Actual Aspects and Advances of

Information Warfare and E–Terrorism

1 Parameters, Properties of Information Warfare (IW).
2 Actual and former Cases of IW and E–Terrorism.
3 Attack Types.
4 Profiling Attackers.
5 Future Developments. Seven Theses.
**Information Warfare**

**Definition**

Attacking computers using computers.

Attacker and defender are nations.
Warfare is defined in the Geneva convention.

Mostly software is the weapon.
Targets are
- Access control system.
- Software.
- Data.

---

**E–Terrorism**

**Definition**

Attacking computers using computers.

Attacker and defender are nations, agencies, companies, persons.

Mostly software is the weapon.
Targets are
- Access control system.
- Software.
- Data.
**Business e-Terrorism: Cases**

- Contractor: Availability of 1 of 7 servers unsufficient.
  Sabotage of the CRM-Servers.

- ...

---

**Business Information Warfare**

*Attacking the most valuable parts of the Business.*

With the aim to disturb or take over the whole Business of a company.
Information Warfare and E–Terrorism

1 Parameters, Properties of Information Warfare (IW).

2 Actual and former Cases of IW and E–Terrorism.

3 Attack Types.

4 Profiling Attackers.

5 Future Developments. Seven Theses.
**Business Information Warfare: Cases**

- Bloomberg / Reuters.
- Virgin Islands / British Airways.
- Manipulated credit transfer (Banking System).
- Manipulation of credit transfer.
- Copying costing data of the biggest German retailer (espionage).

---

**Industrial and Foreign Espionage**

Most damaging stolen information

- Pricing data, manufacturing processes, product development specifications.
- Customer lists, sales data, cost data, contract data, proposals, strategic plans, negotiating positions, compensation data, personnel data, basic research.
Information Warfare

Societies are vulnerable to electronic/digital attacks.

- Vulnerability of a state or society:
  Information societies – highly computerized.

- Vulnerability of critical information infrastructures.

Scenarios

- Manipulating e-voting systems ⇒ Other government.
- Disturb power supply ⇒ business and daily life goes down, companies go bankrupt because of missing business.
- ...

© H. Pohl
Mutual Dependencies, Interactions of Infrastructures

- Logistics: Shipping, carriers, parcel services
- IT-Systems of Partners (contractors, clients)
- Energy supply: Gas, oil, electricity, Water supply, Air
- Transport: River, sea, railway, highways, air
- IT-Processes, IT-Systems, Intranet-, Extranet, Internet-Connections
  company, governmental agency, nation
- Public Services: Fire brigade, police, health service
- Fone, Fax, Mobile Fone
- Internet, ICT
- Banking system
- Energy supply: Gas, oil, electricity, Water supply, Air

IT-Dependability: Monocultures

- Hardware – only a few manufacturers, only a few hardware architectures.
- Software – only a few manufacturers.
- Tools – only a few manufacturers.
- Standards – only a few for the Internet: TCP/IP based.
Information Warfare and E–Terrorism

1 Parameters, Properties of Information Warfare (IW).
2 Actual and former Cases of IW and E–Terrorism.
3 Attack Types.
4 Profiling Attackers.
5 Future Developments. Seven Theses.

Development of Attack Tools

- Password guessing
- Password cracking
- Self-replicating code
- Auto-exploiting vulnerabilities
- Backdoors
- Hijacking sessions
- Know How needed

- Packet forging, spoofing
- Scanning tools
- Sniffer, sweepers
- DDoS
- Online virus generator
- Flash worms
- Packet forging, spoofing
- Scanning tools
- Sniffer, sweepers
- DDoS
- Online virus generator
- Flash worms

Know How needed
**Code Red Worm**

Number infected Servers in Mio.

© H. Pohl

**Flash-/Warhol-Worms**

Number infected Servers in Mio.

© H. Pohl
Viruses per e-mail

Organized Crime

- Guys talking to papers and TV.
- Hierarchical organized: Customer, Manager, Wholesaler, "Hacker".
  Searching Adresses, Data Copying, Manipulating, Hardware, Operating System.
Number of reported Incidents 1995 – 2003

One incident may involve one site or hundreds (or even thousands) of sites.

Number of reported Vulnerabilities 1995 – 2003

About 4,000 security relevant vulnerabilities published.
Patches

- Number of Patches per week ~ 80.
- Only a few companies test the patches and install it.
- Attackers: Reengineering of vulnerabilities by investigating the patch.
  The attacker can make use of the understood vulnerability as long as the patch is not installed.

'Time to patch' becomes shorter – Attackers are faster:
Is the patch published during the week – most of the attacks appear already on the following weekend.

Attacks by layer

Examples:
- Physical access: Remove the disk, FD-Boot, ...
- Intrusion Attacks, TCP Hijacking (Man-in-the-middle), Packet replay.
- Packet manipulation: Address spoofing
- Security Guard
- IP Sequence Number Guessing.
- Routing Attacks (RIP - Routing Information Protocol)
- Tunneling (UDP, ICMP)
- All (unsecure) protocols.
- Password Cracking, e-mail Impersonation, Identity Theft.
- Eavesdropping (data, Passwords, mail) and manipulating on all layers.
- Manipulating the access control: Trap door, Back Door, Social Engineering, Viruses, Worms, Agents, ...
- Buffer Overflow: Overwriting program code.
- Out-of-Bound (OOB) Data: Sending non-defined data ⇒ abnormal behaviour.
- (Distibuted) Denial of Service.
**Actual Damage Costs**

- Viruses and malicious code worldwide loss: $13 Billion.
- Theft of proprietary information (espionage) from Fortune 1000 companies: $45 Billion.
- The acknowledged losses of manufacturing companies averaged per incident: $50 Million.
- 75% of all US companies have disciplined employees for misusing Internet privileges.
- 33% of all US companies (6-150,000 employees) have terminated employees for misuse of the Internet.

