Actual Aspects and Advances of

Information Warfare and E–Terrorism

Prof. Dr. Hartmut Pohl

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.

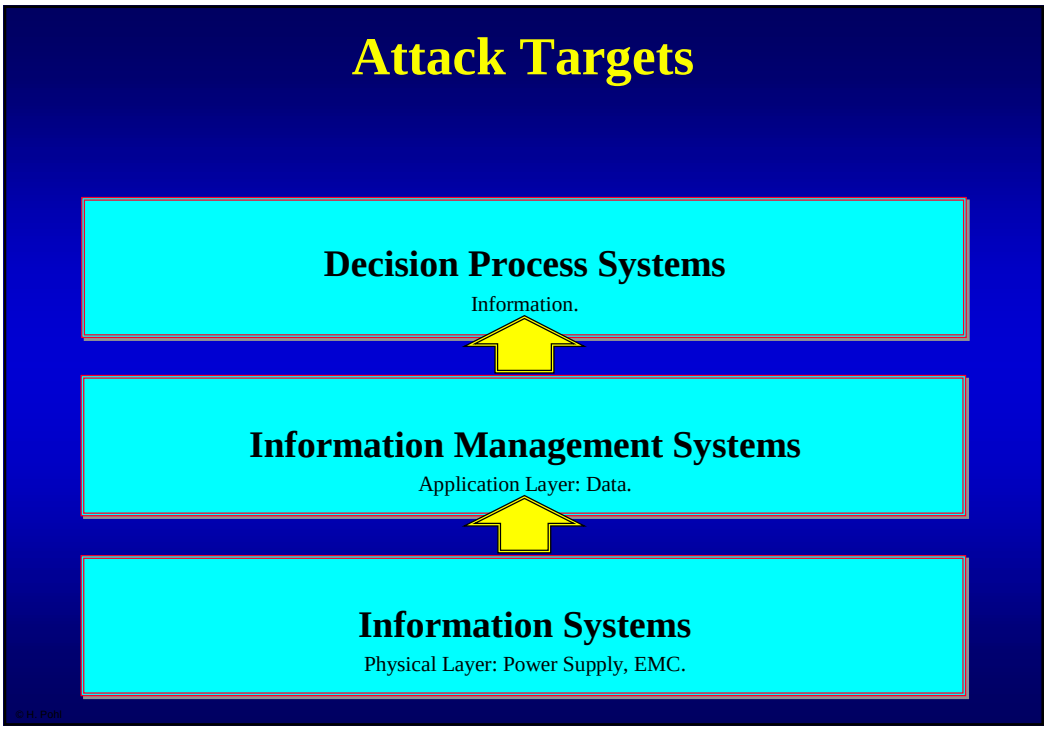
Business e-Terrorism: Cases

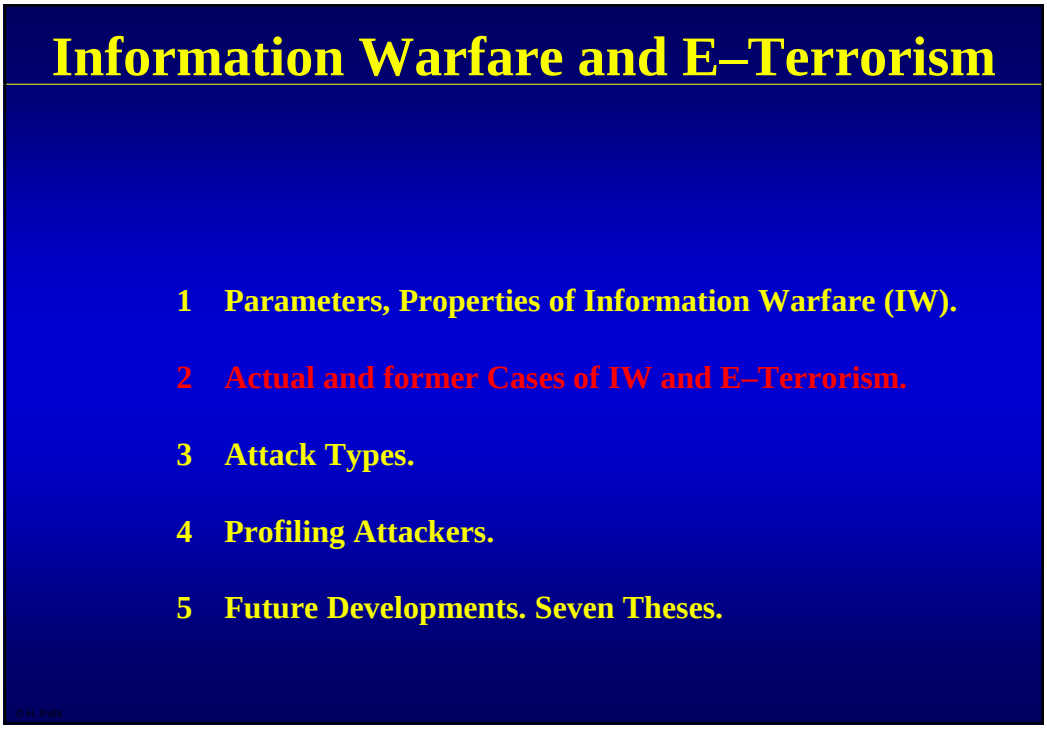
- Contractor: Availability of 1 of 7 servers unsufficient. Sabotage of the CRM–Servers.
- ...

