KnE Social Sciences

FGIC2019
FGIC 2nd Conference on Governance and Integrity 2019
Volume 2019

Knowledge E
enriching | engaging | empowering

Conference Paper

Cyber Warfare Impact to National Security - Malaysia Experiences

Azian Ibrahim[1], Noorfadhleen Mahmud[2], Nadrawina Isnin[2], Dina Hazelbella Dillah[2], and Dayang Nurfauziah Fauz Dillah[2]

[1]Faculty of Industrial Management, Universiti Malaysia Pahang, Lebuhraya Tun Razak, 26300 Gambang, Pahang, Malaysia
[2]Faculty of Administrative Science and Policy Study Universiti Teknologi MARA 94300 Samarahan Sarawak

Abstract

This study analyzed the cyber warfare impact on national security and focusing on Malaysia experiences. The issues regarding cyber warfare have become a serious concern since it was a risk of national security in Malaysia. The objectives of the study are to analyze issues related to cyber warfare that affected Malaysian system security, to determine causes that caused to cyber warfare. This study used a qualitative research approach to evaluate the current defense approaches related to cyber warfare in Malaysia. The interviews were conducted with the respective respondents: the Senior Manager, Research Management Centre, Strategic Research, and Advisory Department of Cyber Security Malaysia Department. This study can contribute to expanding the security of national security by demanding the government to adopt a broad acquisition risk management strategy. It can assist in the development of highly effective aggressive and defensive methods to any company dealing with future cyber warfare challenges and risk.

Keywords: cyber warfare, national security, experiences.

Corresponding Author:
Azian Ibrahim
aziani@ump.edu.my

Received: 5 August 2019
Accepted: 14 August 2019
Published: 18 August 2019

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the FGIC2019 Conference Committee.

1. Introduction

As stated by the Global Information Assurance Certification Paper (2004), cyber warfare can be defined as cyber-attacks provide the terrorists a chance of bigger safekeeping and flexibility in operational. Ideally, it used a computer to attack from anywhere in the worldwide, avoid revealing the assailant to physical injury. In other words, this cyber warfare can have hacked the system of the computer without the owner of the computer knows that their computers been hacked by those cyber-attackers. They can attack the computer from one location to another location just by one click of the mouse. According to Ahmad Hemmat (2011), in recent decades, the world has witnessed the salient social transformation as our lives became inextricably linked and dependent upon technology and more particularly the internet. It has brought the influences in every aspect of people

business and governmental transactions. There is crucial to understand and learn more about cyber-warfare due to the current environment now that all are depending solely on the internet. Furthermore, based on definition from U.S Army's Cyber Operations and Cyber Terrorism Handbook, they distinct cyber warfare as solely the latest form of information fighting and its comprise computer network attack (CNA), which contains the disruption and rejection of operations, damages or abolish resident information both in computers or computer networks or the computers and network themselves (Swanson, 2010). A CNA involves in "hacking" of other nation's computer networks, however, used different data systems as physical weapons when performing an attack. There are important elements that must be highlighted, which are attack and defend. The information would be the one been attacked.

Based on Ahmad Hemmat (2011) stealing information from storage devices and also attack data that has been processed, evaluate, and distribute information. They will attack the networking by using any form or method. Another important element in defending which involve what would be defended or protected. For example, to safeguard the information processes from being stolen and as well as disseminate the information from being attacked and protected on networking as a whole. In most cases, the growth of the technology has brought the progressive changes especially in the field of information sharing and innovation in defenses systems around the world, but this innovation turn into vulnerability is inescapable in today's globalized world.

According to Global Information Assurance Certification Paper (2004), the more developments in information and communications technology have revolutionary effect on the public, especially large impact towards our life and all the activities or actions become much depends on the information infrastructure. Apart from this, cyber warfare has also brought an impact on national security. National security can be defined as the term "security," it may be known as a free from the threat or risk of the simple principles both either in group or individual. While according to (A.Rahman, 2010) the national security can be defined as the national independence and local integrity as the most crucial to be defended.

National security not solely the objectives to be achieved but should be enlightened appropriately to the possible way. According to A.Rahman (2010), in Arnold Wolfares's seminal essay, he defined national security as "ambiguous symbols." In other words, it is combined with the emotional and political appeal within the full range of relevant meanings. There are different meanings of national security in other states. For example, the United States of national security policy in the 1980s and 1990s has to resolve with the Soviet Union and the relation of the United States has with the Soviet Union. It also

happened in Malaysia, whereby Malaysia also has its pre and post-independence. This situation gave diverse stages of national security and threats. The government policies become tighter when there is high pressure on the threats.

The Internal Security Act in Malaysia was first established and has been enforced in parliament on 1st August 1960 which to combat the threats from Communist and subversive action (A.Rahman, 2010). Malaysian Government could not accept 583 Communist members who located in the northern region as a Malaysian citizen after realizing what they had done to the country, especially during the establishment of the Act. National Defense Week has invited challenges from international adversaries, but three strong national defenses imply an efficient military which might threaten people's liberty (A.Rahman, 2010).

