States Department of Defence (US DOD) uses Doctrine, Organizations, Training, Materiel, Leadership, Personnel and Facilities (DOTMLF) (M. Lizotte; F. Bernier; M. Mokhtari; M. Couture; G. Dussault; C. Lalancette & F. Lemieux, 2004). These capability development frameworks are atomic dimensions of the people, processes and technology or tools framework (G. White, 2013).

4.1 POSTEDFIT-B Selection Rationale

In developing the E-CMIRC CDM, POSTEDFIT-B is selected as the capability development framework since it is the most comprehensive framework, and has a proven track record, such as the development of the South African Armoured Capability (C. Gildenhuys, 2013). It is also more comprehensive than the UK MOD and the US DOD capability development frameworks as illustrated in Table 3. A further advantage in following this granular approach, is that trade-offs can be made between the framework elements to optimise the E-CMIRC,

or to compensate for a deficiency in an individual element (Oosthuizen & Roodt, 2008). A comparison between the UK MOD and US DOD capability development frameworks against the SA DOD is made in Table 3.

Table 3: Comparison of Military Capability Development Frameworks

	P	O	S	T	E	D	F	I	T	B
SA DoD	X	X	X	X	X	X	X	X	X	X
UK MoD	X	X	X	X	X	X	X	X		
US DoD	X	X		X	X	X	X			

4.2 National Cybersecurity Incident Characteristics mapped to POSTEDFIT-B

In Section 2, the statement was made that the characteristics of national cybersecurity incidents will have a direct influence on all components of the E-CMRIC CDM model using the POSTEDFIT-B framework. The characteristic of national cybersecurity incidents - that the cybersecurity attack originates from various actors – is used to illustrate its influence on the E-CMIRC CDM model. Table 4 shows the influence of the characteristic on the E-CMIRC CDM model.

Table 4: Cybersecurity attack originates from various actors mapped to POSTEDFIT-B

	E-CMIRC CDM Requirement
Personnel	Personnel skills, technology certifications, experience and qualifications must be selected to facilitate discovery of national cybersecurity attacks.
Organisation	The E-CMIRC operations must be organised in such a way to facilitate discovery of, and reaction to national cybersecurity attacks.
Sustainment	Support elements such as financial, logistics and personnel support need to be tailored to supply and support the national cybersecurity incident management capability facilitated through the E-CMIRC structure
Training	The defined training should include aspects such as how frequent training will take place, the depth and breadth of required skills and competence, as well as whether certification training should be considered. It should be kept in mind that training should be split into technical or technology specific training, as well as service specific training such as incident handling, and monitoring and analysis training. Legal and management training should also be provided.
Equipment	Equipment include aspects such as chairs and tables, office and stationary equipment, an equipped pause area, an equipped visitors area and a war room to name a few.
Doctrine	Doctrine describes the management, control, policy, strategy and regulatory framework of the E-CMIRC. Doctrine should be developed to facilitate the discovery of, and reaction to national cybersecurity attacks.
Facilities	Facilities refer to the physical structure itself – the building and property. The facility should be chosen in such a way that it support the operation of the E-CMIRC.
Information	Information covers aspects such as cyber intelligence data and its processing systems, the format of presented information or cyber intelligence, its timelines and reliability and correlation. This must support the discovery of, and reaction to national cybersecurity attacks.
Technology	Technology describes the technological and tool requirements needed for the E-CMIRC to facilitate discovery of, and reaction to national cybersecurity attacks
Budget	Budget describes the budget needed and financial model followed by the E-CMIRC to facilitate discovery of, and reaction to national cybersecurity

5. Operational Model

In section 3, the POSTEDFIT-B framework was selected and motivated as applicable for using in the development of the E-CMIRC CDM. This section considers operational models to be used for the E-CMIRC. The E-CMIRC CDM provides guidance on how to *build* the E-CMIRC structure, whilst the E-CMIRC Operational Model (E-CMIRC OM) provides guidance on how to *run and operate* the E-CMIRC as a national cybersecurity structure.

