SUSTAINABLE SECURITY ADVANTAGE IN A CHANGING ENVIRONMENT: THE CYBERSECURITY CAPABILITY MATURITY MODEL (CM^2)

Corlane Barclay
University of Technology Jamaica
237 Old Hope Road, Kingston 6

ABSTRACT

With the rapid advancement in technology and the growing complexities in the interaction of these technologies and networks, it is even more important for countries and organizations to gain sustainable security advantage. Security advantage refers to the ability to manage and respond to threats and vulnerabilities with a proactive security posture. This is accomplished through effectively planning, managing, responding to and recovering from threats and vulnerabilities. However not many organizations and even countries, especially in the developing world, have been able to equip themselves with the necessary and sufficient know-how or ability to integrate knowledge and capabilities to achieve security advantage within their environment. Having a structured set of requirements or indicators to aid in progressively attaining different levels of maturity and capabilities is one important method to determine the state of cybersecurity readiness. The research introduces the Cybersecurity Capability Maturity Model (CM^2), a 6-step process of progressive development of cybersecurity maturity and knowledge integration that ranges from a state of limited awareness and application of security controls to pervasive optimization of the protection of critical assets.

Keywords— security advantage, cybersecurity Capability Maturity Model, CM^2, security, privacy, capabilities.

1. INTRODUCTION

Privacy and security are principal concerns in today's highly connected world. The 2013 Norton Report priced the cost of cybercrime at US$113 billion [1]. This may be attributed to the numerous reports of different types of crimes and threats that have affected millions of people in different regions, such as the lottery scam in Jamaica, the Sutxnet virus, online predators and many other antisocial behaviours. Most experts agree that these incidences are a threat to national security, and can impede national development. Therefore, the challenge in this century is to defend against the "unknown, the uncertain, the unseen and the unexpected" [2], and as such, the focus should be less on the threats and more on how one may be threaten and what is needed to deter and defend against such threats [2]. While these directives were given within the context of military transformation, they also resonate within information and cyber security domain(s). Studies continue to show that the fight against cybercrimes require both offensive and defensive measures. This is necessary in an effort to gain a firm and sustainable security advantage. In this research security advantage is defined as the ability to effectively assess, plan, manage, and respond to threats and vulnerabilities through a capability-based approach. In other words, the focus is to: (1) critically examining how cyber criminals and insiders may act; (2) address weaknesses and vulnerabilities in the critical information assets and people; and (3) improve the necessary resources and capabilities (know-how) needed to achieve a more secured cyber and information environment.

For many countries achieving security advantage is a challenging task. The developing regions, which accounts for a significant portion of the online users today [3], are especially at risk since they tend to be burdened with relatively high vulnerability of cyberattacks and low resource capabilities. Therefore, the study is motivated by the search to understand whether countries know what to do to minimize threats and vulnerabilities to achieve security advantage or to identify a general security toolkit that can aid in achieving a minimum level of security assurance. It is reasoned that to move forward, an understanding of the level of readiness, requirements and capabilities needed to achieve security advantage is necessary. However an analysis of academic discourse on cybercrime and security shows that a standardized mechanism to help guide the attainment of security advantage is largely missing. Two known exceptions in this regard are the National Initiative for Cybersecurity Education's NICE Cybersecurity Capability Maturity Model [4] and The Community Cyber Security Maturity Model (CCSMM) [5]. NICE's model comprises of three levels and is centred on the skilled practitioners, integrated governance, and process and analytics for workforce planning in the organization. CCSMM may be considered threat-centred where each level is indicative of the types of threats and the associated activities at each level.

The current state of art suggests that additional discourse on cybersecurity maturity models should have certain requirements: possess proactive and offensive strategies; grounded in academic literature; and aligned to the dynamism of the environment. Additionally, continued development of threat-based and/or capabilities-based solutions and their impact need to be evaluated from an academic standpoint to propel innovation in this important

area. This research delve in this arena by coupling a mature area i.e. maturity models with the evolving area of cybersecurity to offer a capability-centred solution to improving competencies that is targeted at deriving effective responses to cybersecurity threats and vulnerabilities.

This research presents the Cybersecurity Capability Maturity Model (CM^2). CM^2 is a model that illustrates the stages of readiness or preparedness to respond to threats, vulnerabilities and technological advancement that exists within the continuously evolving environment. CM^2 includes six steps centred on "capability-constituents" of society, operational, education, technical, business and legal and regulatory measures. The spectrum of maturity and capability include undefined, initial, basic, defined, dynamic and optimizing stages. CM^2 relies on the principles of the Capability Maturity Model [6], theories on capabilities [7], [8], [9], knowledge integration and security practices to guide its initial development.

