Can maturity models support cyber security?

Ngoc T. Le
University of Technology Sydney
Faculty of Engineering & IT
Broadway NSW 2007 Australia
NgocThuy.Le@student.uts.edu.au

Doan B. Hoang
University of Technology Sydney
Faculty of Engineering & IT
Broadway NSW 2007 Australia
Doan.Hoang@uts.edu.au

***Abstract* - We are living in a cyber space with an unprecedented rapid expansion of the space and its elements. All interactive information is processed and exchanged via this space. Clearly a well-built cyber security is vital to ensure the security of the cyber space. However the definitions and scopes of both cyber space and cyber security are still not well-defined and this makes it difficult to establish sound security models and mechanisms for protecting this space. Out of existing models, maturity models offer a manageable approach for assessing the security level of a system or organization. The paper first provides a review of various definitions of cyber space and cyber security in order to ascertain a common understanding of the space and its security. The paper investigates existing security maturity models, focusing on their defining characteristics and identifying their strengths and weaknesses. Finally, the paper discusses and suggests measures for a sound and applicable cyber security model.**

Keywords – cyber space; cyber security; maturity model; security maturity model; cyber security metrics

I. Introduction

Historically, the definition of cyber security has evolved greatly over the past decades. From the fundamental concept of security, it is defined as the quality or state of being secure - being free from danger [1]. For example, national security can be known as a system of multilayered processes that protect sovereign of a state - its assets, resources, and people against all kind of "national" crises [2]. Therefore, cyber security can be thought of as a system of processes that protect the resources of cyber space. However, definitions of cyber security vary with different organizations. Some use the term “cyber security” but others prefer “information security” or “IT security” [3]. One of the reasons for this usage is that people consider both the cyber space and cyber security from different perspectives. The definition of cyber space has changed considerably since Wiener defined cybernetics in 1948 as *“control and communication in the animal and the machine”* [4]. Over the last few decades, academic organizations focused on the tangible elements in the cyber space when they paid more attention to the infrastructure components of IT systems, and on intangible elements such as the data or the applications within these systems. Recently, the cyber space has grown to include social networks, clouds, Internet of Things (IOTs), smart cities, smart grids, and other software-defined systems.

In order to protect the cyber space, there have been many security models developed. Each focuses on a particular security angle such as risk, asset, identification, physical components, network, data, and application. Hardly a security model considers the security of a system as a whole. It is known that a single minor vulnerability can bring down the whole system and there are myriads of these vulnerabilities. Security models are still being developed. In recent years, a number of security maturity models have been proposed for overall security management.

In 1989, Humphrey recommended a capability maturity model for software quality assessing [5]. This basic model has been adapted for cyber security for a number of reasons. First, security models based on capability maturity model have been applied with reasonable successes for many fields such as IT, business. Second, maturity models provide a completed management process for cyber security. Third, they can be extended to cover many security aspects or domains. Recently, maturity model has been applied for securing many important cyber space such as e-government, e-commerce, education, health, particular in critical national infrastructure such as electricity, water supply, petrol, and transportation [6]. This paper provides a comprehensive review of various definitions of cyber space and cyber security. Prominent cyber security maturity models from 2000 will be discussed and analyzed to identify how they apply to cyber security. Moreover, this paper compares those existing security maturity models, underlines their common aspects, highlights their differences, and more importantly identifies features that have to be addressed in a comprehensive cyber security maturity model.

The remainder of this paper is organized as follows. Section II and III review various definitions of cyber space and cyber security respectively in order to ascertain a common understanding of the space and its security. Section IV investigates the definition of security model, the maturity model, and compares existing cyber security maturity models to identify the strengths and weaknesses of these models. Finally, we discuss features needed for a sound security maturity model.

II. Cyber Space

A. Cyber space

According to Oxford dictionary, it is a single word "cyberspace". However, some authors use two words as in "cyber space", and others prefer "cyber-space". Some organizations use the term "information" as "cyber or cyber space"

In terms of the concept of cyber space, it has been defined and redefined over the years in order to take into account not only emerging technological developments but also the complexity of modern social networks. From the ITU [7], *"the cyber environment includes users, the Internet, the computing devices that are connected to it and all applications, services and systems that can be connected directly or indirectly to the Internet, and to the next generation network (NGN) environment, the latter with public and private incarnations"*. With this definition, the cyber space covers computing elements, resources, and the interconnecting infrastructure as well as users. However, it does not entail interaction among these elements.