5.1 Operational Models

At its core, operating models prescribe where and how work is done across an organisation or capability. Operating models link organisational strategy and organisational design to deliver on organisational strategy (D. Cooper; S. Dhiri & J. Root, 2012). There are many industry standard operating models such as the TM Forum's Enhanced Telecom Operations Map (eTOM) Business Process Framework (Cisco Systems, 2009). Other industry standard operating models are the Insurance Application Architecture (IAA) (IBM, 2009b), the Banking Industry Architecture Network (BIAN) (BIAN, 2016), the Information Framework (IFW) (IBM, 2009a), ITIL (Roth, 2008) and CoBIT (Spafford, G., Wheeler, A. J. & Mingay, 2012). In 2014 KPMG proposed a next generation IT operating model consisting of the broker, integrate and orchestrate IT operating model (Claes S. et al, 2014), while Cognizant proposed an IT operations model with organisation and structure, Process, Technology and Tools and Workforce and Sourcing as core tenets in 2016 (P. Ditrans; A. Anand; M. Ponnuveetil; A. Acharya & S. Dash, 2016).

5.2 TM Forum's Enhanced Telecom Operations Map

The TM Forum's Enhanced Telecom Operations Map (eTOM) Business Process Framework was identified by the authors as an ideal framework for the development of the E-CMIRC. It has the ability to scale to national level, it is comprehensive, and it is relevant to an IT service capability (Jacobs P., 2015). For these reasons, the eTOM Business Process Framework is chosen as the operating model for the E-CMIRC.

The eTOM framework is a complete framework addressing marketing and sales, strategy, infrastructure and product as well as operations and enterprise management (Jacobs P., 2015) (TMForum, 2013). It considers all aspects of business, and categorizes all business activities (Jacobs P., 2015). Milham (2004) states that one of the advantages of the eTOM framework is that it establishes a prevalent vocabulary for business processes as well as functional processes (Milham, 2004). For the purpose of developing the E-CMIRC operations model, the eTOM Business Process Framework will be used, as it is the most applicable model for managing operations using defined processes. The eTOM Framework branches into three levels. These levels are the Strategic, Infrastructure and Product level, the Operations level, and the Enterprise Management level (wiseGEEK, 2013). The eTOM Framework with its horizontal and vertical child-levels are shown in Figure 2 as taken from Jacobs (2015).

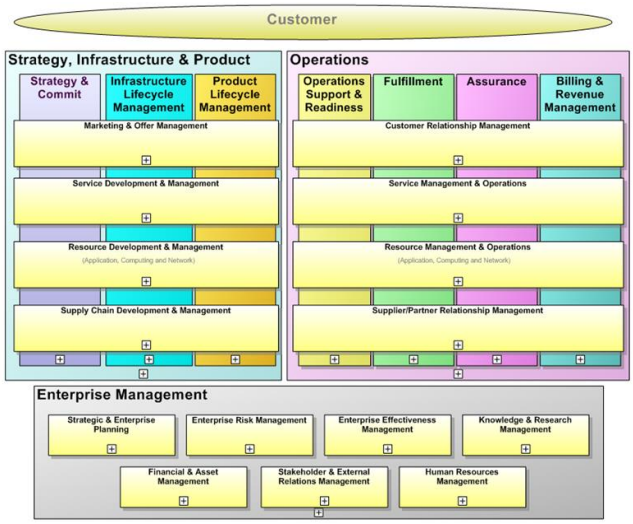

Figure 2: eTOM Framework with Horizontal and Vertical Child Levels

5.3 The E-CMIRC Model

The E-CMIRC structure is developed through fusing the services of SOCs and CSIRTs. The intention of the E-CMIRC structure is to provide nations with a national monitoring and incident response cybersecurity capability, which is scalable, effective, efficient and cost effective. Using the TMForum's eTOM Framework, effectiveness and scalability in terms of operations is achieved. The TMForum's eTOM Framework provides input into the E-CMIRC OM.

Efficiency is ensured through the application of a cybersecurity capability development framework. The framework selected is the POSTEDFIT-B capability development framework, and forms the E-CMIRC CDM. Cost effectiveness is achieved in that only one structure is created to facilitate monitoring and incident response at national level. In future work, we will develop a national cybersecurity maturity model (E-CMIRC MM) to measure and improve on effectiveness. The development of the E-CMIRC structure is displayed in Figure 3.

