Workshop 4:
Capacity building to counter cybercrime

Moderator:

- Alexander Seger, Council of Europe

Speakers:

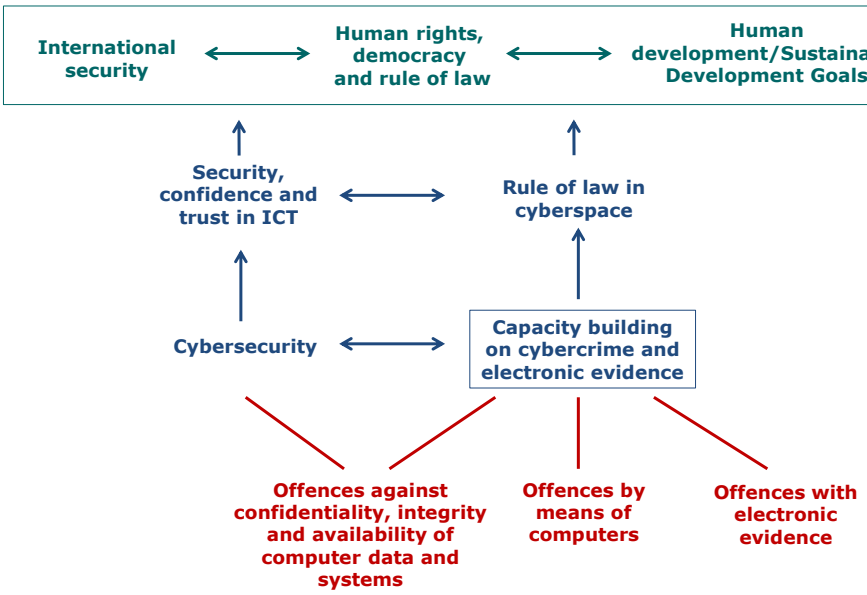
- Imali Kotelawala, Sri Lanka
- Claudio Peguero, Dominican Republic
- George-Maria Tyendezwa, Nigeria
- Oleksii Gichko, Ukraine

Agenda:

- Introduction: What is capacity building on cybercrime?
- Why?
- Frameworks
- Capacity building in practice
- Take-aways

www.coe.int/cybercrime

Introduction: about capacity building on cybercrime

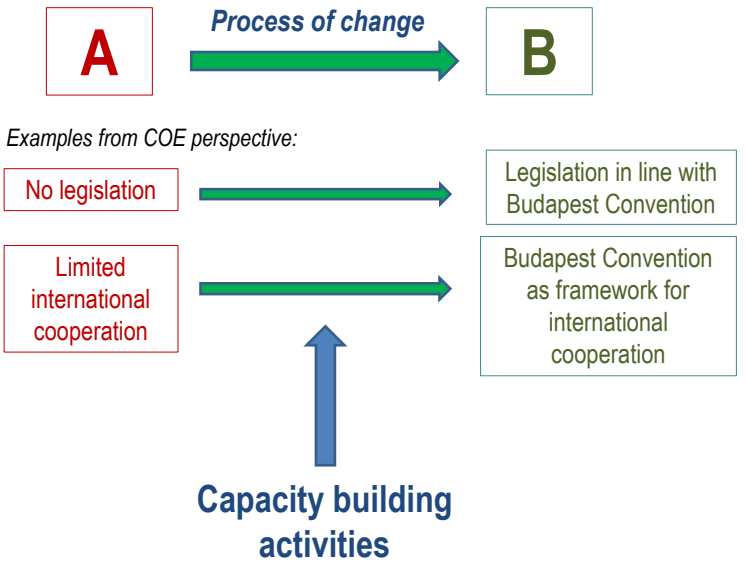


Introduction: about capacity building on cybercrime

"Capacity building" = 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.

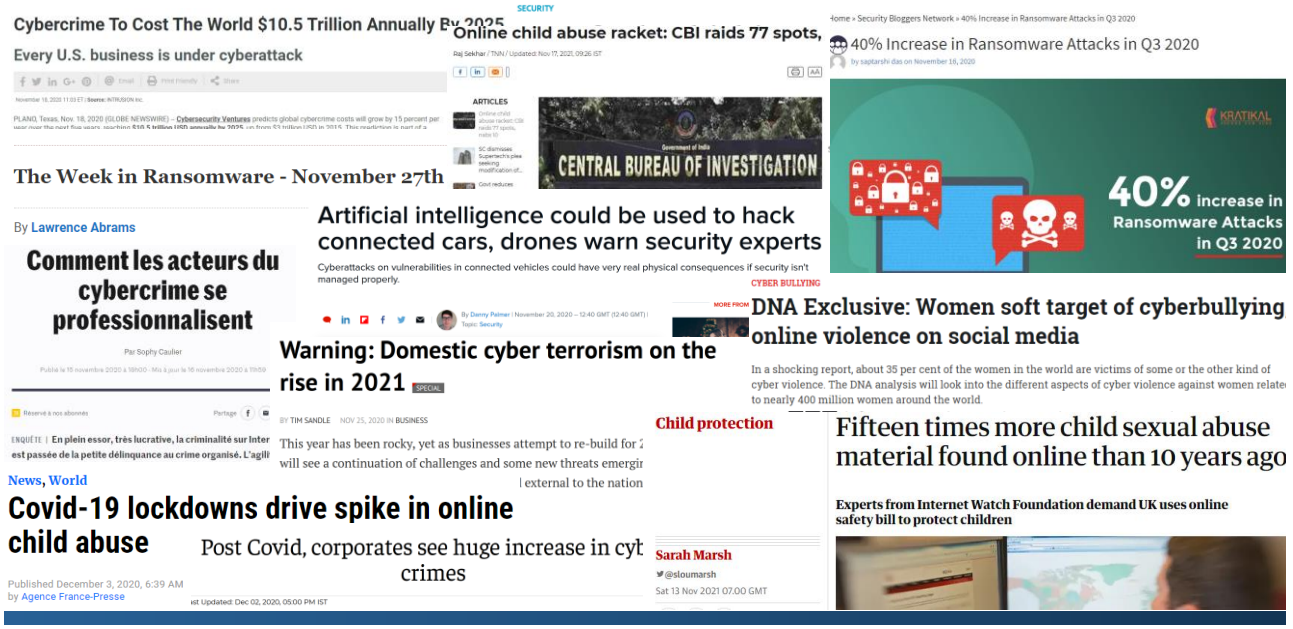
It should be aimed at protecting individuals and society against crime and at protecting the rights of individuals, at promoting security, confidence and trust in ICT, at strengthening human rights, democracy and the rule of law in cyberspace and at contributing to human development.



