itapa
>Information Technologies And Public Administration

Cybercrime in Europe

Jos Dumortier
Professor of Law – University of Leuven/Belgium
Lawfort – Of Counsel – Bar of Brussels

lawfort

Scheme

1. The concept of “cybercrime”
2. The European Cybercrime Convention
3. The EU policy with regard to cybercrime

Text Only Version

WWW.CYBERCRIME.GOV

Computer Crime and Intellectual Property Section (CCIPS)
of the Criminal Division of the U.S. Department of Justice

Search for: Search *Hints ...*

Personalized information if you are a...

Parent, Teacher or Student Go!

Computer Crime (e.g., hacking): Policy · International · Cases · Guidance · Laws · Documents

Intellectual Property Crime: Policy · Cases · Guidance · Laws · Economic Espionage · Documents

Cybercrime Documents: Press Releases · Speeches · Testimony · Letters · Reports · Manuals

Cyberethics Information: Parent or Teacher Kids · Related Web Sites

CCIPS is Hiring Experienced Trial Attorneys

CCIPS is Seeking Experienced Information Technology Specialists

Justice Department Announces International Internet Piracy Sweep:
'Operation Site Down' Attacks Organized Piracy Networks in 10 Countries (June 30, 2005)

Federal Law Enforcement Announces Operation D-Elite, Crackdown on P2P Piracy Network:
First Criminal Enforcement Against BitTorrent Network Users (May 25, 2005)

Buccaneer Defendants Sentenced in United Kingdom(May 6, 2005)

International Documents (COE, G8, EU)

Dispelling the Myths about the USA PATRIOT Act

Current Manual Available on Electronic Search and Seizure

Current Manual Available on Prosecuting IP Crimes

Information on Federal Warez Investigation and Prosecution: Operation Buccaneer

1. The concept of “cybercrime”

- hacking/cracking
- virus attack
- denial of service attack
- spamming
- phishing/identity theft
- warchalking
- child pornography
- racism
- conspiracy
- piracy
- counterfeiting
- port scanning
- spoofing
- spyware
- extortion
- auction scam
- trojan horse
- sabotage
- password trafficking
- ...

Council of Europe Convention:

- Four categories:
  - specific computer-related offenses
  - computer-related fraud or forgery
  - content-related crimes
  - intellectual property infringements

“Specific” computer-related crime

- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices

2. European Cybercrime Convention

- Convention n° 185
- Signed in Budapest, 23 November 2001
- Council of Europe Member States
- Extension to third countries: US, Canada, Japan, South Africa
- Entry into force: 1 July 2004
- Slovakia signed 4 Feb. 2005
- Ratified by 10 countries: Slovenia, Croatia, Hungary, Lithuania, Bulgaria, Romania, Estonia, Albania, Cyprus, FYR Macedonia

Council of Europe

English | Français | Deuts

Convention on Cybercrime
CETS No.: 185

Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States

Opening for signature
Place: Budapest
Date : 23/11/2001

Entry into force
Conditions: 5 Ratifications including at least 3 member States
Date : 1/7/2004

What do you want to know about this treaty ?

- Chart of signatures and ratifications
- List of declarations, reservations and other communications
- Full text in Html Format
- Full text in Word Format
- Summary
- Explanatory Report

n http://conventions.coe.int

Cybercrime Convention: Overview

- Measures to be taken by the countries
  - A. Acts to define as « criminal »
  - B. Criminal procedure
  - C. Jurisdiction
- International co-operation

A. Criminal acts

- Goal: common minimum standard of relevant offences
- Categories:
  - specific computer-related offenses
  - computer-related fraud or forgery
  - content-related crimes
  - copyright infringements

B. Procedural law

- Preservation of stored data
- Production order
- Search and seizure of data
- Real-time collection of data

C. Jurisdiction

- Who is competent in an international environment?
- Territoriality principle
- Nationality principle
- Duty to consult

International co-operation

- Extradition
- Mutual assistance
- 24/7 Network

3. European Union Policy

a) Framework Decision on "Attacks against Information Systems"
b) Mandatory Data Retention
c) ENISA
d) Combat against Piracy
e) Safer Internet Plus

a) Attacks against Information Systems

- Framework Decision adopted 24 February 2005
- Two years for implementation in national law
- Harmonised definitions for illegal access and illegal interference
- Harmonised rules on jurisdiction

b) Mandatory Data Retention

- Draft Council Framework Decision
  - Declaration March 2004
  - Proposal FR/IR/SE/UK April 2004
  - Opposition European Parliament
  - Legal obstacles European Commission
  - Opinion Data Protection Commissioners
  - Latest version: October 2005

- Draft Directive
  - Proposal of 21 September 2005

c) ENISA

Regulation 460/2004 of 10 March 2004

- establishing the European Network and Information Agency
- tasks: information – advice – cooperation – awareness – assistance – tracking of standardization initiatives

Status:

- location: Heraklion (Greece)
- 2005 budget: 6.8 million euros
- work programme 2005

d) Combat against Piracy

- European Directive on Conditional Access
  - prohibition of illegal decoding
  - prohibition to manufacture, distribute, import, possess or market illegal decoding devices

- European Intellectual Property Directives
  - application of copyright rules in the digital environment
  - prohibition for devices which circumvent copyright protection
  - enforcement directive 2004/48/EC

Conditional access

- Directive 98/84/EC on the legal protection of conditional access
- The purpose of the Directive is to create a uniform legal environment for the protection of conditional access services, that is, services offered to the public where access is subject to payment of subscriptions such as pay-TV.
- The Directive requires Member States to prohibit, and provide suitable sanctions against, the manufacture and commercial dealing in illegal decoders, smart cards and the like.

Digital rights

- **Directive on copyright in the information society 2001/29/EC**
  - mandatory exceptions, e.g. for technical copies on the net by network operators
  - exhaustive, optional list of exceptions to copyright (e.g. private copying)
  - introduction of the concept of fair compensation for right holders
  - mechanism to secure the benefit for users for certain exceptions where anti-copying devices are in place

Enforcement of digital rights

- **Directive on the enforcement of intellectual and industrial property rights 2004/48/EC**
  - requires all Member States to apply effective, dissuasive and proportionate remedies and penalties against those engaged in counterfeiting and piracy
  - all Member States will have a similar set of measures, procedures and remedies available for right holders to defend their intellectual property rights

Conclusion

- Building the EU regulatory framework and common policy in this area is a difficult process
- Different national views, in particular on the balance between security needs and individual rights slow down the process
- Results are often only obtained in case of strong external pressure

Contact Details

K.U.Leuven – ICRI Tiensestraat 41 3000 Leuven Tel 016 325 149 jos.dumortier@law.kuleuven.ac.be http://www.icri.be	LAWFORT Woluwedal 20 1930 St. Stevens Woluwe Tel 02 710 78 51 jos.dumortier@lawfort.be http://www.lawfort.be