EUROPEAN WORKSHOP ON INDUSTRIAL COMPUTER SYSTEMS

TECHNICAL COMMITTEE 7 RELIABILITY, SAFETY & SECURITY	Document Number: WP 5017/17 SEC
Plenary O Subgroup Curr O FM O MeD O MDS O RA O Sec X	Category: Workplan O Minutes O Technical X Review O Position Paper O External O
Author(s): EWICS TC7 Security Subgroup	Updates: - Replaces: WP 5017/16
Address: See the EWICS website www.ewics.org	Pages: 22 Restrictions: Members only O None X Date: July 2003
Title: Information Operations - Target, Means and Weapon - Version 1.0	
Contents / Abstract: -	

Acknowledgements:
This Briefing Paper was co-ordinated by Peter Daniel with major input from Eric Luiijf

BRIEFING PAPER

Information Operations
- Target, Means and Weapon -
Version 0.3 July 2003)

INDEX

1. INTRODUCTION 3

2. TECHNICAL DESCRIPTION 6

2.1 Background 6

2.2 Threats 7

2.3 Vulnerabilities 9

2.4 Countermeasures 9

3. INTERNATIONAL AND NATIONAL ASPECTS 11

3.1 USA 11

3.2 European and National Programmes 11

4. CONCLUSIONS 15

5. FURTHER INFORMATION 16

6. REFERENCES 19

7. ABBREVIATIONS 20

ANNEX A: INFORMATION WARFARE DEFINITIONS 22

1. INTRODUCTION

Continuity of critical national infrastructures is so important to national life that loss, significant interruption, or degradation of service would have life-threatening, serious economic or other grave social consequences for the community, or any substantial portion of the community, or would otherwise be of immediate concern to the government. Many safety critical systems form part of and/or have a high reliance on critical national infrastructures. For example, many safety critical systems use public networks to transfer information placing a high reliance on the communications infrastructure. National infrastructure elements include:

- Telecommunications
  - Network services(e.g. data, voice, fax, radio, Internet)
  - Network components (e.g. switches, links, satellites)
  - Remote access (e.g. monitoring, control, management)
- Energy generation and distribution systems (e.g. electrical power, gas, oil)
- Water management (e.g. drinking water, sewerage, storage & distribution)
- Emergency services (e.g. ambulance, fire service, police)
- Transport and logistics systems (e.g. navigational, traffic control, automated warehouses)
- Healthcare systems
- Financial systems
- Government administration systems & defence
- Food sector systems

Incidents have already occurred disabling or threatening services, which could affect safety critical systems, e.g. (see [Luiijf00a]):

- Early 2000, the sewerage system in Brisbane, Australia, regularly overflowed. Over a half a million litres of dirty water poured through the streets, and parks. A disgruntled former employee using a laptop was able to manipulate 300 Supervisory Control and Data Acquisition (SCADA) nodes, which monitored and controlled valves and sluices in the sewerage system.
- In 1999, all doors, at a nuclear power plant, closed into an emergency shutdown state. A guard uploading and playing a computer game on his personal computer in the guardhouse caused this.
- Over 14 days between April and May 2001, a hacker moved around in the California Independent System Operator networks responsible for electrical power distribution in California. Note that this happened during the period California was experiencing brownouts.
- In 2000, a small cable problem caused outage for over 19 hours of all computer services of two hospitals in the Netherlands.
- In July/August 2001, a computer failure caused outage for over a week of all payment systems (credit cards, automatic teller machines (ATMs)) on Malta.
- The Code Red virus in 2001 caused outage of ATM-systems in the UK as well as outage of 10.000's of British Telecom's DSL (Digital Subscriber line) lines due to contaminated controlling systems.

Information Warfare (IW) is being seen by some as the 21st Century method of waging war. The Information Age nations, among other countries are developing 'cyberspace weapons'. Information warriors, with PhDs in computer or electronic science and backed by foreign government aid, may soon be conducting sophisticated information operation attacks against company and government systems. Information Age countries are the most information and information systems dependent countries in the world, and thus, the most vulnerable. It is true they still have their industrial and agricultural sectors, but information and information systems are the life-support of these nations.

Information Operations (IO) is regarded by the military as a much wider concept than the narrow Information Warfare approach where the 'warrior' means are equivalent to hacking and electronic disturbances by e.g. electromagnetic pulses. Information Operations aims to go for the heart and minds of the opponent by attacking his information and information systems while defending and

using one's own information and information systems. This includes for instance aspects of psychological operations and public information provision as well.

Security and Information and Communication Technology (ICT) system managers within government agencies, and particularly in the military, will probably use the definition related to military hacking and electronic disturbance actions. Security and ICT-system managers within the private sector (assuming they were interested in even using the term information warfare) would probably align themselves closer to the definition more in use in the commercial sector. One may wonder if these private sector managers should be concerned about information warfare. As Information Operation actors may be (h)acktivists, state actors, and cyber terrorists, both private and public infrastructures/systems might be the most vulnerable assets of a country. For this reason, these managers should consider whether their operation might be a potential target. For example, an oil spill by a large multinational in a foreign country might trigger environmental hacktivists globally. Regardless, Information Operation will grow in importance as a factor to consider; much as viruses, hackers, and other current threats must be considered. Many, including those in the private sector, believe that the term information warfare goes far beyond the military-oriented definition. Some others have a broader definition of Information Warfare, which includes hackers attacking business systems, governments attacking businesses, even hackers attacking other hackers.

Cyberwar is a popular term, on the civil side, covering the collection of, the efficient use of information including, computers and networks, and the means to suppress (i.e. offensive) the same to an adversary in support of one's purposes and goals. This covers not only military but also a company undertaking information collection to enhance its market share or an activist group doing electronic sit-in and denying other's access.

Information Assurance (IA) is a new term in this field which covers actions taken to protect the nation, 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. IA assures the integrity and availability of information over the entire range of potential disruptions from accidental to malicious. ICT-systems are designed for optimal performance, leaving little time to process integrity of results at each stage and time to recover from failure. A combination which provides little redundancy to assure integrity and availability. IA relates to all information and information systems as opposed to issues, which solely relate to confidential information in terms of use rather than content and corruption, denial, correctness rather than leakage. Even fault-tolerant systems do not address IA.

