Transformative cyber security model for Malaysian government agencies

Perumal, Sundresan; Pitchay, Sakinah Ali; Samy, Ganthan Narayana; Shanmugam, Bharanidharan; Magalingam, Pritheega; Albakri, Sameer Hasan

Published in:
International Journal of Engineering and Technology(UAE)

DOI:
10.14419/ijet.v7i4.15.21377

Published: 01/01/2018

Document Version
Publisher's PDF, also known as Version of record

International Journal of Engineering & Technology, 7 (4.15) (2018) 87-92

SPC

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Transformative Cyber Security Model for Malaysian Government Agencies

Sundresan Perumal[1]*, Sakinah Ali Pitchay[1], Ganthan Narayana Samy[2], Bharanidharan Shanmugam[3], Pritheega Magalingam[2], Sameer Hasan Albakri[2]

[1]Faculty of Science and Technology, Universiti Sains Islam Malaysia (USIM), Bandar Baru Nilai, 71800 Nilai, Negeri Sembilan, Malaysia
[2]Advanced Informatics School, Universiti Teknologi Malaysia, Malaysia
[3]School of Engineering and Information Technology, Charles Darwin University, Australia
**Corresponding author E-mail: sundresan.p@usim.edu.my*

Abstract

The growth of cyberspace world has uprising government agencies in a new way to serve citizen in a proactive, efficient and productive manner. To have an open, stable and vibrant cyberspace, governments should be more resilient to cyber-attacks and able to protect all government agency's interest in cyberspace. Therefore, the government needs a transformative cyber governance security model to protect valuable government agencies' information. The model should be able to detect, defend and deter the vulnerabilities, threats and risks that will emerge in the day to day government administration operation. This paper has introduced a study for some existing cyber governance security models. Thus, it helps in determining the main features of the required model.

Keywords: *Cyber Governance Security; Cyber Security Strategy; Security Defensive Model; Security Threats.*

1. Introduction

Governments always aim to introduce better services to their citizens. One of the best ways to provide easy, stable and fast service is automating these services and deliver it online. Delivering governmental services online will improve the public services [1]. Recently, the government agencies have increased their services that delivered over the cyberspace. The growth of cyberspace helps them to serve citizen in a proactive, efficient and productive manner.

However, the cyberspace is not safe and the cyber-attacks are growing more frequently sophisticated and damaging when they succeed. The number of the cyber-attacks has been increased and the benefit from the technology development. Many organizations suffer from the cybercrime and experienced many cyber-attacks that cause a huge financial loss. Millions of customers' credit and debit card information as well as the customers' email addresses have been stolen by hackers from a Home Depot, 76 million households and seven million businesses were affected [2].

There are many elements that must be considered to secure the cyber environment such as cyber-based systems security, network security, information security, disaster recovery, and end user security awareness. Therefore, the major concern of the cyber governance is the ability of government agencies to secure the technology, data and networks from many threats that they face in their day to day government administration.

This paper has introduced a study for some existing cyber security models as in the United States of America, Australia, Germany, European Union, Japan and China and further compare it with the Malaysia cyber security model. Section 2 mentions some of the cyber security challenges and Section 3 presents different cyber security models. A brief discussion of the cyber security models is given in Section 4. Section 5 discusses the Malaysian cyber security model and compare it with the other models. Finally, Section 6 concludes this paper and the final section highlights our future research work.

2. Cyber Security Challenges

There are many difficulties and challenges faced by the government agencies to secure their cyber-based services. The cyber security model has some aspects that government agencies must consider when the build their cyber-based services and when they attempt to secure them. In this section, we discuss some of these aspects.

In the recent years, the number of the incidences of cyber-attacks have increased and become a concern for nations over the world. New security vulnerabilities and risks emerge suddenly and only few alert-based systems are able to notify. The government agencies realize the possibility of cyberspace exploitation by terrorist organizations [3]. The security threat of cyber terrorism is threatening the services that delivered over the cyberspace and may cause serious damages. Thus, the government agencies must be ready for these sudden security attacks. Furthermore, their security systems should be able to detect the new security threats.