The Design Science (DS) methodology is applied in the development of the CM^2 artifact. This approach is chosen because it involves the analysis of the designed artifacts to help understand, explain and improve on the behavior of the social systems that the artifact becomes a part of [10]. Within this context, many countries are without formal measures or know-how to achieve security advantage or are using rudimentary tools that put them at a disadvantage and impede the development of sound cyber/information infrastructure. Therefore, this study hopes to extend the discourse on cybersecurity and contribute to practice by providing an artifact that offers utility in improving security routines and practices, which it is hope will lead to a safer networked environment. It also offers significance to standard development since the identification of commonly agreed capabilities can be used as indicators to a country's level of preparedness and serve to inform national strategies and policies.

2. RESEARCH BACKGROUND

2.1. Cybercrime, Security and Strategy

Routine Activity Theory [11] [12] is one seminal theory that is commonly used to explain how crime risks increases in the current technological landscape. It suggests that crime risks increases on the convergence of a motivated offender, a suitable target and the absence of a capable guardian. Based on the nature of the Internet, proliferation of social networking sites and other applications and limited awareness of users, the rate of cybercrimes is likely to continue to increase. Therefore capable guardianship is imperative.

There are multiple definitions of cybercrime with no consistent definition to date. A review of the definitions shows general inclusion of traditional illegal behaviours and new forms of criminal acts done electronically or with a computer device. However according to Gercke [13], it is not important that there is no single definition as long as the term is not used as a legal term. A useful classification distinguishes between four different types of offences: offences against the confidentiality, integrity and availability of computer data and systems; computer-related offences; content-related offences; and copyright-related offences [14].

Cybersecurity also has varied definitions. It can be considered broadly as the protection of computers, networks, programs and data from unintended or unauthorized access change or destruction [15]. However, it can be said that the scope and coverage have been extended to include critical assets, including information assets or infrastructure, people and even processes. For instance, the US in a 2013 Cybersecurity Executive Order [16] identified its national critical infrastructure to be its natural gas and oil pipelines, storage sites and refineries as well as electric generation, transmission and distribution facilities. Other countries will likely have context specific assets that are due priority attention and protection from cyber threats. The ITU [17] provided a comprehensive definition that includes in part the "*the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.*" The definition underlined the necessity for improvements in skills and knowledge to produce the necessary safeguards and guidance that can be followed to provide security assurance.

An understanding of cybercrime and security is a necessary step in the provision of offensive and defensive measures for a more secured environment. The strategy defines how these measures are operationalized and therefore form an important step in developing effective security posture at the organizational or national level. For instance, McAfee proposed a multi-point strategy to fight cybercrime to include legal frameworks and law enforcements, education and awareness, and technology and innovation [18]. In the UK, it has been quoted that the launch of its national strategy has helped it to become more secure in doing business [19]. Whether real or imagined, at minimum a national cybersecurity strategy will help in positively influencing confidence from both business partners and consumers. Interestingly, the 2013 UN Report [20] revealed that only 30% of responding countries indicated the existence of a national cybercrime strategy. Countries in Africa, Asia and Oceania reported the lowest levels of cybercrime strategies with around 50% of these countries indicating that such an instrument did not exist. This further underlines the challenges in many countries to identify or harness the capabilities to successfully integrate security knowledge and promote national security. This in turn indicates a general risk to achieving security advantage.

2.2. Capabilities and Competitive Advantage

Organizational capabilities constitute the fundamental source of sustained competitive advantage [9]. Capabilities are alternatively referred to as knowledge, competencies, routines or innovations within the organization. The dynamic capabilities theory is one of the principal theories on developing organizational capabilities [8]. Teece et al [7] described dynamic capabilities as the "*ability to integrate build and reconfigure internal and external competences to address rapidly changing environment*". It underlined the need to be flexible and dynamic in addressing resource demands based on the changing environment. This viewpoint is also a suitable strategy in today's networked environment.

Barney [21] described competitive advantage as the ability to implement a value creating strategy that is not simultaneously being implemented by any current or potential competitor. Similarly sustained competitive advantage is competitive advantage combined with other firms' inability to duplicate the benefits of the value creating strategy. Placing perspective within the context of security environment, an advantage is sought over the criminals, therefore it can be constituted as rivalry with cybercriminals where the country's ability to implement an effective security strategy that cannot be (easily) penetrated by criminal insiders and outsiders would be considered a security advantage. Sustained security advantage therefore is the achievement of security advantage and criminals' inability to exploit vulnerabilities due to the country's ability to keep pace with criminals' tactics, harness technological advancement and support continuous capacity building and development.