The information age has brought with it more international businesses and more international commercial joint projects against more international competitors. This has resulted in more opportunities to steal vital information from partners where, for example, a partner in one project may be competing on another project. Furthermore, because of global commercial competition, the world power of a country is now largely determined by its economic power so, in reality, being in the midst of this global competition called by many the economic war. The new information technologies being implemented as modern information infrastructure determine the effectiveness of a country's economy. At the same time, all this technology makes the life fundamentals – power stations and transport systems – very sensitive to any destructive influence targeting the information infrastructure. Information Warfare gives opportunities to put out of action all highly technological infrastructures.

This global competition, coupled with international networks and telecommunications links, has provided more opportunities for more people, such as hackers, phreakers, crackers, to steal information through these networks. The end of the 'Cold War' in the early 90's has made 'ex-spies' available to continue to practice their tradecraft, but in a commercial environment. This new global environment makes a corporation's proprietary information even more valuable. Proprietary information is all forms and types of financial, scientific, technical, economic, or engineering

information including but not limited to data, plans, tools, mechanisms, compounds, formulas, designs, prototypes, processes, programs, codes or commercial strategies, whether tangible, or intangible and whether stored, compiled or memorised physically, electronically, graphically, photographically or in writing.

When organisations fail to adequately protect their information, they are taking risks that will, in all probability, cause them to lose market share, profits, business, and also help in weakening the economic power and social stability of their country. For that reason, business and government share a responsibility to protect information in this information age of global business. Businesses must identify what needs protection; determine the risks to their information, processes, products etc.; and develop, implement, and maintain a cost-effective security programme. Government agencies must understand that what national and international businesses do impacts their country. They must define and understand their responsibilities to defend against such threats, and they must formulate and implement plans that will assist their nation in the protection of its economy and the unobstructed functioning of their society. Both business and government must work together as only through understanding, communicating and co-operation will they be able to assist their country in the world economic competition.

On the one hand, the current threat to individual computer systems is up to very high. For instance, the increase in economic espionage is also largely due to organisation's vulnerabilities to such threats. Organisations do not adequately identify and protect their information, nor do they adequately protect their computer and telecommunications systems. They do not have adequate security policies and procedures; employees are not aware of their responsibilities to protect their organisation's proprietary information. Many of the employees and their management do not believe they have any information worth stealing or believe 'it can't happen here'. Neither is protection against external tempering with and disruption of information processes a high priority in most organisations.

On the other hand, the risks to the classical national infrastructures are perceived to be low by historically developed protection measures. However, the risks are fast growing because of the increasing reliance on telematics and remote control with multi-integration of functions. Concern is about attacks sufficiently sustained, skilled and determined as to pose a threat to the nation. All systems fail occasionally, hence the need for business continuity plans but consequences on the critical national infrastructures could go beyond the scope of normal organisational planning due to interdependence of various essential infrastructures.

Current terrorist targets have included electrical power systems, transportation systems, citizens, buildings, and government officials. Today's terrorists are not only using technology to communicate and technology crimes to fund their activities, but also beginning to look at the potential for using technology in the form of Information Operation against their enemies. It is estimated that this will increase in the future. Because today's technology-oriented nations rely on vulnerable computers and telecommunications systems to support their commercial and government operations, it is becoming a concern to global private and government organisations. The advantage to the terrorist of attacking these systems is that the techno-terrorists' acts can be done with little expense by few people and cause a great deal of damage to the economy and trust-bases of a nation. For that reason the protection of the critical national infrastructures, and moreover, the critical national information-infrastructure(s), have become a key action in most information age countries. For this reason, the protection of safety critical systems is becoming to get a high priority and the reason for producing this document.

2. TECHNICAL DESCRIPTION

2.1 Background

The main aspects of definitions of Information Warfare/Information Operation (Annex A) are:

Offensive: Deny, corrupt, destroy, or exploit an adversary's information, or influence the adversary's perception.

Defensive: Safeguard ourselves and allies from similar actions also known as 'Information Warfare hardening' and establish consequences by laws concerning punishment, fine and compensation.

Exploitative: Exploit available information in a timely fashion, in order to enhance our decision/action cycle and disrupt the adversary's cycle.

Parts of Information Operation/Information Warfare can be seen as being a factor in threats to information and telecommunications systems. Proper protection should include the critical (information) infrastructures of a nation, which is either publicly or privately owned or may be a hybrid, as these infrastructures provide services vital to other systems that their incapacity, disruption, or destruction could have a detrimental impact on the safety of these systems. Areas of concern are:

- Many infrastructure elements or their components are privately owned and operated by many providers;
- Reliance on automation of vital processes is increasing;
- Systems are increasingly interconnected, including via the Internet;
- Tools to compromise a system are widely available not requiring a high degree of technical skill;
- Infrastructures are becoming global increasing potential compromise;
- Infrastructures converge and are interconnected making complex structures (e.g. telephone network, mobile phone network, internet, telemetry, control signals, automatic teller machines);
- Multiple service providers as well as a manifold of services using common infrastructure components (e.g. fibre links);
- Use of 'standard' or so-called commercial-off-the-shelf (COTS) components (e.g. operating systems, hardware, communications equipment and services) with a fast decreasing 'bio-diversity';
- Many intrusions are not reported;
- Increasing complexity that is wholly comprehended by only a few people, if understood at all;
- Maintaining the correct security posture by overloaded system managers is a burden.
- Infrastructure elements are increasingly reliant on Information and Communication Technology (ICT) systems, which must have high dependability requirements including reliability, security (i.e. confidentiality, integrity, availability, audit, non-repudiation), safety and survivability.

Existing infrastructure elements have well known and easily exploited vulnerabilities. But even if these were dealt with, they would not necessarily provide information assurance when interconnected. It is by no means implied that the interconnected combination of two systems, each being perfectly protected against disruptions and attacks, is properly secured. In general, this will not be the case as there is no tried and tested approach of how to interconnect network components. When combining Information Assurance elements one needs to consider issues including:

- such elements need to be properly combined,
- enhancing protection is limited to the weakest link,
- presently not a well understood or researched subject.

The architects of infrastructure (and the elements) need to understand the threat and risk issues and find appropriate solutions for it using risk management approaches. The requirements should be defined in the relevant security policy (i.e. intra-infrastructure, inter-infrastructure). The security technology employed (e.g. firewalls, cryptographically protected communication, redundant links) should be enhanced with procedures for incident handling and mechanisms for intrusion detection.

