CHAPTER 6:

CONCLUSION

The proliferation and advancement of ICT in Malaysia, in both public and private sectors have brought new threat to Malaysia. The threat, which comes in the form of information warfare, opens up new vulnerabilities to the Malaysian society and threatens national security. Information warfare, where the attackers engage in operations which involve digital non-physical attacks that manipulate and exploit the information infrastructure, is a costly type of warfare that can become a force multiplier during actual conventional warfare. The objectives of the attacker are clear; for exploitation, deception, destruction, and disruption or denial of service against their target.

The attackers or actors in information warfare are various; from individual to nation states and these actors can be categorized according to the threat level. The least dangerous actors are hackers followed by hacktivism, non-state and sub-state actors, and finally nation states, which sit on the highest level of threat. These actors have the ability to engage into at least five forms of information warfare attack which are hackint, offensive information warfare, terrorist information warfare, rogue information warfare, and amateur rogue information warfare. Hackint is operations that involve the collection of secret information and illegal acquisition of information through clandestine cybernetic penetration and disruption, and is concerned with digital espionage and sabotage activity into information systems. Offensive information warfare are operations engaged by nation states which possess offensive cyber attack capabilities by organizing deliberate effort to cripple or totally destroy the military's information capabilities, industrial and manufacturing information infrastructure, and information technology-based civilian and government economic activities. Terrorist information warfare is a type of information warfare attack that comes from an organized political group against the military, industrial, and civilian and government economic information infrastructures of a nation. Meanwhile rogue information warfare is where criminal organization or organized nonpolitical, criminal or mercenary groups wage the ongoing and sporadic deliberate information warfare attack against the military, industrial, civilian, and government economic information infrastructures or activities. Finally, amateur rogue information warfare is defined as the sporadic efforts of untrained and nonaligned individuals or small groups against the military, industrial, civilian, and government information infrastructures or activities of a nation.

These actors and their forms of attack are the menaces that Malaysia must resist as the country is aggressively promoting ICT as a set of tools for economic growth and efficient government administration. ICT operates on information infrastructure – a framework of interdependent networks and systems, generally interlinked at many different levels, comprising identifiable industries, institutions and distribution capabilities that provide a flow of products or services. It is a nationwide interconnection of communication networks, computers, databases and consumer electronics that make vast amount of information available to users which includes all government and civilian information infrastructures. It carries and links the critical infrastructures that constitute the life support systems of the nation. There are five sectors regarded as critical infrastructures, which are information and communication, energy, banking and finance, physical distribution, and vital human services. Information infrastructure is the target of attacks by the actors of information warfare to fulfill their objectives. There are various methods of attack that can be used by the actors to attack the information infrastructure, which include attack on the network connectivity, IP spoofing, password attacks, packet sniffing, software trojans, virus and social engineering. The attackers may use a combination of these methods of attack to optimize the impact of their attacks.

Realizing the threat posed by these actors and the consequences of the damage that these actors might inflict to Malaysia, the government erected and implemented multiple strategies to defend the information infrastructure. There are four defensive strategies taken by Malaysia, which are protection, deterrence, prevention and response. Various government agencies with different roles have been established to carry out the strategies.

In protection strategy, the government established the Government Integrated Telecommunications Network (GITN), which is an integrated communications and IT infrastructure to facilitate multimedia delivery of information and services between intra and inter government and also outside government. The GITN forms the Secured Government Intranet, which will be the foundation for developing the **EG*Net** – the Wide Area Network dedicated for the inter-connectivity between Government agencies implementing the Electronic Government pilot applications. The government also established ICT Security Division, a special division responsible for handling all aspects of information technology security in public sector, which are policy planning, implementation, coordination and monitoring of the security aspect of IT implementation in the public sector, including its role as expert reference on IT security training and the management of cryptology centre in the public sector. In addition to that, the government issued a manual security handbook, The Malaysian Public Sector ICT Management Security Handbook (MyMIS), which is intended as a reference and guide for public sector personnel in managing security in all public sector ICT installations.