The global nature of cyberspace is another challenge for the government agencies. It is almost impossible to secure the national cyberspace without interacting with the global cyber environment [4]. The global cyber security strategies required international collaboration for success. Even on the national level the government agencies need more cooperation to secure their cyber-based services.

Besides, the user awareness of cyber security threats is another domain that government agencies need to consider. Many studies

show that the end user has an essential role in the security of information systems [5-6]. Focusing on the human components by enhancing user awareness in information security has become norm for organizational end-user risk protection [7]. The incident response awareness program must be embedded in the government agencies' security plans, especially the Standard Operating Procedure (SOP) that users should follow when there is a security threat.

Due to the dynamic nature of cyber threats and attack as well as the complexity to predict and understand how cyberspace will be used in the future as the rate of innovation and changes, the government agencies have to tackle the best measure to get along with today's technology. Moreover, the system that form cyberspace contains a vast array of component, sourced from a global and diverse range of supplier. Multiple sub-contractors produce a test package and assemble these components. This makes it difficult to be customized at the national level.

3. Existing Cyber Governance Security Models

Governance refers to the establishment of policies, set of responsibilities and technical controls with continuous monitoring of the implementation by the authorized party in an organization [8-9]. Therefore, according to [9], an information security governance consists of information security objectives for the targeted organization based on the corporate strategic goals that aligns between information security context and stated organizational objectives. Moreover, information security governance impacts all information security policies [10].

The goal is to give a strategic path, determine that the cyber risks are managed appropriately and verify that the resources are well utilized with the aim to ensure that an organization's objectives are achieved. Basically, according to [11], cyber risks can be categorized to criminal and non-criminal activities and also based on type of attacks such as distributed denial of service and insider attacks in cyberspace [12]. Furthermore, cyber risks also based on source of attacks that can be from terrorists, criminals and government parties [11].

The fast-moving changes in the computerized environment with the emergence of cyberspace, more strong and widespread security threats turn a cyber problem into a major business problem [13]. Thus, the need of cyber security governance increases. Cyber security governance sometimes called information security governance also refers to the implementation and management of the security controls, technical controls, audit and assessments, security awareness and trainings among employees towards achieving secure environment [8, 14-15]. There are many cyber security models that have been developed worldwide. In the following paragraphs, a brief discussion of some cyber security models is presented.

3.1. United States of America

The new cyber security model proposed in the United States in 2015 focuses on strong intra-departmental and inter-agency partnership to implement effective cyber security. The model is designed with the motive to detect the emerging threats and protect the data against cyber-attacks and cyber espionage. Similar to that, MITRE Corporation [8] has developed a Cyber Preparedness (Cyber Prep) Framework that merges multiple components of cyber security strategies such as detecting the cyber threats that an organization faces, identifying the level of preparedness of an organization to face the possible threats, setting the objectives by taking into consideration that the different organizations will face different level of threats and finally assisting in the prioritization of cyber security decisions [8, 16].

The USA cyber security strategy has been guided by the following organizing principles; a national effort, protect privacy and civil liberties, regulation and market forces, accountability and responsibility, ensure flexibility, and multi-year planning. It aims to increase the collaboration and information sharing about the cyber threats and vulnerabilities between the governmental and nongovernmental entities. Cyber security must strengthen the personal privacy and protect the civil liberties. Due to rapid changes of cyber threats, the cyber security Strategy must be flexible to be able to respond to cyber-attacks and manage vulnerability reduction [17].

3.2. Australia

The Australian cyber security strategy has been guided by some principles; national leadership, shared responsibilities, partnerships, active international engagement, risk management, and protecting Australian values [18]. The aim of the Australian cyber security policy is "the maintenance of a secure, resilient and trusted electronic operating environment that supports Australia's national security and maximizes the benefits of the digital economy" though its focused is on the "availability, integrity and confidentiality of Australia's Information and Communications Technology (ICT)".

