Regional and International Approaches to Cybercrime

Asia Pacific Regional Mock Court Exercise on Fighting Cybercrime
18-19 Sept 2012, Jakarta, Indonesia

Prof. Dr. Marco Gercke
VARIETY OF APPROACHES

• The development of a legal framework addressing the challenges of Cybercrime is not limited to national approaches but includes regional and international approaches.

• International approaches are important to harmonise Cybercrime and provide the basis for international cooperation.

• Regional approaches are able to address issues where consent can be reached in a region but not on the global level.
VARIETY OF APPROACHES

• Despite the importance of harmonisation the differences in the extent of criminalisation (especially with regard to illegal content) it is very likely that the number of issues covered by regional and international approaches will be limited
REGIONAL SOLUTIONS
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
• 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
# Substantive Criminal Law

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></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>
<td>✔</td>
<td>✔</td>
<td>✔</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>
<td>✔</td>
<td>✔</td>
<td>✔</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>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>ICB4PAC Cybercrime Model law (2011)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</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>
<td>✔</td>
<td>✔</td>
<td>✔</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>
<td>✔</td>
<td>✔</td>
<td>✔</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>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
• 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
- Common Market for Eastern and Southern Africa
- 20 Member States
- In 2011 Comesa presented the Comesa Cybersecurity Draft Model Bill
- Model Law addressing various aspects of Cybercrime
• International Telecommunication Union (ITU) and European Union (EU) co-funded a project in the Caribbean

• The project enabled 15 Caribbean countries to develop their own regional model policy and model legislation for Cybercrime

• Model legislation and policy was developed in 2010 by Caribbean experts

• Already implemented in various countries

• Other regions followed this model
• International Telecommunication Union (ITU) and European Union (EU) co-funded a project in the Pacific

• The project enabled experts from 16 Pacific countries to develop their own model policy and legislation

• Work was finalized in 2011

• Implementation on the way
• Organization of American States (OAS) is an international organisation

• 34 member states (2 out of the 25 independent states of the Americas are suspended)

• OAS adopted a number of recommendations but did until now not undertake approaches to harmonise legislation of the member states
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.
• United Nations Organisation is an international organisation (192 member states)
• In 1990 the UN GA adopted a resolution dealing with computer crime legislation
• In 2000 the UN GA adopted a resolution on combating the criminal misuse of information technology
• In 2002 the UN GA adopted a second resolution on the criminal misuse of information technology
UNITED NATIONS

- In 2010 the UN Crime Congress strengthened the UN’s ability to respond to Cybercrime (capacity building and evaluation of a global legal response)

- Capacity building mandate

- Establishment of a working group

- Consideration of undertaking a comprehensive study of the problem of Cybercrime

41. We recommend that the United Nations Office on Drugs and Crime, upon request, provide, in cooperation with Member States, relevant international organizations and the private sector, technical assistance and training to States to improve national legislation and build the capacity of national authorities, in order to deal with cybercrime, including the prevention, detection, investigation and prosecution of such crime in all its forms, and to enhance the security of computer networks.

42. We invite the Commission on Crime Prevention and Criminal Justice to consider convening an open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.
• In 2003 the UN addressed Cybersecurity with a specific resolution (A/RES/57/239) that highlights the ability to address criminal abuse of information technology.

• In 2010 the UN GA adopted another resolution on Cybersecurity.

• An annex includes a voluntary self-assessment tool.

• One aspect of the self assessment is related to Cybercrime legislation.

13. Review and update legal authorities [including those related to cybercrime, privacy, data protection, commercial law, digital signatures and encryption] that may be outdated or obsolete as a result of the rapid uptake of and dependence upon new information and communications technologies, and use regional and international conventions, arrangements and precedents in these reviews. Ascertain whether your country has developed necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, General Assembly resolutions 55/63 and 56/121 on combating the criminal misuse of information technologies, and regional initiatives, including the Council of Europe Convention on Cybercrime.
COUNCIL OF EUROPE

- Council of Europe is an international organisation focusing on the European integration
- 47 member states
- Convention on Cybercrime (2001)
- First addition protocol to the Convention on Cybercrime (2003)
37 countries ratified the Convention on Cybercrime (status: August 2012)

Only two countries (US, Japan) are not member of the Council of Europe

No mandatory evaluation of the ratification

10 countries have signed but not ratified it in the last 11 years
**REVIEW**

- Despite the technological developments and the changing criminal environment the Convention was not changed in the last 10 years.

- This is especially relevant with regard to procedural law as law enforcement agencies need sophisticated investigation instruments to address recent challenges that are not contained in the Convention.

---

1. Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct, when committed without right, is criminalised:
   a. producing child pornography;
   b. offering or making available child pornography;
   c. distributing or transmitting child pornography;
   d. procuring child pornography for oneself or for another person;
   e. possessing child pornography;
   f. knowingly obtaining access, through information and communication technologies, to child pornography.