In deterrence strategy, the cyber laws serve as the main pillar in entrenching deterrence strategy by erecting clear declaratory policies. Computer Crime Act is essentially a deterrence strategy where this act relates to offences due to the misuse of computers and complement existing criminal legislation. Under this law, unauthorized access or modification to any program or data held in computers is an offence and will be penalized. To invigorate the deterrence strategy, the government set up the Malaysian Computer Emergency Response Team (MyCERT). MyCERT (later incorporated into NISER) determines the attack mode, type of tools used, frequency of attacks, how the attacker exploit the security loopholes, which loopholes the attacker used, and modus operandi of the attack. By knowing the nature of the attack, it is easier for MyCERT to detect an attack and identify the attacker. The probability of the attacker to be apprehended is higher thus creating a sense of nervousness to any potential attacker that their malicious act will be punished accordingly.

NISER plays an important role in implementing prevention strategy. NISER functions as a security body assurance in an effort to assure the public that there is a national body that can handle all security threats and attacks on individuals, organizations and the nation. NISER provides early warning on the events that could give severe impact to Malaysia such as virus and worm attacks. The most important part is NISER provides warning to the government on coordinated attack that might be carried out by the attackers on Malaysia's information infrastructure.

Response, the fourth defensive strategy implemented by Malaysia, is carried out by three government agencies, which are the Royal Malaysia Police (RMP), MyCERT and the Public Prosecutor's Office. The RMP is given mandate to enforce Computer Crime Act 1997. Two units, the Technology Crime Investigation Unit (TCIU) and Computer Crime Forensic Lab (CFL) are set up specifically to conduct investigation and forensic investigation to pursue the criminal when a case is reported. Meanwhile, MyCERT functions by detecting the attackers' cyber location and informs TCIU to apprehend the perpetrators. The perpetrators will then be prosecuted by the Public Prosecutor's Office.

The strength of Malaysia's defensive capability comes from NISER, where this agency plays fourfold strategies, which are protection, deterrence, prevention and response. NISER implements protection strategy through its security enquiry service, advises various parties including the government and public in technical view about the vulnerabilities that they have, approaches to seal the problems, and measures they should take to counter the attacks. NISER is also working on establishing National Information Infrastructure Protection Agenda (NIIPA), a program or action plan to identify and protect critical information infrastructure that is important to the economic, socioeconomic and national security from information warfare attack. In implementing prevention strategy, NISER is actively doing research on new types of attack tools and how the tools are used by the perpetrator. NISER does its own research by constantly browsing the Internet, obtaining and accessing open source information. By knowing the latest tools that might be used on the newly known vulnerabilities, NISER could create measures and countermeasures and provides the information to the government and public. With years of experience, NISER is able to detect information warfare attacks. If the attacks originate outside Malaysia, NISER seeks the help from their foreign counterparts. The ability to detect information warfare attacks directly strengthens the deterrence strategy. If the country is under information warfare attack, NISER is capable of responding to the attack and to act accordingly to defend the country. NISER has the capability to detect and annihilate the first strike, and is capable of launching counterattacks and punishing the perpetrator severely.

Nonetheless, besides the strategies erected by the government and the initiative taken to defend the country from information warfare attack, there still exist a few weaknesses that must be overcome. First, the country depends too much on foreign ICT security software applications. These foreign software are full of security flaws and have a history of being penetrated and defeated by the attackers. Malaysia must reduce its dependency on these foreign security software and design its own software. Second, the enforcement of cyber laws, mainly the Computer Crime Act is weak. The lack of trained personnel is the main factor to the problem. The weak enforcement debilitates the deterrence and response strategies, which may crumble all the strategies implemented.

Third, there is no coordination among the government agencies to protect the country from information warfare attack. The absence of coordination has caused the nonexistence of national cyber defense structure – a structure that is much needed to delineate responsibility across military, civilian government, law enforcement, and private sector organizations.

Overall, Malaysia's civilian information warfare defense capability is weak and serious measures must be taken to alleviate the weaknesses. Besides the weaknesses that are stated above, there is another aspect that the government should react to. The government should develop the internet intelligence capability to sniff and determine the probable attack that might be carried out by any attackers. Internet intelligence is about intelligence activity on the cyberspace or internet to find any anomaly or sudden flow of internet traffic on the country's information infrastructure, which might resemble an information warfare attack. This type of intelligence requires both technical intelligence and human intelligence, and the intelligence agents must possess the expertise to analyze and determine whether there is an imminent attack on Malaysia. This type of intelligence is still new, nonetheless it is very important and the government should make an effort to establish this type of intelligence team in the country.

Information warfare is a real threat to Malaysia, and the government should prepare to triumph over the threat by strengthening its defense capability and implementing a number of measures to alleviate the weaknesses.