SUMMARY

In the present electronic age, computers and the networking play a very important role in almost every facet of our lives. Government agencies, businesses, and educational organizations utilize computers to such an extent that their routine operations would significantly be held up if they encounter computers, computer systems or network impede. While using of computer and computer system would enhance the ability of organizations to conduct activities in a cost-effective and efficient manner, however, along with it comes the vulnerabilities. Someone may use those vulnerabilities to do damage to economies states by bringing down such as electrical power, finance, and telecommunications through the Internet.

The purpose of this paper is to discuss the cyber warfare from both an offensive and defensive standpoint. The scope of the paper is as follows:

1. Why cyber warfare is important to be understood?
2. What is cyber warfare?
3. The information security;
4. The offensive cyber warfare; and
5. The defensive cyber warfare.

This paper with title, *"Information Warfare: Cyber Warfare is the future warfare"* therefore is expected to provide its readers with a better understanding of cyber warfare in term of why, when, what, who, where and how. A thorough understanding of the subject therefore, would certainly facilitate the development of highly effective offensive and defensive strategies of an organization in meeting the future challenges of cyber warfare threat.

INFORMATION WARFARE: CYBER WARFARE IS THE FUTURE WARFARE

"Cyber attacks offer terrorists the possibility of greater security and operational flexibility. Theoretically they can launch a computer assault from almost anywhere in the world, without directly exposing the attacker to physical harm…" **[1]**

George Tenet, the Director of Central Intelligence of the United States

1.0 **Why cyber warfare important to be understood?**

It is important to learn and understand cyber warfare due to simple reason that is because of the environment that we are in now. The environment is the information technology environment.

The great advances in information and communications technology have an unprecedented impact on our society; a considerable percentage of our life and activities has come to depend heavily on information infrastructure. This dependence is very much apparent in both the public and private sectors. Vital factors of public life such as air, road, and railway traffic control, the dissemination of energy like electricity or gas, telecommunication systems **[2]**, key government sectors such as national defense are now organized and controlled through the use of computers and networked systems. The situation is not much different in the private sector, computers and the internet are highly involved in the way we work, communicate, buy or sell products, run businesses, control or invest money. Banks, stock markets, and other monetary institutions that transfer or handle vast amounts of money base their operation entirely on computer systems. **[3]**

That is why this subject is important and has been seriously thought-out by, not only by the military Intelligence organizations, but also the executive officers at banks, Securities firms, and other companies. Defense and intelligence officials fear that enemy nations, terrorists and criminal groups may carry out cyber warfare assaults against networks like:

1. *The banking system* - stock exchange, logic bombs could cripple the markets and destroy records of transaction, money can be stolen by cracking networks. **[4]**

2. *Electric utilities in several states and Power plants* – power grids can be knocked out causing local or regional black-outs**.[5]**

3. *Telephone networks* - can be knocked down.

4. *Air traffic control centers* - plane crashes/collisions can be caused by disabling and creating malfunctions on computer systems and on-board avionics computers. **[6]**

5. *Trains, subways* - crashes can be caused by mis-routing trains. **[7]**

6. *Battlefield tanks* - sophisticated computer controls can be crippled. **[8]**

While the information technology makes our lives more convenient, it makes us more vulnerable **[9].** This great dependence on information technology has created a new form of vulnerability for society. Public or private life can be highly disturbed by those who are able to manipulate information technology for illegal purposes**.[10]**

In this digital age, warfare is no longer limited to military versus military engagements. In the cyber-world, a digital enemy can bypass our military and take down what is near and dear to us. Destroying critical national infrastructure such as automated power plants, stock markets and transportation systems could disable this nation without firing a shot. **[11]**

It is therefore the clear rewards of information technology have new risks that need to be better understood and managed. A cyber attack could not only disrupt the daily lives, but could also jeopardize the national and economic security. In cyber warfare one doesn't need fighter planes and billions of dollars to launch an attack. One can pay someone some money to "launch an attack" and it will cost less than mobilizing a tank **[12]** or aircraft carrier. While the tools we use to protect the systems against these bandits such as firewall are expensive and complicated, the hackers often use tools that are free and simple to operate. **[13]**

2.0 What is cyber warfare?

There are many literatures written defining cyber warfare. One of the literatures defines cyber warfare as "attacking and defending information and computer networks in cyberspace, as well as denying an adversary's ability to do the same" **[14]** will be used in this assignment.

There are 2 important elements in the definition here, those is attack and defend:

What would be attacked?