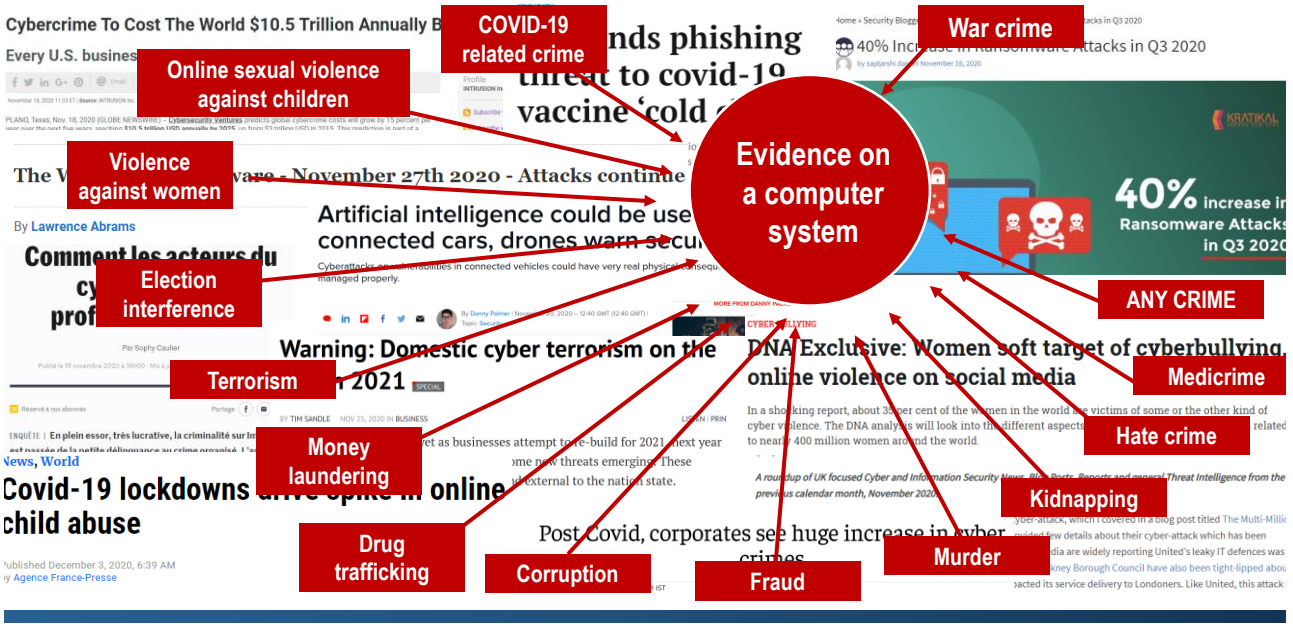
Why capacity building on cybercrime?

- Challenges of cybercrime and e-evidence and to an effective criminal justice responses. Perspectives of:
  - Dominican Republic
  - Ukraine
  - Sri Lanka
  - Nigeria

Why capacity building on cybercrime? Cybercrime

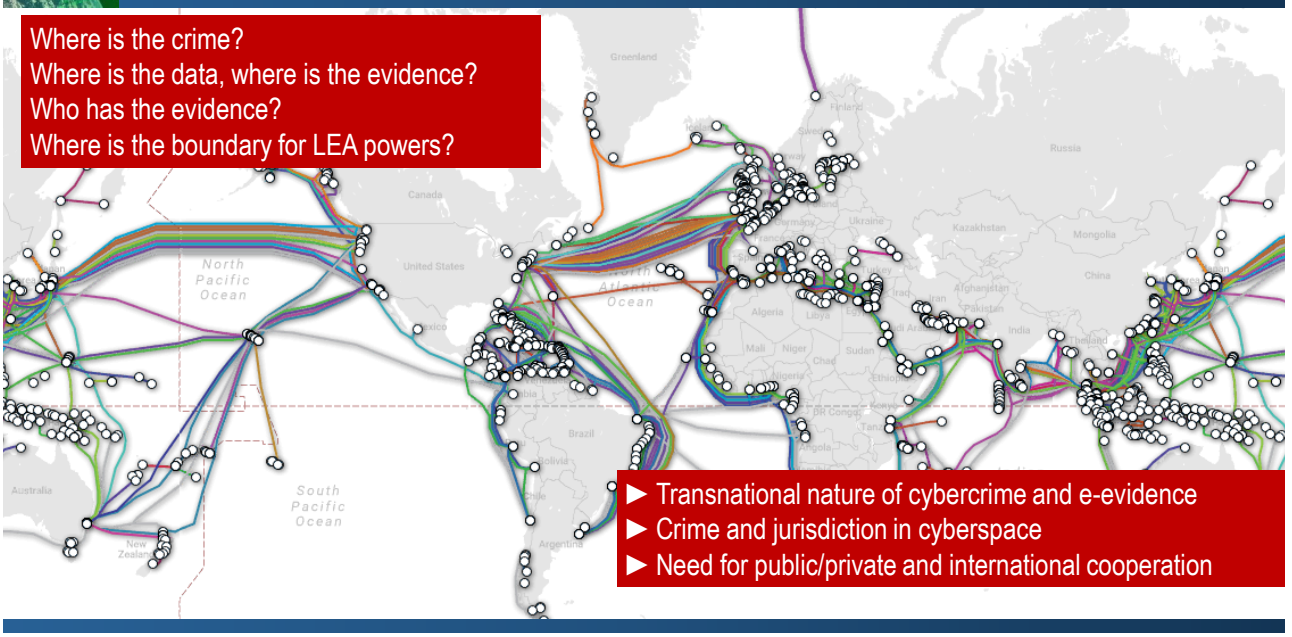


… and e-evidence re all types of crime



Cybercrime and e-evidence: the problem of territoriality and jurisdiction

Where is the crime?
Where is the data, where is the evidence?
Who has the evidence?
Where is the boundary for LEA powers?



- Transnational nature of cybercrime and e-evidence
- Crime and jurisdiction in cyberspace
- Need for public/private and international cooperation

Why capacity building on cybercrime?

The “0.1% problem”

Dominican Republic

Why capacity building on cybercrime? Challenges

Biggest challenges:

Why capacity building on cybercrime? Challenges

Biggest challenges:

#1

#2

#3

Why capacity building on cybercrime? Challenges

Biggest challenges:

#1 BUDGET

#2

#3

Why capacity building on cybercrime? Challenges

Biggest challenges:

#1 BUDGET

#2 BUDGET

#3

Why capacity building on cybercrime? Challenges

Biggest challenges:

#1 BUDGET

#2 BUDGET

#3 **BUDGET**

Challenges encountered regarding cybercrime and criminal justice capacities

INTERNATIONAL COOPERATION

- ACCESS TO THE EVIDENCE FOR INVESTIGATIONS
- STOPPING MONEY FLOWS / ASSET RECOVERY
- FILE DECRYPTION

Why capacity building on cybercrime? Challenges

SUSTAINABILITY OF SPECIALIZED UNITS

- Specialized forensic equipment
  - Relatively short life span
  - Technology changes way too fast

Why capacity building on cybercrime? Challenges

SUSTAINABILITY OF SPECIALIZED UNITS

- Specialized forensic equipment
  - Relatively short life span
  - Technology changes way too fast
- Software licenses
  - Perpetual ever-increasing yearly cost

Why capacity building on cybercrime? Challenges

SUSTAINABILITY OF SPECIALIZED UNITS

- Specialized forensic equipment
  - Relatively short life span
  - Technology changes way too fast
- Software licenses
  - Perpetual ever-increasing yearly cost
- Specialized investigators and forensic analysts salaries
  - People come and go
  - Training needs to be almost perpetual

Why capacity building on cybercrime? Challenges

SUSTAINABILITY OF SPECIALIZED UNITS

- Specialized forensic equipment
  - Relatively short life span
  - Technology changes way too fast
- Software licenses
  - Perpetual ever-increasing yearly cost
- Specialized investigators and forensic analysts salaries
  - People come and go
  - Training needs to be almost perpetual
- Units deployment countrywide

Why capacity building on cybercrime? Challenges

Ukraine

Why capacity building on cybercrime? Challenges

The cyber department of Ukraine ‘s Security Service (SSU) dismantled a gang that stole accounts of about 30 million individuals.