Australia on the other hand, has proposed a cyber security strategy that includes a national partnership, strong cyber defense to prevent cyber threats, address the international responsibility and influence, improve the technology and enabling innovation and finally to inculcate cyber smart nation [18]. Some of these components such as the intra-organization relationship between government agencies, international partnerships in terms of sharing technology that could detect, defend and deter different level of threats and designing policies are not found in cyber security strategies in Malaysia [8, 18-19].

3.3. Germany

A cyber security strategy framework that was proposed by the Federal Government emphasizes the importance of national and international law enforcement authorities' partnership to aid in the enforcement of internal rules of conduct and the mix of internal and external criminal law [20-21] to combat the vast growing cyber threats. In their model, the first focus is given to choosing the right protective measures and powers for the critical information infrastructure in the case of specific threats to be found. Secondly, rules are made to ensure every government agency to purchase proper security products, trustworthy IT systems and services made available on time. In order to further strengthen the IT security in the public administration, the government looks into creating a uniform and secure network infrastructure in the federal administration and that the resources are shared at the central and local level.

Germany also includes a cyber response or incident response by activating the process of coordinating IT security incident monitoring and response that in-cooperates all states' administration at the central and local level. This security infrastructure that merges federal and local administration has not been implemented or deployed by the government of Malaysia. Cooperation between public and private sectors plus the ideas and research from academia are also projected on the Germany's cyber security strategy model with the motive to manage effective cyber defensive tools at different level of administration. Germany is also looking into cooperating the ideas from international organizations, concerning cyber security in their external cyber policy. Personnel development is another criterion for the implementation of a successful cyber security strategy where personnel exchanges between federal authorities and appropriate training are acquired [20].

The Germany Cyber Security Strategy has some basic principles; The level of cyber security must commensurate with the importance and protection required by interlinked information infrastructures, availability of information and communications technology, the integrity, authenticity and confidentiality of data in

cyberspace, information sharing and coordination, international cooperation to ensure the coherence and the capabilities of the international community to protect cyberspace [20].

3.4. European Union

Similar to the initiative of Malaysian government that is to have the support from the National Information Technology Council Malaysia, Law Enforcement Agencies and Regulators and the Cyber Security Malaysia, EU focuses on three main pillars that are the network and information security, law enforcement and defence with the incorporation of the academic industry. The difference between Malaysia's and EU's cyber security strategy is the EU has proposed integration and dependency of all these three pillars with each other in the national, EU and international level. At the national level, the members are required to state and understand clearly their roles and their responsibilities, share the new trends of attacks and optimize the proposed response actions [22]. At the EU level, collaboration is established to focus on the cyber-attack trend analysis, risk assessment, training and sharing of best practices. European Network and Information Security Agency (ENISA), European Cybercrime Centre (EC3) and EDA cyber defence together with CERT-EU are expected to support the development of trusted community using technical and policy experts.
In addition to that, at the international level, the higher officials are aimed to promote a peaceful, open and transparent use of cyber technologies besides engaging themselves in policy dialogues with the international partners and organizations [22]. The EU cyber security strategy clarifies the principles that should be followed by the European Union countries; The EU's core values apply as much in the digital as in the physical world, protecting fundamental rights, freedom of expression, personal data and privacy, access for all, democratic and efficient multi-stakeholder governance, and a shared responsibility to ensure security.