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.


Attack Targets
Decision Process Systems
Information.
Information Management Systems
Application Layer: Data.
Information Systems
Physical Layer: Power Supply, EMC.
© H. Pohl


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.
© H. Pohl

Business Information Warfare: Cases

- Bloomberg ./. Reuters.
- Virgin Islands ./. British Airways.
- Manipulated credit transfer (Banking System).
- European Commission, Brussels ./. US Agencies.
- 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.

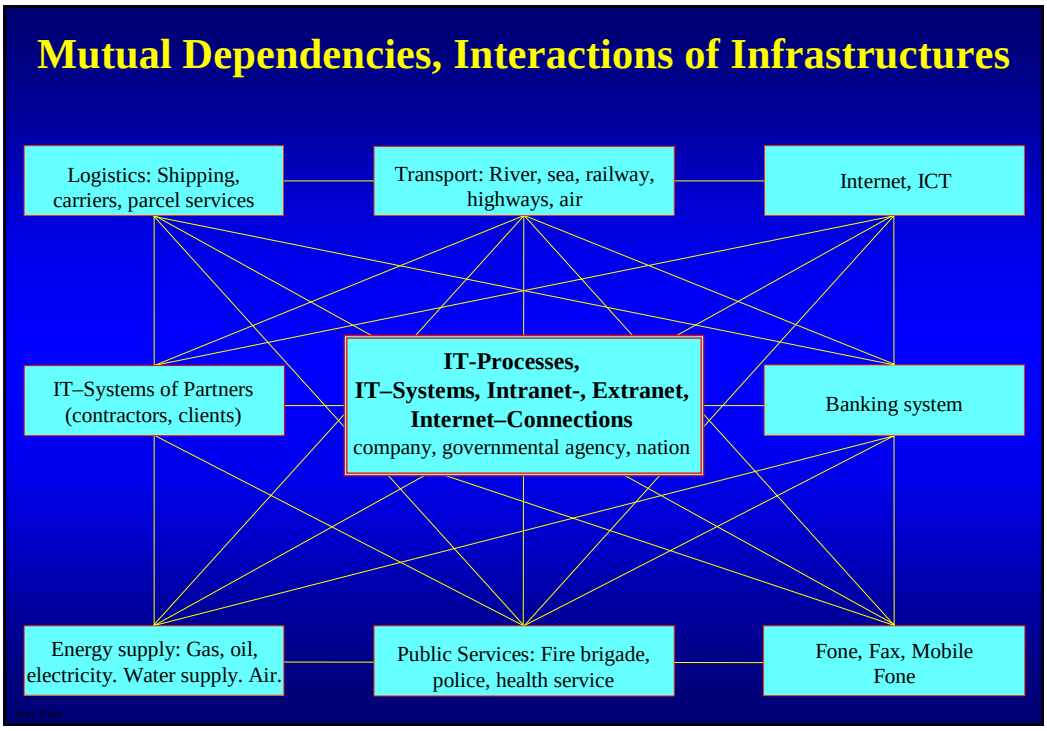
Information Warfare

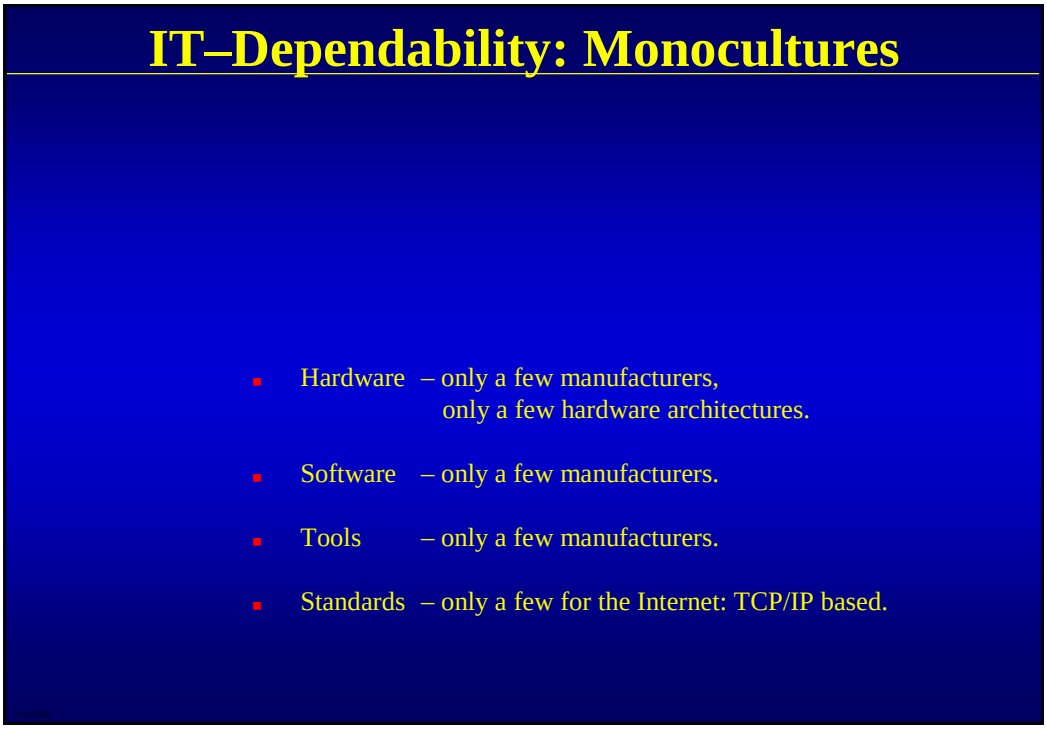
Societies are vulnerable to electonic/digital attacks.

- 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 bussiness.
- ...


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


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.
© H. Pohl

Information Warfare and E–Terrorism

1 Parameters, Properties of Information Warfare (IW).

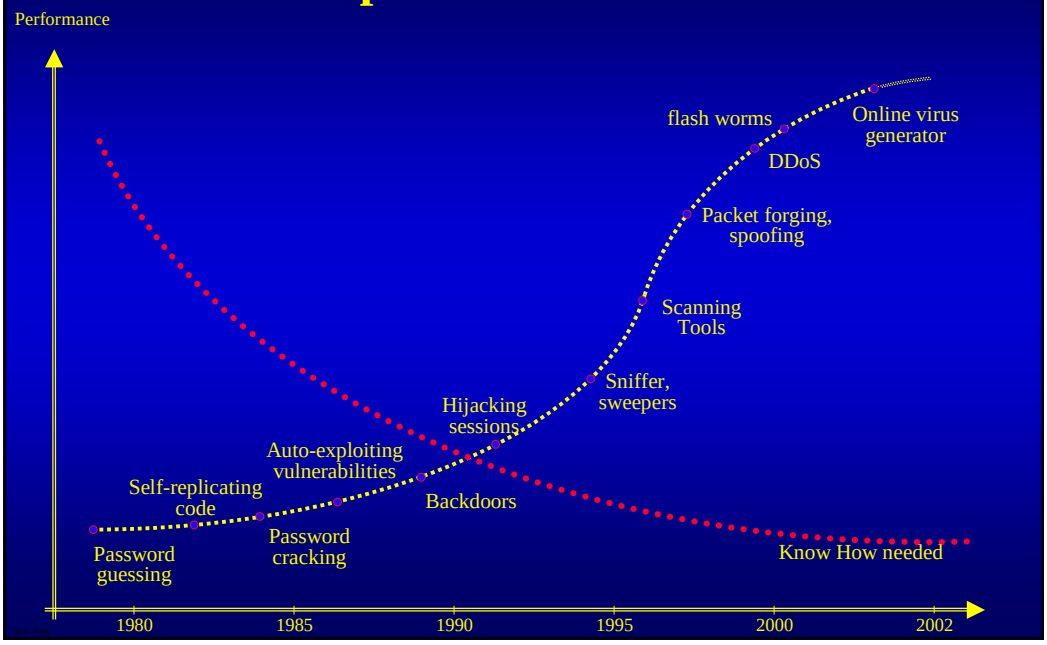
2 Actual and former Cases of IW and E–Terrorism.