In conclusion, cyber warfare has brought the impact on national security when national security is weakened and easily can be hacked by those attackers. National security should be tightening as the technology nowadays can be reached easily, especially by those attackers, and the government must ensure their security more tighten as technology is moving forward. Therefore, this research will discover the issues related to cyber warfare that affected Malaysian system security, which aims to determine the factors that contribute to it and make an evaluation of the current defense approaches.

2. Statement of Problem

War, crime, and terrorism are outdated ideas which happen in a physical way, whereas cyber warfare is one that is used in conventional media as with information warfare. Lots of definition related to cyber war and it refers to the war on the internet or known as cyberspace which consists of Cyber-attacks alongside to a nation and communication network as well as cyber-terrorism where they used cyberspace to commit terrorism. It's being acknowledged as prohibited attacks and risk of attacks. They used computers, networks, and any information stored. Usually, cybercrime is faced by many parties and not only effect on individual but also the organization as well as the nation. According to Yunos (2008), the intention of doing a cybercrime is further towards computer-related crimes and to achieve monetary as their attention.

From the information security point of view, the risk is well-defined as possible to cause an undesirable case may affect assets, systems, or organizations. Three types of dangers have been identified, which is intentional, accidental, and environmental. Intentional threats include used fake or prohibited software while service down, a

mistake in people design or hardware failure can be considered as an accidental threat. Meanwhile, environmental dangers are further on the environmental effect such as quakes, thunderstorms, or lightning. As generally understood, these three threats cannot be removed but having effective measures to control such pressures inside each organization, which believed it can be reduced.

According to Yunos (2008), threats can cause an undesirable effect on safety, socio-economy, and human lives if not correctly controlled. New challenges faced by investigating computer-related crime by forensic specialists, as stated by Broadhurst (2006). Change away from “script kiddie” reliefs to cruel software which program aimed to rip-off information, specifically special identification data.

The challenges of taking out evidence from computers or servers are increased because of the more significant use of encryption and access protection. Many victims are not willing to lodge a report any wrong wrongdoings with regards to cybercrime, and this becomes a never-ending problem. As a consequence, these activities will lead to infrastructure security are dangerous. The available online source code and automatic “easy to use” hacking devices which act as system observation had offer variety manipulation tools and set up “spy-ware.” Key logging monitoring or program is an example that leads to other unlawful activity together with shakedown, financial or internet fraud, theft, telecommunications theft, and economic surveillance.

Furthermore, “patch” pledge an act to measures and have proved as insufficient due to numerous users unsuccessful to informed (both the software was legal nor illegal) as “MS blaster” proven, even though the accessibility of an active patch previous months before they relief of this specific malicious code.

According to Broadhurst (2006), many organizations of law enforcement are not able to answer efficiently to cybercriminals, including developed country, “play catch-up” with cyber-savvy wrongdoers. In a few years back, there is a keen technique in taking a customer’s identification by using web-page “jacking”. One of the cases that have been reported in December 2003, where an example of cyber-theft happen at copied Hong Kong and Shanghai Banking Corporations’ internet banking website that cooperated an unknown number of customers’ identification. Currently, cyber-criminals were operated for failed or failing situations. These will lead to wrongdoing to the worldwide economy, by providing a safe place.

According to Broadhurst, it is never happening before wherewith as lower cost the offender can face a terrible loss or destruction towards individuals, companies, and governments for another sphere. For instance, a 14year-old Hong Kong Boy was detained because of forming a malicious website which he claimed the website is

getting accredited by a well-known local newspaper. False information regarding SARS epidemic has been a blast on that website. Widespread panic was triggered among the Hong Kong community due to rumors that Hong Kong would be declared a red signal.

Other issues arise was in superstores where it is over-run by fearful citizens to buy more than usual of foodstuffs to get prepare for the quarantine rumor in Hong Kong. The situation becomes well after a few hours later when the government made a press conference and repeated an announcement which rejecting the unauthorized statement.

Meanwhile, a teenager (14-year-old) was found guilty and positioned below the welfare house for one year. From these threats is has shown that the sensitivity of "information security" is no longer in place. Everyone now can easily involve in this new medium to do a criminal, commercial communication, or relaxation purpose. They do not require more technical or computer specialist to do.