3.5. Japan

The Japan cyber security policy has been developed over the last years, before 2005, the focus of the strategy was on how to handle the security incidents. in 2005, Japan established a comprehensive foundation for information security, and the focus of Japan strategy was to build Japan model of information security with three main aspects; safety and security, reliability, and quality. In 2010, due to the huge depends on the digital service, the Japanese government issued a new information security strategy under title "Information Security Strategy to Protect People" [23].
In 2015, Japanese government updated their cyber security strategy and defined their final objective as "Ensure a free, fair, and secure cyberspace; and subsequently contribute to improving socio economic vitality and sustainable development, building a society where the people can live safe and secure lives, and ensuring peace and stability of the international community and national security". At the end of 2015, Japan established the "Cyber Security Strategy Headquarters" to coordinate the different cyberspace-related stakeholders and to increase the cooperation between the national cyberspace-related stakeholders in the international organizations.
The published cyber security strategy in 2015 has mentioned five principles that cyberspace-related stakeholders should focus on. These principles are 1) assurance of the free flow of information, 2) the rule of law, 3) openness, 4) autonomy and 5) collaboration among multi-stakeholders. The aims of these principles are to stabilize the global market, and inspire innovations, and contributes to national and international security.
Japan's cyber security strategy focuses on the proactive defence approach. It assumes that there is no hundred percent secure computing system, thus more proactive measures should be used to secure digital systems. Furthermore, Japan cyber security has encouraged the Japanese public and private stakeholders to give more attention to the Internet of Things systems security as an emerging interconnected information society that include all kinds of physical objects, from personal computers, home electric appliances and automobiles, to robots and smart meters, are connected to networks including the Internet [24].
Cyberspace is a multi-dimensional space and many stakeholders are involved. Japanese cyber security strategy has highlighted the importance of cyberspace-related stakeholders' cooperation and collaboration. They share responsibilities and duties of the cyberspace security. Even at international level Japan welcome the partnerships with countries that share common values with Japan. Japan has built an important partnership and cooperation with many countries such as US, European countries and Asia Pacific region countries [23].

3.6. China

Due to the development in the network and communication technologies, cyberspace has become an important element in all aspects of people's life and work, online education, healthcare, shopping, and finance. The Internet has been used in all sectors of national economy and contributes in its development. The Chinese cyber security strategy considered the cyberspace security as a part of national sovereignty. China cyber security strategy has clearly stated that there is no modernization without informatization and there is no national security without cyber security [25].
China in their cyber security strategy published entitled "National Cyber security Strategy" in 2016 and "International Strategy of Cooperation on Cyberspace" in 2017 at 'NATO Cooperative Cyber Defense Centre of Excellence" focuses on four main principles; peace, sovereignty, shared governance, and shared benefits. China cyber security strategy considers the international cyber security is important as the national cyber security. The china safeguarding contributes to the global cyber security and even world peace. China welcomes the international cooperation and information exchange with all countries based on mutual respect and mutual trust. China calls for reforming the global Internet governance system and promoting the internationalization of the management of Internet addresses, domain name servers and other such basic resources [25].
The China cyber security strategy aims to achieve the following objectives; safeguarding sovereignty and security, developing a system of international rules, promoting fair internet governance, protecting the legitimate rights and interests of citizens, promoting cooperation on the digital economy, and building platform for cyber culture exchange.

4. Discussion

This section presents a brief review of some of the existing cyber security models. In this section, we will discuss the common principles that exist in most of the cyber security models. Table 1 summarizes the main principles for each cyber security included in this study.

Table 1: The main principles for Cyber Security

Country	Main Principle	Last Update
USA	1. A National Effort 2. Protect Privacy and Civil Liberties 3. Regulation and Market Forces 4. Accountability and Responsibility 5. Ensure Flexibility 6. Multi-Year Planning	2015
Australia	1. National leadership 2. Shared responsibilities 3. Partnerships 4. Active international engagement 5. Risk management	2016

Country	Main Principle	Last Update
	6. Protecting Australian values	
Germany	1. The level of cyber security must commensurate with the importance and protection required by interlinked information infrastructures, 2. Availability of information and communications technology, 3. The integrity, authenticity and confidentiality of data in cyberspace 4. Information sharing and coordination 5. International cooperation to ensure the coherence and capabilities of the international community to protect cyberspace	2011
European Union	1. Implementation of EU's core values 2. Protecting fundamental rights, freedom of expression, personal data and privacy 3. Access for all 4. Democratic and efficient multi-stakeholder governance 5. A Shared responsibility to ensure security	2013
Japan	1. Assurance of the free flow of information 2. The rule of law 3. Openness 4. Autonomy and collaboration among multi-stakeholders	2015
China	1. Peace 2. Sovereignty 3. Shared Governance 4. Shared Benefits	2017

Based on the brief review for cyber security strategies of USA, Australia, Germany, European Union, Japan, and China, we come out with a list of nine common principles. These principles exist in most of the models even though it has been listed under different titles and expressions.