Multiple sources of competitive advantage are proffered by experts that provide a platform for understanding security advantage. For instance, knowledge [22], Information & Communication Technologies (ICT) [23], Human resources [24], customer value [25] have been cited. Porter [26] also identified five forces that shape competitiveness as the bargaining power of suppliers and buyers, threats of new entrants and substitute products or services and rivalry among competitors. Porter [27] further suggested that a nation's competitiveness depends on its capacity to innovate and upgrade and offered four determinants of national competitive advantage. Factors conditions - the nation's position in factors of production such as skilled labour or infrastructure. Demand conditions – the nature of home market demand for product and service. Related and supporting industries – the presence or absence of supplier industries and other related industries. Strategy, structure and rivalry – conditions governing how companies are created organized managed along with the nature of domestic rivalry. Drawing a parallel to the security environment these sources of competitiveness may relate to capacity of the citizens, the nature of security development in the country and demand for privacy and security, network of products and services to support the security demand conditions and the nature of the dynamism in the environment, rivalry with criminals and how security strategies are created, organized and managed.

2.1. Capability Maturity Model

The Capability Maturity Models (CMMs) including CMM Integration (CMMI) were developed to provide process improvement in organization processes including software development and management cycle. CMMs contain the essential elements of effective processes for one or more bodies of knowledge and are based on the works of researchers such as Crosby, Juran, Deming and Humphrey [6]. The key differences between CMM and CMMI are that CMM was designed for the software industry specifically has 18 process areas while CMMI has applicability to other industries and has 25 process areas.

The purpose of CMMI is to provide guidance for improving the organization's processes and ability to manage the development, acquisition, and maintenance of products or services. The CMMI is noted to aid in improving product quality, reducing cycle time and cost and improving ability to meet project targets. There are six capability levels, designated by the numbers 0 through 5:

0. Incomplete
1. Performed
2. Managed
3. Defined
4. Quantitatively Managed
5. Optimizing.

An incomplete process as the name suggests is a process that is either not performed or partially performed. This may occur where one or more of the specific goals of the process area are not satisfied. Capability level 1 process is characterized as a performed process that is characterized by unpredictability and is primarily reactive in nature. Level 2 is characterized by processes that are repeatable. It also uses basic project management to track cost and schedule and is reactive is nature. Level 3 is a proactive process level and characterized by defined processed that are well understood by the organization. Standards, procedures, tools and methods are developed to aid completion of tasks. Level 4 is characterized by measurement where quality and process performance are established and used as criteria in managing the process. The quality and process performance are understood in statistical terms and are managed throughout the life of the process. Level 5 is characterized as an optimizing process that is changed and adapted to meet relevant current and projected business objectives. The level focuses on continually improving the process performance through both incremental and innovative technological improvements.

3. DS RESEARCH APPROACH

DS research methodology involves the creation and evaluation of artifacts that can be used to solve identified problems in the environment [28]. An artifact can be described as an entity or thing that has, or can be transformed into, a material existence as an artificially made object (e.g. model and instantiation) or process (e.g.

method and software) [28] [29]. In short the artifact may include any designed solution or object that solves a problem within a context [30] [31], thereby providing a link between research and practice [31]. This research thereby seeks to develop a standardized model to aid in the determination of a country or organization's readiness and preparedness to effectively counter cybercrimes and manage cyber security processes. The CM^2 is the artifact, a formal capability maturity model, where the model is a simplified representation of the world [8]. Its originality is in the structure and characteristics of the maturity levels. In order words, the capability-focused approach to addressing security threats and vulnerabilities and a formal defined view of security advantage provide novelty.

DS research contribution can be categorized into an invention, improvement, or exaptation [10]. An invention presents new solutions to new problems. It is a radical breakthrough that is a clear departure from the accepted ways of thinking and doing. An improvement creates better solutions in the form of more efficient and effective products, processes, services, technologies, or ideas by developing new solutions for known problems. Exaptation involves an extension of known design knowledge into a new field which is non-trivial and interesting, that is, extending known solutions to new problems. This study therefore offers contribution in the form of an improvement where the known solution of maturity models are used to apply in the cyber and information security domain(s) to outline the stages of progressive development an entity can take as it improves its maturity and capability in the management of cybersecurity. This contribution is a departure from existing models (e.g. [4] [5]) in terms of both form and substance. The six stages of capabilities provide a more realistic roadmap or at minimum an alternative roadmap, and focuses not on the threats but the capabilities needed to achieve security advantage.

This approach is suitable for this research since it serves to provide a link between research and practice in the development of CM^2 thus providing a contribution in the form of an improvement to the current knowledge base. Further, the DS methodology has been applied successfully in multiple contexts which have some parallel to this study, for example in project management [32], cybersecurity strategy development [33] and engineering method [34].

Peffers et al [31] provide a clear outline of the steps necessary to help assure the successful application of the DS methodology (Figure 1).