A suitable risk analysis process could be based on that defined by the company MITRE as assessing the boundaries of the minimum essential information infrastructure (MEII):

- Determine what information functions are essential to successful execution of mission;
- Determine what information systems are essential to accomplish those missions;
- For each system identify vulnerabilities to expected threats;
- Identify security techniques that can mitigate each vulnerability and investigate the priorities and interactions between the safety and security measures and resolve any conflicts.

Because of the convergence of infrastructures, intertwining and complexity that is driven by the market, such a risk analysis cannot be done only once, but to remain current, is impossible because of the multiple layers of dependency:

- ICT provider(s), e.g. virtual private network,
- ICT base service provider(s), e.g. telecommunication company leased line,
- ICT based backbone network(s), e.g. high-speed switching networks of companies like BT, MCI etc.,
- physical infrastructure(s), e.g. communication links, Telehouses, Data Hotels,
- owner grid underlying ICT-operations (self generated).

A *threat* is a potential action or event that would trigger one or more impacts rendering the systems and infrastructures insecure, unsafe and/or unreliable. *Vulnerabilities* in the infrastructure IT components can be exploited by various threats through deliberate attacks, technical failures and accidental human errors, compromising these components with the risk that the impact on the system could be disastrous. *Countermeasures* are procedures or mechanisms, which protect the system (component) or infrastructure by reducing one or more elements of risk or detecting an impact or threat occurrence or recovering from an impact. This will be described in the next paragraphs (2.2 – 2.4).

2.2 Threats

The first stage of protection should be a threat analysis, the elements of which are:

- Potential objects of attack
- Who or what might present a threat?
- Capability (e.g. What are they able to do and their skills, knowledge, resources, equipment)
- Intent:
  - What do they want to achieve?
  - How determined are they?
  - How are they likely to go about it?
  - How ruthless will they be?
- What kind of reward is possible (e.g. insurance, compensation)?

Threat Agents

Sources of unintentional threats include natural catastrophes (e. g. earthquakes, storms), biological (e.g. fungi, animals) and natural effects (e. g. corrosion, degradation, wear-and-tear)
Sources of intentional threats include:

- Employees – do not underestimate the insider threat!
- Recreational and institutional hackers
- Information investigators and brokers
- Criminals including international crime syndicates
- Information bandits collecting information for resale
- Activists
- Dissidents and terrorists
- Spies – including commercial competitors
- State sponsored and private intelligence agencies

Reasons include:
- Incompetence, negligence, laziness of own employees
- Lack of training
- Work around (e.g. turn off due to too many false alarms)
- Curiosity of 'hackers'
- Hunger of animals
- Fraud
- Blackmail
- Dissatisfaction
- Mischief
- Revenge (e.g. disgruntled employee)
- Sabotage
- Impairment (e.g. psychological, physical)
- Psychopathic
- Espionage (e.g. obtaining intelligence)
- Self-Advancement (e.g. publicity seeking, action groups)
- Terrorism
- Information Superiority (military or commercial)

Incidents

Incidents could be caused through either intentional or unintentional events. Examples of unintentional incidents that could be exploited are:
- Errors and Omissions (e.g. management, operators, developers, installers, documentation);
- Inappropriate training / supervision;
- Environmental/nature (e.g. flood, earthquakes, high/low temperatures, chemical contamination, missile, dust, vibration, plague);
- Relocating equipment;
- Inadequate Maintenance;
- Technical failures;
- Supporting infrastructure failures (e.g. power failures).

Example of intentional or malicious events include:

Illegal information extraction:
- Infrastructure monitoring (e.g. line tapping)
- Network monitoring (e.g. watching, sniffing, grabbing, war driving);
- Tapping of electromagnetic emanations (Van Eck bugging);
- Monitoring disposals/dumpster diving;

Attack Methods:
- Spoofing, masquerading and fictitious users (e.g. obtaining free services);
- Software attacks (e.g. Trojan Horses, time & logic bombs, e-mail, viruses, worms);
- Software and hardware backdoor/trapdoor insertion and use (including chipping);
- Infrastructure interference (e.g. denial of service, sabotage by disgruntled or striking employees);
- Human/social engineering, in- and outsider jobs;
- Network tampering (e.g. packet insertion, modifying, war dialling, war driving);
- Private Automated Branch Exchange (PABX) hacking/bugging;
- Electronic interference e.g. (jamming, electromagnetic interference, electromagnetic compatibility, electromagnetic pulse);
- Process bypassing;
- Re-routing (e.g. Call Forwarding forgery);
- Using network vulnerabilities (e.g. vulnerability scanning, insertion of exploitable code);
- Theft (e.g. equipment theft, back-up theft));
- Physical disruption;
- Physical destruction.

2.3 Vulnerabilities

Vulnerabilities of a system are internal weak points which can be in the design/architecture of the system and can be exploited through the complexity, scalability, flexibility, operation, configuration, accessibility and the supporting facilities. Design and architecture vulnerabilities cover single points of failure and replication of flaws in multiple identical modules. Complexity issues include sensitivity to variations in user input and predictability of external behaviour. Flexibility entails security issues like ease of modification and maintenance. Operation and configuration issues include vulnerabilities to denial of service attacks through lack of capacity and recoverability after an attack. Accessibility includes physical access, logical access especially in remote access and access to system information. Supporting facilities include power, heating, water, air-conditioning and communications.

2.4 Countermeasures

Countermeasures can be grouped into technical, personnel, physical, procedural, legal and compensation measures and can be classified according to protection, detection and reaction measures. If, apart from protection against unintentional disruptions, we want to protect against deliberate (information operations) attacks, the security manager must be comprehensive and proactive. Now, as in the past, the basic triad of information security processes are usually installed (i.e. individual accountability, access control, audit trail systems). This 'passive defence' kept the honest user honest, but it didn't do much to stop the more computer-literate attacker. We can no longer afford such an approach and would be remiss in our responsibilities if we did not start looking at how to 'information warfare'-harden our systems. This means to provide a defensive shield, early-warning, and a countermeasures system to protect our government and business information infrastructures in the event of Information Warfare-type attacks in addition to the protection against all non-Information Warfare types of threat. Issues on security measures to be considered which are different from the approach to safety include:

- Restricting access to information on security measures
- Different measures used dynamically
- Persons or measures used for surveillance changed from time to time
- Stimulation of an attack for trapping an attacker
- Restricting access to information on impact of an attack.

