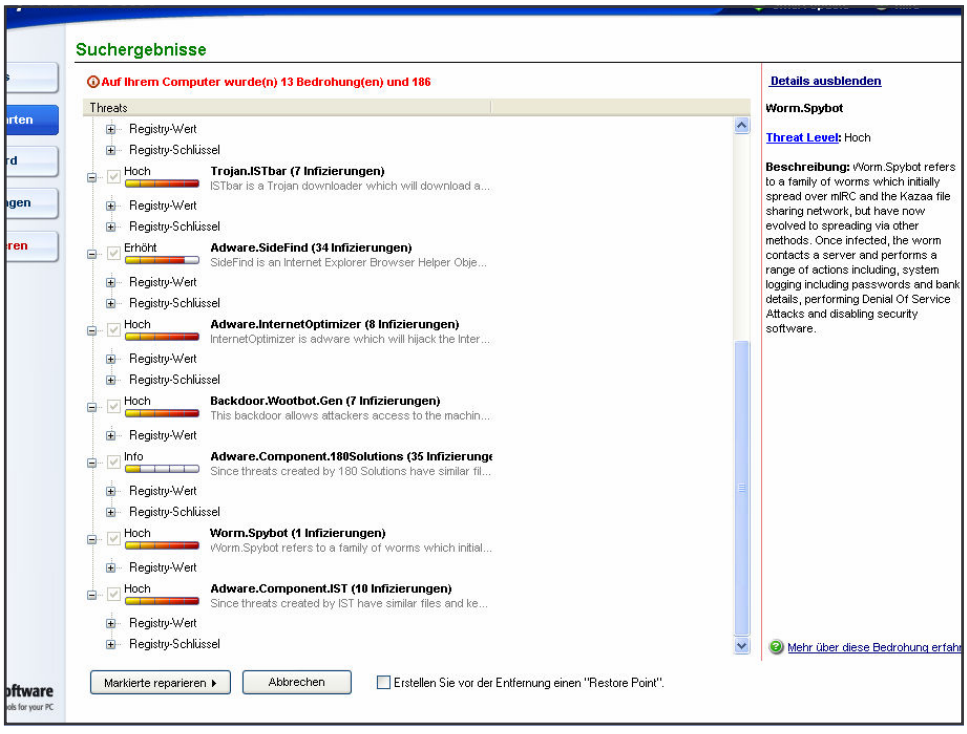
COUNCIL OF EUROPE CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Cybercrime: threats and challenges

Workshop on cybercrime legislation and training of judges (Plovdiv, Bulgaria, 17-18 December 2007)

Alexander Seger
Council of Europe,
Strasbourg, France
Tel +33-3-9021-4506
alexander.seger@coe.int



1 Why take measures against cybercrime?

Cybercrime – current challenges

Put cybercrime in context:

- In 2007, 1 billion+ Internet users worldwide. Probably 99.9% use ICT for legitimate purposes
- Need to balance concerns for security and fundamental rights and freedoms

1. Dependency of societies on information and communication technologies. This dependency makes societies highly vulnerable to cybercrimes

WORLD INTERNET USAGE AND POPULATION STATISTICS

World Regions	Population (2007 Est.)	Population % of World	Internet Usage, Latest Data	% Population (Penetration)	Usage % of World	Usage Growth 2000-2007
Africa	933,448,292	14.2 %	**43,995,700**	4.7 %	3.5 %	874.6 %
Asia	3,712,527,624	56.5 %	**459,476,825**	12.4 %	36.9 %	302.0 %
Europe	809,624,686	12.3 %	**337,878,613**	41.7 %	27.2%	221.5 %
Middle East	193,452,727	2.9 %	**33,510,500**	17.3 %	2.7 %	920.2 %
North America	334,538,018	5.1 %	**234,788,864**	70.2 %	18.9%	117.2 %
Latin America/Caribbean	556,606,627	8.5 %	**115,759,709**	20.8 %	9.3 %	540.7 %
Oceania / Australia	34,468,443	0.5 %	**19,039,390**	55.2 %	1.5 %	149.9 %
WORLD TOTAL	6,574,666,417	100.0 %	**1,244,449,601**	18.9 %	100.0 %	244.7 %

2. Malware – that is, malicious codes and programmes including viruses, worms, trojan horses, spyware, bots and botnets – is evolving and rapidly spreading

Software inserted into an information system that causes harm to this or other systems

For example: more than 210,000 new malicious code threats reported Jan-June 2007 (Symantec)

Types:
- Backdoors allowing unauthorised access
- Key loggers
- Rootkits concealing that a computer is compromised
- Spam as a vector for malware
- Spyware capturing and transmitting user data
- Trojan horses to circumvent security measures and carry out attack
- Virus to reduced system performance, destroy data or cause other damage
- Worms (self-replicating)

2. Malware ...

Disseminated through:

- Email
- Web
- Instant messengers
- P2P
- Shared-file systems
- Internet Relay Chat
- Removable media

Used for:

- Denying access (distributed denial of service attacks through bots and botnets)
- Extortion
- Stealing information, including identity theft

2. Malware ...

Bots and Botnets

Covertly installed programmes on a computer to allow unauthorised remote control

Can be used
- ➢for distributed denial of service (DDOS) attacks
- ➢to harvest confidential information (identity theft)
- ➢to distribute spam, spyware, adware
- ➢for phishing attacks

For example:> 52,000 active bot-infected computers per day in 2007, 27% of bot infected computes in China, 13% in USA, 10% in Poland; 43% of command and control servers in USA; 61% of DOS attacks targeted USA (Symantec)

2. Malware ...

Identity theft

The misuse of the identity (name, date of birth, address, financial information or other personal details) of another person without knowledge or consent
Used to commit a wide variety of crimes
Forms:
- ➢"Theft": Bin raiding, hacking, spyware and other crimeware (e.g. Keyloggers), skimming of credit cards etc.
- ➢Social engineering (deception and psychological manipulation to make people comply with a request):
  - Phishing ("password fishing"), spoofing (fake sites or emails), pharming, vishing, smishing etc

For example: 12.5 million phishing emails per day blocked in 2007 (Symantec); 18% increase in unique phishing messages in 2007 compared to first half of 2006; 59% phishing sites based in USA

Make identity theft a separate offence?