According to Gaurav Raghuvanshi, (2015), the recent case where it was involved Malaysia Airlines Website that has been hacked or attacked by a group of hackers. The group was calling itself as 'Cyber Caliphate.' The website has been hacked by this group that attempts to resolve a mark with a U.S. computer game firm. Users who go to that website have experienced different image as usual. They notice that the message stated 'ISIS WILL PREVAIL' was pop up on their browsers window and they have a difficulty to do a transaction. They cannot make an online ticket booking because that service was not available. It happens to Malaysia Aircraft (A380 plane) where '404-Plane Not Found 'was appeared and it was 'done by Cyber Caliphate.' Both messages showed on the website. After that, the website had displayed different image which the website appeared a weird image. On the same day, the transporter changed the effected site with an appropriate version which gave customers to reserve flight tickets.

According to Pierluigi Paganini (2014), the financial institution also being effected in 2014. Affin Bank, Al-Rajhi Bank and Bank of Islam and other 17 bank outlets belonged to United Overseas Bank are reported being hacked by the Latin American gang. The losses were about more than RM3 million Malaysia Kini (2014) reported.

According to Mohd Hafizzuddin, in June 2011, Malaysian websites have been attacks by cyber-attacks and the hackers known as "Anonymous." It is being reported by Malaysia's Communications and Multimedia Commissions (MCMC) that about fifty-one of webpages in the "gov.my" domain was attacked. Forty-one suffered different ranks of interruption. This was disseminated through denial of service (DDoS).

Effected "gov.my" websites was reported cannot be accessible for the public. Due to this, the Malaysia Computer Emergency Response Team (MyCERT) performed a quick

action to resolve the destruction caused by 6 “Anonymous.” Within 24 hours prior to the attacked, all the affected “gov.my” websites were speedily back to normal.

According to Mohd Hafizzuddin, Malaysia has established a national cyber-security specialist that was known as Cyber Security Malaysia (CSM). It was parked under the Ministry of Science, Technology, and Innovation (MOSTI) in 1997 were formerly known as the National ICT Security and Emergency Response Center (NISER). Generally, this agency was established in order to observe Malaysia’s e-security aspect. Besides that they act national cyber-security to implement the policy, center of technical coordinator as well as a center for cyber risk research and assessment center.

According to MOSTI, there are 8 procedures under The National Cyber Security Policy which are Effective Governance, Legislative & Regulatory Framework, Cyber Security Technology Framework, Culture of security and Capacity Building, Research & Development towards Self-Reliance, Compliance, and Enforcement, Cyber Security Emergency Readiness, International Cooperation. In assisting Malaysia’s moving forward to a knowledge-based economy (K-economy), National Cyber Security Policy was created. The Policy was framed based on a National Cyber Security Framework which consists of regulation and control, technology, cooperation between public-private, institutional as well as worldwide aspects.

According to Mohd Hafizzuddin, in order to safeguard national security, efforts to infiltrate an infrastructure of a sovereign nation could further evolve from standard hacking and denial of services to the destruction and crippling the entire nation’s survivability or its ability to defend itself. The basic infrastructure and networks need to dependable, and governments have to implement a complete method to guard itself against any offensive activities. An essential vibrant of computer security is that the defenders must continually furnish themselves to protect vital information since enemies can attempt attacks at any time.

3. Research Objectives

There are several objectives of the study on the cyber warfare impacts towards national security based on Malaysian experience which are: (i) To analyze issues related to cyber warfare that affected to Malaysian system security (ii) To determine factors contribute to cyber warfare (iii) To evaluate the current defense approaches related to cyber warfare in Malaysia.

4. Literature Review

There are various terms of cyber warfare used in literature. Cyber-warfare can be well-defined as attacking and protecting information and computer networks in cyberspace, as well as denying an adversary's ability to do the same (Global Information Assurance Certification Paper, 2004). According to Parks and Duggan (2011), cyber warfare is the mixture of computer networks attack and defense which support with technical operations, and it is supported by Billo (2004) cyber-warfare consists of units organized along nation-state boundaries, either in an offensive or defensive operations. Through electronic means which used computers to attack other computer or network. While national security is referring to how protective measures of the state is taken. How they are avoiding their provinces and people from physical attack by others which include protection against important state economic, politic, military, social, and cultural and interests from being attacks by foreign or domestic sources which may harm, erode, or abolish these interests, thus threatening the strength of the state. This protection can carry out by military or non-military means (David S. Alberts, 2000). Since 1998, Scott Borg argued at a conference in Colarado Springs that lots of cyber-attacks have taken place. From 1998 to 1999, Kashmir, India, and Pakistan have developed cyber militias to carry out attacks against one another (Caplan, 2013) and each of this country has used this strategy in their long-run conflicts.

According to Caplan (2013), the United States utilized cyber-attacks in Operation Allied Forces when the NATO airstrikes on Serbia, provoking an eventual counterattack by Russian hackers. With the help of Iranian technology during the year of 1999, Hamas has attacked Israeli cyber targets. Due to this, cyber-attacks have started as a key feature of the Arab-Israeli conflict. Cyber-attacks were also used in the conflict between Turkey and Armenia in the year 2000. After that year, the terrorist 13 organization Hezbollah started to attack against Israel. In 2006, it was turned for Indonesia and Malaysia began to utilize cyber-attacks in their dispute over the Celebes Sea. In 2007 Russian had to attack Estonia and it is called a Web War One. There were many important Estonian websites were flooded by request to access that make the server breaking up. This case one of the utmost wired compared to others state. As a result, Estonians cannot use their internet banking, online newspapers, or government portal services.

