Journal of Theoretical and Applied Information Technology
15th December 2017. Vol.95. No 23
© 2005 – ongoing JATIT & LLS

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

NATIONAL CYBER SECURITY STRATEGIES FOR DIGITAL ECONOMY

[1]CHOOI SHI TEOH, [2]AHMAD KAMIL MAHMOOD

[1]Faculty of Science & Information Technology, Universiti Teknologi Petronas, Malaysia

[2]Associate Professor. Faculty of Science & Information Technology, Universiti Teknologi Petronas, Malaysia

E-mail: [1]chooi_g03449@utp.edu.my, [2]kamilmh@utp.edu.my

ABSTRACT

Digital economy is strengthening in prominence and relevance in the era of increasingly connected world in the cyberspace. The boom in digital economy, however, is coupled with cyber threats and cyber risks for nations in the form of malware, escalating organized cybercrime, personal information and data breach, and Advanced Persistent Threat (APT). As such, nations need to prepare for the cyber threats from new frontiers namely Internet of Things (IOT), mobile and cloud technologies. National cybersecurity strategy (NCSS) is an essential element as cybersecurity is needed to protect and enable digital economy. This article seeks to gain insights on the relationship between the development of the NCSS and the success of digital economy of the nation based on literature from journal articles, global reports, current industry happenings and market trends. NCSS of nine nations were analyzed centered on digital economy success. Interestingly, it was found that the readiness of nation to reap digital economy is not correlated to the development and publication of the nation's NCSS. In order for digital economy to thrive, the digital confidence of the stakeholders should be high. Nations with high digital confidence depend less on the national level NCSS to strengthen the trust and confidence in digital space. Nevertheless, the NCSS is still a need as a foundation for long term strategy to cement the cybersecurity of the nation, as cyber threats and risks keep evolving and will remain a challenge. A country like Singapore is intensifying its efforts and commitment in national cybersecurity. The existing top ten nations in digital economy has NCSS providing the necessary foundation for digital economy to flourish further. Though a NCSS is not a requirement for nation to begin digital economy, NCSS is a requirement for a nation to continuously develop and to be successful in digital economy.

Keywords: *Cybersecurity, Digital Economy, National Cybersecurity Strategy, Critical Infrastructure, Cybercrime*

1. INTRODUCTION

The connected world offers amazing opportunities as the global population is shifting to the cyberspace. In order to be relevant and competitive, businesses need to be online and innovate to be part of digital economy. Technology and economy merged to transform the way of doing business to access new market and wealth creation. Information is an agent of integration and enabler of innovation in business [1]. It is time to embrace disruptive technologies and innovation, as it is business unusual. The social transformation is happening now as connected world changes our societal fabric in politic, economy, technology and culture. This digital evolution impacts the world in multiple facets, from e-economy, social movements, government elections and awareness of global issues swiftly [2].

In evolving cyberspace, the technology keeps pushing the boundary of digital economy. One of the most disruptive innovation is bitcoin, which breaks barriers and create new rules. This open network banking defines the world's first digital currency based on peer to peer agreement. It started as peer to peer agreement currency in 2010, with 10,000 bitcoin transacted for a pizza, with each bitcoin at USD0.0025 [3]. By 14 August, 2017, bitcoin soared passed USD4,000 [4]. The digital currency redefines financial sector, as it removes the middle man, and creates a community to maintain and thrive within the system. The year 2017 sees the dramatic rise of bitcoins with the value quadrupled from January to August 2017 [4]. Bitcoin has also been marred by linkage with Silk Road bust and anonymities of cyber criminals. In 2017, the waves of WannaCry and Petra ransomwares hit globally. Both demanded payment in bitcoins [5]. The cryptocurrency and blockchain technology will expand and gain prominence as Digital Asset Research Lab was launched as research and development initiative between Blockchain (a software platform digital assets) and Imperial College London's Centre of Cryptocurrency Research and Engineering (IC3RE) [6].

As the relevance of digital economy increases, the need for secured cyberspace increases. Cyber threats aspect is inescapable in digital progress [2, 7]. In the growth of cyber dominance, cybersecurity is a need. For nations to leverage and prosper in digital economy, national level strategy is developed to provide the necessary foundation and infrastructure to secure the cyberspace. Cybersecurity is a crucial element in national security [8]. Nations need to balance the needs of digital economies and to ensure the reliability and security of the cyberspace [9]. Protection against cyber threats had become top priority for nations across the globe. In 2015, UK government had affirmed cyber threats as Tier One risk in their 2015 National Security Strategy (NSS) [10]. The Department of Defense in US had developed its first cyber strategy in 2011, and released the updated Department of Defense Cyber Strategy in 2015 [11]. For national cybersecurity, it is vital to focus on critical infrastructure protection, combating cybercrime effectively and national defense capabilities.

In this article, we focus on the national cybersecurity strategies (NCSS) of the top ten nations in digital economy readiness. The objective of this paper is to examine the NCSS and how it influences the digital economy in the nations. The aim is to gain insights into the correlation of NCSS development to the progress of digital economy in the nations. The rise of digital economy changes of everything, from business models to roles of CIOs [12]. Cybersecurity is no longer about preventing attack, it is the cornerstone of digital economy [13]. The digital disruption creates opportunities and development to businesses and nations. We analysed the NCSS of the nations, and the extent of relationship to the digital economy of the nations.

2. RELATED WORK

2.1 Digital Economy

Digital economy is defined as economy base on electronics goods and services and formed by electronic business models, integrated with global network of economy and social, enabled by ICT such as internet technologies [12].

