African Union Commission – Council of Europe Joint Programme
Cyber Security and Cybercrime Policies for African Diplomats

Cybercrime legislation in Africa

Regional and International standards

Matteo Lucchetti

Project Manager at the Cybercrime Pogramme Office
of the Council of Europe (C-PROC) in Bucharest, Romania

matteo.lucchetti@coe.int

AUC HQ, Addis Ababa, 12 April 2018

Cybercrime as a criminal justice matter – Main Challenges

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

- Cybercrime legislation – Harmonization
  - Definition of cybercrimes
  - Where was Crime Committed? Which Country has jurisdiction?
  - Need to adopt global standards, International Treaties – UN Treaty – Status?

- Coping with new technological paradigms
  - Cloud Computing – “Evidence in the Cloud”
  - Darknet and virtual currencies
  - Internet of Things

- Dimension of the phenomenon not measurable due to unavailability of reliable statistics
  - 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

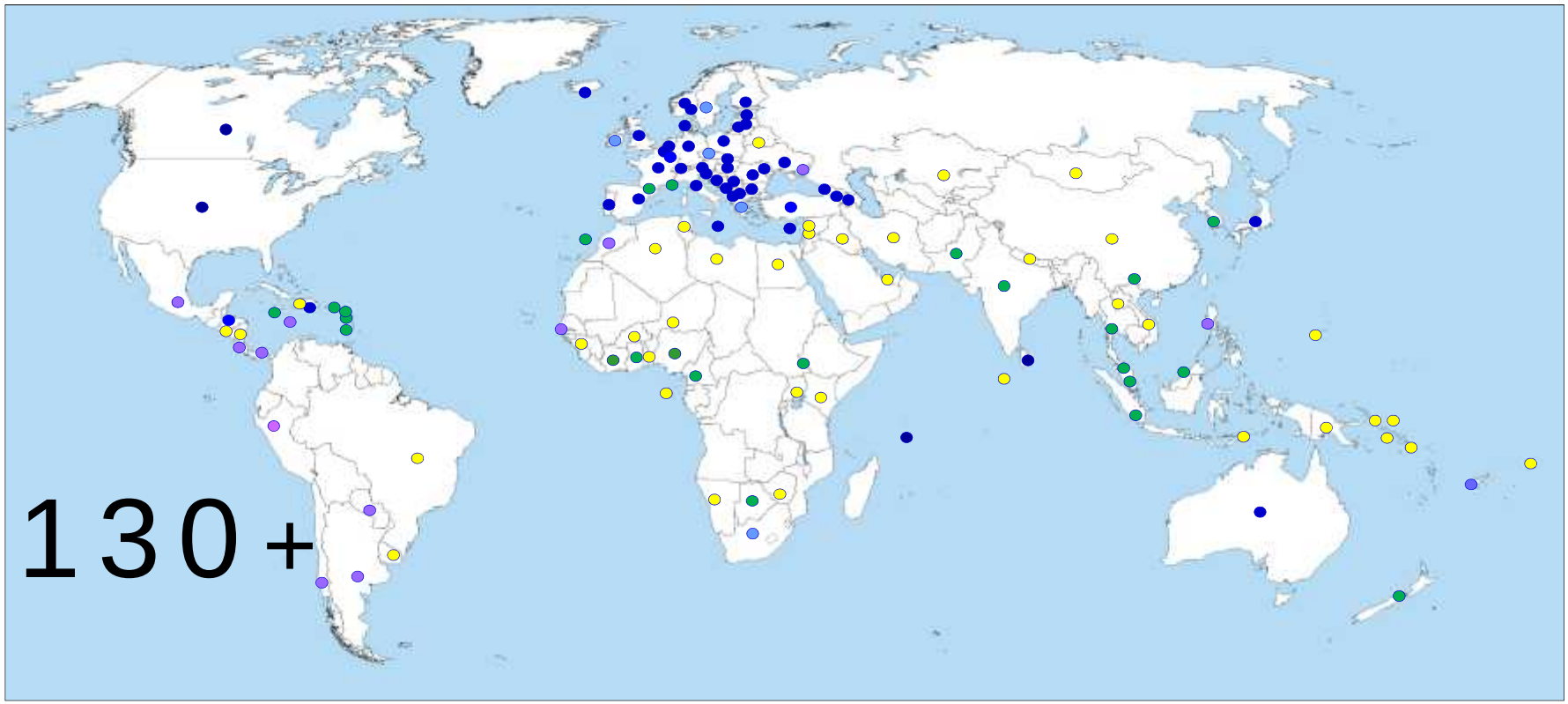
- Limited technical capabilities to support a successful investigation
  - Data/ mobile forensics laboratories outdated
  - Malware forensics and reverse engineering capacities
  - Collaboration with local telecommunication service providers

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

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
- It provides conditions and safeguards to meet the rule of law
- 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: 57

Signed: 4

Invited to accede: 10
= 71

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
- Production order
- 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
- Production order
- 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
- Production order
- 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 Malabo Convention and the Budapest Convention

Comparative analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime

(available upon request)

Scope

The AU Convention is broader than the Budapest Convention in that it covers:

- Chapter I – Electronic transactions
- Chapter II – Personal data protection
- Chapter III – Cyber security and cybercrime

The AU Convention unites different aspects related to information technology law, also including certain non-digital and non-criminal justice issues.