Based on Ahmad Hemmat (2011) in his research paper, Russia's earliest examples of politically motivated explicit cyber-attacks date back to as far as 2002. In 2008, they used cyber-attacks evolved from selective targets to becoming key component of Russian military strategies. In re-act to Georgia's attack to protestors in South Ossetia,

massive damage to the networks was did against the Georgian government. This is the first time that cyber-attacks overlapped with land, marine, and air attack by one state to another in the history of warfare. The aimed is to overload and ultimately shut down Georgian servers through their cyber infrastructure. As a result, the servers in Georgia were filled with inbound attacks, but no outbound traffic could get through (Caplan, 2013). In conclusion, those were the history of cyber warfare that has emerged until now and become one of the serious problems that need to be resolved before it spread widely

Cyber-terrorism can be defined as interfaces between people intentions and information technology for extreme events on the Internet or the cybernetic world (Bogdanoski, 2013). Also can be defined as the use of computer network devices to shut down critical national infrastructures like energy, transportation, and government operation to pressure or threaten a government or civilian population (Lewis, 2002). They used information technology to bring together and perform attacks against networks, computer systems, and telecommunications infrastructure either to swapping the information or acting electronic risk.

According to Lewis (2002), there were four elements of reassessment of the cyber threat. The elements are as follows:

1. Positioned both cyber warfare and cyber terrorism in the historical perspective of attacks against infrastructure.

2. Observe any cyber-attacks towards a backdrop of repetitive infrastructure problems. For example, there is extensive data on power outages, flight delays, and disruptions of communication that generally occur and the consequences of these routine failures can be used to gauge the effect of cyber-warfare and cyber-terrorism.

3. Measure the dependence of infrastructure on computer networks and redundancy present in these systems.

4. Must consider the use of cyber-weapons in the context of the political goals and motivations of terrorists and whether cyber-weapons are likely to achieve these goals.

Cyber weapons are new warfighting and it is not an old weapon of fighting. There are various options of cyber weapons that may choose by individuals or nations, including syntactic, semantic, and mixed weapons (Swanson, 2010).

By using Syntactic weapons, they target computers operating system which contains malicious code such as viruses, worms, Trojan Horses, disseminated denial of service (DDoS) and spyware. The cyber attacker shuts off a website by blasting it with vast volumes of traffic by using the DDoS attacks. Whereas in the semantic attack, to avoid producing any errors without the handler's awareness, they will convert information's enters into the computers system. In other words, the semantic weapon targeted the exactness of information to which the computer user has the right to use.

The mixed weapon is the combination for both of the weapons which are a syntactic and semantic weapon. It also can be called as "blended weapons." This weapon is to attack 18 both of the information and the computer's operating system, causing a further refined attack. For instance, based on what Swanson (2010) stated that assorted weapon is a "bot network," which is a multiplying of "bots," secretively fixed on not guilty to other computers.

Bots can be defined as automatic computer programs that spoil other computers. He or she can who has access to controlling it can detect, duplicate, and transfer sensitive data in a swarm attack against targeted computers. This person we called as a hacker. The attacked computers or networks that being infected by harmful software then will be controlled under an attacker in a remote control location (Swanson, 2010).

According to the Global Information Assurance Certification Paper (2004), information is an important valuable asset to any organization and is the main critical success factor. Lacking information security leads us at a certain level of threat. Based on Kenneth J. Knapp (2006) stated in his journal, for years, ' system security was a backburner issue among IT executives (Straub and Welke, 1998).

Security is now moving to the forefront follows the changes in the threat environment. A recent survey conducted by Lutfman and McLean (2004) in the same journal also, stated that security and privacy as the third top issue. Those who have specialties skilled in the particular area of security is high demand by the organization that wishes to protect their information security.

Furthermore, all information security controls and safeguard, and all dangers, vulnerabilities, and security process are a focus on this tenets yardstick (Global Information Assurance Certification Paper, 2004). Information is the highest significant asset in any organization. Regardless of any types of information takes either electronic, hardcopy, or a person's knowledge. The need for protection remains significance in order to offer business stability, capitalize on business opportunities, and soften potential risks to lose or damage.

