Safeguarding Malaysia's Cyberspace against Cyber Threats: Contributions by CyberSecurity Malaysia

Fazlan Abdullah [1], Nadia Salwa Mohamad [2], and Zahri Yunos [3]
[1,2,3] CyberSecurity Malaysia, Seri Kembangan, Malaysia
fazlan@cybersecurity.my, nadia.salwa@cybersecurity.my, zahri@cybersecurity.my

Abstract - **The world today is becoming dependent on Information and Communication Technology (ICT). Cyber threats on ICT infrastructures can lead to catastrophic damage and disruption, hence an effective information security policy framework is vital in securing the Critical National Information Infrastructure (CNII). Malaysia has implemented the National Cyber Security Policy (NCSP) to safeguard Malaysia's CNII against cyber threats. The implementation of NCSP initiatives requires the commitment and involvement of multiple stakeholders to ensure continuous momentum. Thanks to the implementation of the NCSP initiatives, Malaysia's commitment and effort in ensuring resilience against cyber threats has been recognized at the international level.**

KEYWORDS - Critical National Information Infrastructure (CNII), Cyberattacks, Cyber Threat, Cyber Security, Cyber Security Policy

I. INTRODUCTION

The high dependency on the use of Information and Communication Technology (ICT) for social, political and economic activities makes many nations around the world vulnerable to the ever-increasing range of cyber threats. These threats can jeopardize every level of society and industry, from public users who use ICT equipment to the Critical National Information Infrastructure (CNII) which is dependent on the ICT systems for the operation of their infrastructure, for example in the banking, government, energy, water and telecommunications sector.

Interdependencies between these infrastructures have raised concerns that successful cyberattacks may have serious cascading effects on others, resulting in potentially disastrous impact. Therefore, it is necessary to have a strategy at the national level for protecting CNII from cyber threat activities.

II. RELATED WORK

A. Critical National Information Infrastructure (CNII)

Advancement in the use and dissemination of ICT are seen as closely connected to the notion of critical infrastructure protection. CNII are the foundation of a nation's economic, political, strategic and socio-economic activities [1][2][3]. In recent years, CNII has become progressively more dependent on ICT, as there exist infrastructure interdependencies of CNII sectors [4]. In most cases, the ICT system forms the backbone of a nation's critical infrastructure (e.g. electrical grid), which means that a major security incident in a particular system could have significant impact on the reliability and safety of the operations of the physical systems dependent on it [5].

Interdependency is a bidirectional relationship between infrastructures, through which the state of each infrastructure is influenced by, or correlated to the state of the other. Many stakeholders are concerned with cyberattacks against interdependent critical infrastructures, such as telecommunications, power distribution, transportation, financial services and essential public utility services.

B. Theoretical Concept of Cyberattacks Targeting CNII

It is important to understand the infrastructure of computer networks that are at risk, especially those which support CNII operational functions [6]. Threats may be in the form of attacks launched using, or against, computer networks. Cyberattacks on CNII are possible, whereby the motives, resources and willingness to conduct operations of different kinds against specific targets are fundamental [7]. If perpetrators follow the lead of hackers, they theoretically have the capability to use ICT to conduct cyberattacks against specific targets. The cyber world, which encompasses computer-related technologies such as the Internet and World Wide Web, gives perpetrators access and freedom over vast geographic areas. Among the most advanced countries, the US Department of Defense has placed cyber threats as the top national security threat to the United States.

There is a great deal of concern regarding serious attacks against CNII [8]. CNII is a complex, interconnected system with a vital role in underpinning our economy, security and way of life. CNII facilities pose high-value targets, which, if successfully attacked (physically or cyber-wise), have the potential to disrupt the normal rhythm of society, cause public fear and intimidation, and generate substantial publicity [9]. The CNII in a given country is often an attractive target for perpetrators owing to the large-scale economic and operational damage that can potentially occur with a major failure. In this case, the CNII's industrial control system is the potential target.