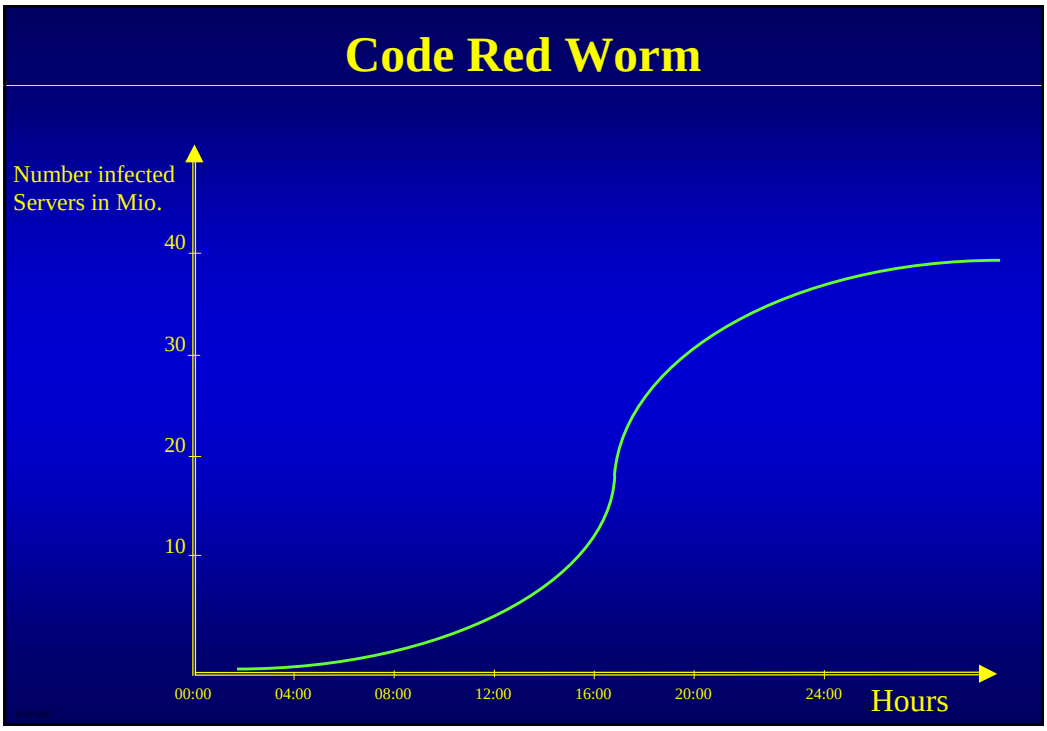
3 Attack Types.

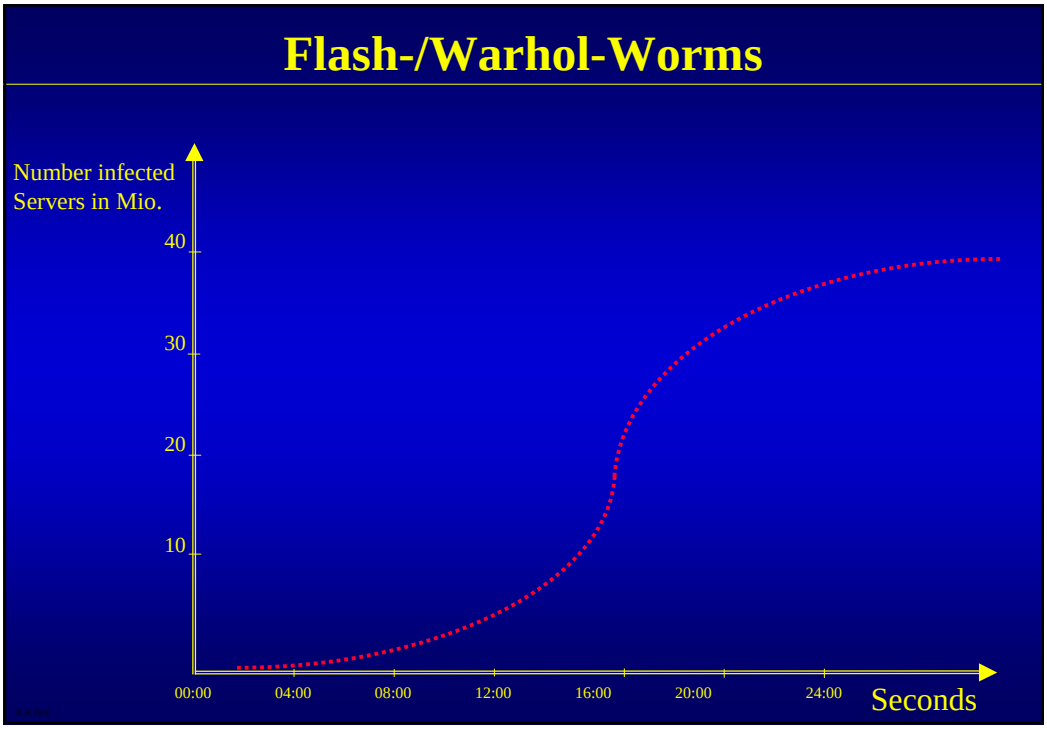
4 Profiling Attackers.

