CHAPTER 4:
MALAYSIA'S STRATEGIES TO DEFEND ITS INFORMATION INFRASTRUCTURE

4.1 Introduction
This chapter will discuss the strategies taken by Malaysia to defend its information infrastructure. There are four strategies taken by Malaysia, namely: protection, deterrence, prevention and response. Each of these strategies will be explained in this chapter. Furthermore, this chapter will explain which government agencies are responsible to implement these strategies and how these strategies are implemented by various government agencies.

4.2 Protection
The first strategy implemented by Malaysia in defending its information infrastructure is protection. Protection is about hardening particular nodes in Malaysia’s information infrastructure and restoring the system by implementing attack assessment and restoration. Attack assessment serves as an essential device to determine the impact of an attack on critical functions and the appropriate response to an attack. Restoration of the infrastructure implies some capability to repair the damage and the availability of resources such as personnel, software and backup data. Protection is crucial in order to reduce and perhaps even eliminate vulnerabilities. Protection involves implementing both technical and non-technical measures.
Technical measures are tools used to secure information system. Such tools are numerous and new tools are created periodically to counter new sophisticated attack tools. The most common tools are cryptography, steganography, biometrics, firewalls, encryption, access control monitors, automated intrusion detection, audit logging and vulnerability assessment tools. Physical protection, which includes locks and keys are also important to protect any physical medium, including the physical environment, papers, disks, tapes, computer systems, and local telecommunication system. They can be placed on the doors to buildings and offices, external gates, safes, desks, filing cabinets, and any other physical enclosure. The lock serves both as a passive access control device and as a mechanism for concealing the contents of the locked object.

Non-technical measures refer to standard operating procedures adopted to implement technical security measures. Most intrusions into computer systems are not traceable to faulty technical means but rather to faulty implementations and procedures. It is the people, not hardware and software, who are often the most exploitable weak links in information systems. The unwitting compromise of passwords and other security breaches can be minimized through threat awareness indoctrination, training and education, monitoring, and, as appropriate, penalties for violating security procedures. People whose actions can compromise information system security can be made aware of this potential and urged to take steps to protect these systems with appropriate seriousness. They can be informed about how hostile agents might attempt to compromise information systems, so that they minimize their personal vulnerability and
detect and report potentially hostile activities. Training can be made to seem more relevant through tailoring to the specific responsibilities and access of the trainees.\textsuperscript{5} Traditional counterespionage and intelligence activity is the best way to alleviate threats posed by insiders. There must be a thorough and constant check of each employee's background, behavior, attitude and activity. Any suspicious activity by any employee must be investigated swiftly so that preemptive action can be taken. Procedures regarding obtaining and screening sensitive information are also important to ensure protection from malicious insiders.

In implementing the Multimedia Super Corridor's (MSC) flagship applications, two of the applications, which are the Electronic Government (EG) and Multipurpose Card (MPC) require much concern and attention by the government because any flaw within these applications will give direct impact and threat to national security. The implementation of the various EG projects are going to affect the community at large as a result of new forms of service delivery. Processes involving the daily lives of citizens such as the registration of births, school registration, the issuance and renewal of identity cards and driving licenses as well as the filing of tax returns will be transacted electronically. Government-business transactions such as business registration, company registration, tax payment, issuance of import/export licenses and procurement will undergo changes through the use of information technology and multimedia.

EG will also facilitate intra-agency connectivity, facilitate the creation of efficient and paperless administrative machinery resulting in more efficient and effective
communications and thus leading to higher productivity. The Multipurpose Card or MPC contains key government and private sector applications and will replace the different government and private sector cards that an individual normally uses. Eight MPC applications have been selected for initial implementation, which are national identity card, driving license, health card, immigration application, electronic cash (e-cash), automated teller machine (ATM), debit and credit card.

In brief, EG and MPC are interrelated, serve, communicate with and facilitate each other continuously in providing services to the public. Thus, any security breach to any one of these flagships would open a ‘window of opportunity’ for the attacker to roam freely and warrant him the muscle to cause severe damage to the individual, corporate sector and the entire nation and hence jeopardize national security.

This situation presents a dilemma to the government whether to put national security at the highest priority or to embrace economic prosperity. National security corresponds to systems security but economic prosperity relies on connectivity. The MSC has forbidden Malaysia from implementing an “air-gapped” or “stand alone” computer system, as such a closed system would prohibit the implementation of the MSC’s flagships and also limit utility and convenience. “Air-gapped” is where a computer system is in a secure location that receives no input whatsoever from the outside world and thus cannot be broken into. An air-gapped computer system has no connection with the global networks such as the Internet or the international phone system (for example, via modem). However, without the connection, the MSC’s flag applications cannot be implemented
because connectivity is the essence of the MSC, and the MSC is established to exploit to the fullest the potential of global connectivity especially in ensuring economic profit. Worldwide Manufacturing Web and Borderless Marketing are examples of ways in which the MSC can have access to fast and reliable global connectivity to achieve its objectives.

