Information Warfare
an introduction

Reto E. Haeni
r.haeni@cpi.seas.gwu.edu

The George Washington University
Cyberspace Policy Institute
2033 K Str. Suite 340 N
Washington DC 20006

Washington DC, January 1997

Table of Contents

1 Abstract

The term Information Warfare is widely used in today's news. Often, it is misinterpreted and points to high-tech weapons which are used in mass armies.

Information Warfare is defined by:

> **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.**

The history of warfare is described in three waves. During the agrarian revolution, warfare was fought by a warrior class based on information. With the industrial revolution, the war changed to mass destruction. Nation states used mass armies to protect and expand their societies through wars with high casualties. In the information age, warfare changes to Information War. The ultimate destructive capability is no longer mass destruction but critical data deletion. Information attacks with minimal casualties are characterizing the war.

On the battlefield, information technology is still used today mainly to make weapons smarter and to minimize one's own casualties with providing the troops with third wave technology in second wave weapon system. The actual doctrine is AirLand battle and the command structure is Command, Control, Communication and Information (C3I) or with adding Computer (C4I). Soft War is used to demoralize enemy troops by sending wrong information and morphed TV programs to them.

Possible Information Warfare Weapons are used (or at least could be used) by modern armies as well as by terrorists. They are for example:

- Computer Viruses
- Worms
- Trojan Horses
- Logic Bombs
- Trap Doors
- Chipping
- Nano Machines and Microbes
- Electronic Jamming
- HERF Guns - EMP Bombs

Information Warfare is developed by high-tech societies and armies. The Information Warfare weapons can only be used against an enemy which has also similar high-tech capabilities. The use against first or second wave armies is limited. Information Warfare can also be used in terrorist actions against an information society without exposing the terrorists themselves to danger as they can cause severe damage with remote actions.

2 Introduction

Today's news is overwhelmed with information on the latest breakthroughs in communications, the Information Superhighway (easier said, the Internet), Cyberwar, and Information Warfare. Soldiers are shown with "Star Wars" equipment fighting on the battlefield, and the news are broadcasting this "information" all over the world.
In this paper, I define "real" Information Warfare (IW) and show how IW is or could be used in the present or in the near future. I wrote this paper with a target audience of non technical readers in mind. The paper will provide an introduction to Information Warfare to everyone who is interested in this field and link the experienced reader to supplementary documentation.

3 What is Information Warfare

3.1 Definition

One of the problems with Information Warfare (IW) was that for a long time no official definition existed. The main reason for this is that this kind of warfare is relatively new and that the term IW has many different meanings. On one hand, there is the military aspect of it but on the other hand, IW is also used to describe the “war“ on the Internet.

While the DoD was defining Information Warfare for a certain time exclusively for the military field with referral to the support of national military strategy, there exists now a wider approach as a definition for Information Warfare. This definition can be used for the military as well for the civilian side of IW. The Chairman of the Joint Chiefs of Staff Instruction (CJCSI) Number 3210.01, dated 02 January 1996 provides the following, unclassified, definition

Paragraph 5, definitions, subpara c states:

> ***Information Warfare (IW).*** **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.**

Information Systems are also defined in the same paragraph (subpara a) as:

> ***Information Systems*****. The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.**

3.2 .A practical description

In his book *Information Warfare*, Winn Schwartau [8] describes a different way to define Information Warfare. He does not try to define all levels of IW in one and the same description, but he split the definition into the following three classes:

3.2.1 Class1: Personal Information Warfare

The first class describes attacks against an individual's electronic privacy. This includes the disclosure of digital records and database entries wherever information is stored. The average person today has little control over the information stored. We cannot control the amount of information concerning us even if it is correct or not. According to a USA Today poll, 78% of Americans are concerned about the loss of privacy [8].

In the past, a spy had to tap phone lines and had to use miniature cameras and microphones to get desired information about a person. Today, he still has the capability to use this utilities (which are more miniaturized and easier to use than ever) but most of the information about a person will be available in existing databases. To blackmail someone, it is no longer necessary to survey him/her for months, today's Information Warrior gets the desired information with the help of a computer over the telephone line.
Do we have to be concerned about information that get public? To be honest, most of us do not want that the credit card bills, bank account numbers, financial transactions such as loans, video rentals, medical history, emergency room services, prescriptions, criminal offenses, arrests, court records and other information printed in the newspapers, spread to our friends or distributed over the world on the Internet. Worse, if someone provides private information, who says that this information has to be true? You can spend a lifetime denying published information where no one takes the responsibility for the integrity of the data.