The Malabo Convention and the Budapest Convention

Cybercrime offences

- With regard to cybercrime and electronic evidence, the AU Convention criminalizes most of the conduct foreseen under the Budapest Convention.

Procedural powers

- The AU Convention provide for a sub-set of procedural powers that are also contained in the Budapest Convention and that are useful for investigating and prosecuting cybercrime and securing electronic evidence in domestic investigations.

International cooperation

- The AU Convention does not contain specific provisions and does not constitute a legal basis for international cooperation on cybercrime and electronic evidence.

The Malabo Convention and the Budapest Convention

Complementarity

- The AU Convention represents a political commitment by African States to take measures on a range of issues, including cybercrime.
- Those provisions that are available within the AU Convention are largely not in conflict with the Budapest Convention.
- Many high-level principles in the AU Convention appear to mandate the subsequent adoption of internationally recognized best practices and existing means of international cooperation.
- African States will need to cooperate with the authorities of countries in other regions of the world where electronic evidence is often stored or where service providers are located. Relevant States in this respect are already Parties to the Budapest Convention (e.g. US).
  Joining this treaty would offer a legal framework for African countries to engage in cooperation with these countries.

Cybercrime legislation in Africa
Substantive Provisions (as of March 2018)

The Budapest Convention as a reference model in Africa

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

The Cybercrime Convention Committee (T-CY)

Established under Article 46 Budapest Convention

Membership (October 2017):

- 57 Members (State Parties)
- 14 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 21 staff

- Task: 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

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 Extended

Funded by the European Union and the Council of 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	60 months (Mar 2016 – Feb 2021)
Budget	EUR 13.5 million
Funding	European Union (Instrument Contributing to Peace and Stability) and Council of Europe
GLACY+ Priority and Hub countries	• (Cape Verde) • Dom. Republic • Morocco • Senegal • (Costa Rica) • Ghana • (Nigeria) • Sri Lanka • (Chile) • Mauritius • Philippines • Tonga

GLACY+
Global Action on Cybercrime Extended

CYBERCRIME LEGISLATION, POLICIES AND STRATEGIES

- To promote consistent cybercrime legislation, policies and strategies as stand-alone and as part of broader cybersecurity

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.

Agreement AUC – COE for a collaboration in the area of cybercrime

Agreement for cooperation with the African Union Commission to jointly assist African Countries in the strengthening of:

- their domestic legislation on the basis of the "Budapest Convention on Cybercrime" and the "African Union Convention on Cyberspace Security and Protection of Personal Data - Malabo Convention";
- institutional capacities, training and international/regional cooperation;
- cybercrime policies and strategies.

Through:

- Participation of CoE in African Summits on topics related to cybercrime;
- Joint organisation of an awareness raising seminar on the Budapest Convention in Addis Ababa with the participation of Ambassadors to the African Union in view of building synergies between the Budapest Convention and the Malabo Convention;
- Joint organization of an "AFRICAN FORUM ON CYBERCRIME" within the framework of the GLACY+ Project in 2018 aimed at promoting a coherent approach to capacity building on cybercrime and electronic evidence in Africa.

The African Forum on Cybercrime
Addis Ababa, 16-18 October 2018

Agreement ECOWAS – COE for a collaboration in the area of cybercrime

- Agreement for cooperation with the ECOWAS Commission
  - Regional/International meeting on harmonisation of legislation on Cybercrime and EE, rule of law and human rights safeguards with participation of all ECOWAS Member States
  - Judicial training on cybercrime and electronic evidence for all ECOWAS countries
    - Francophone and Lusophone countries in Senegal, March 2017
    - Anglophone countries in Ghana, December 2017

GLACY+ Activities in the African Region

- East African Regional Conference on Cybercrime and Electronic Evidence, in collaboration with the GPEN and with the participation of regional and international organizations and countries from East Africa (Mauritius)
- Development of Cybercrime investigations, digital forensic capabilities and workshop on interagency cooperation and PPP (Mauritius)
- Workshop on data protection and INTERPOL Tools and Services and support on how to set-up and strengthen the 24/7 POC (Senegal)
- ECTEG Course, Cybercrime and digital forensics specialized training for law enforcement officers (Ghana)
- First responders Training of Trainers (Senegal)
- Advisory missions on cybercrime and cyber security policies and strategies (Ghana, Mauritius, Senegal)
- Judicial ToT on cybercrime and e-evidence (Ghana, Mauritius, Senegal)
- ToT for Judiciary Police (Morocco)

GLACY+ Activities in the African Region

- Meeting of the INTERPOL WG of the Heads of Cybercrime Unit of the African Region (Mauritius)
- Regional training for judges and prosecutors of the ECOWAS Region (Francophone and Lusophone in Senegal, Anglophone in Ghana)
- Advisory missions on legislation (Mauritius, Burkina Faso, Uganda)
- Support for the Technical Committee on Digital Rights and Freedom (Nigeria)
- Streamlining MLA procedures on cybercrime and electronic evidence (Mauritius, Senegal)
- In addition, several international events are organized/ supported, with participation of GLACY+ countries (e.g. ICANN Capacity Building WS for African LEAs, Nairobi, January 2017)

