EU/COE Joint Project on Global Action on Cybercrime

Capacity Building on Cybercrime

The experience of Council of Europe and possible synergies with the ASEAN initiative

Matteo Lucchetti
Project Manager, Council of Europe C-PROC Bucharest, Romania

Bangkok, Thailand, 15 September 2016

Agenda

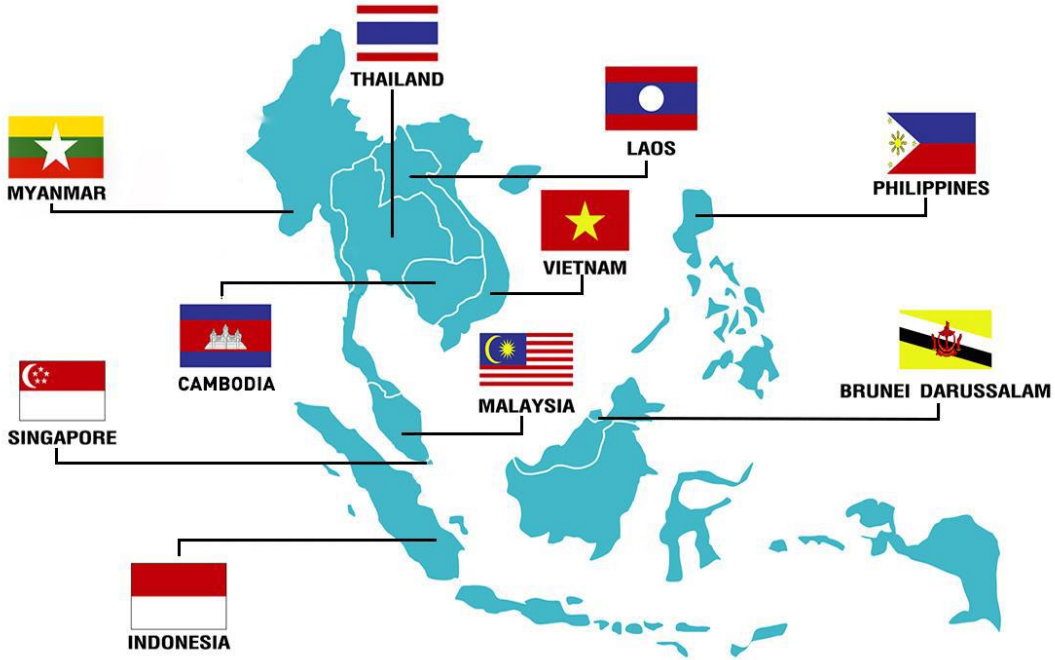
- **Cybercrime general situation in the ASEAN region**
  - Common forms of cyber threats
  - Main challenges reported in the ASEAN region

- **The global action on cybercrime of the Council of Europe, capacity building in the ASEAN region**
  - The role of Council of Europe
  - The Budapest Convention, general overview and outreach
  - C-PROC and capacity building programmes
  - GLACY and GLACY+
  - Activities developed in the region

- **Opportunities and possible synergies in the establishment of the ASEAN Cyber Security and Cybercrime Center**

Cyber threats reported in the region

- Online financial frauds
- ATM malware/ skimming
- Payment card frauds
- Online identity theft/ Impersonation scam
- Unauthorized access/ Intrusions/ Data breach
- Defamation
- Extortion
- Online child pornography
- Terrorist recruiting
- 419/ romance scam
- E-commerce frauds
- Unauthorized/ Illegal gambling and betting
- Drug dealing and smuggling



Cybercrime in the ASEAN Region
Challenges

- Cybercrime legislation in place only in a few countries, **heterogeneous legislative framework**
  - Definition of cybercrimes
  - Dual criminality

- **Lack of common understanding** on cybercrime amongst the criminal justice authorities
  - Traditional crimes committed using computers/ Internet (Cyber extortion, Love scam, etc.) vs. Computer being the target

- **Reliable statistics** not fully available
  - Reported, Investigated, Prosecuted, Adjudicated Cases
  - Number and types of electronic evidences extracted, Devices analyzed

Challenges

- Cybercrime investigation units are usually understaffed and not **adequately trained/ skilled**
  - Use of VPN/ Tunneling and Proxy/ Use of darknets and virtual currencies
  - Understanding of the Modus Operandi/ Evidence to collect
  - Investigation into possible forms of Organized Crime vs. Single criminal

- **Limited technical capabilities** to support a successful investigation
  - Data/ mobile forensics laboratories often outdated
  - Malware forensics and reverse engineering capacities
  - Collaboration with local telecommunication providers

- **International cooperation**
  - Limited success in interacting with international large service providers (Social Networks, etc.)