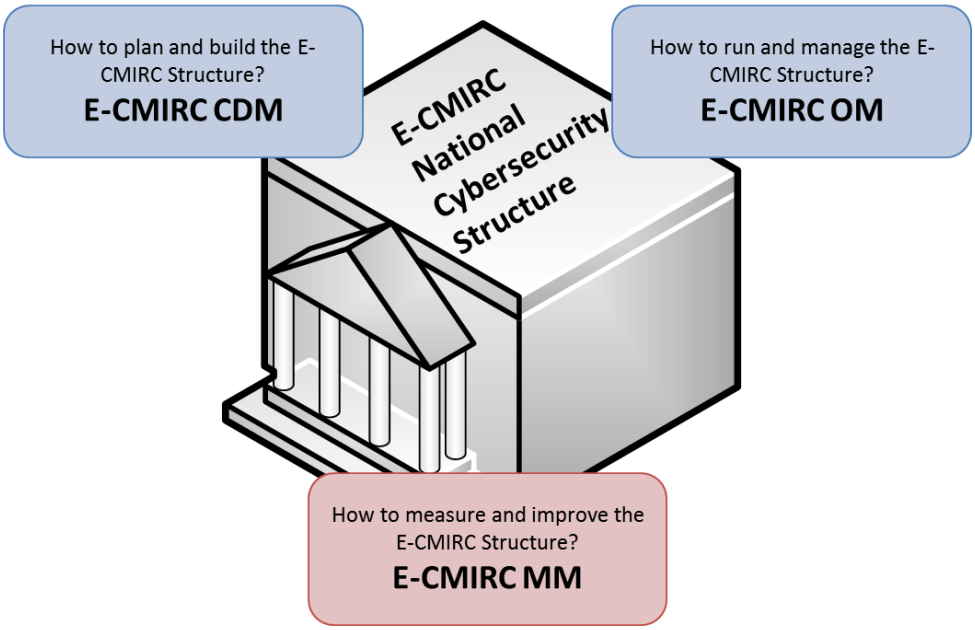

Figure 3: E-CMIRC Structure Components

5.4 Summary

The eTOM Framework is comprehensive, and the model drills down to four levels (Jacobs P., 2015). During the development of the E-CMIRC model, the capability development framework (POSTEDFIT-B) was identified, as well as the operations model (TM Forum's eTOM Framework). The selection of applicable element from the POSTEDFIT-B Framework and the eTOM Framework would differ from country to country, and the intention is for the country developing and implementing the E-CMIRC capability to select the appropriate elements from the eTOM Framework.

6. Presentation of the E-CMIRC Model

The E-CMIRC structure, as a national capability has to comply with national legal and regulatory requirements. It also has to be governed effectively and efficiently. To give effect to this, a capability development framework was selected to be used in the development of the E-CMIRC structure. The POSTEDFIT-B framework used by the South African DOD for capability development was selected based on the fact that the framework application and success is proven at national level, and it was also found that the framework is more comprehensive than its national counter parts.

The E-CMIRC structure is presented as symbolic model in the shape of a three-dimensional cube. The first or upper side of the cube covers the national monitoring and incident management capability. The second side of the cube represents the selected operating model, which is the TM Forums eTOM Framework with levels Strategy, Infrastructure and Product, Operations and Enterprise Management. The intention is for the entity developing the E-CMIRC structure, to drill down to all four levels of the framework, and identify the applicable eTOM Framework business processes based on the selected national cybersecurity dimensions, mandate and domain, as well as services.

The third side of the cube represents the selected capability development framework, which, in the case of the E-CMIRC, is the POSTEDFIT-B Framework. The intention is for the entity developing the E-CMIRC to use the POSTEDFIT-B Framework to ensure that all aspects are considered during the development cycle. This granular approach allows for trade-offs to be made between the framework elements to optimise the E-CMIRC, or to compensate for a deficiencies in individual elements (Oosthuizen & Roodt, 2008). The E-CMIRC model is presented in Figure 4.