The Budapest Convention in the African Region

- Mauritius and Senegal are full parties to the Budapest Convention
  - Mauritius is also member of the T-CY Bureau
- Cape Verde, Ghana, Morocco, Nigeria have been invited to accede
  - Legislation fully in line with the provisions of the BC
- South Africa has signed the Convention, but has not ratified it
- Algeria, Tunisia, Morocco priority countries in the CyberSouth Project
- Support in the harmonization of national legislation on cybercrime has been provided to Kenya (Feb 2016, Bill currently in the Parliament), Burkina Faso (Feb 2018, Bill drafted) Uganda (Jan 2018, drfat Bill expected by end of 2018).
- Further advisory mission on cybercrime legislation have been planned in the Gambia (May 2018), Mauritania (June 2018)
- Support in the harmonization of the national legislation on cybercrime has been also requested by Guinea Bissau, Niger, Zambia

Cybercrime@Octopus Community

- Country Wiki
- Training Materials
- Cybercrime@CoE Update
- Cybercrime Digest

Cybercrime Digest

Bi-weekly update and global outlook by the
Cybercrime Programme Office of the Council of Europe (C-PROC)

16-31 May 2017

Source: Nuku'alofa Times

Date: 23 May 2017

The Pacific Response to Cybercrime: effective Tools and Good Practices

"Opening the Pacific Island Law Officer's Network Cybercrime Workshop at the Tanoa Dateline International Hotel this morning, Tonga's Deputy Prime Minister Hon Siaosi Sovaleni said that many of the Pacific Island States face a threefold challenge when it comes to dealing with cybercrime and electronic evidence: (a) putting in place a comprehensive legislative framework in line with international standards, (b) improving capacities and know-how within the criminal justice sector to effectively investigate, prosecute and adjudicate cases of cybercrime and other offences involving electronic evidence, and (c) engage in efficient international cooperation. He said the conference is a great opportunity for countries to work together on finding solutions as no country can face the cybercrime challenges alone." Senior officials from 13 Pacific island countries participated in the event, organized by PILON and supported by Council of Europe. READ MORE

RELATED ARTICLES

Tonga Ministry of Information & Communication, Pacific Islands Law Officers' Network cybercrime Workshop 23 – 25 May 2017, Nuku'alofa, Kingdom of Tonga, 24 May 2017

Source: Europol

Date: 18 May 2017

27 arrested in successful hit against ATM black box attacks in Europe

"The efforts of a number of EU Member States and Norway, supported by Europol's European Cybercrime Centre (EC3) and the Joint Cybercrime Action Taskforce (J-CAT), culminated in the arrest of 27 individuals linked with so-called ATM "Black Box" attacks across Europe. Perpetrators responsible for this new and sophisticated method of ATM jackpotting were identified in a number of countries over different periods of time in 2016 and 2017. There were arrests in Czech Republic (3), Estonia (4), France (11), the Netherlands (2), Romania (2), Spain (2) and Norway (3)." READ MORE

RELATED ARTICLES

EAST, ATM Black Box Attacks spread across Europe, 11 Apr 2017

Source: A.M. Costa Rica

Date: 22 May 2017

Legislators approve the Convention on Cybercrime in Costa Rica

"The Costa Rican legislature gave the second approval towards ratifying the Budapest Convention, according to a statement made by the science and technology ministry Friday afternoon. […] The Ministerio de Ciencia, Tecnología y Telecomunicaciones praised the legislative approval of the ratification. The ministry said that this would allow authorities to receive access to procedures, tests and collaborative initiatives around the world to detect cybercriminals. […] Costa Rica places seventh in the number of cyber attacks registered in Latin America, the ministry said." READ MORE

- Join today https://www.coe.int/en/web/octopus/home

African Union Commission – Council of Europe Joint Programme
Cyber Security and Cybercrime Policies for African Diplomats

Thank you

Matteo Lucchetti

Project Manager at the Cybercrime Pogramme Office
of the Council of Europe (C-PROC) in Bucharest, Romania

matteo.lucchetti@coe.int

AUC HQ, Addis Ababa, 12 April 2018

African Union Commission – Council of Europe Joint Programme
Cyber Security and Cybercrime Policies for African Diplomats

Back-up

Matteo Lucchetti

Project Manager at the Cybercrime Pogramme Office
of the Council of Europe (C-PROC) in Bucharest, Romania

matteo.lucchetti@coe.int

AUC HQ, Addis Ababa, 12 April 2018

The accession process

1. Expression of interest
2. Analysis of the legislation and of the context
3. Advisory mission on cybercrime legislation
4. Legislation in line with the provisions of the Budapest Convention
5. Request to join the BC, formalized by the Government and sent to the Council of Europe
6. Analysis of the request from the Treaty Office and decision from the Cybercrime Convention Committee
7. Invitation for the Country to join the BC
8. Ratification and instruments of accession deposited in Strasbourg

GLACY+ Objective 1
Capacities of police authorities

Obj 1	To promote consistent cybercrime policies and strategies.
Result 1.1	Cybercrime policies and strategies as part of national cybersecurity frameworks strengthened in at least 16 countries (priority and a number of other countries) and experience shared with other countries.
Result 1.2	Policy dialogue and cooperation on cybercrime enhanced between international and regional organisations.