CNII organizations that provide critical services have long used a control system commonly known as Supervisory Control and Data Acquisition (SCADA) for gathering real-time data, controlling processes and monitoring equipment from remote locations [10]. SCADA serves to monitor and control the delivery of critical services, such as power, waste treatment, and nuclear, transport and water systems. These systems are frequently unmanned and accessed remotely by engineers via telecommunication links. Typically, SCADA systems are closed operating environments (or stand-alone systems). However, new research indicates a tendency for systems to move towards open standards (or networked architectures), such as Ethernet, TCP/IP and web technologies where vulnerabilities are more widely known [11].

A number of existing case studies represent the incidence of terrorist attack acts on CNII. One captured al-Qaeda computer reportedly contained engineering and structural features of a dam downloaded from the Internet [12]. In another case, it was found that al-Qaeda operators studied software and programming instructions for digital switches that run power, water and transportation grids. SCADA systems have also been accessed by terrorist and extremist groups to gather information on potential targets.

Therefore, it can be concluded that protecting CNII organizations against cyberattacks is deemed critical to a nation. The reason is that the destruction or disruption of ICT systems that provide critical services could significantly impact economic strength, image, defence and security, a government’s functioning capabilities, and public health and safety. This observation is relevant, because CNII organizations are likely targets due to the high degree of interdependency between these critical sectors. Besides, the impact would be much greater and wider compared to non-CNII organizations. As a result of weaknesses or vulnerabilities in the SCADA system within CNII organizations, adversaries may conduct terrorist activities by utilizing the cyberspace to carry out cyberattacks on CNII facilities.

C. Cyberattacks on CNII: Case Studies

The Stuxnet attack against the Iranian Nuclear program demonstrates the impact that a sophisticated adversary with detailed knowledge of process control systems can have on critical infrastructure [13]. Stuxnet is believed to have destroyed 984 centrifuges at Iran’s uranium enrichment facility in Natanz [14]. The attack alarmed the world towards vulnerabilities in the highly sophisticated facility and industrial control system.

Another cyberattack that has attracted the world’s attention and raised concerns regarding e-banking systems is the Bangladesh Bank Heist that was reported in February 2016. The Bangladesh Bank was compromised through firewall exploitation, which facilitated a breach in the Society for Worldwide Interbank Financial Telecommunications’ (SWIFT) Alliance Access Software for making payment instructions [15]. The US Central Bank approved five of the payment instructions and made the payments to accounts in Sri Lanka and Philippines – including $81 million to four accounts in the names of individuals [16]. Investigation is ongoing and no arrests have been made despite the US Federal Bureau of Investigation, Interpol, Bangladesh police and authorities in the Philippines working on this case [17]. This cyberattack on the banking industry triggered cross-border action in safe audit procedures, security and architecture of the SWIFT network, as well as personnel negligence with e-banking systems and Standard Operating Procedures (SOP).

Global ransomware attacks are increasing as reported by Europol [18]. The most recent cyberattack, WannaCry, has affected hundreds of thousands of computers by exploiting vulnerabilities in Microsoft's Windows XP software and creating havoc around the world [19]. WannaCry is a dangerous combination of two malicious software components: a worm and a ransomware variant [20]. Hospitals, companies, universities and governments across at least 150 countries were hounded by a cyberattack that locked computers and demanded ransom [21]. CyberSecurity Malaysia's MyCERT department issued alerts and advisories on the WannaCry Ransomware threat [22] [23] [24].

The rise in planned cyberattacks by hacktivists on Malaysia with high damage potential for interdependent networks and information systems across the country has demanded high attention be paid to CNII protection initiatives. The most remembered cyber threat by hacktivists was the coordinated cyberattack called "Operation Malaysia" in 2011 by the Anonymous group, which conducted DDOS attacks on Malaysia's government websites in protest of Malaysia's blocking of certain websites [25] [26].

III. METHODOLOGY

The methodology used for this research is qualitative and the approach used is literature review from secondary sources. There will be no numeric data or quantitative data produced. Due to limited literature with regards to cyber incidents happening around the globe, the journal also looks at newspaper article for information and references.

IV. DISCUSSION

A. International Telecommunication Union (ITU) National Cyber Security Guideline

In this rapidly changing and sophisticated cyber-threat environment, all states and organizations need to have comprehensive, flexible and dynamic cybersecurity strategies. A national cybersecurity strategy is a plan of action to increase the security, resilience and self-reliance of national infrastructures in delivering services against cyber threats.