According to Andrew Adams (2012) in 2011, the Internet came under a tremendously noticeable risk from the military. We do not refer to military forces attacking either the physical or informational infrastructure of the Internet but of growing claims by the US, UK and other military forces that they should be funded and authorized to conduct cyber-attacks to counter apparent threats to national security or national interests. While the concept of using communications infrastructure for military activity dates back to at least the early 90s, it is only very recently that the militaries of democratic regimes began proposing an explicit doctrine of legitimate cyber-offense. In this paper, we analyze the validity of these proposals by the military and find them lacking in justification both philosophically and practically. Based on the constitutional pacifism of Germany and Japan, we propose that military assets be focused on improving cyber-defense capabilities and not authorized to develop or deploy cyber-attack capabilities.

According to Lewis (2002), the military case for increasing its circle of activities to cyberspace is based upon the reality and potential for cyber-attacks. Although in the twentieth century there was a clearly defined principle (not always followed) that military personnel should be deployed primarily against other military personnel in attack and only in defense against civilian targets, this standard has come under pressure in many quarters in the last twenty years. It has been asserted that government-sponsored or even covertly condoned, cyber-attacks constitute military action.

According to Mohd Hafizzuddin (2011), there were cyber-attacks on Malaysian websites by the hacker known as “Anonymous.” According to the report from Malaysia’s Communications and Multimedia Commissions (MCMC), 51 of websites in the “gov.my” domain was attacked, where 41 of them suffered various levels of disruption. The caused: 24 a distributed denial of service (DDoS). The effected: inaccessibility of the “gov.my” websites for the public. As a result, the Malaysia Computer Emergency Response Team (MyCERT) acted quickly to mitigate the destruction caused by “Anonymous.” The affected “gov.my” websites were quickly put back online within 24 hours before the attack.

Mohd Hafizzuddin reviewed that it was noticeable to have Cyber Security Malaysia (CSM) established as the national cyber-security specialist for Malaysia. This agency, under the purview of the Ministry of Science, Technology, and Innovation (MOSTI) was earlier known as the National ICT Security and Emergency Response Center (NISER) in 1997, to monitor Malaysia’s e-security aspect. Besides that, CSM also plays a role as the national cyber-security policymaker, the national technical coordination center, and the cyber threat research and risk assessment center.

Mohd Hafizzuddin stated that in order for Malaysia's to dependence on cyberspace, infrastructure and networks must be dependable; therefore, the governments have to embrace a comprehensive method to protect from aggressive actions. The vibrant partnership between the private sector, the government law enforcement community and the national security community is vital in the way to boost up an ongoing national cyber defense competency. A new element of cyber defense that need to consider is the supply chain. In today world, the supply chain had become important in worldwide, and due to that, it has faced some weaknesses which can affect terrible damage if it is not being controlled properly.

Malaysia According to Borneo Post Online (2013), Malaysia is the sixth greatest open to cyber-crime. Malaysia is also reported to be significantly revealed to Android PC and devices malware attacks and listed ten riskiest countries. In the event of a cyber-crime, victims can lodge a report with Cyber Security Malaysia. Out of the RM1 billion in losses from cyber-crime in the first six months of this year, 9,857 cases were reported with 7,801 of these solved and 3,385 people arrested. Last year, the losses amounted to RM1.115 billion with 8,920 of the 11,543 reported cases solved and 3,712 people arrested.

According to Bukit Aman Cyber Crime and Multimedia Criminal Investigation officer ASP Mohd Syafiq Jinuin Abdullah, the regularity of cyber-crime cases had increased progressively, where about 6,586 reports of such cases were lodged last year with RM34 million incurred in losses compared with 6,238 cases involving RM18 million in 2010. He said online love scams usually involved African nationals whose love affairs with local women saw the latter being duped and losing their life savings to their paramours in extreme cases. A study showed that women who fall prey to the scams are single-mothers, unmarried women, and women with marital problems.

On cheating online purchases, it usually is reported by individuals who bought goods via online like mudah.my, e-lelong, and alibaba.com websites. The websites were not scams, but these websites assist as a platform for truthful traders to sell their products; however, they tend to invite fraud due to a lack of detailed procedures to control those involved in such scams.

Another cyber-crime method that has taken place was the fraud through online financial. It happened when consumers were fooled by unauthorized bankers or police officers that asking information such as bank account numbers. They claimed that the victim had won a contest or some other cases it is required to settle a credit card. They did not realize to be a victim until they know their money had been taken out without their approval.

Zahri Yunos (2008) reviewed that in 2001, Malaysia online systems were attacked by the Code Red worm. This is a typical case of how the system being attacked. Due to this, the Malaysia national communication network was stoppage, and it takes one quarter to remove these problems and losses caused were RM22mil. The viruses spread very fast, and this loss is not including other business losses as well as other sectors. In 2003 cyber-attacks caused by the Blaster and Naachi has been reported. Both worms started with the propagation of the Blaster worm through the scanning of vulnerable machines via the network, followed by Naachi worms. These worms used the weaknesses that have in the Windows NT, 2000, and XP software. The price for removing this was about RM31mil, which not counting any losses on intangible aspect like productivity and loss of business opportunity.

