International Workshop on reporting systems and criminal justice statistics on cybercrime and electronic evidence

Matteo LUCCHETTI

Polixenia CALAGI

Cybercrime Programme Office of the Council of Europe (C-PROC) – Bucharest, Romania

matteo.lucchetti@coe.int
polixenia.calagi@coe.int

Accra, 29 March 2017

Cybercrime: Narrow and Broader Sense

- Normally used to describe a criminal activity in which a computer or a network are an essential part of a crime
- However cybercrime is also used to include other traditional crimes in which those same computers or networks are used to make the illicit activity possible

THE COMPUTER IS A TOOL OF THE CRIMINAL ACTIVITY
e.g. Spamming, criminal copyright crimes through peer-to-peer networks, etc.

THE COMPUTER OR THE NETWORK IS A TARGET OF CRIME
e.g. Unauthorized access, Malicious code, Mobile malware, ATM/POS malware, etc.

THE COMPUTER OR THE NETWORK MAKE COMMISSION OF CRIMES EASIER
e.g. Nigerian fraud, Hacking, Phishing, Child Pornography, Drug smuggling

THE COMPUTER OR THE NETWORK IS THE PLACE OF THE CRIMINAL ACTIVITY
e.g. Telecommunications' fraud

Cybercrime as a criminal justice matter – Main Challenges

- **Lack of common understanding** on cybercrime amongst the criminal justice authorities

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

- Coping with **new technological paradigms**
  - Cloud Computing
  - Darknet and virtual currencies
  - Internet of Things

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

Cybercrime as a criminal justice matter – Main 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  - Data/ mobile forensics laboratories outdated
  - Malware forensics and reverse engineering capacities
  - Collaboration with local telecommunication service providers

- **International cooperation**
  - Police to Police
  - International Judicial Cooperation
  - Interactions with international large service providers (Social Networks, etc.)

The approach of Council of Europe

1 Common standards: Budapest Convention on Cybercrime and relates standards

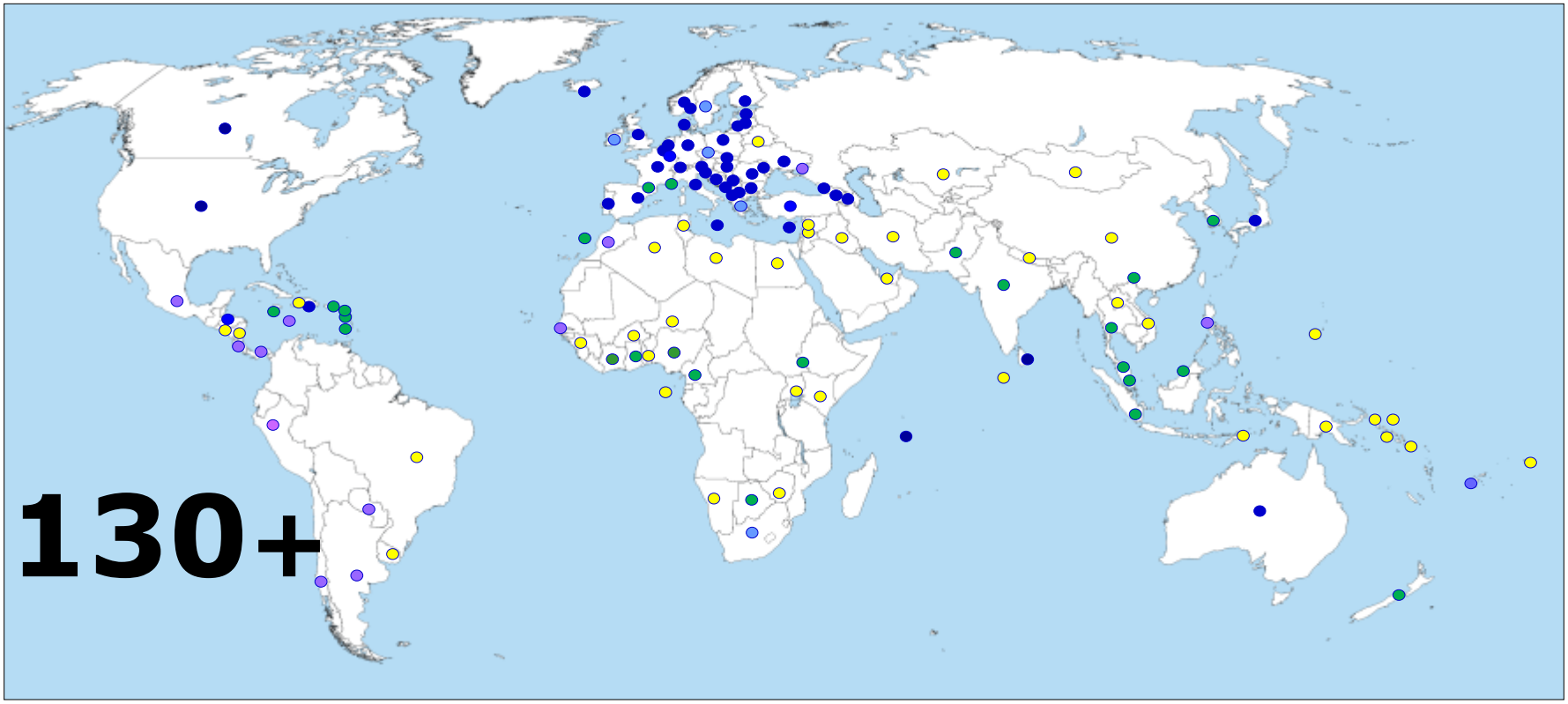
2 Follow up and assessments: Cybercrime Convention Committee (T-CY)