5 Future Developments. Seven Theses.

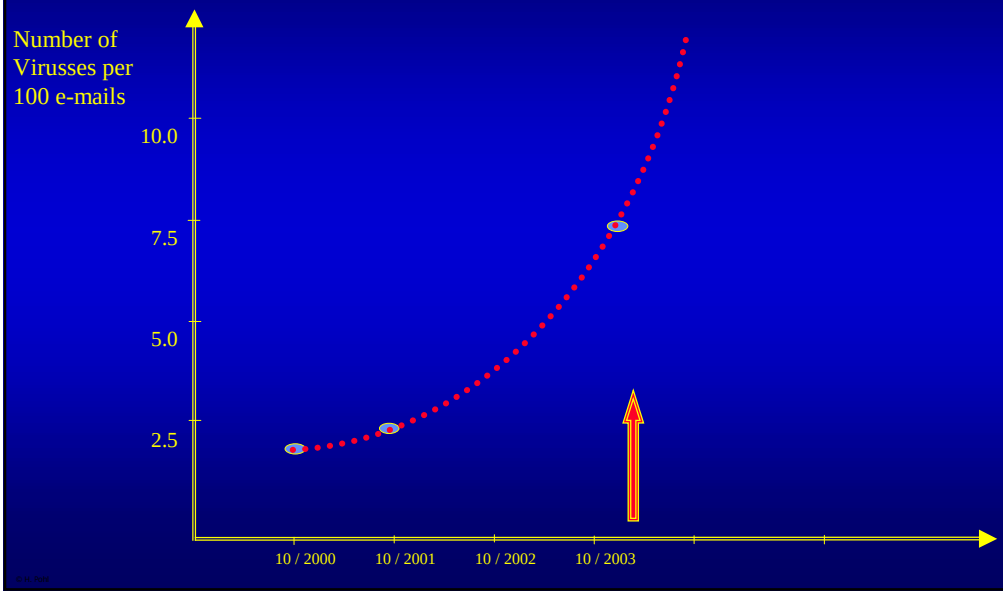
Development of Attack Tools




Code Red Worm
Number infected
Servers in Mio.
40
30
20
10
00:00
04:00
08:00
12:00
16:00
20:00
24:00
Hours


Flash-/Warhol-Worms
Number infected
Servers in Mio.
40
30
20
10
00:00
04:00
08:00
12:00
16:00
20:00
24:00
Seconds

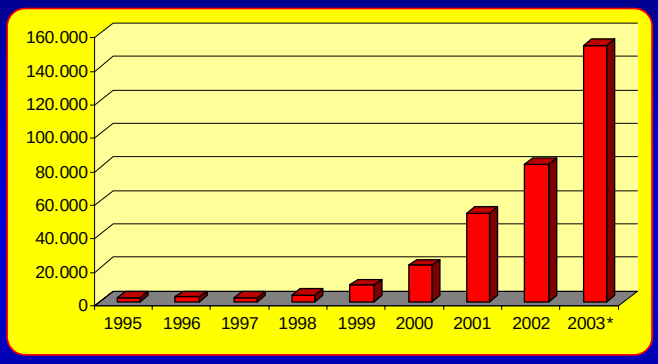
Viruses per e-mail



Organized Crime

- Guys talking to papers and TV.
- "Silent Guys", "Advisers", "naive" Practicians.
- Hierarchical organized: Customer, Manager, Wholesaler, "Hacker".
  Searching Adresses, Data Copying, Manipulating, Hardware, Operating System.

