Information Assurance and the Information Society

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

About the Author

Eric (H.A.M.) Luiijf M.Sc.Eng. is a principal research consultant Telematics and Information Security at TNO-FEL in the Netherlands. He graduated at the Mathematical Department of the Technical University of Delft in 1975. He is currently involved in end-to-end information security and telecommunication R&D projects, ICT-standardisation, securing privacy in new ICT environments, Internet and Intranet security, and boundary protection devices. Eric is the TNO programme co-ordinator on information warfare/ information operations and information assurance.
He has published many articles and papers in the field of information security and telematics and has contributed to several Internet requests for comment (RFCs).

Mailing address: TNO Physics and Electronics Laboratory (TNO-FEL), P.O. Box 96864, 2509 JG, The Hague, The Netherlands; Phone: +31 70 374 0312; Fax: +31 70 374 0651; Email: luiijf@fel.tno.nl.

Descriptors

Information warfare, information operations, information security, information infrastructure, protection, cybercrime, hacking, information highway, information age, infrastructure convergence, information society, security services

EICAR Prodeedings 1999 Edited by Urs E. Gattiker, Lia Pedersen and Karsten Petersen

Information Assurance and the Information Society

Abstract

Society is on the verge of a new era: the information age. Economical changes, a new way of looking at services and new types of conflict are forecasted. Some glimpses of these changes were noticed during the Persian Gulf War. Government decision units, organisations, society and critical industries become more and more inter-networked. They rely heavily upon essential, global and converged infrastructures. Most of these infrastructures are controlled by complex information and communication technology. Society as a whole - and the "western society" in particular - depends heavily on information (global) infrastructures and should look carefully at the related threats.

This paper discusses "Information Assurance", the civil defence side of "Information Warfare", and the taxonomy of threat areas in the information age in the 21st century. Currently, governments, society and industry largely neglect these upcoming information warfare threats. The paper identifies current and forecasted issues to be discussed and dealt with by politicians, governments, society and industry.

Not so long ago, Cyber Warfare, automated shooters, smart ammunition and high energy power guns existed only in science fiction literature and movies like Star Wars. Nowadays, Information Warfare (IW) is a hot research topic. IW will be a major basis for military operations in 21st century conflicts, but casts its shadow already ahead. Although most information warfare concepts and doctrines are still in an embryonic phase, they are already part of real military operations (US Army, 1996; US JChoS, 1998).

Not only in the military cyberspace realm, but daily in our new information-age society people, organisations, agencies and governments are confronted with threats against, and vulnerabilities of our information infrastructure and information systems. At the same time, our daily economical life and our safety rely more and more on the integrity, availability and reliability of systems and infrastructures.

Currently, government decision units, organisations, society and critical industries become more and more inter-networked. They rely heavily upon essential, global and converged infrastructures. Most of these infrastructures are controlled by complex information and communication technology. Due to these converging information infrastructures and their globalisation, society is facing new global threats whilst defences are low. Klinefelder (1997) discusses many examples, including economic espionage by the Russian and French governments. Even worse, non-military organisations (NMO's), terrorist and action groups and other adversaries with a relatively low budget can raise many threats against the new information age societies (Staten, 1998). The combination of these factors makes our information society very vulnerable to economic espionage both by companies and other governments; action groups; terrorist groups; countries and other adversaries. When not already present as a real danger today, it will be tomorrow.

This requires a lot of research on identifying all vulnerabilities and on new ways for countering the threats efficiently and effectively. Before that, all involved in information and network security should become aware of the risks information warfare or "cyber warfare" might impose to the information systems and infrastructure they are supposed to protect. This paper aims to raise awareness about these issues by discussing the terminology and concepts of Information Warfare (IW) the emphasis on the non-military issues. This includes convergence of infrastructures and threats of using common-off-the-shelve (COTS) systems.

Unfortunately, despite the warning signals by hackers, trojan horses (e.g. Back Orifici and Netbus) and virii, power outages and broken fibres, the non-military information age society seems to be unable to comprehend the effects of the information age. There is an unwillingness to investigate and research its vulnerability and to take proper actions to counter the threats. Most politicians and governments avoid the discussion on how vulnerable our society already has become.