3 Capacity building: C-PROC ▶ Technical cooperation programmes

Council of Europe's Convention on Cybercrime – The Budapest Convention

- Opened for signature November 2001 in Budapest
- Followed by Cybercrime Convention Committee (T-CY)
- Open for accession by any State
- As of today, the only **international Treaty on cybercrime and electronic evidence**
- It gives high-level, technology-neutral definitions of cybercrime offences
- It sets standard procedures for investigation and prosecution on the national level, and puts relevant obligations on involved parties
- It defines procedural provisions for international cooperation, police-to-police and judicial
- Guidance notes are published by T-CY to interpret BC provisions in the light of new threats and new technological paradigms

Reach of the Budapest Convention



Budapest Convention
Ratified/acceded: 53

Signed: 6

Invited to accede: 8
= 67

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

Further States drawing on Budapest Convention for legislation = 45+

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

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

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

The Cybercrime Convention Committee (T-CY)

Established under Article 46 Budapest Convention

Membership (May 2016):

- **53 Members** (State Parties)
- **17 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**

Cybercrime Programme Office of the Council of Europe in Bucharest (C-PROC)

- **Committee of Ministers decision October 2013**
- **Operational as from April 2014**
- **Currently 19 staff**

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

Current capacity building programmes

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 EU/COE Joint Project on Global Action on Cybercrime (just concluded)

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 EU/COE Targeting crime proceeds on the Internet

CyberSouth EU/COE Joint Project on Cybercrime and Electronic Evidence

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** • **Morocco** • **Philippines** • **Senegal** • **South Africa** • **Sri Lanka** • **Tonga**

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

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.

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+ countries	• Dom. Republic • Ghana • Mauritius • Morocco • Philippines • Senegal • Sri Lanka • Tonga