Number of reported Incidents 1995 – 2003



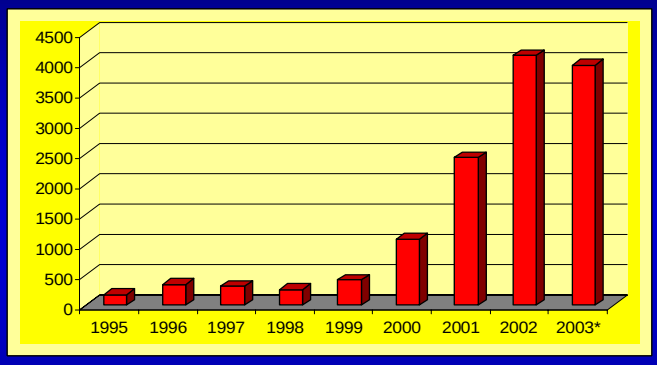
1995	1996	1997	1998	1999	2000	2001	2002	2003*
2.412	2.573	2.134	3.734	9.859	21.756	52.658	82.094	153.140

CERT/CC

* January until September: 114.855

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

Number of reported Vulnerabilities 1995 – 2003



1995	1996	1997	1998	1999	2000	2001	2002	2003*
171	345	311	262	417	1.090	2.437	4.129	3976

About 4.000 security relevant vulnerabilities published.

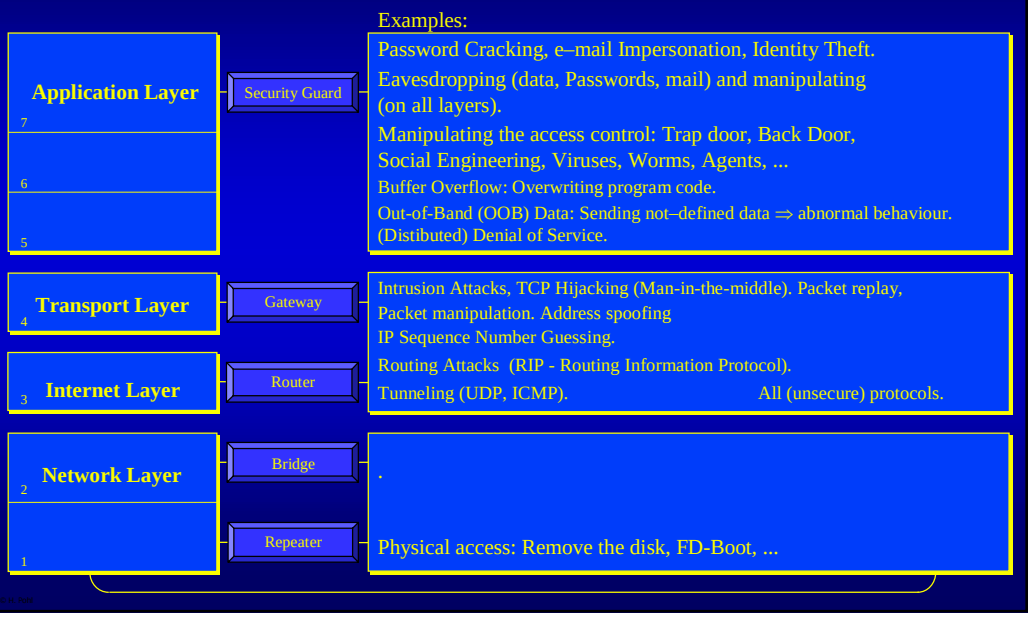
CERT/CC

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



Actual Damage Costs

- Viruses and malicious code world wide loss $13 Billion.
- Theft of proprietary information (espionage) $45 Billion.
  Fortune 1000 companies.
- 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.

Fortune 1000 companies 2001

Threat Spectrum

Type	Attacker	Aim
National Security Threats	Information Warrior	Strategic Advantage, induce Chaos, Specific Target
	National Intelligence	Information for Political, Military, Economic Advantage
Shared Threads	Terrorists	Visibility, Publicity, Chaos, Political Change
	Industrial Espionage	Competitive Advantage, Intimidation
	Organized Crime	Revenge, Retribution, Financial Gain, Institution. Change
Local Threats	Institutional Hackers	Monetary Gain, Prestige
	Recreational Hackers	Thrill, Challenge