1. Information - such as stealing information from storage devices for instance.

2. Information based processes - attack on processes that collect, analyze, and disseminate information using any medium or form **[15]** and attack on the networking.

3. Information and communication systems - attack on the infrastructure, organizations, personnel and components that collect, process, store, transmit, display, disseminate and act on information. **[16]**

What would be defended (protected)?

1. Information - such as protect from being stolen for instance.

2. Information based processes - protect the processes that collect, analyze, and disseminate information from being attacked and protect our networking.

3. Information and communication systems - protect our infrastructure, organizations, personnel and components that collect, process, store, transmit, display, disseminate **[17]** from being attacked.

3.0 **Information Security**

When we talk about cyber warfare, we cannot detach ourselves from discussing one pertinent issue in cyber space that is the information security tenets. Information is the most valuable asset to an organization and information is the critical success factor number one. Without information security we are putting ourselves at risk.

In fact all information security controls and safeguards, and all threats, vulnerabilities, and security process are subject to this tenets yardstick. Information is the most important asset any organization holds. It does not matter what form the information takes, either electronic, hardcopy or a person's knowledge. Whichever way the information is stored, the need for protection is of paramount importance in order to provide business continuity, maximize business opportunities and mitigate potential risks to loss or damage. **[18]** Some of the main information security tenets are: Confidentiality, Integrity, Availability, Authentication and Non-repudiation.

1.3.1 *Confidentiality.* Confidentiality is the assurance that information is not disclosed to unauthorised individuals or processes. Information requires protection from unauthorised disclosure. It deals with controlling who gets to read information in computer data and program files or information that may be on hard copy, for example, traditional files, documents etc. **[19]**

Confidentiality access control models deal with who may access what data in a computer system. Privacy, sensitivity, and secrecy are the issues here. Examples include the protection of personnel (financial, medical, legal) data, marketing or business plans, product announcements, product formulae, and manufacturing and process development techniques. **[20]**

1.3.2 *Integrity.* Integrity is ensuring that information retains its original level of accuracy. Information must be accurate and complete, and requires protection from unauthorised, unanticipated or unintentional modification. It also deals with ensuring that computer programs are changed in a specified and authorised manner. **[21]**

The more commonly agreed-upon objectives of integrity include:

1.3.2.1 Ensuring the consistency of data values within a computer system; **[22]**

1.3.2.2 Recovering to a known consistent state in the event of a system failure**; [23]**

1.3.2.3 Ensuring that data is modified only in authorised ways, whether by users or by the system; **[24]** and

1.3.2.4 Maintaining consistency between information internal to the computer system and the realities of the outside world; **[25]**

1.3.2.5 Integrity access control models deal with not only who may access what data but also how and when the data is accessed. That is accountability**. [26]**

1.3.3 *Availability.* Availability is the timely, reliable access to data and information services to authorised users. Information must be available on a timely basis, wherever it is needed, to meet business requirements or to avoid substantial losses. It deals with assuring that system users have uninterrupted access to information and system resources such as data, programs, and equipment. **[27]**

1.3.4 Authentication. Authentication is the process of recognising/verifying valid users or processes and what system resources a user or process is allowed to access. **[28]**

1.3.5 *Non-repudiation*. Non-repudiation is the assurance that business transactions as well as information exchanges between enterprise locations or with partners may be trusted. The senders or receivers that exchange between the two cannot subsequently be denied by either. **[29]**

The information security tenet needs to be adhered. If we don't, there will be threat to information. Threats to information are threats to quality, threat to effectiveness and a threat to organizational existence. The Information security tenet is the response to the risks that organizational information is facing.

4.0 **The Offensive Cyber Warfare**

This section will discuss the potential attackers and what motivate them to attack and the challenges of cyber warfare as compare to conventional warfare.

Who Breaks into Systems and Why? In cyber warfare, we are not only facing with individuals who may attack our computer systems, but more than 30 nations have sponsored programs to disrupt information systems worldwide. **[30]** There are many sources of threats to computer security. Each of the group has different motivations and poses a different type of threat **[31]**. To effectively resist attacks against its information and information systems, an organization needs to characterize its adversaries, their potential motivations, and their classes of attack **[32].** It is a challenge for us now to really determine the cyber space potential attackers as it is hard to identify them. Potential adversaries might include - motivated by:

1. National intelligence/competitors - intelligent gathering; denial of service;
2. Cyber warrior - militarily motivated; denial of service;
3. Cyber Terrorist - politically and often religiously motivated;
4. Corporate competitors/Industrial espionage - seeking competitive information; theft of intellectual property;
5. Organized crime/criminal element - economically motivated and seek information that can be sold or used to extort money from victims; **[33]**
6. Insider/employees – Embarrassment.
7. Hacker - just pride in exploiting a notable target; denial of service**. [34]**

The classes of attack may include: Passive monitoring of communications; Active network attacks; Close-in attacks; **[35]** and Exploitation of insiders.