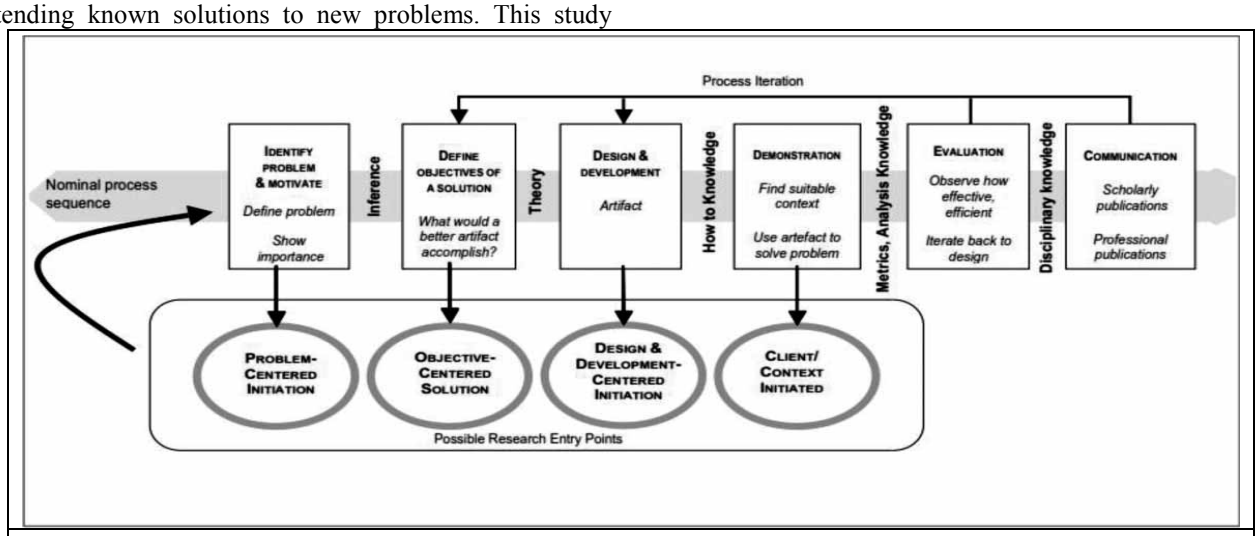

Figure 1. DS methodology process model (Peffers et al., 2007)

Step 1: Problem identification and motivation. The research problem and justification of the value of a solution are identified at this stage. It is noted that cybercrimes continue to proliferate new vulnerabilities are detected including zero-day vulnerabilities, insider and outsider threats. Two key issues are underlined, the resources needed to effectively defend a group's critical information asset and people are mounting and there is a lack of standard process or measures to help determine how one is doing or what requirements are necessary to effectively manage. Therefore, there is the motivation to offer a standardized tool that can aid in this objective.

Step 2: Objectives of a solution. Based on the identified problem and motivation, the objectives of the solution are identified. The objectives of the study is to offer a model that can be used as a basis for assessment of readiness to effectively many cyber security considerations and acknowledge the capabilities required to do so.

Step 3: Design and development. This involves the solution or artifact is created to address the outcome of the previous steps. CM^2 is influenced by several considerations, creation of the solution or artifact. As noted previously, the CMM Model [6], and theories of capabilities [7] [8] and perspectives are used to inform the characteristics of the model. Six steps of progressive maturity to tackle cyber security issues are offered. This is explained in detail in the subsequent section. It is anticipated that several rounds of development and refinement will be required to enhance the features of the artifact.

Step 4: Demonstration. Explication of how the artifact fulfills its objectives or solves the stated problem(s) is done. At this stage of the research, a proof of concept of the artifact is demonstrated through the use of informed arguments to illustrate the solution's utility and relevance. This demonstration strategy is appropriate based on the suggestions of Gregor and Hevner [10] and Hevner, et al [30].

Step 5: Evaluation. The evaluation step observes and measures how well the artifact supports a solution to the problem. It involves comparing the objectives of a solution to actual observed results from use of the artifact in the demonstration. Hevner et al [28] proposed five types of evaluation approaches which have been used extensively in DS studies. Descriptive evaluation method that includes the use of informed arguments is used here. Future efforts will include application of other types of evaluation techniques.

Step 6: Communication. This step involves communicating the artifact's development. The problem and its importance, the artifact, its utility and novelty, the rigor of its design, and its effectiveness to researchers and other relevant audiences are shared. This step is applied through the reporting of the artifact's background and characteristics in this paper.

4. CYBERSECURITY CAPABILITY MATURITY MODEL (CM^2)

CM^2 is intended to provide guidance on the necessary considerations and requirements to achieve and maintain security advantage. The principal underlying pillars are *society, technical, operational, business, legal and regulatory, and education/capability building* measures. CM^2 can serve as a basis of comparative assessment across nations and over time engender cross-border collaboration through buy-in. The initial conceptual characteristics are outlined in this section.