GLACY+ Objective 2
Capacities of police authorities

Obj 2	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.
Result 2.1	Assessments/cyber reviews (initial and final) of law enforcement capacities available for priority countries.
Result 2.2	Cybercrime and computer forensics units strengthened in priority countries and experience shared with other countries.
Result 2.3	Law enforcement training strategies available in priority countries, including access to ECTEG training materials.
Result 2.4	At least 500 LE officers trained in basic cybercrime investigations and computer forensics as well as related rule of law requirements.
Result 2.5	International police-to-police cooperation on cybercrime and electronic evidence is more effective.

GLACY+ Objective 3
Capacities of police authorities

Obj 3	To enable criminal justice authorities to apply legislation and prosecute and adjudicate cases of cybercrime and electronic evidence and engage in international cooperation.
Res 3.1	Assessments of criminal justice capabilities available for pri. countries
Res 3.2	Legislation on cybercrime and electronic evidence strengthened in line with the Budapest Convention and rule of law and human rights standards in priority countries and reforms have been initiated in additional countries.
Res 3.3	Judicial training academies in at least ten countries are providing training on cybercrime and electronic evidence as part of their regular curricula and experience has been shared with other countries.
Res 3.4	Institutions strengthened and procedures improved for international judicial cooperation related to cybercrime and electronic evidence in at least 10 countries and experience shared with other countries.

GLACY+
Good practices to share

- Capacity building backed up by common standards (example: Budapest Convention) and follow up mechanism (example: Cybercrime Convention Committee of the Parties)
- Political commitment to implement standards (Example: signature or formal request for accession to Budapest Convention) as a prerequisite for full range of support
- Rule of law conditions: strengthening legislation, including safeguards for procedural powers, as starting point
- Sequencing of activities: Initial situation reports ▶ committing decision makers and counterpart organisations ▶ implementing activities ▶ assessing progress made ▶ feeding results back into policies
- Country project teams ▶ Example GLACY+: cooperation with 8 x 5 institutions
- Capacities for capacity building ▶ C-PROC

African Union Commission – Council of Europe Joint Programme
Cyber Security and Cybercrime Policies for African Diplomats

Cybercrime and cyber security strategies

Matteo Lucchetti

Project Manager at the Cybercrime Pogramme Office
of the Council of Europe (C-PROC) in Bucharest, Romania

matteo.lucchetti@coe.int

AUC HQ, Addis Ababa, 12 April 2018

The EU Cybersecurity strategy

- Member States will have to put in place a minimum level of national capabilities by
  - establishing NIS national competent authorities,
  - setting up well-functioning Computer Emergency Response Teams (CERTs), and
  - adopting national NIS strategies and national NIS cooperation plans;

- NIS national competent authorities will have to exchange information and to cooperate so as to counter NIS threats and incidents

The EU Cybersecurity strategy

- Operators of critical infrastructure (such as energy, transport, banking, stock exchange, healthcare),
- key Internet enablers (e-commerce platforms, social networks, etc) and
- public administrations

will be required to assess the risks they face and to adopt appropriate and proportionate measures to ensure NIS.

These entities will also be required to report to competent authorities incidents with a significant impact on core services provided.

The NIS Directive

- The aim of the proposed Directive is to ensure a high common level of network and information security (NIS) across the EU. Ensuring NIS is vital to boost trust and to the smooth functioning of the EU internal market. Regulatory obligations are required to create a level playing field and close existing legislative loopholes.

The Directive on security of network and information systems (the NIS Directive) was adopted by the European Parliament on 6 July 2016.

The Directive entered into force in August 2016.

Member States will have 21 months to transpose the Directive into their national laws and 6 months more to identify operators of essential services.

The NIS Directive

New National Strategy

- Define a Competent Authority, Set up a National CERT (Computer Emergency Response Team)

Co-operation network

- Exchange of information between authorities, early warnings on information security, co-ordinated response

Security Requirements

- Appropriate technical and organizational measures to manage security risks
- Incident notification to competent authorities, if significant impact on continuity of the service – Limited to critical infrastructure operators. If personal data are involved → Notification to DPA and affected individuals

Use of Standards

- Commission has responsibility to draw NIS standards

Enforcement

- The competent authorities in each member state are to be given powers to investigate cases of non-compliance of public bodies and market operators with the NIS Directive, which may include undergoing a security audit

Quick Facts on GDPR

The GDPR in a Nutshell (What It Does and Why It Matters)

- GDPR mandates that rights are to be respected by all organizations located in the EU and operating in the EU market. This includes all companies that sell goods or services, or process and store the personal data of EU citizens.
- GDPR requires companies to provide users the right to erase their data, object to processing, etc.
- Companies are required to disclose the purpose for which data is going to be used, for how long, and whether it may be transferred to a third party, etc.
- The EU requires all entities involved in data storage or processing to adhere to a "privacy by design" concept and maintain data processing records.
- **Breach reporting**—breaches affecting EU users should be reported within 72 hours to EU authorities and customers.
- Fines are serious—from €10-20 million or 4% of a company's global turnover in the previous year, whichever is more. If GDPR had been in full force by the time of the announcement, Equifax would have paid a jaw-dropping $68.5 million in fines.