Apart from the attack from malicious intentions, it is also important to resist detrimental effects from non-malicious events such as fire, flood, power outages and user error. **[36]**

Some approaches to attacking networks:

1. *Application-layer attacks*. Application-layer attacks are implemented using several different methods. One of the most common methods is exploiting well-known weaknesses in software that are commonly found on servers, such as send mail, HTTP, and FTP. By exploiting these weaknesses, hackers can gain access to a computer with the permissions of the account running the application, which is usually a privileged system-level account. These application layer attacks are often widely publicized in an effort to allow administrators to rectify the problem with a patch. Unfortunately, many hackers also subscribe to these same mailing lists. The primary problem with application-layer attacks is that they often use ports that are allowed through a firewall. For example, a

hacker executing a known vulnerability against a Web server often uses TCP port 80 in the attack. Because the Web server serves pages to users, a firewall needs to allow access on that port. From a firewall's perspective, it is merely standard port 80 traffic**. [37]**

2. *Auto rooters*. Auto rooters are programs that automate the entire hacking process. Computers are sequentially scanned, probed, and captured. The capture process includes installing a rootkit on the computer and using the newly captured system to automate the intrusion process. Automation allows an intruder to scan hundreds of thousands of systems in a short period of time. **[38]**

3. *Backdoors*. Backdoors are paths into systems that can be created during an intrusion or with specifically designed Trojan horse code. The backdoor, unless detected and vulnerabilities patched, can be used again and again by an intruder to enter a computer or network. Often an intruder will use the computer to gain access to other systems or to launch denial-of-service (DoS) attacks when they have no further use for the computer**. [39]**

5.0 **The challenges of cyber warfare**

1. *No physical boundaries*. The world's network, referred to by many as "cyberspace," has no physical boundaries. The enemy doesn't have to be a nation, just a group of like-minded individuals connected by the web in chat rooms **[40].** Our increasing connectivity to and through cyberspace increases our exposure to adversaries. Cyber attacks can supplement or replace traditional military attacks, greatly complicating and expanding the vulnerabilities we must anticipate and counter. The resources at risk include not only information stored on **[41],** but all of the components of our national infrastructure that depend upon information technology and the timely availability of accurate data. These include the telecommunications infrastructure itself; our banking and financial systems; the electrical power system; other energy systems **[42].**

2. *No front line*. There is no general battlefield frontline and it could be anywhere the satellites and the World Wide Web operate. Cyber warfare has brought the battlefield home. With economies becoming increasingly reliant on complex, inter-connected computerized systems, cyber warriors will have the potential for disrupting societies by causing computer mayhem, leading, for example, to power blackouts, rail crashes and chaos at the **[43]** stock exchanges from anywhere.

3. *No physical present*. In cyber warfare, attackers don't have to necessarily destroy the systems but just disrupt them. They don't have to physically enter the

organization or a nation state **[44]**; they merely have to access the systems. No large military force strike unit is required to conduct cyber warfare. In cyber warfare, the ability to eliminate the likelihood of war **[45]** is really a challenge because of the offensive ability to wage war is difficult to counter. That is a big issue.

4. *Difficult to detect and hard to track*. In the offensive mode, we may never even know who the attackers were; disinformation flow is very easy **[46].** If the attack is well planned and coordinated it is hard to find out where it came from and who is responsible for it. One might even be able to wage a clandestine war of sabotage, causing a lot of harm without being detected and thus subjected to retaliation. That is an absolute illustration of the real challenge and opportunity that information warfare represents. We can launch an attack, and it can appear as if it came from somewhere far distant from its actual point of origin. Likewise, when an attack is launched against us, it's very, very difficult to discover where that attack came from. Even if you can discover the source, it's very difficult then to launch a strike. What are you striking and why are you doing so? What public response, public support, will there be for the actions that you are taking if thousands of people die? How do you actually persuade people that this was the right thing to do? There is no evidence to cite of dead babies lying in the street. There is no man standing on the street corner with a gun in his hand. It is not the kind of thing that people are used to. This presents a real challenge **[47].** According to Jed Pickel, technical coordinator with the Computer Emergency Response Team (CERT) Co-ordination Centre, attacks were made even more difficult to combat if the perpetrators did not use one specific tool or method. For the nation state the potential of cyber warfare is something that's attractive, but it's also extremely threatening, because cyber warfare is not about nations; it's about the power that is given to individuals **[48].**