What should be done to raise the security barriers on the information highway and who should be in charge? The paper identifies issues for the 21st century and presents several recommendations for politicians, responsible government agencies and the information security research community as a course for action.

Introduction to Information Warfare (IW)

The first Information Warfare ideas were stimulated by several publications in the USA that are regarded now as IW-literature classics (Arquilla, 1993; Toffler, 1980; Toffler, 1993; Libicki, 1995). In these publications it is recognised that the so-called 'western society' is on the verge of the information age. Information has become a major source of power. The Tofflers state that major changes in economics, production factors and type of potential conflicts are taking place in our society. This analysis of possible future conflicts, which probably might be caused by disagreements over ideology and/or economical factors and the importance of information in these conflicts, resulted in the invention of the term "Information Warfare". Some initial Information Warfare-concepts were developed from these ideas and were taken into the field during the Persian Gulf war (Campen, 1992).

To clear some confusion about the term "Information Warfare", we first need to place the notion "information" in the flow from "data" to "wisdom". By observing the real world one collects either by automatic or other means "data" (measurements, sensing, simple facts). We extract information by correlating, aligning, sorting and indexing collected (raw) data, and eventually using earlier collected information as well. Input to this process is one's goal (Waltz, 1998).

Knowledge is obtained from information by applying processes like inference, induction, deduction and reasoning. Knowledge causes one to understand the meaning of information. Knowledge in itself is useless, unless it is used as "wisdom" for decision aiding and planning. Information Warfare concepts address all these aspects from raw data collection or disturbance to the use of knowledge. This both in offensive and defensive ways as well as making efficient and effective use of all available information.

As the term ”war” in “Information Warfare” is political sensitive in most countries, the less sensitive and better fitted term Information Operations (Info Ops) has been introduced lately (US Army, 1996). In a very short period, this term has been adopted by most countries as well as by the North Atlantic Treaty Organisation (NATO, 1998). Information operations comprise all activities that target information bases of an adversary, protect one’s own information assets and make efficient use of one’s own information. Information Operations is a military defined concept and doctrine (US Army, 1996; US JChoS, 1998), but interacts largely with society as the majority of the targets either attacked or to be defended by Information Operations means are not military but civil targets.

Currently, there are no world wide accepted definitions of the terms Information Operations and Information Warfare. For instance, in the United States each armed service developed its own definition of IW. Depending on the background of the specific military service and the political impact of a definition, different approaches are taken. Sometimes offensive aspects are not included in the definition, sometimes psychological warfare aspects are left out because of political sensitivity.

Looking at the Nolan curve for maturity of information technology (Nolan, 1979), the Information Warfare technology is still in its initial or 'dawn' phase. Using this curve, it will be clear that all those currently working on and studying information warfare just might have an initial feeling of the dawn of new conflict types. They do not and can not fully understand yet where (future) Information Warfare might take us. Real insight will only break through when the controlled phase of the Nolan curve is reached and even then, one still cannot understand well where technology may take us. For that reason, a globally accepted definition of Information Warfare and its derivatives can not be expected soon.

Nevertheless, there is an international drive towards more common and focused definitions. Information Operations is defined by (US JChoS, 1998) as "Actions taken affect adversary information and information systems while defending one's own information and information systems". Note that the term system in this definition includes communications and infrastructure. NATO will use a slightly adapted version of this definition. For political reasons, NATO makes a clear distinction between offensive and defensive Info Ops (NATO, 1998).

Information Warfare (IW) is nowadays defined as "Info Ops conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries" (US Army, 1996). Note however, that the term Information Warfare is still used at large as the overall librarian notion for this new technology and doctrine area.
Under this IW-at-large umbrella notion, many old and new terms and technologies are recognised: electronic warfare, information assurance, Information Operations, high energy radio frequency/ high power microwave/ non-nuclear electro-magnetic pulse (HERF/ HPM/ NNEMP) weapons, netwar, hacking, cyber attacks, Minimum Essential Information Infrastructure (MEII), intelligence-based warfare, psychological operations and cyber war, to name a few.