In 2011, the International Telecommunication Union (ITU) published the ITU National Cybersecurity Strategy Guide as a reference model for national strategy elaboration. The ITU, a specialized agency of the United Nations (UN) for ICT, is an organization based on public-private partnership with current membership of 193 countries and 800 private sector entities and academic institutions.

Cyber security has been at the top of the UN agenda, for it is crucial to the socio-economy of the global community. UN has issued resolutions on five (5) cybersecurity matters: Combating Criminal Use of ICTs (A/RES/55/63 and A/RES/56/121), Culture of Cybersecurity (A/RES/57/239), Critical Infrastructure (A/RES/58/199) and Global Culture of Cybersecurity (A/RES/64/211) [27].

Based on the ITU National Cybersecurity Strategy Guideline, ten (10) elements are the main features of a holistic, multi-stakeholder and strategy-led cybersecurity program (Table 1).

Table 1: Elements of ITU National Cyber Security Guide

No.	Element of ITU National Cyber Security Guide
1	Top Government Cybersecurity Accountability Top government leaders are accountable for devising a national strategy and fostering local, national and global cross-sector cooperation
2	National Cybersecurity Coordinator An office or individual overseeing cybersecurity activities across the country
3	National Cybersecurity Focal Point A multi-agency body that serves as a focal point for all activities dealing with the protection of a nation's cyberspace against all types of cyber threats.
4	Legal Measures Typically, a country reviews and, if necessary, drafts new criminal laws, procedures, and policies to deter, respond to and prosecute cybercrime.
5	National Cybersecurity Framework Countries typically adopt such framework that defines minimum or mandatory security requirements on issues such as risk management and compliance.
6	Computer Incident Response Team (CSIRT) A strategy-led program that contains incident management capabilities with national responsibility. The role is to analyse cyber threat trends, coordinate responses and disseminate information to all relevant stakeholders.
7	Cybersecurity Awareness and Education A national program should exist to raise awareness about cyber threats.
8	Public-Private Sector Cybersecurity Partnership Governments ought to form meaningful partnerships with the private sectors

9	Cybersecurity Skills and Training Program A program that should help train cybersecurity professionals
10	International Cooperation Global cooperation is vital due to the transnational nature of cyber threats.

The ITU National Cybersecurity Strategy Guideline is centred on matters that all countries should consider as part of the national cybersecurity strategy, such as national values, need and threat variance, national capabilities, culture and national interest. Being aware of the multi-stakeholder aspect of cybersecurity, ITU has thus developed the ITU Global Cybersecurity Agenda (GCA) -- a cross-border framework for international cooperation in cybersecurity.

GCA boosts cooperation between members and partners to prevent duplication in strategic initiative implementation. GCA recommends 5 pillars or areas in cybersecurity activities within ITU, as stated in Table 2.

Table 2: Global Cybersecurity Agenda (GCA) Pillars

Pillar	Areas in Cybersecurity Activities
Pillar 1	Legal Measures
Pillar 2	Technical and Procedural Measures
Pillar 3	Organizational Structures
Pillar 4	Capacity Building
Pillar 5	International Cooperation

B. Global Cybersecurity Index Framework by ITU

Cybersecurity ranges over a broad spectrum of fields across several industries and sectors. ITU, a specialized agency of the United Nations for ICTs, is committed to connecting nations, and protecting and supporting the fundamental rights of a person to communicate. The Global Cybersecurity Index (GCI) is a survey for measuring the commitment of Member States to cybersecurity. GCI is based on the ITU GCA, and is a framework for international cooperation to enhance confidence and security in the current information society. GCA is constructed upon the five (5) strategic areas of GCI: Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building and International Cooperation [27].

GCI is included under Resolution 130 (Rev. Busan, 2014), with the first survey held in 2013-2014 in partnership with ABI Research. A new survey was carried out in 2017 using an enhanced reference model as a result of the extensive participation and collaboration of experts, industry stakeholders, contributing partners and GCI partners [28].

The objective of the GCI initiative is to assist member states identify areas for improvement in the field of cybersecurity, take constructive action for ranking as well as raise the countries' commitment to cybersecurity. Table 3 explains briefly the five (5) strategic pillars and sub-pillars of GCI [28].