5. Methodology

Preliminary contacts were made to obtain the permission of the officers of the Cyber Security Agency and Malaysian Communication and Multimedia Commission to be interviewed. The sampling techniques best described as purposive and convenience, respectively.

6. Results

Objective 1: *To analyse issues related to cyber warfare that affected Malaysian system security*

In Malaysia, current issues related to cyber warfare are always about the elasticity of the Critical National Information Infrastructure (CNII) as provision for any cyber threats. CNII is defined as properties (real and virtual), systems, and functions that are vital to the nations. Their incapability or damage will give shocking impact to National such as economic strength, image, defense and security, impact on government functionality and public health and safety.

The National economic strength is where the self-assurance of the nation's key growth area can able to compete successfully in the global market while preserving satisfactory standards of living. To enhance national stature and sphere of influence, it's important to maintain a good national image.

National defense and security are to guarantee sovereignty and independence while maintaining internal security whereas Government capability is to functions and maintains order while performing and deliver minimum crucial to public services. Public

health and safety, they are responsible for bringing and maintaining optimal health care to all residents. There are ten sectors under CNI, which include National Defence & Security, Banking & Finance, Information & Communications, Energy, Transportation, Water, Health Services, Government, Emergency Services and Food & Agriculture.

The strength of any nation's security, against cyber-attacks, is as strong as its weakest link/point, and the National Cyber Security Policy (NCSP) was established to increase the resiliency of our CNII.

To assists Malaysia moving forward to a knowledge-based economy (K-economy), National Cyber Security Policy has been designed. A policy that formulated is based on National Cyber Security Framework. Its covers legislation and regulation, technology, a collaboration between the public and private sector, institutional as well as institutional aspects. NCSP seeks to address the risks to the Critical 41 National Information Infrastructure (CNII), which comprises the networked information systems often critical sectors.

The issue affected Malaysian system security is any CNII system that is compromised is capable of disrupting the well-being of the nation. It is always a catch-up scenario, as cyber threats are always evolving. The Malaysian system needs to continuously enhance the knowledge and adopt more IT-savvy in order to stay ahead of cyber threats practices in securing the CNII operations.

Besides, the table also explained what would be attacked in the cyber warfare which the Cyber Security stated that if the attack intention is to disrupt the national economy, therefore, any of the CNII organizations are a potential target. When the cyber warfare attacked, the things that are protected are systems that do not have an internet connection and have their independent power supply such as its generator. In contrary, all electronic devices are vulnerable to an Electro-Magnetic Pulse (EMF) type of weapon.

Government documents have also been affected by cyber warfare as information theft is always a concern as the illegally obtained information could have a negative impact on the economic fortune of the nation. On top of that, from the country perspective, the victims that usually attacked by cyber warfare is CNII organizations while from economic perspectives, it could be the business with valuable trade secrets. Cyber-warfare can harm the security system when any systems that are not adequately secured are at risk. The only differences are in the impact or implication when these systems are compromised. All systems are vulnerable as Malaysia is dependent on these "foreign" technologies.

Objective 2: *To determine factors contribute to cyber-warfare*

Few aspects that contribute to cyber warfare which are economic gains or advantages, corporate espionage, nation spying, to destabilize a nation, and many others. The factors mentioned are motivations or reasons that contribute to the attacks which typically are done through hacking into any computer or system, figure out the flaws, and exploit those flaws to increase control of that system and take the sensitive information or destroy the system to sabotage the "enemies."

Based on our finding, cyber-attacks have various impacts on the national security, which can jeopardize the political, economic, and social welfare of the country. The challenge of cyber warfare in Malaysia is in the fast detection of Advanced Persistent Threat (APT). Due to the pervasive and high interconnectivity in the cyber world, the scale of damages will be substantial from attacks on the CNII, for example, if TNB Power Transmission/Distribution services are down even though their power generation services are producing electricity.

Objective 3: *To evaluate the current defense approaches related to cyber warfare in Malaysia*

Cyber Security Malaysia claims that the current defense approach adopted against cyber-attacks is more of a proactive and preventive approach rather than reactive. The defense is done on an integrated and comprehensive approach rather than on a case basis. Preparedness as per the NCSP Policy Thrust Number 7, Cyber Security Emergency Readiness. Cyber Security Malaysia have been organizing with the National Security Council, regular Cyber Threat Simulation exercise called X-MAYA with CNII organization as part of the CNII preparedness in the event they are attacked.

Cyber Security has various Cyber Security Awareness for Everyone programme (www.cybersafe.my), which is a preventive programme and which is hard to measure as how do one measure something that was avoided or did not happen. The fact that there is still Malaysian being victims of cybercrime in the local media shows that more needs to be done. Cyber Security Malaysia is also assisting local Law Enforcement Agencies and the public by providing hotline e-mail at (cyber999@cybersecurity.my) in combating cybercrimes. The public can freely make any complain regarding the cyber-security issues to the mentioned email.