5. *Easy to organize and cheap*. One doesn't need more than a couple of computers with internet access to organize and launch cyber warfare. Hackers often use tools that are free and simple to operate. For example, there is a tool on the Internet that can reveal any dictionary password in less than a minute **[49].** With some software and some experience and know-how one would be able to do the job. Thus it is far easier to finance cyber warfare than a conventional war. Some disgruntled programmers who are willing to sell their abilities to any buyer are probably easy to find anywhere. On the other hand, a protection device such as a digital firewall can cost nearly $100,000 **[50].**

6. *24 hours a day and 7 days a week*. In physical world, we normally work from 9 am to 5 p.m. However, in cyber space, attack can be waged at any time. As a result attack by the attacker in cyber warfare hard to predict

and anticipate because attacker can attack at any time they choose, 24 hours a day and 7 days a week.

Incident reports. Example of incidents reports:

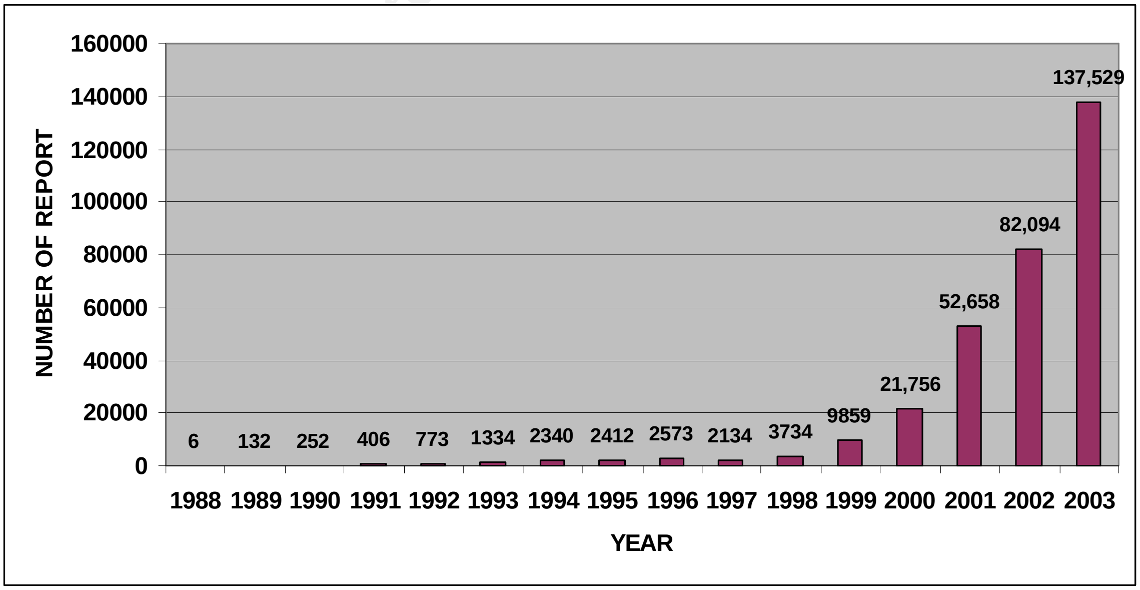
1. The Code Red worm. Attack from June to November 2001, infected more than 350,000 hosts in 24 hours, caused a lot of traffic, clogging the bandwidth and slowdowns on the Internet, affects computers running IIS Server (i.e. Win 2000 OS). **[51]**

2. W32.Netsky.D@mm is a mass-mailing worm that is a variant of W32.Netsky.C@mm. The worm scans drives C through Z for email addresses and sends it to those that are found. The Subject, Body, and Attachment names vary. The attachment will have a .pie file extension. **[52]**

3. The U.S. Army, Navy and Air Force combined suffered 715 cyber attacks last year, according to a report from the General Accounting Office (GAO) released last week. **[53]**