African Union Commission – Council of Europe Joint Programme
Cyber Security and Cybercrime Policies for African Diplomats

Thank You

Matteo Lucchetti

Project Manager at the Cybercrime Pogramme Office
of the Council of Europe (C-PROC) in Bucharest, Romania

matteo.lucchetti@coe.int

AUC HQ, Addis Ababa, 12 April 2018

Offences against the confidentiality, integrity and availability of computer data and systems (1/2)

- Illegal Access (Art. 2)
  - To access to the whole or any part of a computer system without right
  - Intentionally
- Illegal Interception (Art. 3)
  - Intentionally, and without right
  - To intercept, by technical means, non-public transmissions of computer data
  - To, from or within a computer system
- Data Interference (Art. 4)
  - Damaging, deletion, deterioration, alteration or suppression of computer data
  - Intentionally, without right

Offences against the confidentiality, integrity and availability of computer data and systems (2/2)

- System Interference (Art. 5)
  - The serious hindering of the functioning of a computer system
  - By inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data
  - Intentionally, without right

- Misuse of devices (Art. 6)
  - Intentionally, withuot right
  - To produce, sale, procure for use, import, distribute or otherwise make available
    - A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2 – 5;
    - a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offences established in Articles 2 – 5
  - To possess an item referred to in paragraphs (a)(1) or (2) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 – 5.

Computer-Related Offences

- Computer-related Forgery (Art. 7)
  - Input, alteration deletion, or suppression of computer data, resulting in inauthentic data
  - With the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible
  - Intentionally, without right

- Computer-related fraud (Art. 8)
  - Intentionally, withuot right
  - The causing of a loss of property to another by:
    - (a) any input, alteration, deletion or suppression of computer data,
    - (b) any interference with the functioning of a computer or system,

    with the intent of procuring, without right, an economic benefit for oneself or for another

Content-Related Offences

- Child Pornography (Art. 9)
  - Intentionally, without right
    - (a) producing child pornography for the purpose of its distribution through a computer system;
    - (b) offering or making available child pornography through a computer system;
    - (c) distributing or transmitting child pornography through a computer system;
    - (d) procuring child pornography through a computer system for oneself or for another;
    - (e) possessing child pornography in a computer system or on a computer-data storage medium.
  - Includes pornographic material that visually depicts
    - (a) a minor engaged in sexually explicit conduct;
    - (b) a person appearing to be a minor engaged in sexually explicit conduct;
    - (c) realistic images representing a minor engaged in sexually explicit conduct.
  - “minor” shall include all persons under 18 years of age

Content-Related Offences

- Intellectual Property Rights – IPR (Art. 10)
  - Doesn't create a new regulation on the subject, purpose is to apply previous rules on copyright, extending relevant provisions to the on-line reality
  - Infringements infringements of copyright on-line, or committed by the means of a computer system, must be punished as if it was committed in the real world
  - References to existing international treaties
    - Paris Agreement (24 July 1971)
    - Bern Convention
    - WIPO Treaties

- Ancillary liability and sanctions
  - Aiding and abetting (Art. 11)
  - Criminal responsibility of legal entities (Art.12)

Procedural powers – Art. 16

- Expedited preservation of stored computer data (Art. 16)
  - To enable competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.
    - May be exercised through judicial order, administrative order, directive, search & seizure, production order. It's not a general data retention obligation
    - Manner of preservation may be determined by the Party
  - To oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.
  - To oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.
    - Suspects not to become aware of the ongoing investigation, Protection of privacy, Prevents tampering/ deleting by other persons

Procedural powers – Art. 17

- Expedited Preservation and Partial Disclosure of Traffic Data (Art. 17)
- in respect of traffic data that is to be preserved under Article 16
  - Available regardless of whether one or more service providers were involved in the transmission
    - Multiple service providers usually involved in transmissions of communications. Traffic data often shared between service providers for commercial, security or technical purposes
  - Disclosure of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted
    - Purpose to enable identification of source and destination of communication

Procedural powers – Art. 18

- Production Order (Art. 18)
- To empower law enforcement authorities to order:

  a) a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

  b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

- Order to provide
  - data stored in a computer system under their responsibilities
  - subscriber information
- The production order must specify the nature and extent of the required data
  - the data required by the investigation must be previously determined

Procedural powers – Art. 18

- Production Order (Art. 18) – cont'd
  - Person must be physically present in territory. Data does not need to physically be present in territory
  - Individul cases, concerning specific persons, e.g.
    - Allowed: production of email address associated with a particular name
    - Not allowed: production of ALL email communications during last three years associated with a particular name
  - Physical possession of data concerned; OR Free control over production of data concerned ("constructive possession") whether or not within territory
  - Does not impose obligation to retain data. However retention necessary for power to be effective
  - Offering services in the territory
  - Subscriber information most frequently required in criminal investigations