4.1. Data Confidentiality, Integrity and Authenticity

Data confidentiality, integrity, and authenticity is one of the fundamental principles that must be achieved by any cyber security plan. Due to the involving of the cyber services in different government and private sectors, the data in the cyberspace can be critical and its violation will have significant influence on many people's lives.

4.2. Protecting User's Privacy and User's Civil Right

Protecting the personal data privacy and the fundamental civil rights of the people is essential task for the cyber security programs. Furthermore, it should be maintained even during responding to a cyber-attack or during digital investigations.

4.3. Availability of Online Services

Information and communications technology has become the backbone of the economic growth and is a critical resource which all economic sectors rely on. Any cyber security strategy must ensure critical systems that running in the key sectors such as finance, health, energy and transport will be available even when it is under sophisticated cyber-attack.

4.4. Protecting Critical National Cyber Assets and Infrastructures

The cyber-attacks are multifaceted and it may attack the national civilian and military cyber assets. Cyber security strategy must ensure of protecting both national civilian and military cyber assets. Research and development, and closer cooperation between governments, the private sector and academia are essential to enhance the cyber security approaches and methods.

4.5. Adapting Proactive Cyber Security Approaches and Techniques

Cybercriminals are always developing their methods of cyber-attacks. The fact that there are vulnerabilities in the cyberspace because of its digital-based structure, the cyber security policy must include proactive necessary measurements and conducting analyses of future social changes and potential risks.

4.6. Raising Cyber Security Awareness amongst Citizens, Government Officials, IT Professionals

The human factor is the most weaken factor in the cyber security. Increasing the users' awareness and users' knowledge about cyber security will help to reduce the security vulnerabilities and increase the person's contribution in the cyber security efforts.

4.7. Encourage and Organize the Cooperation and Collaboration between Governmental and Nongovernmental

All cyber-related multi-stakeholders, from governmental entities, and cyber-related business operators, to private enterprises must build an efficient collaborative communication and information sharing among them to obtain information on the occurred incident, including attackers' methods and to share knowledge and expertise.

4.8. Active Cooperation and Collaboration between National and International Cyber Stakeholders

The efficient and effective cooperation must not be only at national level, but also at international level. The cooperation and in partnerships between the countries around the world will make the global cyberspace stable and cyber services and resources will be available for both international and national beneficiaries.

4.9. Ongoing Security Enhancement and Security Risk Assessment

Securing cyberspace is an ongoing process, as new technologies appear and new vulnerabilities are identified. The cyber security strategy must include a continuous enhancement for the security measurements and cyber security defences methods and techniques.

5. Malaysian Cyber Security

In this section, we discuss about the importance of cyber security strategies and the existing components of the cyber security model or framework in Malaysia. The cyber security controls' important components that are detect, defend and deter the known and new threats are vital to ensure that the Critical National Information Infrastructure (CNII) in Malaysia are well protected and adequate to defuse the threat and to minimize or mitigate the information security risk faced. The National Information Technology Council (NITC) of Malaysia has addressed the protection towards the networked information system of ten critical sectors; national defence and security, banking and finance, information and communications, energy, transportations, water, health services, government, emergency services, food and agriculture [19].