The US National Security Presidential Directive 54/Homeland Security Presidential Directive 23, 2008, defines cyber space as *"the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries"* [8]. This definition emphasizes on critical industries and the interdependency among information elements through interconnecting infrastructures.

In contrary, the European Commission defines cyber space as *"the virtual space in which the electronic data of worldwide PCs circulates"* [9]. The definition focuses on electronic data and its abstract operational infrastructure.

Different countries, in their cyber security strategies, define cyber space in a narrow sense. According to Australia's Cyber Security Strategy [10], cyber security refers to the safety of computer systems. This implies that cyber space is just about computer systems and many elements are not included. According to Canada's Cyber Security Strategy [11], cyber space is the electronic world created by interconnected networks of information technology and the information on those networks. It is a global common where people are linked together to exchange ideas, services and friendship. According to The Netherland's National Cyber Security Strategy [12], Cyber security refers to efforts to prevent damage caused by disruptions to, breakdowns in or misuse of Information and Communication Technology (ICT). Cyber space is all things within the realm of the ICT. According to Germany's Cyber Security Strategy [13], cyber space is the virtual space of all IT systems linked at data level on a global scale. According to New Zealand's Cyber Security Strategy, cyber space is considered as the global network such as the Internet [14].

The definition of cyber space is thus quite diverse. It is exactly this point that leads to different emphases in the definitions of cyber security.

B. Elements of the cyber space

In order to clearly identify elements of the cyber space, many authors classify them into categories. Damir Rajnovic differentiated three broad categories of elements: tangibles, intangibles and network-related items in the definition of cyber space [15]. Rain Ottis and Peeter Lorents took into account the time and human element in defining cyber space [16]. They defined cyber space as "a time-dependent set of interconnected information systems and the human users that interact with these systems". With this definition, human and interaction are at the center of operation of cyber space"; specifically they asserted *"Cyber space is an artificial space, created by humans for human purposes."* Shackelford noted two aspects of cyber space: *"First, cyber space is commonly conflated with the Internet as a global network of hardware, emphasizing the critical infrastructure concerns of governments. Second, cyber space has been conceptualized as a domain to be dominated"* [17]. One is a physical interconnected critical infrastructure and the other is a conceptual space for interaction.

TABLE I.
Cyber space entities referenced in the definition of cyber space by various cyber space government strategies and organizations

Organization/ Nation	Real -Virtual	Infrastructure	Interaction
ITU	*	*	
EC	*		
Australia	*		
Canada	*	*	
Denmark	*	*	
Germany	*	*	
Japan	*	*	
Netherlands	*		
New Zealand	*		*
Norway	*	*	
UK	*	*	*
USA	*	*	*

* Element referenced by the definition

From the discussion above on the variations in the definition of cyber space by various governments and organizations, we suggest a definition that consolidates the common elements of these definitions but in addition, embraces the dynamic aspect of the cyber space: the interaction of entities. We suggest that a cyber space consists of 3 key elements: real and virtual entities, interconnecting infrastructure, and interaction among entities through the infrastructure. Real and virtual entities include real things of physical devices such as computers, sensors, mobile phones, electronic devices and virtual abstraction of entities such as data/information, software, and services. Infrastructure includes networks (e.g., the Internet), databases, information systems and storage that interconnect and support entities in the space. Interaction encompasses activities and interdependencies among cyber space entities (that are capable of interacting including human beings) via the interconnecting infrastructure and the information within concerning communication, policy, business and management.

The Table 1 shows the existence of these three key elements in various definitions from different countries and organizations. We identify that real-virtual entity is referenced in all definitions; most definitions explicitly include infrastructure; and some definitions consider interaction.

In order to provide a common understanding of the space and its security, we suggest a unified definition of the cyber space as *the space that embraces all three key elements: real and virtual entities, interconnecting infrastructure, and interaction among entities*. In particular, the emphasis is on interaction as it is fundamental to security; without interaction among entities, including human beings, the question on security may not make sense.