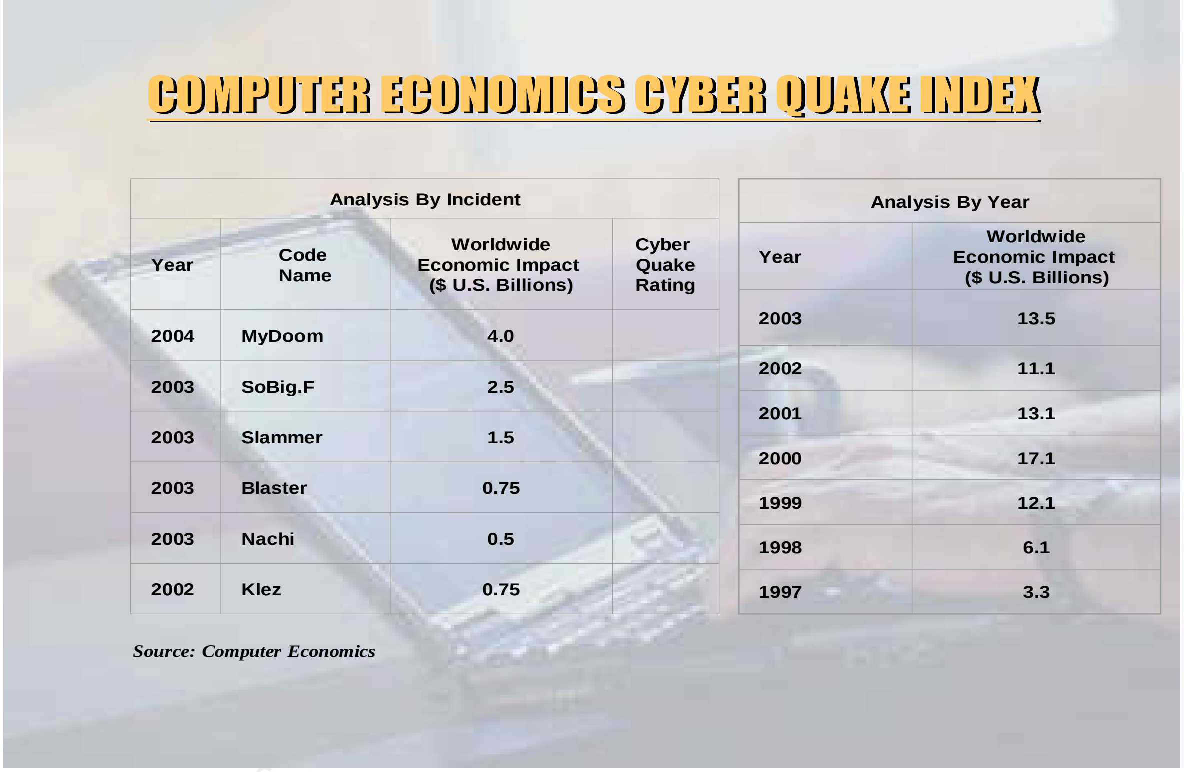
CERT intrusion/attack statistics. According to CERT, as shown on the graphic below, the statistics of reports showed that attack is on the rise world wide and it is alarming. There was small in number of attack from 1988 to 1999, then suddenly rise to 5 figure digit in 2000 and 137,529 in 2003. **[54]**

NUMBER OF INCIDENTS REPORTED



Source: Computer Economics (8 March 2004)

The Economic Impact. The economic impact of virus/worm attacked is huge. There were big money losses. According to Computer Economics (8 March 2004) in 2003 the worldwide economic impact by the outbreak amounted to US $13.5 billions. The FBI estimates that electronic crimes are running at about $10 billion a year. But only 17 percent of the companies victimized report these intrusions to law enforcement agencies. Their main concern is protecting consumer confidence and shareholder value. They say that reporting cyber-robberies expose them to leaks and that there is no substitute for constantly enhancing their own defensive electronic security. **[55]**



COMPUTER ECONOMICS CYBER QUAKE INDEX

Analysis By Incident

Year	Code Name	Worldwide Economic Impact ($ U.S. Billions)	Cyber Quake Rating
2004	MyDoom	4.0	
2003	SoBig.F	2.5	
2003	Slammer	1.5	
2003	Blaster	0.75	
2003	Nachi	0.5	
2002	Klez	0.75	

Analysis By Year

Year	Worldwide Economic Impact ($ U.S. Billions)
2003	13.5
2002	11.1
2001	13.1
2000	17.1
1999	12.1
1998	6.1
1997	3.3

Source: Computer Economics

6.0 **The defensive cyber warfare**

How secure is your perimeter defense? How to make the system secure, reliable, scalable, and manageable?