In 2002, Malaysian Administrative Modernisation and Management Planning Unit (MAMPU) has come up with a comprehensive approach to prevent the information security breaches that could jeopardize the confidentiality, integrity and availability of the government sector's information and consequently may be of damage to the nation [26]. The steps include assessing the current security strengths and vulnerabilities, developing ICT security

policies, standards and processes, designing and developing a customized security architecture and evaluating and selecting the best security system for the organization. This approach has faced out and been replaced with the current strategy [19].

The current National Cyber Security proposed approach in Malaysia blends the law, policies, technologies and trainings that comprise effective governance, legislative and regulatory, cyber security technology, culture of security and capacity building, research and development towards self-reliance, compliance and enforcement, cyber security emergency readiness and international cooperation. The aim is to ensure government agencies' service delivery is secure and trusted [19].

The initiative by Malaysian government towards achieving a secure cyberspace environment in the government sectors is the cooperation between National Information Technology Council Malaysia that formulates and coordinates policies, the Law Enforcement Agencies and Regulators such as Royal Malaysian Police, Bank Negara Malaysia, Malaysian Communication and Multimedia Commissions that focuses on preventing and combating terrorism with the technical support and services provided by Cyber Security Malaysia. However, the implementation of this approach still has not reached the expectation of the nation [27].

The approaches above work independently under separate domain and it is found that each domain is based on their own requirements and objectives. Currently, with the growth of information technology, cyber resources are shared between government agencies. The domain that works individually fails to monitor information security trends throughout the inter-agency that has caused the threat profiles and the latent risk to remain obscure for the government [28]. Therefore, a single national cyber security governance model is needed to eventually link the domains to achieve a safe cyberspace for the government agencies' information system.

The global cyberspace is shared between the countries over the world. Different countries have different national organizations that provide cyber-based services and connected the international cyberspace. Thus, the cyber security governance needs an effective cooperation between pertinent originations. The cooperation should be on both national and international levels. At the national level, the cooperation and partnership must include not only the government agencies, but also the private organizations that provide cyber-based services. The internet service providers must have a strong and resilience collaboration to secure the cyberspace, not only at national level but also at the international level [4]. Our research explores the strategic integration that can be done in Malaysia between cyber security elements and different official government agencies at the national and the international levels that merges the technical controls, operational security measures and private partner agency's strategies by introducing a new model that comprises three major components that are detect, defend and deter the vulnerabilities, threats and risks that will emerge in day to day government administration operation.

6. Conclusion

National Information Technology Council (NITC) of Malaysia has addressed the protection towards the networked information system of ten critical sectors; national defence and security, banking and finance, information and communications, energy, transportations, water, health services, government, emergency services, food and agriculture. The different Malaysian government agencies work independently under separate domain and it is found that each domain is based on their own requirements and objectives. However, the Malaysian government agencies need a novel transformative cyber governance security model that enables it to collaborate effectively and efficiently to protect valuable government agency's information and reach the expectation of the nation.

7. Future Work

For future work, we are going to propose an appropriate defensive model that can be utilized to collect threats information to perform a detailed intelligent incident response. Furthermore, the findings from incident response will be used as deterrent measures in our proposed model. The proposed model contains a comprehensive set of detecting, defending and deterrent measure against identified vulnerabilities, threats and risks in the government agencies.

Acknowledgement

This work was supported by the Universiti Sains Islam Malaysia (USIM) [Grant No: PPP/USG-0115/FST/30/11815].

References

[1] Bailey, A., Minto-Coy, I., & Thakur, D., "IT governance in E-government implementations in the Caribbean: Key characteristics and mechanisms", In L. Rusu, & G. Viscusi (Eds.), Information Technology Governance in Public Organizations. (2017), Cham: Springer, pp. 201-227.

[2] Patrick, H., & Fields, Z., "A need for cyber security creativity", In Z. Fields (Ed.), Collective Creativity for Responsible and Sustainable Business Practice. (2017), Pennsylvania: IGI Global, pp. 42-61.

[3] Albahar, M. (2017), Cyber attacks and terrorism: A twenty-first century conundrum. Science and Engineering Ethics, 2017, 1-14.

