INFORMATION ASSURANCE, A LONG WAY TO GO

Eric (H.A.M.) Luiijf M.Sc.Eng.
TNO Physics and Electronics Laboratory (TNO-FEL), The Netherlands

ABSTRACT

Information and Communication Technology (ICT) has an immense impact on the Military Mode of Operation. Modern Armed Forces are increasingly using commercial-off-the-shelf (COTS) hardware and software. Military and government decision-making units, critical industries, and society as a whole, are becoming more and more inter-networked. They rely heavily on essential, global, converged and entangled infrastructures. Most of these infrastructures are controlled by complex ICT. Both military command and control systems and society as a whole have become very dependent on the information infrastructures.
Information Assurance, as part of defensive Information Operations, aims to safeguard both the security posture of one's own Armed Forces and the essential information infrastructures.
This paper discusses both military and civil aspects of Information Assurance. It provides the reader with an overview of the clear and present threats from Cyberspace on the Armed Forces and society as a whole. A Cyber attack taxonomy ordered both by hacking method and reason of attack is presented. The paper discusses the strong need for Information Assurance and concludes with a list of internationally unresolved issues.

INTRODUCTION

Not so long ago, Cyberspace based warfare, automated shooters, smart ammunition and high-energy power guns existed only in science fiction literature and movies like Star Wars. Nowadays, Information Operations (Info Ops) changed from conceptual thinking into reality and has become a hot topic, both for the military and for governments.
During the last two decades, Information and Communication Technology (ICT) gained a large impact on the Military Mode of Operation. At the same time, Defence is no longer the main driver in ICT-developments. The modern Armed Forces increasingly use commercial-off-the-shelf (COTS) hardware and software. Also, military and government decision-making units, organisations, society and critical industries increasingly become inter-networked. For essential functions they rely heavily upon global, converged, entangled and often public infrastructures. Most of these infrastructures are controlled by complex ICT systems. Both military command & control systems and society as a whole - and "western society" in particular - have become very dependent on the information infrastructure and need to look carefully at the related threats.

Almost daily, hackers explore vulnerabilities in our global ICT infrastructures and in computer systems. Until now, ideological and cultural adversaries, such as individuals, guerrilla and terrorist groups, have not yet fully discovered "Information War" as a major means to disrupt military operations as well as society. Physical destruction by means of bombs and killing people by means of terror actions are still preferred above Cyberspace actions. However, some activists already have discovered the simple poor man's means to do so. While hidden in the fourth dimension, the info sphere, they attain a secure physical distance in time and place.

Armed Forces, governments and society as a whole need to be prepared in order to counter these new information-infrastructure threats. However, the current lack of awareness about information security and information infrastructure vulnerabilities, give rise to the fear that the clear and present Cyber threat danger is not yet taken seriously.

Information Assurance, as part of defensive Info Ops, aims to safeguard both the security posture of one's own Armed Forces information and the essential information infrastructures. This paper discusses both military and civil aspects of Information Assurance. A Cyber attack and attackers taxonomy and an introductory overview on hacking tools and techniques is presented. The paper concludes with a list of internationally unresolved issues.

INFORMATION ASSURANCE

The NATO MC422 'Information Operations Policy' [1] defines Information Operations as: "Actions taken to influence decision makers in support of political and military objectives by affecting other's information, information based processes, C2 systems and CIS, while exploiting and protecting one's own information and/or information systems. There are two main categories of Info Ops: defensive Info Ops and Offensive Info Ops, depending upon the nature of the actions involved".

For the information protection of one's own assets, the term 'Information Assurance' was introduced by the US Forces [2/ 3/ 4]. They defined Information Assurance: "Information Operations that protect and defend information and information systems by ensuring their: availability, integrity, authentication, confidentiality and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities".
I regard this definition inadequate for several reasons. First of all, the US definition states an incomplete list of information security aspects, it neglects for instance security aspects as reliability, survivability, safety, and audit to name a few. Secondly, this definition largely neglects the protection of the critical and essential infrastructures, which is required for the politico-military freedom to act and decide. The infrastructures are nowadays global, intertwined and most often in control by commercial companies.

To cover all these aspects, I propose the following high-level definition for Information Assurance: "Information Assurance are actions taken to protect the State/Union, its society, its international allies, its economical national and international interests against the effects of attacks on, and disturbances of, information, information systems, information infrastructures, information-based processes, and essential information infrastructures and services."

This definition takes into account all civil information assets and infrastructures that are critical to a nation or to an economic entity like the European Union and its allies. Of course, Information Assurance cannot and should not stop at the countries' border. At large, Information Assurance should be based upon mutually agreed support between countries and unions. One can argue that the aforementioned definition of Information Assurance should be "Stateless" as the information highway crosses many countries' borders. Currently, however, the State or Union is the highest organisation structure that can nationally and internationally address the vulnerability of the information society to its broadest extent, from disruption of information highway-based services to psychological information operations (Psy Ops).