The growth and potential of digital economy depend on the trust on the internet and in cyberspace. Digital economy is estimated at 22.5% of the world economy and yet it has not been fully exploited [13]. The leader in digital economy, the US, amassed USD 5.9 trillion through digital economy, which equates 33% its Gross Domestic Product(GDP) [13]. Digital investments have growth multiplier effect in national GDP, where it increases the national economic output. In US, this digital investment is expected to translate into additional 2.1% of GDP in 2020, equivalent to additional USD 421 billion [13].

Nations are at the infancy of the Fourth Industrial Revolution, transitioning to new era where digital, biological and physical world merge [14]. In this digital revolution, opportunities and growth rest on conducive regulatory and business environment, ICT readiness on emerging technologies, and usage of ICT in societal-wide adoption and leverage [15]. For a nation to thrive and prosper in this century, digital intervention is unavoidable. World Economic Forum published Networked Readiness Index (NRI) to assess and compute nations' readiness to capture and reap the benefits of emerging technologies in digital economy [15]. The top ten nations based on NRI are listed in Table 1.

Table 1: The Networked Readiness Index 2016

RANK	NATION / ECONOMY	INCOME LEVEL *	GROUP **
1	SINGAPORE	HI	ADV
2	FINLAND	HI-OECD	ADV
3	SWEDEN	HI-OECD	ADV
4	NORWAY	HI-OECD	ADV
5	UNITED STATES	HI-OECD	ADV
6	NETHERLANDS	HI-OECD	ADV
7	SWITZERLAND	HI-OECD	ADV
8	UNITED KINGDOM	HI-OECD	ADV
9	LUXEMBOURG	HI-OECD	ADV
10	JAPAN	HI-OECD	ADV

(Source : World Economic Forum - The Global Information Technology Report 2016: Innovating in the Digital Economy [16]) *Income Level : HI = high income economies that are not members of the OECD; HI-OECD= high income OECD members**Group: ADV= Advanced Economies

In this digital revolution, the opportunities are coupled with risks. Hyper connectivity exposes nations to cyber threats. Digital economy raises the issues of security, privacy and trust [12]. Nations and governments need to employ new technologies to capture the benefits and to improve cybersecurity to mitigate cyber risks. Cybersecurity is key enabler for digital-enabled economy and society.

The opportunities and boom in cyberspace are coupled with risks and cyber threats. As digital economy is expanding, cybercrime is a growth industry. In 2014, global cybercrime cost more than USD 400 billion annually, the number rose to USD 450 billion in 2016 [16]. Another record reported global cybercrime cost to reached USD 575 billion annually [17]. For the top four largest economies (US, China, Japan and Germany), total loss in cybercrime reached USD 200 billion [16]. In cybercrime, the loss not limited to actual losses due to the attack, as it involves recovery and opportunity costs. A study in Italy reported that losses in cybercrime was USD 875 million, yet the cost of recovery and opportunity lost was USD 8.5 billion [16]. Cybercrime also affects company reputation, goodwill and stock prices. Year 2013 is the beginning of cybercrime-driven mega data breaches, with eight mega breaches [18]. A mega breach is defined as a breach of more than 10 million records [17]. In 2015, the trend of mega breaches grew to loss of 429 million identities in mega breaches and yet this number hides a bigger number that remained unreported [17].

For a nation to protect its ICT investment and enable digital economy, articulation and publication of national cyber security strategy is identified as an essential element [7]. To achieve the necessary economic outcome, the NCSS need to state the strategic objectives, identify the responsible and accountable entity, develop specific, measurable, attainable, results-oriented and time-measurable (SMART) outcomes, and commit implementation plan based on available resources and support [7].

2.2 Cyber Threats to the Nations

For a nation, threats in cyberspace are divided into the cyber threats tools, the threats agents and also the attack vector. The cyber threats tools are the "what", threat agents are the "who" and the attack vector is the "how" [19]. The major risks for a nation encompasses cyber espionage, organised crime in cyberspace, hacktivism, and cyber terrorism [20]. Threats are from various sources, from the commonly recognised sources such as criminals, malware, or even targeted cyber attacks. However, the future of cyberspace is also threatened by policies, as the right balance of policies will enable the growth of innovation and advancing cybersecurity [21].

The cyber threats for a nation are identified as below:

2.2.1 Malware and Zero-Day Attack - The global proliferation of malicious software or malware had increased the threats and risks in cyberspace. Malware had also started to infect mobile devices, with more than 8 million samples of malware in 2015 [19]. Nowadays, malware is designed to be sophisticated and efficient. The number of malware had been increasing, with the reported number of malware reached 2 billion threshold in Jan 2016 [19] . Malware is a convenient and efficient tool to executed a cyber attack. The demand remains high as the shift of cyber attack motivation shift from curiosity and fame-seeking to illicit financial gain [22]. The top malware types are Trojan, Worms, Exploits, Virus and Backdoor. While Trojan is accounted for the majority of the Malware at 67%, there was a rise in greater percentage of worms in 2015 [23]. Top countries hosting online resources are Russia ca. 50%, US ca, 12%, The Netherlands ca. 8% Germany ca. 5% and France ca. 3% [19]. In 2015, 54 zero-day vulnerabilities were found, making it an average of one every week [17]. Advanced attack groups are using the zero-day vulnerabilities in their toolkit for their exploits. It had become a commodity product that is hunted professionally since 2014. In 2016, there is a change of tide, with drop of zero-day vulnerabilities and malware. However, email became with main vector of malware propagation, with email malware rate increased to 1 in 131 emails [5]. For 2016, the top keyword in the malware email campaigns was "Invoice" [5].