The defensive strategies using by cyber-security Malaysia to defend the national security being attacked by cyber warfare is being awareness, readiness, and knowledge sharing among the CNII organization. The National Cyber Security Policy addresses the need of the nation in order to avoid the national security attack. The current systems and policies are adequate to defend against the current threats, but there are no guarantees for tomorrow since the threat is always evolving. This is because Malaysia is ranked

Joined 3rd with Australia & Oman in the International Telecommunication Union's (ITU) 2014 Global Cyber Security Index.

7. Summary of Findings

From the findings on objective 1, it could be found that there are many issues related to cyber warfare that affected Malaysian system security. The issues are related to the CNII sectors, which consist of ten sectors. The cyber warfare could have attacked the Malaysian system security depend on the strength of resiliency of the CNII against any cyber threat.

Apart from that, in the findings of objective 2, it shows that there are various elements that can add to the cyber warfare in Malaysia which using various methods. The consequences of the cyber-attack not only harm the targeted victim but also the whole country will bear the adverse impacts. There is major challenge that the country must face, which is the fast detection of Advanced Persistent Threat (APT). Apart from that, due to the pervasive and high interconnectivity in the cyber world, there is a broad scale of damages caused by cyber-attack.

Last but not least, in objective 3, the findings discuss the current defense approach adopted against cyber-attacks by Cyber Security Malaysia. There are also defensive strategies using by cyber-security Malaysia to defend the national security being attacked by cyber warfare, namely being awareness, readiness, and knowledge sharing among the CNII organization. Besides, the applicable policy in Malaysia is the National Cyber Security Policy, which addresses the need of the nation to avoid the national security attack.

8. Conclusion and Recommendation

There are several consequences of the present research. From this study, it is proven that the Malaysian cyber-security is still lacking in some part of it, and there are many holes to be fixed. The government should follow the best practices in the developed country which experienced much longer in cyber security, for example, the United States. This is because there are still many cases of cyber attacking the national data system and individual privacy. Despite that, there are a lot of losses in terms of monetary and pride. The companies and organizations in Malaysia should not only depend on the government in protecting their respective cyber -security. Each of them should take their approaches and alternatives in adopting a new system as long as the system is

legal. The government should be bold in investing a lot in cyber-security purposes. This is because the money invested will be worth if any data breach can be detected in the early stages. This will help the government to avoid a lot of risks and losses.

Ethan Oberman (2014), the government need to be alert on the significance of guarding the sensitive national data because the range and cost of data breached are kept on increasing. The current era, all organizations, and companies are involved in controlling their valued information. All level need to understand this concept and not allow any delayed in any practices.

Malaysia has witnessed a massive breach of data that were arising due to malicious programs, and the financial impact is huge because of a data breaches. The cyber-security awareness in Malaysia also not communicated well through all citizens regardless of the walks of life. Ethan Oberman (2014) stated that lacking communication between IT and superior about the significance of cyber-security and damage a data breach may turn the company's public image to the bottom line. It is showed that the importance of communication about security awareness should be carried out to all levels of management.

This is because the consequences not only tarnish the organizations' and companies' but also the government as the responsible body to protect the national cyber-security in every level using various methods and approaches. The Malaysian cyber-security controls do not provide suitable protection for innovative cyber-attacks. This is because according to our finding, the government uses the proactive approach rather than a reactive approach which they only depend on the existing system in order to fight against the current cyber-attacks. This will be worsened when the government cannot find a way to fight the advanced cyber-attacks and still looking for the best way while the attacker is enjoying the moment the government is wasting. Malaysian cyber-security needs much improvement and still lacking in some part of it. There are several initiatives that have been mentioned by President Barack Obama (2008) that can be adopted into Malaysian cyber-security.

Firstly, use only Trusted Internet Connections to manage the Federal Enterprise Network and act as a single network enterprise. Secondly, install a sensor across Federal enterprise to detect any interference. It's very important for Malaysia Government network defense to use a passive sensor in Intrusion Detection Systems. Through the system, they can identify any unofficial users who plan to gain access to the network. Thirdly, set up the used of interference prevention systems through the Federal enterprise. As a result of these new ways, it is the next advancement to protect civilian Departments and Agencies of the Federal Executive Branch. Next is to pursue

research and development (R&D). These R&D activities are being sponsored by the government. Currently this initiative in the midst of developing strategies and structures in order to standardize all cyber R&D related works. Including R&D sponsored or lead by Malaysia Government. Fifthly, enhance situational awareness by connecting each of the cyber operations centers. Its need to ensure the government information security offices and strategic operations centers provide any information or data of dangerous activity to the federal system. Parallel with the practice where privacy protection and other protected information will be provided consistently to those who provide any wrongdoings.