To provide for information system defence, an aggressive programme must be implemented. We know our systems are vulnerable to attacks. We all know what hackers have done to our systems. Now, imagine what damage can be done by professionally educated and trained information bandits which have the full support of a foreign government, millions of dollars to support their efforts.

As noted earlier, assuming the dependence of the information age nation's military on the commercial telecommunications infrastructure, as well as on commercial power grids, transportation systems, etc., the first attack against an information age nation, or a prelude to that attack, may come in the form of system outages. How does the security manager differentiate between accidents, acts of nature, or man-made attacks? In addition to national security concerns on infrastructures, is the reliance of commercial organisations on commercial infrastructure services. Using a contract with a service provider together with a back-up contract with an alternative service provider, ensures two alternative connection routes. But the initial service provider could also lease capacity from the alternative service provider again or use the same ditch for infrastructure provision a couple of kilometres further down the road resulting in an unknown single point of failure until Murphy's law happens again ("If anything can go wrong it will").

In the information systems business, that trend also continues and may be increasing – microprocessors manufactured in one country, software written in another country, systems integrated and shipped from another country. No one checks or is even able to determine if malicious code is embedded in the firmware or software waiting for the right sequence of events to be activated, to release that new, devastating virus, to re-route information covertly to our adversary. Consideration must be given to networking with other security managers to establish an Information Warfare early-warning network, as well as to share Information Warfare-Defensive and Information Warfare-Countermeasures information. This can be equated somewhat with the early warning radar site that the military has scattered through our sphere of influence. These systems are to alert us to impending attacks.

An information system defence programme needs to include:
- Protecting systems according to best-practice standards similar British Standard BS7799:2000/ ISO/IEC 17799:2000;
- Defence-in-depth – separate domains, distributed systems, duplicated communications;
- Detection – Firewalls, fraud engines, intrusion detection systems;
- Refining threat indications and warnings – from detection statistics;
- Consistency;
- Beside the operative organisation with security duties and functions, a separate organisation has to be like a security company or state organisation, especially for surveillance and auditing;
- Involving law and security agencies (e.g. police);
- Neutralisation of potential attackers;
- Contingency strategies.

An important part of defences is the management of information security, where the international best-practice standard for information system security ISO/IEC 17799 was produced in 2000. This standard is fitting for common business systems, but does not fully cover the need for distributed processes, industrial computing systems, and remote measuring and control as used in for instance transportation systems. EWICS TC7 has produced a briefing paper on information security management that is available through its web page (www.ewics.org).

Information Security Policies define the requirements for protection of information systems covering;
- confidentiality (protection against leakage),
- integrity (protection against corruption/unauthorised modification),
- availability (protecting against denial-of-service as well as timeliness).

However, in practice implementations of such policies do not place enough emphasis on the information assurance aspects. Telecommunications and distributed systems need multi-layer approaches and the impact of areas not under one's own control need to be considered**.** Security is a dynamic process with risk analysis and security audits being undertaken on a regular basis.

Early warning measures should be implemented – which includes activities on:
- Intelligence on potential attackers;
- Detection of reconnaissance and other preparations;
- Try trace-back to perpetrator;
- Recognition of attacks;
- Immediate response.

3. INTERNATIONAL AND NATIONAL ASPECTS

3.1 USA

The US Presidential Decision Directive 63 [PDD63] by the Clinton administration in reaction to the President's Commission on Critical Infrastructure Protection (PCCIP-report [PCCIP97]):

- sets a goal of a secure information system infrastructure by 2003 and increased government security by 2000,
- requires federal agencies to serve as a model in reducing cyber and physical infrastructure vulnerabilities,
- seeks participation of private industry,
- sets up a new structure to deal with this challenge.

In 2002, the Bush administration issued a National Strategy to Secure Cyberspace which stresses these issues further and present a manifold of lines of action.

InfraGard is a US pilot project, developed by the US Federal Bureau of Investigation (FBI) Cleveland to increase information sharing, promoting the government alliance with the private sector. It provides a mechanism for system owners and operators to communicate with colleagues to improve the dissemination of security information. Its primary features are:

- Intrusion alert network,
- Secure web site,
- Chapter committees dedicated to concerns of membership,
- Seminars and training,
- Meetings with colleagues.

The membership is representatives from private industry, government agencies, academic institutions, state and local law enforcement. The membership requirements are a membership agreement, confidentiality pledge and a commitment to actively participate.

The National Infrastructure Protection Center (NIPC) mission is to detect, deter, prevent, warn of, assess, respond to, and investigate unlawful acts that threaten critical infrastructures addressing both physical and cyber attacks. NIPC is composed of multiple government agencies, federal, state, and local law enforcement as well as private sector representatives.

3.2 European and National Programmes

In 2002, the European Council and several other countries accepted the European Cybercrime convention which intend to harmonise the national computer crime legislation giving a basis for mutual assistance in stopping and resolving cybercrimes. Most European nations have now dedicated computer crime units with a 24/7-manned international assistance contact point. Also, European nations have put in place initiatives on protecting critical national infrastructures with the European Commission (EC) proposing a common approach in the area of network and information security [EC2002], [EU2002]. The European Dependability Development Support Initiative (DDSI) supports the development of dependability policies across Europe and across sectorial boundaries. It establishes networks of interest, provides baseline data and develops policy roadmaps.

In Austria, Department II/16-ITB, in the Ministry of the Interior set up in 1999 has a contact e-mail address to send information about possible criminal activities. Austria signed the Council of Europe Cybercrime convention on 23rd November 2001. An IT Security Handbook for public administration has been released. The first part deals with IT security management, the second part looks at IT security measures and the third part detailing a checklist of IT controls will be soon released.

In Denmark, the IT-sikkerhedsrådet oversees the critical information infrastructure. The National Centre of Investigative Support within the National Police Commissioner's Office has an IT-support unit, which handles all IT-related crime. The Danish Government IT Security Council was created in 1995 which produces an annual report on the status of ICT-security in Denmark. Recently it produced a report on Internet vulnerability. The Council's mandate expired this year and the government is considering the expansion of the mandate. The Danish Computer Emergency Response Team (DK-CERT) was established in 1991.