2.2.2 Rampant organised cybercrime - Cyber criminals had leveraged the cyberspace in their crimes through cyber-dependent crimes and cyber-enabled crimes. In UK, internet banking fraud rose to 133.5 million pounds in 2015 [24]. It is reported that the average economic impact of cybercrime per organisation is USD15.42 million in US for year 2015 [25]. This cost of cybercrime is increasing by the year. In UK, the companies lose up to 37 billion euro per year. In 2016, cybercriminals became bolder, with attacks against banks to steal millions. The Banswift group stole USD81 million from Bangladesh Central Bank, capitalising on Swift codes [5]. Another sophisticated group called Odinaff also targeted banks and financial institutions, using malware and Swift. The cost of cybercrime to a nation, is not limited to the monetary cost, as it also involves national security, public confidence and the cost of stolen intellectual property [16]. Ransomware started in 2016 with average ransom shot to USD1,077[5]. In May 2017, WannaCry attacked more than 230,000 computers in over 150 countries, cemented as the first major global ransomware [26]. This is quickly followed by Petya ransomeware attack in June 2017. Both ransomwares demanded ransom to be paid in bitcoins as it is decentralised, unregulated and high anonymity.

2.2.3 Personal information and data breach - In the age of internet, information is fuel. Data breaches started to be rampant in 2011, when it was reported as the Year of Data Breach [18]. In the year 2013, there were eight mega breaches. 2013 was the beginning of Mega Breaches [18]. In 2015, the reported mega breaches are 13[5]. The total number of identities stolen was 563,807,647. In 2016, this number doubled to 1.1 billion identities stolen, with 15 mega breaches [5]. Of the breaches recorded in 2016, 85% happened in the US. The personal data stolen feeds the underground economy, where everything has a price. One can find a Netflix account, to an online banking account for sale. Credit card details are the most popular goods in the underground marketplace, with price differs according to country, the card level and other additional information [5].

2.2.4 States and State-sponsored attacks - Increasingly, states and state-sponsored groups are targeting the national network, for political diplomatic, technological, commercial and strategic motives [24]. These attacks' principal focus are the critical national infrastructures such as government, defence, finance, energy and telecommunications sectors [24]. The connectivity of the critical national infrastructures amplifies the cascading effect and impact of breakdown of critical national infrastructures [27]. A prime example is the Estonia attack on 27 April 2007. The most wired country was attack by tsunami of botnets [19]. The attacks were regarded to have come from Russia with state approval, yet it is considered unconfirmed [28]. Stuxnet was a worm used to cripple the Iran's nuclear plant in 2010. This sophisticated virus managed to destroy the fastspinning centrifuges. In 2016, the US presidential election campaign was also marred and influenced by "living off the land" attack executed by state-sponsored group [5]. The term "living off the land" refers to technique of cyber attack using resources at hand without malware and exploits [5]. The speculation of interference by foreign power continues to be debated, especially with a handful of key elections due in 2017. In 2016, many states had developed cyber espionage capability and some had advanced to offensive cyber skills including destructive capabilities [24].

2.2.5 Advanced Persistent Threat (APT) - In 2015, there was a rise of APT targeting governments and major corporations [23]. APTs are sophisticated and stealth programs that are usually custom-designed to infiltrate and lurk in the computer systems and networks of the specific organisations, making them a silent menace to camping, that deal in sensitive trade or production information, performed by threat agents of high capacities [19, 23]. In 2015, F-Secure detailed a well-resourced, highly dedicated and well-organised cyber espionage group called the Dukes. The group, was believed to be working for the Russian Federation since 2008, targeting state bodies [23]. The main objective of APT is to steal data and thus, requires high level of stealthiness and prolonged period of months or years [19]. The APT usually covers all the phases in a kill chain [19]. It starts with reconnaissance, a phase of strategic information gathering. Then "weaponisation" and followed by "exploitation" [19]. In September 2015, to protect economic and organisations interests, US and China reached an agreement that "neither country will conduct economic espionage in cyber space" [5]. Targeted attack was rampant in 2016, with incidents in Europe, US, Asia and the Middle East. Some targeted attack groups identified has motives of espionage, sabotage and subversion, possibly originated from Russia, China, US, Western Region, Iran and North Korea[5].

Digital economy thrived and empowered by digital connectivity, is accompanied by costs and challenges. As nations joining the bandwagon to ride the success of digital economy, securing a nation's cyberspace is an unparalleled task. Cyber threats to nation evolve, revamp and borne so often due to dynamism of cyberspace. Speed of things and time to markets should not be prioritised at the expense of cybersecurity. In cyberspace, the offence and the defence has the same innovations, however, the defence is hands-bound with regulations and processes. The offence has another advantage in cyber attack, as the ratio of offence to defence, is always many-to-one [29]. A cybersecurity team needs to defend continuously against cyber attackers, while a malicious offender just need to have one successful attack. Nations need to prepare for the new frontiers in cybersecurity. The incoming threats will be from IOT, mobile and cloud technologies[5].

3. METHODOLOGY

This article is based on literature research. The researchers accessed information from variety of literatures, based on journal articles, global reports, current industry happenings and market trends. After the literatures were gathered, the researchers sort them out to determine the relevance to finalise the representative literature to the topic [30]. The relevance of the literatures chosen is based on purpose, authority, effectiveness and reliability [30].