Libicki (1996) recognised seven different classes of Information Warfare:

- Command and Control warfare (C2W): offensively either going after the neck (command infrastructure) or the head (main command centre/decision makers);
- Intelligence Based Warfare (IBW): how to affect the adversaries information - knowledge cycle;
- Electronic Warfare (EW): deny the use of certain communication frequencies, inject false information and extract information for one's own purposes. Tempest measures protect equipment on one hand against radiation hazards and unwanted

radiation of information on the other. High Power Microwave aims to destroy electronics;
- Psychological Operations (PSYOPS), e.g. a hidden message in a picture or video concerted with other 'stimuli' to influence the adversary's mind with a 'convincing truth';
- Economic Information Warfare (EIW), includes economic blockade, intelligence gathering and economical espionage;
- Cyber Warfare (Net warfare), going after the information infrastructures and trying to influence the strategic assets and the political, economical and societal infrastructures;
- Hacking: techniques aimed at, e.g. extracting sensitive information from adversary's sources, stealthily modifying information or openly discrediting information in systems.

Another approach is by Schwartau (1996). He recognises three classes of information warfare: type 1 or personal information warfare, aimed at one's privacy; type 2 or corporate information warfare, the war between corporations, e.g. corporate espionage; and, type 3, global information warfare. This breakdown of information warfare is not used often in other studies, probably because the type 3 information warfare is currently the one which attracts most research.

When looking at the different type of information based conflicts that might occur following (Waltz, 1998), one should look at the who and why of potential adversaries. It is clear that the major emphasis in the high technology - physical conflicts lies with the military (information operations; command and control warfare). The Cyber terrorist - a premeditated, politically motivated subnational group or clandestine agent (Pollitt, 1998) - poses unconventional threats to a wide range of military and non-military targets, including the economical base (Fialka, 1997). Remarkably, although high-tech information technology is used, success in attacking critical information bases and infrastructures does not require major investments. Many quite helpful and sophisticated hacking tools can even be acquired for free from the Internet (Luiijf, 1998b). The chances of being detected are quite low as research by the US General Accounting Office indicates (GAO, 1996). The chances of being caught are even lower (GAO, 1996). Also, so called red teams demonstrate the vulnerability of large organisations (Behar, 1997).

The question "information warfare, what is new?" can be answered in two ways. First of all, the basic principles of all these warfare aspects have been well known for quite a long time. The sentences "The reason why the enlighted ruler and the wise general are able to conquer the enemy whenever they lead the army and can achieve victories that surpass those of others is because of foreknowledge" and "A military operation involves deception" were written long ago by Sun Tzu, a Chinese warrior-philosopher (Sun Tzu, c. 500 BC). Many more recent, pre-information age examples are available (Fogleman, 1995).
Nevertheless, 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 or even detection makes "information warfare" in principle quite attractive for individuals, economic adversaries, action and terrorist groups, cyber-mafia's (Rosé, 1998), unfriendly government agencies as well as other adversaries.

A major advantage for the virtual terrorist is that he/she does not need to approach, in time or place, to the system or infrastructure in attack. 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.

Information Assurance and Information Infrastructures

Observing the various information warfare definitions, one can conclude that most of these definitions only regard the strict military 'playing fields'. Sometimes for political reasons, but more often because one disregards different (defence) perks, e.g. in (GE Army, 1997). Most of the US papers on Information Warfare are written by officers graduating at officers schools. Their scope is often limited to the military environment, and although the identified threats are global, the topic is approached from a limited US world view. With information dominance and information supremacy, a form of total control, can be reached (Gray, 1997; US Army, 1996).
This limited view overlooks that information infrastructures are now global and are highly interconnected and interdependent of each other. In this respect, it is worth noticing that over 95% of the US military communication links make use of commercially leased lines and satellites (Hamre, 1998). During operation Desert Storm, this figure was even higher.

