Council of Europe activities on cybercrime

Review 2014 / Outlook 2015

Strasbourg, 3 February 2015

Alexander Seger
Council of Europe

www.coe.int/cybercrime
Cybercrime

- Hundreds of millions of data sets of individuals (email account data, credit card details, address books, patient records etc.) stolen each year ► Attacks against the right to private life

- Cyber attacks (DDOS, website defacement etc.) against media, civil society, individuals or public institutions ► Attacks against the freedom of expression

- Daily attacks against democratic governments, parliaments, public institutions and critical infrastructure ► Attacks against democracy

- Political disagreements and military conflict accompanied by cyber attacks ► Threat to peace and stability

- Overall, millions of attacks against computers – per day and growing (vulnerabilities)
Electronic evidence

- Evidence in digital form on computer systems is essential for criminal proceedings in relation to ANY type of crime.
  - Example: whom did suspects/offenders (e.g. terrorists) communicate with, where were they at a specific moment in time, is there a connection between different crimes (e.g. terrorist activities)?

- Accessing electronic evidence in increasingly complex:
  - Data stored in foreign, multiple or unknown jurisdictions
  - Multitude of devices
  - Encryption
  - What rules/laws apply?
Criminal justice versus national security measures

- Specified criminal investigations ≠ mass surveillance: confusion in the public/political debate

- Implications:
  - Domestic procedural rules on electronic evidence unstable (see also ECJ Data Retention judgment)
  - Additional requirements for criminal justice access to data
  - Difficult to negotiate additional criminal justice solutions to cybercrime and electronic evidence
  - Unilateral actions and informal arrangements in the absence of international solutions "jungle scenario" with additional risks to human rights and rule of law
Implications

- Victims have limited expectation of justice in cyberspace. Rule of law? Rights of victims?
- Need to make Mutual Legal Assistance more efficient ➤ implement T-CY recommendations
- But is it realistic that governments send tens or hundreds of thousand of MLA requests per year? Where to send MLA request if jurisdiction of data is unknown? ➤ Additional solutions required
- Electronic evidence a transversal challenge. Related to international cooperation in criminal and civil matters, money laundering, sexual exploitation of children, terrorism, Medicrime, manipulation of sports events, data protection, etc. ➤ Need to ensure a coherent approach at COE
A strategic approach to cybercrime
And part of CoE Internet Governance Strategy

1 Common standards: Budapest Convention on Cybercrime and relates standards

“Protecting you and your rights in cyberspace”

2 Follow up and assessments: Cybercrime Convention Committee (T-CY)

3 Capacity building: C-PROC Technical cooperation programmes

www.coe.int/cybercrime
Review 2014: Enlarged reach of and membership in the Budapest Convention

125+

Budapest Convention
Ratified/acceded: 44
Signed: 9
Invited to accede: 10
= 63

Other States with laws/draft laws largely in line with Budapest Convention = 20

Further States drawing on Budapest Convention for legislation = 43+
Comment on the accession procedure (Article 37 Budapest Convention)

**Current practice**

1. **Non-m/s sends request**
2. **CoE Secretary General**
3. **Consultation with non-m/s Parties**
4. **CM**
5. **GR-J**
6. **Invitation to accede**
7. **Accession**

- If no objection by M/S that are Parties, informal consultation with CoE M/S stops.
- If objection procedure stops, return to CM.
- If objection procedure stops, further informal or return to Committee for opinion?

**Streamline practice?**

1. **Non-m/s sends request**
2. **CoE Secretary General**
3. **Consultation with all CoE M/S and contracting Parties**
4. **CM**
5. **GR-J**
6. **Invitation to accede**
7. **Accession**

- If no objection, return to CM “to resume consideration.”
- If objection procedure stops, further informals or return to Committee for opinion?
Established under Article 46 Budapest Convention

Membership (status December 2014):
- 44 Members (State Parties)
- 19 Observer States

Functions:
- Assessments of the implementation of the Convention by the Parties
- Guidance Notes
- Draft legal instruments
- Etc.