An agency in Finland under the Ministry of Transport and Communications (FICORA) is a general administrative authority for issues concerning electronic communications and information society services. FICORA has duties concerning protection of privacy and data security in electronic communications and is involved in communications security work. FICORA checks telecommunications operators for compliance to the relevant security acts and ensures they are prepared for emergencies. The Ministry of Finance established the government's IT-security board (VAHTI) ten years ago to co-ordinate IT-security work within government. The National Bureau of Investigation combats international cyber-crimes and the Security Police are responsible for preventing cyber-crimes and carries out technical security checks. Finland also has its Computer Emergency Response Team (CERT-FI). The Finnish Information Society Centre (TIEKE) is a meeting point for public and private information society developers.

In 2000, the French Central Office for the Fight Against Hi-Tech Crime was launched. It is linked to the French Ministry of Interior and co-operates with Interpol. Similarly, in 2000, a new Central Direction for Security of Information Systems (DCSSI) was created linked to the General Secretary of National Defence (SGDN). The strategy of the Security of Information Systems (SSI) involves two levels. First DCSSI contributes to the SSI Inter-Ministerial Committee and provides expertise to the public and private sector. It also has a training centre for administration staff. Secondly, it co-ordinates activities among government administrations. France has three Computer Emergency Response Teams; CERT-RENATER dedicated to the National Network of Telecommunications for Technology, Education and Research, CERT-A dedicated to the French administration sector and CERT-IST for the private sector.

In November 2000, the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI), an agency within the portfolio of the Federal Ministry of Interior established the programme of action "KRITIS" (Kritische Infrastrukturen). This initiative comprises several projects with the goal to conceptually plan a warn and report system for threats of ICT-systems within the critical structure areas of Germany as well as edit a compendium with recognised safeguards for ICT-security critical environments. After the event of September 11, a special project group within the German Federal Ministry of Interior was implemented. A special staff (Sonderstab) was set up with representatives of concerned ministries, agencies and critical infrastructures. A working group on the protection of infrastructures (Arbeitskreis sichere Infrastrukturen AKSIS, www.aksis.de) supports the activities.

In Italy, there exist mainly three laws regulating the legislation on Information Security. The Legislative Decrees D. Lgs. 29/12/1992, n. 518, which was modified by the copyright Law n. 633/1941, introduced specific regulation on computer programs. The Law 23/12/1993, n. 547 introduces the notion of computer crime into the Italian penal code. The Law 31/12/1996, n. 675 regulates the handling of personal data. This law has been further integrated by the Presidential Decree DPR 28/7/1999, n. 318, establishing the essential security criteria on personal data handling and storage. Other laws regulate the usage of IT within the Italian Public Administration. The main aim of some IT laws has been to support modernisation (related to major IT usage) within the Public Administration. There is still a lack of standardise level of protection for the different Information Infrastructures. Most of the effort has been devoted towards IT initiatives, like the FSI (Forum per la Società dell Informazione) and the E-government initiative. The main initiative aimed at tackling

cybercrime is the Law 1/4/1981 n.121 (re-organisation of the Interior Ministry, Public Security Dept.). It assigns to the Public Security Department the task of co-ordinating both the police forces and their data handling, specifying in which bodies data can be collected, handled and legally accessed both at national and international level.

The governmental organisations related to Information Security include:

- the AIPA (Autorità per l'informatica nella Pubblica Amministrazione, the public authority that oversees the diffusion of ICT within the public administration);
- the RUPA Technical Centre, which supervises service provision contracts and defines and executes ICT public programmes.

Italian non-governmental organisations related to Information Security include:

- The CERT-IT (The Italian Computer Emergency Response Team) founded in February 1994. The CERT-IT is a non-profit organisation mainly supported by the Department of Computer Science of the University of Milan. CERT-IT became a member of the International Forum of Incident Response and Security Teams (FIRST) in 1995, as the first Italian CERT to be admitted. The main goal of CERT-IT is to contribute to the development of security culture in the computer world, in particular the Italian computer world.

- The CLUSIT (Associazione Italiana per la Sicurezza Informatica) is a non-profit association founded on 4 July 2000. CLUSIT aims to be a rallying point for all national IT security stakeholders, encompassing the legal social and technological dimensions of the problem.

- The ANASIN (Associazione nazionale delle aziende di servizi di informatica e telematica) founded on 18 July 2000 represents IT industry (e.g., software industry, telecommunication industry, etc.). It is a founder member of the EISA (European IT Services Association), founder of the FEDERCOMIN (Federazione delle Imprese delle Comunicazioni e dell'Informatica) and member of the FITA (Federazione Italiana Industrie e Servizi Professionali e del Terziario Avanzato). The ANASIN is involved in many projects in collaboration with the Interior Ministry, the Public Function ministry and AIPA.

An initial essay study “In Bits and Pieces” [Luiijf00b] on the vulnerability of critical information-infrastructures in The Netherlands was prepared for Infodrome, a project by the Dutch government that tried to identify government policy issues caused by ICT developments impacting society. A vulnerability study (KWINT) of (the Netherlands part of) the Internet was completed by early 2001 [Till/Luiijf01]. The Dutch cabinet decided for a number of actions according to the KWINT-memorandum including free distribution of the Dutch translation of ISO/IEC 17799:2000 “Code voor Informatiebeveiliging”, transparency of performance and security statistics by Internet service providers (ISPs), and the establishment of a Computer Emergency Response Team for the government constituency (CERT-RO, since June 2002) co-located with a virus/malware information and warning centre (by December 2002) for the public and small and medium enterprises (SMEs).

CERT POLSKA is the official name of the Polish Computer Emergency Response Team since January 2001. It was formerly known as CERT NASK. Since February 1997 CERT POLSKA has been a full member of the worldwide Forum of Incident Response and Security Teams (FIRST). CERT NASK was established in March 1996 according to the disposition of the NASK (Naukowa i Akademicka Siec Komputerowa, Research and Academic Network in Poland) Director. Current CERT POLSKA headquarters is located at the NASK site in Warsaw. Its team consists of people employed in NASK supported by experts from Polish universities. Information related to network and computer security can be obtained from the official CERT POLSKA website. Services to its constituency:

- CERT POLSKA team registers any request, alert, incoming and outgoing information and provides statistical data and reports on registered incidents (e.g. number and types of attacks);

- provides help for sites which have security problems on the level specified by those sites (technical help, advise, consultation);
- gives current information about security problems and their solution (currently Web server, "nask-info" mailing list, in future dedicated mailing list) and sends several categories of direct e-mail (plain or using Pretty Good Privacy - PGP) in case of issuing security alerts, warnings and information to constituency (fax and phone is also in use).