The second option for Malaysia is to choose for “one way gates” in which the system can access a network but cannot be accessed from that network. This system provides security, but is still limited in its flexibility and utility. Malaysia has no option except to embed closed or partially closed systems within a larger, open network architecture, which is also known as enclaving, balancing between national security and economic prosperity. Enclave protection, in abstract form, is setting up a perimeter and then protecting it from penetration typically with firewalls.

For that reason, a robust enclaving system is needed to provide a high availability and secure network to ensure the smooth flow of Government information and services. In 1999, the Government has therefore 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.

GITN is positioned in the Government domain and its role is to link Government systems and processes into a common network. The network links all aspects of Government as a
single entity, to businesses and citizens throughout Malaysia and the world. This requires a high level of security measure, since it should only allow the flow of authorized Government information and services between users, whereby the access points to Gateway providers, need to be heavily managed.\textsuperscript{11} The GITN plays a major role within the Electronic Government model. It provides an integrated communications and computing infrastructure which consists of a high speed nation-wide Frame Relay Network and a TCP/IP network to form the Secured Government Intranet. This will be the foundation for developing the \textbf{EG*Net} – the Wide Area Network dedicated for the inter-connectivity between Government agencies implementing the Electronic Government pilot applications. The \textbf{EG*Net} is a fully managed, integrated Virtual Private Network (VPN) built upon GITN’s Frame Relay Network and secure Government Intranet infrastructure.\textsuperscript{12}

A VPN creates a secure path of communication over an insecure connection. It could also be considered a mechanism to connect hosts or networks such that they can communicate in a secure fashion, as though they were behind the same firewall, while actually communicating over a public medium. A VPN is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization’s network. The VPN solution would ensure the \textbf{EG*Net} of a high level of network security, with high availability and reliability.\textsuperscript{13} VPN is a type of network architecture that allows communication between sites using a public network such as the Internet to go over an encrypted channel. Since
Picture 1
network communication over the Internet is vulnerable to "snooping" (electronic eavesdropping), setting up a VPN guarantees private communication between two sites.\textsuperscript{14}

Picture 1 shows the secured government intranet to protect against information warfare attack.\textsuperscript{15} The intranet system uses multilayer of firewalls and routers as protection to harden the information infrastructure nodes from easy access and penetration by the attacker. The attacker, which obviously will come from the Internet, has to pass through the router first before penetrating the first layer of firewall to get access to the GITN Frame Relay network (type of network that transfers data at a fast speed and big volume). A router is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The router itself serves as the demilitarized zone (DMZ) by putting access control lists on the access router. In computer networks, a DMZ is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data.\textsuperscript{16}

The DMZ is that part of the network that does not belong to either the Internet network or the Internet. This is generally the area between the access router and the bastion host, a particularly vulnerable system that has been fortified against attacks.\textsuperscript{17} On the Internet, a bastion host is the only host computer that a company allows to be addressed directly from the public network and that is designed to screen the rest of its network from security exposure. From the picture it can be seen that each agency's computers have their own DMZ and firewalls. So, before a hacker could penetrate into any of the
Picture 2
agency's computer, he has to fool two access control lists (the DMZ) and defeat two firewalls. Each agency's computer does not have direct link or connection with each other. For example, computers in Agency D do not connect directly with computers in Agency C, and vice versa.

This type of network architecture would prevent the potential hacker, if he succeeds in penetrating into one of the agency's computer, from easy and direct access to computers of another agency. Even though he can use the penetrated computer as a launching pad to attack other computers, he has to go back to the GITN Frame Relay network and penetrate another agency's DMZ and firewall before he could slip into the computer. These multilayers of technical protection not only could harden the nodes from unwanted users but at the same time provide utility and convenience to the legitimate users. Furthermore, this network provides a single secured gateway for all Government agencies to connect to the Internet. Regardless the insiders, hackers have only one path to penetrate into the network thus making it easier for the system administrator to monitor the traffic for suspicious activities.

Picture 2 shows the structure of Electronic Government application connecting all government agencies' computer that enables fast communication and transaction. The implementation of the application is made in stages, to give enough room to look for security flaws. This increases the reliability of the application. Since 2001, the EG-Net has interconnected more than 500 locations nation-wide involving Government agencies at federal, state and district level. The architecture of EG-Net provides various types of
technical protection, such as the DMZ, firewall and encryption. These protection mechanisms provide multilayer shields to the information infrastructure from being too vulnerable to the attackers.

EG*Net is developed by GITN Sdn Bhd (GSB).\textsuperscript{19} GSB provides EG*Net Support Services to monitor and administer the network of EG*Net. The task of operating and monitoring the networks is carried out centrally and proactively at the Network Control Centre (NCC) in Kuala Lumpur. There are two main components of the EG*Net Support Services, which are the Helpdesk Services and Technical Support Services.