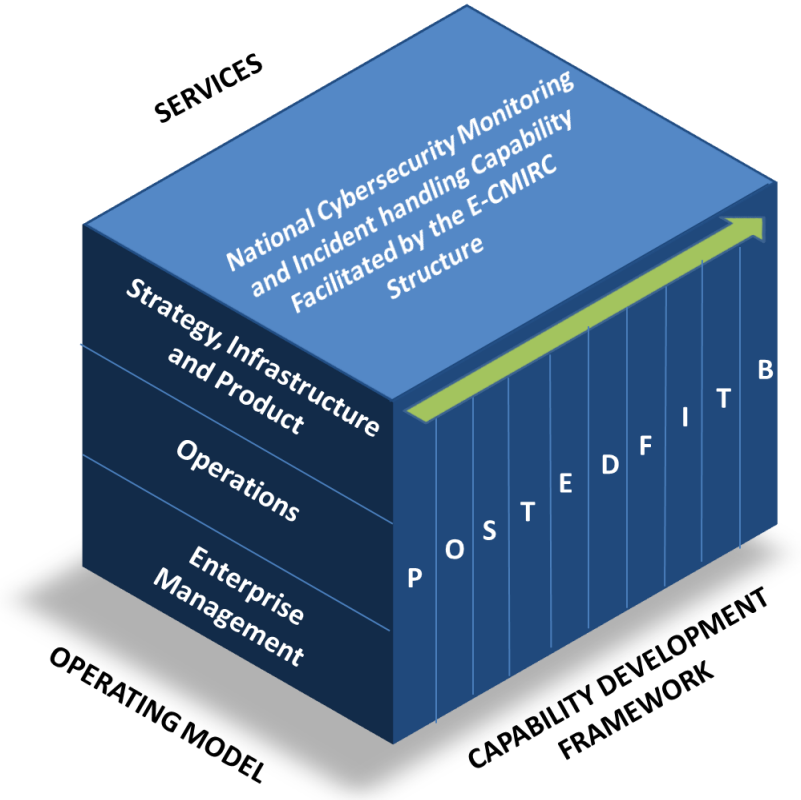

Figure 4: E-CMIRC Integrated CDM and OM Model

7. Future work

In future work, additional national cybersecurity services will be determined together with their capabilities and structures supporting them. Following a Systems Engineering approach, measures of effectiveness (MoE's) and measures of performance (MoP's) will be determined for each of the national cybersecurity capabilities. A Maturity model is also under development to baseline national cybersecurity service's process maturity, allowing process maturity to be benchmarked, and improved on at national level.

8. Conclusion

The E-CMIRC model can be used as a baseline for minimum requirements when building a national cybersecurity capability. This is achieved through the application of the E-CMIRC CDM with the POSTEDFIT-B military capability development framework adapted to address the requirements of a national cybersecurity capability. Once the national cybersecurity capability is built, is has to be operated and run effectively and efficiently. Guidance on how to effectively and efficiently manage a national cybersecurity capability is provided by the E-CMIRC OM using the TMForum's eTOM business process framework.

In building a national cybersecurity capability – whether it is a logical service, or whether the service is facilitated through a structure (such as the proposed E-CMIRC), the E-CMIRC CDM and E-CMIR OM provides a very complete, proven and scalable model for the building and implementation of national cybersecurity capabilities.

References

A. Segovia. (2015). How to handle incidents according to ISO 27001 A.16. Retrieved April 26, 2016, from http://advisera.com/27001academy/blog/2015/10/26/how-to-handle-incidents-according-to-iso-27001-a-16/

BIAN. (2016). Banking Industry Architecture Network. Retrieved October 4, 2016, from https://bian.org/

Brigadier-General C. Gildenhuys. (2013). Armour…Combat Arm of Decision, (7). Retrieved from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&cad=rja&uact=8&ved=0ahUKEwionLnXpbTPAhUrBMAKHZw9A_IQFgg8MAQ&url=http://www.army.mil.za/publications/journal/2013_publish/2/SAAJ_7%202013%20INNER%20PRINT.pdf&usg=AFQjCNHj

C. Kerr; R. Phaal & D. Probert. (2003). A framework for strategic military capabilities in defense transformation. In *11th International Command and Control Research and Technology Symposium "Coalition Command and Control in the Networked Era."* Retrieved from www.dodccrp.org/events/11th_ICCRTS/html/papers/061.pdf

Cisco Systems. (2009). Introduction to eTOM. Retrieved from http://www.cisco.com/c/en/us/products/collateral/services/high-availability/white_paper_c11-541448.html

Claes S. et al. (2014). Next Generation IT operating models - KPMG. Retrieved January 5, 2016, from http://www.kpmg.com/BE/en/IssuesAndInsights/ArticlesPublications/Documents/Next-Generation-IT-Delivery-Models.pdf

D. Cooper; S. Dhiri & J. Root. (2012). Winning operating models. Retrieved October 4, 2016, from http://www.bain.com/Images/BAIN_BRIEF_Winning_operating_models.pdf