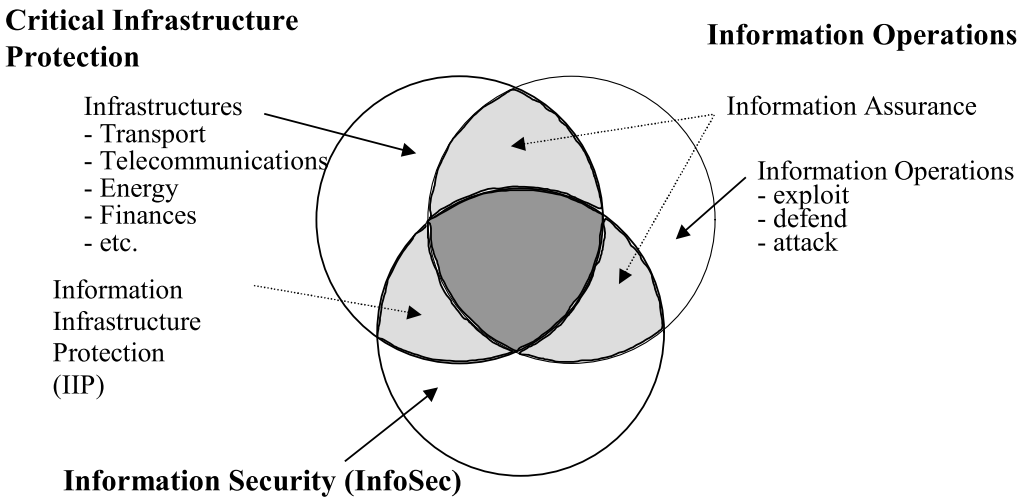

Figure 1: Relationship Information Assurance with Info Ops, Info Sec and Infrastructure Protection (from note [5])

Figure 1 shows the interrelationship of Information Assurance with Information Infrastructure Protection, Information Security and Information Operations.

Currently, the Armed Forces, government decision-making units, and critical industries become increasingly inter-networked and rely heavily upon global, intertwined and converged infrastructures. As an example, over 95% of the communication by the US Armed Forces during Operation Desert Storm went over commercial leased lines and satellites [6].
Most of these information infrastructures are controlled by complex information and communication technology. The basic building blocks for these infrastructures, however, are the same commercial-off-the-shelf (COTS) hardware and software that is used all over the globe. Knowledge about, and programs to exploit vulnerabilities in, commercial hardware and software can be acquired easily. A vulnerability found by a hacker in the early evening in Australia could become common knowledge in other parts of the world almost at the speed of light. In other words, systems in Europe and the US can already be under attack at daybreak or even during the night, at local time.

One of the tasks of a nations' Armed Forces is to prevent that attacks on the nation occur, and to defend the nation in case of an adversary's attack. The question is what role the Armed Forces will have to fulfil in defending the nations' Cyberspace. Especially when it needs to be taken into account that the Cyberspace extends over traditional international legal borders and far outstretches the "normal" military battle-space dimensions of land, sea and air.
Moreover, when looking at possible future conflicts, there is an increasingly growing probability for asymmetrical and low intensity type conflicts in which Information Operations will play a fundamental role. Thereby, it should be taken into account that the threats are not local to an operation "theatre", but can originate from an adversary anywhere out of the global society at any time in "Cyberspace". The Cyber terrorist - a premeditated, politically motivated non-military organisation (NMO), sub national group, clandestine agent or action group – [7] or their supporters poses unconventional threats to a wide range of military and non-

military targets, including the economical base. In a short period of time, they can raise attacks against the new information age societies. Crippling of the information infrastructure of a single nation, for instance, that takes part in an alliance could blunt, or even stop, the deployment of the Armed Forces of the whole alliance.

When looking at the defence side, it can be concluded that the Armed Forces and the ICT-based society are largely unprepared for dealing with the new global threats. Although high-tech information and communication technology is required, success in attacking critical information bases and infrastructures does **not** require major investments and thus are easily affordable for potential adversaries. Many quite helpful and sophisticated tools and documentation can be downloaded for free from the Internet [8]. The chances of being detected are quite low as research by the US General Accounting Office indicates. The chances of being caught are even lower [9]. It can thus be concluded that a heavily increased level of Information Assurance is essential to counter these threats.

VULNERABILITY AWARENESS REVIEW

Despite the many warning signals by hackers, Trojan Horses (e.g. Back Orifici and Netbus) and virii, power outages and broken fibres, as well as the Y2K-problem awareness, both the Armed Forces and the information age society seem to be unwilling to investigate and research its vulnerability and to take appropriate action.
Although the Armed Forces in a number of nations deal with Information Operations, the protection of the government's emergency management assets and infrastructures, to be used by government agencies and supporting Armed Forces, is often overlooked. With exception of a small number of nations [10], the continuity and protection of essential information infrastructures and information systems is not taken seriously. Those nations that undertook some action, understand that they are faced with a large task that should be dealt with in co-operation of Defence, government agencies, and public-private collaboration[11]. Also, legal issues and conflicting regulations prohibit a 'ready-for-battle' course of action.

