CHAPTER 5:

AN ANALYSIS OF THE MALAYSIAN DEFENSIVE CAPABILITY

5.1 Introduction

This chapter will analyze the Malaysian defensive capability vis-à-vis the forms of information warfare attack. The analysis will look into the strengths and weaknesses of the Malaysian defensive capability. In analyzing the strength of Malaysia's defensive capability, focus will be given to the roles and competencies of NISER in providing sturdy defense to Malaysia's information infrastructure. This is because NISER is the agency that has been established to defend Malaysia's information infrastructure. Meanwhile, analysis of the weaknesses of Malaysia's defensive capability will look into the problem that is faced by Malaysia right now and focus also will be on NISER's roles.

5.2 The Strength of Malaysia's Defensive Capability

In defending Malaysia from information warfare attack, NISER conducts four strategies, which are **protection, deterrence, prevention** and **response**. In protection strategy, NISER's role is indirect rather than direct approach. NISER protects the country through its security enquiry service, by which it conducts lectures and awareness programs to enhance public knowledge on ICT threats and countermeasures, disseminates ICT security information through its announcement lists to inform the public on the latest issues in ICT security and remedial solutions that need to be executed, and provides a range of updates as soon as security threats are uncovered.[1] NISER has gathered and compiled thousands of attack incidents which provides a library of reference for NISER to study and do research about the distinguishing traits of the attacks. By knowing types of tools or weapons used by the attackers, NISER could advise various parties 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 constantly 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, and obtaining and accessing open source information.[2] There are a lot of documents and issues posted by various parties. In addition, there are more than 700 sites[3] and bulletin boards which host thousands of attack tools, evidence eliminator tools, network scanner tools and other tools, and these are freely accessible and downloadable by anybody. These boards are also used to distribute very sophisticated user-friendly "point-and-click" hacker tools that enable even amateurs to attack computers with a high degree of success. By knowing the latest tools that might be used on the newly known vulnerabilities, NISER could create measures and countermeasures and provide the information to the public. This proactive role would alleviate the severity or impact of attacks and would prevent chaos to the Malaysian IT community.

In addition, NISER studies the national and international activities on cyber security issues or information security issues and specific policies imposed by the international community. These issues are analyzed from the aspect of their impact and implication to Malaysia from the security point of view. NISER then advises the government on how to overcome it and suggests the initiatives that should be taken in order to protect this country from being labeled as incompetent or not being able to manage its information infrastructure and assets.[4]

In detecting information warfare attack, NISER has developed a credible capability through MyCERT, which has gained years of experience. For example, MyCERT managed to detect an intrusion and web defacement on Malaysia's Parliament homepage before it was realized by the system administrator. NISER then informed MAMPU about the incident and then a police report was made by MAMPU.[5] NISER is handy in helping the police to conduct investigation on hacking incidents, especially in identifying the origin of the attacker. NISER identified that the attacker of Parliament's website originated from Brazil. In identifying the specific origin of an attack, NISER uses its rapport with other CERTs around the world.

Like the labyrinth of a spider web, the Internet is interconnected with many countries around the world. Any activity on any information infrastructure will leave its own unique 'footprint'. Even though the attacker might use scores of intermediary machines from various countries, the location of the attacker can be identified through reverse engineering process, with the help from the respective countries' CERTs. Even if the attacker stays and launches his attack from an underdeveloped country, he still needs to use the developed countries' information infrastructure to exploit its high speed and vast connection, and most of the developed countries have their own CERTs. So, CERTs from these countries help each other in tracking down the perpetrator.

As an agency that is given responsibility to address ICT security issues at the national level, NISER actively conducts research and survey on the current security preparedness of the Malaysian public and private sector from time to time. In the latest survey done, titled *NISER ICT Security Survey For Malaysia 2000/2001*, NISER found that Malaysian organizations experienced a high incidence of ICT security breaches, recording a level of sixty eight percent (68%). Among the various breaches, virus attacks are the most prominent; about half (47%) of the organizations experienced a virus attack, posing the greatest threat in terms of financial loss and frequency of occurrence.[6] The main purpose for NISER to conduct the survey was to gauge the security awareness level among organizations as well as to assist in determining the scope of ICT security breaches in Malaysia.