The EG*Net Helpdesk Services monitor the management and operations of the EG*Net and act as the main point of contact for queries and fault reports made by the user. This is done through their services, which are the Call Management and the Fault/Problem Management. The Call Management provides a central point for all communication and interactions between the EG*Net users with the Helpdesk and collects, records, disseminates and tracks caller issues. The users can call the Helpdesk whenever problems arise. The Fault/Problem Management identifies the faults and problems detected by the Helpdesk or reported to the Helpdesk and records details of the problems through incident reports. The incident reports then will be handed to the Technical Support Services to fix the problems or the faults. Overall, the Helpdesk monitors the progress of customer service activities including installation, maintenance and network upgrades. Helpdesk is also responsible for providing comprehensive fault management services and managing both normal service and fault repair activities.
The Technical Support Services (TSS) are provided directly from the Network Control Centre (NCC) in Kuala Lumpur as well as from GSB's regional support centers located at strategic locations around the country; in Kuala Lumpur, Putrajaya, Pulau Pinang, Johor Bahru, Kuala Terengganu, Kuching and Kota Kinabalu to ensure that they provide their service to cover the whole of Malaysia. The Technical Support Services personnel comprising network engineers and field service engineers provide technical support services for on-line and on-site support and maintenance. In the event of information warfare attacks to EG*Net, these Support Services teams will perform damage assessment and restoration of critical functions on the system and interdict the attackers from continuing to cause damage to the system. These teams are the computer experts, defending the government information infrastructure, focusing their energy and skills just for the protection of the system without holding other responsibilities.

The Electronic Government application is built to have its own mechanisms of protection, to ensure the reliability of the infrastructure itself. These protection elements do not include other initiatives and efforts erected within the government itself. On the part of the government, through MAMPU (Malaysia Administrative and Management Planning Unit), on 1st January 2000, the government established ICT Security Division, a special division responsible for handling all aspects of information technology security operations in the public sector, which are policy planning, implementation and coordination and monitoring of the security aspect of IT implementation in the public sector. This includes their role as expert reference on IT security training and the management of a cryptology centre in the public sector. The division is divided into
three sections: the Policy, Standard & Audit Planning Section; the Business Resumption,
CERT & Cryptology Section and the Accreditation, Training & Acculturation Section.\textsuperscript{21}

Each section concentrates on different tasks and executes specialized activities within.
Among the activities handled by the Policy, Standard & Audit Planning Section are:\textsuperscript{22}
  
  - Specifying the vision and direction for IT security in the public sector.
  - Outlining and legislating policy, standard and IT security auditing plan.
  - Implementing IT security audit and compliance of IT system.
  - Advising departments in the public sector regarding IT security.

Activities that are handled by the Business Resumption, CERT & Cryptology Section,
and the Accreditation Section are:\textsuperscript{23}

  - Outlining and managing contingency plan and establishment plan of cryptology
    laboratory.
  - Receiving IT emergency reports from the public sector and providing continuous
    technical assistance and support.
  - R & D and testing of cryptology/algorithm set in the public sector.
  - Implementing IT emergency procedure from the aspect of operation during
    emergency, training program and restoration of operation in the event of
    intrusion.
  - Performing penetration test on government’s IT installation and preparing the test
    report.
Meanwhile, the Accreditation, Training & Acculturation Section serves the public sector IT security through:

- Outlining expert recognition plan/program and planning IT security content.
- Assistance in developing content of training and acculturation of IT security.
- Coordination and carrying out IT security best practices for public servants.

The ICT Security Division plays a significant role in protecting government’s information infrastructure from being intruded especially from falling victim to massive and coordinated attacks. The main function of this division is protection, both technical and non-technical. The government is aware that most of the intrusion cases are caused by human carelessness. Therefore, training and acculturation programs are designed and updated vis-à-vis new threats to make users become more responsible in using the system and be more serious about information system security as well as be more accustomed to the security measures.

The division constantly monitors the level of compliance of IT security standard by performing IT security audit. The security audit serves two purposes: first, as awareness to public servants to adhere closely to all standards and procedures regarding IT security where failing to comply would result in penalties or bad assessments by their immediate supervisor. Secondly, the audit provides the benchmark of readiness and preparedness of IT security of every agency in specific and the government in general.
Besides that, the ICT Security Division is a Government Computer Emergency Response Team (G-CERT) for the public sector.\textsuperscript{25} By having its own CERT, the government could expect faster response in incidence handling. In addition to that, the division regularly performs penetration tests on the government’s IT installation; the clandestine exercises to test the security of the government’s computer networks. The tests can reveal the vulnerabilities of the computer system and system administrator’s reaction, whether there is an intrusion, and whether it is detected and reported or nothing is done. The result of the test also discloses whether the system administrator is doing his job on installing new software patches to plug on the loopholes that is constantly found in the system.