A fundamental dynamic of computer security is that defenders must always succeed in protecting systems. If attackers do not succeed, they can try again later or move on to another target that may be easier to steal information from, damage, or disable. However, the defenders must continually succeed in order to keep systems up and running, to protect vital information, to maintain their jobs, or to comply with the terms of a security contract. Attackers have the easy side of cyber warfare and have the advantage of being able to come back many times and attempt an attack. **[56]**

A second dynamic that favors the attacker is the growth of computer networks and the increase in Internet connectivity. There are many systems connected to so many other systems in numerous ways, it has become almost impossible to tally the number of systems that are connected**.[57]**

A third dynamic that favors attackers is that they can easily have accessed to all of the same technology the defender has, as well as technical system information, including weaknesses in hardware and software. Although the companies that produce IT products put forth considerable effort to conceal the weaknesses of their systems and software, it is virtually impossible to hide this information from people who really want to gain access. There are many Web sites, user manuals, bug reports, and books that provide a continuous flow of information about how IT products work and what kinds of weakness are present in the products. **[58]**

Attackers also have an advantage in that they can use the Internet and become members of the same clubs, chat rooms, bulletin boards, and e-mail lists that defenders use to help them obtain information about products or confer with their peers. Individuals can easily assume identities and remain anonymous as they wander the Web seeking out information that helps them develop information warfare attack tactics. **[59]**

It is a long-standing and well documented principle of security that security in layers is the best way to protect information. After all, we would never be able to accept increasing levels of risk if we rested the burden of protection in one proverbial basket. In today's networking environment, more and more system administrators are using some kind of defense in depth. Information will never be protected by technical means alone no matter how many levels of security may be built into the system. Thus protection may range from using a personal firewall with virus scanning software such as Zone Alarm **[60]** to a large, well-instituted and supported program that utilize every aspect of defense from policy to intrusion detection.

Defense-in-Depth is a tool of information assurance that gives networks a fighting chance against would-be hackers. Defense-in-Depth utilizes layers of security giving the network administrator, users, and security personnel time to detect and react to intrusion and attacks. This greatly reduces the likelihood of a complete breach of system defenses. Ideally, the defense-in-depth should buy us time to detect and respond to a breach, thus reducing its impact. It would seem that the more sophisticated the defenses, the less chance of compromise of information and greater amount of risk acceptance.

.

Superior implementations of Defense-in-Depth strategy integrate the capabilities of people, operations, and technology to establish multi-layer, multi-dimensional protection. This may seem easier said than done, but we must realize that information assurance is a dynamic process that requires constant evaluation and assessment.

Employing an in-depth defense starts with a commitment to this process and a realization that defenses are more than just firewalls and encryption. Defense-in-Depth is a logic-based process that starts with evaluation of assets, needs and risks which translates to implementation of technical and non-technical countermeasures, and continues with constant self assessment.

Any strategy for enhancing the robustness of the critical infrastructures must contain three basic elements:

1. Increased protection against cyber attack;

2. The ability to detect when an attack is occurring **[61]**; and

3. The capability to respond and/or recover when an attack is detected. **[62]**

Increased protection against cyber attack is founded upon encryption technology:

1. Including digital signatures - to provide the authentication, integrity, non-repudiation, and privacy/confidentiality services necessary for information assurance. **[63].**

2. Strong digital-signature-based authentication used to provide positive access control is perhaps the most powerful tool in protecting against cyber attack. Digital signature also provides for integrity of electronic information and non-repudiation of cyber-transactions. **[64].**

3. Encryption is applied to desktops, file servers, and across networks to assure the privacy of sensitive government, business, and personal information. Once the almost exclusive province of governments, encryption technology is now widely available in the commercial marketplace, and is a fundamental enabler for information assurance. **[65].**

4. Apply the technology in a coherent and effective way to all critical infrastructures. To do this requires both a framework for application of the encryption services in a scalable, interoperable way, along with the establishment of a supporting public key infrastructure (PKI) to provide robust

and globally recognizable digital signature and encryption key certificates, the individually unique "electronic ID" of the Information Age. **[66].**

The ability to detect when an attack is occurring:

1. The ability to identify a strategic cyber attack against one or several critical infrastructure components, and respond in appropriate fashion, is clearly a significant national security issue. One complicating factor is that computer intrusions have been traditionally regarded as a criminal event and within the purview of law enforcement. When an intrusion occurred, the intruder was (hopefully) tracked down, arrested, and prosecuted. Further, many private sector entities were reluctant to share information about computer intrusions, fearing adverse press coverage and public reaction. To build an effective national cyber-defense capability, new rules of engagement must be developed to allow open and dynamic collaboration among the private sector, the law enforcement community, and the national security community. **[67].**