Where the military in various countries are looking now at Info Ops, they intend to overlook the defence of the government's emergency management assets as well. In many countries, the military are called upon during major natural or other disasters. For that reason, emergency management infrastructures should be regarded as (civil

defence) command and control assets as well when considering defensive Info Ops. Just because the US military is legally not allowed to operate in the US itself, causes these threats to overlooked by most (US) studies.

The vulnerabilities of the basic infrastructures were studied in Australia (Cobb, 1997), and by the US President's Commission on Critical Infrastructure Protection (PCCIP, 1997a; PCCIP, 1997b). These studies and their outcome, however, have not yet caused an approach where the information and communication technology (ICT)-infrastructure of the society is regarded as an asset to be protected by a joint military and civil defence policy and means. Below, the main findings of these studies are briefly outlined.

The PCCIP 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 vulnerabilities and threats were characterised as follows:

- 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 the 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.
- Increasing vulnerabilities:
  - *Classical threats* (e.g. dynamite, a truckload of fertiliser and diesel fuel) are among the likely threats to our infrastructures.
  - *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, and the perpetrator would be harder to identify and apprehend.
  - *System complexities and interdependencies*: The energy, and, in particular, communications infrastructures especially 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.
- A wide spectrum of threats: either aimed at causing substantial disruption in services or at destruction of the equipment used to provide services. Identified threats fall into the following categories: natural events and accidents, blunders, errors, and omissions, insiders, recreational hackers, criminal activity, industrial espionage, terrorism, national intelligence gathering by other countries and information warfare.
- Lack of awareness: most services are all taken for granted. Within government and among industry decision-makers, awareness of vulnerabilities is limited.
- Lack of national focus or advocacy for infrastructure protection.

The PCCIP concluded that infrastructures have always been attractive targets. Borders and friendly neighbours provided some protection in the past. Today, the evolution of cyber threats has changed the situation dramatically. In cyberspace, national borders are no longer relevant. Potentially serious cyber 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.

Disruption of the services on which economy and our well being depend could have significant effects, and, if repeated frequently, could seriously harm public confidence. Military and private infrastructures are becoming less and less separated. It is becoming more and more difficult to differentiate between threats from local criminals and foreign powers. The techniques of protection, mitigation, and restoration are largely the same. The PCCIP concluded that the responsibility for infrastructure protection and assurance can no longer be delegated on the basis of who the attacker is or where the attack originates. Rather, the responsibility should be shared co-operatively among all players.

The inter-relationships of infrastructures are 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. Most "western societies" use the same commercial-off-the-shelf equipment and systems in their infrastructure, in government, in organisations and industries. 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.

Recommendations by the PCCIP included: the establishment of an Information Analysis and Warning Center to catalog incidents of computer security breaches; the formation of a government-industry "framework to co-ordinate the security roles of the state, local governments and industry; and to quadruple the research on cyberspace security to 1 billion US$ a year by the year 2004. The Clinton Administration reacted soon (PDD63, 1998) and established the National Information Protection Center (NIPC). An interesting observation is that the Clinton Administration establishes a 'national' center chartered to address only 'national' territory (PDD63, 1988), where the PCCIP identified that the threats to the US and their allies are 'global' (PCCP, 1997a) and that there are no borders in cyberspace. Moreover, the NIPC is supposed to have an intelligence and countering role. The intelligence about cybercrime activities should be received from the public sector, government with exception of the military and FBI crime units. However, due to legal issues with respect to liability and anti-trust laws, the co-operation by the public sector is minimal. A lengthy process of changing laws is required before the NIPC could become a real counter unit (vanCleave, 1998).

Apart from the PCCIP study, we collected some examples of ICT-assets and vulnerabilities of our so-called "western" society (at large) and how society deals with them:

- All international phone traffic is switched via two exchanges in Sydney, Australia. The Australian inter-bank balances have to be settled each day in a 45 minutes' window with the Society for Worldwide Interbank Financial Telecommunications (SWIFT) in Brussels. This causes the Australian financial world to heavily rely upon international telephone lines, undersea cables and other communication infrastructures in order to reach Brussels and to start business each morning (Cobb, 1997).