Another important role of ICT Security Division is outlining and managing contingency plan in response to information warfare attacks. Contingency plan is an important element, especially in the event of information warfare attack, to keep critical functions operating, seclude sensitive database from the system, isolate contaminated databases, shut down intruded nodes, proceed with repairs and allow applications to continue operating with unaffected data. Enduring the operation especially ensuring critical information infrastructure that is vital to the normal functioning of human interaction and economy even when the information infrastructure is under severe attack, could defeat the attacker’s objective. By having a contingency plan, the government can still resume at least minimal application of its operations even during information warfare attacks.\textsuperscript{26}
In 1999, there were 36 cases involving intrusion and changing of information in government websites. After the establishment of ICT Security Division on 1st January 2000, the reported cases for the year 2000 were reduced to 21. The role of the division and its activities has successfully reduced the vulnerabilities of the government’s computer. From 1999 to 2001, 60 government websites were hacked. According to chief secretary to the government, Samsudin Osman, despite the high number, none of the government agencies affected had completely lost its data. However, no details were revealed on the damage or amount of data stolen or used for ulterior motives.27

Realizing that government agencies now face the additional responsibility of securing ICT-based government information and systems as well as ensuring that they are available to authorized users, the government has issued a manual security handbook on January 2002, to be adhered to by all of its agencies. The Malaysian Public Sector ICT Management Security Handbook (MyMIS) is intended as a reference and guide for public sector personnel in managing security in all public sector ICT installations. MyMIS serves to complement the ICT security measures taken earlier by the government by way of Pekeliling Am Bil. 3 Tahun 2000 entitled ‘Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan’ (Government Information and Communications Technology Security Policy Framework) and Surat Pekeliling Am Bil. 1 Tahun 2001 entitled ‘Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)’ (Information and Communication Technology (ICT) Security Incident Reporting Mechanism).28
The handbook provides the necessary guidelines on ICT security management safeguards to enable implementation of minimal security measures. It discusses elements of management safeguard, common operational and technical issues and legal implications. Basically the handbook covers all aspects of protection, explaining the roles and responsibilities, from management to vendors, contractors and external service providers and also about security awareness, training, acculturation and education and legislation aspects. According to Dr. Muhammad Rais, Director General of MAMPU, by implementing security guidelines stated in MyMIS, threats and intrusion on computer network systems can be reduced.$^{29}$

In protecting the system against the malicious insider, three measures are taken. The first is to prohibit 'sniffer' or 'network analyzer' software on the system; the second is to delete the software or change permissions so that it can only be used by system administrator if the software is bundled with systems; the third is to install a firewall between internal networks and systems. On top of that, every agency is encouraged to archive audit trails of user activities and to archive activities of users who have access to sensitive information.$^{30}$

### 4.3 Deterrence

The second strategy implemented by Malaysia in defending its information infrastructure is deterrence. Deterrence implies reducing the incentive of other actors to engage in information warfare attacks through credible threats of retaliation.$^{31}$ Fundamentally, it is an attempt to prevent an attack before it begins as a means to enhance security.$^{32}$ Even
though it is a Cold War product, deterrence concept is still relevant and useful in defending cyberspace from information warfare attack. However, because the nature of digital warfare is different from nuclear warfare, such as anonymity and proliferation of attack points where any site on the Internet can be a launching pad for an attack, a different kind of deterrence is needed than the one that has been developed previously. Deterrence of information warfare attack must be based primarily on three main pillars, which are detection, policy and counterstrike ability.

Detection is the ability to identify an attack and the attacker. In developing strong deterrence posture, the ability to detect an information warfare attack is the determining actor. The failure to effectively detect and report the attacks has consequence for deterrence. First, the lack of ability to detect an attack undermines a state's ability to defend and counterattack. Defense is more difficult because without information as to the type of attacks occurring and the point-of-breach of its systems, a state will have less than complete knowledge of its vulnerabilities. Without good knowledge of its vulnerabilities, erected defenses are unlikely to be effective. Counterattack is more difficult because without knowledge of an initial move, there can be no effective counterattack. Second, lack of reporting similarly affects deterrence. If an attack is undetected or goes unreported, it is unlikely that the attempt will result in a cost to the attacker and consequently, deterrence is negatively affected. Intrusion detection can be done by watching network traffic or by reviewing audit logs. If detection is early enough, the activity might be aborted before any damage occurs. Even if a particular act
is not stopped, knowing that it took place can alert security staff to vulnerabilities that might be fixed.

The second main pillar in developing deterrence in information warfare is policy. There is a clear declaratory policy which specifies what punishment an aggressor can expect if he carries out a particular unacceptable behavior or attack. A clear declaratory policy of types of punishment to the attacker can come in the form of law or security policy. The policy can be a guideline on types of retaliation that will be carried out to the perpetrator. It is important that the public be informed of the policy so that it could act as a warning to the potential perpetrator.

Counterstrike ability, the third main pillar, requires establishing the credibility to retaliate in the eyes of the prospective adversary and willingness to respond in ways that cause unacceptable damage to the attacker. For deterrence to be a viable strategy, therefore, the potential attacker must have strong reason to believe that he is likely to be caught and to be punished with a devastating response. Response can come in the form of information warfare and non-information warfare attacks. However, even though counterattacks with conventional weaponry would have powerful deterrent leverage, only in-kind counterstrikes will be morally acceptable. To do these, a nation should have a professional standing ‘army’ of computer experts. This ‘army’ would conduct destructive or limited offensive operation on the perpetrator as a promise to counterstrike.
The Malaysian government realizes that its ambitious projects such as the Multimedia Super Corridor and Electronic Government are vulnerable to information warfare attack. The attack may result in damage such as loss of confidentiality, information integrity, authenticity, availability and financial loss. Therefore, as part to reduce such threats, the government entrenched deterrence strategy by erecting clear declaratory policies, in the form of cyber laws. Cyber laws form an important component of the legal framework needed to facilitate the development of ICT systems by countering the threats and abuses.