4.1. Security Advantage & Capabilities

To promote security advantage through advancement in capabilities, a five factor model is proposed. This 5-factor model in turn influences the stages of CM^2 as the basis for capability development in cybersecurity. It is proposed that to achieve sustainable security advantage countries need to dynamically build its capabilities to counter threats, vulnerabilities and advance with technology. Technological development will serve as an enabler to further advancement and a platform for new threats and vulnerabilities. The environment consists of rivalry and dynamisms due to events such as technological development, changes in social norms and other factors. Threats from criminal insiders and outsiders, vulnerabilities in critical assets and capabilities of members of the society interact where the more advanced the capabilities the better able the society is to counter any changes or shock from the other factors, figure 2. Capabilities span the pillars and ought to be responsive to the dynamism of the environment. Therefore, at the national level focus can be on development of capabilities in different areas or pillars to enhance security advantage.

Development of capabilities is the central theme in advancing maturity towards managing cybersecurity. Analysis of the environment and literature has shown that competencies that extend beyond technical measures are imperative to combating cybercrimes [13] [35]. Progressive development of routines and competencies in the different areas are envisioned as different stages of maturity are achieved. Further, it is expected that an optimal mix of capabilities necessary to maintain security advantage will evolve with changes in the environment. The levels of integration of knowledge impacts the maturity levels illustrated in CM^2. Teece et al [7] identified three characteristics of knowledge integration that are applicable here: *efficiency, extent and flexibility*. In other words, the depth and breadth of integration of capabilities, combined with ability to dynamically respond to environmental changes across sectors can be sound indicators of advancement.

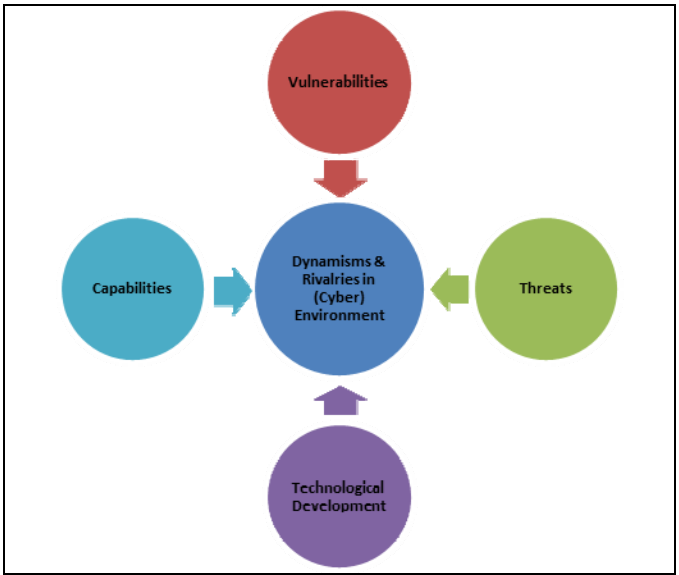

Figure 2. 5-Factor Model of the Cyber-environment

Education and capacity building measures promote learning on the requisite areas necessary to enhance proactive responses to cyber crimes and security. Areas of technical competency aligned to the security bodies of knowledge, laws, standards and regulations, psychology could be part of the core focus for example and will impact the other areas. The promotion of formal education from primary to tertiary levels, research and awareness across all sectors of society are anticipated. *Technical* measures promote advancement in the solutions necessary to develop and evaluate critical assets, hardware, software and network infrastructures, vulnerabilities and security. This may include areas of network and computer security, social engineering, digital forensics, surveillance, analytics among other areas. *Business* measures consider the strategic level considerations necessary to assure success of the operational targets, including development and evaluation

of national strategies, policies and standards. International cooperation is also an integral part of this area. *Operational measures* involve the tactical countermeasures and strategies employed on a daily basis. Society and business responses inform the tactics. *Legal and regulatory* measures consider the full process implications of legislative development, implementation and enforcements. Therefore, it considers activities beyond the development of appropriate laws to the supporting processes to ensure that the laws are effective and are being enforced. The resources and capabilities necessary to support this endeavour are also undertaken. As is seen, the capabilities and pillars are tightly coupled and impact each other within the society. Constraints and limitations that are context-specific will impact the progression across the levels. For example, developing economies may be faced with monetary challenges to undertake certain initiatives.

4.2. Level of CM^2

There are six capability and maturity levels for improving security advantage and cybersecurity capabilities which are indicated by the levels 0 to 5, table 1. The stages of human development are used to define the transition since a corollary can be seen, in that, through advancement in age and experience maturity is generally achieved. Also, it helps to clearly describe the level of capabilities or competencies in cybersecurity achieved at each stage (figure 3):

0. Undefined or Prenatal;
1. Initial or Infant;
2. Basic or Child;
3. Defined or Adolescent;
4. Dynamic or Adult;
5. Optimizing or Sage.