This is the first approach to class 1 warfare, but it can easily become worse. As we saw in the movie *The Net* with Sandra Bullock, we strong rely on the information about us. If someone is able to edit information in law enforcement databases, how would you explain to a police officer that the credit card you used is not stolen, that your passport is not faked, that your real name is not Juan Garcia, that you never smuggled drugs and did not kill three people and that you are not wanted all over the world by Interpol if the computer in the car of the patrolman, which you called because someone sold your house during your holidays, says so.

Put together, we can say:

- Thousands of databases hold together the digital images of our lives.
- Computers constantly exchange information about each of us.
- Available information does not have to be correct
- Getting erroneous information corrected is almost impossible

Class 1 Information Warfare does not seem to be a potential threat but can easily destroy someone's identity or even link to class 2 or even class 3 Information Warfare.

3.2.2 Class2: Corporate Information Warfare

This class describes competition, or better said, today's war between corporations around the world.
It is easy to imagine that a company could invest $ 1M in a system that allows them to break into a competitors database and copy research results worth over $ 15 M. To make sure that the

competitor will not be the first on the market with the new product, they could also destroy the original database on the fly and make it look like a possible accident with a virus on the mainframe.

This description of corporate information warfare is not new. This kind of "espionage" is well known from the cold war where Russian and American spies tried to gather information about each others nation.

Today, corporate information warfare has a new dimension. Not only can one corporation try to get the research results of a competitor, states became involved in this "game". It is possible that a state encourages students to study abroad (e.g. in the United States) and asks them to keep an eye open, not only to the lectures at the University but also to work as interns in US corporations and give the information back to their government.

Class 2 Information Warfare is not only about the acquisition of information, it is also possible to spread information, real or fictious. The possibility that a drug competitor corporation (or a foreign government with its own chemical production in their country) spreads the information that the widely used ABC drug against asthma by the US corporation X causes significant lung cancer, the doctors will probably stop with the prescription of ABC until a study will be published. This study could be fake and part of a whole campaign of well-designed desinformation. The damage is made and millions of dollars for the X corporation is lost until they can prove (if they can) that their product is OK.

This previous example uses a drug manufacturer. In today's world, many processes are controlled by computer chips. It would be even easier for an IC manufacturer to claim that the widely used chip by their competitors does not work as it should. Would you buy a car with an airbag where it was written in the newspapers that the chip that controls the airbag does not work properly in 40% of all cases? How will the company prove contrary? You cannot test the system easily by yourself if it functions, you have to trust the manufacturer. If a corporation looses the trust of their customer, they also lose millions of dollars.

Also class 2 warfare can cause global changes. What if, for example, Jennifer Flowers announced her complaint against Bill Clinton not months before his election but only a few day before the Democratic National Convention? US history and it's influence on world's history could have changed.

3.2.3 Class 3: Global Information Warfare

This type of Warfare works against industries, global economical forces or against entire countries or states. It is not any more sneaking in Research data of a competitor but about the theft of secrets and then turning this information against its owners.

In this class, you can multiply the power of class 1 and class 2 warfare by a large factor and still not be able to imagine all the damage that can be done within global information warfare. Here, money and personal are not the critical factor. Second and third world countries are spending billions of dollars every year in airplanes, bombs and bullets. What if a country decides that they will spend only a tenth of its yearly expenses for second wave weapons (see [11] or the following chapter) in third wave weapons. As an example, a dictator in the South East could about 200 million dollars a year in third wave weapons and be able within about three years to damage the US industry and government in an unimaginable way. In relation to traditional weapons, Information Warfare opens new horizons of cost effectiveness for terrorists or enemy governments. Class three warfare enables attacks over ten thousands of miles with dramatic effects. With the weapons described in one of the following sections of this paper, the described dictator would be able to crash Wall Street, shut down the banking system of the US; then the last wall street crash will look harmless in comparison to the effects that would follow.

4 History of Warfare

In their book *War And Anti War* [11], Alvin and Heidi Toffler approach the history of warfare using a model of three waves. The following sections briefly discuss these three waves.