In relation to ICT security, cyber laws were enacted to:38

- Regulate and protect the ICT industry from misuse and illegal activities or activities that assist in the commissioning of illegal activities. Above all, cyber laws seek to promote the development of local ICT-based industries;
- Describe in clear terms activities construed under the law as offences;
- Describe in detail penalties for transgression; and
- Provide soft infrastructure to lend support to the MSC initiative.

Malaysian Cyber Laws consist of six acts, which are Digital Signature Act 1997, Computer Crime Act 1997, Telemedicine Act 1997 (yet to be enforced), Copyright (Amendment) Act 1997, Communications & Multimedia Act 1998 and Malaysian Communications & Multimedia Commission Act 1998. Among these Acts, the Computer Crime Act is essentially a deterrence strategy. 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 computer is an
offence and will be penalized. Even though this Act is modeled after the UK Computer Misuse Act 1990 and the Singapore Computer Misuse Act 1993, the penalties imposed are heavier.

For example, for offence of unauthorized access to computer material, the penalty for UK is maximum of 2,000 pounds fine or six months' jail or both, in Singapore it is S$2,000 or two years' jail or both, but in Malaysia, with the same offence, the offender will get RM50,000 or five years' jail or both. In section 4 Computer Crime Act stated that, a person with an offence of unauthorized access with intent to commit or facilitate commission of further offence, will get ten years of jail or RM150,000 of fine or both. These punishments entitle the Computer Crime Act to have the most severe penalties for computer crimes in the world. This Act also has an effect outside Malaysia if the offences are committed by any person in any place outside Malaysia if the computer, program or data is in Malaysia or capable of being connected to or used with a computer in Malaysia.

To make the cyber laws relevant, the government constantly reviews it, such as the move to tighten laws to deal with misuse and abuse of the Internet. Energy, Communications and Multimedia Minister Leo Moggie said the government is looking at tackling the problem "with an open mind and not to curb freedom in the cyber world". Moggie said the ministry is constantly reviewing cyber laws to plug loopholes and his officers are working closely with the Attorney-General's Chambers in strengthening the laws to ensure that they are relevant in the fast-paced cyber world. "Some of the existing legislations were drafted between three and four years ago, and we have to consistently
revise them so that they are relevant in accordance with current need," he added. To counter the threat from insiders, the government uses the Official Secrets Act (OSA) as a clear declaratory policy that specifies what punishment an insider can expect if he carries out a particular unacceptable behavior.

On January 13, 1997, the government set up Malaysian Computer Emergency Response Team (MyCERT) to react against possible information warfare attacks on individual, corporation or on the government itself. MyCERT was established under the Ministry of Energy, Communications and Multimedia and operates and receives instructions from Mimos Berhad at Bukit Jalil, Technology Park Malaysia. MyCERT has become a center of reference for the Internet community in Malaysia to deal with computer security incidents and methods of prevention. MyCERT works closely with the CERT Coordinating Center in Carnegie Mellon University, United States and other CERTs around the world in order to cope with rising threats and provides security information to the public. With the vision to reduce the probability of successful attack and lower the risk of consequential damage, MyCERT works closely with the Royal Malaysian Police, assisting the police to investigate security incidents and attacks.

MyCERT plays critical roles in defending Malaysia from information warfare attack through building up the deterrence strategy. These roles can be seen by its functions, which are providing reference on network and security matters, centralizing reporting of security incidents and facilitating communication to resolve security incidents, disseminating security information including system vulnerabilities, defense strategies
and mechanism, acting as a repository of security related information, and playing an educational role in educating the public with regard to computer security in Malaysia.

By becoming a center of incident reporting for public, MyCERT is able to determine the attack mode, type of tools used, frequency of attacks, how the attacker exploits the security loopholes, which loopholes the attacker used, and modus operandi of the attack. By knowing the characteristic of the attacks and vulnerabilities of the systems, MyCERT could effectively disseminate to the public security tools and techniques and provide defense strategies and mechanism to detect intrusions. Consequently, the ability to detect an information warfare attack is improved and this provides a warning to the attacker that their malicious activity is not encouraged and that they will be hunted out and punished. Efficient detection ability strengthens deterrence strategy.