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.**

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.**

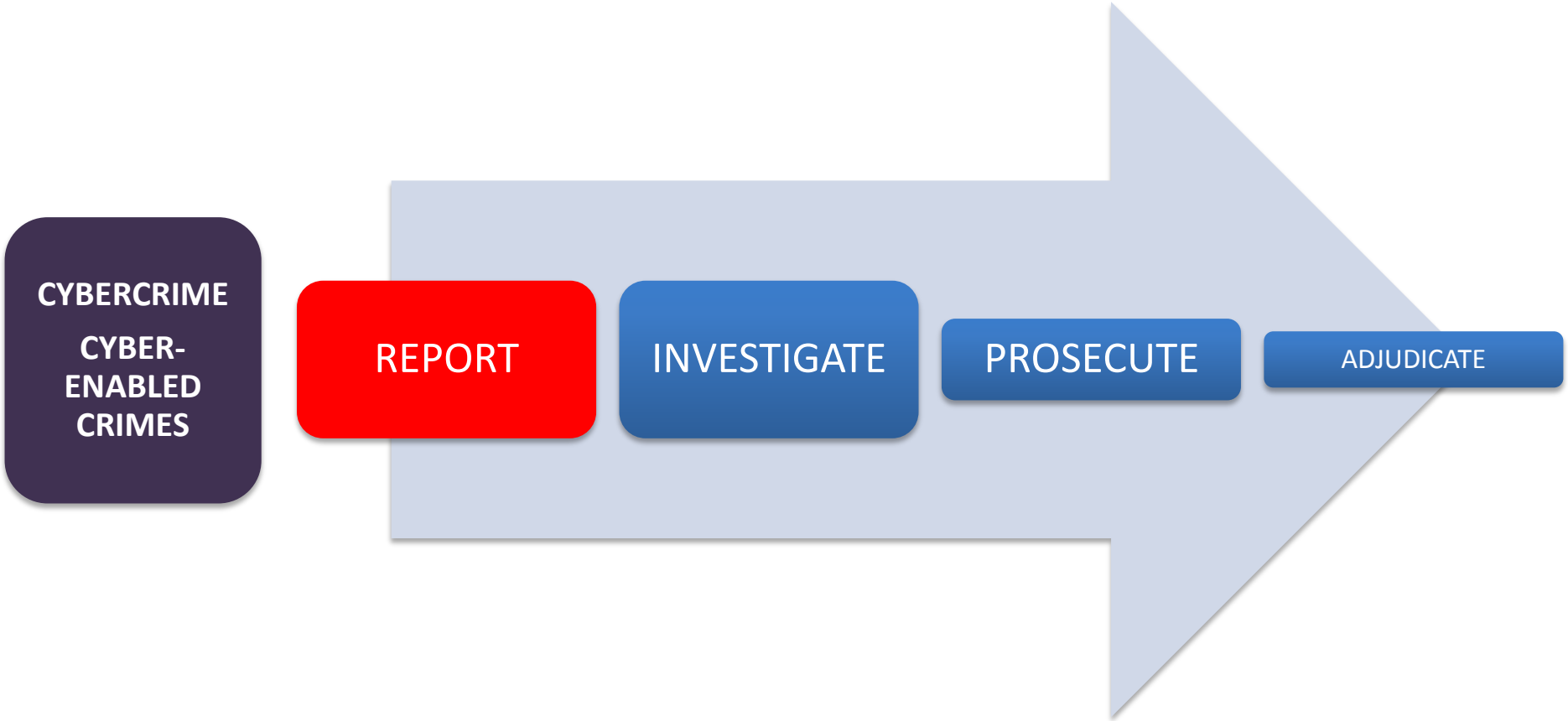
TO INCREASE THE NUMBER OF DOMESTIC AND INTERNATIONAL PROSECUTIONS AND CASES ADJUDICATED ON CYBERCRIME AND ELECTRONIC EVIDENCE

Enhanced capacities of prosecutors and judges regarding cybercrime and electronic evidence will contrbute to the rule of law, including the aplication of legislation as well as international cooperation. **Priority countries will encourage other countries to follow their example**