Table 3: Strategic pillars and sub-pillars of GCI

Strategic Pillars	Sub-Pillars
Legal Measures Existence of legal institutions and frameworks dealing with cybersecurity and cybercrime	• Cybercriminal legislation • Cybersecurity regulation • Cybersecurity training
Technical and Procedural Measures Existence of technical institutions and frameworks dealing with cybersecurity	• National CIRT • Government CIRT • Sectoral CIRT • Standards for organizations • Standards and certification for professionals • Child online protection
Organizational Structures Existence of policy coordination institutions and strategies for cybersecurity development at the national level	• Strategy • Responsible agency • Cybersecurity metrics
Capacity Building Existence of research and development, education and training programs; certified professionals and public sector agencies fostering capacity building	• Standardization bodies • Good practices • R&D programs • Public awareness campaigns • Professional training courses • National education programs and academic curriculums • Incentive mechanism • Homegrown cybersecurity industry
International Cooperation Existence of partnerships, cooperative frameworks and information sharing	• Inter-state cooperation • Multilateral agreements

networks	• International forum participation • Public-private partnerships • Inter-agency partnerships

C. CNII Protection Framework in Malaysia

The revolution of information and interdependency of ICT infrastructures has increased the risk of various new vulnerabilities and dynamic threats to critical infrastructures. The Government of Malaysia is deliberately adopting ICT as a key enabler for socio-economic development. Thus, adopting an integrated and broad approach to protect critical infrastructure is necessary.

NCSP development started in 2005 and was accepted by the government for implementation in 2006. The NCSP aims to develop and establish a comprehensive program and framework to ensure the effectiveness of information security controls over critical assets and that the CNII is protected up to a level that is commensurate to the risks faced. Key areas considered during policy development are legislation, technology, institutional, public and private cooperation as well as international engagement.

The policy covers ten (10) CNII sectors identified and defined in the policy (Table 4).

Table 4: Ten (10) CNII Sectors Identified

National Defence & Security	Water
Banking & Finance	Health Services
Information & Communication	Government
Energy	Emergency Services
Transportation	Food & Agriculture

The NCSP has eight (8) Policy Thrusts (PT) covering the specific areas listed in Table 5.

Table 5: Elements of ITU National Cyber Security Guide

Policy Thrust (PT)	Initiatives
PT 1: Effective Governance	• Centralize coordination of national cybersecurity initiatives. • Promote effective cooperation between public and private sectors. • Establish formal and encourage informal information exchange.
PT 2: Legislative and Regulatory Framework	• Review and enhance Malaysia's cyber laws to address the dynamic nature of cybersecurity treats. • Establish progressive capacity building programs for national law enforcement agencies. • Ensure that all applicable local legislation is complementary to and in harmony with international laws, treaties and conventions.
PT 3: Cybersecurity Technology Framework	• Develop a national cybersecurity technology framework that specifies cybersecurity requirement controls and baselines for CNII elements. • Implement an evaluation/certification program for cybersecurity products and systems.
PT 4: Culture of Security and Capacity Building	• Develop, foster and maintain a national culture of security. • Standardize and coordinate cybersecurity awareness and education programs across all CNII elements. • Establish an effective mechanism for cybersecurity knowledge dissemination at the national level. • Identify minimum requirements and qualifications for information security professionals.
PT 5: Research and Development Towards Self-Reliance	• Formalize the coordination and prioritization of cybersecurity research and development activities. • Enlarge and strengthen the cybersecurity research community. • Promote the development and commercialization of intellectual properties, technologies and innovations through focused research and development. • Nurture the growth of the cybersecurity industry.
PT 6: Compliance and Enforcement	• Standardize cybersecurity systems across all CNII elements. • Strengthen the monitoring and enforcement of standards. • Develop a standard cybersecurity risk assessment framework.
PT 7: Cybersecurity Emergency Readiness	• Strengthen the national computer emergency response teams (CERTs). • Develop an effective cybersecurity incident reporting mechanism. • Encourage all CNII elements to monitor cybersecurity events. • Develop a standard business continuity management framework. • Disseminate vulnerability advisories and threat warnings in a timely manner. • Encourage all CNII elements to perform periodic vulnerability assessment programs.