3. Spam nuisance and carriers of malware

- More than 60% of email traffic considered spam
- 47% of spam detected worldwide originated from USA
- 1 / 233 spam contained malicious codes

(Symantec data for Jan-June 2007)

4. Child pornography and sexual exploitation on the internet increasingly commercial

- Increasing reporting on child pornography on the internet
- Problem: legislative gaps in many countries
- Child porn sites hosted in many different countries (see www.iwf.org.uk)
- Increasing number of commercial sites
- Convention on Cybercrime: opportunity for broad criminalisation and international cooperation against child porn on the internet

5. Offenders increasingly organising for crime aimed at generating illicit profits

- ICT facilitate offences by OC groups and networks, in particular economic crime
- ICT creates vulnerabilities -> exploited by OC
- ICT facilitate logistics, anonymity and reduce risks of OC
- ICT facilitate global outreach of OC
- ICT shape OC -> networks

Emergence of underground economy servers to sell stolen information

Breakdown of goods in 2007:
1 Credit cards 22%
2 Bank accounts 21%
3Email passwords 8%
4Mailers 8%

6. Botnets one of the central tools of criminal enterprises (DDOS, extortion, placing of adware and spyware)

Underground service economy developing: botnets for rent

Division of labour in criminal projects:

- **Coder = writer of malicious code**
- **Launcher = runs the code**
- **Miner = extracts data**
- **Washer = launders proceeds**

(Europol)

7. Shift in the threat landscape: from broad, mass, multi-purpose attacks to specific attacks on specific users, groups, organisations or industries, increasingly for economic criminal purposes

For example:

- data breaches with possible identity theft: 30% in education sector, 26% government, 15% health, 14% financial sector in 2007 (Symantec)
- 72% of spoofed websites were sites of financial service organisation

8. Growing risk of cyber-attacks against critical infrastructure

The question of cyberterrorism

Terrorist may use information and communication technologies for:

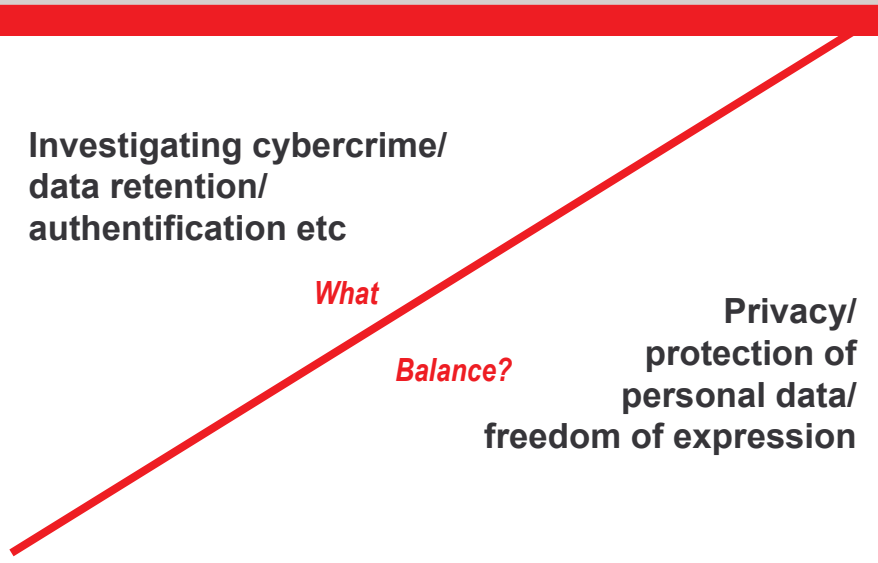
- Attacks via the internet aimed at essential electronic communication systems, IT infrastructure and other systems and infrastructure
- Dissemination of illegal contents, including threats, inciting, advertising, fundraising, recruitment, dissemination of racists and xenophobic material
- Logistical purposes, including communication, target analysis, acquisition of information

New challenges

9. Remote storage of data (problem for investigators)

10. Next-generation-networks (NGN), including VoIP (problem for investigators)

Issues (1)



Issues (2)

Law enforcement

What

relationship?

Service providers

Issues (3)

Efficiency of investigations/
technical possibilities

What

safeguards?

Due process

Threats: overview

Dependency of societies on information and communication technologies.
This dependency makes societies highly vulnerable to cybercrimes

- Shift in the threat landscape: from broad, mass, multi-purpose attacks to specific attacks on specific users, groups, organisations or industries, increasingly for economic criminal purposes
- Malware – that is, malicious codes and programmes including viruses, worms, trojan horses, spyware, bots and botnets – is evolving and rapidly spreading
- Spam nuisance and carriers of malware
- Child pornography and sexual exploitation on the internet increasingly commercial
- Offenders increasingly organising for crime aimed at generating illicit profits
- Offences related to identity theft
- Use of internet for terrorist purposes (attacks against infrastructure, logistics, recruitment, finances, propaganda)
- Botnets one of the central tools of criminal enterprises (DDOS, extortion, placing of adware and spyware)
- Growing risk of cyber-attacks against critical infrastructure

But: Vast majority of people use ICT for legitimate purposes
Need to balance security and civil rights concerns

Thank you.

Alexander.seger@coe.int