4.1 Agrarian wave

The agricultural revolution started the first great wave of change in our history. It led to the first of today's known societies. Agriculture enables communities to produce economic products which in that age were athe cause of many wars. The link between war and soil was close at this time. The people were kept ignorant by their statesman to keep them focused on farming and warfare. The soldiers were occupied for the most time of the year with working on the fields. Volunteer soldiers came mainly from farms which did allow them to be absent during the winter months. The harvest called back the soldiers so that only a month or two were left where these farmers could find time to fight. The armies were mainly poorly organized and equipped. There were also few exceptions to this rule. The example of a strongly led and equipped army is surely the Roman legions in their heyday.
In most First Wave armies, the soldiers pay was irregular and low. They were paid usually in kind rather than money. The pay of a soldier in the Roman army after a lifetime warfare was usually a little parcel of land somewhere.

4.2 Industrial wave

The industrial Revolution changed the way wars were fought. The element of mass production introduced weapons of mass destruction (nuclear and chemical). The mass armies were not loyal to the landowners but to modern nation states which were paying the soldiers. The change from one wave to the other did not happen in a short period but, similar to the industry, took its time to change the warfare. During the transition period, a few wars were actually fought with both types of armies. A good example is the American Civil War (1862-63) where the industrialized North defeated the agrarian South. The big change in warfare was indicated by the manufacture of standardized arms like musketes with bayonets and their accessories. The parts became interchangeable and the industry acted quickly to the needs on the battlefield. Standardization was not only used to produce weapons themselves, but was also applied to military training, organization and doctrine. Like in business, armies developed general staffs and also the orders changed from oral commands to written commands like memos, as used in business. Mechanized warfare was then only a logical step in this evolution to dramatically increase firepower and to change the doctrine.
World War II exposed the disastrous way of fighting mass destruction warfare. Not only that millions of men fought in this war but also 15 million soldiers were killed during this period. The Nazis killed 6 million Jews [11] in factory style. Therefore, mass destruction was used on the field even before the first nuclear bomb exploded over Hiroshima.
The time after World War II was described as the time of the theory of mass destruction. The doctrine in the cold war was not to priorizate targets or precise targeting but to destroy everything in order to win the war. Strategic bombing and ballistic missiles were designed for use on a massive scale and small battlefield nuclear and chemical devices were added to the weapons arsenal.

4.3 Information wave

In the late 1970s and early 1980s, third wave technologies and ideas began to change the industrial wave societies. The mass society became slowly a communication society. With this development the military doctrine began to change. The duality between the two waves was expressed in the Gulf War of 1990-91 where a dual war was fought by the allies. On one hand, mass destruction was used like in World War II with large bomb carpets over the enemy troops but on the other hand, high tech weapons were used to aim the targets precisely. The fear that the allies high-tech military would fail in the desert environment of Kuwait and Iraq was widely spread at the beginning of the war. This fear, combined with the battle-tested army of Saddam Hussein, feeded the concern about potenial huge allied losses. This could have become true if the Gulf had been fought in the typical second wave way. However, the Air-Land Battle doctrine already had been known in the military world but Saddam Hussein seems to have been unaware of it. The allies were preparing the battlefield in the second wave way using carpet bombing and stupid bomb drops. At this time, no high tech weapons were used or needed but bombs dating from 1968, out of the Vietnam War were used to hold down and demoralize the enemy. During the same time, Nighthawk stealth fighters (F-117 A) attacked their targets in Baghdad. They flew attacks on air-defense centers and military control facilities to blind the enemy. The allies were deepening the

battle in three dimensions. Distance, altitude and time were used in the AriLand Battle doctrine. The front was in the rear and at the sides and not where the enemy had planned. An important point was to destroy the command facilities and the communications to prevent the information flow up and down the command chain. Therefore, Iraq was the first fought AirLand Battle and a first step towards the Information War by using smart weapons and computers (there were more than 3000 computers in the war zone actually linked to computers in the US [11]).

Also if Toffler as first described the history of warfare using a model of three waves, I do not agree with him that the Gulf war belongs into the Information wave. At the beginning of his section describing the third wave, he mentions that Desert Storm was fought in a dual way, but he never describes the Information War in its proper meaning. Information Warfare in the proper use was probably not used in the Gulf war. Information Warfare, as tabulated in the next chapter, would be fought, if the destruction capability would no longer be mass destruction weapons but critical data deletion. The Information War would be present, if the technology would no longer be used to make traditional weapons smarter but to replace them.