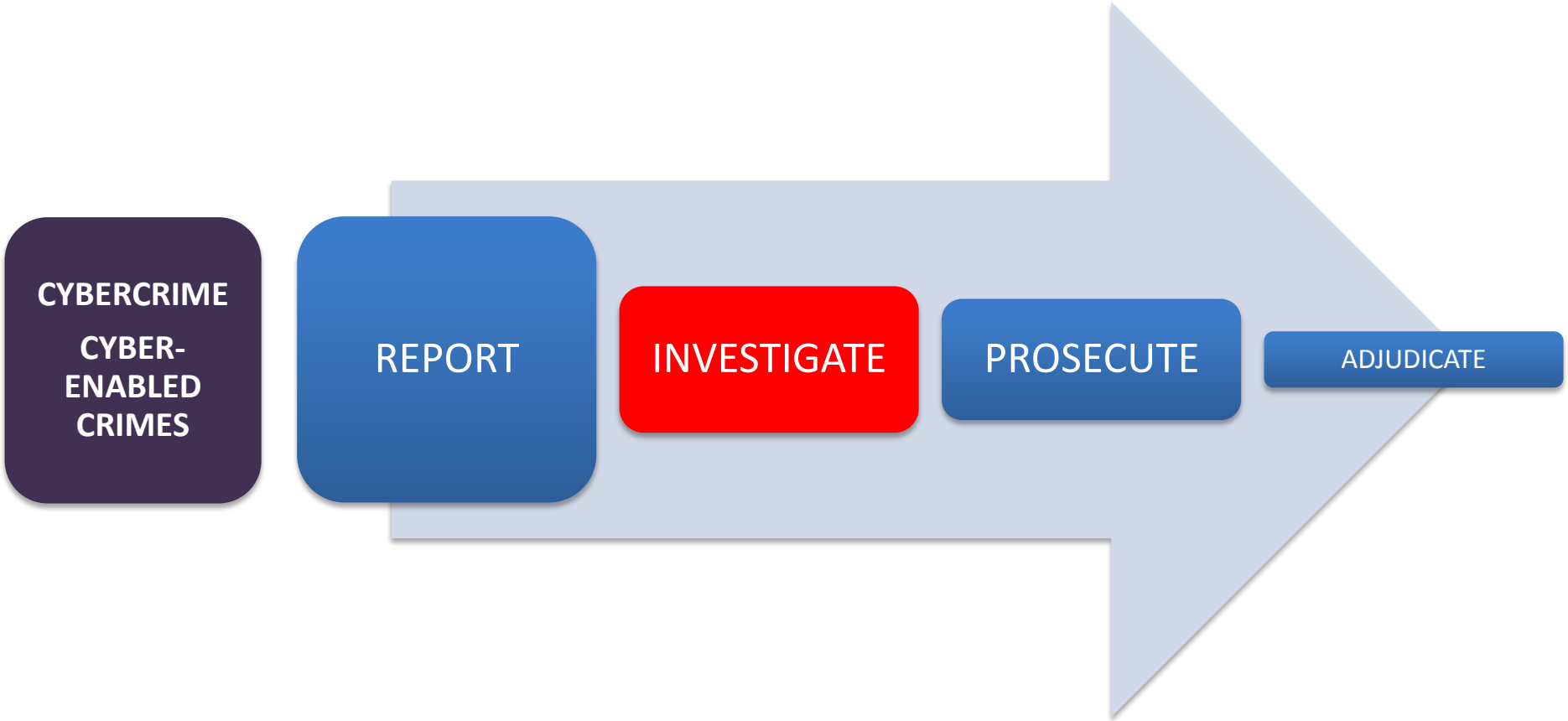
Cybercrime: A criminal justice matter

Cybercrime: A criminal justice matter

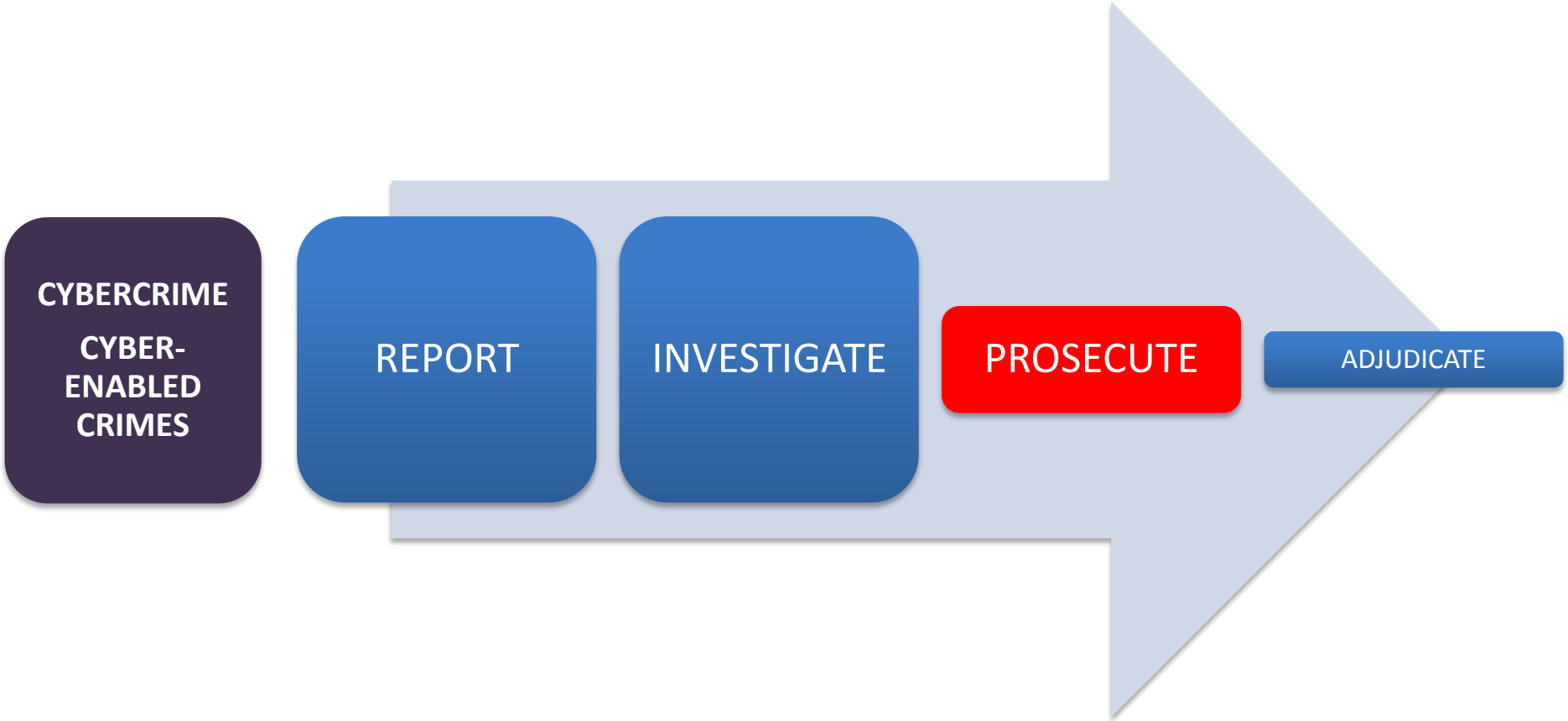
Cybercrime: A criminal justice matter



Cybercrime: A criminal justice matter



Cybercrime: A criminal justice matter



Cybercrime: A criminal justice matter

Previous activities on cybercrime statistics and reporting systems

- International workshop on statistics and reporting systems (during the Launching conference), in Dakar, Senegal, 24-27 March 2014
- Good practice study on cybercrime reporting mechanisms, September 2014
- International workshop on criminal justice statistics and reporting systems (during Colombo conference), Colombo, Sri Lanka, 26-27 March 2015
- Workshop on Crime Statistics and Reporting related to Cybercrime and Electronic Evidence, Manila, Philippines, 16-17 July 2015
- Advisory missions on cybercrime reporting systems, combined with workshop on reporting systems and legal basis for interagency cooperation, January-June 2016
- International Workshop on Effectiveness of legislation on cybercrime and electronic evidence measured through statistics, in Rabat, Morocco, 27-28 July 2016
- Initial situation assessments in the GLACY+ countries

Cybercrime statistics collection and analysis - Main challenges

- Fragmentation of reporting bodies in the same country, in the same institutions, the need for a single point of contact who could centralised all the statistics collected
- Cybercrime cases go undetected/ unreported due to issues in the reference legislation or obsolete reporting systems
- Lack of specialised training for the officers who collect the data, first responders
- Lack of classification of different offences that can be committed through the use of technology (e.g based on the BC)
