CHAPTER 3:
MALAYSIA’S INFORMATION INFRASTRUCTURE AND ITS VULNERABILITIES

3.1 Introduction

In this chapter, I will explain Malaysia’s information infrastructure and why the information infrastructure becomes a vital component for Malaysia. Furthermore, I will explain the vulnerabilities of this infrastructure, where if these vulnerabilities are exploited by the actors of information warfare, it will result in costly and catastrophic consequences to Malaysia. This chapter will also describe the methods that can be used by the actors of information warfare to attack Malaysia's information infrastructure.

3.2 Malaysia's Information Infrastructure

Malaysia's information infrastructure is a framework of interdependent networks and systems, generally interlinked at many different levels, comprising identifiable industries, institutions and distribution capabilities that provide a flow of products or services. It is a nationwide interconnection of communication networks, computers, databases and consumer electronics that make vast amount of information available to users which include all government and civilian information infrastructure. These infrastructures are crucial for the organizations, the functionality, the economic stability and the security of Malaysia. The information infrastructure is the term usually used to describe the totality
of such interconnected computers and networks, and the essential information flowing through them.

The distinguishing characteristic of the Malaysia's information infrastructure is that it is all embracing; it links other infrastructure systems together. When the information infrastructure is not functioning, many other critical infrastructure systems in Malaysia will shut down relatively quickly. Critical infrastructures are the infrastructures that constitute the life support systems of the nation. There are five sectors regarded as critical infrastructures, which are information and communication, energy, banking and finance, physical distribution, and vital human services. Through increased automation and connectivity, the critical infrastructures of a country become increasingly interdependent. Computers and communication systems, for example, support energy distribution, emergency services, transportation, and financial services. In such networks, data flow directly into control systems and affect their physical functions. Operations can take place in an instant and come from anywhere in the world.

The information and communication sector includes all the telecommunication equipment, the computer and network technologies and techniques (i.e. both hardware and software), and the lines providing connectivity and the Internet-based services. It obviously includes the Public Switched Telephone Networks (PSTNs) providing voice, data, video connectivity and private lines, in addition to the million of computers used for commercial, academic and government use and in private homes. This sector includes the support for processing, storage and transmission of data and information, including the
data and information themselves. Currently, all of these infrastructures are merging globally.

Energy is the second sector regarded as critical. The complex systems of production, storage and distribution of every form of energy characterize the energy domain: natural gas, crude and refined petroleum and electricity. For example, the electrical power grid of Malaysia is part of this infrastructure; this domain also fuels the transportation services, manufacturing operations and home utilities and is essential to many other infrastructures. It is a key component to other infrastructures and vital for the economic stability of Malaysia.

The banking and finance constitutes the third critical sector, which includes entities such as banks, commercial organizations, investment institutions, trading houses and associated operational organizations and support activities like financial transaction services, electronic payments and related messaging systems. In Malaysia, this infrastructure manages billion of ringgit, from individual deposits and paychecks, to transfers for major global enterprises. This sector is highly dependent on computers, databases and networks to manage and transact trillion of dollars of funds and other monetary instruments around the globe daily.

The physical distribution makes up the fifth sector. This sector characterizes the networks of roads and highways, railways and the airspace system (airlines, aircrafts and
airports). It also includes national pipelines, ports and waterways. This infrastructure allows moving goods and people within and beyond the borders of Malaysia.

Last, the vital human services sector includes emergency services (e.g. police, firefighting and rescue services), government services, state and local agencies, and countrywide water supply systems serving, among others, agriculture, industries and homes.

3.3 The Vulnerabilities of Malaysia’s Information Infrastructure

The critical infrastructures are vulnerable to information warfare attack because it depends heavily on the information infrastructure to operate. Attacks on Malaysia’s information infrastructure could severely damage the economic foundation of Malaysia, creating chaos and disorder, jeopardizing national security and could claim casualties. Each critical infrastructure presents different types of risk that can be exploited by the attackers when they attack the information infrastructure, take control of it and eventually damage it. The primary threats to information and communications sector are system failures, instability arising from the increased volume and complexity of interconnection, and theft of information.

