THE NEED FOR NATIONAL LEGISLATION AS WELL AS REGIONAL AND INTERNATIONAL HARMONIZATION IN FIGHTING CYBERCRIME

ESCWA Conference
20.12.2012, Beirut
Prof. Dr. Marco Gercke

WHY COUNTRIES SHOULD CARE ABOUT CYBER SECURITY AND CRIME
INTRODUCTION

John von Neumann
“Theory of self-reproducing automata”

Creeper Virus

Millions of Computer Viruses

Iran Oil Terminal

Stuxnet

Flame

1949 1971 1980

09 10 11 12

WHAT HAS CHANGED WITH REGARD TO ATTACKS?
SPY ASPECT

- In the past most spy-related activities required at least once physical presents at the observed location

- Today it is possible to install a spyware remotely on thousands of computer systems in parallel
- Spyware is capable of not only intercepting mail/text communication but also take screenshots, activate microphones and webcams

PHYSICAL SABOTAGE

- In the past attacks against nuclear programs where largely carried out against infrastructure

- Stuxnet underlined that the capability of a software tool is not necessary limited to deleting data but it has the potential to physically destroy objects (centrifuges) from the distance without any interference with buildings and life of people.
WHY SHOULD THERE BE REGIONAL HARMONIZATION?

COMMONWEALTH OF NATIONS

- The Commonwealth of Nations is a voluntary association of sovereign states
- Currently 53 associated states
- In 2002 the Commonwealth presented a model law on Cybercrime that provides a legal framework to address Cybercrime
- The model law was intentionally drafted in accordance with the Convention on Cybercrime
COMMONWEALTH OF NATIONS

- In addition to substantive criminal law and procedural law the Commonwealth also discussed the importance of digital evidence.
- Without admissibility of digital evidence courts are in most cases unable to sentence offenders.
- In 2002 Commonwealth therefore presented a model law on digital evidence.

ECONOMIC COMMUNITY OF WEST AFR.

- The Economic Community of West African States is a regional group of west African Countries.
- Founded in 1975 it has currently fifteen member states.
- In 2009 ECOWAS adopted the Directive on Fighting Cybercrime in ECOWAS that provides a legal framework for the member states.
- Directive includes substantive criminal law as well as procedural law.
**EAST AFRICAN COMMUNITY**

- 5 Member states (Kenya, Uganda, Tanzania, Burundi, Rwanda)
- Within the framework of an update of ICT legislation (EAC Legal Framework for Cyberlaws) EAS also addressed the issues of Cybercrime
- Provisions dealing with the criminalisation of certain conduct became part of the draft legislation

**COMESA**

- Common Market of Eastern and Southern Africa
- In 2011 COMESA presented a Cybersecurity model law that included various provisions related to Cybercrime
ESCWA

- United Nations Economic and Social Commission for Western Asia
- Between 2008 – 2011 ESCWA carried out a project on “regional harmonization of cyber legislation to promote the knowledge society in the Arab world”
- This included the production of harmonization instruments (including Cybercrime)

LEAGUE OF ARAB STATES

- In 2003/2004 the Council of Ministers of Justice and the Council of the Ministers of Interior adopted the Emirates Model Arab Law on Combating Information Technology Systems and suchlike Offences
The European Union is a political Union of 27 member states. One of the mandate of the EU is to harmonise legislation in selected areas. It has adopted several Framework Decision and Directives to harmonise the legislation with regard to Cybercrime. The 27 member states are obliged to implement the legislation within the given time period.

**Substantive Criminal Law**

<table>
<thead>
<tr>
<th>Model/Law/Convention</th>
<th>Substantive Law</th>
<th>Criminal Law</th>
<th>Cybercrime Law</th>
<th>Copyright Law</th>
<th>Identity Theft</th>
<th>Threat Assessment</th>
<th>Cybercrime Protection</th>
<th>Spam</th>
<th>Malware/Adware</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMESA Model Bill (2011)</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIPCAR Cybercrime Model Law (2010)</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CoE Cybercrime Convention (2001)</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICOPAC Cybercrime Model Law (2011)</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Different EU instruments</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Draft African Union Convention (2011)</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIPCAR Cybercrime Model Law (2010)</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIPSA Draft Model</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
WHY DO WE NEED INTERNATIONAL HARMONIZATION?
WHY SHOULD ARABIC COUNTRIES BE MORE INVOLVED?

UN MEMBER STATES
WHO IS INVITED TO DRAFT THE COE CONVENTION?

IMPLEMENTATION 10 YEARS
DONT COPY/PASTE FROM OTHER COUNTRIES AND REGIONS

EXAMPLE: CHILD PORNOGRAPHY

- As cooperation requires legislation gaps can have significant impact
- In the early discussion about legal response to an online distribution of child pornography the drafter of regulations focused on digital images
- Today not only images and videos but also audio recordings of the sexual abuse of children are distributed online
- Older approaches often use language (such as “visually” or “image”) that excludes such material

Convention on Cybercrime
2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:
   a. a minor engaged in sexually explicit conduct;
   b. a person appearing to be a minor engaged in sexually explicit conduct;
   c. realistic images representing a minor engaged in sexually explicit conduct.

EU Directive Child Pornography 2011
(c) “child pornography” means:
   (i) any material that visually depicts a child engaged in real or simulated sexually explicit conduct;
EXAMPLE: CHILD PORNOGRAPHY

- As cooperation requires legislation gaps can have significant impact
- In the early discussion about legal response to an online distribution of child pornography the drafter of regulations focused on digital images
- Today not only images and videos but also audio recordings of the sexual abuse of children are distributed online
- Older approaches often use language (such as “visually” or “image”) that excludes such material

EXAMPLE: CHILD PORNOGRAPHY

- ICB4PAC skeleton consequently avoids the term “visually”
- In addition the definition in ICB4PAC contains a clarification that audio material is included

(4) Child pornography means pornographic material that depicts presents or represents: a child engaged in sexually explicit conduct; a person appearing to be a child engaged in sexually explicit conduct; or images representing a child engaged in sexually explicit conduct; this includes, but is not limited to, any audio, visual or text pornographic material.
BE MINDFUL THAT MORE IS NECESSARY THAN JUST LAWS

COMPONENTS

- Substantive Criminal Law
COMPONENTS

National Cybersecurity Strategy
Cybercrime Policy
Crime Prevention, Technology

Definition
Substantive Criminal Law
Procedural Law
International Cooperation
Electronic Evidence
Liability of ISPs

Policy

- The relevance of a policy was highlighted during today's conference when the first speaker raised that in many countries different ministries "feel" responsible for the topic Cybercrime.
- A cybercrime policy can address those issues.
Cybercrime Research Institute

FREE TOOLS

http://www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html

http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFA.pdf

Cybercrime

Cybercrime Research Institute

Prof. Dr. Marco Gercke

Nehler Str. 35
D-50733 Cologne, Germany
gercke@cybercrime.de
www.cybercrime-institute.com