- Klinefelder (1997) reported that the New York brokerage and trading houses alone pass US$ 1.9 trillion over their computer networks. The US Federal Reserve System transfers US$ 1 trillion per day. Cobb indicated that the SWIFT network transfers US$ 2500 billion between banks per day. Consider the amount of money your country spends yearly on the protection of critical infrastructures as a percentage of these figures. The outcome will have many zeroes after the comma. And, although important, the money exchanges play only a minor role when considering the total economic infrastructure of a country.

- Disruption by natural disasters, e.g. the Hansin Dai-Shinsai earthquake on January 17, 1995 with its epicentre near Kobe demonstrated the vulnerabilities of our ICT based society in another way. 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 (Noam, 1995). The same kind of lessons were learned during the last major earthquake in 1995 in the San Francisco bay area (Noam, 1995).

- On April 18, 1998, a large part of AT&T frame relay network in the USA went down for over a day due to a software failure. Over 6600 large businesses lost their IT-connectivity. Note that a prolonged ICT-down time of over 2 days might cause a bank or an airliner to go broke; a large insurance company might survive 5 days.

- 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 financial district). They also planned to place realistic 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 disruptions throughout the whole UK. It was estimated that it would have disrupted all power services in London for at least

1, probably 1.5 day. 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.

- Trying to obtain tickets for the 1998 World Cup soccer games in France on April 22, 1998, soccer fans caused the telephone networks in several European countries to collapse. In the Netherlands, 30 central office switches went down. For several hours no phone traffic was possible to or from Amsterdam, Rotterdam and Eindhoven. The emergency number 112 became unreachable. One mail order company alone claimed a loss of over 0.5 million US$. Newspapers stated that the French messed up. Nobody calculated the total economic loss. Neither newspapers nor governments drew conclusions on the infrastructure vulnerability problem. I concluded that 'Soccer is infrastructure warfare' (after Rinus Michels, former Netherlands soccer coach).

- 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 (Oakes, 1999).

- The Amsterdam Internet Exchange (AMS-IX) went down for several hours on December 26, 1998 due to an explosion in a power transformer. Effectively, the Netherlands was largely cut off of the Internet (Oonk, 1998). As this happened on a public holiday, hardly any businesses were affected. No government action has been noticed.

- Outsourcing causes information of many companies to be concentrated on one spot. The vulnerabilities and threats are regarded as a per company issue. That hackers or terrorists might go after the sensitive organisation that uses the same physical system is a threat companies that outsource their IT-operation do not take into account in their vulnerability analysis, if they do them at all.

From these examples it should be clear that government, society, organisations and critical industries need to prepare jointly for defending their assets in the information age. For the information protection of one's own assets, the term 'Information Assurance' has been introduced by the US Army (US Army, 1996). Information Assurance is defined as: "Information Operations that protect and defend information and information systems by ensuring their: availability, integrity, authentication, confidentiality and non-repudiation". I regard this definition inadequate for several reasons. First of all, it states a number of information security aspects but overlooks a number of them, e.g. reliability, safety, audit to name some. Secondly, this definition

largely neglects the civil infrastructures that are at stake as explained and demonstrated earlier.

Therefore, this paper proposes the following definition for Information Assurance: "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 infrastructures and services." This definition takes all civil information assets and infrastructures into account that are critical to a country or a coalition like the European Union and its friendly allies. Information assurance should not stop at the countries' border, or in case of an organisation at the border of one's own domain. It should be based upon mutually agreed treaties between neighbours in cyberspace. Neighbours in cyberspace can be countries or unions, but also intelligence services, service providers and infrastructure providers (power, telecommunications, etc.).

One can argue that the definition of Information Assurance should be stateless as the information highway crosses all country borders. However, currently the State or Union is the only organisation that can address the vulnerabilities of the information society to its broadest extend, from disruption of information highway based services to psychological information operations.