The cyber department of Ukraine ‘s Security Service (SSU) has taken down a group of hackers that is behind the theft of about 30 million individuals. The gang was offering the stole accounts for sale on the dark web, according to the SSU they earned almost UAH 14 million from the sale.

Russian cyber operations in Ukraine continue even as army loses ground

By JOHN SAKELLARIADIS | 09/19/2022 10:00 AM EDT

Ukraine-Krieg und Ransomware verschärfen angespannte IT-Sicherheitslage

24. September, 2022 11:48

Timeline of recent cyberattacks in Ukraine

To Prosecute Putin for War Crimes, Safeguard the Digital Proof

Holding Russia accountable for atrocities in Ukraine requires the

How digital evidence of war crimes in Ukraine is being collected, verified and preserved

Researchers gather evidence of possible Russian war crimes in Ukraine

‘Open-source intelligence community’ is already collecting and studying video and photo evidence

Why capacity building on cybercrime? Challenges

Since 2016, **Ukraine has created a legislative framework** for ensuring the cybersecurity of the state and the basis for combating cybercrime

In 2016, **the CyberSecurity Strategy of Ukraine was adopted,** which was an important step in introducing long-term planning approaches in this area. Over the years, the efforts had been made to establish and develop a national cybersecurity system

In addition, in 2021, **the Law of Ukraine "On Critical Infrastructure",** which defines the legal and organizational basis for the creation and operation of a national system for protecting critical infrastructure, contains only requirements for classifying objects as critical infrastructure

In 2021, **a new version of the Cybersecurity Strategy of Ukraine** for the next 5 years was adopted

In 2017, **the Law of Ukraine "On the Basic Principles of Ensuring Ukraine's Cybersecurity" was adopted,** which is the legal basis for the creation of a national cybersecurity system and its main subjects' tasks in the field of cybersecurity. Regulatory support for cyber defense of critical information infrastructure has been improved, the procedure for its definition and general requirements for its cyber defense have been adopted

On problematic issues, there remains the lack of an approved list of critical infrastructure facilities, which complicates the implementation of measures to protect them

Why capacity building on cybercrime? Challenges

REGARDING THE CONVENTION ON CYBERCRIME

September 2005

THE CONVENTION WAS RATIFIED BY UKRAINE

Ukraine has undertaken to implement the provisions of this document in the national legislation. According to Convention cybersecurity subjects of different countries should be able to interact internationally, by preserving and providing access to the necessary information within the framework of criminal investigations at the relevant requests

Law enforcement agencies of Ukraine use this opportunity, send appropriate requests to the competent structures of the countries participating in the Convention, which makes it possible to obtain an evidence base

Ukraine has not yet fully implemented the provisions of the convention into national legislation. The legislation of Ukraine does not contain provisions on the mandatory storage of data by national providers

For example, there are no rules requiring ISPs to store information for 90 days, as required by Article 16, paragraph 2, of the Budapest Convention

In the Ukrainian legislation there is only administrative liability in the form of a fine for non-compliance with the terms of information storage

Why capacity building on cybercrime? Challenges

IN ORDER TO ENSURE THE IMPLEMENTATION OF CERTAIN PROVISIONS OF THE CONVENTION ON CYBERCRIME, THE FOLLOWING ISSUES WERE DISCUSSED WITH THE VERKHOVNA RADA OF UKRAINE SINCE 2019, LEADING TO FOLLWING RESULTS (SOME DRAFTS ARE STILL IN DEVELOPMENT):

1

Law "On Amendments to the Criminal Procedure Code of Ukraine and the Law of Ukraine On Electronic Communications to Increase the Effectiveness of Pre-Trial Investigations in Hot Pursuit and Counteraction to Cyber Attacks" was adopted in March 2022:

- Preservation powers under Article 16 of the Budapest Convention mostly implemented;
- Partial implementation of production orders (Article 18);
- Detailed implementation of search/seizure provisions (Article 19);
- Orders/procedural document in electronic format (better speed of proceedings).

2

Two more drafts (on matters of electronic evidence and on procedural rules on e-evidence) were developed together with the Council of Europe and address the following remaining issues in the laws of Ukraine for compliance with the Budapest Convention:

- Traffic data disclosure (Article 17)
- Full scope of production orders (Article 18)
- Admissibility of electronic evidence as a standalone concept (or equivalent common judicial practice)
- Categories of data (subscriber, traffic, content)
- Safeguards and guarantees under Article 15, especially with regard to real-tie collection of traffic data and monitoring of context powers.

Challenges Encountered in Cybercrime and Criminal Justice Capabilities

A Sri Lankan Perspective

Imali Kotelawala
Assistant Secretary (Legal)
Ministry of Justice, Prison Affairs and Constitutional Reforms

Sri Lankan Digital Landscape

Total Population
21.54Mn

Internet Users
11.34 Mn
Vs Population
52.6%

Accounts with a FI
Vs Population
73.6%

No 1 in South Asia in Networked Readiness Index (NRI)

Mobile Connections
32.29 Mn
Vs Population
149.9%

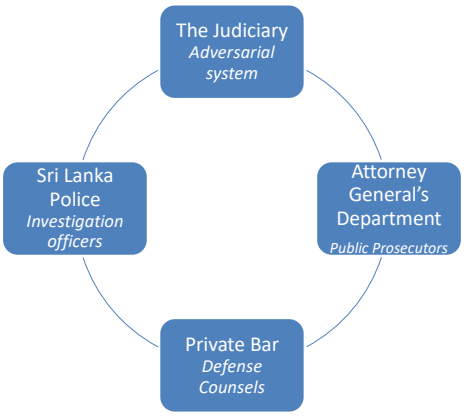
Active Social Media Users
8.2 Mn
Vs Population
38.1%

Digital Payment in Past Year
Vs Population
47.2%

ICT Sector - 5th Largest Revenue Earner for Sri Lanka
Expected USD 3Bn by 2024

Overview of the Criminal Justice System

- *Adversarial and a victim centric prosecutorial system*
- *Degree of proving a criminal case is beyond a reasonable doubt*