As an example, the US President's Commission on Critical Infrastructure Protection (PCCIP) [12/ 13/ 14] looked at vulnerabilities in the following areas: information and communications, energy (electrical power systems, gas and oil transportation and storage), banking and finance, physical transportation (including air traffic control), and vital human services. The PCCIP reported that there is an increasing dependence on critical infrastructures. The developments of computer technology and astonishingly rapid improvements thereof have ushered the information age and affect almost all aspects of commerce and society. Our security, economy, way of life, and perhaps even survival, are now dependent on the interrelated trio of electrical energy, communications, and computers. The inter-relationships of infrastructures are, to say the least, worrisome. Everyone foresees the worst if more than a single infrastructure is disturbed, either deliberately or just by 'acts of God'. "The capabilities to launch an attack against the nation's information infrastructures are now quite widespread, and an attack is probably not that far away," warned Philip LaCombe, the director of the PCCIP. Disruption of the services on which the economy and our well being depend could have significant effects, and, if occurring frequently, could seriously harm public confidence.

The PCCIP concluded that the increasing vulnerability comprises the classical threats to infrastructure, and the new Cyber threats. The right command sent over a network to a power

generating station's control computer could be just as effective as a backpack full of explosives. The perpetrator would be harder to identify and apprehend, to boot. Moreover, infrastructures are growing in complexity and are operating close to their designed capacity. This increases the likelihood of cascading effects that begin with a rather minor and routine disturbance and end only after a large regional outage. Because of their technical complexity, some of these dependencies may be unrecognised until a major failure occurs. This failure can either be introduced by a ('stimulated') operational mistake, a technical failure, and an act of sabotage or – new – by an act of 'cybortage'.

Although infrastructures have always been attractive targets, borders and friendly neighbouring nations provided some protection in the past. Today, this situation has changed dramatically as national borders are no longer relevant in Cyberspace. Potentially serious Cyberspace attacks can be conceived and planned without detectable logistic preparation. They can be invisibly reconnoitred, clandestinely rehearsed, and then mounted in a matter of minutes or even seconds without revealing the identity and location of the attacker. As the Armed Forces increasingly use the same infrastructures, it becomes more and more difficult to distinguish between attacks on Armed Forces and attacks on society as a whole.

Almost daily one can read in the newspaper examples of ICT-vulnerabilities in our so-called "western" society (at large) and how the Armed Forces and society deal with them. People seem to smile about the incidents and forget about the impact that may occur when information systems and infrastructure are deliberately targeted on a larger scale.
Seen in this light, it is worthwhile to revisit some examples:

The lessons learned from disruptions by natural disasters, e.g. the Hansin Dai-Shinsai earthquake on January 17, 1995 with its epicentre near Kobe. The vulnerability of our ICT-based society was demonstrated in many ways. Although there was sufficient food available, it could not be sold as the ATM system was disrupted causing a lack of cash. Emergency backup communication via satellite was disrupted as the earthquake offset the satellite dishes and nobody in the disaster area knew how to realign them. The last major earthquake in 1995 in the San Francisco Bay area showed the same kind of ICT-vulnerabilities [15].

After learning from the financial market chaos caused by the London Square Mile bomb explosion on November 4, 1992, the Provisional IRA used hoax calls to disrupt infrastructure services (e.g. underground; the London financial district). They also planned to place either real or realistic-looking dummy bombs at six electricity substations at the outside of the London (security) "ring of steel". If the plan had been successful, the utility companies involved would have switched off *themselves* all power in a controlled way. This to reduce chances of cascading downed circuits throughout the whole UK. It was estimated that it would have disrupted all power services in London for at least 1, probably 1.5 days. The chaos and psychological effects would have been tremendous. The PIRA did not understand (yet) that transmitting the right commands on the right remote control lines causes the same effect.

Soccer fans, trying to obtain tickets for the 1998 World Cup soccer games, caused the telephone networks in several European countries to collapse on April 22, 1998. In the Netherlands alone, 30 central office switches went down for several hours. This included the four major cities and the emergency numbers. After Rinus Michels, former Netherlands soccer coach, I concluded that 'Soccer is infrastructure warfare'.

Vending machines supposedly dial the distributing company when they are near empty. However, some of the incorrectly installed machines in Australia dialled the default number 000, which is the emergency number in Australia. As there were thousands of machines installed, about 1 million 'mistake' calls per year were made to the emergency service, blocking access for those who really required help. This kind of widespread irregular 'attacks' turned out to be hard to tackle.

On March 10, 1997, a young hacker took down the Bell Atlantic central office switch in Worcester near Boston, USA. As a result, the airport lacked telephone and data services for over 6.5 hours. On January 4, 1999, five people broke into a Las Vegas Sprint telephone office and made off with telephone switching equipment. It caused a 7-hour interruption of phone service to 75.000 customers [16].

On May 19, 1998, a PanAmSat Galaxy IV satellite spun out of control, disrupting pager service to 80-90% of the 40 million pagers used in the US for over 3 days. Doctors were among the first affected as hospitals page them in emergencies as well as police officers. The Amsterdam Internet Exchange went down the December 26, 1998 due to a defective power transformer. Effectively, the Netherlands was largely cut off from the Internet for a number of hours. On June 16, 1999, 4 fibres were cut in Groningen causing a grinding halt of mobile and fixed telephone services as well as loss of data services in the northern Netherlands provinces.

