Purpose of the side-event

On the basis of “broad international agreement” on capacity building as an effective way to address the challenge of cybercrime:

- to illustrate how policies agreed upon by the CCPCJ can be translated into specific action.
- to encourage bi-lateral donors and international organisations to further expand capacity building programmes and to seek synergies between different initiatives.

Organised by the Council of Europe
Partners: Governments of Estonia, Japan, Norway, Romania and Panama, the Department of Justice of the Philippines, the Organisation of American States (OAS), and the United Nations African Institute for the Prevention of Crime and the Treatment of Offenders (UNAFRI)

1 Capacity building on cybercrime: concept and impact
(Alexander Seger, Council of Europe)

“Capacity building” is understood as enabling criminal justice authorities to meet the challenge of cybercrime and electronic evidence.

This entails strengthening the knowledge and skills and enhancing the performance of criminal justice organisations including their cooperation with other stakeholders.

It should be aimed:

- at protecting individuals and society against crime and at protecting the rights of individuals
- at promoting security, confidence and trust in ICT
- at strengthening human rights, democracy and the rule of law in cyberspace
- at contributing to human development.
1 Capacity building on cybercrime: concept and impact

- Human rights and rule of law
- Human development and democratic governance
- Security, confidence and trust in ICT
- Rule of law in cyberspace
- Cybersecurity
- Offences against confidentiality, integrity and availability of computer data and systems
- Offences by means of computers
- Electronic evidence

2 Capacity building on cybercrime: the approach of the Council of Europe

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
Strengthening cybercrime legislation: examples of workshops in East and West Africa (Maureen Owor, Uganda)

Snapshot of Africa’s legal response to cybercrime

- Disproportionate focus on e-commerce laws
- Inconsistency with international treaties
- Scattered legislation
- Slow adaptation to changing nature of crime
- Broad procedural powers
- Inadequate conditions and safeguards
- Eschews customary justice

Strengthening cybercrime legislation - examples from East and West Africa

Dr Maureen Owor
mhowor@gmail.com
Fellow, African Centre on Cyberlaw and Cybercrime Prevention

The East African project, Tanzania 2013

Substantive and procedural innovations:

- Legislative developments
  - Tanzanian Cyber Crime Bill (2013)
  - Kenya e-evidence developments
  - Rwanda and Burundi reforms
- Harmonisation of legislation
- Domesticating cybercrime law through sentencing initiatives
  - Uganda sentencing guidelines
  - Tanzania compensation laws
Strengthening cybercrime legislation: examples of workshops in East and West Africa

West African experiment – Ghana 2014

Outcomes of the cybercrime workshop
- Legislative audit at national & regional level:
  - Ghana Electronic Act 2008
  - Nigeria (Executive) Cybercrime Bill 2013
  - Niger legal framework
  - ECOWAS Directive 1/08/2011
- Checklist on procedural powers, electronic evidence, conditions and safeguards.
- Draft training strategies and content for training manuals checklist.

Addressing cybercrime and cybersecurity: examples from Latin America (Belisario Contreras, OAS)

OAS Cyber Security Framework
- OAS Declaration “Strengthening Cyber Security in the Americas” (2012)
- OAS/REMJA Recommendations (1999 to present)
- OAS/CICTE Workplan, REMJA Cybercrime Group of Experts, CITEL PCC1 Group

Areas of Work:
- REMJA Cybercrime Group of experts:
  Promote the development of Cybercrime legislation
  Training of judges and prosecutors
- CITEL PCC 1
  Promotion of technical standards and a secure architecture of the Internet.
Addressing cybercrime and cybersecurity: examples from Latin America

- OAS/CICTE Cyber Security Program Initiatives
  - Development of National Cyber Security Strategies
    - Adopted: Colombia, Panama and Trinidad and Tobago
    - In process: Bahamas, Dominica and Jamaica
  - Promotion of National CERTs
  - Cyber Security Technical Training Courses
  - Crisis Management Exercises
  - Training on Industrial Control Systems
  - Promotion of PPPs and engagement with civil society

Success Stories

What’s needed?

Legislation

- Expanded Anti-Trafficking in Persons Act of 2013
- Cybercrime Act of 2012
- Data Privacy Act of 2012
- Anti-Child Pornography Law of 2009
- Anti-Photo and Voyeurism Act of 2009
- Anti-Trafficking Act of 2003
- E-Commerce Act of 2000
- Access Devices Regulation Act of 1998
Capacity building in the Philippines

Responses

- Advocacy
  - Academic program for certified trainings and academic degree
  - Extensive information dissemination
  - Research Agenda
  - Capacity building for criminal justice actors

- Programs
  - Information Sharing and Database
  - Research Agenda

- Policy
  - Regulation and Standards

- Operations
  - Multi-Disciplinary Quick Response Teams
  - Computer Forensics Laboratories and Investigation Facilities

- Strategic Partnerships
  - International Cooperation
  - Engagement of Industry Partners
4 Capacity building in the Philippines

Philippines = invited to accede to Budapest Convention on Cybercrime

Support through GLACY Project on Global Action on Cybercrime (EU/COE)

To strengthen capacities for implementation:

- Engagement of decision-makers
- Legislation
- Judicial training
- Law enforcement training
- International cooperation
- Information sharing
- Assessment of progress

5 Comments and conclusions by partners: Estonia

- There is a need for a legal basis for international cooperation
- Need for a network that works 24/7
- Exchange of information at different levels, cooperation in criminal matters, mutual assistance, extradition
- Cooperation that enables not only to investigate cybercrimes, but also to detect and prevent them
Results through capacity building?

- Capacity building based on the Budapest Convention standards
- Legislation: substantive law, procedural law, law on international cooperation
- Ability to implement national legislation effectively in practice
- Budapest Convention has been proved to be an effective instrument: legal base for the cooperation and fully operating 24/7 network
- Works in practice, number of parties is increasing
- The more parties, the more opportunities to cooperate with each other and fight cybercrime

Few examples of international criminal cases:

- **RBS Worldpay**
  8 November 2008
  In less than 12 hours 2,100 ATM-s were used in 280 cities worldwide
  More than 9 million USD were withdrawn
  Cooperation between Estonia and US
  Five suspects in Estonia, one suspect extradited to US

- **Operation Ghost Click**
  DNSChanger. About 4 million computers infected in more than 100 countries between 2006-2011. About 24 million USD profit from fraud.
  Six suspects in Estonia
  Accusations submitted against them both in Estonia and US
  Extraditions to US
Why and how Panama joined the Budapest Convention:

- Cyber-attacks against State institutions in 2011
- Investigations/prosecutions show gaps in legal framework
- Drafting of bills to amend legislation in line with international standards (Budapest Convention)
- Need for international cooperation
- Request for accession in January 2012
- Deposited instrument of accession in March 2014

Capacity for capacity building: Need for infrastructure

- C-PROC (Cybercrime Programme Office of the Council of Europe in Bucharest, Romania)
  - Operational from April 2014
  - **Purpose:** assisting countries worldwide in the strengthening of their criminal justice capacity to respond to the challenges posed by cybercrime and electronic evidence on the basis of the standards of the Budapest Convention on Cybercrime
  - **Projects:**
    - GLACY joint project EU/COE on Global Action on Cybercrime
    - Cybercrime@EAP
    - Project Cybercrime@Octopus