For the purpose of the research, the representative literatures chosen were from year 2010 - 2017. The issues in cybersecurity are current and fast moving. Representative literature on the topic need to be current to be relevant. In this article, reports, journal article and technology news from reliable sources were included. It provides a review of recent practices and development in digital economy and NCSS.

4. NATIONAL CYBERSECURITY STRATEGIES FOR DIGITAL ECONOMY

Opportunities through digital economy in cyberspace go hand in hand with cyber risks and cyber threats. Cybersecurity is a need in the progress and growth of digital economy. As nations capitalising on digital revolution, cybersecurity is a national priority to foster economic welfare [31]. Based on NATO and ENISA, in the period of 2013-2016, there was a total of 48 national cybersecurity strategies (NCSS) released. In NCSS, the main objectives are maintaining secure, resilient and trusted electronic operating environment, promoting economic and social prosperity, promoting trust, business and economic growth, addressing risks of ICT and strengthening resilience of infrastructures [9]. Each NCSS has variance in scope and depth, with main priorities as roles and responsibilities of cybersecurity, situational awareness, legislation matters, training and R&D, secured ICT products and services and international cooperation [32].

The top ten NRI nations are equipped with national cybersecurity strategies (NCSS). These NCSS published from 2003 till 2016. It is important that all these strategies remained updated and current, as cyber threat landscape is evolving [33]. For the purpose of analysis in this article, nine NCSS are analysed as shown in Table 2. NCSS from Sweden is not included as the document is in Swedish.

From the nine NCSS, the most recent ones are NCSS from Singapore and United Kingdom [10, 34]. For the digital-savvy nation of Singapore, it is the first NCSS. The NCSS of Singapore is comprehensive and inclusive of governance and legislative framework for cybersecurity. It also introduced the situational awareness capability, to enable stakeholders to act swiftly in cybersecurity incidents. The UK is an exemplary example in NCSS as it released its first NCSS in 2009, followed by National Cyber Security Strategy 2011-2016. The latest instalment for 2016 - 2020, is updated, current and relevant to the cyber threat landscape [10].

NCSS are built differently in every nations, based on the priority and cyber threats, even EU and US are driven by different visions [31, 35]. Some of the fundamental elements for NCSS are organisational, legal and technological [8]. The nine NCSS for the nations provided the strategy to build and provide the trusted cyber environment required for digital economy to prosper. In order digital economy to thrive, security is a need [29]. Singapore, Finland and Switzerland are prospering in digital economy although they only have the first NCSS [34, 36, 37]. This is due to the strong and effective private sector and industry that support the cyber environment. It leads to increase of digital confidence and trust among the digital citizens and organisations. United States and Norway pioneered the effort of NCSS, with the first NCSS released in 2003. United States had been actively publishing cybersecurity policy and strategy for specific purpose and yet to release another national cybersecurity strategy since 2003 [38]. Each of the document is purposeful in various aspects of cybersecurity such as critical infrastructure framework and DOD cybersecurity strategy, however it does not synthesise the holistic cybersecurity strategy in US. Japan was pioneer in Asia with the first release in 2006.

Table 2: National Cyber Security Strategies

Nations	SGP	FIN	NOR	USA	NLD	CHE	GBR	LUX	JPN
Year	2016	2013	2012	2003	2013	2012	2016	2015	2015
NCSS	CYBER SECURITY STRATEGY	FINLAND'S CYBER SECURITY STRATEGY	CYBER SECURITY STRATEGY FOR NORWAY	NATIONAL STRATEGY TO SECURE CYBERSPACE	NATIONAL CYBER SECURITY 2: FROM AWARENESS TO CAPABILITY	NATIONAL STRATEGY FOR THE PROTECTION OF THE SWITZERLAND AGAINST CYBER RISKS	NATIONAL CYBER SECURITY STRATEGY 2016-2021	NATIONAL CYBER SECURITY II	CYBER SECURITY STRATEGY
First NCSS	Yes	Yes	No (2003)	Yes	No (2011)	Yes	No (2009)	No (2011)	No (2006)
Size (pages)	27	44	32	60	36	42	80	41	58
CIP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CCP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CPD	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
R&D	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IC	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP	No	No	No	No	Yes	Yes	Yes	Yes	No
M	No	No	No	No	No	Yes	Yes	No	No
NCC	2016	2014	2014 (research purpose)	2008	2012	2003 (research purpose)	2016	Planned 2017	2015

*CIP = CI Protection *CCP = Cyber Crime Protection *CPD = Cyber-security Professional Development
*IC = International Collaboration *PA = Public Awareness *IP = Implementation Plan
*M = Measurable *NCC = National Cyber-security Centre

Finland and Luxembourg defined the meaning and scope of cybersecurity in the document [37, 39]. This is important as it specify the boundary as nations has different understanding of the scope of cybersecurity. The clarity avoids misinterpretations of responsibilities nationally and internationally.

In the NCSS, the strategic elements are focused on protection of critical infrastructure, defence against cybercrime, cybersecurity professional development, increasing public awareness, improving research and development (R&D) and international collaborations [10, 11, 33, 34, 36, 37, 39]. In this article, the pillars of NCSS for digital economy, critical infrastructure protection, defence against cybercrime, cybersecurity professional development and national cybersecurity center and R&D are discussed.