III. Cyber Security

As mentioned earlier, before the term "cyber security" came to existence, computer security, IT security, or information security are used in security documents and literature. We highlight several definitions of cyber security for discussion and clarification. Referring to the code of law of the US (section 3542, Chapter 35, title 44), information security is defined as *"protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality and availability"*. According to Gasser and Morrie, [18] *"computer security, also known as cyber security or IT security, is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide"*. ITU defines *"Cyber security is 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. In which, organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment"* [19].

From these definitions, information security emphasizes on the confidentiality, integrity and availability of information. Computer security emphasizes on the availability, integrity, and corrects operations of systems and information within as well as intended services. Cyber security, however, is more explicit and comprehensive in that it emphasizes on the protection of the organization's assets (hardware system, information, connecting infrastructure, services and human beings) using tools, processes, concepts and necessary interaction among elements within. We suggest the following definition.

"Cyber security can be considered systems, tools, processes, practices, concepts and strategies to prevent and protect the cyber space from unauthorized interaction by agents with elements of the space to maintain and preserve the confidentiality, integrity, availability, and other properties of the space and its protected resources."

We believe that this definition unified previous definitions and importantly it clearly defines the scope of cyber security. Firstly, the term cyber security is used instead of "information security" or "IT security" to say that it is the security of cyber space as explicitly defined in the last section. That means that cyber security covers all real and virtual entities, infrastructure and information within, and all possible interactions among entities (including human beings) via the infrastructure and information contained. The terms information security or IT security implies security only in a narrower sense.

Secondly, prevention, not just protection is an integral part of the definition. According to the Oxford Dictionary, "protection" [20] is the act of protecting somebody/something; the state of being protected and "prevention" [21] is the act of stopping something bad from happening. It makes sense to look at security in a wider context where prevention and protection are hand in hand. Preventing some vulnerability to be exploited and damage a cyber space can be considered protecting the space and on the other hand, knowing how to protect the cyber space implies to some extend the knowledge of security breaches occur and how they can be prevented. For example, using anti-virus system is generally known as an act of protection, while deploying an Intrusion Detection System (IDS) or an Intrusion Prevention System (IPS) is known as an act of prevention. Today, building prevention systems that predict and provide report on potential threats is equally as important as building protection systems. In fact, it is strongly believe that completeness of the cyber security system requires both prevention and protection.

Thirdly, with rapid emergence of many modern technologies such as cloud, Internet of Thing, social network, additional considerations, such as adaptability, non-repudiation, or safety may be added to the triad rules of CIA (Confidentiality, Integrity, and Availability) of cyber security. Because, today in order to achieve a model that is invariant to new and emerging technologies such as cloud, Internet of Things, additional of properties such as safety and adaptability may need to be included in the definition.

IV. Cyber Security Maturity Model

A simple and fundamental question that has to be asked concerning a cyber space or any systems is whether the cyber space is secure or at least to what level it is secure. For example, is a cyber space secure when we found and fixed a huge number of bugs, viruses, spams, malware? Or is a cyber space secure when we invest substantial funding on a firewall system and an IDPS (intrusion detection and prevention system)? It is difficult to see that a cyber space is safe and secure based on the numbers of vulnerabilities found and fixed as one has no idea of the number of bugs undetected. This implies that vulnerability is just one on the many aspects of security. Yet, many of current security models deal with security problems in an ad hoc manner; a specific security measure is put into action just to treat the issue at hand without regard or understanding its impact on the whole cyber space. They handle security from a bottom-up perspective and case specific. They provide no assurance of the overall level of security of the protected entity. What we need is to view and study cyber security holistically from a top-down perspective to produce a security model that us to make assessment of the overall security level of the entity we want to protect. Furthermore, the model should allow us identify the entity's weaknesses and measures to deal with them. Measures may include resources to be invested, strategies to be devised, and practices to be enforced in order to better protect the entity. According to Oxford Dictionary, a model is, *"a simple description of a system, used for explaining how something works or calculating what might happen, etc."* [22]. Therefore, cyber security model could be understood as the description of how cyber security system operates together with measurement tools to determine the level or the state of cyber security of the cyber space, and strategies and actions to strengthen or prevent exploitation of weaknesses in the future.