Information Warfare and E–Terrorism

1 **Parameters, Properties of Information Warfare (IW).**

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

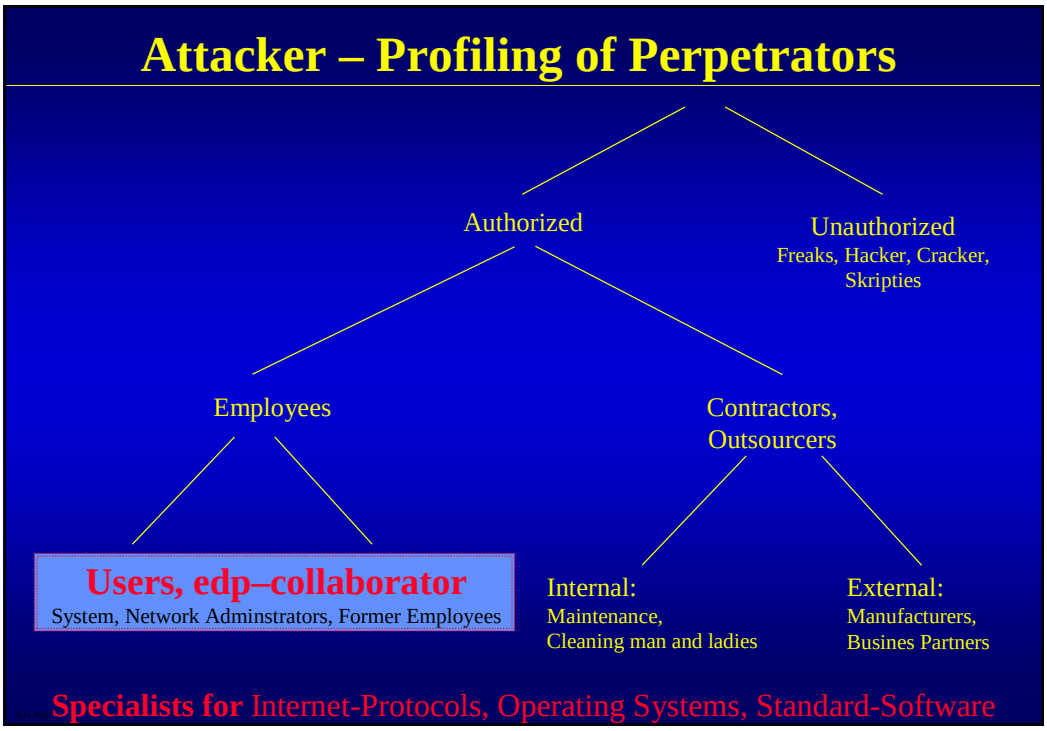
3 **Attack Types**

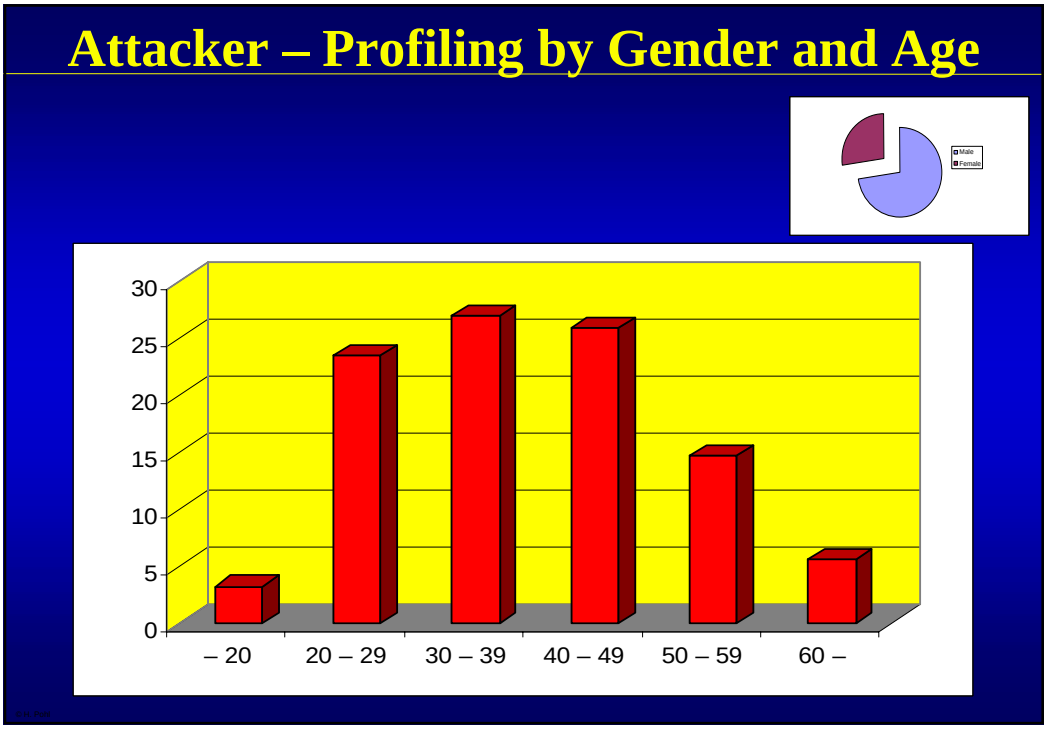
4 **Profiling Attackers.**

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
Unauthorized
Freaks, Hacker, Cracker, Skripties
Employees
Contractors, Outsourcers
Users, edp–collaborator
System, Network Adminstrators, Former Employees
Internal:
Maintenance, Cleaning man and ladies
External:
Manufacturers, Busines Partners
Specialists for Internet-Protocols, Operating Systems, Standard-Software


Attacker – Profiling by Gender and Age
Male
Female
30
25
20
15
10
5
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?

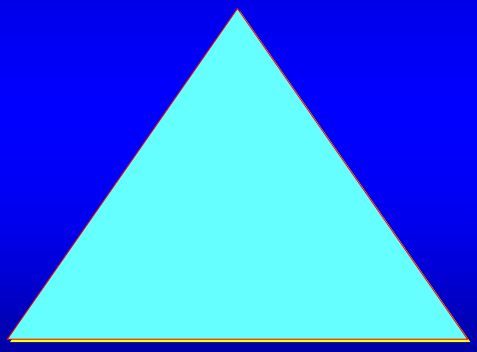
- **Complexity** — Hardware, Operating System, Tools, Data Base Sstem, Application Software, Peripheral Components (USB, Bluetooth, Wireless)
- **Design** — Security Design?
- **Bugs, Errors** — Bad Programming
- **Networks, Interaction** — Partners, Contractors, ERP – Ubiquity, Pervasion