---

**Threat Spectrum**

<table>
<thead>
<tr>
<th>Type</th>
<th>Attacker</th>
<th>Aim</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Security Threats</td>
<td>Information Warrior</td>
<td>Strategic Advantage, induce Chaos, Specific Target</td>
</tr>
<tr>
<td></td>
<td>National Intelligence</td>
<td>Information for Political, Military, Economic Advantage</td>
</tr>
<tr>
<td>Shared Threats</td>
<td>Terrorists</td>
<td>Visibility, Publicity, Chaos, Political Change</td>
</tr>
<tr>
<td></td>
<td>Industrial Espionage</td>
<td>Competitive Advantage, Intimidation</td>
</tr>
<tr>
<td></td>
<td>Organized Crime</td>
<td>Revenge, Retribution, Financial Gain, Institution, Change</td>
</tr>
<tr>
<td>Local Threats</td>
<td>Institutional Hackers</td>
<td>Monetary Gain, Prestige</td>
</tr>
<tr>
<td></td>
<td>Recreational Hackers</td>
<td>Thrill, Challenge</td>
</tr>
</tbody>
</table>
Information Warfare and E–Terrorism

1 Parameters, Properties of Information Warfare (IW).
2 Actual and former Cases of IW and E–Terrorism.
3 Attack Types
4 Profiling Attackers.
5 Future Developments. Seven Theses.

Motives of Computer Abuse

- Make a joke, Play instinct.
- Need for admiration (open - covert)
- Avarice (money)
  - Occasion: Satisfaction of one's needs, dissatisfaction; discontent, unhappiness.
  - Economic espionage by competitors.
  - Illegal transfer of technology: Former SU, Asia, ...
- Destructive mania
  - Sabotage: Alter, damage or delete information, denial of Service.
  - Vandalism.
- Political
  - Damage public image, political statement or terrorism.
- Inadmissible /criminal exercise of power.
Attacker – Profiling of Perpetrators

Authorized

Employees

Unauthorized

Freaks, Hacker, Cracker, Skripties

Contractors, Outsourcers

Internal:

Maintenance, Cleaning man and ladies

External:

Manufacturers, Business Partners

Users, edp–collaborator

System, Network Administrators, Former Employees

Specialists for Internet-Protocols, Operating Systems, Standard-Software

Attacker – Profiling by Gender and Age

Gender: Male, Female

Age: 0–20, 20–29, 30–39, 40–49, 50–59, 60–
Information Warfare and E–Terrorism

1 Parameters, Properties of Information Warfare (IW).
2 Actual and former Cases of IW and E–Terrorism.
3 Attack Types.
4 Profiling Attackers.
5 Future Developments. Seven Theses.

Why Security Problems?

- **Complexity**
  Hardware, Operating System, Tools, Data Base System, Application Software, Peripheral Components (USB, Bluetooth, Wireless)

- **Design**
  Security Design?

- **Bugs, Errors**
  Bad Programming

- **Networks, Interaction**
  Partners, Contractors, ERP – Ubiquity, Pervasion

- **Programs**

- **Men**
  Unpredictable Employees and others.
Cyberwar, Cyberterrorism and Industry

- **Information Warfare** and E-Terrorism are plausible war alternatives.
- The weapons (attack types) of Information Warfare can **outflank and circumvent** military establishments. Military establishment is not prepared.

The Security Needs

- Education
- Business: Security Strategies
- Attack and Security Information Sharing
- Law Enforcement
- International Working Partnership
The Attackers’ Advantage

- Ubiquity: Cheap global access to the Internet. Computers are available all over the world.


- Global high quality Knowledge of Communication and Information Technology (CIT): Specialists in networking, operating systems, application software as enterprise resource management (SAP, Peoplesoft).

- The Defender must succeed – The attacker need not. Warriors and Terrorists are hunting in packs and Coordinate their attack in time and space.

Law Enforcement, Arms Control

- Law Enforcement normally operates in a Reactive Mode. Law Enforcement’s electronic capabilities are about 5 – 10 years behind the transnational terrorism curve.

- No international regulation. European Network and Information Security Agency – ENISA.

- Internet Police? There is no single international organization responsible for Internet Security.

- There are no discussions on voluntary arms control until today.
Development of automated Tools

- Distributed Intrusion Protection System (DIPS).
- Distributed IDS (DIDS): Early Warning System.
- Intrusion Protection Systems (IPS).

7 Theses IW

1. Aims and Motives.
2. Attack Types.
3. Perpetrators and Motives.
5. Critical Infrastructure Protection.
7. Arms Control.
Summary

- High Technical Level of Computer Usage of Warriors and Terrorists. Computers are cheap and Internet usage too [asymmetric warfare].

- The Threat of Information Warfare and E-Terrorism is real and will become extremely harmful.

- The Internet is the Battlefield with fone and mobile devices.


A Multiple Threat and a Shared Responsibility for all Peaceloving People and Nations.