Recently, many models have been developed to enhance the security of cyber space. Depending on the approaches of the researchers and the scale of their cyber space research, these studies focus on different angles of cyber security such as technologies, hardware, software, data, information, network, and risk management. Among those proposed models, the cyber-security maturity model provides to some extent a roadmap for organizations for measuring, assessing, and enhancing cyber security. Relative to other models, it provides managers sound footing for making informed security assessment of their organization.

As mentioned above, maturity models are based on the Capability Maturity Model (CMM)**.** To understand how maturity models assist cyber security, a brief of description of the CMM is in order.

In 1989, Humphrey recommended the CMM to assess quality of software and to help software organizations improve the maturity of their software processes in terms of an evolutionary path from ad hoc, chaotic processes to mature, disciplined software processes. The fundamental ideas of CMM are: (1) the model is divided into 5 levels from initial to optimizing level, from simple to complex, from low requirement to higher requirement; (2) each level has maturity requirement. It means that to achieve the definite maturity level, the standard requirements of quality and technology need to be implemented by several sets of practices; (3) to reach the higher level, the software must be passed all lower levels (see the Figure 1).

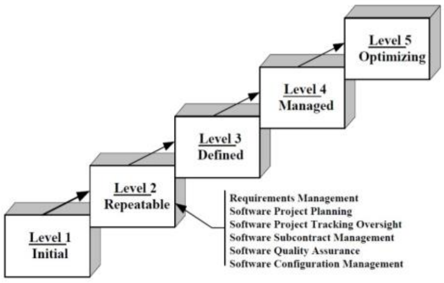

Level 5
Optimizing
Level 4
Managed
Level 3
Defined
Level 2
Repeatable
Level 1
Initial
Requirements Management
Software Project Planning
Software Project Tracking Oversight
Software Subcontract Management
Software Quality Assurance
Software Configuration Management

Fig 1. Capabilities maturity model process levels (Humphrey 1989)

Eventually, maturity models show the level of perfection or completeness of certain capabilities. They define maturity levels which measure the completeness of the analyzed objects via different sets of (multi-dimensional) criteria.

The structure of the cyber security maturity model can be explained in terms of its functions, key components, and types of maturity model [23]. The main functions of maturity model are: means for assessing and benchmarking performance; roadmap for model-based improvement; and means to identify gaps and develop improvement plans. The key components are: maturity levels are the security measurement scale or transitional states; security domains are logical groups of practices, processes; attributes are core contents of the model arranged by domains and levels; diagnostic methods for assessment, measurement, gap identification, and benchmarking; improvement roadmaps to guide improvement efforts such as Plan-Do-Check-Act or Observe-Orient-Decide-Act. Three types of maturity models are progression, capability, and hybrid. While progression model describes levels as higher states of achievement, advancement such as maturity progression for human mobility being from crawl, walk, jog to run, capability model shows levels as the extent to which a particular set of practices has been institutionalized such as Humphrey model above. Hybrid model is the combination of best features of progression and capability maturity models. In which, maturity levels express both achievement and capability.

Most recent cyber security maturity models are hybrid models where they take security levels and domains into the integrated framework. We will analyze several models to clarify how maturity model support cyber security.

Since 2000, City Group kicked off cyber security maturity models with the name Information Security Evaluation Maturity Model (ISEM). Until now, a dozen of cyber security maturity models has been developed and applied to different fields and organizations of different scales.

In 2007, Information Security Management Maturity Model (ISM3) was developed by ISM3 consortium [24] with five levels: undefined, defined, managed, controlled and optimized. This model focuses on evaluating, specifying, implementing and enhancing process oriented information security management systems. The advantage of the model is that it considers organizational culture as a security issue. Moreover, it is based on previous cyber security standards and practices like ISO 9000, and ISO 17799/27001. The ISM3 model is applicable to organizations of different sizes. Cyber security measurement is based on measuring activities, effectiveness and quality.

From 2007, in the program review for information security management assistance (PRISMA) [25], National Institute of Standard and Technology (NIST) created Information Security Maturity Model (ISM2) to evaluate the cyber security level of an organization. This model includes five levels: policies, procedures, implementation, testing, and integration. The key contributions of this model are evaluation capabilities and support system of documents to implement best practices for attaining standards of cyber security. The main metrics to assess cyber security level is based on standards (mainly qualitative measurement).

