Cooperation without adequate safeguards:
Issues with the CoE Convention on Cybercrime

Meryem Marzouki
CNRS - LIP6/PolyTIC - www-polytic.lip6.fr
European Digital Rights (EDRI) - www.edri.org
Meryem.Marzouki@lip6.fr

Council of Europe Octopus Interface Conference
"Cooperation against Cybercrime"
Strasbourg - June 11-12, 2007

About EDRI

- **Launch:** June 2002

- **Mission**: Defense of civil liberties in the information society

- **Membership**: NGOs. 25 members from 16 European countries (Austria, Belgium, Bulgaria, Czech Republic, Denmark, Finland, France, Germany, Ireland, Italy, Macedonia, The Netherlands, Romania, Spain, Switzerland, UK) + observers

- **Themes**: Privacy, Freedom of Expression, Copyright and patents, E-voting

- **Activities**: Lobbying, Campaigning, Information sharing, raising awareness

- **Observer status**: WIPO, CoE (HR in IS), EC RFID Expert Group

- **Members Involvement**: UN WSIS (HR caucus, Privacy & Security WG,…), UN IGF Dynamic Coalitions (Privacy, FoE online,…)

- **Publication**: Biweekly newsletter since January 2003 (edrigram)

- **Website**: www.edri.org

EDRI and the CoE Convention on Cybercrime

- **Since 2002:** Actions mostly at national levels (implementation) and at EU level (data retention, IPR Enforcement, Content regulation…)

- **EDRI founders**: Members of Global Internet Liberty Campaign (GILC, www.gilc.org)

- **GILC**: formed in 1996, 35 members in 1997, 1/3 EU orgs

- **GILC campaign against CoE Convention on Cybercrime:**

  - Started in 2000 when first draft was made public (v.19)
  - Oct. 18, 2000: first letter to CoE (v.22)
  - Dec. 12, 2000: second letter to CoE (v.24-2)
  - International and national campaigns
  - November 2001, after signature: "Eight Reasons The International Cybercrime Treaty Should be rejected"
  - Feb. 7, 2002: letter to CoE asking for publication of 1st Protocol draft
  - Feb. 10, 2002: draft of Protocol unveiled (v.3 published by CoE on Feb. 20)

"Eight Reasons The International Cybercrime Treaty Should Be Rejected"

Reason #1: Lack of Privacy and Civil Liberties Protections

- No provision to protect citizens' privacy: only vague references in preamble

- No adequate, harmonized safeguards (art.15). April 2000 Opinion of EU Privacy Commissioners not taken into account:
  - "Establishment, implementation and application of the powers and procedures […] are subject to conditions and safeguards provided for under domestic law […]": what happens when they are not effectively in place?
  - Convention expected to be signed and ratified by non CoE countries. Already into force in USA. No adequate privacy protections in some of these countries, while data must be provided upon their request.

Reason #2: A Far Too Broad Convention

- Through its procedural provisions, Convention covers any crime where evidence could be in computerized form

- Computers everywhere in modern life

Reason #3: No Dual Criminality Requirement For International Cooperation

- LEA of a given country forced to cooperate in investigations of behavior illegal in another country, but legal within its borders

- Surveillance of citizens who committed no crime under their own laws

- Mutual assistance requests may come from countries with minimal civil liberties protections

- Danger is growing with new signatures actively encouraged

Reason #4: Protection of Political Activities too weak

- Consequence of no dual criminality requirement: use of the Convention to force one country to cooperate in politically inspired investigations by another.

- Exceptions allowing to refuse cooperation in such cases are limited and not included in all provisions (e.g. real-time data monitoring, art. 33)

- No definition of “political offenses”: a political offense in one country may be a criminal matter in another

- In some provisions, no judicial approval or oversight needed for authorization of official assistance (art.27-2.b): a law enforcement agency could solely decide that an offense is not political and start surveillance

- No reporting requirement of cooperation with foreign countries: no democratic control

Reason #5: Further unbalance of IP laws allowed

- Copyright infringements are criminalized, without any mention of counterbalancing rights (fair use, parodies criticisms,…)

Reason #6: Police given invasive new surveillance powers

- Convention allows for systems for direct access of ISPs and telecom operators networks

Reason #7: Broad criminalization of hacking tools

- Criminalization of tools rather than behaviors

Reason #8: A Convention Drafted in a Closed and Secretive Manner

- A non democratic process: no inclusion of public interest groups, mainly law enforcement authorities

- Little efforts to include concerns of privacy and civil liberties groups

- Lack of balance with adequate safeguards to enforce human rights and the rule of law

Further issues

- The harmonization of content-related offenses:

  - "Minor" equated to "person appearing to be a minor" and to "realistic image of a minor" (some countries: writings, printings, drawings, literary works, sounds)

  - Consequences: threats to freedom of expression and creation (US Supreme Court 2002: criminalization of "virtual child porn" unconstitutional), devaluation of seriousness of child abuse (Statement by Portugal on EU Framework decision 2004/68/JHA of 22/12/03)

  - Age in child porn law (18 in EU, 18 to 16 in Convention) inconsistent with age of sexual consent (13 to 18 in EU countries)

  - Consequences: "efficiency" matters more than rights and legal bases

Further issues (2)

- The increasing delegation of powers to private actors

  - Public-private cooperation more and more encouraged for content regulation through reporting to hotlines, blocking of websites, and filtering of content

  - Hotlines are seldom run or controlled by judicial authorities (in EU, only Belgium and France. Other EU countries: contract/soft law or self-decision)

  - Consequences: possible breaches of freedom of expression, privacy and the rule of law, possible loss of evidences; no transparency, no accountability; massive overblocking of legal content

- The main problem is not addressed

  - Competence of jurisdictions: the Protocol against racism and xenophobia will never solve the Yahoo! case

Conclusion and Recommendations

- The CoE Convention on Cybercrime opened the way to more and more invasive laws, and to the inversion of values: from presumption of innocence to presumption of guilt, from trust to suspicion

- On-line activities and behaviors are more criminalized than their off-line equivalent. Citizens benefit from less protections and safeguards on-line than off-line.

- Before any further extension in scope and/or ratification/accession: need for an assessment of the Convention and its national implementations with regards to human rights, democracy and the rule of law

- Devote an equivalent energy to extend ratifications/accessions to Convention n°108: Protection of Individuals with regard to automatic processing of Personal data (1981)