In Norway, the government has established a centre for the study on vulnerability and protection of the national information infrastructure (Senter for informasjonssikring, SIS). It is established as a three-year project, running from 01.04.2002. The objective of the project is to establish a centre that can be the responsible for the national coordination with respect to reporting of incidents, warnings, analysis and exchange of experiences. The establishment was in accordance with the recommendations from the "Vulnerability-committee" (NOU 2000:24). The main tasks of SIS are to:

(1) get a complete picture of the threats against Norwegian information infrastructure,
(2) exchange information, competence and knowledge about threats and possible treatments,
(3) to maintain contact and co-operation with organisations in other countries.

The centre will not have any authority role. From 2003 the government has also proposed a re-organising of the military, establishing a Norwegian Defence Logistics Organisation. They will be supported by the Defence Research Institute (Forsvarets forskningsinstitutt, FFI). Their R&D is organised within eight programmes, one of which is on information warfare. The warning-system for digital infrastructure, VDI, is a joint venture between the Norwegian intelligence and security services, and private business and operators for mapping the extent of the threat to vulnerable digital infrastructures. The Norwegian academic network for research and education established the Norwegian Computer Emergency Response Team (UNINETT CERT) in 1995.

In Sweden, an Information Operations Defensive (IO-D) initiative with over 30 organisations (e.g. the ministry of trade, ministry of defence, broadcasting companies, banks, police), prepared a reactive capability for the government in case the Swedish information-infrastructure is attacked. In July 2002, the Swedish Emergency Management Agency (SEMA) was established which has the task to maintain the protection of all critical infrastructures, including the information-infrastructures. In addition there is an information security organisation within the Swedish National Post and Telecom Agency (PTS).

In 1998, the Federal Council defined its 'Strategy for the Information Society Switzerland' where security and availability are one of the strategy's eight fields of activity. Two years later the Swiss Federal Council released its new security policy. In the same year, the key policy document 'Concept Information Assurance' with three pillars was published. Firstly, the Federal Strategy Unit for Information Technology (FSUIT) has developed a concept for a crisis management system involving a 'Permanent Analysis and Reporting Centre' and an 'Information Assurance Task Force'. The second pillar is the unit 'ICT infrastructure' part of the Federal Office for National Economic Supply (NES) and the third pillar is InfoSurance, an IA initiative by industry and public organisations. A number of bodies in the public sector deal with IA, the main ones being FSUIT and the Division for Information Security and Faculty Protection (DISFP) reporting to the Federal Department of Defence. There are government sponsored Computer Emergency Response Teams (e.g. SWITCH-CERT) and commercial (e.g. Nextra) CERTs.

In the UK, the National Infrastructure Security Co-ordination Centre (NISCC) has been formed as part of the implementation of government policy for the protection of the National Infrastructure against electronic and information attacks. Its mission is to develop the UK's preparedness to deal with major electronic attack incidents should they arise. The NISCC will co-ordinate and develop existing work in a number of government departments and agencies, and in the private sector. This will include developing arrangements to monitor and increase awareness of the threat, to defend against it, and to react to actual attacks. For organisations external to government, it provides a first point of contact on Critical National Infrastructure (CNI) issues. It incorporates the UK Government Computer

Emergency Response Team and the existing CNI electronic attack response group arrangements. The NISCC includes the unified reporting and alerting scheme (UNIRAS), which is the UK government Computer Emergency Response Team. The Government Security Co-ordinating Centre (GOSCC) is responsible for the security of the UK government intranet. The Information Assurance Advisory Council (IAAC) is an initiative by Kings College, London and is a meeting place between mainly industry and academia.

4. CONCLUSIONS

Many safety critical systems form part of and/or have a high reliance on critical national infrastructures where incidents, seen by some as 21st Century method of waging war, have already been reported. These critical infrastructures, which are either publicly or privately owned or may be a hybrid, should be protected, as these infrastructures provide services vital to other systems that their incapacity, disruption, or destruction could have a detrimental impact on the safety of these systems.

As well as the risks rapidly increasing, so is the growing reliance for safety critical systems on telematics and remote control with multi-integration of functions. Techno-terrorist acts can be done with little expense by few people and cause a great deal of damage to the economy and trust-bases of a nation. Also, there are professionally educated and trained information bandits who could have the full support of a foreign government, millions of dollars to support their efforts. For this reason, the protection of the critical national information infrastructures have become a key action in most information age countries and critical infrastructure protection programmes have been set up providing information on threats and vulnerabilities.

Private organisations and government share a responsibility to protect these critical infrastructures. Organisations must identify information and information systems needing protection; determine the risks and develop, implement, and maintain a cost-effective security programme. Government must define and understand their responsibilities to defend against such threats, and they must formulate and implement plans that will assist their nation in the protection of its critical infrastructures. Both private organisations and government must work together as only through understanding, communicating and co-operation will they be able to assist their country in protecting critical infrastructures.

An information assurance programme should be implemented to protect the integrity and availability of information over the entire range of potential disruptions from accidental to malicious. The threat and risk issues need to be understood and appropriate solutions for it found using risk management approaches. The first stage of this programme should be threat analysis leading on to a risk analysis. From the risk analysis the vulnerabilities of a system can be identified and countermeasures implemented. The security technology employed should be enhanced with security procedures including incident handling and mechanisms for intrusion detection. These countermeasure requirements should be defined in the security policy. To provide for information system defence, it is recommended that an aggressive programme must be implemented which should include:

- Undertaking a threat analysis;
- Liasing with international and national programmes on threats and vulnerabilities;
- Undertaking a risk analysis on a regular basis;
- Producing and implementing a security policy;
- Protecting systems according to best-practice standards similar to British Standard BS7799:2000/ ISO/IEC 17799:2000;
- Implementing defence-in-depth security countermeasures;
- Providing security breaches detection and reporting systems;
- Refining threat indications and warnings – from detection statistics;
- Regular auditing and monitoring perhaps through an independent organisation;

- Implementing a security awareness campaign;
- Producing and implementing a Disaster Recovery Plan and testing it on a regular basis.