Level 0 stage is characterized by an undefined process which is the lowest possible level of capabilities. At this stage there is a lack of coordinated cybercrime strategy, policies or existing laws. In other words, efforts are largely non-existent. Some reports [17] [20] may indicate that there may be developing economies that are still at this stage due to lack of any formal national cybersecurity strategy for example or any clear mechanisms for responding to threats and vulnerabilities.

Level 1 stage is characterized by an initial process that is at an infancy level and efforts are predominantly fractured and disconnected. This suggests that cybersecurity initiatives may be in existence however these are largely uncoordinated. Additionally, at the national level, only one area of capability is the initial centre of focus, for example, a technical measure such as development of emergency response team (CERT). Also, the approach is largely reactive and threat-based. Therefore, a focus on an implementation of specialized team e.g. a CERT without coordinated solutions in areas of legislation, capacity building and general awareness would indicate a country's first step in a complex journey of preparedness.

Level 2 stage is characterized by a basic stage that improves on the initial stage. There is still a reactive and threat-based approach, and at minimum, one additional capability is considered, such as an implementation of a CERT program accompanied by ad-hoc legislative development. Here the focus is still on threats therefore any devised strategies will only be in response to perceived threats or vulnerabilities that are considered high priority.

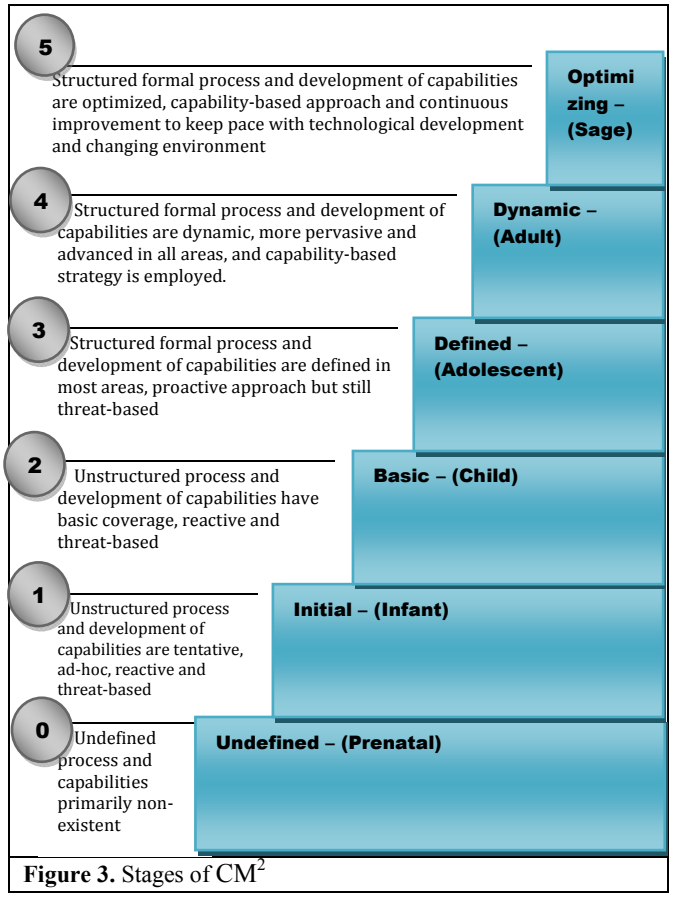

Figure 3. Stages of CM^2

Level 3 stage is characterized by a defined process that improves on the basic stage. The approach is more coordinated, and likely to be government or agency led. A majority but not all of the capabilities are the focus of the cybersecurity approach at the national level. Therefore, considerations across the spectrum of capacity development, legal requirements, technical and operational considerations, etc would likely be represented in a formal strategy or policy. There is also a good level of knowledge integration with a shifting to proactive offensive measure such as monitoring and detection capabilities, and legislative development and enforcement

Level 4 stage is characterized by a dynamic process that improves on the defined stage. Capability-centred approach to cybersecurity management is undertaken with strong coordinated and proactive measures. All the capabilities are undertaken with strong emphasis on education and training for example. Therefore critical assessment is made of the environment with prediction of trends, and strategies or countermeasures are developed to respond. In other words, the areas of technical measures, business, legislative and

regulatory measures and capacity building are considered individually and holistically to improve security advantage.

Level 5 stage is characterized by an optimizing process that improves level 4 or the 5th stage of maturity. A capability-centred -approach to cybersecurity management is also undertaken with coordinated proactive measures. All the pillars of capabilities are harnessed with strong emphasis on innovation and research with advanced prevention and detection measures available across key sectors of society. Innovative approaches are continuously examined and developed to improve and maintain a secured environment. This may also result in playing a role in global governance of the environment.