PT 8: International Cooperation	• Encourage active participation in all relevant international cybersecurity bodies, panels and multi-national agencies. • Promote active participation in all relevant international cybersecurity events, conferences and forums. • Enhance the strategic position of Malaysia in the field of cybersecurity by hosting an annual international cybersecurity conference.

D. Malaysia’s NCSP Framework and ITU GCI

The elements used in the development of NCSP are similar to the elements recommended by ITU GCI for the development of a national cybersecurity policy. Table 6 compares the elements in both frameworks based on the people, technology and process components. GCI recommends five (5) key areas in the guideline, whilst NCSP identifies eight (8) key areas in policy development.

Table 6: Elements of NCSP and GCI

Cyber security Policy	Strategic Areas / Pillars	Influencing Factor	Framework
Malaysia’s NCSP	Culture of Security & Capacity Building	People	Awareness & Competency Development
GCI	Capacity Building		
Malaysia’s NCSP	R&D Towards Self Reliance. Cyber Security Emergency Readiness. Cyber Security Technology Framework.	Technology	Technology Development
GCI	Technical and Procedural Measures		
Malaysia’s NCSP	Legislative & Regulatory Framework	Process	Cyber Laws & Enforcement
GCI	Legal Measures		
Malaysia’s NCSP	Compliance & Enforcement (Standard)	Process	Security Management
GCI	Legal Measures		
Malaysia’s NCSP	International Cooperation	Process	International Cooperation
GCI	International Cooperation		

E. National Cybersecurity Policy Implementation Progress to Date in Malaysia

Since the policy was approved in 2006, multiple initiatives have been planned under each PT. Moreover, each PT’s activities are driven by the respective ministries and government agencies as thrust drivers. The implementation approach of NCSP is to develop self-reliance in technology, develop human capital, monitor the compliance mechanism, evaluate and improve the mechanism, and create a cybersecurity culture. A brief description of the NCSP implementation is given as follows.

PT 1: Effective Governance

Initially, NCSP development and implementation was led by the Ministry of Science, Technology and Innovation Malaysia (MOSTI) with focus on establishing a governance structure and various committees. The committees cover each key aspect, such as policy, content, crisis management, legislation, acculturation and capacity building, and compliance and enforcement. To oversee the implementation of the NCSP thrusts and strategies, the National Cyber Security Coordination Committee (NC3) was formed in 2008.

In 2011, the stewardship of the NCSP was handed over to the National Security Council as the central coordinating body. Subsequently, the high-level e-Sovereignty Committee was established to oversee the overall cybersecurity governance in Malaysia, chaired by the Deputy Prime Minister of Malaysia.

On January 2017, the government of Malaysia established the National Cyber Security Agency (NACSA), which reflects the government’s seriousness to address cybersecurity threats in a more coordinated manner.

PT 2: Legislative & Regulatory Framework

In boosting the legislative and regulatory aspects of cybersecurity, Malaysia adopted the

Information Security Legal and Regulatory Framework. A 'Study on the laws of Malaysia to accommodate legal challenges in the Cyber Environment' in 2009 and a 'Feasibility Study on the Cyber Security Standards Act' in 2015 were also conducted. As proposed by the adopted framework, the current legislation including the Computer Crime Act 1997, Communication and Multimedia Act, *Arahan Tetap Keselamatan Kerajaan*, and Evidence Act 1950 have been reviewed and are being amended.

In 2010, the Personal Data Protection Act 2010 and Department of Personal Data Protection were established for the protection and security of personal data. In supporting the law enforcement agencies and regulatory bodies in digital forensic investigation capabilities, CyberSecurity Malaysia's Digital Forensics Labs was established in year 2002. The capacity and capability of the lab was further enhanced with other expertise such as audio forensics, video forensics and closed-circuit television (CCTV) forensics.

PT 3: Cybersecurity Technology Framework

The framework was established for cybersecurity controls to be implemented and enforced based on recommended standards and guidelines. The security controls applied are commensurate with the potential organizational impact due to any security breaches caused by forfeiture of confidentiality, integrity or availability. The ISO 27001 Information Security Management Systems standard was identified as a baseline for compliance under PT 3. On 24th February 2010, the Malaysian Cabinet meeting had decided that CNII agencies shall implement MS ISO/IEC 27001 (Information Security Management System-ISMS) to safeguard and protect organizational data and information [29] [30].