Stakeholders of the Criminal Justice System

Sri Lanka: Reported Incidents

Incident Type	No of Incidents - 2019	No of Incidents - 2020	No of Incidents - 2021
DDOS	2	1	13
Ransomware	6	24	45
Abuse/Hate/Privacy violation	307	70	182
Malicious Software issues	8	9	10
Phone Hacking	1	6	7
Scams	5	157	322
Phishing	5	17	98
Website Compromise	175	85	282
Financial/Email frauds	7	57	115
Intellectual property violation	1	1	8
Server Compromised	2	6	13
Social media	2662	15895	16795
Other	364	48	144

Challenges in prosecuting cybercriminals

Lack of data due to anonymity and attribution

Technical challenges

Obstacles in international cooperation

Challenges of public-private partnerships

Loss of location

Challenges associated with national laws

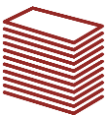
Limited abilities of law enforcement authorities

Awareness

Delays in the Criminal Justice System

Heavy case load in criminal courts

(Increase of courts cannot be implemented)



Lack of trainings given to the stakeholders of the criminal justice system

(Due to COVID19 and ongoing economic crisis)

Insufficient number of judges in the courts of first instance

(No. of the Judges in the Supreme Court and the Court of Appeal were increased by the 20th Amendment to the Constitution)

Lack of updated knowledge of investigations on cross border cybercrime

Laws delays in criminal courts will be reduced by the introduction of pre-trial conferences by Criminal Procedure Code Amendment Act, No.02 of 2022 which promotes lawful, fair and expeditious trial.

Evolving Cyber Threat Landscape and Resulting Expertise Gap

Why capacity building on cybercrime? Challenges

Terlumun George-Maria TYENDEZWA, CFE

Deputy Director, Federal Ministry of Justice, Abuja, Nigeria

*Vice-Chair of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, pursuant to GA Resolution A/RES/74/247.

Why capacity building on cybercrime? Challenges

- **Policing & Investigating Cybercrime - Issues faced**

- Domestic coordination/synergy
- Search and Seizure of Stored Computer Data
- Real Time Collection of Traffic Data
- Interception of Content Data –
- Collecting & sharing info/intel /locating offenders, differentiating Intelligence & Evidence
- Digital Evidence Gathering – Standards/ Admissibility/ Forensics/
- Data privacy, data retention(or lack of) - Impact
- Technical equipment and tools// capabilities

Why capacity building on cybercrime? Challenges

- **Prosecuting & Adjudicating Cybercrime - The Issues**

- Substantive law Issues -
- Procedural - Evidence Gathering – Admissibility/
- Lack of early interface between investigators and prosecutors,
- Access to Electronic Evidence for the Prosecution Stage
- Digital Evidence handling & Court room presentation –/
- Capacity-building - Judges, & prosecutors/

Why capacity building on cybercrime? Challenges

- **International Cooperation - The Issues**

- Policies & legislation// Budapest Convention/Malabo Convention//national legislation/
- Formal cooperation – advantages & disadvantages
- Informal cooperation – Solving the tracing problem – flexible & faster LE contacts/resources/Networks /LEA-Private Sector direct cooperation// Complexities & Delays,
- Data privacy, & data retention(or lack of) Disclosure Management - Impact
- Technical capacity/Tools and capabilities .

Frameworks for capacity building

The mechanism of the Budapest Convention

Budapest Convention on Cybercrime (2001):

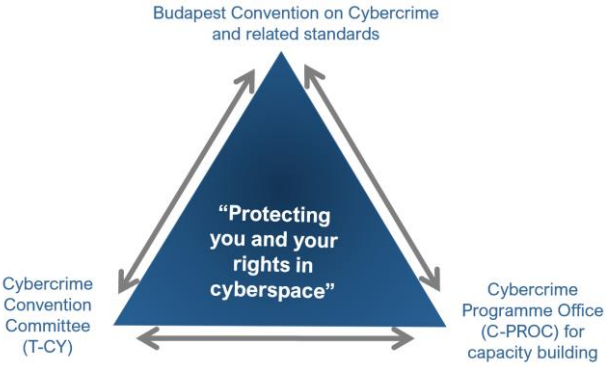
1. Specific offences against and by means of computer systems
2. Procedural powers with safeguards to investigate cybercrime and collect electronic evidence in relation to any crime
3. International cooperation on cybercrime and e-evidence

+ 1st Protocol on Xenophobia and Racism via Computer Systems

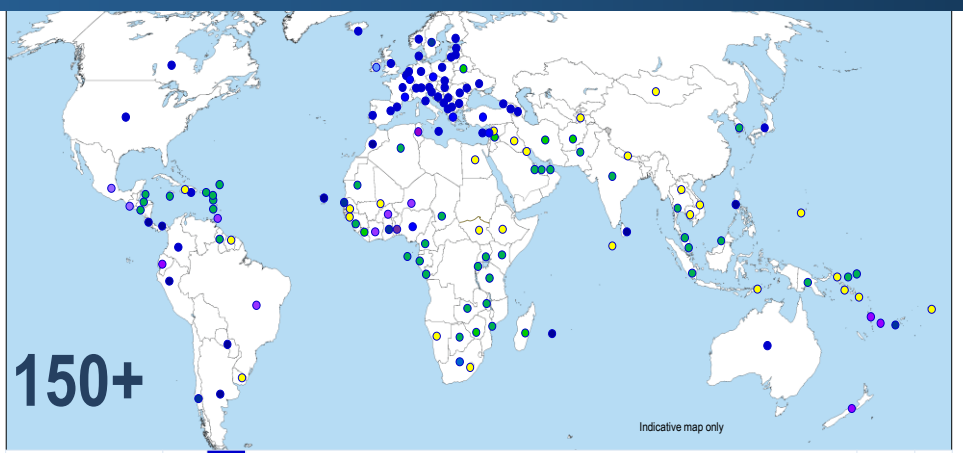
+ Guidance Notes

+ 2nd Protocol on enhanced cooperation on cybercrime and electronic evidence (Strasbourg, 12 May 2022)

By September 2022: 67 Parties and 15 Observer States



Reach of the Convention on Cybercrime



Parties:	67				
Signed:	2		Other States with substantive laws broadly in line with Budapest Convention:	45+	
Invited to accede:	13		Further States drawing on Budapest Convention for legislation:	30+	
=	**82**		=	**75+**	

The Convention on Cybercrime: backed up by capacity building

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

- Support processes of change towards stronger criminal justice capacities on cybercrime and e-evidence in line with the Budapest Convention and with rule of law safeguards
- 5 ongoing projects with a cumulative budget of EUR 38+ million
- 40 staff
- Some 400 activities per year
- Capacity for virtual capacity building
- Cooperation with 120+ countries in 2021/2022
- Joint projects with the European Union
- Voluntary contributions by Canada, Hungary, Japan, UK and USA in 2021/22
- Support to T-CY

iPROCEEDS-2: Cooperation between Internet Service Providers and Law Enforcement Agencies Implementation of Cyber Crime Inv