- Heterogeneous processes to collect, analyse and report statistics on cybercrime and electronic evidence amongst different judicial authorities, law enforcement agencies and other involved entities

Previous activities on cybercrime statistics and reporting systems

- International workshop on Cybercrime statistics, Accra, GHANA, 29-30 March 2017
- Advisory mission in all the eight GLACY+ priority countries, within the next 3 years, by February 2020:
    - 2 priority countries in 2017
    - 3 priority countries in 2018
    - 3 priority countries in 2019
- Follow up to the implementation of the recommended actions
- Report on Cybercrime statistics and methodology

Cybercrime Reporting Systems and Criminal Justice Statistics – Open Issues

- **Cybercrime Reporting Systems**
  - What types of cybercrime are reported
  - What are the sources of cybercrime reports
  - Which agencies are responsible to receive reports
  - Interagency cooperation and collaboration with the private sector on cybercrime reporting
  - Availability of data for cases of cybercrime that are reported, on the national level
  - Challenges and possible improvements in cybercrime reporting systems
- **Criminal Justice Statistics**
  - How data and statistics are collected and analysed, and where
  - What is the use of aggregated statistics, if any
  - Availability of data for cases that are investigated, prosecuted, adjudicated, on the national level
  - Availability of data for evidences that are extracted, number of devices that are analysed, number of electronic evidences submitted to the court, number of electronic evidences admitted to the court
  - Challenges and possible improvements in criminal justice statistics related to cybercrime and cyber-enabled crimes

THANK YOU!

Matteo LUCCHETTI

Polixenia CALAGI

Cybercrime Pogramme Office of the Council of Europe (C-PROC) – Bucharest, Romania

matteo.lucchetti@coe.int
polixenia.calagi@coe.int

Accra, 29 March 2017