Surviving possible attacks, e.g., from virtual terrorists, for whatever ideological or other reasons, requires countries, governments and organisations to be prepared (Rathmell, 1997). Lack of awareness, security management and proper risk analysis causes a potential of high, unmanaged risks (Farmer, 1996; Luiijf, 1998a). The use of commercial-off-the-shelf systems and software increases the potential vulnerabilities of systems and infrastructures in case known exploitable vulnerabilities are not countered as soon as possible. As the (virtual) ICT world, the global connectivity and inter-networking cross many international borders, international co-operation will be essential to counter attacks. These attacks can be mounted using cheap means (Pollitt, 1998). The attacker has the advantage of being place and time independent from the target. The fact that military and emergency management communications partly or sometimes even largely rely upon civil infrastructures is of great concern.

As far as known from public sources, only a few European countries are executing studies like the US PCCIP did. Countries that are looking at information assurance and infrastructure protection are Germany (BSI/AG Kritis), Sweden and UK. One of these study groups reported that they hardly get support by industry and other government agencies.

Encryption technology might help to protect the integrity and confidentiality of information in this area. Problems are: key management, key exchange, unavailability of strong encryption in many countries, unclear or unsettled law enforcement policies as well as the trust in the technology itself. Key recovery for the organisations' ability to

use the information after a key is lost conflicts with secrecy goals. Very strong discussions on this topic are currently going on in many countries as well as in the European Union (EC, 1998). This discussion is fed by the continuous try to invalidate weak encryption key lengths by trying to break encryption challenges jointly over the Internet (RSA, 1998).

Discussion and Conclusion

Taking many security publications and reports by for instance the US FBI, the UK National Computer Centre, the Computer Security Institute and accountancy companies into account (Luiijf, 1998a; Luiijf, 1998b), a number of observations can be made:

Although information warfare is a real and growing threat to organisations, governments and society, the insider is still responsible for 60%-80% of the information security breaches (BISS, 1998). The attackers are helped by a lack of defences. Due to negligence and lack of security awareness, this is the main cause of successful attacks. The outsider can attack with the good help of public domain tools and good information available on Internet. Only stupid attackers are discovered as intrusion detection means are still immature.

With respect to information Assurance, most government agencies, public and civil organisations have sensitive systems and networks that have unlocked doors waiting to be opened by unauthorised people. In general one is 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 bad things that will happen.

The economic electronic intelligence gathering industry, either using ethical or non-ethical methods is growing fast. There are indications that obtaining financial advantages by using non-ethical economical attacks is growing given the low chance of detection (Fialka, 1997). Fraud and (organised) financial crime is reported to take place on the information highway, where crime organisations have found their way to go after the non-virtual money. Pay-off is high and detection chances are low. An advantage for the criminals is that there is no cyber police yet. (Rosé, 1998).

The energy radiation weapons are currently nations' tools, which eventually might fall into hands of organised crime and sub-nation groups. However, jamming transmitters which block GSM-telephone frequencies for distances up to hundreds of meters can be freely bought in Japan.

Although real virtual and cyber terrorists have not been signalled yet (Pollitt, 1998), society is very vulnerable as soon as the first politically motivated individual or terrorist group grabs the idea. The required means can be bought for a couple of thousand dollars. The knowledge and tools are on-line available and require only a limited in-sight and experience.

One can conclude, that given the current lack of awareness about the security of information, information systems and information infrastructures, our 'western' society should fear for the worst. A lot of research in countering information warfare threats

against our information, information based processes, systems and infrastructure is required.

Issues for the 21st Century

Issues for governments and politicians

Our "western society" infrastructures are ICT-dependent, are inter-networked and are highly vulnerable. Around 80%-90% of what one need to know to defend one's nation is nowadays in the private sector, out of government control. Fundamental changes in the approach to information assurance in the 21st century society are required. The national defence organisations are neither legally allowed nor provided with means, training and knowledge to counter cyber space attacks on non-military assets.
Actions are required on the following issues:

1) Most European governments are lacking awareness about the vulnerability of their own society. National repeats of the US PCCIP study are either not taking place or are hampered by lack of co-operation by other government agencies and industry. It is time for a European wide approach and commitment.