In conclusion, from the survey NISER found that the current state of Malaysian organizations' networks is highly vulnerable. Based on the findings from the survey, NISER, in the context of advisory capacity, gives professional advice to the public on the necessity to reinforce their protection mechanism such as the usage of firewall and multiple security system.[7] The government also tries to embrace 'defense in depth' strategy, which is a strategy to enhance information security collectively and in 'layers', like the layers of an onion. The strategy, requires the effort of all individuals, government and non-governmental organizations, law enforcement agencies and security experts to harden the information infrastructure thus making the national information security built in layers and difficult to be penetrated. Even though this strategy is still not applied comprehensively, it has shown some positive results. According to Major Husin, director of NISER, despite the fact that from August 1997 to October 2002, 3,251 incidents were reported, information warfare threats in Malaysia are considered as 'under control' yet still regarded as dangerous and should be resisted.[8]

Even though the government is against Internet censorship and control, and has vowed not to conduct monitoring on cyberspace activity, in situations that could compromise national security, there is an exception and the government would intervene. NISER, however, does not monitor the internet traffic. Monitoring the cyberspace is done by this newly formed Cyber Warfare Division, a division of the Malaysian Army. This division is part of Malaysia's effort in strengthening the national defense to face cyber warfare. The division engages in offensive and defensive information warfare.[9] So far, nothing much is known about this newly established division.

While some of NISER's roles are proactive, it still remains as a defensive organization. NISER does not engage in offensive information warfare although it has the capability to do so. In terms of capability to engage in information warfare, Major Husin Jazri, Director of NISER stated that his agency has limited firepower. Limited in this context, according to him, means that NISER is capable of absorbing first strike, and capable of launching counterattack and punishing the perpetrator severely. Unlike conventional warfare, in information warfare, capability is measured by knowledge and not solely by equipment.

Information warfare is unique because each attack is distinctive and not known for a while. It always gives a window of opportunity and advantage to the attacker. The defender requires time to do analysis and formulate the measures and countermeasures. If a country is under information warfare attack, where the attack tools are commonly known, the attack can be annihilated easily. But if the attack tools are indigenous tools and ingeniously created, and the attack is unconventional, it requires the defender's team to study the attack comprehensively before any countermeasures can be created. Designing and devising the countermeasures require knowledge and competence in technology. Any party who is able and competent in handling technology issues and able and competent to translate those technology requirements into strategic need and strategic value will prevail. Major Husin is confident that NISER is able and competent in technology.

For now, NISER is acting in an advisory capacity to the government. However, if the government changes its policy from defensive to offensive posture, it is not NISER who will become offensive but other agencies. NISER will provide the respective agencies with expert advice and technical know how, until they are able to do it themselves. The ultimate aim is to create self reliance at the end of the day. NISER will continue performing its fundamental responsibility, i.e. to train and increase the number of local ICT security consultants and experts.

A few years ago, information warfare was regarded as 'low level threat' by the National Security Division (NSD). However, recently, it is considered as 'medium level threat' and the NSC has included information warfare within national threat list and priorities. This is because information warfare attacks are increasingly agitating sovereignty, breaking the law, threatening public safety and causing chaos to the economy as the country increasingly relies on ICT. These worries have led to the creation of the National Information Security Committee (NISC), which was formed in mid 2002. NISC is chaired by the Chief Secretary of Malaysia but members of the committee are yet to be determined. The main function of this committee is to coordinate defensive strategies between government agencies and mobilize resources in the event of information warfare attack.[10]

Realizing the threat of attack is possible, the government is 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 economy and national security from information warfare attack.[11] The NIIPA, which resembles the United States' Minimum Essential Information Infrastructure[12] (MEII), is a security blue print that could manage effectively cooperation between agencies involved in order to plan, manage, protect, coordinate and perform national cyber defense.

NIIPA is a proactive step for Malaysia in confronting any possibilities in digital era, especially enemies who want to destroy national information infrastructure. Among the areas that are identified for the ICT security aspects are telecommunication and network system, system security, cryptography, database, applications, management, assessment and standard criteria, cyberlaw, continuous business plan and operation. The NIIPA would simplify the problem of systemic defense by nailing down specifically whichever elements of the vast information infrastructure that merit defending. Protecting this smaller target would be easier than attempting to defend all systems nationwide. The NIIPA implies that the essential elements of the information infrastructure can be identified, hardened against attack or isolated from possible contamination by the rest.[13]