Information Assurance. Defense in depth strategy is an element of Information Assurance. Information Assurance is achieved when information and information systems are protected against such attacks through the application of security services such as: Availability, Integrity, Authentication, Confidentiality, and Non-Repudiation. The application of these services should be based on the Protect, Detect, and React paradigm. This means that in addition to incorporating protection mechanisms, organizations need to expect attacks and include attack detection tools and procedures that allow them to react to and recover from these attacks. An important principle of the Defense in Depth strategy is that achieving Information Assurance requires a balanced focus on three primary elements: People, Technology and Operations. **[68]**

Successful Mission Execution

People. Achieving Information Assurance begins with a senior level management commitment based on a clear understanding of the perceived threat. This followed through with effective Information Assurance policies and procedures, assignment of roles and responsibilities, commitment of resources, training of critical personnel e.g. users and system administrators. This includes the establishment of physical security and personnel security measures to control and monitor access to facilities and critical elements of the Information technology environment. **[69]**

Technology. A wide range of technologies are available nowadays for providing Information Assurance services and for detecting intrusions. To insure that the right technologies are procured, an organization should establish effective policy and processes for technology acquisition. These should include: security policy, Information Assurance principles, system level Information Assurance architectures and standards, configuration guidance, and processes for assessing the risk of the integrated systems. The Defense in Depth strategy recommends several Information Assurance principles **[70]** which include:

a. *Defense in Multiple Places*. Given that adversaries can attack a target from multiple points using either insiders or outsiders, an organization needs to deploy protection mechanisms at multiple locations to resist all classes of attacks. As a minimum, these defensive "focus areas" should include**:[71]**

1. Defend the Networks and Infrastructure - Protect the local and wide area communications networks (e.g. from Denial of Service Attacks) - Provide confidentiality and integrity protection for data transmitted over these networks (e.g. use encryption and traffic flow security measures to resist passive monitoring) **[72]**

2. Defend the Enclave Boundaries (e.g. Detection to resist active network attacks).

3. Defend the Computing Environment (e.g. provide access controls on hosts and servers to resist insider, close-in, and distribution attacks). **[73]**

b. *Layered Defenses*. Even the best available Information Assurance products have inherent weaknesses. So, it is only a matter of time before an adversary will find an exploitable vulnerability. An effective countermeasure is to deploy multiple defense mechanisms between the adversary and his target. Each of these mechanisms must present unique obstacles to the adversary. Further, each should include both "protection" and "detection" measures. These help to increase risk (of detection) for the adversary while reducing his chances of success or making successful penetrations unaffordable. Deploying nested Firewalls (each coupled with Intrusion Detection) at outer and inner network boundaries is an example of a layered defense. The inner Firewalls may support more granular access control and data filtering. **[74]**

c. Specify the security robustness (strength and assurance) of each Information Assurance component as a function of the value of what's it is protecting and the threat at the point of application. For example, it's often more effective and operationally suitable to deploy stronger mechanisms at the network boundaries than at the user desktop. **[75]**

d. Deploy robust key management and public key infrastructures that support all of the incorporated Information Assurance technologies and that are highly resistant to attack. This latter point recognizes that these infrastructures are lucrative targets. **[76]**

e. Deploy infrastructures to detect intrusions and to analyze and correlate the results and react accordingly. These infrastructures should help the "Operations" staff to answer questions such as: Am I under attack? Who is the source? What is the target? Who else is under attack? What are my options? **[77]**

Operations. The operations leg focuses on all the activities required to sustain an organization's security posture on a day to day basis. **[78]**

7.0 **Conclusion**

The threat of cyber warfare is real. The low cost of mounting the attacks, has made defense a very challenging task. This situation is getting worse with the rapid proliferation of information technology and know-how. As more computers are connected to networks as the need for connectivity increases, vulnerability is also increasing.

I hope this paper would provide readers with a better understanding of cyber warfare. Understanding the subject would without doubt help the organization understanding on how to meet the future challenges of cyberwarfare threat.

8.0 **References**

[1] George J.Tenet, "Testimony by Director of Central Intelligence", Before the Senate Committee on Government Affairs (24 June 1998)
http://www.cia.gov/cia/public_affairs/speeches/archives/2000/cyberthreats_022300.html

[2] Varvara Mitliaga, “Cyber-Terrorism: A Call for Government Action?”, BILETA Annual Conference (April 9th – 10th 2001)
http://www.bileta.ac.uk/01papers/mitliaga.html

[3] Ibid.

[4] Current Events: Information Warfare and the Internet
http://www.mandia.com/kelly/cyber_warfare.html

[5] Ibid.

[6] Ibid.

[7] Ibid.

[8] Ibid.

[9] Brigadier General Robert F. Behler, “Is America Losing the Cold War in Cyber-Space?”, Federal Computer Week's (MAY 25, 1998)
http://www.fas.org/irp/news/1998/05/virtual_cold_war.htm

[10] Ibid., p.2.