4.4 The three waves tabulated

Wave	1st	2nd	3rd
Descriptor	Agrarian	Industrial	Information
Physical Security provided by	A Warrior class, Mercenaries, Militia	Professionals Citizens	Information knowledgeable leaders
Dominant Soc., Pol., Econ. Force	Tribe, City, State, Family	Nation-State, Factories	Global conglomerates
Economy dominant by	Trade	Money	Symbols (e.g. in a database)
War Characterized by	Representational Conflict	Mass Armies, high casualties	Information Attacks, minimal casualties
Ultimate Destructive Capability	Gunpowder	mass destruction (nuclear, chemical...)	Critical Data Deletion
Leadership	Hierarchical	Top down orders	Low level empowerment, flat structures
Information Based Warfare	yes	yes	yes
Information technology in war	no	yes	yes
Information War	no	no	yes

table No. 1, adapted from [1], [3] and [11]

5 The military view of Information Warfare

5.1 Third wave technology in second wave weapon systems

Information Warfare is omnipresent in today's newspapers. Several times a week, you can follow reports concerning new, miniaturized weapon systems. By 2010, the Army hopes to digitize the battlefield [8] and link every soldier and weapon system with wireless links. A report on the 21st century land warrior, out of the Marine Officer training camp at Fort Quantico, shows the new battle gear for a so called cyberwarrior: a lightweight helmet with mounted display, night vision sensors and flat video panel (all voice activated), Integrated Headgear, Body Armor with room for a computer in the lumbar area which gives friend or foe identification capability to the soldier, detects mines and chemicals, and has a built in GPS. The weapon is equipped with a thermal sight capable of sending still-frames back to the high command and is connected (wireless) to the helmet monitor which allows the soldier to aim at a target without exposing his body to the enemy. Also if this sounds quite like "Star Wars", the technique is available and this equipment will soon be present on the battlefield and will help to reduce casualties. Nevertheless, this is not a part of Information Warfare. IW is "war" without using a tank at all, not only by using the technology to make the tank smarter. But also if Information Warfare will replace a smaller or larger part of today's weapon system, there is no way that this technology can replace the soldier until "war" changes so that nobody is involved physically.

5.2 C3I

At the head of the information army, there is the so called C3I - Command, Control, Communications and Intelligence. Often today its called C4I with Computers added into the term. At this level, the decisions are made and the money flow is controlled. C3I is a small group with specialists dedicated for each area of interest. As an example, I describe here the C3I group of the OSD (Office of the Assistant Secretary of Defense).

- Assistant Secretary of Defense (Command, Control, Communications and Intelligence)
- Principal Deputy Assistant Secretary of Defense (Command, Control, Communications and Intelligence)
- Deputy Assistant Secretary of Defense (Command, Control and Communications)
- Deputy Assistant Secretary of Defense (C3I Acquisition)
- Deputy Assistant Secretary of Defense (Information Management)
- Deputy Assistant Secretary of Defense (Intelligence & Security)
- Deputy Assistant Secretary of Defense (Plans & Resources)
- Director, Information Warfare (IW)
- Deputy Director, US Nuclear Command & Control System (NCCS) Support Staff (NSS)
- Director, C4I Integration Support Activity (CISA)

You can review the actual C3I group of the US OSD at http://www.dtic.dla.mil:80/c3i/c3iorg1.html.

5.3 Soft War

This kind of warfare matches the definition of Information Warfare only in a global way. The aim is not directly to achieve information superiority, but to manipulate the enemy (or ones own population) with false or adapted information. The TV is used to shape the another Nation's will, changing the view of reality. There could be broadcast, for example, a "morphed" TV program that shows the enemy troop leader or foreign politicians making unpopular announcements, with the goal to alienate them from their troops/people. This kind of warfare is mostly used in combination with "jamming" which is described in the next section.

Another application of soft war is to use it in one's own country. An incident in the Gulf War could be mentioned here. In a world wide broadcasted news block, CNN showed a women who described how the Iraqi soldiers were carrying live important equipment for new born babies out of the Kuwaiti hospitals. Later, it was discovered, that this women was related to the Kuwaiti Embassy in Washington DC. Therefore, the interview was set up [2]. A controlled media can and will be used to broadcast for public relations.

6 Examples of available (or possible) IW weapons

6.1 Computer Viruses

> "A virus is a code fragment that copies itself into a larger program, modifying that program. A virus executes only when its host program begins to run. The virus then replicates itself, infecting other programs as it reproduces." [7]

Viruses are well known in every computer based environment, so that it is not astonishing that this type of rough program is used in the Information Warfare. We could imagine that the CIA (or Army, Air Force ....) inserts computer viruses into the switching networks of the enemy's phone system. As today's telephone systems are switched by computers, you can shut them down, or at least causing massive failure, with a virus as easy that you can shut down a "normal" computer. An example what the damage a virus could cause exists. We can compare it with the system crash of AT&T long distance switching system on January 15, 1990 [10].