Diamond, J. (2016). Russian hacking and the 2016 election: What you need to know. Retrieved January 16, 2017, from http://edition.cnn.com/2016/12/12/politics/russian-hack-donald-trump-2016-election/

Ed Vaizey. (2016). Two thirds of large UK businesses hit by cyber breach or attack in past year. Retrieved January 16, 2016, from https://www.gov.uk/government/news/two-thirds-of-large-uk-businesses-hit-by-cyber-breach-or-attack-in-past-year

eWorks Moodle. (2016). Content Development Demo. Retrieved January 23, 2017, from https://moodle.eworks.edu.au/mod/book/view.php?id=6988

F. Wamala. (2012). ITU Nationall Cyber security strategy guide,. Retrieved February 18, 2016, from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

G. White. (2013). Capability Based Planning… and Grass. Retrieved September 29, 2016, from http://enterprisearchitects.com/capability-based-planning-and-grass/

GCHQ. (2016). GCH-Who? Retrieved April 20, 2016, from http://www.gchq.gov.uk/Pages/GCH-Who.aspx

IBM. (2009a). Information Framework (IFW). Retrieved October 4, 2016, from http://www.ibm.com/support/knowledgecenter/SSQH9M_7.0.0/com.ibm.ws.icp.bkkpayfep1.doc/bkk/pay/paymdev/concept/ci/indstds/c_ifw.html

IBM. (2009b). Insurance Application Architecture (IAA). Retrieved October 4, 2016, from http://www.ibm.com/support/knowledgecenter/SSAVUV_7.0.0/com.ibm.ws.icp.insp_cfep1.doc/ins/pc/p_cdev/concept/ci/indstds/c_iaa.html

ISO/IEC. (2011). ISO/IEC 27035:2011 Information technology — Security techniques — Information security incident management. Retrieved February 24, 2016, from http://www.iso27001security.com/html/27035.html

ITIL. (2011). Incident Management. Retrieved June 5, 2015, from http://wiki.en.it-

processmaps.com/index.php/Incident_Management
ITU-T. (2004). Incident organization and security incident handling: Guidelines for telecommunication organizations. Retrieved April 26, 2016, from https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.409-200405-I!!PDF-E&type=items
J. Creasey. (2013). Cyber Security Incident Response Guide v1. Retrieved April 20, 2016, from http://www.crest-approved.org/wp-content/uploads/CSIR-Procurement-Guide.pdf
J. D. Christopher. (2014). CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2). Retrieved from http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program
Jacobs P. (2015). *Towards a framework for building security operation centers*. Rhodes Universtity. Retrieved from http://contentpro.seals.ac.za/iii/cpro/DigitalItemViewPage.external?lang=eng&sp=1017932&sp=T&suite=def
Kissel, R. (2013). Glossary of Key Information Security Terms. Retrieved November 9, 2015, from http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
M. Lizotte; F. Bernier; M. Mokhtari; M. Couture; G. Dussault; C. Lalancette & F. Lemieux. (2004). Towards a Capability Engineering Process. Retrieved September 29, 2016, from http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA432358
Merriam-Webster. (2016). Model. Retrieved January 29, 2016, from http://www.merriam-webster.com/dictionary/model
Milham, D. (2004). How can the eTOM Framework help Service Providers in today's market place? *Network Operations and Management Symposium*, *Volume 2*, 59–71. http://doi.org/10.1109/NOMS.2004.1317641
N. Brownlee & E. Guttman. (1998). Expectations for Computer Security Incident Response. Retrieved April 26, 2016, from https://tools.ietf.org/html/rfc2350#page-18
NATO Cooperative Cyber Defence Centre of Excellence. (2012). *National Cyber Security Framework Manual*. Retrieved from https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf
NATO Cooperative Cyber Defence Centre of Excellence. (2016). Cyber Definitions. Retrieved August 1, 2016, from https://ccdcoe.org/cyber-definitions.html
Office, C. (2011). Cyber Security Strategy. Retrieved August 17, 2016, from http://webarchive.nationalarchives.gov.uk/20120404150643/http://cabinetoffice.gov.uk/resource-library/cyber-security-strategy
Office of Government Commerce. (2000). ITIL. Retrieved from http://www.itil-officialsite.com/
Oosthuizen, R., & Roodt, J. H. (2008). Credible Defence Capability: Command and Control at the Core. *Land Warfare Conference*. Retrieved from http://researchspace.csir.co.za/dspace/handle/10204/3167
P. Cichonski; T. Millar; T. Grance & K. Scarfone. (2012a). *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology, 800-61. Revision 2*. *NIST Special Publication* (Vol. 800–61). Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
P. Cichonski; T. Millar; T. Grance & K. Scarfone. (2012b). Computer Security Incident Handling Guide (Draft). Retrieved April 25, 2016, from https://citadel-information.com/wp-content/uploads/2012/08/nist-sp800-61-draft-computer-security-incident-handling-guide-2012.pdf
P. Ditrans; A. Anand; M. Ponnuveetil; A. Acharya & S. Dash. (2016). Why New-age IT Operating Models are Necessary for Enhanced Operational Agility. Retrieved October 5, 2016, from https://www.cognizant.com/whitepapers/why-new-age-it-operating-models-are-necessary-for-enhanced-operational-agility-codex1399.pdf
P. Jacobs; S.H. von Solms & M.M. Grobler. (2016). E-CMIRC – Towards a model for the integration of services between SOCs and CSIRTs. In *Proceedings of The 15th European Conference on Cyber Warfare and Security* (p. 350). Retrieved from https://books.google.co.za/books?id=ijaeDAAAQBAJ&pg=PA350&lpg=PA350&dq=E-CMIRC+–+Towards+a+model+for+the+integration+of+services+between+SOCs+and+CSIRTs+jacobs&source=bl&ots=50kTs5LXP_&sig=vQetp1xRqVtCPukMqSi1yZgpKFU&hl=en&sa=X&redir_esc=y#v=onepa
Praxiom Research Group. (2016). ISO 27000 Infosec Definitions. Retrieved August 2, 2016, from http://www.praxiom.com/iso-27000-definitions.htm#Information_security_incident
R. Heffner. (2010). Business Capability Architecture: Technology Strategy For Business Impact. Retrieved June 2, 2016, from http://blogs.forrester.com/enterprise_architecture/2010/02/business-capability-architecture-technology-strategy-for-business-impact.html
R. Simansius. (2011). Resolution No 796 of 29 June 2011 on the approval of the programme for the