Recently, Public Switched Telephone Networks are becoming more and more software driven, remotely maintained and managed through computer networks thus increasing the possibility of electronic intrusions. The existence of megacenters for operations support creates single points of failure and makes targeting of hostile actions easier. The
infrastructure vulnerability has probably grown during the 1990s; as far as Internet is concerned, high-level security was not a primary design consideration during its evolution and deployment.\textsuperscript{13}

The level of vulnerability has been raised by the recent rapid proliferation of industry-wide information systems based on open architectures used in the operating environment, including increasing reliance on communication links, running sometimes over public telecommunication networks.\textsuperscript{14} As a particular example, Tenaga Nasional, the main electricity provider company in Malaysia uses the Supervisory Control and Data Acquisition system (SCADA) to monitor and control energy infrastructure, induces the risk of serious damage and disruption by networked means.

SCADA is used by the electric power, oil and gas industries; possible electronic intrusion through public communication networks could cause significant disruption in case an intruder were able to access the system, modifying data used for operational decisions or taking control of programs for critical industry equipment. Dangers also come from the extended use of commercial off-the-shelf (COTS) hardware and software. COTS are considered risky because detailed specifications might not be available or simply not met in all the components, causing limitation of functionality or faults because of lower quality standards.\textsuperscript{15} Petronas, the Malaysian oil company, for example, use COTS' SAPP Application software in managing its oil operation around the world, which leaves Petronas's operations vulnerable to attacks.
Banking and finance sector is vulnerable when there is disruption of telecommunications and electric power services. In addition to large-scale infrastructure vulnerabilities, this area also suffers because of important opportunities for theft and fraud in individual institutions; insiders, who might use authorized access to collect confidential information or operate systems for personal profit, constitute the most persistent security threat.

Like in other areas, cyber vulnerabilities are emerging in the physical distribution sector as the sector increasingly relies on Malaysia’s information infrastructure. Every aspect of the transportation industry is affected, for example the rapidly expanding use of Intelligent Transportation Systems to optimize and increase overall efficiency. In some case, data publicly available on the Internet could be used to collect information on potential military targets.

In the vital human services sector, the main concern about cyber vulnerabilities is that some emergency systems can be overloaded through misuse. This can be done through hacking into the telephone network of the emergency services system. The attacker can disable the emergency services system by making multiple, simultaneous telephone calls which could tie up all the emergency services phone line, thereby blocking any legitimate caller from reaching the network and making the emergency lines unavailable for a live call that may be seeking help. The attacker may also release a computer worm that destroys the emergency system’s computer and tying up emergency lines.
3.4 Methods of Attacking Malaysia's Information Infrastructure

Conceptually, every information system consists of four types of components: physical systems, transmission systems, software, and data. Each component is critical to the functioning of the information system and is potentially vulnerable to either corruption or disruption. Since this dissertation focuses on system and computer intrusion that can be used to attack the data, software, and even transmission components of an information system, physical components are invulnerable to such attacks, and will not be discussed here.

The growing complexity of connections and systems to public networks has opened up a vast opportunity to the attackers to employ variety of means and tools to intrude into networked computers. Over the years, the complexity of attack techniques has increased and makes the attacks even harder to trace. The following illustrates eight common methods of attacking Malaysia's information infrastructure, but this list is far from exhaustive.

3.4.1 Attack on the Network Connectivity

This attack could broadly affect the key components of the Internet. There are four types of network connectivity attack, which are the distributed denial of service, worms, attacks on the Internet Domain Name System (DNS), and attacks against or using routers.
1. Distributed Denial of Service. Distributed denial of service attack is where multiple systems are used to attack one or more victim systems where it could deny service to legitimate users of the victim systems. The degree of automation in attacks tools enables a single attacker to install their tools and control tens of thousands of compromised systems for use in attacks. Intruders often search address blocks known to contain high concentrations of vulnerable systems with high-speed connections. Cable modem and university address blocks are increasingly targeted by intruders planning to install their attack tools. Denial-of-service attacks are effective because the Internet is comprised of limited and consumable resources, and Internet security is highly interdependent.¹⁹