It is worth noting that while the study is influenced CMMs [6], it does not seek to be a replica and offers its own unique contributions. The CM^2 distinguishes itself through distinct indicators and areas of cybersecurity capabilities. The levels of knowledge integration of the pillars of capabilities (i.e. society, education, operational, technical, business, and legal) are used as the basis to indicate the levels of maturity in CM^2. CM^2 is distinct from CMMI is following ways: it is not relating to software or an industry but rather the environment since a holistic view is necessary to respond to cybersercurity concerns; the stages of maturity are determined by multi-dimensional capabilities; and it is not focused on measurement or to be quantitatively management but rather on a comprehensive multi-perspective strategy to creating and maintaining security advantage. It also distinguishes itself from existing cybersecurity models in its approach by adopting a capability-centred approach and using different indicators for maturity.

The CM^2 can provide utility to countries interested in developing capabilities to enhance their cybersecurity efforts. Although it is preliminary stages the dimensions or pillars of capabilities identify possible areas of focus that ought to be considered in a holistic and coordinated cybersecurity strategy.

Table 1. CM^2 - Overview of Capabilities

INDICATORS	LEVEL 0 UNDEFINED	LEVEL 1 BASIC	LEVEL 2 INITIAL	LEVEL 3 DEFINED	LEVEL 4 DYNAMIC	LEVEL 5 OPTIMIZING
Attitude to threats & vulnerabilities	Largely ignorant	Basic awareness	Reactive	Reactive	Proactive	Highly proactive
Technological Development	Limited awareness and use	Basic use	Effective use	Effective use and application	Innovation	Pervasive innovation
Societal response	Limited levels of awareness and efficiency and largely inflexible	Low levels of awareness, low efficiency and inflexible	Medium levels of awareness, efficiency and flexibility	Medium to High levels of awareness, efficiency and flexibility	High levels of awareness, efficiency and flexibility	Pervasive levels of awareness, efficiency and flexibility
Technical measures	Undefined/ Limited	Unstructured ad-hoc measures	Unstructured Threat-based measures	Structured threat-based measures	Structured capability-based measures	Highly structured capability-based measures
Business measures	Undefined/ Limited	Unstructured ad-hoc measures	Unstructured Threat-based measures	Structured threat-based measures	Structured capability-based measures	Highly structured capability-based measures
Legal & Regulatory measures	Undefined/ Limited	Unstructured ad-hoc measures	Unstructured Threat-based measures	Structured threat-based measures	Structured capability-based measures	Highly structured capability-based measures
Operational measures	Undefined/ Limited	Unstructured ad-hoc measures	Unstructured Threat-based measures	Structured threat-based measures	Structured capability-based measures	Highly structured capability-based measures
Education/capability building measures	Undefined/ Limited	Unstructured ad-hoc measures	Unstructured Threat-based measures	Structured threat-based measures	Structured capability-based measures	Highly structured capability-based measures

5. CONCLUSION

The research underlines the importance of achieving and maintaining security advantage in the today's society. Two contributions are presented: the development of the 5-factor model capability perspective and the development of the capability-focused cybersecurity capability maturity model. The 5-factor model serves as a basis for the key considerations for developing and maintaining security advantage where there is a paradigm shift from threat-based perspective and toward capability-based perspective. Thus, the focus is on the development of capabilities encompassing the development of key human resources and attention to innovation to keep pace with technological development, threats and vulnerabilities within the dynamic environment. The (CM^2) is introduced as a basis to help guide nations in the development of competencies and skills necessary to proactively manage the dynamism and rivalries in the cyber environment. Six stages of maturity are proposed from level 0 to level 5 where the efficiency, extent and dynamism of the capabilities are used as the basis to determine advancement. The study contributes to both research and practice. It is now accepted that discourse on cybersecurity must extend beyond technical solutions [13][35], therefore this study extends the discourse to include considerations that hitherto resides in management and strategy domains. Government and policymakers can find value and utility in the CM^2 artifact. Development of policies can be guided by attention to specific pillars of capabilities to gradually enhance citizens' skills and

competencies in cybersecurity and develop maturity over time, for example.This study is still in its infancy and the indicators and characteristics across each pillar are being developed and will be part of future work. Specific set of characteristics and indicators at each level of maturity will also be developed. Future studies will also involve overcoming current limitations and improving the artifact based on consultations with potential users. Assessment of countries across multiple regions and their placement in the CM^2 model will also be explored. The security advantage construct will also be further examined.

REFERENCES

[1] Norton 2013 Report, http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013 (visited on 2013-12-07)

[2] Rumsfeld, D. H. (2002). Transforming the military. Foreign Aff., 81, 20.