4.4 Prevention

The third strategy implemented by Malaysia in defending its information infrastructure is prevention. In this context, prevention means hindering the ability of such enemies to acquire, deploy, or successfully use information warfare weapons and techniques. However, limiting the spread of capability will be very difficult. Computer and communication technologies have already spread throughout the world. Essential knowledge about computer operating systems and programming is also widely available. Nonetheless, developing a capability to preempt or thwart an attack could prevent or limit the deployment and use of information warfare tools. This requires having the ability to identify potential attackers, a concept of warning in the information warfare context to
determine when an information warfare attack is imminent, and an offensive information warfare capability both to collect information about potential attackers and to respond in a pre-emptive manner to warnings of imminent information warfare attack.\textsuperscript{45}

The Internet is a potentially lucrative source of intelligence that can be used to collect information about the potential attacker. This intelligence can include reports on current events, analytical assessments by politically astute observers on or near the scene of those events which many of whom offer unique insights, and information about the plans and operations of politically active groups.\textsuperscript{46} Sturdy prevention strategy requires a team of computer experts to fully utilize the vast and open source on the Internet, to perform intelligence gathering, constant and active monitoring activity on the cyberspace, and the computer experts’ team will want to break into a network for one of several reasons:

1. To listen to conversations between the computers on the network.

2. To gain illicit entry into the computers and look around for valuable data.

3. To gain illicit entry into the network for the purpose of shutting it down.

4. To learn passwords and access code that will give the computer experts’ team unlimited access to the networks any time he chooses.

5. To listen to “private” e-mail between users on the network.\textsuperscript{47}

The Internet can be used to provide early warning of impending security threats. Internet message traffic about developing situations tends to precede news and intelligence reporting, since the individuals who originate that traffic are not constrained by the resource limitations to which news and intelligence organizations are subject. It is likely
that routine monitoring of messages originating in other countries would help provide strategic warning of developing security threats. The computer experts' team can intervene to execute a preemptive strike so that the enemy's ability to carry out a planned attack is crippled. Moreover, information warfare attack warning can be signaled to put on high alert and prepare for the upcoming attack. Organizations can respond to a rising threat of intrusion by increasing the difficulty of access or restricting the number of individuals who may be able to access certain capabilities and files.

With its ambitious projects such as the Multimedia Super Corridor and Electronic Government making progress and moving ahead, the Malaysian government is concerned about the need to enhance the security of its information infrastructure. These concerns have turned into a pressing issue at the national level as Malaysia is facing shortages in ICT security expert and there is the need to mobilize and optimize the engagement of such personnel for ICT security. It is important that the country be self-reliant in core ICT security areas and not depend solely on foreign-based technology. Adding to that, there is tremendous growth in the number and varieties of ICT applications and devices produced by suppliers. However, many are lacking in fundamental security functionality, and this has created an exponential explosion in the need for a trusted reference and specialist centre in ICT security. This is to support not only the reactive measures, but also the proactive measures in ICT security.

Realizing this vital need, the 6th National Information Technology Council (NITC) Meeting on 15th January 1998 agreed upon the need for establishing the National Network Security and Accreditation Agency which in turn gave birth to the National ICT
security and Emergency Response Centre (NISER). NISER, which serves as a central body to address ICT security issues at the national level. It has also been given the task of expediting and synergizing standards and guidelines on ICT security-related issues from various bodies to reduce duplication of efforts.\textsuperscript{50} MyCERT, which was the first step towards the establishment of NISER, is incorporated into NISER.\textsuperscript{51}

In the medium term, NISER functions as a security body to assure the public that there is a national body that can handle all security threats and attacks on individuals, organizations and the nation. Towards the end, the centre will also create awareness in security issues as well as provide training and consultancy services. In the long run, NISER will be used to co-ordinate, plan and prioritize research and development (R&D) activities, to act as a registration system for ICT security products and professionals providing consultancy services and to encourage global participation at international forums and workshops in an effort to create a network of relationships to draw resource from in times of emergencies.\textsuperscript{52}

NISER is the agency that provides early warning on the events that could give severe impact to Malaysia. For example, NISER provided warning on the outbreak of Nimda and Code Red viruses before these viruses reach Malaysia. NISER alerted the public and various agencies in a serious and collaborative manner on the severity of attack and the need to react fast.\textsuperscript{53} On warnings about coordinated attack, however, before any warning can be signaled, sniffing and locating potential attacks is a crucial strategy. NISER sniffs the incoming danger by collaborating with local and foreign agencies and assessing
the network by picking up the peculiarity. As mentioned earlier, Internet is interconnected and any suspicious activity on any of the country’s information infrastructure would cause peculiarity. This peculiarity will cause suspicions that would demand the respective country’s CERT to investigate. The peculiarity can be in the form of a sudden change in the amount of network (i.e. Internet) traffic from a country.