2) As the information society becomes more and more global, governments have to deal with global threats. How to deal with cyber space problems, as governments already have problems in dealing with the problems of today's society.

3) The role of the national security communities in the 21st century, given the threats of cyber and infrastructure terrorism, is unclear. The question on how to organise an international 'cyber' security service to fight cross-border threats needs to be answered. At the same time the roles and responsibilities of the private sector, government agencies and defence with respect to the critical infrastructures should be clarified.

4) One might expect either sooner or later the uprise of international cyber terrorism. Only the P8 Senior Level group on transnational organised crime (Lyon group) is developing some anti-cyber warfare capabilities (G7P8, 1996). Transnational support, however, 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 involves criminals, not terrorists. Countries need to develop policy, intelligence, multi-national support teams and effective counter means in order to be prepared for cyber terrorism attacks.

5) Emergency preparedness requires training and rehearsals. To be prepared for cyber attacks, regular training rehearsals should take place. As there is no 'cyber police', the question is who will write the scenario's? Another research question is about the number of rehearsals in cyber space (crossing national borders) that are necessary to be effectively trained.

6) Some organisations, agencies and governments actively use tiger or infiltration teams that try to break-in into their sensitive systems. Should all governments develop such capabilities? Should countries co-operate at a technical level? Should this continuous assessment include international infrastructures?

7) There is a lack of management attention and information security awareness in most organisations. How to start with awareness programs and organisation of information assurance that raise the security barriers in one's country information infrastructure as well as in the cross border infrastructures?

Issues for information security researchers

1) Hacking and phreaking are a reality in our information society. However, most of the hackers are recreational hackers. How can one tune intrusion detection tools to recognise the 'probing' spies, criminals and terrorists in the haystack of the background noise?

2) Intrusion detection is the second line of defence. Intrusion detection with a hostile information warfare environment as a threat requires many new advancements.

3) To know what part of an attacked system is still reliable might improve restoration time after loss of integrity many fold, especially now systems are moving to information bases of many terabytes.

References

Arquilla, J. and Ronfeldt, D.F. (1993). Cyberwar is Coming!, Comparative Strategy, Vol. 12, No. 2. [On-line] Available: http://gopher.well.sf.ca.us:70/0/Military/cyberwar

Behar, R. (1997, February 3). Who's reading your Email. Fortune, pp.29-36. [On-line] Availble: http://www.pathfinder.com/@@Yh7gigUAASAxSoj0/fortune/1997/970203/eml.html

BISS. (1998) BISS'98 report. United Kingdom: UK National Computer Center. [On-line] Available: http://www.ncc.co.uk

Campen, A.D. (Ed.) et al. (1992). The first information war: The story of communications, computers, and intelligence Systems in the Persian Gulf war. AFCEA International. Fairfax, VA, USA: AFCEA Press. ISBN 0916159248.

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

EC (1998). European Commission European expert hearing on digital signatures and encryption, Copenhagen, April 1998 [On-line] Available: http://www.fsk.dk/fsk/div/hearing

Farmer, D. (1996). Abstract: Shall we dust Moscow? Security survey of key Internet hosts & various semi-relevant reflections. [On-line] Available: http://www.trouble.org/survey/

Fialka (1997). War by other means. New York, USA: W.W. Norton.

Fogleman, R.R. (1995). Information Operations: The Fifth Dimension of Warfare. Defense Issues. Vol.10, No. 47, US Department of Defense, Washington, USA. [On-line] Available: http://www.defenselink.mil/speeches/1995/s19950425-fogleman.html

GE Army (1997). StreitKräfteEinsatz 2020 (SKE2020). Bundeswehr, Germany.

Gray, J.V. (1997). Information Operations: a research aid. IDA Document D-2082: Institute for Defense Analysis, Alexandria, Virginia, USA.