Budapest Convention: scope

Criminalising conduct

- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Fraud and forgery
- Child pornography
- IPR-offences

+

Procedural tools

- Expedited preservation
- Search and seizure
- Interception of computer data

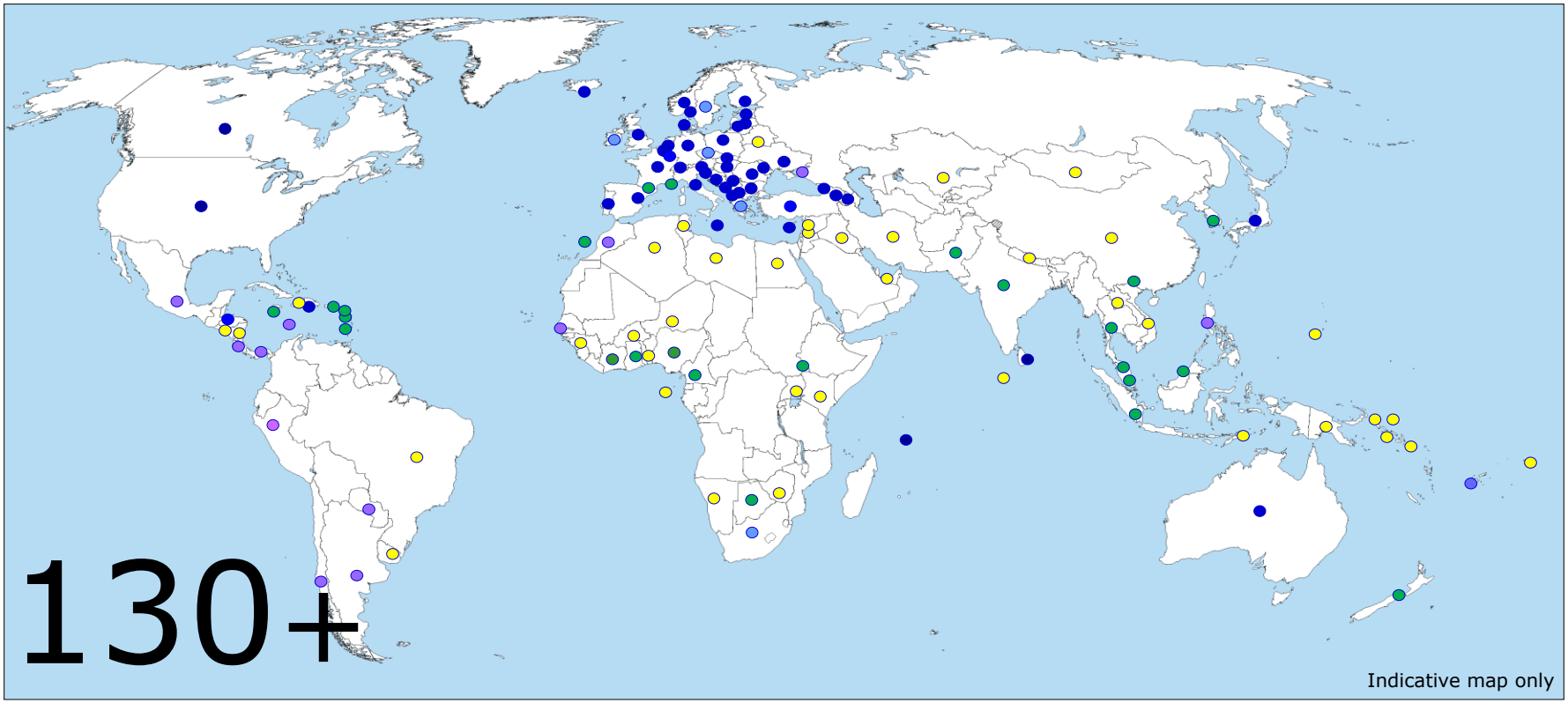
+

International cooperation

- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

Harmonisation

Reach of the Budapest Convention



Budapest Convention
Ratified/acceded: **49**

Signed: 6

Invited to accede: 11
= 66

Philippines

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

Thailand
Singapore
Malaysia
Indonesia
Brunei

Further States drawing on Budapest Convention for legislation = 45+

Laos
Vietnam

The approach of Council of Europe

1 Common standards: Budapest Convention on Cybercrime and related standards

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

3 Capacity building: C-PROC ▶ Technical cooperation programmes

Budapest Convention
The Cybercrime Convention Committee (T-CY)

Established under Article 46 Budapest Convention

Membership (May 2016):

- **49 Members** (State Parties)
- **19 Observer States**
- **12 organisations**
  (African Union Commission, Commonwealth Secretariat, ENISA, European Union, Eurojust, Europol, INTERPOL, ITU, OAS, OECD, OSCE, UNODC)

Functions:

- **Assessments of the implementation of the Convention by the Parties**
- **Guidance Notes**
- **Draft legal instruments**

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

- **An effective follow up mechanism**
- **The T-CY appears to be the main inter-governmental body on cybercrime matters internationally**

- Committee of Ministers decision October 2013
- Operational as from April 2014
- Currently 18 staff / expected to increase to 20+

- **Support to countries worldwide to strengthen criminal justice capacities on cybercrime and electronic evidence**

Current capacity building programmes

GLACY EU/COE Joint Project on Global Action on Cybercrime

GLACY+ EU/COE Joint Project on Global Action on Cybercrime

Cybercrime@EAP II EU/COE Eastern Partnership

Cybercrime@EAP III EU/COE Eastern Partnership

iPROCEEDS Cooperation on Cybercrime: targeting crime proceeds on the Internet

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Cybercrime@Octopus (voluntary contribution funded)

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

GLACY

EU/COE Joint Project on Global Action on Cybercrime

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

To enable criminal justice authorities to engage in international cooperation on cybercrime and electronic evidence on the basis of the Budapest Convention on Cybercrime

Duration	36 months (Nov 2013 – Oct 2016)
Budget	EUR 3.35 million
Funding	European Union (Instrument for Stability, IfS) and Council of Europe
Geo scope	**Countries prepared to implement the Budapest Convention** – Parties, Signatories or Invitees.
GLACY Priority countries	• Mauritius • Senegal • Tonga • Morocco • South Africa • **Philippines** • Sri Lanka

GLACY
Expected Results

GLACY in the ASEAN region
Philippines

2014			
Nr. crt.	**Activity**	**Description**	**Period**
1	1.2/ 2.1/ 3.1/ 4.1	National situation report and country assessment in Philippines	2014

2015			
Nr. crt.	**Activity**	**Description**	**Period**
1	3.6	Support to national delivery of basic judicial course	9-11 March 2015
2	4.3	Support for joint training of investigative agencies	13 March 2015
3	3.4	Judicial Introductory Training on Cybercrime – **Trainers Course**	13-17 July 2015
4	4.3	First Responders Course for Law Enforcement – **Training of Trainers**	13-17 July 2015
5	5.4	Workshop on **International Cooperation** in Cybercrime	14-15 July 2015
6	6.2	Crime statistics and reporting related to cybercrime and electronic evidence	16-17 July 2015
7	3.4	Public Attorney's Introductory Training on Cybercrime – **Trainers Course**	20-24 July 2015
8	**5.5**	**Regional Cybercrime – Cyber security Assessment Conference (ASEAN)**	**11-12 November 2015**

GLACY in the ASEAN region
Philippines

2016			
Nr. crt.	**Activity**	**Description**	**Period**
1	4.3	Mauritius: Second international workshop on adaptation and update of the Electronic Evidence Guide through development of the Standard Operating Procedures fr digital forensics (with participation of all GLACY countries)	21-23 March 2016
2	3.5	South Africa: International workshop on judicial training curricula integration, combined with conference for the regional/ district magistrates and finalization of introductory judicial training support (participation of all GLACY countries)	11-13 April 2016
3	5.2/ 5.4	Sri Lanka: International workshop and training for 24/7 points of contact of the GLACY countries, with a side meeting on the Standard Operating Procedures for digital forensics (with participation of all GLACY countries)	25-27 April 2016
4	3.6	Additional support to **national delivery of introductory judicial course**	15-17 June 2016
5	4.3	Digital **data forensics for LE and CERT** (basic course)	15-17 June 2016
6	4.3	Live data forensics for LE and CERT (advanced course)	20-22 June 2016
7	3.4	Advanced judicial training	20-22 June 2016
8	3.4	Judicial conference for Judges, Prosecutors and Public Defenders	23-24 June 2016
9	4.2	**Study visit of Sri Lanka CERT and police/ forensics experts** on benchmarking digital forensics servicesand standard operating procedures	27-29 June 2016
10	2.3/ 7.1/ 7.6	Morocco: International workshop on effectiveness of legislation mesured through statistics (with participation of all GLACY countries)	27-28 July 2016

New capacity building programme GLACY+

GLACY+

EU/COE Joint Project on Global Action on Cybercrime Extended

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

GLACY+ is intended **to extend the experience of the GLACY project**, which supports seven priority countries in Africa and the Asia-Pacific region. These **countries may serve as hubs to share their experience within their respective regions**. Moreover, countries of Latin America and the Caribbean may now also benefit from project support.