The Cyber security Capability Maturity Model (C2M2) was developed by the Department of Energy (DOE) to help critical infrastructure organizations evaluate and potentially improve their cyber security practices [6] (Figure 2). This model has been used to create Electricity Subsector Cyber Security Capability Model (ES-C2M2) and the Oil and Natural Gas Subsector Cyber Security Capability Model (ONG-C2M2). The specialty in the design of the architecture is that the model uses ten security domains and each domain contains a structured set of cyber security practices. Each set of practices represents the activities that can be performed to establish mature capability in the domain. To measure maturity level of cyber system C2M2 uses a scale of maturity indicator levels (MILs) 0-3 (not performed, initiated, performed, and managed). For example, if a cyber-system attains level 2; all 10 domains must be at least level 2.

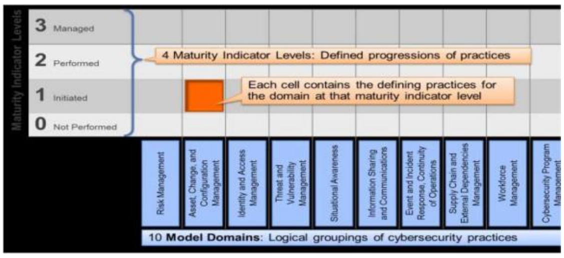

Maturity Indicator Levels
3 Managed
2 Performed
1 Initiated
0 Not Performed
4 Maturity Indicator Levels: Defined progressions of practices
Each cell contains the defining practices for the domain at that maturity indicator level
Risk Management
Asset, Change, and Configuration Management
Identity and Access Management
Threat and Vulnerability Management
Situational Awareness
Information Sharing and Communications
Event and Incident Response, Continuity of Operations
Supply Chain and External Dependencies Management
Workforce Management
Cybersecurity Program Management
10 Model Domains: Logical groupings of cybersecurity practices

Fig 2. ES-C2M2 Structure (Curtin, P. et. al 2015)

Another maturity model is Community Cyber Security Maturity Model (CCSMM) [26] (Figure 3). This model also has 5 levels from the initial to the vanguard level. The significant point of this model is that the author added the third dimension namely geography with three different scales including organization, community and state. This model is applicable to different cyber systems of different sizes from small size companies to big size organizations such as a ministry or a state. This model was implemented in five states within the United States of America with funding from the National Cyber Security Division of the Department of Homeland Security (USA).

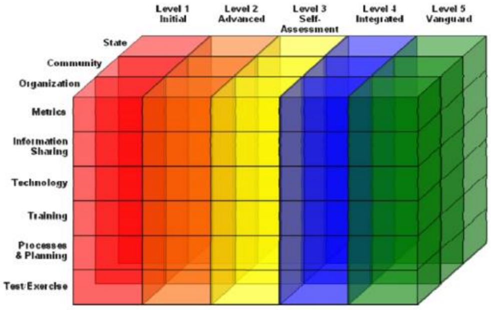


Fig 3. CCSMM Model (White, G. et. al 2011)

To consolidate our understanding of maturity models and how they are applied in cyber security, we compare a dozen of cyber security maturity models. Table 2 shows the features of these models.

In order to discuss the strengths and weaknesses of existing model, we identify the similarities and differences among these models as follows.

Similarities:

- Type of maturity model: all models are hybrid maturity models with their multi dimensions including security domains and maturity levels.

- Security domains: basically, most security domains range from infrastructures, data, networks, to human, application, communications, compliance, legal and contractual.

- Maturity levels: most models use a 5-level framework to assess security state of each domain. These 5 levels can be seen as a 3-stage process. The first stage is the beginning with no security management, policy. The second stage focuses on implementing security standards to be able to control security issues. The last stage is an automatically security management with full security implementation. This stage is considered the resilient stage or highest security.

- International security standards: to implement best security practices, security standards such as NIST, ISO 27000 series, COBIT are applied to perform and measure security levels in all cyber security maturity models.

- Process: most models have implementation process through 4 steps from evaluation, gap identification, priority and plan, and plan implementation.