2. Worm. Worm is an effective tool to attack and cripple a network connectivity. A worm is a self-propagating malicious code. The highly-automated nature of the worms coupled with the relatively widespread nature of the vulnerabilities it exploits allows a large number of systems to be compromised within a matter of hours. The biggest impact of worms is that their propagation effectively creates a denial of service in many parts of the Internet because of the huge amount of scan traffic generated, and they cause much collateral damage (for example printers that crash or print reams of junk output).²⁰

3. Attacks on the Internet Domain Name System. Domain Name System (DNS) is the distributed, hierarchical global directory that translates names (www.mokhzani.com) to numeric IP address (189.172.13.5). Threats to DNS
include *cache poisoning*, where the attacker can redirect traffic intended for a legitimate site to a site under the attacker's control. For example, when a user pointing his browser at [www.mokhzani.com](http://www.mokhzani.com), he would be directed to other unrelated site and would have no way of getting to the correct site except by typing in its IP address.\(^{21}\) *Compromise data* is another technique used by the 'actors' to attack the network connectivity. This is when the attackers compromise vulnerable DNS servers, or hack into the server that hosts the information resources, and giving them the ability to modify the data served to users.\(^{22}\) The attackers could even erase the data in the servers. The third type of attack on an Internet DNS is a denial of service attack. It is where a large denial-of-service stacks on some of the name servers that could cause widespread Internet slowdown or effective outages.\(^{23}\) The last type of attack is domain hijacking, where attackers designate the domain registration processes to take control of legitimate domains by leveraging insecure mechanisms used by customers to update their domain registration information.\(^{24}\)

4. *Attack against or using routers*. Hackers also attack the routers or use the routers to wage an attack on the network connectivity. Routers are specialized computers that direct traffic on the Internet. Threats to network connectivity fall into few categories. First, it happens when the hackers use routers as attack platforms. Intruders use poorly secured routers as platforms for generating attack traffic at other sites, or for scanning or reconnaissance. The second category is denial of service. This is done by 'suffocating' the networks with massive data
traffic. Although routers are designed to pass large amount of traffic through them, they are often not capable of handling the same amount of traffic directed at them.

Intruders take advantage of this characteristic attacking the routers that lead into a network rather than attacking the systems on the network directly. The third category is exploitation of trust relationship between routers. For routers to do their job, they have to know where to send the traffic they receive. They do this by sharing routing information between them, which requires the routers to trust the information they receive from their peers. As a result, it would be relatively easy for an attacker to modify, delete, or inject routes into the global Internet routing tables to redirect traffic destined for one network to another, effectively causing a denial of service to both (one because no traffic is being routed to them, and the other because they’re getting more traffic than they should). Although the technology has been widely available for some time, many networks (Internet service providers and large corporations) do not protect themselves with the strong encryption and authentication features available on the routers.25

3.4.2 IP Spoofing

IP Spoofing falls into the second method of attack. Every packet traversing the Internet has a source (From) and destination (To) field. Each of these contains the Internet Protocol (IP) address of a computer on the Internet. A common attack, called “IP spoofing” is to forge the From address so that the message appears to
have originated from somewhere other than its actual source. Normally, the false address is that of a host which is trusted by the receiving host so that the packet will be accepted and acted upon, in some cases allowing an intruder to penetrate right through a firewall. A false identification may allow the hacker to gain privileged access because the server will falsely believe the hacker to be coming from within the internal network or from another trusted network. A false identification may also allow a hacker to hijack a user’s communication with the server, intercepting out-going messages and substituting his own responses. Well-configured systems can guard against most types of IP spoofing, but many fail even to try. Some types of IP spoofing, particularly session hijacking form within trusted networks, are extremely difficult to protect against.

3.4.3 Password Attacks

Password attacks are one of the popular methods of attack used by the attackers to gain access into systems. This is the simple expedient of guessing, or cracking through brute-force techniques, the passwords needed for entry into a computer system. Typically, the passwords for user accounts are stored in a system file in encrypted form, where the password is used as a key to encrypt a known block of data. If hackers can get access to this file, they may be able to break the passwords using a software tool such as Crack or L0phtCrack. These programs perform what is called a “dictionary attack”. They take each word in a dictionary, use it as a key to encrypt the known block of data, and then compare the result with an entry in the password file. If they match, then the word is the desired
password for the account. In addition to dictionary words, the program might try commonly used patterns, for example, names spelled backward and keyboard sequences such "asdf."\textsuperscript{28}