On March 26, 1999 the Melissa macro worm spread very quickly over the Internet. Many US government sites, including a military base that supported the Kosovo Operation, turned out to be vulnerable. The worm luckily had no destructive 'payload' [17].

From these and many other, almost daily occurring big incidents, it should be clear that the Armed Forces, government, society, organisations and critical industries need to prepare jointly for defending their assets in the information age.

CYBER ATTACKS: FACT OR FICTION?

Cyber attacks and Cyber terrorism can be found on the Information Operations road map. The question is whether one should regard this as a future, a futuristic or an actual today threat. Is it real or is it fiction?

Studying this question, open information bases do not give very substantial facts. For instance, computer crime is not recorded as a separate item by most Bureaus of Statistics. It probably will be categorised under crimes like fraud, falsification or another category. Thus, no sociological breakdown of Cyber attackers is at hand. The ones caught range from schoolboys, students, a brain damaged man living on social security, to real terrorists. Some hacker groups, e.g. Master of Downloading (MOD) have multinational membership [18]. On the other hand, terrorism itself will remain a major trans-national problem, driven by continued ethnic, religious, nationalist, separatist, political, and economic motivations. Cyber terrorism is likely to come out of its infancy soon. Thus, in order to address the question "Cyber attacks: fact or fiction?" we have to make an assessment to categorise the different Cyber attack aspects, look for indications, look for our vulnerabilities, evaluate reports and draw

some conclusions.

CYBERWAR – THREAT ASSESSMENT

When looking at the different types of conflicts that might occur, one should look at the type and the driving intent of potential adversaries. Table 1, based on Waltz [19], provides such a breakdown.

Guerrilla Wars

		High-tech	**Low-tech**	
Economic Based Wars	**Physical conflict**	1. Military C2W . high intensity battle space . economic pressure & power . precision targeting . stealth: physical . C4I technology	3. Guerrilla warfare . low intensity battlespace . ruthlessness . random targeting . stealth: natural environment . human networks (as technology)	**Terrorism**
	Abstract conflict	2. NetWar, CyberWar . Cyberspace conflict . knowledge as power . information base targeting . stealth: using ICT . global networks (as technology)	4. Ideological warfare, conflict and power . mass/society targeting . stealth: ideological . ideological human networks	

Cultural Wars

Table 1: Typology of four conflict types (Waltz, note19)

It is clear that the major emphasis in box 1 lies with the military (information operations; command and control warfare). The high-tech Cyber terrorist (box 2 in figure 1) - a premeditated, politically motivated non-military organisation (NMO), sub national group, clandestine agent or action group –(see note 7) or their supporters poses unconventional threats to a wide range of military and non-military targets, including the economical base.

A major advantage for the virtual protagonist (boxes 3 & 4) is that he/she does not need to be around, in time or place, when attacking a system or infrastructure. Mounting a delayed attack is easy, as the modem dial-up for an attack launch can easily be automated. The global infrastructures make it easy to choose the country from which an attack is mounted, and by the way, it is easy to stealthily use international phone lines to reach a modem in another country. For security services, governments and organisations under attack, it will be hard to have indications of which targets might be selected. Lacking this intelligence, there is hardly

time for some warning. Tracking and identifying virtual terrorist groups may be even more difficult, if not impossible.
The possibility to use these aspects as a tactical means using new and combined technologies makes it quite different from earlier warfare means. The relatively low cost, high potential success rate and low probability of own losses makes "Offensive Information Operations" in principle quite attractive for individuals, economic adversaries, as well as protest and terrorist groups.

THE TAXONOMY OF CYBER ATTACKERS

Type of the trade

The first breakdown is to look at the type of hacking trades within the hacking underground:

- **Hackers**, who try to break in to demonstrate the vulnerability of computer systems and networks by exploiting "less well" managed systems and/or known bugs. Their intention is most often not a malicious one, but mere a kind of wondering what will happen if…. These include sniffers and snoopers, who listen on the networks for plain passwords.

- **Crackers**, who break into computer systems, try to destroy or modify information or exploit these systems e.g. to distribute software illegally. Software crackers are specialists in this group who like to break software security/self checks. Software with broken self-checks or valid licence numbers is placed on web servers (‘warez’).

- **Phreakers** (phone freaks), exploit phone exchanges, the cellular phone system and use phone signalling for fraud. They also may be involved with smart cards and credit card fraud. The phreaker group “Phone masters” broke into switches of AT&T, Southern Bell, BT, had access to portions of the US power grid and air traffic control systems. They forwarded FBI phone lines to phone-sex chat lines in Germany and other countries and got access to lists of tapped phone lines (in the end, their lines as monitored by the FBI showed up as well).

- **Social engineers**, who are deceptive collectors of information that allow them to collect passwords or other vital information to access systems and networks. **Thrashers** are social engineers, who use physical collecting methods. So called **dumpster-divers** like going through the company’s garbage to find valuable information that can be helpful to prepare a social engineering attack or to attack directly.