Sixthly, plan such government-wide cyber counterintelligence (CI) need to be created and practiced since this plan was required to manage activities that happen across Federal Agencies. It is responsible is to spot, prevent, and alleviate the external cyber intelligence risk to Malaysia and private sector information systems. Finally, upsurge the confidence of our categorized networks. All sensitive information from Federal Government's which can support war-fighting, diplomatic, anti-terrorism, law enforcement, intelligence, and national security operations need to categorized or known as classified network. In order to secure the Malaysia Government in cyberspace, lots of investment or dollars have been spent however only the people who have an understanding, expertise and talents can implement those technologies. Implementation of CNCI in Federal Government or private sector is difficult due to not enough expert areas furthermore no stable career field in cyber-security. Currently, we have good cyber-security training and personal development programs but its lack of unity of effort. Developing a skilled workforce that equipped with technologically and cyber-savvy of next-generation employees are crucial. Therefore we can take technical advantage for future cyber-security.

Acknowledgement

We would like to thank Yayasan Bank Rakyat for the financial support by sponsoring this paper to be presented in the FGIC 2^{nd} Conference on Governance and Integrity 2019.

References

[1] Andrew Adams, P. R. (2012). A Non-Militarised Approach to Cyber-Security. 11th European Conference on Information Warfare and Security (pp. 1-8). Laval: Academic

Publishing International Limited.

[2] Billo, C. G. (2004). CYBER WARFARE: An analysis of the means and motivations of selected nation states. INSTITUTE FOR SECURITY TECHNOLOGY STUDIES.

[3] Bogdanoski, M., & Petreski, D. (2013). Cyber terrorism–global security threat. Contemporary Macedonian Defense-International Scientific Defense, Security and Peace Journal, 13(24), 59-73.

[4] BorneoPost, O. (2013, August 29). Cyber-crime a ticking bomb in Malaysia. BorneoPost Online, p. 2. Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. Emerald insight.

[5] Caplan, N. (2013). Cyber Warfare: The Challenge to National Security. Global Security Studies, winter 2013, Volume 4, Issue 1, 96-97.

[6] David S. Alberts, D. S. (2000). National Security Implications of the Information Age. Volume II Information Age Anthology, 10.

[7] GAURAV RAGHUVANSHI, N. P. (2015, January 26). Malaysia Airlines Website Hacked by Group Calling Itself 'Cyber Caliphate'.

[8] Global Information Assurance Certification Paper. (2004). Retrieved November 2, 2014, from SANS Institute: http://www.giac.org/paper/gsec/3873/information-warfare- cyber-warfare-future-warfare/106165

[9] Hemmat, A. (2011). Cyber Warfare (Russia, China, Iran). 18-20. 59 Ibid. (2010). Countering Challenges to the Global Supply Chain. Cyber Threats to National Security, Symposium One: Countering Challenges to the Global Supply Chain (p. 7). Virginia: CACI International Inc.

[10] Kenneth J. Knapp, W. R. (2006). CYBER-WARFARE. E-security.

[11] Lewis, J. A. (2002). Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic and International Studies, 2.

[12] Majid, D. M. (n.d.). Cybercrime: Malaysia. Royal Malaysia Police.

[13] Mohamad Faisol Keling, M. N. (2011). The Malaysian government's efforts in managing military and defence development. International Journal of Business and Social Science, 181.

[14] Mohd Hafizzuddin, M. D. (n.d.). Cyberplanning and Cyber Defense: A Malaysian Perspective.

[15] Moyer, L. R. (2004). Cyber-security, cyber-attack, and the development of governmental response: the librarian's view. New Library World, 248-255.

[16] Obama, B. (2008). The Comprehensive National Cybersecurity Initiative. Retrieved June 8, 2015, from The White House President Barack Obama: https://m.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

[17] Oberman, E. (2014, July 3). A Lack of Communicationon Cyber Security Will Cost Your Business Big (Infographic). Retrieved June 12, 2015, from Entrepreneur: http://www.entrepreneur.com/article/235318 Olga Angelopoulou.

[18] R. Parks, D. Duggan, Principles of cyberwarfare, Security Privacy, IEEE 9 (5) (2011) 30–35. doi:10.1109/MSP.2011.138.

[19] S. V. (2012). Who are you today? Profiling the ID Theft Fraudster. 11th European Conference on Information Warfare and Security (pp. 25-34). Laval: Academic Publishing International Limited. Schreier, F. (n.d.). On Cyberwarfare. DCAF HORIZON 2015 WORKING PAPER No. 7.

[20] Steinberger, R. (2014). Proactive vs. Reactive Security. Retrieved June 9, 2015, from crime research: http://www.crime-research.org/library/Richard.html.

[21] Swanson, L. (2010). The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict. Digital Commons at Loyola Marymount University and Loyola Law School.

[22] Yunos, Z. (2008, September 23). The Reality of Cyber-Threats Today.