11 NOVEMBER 20

Provided under the Joint Project of the Europe the Ministry of Internal Affairs of Federation c between Internet Service Providers and Law E

GLACY+: Judicial Trainers on Cybercrime and E-Evidence gather to discuss medium-term development of a global network of

ence was held on the 17th of . The meeting built on the results

CyberEas

12 NOVEMBER 2

A new online Thursday, 12 women by in

al meeting on the rocedures (SOPs) and ime Investigations and E-

Kiko's exci

20 NOVEMBER 202

The Council of (EndOCSEA@E character frien

ond online national meeting on the in Cybercrime Investigations and E-

on cybercrime legislation

GLACY+: Confere during th Portugu

18 – 20 NOVEMBER 2020 | ONLINE | MULTIPLE COUN

nd investigators took part in the r professionals of justice, co-operation...

effects of COVID-19 on

GLACY+: towards

9 NOVEMBER 20

The webinar on "Effective Access to Electronic Evidence: towards a new Protocol to the Budapest Convention", held on November 9th, 2020, was a joint initiative of the Cybercrime Programme Office (C-PROC) of

he Council of Europe teamed up on November 10th in delivering a webinar dedicated to debating the effects of the pandemic on cybercrime in the Pacific. The event gathered more than 50 cybercrime policy makers, criminal justice and law

CyberEast: Fourth Regional Cyber Cooperation Exercise

13 - 16 SEPTEMBER 2022 | ISTANBUL, TÜRKIYE

In the world of today, the increasing number of attacks against computer systems and data is a growing concern for both cyber security professionals and criminal justice authorities. This is the reason why the CyberEast and CyberSecurity EAST projects, co-funded by the European Union, seek to...

Panama and the Convention on Cybecrime: GLACY+ workshop on domestic legislation

PANAMA&ONLINE | 15 SEPTEMBER 2022

On 15 September, the Council of Europe, through the GLACY+ joint project wih the European Union, held a hybrid workshop with the authorities of Panama in view of further harmonising national legislation on cybercrime and electronic evidence with the provisions of the Budapest Convention on...

GLACY+: Supporting national delivery of an introductory course on cybercrime and electronic evidence in Benin

2 SEPTEMBRE 2022 | COTONOU, BENIN

From 30 August to 2 September, a group of judges and prosecutors from Benin, who had been trained to become national trainers during a dedicated workshop earlier in August, delivered for the first time an introductory course on cybercrime and electronic evidence to their peers. During the first...

Underground Economy Conference 2022 – a prime example of public/private cooperation

5 - 8 SEPTEMBER 2022 | STRASBOURG, FRANCE

From 5 to 8 September 2022, the Council of Europe co-hosted for the third time the Underground Economy Conference at the Palais de l'Europe. This prominent international information security event, co-organised by Team Cymru and the Council of Europe, brought together around 500 experts from law...

Capacity building in practice

CyberSouth: Judicial Training Course on International Co-operation on Cybercrime and Electronic Evidence in Lebanor

13-15 JULY 2022 | BEIRUT, LEBANON

From 13 to 15 July 2022, the Cybercrime Programme Office of the Council of Europe (C-PROC), within the framework of the joint European Union – Council of Europe CyberSouth project and in co-operation wit the Lebanese Ministry of Justice, organised a judicial training course on international...

GLACY+: Reviewing project progress and planning activities during the project's 12th Steering Committee meeting

13 JULY 2022 | ONLINE

On 13 July 2022, the Council of Europe together with the European Union and INTERPOL, hosted the 12th meeting of the GLACY+ Steering Committee to discuss developments in priority countries, review GLACY project activities held in the first half of 2022 and shape future project activities. During...

iPROCEEDS-2: Another Specialised Judicial ToT delivered for Serbian prosecutors

12 - 14 JULY 2022 | BELGRADE, SERBIA

During 12 – 14 July 2022 the iPROCEEDS-2 project, a joint project of the European Union a the Council of Europe has delivered another Specialised Judicial Training of Trainers on Training Skills, this time for Serbia prosecutors, in Belgrade, Serbia. A cohort of 17 prosecutors delegates took...

iPROCEEDS-2: Regional Cybercrime Exercise on a Ransomwa Attack

11 - 14 JULY 2022 | IZMIR, TURKIYE

Over the last years, ransomware attacks have been confirmed as one of cybercrime's ma business models, pushing aside other well-established operating modes like phishing, online frauds, banking trojans, anc distributed denial-of-service (DDoS) attacks. When such an attack occurs, response time...

Capacity building in practice

Examples from:

- Ukraine
- Sri Lanka
- Nigeria
- Dominican Republic

Ukraine

Capacity building in practice: Ukraine

CYBERCRIME@EAP projects 2011-2018

Joint regional projects of the European Union and the Council of Europe on **cooperation against cybercrime** under the Eastern Partnership Facility

Participating countries: Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine

The projects were aimed **at strengthening the capacities** of Eastern Partnership countries to cooperate effectively against cybercrime

4 projects between 2011 and 2018

Components:

- Policies and awareness of decision-makers
- Harmonised and effective legislation
- Judicial and law enforcement training
- Law enforcement – Internet service provider cooperation
- International judicial and police cooperation
- Financial investigations

Capacity building in practice: Ukraine

CyberEast 2019-2023

Joint project of the EU and the Council of Europe:
to support cyber resilience and criminal justice capacities of the Eastern Partnership countries (Armenia, Azerbaijan, [Belarus,] Georgia, Moldova and Ukraine)

- Legal frameworks
- Capacities of judicial and law enforcement authorities
- Interagency cooperation (focus on CSIRTs)
- International cooperation and cooperation with service providers

Since start of war of aggression by Russia:

- Amendments to laws to increase effectiveness of hot pursuits and action against cyber attacks adopted
- Training on use of OSINT and e-evidence in war crime proceedings
- Review of legislation on admissibility of open-sourced evidence in criminal proceedings underway
- Training on ransomware and handover of translated course
- Advanced cybercrime training of Ukrainian judges in Romania

CYBER POLICE DEPARTMENT OF THE NATIONAL POLICE OF UKRAINE

On October 13, 2015, **the Department of Cyberpolice** was established as a structural unit of the National Police.

The purpose of creating the Cyberpolice in Ukraine was to **reform and develop units of the Ministry** of Internal Affairs of Ukraine, which ensured the training and functioning of highly qualified specialists in expert, operational and investigative police **units involved in combating cybercrime**, and capable of using the latest technologies at a high professional level in the operational and service activity.