Procedural powers – Art. 19

- Search and seizure of Stored Computer Data (Art. 19)
  - To empower its competent authorities to search or similarly access:
    - a computer system or part of it and computer data stored therein; and
    - a computer-data storage medium in which computer data may be stored in its territory
  - Grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system → the authorities shall be able to expeditiously extend the search or similar accessing to the other system.
  - Power to: seize or similarly secure a computer system or part of it or a computer-data storage medium; make and retain a copy of those computer data; maintain the integrity of the relevant stored computer data; render inaccessible or remove those computer data in the accessed computer system.
  - To empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred
    - Sys Admin, legal basis for cooperation for legitimate businesses

Procedural powers – Art. 20

- Real-time Collection of Traffic Data (Art. 20)
  - To empower its competent authorities to:

    a) collect or record through the application of technical means on the territory of that Party, and

    b) compel a service provider, within its existing technical capability:

       a) to collect or record through the application of technical means on the territory of that Party; or

       b) to co-operate and assist the competent authorities in the collection or recording of,

    traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

    - Only applies to extent of technical capability of service provider, whether such technical features are ordinarily used or not, Does not impose obligation on service providers to:
      - Develop new equipment
      - Hire expert support
      - Engage in costly re-configuration of systems
  - To oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

Procedural powers – Art. 21

- Interception of Content Data (Art. 20)
  - To empower its competent authorities to:

    a) collect or record through the application of technical means on the territory of that Party, and

    b) compel a service provider, within its existing technical capability:

       a) to collect or record through the application of technical means on the territory of that Party; or

       b) to co-operate and assist the competent authorities in the collection or recording of,

    content data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

    - General or indiscriminate surveillance or collection of large amounts of content data not permitted
    - Only applies to extent of technical capability of service provider, whether such technical features are ordinarily used or not, Does not impose obligation on service providers to:
      - Develop new equipment, Hire expert support, Engage in costly re-configuration of systems
  - To oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

International cooperation – Art. 26

- Spontaneous Information (Art. 26)
  - The authorities from a Party, within an internal investigation, discover that some of the information they obtained must be forwarded to the authorities of other Party
  - It can be done if the information seems to be useful or necessary to the beginning or the developing of an investigation respecting to a criminal offence in the framework of the Convention
  - According to Article 26, 2, this dispatch of information can be submitted to certain conditions, mainly of confidentiality
    - Purpose to protect identity of a means of collecting information, confidentiality of ongoing onvestigation

International cooperation – Art. 29

- Expedited Preservation (Art. 29)
  - Expedited preservation of data stored in a computer system
  - Parallel framework to the internal provision, it allows one contracting Party to require from other Party the expedited preservation of data, if at the same time expresses its intention of sending a formal request of assistance for a search, or a seizure, or any similar measure
  - The requested party must act as necessary, with all the due diligence, to preserve the requested data, according to its own national law
  - Dual criminality cannot be required by the requested party, as a condition of preservation of the data (except offenses other than Art 2-11 or political, sovereignty, security, public order, or other essential interests)
  - Only a preservation measure for urgent reasons and does not imply automatically disclosure of the preserved data (non-intrusive)

International cooperation – Art. 30

- Expedited Disclosure of Preserved Traffic Data (Art. 30)
  - International equivalent of domestic power established under Article 17
  - Where pursuant to Article 29 request, requested state observes that preserved traffic data reveals that transmission of the communication was routed through a service provider in (i) a third state; or (ii) the requesting state itself, it must expeditiously disclose such preserved traffic data
  - Disclosure must be of sufficient amount of data to identify service provider(s) involved and path of communication
  - Same grounds for refusal as before:
    - Request in relation to political offence or offence connected to political offence
    - Execution of request will prejudice sovereignty, security, ordre public or other essential inte

International cooperation – Art. 31

- Mutual assistance regarding accessing of stored computer data (Art. 31)
  - Request to another State to search [or similarly access] or seize [or similarly secure] and disclose data stored by means of a computer system
    - Located within the territory of the requested State
    - Including data that has been preserved pursuant to Article 29
  - The request shall be responded to on an expedited basis where:
    - there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or
    - the instruments, arrangements and laws in place otherwise provide for expedited co-operation.

International cooperation – Art. 32

- Transborder Access to Stored Computer Data with Consent or Where Publicly Available (Art. 32)
  - Possibility given to law enforcement from a Party to obtain evidence stored in a computer physically located in other Party's territory
  - Without any request of international cooperation if, during a concrete investigation, the officers in charge

    a) need to obtain open source information from a computer located in a foreign country ;

    or

    b) access data with the lawful and voluntary consent of the lawfully authorised person
  - Does not require mutual assistance between Parties. Does not require notification to the other party. Does not exclude notification if Party deems it appropriate
  - Article 32b
    - Explicit consent usually required
    - Person who has the lawful authority to disclose the data depends on circumstances, laws and regulations