[4] Shafqat, N., & Masood, A. (2016), Comparative analysis of various national cyber security strategies. International Journal of Computer Science and Information Security, 14(1), 129.

[5] Dhillon, G., Syed, R., & Pedron, C. (2016), Interpreting information security culture: An organizational transformation case study. Computers and Security, 56, 63-69.

[6] Hsu, J. S. C., Shih, S. P., Hung, Y. W., & Lowry, P. B. (2015), The role of extra-role behaviors and social controls in information security policy effectiveness. Information Systems Research, 26(2), 282-300.

[7] Banfield, J. M., A study of information security awareness program effectiveness in predicting end-user security behavior. Eastern Michigan University, (2016).

[8] Bodeau, D., Boyle, S., & Fabius-Greene, J., Cyber security governance. A component of MITRE's cyber prep methodology. The MITRE Corporation, (2010).

[9] Bhaduri, S. N., & Selarka, E., Corporate Governance and Corporate Social Responsibility—Introduction. In Corporate Governance and Corporate Social Responsibility of Indian Companies. (2016), Berlin: Springer, pp. 1-10.

[10] Ramtohul, A., & Soyjaudah, K. M. S. (2016), Information security governance for e-services in southern African developing countries e-Government projects. Journal of Science and Technology Policy Management, 7(1), 26-42.

[11] Eling, M., & Schnell, W. (2016), What do we know about cyber risk and cyber risk insurance? Journal of Risk Finance, 17(5), 474-491.

[12] De Bruin, R., & Von Solms, S. H., "Cybersecurity governance: How can we measure it?" Proceedings of the IEEE IST-Africa Week Conference, (2016), pp. 1-9.

[13] Kshetri, N., & Murugesan, S. (2013), EU and US cybersecurity strategies and their impact on businesses and consumers. Computer, 46(10), 84-88.

[14] Machado, M. N. C. (2015). Cyber security governance.

[15] FORCE, C. G. T., "Information security governance: A call to action", (2004), http://www. cyberpartnership. org/init-governance. html.

[16] Bodeau, D. J., Graubart, R., & Fabius-Greene, J., "Improving cyber security and mission assurance via cyber preparedness (cyber prep) levels", Proceedings of the IEEE Second International Conference on Social Computing, (2010), pp. 1147-1152.

[17] USA Cyberspace Policy Review, (2009), A.a.T.a.R.I.a.C. Infrastructure.

[18] Government of Australia. (2016), Australia's cyber security strategy. Enabling innovation, growth and prosperity.

Commonwealth of Australia, Department of the Prime Minister and Cabinet.
[19] Government of Malaysia. (2006), M.o.S.T.a.I., National cyber security policy: The way forward. Federal Government Administrative Centre.
[20] Government of Germany. (2011), Cyber security strategy for Germany. https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile.
[21] Sarma, S., (2016), Cyber security mechanism in European Union. https://icwa.in/pdfs/VP/2014/CyberSecurityMechanisminEuropeanUnionVP26042016.pdf
[22] European Commission. (2013). Cybersecurity strategy of the European Union: An open, safe and secure cyberspace.
[23] European Commission, (2013). High representative of the European Union for Foreign Affairs and Security Policy.
[24] Min, K., & Chai, S. W. (2016), An analytic study of cyber security strategies of Japan. International Journal of Security and Its Applications, 10(10), 37-46.
[25] Government of Japan. (2015), National cyber security strategy.
[26] Government of China. (2016), China national cybersecurity strategy.
[27] Malaysian Administrative Modernisation and Management Planning Unit, Prime Minister's Department, Malaysian public sector management of information and communications technology security handbook (MyMIS), (2002). http://www.mampu.gov.my/images/Orang-Awam/MyMIS.pdf.
[28] Hashim, M. S. B., "Malaysia's national cyber security policy: The country's cyber defence initiatives", Proceedings of the IEEE Second Worldwide Cybersecurity Summit, (2011), pp. 1-7.