In defending against coordinated and widespread attacks on national information infrastructure, the government has outlined a plan which has three 'layers'. NISER and MAMPU shall be the first 'layer' of defense to interdict the attacks. If the attacks are interdicted, the situation will not be brought to the attention of NISC. If both agencies fail, the NISC will take over the situation, call for emergency meeting, devise a defensive strategy and interdict the attacks. But if the attacks fail to be interdicted and the situation is out of control even at NISC level, the situation will be brought to the attention of National Disaster and Relief Committee, the highest committee within Malaysia.[14] Currently the committee is chaired by the Deputy Prime Minister. This committee has the power and supremacy to mobilize all resources the country has in whatever means to defend the country. If the attacks still fail to be interdicted, this committee shall propose to the Prime Minister, Director of National Operation, to declare the situation as 'national disaster' or 'national emergency'.

According to Major Husin, if the attack has breached a certain level of security perimeter, they have the contingency plan and mechanism to react appropriately in the event of crisis. NISER has the detection mechanism to alert them whenever there is a coordinated and widespread attack to the country. So far, NISER has not recorded any attempt on coordinated attack. But if the attack really happens, Major Husin is confident that NISER, with the help and collaboration of various agencies, can sustain such attack and defend the country.

5.3 The Weaknesses of Malaysia's Defensive Capability

Despite the strengths mentioned above, Malaysia's defensive capability is shackled with three major problems which are:

1) Malaysia depends too much on foreign Information and Communication Technology (ICT) security solutions without having a clear planning on how to develop local security applications.[15] Computer systems are similar to human immune systems. Some immune systems are resistance to some types of diseases while others are not. This is the way nature protects the human race from extinction, i.e. through diversification of immune systems. The same thing happens to computer systems. Some computer systems are immune from certain types of computer viruses because the viruses are not created to affect those systems. The problem of global computer virus plague is rooted from the usage of certain types of popular systems, such as Microsoft's Windows system and the usage of certain types of antivirus and firewall software to protect the system from malicious acts. If a virus is deliberately created to exploit and destroy Windows system and designed to fool those security systems that protect Windows, the virus will be likely to be successful in creating chaos at the global level, contaminating Windows' based computers, before the remedy is found. That is how the Code Red, Love Bug and Melissa viruses easily spread and corrupted millions of computers over the globe. Today, there are four main types of computer systems used which are Microsoft Windows, Macintosh, Linux and Unix. Each of these systems has different firewalls or security systems for protection. The problem in Malaysia is, if the country depends too much on the foreign ICT security solutions, Malaysia is risking and exposing itself to information warfare attack.

This is because security flaws on the foreign ICT security solutions are widely known and regularly found either by the developers theselves or by the hackers. Flaws are usually discovered in a product after its release because the developers have rushed their products into the market without having them undergo a series of thorough security test. Hacker publications and web sites offer "how to" instructions and software tools for exploiting vulnerabilities as soon as they are discovered. Besides that, companies that produce ICT security solutions regularly reveal the product weaknesses that they found from time to time on their homepage so that users who bought their products could repair them on their own based on their instructions. The posted information can be accessed and exploited by anybody. Currently Malaysia solely depends on foreign ICT security products to protect its systems. Malaysia does not have its own immune system that could hinder viruses, for example, from contaminating its computer systems. There is no diversification of ICT security systems in Malaysia. It is a must for Malaysia to create its own indigenous ICT security solutions because it could harden the national information infrastructure (NII) from easy access and penetration compared to the effect of using foreign security solutions.

Malaysian organizations experience a high incidence of ICT security breaches, recording a level of sixty eight percent (68%), where virus attack contributes 47% of the breaches. The high percentage of breaches occurs even though ninety two percent (92%) of organizations have had ICT security systems in place since the year 2000. The most common ICT security systems used by the Malaysian organizations are identity authentication, anti-virus solutions and firewalls.[16] The main point here is to create a robust system because it is impossible to design a totally immune system. Any computer system can be fooled and manipulated; all it needs is creativity. Developing local security applications is one of the best ways to make NII robust from malicious acts. With the emergence of more sophisticated viruses and tools of attack, NISER feels that a stronger security system such as the usage of firewalls and multiple security systems is deemed necessary for greater protection.[17]

2) **The second issue that is hampering Malaysia is the enforcement of law.**[18] The enforcement aspect in legislation related to ICT is still weak and there are aspects that have to be updated and improved. Vice President of MIMOS, Dr. Mohamed Awang Lah said Malaysia has cyber laws, but the enforcement and implementation problems must be addressed and need serious attention.[19] The implementation of cyber laws needs to be tidied up in order to effectively tackle problems related to network and computers. Among the enforcement problems are inadequacy of manpower, lack of coordination between government agencies and destitution of expertise. The police's Technology Crime Investigation Unit (TCIU) and Computer Crime Forensic Lab (CFL) seem

handicapped vis-à-vis the increasing number of attacks and is unable to provide strong response posture to the potential attacker.