Another initiative implemented under this framework is the Malaysia Common Criteria Certification (MyCC) Scheme, which is aimed to increase Malaysia's competitiveness in quality assurance of information security based on Common Criteria Standard ISO/IEC 15408. The scheme implements a security evaluation and certification program that will facilitate CNII to procure technology with documented assurance. The MyCC Scheme is operated by the Information Security Certification Body (ISCB), a department of Cybersecurity Malaysia, which manages information security certification. Malaysia became a member of the Common Criteria Recognition Arrangement (CCRA) in 2007. The Government of Malaysia also agreed that the CC Certification would be one of the criteria in the procurement of information technology, especially local systems or products. To date, there are sixty-eight (68) products and systems have been certified under the MyCC Scheme. ITU has credited the establishment of CyberSecurity Malaysia's ISCB department and the establishment of the MyCC Scheme in the GCI 2017 survey report [28].

PT 4: Culture of Security & Capacity Building

The Government of Malaysia has been aware of the need for greater awareness and understanding of cybersecurity issues and for developing a positive cybersecurity culture. Hence, a study entitled National Strategy for Cyber Security Acculturation and Capacity Building was carried out in 2010 to evaluate current national and CNII awareness education programs and campaigns.

To ensure the success of the cybersecurity awareness, acculturation and education programs, coordinated initiatives and efforts have been driven by relevant organizations to increase the level of cybersecurity awareness, best practices and safe use of the Internet across all CNII as well as public elements.

One of the main initiatives is Cyber Security and Awareness for Everyone (CyberSAFE), which is a program that provides awareness for children, youth, parents and organizations. To date, more than 170,000 people have participated in the CyberSAFE Program. Another initiative is the development of the "Guideline to Determine Information Security Professional Requirements for CNII Agencies or Organizations." [31] This guides CNIIs with ensuring their organizations have sufficient trained professional to handle technical and non-technical cybersecurity issues within their organizations.

In addition, CyberSecurity Malaysia has collaborated with local universities in cybersecurity tertiary programs, such as Master of Cyber Security in collaboration with Universiti Kebangsaan Malaysia (UKM), Master of Protective Security Management with International Islamic University Malaysia (IIUM) and Degree of Cyber Security and Cyber Security Technology with the National Defence University (Universiti Pertahanan Nasional Malaysia - UPNM).

In the ITU GCI 2017 survey, Malaysia was ranked second in the Asia Pacific region, scoring a perfect 100 on capacity building as a result of Malaysia's initiatives. The ITU GCI 2017 report also cited CyberSecurity Malaysia's professional training programs via higher education institutions in Malaysia as well as its CyberGuru website, dedicated to professional security training as contributing to the capacity building score in the survey. The professional training programs and the CyberGuru website are managed by CyberSecurity Malaysia's Cyber Security Professional Development (CSPD) department.

PT 5: Research & Development towards Self-Reliance

The NCSP implementation also focuses on Research & Development towards Self-Reliance through Policy Thrust 5. Led by MIMOS Berhad, an organization under MOSTI, MIMOS spearheaded the development of the National Cyber Security Research and Development Roadmap for Self-reliance in cybersecurity technologies.

The initiative of this thrust is to identify and monitor information security-related research and development projects. Among research projects and cooperation for supporting this thrust are CyberSecurity Malaysia's MyCERT National Malware Research Centre, CyberCSI, Cryptography Research, SCADA Research Lab collaboration between CyberSecurity Malaysia, and the cybersecurity industry.

Through research and development efforts, CyberSecurity Malaysia has successfully developed services such as Cyber999 for handling cybersecurity incidents and the MyCyberSecurity Clinic for data recovery and sanitation.

PT 6: Compliance & Enforcement

On 24 February 2010, the government of Malaysia agreed for all CNIIs to implement and undergo certification based on MS ISO/IEC 27001 Information Security Management System (ISMS) standards within 3 years. A task force led by the National Security Council and comprising regulators and government bodies overseeing the CNIIs, was formed to ensure compliance to this directive. To date, more than one hundred thirty-eight (138) CNIIs have been ISMS-certified [29].