- **Satcom, CATV cable modems and pay-TV** hackers crack the scrambling of signals in order to view the transmissions for free. Their actions currently have only economical impact. With the offerings of Internet access over CATV cable modems, confidentiality, integrity and privacy threats become an issue. However, these fall under the other categories.

- **VX** - Virii Creators, people who write viruses and the like. The so-called ‘lamers’ are of a lower class: "they use virus construction kits, makes small useless modifications or just infect others' computers".

- **Screen** (‘eaves’) **droppers** stealthily monitor distant computer screens using the electro-magnetic radiation of screens. These ‘(Wim) van Eck systems’ might pick up screens from a distance of 1 km. Transient Electro-Magnetic Pulse Emanation STandard (TEMPEST) measures largely take away this risk.

- **The insider**: can be any of the above and can have ‘unlimited’ access to internal information and systems.

Reason of attacks

Secondly, we can order Cyber-attacks by the reason of the attacks and who is behind it (attribution):

- **Incompetence, negligence**. *Who:* the insider. *Goal:* obviously no goal.
  Note that everything being said about the external hacker threat should be balanced with the results of many studies that show that the insider is responsible for 60%-80% of the information security breaches. Lack of defences due to negligence and lack of security awareness is the main cause of successful attacks. The outsider can often attack by making use of the doors left unlocked by the system and network administrators. Moreover, hardly any organisation takes measures to detect unauthorised insider activities.

- **Internal denial of service**. *Who:* the disgruntled employee.who wants to hurt his employer *Goal:* burned grounds (deleted or damaged information) or locked information (key known only to employee).

- **Recreational / amateur hacking**. *Who:* any single or small group of teenager(s), student(s) and technology interested person(s), sometimes working in peer-groups. *Goal:* trying to understand ICT and the way security sometimes (often) does not work (curiosity). *Edge risk:* the person might become a 'small criminal' by obtaining financial gains (e.g. phreaking, smart card fraud).

- **Electronic disobedience**. *Who:* activist group; supporters of a cause. *Goal:* obtaining media attention and temporary service interruptions by denial-of-service attacks. *Edge risk:* become more violent when actions have no impact. Example: Electronic Disturbance Theatre (EDT) in support of the Mexican Zapatista fighters flooded web servers of the Mexican President, the Frankfurt Stock Exchange and the US Department of Defense with web page requests. Result was a denial-of-service.

- **Publicity seeking hacking/bragger**. *Who:* any single or small group of teenager(s), student(s) and technology interested person(s) as well as (semi) professional hacker group. *Goal:* the intent is to obtain a large media attention by breaking into a high valued ICT system and bragging about it. *Edge risk:* become involved / hired by criminals or sub national group.

- **Legal support seeker**. *Who:* hired semi-professional hacking person or group; disgruntled “former” employee. *Goal:* try to discredit an ICT-service and/or service provider to prove his/hers own innocence. *Edge risk:* becoming 'violent' trying to make his/her point.

- **Obtaining intelligence**. *Who:* National intelligence communities, economic information collectors (business intelligence firms), economic and industrial espionage and hired professional hacking persons/groups.
  Goal: national and business intelligence to obtain advantage over other nation(s) and organisation(s).

- **Action group cause; criminal protagonists ('hacktivists')**. *Who:* any motivated group with technological knowledge or support. *Goals:* seeks publicity and tries to annoy the objected organisation or government department or agency. *Means:* looks for denial-of-service attacks, e.g. by overloading, as well as loss of integrity of systems. *Edge risk:* becoming 'violent' trying to make their point and move to terrorism.
  As an example, in August 1999, the 1996 Nobel Peace Price winner José Ramos-Horta threatened the Indonesian government. A group of over 100 hackers all over the world sympathises with the East Timor struggle for independence and is willing to attack Indonesia's main economic assets (banks, telecom operators, airliners) in case the Indonesian government does not accept the outcome of the referendum held in East Timor.

- **Economic gain**. *Who:* unscrupulous business party or "ethical flexible" employee. *Goal:* obtain benefits by crippling competitors' ICT-business.

- **Vandalism**. *Who:* mainly disgruntled employee or individual. *Goal:* hit the economic values of an organisation.

- **Criminal activities**. *Who:* professional hacking persons/groups either with criminal goals themselves or hired by criminals or criminal groups. *Goal:* operation (if possible stealthy) to obtain intelligence, counter-intelligence (e.g. obtain, destroy, discredit or destroy police information), to disrupt security infrastructures during a planned action or to obtain a financial gain.

- **Cyber terrorism**. Who: premeditated, politically motivated sub national group, clandestine agent, organised crime groups or unscrupulous economic competitors. Might make use of paid professional hacking group or person(s). Whether the attack is foreign or domestic does not make any difference. Goals: a wide range of military and non-military targets, including the economical base.

Note that apart from the Cyber attackers, the new ICT means in general and the Internet in particular, are used as a communications means for sub-nation, terrorist and criminal information dissemination (e.g. bomb recipes, lock picking courses, offers for illegal passports) and secret communication. These categories are not treated in this paper.