Capacity building in practice: Ukraine

THE CYBERSECURITY DEPARTMENT OF THE SECURITY SERVICE OF UKRAINE

The Cybersecurity Department of the Security Service of Ukraine was **established in 2012**

With the assistance of the UKRAINE-NATO Cybersecurity Trust Fund in 2016, the Department began to effectively implement measures to combat cybercrime and ensured the creation and development of the Cybersecurity Situation Center at the SSU

Technical equipment and software for the work of the SSU Center was received in July 2017 within the framework of the implementation of the first stage of the Agreement on the implementation of the NATO-Ukraine Trust Fund on Cybersecurity

Capacity building in practice: Ukraine

According to the **Law of Ukraine "On the Basic Principles of Cybersecurity"** of October 5, 2017, the National Police of Ukraine ensures the protection of human and citizen rights and freedoms, the interests of society and the state from criminally unlawful encroachments in cyberspace, takes measures to prevent, detect, stop and disclose cybercrimes, increase public awareness of security in cyberspace

The Security Service of Ukraine carries out prevention, detection, termination and disclosure of criminal offenses against the peace and security of mankind committed in cyberspace, carries out counterintelligence and operational-search measures aimed at combating cyberterrorism and cyber espionage, secretly checks the readiness of critical infrastructure facilities for possible cyberattacks and cyber incidents; the interests of the state; investigates cyber incidents and cyberattacks against state electronic information resources, information, the requirement for the protection of which is established by law, critical information infrastructure; provides response to cyber incidents in the field of state security

The priority direction of the development of cyber security of Ukraine, determined **by the Cyber Security Strategy of Ukraine,** is aimed at developing the potential of the security and defense sector in the field of cyber security, which involves the separation of responsibilities between the Cyber Police and the Department of Cyber Security of the Security Service of Ukraine

IF THE CONSEQUENCES OF A CYBERCRIME AFFECT THE SECURITY OF UKRAINE AT THE NATIONAL LEVEL, THEN IT SHOULD BE INVESTIGATED BY THE SSU

- **IF AN APT GROUP SPONSORED BY ANOTHER STATE IS FOUND, OR A HACKER GROUP MANAGED BY A FOREIGN SPECIAL SERVICE IS FOUND, THE INVESTIGATION IS CARRIED OUT BY THE SSU**

Capacity building in practice: Ukraine

UNTIL 2016 NO CONCEPT OF "COMBATTING CYBERCRIME" IN UKRAINE

1

However**, thanks to the projects of the Council of Europe,** an assessment of national legislation was implemented

2

After gaining the **best experience** of the CE countries in the field of ensuring cyber security, it became clear the need to create law enforcement agencies in Ukraine that should fight cybercrime

3

In addition, a separate department has been created in the Office of the Prosecutor General of Ukraine and appropriate prosecutors have been appointed to provide procedural support for cybercrime investigations

4 War of aggression is accompanied by cyber attacks + Evidence of war crimes may be e-evidence = Effective criminal justice response is essential

Nigeria

Capacity building in practice

I. National Cybersecurity Policy And Strategy

The President approved and launched Nigeria's first **National Cybersecurity Policy and Strategy on 05th February, 2015,** and second iteration was launched in 2021.

II. The national CERT (www.cert.gov.ng)was set up and became operational in 2015. One sectoral CERT (http://cerrt.ng/) is also operational with more sectors to follow shortly.

III. **Amendment of the** Evidence Act, 2011 – Sections 84 and 258 :
Specific provisions for Admissibility of electronic evidence.

Capacity building in practice

IV. The Administration of Criminal Justice Act, 2015 – Sections 15(4), 18,37-39, 43 – 44, 106, 143, etc. **The ACJA, 2015 introduced several innovations into the criminal procedure space that are worth noting, such as :**

- ✓ **Witness protection measures – S. 232**
- ✓
- ✓ **Prescribed time frame for remand orders – S. 296,**

- ✓ **Video recording of suspect interviews**

Capacity building in practice

V. The Cybercrime (Prohibition, Prevention, Etc.) Act, 2015 - Enacted,

Section 41*"(2) The Attorney – General of the Federation shall strengthen and enhance the existing legal framework to ensure –*

(a) conformity of Nigeria's cybercrime and cyber security laws and policies with regional and international standards;
(b) maintenance of international co-operation required for preventing and combating cybercrimes and promoting cyber security; and
(c) effective prosecution of cybercrimes and cyber security matters."

Capacity building in practice

The Cybercrime (Prohibition, Prevention, Etc.) Act, 2015 – Enacted …

- ***S. 42 – Cybercrime Advisory Council***

Inaugurated on 18th April 2016 – working to improve implementation, coordination, monitoring and evaluation,

- *GLACY+ Project National Coordination Team – inaugurated and coordinated capacity-building cutting across law enforcement, prosecutors, judges and other stakeholders.*
- Development of Nigeria's first **National Cybercrime Strategy** is underway to enhance the fight against cybercrime.

- *Accession to the Budapest Convention on* Cybercrime – 06thJuly 2022

Capacity building in practice

Going forward

- Legislators/Policymakers – commit political will to improve legal framework and ensure adequate personnel and resources
- Improve domestic inter-agency coordination & synergy
- Enhance government/LEA and Private sector collaboration/partnerships/trust
- Cyber capacity-building & Training – capabilities to secure and forensically obtain electronic evidence more quickly and effectively, particularly for:
  - ✓ Law Enforcement Officers, Investigators, Analysts,
  - ✓ Judges, Prosecutors, CAUs, lawyers/CSOs/
  - ✓ Ensure understanding of international co-operation frameworks & tools available and their appropriate use/dynamics.
- Networking and knowledge sharing – JITs/Engagement on regional and international level to enhance enforcement capabilities … respecting rights, growing trust and building resilience.

Legal Framework & Capacity Building to Combat Cybercrime

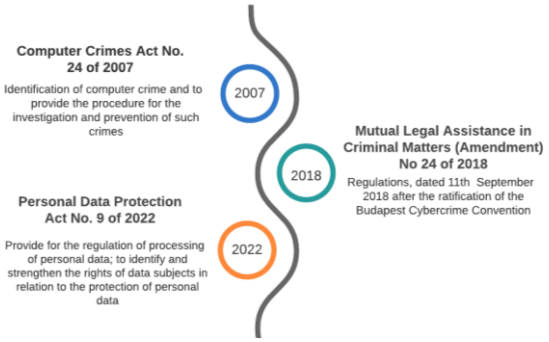
Sri Lankan Perspective

Imali Kotelawala
Assistant Secretary (Legal)
Ministry of Justice, Prison Affairs and Constitutional Reforms

Laws to Counter Cybercrime

- **Extradition Law, No. 8 of 1977** — 1977
- **Evidence (Special Provisions) Act No. 14 of 1995** — 1995
  Admissibility of audio visual recordings, and of information contained in statements produced by computers in civil and criminal proceedings
- **Penal Code (Amendment) Act No. 22 of 1995** — 1995
- **Amendment to Monetary Law Act No. 32 of 2002** — 2002
  Scriptless Securities Trading – Public Debt Settlement System
- **Intellectual Property Rights Act, No 36 of 2003** — 2003
  Protection of software and intellectual ICT outputs
- **Convention On The Suppression of Terrorist Financing Act No.25 of 2005** — 2005
- **Payment and Settlement Systems Act No. 28 of 2005** — 2005
  Legal Framework for Digital Banking and Mobile Payment Licenses
- **Prevention of Money Laundering Act No. 5 of 2006** — 2006
- **Financial Transactions Reporting Act No. 6 of 2006** — 2006
- **Penal Code (amendment) Act No. 16 of 2006** — 2006
- **Electronic Transactions Act No, 19 of 2006, amended by Act No. 25 of 2017** — 2006
  to give effect to the provisions of the united nations convention on the use of electronic communications in international contracts
- **Payment Devices Fraud Act, No. 30 of 2006** — 2006