Duration	48 months (Mar 2016 – Feb 2020)
Budget	EUR 10 million
Funding	European Union (Instrument Contributing to Peace and Stability) and Council of Europe
GLACY+ prospect countries	• (Cape Verde) • Mauritius • Senegal • Tonga • Dom. Republic • Morocco • South Africa • Ghana • **Philippines** • Sri Lanka

To strengthen the capacities of States worldwide to apply legislation on cybercrime and electronic evidence and enhance their abilities for effective international cooperation in this area.

CYBERCRIME AND CYBERSECURITY POLICIES AND STRATEGIES

- To promote consistent cybercrime and cybersecurity policies and strategies.

POLICE AUTHORITIES AND INVESTIGATIONS

- To strengthen the capacity of police authorities to investigate cybercrime and engage in effective police-to-police cooperation with each other as well as with cybercrime units in Europe and other regions.

CRIMINAL JUSTICE AND INTERNATIONAL COOPERATION

- To enable criminal justice authorities to apply legislation and prosecute and adjudicate cases of cybercrime and electronic evidence and engage in international cooperation.

Inception phase and Launch – March/ October 2016

- Formalization of a cooperation agreement with **Interpol as implementing partner**
- Involvement of **Project Partners** (Europol EC3, USA, France, Romania, Estonia, UK) and definition of collaboration principles
- Enhancement of the policy dialogue and **cooperation on cybercrime with international and regional organizations** (UNODC, ASEAN, ECOWAS, OAS, ECTEG, Eurojust, ENISA, etc.)
- Establishment/ confirmation of the **country teams of the GLACY+ priority/ hub countries**
- **In-country assessments of GLACY+ priority/ hub countries** and initial situation report
- Drafting of a preliminary version of **the GLACY+ workplan**
- **Launch event** with participation of all GLACY+ Countries

26-28 October 2016	*Bucharest, ROMANIA*	***Closing conference of the GLACY Project, in conjunction with the launching event of the GLACY+ Project***

Octopus Conference

Strasbourg, FR, 16-18 November 2016

Focus

- **Budapest Convention: 15th anniversary**
- Crime and jurisdiction in cyberspace: the way ahead

Workshops

- **Service provider / law enforcement cooperation** on cybercrime and electronic evidence
- Criminal justice **access to evidence in the cloud**: results of the Cloud Evidence Group
- **Capacity building on cybercrime**: lessons learnt
- The state of cybercrime **legislation in Africa, Asia/Pacific and Latin America/Caribbean**
- **Terrorism and information technology**: the criminal justice perspective
- **International cooperation**: enhancing the role of 24/7 points of contact
- Seeking synergies: Policies and initiatives on cybercrime of **international and private sector organisations**

Participation is free of charge but subject to registration. Registration will be open from 15 September to 15 October 2016 at www.coe.int/cybercrime.

Possible activities

- To provide **strategic advisories** on cybersecurity and cybercrime legislation and policies, in line with international best practices and standards
  - Harmonisation of local legislation to international standards
  - Support in the definition and the implementation of national cybersecurity and cybercrime strategies
- To support the establishment and the consolidation of **national CERTs/ CSIRTs**, their setup and the accreditation to international networks
- To organize **region-wide capacity building programmes**
  - Law enforcement training and integration of cybercrime and electronic evidence modules in the training curricula
  - Judicial training for judges, magistrates and prosecutors and integration of cybercrime and electronic evidence modules in the training curricula
  - Implementation of forums for Public-Private collaboration
  - Development of capacities to handle international cooperation, both on national level and on regional level

Comments on the ASEAN initiative
Possible activities

- To provide **centralized operational security services**
  - PREVENTION (Early warning, Open source intelligence, Information sharing)
  - REACTION (Region-wide incident handling coordination, Fostering joint investigation)
  - TECHNICAL SUPPORT (Malware forensics, Security standards and certifications)

- To be a **qualified international hub for the region** in the dialogue with international service providers and to provide a recognizable and acknowledged **interface to other international networks and communities**
  - Participation in relevant international communities (e.g. Octopus Conference)

- To foster **R&D initiatives**

Comments on the ASEAN initiative
Synergies with GLACY+

The GLACY+ Programme aims at creating hubs where to develop capacity building activities on cybercrime and electronic evidence which could target the whole region

Any form of possible synergy with the ASEAN Secretariat is most welcome, in terms of:

- developing joint initiatives/ trainings/ events, addressing judicial authorities, law enforcement and other public authorities
- providing assistance to draft/ review/ amend/ implement legislation and national cybercrime/ cyber security strategies, in accordance to international standards
- design/ implement/ support reliable procedures for international cooperation,
- fostering information sharing on cybercrime between public entities and private sector, in accordance with international best practices

EU/COE Joint Project on Global Action on Cybercrime

THANK YOU

Matteo Lucchetti
Project Manager, Council of Europe C-PROC Bucharest, Romania

Matteo.LUCCHETTI@coe.int

Bangkok, Thailand, 15 September 2016