4.1 CI Protection

Cybersecurity for critical infrastructures (CI) is crucial as critical infrastructures becoming highly connected and interdependent, to improve efficiency and costings. Each nation defines and chooses CI sectors differently, based on cyber threats perception, socio-political factors, and even country specific peculiarities [38]. In NCSS analysed, NCSS Singapore is the only which listed the CI sectors. In NCSS Singapore, 11 CII sectors are divided into Services, Utilities and Transport are identified. Services CII are led by Government Technology Agency (GovTech), Ministry of Home Affairs (MHA), MOH Holdings, Info-Communications Media Development Authority (IMDA) and Monetary Authority of Singapore (MAS). The Utilities CII are led by Energy Market Authority (EMA), Public Utilities Board (PUB) and Info-Communications Media Development Authority (IMDA). Transport CII lead by Land Transport Authority (LTA), Maritime and Port Authority (MPA) and Civil Aviation Authority of Singapore (CAAS).

The management of cybersecurity of CI in each of NCSS is different and yet with some similarities. In UK and Singapore, government take major role in leading the CI protection. For Singapore, the effort in CI protection divided into four major steps by strengthening the governance and legislative in cybersecurity, committing cybersecurity effort in government including allocating 8% of Government ICT budget on cybersecurity, enhancing cyber situational awareness to increase capability to response to cyber threats and implementation of dedicated CII protection program [34]. In UK NCSS, ensuring CNI is secured and resilient against cyber attack is priority. CNIs are responsible for cybersecurity of the critical systems and must possess tested capabilities to respond to attacks, with the necessary investment in staff and technology. The government will facilitate critical information sharing, conduct cyber exercises, offer advice and guidance on cyber risks and initiate cybersecurity-working collaboration. The NCSS also calls for introduction and initiation of high-end security to support the increasing need and demand in cybersecurity. On the other hand, in Finland, most critical infrastructures are owned and generated by private sector. The NCSS stated the goal to guarantee operations of CI businesses and there is plan of Cyber Security Centre will provide the situational awareness.

In Switzerland, NCSS focused on decentralised structure. NCSS Switzerland identified resilience of CI to cyber attacks as one of the overriding goals, to be achieved in decentralised structure. The emphasis for CI are risk and vulnerability analysis, and continuity and crisis management.

NCSS of US, Luxembourg, Japan, Norway and Netherlands highlight the need of partnership and cooperation to achieve cybersecurity protection for CI. In NCSS US, one of the key goals is to prevent cyber attacks against CI. The key priority is partnership between government and industry to enable a national cyberspace security response. The coordinated effort targets to improve national incident management and exercise cybersecurity continuity plan. A national cyber threats and vulnerabilities reduction program to access national vulnerabilities, assess emerging systems and secure processes and mechanisms were included. NCSS Luxembourg emphasises on strengthening national cooperation amongst stakeholders including CI to increase synergies and avoid duplications. The resilience of digital infrastructure is increased by sharpening operational aspect, cyber simulations and exercises and governance tools and frameworks. In Japan, NCSS calls for strong public and private partnership for CI to enhance safety standards implementations and efforts to reexamine existing measures and activities to improve cybersecurity. It outlines the constant review and improvement for CI protection, ensure effective and prompt information sharing and governmental support tailored to CI sectors.

In Norway NCSS, each sectorial ministry is responsible for identifying CI in their sector and ensuring adequate security. It also calls out for coordinated security measures and regular drills. The cybersecurity drills serve as competency improvement and also platform for coordination and cooperation.

Netherlands focus on risk-based approach to increase resilience of CI and national detection and response network to cooperate on real-time analysis and sharing of threat information.

4.2 Defence against Cybercrime

In order to create a safe and secure cyberspace for the people, cybercrime defence is crucial. The internet had presented the criminals a platform to commit cybercrime in anonymity, quickly and widely. In the cyberspace, no nation is an island, as the world is now a connected global village. International collaboration is crucial in protecting nation and defending against cybercrime. Knowledge sharing and collaboration efforts amongst nations are critical to mitigate the impact of cyber attacks. The deep linkage and collaborations amongst nations enhance and increase collective cybersecurity.

Singapore, Finland, Norway and the Netherlands identified police in the NCSS to combat cybercrime. NCSS of Singapore outlined National Cybercrime Action Plan (NCAP). The plan is multi-facetted from people, enforcement, legal and international partnership. Public awareness and education are key to prevent cybercrime. The police force and relevant agencies to increase the capacity and capability against cybercrime, and supported by the strong legislative. The NCSS also outlines the international collaboration to increase cybercrime awareness and prevention. In Finland NCSS, in cybercrime prevention, it stated that police need to have the necessary power and capabilities to prevent, expose and solve cybercrime. It calls for necessary competencies in investigation in digital evidence and legal system to combat cybercrime. Norway NCSS penned ability to prevent, detect and investigate cybercrime as one of the strategic priorities. It states that all stakeholders to implement cybercrime prevention measures on their own initiative in their organisations. Authorities and police to make this a priority and increase the capacity and capability in handling cybercrime. It calls for police to have presence online, openly and covertly, to prevent, avert and investigate cybercrime. It must proceed to collaboration and information sharing amongst cybercrime prevention stakeholders. In Netherlands, NCSS stated tackling cybercrime as one of the main objectives, with action plan. It prioritises the fight against cybercrime by improving the capacity and capability of the police in cybercrime, supported by the legal system. It places emphasis on financial sector cybercrime. International collaboration in investigation, knowledge and expertise sharing are key in combating cybercrime.

US and Switzerland take a different approach by classifying cyber attacks as crime, to highlight the severity and priority. In US NCSS, cyber attacks classified as crime and threats and vulnerabilities are identified to remediate. It seeks swift apprehension and punishment for cybercrime. It also promotes international collaboration and global efforts for investigation and prosecution of cybercrime. Similarly, NCSS Switzerland placed cyber attacks as severe crime against the state and a special economic crime. New risks regarding cybercrime are identified, analysed and evaluated, as effective reduction in cyber risks especially in cybercrime is one of the main overarching goals.