3.4.4 Exploiting Software Bugs

The fourth method of attack invariably used by the attackers is by exploiting software bugs. A large part of what makes information systems open to attack is that they contain bugs, often and pertinently referred to as undocumented features.\textsuperscript{29} Many of the software programs controlling intercomputer communications have contained serious bugs. Hackers that discover these bugs can often use them to disrupt operations, steal data, or gain control of machines with which they are legitimately entitled to communicate. Such bugs, once discovered, can usually be easily fixed. However, because software evolves so rapidly, new problems are always emerging. Even a perfect fix lasts only until the next innovation hits the system.\textsuperscript{30}

3.4.5 Packet Sniffing

A packet sniffing attack is where the attackers steal and use the information that contains inside the data packet. Internet transmissions travel in small data packets through several intermediate hosts before arriving at their ultimate destinations. Each data packet contains the address of the sender and recipient, as well as the data being sent.\textsuperscript{31} Espionage and intelligence operations can be conducted by breaking into computer systems and by intercepting network traffic with "sniffer"
Network managers use sniffers to analyze network traffic and network statistics. Hackers, however, may use sniffers to steal information, such as password. Sniffers are typically used to collect user names and passwords, thereby facilitating subsequent break-ins, but they may also used to pick up e-mail and other types of network traffic. Once inside a computer system, intruders can search for categories of information and download documents and e-mail. In some cases, hackers penetrated the systems of regional Internet service providers, where they accumulated vast quantities of login data from their installed sniffers.

3.4.6 Software Trojans

In most of the hacking incidents reported, hackers often use software Trojans to destroy the systems and delete the data contained inside the system. A software Trojan horse is a program that, when activated, performs some undesirable action not anticipated by the person running it. It could delete files, reformat a disk, or leak sensitive data back to its author. If execution of the code is triggered by some event, the Trojan horse is also called a "logic bomb" or, in the case of a clock trigger, a "time bomb". The malicious code is typically hidden inside a systems or application program that looks innocent if not outright attractive. It can be planted in virtually any program, including a word processor, spreadsheet application, computer game, financial application, or system utility. The Trojan version might be distributed through e-mail or posted on the Web. Unsuspecting
users could pick it up by opening an e-mail attachment or downloading software from the Web.

3.4.7 Virus

Virus is probably one of the most popular types of attack used by the “actors” in waging information warfare. A computer virus is defined as “a program that can ‘infect’ other programs by modifying them to include a possibly evolved copy of itself. With the infection property, a virus can spread throughout a computer system or network using the authorizations of every user using it to infect their programs. Every program that gets infected may also act as a virus, and thus the infection grows. A virus can be inserted to the computer systems from a variety of sources, including floppy disks, CD-ROMs, electronic mail attachments, and web pages with embedded code that is downloaded and run on the user’s machine. Viruses also can be inserted into the target’s computer systems by using microwaves and cables.

3.4.8 Social Engineering

Intruders believe that there are two easier ways to penetrate a system: first, by impersonating an authorized employee or vendor agent to affect the disclosure of sensitive access information or allow physical access to a facility housing critical systems and second, by fraudulently influence system hot line support personnel to give out information and or affect system changes e.g. the reset of a user’s password. These methods of attack are called social engineering or confidence
game and hackers often exploit users' naïveté to gain system access. Such confidence games usually involve getting users to reveal their passwords or other personal data by claiming to be the system administrator or by providing a false log-in prompt or false Web site. Hackers often use social engineering to gain entry into computer systems. They might pretend to be a new technical or security consultant who needs a password to fix a problem or a high-ranking person who is having trouble getting access to the system and needs help.