METHODS OF CYBER ATTACK

Apart from the insider misuse, most of the Cyber attack trades have their own underground information circles with sometimes even quite open web information bases (see note 8). Combinations occur, e.g. phreaker tool and knowledge is used to open a free circuit to a telephone exchange. Hackers might pass through multiple computer systems and exchanges

before they get to their target that could mean going through multiple states or countries. Some hacking groups are well established and have their own regular publications (e.g. 2600 in the US, which has been around for over 10 years; Chaos Computer Club (CCC) in Germany). Many E-zines on this topic can be found on the World Wide Web as well. The hacker/phreaker circles document their knowledge, findings and even hardware designs quite well. Even knowledgeable UNIX and Windows/NT systems managers use these sources for obtaining more insight. Most of these documents and databases with information related to system weaknesses can be found on the Web.

Apart from physical attacks, the different types of information attack means vary from a strict software mode of attack to electro-magnetic spectrum means. An example list of these means follows below:

- **Computer virii**: code that self-replicates when executed and stealthily infects executable code, including macrocode. Apart from the replication code, a virus contains a payload that might be friendly or malicious. Virii are unguided pieces of software. Their infecting speed is depending on the type of infection mechanism used. Although sometimes destructive and annoying, virii are a less obvious Information Operation means

- **Trojan Horse**: code that has hidden side effects. Goodies and nice websites with active code (Java, ActiveX) pose a danger for those downloading code or visiting such sites.

- **Worm**: self-replicating code that uses network functionality, e.g. Email distribution mechanisms, to spread. The Melissa 'virus', which swiftly spread through the Internet in 1999, was such a worm.

- **Logic bomb** and **time bomb**: a stealthily piece of code that executes when a certain – externally triggered – condition, e.g. time, removal of a file, change on an external website, occurs.

- **Logic torpedo**: a virus type that tries to advance towards a certain set goal, being a system or program to deliver its payload there.

- **Data manipulation**: ranges from discrediting information integrity by changing data bits to **video morphing** in which video or still picture information is manipulated in such a way that for instance a President shaking hands with someone he never met in his whole life.

- **Backdoor** or **trapdoor**: an opening in the system left by a programmer or system administrator allowing unauthorised users to gain access to part of or the full system.

- **System design** and **coding flaws**: for each operating system, network software, network switching elements, and boundary protection devices (firewalls, guards), lists with vulnerabilities and patches are published by the vendors and Computer Emergency Response Teams. Usually, the system administrators have no or limited time to install patches as soon as this information gets out. This results in well-known open doors in many production systems.

- **Overloading**: bombarding a system with so many requests that the system cannot cope with the influx resulting in a denial-of-service for authorised users. A tool that was designed for flooding is Floodnet by the Electronic Disturbance Theatre.

- **Chipping**: modifying chips in such a way that the chip contains a backdoor or logic bomb.

- **Blue boxes**: tapping into phone lines and 'playing' with the signalling.

- **War dialler**: a software and modem set-up that allows fast sequential dialling of list(s) of telephone numbers in order to detect active modems or telephone lines that allow 'after-dial'.

- **Electro-magnetic spectrum** means, some examples:

  - Tapping information using the radiation of screens and soft tempest (software stimulated emissions)

  - Tapping other EM-spectrum signals,

  - Interfering with radio signals, e.g. a GSM-suppresser, as well as high-peak power ultra-wide band spectrum transmitters,

  - Electro-magnetic pulses, overloading and even destroying system circuits,

  - High-power microwave tools.

EVALUATION OF CYBER ATTACKS

To estimate the threats of Cyber attacks, the table below gives an estimate of the target likelihood by target and by motive. At the same time, the table shows whether validated attacks were reported by open sources.

CYBER ATTACKS	Validated Attacks (Status September 1999)	Targets				
		Infor-mation	Systems & Small Networks	Organi-sation & Industry	Govern-ment	Infra-structure & Society
Incompetence, negligence	Widespread	Main target	Main target			
Internal denial-of-service	Widespread	Main target	Limited	Main target		
Recreational hacking	Widespread	Limited	Main target			
Electronic disobedience	Limited		Target	Main Target		
Publicity seeking hacking	Widespread	Main target	Limited			
Legal support seeker	Limited	Main target	Limited			
Obtain economic intelligence	Limited, fast growing	Main target				
Economic attack / gain	Limited, fast growing	Main target	Main target	Main target		Limited
Obtain national intelligence	Known to occur	Main target		Limited?	Target?	
Action group / hacktivists	Limited, growing	Limited	Main target	Main target	Main target	Limited
Vandalism	Limited		Main target	Target	Target	Limited
Criminals: simple crime	Limited	Main target		Target		
Criminals: financial crime	High, fast growing	Main target	Phreak-ing	Target		
Organised crime	Unknown	Main target		Main target	Target	
Cyber terrorism	PIRA: limited				Target	Main target
	Limited	Main target	Target	Target	Target	Main target

Recently, network support personnel of the US Space and Naval Systems Warfare Center (SPA WAR) in San Diego were asked to investigate user complaints about a slow printer. Hackers had diverted the printer stream to a server in Russia, which in turn finally sent the output to the printer in question [20]. One can only guess what happened with the printer output. During the Kosovo crisis, attacks were reported from sources in Serbia and Russia, as well as from sympathisers in other countries, on NATO systems, US government systems, and defence systems of coalition partners. Apart from denial-of-service attacks and defacing of web sites, attempts were made to intrude defence networks.

