COUNCIL OF EUROPE CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Cybercrime – the challenge

Regional conference on cybercrime
Casablanca, Morocco, 19-20 June 2007

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

1

First session
Cybercrimes: identification and specification

I. **Situation analysis and identification of new threats (Octopus Interface Conference, Strasbourg, 11-12 June 2007)**

II. **For discussion: Identify theft, cyber-terrorism**

III. **Cybercrime typology according to the Convention on Cybercrime**

Council of Europe

2

Octopus Interface Conference – Strasbourg, 11-12 June 2007

Cybercrime situation analysis and identification of new threats:

1. **Dependency of societies on information and communication technologies. This dependency makes societies highly vulnerable to cybercrimes**
2. **Malware – that is, malicious codes and programmes including viruses, worms, trojan horses, spyware, bots and botnets – is evolving and rapidly spreading. Used for:**
   - **Denial of service attacks**
   - **Identity theft (phishing and other social engineering techniques)**
   - **Fraud, money laundering and other economic crimes**
3. **Spam nuisance and carriers of malware**

Council of Europe

Cybercrime - the challenge 3

3

4. **Child pornography and sexual exploitation on the internet increasingly commercial**
5. **Offenders increasingly organising for crime aimed at generating illicit profits**
6. **Botnets one of the central tools of criminal entreprises (DDOS, extortion, placing of adware and spyware). Underground service economy developing (botnets for rent)**
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**

Council of Europe

Cybercrime - the challenge 4

4

Council of Europe

New challenges

8. **Growing risk of cyber-attacks against critical infrastructure**

9. **Remote storage of data (problem for investigators)**

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

5

II Cybercrimes: issues for discussion

Council of Europe

Identify theft and identity fraud

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

6

II Cybercrimes: issues for discussion

Identify theft and identity fraud

Council of Europe

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 discussion:

- **Should identity theft be made a separate offence?**
- **Or sufficiently covered by existing legislation and instruments (e.g. Convention on Cybercrime)?**

Cyberterrorism

Council of Europe

Terrorist may use information and communication technologies for:

- **Attacks via the internet aimed at essential electronic communcation systems, IT infrastructue 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**

Cybercrimes: issues for discussion

Cyberterrorism: New instruments required?

(question under discussion at the CoE's Committee on Terrorism, CODEXTER)

- Cyberattacks covered by Art 4 (data interference) and Art 5 (system interference) of the Convention on Cybercrime
- Investigative tools and international cooperation also covered by the Convention
- Recruitment, incitement etc covered by the Convention for the Prevention of Terrorism (CoE)
- Most other issues covered by other existing Conventions.

Council of Europe

Cybercrime - the challenge 9

9

Cybercrimes: issues for discussion

Cyberterrorism: New instruments required? (question under discussion at the CoE's Committee on Terrorism, CODEXTER)

- Main challenge: ensure broad and full implementation of the Convention on Cybercrime
- Other proposals:
  - Rules regarding illegal content (versus freedom of expression
  - Common rules for Service Providers (such as notice and takedown procedures)
  - Data retention (to permit traceback)
  - Covert online searches (problematic in terms of privacy)

Council of Europe

Cybercrime - the challenge 10

10

III Typology of cybercrimes

The Convention on Cybercrime

Chapter I: Definitions

(what is a computer system, computer data, service provider, traffic data)

Chapter II: Measures at national level

Section 1 - Substantive criminal law

(behaviour that is to be made a criminal offences)

Section 2 - Procedural law

(measures for more effective investigations of cybercrimes)

Section 3 - Jurisdiction

Chapter III: International cooperation

Section 1 - General principles of cooperation

Section 2 - Specific provisions for more effective cooperatio

Chapter IV: Final provisions (including accession by non-member states)

Council of Europe

Typology of cybercrimes (Convention on Cybercrime)

1. Offences against the confidentiality, integrity and availability of computer data and systems

- Art 2: illegal access
- Art 3: illegal interception
- Art 4: data interference
- Art 5: system interference
- Art 6: misuse of devices

2. Computer-related offences

- Art 7: computer-related forgery
- Art 8: computer-related fraud

3. Content-related offences

- Art 9: Child pornography
- Protocol: Xenophobia and racism

4. Infringement of copyright and related rights

- Art 10 copyright related offences

Council of Europe

Council of Europe

Thank you.

Alexander.seger@coe.int

13