Prevention of Cybercrime

Pedro Verdelho, (Public Prosecutor), Portugal
Draft Comprehensive Study - Prevention

Some key factors

- national cybercrime laws
- national cybercrime strategies
- public awareness
- law enforcement capacity and training
- public - private cooperation
First Conclusion:

You need to **prosecute** criminals;

But **prevention is more important**.
Second Conclusion:

Prevention is:
• to have in place a legal framework:
  • on cybercrime
  • on obtaining digital evidence
  • permitting international cooperation at this respect

• The Budapest Convention is the reference
Some **153 (79%)** members of the United Nations used the Budapest Convention as a guideline or as a source for their reforms on cybercrime and digital evidence.

Some **106 States (55%)** seem to have adopted specific domestic provisions corresponding broadly to the substantive criminal law articles of the Budapest Convention.

An additional one third of States had adopted at least some specific substantive criminal law provisions in line with the Convention.

Some **82 States (42%)** had specific procedural powers largely in place while many States still rely on general procedural law provisions to investigate cybercrime and secure electronic evidence.
Second Conclusion (b):
The **Budapest Convention** is a worldwide **model**

There is still **room and need to improve domestic legislations**

This is a **key point** to include in a future roadmap of the UN work on cybercrime

*Workshop on drafting a cybercrime Bill – Banjul, Gambia, 2020*
Third Conclusion:

Prevention is:

• **institutions** that are able to investigate

• **trained officers** (judges, prosecutors, police)

• technical capacities
Cybercrime Programme Office (C-PROC) of the Council of Europe
(since October 2013)

(strengthening capacities for more effective capacity)
(supported about one thousand activities since it became operational in April 2014)

(currently manages projects with a volume of some EUR 40 million)

<table>
<thead>
<tr>
<th>Project title</th>
<th>Duration</th>
<th>Budget</th>
<th>Funding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybercrime@Octopus</td>
<td>Jan 2014 – Dec 2020</td>
<td>EUR 4 million</td>
<td>Voluntary contributions (Estonia, Hungary, Japan, Monaco, Netherlands, Romania, Slovakia, UK, USA and Microsoft)</td>
</tr>
<tr>
<td>GLACY+ project on Global Action on Cybercrime Extended</td>
<td>Mar 2016 – Feb 2024</td>
<td>EUR 19 million</td>
<td>EU/CoE JP</td>
</tr>
<tr>
<td>iPROCEEDS-2 project targeting proceeds from crime on the Internet in South-Eastern Europe and Turkey</td>
<td>Jan 2020 – June 2023</td>
<td>EUR 5 million</td>
<td>EU/CoE JP</td>
</tr>
<tr>
<td>EndOCSEA@Europe project against Online Child Sexual Exploitation and Abuse</td>
<td>July 2018 – Dec 2020</td>
<td>EUR 0.85 million</td>
<td>End Violence against Children Fund</td>
</tr>
</tbody>
</table>
Third Conclusion (b):

On the grounds of the framework of Budapest Convention
- Law enforcement agents from all over the world are being trained
- Capacity is being raised
- Countries are more and more able to face cybercrime
Fourth Conclusion:

Prevention is:
• to be able to cooperate
  • with private parties – providers, industry...
  • Internationally

• Again, the Budapest Convention is the reference
Budapest Convention: cooperation with the private sector

- Directly to request **preservation** from US providers
- Directly request **subscriber information** directly from US providers (Article 18.1.b of the Convention)

- Guidance Note of the T-CY (March 2017) on Production orders for subscriber information (Article 18 Budapest Convention)
  - shows how may serve as a legal basis for requesting subscriber information from a service provider offering its service in the territory of a Party

- Cooperation with US-based providers is especially significant
Forth Conclusion (b):

The **Budapest Convention** provides the appropriate legal framework to create and develop cooperation with private parties, in concrete investigations.
Fifth Conclusion:

Prevention is:
To have in place a national
a Cybercrime Strategy
or
a Cyber Security
Strategy
(including cybercrime)
Eastern Partnership Project of the Council of Europe (Cybercrime@EAP) - 2018

<table>
<thead>
<tr>
<th>Cybersecurity strategy</th>
<th>Armenia</th>
<th>Azerbaijan</th>
<th>Belarus</th>
<th>Georgia</th>
<th>Moldova</th>
<th>Ukraine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity strategy in place</td>
<td>At drafting stage</td>
<td>At drafting stage</td>
<td>No</td>
<td>Yes</td>
<td>As a draft Programme</td>
<td>Yes</td>
</tr>
<tr>
<td>Cybersecurity strategy names preventing cybercrime as a key objective</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Computer emergency response team(s), CERTs</td>
<td>Yes (non-governmental)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cooperation on both national and international level</td>
<td>Present</td>
<td>Present</td>
<td>Present</td>
<td>Present</td>
<td>Present</td>
<td>Present</td>
</tr>
<tr>
<td>Cooperation with private sector</td>
<td>Present</td>
<td>Present</td>
<td>Present</td>
<td>Present</td>
<td>Present</td>
<td>Informal</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cybercrime strategy</th>
<th>Armenia</th>
<th>Azerbaijan</th>
<th>Belarus</th>
<th>Georgia</th>
<th>Moldova</th>
<th>Ukraine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybercrime strategy in place</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes - part of Organized Crime Strategy</td>
<td>As a part of draft Programme</td>
<td>Yes, as part of the Cybersecurity Strategy</td>
</tr>
<tr>
<td>Specialized cybercrime units</td>
<td>In place</td>
<td>In place</td>
<td>In place</td>
<td>In place</td>
<td>In place</td>
<td>In place</td>
</tr>
<tr>
<td>Public/private cooperation</td>
<td>In place</td>
<td>In place</td>
<td>In place</td>
<td>In place</td>
<td>In place</td>
<td>In place</td>
</tr>
<tr>
<td>International cooperation</td>
<td>Cooperation agreement</td>
<td>Informal</td>
<td>Cooperation agreement</td>
<td>Cooperation agreement</td>
<td>Informal</td>
<td>Informal</td>
</tr>
<tr>
<td>Establishment of platforms for reporting cybercrime</td>
<td>No</td>
<td>Several options</td>
<td>Several options</td>
<td>Several options</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

https://rm.coe.int/eap-cybercrime-and-cybersecurity-strategies/168093b89c
Summary of Conclusions / Recommendations

1 - Prevention requires a **domestic legal framework**; the **Budapest Convention** is the **reference and a worldwide model**; important updates will be made by the 2nd Additional Protocol (still under discussion)

2 - Prevention requires **capacity building**; on the grounds of the **framework of Budapest Convention** capacity is currently being developed all over the world

3 - Prevention requires ability to **cooperate, both internationally and with private parties** (providers, industry...); again, the **Budapest Convention** is also the appropriate legal framework at this respect

4 - Prevention requires national **cybercrime or cyber security strategies**; the technical projects under the framework of **Budapest Convention** by the **C-PROC** of the Council of Europe are supporting drafting strategies all over the world
prevention avoids sanction!

thank you for your attention.

Pedro Verdelho

(pedro.verdelho@pgr.pt)