International cooperation Art. 33/ 34

- Mutual Assistance Regarding Real Time Collection of Traffic Data (Art. 33)
  - Key traffic data often deleted automatically by service providers before it can be preserved; thus real-time power required
  - Enables a Party to request another Party to exercise its domestic power equivalent to Article 20
  - States may limit the range of offences for which mutual assistance may be provided under this article. Range of offences covered cannot be more narrow than range of offences available in equivalent domestic case

- Mutual assistance regarding the interception of content data (Art. 34)
  - Mutual assistance in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.
  - International equivalent of domestic procedural power under Article 21

24/7 Network – Art. 35

- 24/7 Network (Art. 35)
  - Obligation to create a permanently available contact point
    - a so called 24/7 network of contact points
  - General objectives of these contact points to facilitate international co-operation
    - giving technical advisory to other contact points
    - activating the proper mechanism to expedited preservation of data
    - urgently collecting evidence
    - identifying and discovering suspects
  - Operational network of experts on high-tech criminality to provide quick help and cooperation even if a formal cooperation request must follow this informal way
  - One single point of contact for each country, available 24 hours a day, 7 days a week, Direct communications between the points
  - Mainly planned to provide the possibility to immediately preserve traffic data and other stored data worldwide

African Union Commission – Council of Europe Joint Programme
Cyber Security and Cybercrime Policies for African Diplomats

Investigation challenges and the electronic evidence in the cloud

Matteo Lucchetti

Project Manager at the Cybercrime Pogramme Office
of the Council of Europe (C-PROC) in Bucharest, Romania

matteo.lucchetti@coe.int

AUC HQ, Addis Ababa, 12 April 2018

Electronic Evidence in the cloud

- Budapest Convention: Criminal Justice International Treaty
- Cybercrime AND electronic evidence
- Electronic evidence in the cloud → on servers in foreign, unknown, multiple or shifting jurisdictions
- No data → no evidence → no prosecution → no justice → no rule of law
- Less than 1% of cybercrime reported eventually adjudicated → How to promote rule of law in cyberspace? Are governments meeting obligation to protect?
  (see for example K.U. vs Finland - http://humanrightshouse.org/Articles/11059.html)
- Issues, solutions and recommendations proposed by the T-CY Cloud Evidence Group

T-CY Cloud Evidence Group

How to ensure the rule of law in cyberspace through more efficient access to electronic evidence for criminal justice purposes?

- Assessment of mutual legal assistance provisions → 24 recommendations to make MLA more efficient (Dec 2014)
- Transborder access to data (T-CY Transborder Group 2012-2014)
  - Clarification of Article 32b Budapest Convention → Guidance Note (Dec 2014)
  - Additional options for transborder access → necessary but politically not feasible in 2014. (Risk of increasing unilateral action)
- T-CY Cloud Evidence Group (2015-2016): Proposals submitted to Cybercrime Convention Committee in November 2016

CEG – Issues identified

1. Differentiating subscriber versus traffic versus content data
2. Effectiveness of MLA
3. Loss of location and transborder access jungle
4. Provider present or offering a service in the territory of a Party
5. Voluntary disclosure by private sector entities (US-based providers)
6. Emergency procedures
7. Data protection

I.1. Subscriber vs traffic vs content data

- Subscriber information most often required in criminal investigations
- Less privacy-sensitive than traffic or content data
- Rules for access to subscriber information not harmonised
- Subscriber information held by service providers and obtained through production orders → Lesser interference in rights than search and seizure

I.2. Mutual legal assistance

- Mutual legal assistance remains a primary means to obtain electronic evidence for criminal justice purposes
- MLA needs to be made more efficient
- Often subscriber information or traffic data needed first to substantiate or address an MLA request
- MLA often not feasible to secure volatile evidence in unknown or multiple jurisdictions

I.3. Loss of location (1/2)

- In “loss of location” situations (unknown source of attack, servers in multiple or changing locations, live forensics, etc.) MLA not feasible → principle of territoriality not always applicable
- Direct transborder access to data may be necessary. What conditions and safeguards?
- Article 32b Budapest Convention limited → Absence of international legal framework for lawful transborder access
- Unilateral solutions by governments / jungle → risks to rights of individuals and state to state relations

I.3. Loss of location (2/2)

- T-CY Guidance Note on Transborder Access to Data (Article 32), December 2014
  - Regarding Article 32b, typical situations may include:

    "A suspected drug trafficker is lawfully arrested while his/her mailbox - possibly with evidence of a crime - is open on his/her tablet, smartphone or other device. If the suspect voluntarily consents that the police access the account and if the police are sure that the data of the mailbox is located in another Party, police may access the data under Article 32b."

- Long-arm doctrine of EU anti-trust law (Cases ICI 48/69; Woodpulp 89/85)
  - the European Commission recommends that competition authorities within the European Union obtain access to servers anywhere in the world to gather evidence in anti-trust proceedings:

    "To have effective powers to gather digital evidence, it is important that the Authorities can in the exercise of their inspection powers gather digital information which is accessible to the undertaking or person whose premises are being inspected irrespective of where it is stored, including on servers or other storage media located outside the territory of the respective national competition authority or outside the European Union."