[3] Chen, W., & Wellman, B. (2004). The global digital divide–within and between countries. IT & society, 1(7), 39-45.

[4] National Initiative for Cybersecurity Education (NICE). Cybersecurity Workforce Framework. NICE, 2011. http://csrc.nist.gov/nice/framework/documents/national_cybersecurity_workforce_framework_printable.pdf (visited on 2014-02-22)

[5] White, G. B. (2011, November). The community cyber security maturity model. In Technologies for Homeland Security (HST), 2011 IEEE International Conference on (pp. 173-178). IEEE.

[6] CMMI, Team, C. P. (2002). Capability Maturity Model® Integration (CMMI SM), Version 1.1. Software Engineering Institute, Carnegie Mellon University/SEI-2002-TR-012. Pittsburg, PA.

[7] Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. Strategic management journal, 18(7), 509-533.

[8] Teece, D., & Pisano, G. (1994). The dynamic capabilities of firms: an introduction. Industrial and corporate change, 3(3), 537-556.

[9] Grant, R. M. (1996). Prospering in dynamically-competitive environments: organizational capability as knowledge integration. Organization science, 7(4), 375-387.

[10] Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. Management Information Systems Quarterly,37(2), 337-355.

[11] Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American sociological review, 588-608.

[12] Felson, M., & Cohen, L. E. (1980). Human ecology and crime: A routine activity approach. Human Ecology, 8(4), 389-406.

[13] Gercke M. (2012), Understanding cybercrime: phenomena, challenges and legal response 2012, http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm (visited on 2013-12-01)

[14] Council of Europe Convention on Cybercrime (CETS No. 185), available at: http://conventions.coe.int

[15] http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm (visited on 2013-12-01)

[16] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity. (visited on 2013-12-01)

[17] ITU, Overview of Cybersecurity, http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx (visited on 2013-12-01)

[18] McAfee, Multipoint Strategy to Fight Cybercrime, http://www.mcafee.com/us/resources/misc/mfe-plan-to-fight-cybercrime.pdf.

[19] Marshall, T. Cybercrime Strategy 'Has Made UK Secure, http://news.sky.com/story/1181481/cybercrime-strategy-has-made-uk-secure (visited on 2013-12-01)

[20] UN 2013, Comprehensive Study on Cybercrime, http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (visited on 2013-12-08)

[21] Barney, J. (1991). Firm resources and sustained competitive advantage. Journal of management, 17(1), 99-120.

[22] Argote, L., & Ingram, P. (2000). Knowledge transfer: A basis for competitive advantage in firms. Organizational behavior and human decision processes, 82(1), 150-169

[23] Powell, T. C., & Dent-Micallef, A. (1997). Information technology as competitive advantage: the role of human, business, and technology resources. Strategic management journal, 18(5), 375-405.

[24] Barney, J. B., & Wright, P. M. (1997). On becoming a strategic partner: The role of human resources in gaining competitive advantage.

[25] Woodruff, R. B. (1997). Customer value: the next source for competitive advantage. Journal of the academy of marketing science, 25(2), 139-153.

[26] Porter, M. E. (2008). The five competitive forces that shape strategy. Harvard business review, 86(1), 78

[27] Porter, M. E. (2011). Competitive advantage of nations: creating and sustaining superior performance. Simon and Schuster.

[28] Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS quarterly, 28(1), 75-105.

[29] Goldkuhl, G., & Cronholm, S. (2003). Multi-grounded theory: Adding theoretical grounding to grounded theory. In Proceedings of the 2nd European Conference on Research Methods in Business and Management Studies (ECRM 2003), MCIL, Reading, UK (pp. 177-196).

[30] Gregor, S., & Hevner, A. R. (2011). Introduction to the special issue on design science. Information Systems and e-Business Management, 9(1), 1-9.

[31] Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research.Journal of management information systems, 24(3), 45-77.

[32] Barclay, C., & Osei-Bryson, K. M. (2009). Toward a more practical approach to evaluating programs: The Multi-Objective Realization approach. Project Management Journal, 40(4), 74-93.

[33] A. Dennis, R. Jones, D. Kildare C. Barclay & A. Gordon. (2013). Developing A National Cybersecurity Framework for Jamaica: A Design Science Approach, Proceedings of the 12th International Conference on Social Implications of Computers in Developing Countries, Montego Bay, Jamaica

[34] Rosenkranz, C., & Holten, R. (2011). The variety engineering method: Analyzing and designing information flows in organizations. Information Systems and e-Business Management, 9(1), 11–49.

[35] Barclay C. (2013). Using Frugal Innovations to Support Cybercrime Legislations in Small Developing States: Introducing the Cyber-Legislation Development and Implementation Process Model (CyberLeg-DPM). Information Technology for Development, 1-31.