- **Programs** — Try–out, Attacks, Attack–Tools.
- **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 prepaired.

The Security Needs

Education



Business: Security Strategies

Attack and Security Information Sharing

Law Enforcement

International Working Partnership

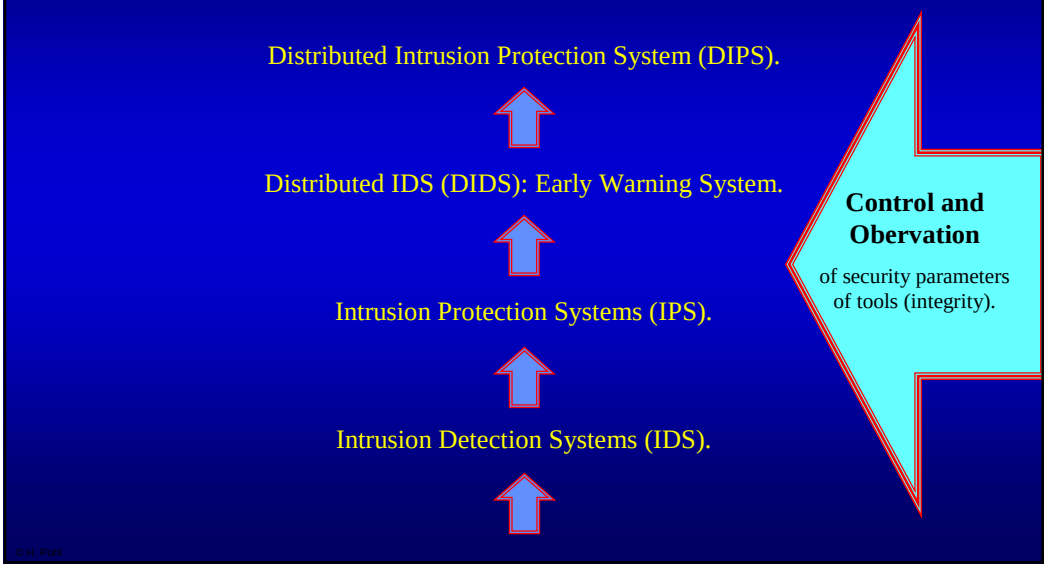
The Attackers Advantage

- Ubiquity: Cheap global access to the Internet.
  Computers are available all over the world.
- Growth in Networks and connectivity.
  Operations vs. Security vs. Cost.
- 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



7 Theses IW

1 Aims and Motives.

2 Attack Types.

3 Perpetrators and Motives.

4 National Activities vs. Coordinated Global Planning.

5 Critical Infrastructure Protection.

6 Legal, Political and Technical Security Measures.

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.
- The Government, Industry, Commerce and E-Commerce
  and Individual Users live in the Battlefield: Militarization of the economy.

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