For example, an increase in Internet Control and Message Protocol packets coming from a country could indicate that the country’s information infrastructure is being used by a potential attacker to gather data about other hosts on the Internet as potential targets. A sudden increase in the number of viruses being spread through the Internet to a specific country’s hosts could be another indicator of possible information warfare attack. An opponent could conceivably use viruses to prepare the battlefield by rendering key civilian systems inoperable at critical times. If these examples of peculiarity happen within information infrastructure that belongs to Malaysia, NISER would signal the early warning to the public. However, if it happens outside Malaysia, NISER will seek assistance from its foreign counterpart for further investigation. With a network of cooperation between NISER and worldwide CERTs that would update each other on threats, attacks and vulnerabilities, possible attack can be traced and sufficient preparation can be made to annihilate the attack.
4.5 Response

The fourth strategy implemented by Malaysia in defending its information infrastructure is response. Appropriate and effective responses to attacks include identification, interdiction, apprehension, and punishment. The identification process must be executed once the intrusion detector triggers the alarm and the process of identifying the perpetrator should be finished before the perpetrator ceases the attack. It is important to identify the attacker's origin of attack, methods of attack and the target of attack as it could provide crucial information to interdict the attack and to punish the attacker. By knowing the target and the methods of attack used by the attacker, the defender can devise and launch specific counterattack or defensive mechanism the minute that their information infrastructure comes under attack. The defender must stop the attack before it causes greater damage. One of the techniques to stop the attacker is to force him out of the system.

After the attacker is identified, rapid apprehension of the attacker by the law enforcement officers must be carried out. This is to prevent the attacker from destroying the evidence or fleeing off from the location where the attacker started the attack. Skilled hackers can eliminate their trace and forensic evidence effectively that leaves law enforcement officer with no evidence to prosecute or detain them. Apprehending the attacker red handed is possible if the attacker is a local person. Nonetheless, the probability of apprehending a foreign attacker red handed is nearly zero because of many factors, such as the need for good cooperation with foreign law enforcement agencies, the difficulty to coordinate apprehension action and time. Time can be considered as the biggest hurdle because the
attacker can cease their attack at any moment and thus erase their 'existence' while the defender needs enough time (where it can take long) to precisely locate the attacker and.o contact and coordinate apprehension action with their foreign counterpart. If the perpetrator launches the attack and stays within the sovereign territory of a state, provision in the local civilian law can be used to punish him. Otherwise, if the attacker is staying abroad, using international law or diplomatic initiatives to expedite extradition agreement is the best way to make sure the attacker will be punished. All information regarding the origin of attack, methods of attack and the target of attack can be used against the attacker in the court when he is prosecuted.

However, before any punishment can be carried out, investigation, compiling of evidence and prosecution are the tasks that have to be solved first. These tasks require both the criminal investigator and prosecutor to be able to understand the nature and character of information warfare. Criminal investigators must possess knowledge of information warfare tactics, computer crime and must know how to collect evidence through forensic accounting skills. According to Erbschloe, investigators need the following skills and knowledge.\textsuperscript{56}

- Excellent Internet skills, including technology that supports Internet communication. They need to be highly skilled Internet users, and they need to know where to look for signs of criminal activity on the Internet.
- The ability to create false identities in cyberspace just as they would if they were involved in an undercover operation in the physical world.
- The ability to record or capture data from Internet sites such as chat rooms, or other electronic communities that can serve as evidence or help to compile information to facilitate the investigation of illegal activity.

- The ability to track Internet usage and activities of specific individuals or groups to facilitate the investigative process.

Public prosecutors must also possess some level of understanding about information warfare attack so that successful prosecution will stop the perpetrators from continuing their activity at least for the time being. Erbschloe suggested that public prosecutors have to comprehend these two areas:57

- The compilation and presentation of credible evidence, much of which is likely to be in in electronic form or collected through electronic means.

- Prosecutors must develop an understanding of technology and information warfare and computer crime processes at a sufficient level to make credible arguments in court during the course of prosecution.

In Malaysia, there are three government agencies that are responsible for carrying out the response strategy, which are the Royal Malaysia Police, MyCERT and the Public Prosecutor’s Office. The Royal Malaysian Police is given mandate to enforce Computer Crime Act 1997. Two units, the Technology Crime Investigation Unit (TCIU) and Computer Crime Forensic Lab (CFL) which are under Commercial Crime Investigation Division were set up specifically to conduct investigation and forensic investigation to pursue the criminal when a case is reported. The establishment of these units reflects the
seriousness of the government to make cyberspace a safe haven as a business environment and to give a layer of reliable security to Malaysia's grandest project, the Multimedia Super Corridor.

Within TCIU, there are four units, each concentrating its resources and personnel on different tasks, which are the Personal Computer Unit that handles computer intrusion cases, Internet Unit that focuses on cases like spamming e-mail, Software R&D Unit which focuses on research and development on tools and latest software, and Investigation Unit, which conducts interrogation and apprehension of offenders. The main function of CFL is to do computer analysis to examine and to find out whatever information that is related to the crime particularly evidence contained in hard disks. The lab also gives consultation service to the investigation officer and navigates them on what they should and should not do during investigation and also educates them on evidence gathering techniques.