So, when discussing the question: “Cyber attacks: fact of fiction”, it can be concluded that all types of Cyber threats have been realised in one way or another. Daily, one can find articles in

the news about hacked systems, credit cards and affected infrastructures. However, full-scale attacks with a major impact on Armed Forces and/or society have not (yet!!) been realised.

OPEN ISSUES

The information infrastructures are ICT-dependent, intertwined and inter-networked. They are highly vulnerable. Around 80% to 90% of the information needed to defend one's nation is nowadays in the private sector, in other words: is beyond government control. Fundamental changes in the approach to information assurance in the 21st century society are required. In the following some of the open issues are highlighted.

Organisations in general are not paying enough attention to information security, neglect warnings, cannot keep up to date with significant changes in the network environment and are unprepared for the things that may happen. I am quite convinced that many government agencies have sensitive systems and networks that have unlocked doors waiting to be opened unauthorised. The economic electronic intelligence gathering industry, both ethical and non-ethical, is mushrooming. There are indications that obtaining financial advantages by using non-ethical economical attacks is growing, given the low chance of detection. How long will society accept these risks?

Most governments lack awareness on the vulnerability of their own society. The outcry on international Cyber terrorism can be expected sooner or later. Studies like the US PCCIP study are either not realized in most countries or are hampered by lack of co-operation by other government agencies and industry. In Cyberspace, one can be attacked either from across the street or from somewhere in Timbuktu, which makes it rather difficult to go after Cyber attackers. The only solution is to keep the gates closed at all times, meaning one has to be continuously vigilant.[21] Organisations using information and communication means at large, as for instance the Armed Forces, have very limited resources both in terms of quality (knowledge) and quantity (number of system managers). It is already a burden to keep the information infrastructure working on a day-to-day basis. Resources to maintain the security posture are scarce. Organisations should become aware that Information Assurance should be high on their priority list in order to survive adversaries' Information Operations. The question is whether actions will be taken in time or that we will experience some electronic Pearl Harbor.

To address these issues, a fundamental international legal effort is required to address Cyberspace, the international legal fundaments, international police co-operation, the legal definition of Cyber attack and what kind of defences against Info Ops are allowed. Currently, international legal support is ineffective due to complex procedures. The adversary on the other hand requires only small bit streams that are measured in seconds. Secondly, the current preparedness of police involves criminals, not terrorists. Who will defend countries against Cyber terrorism? What will be the role of the security services in the 21st century given the threats of Cyber and infrastructure terrorism? How should inter-State information exchange be organised to fight cross-border threats?

Emergency preparedness requires training and rehearsals. Information Assurance requires the Armed Forces, governments and critical information infrastructure suppliers to be prepared for managing protective actions in case of an attack. The question is how to develop realistic

rehearsal scenarios, particularly when considering the cross-border aspects of Cyberspace.

Increasingly, Armed Forces and governments agencies actively use ‘Tiger’ or infiltration teams that try to break-in into their own sensitive systems. There are a number of legal issues when deploying these so-called ‘Red Team’ capabilities that need to be solved. Proper Information Assurance requires actively seeking holes in one's defences in combination with intrusion detection and trained counter-teams. When looking at the international aspects, the question is whether countries should co-operate with Red Team activities at a technical level? Is a continuous assessment of international information infrastructures required?

There is currently a lack of management attention on information security awareness. The question is how to start Information Assurance awareness at the right level in the Armed Forces and in government organisations.

A simple solution by some to the Information Assurance problem is to deny all electronic communication and information exchange. On the other hand, there is the pressure for sharing of international information and intelligence between coalition partners and governments. How to maintain the confidentiality, integrity and availability of one's own information if a certain degree of exchange is required before obtaining information from other parties. To deal with this dilemma, further Information Assurance developments are required.

And last but by no means least, hacking and phreaking are a reality. However, most of them are recreational hackers. The question, however, then is which alerting tools should be developed to recognise the 'probing' spies, criminals and terrorists in the haystack of background noise?

CONCLUSION

To survive possible Cyber attacks, e.g., from virtual terrorists, for whatever ideological or other reasons, requires countries, governments and organisations to be prepared. The Cyber attacker has the advantage of being place and time independent from the target, whilst the technology required is relative cheap to acquire. Information Assurance is supposed to be the answer to the asymmetrical threat. For that reason, Information Assurance, which includes aspects of information security, information infrastructure protection and defensive Information Operations, requires much more attention than currently is the case. The lack of awareness, security management and proper risk analysis causes a potential of high, unmanaged risks. The use of commercial-off-the-shelf (COTS) hardware and software increases the potential vulnerabilities of systems and infrastructures in case known exploitable vulnerabilities are not countered as soon as possible. COTS producers are reluctant to add mechanisms that support Information Assurance and trustworthiness. The question is how to maintain trustworthiness while predominantly using COTS components [22]. And, as the (virtual) ICT world, the global connectivity, converged infrastructures and inter-networking cross many international borders, effective international co-operation will be essential to counter attacks to the national or defence information infrastructure.