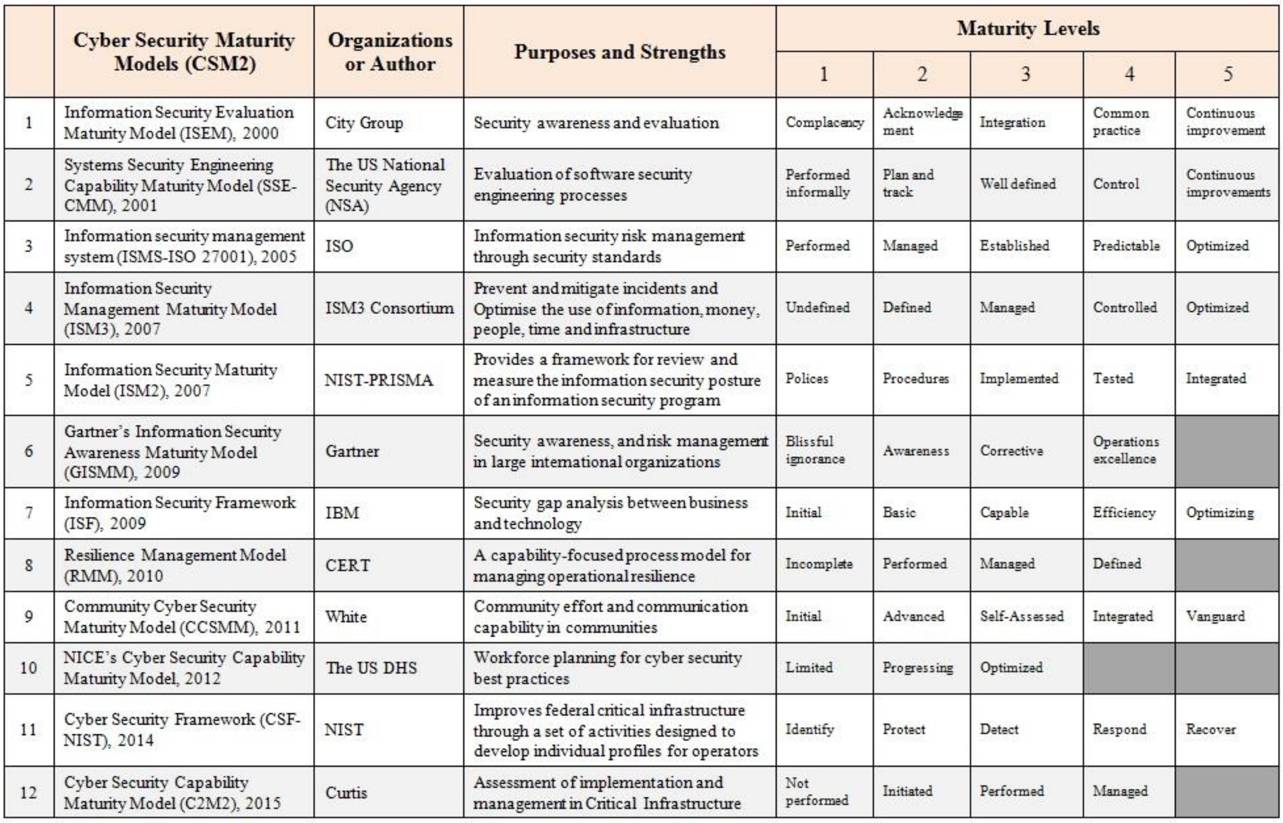
Differences:

- Each model has different goals and advantages, with Information Security Framework, IBM wants to fill the gap between business and technical element, while DOE is interested in implementation and management in C2M2. CCSMM model tends to deal with community and sharing problems.

- Security domains: each model has some different specific domains with different security requirements because of the goals of the model. For example, DOE's C2M2, it focuses on Event and Incident Response Continuity of Operations domain or Identity and Access management domain because the national critical infrastructure requires attention in incident response and authentication aspects of security.

- While almost models use 2 dimensions, model including domains and levels, CCSMM model has 3 dimensions by adding the community (organization, community, state) dimension. This makes the model more suitable for organizations of different sizes, however, the model is complex as it incorporates many standards and implementing practices.