Insiders are also considered as part of social engineering. Insiders consist of employees, former employees, temporaries, contractors, and others with inside access to an organization’s information resources. Insiders act as an information brokers, selling sensitive information and passwords of computer systems that store classified information to foreign government, competitors, organized crime, and terrorist groups. Insiders pose the biggest threats, from the viewpoint of both national security and cyber crime. Some insiders are moles; acting as an agent for foreign government to steal information. Insiders are motivated by money, ideology, revenge, and the desire to help the outsiders who exploit them.
3.5 Conclusion

With its connection to economic and life support activities, it is obvious that the information infrastructure has become a vital nerve to Malaysia. The information infrastructure is one of the most important components to generate digital economy, where this type of economy is projected to spearhead Malaysia's economic growth in the 21st century. Malaysia's information infrastructure is linked to almost every institution in this country, from hospitals, manufacturing industries, government agencies, financial institutions, research laboratories, universities to defense and security apparatus. This infrastructure must to be protected from its vulnerabilities as it provides many advantages and benefits to Malaysia. The vulnerabilities of Malaysia's information infrastructure provide a window of opportunities for the actors in information warfare to attack it by using different methods of attack. Therefore, the Malaysian government needs to protect the infrastructure because attacks on the infrastructure may undermine Malaysia's economy and security.
ENDNOTES


4. Ibid p 17


8. Ibid


10. Ibid


12. Before the introduction of computers, the phone system was simple and somewhat easier to grasp. The telephone switchboard, known as a "cordboard," was made of shiny wooden panels, with ten thousand metal-rimmed holes punched in them, known as jacks. Each of these ten thousand holes has its own little electric light bulb, known as a "lamp," and its own printed number code. When a bulb is lights up, it means that the phone at the end of that line has been taken off the hook. Whenever a handset is taken off the hook, that closes a circuit inside the phone which then signals the local office, i.e. the operator, automatically. There might be somebody calling, or then again the phone might be simply off the hook. The operator (basically is the "switching system") needs to scan the switchboard to look for lit-up bulbs to record the number code for billing purposes. Over the first half of the twentieth century, "electromechanical" switching systems of growing complexity were cautiously introduced into the phone system. After 1965, the phone system began to go completely electronic, and this is by far the dominant mode today. Electromechanical systems have "crossbars," and "brushes," and other large moving mechanical parts, which tend to wear out fairly quickly. Fully electronic systems are inscribed on silicon chips, and are lightning-fast, very cheap, and quite durable. They are much cheaper to maintain than even the best electromechanical systems, and they fit into half the space. And with every year, the silicon chip grows smaller, faster, and cheaper. These silicon chips are controlled by computer software, and the electronic switching systems can be accessed and control from anywhere. An Electronic Switching Station can scan every line on its "board" in a tenth of a second, and it does this over and over, tirelessly, around the clock. Instead of eyes, it uses "ferro brushes" to check the condition of local lines and trunks. Instead of hands, it uses "signal distributors," "central pulse distributors," "magnetic latching relays," and "reed switches," which complete and break the calls. Instead of a brain, it has a "central processor." Instead of an instruction manual, it has a program. Instead of a handwritten logbook for recording and billing calls, it has magnetic tapes. The modern telephone system has come to depend, utterly and irretrievably, upon software to control the operation. The Electronic Switching Station uses an interface known as the "master control center" to enable the telephone engineers to test local and trunk lines for malfunctions, check various alarm displays, measure traffic on the lines, examine the records of telephone usage and the charges for those calls, and change the programming. Anybody else who gets into the master control center by remote control can also do these things. Sterling, B. (1992), *Hacker Crackdown - Law and Disorder on the Electronic Frontier*, New York: Bantam Books, Chapter 1.
15 Ibid p 3.
16 Ware, W., The Cyber-Posture of the National Information Infrastructure, RAND Paper MR-976-OSTP.
18 Router is a device that determines the next network point to which a packet should be forwarded toward its destination. Routers are the air traffic controllers of the Internet, ensuring that information, in the form of packets, gets from source to destination. A packet is the unit of data that is routed between an origin and a destination on the Internet.
20 Ibid
22 Ibid
31 Ibid p. 411.


14 One way to destroy data on a computer is with a "logic bomb". This is a program with malicious code that lies dormant until some event occurs, at which point it executes. If execution is triggered by a date or time, as is often the case, the program is also called a "time bomb". See Denning, D. (1999), Information Warfare and Security, New York: Addison-Wesley, pp. 154.


17 Hank Kluepfel, Countering Non-Lethal Information Warfare. This article is posted at the World Wide Web at www.infowar.com/civil_def/kluepfel.html [accessed on 8 April 2002]