    Source: European Competition Network "Recommendation on the power to collect digital evidence, including by forensic means" http://ec.europa.eu/competition/ecn/ecn_recommendation_09122013_digital_evidence_en.pdf

I.4. Service provider offering a service in the territory of a State Party

- When is a service provider
  - "present" in the territory of a State?
  - "offering a service" in the territory of a State?
- Therefore, when is a service provider subject to a domestic production or other type of coercive order?
- If domestic production orders for subscriber information → reduction of pressure on MLA system

I.5. “Voluntary” disclosure by private sector entities

- More than 100,000 requests/year by European States to major US providers. Mostly related to disclosure of subscriber or traffic data (ca. 60%)
- Providers decide whether or not to respond to lawful requests and whether to notify customers
  - Provider policies/practices volatile
- Data protection concerns
- No disclosure by European providers
- No admissibility of data received in some States
- Clearer / more stable framework required

I.5. “Voluntary” disclosure by private sector entities

	Requests for data sent to Apple, Facebook, Google, Microsoft, Twitter and Yahoo in 2015		
Parties	Received	Disclosure	%
Austria	254	119	47%
Belgium	1 992	1 453	73%
Canada	1 157	884	76%
France	27 213	14 746	54%
Germany	29 092	15 469	53%
Italy	7 847	3 591	46%
Netherlands	1 605	1 213	76%
Poland	2 378	820	34%
Portugal	3 255	1 751	54%
Spain	4 151	2 092	50%
United Kingdom	29 937	21 075	70%
USA	89 350	70 116	78%
Total excluding USA	138 612	82 529	60%
Total including USA	227 962	152 644	67%

I.6. Emergency procedures

- Emergency procedures needed to obtain evidence located in foreign jurisdictions through
- Mutual legal assistance
- Direct cooperation with a service provider

I.7. Data protection and other safeguards

- Data protection requirements normally met if powers to obtain data are defined in domestic criminal procedure law and/or MLA agreements
- MLA not always feasible
- Increasing “asymmetric” disclosure of data trans-border
- From LEA to service provider → Permitted with conditions
- From service provider to LEA → Unclear legal basis → providers to assess lawfulness, legitimate interest → risk of being held liable + Confidentiality requirements
- Clearer framework for public to private to public disclosure trans-border required

CEG – Solutions identified

Five options to be pursued in parallel:

1. More efficient MLA

2. Guidance Note on Article 18

3. Domestic rules on production orders (Article 18)

4. Cooperation with providers: practical measures

5. Protocol to Budapest Convention

S.1. More efficient MLA

- Implement legal and practical measures → Recommendations 1 – 15 of T-CY assessment report on MLA at domestic levels
  - More resources and training
  - Electronic transmission of requests
  - Streamlining of procedures
  - Etc.
- Parties to establish emergency procedures for obtaining data in their MLA systems
- Parties to facilitate access to subscriber information in domestic legislation (full implementation of Article 18 Budapest Convention)

S.2. Guidance Note on Article 18

- Guidance Note on Article 18 Budapest Convention on production of subscriber information:
  - Domestic production orders if a provider is in the territory of a Party even if data is stored in another jurisdiction (Article 18.1.a)
  - Domestic production orders for subscriber information if a provider is NOT necessarily in the territory of a Party but is offering a service in the territory of the Party (Article 18.1.b)

S.3. Domestic rules for production orders

- Proper implementation of Article 18 at domestic levels
- Lighter regime for production of subscriber information (as compared to traffic and content data)
- Use of information obtained as evidence in criminal proceedings

S.4. Cooperation with providers

Pending longer-term solutions:

- Practical measures to facilitate trans-border cooperation between service providers and criminal justice authorities
- Focus on disclosure of subscriber information upon lawful requests in specific criminal investigations
- Emergency situations
- Consideration of legitimate interests and data protection requirements

S.5. Protocol to the Budapest Convention (1/2)

A. Provisions for more efficient MLA

- International production orders
- Simplified MLA for subscriber information
- Direct cooperation between judicial authorities in MLA
- Joint investigations and joint investigation teams
- Requests in English. Audio-video hearings.
- Emergency procedures

B. Direct cooperation with providers in other jurisdictions

- Disclosure of data by LEA to a service provider abroad in specific situations
- Disclosure of subscriber information by service providers to LEA abroad with conditions and safeguards
- Direct preservation requests to providers abroad
- Admissibility of data obtained directly in domestic proceedings
- Emergency procedures

S.5. Protocol to the Budapest Convention (2/2)

C. Framework and safeguards for existing practices of trans-border access to data

- Transborder access to data with lawfully obtained credentials
- Transborder access in good faith or in exigent circumstances
- The power of disposal as connecting legal factor

D. Data protection

- Requirements for transfer transborder by LEA to a service provider abroad
- Requirements for transfer transborder by a service provider to LEA abroad

- The Protocol Drafting Group was kicked-off in September 2017
- The negotiations are expected to be concluded by end of 2019

African Union Commission – Council of Europe Joint Programme
Cyber Security and Cybercrime Policies for African Diplomats

Thank You

Matteo Lucchetti

Project Manager at the Cybercrime Pogramme Office
of the Council of Europe (C-PROC) in Bucharest, Romania

matteo.lucchetti@coe.int

AUC HQ, Addis Ababa, 12 April 2018