The major difficulty is the small number of professional staff trained to investigate information warfare attack cases.[20] This means that the burden to investigate cases and the pressure to settle unresolved cases is heavy. Piling up of unresolved cases is not a good indication because eventually, the public will lose its confidence in the police for reacting fast to ensure cyberspace security. Ideally, effective and efficient investigation requires an investigator to handle a small number of cases so that he could focus more and provide in-depth investigation thus solving the cases at a faster rate. Failing to accelerate the investigation will set loose the attacker and the probability to lose forensic evidence is high. There are a lot of tools to eliminate a 'footprint' or log activity, and experienced hackers could easily destroy the evidence and evade being caught. The TCIU's chief inspector Mahfuz Abdul Majid admitted that the workload is heavy and Bukit Aman may be unable to cover the whole country efficiently. In countering that problem, the Royal Malaysian Police had put forth a proposal to increase its six-man team in 2002 to a staff strength of 21 in early 2003.[21]

Effective implementation and enforcement of cyber laws require the law enforcement officers to possess expertise and excellent knowledge but currently this is not the case. State police have the authority to investigate reported attacks but they possess little expertise and knowledge. In other words, they are incapable of conducting effective investigation on more hi-tech cases and these cases are often handled by the Technology

Crime Investigation Unit (TCIU) in Bukit Aman because the team is more equipped. Often the TCIU conducts seminars to the state contingents to provide expertise and know how to investigate information warfare attacks.[22] Not surprising that until now, only one IW attack case is being is being investigated even though the number of reported attacks has skyrocketed. The case, which is on trial, will be the first case for the police to face challenge and objection from the defendant's lawyer in proving their capability in investigating, collecting and compiling evidence on information warfare attack.

This situation happens because the police fail to gather evidence and in most cases, their investigation leads to 'grey areas' where they have no indicator and clue to continue the investigation, as a result of which, in the end, they had to close the investigation. District Attorney Office is facing the problem to prosecute because the police fails to present adequate and credible evidence.[23] This also shows that both the Technology Crime Branch and Computer Forensic Lab officers do not achieve and possess the necessary level of skills needed to conduct investigation. The irony is that the government realizes the inability of its law enforcement agency to conduct investigation on information warfare attacks. MAMPU reminded the public in the MyMIS Handbook that the local law enforcement agency may not be well-equipped to handle high-tech crime as the agency is focussed more on problems related to violent crime and drugs and has limited budgets.

Moreover, MAMPU added, with technology changing so rapidly, most local law enforcement officers lack the technical training to adequately investigate an alleged intrusion.[24] TCIU's officer Assistant Superintendent Victor Sanjos agrees with the statement by saying that the rapid change in technology and technicality has forced them to update frequently and has caused them rigidity. Lack of technical knowledge happens especially to the state contingent police.[25] According to Superintendent Kamarudin, monitoring cyberspace is inevitable and the police have to do it but again, their major setback is knowledgeable manpower.[26] Surveillance, monitoring and reconnaissance of cyberspace requires a team of computer professionals, and this team of `cybercops' must be well-trained and updated with the latest tools and techniques to sniff potential attacks, and developing this team demands huge resources such as time. Moreover, it is hard to attract computer professionals to work in the public sector. They are more interested to work in the private sector because they would receive higher salary and other handsome benefits.

Malaysia has put much effort in developing and strengthening its deterrence strategy in defending its cyberspace. It has established two Computer Emergency Response Teams, namely the G-CERT and MyCERT, to develop sturdy ability in detecting information warfare attack. Incidents reporting have improved drastically since these CERTs were set up because users are consistently given security information and security mechanism to protect from intrusions and to detect intrusions. Still, awareness about incident reporting is low and need to be heightened because only twenty seven percent (27%) of the organizations that experienced security breaches made the effort to report the breaches to a third party or authority.[27] The enforcement issue is also decaying the deterrence strategy. Inadequacy in responding to the attacks means Malaysia's counterstrike ability is puny. Malaysia has the most severe punishment procedures in information warfare related offences but it fails to convince the potential attacker that he is likely to be caught and to be punished with a devastating response.