TABLE II.
Synthesizing and Analysis of Cyber Security Maturity Models (CSM2)



	Cyber Security Maturity Models (CSM2)	Organizations or Author	Purposes and Strengths	Maturity Levels				
				1	2	3	4	5
1	Information Security Evaluation Maturity Model (ISEM), 2000	City Group	Security awareness and evaluation	Complacency	Acknowledgement	Integration	Common practice	Continuous improvement
2	Systems Security Engineering Capability Maturity Model (SSE-CMM), 2001	The US National Security Agency (NSA)	Evaluation of software security engineering processes	Performed informally	Plan and track	Well defined	Control	Continuous improvements
3	Information security management system (ISMS-ISO 27001), 2005	ISO	Information security risk management through security standards	Performed	Managed	Established	Predictable	Optimized
4	Information Security Management Maturity Model (ISM3), 2007	ISM3 Consortium	Prevent and mitigate incidents and Optimise the use of information, money, people, time and infrastructure	Undefined	Defined	Managed	Controlled	Optimized
5	Information Security Maturity Model (ISM2), 2007	NIST-PRISMA	Provides a framework for review and measure the information security posture of an information security program	Polices	Procedures	Implemented	Tested	Integrated
6	Gartner's Information Security Awareness Maturity Model (GISMM), 2009	Gartner	Security awareness, and risk management in large international organizations	Blissful ignorance	Awareness	Corrective	Operations excellence	
7	Information Security Framework (ISF), 2009	IBM	Security gap analysis between business and technology	Initial	Basic	Capable	Efficiency	Optimizing
8	Resilience Management Model (RMM), 2010	CERT	A capability-focused process model for managing operational resilience	Incomplete	Performed	Managed	Defined	
9	Community Cyber Security Maturity Model (CCSMM), 2011	White	Community effort and communication capability in communities	Initial	Advanced	Self-Assessed	Integrated	Vanguard
10	NICE's Cyber Security Capability Maturity Model, 2012	The US DHS	Workforce planning for cyber security best practices	Limited	Progressing	Optimized		
11	Cyber Security Framework (CSF-NIST), 2014	NIST	Improves federal critical infrastructure through a set of activities designed to develop individual profiles for operators	Identify	Protect	Detect	Respond	Recover
12	Cyber Security Capability Maturity Model (C2M2), 2015	Curtis	Assessment of implementation and management in Critical Infrastructure	Not performed	Initiated	Performed	Managed	

Discussion

It is believed that at this juncture security modelling requires introspection because of its fragmented and local approach and that cyber security maturity models have advanced the field along an alternative path worthy of closer investigation. Cyber security maturity models have shown that they help managers to better manage security of their organizations [27, 28]. They allow better security risk management, produce cost saving, promotes self-improvement, and support good security procedures and processes. More importantly, they encourage all stakeholders to take steps along a secure mature path as mapped out by the maturity model, rather than activate security controls blindly without regard to the security of the overall organization. Despite all these benefits, maturity models only provide a bare minimum compliance model rather than an aspired cyber security model that can deal with emerging cyber environment, its demanding usage, as well as its sophisticated attacks. The new model should be used not only by the management but also by security experts and practitioners to both assessing the overall security status of the organization/system and taking measure to strengthen weaknesses of any specific aspects of the system as identified by the assessment. Three specific issues should be addressed: First, identifying the maturity levels of cyber security of each domain is arbitrary and subjective as a result of checking for compliances; a security model should be more than compliance. Second, most cyber security maturity models draw on International cyber security standards such as ISO27000 series or NIST. Security practices in these standards are mainly measured by qualitative metrics/processes; quantitative metrics should be essential for any security assessment. Third, the model should be flexible for addressing specific dimension of a cyber spaces or extensible for dealing with emerging cyber spaces.

Conclusion

This paper reviewed and consolidated the definitions of cyber space and cyber security. We identified and defined three fundamental elements of the cyber space: real and virtual entities in the cyber space, the interconnecting information infrastructure that connects and mediates these entities, and the interaction among entities. On the concept of cyber security, we confined its scope over the cyber space, suggested the inclusion of prevention aspect on security and made provision for additional security properties. We described the fundamentals of the maturity models and why they are relevant model for cyber security. We reviewed and compared existing cyber security maturity models to identify their strengths and weaknesses. More importantly, we argue for a stronger security model, with the maturity model as a starting point because of its strength in security compliance and its usefulness for management. However, the new model should include relevant quantitative metrics for measurable and actionable assessment. It has to present a balance picture of the overall security of an organisation/system in terms of qualitative assessment for management and quantitative assessment for security experts. It needs to be extensible and adaptable for application to different types of cyber space (organizations and systems).