6.2 Worms

> "A worm is an independent program. It reproduces by copying itself in full-blown fashion from one computer to another, usually over a network. Unlike a virus, it usually doesn't modify other programs."[7]

Also if worms don't destroy data (like the Internet Worm, described in [5]), they can cause the loss of communication with only eating up resources and spreading through the networks. A worm can also easily be modified so that data deletion or worse occurs. With a "wildlife" like this, I could imagine breaking down a networked environment like a ATM and banking network.

6.3 Trojan horses

> "A Trojan horse is a code fragment that hides inside a program and performs a disguised function. It's a popular mechanism for disguising a virus or a worm"[7]

A trojan horse could be camouflaged as a security related tool for example like SATAN (Security Administrating Tool for Analyzing Networks). SATAN checks UNIX system for security holes and is freely available on the Internet. If someone edits this program so that it sends discovered security holes in an e-mail message back to him (lets also include the password file? No problem), the Cracker learns much information about vulnerable hosts and servers. A clever written trojan horse does not leave traces of its presence and because it does not cause detectable damage, it is hard to detect.

6.4 Logic bombs

> "A bomb is a type of Trojan horse, used to release a virus, a worm or some other system attack. It's either an independent program or a piece of code that's been planted by a system developer or programmer."[7]

With the overwhelming existence of US based software (e.g. MS Windows or UNIX systems), the US Government, or whomever you would like to imagine, could decide that no software would be allowed to be exported from that country without a Trojan horse. This hidden function could become active when a document with "war against the USA" exists on the computer. Its activation could also be triggered from the outside. An effect could be to format the computers harddisks or to mail the document to the CIA.

6.5 Trap doors

> "A trap door, or a back door, is a mechanism that's built into a system by its designer. The function of a trap door is to give the designer a way to sneak back into the system, circumventing normal system protection."[7]

As I mentioned in the last section, all US software could be equipped with a trap door that would allow IW agencies to explore systems and the stored data on foreign countries. This could be most useful in cases of military strategic simulations and plans and would provide the DoD's intelligence with vital information.

6.6 Chipping

Just as software can contain unexpected functions, it is also possible to implement similar functions in hardware. Today's chips contain millions of integrated circuits that can easily be configured by the manufacturer so that they also contain some unexpected functions. They could be built so that they fail after a certain time, blow up after they receive a signal on a specific frequency, or send radio signals that allow identification of their exact location - the number of possible scenarios exceeds, by far, the scope of this paper. The main problem with chipping is that the specific (adapted) chip be installed in the place that is useful for the Information Warrior. The

easiest solution is to built the additional features into all the chips manufactured in the country that is interested in this type of IW.

6.7 Nano machines and Microbes

Nano machines and Microbes provide the possibility to cause serious harm to a system. Unlike viruses, we can use these to attack not the software but the hardware of a computer system. Nano machines are tiny robots (smaller than ants) that could be spread at an information center of the enemy. They crawl through the halls and offices until they find a computer. They are so small that they enter the computer through slots and shut down electronic circuits.

Another way to damage the hardware is a special breed of microbes. We know that they can eat oil, what about if they were bred for eating silizium? They would destroy all integrated circuits in a computer lab, a site, a building, a town.....

6.8 Electronic jamming

In the old days (and even today) electronic jamming was used to block communications channels at the enemy's equipment so that they can't receive any information. The next step is not to block their traffic, but instead overwhelm them with incorrect information. This type of disinformation can also be combined with the possibilities described in the section "soft war"

6.9 HERF Guns - EMP Bombs

HERF stands for High Energy Radio Frequency. HERF guns are able to shoot a high power radio signal at an electronic target and put it out of function. The damage can be moderate (e.g. that a system shuts down, but can be restarted) or severe (e.g. the system hardware has been physically damaged). Electronic circuits are more vulnerable to overload that most people would suspect. This mechanism uses HERF guns with big success. In essence, HERF guns are nothing but radio transmitters. They send a concentrated radio signal to the target. The target can be a mainframe inside a business building, an entire network in a building, or as today's planes and cars are stuffed with electronic equipment, the target can even be a moving vehicle with all the inherent dangers for the people who are inside.
EMP stands for electromagnetic pulse. The source can be a nuclear or a non-nuclear detonation. It can be used by special forces teams who infiltrate the enemy's and detonate a device near their electronic devices. It destroys the electronics of all computer and communication systems in a quite large area. The EMP bomb can be smaller than a HERF gun to cause a similar amount of damage and is typically used to damage not a single target (not aiming in one direction) but to damage all equipment near the bomb.