PT 7: Cyber Security Emergency Readiness

The establishment of the Computer Emergency Response Teams (CERT) is one of the initiatives to reduce and mitigate cyber threats. Malaysian CERT (MyCERT) was formed on 13 January 1997 to facilitate and handle computer security incident responses to emergencies.

In 2008, the National Security Council developed the National Cyber Crisis Management Plan (NCCMP) in order to manage cyber emergencies. NCCMP was later further developed into the National Security Directive No. 24: National Cyber Crisis Management Policy and Mechanism, which was launched in 2013. This directive aims to ensure a high level of preparedness in the face of threats and cyberattacks at the national level.

The National Security Council, with CyberSecurity Malaysia as the technical expert agency, have co-organised a periodic national cyber crisis drill entitled X-Maya since 2008. The main objective of the drill is to exercise the workability of the National Cyber Security Response, Communication & Coordination Procedure and to raise awareness of the national security impact associated with the significant cyber incidents among CNII. To date, X-Maya has been held 6 times, with the latest drill held on 7th March 2017.

PT 8: International Corporation

This thrust is essential as cybersecurity threats are not affected by physical countries' boundaries and borders. One of the main objectives identified by this thrust is to increase Malaysia's involvement and participation at the international level in key international cyber security organizations and platforms to mitigate cyber threats from information sharing and to overcome cybersecurity challenges among member countries. Malaysia is a member of the Forum of Incident Response and Security Teams (FIRST) and the Regional Asia Information Security Exchange Forum Meeting (RAISE) -- a cooperative platform for information sharing, communications and promoting best practices.

Among key initiatives under this thrust, CyberSecurity Malaysia became the co-founder, first chair and permanent secretariat of the Organization of Islamic Cooperation – Computer Emergency Response Team (OIC-CERT). CyberSecurity Malaysia is also a co-founding member and current deputy-chair of the Asia Pacific Computer Response Team (APCERT).

V. CONCLUSION

Cyber threats are problems of today and the future. While developments in the area of ICT allow for enormous gains in efficiency, productivity and communications, they also create opportunities for those with devious ambitions to cause harm. We have to be prepared for the worst, especially to protect our critical national information infrastructure.

Securing CNII against cyber threat activities requires the efforts of the entire nation. The government alone cannot sufficiently secure CNII. It calls for public-private-community cooperation in addressing the matter. The government can take the lead in many of these efforts, provided it is supported by the private and community sectors. Thus, a comprehensive master plan to create a secure and sustainable CNII for Malaysia against cyber threats must be formulated and developed.

As a result of the successful implementation of the NCSP Thrusts and initiatives, Malaysia has managed to attain 3rd place among 193 countries worldwide in the ITU GCI 2014 survey and maintain its position in the subsequent ITU GCI 2017 survey. In securing CNII, Malaysia is recognized as a champion by the World Summit Information Society (WSIS) Prizes 2016 and 2017 for international collaboration.

Securing CNII is a continuous effort and policy reviews are crucial to ensure it is abreast with the latest, dynamic and complex technologies. Research in this area, especially policy updates and reviews, can possibly be further conducted to lead to the development of a better strategy and policy framework to counter cyber threats.

VI. REFERENCES

[1] Ministry of Science, Technology and Innovation Malaysia, "National Cyber Security Policy." 2006.

[2] US Department of Homeland Security, "Blueprint for a Secure Cyber Future - The Cybersecurity Strategy for the Homeland Security Enterprise," 2011.

[3] J. Russell and R. Cohn, *Critical Infrastructure Protection*, Bookvika Publishing, 2012.

[4] T. G. Lewis, T. J. Mackin, and R. Darken, "Critical Infrastructure as Complex Emergent Systems," *Int. J. Cyber Warf. Terror.*, vol. 1, no. 1, pp. 1–12, 2011.

[5] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for Critical Infrastructures: Attack and Defense Modelling," *IEEE Trans. Syst. Man Cybern.*, vol. 40, no. 4, pp. 853–865, 2010.

[6] H.-C. Chu, D.-J. Deng, and H.-C. Chao, "Potential Cyberterrorism via a Multimedia Smart Phone Based on a Web 2.0 Application via Ubiquitous Wi-Fi Access Points and the Corresponding Digital Forensics," *Multimed. Syst.*, vol. 17, no. 4, pp. 341–349, Nov. 2011.