Laws to Counter Cybercrime

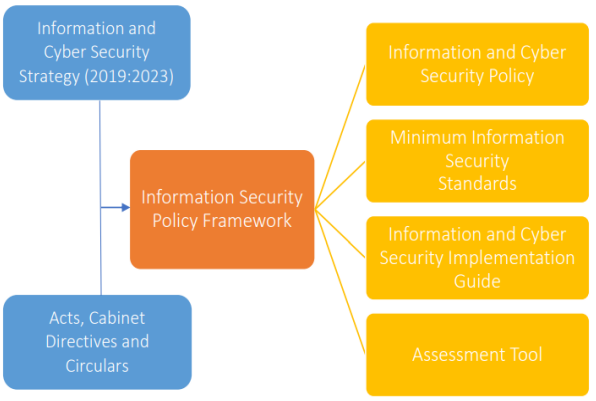


- Personal Data Protection Act is based on the 2nd Additional protocol mappings.

Policies and Standards

- Introduction of the government security policy (2009) based on ISO 27000
  The Central Bank of Sri Lanka (CBSL) along with the Sri Lanka Banks Associations (SLBA) and Sri Lanka CERT (a subsidiary of ICTA) have worked together to establish a common baseline security standard, based on a globally recognized ISO 27000 series of international standards for Information Security
- National Data Sharing Policy
  The objective of the policy is to define a set of guidelines and principles to help create an ecosystem for the enhanced access to the sharable data to relevant stakeholders protecting the rights of the information provider and the seeker.
- Information and Cyber Security Policy for Government Organizations
  Implemented in August 2022

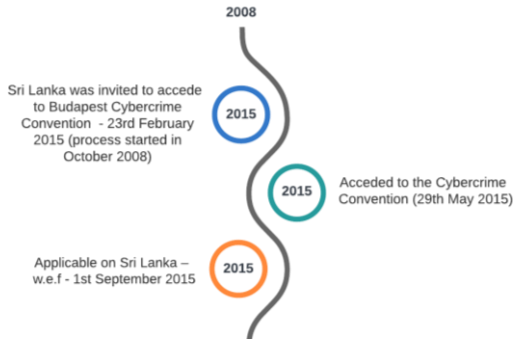
Information and Cyber Security Policy
for Government Organizations



Information Security Policy Framework

Overview of the Policy

The Budapest Cybercrime Convention



Challenges Addressed by the Budapest Cybercrime Convention

- Regulatory and Law reform based on "International Standards".
- Harmonization of Legislation.
- Continuous improvements based on regular assessments.

- 1st Country in South Asia & 2nd in Asia after Japan
- Fastest ever Accession in Council of Europe history

Sri Lanka Computer Emergency Readiness Team (CERT)

Focal point for cyber security

Established in 2006 by ICTA to address the potential increase of cyber security incidents.

A fully owned by the Government of Sri Lanka and it's under the Ministry of Technology

APCERT, APNIC, FIRST, CYBER4Dev, CAMP, JPCERT CC
Japan Computer Emergency Response Team Coordination Center
JPCERT コーディネーションセンター

Services

- General services such as incident handling, awareness services, consultancy services
- Managed Services such as Vulnerability Assessments, Penetration Testing, System Hardening, On-site and off-site consultation
- Digital forensics investigation services
- Research & Policy Development

Projects

- National Cyber Security Operations Centre (NCSOC)
- National Information and Cyber Security Strategy of Sri Lanka (2019-2023)
- Drafting Minimum Information Security Standards for Government Organizations.
- Drafting Web Application Security Guidelines for Government Organizations
- Drafting Website Security Guidelines for Government Organizations
- Publication of Handbook on Information Security

The National Cyber Security Strategy

1. **Establishment of a governance framework**
   Establishment of a governance framework to implement National Information and Cyber Security Strategy.
2. **Enactment and Establishment of Legislation, Policies and Standards.**
   Formulation of legislation, policies and standards to create a regulatory environment to protect individuals and organizations in the cyber space
3. **Development of Competent Workforce**
   Development of a skilled and competent workforce to detect, defend and respond to cyber attacks.
4. **Resilient Digital Government and Infrastructure**
   Work with public sector authorities to ensure that digital government systems implemented and operated by them have the appropriate level of cyber security and resilience.
5. **Raising awareness and empowerment of citizens**
   Make our citizens more competent in protecting their identity, privacy and economic assets in cyber space.
6. **Development of public-private, local partnerships.**
   Development of public-private, local-international partnerships to create a robust cybersecurity ecosystem.

Training Programs

- Effective Capacity Building Measures
  - For Judicial, AG's Dept, CID Units through GLACY + Program
  - ToT for Judicial authorities & adoption of e-Evidence Guide (over 300 Judges trained) – International Coop, e-Evidence & Data Privacy
  - Sri Lanka Judicial Delegation – Training for Nepal Judges – 2017
  - Over 650 Police officer trained by CID Cybercrime Unit

Global Position

- National Cyber Security Index – 77th
- Global Cybersecurity Index – 83rd
- ICT Development Index – 117th
- Networked Readiness Index – 78th

Development Level:
Developing Country

Area(s) of Relative Strength
Organizational, Technical Measures

Area(s) of Potential Growth
Capacity Development Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
58.65	13.05	14.15	14.82	6.58	10.04

Source: ITU Global Cybersecurity Index v4, 2020

Global Cybersecurity Index – Sri Lanka

National Cyber Security Index

GENERAL CYBER SECURITY INDICATORS		
1	Cyber security policy development	57%
1.1	Cyber security policy unit	
1.2	Cyber security policy coordination format	
1.3	Cyber security strategy	
1.4	Cyber security strategy implementation plan	
2	Cyber threat analysis and information	20%
2.1	Cyber threats analysis unit	
2.2	Public cyber threat reports are published annually	
2.3	Cyber safety and security website	
3	Education and professional development	100%
3.1	Cyber safety competencies in primary or secondary education	
3.2	Bachelor's level cyber security programme	
3.3	Master's level cyber security programme	
3.4	PhD level cyber security programme	
3.5	Cyber security professional association	
4	Contribution to global cyber security	50%
4.1	Convention on Cybercrime	
4.2	Representation in international cooperation formats	
4.3	International cyber security organization hosted by the country	
4.4	Cyber security capacity building for other countries	