[11] Ibid., p.9.

[12] Ibid., p.4.

[13] Ibid., p.9.

[14] Kenneth V. Peifer, B.S., "AN ANALYSIS OF UNCLASSIFIED CURRENT AND PENDING AIR FORCE INFORMATION WARFARE AND INFORMATION OPERATIONS DOCTRINE AND POLICY", GRADUATE SCHOOL OF LOGISTICS AND ACQUISITION MANAGEMENT AIR FORCE INSTITUTE OF TECHNOLOGY (December 1997)
http://iwar.org.uk/iwar/resources/usaf/maxwell/students/1997/peifer_kv.pdf

[15] Ibid.

[16] Ibid.

[17] Ibid.

[18] *Mr. Julian Curmi B.Sc. ACIB CISA CISSP , "*Compulsory Cost-effective Controls"
http://www.speedyadverts.com/SATopics/html/information_security.html

[19] Ibid.

[20] Ibid.

[21] Ibid.

[22] Ibid.

[23] Ibid.

[24] Ibid.

[25] Ibid.

[26] Ibid.

[27] Ibid.

[28] Ibid.

[29] Ibid.

[30] Ibid., p.9.

[31] “Economic Impact of Network Security Threats”, White Paper (2003).
http://cco-sj-2.cisco.com/warp/public/cc/so/neso/sqso/roi1_wp.htm

[32] **“**A practical strategy for achieving Information Assurance in today’s highly networked environments”, Defense in Depth, National Security Agency.
http://nsa1.www.conxion.com/support/guides/sd-1.pdf

[33] Ibid., p.31.

[34] Husin Jazri, "Challenges of Cyber Warfare", NISER (23 June 2003).

[35] Ibid., p.32.

[36] Ibid.

[37] Ibid., p.31.

[38] Ibid.

[39] Ibid.

[40] “What is Cyber Warfare (Strategic Information Warfare)?”, Cyber Warfare.
http://faculty.bus.olemiss.edu/breithel/b620s02/riley/Cyber_War.htm

[41] Lieutenant General Kenneth A. Minihan, “DEFENDING THE NATION AGAINST CYBER ATTACK”, INFORMATION ASSURANCE IN THE GLOBAL ENVIRONMENT (November 98)
http://usinfo.state.gov/journals/itps/1198/ijpe/pj48min.htm

[42] Ibid.

[43] Michael Evans, “War planners warn of digital Armageddon”, The Times (UK), (November 20, 1999)
http://au.geocities.com/cpa_blacktown_03/1999112103.htm

[44] Ibid., p.40.

[45] Ibid., p.41.

[46] Ibid., p.40.

[47] Ibid., p.41.

[48] Ibid., p.41.

[49] Ibid., p.9.

[50] Ibid., p.9.

[51] Rob Lemos, "Virulent worm calls into doubt our ability to protect the Net", CNET News.com (27 July 2001).
http://news.com.com/2009-1001-270471.html

[52] "Spread of New Variants of W32.Beagle@MM and W32.Netsky@MM Worms", MyCERT Special Alert (2 March. 2004).
http://www.mycert.org.my/advisory/MA-070.032004.html

[53] “Pentagon computers attacked 715 times last year”, PC Plank, Security News (4/05/2001)
http://www.pcflank.com/news_archive.htm

[54] "The Cost Impact of Major Virus Attacks Since 1995", CEI Computer Economics (8 March. 2004).
http://www.computereconomics.com/article.cfm?id=936

[55] Robert J. Bodisch, “The Perfect Terrorist Weapon: Cyber Warfare”, CLOSE UP, A Publication of the Texas Commission on Law Enforcement Volume 8 Number 4 (November 2002)
http://www.tcleose.state.tx.us/closeup/CloseUpNov2002.pdf

[56] Ibid., p.31.

[57] Ibid.

[58] Ibid.

[59] Ibid.

[60] "Smarter Security", Zone Labs (8 March 2004).
http://www.zonelabs.com/store/content/company/products/znalm/freeDownload.

[61] Ibid., p.41.

[62] Ibid.

[63] Ibid.

[64] Ibid.

[65] Ibid.

[66] Ibid.

[67] Ibid.

[68] Ibid., p.32.

[69] Ibid.

[70] Ibid.

[71] Ibid.

[72] Ibid.

[73] Ibid.

[74] Ibid.

[75] Ibid.

[76] Ibid.

[77] Ibid.

[78] Ibid.