Two plenaries/year as well as Bureau and working group meetings

The T-CY appears to be the main inter-governmental body on cybercrime matters internationally
Guidance Notes

Common understanding of the Parties on how to apply the Convention and address new phenomena

Adopted in 2013/14:

- “botnets”
- “distributed denial of service attacks”
- “identity theft and phishing in relation to fraud”
- “critical information infrastructure attacks”
- “new forms of malware”
- “transborder access to data (Article 32)”
- “spam”

The Budapest Convention remains relevant even if technology and crime evolve
Assessment of mutual legal assistance provisions of Budapest Convention

T-CY assessments essential for quality of implementation of Budapest Convention

Report on 2\textsuperscript{nd} cycle of assessments (2013/2014) adopted by T-CY 12 (December 2014)

► 24 recommendations to enhance the efficiency of mutual legal assistance

- Recs for domestic follow up by Parties
- Recs to be addressed through capacity building programmes
- Recs requiring an Additional Protocol
- Follow up by ”Cloud Evidence Group” of the T-CY
The question of transborder access to data

- Guidance Note on Article 32 adopted by T-CY in Dec 2014
- Additional Protocol on transborder access necessary but not (yet) feasible because:
  - Governments divided
  - Reports on mass surveillance
  - Data protection framework still in the making
  - Regulations on criminal justice access unstable following data retention judgment
  - Developments regarding jurisdiction
- Follow up through “Cloud Evidence Group”

“The lack of concern for the rights of victims has been a distressing revelation for the Transborder Group”
Cloud Evidence Group of the T-CY

- Established by T-CY 12 (December 2014)
- Duration: January 2015 – December 2016
- Task: To explore solutions on criminal justice access to evidence stored on servers in the cloud and in foreign jurisdictions, including through mutual legal assistance
- Follow up to T-CY assessment of MLA provisions and work on transborder access to data
Cybercrime Programme Office of the Council of Europe (C-PROC) in Romania

- Committee of Ministers decision October 2013
- Operational as from April 2014
- Task: Support to countries worldwide to strengthen criminal justice capacities on cybercrime and criminal justice
- 7 staff by December 2014
- 3 projects in 2014:
  - GLACY EU/COE Joint Project on Global Action on Cybercrime
  - Cybercrime@EAP EU/COE Eastern Partnership
  - Cybercrime@Octopus (voluntary contribution funded)
- New projects in 2015
<table>
<thead>
<tr>
<th>C-PROC</th>
<th>Activities (examples from November/December 2014 only):</th>
</tr>
</thead>
<tbody>
<tr>
<td>GLACY</td>
<td>Sri Lanka: Needs assessment mission</td>
</tr>
<tr>
<td>GLACY</td>
<td>South Africa: Law enforcement 1st responder trainer course</td>
</tr>
<tr>
<td>GLACY</td>
<td>Morocco: Introductory judicial training course</td>
</tr>
<tr>
<td>GLACY</td>
<td>Philippines: Judicial training and interagency cooperation workshops</td>
</tr>
<tr>
<td>Cybercrime@EAP</td>
<td>Moldova: International workshop on cybercrime capacity building for Eastern Partnership countries</td>
</tr>
<tr>
<td>Cybercrime@Octopus</td>
<td>India: contribution to conference on cyberlaws</td>
</tr>
<tr>
<td>Cybercrime@Octopus</td>
<td>C-PROC Romania: Study visit of Jordanian delegation</td>
</tr>
<tr>
<td>GLACY</td>
<td>Strasbourg: Project Steering Committee Meeting</td>
</tr>
<tr>
<td>GLACY</td>
<td>Senegal: Introductory judicial training course</td>
</tr>
<tr>
<td>GLACY</td>
<td>Morocco: Law enforcement training strategy workshop</td>
</tr>
<tr>
<td>Cybercrime@Octopus</td>
<td>T-CY Strasbourg: Study on cybercrime model laws</td>
</tr>
</tbody>
</table>
Outlook 2015

- Cybercrime and e-evidence: more crime, more complex, more victims
- Budapest Convention will remain the main international framework on cybercrime and the T-CY the main intergovernmental body to address crucial challenges. Problem: resources?
- Support implementation of Protocol on Xenophobia and Racism: resources?
- More capacity building through C-PROC with extra-budgetary resources
- CoE Internet Governance Strategy 2016-2017
- Data protection framework
- Global Cyberspace Conference, The Hague, 16-17 April 2015
- UN Congress on Crime Prevention and Criminal Justice, Doha, 12-19 April 2015