The fact that Armed Forces and emergency management communications rely partly, or sometimes even largely, upon third party-owned civil infrastructures is of great concern. International co-operation is still based on antiquated mail-coach technology and lengthy

administrative, if not bureaucratic, procedures. The Cyber attacker, on the other hand, uses the light-speed electronic highway, and is informally organised. There is still a long way to go to close the Information Assurance gap. This requires both raising the awareness at the highest decision-making levels, major technological developments, and global co-operation on harmonised legal systems and criminal investigative support.

To summarise, the current status of Information Assurance in the Armed Forces and in society as a whole, makes us fear for the worst.

NOTES

[1] NATO (1999), *NATO MC422 Information Operations Policy* (January 12, 1999)

[2] US Army. (1996). *Field Manual No. 100-6, Information Operations* (FM 100-6). [On-line] Available: http://www.jya.com/fm100/fm100-6.htm

[3] Department of Defense Directive (1996). (DoDD) S-3600.1.*Information Operations (IO)* (December 9, 1996)

[4] US Joint Staff (1996). *Information Assurance. Legal, Regulatory, Policy and Organizational Considerations*. J-6A 009773-97. 3rd edition (1997)

[5] Stein, Dr. W., *Information Warfare in Umfeld von IT-Sicherheit und Schutz der kritischer Infrastrukturen.* Seminar CCG. June 22-24, 1999.

[6] Hamre, Dr. J.J. (1998). DoD Speech to Fortune 500 Chief Information Officers Forum on July 21. US DoD. Aspen, Colorado. [On-line] Available: http://www.defenselink.mil/news/Aug1998/t08121998_t072198.html

[7] Pollitt, M.M. (1998), *Cyber terrorism, fact or fancy?* Computer Fraud & Security, (2) pp 8-10. Elsevier Science Ltd.

[8] Luiijf, H.A.M. (1998). TNO-FEL's URLography on Information Warfare. [On-line] Available: http://www.tno.nl/instit/fel/infoops

[9] US GAO (1996*). Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, GAO Executive report B-266140. [On-line] Available: http://www.infowar.com/CIVIL_DE/gaosum.html-ssi

[10] Publicly known infrastructure assurance activities are on-going in: Australia (note 11), Canada, Egypt, Germany (BSI/AG KritIS), Sweden, Taiwan, the United Kingdom and the USA (note 12-14).

[11] Cobb, Dr. A. (1997). *Australia's Vulnerability to Information Attacks*. Australian Strategic and Defence Studies Centre, Australia. ISBN 07315 27232. [On-line] Available: http://coombs.anu.edu.au/~acobb/X0016_Australias_Vulnerabi.html and http://www.infowar.com/CIVIL_DE/civil_100497a.html-ss*l*

[12] PCCIP (1997). *Research and Development: Recommendations for Protecting and Assuring Critical National Infrastructures*. Washington, D.C., USA. . [On-line] Available:

http://www.pccip.gov

[13] PDD63 (1998), *Presidential Directive 1998, number 63: Critical Infrastructure Protection Directive*. Washington, D.C., USA. [On-line] Available: http://www.ciaoorg

[14] (US) President's Commission on Critical Infrastructure Protection by Executive order #13010 of July 15, 1996. PCCIP (1997). *Critical Foundations: Protecting America's Infrastructures*. Report 040-000-00699-1, United States Government Printing Office (GPO), Washington, D.C., USA. [On-line] Available: http://www.pccip.gov

[15] Noam, E.M., Sato, H. (1995). *Kobe's lesson: Dial 711 for 'open' emergency communications*. Columbia Institute for Tele-Information, USA. [On-line] Available: http://jisp.cs.nyu.edu/RWC/rwcp/people/yk/shinsai/comm-proposal.txt

[16] Oakes, C. (1999). *Thieves hit phone center*. Wirednews. January 4, 1999.

[17] US GAO (1999). *The Melissa computer virus demonstrates urgent need for stronger protection over systems and sensitive data.* Report GAO/T-AIMD-99-146, April 15, 1999. [On-line] Available: http:///www.gao.gov

[18] AntiOnline (1998). Coverage of a chat with the Masters of Downloading (MoD) hackers group that attacked US DoD and NASA systems and claimed more attacks.

[19] Waltz, E. (1998). *Information Warfare principles and operations*. Artech House, Inc., Norwood, MA, USA. ISBN 0-89006-511-X.

[20] Bruno, L., Gareiss, R. (1999). *Cloak-and-Printer*. Data Communications. July 1999, p.14.

[21] A detailed discussion on vulnerability assessment and some of the tools used by vulnerability assessment teams can be found in Chapter IV, the article by Parker and Veltman .

[22] US National Research Council. (1999). *Trust in Cyberspace*. Washington DC, USA.