References

[1] Whitman, M. and H. Mattord, *Management of information security*. 2013: Cengage Learning.

[2] Wikipedia. *National security*. 2015 29/11/2015]; Available from: https://en.wikipedia.org/wiki/National_security.

[3] Von Solms, R. and J. Van Niekerk, *From information security to cyber security*. computers & security, 2013. **38**: p. 97-102.

[4] Wiener, N., *Cybernetics or Control and Communication in the Animal and the Machine*. Vol. 25. 1961: MIT press.

[5] Humphrey, *CMM*. IEEE, 1989. **1**(1999).

[6] Curtis, P.D. and N. Mehravari. *Evaluating and improving cybersecurity capabilities of the energy critical infrastructure*. in *Technologies for Homeland Security (HST), 2015 IEEE International Symposium on*. 2015.

[7] ITU, *Overview of cybersecurity (ITU-T X.1205)*. 04/2008. 8.

[8] States, T.U., *Cybersecurity policy*, in *National Security Presidential Directive 54/Homeland Security Presidential Directive 23*. 2008.

[9] Commission, E. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* 2013 [cited 2015; Available from: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.

[10] Government, A.s. *Strong and Secure. A Strategy for Australia's National Security*. 2013 [cited 2016 24 August]; Available from: http://apo.org.au/files/Resource/dpmc_nationalsecuritystrategy_jan2013.pdf.

[11] Government, C.s. *Canada's Cyber Security Strategy. For a Stronger and More Prosperous Canada (2010)*. 2010 [cited 2016 24 August]; Available from: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf.

[12] Government, T.N. *National Cyber Security Strategy 2: From Awareness to Capability (2013)*. 2013 [cited 2016 24 August]; Available from: http://english.nctv.nl/images/national-cyber-security-strategy-2_tcm92-520278.pdf.

[13] Government, G.s. *Cyber Security Strategy for Germany (2011)*. 2011 [cited 2016 24 August]; Available from: https://ccdcoe.org/cyber-security-strategy-documents.html.

[14] Government, N.Z.s. *New Zealand's Cyber Security Strategy*. 2015 [cited 2016 24 Ausgust]; Available from: http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-december-2015.pdf.

[15] Rajnovic, D. *Cyberspace – What is it?* July 26, 2012 [cited 2015; Available from: http://blogs.cisco.com/security/cyberspace-what-is-it.

[16] Ottis, R. and P. Lorents. *Cyberspace: Definition and implications*. in *Proceedings of the 5th International Conference on Information Warfare and Security*. 2010.

[17] Shackelford, S.J., *Toward Cyberpeace: Managing Cyberattacks through Polycentric Governance*. Am. UL Rev., 2012. **62**: p. 1273.

[18] Gasser, M., *Building a secure computer system*. 1988: Van Nostrand Reinhold Company New York, NY.

[19] Craigen, D., N. Diakun-Thibault, and R. Purse, *Defining Cybersecurity*. Technology Innovation Management Review, 2014. **4**(10).

[20] Dictionary, O. *Definition of Prrotection*. 2015; Available from: http://www.oxforddictionaries.com/definition/learner/protection.

[21] Dictionary, O. *Definition of prevention*. 2015; Available from: http://www.oxforddictionaries.com/definition/learner/prevention.

[22] Dictionary, O. *Definition of model*. 2015 1 December 2015]; Available from: http://www.oxforddictionaries.com/definition/learner/model.

[23] Allen, J. and N. Mehravari, *How to Be a Better Consumer of Security Maturity Models*. 2014, DTIC Document.

[24] Consortium, I., *Information security management maturity model*. 2009, Versión.

[25] Karokola, G., S. Kowalski, and L. Yngstrom. *Secure e-government services: Towards a framework for integrating it security services into e-government maturity models*. in *Information Security South Africa (ISSA), 2011*. 2011. IEEE.

[26] White, G.B. *The community cyber security maturity model*. in *Technologies for Homeland Security (HST), 2011 IEEE International Conference on*. 2011. IEEE.

[27] Siponen, M. and R. Willison, *Information security management standards: Problems and solutions*. Information & Management, 2009. **46**(5): p. 267-270.

[28] Stevanović, B., *Maturity models in information security*. International Journal of Information, 2011. **1**(2).