5. FURTHER INFORMATION

Austria
Secure Information Technology Center - Austria
www.a-sit.at

Denmark
Digital Denmark – Conversion to the Network Society
www.fsk.dk/cgi-bin/doc-show.cgi?doc_id=23026

Danish Ministry of Research and Information Technology
www.fsk.dk/cgi-bib/news-archive-list.cgi

Internet Vulnerability Report
www.fsk.dk/fsk/publ/2001/itsikker/index.htm

Finland
National Fund for Research and Development/Information Society Strategy
www.sitra.fi/tietoyhteiskunta/english/st5/eng01.htm

National Technology Agency
www.tekes.fi/eng/default.asp

Information Society Development Centre
www.tieke.fi

FICORA
www.ficora.fi/englanti

Security Police
www.poliisi.fi/english/index.htm

France
Central Office for Fight Against Hi-Tech Crime / Central Direction for Security of Information Systems DCSSI
www.scssi.gouv.fr

French Information Warfare Resources
www.infoguerre.com

Computer Emergency Response Team
www.certa.ssi.gouv.fr

Germany
Bundesministerium des Innern
Referat IT 3, Alt Moabit 101D, D-10559 Berlin
www.bmi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Referat III 2.4, Godesberger Allee 183-189, D-53175 Bonn
www.bsi.bund.de

Italy
AIPA (Autorità per l'informatica nella Pubblica Amministrazione)
www.aipa.it

RUPA Technical Centre
www.ct.rupa.it

CERT-IT (The Italian Computer Emergency Response Team)
http://idea.sec.dsi.unimi.it

CLUSIT (Associazione Italiana per la Sicurezza Informatica)
www.clusit.it

ANASIN (Associazione nazionale delle aziende di servizi di informatica e telematica)
www.anasin.it

The Netherlands
Infodrome
www.infodrome.nl

Computer Emergency Response Team CERT-RO
www.cert-ro.nl

R& D : TNO's URLography
www.tno.nl/instit/fel/infoops
info@fel.tno.nl

Norway
Forsvarets forskningsinstitutt (FFI)
FFI, Postboks 25, N-2027 Kjeller, Phone +47 63807000, Fax +47 63807115
www.ffi.no

Senter for Informasjonssikring (SIS)
SINTEF Tele og Data, N-7465 Trondheim, Phone: (+47) 73 59 30 00
www.norsis.no
post@norsis.no

Computer Emergency Response Team UNINETT CERT
http://cert.uninett.no

Poland
Computer Emergency Response Team CERT POLSKA.
Tel.+48 22 5231274; Fax. +48 22 5231399
www.cert.pl
cert@cert.pl

Sweden
National Office for IO/CIP studies
c/o Swedish National Defense College (Försvarshögskolan)
www.fhs.mil.se

Swedish Emergency Management Agency (SEMA)
www.krisberedskapsmyndigheten.se/english/

Swedish National Post and Telecom Agency (PTS)
www.pts.se

Switzerland
Information Society Project Switzerland
www.isps.ch

Division for Information Security and Facility Protection (DISFP)
www.vbs-ddps.ch/internet/groupgst/en/home/integral.html

National Science Foundation: Swiss Priority Programme for Information and Communications Structures
www.spp-ics.snf.ch

Comprehensive Risk Analysis and Management Network (CRN)
www.isn.ethz.ch/crn/

Infosurance
www.infosurance.ch

Computer Emergency Response Teams
www.switch.ch
http://cert.nextra.ch

United Kingdom (UK)
National Infrastructure Security Co-ordination Centre (NISCC)
PO Box 832, London, SW1P 1BG, United Kingdom
Tel: +44 207 821 1330, Fax: 0207 821 1686
www.niscc.gov.uk

Information Assurance Advisory Council (IAAC)
36 Regent Street, Cambridge CB 1DB, United Kingdom
Tel: +44 1223 307711, Fax: +44 1223 358845
www.iaac.org.uk

USA

Department of Homeland Security (DHS)
www.dhs.gov

Europe
Dependability Development Support Initiative (DDSI)
www.ddsi.org

6. REFERENCES

[Denning99]	Denning, Dorothy E (1999). Information Warfare and Security. Addison-Wesley ISBN: 0-201-43303-6.
[DoDD]	US Department of Defense Directive 5160.54
[EC2002]	European Convention on Cybercrime ETS No 185 (http//conventions.coe.int)
[EU2002]	eEurope action plan 2003-2005 (http://europa.eu.int/eeurope)
[FM 100-6]	Information Operations, US Army, 27/8/1996
[HSAIW]	Information Warfare conference proceedings, H.Silver and Associates, London, 13&14 November 1997
[IDA97]	Information Operations: A Research Aid, J.V. Gray et al., IDA, September 1997, IDA document D-2082 (http://www.infowar.com)
[JP3-13]	Joint Pub 3-13, 'Joint Doctrine for Information Operations', Joint Chiefs of Staff, 9 October 1998. (www.dtic.mil/doctrine/)
[Luiijf00a]	Luiijf, H.A.M, (2000). Information Assurance Under Fire. In: SMI Conference on Information Assurance and Data Security, 2nd &3rd February 200, The Hatton, London. SMI Conferences Ltd, London.
[Luiijf00b]	Luiijf, H.A.M, Klaver, M.H.A. (2000). In Bits and Pieces, Essay on the vulnerability of Dutch information-infrastructures, Infodrome, Amsterdam (www.tno.nl/instit/fel/refs/pub2000/luiijf_bitbreuk_english.pdf)
[MCM-069-98]	[NR] NATO Information Operations (INFO OPS) concept, May 1998
[MC422]	NATO Information Operations Policy, 12 January 1999
[NRC99]	Realising the Potential of C4I: Fundamental Challenges. Committee to Review DOD C4I Plans and Programs, National Research Council, May 1999. (www.nap.edu/catalog/6457.html)
[PCCIP97]	President's Commission on Critical Infrastructure Protection (PCCIP) (1997) Critical Foundations: Protecting America's Infrastructures: The Report on the President's Commission on Critical Infrastructure Protection, Washington D.C.: US Government press.
[PDD63]	Presidential Decision Directive 63 (PDD63; 1998): The Clinton Administration's Policy on Critical Infrastructure Protection
[Sign0798]	Information Operations, AFCEA's Signal, July 1998
[Till/Luiijf01]	Till, J. van, Luiijf, H.A.M. et all (2001). Samen werken voor veilig Internet verkeer: Een e-Deltaplan (KWINT) (Dutch: www.minvenw.nl/dgtp/home/data/scriptgifs/985003518-1.pdf).