The role of the police in combating information warfare attacks is reactive rather than proactive. As provided by Computer Crime Act, their power to act only exists when an attack is reported. However, the police only investigates isolated and secluded types of information warfare attacks and not the coordinated and sustained attacks. The police does not get involved in intrusion detection as it is the responsibility of the systems' owners. Their main role revolves around response strategy, where they have to detect, apprehend and charge the offender in court.
According to Assistant Superintendent Victor Sanjos, there were cases where the TCIU managed to apprehend the attacker while he was still online intruding into the victim's computer. Apprehending the perpetrator while he is still online is important because this action would display rapid precision detection and identification capability of the TCIU and would strengthen the deterrence strategy in the eyes of the attackers. In another incident, to show to the public and potential attacker that the police are skillful enough to detect and identify the attackers who are still at large, the police made a press statement king an offender who hacked the Road Transport Department’s website to surrender as had been identified.\(^{60}\)

yCERT and the police work hand in hand to investigate, detect and apprehend the attacker. In detecting the attacker, traditional investigation works to locate and identify the attackers at the physical site once MyCERT and the TCIU are able to locate them through the Internet Protocol (IP) address. In pursuing local attackers, an Intelligence Unit within Commercial Crime Investigation Division is responsible to gather intelligence information on the perpetrators. The role of the police role in gathering intelligence is believed to be limited to traditional intelligence gathering. The Intelligence Unit is involved in traditional intelligence operation in pinpointing the physical location of local attackers (after their cyber locations are identified by MyCERT and TCIU through IP addresses) so that they can be apprehended. If the attack originates outside Malaysia, the police seek assistance from Interpol in detaining and extraditing the perpetrator. The TCIU also has good rapport with foreign law enforcement agencies.
from Singapore, Hong Kong, United Kingdom, Japan, U.S. and TCIU also provides assistance to these foreign law enforcement agencies.

The government realizes that, in order to invigorate the response capability, training for the judiciary, prosecution and police in cyber laws is crucial so that they will be better equipped to deal with computer-related crimes. The Minister in the Prime Minister's Department Dr. Rais Yatim said discussions had been held with the Chief Justice to incorporate this into the IT training for judges which had taken off in the year 2002. The relevant authorities and the private sector had been asked to contribute to the training, adding that the course content for judges was information-based whereas that for the police and deputy public prosecutors included the technological details of information technology. One of the government agencies that hold courses for the judges and public prosecutors is Institut Latihan Kehakiman dan Perundangan (ILKAP). For a start, four seminars related to computer-related crimes for session judges and public prosecutors were held in 2002.

4.6 Conclusion

The Malaysian government is trying very hard to defend its information infrastructure from falling victim to information warfare attack. At least four government agencies are given the task to carry out the defensive strategies. The strategies implemented not only focus on the physical aspects such as protecting the computers and network system by installing firewalls, but also on steps to educate the users about the danger and possible attack of information warfare. The Malaysian government realizes that awareness and
knowledge among the computer users to protect their own computer system and to report incidence related to information warfare attack are as important as defending the information infrastructure physically. Therefore, numerous education and awareness programs are carried out by MyCert and ICT Security Division. The seriousness of the government to defend its information infrastructure can be seen by the establishment of NISER, and the Technology Crime Investigation Unit (TCIU) and Computer Crime Forensic Lab (CFL) of the Royal Malaysian Police. These agencies are deliberately established to implement defensive strategies to defend the information infrastructure. Moreover, the decision to hold training for the judges and public prosecutors is a sign that the government is serious to prosecute and punish the perpetrators in court.
ENDNOTES


9 Ibid

10 Ibid


12 Ibid

13 Ibid


16 For further explanation, please refer to appendix of computer glossary.


19. GITN Sdn Bhd is a joint-venture company between Permodalan Nasional Berhad and Telekom Malaysia Berhad. Telekom Malaysia Berhad is a telecommunications service provider that can provide information warfare support in terms of providing how their systems are built and can relate important design and construction details to the government. See Erbschloe, M. (2001), Information Warfare: How to Survive Cyber Attacks. California: Osborne/McGraw-Hill, pp. 212.


22. Ibid

23. Ibid

24. Ibid


27. Staff, 60 govt Web sites hacked, Malaysia CNET.com, 6 April 2001.


37 Computer experts’ team consists of a force of professional and highly skilled computer network operators, not just a few technically savvy malcontents. These technicians will know the holes that exist in popular software packages and the slips-up network operators commonly make in maintaining firewalls and other security measures. They will also know from their own experience the shortcuts taken by sloppy or lazy operators. See Berkowitz, B. (2000), Information Warfare: Time to Prepare, Issues in Science and Technology.


43 Introduction page in Mycert homepage. The url is www.mycert.org.my [accessed on 27 August 2002]


50 Information about NISER. The information is available at www.niser.org.my/aboutus [accessed on 13 September 2002]

52 Ibid
53 Ibid
54 Ibid


57 Ibid p. 275.

58 Interview with ASP Victor Sanjos, Technology Crime Investigation Unit, Royal Malaysian Police on 23 September 2002.

59 Interview with DSP Abdul Aziz, an analyst in Computer Crime Section, Royal Malaysia Police on 1st October 2002.


62 List of training for the year 2002 conducted by Institut Latihan Kehakiman dan Perundangan (ILKAP) or Judicial and Legal Training Institute. The URL is www.ilkap.gov.my [accessed on 23 August 2002]