As cybercrime is cross-border and global, international cooperation and coordination in investigation and prosecution are essential. Luxembourg, Japan, Singapore, Netherlands, US and UK highlight partnership and collaboration to combat cybercrimes. NCSS Luxembourg focus on improving legal framework and international collaboration to combat cybercrime. In Japan NCSS, the government promote information gathering for understand cyber vulnerabilities, and promote security measure to the people. It also enhances measure against cybercrime by improving response, investigation capabilities and international coordination to combat cybercrime.

In UK, NCSS states the capacities and capabilities improvement of law enforcement in handling cybercrime. The NCSS states a creative way to deter cybercrime. It looks into preventive step by studying cybercrime business model to increase the cost of executing cybercrime in UK, and also introduce early intervention program to deter development of cybercriminals. It has collaboration and intelligence sharing between government and private sector to counter cybercrime. International partnerships are implemented for investigation and prosecution cybercriminals. The NCSS also state a 24/7 reporting and triage capability called Action Fraud.

4.3. Cybersecurity Professional Development

As the challenges and threats grow in cyberspace, cybersecurity workforce need to be expanded and strengthened. The demand for the skilled cybersecurity professional outweighs the availability of the talent. An additional 1.5 million cybersecurity professionals are needed globally by 2020 [40]. Every nation dependent on digital economy deemed cybersecurity professional development as a long term goal. The shortage will be stark and the demand will increase exponentially as the digital market grow.

Finland, Netherlands, Luxembourg, UK and Japan plan for the long term cybersecurity professional talent pool by incorporating cybersecurity knowledge and skills into their education systems from primary to higher education. In Finland NCSS, the goal is to improve understanding, competence and skills among the authorities, businesses and citizens to create a strong cybersecurity community. The plan is to develop the competency through research. Finish education systems have cybersecurity skills included at all levels of education (comprehensive school, vocational, secondary school and higher education), and also successive national and international cyber exercises where competence and skills are sharpened. Netherlands NCSS aims for cybersecurity knowledge infrastructure to support the nation's resilience, develop expertise and finding niche. It uses multidisciplinary approach which includes non-technical sub-area where cybersecurity has a prominent role and encourage innovation. The NCSS includes a task force for cybersecurity education where private and public sector collaborate to increase quality and breadth of cybersecurity at all academic levels (primary, secondary and professional). The tasks include revising curriculum, development of learning modules and increasing certifications of information security professionals. Luxembourg NCSS plans to introduce cybersecurity training in primary and secondary education. Trainings on cybersecurity are included for different levels and aspects of practitioners, from operators of CIs, civil servants and decision makers.

NCSS UK listed the issues of cybersecurity skills shortage as lack of young generation in the industry, current shortage of cybersecurity specialists, insufficient exposure of security concepts and elements in computing courses, lack of qualified teachers and absence of established career and training pathways. The NCSS defines clear roles and responsibilities of government and industry to address the matter. It aims to integrate cybersecurity skills into education systems, from primary to post graduate levels. Trainings and recognised career pathways made available for practitioners. The UK NCSS also approach to address gender-imbalance in the industry and to tap into the widest talent pool to strengthen cybersecurity skills. UK is the only NCSS which strikes the chord on the gender imbalance issue in the industry. Japan NCSS stated the great shortage of quality and quantity of cybersecurity workforce. It promotes the development and assurance of the human resource with technological capabilities with high ethical standards. NCSS states comprehensive plan for human development in cybersecurity through promotion in higher education and vocational training, discover and nurture the best talent to excel in cybersecurity, create long term career path for cybersecurity experts and strategising human resources to maximise organisational capacities in cybersecurity. The NCSS has long term thinking by embedding cybersecurity into the elementary and secondary education.

Similar to UK and Japan, Singapore plans to attract human resource in cybersecurity with well-defined and attractive career path in cybersecurity. Singapore NCSS aims to establish a professional cybersecurity workforce to ensure Singapore has well-trained talents in cybersecurity. It encourages more professionals to garner internationally-recognised certifications and create a sustainable and strong community to practise cybersecurity.

NCSS Norway calls for joint and coordinated program for awareness and training to build culture of cybersecurity. Public authorities are tasked to survey and measure the level of cybersecurity competency of businesses and citizens. US NCSS calls to foster sufficient training and education program to support cybersecurity needs. It states to increase efficiency in training programs and to promote recognised cybersecurity certification for the professionals. As reported in 2016, US target to train 100.000 cybersecurity practitioners by 2020 [29]. NCSS Switzerland plans competence building option document as a reference to detect gaps and as guidelines for skills and competence building for practitioners in cybersecurity. Training guidelines encompass administrative, technical and strategic level.

The societal trust and confidence in the cyberspace are the core of digital economy, as the public confidence drives the economy. Thus, public awareness and knowledge in cybersecurity increase the trust to strengthen digital economy. The professional cybersecurity workforce contributes to building the societal trust as they support and sustain the security in cyberspace.

4.4 National Cybersecurity Center and R&D

Nations are intensifying efforts in cybersecurity by setting up national cybersecurity centers for the purpose of preemptive, detection, mitigation and recovery efforts in cybersecurity. All of the nine nations have national cybersecurity centers except Luxembourg. These centers specialised in cybersecurity incidents handling and mitigation of cybercrime except for Switzerland and Norway which focus on R&D only. The earliest was by United States in 2008, and the most recent were Singapore and United Kingdom in 2016. The national cybersecurity centers in Switzerland (Zurich Information Security & Privacy Centre) and Norway (Center for Cyber and Information Security) committed on the nation's research and development with multiple stakeholders. Luxembourg government stated that it is to be the next cybersecurity hub, and the launch of Cyber Security Centre of Competences is expected in 2017 [41].