The response capability also is still not convincing. Although NISER is doing extensive research on attack tools and security issues, and actively looking for anomaly on the NII, its efforts are not sufficient. True, NISER can identify the perpetrator with its technology and expertise[28] but apprehension and punishment of the perpetrator are still weak. The main reason is that law enforcement agencies are facing shortages of qualified and professional investigators in solving piles of cases thus creating enforcement issue. Moreover, cybernetic intelligence operation does not seem to exist and even if the operation is present, it seems incapable of sniffing potential attack even on government sites. Only one case has been prosecuted so far, and this situation gives a wrong signal to the offenders and potential attackers that they are invincible and superior to the defender. Furthermore, according to experts, Malaysia's existing legislation governing electronic commerce and online transactions does not adequately protect against breach of security, especially in the area of network intrusion. Most of these laws are very limited and focus on attempts to regulate pornography, obscenity and copyright infringement and were enacted to regulate the provision of essential online services and telecommunication convergence. For cases relating to network intrusion and breach of network security, or hacking, existing laws are ambiguous and in most cases outdated.[29]

For instance, the police cannot react against illegal network scanning activity because under existing cyberlaws, the provision for prosecution exists only when there is damage done to the network or the website. Illegal network scanning activity is usually done by hackers to collect information on particular systems or computers especially about the vulnerabilities of the systems which potentially become their target. Hackers will launch an attack if there is room for them to do so.[30] This activity can be considered as reconnaissance, a preparation to find security loopholes before an attack is launched. For these reasons, Malaysia's deterrence strategy can be considered as a failure. In the near future, wireless technology and its usage will be widespread and far-reaching, thus creating a new concern. Attackers are even harder to detect especially their physical location because wireless technology will enable users (especially hackers) to operate virtually anywhere on earth. Attackers can vanish into thin air in seconds once they feel they are detected or when they have finished their job. Malaysia should expect attacks from mobile hackers which will make apprehension and counterstrike more difficult.

3) The third major problem that is fettering Malaysia from building up a sturdy defense capability is that there is no coordination between various government agencies to outline, manage, protect and implement the national cyber defense structure.[31] This means that until now, Malaysia does not have the national information warfare defense structure to protect the national information infrastructure. Each of the computer-dependent nations needs to develop and implement an information warfare defense strategy. This strategy requires the establishment of an integrated defense structure that delineates responsibility across military, civilian government, law enforcement, and private sector organizations.[32] The main purpose of the integrated defense structure is to manage the response to information warfare attack and to define the roles of military units, civilian government agencies, civilian law enforcement agencies, technology-producing companies, and private companies who are dependent on information technology in the response to or initiation of information warfare activities.

To prepare against the possible threats of information warfare, the United States established an integrated defense structure called Joint Doctrine For Information Operations. The structure provides the doctrinal foundation for the conduct of information warfare in joint operation with the military and civilian agencies. It set forth doctrine to govern the joint activities and performance of the Armed Forces of the United States in joint operations and provides the doctrinal basis for U.S. military involvement in multinational and interagency operations.[33] Unfortunately such structure does not exist in Malaysia. Each agency's operation is decentralized, making the effort to correspond to defensive strategy difficult. Moreover, procedures and processes for coordinating the efforts of military units and civilian law enforcement agencies to effectively initiate either offensive or defensive information strategies within Malaysia are virtually nonexistent. The newly formed National Information Security Council (NISC) is yet to function and still struggling to delineate its structure. The NISC should be a coordination center for the respective agencies to meet, swap information and synchronize their operation in the wake of coordinated and sustained attack but it has not called for its first meeting yet.[34]

So far, there is no information warfare game and simulation conducted by any of the government agencies. Even NISER does not conduct such activity but Major Husin said they might occupy it in the future.[35] The police said that they do not need such simulation because they are facing real hard cases.[36] There are agencies that conducted penetration testing on their system in cooperation with private firms[37] but their efforts are seen as an individual efforts and do not involve large-scale or nation-wide coordination with other agencies. The main reason war games should be conducted is to test the coordination, command and control swiftness, the ability of the agencies to control a chaotic situation, to apply the Standard Operating Procedure (if the S.O.P exists), to test the skills and to gain additional experience in managing the battle process, identifying weaknesses and rectifying the. This shows that the agencies responsible to defend the country from cyber attack do not understand the necessity, objectives and importance of conducting simulation.