7 Information Warfare in use

7.1 Who uses (or could use) Information Warfare

Who uses Information Warfare against who today and the military use of IW is not officially known, at least only from public sources. There has been a wide discussion on whether IW tools were used in the Persian Gulf War and whether the CIA had overtaken a wireless network of the Iraqi Army, but these messages were fake or could not be proven. Desert Storm was mostly a war where "smart" weapons were used to destroy the enemy's headquarters.

Soft War was widely used to demoralize the enemy troops in Desert Storm. Ten of thousands of pamphlets were dropped over enemy forces, part of them in thousands of plastic cans to draw the attention of the Iraqis toward the sea.

Information Warfare, in its wider sense, is daily used between individuals and corporations. Computer system penetrations are reported daily to emergency report teams that are in charge to take countermeasures. Often, the attackers (crackers) are arguing that they do not commit a crime but improving the security of the system by pointing to its weaknesses. However, data disclosure and denial of service are a serious problem.

7.2 Who is vulnerable?

The contradiction about Information Warfare is, that it is forced by nations that are highly technologized. Information War on the battlefield will therefore be used mostly by them. Unfortunately, today, most potential enemies do not have the technological capability. IW can successfully be used against them. The enemy has to have high tech weapons and communication to use IW in a practical manner. Therefore, countries which develop these new kind of weapons and tactic are also the most vulnerable. Third wave weapons cannot be used against first wave armies and partisans activities. And they only have a partial effect against second wave armies. Information Warfare can also be used in a "non military" way against individuals and whole societies. This new style of warfare gives potential enemies the power to disrupt the communication capabilities of a country and thereby break down its business.

The Information Warfare weapons could more likely be used in the near future as terrorist weapons rather than on the battlefield by the regular armies. Today's communication society is extremely vulnerable to disruptions. Instead of planting a bomb in a airplane with all the dangers for the terrorists, they could shut down all the communication capabilities from the tower of a airport to the hundreds of airplanes that the control center guides. A accident following this disruption would be most likely.

8 Conclusions

The US and other high tech states are moving from second to third wave forms of society and to third wave war. Today, third wave weapons are used in a second wave armies and societies. In the news, the use of high-tech weapons is often mistaken as Information Warfare.

The US and other high tech societies are especially vulnerable to Information Warfare attacks. They rely heavily on today's electronic communication and data exchange. An offender can attack these information backbones with (in comparison to the damage) low investment of finance and equipment.

Our systems are mainly vulnerable for the following reasons:

- High tech equipment is available all over the world (for friend and enemy).
- The awareness of the danger of Information Warfare is mostly not appropriate at the executive level.
- A lot of computer systems are poorly managed and poorly equipped to prevent against intruders
- Attackers use sophisticated tools to break into systems or get desired information
- Attacks over the Internet can originate from places that are physically located on the other side of the globe.
- It is impossible to make a system absolutely secure

Corporate Information Warfare is used every day in our society. Only a small part of all incidents are known. Many incidents are never discovered and most others are not known outside of the organization for fear of negative reactions.

9 References

[1] Alger John I., Dr. *Information Warfare, Hackers Crackers and the Projection of Power*, (Seminar notes, GWU 1995)

[2] BBC, *The i bomb*, (video 30min, BBC Horizon 1995)

[3] Campen Alan D,. *Conference notes* (Information Warfare Conference, Washington DC 1995)

[4] Hoffman Lance J., *Building in Big Brother, the cryptographic policy debate*, (Springer Verlag 1995)

[5] Hoffman Lance J., *Rogue Programs: Viruses, Worms and Trojan Horses*, (VNR 1990)

[6] Rosenberg Stuard, Jo Seiler, *Conference notes* (Information Warfare Conference, Washington DC 1995)

[7] Russel Deborah and Gangemi G.T., *Computer Security Basics*, (O'Reilly & Associates, 1994)

[8] Schwartau Winn, *Information Warfare, Chaos on the electronic superhighway*, (Thunder's mounth press 1994)

[9] Seanor Joseph C. III, *Conference notes*, (Information Warfare Conference, Washington DC 1995)

[10] Sterling Bruce, *The Hacker Crackdown*, (Bantam Books 1993)

[11] Toffler Alvin and Heidi, *War and Anti War, making sense of today's global chaos*, (Warner books 1993)

[12] Waller Douglas, *Onward Cyber Soldiers*, (Time Magazin, August 21, 1995)