development of Electronic Information Security (Cybersecurity) for 2011-2019. Retrieved August 1, 2016, from www.ird.lt/doc/teises_aktai_en/EIS%28KS%29PP_796_2011-06-29_EN_PATAIS.pdf

Republic, C. (2014). Draft Act on on Cyber Security and Change of Related Acts. Retrieved August 1, 2016, from www.govcert.cz/download/nodeid-1246/

Roth, I. (2008). ITIL Overview. Retrieved from http://www.itilcertification.org/

SEBoK. (2016). Representing Systems with Models. Retrieved October 7, 2016, from sebokwiki.org/wiki/Representing_Systems_with_Models

Software Engineering Institute. (2016). CSIRT Frequently Asked Questions (FAQ). Retrieved June 1, 2016, from https://www.cert.org/incident-management/csirt-development/csirt-faq.cfm?

Spafford, G., Wheeler, A. J. & Mingay, S. (2012). Updates in COBIT 5 Aim for Greater Relevance to Wider Business Audience. Retrieved from https://www.gartner.com/doc/1982323

T. Graves. (2012). Service, function and capability. Retrieved June 2, 2016, from http://weblog.tetradian.com/2012/09/22/service-function-capability-again/

T. Roberts. (2014). Cyber Security Capability Maturity Model (CMM) - Pilot. Retrieved February 18, 2016, from https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cyber-security-capability-maturity-model-cmm

TMForum. (2013). Business Process Framework. Retrieved from http://www.tmforum.org/BusinessProcessFramework/1647/home.html

Tøndel, I. A., Line, M. B., & Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. *Computers & Security*, *45*, 42–57. http://doi.org/10.1016/j.cose.2014.05.003

V. Agrasala. (2010). Events vs Incidents – "Too easy" and "So confusing" at the same time! Retrieved July 29, 2016, from https://vagrasala.wordpress.com/2010/03/16/events-vs-incidents-too-easy-and-so-confusing-at-the-same-time/

White, L. (2016). Tesco Bank's Cyber Attack Investigated by UK's National Crime Agency. Retrieved January 16, 2017, from http://www.insurancejournal.com/news/international/2016/11/08/431824.htm

wiseGEEK. (2013). What is ETOM? Retrieved from http://www.wisegeek.com/what-is-etom.htm