7. ABBREVIATIONS

AKSIS	Arbeitskreis Sichere Infrastrukturen (Working group on secure/safe infrastructures)
ANASIN	Associazione nazionale delle aziende di servizi di informatica e telematica
ATM	Automatic Teller Machine
BS	British Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT	British Telecom
CERT	Computer Emergency Response Team
CIP	Critical Infrastructure Protection
CLUSIT	Associazione Italiana per la Sicurezza Informatica 20
CNI	Critical National Infrastructure
COTS	Commercial-Off-The-Shelf
CRN	Comprehensive Risk Analysis and Management Network
DCSSI	French Central Direction for Security of Information Systems
DDSI	Dependability Development Support Initiative
DISFP	Division for Information Security and Faculty Protection
DoD	US Department of Defense
DSL	Digital Subscriber Line
EISA	European IT Services Association
E-M	Electro-Magnetic
EMC	Electro-Magnetic Compatibility
EMI	Electro-Magnetic Interference
EMP	Electro-Magnetic Pulse
FFI	Forsvarets forskningsinstitutt
FICORA	Finland’s Ministry of Transport and Communications
FBI	US Federal Bureau of Investigation
FEDERCOMIN	Federazione delle Imprese delle Comunicazioni e dell'Informatica
FFI	Forsvarets forskningsinstitutt
FIRST	Forum of Incident Response and Security Teams
FITA	Federazione Italiana Industrie e Servizi Professionali e del Terziario Avanzato
FSI	Forum per la Società dell Informazione
FSUIT	Federal Strategy Unit for Information Technology
GOSCC	UK Government Security Co-ordination Centre
IA	Information Assurance
IAAC	Information Assurance Advisory Council
ICT	Information and Communication Technology
IEC	International Electrotechnical Committee
IO	Information Operations
IO-D	Information Operations Defensive
ISO	International Organization for Standarization (www.iso.ch)
ISP	Internet Service Provider
IT	Information Technology
IW	Information Warfare
KRITIS	Kritische Infrastrukturen (Critical Infrastructure)
KWINT	Kwetsbaarheid van het Internet (Dutch Internet Vulnerability study)
MCI	Maxwell Communications Incorporated
MEII	Minimum Essential Information Infrastructure
NASK	Research and Academic Network in Poland
NES	National Economic Supply
NIPC	National Infrastructure Protection Centre
NISCC	National Infrastructure Co-ordination Centre
PABX	Private Automated Branch Exchange

PC	Personal Computer
PGP	Pretty Good Privacy
PCCIP	President's Commission on Critical Infrastructure Protection
SCADA	Supervisory Control and Data Acquisition
SEMA	Swedish Emergency Management Agency
SGDN	French General Secretary of National Defence
SIS	Senter for informasjonssikring
SME	Small and Medium Enterprise
SSI	Security of Information Systems
TIEKE	Finland’s Information Society Centre
UNIRAS	Unified Reporting And Alerting Scheme
VAHTI	Finland’s Ministry of Finance IT-security board

ANNEX A:
INFORMATION WARFARE DEFINITIONS

A.1 Information Warfare definitions, non-nation bound

Thomas Rona [Lib]:
The strategic, operation, and tactical level competitions across the spectrum of peace, crisis, crisis escalation, conflict, war, war termination, and reconstitution/restoration, waged between competitors, adversaries or enemies using information means to achieve their objectives.

Working definition US National Defense University (R. Neilson and C.B. Giasson, 1995):
Information Warfare is an approach to conflict focusing on the management and use of information in all its forms and at all levels to achieve a decisive advantage in pursuit of national security goals.
[Information based warfare is both offensive and defensive in nature - ranging from measures to prohibit adversaries from exploiting information to corresponding measures to ensure the integrity, availability and interoperability of friendly information assets.
Information based warfare is also waged in political, economic and social arenas and it is applicable over the entire national security spectrum from peace to war and tooth to tail.]

A.2 United States

Emmer Paige 1995; (US) DoD as well at that time:
Actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and defending our information and systems.

US AIR FORCE:
Any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions.

US ARMY (DoD definition of Information Warfare):
Actions taken to achieve information superiority by affecting adversary information, information based processes, and information systems, while defending ones own information, information based processes, and information systems.

US Joint Chiefs of Staff [CJCSI 3210.01, 1996] definition of Information Warfare:
Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks **while defending** one's own information, information-based processes, information systems, and computer-based networks.
In 1994, the Defense Science Board had added "in support of military strategy" to the first sentence, but that was dropped in this line. NATO had that one back in.

US Department of Defense Information Operations (Info Ops):
Information Operations are: Continuous *military* operations within the *military* information environment that enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations. Information Operations include the interacting with the global information environment and exploiting or denying an adversary's information and decision capabilities. [FM 100-6 definition]. (*qualitative aspect*)

US Special Operations Command (SOCOM) over Information Operations:
Information Operations is a *strategy* that integrates various capabilities to gain *information superiority* that supports national and/or military objective(s).
(not just a weapon, means or capability) [InfoW98]

US Joint Chiefs of Staff Joint Pub 3-13 about Information Operations:
Information Operations capitalise on the growing sophistication, connectivity, and reliance on information technology. Information Operations target information technology or information systems in order to affect the information-based process whether human or automated. (Information Operations battlespace is the infrastructure) [JP3-13]

A.3 United Kingdom

UK Royal Navy (Captain Patrick Tyrell): *1*
The deliberate, unauthorised and systematic attack on critical national information activities to exploit the information contained within the system, deny service to the authorised user, modify or corrupt data.

A.4 Germany

German Defence (1997) concept Information Warfare-definition by Task Group Force 2020 [HSAIW]:
"Information Warfare comprises all arrangements and measures which enable a nation or supranational organization, especially if a crisis develops, a conflict escalates or a threat emerges, to ensure the political, economic or military freedom of decision-making and freedom of action both by the interference with, manipulation or elimination of enemy information, information-based processes and information infrastructures and by defense of such attacks on basis of an information advantage. Information Warfare uses the results of available procedures of information processing, adds new forms and relies on an efficient information management."

1 Mr. Pat Tyrrell was an Assistant Director CIS from 1992 to 1996 and since then April 1997 Commander of the Defense Intelligence and Security School at Chicksands. He is a member of the Kemble Group, a 'think tank' on the domain of management issues that emerge from information society developments.