The problem is, potential attackers are serious about achieving their objectives and consistently practice their skills. Hackers even conduct simulations to sharpen their skills. There are situations where hackers simulate inside their computers various types of computer networks and systems they want to attack. They diligently design tools and programs to defeat the defense software that protect the computer systems they wish to attack.[38] In developing defense strategies for greater system survivability, a set of attack scenarios is needed against which those strategies can be tested. The focus should be on how postulated nation-states, transnational terrorist groups, and non-state actors might perform cyberspace reconnaissance and attacks on information systems and information infrastructures to accomplish their objectives. The intruder's activities might include the covert use of hacker tools as well as a wide range of insider techniques to accomplish specific long-term objectives. With such scenarios available, the government and commercial unit leaders could then test their essential systems' robustness and survivability against worst case attacks.[39] The best way to test and measure the defensive capability of these agencies is through war games.

Information on warfare attack must be conveyed efficiently, other wise it could lead to the frenetic collapse of a nation. Rapid neutralization of the attack could only be done through precision coordination which needs ongoing war games for improvisation. It is true that NISER can sustain such attack but only with anticipation of other agencies' collaboration. Without precision coordination and collaboration, Malaysia could suffer significant damage on the first wave of attack. Without constant drilling, it is difficult to respond to the attack collectively and in a timely manner. The second wave of attack could be interdicted, but the damage would already have been done and the attackers achieved their objective.

5.4 Conclusion

NISER plays a vital and significant role in defending Malaysia's information infrastructure from information warfare attack. NISER's responsibility encompasses the government sector, private sector and the public by actively disseminating ICT security information, warning about possible information warfare attack and conducting research to invigorate the deterrence strategy. Besides that, NISER collaborates and cooperates with foreign agencies to trace whether the location and forms of attacks if the attacks originate outside Malaysia. Nonetheless, the Malaysian government does not rely on its agencies solely to defend the country from information warfare attack. The proposed establishment of NIIPA is a proactive step to reduce the impact of attacks, if Malaysia faces a coordinated and sustained information warfare attack. NIIPA will ensure that the vital components of information infrastructure especially the critical infrastructures will still function even if Malaysia is under severe information warfare attack.

However, Malaysia also faces serious setbacks in defending itself from information warfare attack. The overdependence on foreign ICT security solutions must be tackled as soon as possible because this would 'open' a good opportunity for the possible attackers to wage information warfare attack. Malaysia must develop its own ICT security solutions in order to reduce the weaknesses that are contained in the foreign products. The problem of enforcing the laws has made the response and deterrence strategies weaken which make the total defense strategies look shaky in the eyes of the attackers. Malaysia has no other option except to increase the number of skilled police officers to alleviate this problem. Malaysia is facing another weakness that is serious and needs special attention by the government, which is the absence of a platform to coordinate operations and to conduct simulations or war games between government agencies. The worst part is the country might be in a state of chaos if there is a coordinated and sustained attack because none of the agencies have the experience to manage the response to information warfare attack. Moreover, without this platform, there might exist an overlapping of operations and functions between agencies where this problem could lead to the wastage of resources.

ENDNOTES

[1] Information about NISER's security enquiry service. The information is on the world wide web at available at http://www.niser.org.my/services/sec_enq.html [accessed on 13 September 2002]

[2] Interview with Major Husin Jazri, Director of NISER on 3rd October 2002.

[3] Interview with DSP Abdul Aziz, an analyst of Computer Crime Section, Royal Malaysia Police on 1st October 2002.

[4] Interview with Major Husin Jazri, Director of NISER on 3rd October 2002.

[5] Ibid

[6] NISER ICT Security Survey For Malaysia 2000/2001. The report is available at NISER's hompage at www.niser.com.my [accessed on 24 October 2002]

[7] Ibid

[8] Mohd Ridzwan Md. Iman, *Terorisme siber - Maklumat, data, rangkaian sasaran penjenayah*, Berita Harian, 31 January 2002.

[9] ___________, *Kementerian Pertahanan tubuh cawangan perangi siber*, Berita Harian, 2 May 2001.