G7P8 (1996). Report on G7/P8 meeting in Lyon, France. [On-line] Available: http://insight.mcmaster.ca/org/efc/pages/doc/g7.html

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

Jackson, T. and Wilikens, M. (1998). Survivability of Networked Information Systems and Infrastructures. Joint Research Centre, Ispra, VA, Italy. [On-line] Available: http://ntsta.jrc.it/dsa/surviv.htm

Klinefelter, Col. S. (1997). The National Security Strategy and Information Warfare. U.S. Army War College, Carlisle Barracks, PA.

Libicki, M. (1995). What is Information Warfare?. Strategic Forum, No. 28. [On-line] Available: http://www.ndu.edu/inss/actpubs/act003/actpub.htm

Luiijf, H.A.M. (1998a). Information Assurance and the Information Society. In: Security services in the information society - Assets, cyber attacks and encryption. Berne, Switzerland: Club de Berne.

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

NATO (1998). NATO MCM-0969-98: NATO Info Ops concept. Brussels, Belgium: NATO Headquarters.

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://www.ctr.columbia.edu/vi/papers/citinoa6.htm

Nolan, R.L. (1979). Managing the crisis in data processing. Harvard Business Review, (3/4) pp. 115-126.

Oakes, C. (1999, January 4). Thieves hit phone center. Wirednews.

Oonk, P. (1998, December 26). Ontploffing in transformatorhuis legt grote delen van Nederlands Internet plat. Pine Security Digest. [On-line] Available: http://security.pine.nl

PCCIP (1997a). Critical Foundations: Protecting America's Infrastructures. Report 040-000-00699-1, Washington, D.C., USA: United States Government Printing Office (GPO). [On-line] Available: http://www.pccip.gov

PCCIP (1997b). Research and Development: Recommendations for Protecting and Assuring Critical National Infrastructures. Washington, D.C., USA: United States Government Printing Office (GPO). [On-line] Available: http://www.pccip.gov

PDD63 (1998), Presidential Directive 1998, number 63: Critical Infrastructure Protection Directive. Washington, D.C., USA United States Government Printing Office (GPO). [On-line] Available: http://www.ciao.org

Pollitt, M.M. (1998), Cyberterrorism, fact or fancy?. Computer Fraud & Security, (2) pp 8-10.: Elsevier Science Ltd.

Rathmell, Dr.A., Overill, Dr.R. , Valeri, L. , Gearson, Dr. J. (1997). The IW Threat from Sub-State Groups: an Interdisciplinary Approach. INSS/National Defense University, Norfolk, USA. [On-line] Available: *http://www.kcl.ac.uk/orgs/icsa/terrori.htm*

Rosé, Ph. (1998). Cyber-Mafias: Organised crime in information age. Paper presented at InfowarCon'98, Washington D.C., USA: MIS Training Institute.

RSA, (1998). RSA challenges. [On-line] Available: *http://www.rsa.com/rsalabs/html/challenges.html*

Schwartau, W. (1996). Information Warfare. Second edition. New York, USA: Thunder's Mouth Press. ISBN 1-56025-132-8.

Staten, C.L. (1998). Asymmetric Warfare, the evolution and devolution of terrorism; the coming challenge for emergency and national security. [On-line] Available: http://www.infowar.com/class_3/class3_043098a_j.html-ssi

Sun Tzu (c. 500 BC), The Art of War.

Toffler, A. and Toffler, H. (1980). The third wave. New York, USA: Bantam Books.

Toffler, A. and Toffler, H. (1993). War and anti-war: Survival at the dawn of the 21st century.. USA: Warner Books.

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

US GAO (1996). Information Security: Computer Attacks at Department of Defense Pose Increasing Risks, GAO Executive report B-266140. Washington, USA: United States Government Printing Office (GPO). [On-line] Available: http://www.infowar.com/CIVIL_DE/gaosum.html-ssi

US JChoS (1998). Joint Doctrine for Information Operations. Joint Pub JP 3-13. US Joint Chiefs of Staff. [On-line] Available PDF download: http://www.dtic.mil/doctrine/jel/c_pubs2.htm

vanCleave. Information Assurance: a view from the Hill. Keynote address presented at InfowarCon'98, Washington D.C., USA: MIS Training Institute.

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