BASELINE CYBER SECURITY INDICATORS		
5	Protection of digital services	0%
5.1	Cyber security responsibility for digital service providers	
5.2	Cyber security standard for the public sector	
5.3	Competent supervisory authority	
6	Protection of essential services	0%
6.1	Operators of essential services are identified	
6.2	Cyber security requirements for operators of essential services	
6.3	Competent supervisory authority	
6.4	Regular monitoring of security measures	
7	E-identification and trust services	11%
7.1	Unique persistent identifier	
7.2	Requirements for cryptosystems	
7.3	Electronic identification	
7.4	Electronic signature	
7.5	Timestamping	
7.6	Electronic registered delivery service	
7.7	Competent supervisory authority	
8	Protection of personal data	100%
8.1	Personal data protection legislation	
8.2	Personal data protection authority	

INCIDENT AND CRISIS MANAGEMENT INDICATORS		
9	Cyber incidents response	50%
9.1	Cyber incidents response unit	
9.2	Reporting responsibility	
9.3	Single point of contact for international coordination	
10	Cyber crisis management	20%
10.1	Cyber crisis management plan	
10.2	National-level cyber crisis management exercise	
10.3	Participation in international cyber crisis exercises	
10.4	Operational support of volunteers in cyber crises	
11	Fight against cybercrime	67%
11.1	Cybercrimes are criminalized	
11.2	Cybercrime unit	
11.3	Digital forensics unit	
11.4	24/7 contact point for international cybercrime	
12	Military cyber operations	83%
12.1	Cyber operations unit	
12.2	Cyber operations exercise	
12.3	Participation in international cyber exercises	

Ranked 77th (2021)*

*Multiple actions have been initiated for the improvement of some indicators since then

Dominican Republic

Legal framework

- 2003 Started drafting cybercrime bill *(BC framework)*
- 2004 Inserting provisions in the penal code *versus*

  special substantive and procedural law

Capacity building in practice: Dominican Republic

Legal framework

- 2003 Started drafting cybercrime bill *(BC framework)*
- 2004 Inserting provisions in the penal code *versus*

  special substantive and procedural law
- 2004 Draft cybercrime bill submitted to National Congress

Capacity building in practice: Dominican Republic

Legal framework

- 2003 Started drafting cybercrime bill *(BC framework)*
- 2004 Inserting provisions in the penal code *versus*

  special substantive and procedural law
- 2004 Draft cybercrime bill submitted to National Congress
- 2007 Law 53-07 against High-Tech Crime approved

Capacity building in practice: Dominican Republic

Legal framework

- 2003 Started drafting cybercrime bill *(BC framework)*
- 2004 Inserting provisions in the penal code *versus*

  special substantive and procedural law
- 2004 Draft cybercrime bill submitted to National Congress
- 2007 Law 53-07 against High-Tech Crime approved
- 2008 Requested and received invitation to accede Budapest Convention

Capacity building in practice: Dominican Republic

Legal framework

- 2003 Started drafting cybercrime bill *(BC framework)*
- 2004 Inserting provisions in the penal code *versus*

  special substantive and procedural law
- 2004 Draft cybercrime bill submitted to National Congress
- 2007 Law 53-07 against High-Tech Crime approved
- 2008 Requested and received invitation to accede Budapest Convention
- 2013 Budapest Convention ratification and entry into force

Legal framework

- 2018 First National Cybersecurity Strategy with a cybercrime complementary strategy

Capacity building in practice: Dominican Republic

Legal framework

- 2018 First National Cybersecurity Strategy with a cybercrime complementary strategy
- 2022 Proposed ammendment to cybercrime law

Legal framework

- 2018 First National Cybersecurity Strategy with a cybercrime complementary strategy
- 2022 Proposed ammendment to cybercrime law
- 2022 Draft data protection bill

Capacity building in practice: Dominican Republic

Legal framework

- 2018 First National Cybersecurity Strategy with a cybercrime complementary strategy
- 2022 Proposed ammendment to cybercrime law
- 2022 Draft data protection bill
- 2022 Draft cybersecurity bill

Legal framework

- 2018 First National Cybersecurity Strategy with a cybercrime complementary strategy
- 2022 Proposed ammendment to cybercrime law
- 2022 Draft data protection bill
- 2022 Draft cybersecurity bill
- 2022 Domestic process to sign BC 2nd. Additional Protocol ongoing

Capacity building in practice: Dominican Republic

Legal framework

- 2018 First National Cybersecurity Strategy with a cybercrime complementary strategy
- 2022 Proposed ammendment to cybercrime law
- 2022 Draft data protection bill
- 2022 Draft cybersecurity bill
- 2022 Domestic process to sign BC 2nd. Additional Protocol ongoing
- 2022 Second version of the National Cybersecurity Strategy **2030**

Specialised institutions

- 2003 DIDI - Cybercrime Investigation Division
  - National Department of Investigations
  - First case labeled as “cyber”
  - Why NDI?

Capacity building in practice: Dominican Republic

Specialised institutions

- 2003 DIDI - Cybercrime Investigation Division
  - National Department of Investigations
  - First case labeled as “cyber”
  - Why NDI?
- 2004 DICAT - High-Tech Crime Investigation Department
  - National Police

Specialised institutions

- 2003 DIDI - Cybercrime Investigation Division
  - National Department of Investigations
  - First case labeled as "cyber"
  - Why NDI?
- 2004 DICAT - High-Tech Crime Investigation Department
  - National Police
- 2013 PEDATEC – Specialized High-Tech Crime Prosecution Service
  - Attorney General's Office (Prosecution service)

MINISTERIO PÚBLICO

Capacity building in practice: Dominican Republic

Global Action on Cybercrime Extended **(GLACY+)**

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Implemented by the Council of Europe
Funded by the European Union and the Council of Europe
EUROPEAN UNION

Capacity building in practice: Dominican Republic

Capacity building in practice: Dominican Republic

Latin **A**merica and **C**aribbean
Cyber **C**apacities **C**entre (**LAC4**)

EU CyberNet

Funded by the European Union

Latin **A**merica and **C**aribbean **C**yber **C**apacities **C**entre (**LAC4**)

Purpose and functions

- LAC4 is a training and knowledge hub for *sharing* EU's *collective expertise and building up regional capacity and collaboration in* both *cybersecurity and cybercrime*
- Physical training facility located in Santo Domingo, Dominican Republic
- LAC4 is:
  - State-of-the-art hybrid training facility
  - Capacity to *develop and provide technical, policy and strategic level courses and simulation*
  - Platform for *doctrine development and research coordination*
  - Channel to cyber capacity building projects, training modules and materials developed in the EU
- LAC4 will operate in collaboration with the EU cyber capacity building projects and programmes, EU MSs, regional organizations, private sector, academia and civil society

Capacity building in practice: Dominican Republic

LAC4 hub countries concept

- LAC4 *sub-regional hubs* are countries that have the maturity and potential to serve as focal points for promoting cybersecurity and counter-cybercrime skills development and knowledge sharing across the region.
- The sub-regional hubs will help LAC4 to *identify the specific capacity building needs* and ensure a coherent and sustainable support by the EU, and also better coordination amongst all the different projects.
- Dominican Republic (Caribbean), Uruguay (Southern Cone), Ecuador (Andean Region), Costa Rica (Central America) & Brazil.

Other capacity building partners

CYBERCRIME

INTERPOL

Discussion and take-aways