[10] Interview with Mr. Muin, Director of National Intelligence Committee on 3 January 2003.

[11] Hizral Tazzif Hisham, *NIIPA guna kaedah FBI halang pengganas siber*, Berita Harian, 14 November 2001.

[12] Minimum Essential Information Infrastructure (MEII) is a program to create an information infrastructure that is nearly invulnerable against attack and is easily reconstituted. This means identifying and protecting the minimum mixture of information systems necessary to ensure the nation's continued functioning in the face of an information warfare attack. MEII components would be required to take extraordinary measures, both technical and nontechnical, to ensure their security and ability to recover quickly from attacks. See Khalilzad, Z. (1999), 'Defense in a Wired World: Protection, Deterrence and Prevention' in Khalilzad, Z., White, J., Marshall, A., *The Changing Role of Information in Warfare*, RAND Publication, pp. 415-416.

[13] Ibid p. 416

[14] Interview with Mr. Muin, Director of National Intelligence Committee on 3 January 2003.

[15] Hizral Tazzif Hisham, *Pencerobohan komputer dianggap tidak serius*, Berita Harian, June 19, 2002. The news article is also on the World Wide Web at *http://www.emedia.com.my/Current_News/BH/Wednesday/Komputer/20020619111707/Article/*

[16] NISER ICT Security Survey For Malaysia 2000/2001.

[17] Ibid

[18] Hizral Tazzif Hisham, *Pencerobohan komputer dianggap tidak serius*, Berita Harian, June 19, 2002.

[19] Mohd Ridzwan Md Iman, *Perundangan Siber - Penguatkuasaan lemah dan perlu diperbaiki*, Utusan Malaysia, November 15, 2001.

[20] Both Technology Crime Branch and Computer Forensic Lab have less than 10 professional investigators.

[21] Rozana Sani, *Police to beef up tech crime team*, Computimes, April 4, 2002.

[22] Ibid

[23] Interview with Deputy Public Prosecutor, Ahmad Zakhi on 22 September 2002.

[24] Malaysia Administrative and Planning Unit, *The Malaysian Public Sector ICT Management Security Handbook (MyMIS)*, Prime Minister's Department, 2001. p. 5-10. The handbook is downloadable at http://www.mampu.gov.my/ICT/MyMIS/MyMIS.htm

[25] Interview with ASP Victor Sanjos, Technology Crime Branch, Royal Malaysian Police on 23 September 2002.

[26] Conversation with Supt. Kamarudin, head of Computer Crime Section, Royal Malaysia Police on 1st October 2002.

[27] NISER ICT Security Survey For Malaysia 2000/2001

[28] There was a case where MIMOS, the country's leading Internet access provider and the current home to NISER, was hacked on one of its system. NISER traced the attack and believed the attack had originated in the United States but was launched through some 10 compromised machines located in various countries. These included Malaysia (but not within MIMOS), Indonesia, the United States and New Zealand. See Aimie Pardas, *Highlights: Mimos' assurance on security of servers*, Computimes, 8 May 2001.

[29] Edwin Yapp, *Cyberlaws need to evolve says security expert*, The Star, February 26, 2002.

[30] Ibid

[31] Hizral Tazzif Hisham, *Pencerobohan komputer dianggap tidak serius*, Berita Harian, June 19, 2002.

[32] Erbschloe, M. (2001), *Information Warfare: How to Survive Cyber Attacks*, California: Osborne/McGraw-Hill, pp 9-10.

[33] U.S. Joint Chiefs of Staff (1998), *Joint Doctrine for Information Operations*, Joint Pub. 3-13, Washington D.C: Department of Defense.

[34] Interview with Mr. Muin, Director of National Intelligence Committee on 3 January 2003.

[35] Interview with Major Husin Jazri, Director of NISER on 3rd October 2002.

[36] Interview with ASP Victor Sanjos, Technology Crime Branch, Royal Malaysian Police on 23 September 2002.

[17] Interview with Major Husin Jazri, Director of NISER on 3rd October 2002.

[18] [illegible], Discovery Channel, ASTRO Channel 50. Screened on 22 September 2002 at 9.00 am.

[19] Securing the U.S. Defense Information Infrastructure, RAND paper, p 83-84. The paper is available on RAND's homepage at http://www.rand.org/publications/MR/MR993/ [accessed on 5 August 2002]