Technological improvement and R&D set the innovation for the nation to flourish and to defend in cyberspace. Each NCSS stated the focus on R&D to increase competitiveness by translating innovations into cutting-edge products and spurring the development of highly skilled professionals and researchers. In the NCSS of United Kingdom, it prioritised development of cryptography and offensive cyber skills. This is in line with the progress and development digital economy and digital currency. Japan is the only one which focus on Internet of Things (IOT). The Japan NCSS highlight improvement of IOT to be part of Japan's socio-economic vitality and sustainable development while ensuring "security as a quality feature" as a prerequisite [42].

In the nine NCSS analysed, few have implementation plans and even fewer have measuring process. Netherlands, Switzerland, UK and Luxembourg incorporated the implementation plans. Only UK and Switzerland follow through with measurement to monitor the progress and success of NCSS. Implementation plan and measurement are essential to ensure that NCSS is executed accordingly and in a timely manner.

Based on the ranking of NRI, the most ready nation for digital economy is Singapore, which is the latest amongst the nine nations to release NCSS [15, 34]. The nation was ready, with trust and confidence in the cyberspace which translates into conducive environment with high adoption by stakeholders [15]. The success of the digital economy lies on the trust of the consumers and organisations to the technology and the digital economy environment [29]. Since 2016, Singapore had been ramping cybersecurity efforts highly, including the introduction of Cyber Security Bill 2017. The bill empowers Commissioner of Cybersecurity, consolidate and harmonise bill for CII, designate and prioritise CII, proactive to cybersecurity threats and incidents and regulate cybersecurity providers [43]. With the addition of national effort on cybersecurity, Singapore will thrive further in the digital economy.

5. OPEN RESEARH ISSUES

Since 2000, the digital economy evolved steadily till it created digital evolution. The mobile connectivity now has stamped cyber vulnerability to be inescapable aspect of digital evolution [2]. There are increasing researches done regarding digital economy: introduction of Digital Evolution Index [2], the change of role and responsibilities of CIO to ride digital economy [12], digital identity management for digital economy [14] and future researches on cybersecurity in digital economy [13]. In terms of NCSS, Luiijf discussed and compared nineteen NCSS [33]. Despite that, the aspect of NCSS in digital economy is relatively unexplored. Cybersecurity is comprehensive and not to be done in isolation, especially in highly connected society. Some of the issues are discussed in the subsequent subsections.

5.1 CI Protection

CIs are the backbone of nations' functionality, including national and economic security [46]. In the name of efficiency and convenience, CIs in nations are highly connected and leveraging on cyberspace. A break in the weakest link ripples across the economy and the impacts are multiplied because the risks interconnect and create cascading effects across all sectors [46].

5.2 Defense Against Cybercrime

The "bright lights" of cyberspace is marred with the rise of cybercrime. Due to the speed, anonymity and ease of cybercrime executions, the exponential rise of cybercrime is alarming. The white hats and the governments are on defense against cybercrime, and yet are plagued with issues of cross border investigation and prosecution.

5.3 Cybersecurity Professional Development

As the demand for skills and knowledge in cybersecurity increases, the lack of professional in the industry becomes stark. By 2020, 1.5 million additional cybersecurity professionals are in demand globally [42]. It is also a field of knowledge that evolves and changes quickly. The demand for new talent and professionals increases and the existing pool of talents need to be constantly updated and upgraded.

5.4 National Cybersecurity Center and R&D

Nations are strategizing the future of their nations through cybersecurity. National cybersecurity centers are established for defense and offence purposes. As connectivity increases in society, the issues of ethics and privacy need to be considered and addressed.

6. CONCLUSIONS

In digital economy, innovation is permanent. The Digital Revolution poised new challenges to business and nations, as boundaries are tested and redefined constantly. Digital economy leverages on the cyberspace and it is coupled with the evolving cyber threats. For nations to prosper in digital economy, readiness in technology environment and networked infrastructure depends on the trust and confidence of the stakeholders, namely government, private sector and individuals. These trust and confidence of the stakeholders are the enablers of the digital economy.

One of the method to increase trust and confidence in cyberspace is implementation of national cyber security strategies which address cybersecurity issues. The common emphasis of the NCSS analyzed are critical infrastructure protection, cybercrime protection, cybersecurity professional development, cybersecurity public awareness, research and development (R&D) and international collaborations. The development of national cybersecurity centres creates national nexus to preempt, response and mitigate cyber threats and incidents. An actionable and measurable NCSS should include implementation plan and measurement. This enable a measurable progress in a timely manner. The core is, cybersecurity of the nation is strengthened.

In this research, the readiness of nation to reap digital economy is not correlated to the development and publication of the nation's NCSS. In order for digital economy to thrive, the digital confidence of the stakeholders is high. Nations with high digital confidence like Singapore, depend less on the national level NCSS to strengthen the trust and confidence in digital space. The NCSS is still a need as a foundation to long term strategy to cement the cybersecurity of the nation, as cyber threats and risks keep evolving. Singapore is beginning to intensify its efforts and commitment in national cybersecurity. The existing top ten nations in digital economy has NCSS. It provides the necessary foundation for digital economy to flourish further. A NCSS is not a requirement for nation to begin digital economy, however, NCSS is a requirement for a nation to continuously develop and be successful in digital economy.