[7] R. Heickero, "Terrorism Online and the Change of Modus Operandi," *Swedish Def. Res. Agency, Stock. Sweden*, pp. 1–13, 2007.

[8] I. Bernik and K. Prislan, "Cyber Terrorism in Slovenia - Fact of Fiction," in *The 3rd International Multi-Conference on Complexity, Information and Cybernatics*, 2012.

[9] J. Jarmon, "Cyber-terrorism," *J. Terror. Secur. Anal.*, pp. 102–117, 2011.

[10] S. W. Beildleman, "Defining and Deterring Cyber War," *Mil. Technol.*, pp. 57–62, 2011.

[11] R. Lemos, "SCADA system makers pushed toward security," *Security Focus*, 2006.

[12] The Lipman Report Editors, "Cyberterrorism: The Invisible Threat Stealth Cyber Predators in a Climate of Escalating Risk," *Guardsmark, LLC, Memphis, Tennessee, USA*. 2010.

[13] B. Kesler, "The Vulnerabilities of Nuclear Facilities to Cyber Attacks," *Strategic Insights*, vol. 11, pp. 15–25, 2011.

[14] W. J. Broad, J. Markoff, and D. E. Sanger, "Israeli Test on Worm Called Crucial in Iranian Nuclear Delay," *New York Times*, Jan 15, 2011.

[15] S. Quadir, "Bangladesh Bank exposed to hackers by cheap switches, no firewall - Police," *Reuters*, 2016.

[16] K. N. Das and J. Spicer, "How the New York Fed fumbled over the Bangladesh Bank Cyber-Heist," *Reuters*, 2016.

[17] K. Lema, “Philippines Urges Bangladesh to Share Results of Heist Investigation,” *Reuters*, 2016.

[18] M. Hayden, “A Timeline of the WannaCry Cyber-Attack,” *ABC News*, 2017.

[19] AFP, “Global ransomware attacks on the rise: Europol,” *The Star Online*, 2017.

[20] “WannaCry Ransomware,” *Europol*, 2017.

[21] J. Wattles, “Who Got Hurt by the Ransomware Attack,” *CNNMoney*, 2017.

[22] The Sun, “WannaCry ransomware attack in Malaysia confirmed,” May 16, 2017.

[23] MA-661.052017: MyCERT Alert – WannaCry Ransomware,” 2017. [Online]. Available: https://www.mycert.org.my/en/services/advisories/mycert/2017/main/detail/1263/index.html.

[24] W. Z. A. Zakaria, M. F. Abdollah, O. Mohd, and A. F. M. Ariffin, “The Rise of Ransomware,” Proceedings of the 2017 International Conference on Software and e-Business, [Online] pp. 66–70, 2017. Available: http://delivery.acm.org/10.1145/3180000/3178224/p66-Zakaria.pdf?ip=175.139.192.49&id=3178224&acc=ACTIVE%20SERVICE&key=69AF3716A20387ED%2E624C05D357EE4F12%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&__acm__=1542614296_0b300d3e7203ebedea3b3a3994bc7e32

[25] N. Koswanage, “Malaysia tries to stop threatened cyber attack,” *Reuters*, 2011.

[26] C. Fuchs and D. Trottier, ed., *Social Media, Politics and the State*, Protests, revolutions, riots, crime and policing in the age of Facebook, Twitter and YouTube, New York, Routledge, 2014

[27] D. F. Wamala, “ITU National Cybersecurity Strategy Guide.” International Communication Union (ITU), 2011.

[28] “Global Cybersecurity Index (GCI) 2017.” International Communication Union (ITU), 2017.

[29] Jabatan Perdana Menteri Malaysia, “Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 Dalam Sektor Awam.” 2010.

[30] S. N. Hamdan, S. Ismail, and M. A. Khalid, “Preparation towards ISMS Certification 27001: An Experience in Malaysian Nuclear Agency,” vol. 44, no. 49, 2011.

[31] CyberSecurity Malaysia, “Guideline to Determine Information Security Professionals Requirements for the CNII Agencies / Organisations.” 2013.