REFERENCES

[1] Hemmatfar, M., M. Salehi, and M. Bayat, Competitive advantages and strategic information systems. International Journal of Business and Management, 2010. **5**(7): p. 158-169.

[2] Chakravorti, B., *Where the Digital Economy is Moving Fastest*. 2016, Harvard Business School: Harvard Business Review.

[3] Lee, T., Five years of Bitcoin in one post. 2014, Washington Post.

[4] Iyengar, R., Bitcoin has doubled in value in a month to over $4,000, in CNN. 2017.

[5] 5.Symantec, 2017 Internet Security Threat Report. 2017.

[6] Campbell, R., Bitcoin Wallet Blockchain Partners Imperial College London to Launch Research Lab. 2017, Cryptocoins News.

[7] Hathaway, M.E., *Cyber Readiness Index 1.0*. 2013, Hathaway Global Strategies LLC: Great Falls, VA.

[8] Elkhannoubi, H. and M. Belaissaoui. Fundamental pillars for an effective cybersecurity strategy. in Computer Systems and Applications (AICCSA). 2015.

[9] NATO, National Cyber Security Strategy Guidelines, CCDCOE, Editor. 2013: Tallinn, Estonia.

[10] UK.Government, National Cyber Security Strategy 2016-2021. 2016.

[11] US, D., The Department of Defense Cyber Strategy. 2015.

[12] 12.Weill, P. and S.L. Woerner, The Future of the CIO in a Digital Economy. MIS Quarterly Executive, 2013. **12**(2).

[13] Mulligan, C., Cybersecurity: cornerstone of the digital economy, in Imperial College Business School London. 2017, Imperial College London: London.

[14] Al-Khouri, A.M., *Emerging Markets and Digital Economy*. International Journal of Innovation in the Digital Economy, 2012. **3**(2): p. 57-69.

[15] Knickrehm, M., B. Berthon, and P. Daugherty, *Digital Disruption: The Growth Multiplier*. Accenture Strategy, 2016.

[16] Schwab, K., *Fourth Industrial Revolution*. 2016, World Economic Forum.

[17] Baller, S., S. Dutta, and B. Lanvin, The Global Information Technology Report

2016: Innovation in the Digital Economy. 2016, World Economic Forum: Geneva.

[18] McAfee, Net losses: Estimating the Global Cost of Cybercrime. 2014.

[19] Symantec, 2016 Internet Security Threat Report. 2016.

[20] Symantec, 2014 Internet Security Threat Report. 2014.

[21] ENISA, ENISA Threat Landscape 2015. 2015.

[22] Republic, C., National Cyber Security Strategy of the Czech Republic (2015-2020). 2015.

[23] Burt, D., et al., Cyberspace 2025 today’s decisions, tomorrow’s terrain. Microsoft, 2014.

[24] Choo, K.-K.R., The cyber threat landscape: Challenges and future research direction. Computer & Security, 2011. **30**: p. 719-731.

[25] Secure, F., Threat Report 2015. 2015.

[26] UK.Government, UK National Cyber Security Strategy. 2016.

[27] ENISA, The cost of incidents affecting CIIs. 2016.

[28] Solon, O. and A. Hern, 'Petya' ransomware attack: what is it and how can it be stopped?, in The Guardian. 2017.

[29] W.E.F.-. The Global Risks Report 2016.

[30] Belam, M., We're living through the first world cyberwar – but just haven’t called it that. The Guardian, 2016.

[31] Commission on Enhancing National Cybersecurity. Report on Securing and Growing the Digital Economy. NIST. 2016.

[32] Lin, G., Higher Education Research Methodology- Literature Method. International Education Studies, 2009. **2**(4): p. 179-181.

[33] Luiijf, E. and K. Besseling, *Nineteen national cyber security strategies.* International Journal of Critical Infrastructure, 2013. **9**.

[34] Lehto, M. *The Ways, Means and Ends in Cyber Security Strategies*. in *12th European Conference on Information Warfare and Security*. 2013. Finland: Academic Conferences and Publishing International Limited.

[35] Norway, Cyber Security Strategy for Norway. 2012: p. 32.

[36] Singapore, Singapore's Cybersecurity Strategy. 2016: p. 27.

[37] Kshetri, N. and S. Murugesan, EU and US Cybersecurity Strategies and Their Impact on Businesses and Consumers. Computer, 2013. **46**(10): p. 84-88.

[38] Switzerland, National strategy for the protection of Switzerland against cyber risks. 2012: p. 42.

[39] Finland, *Finland's Cyber Security Strategy*. 2013, Secretariat of the Security Committee.

[40] Shafqat, N. and A. Masood, *Comparative Analysis of Various National Cyber Security Strategies.* International Journal of Computer Science and Information Security, 2016. **14**(1): p. 129-146.

[41] Luxembourg, National Cybersecurity Strategy II. 2015: p. 23.

[42] Suby, M. and F. Dickson, The 2015 (ISC)2 Global Information Security Workforce Study. 2015, ISC2.

[43] PWC, Luxembourg to become a Cyber Security hub. 2016.

[44] Japan, Cybersecurity Strategy. 2015: p. 58.

[45] 45.Tham, I., 5 key proposals from Singapore's new Cyber Security Bill, in The Straits Times. 2017: Singapore.

[46] Teoh, C.S., A.K. Mahmood, and S. Dzazali. Is NIST CSF applicable for developing nations? A case study on Government Sector in Malaysia. in PACIS 2017. 2017. Langkawi.