Version 15/10/2018

AFRICAN FORUM ON CYBERCRIME

Policies and Legislation, International Cooperation and Capacity Building

Conference Programme

Addis Ababa, 16-18 October 2018

Organized and funded by:

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

UNODC

United Nations Office on Drugs and Crime

INTERPOL

The Commonwealth

INTERNATIONAL NARCOTICS & LAW ENFORCEMENT

JUSTICE & SECURITY

UNITED STATES DEPARTMENT OF STATE

DEPARTMENT OF JUSTICE

QUI PRO DOMINA JUSTITIA SEQUITUR

Foreign &
Commonwealth
Office

Home Office

OUTLINE

1. Background

The continuous development of information and communication technologies towards more sophisticated services and applications goes hand in hand with the rise of crimes committed against or through the use of computer systems.

According to recent statistics, the African continent is exhibiting one of the fastest growth rates in Internet penetration worldwide, with digital connectivity that has almost tripled in the last five years. In the same period, both governments and private sector entities in Africa have been experiencing an equally increasing trend of cyber-attacks, in line with what has been recorded also on the global level.

The large-scale theft of personal data, computer intrusions, bullying, harassment and other forms of cyber violence, or sexual violence against children online, are attacks against human rights. Hate speech, xenophobia and racism may contribute to radicalisation leading to violent extremism. Attacks against computers and disinformation used in elections and election campaigns are attacks against the functioning of fundamental institutions and political stability. Daily attacks against critical information infrastructure affect national security and economic and other national interests as well as international peace and stability.

Moreover, evidence in relation to fraud, corruption, murder, rape, terrorism, the sexual abuse of children and, in fact, any type of crime may take the form of electronic evidence, which is volatile, often intangible and many times located in foreign jurisdictions. Accessing such evidence also has implications for human rights and the rule of law. Effective, legally compliant and robust procedures for the identification, collection and preservation of electronic evidence are therefore essential.

The diversity, prevalence and wide ranging impact, as well as the cross-border nature of such threats make it a high level priority for each State to focus on how to develop policies and legislations that allow for efficient and effective international cooperation, both in the prevention and fight against criminal acts committed through the Internet. At the same time, a balance must be struck between the fundamental rights of the individuals and the principles of necessity and proportionality governing the procedures put in place by criminal justice authorities.

In such a context, criminal justice authorities can fulfil their roles effectively only if they are equipped with the skills and knowledge to apply it. Given the scale of this challenge and the scarcity of resources, international organisations need to join forces and develop synergies to support countries in a consistent and effective manner, through effective capacity building initiatives.

As a joint organizational effort of African countries, regional and international organizations, the **First African Forum on Cybercrime** will focus on three major thematic streams:

- **Cybercrime policies and national legislations**, with respect to regional and international standards and relevant implementation practices;

- **International cooperation** to fight against cybercrime and proper handling cross-border of electronic evidence;

- Strengthening criminal justice authorities through adequate plans of **capacity building** and synergies with related programmes implemented in Africa.

2. SUPPORTING ORGANISATIONS/INSTITUTIONS

The African Forum on Cybercrime is organized by the **African Union Commission** and supported by a number of partnering organizations:

- **The Council of Europe;**
- **The European Union;**
- **INTERPOL;**
- **UNODC;**
- **US DOJ/State Department;**
- **UK Government;**
- **The Commonwealth Secretariat.**

A number of regional organizations have also been invited to participate in the Forum, including: the Economic Community of Central African States (**ECCAS**); the Common Market for Eastern and Southern Africa (**COMESA**); the Intergovernmental Authority for Development (**IGAD**); the Southern African Development Community (**SADC**); the New Partnership For Africa's Development (**NEPAD**); the Economic Community Of West African States (**ECOWAS**); the East African Economic Commission (**EAC**); the Union Maghreb Arab (**UMA**); the African Union Mechanism for Police Cooperation (**AFRIPOL**) and the African Centre for the Study & Research on Terrorism (**ACSRT**).

3. Expected outcomes

Representatives of participating countries will be able to discuss the current situation and share best practices with regional and international organizations, thus creating a network of professionals that will allow them:

- To improve the effectiveness of their daily endeavours through the exchange of information regarding common challenges and tasks;

- To strengthen their capacities to face new challenges in criminal law investigations that have a cybercrime component and evaluation of electronic evidence;

- To promote and improve regional cooperation protocols between internet service providers and criminal investigators;

- To strengthen regional mechanisms on criminal justice matters.

It is expected that by the end of the Forum:

- Representatives of participating countries will be in a better position to benefit from the support available from different international organisations for the strengthening of their criminal justice capacities on cybercrime and electronic evidence.

- International organisations will have strengthened their cooperation and synergies in view of future support to countries of the region. The Forum itself is expected to set an example of such cooperation.

4. Participants

Governments of all African countries are invited to nominate up to five officials that are involved in matters related to cybercrime and electronic evidence.

Recommended participants should include representatives from criminal justice authorities, law enforcement, prosecution services, judiciary, representatives of relevant ministries, legislators, policy makers or other entities deemed relevant for the event.

The invitation will be extended to the diplomatic community of the Embassies to the African Union Commission in Addis Ababa.

Private sector organisations are also participating.

5. Location

The Forum will take place at the African Union Commission premises in Addis Ababa, Ethiopia, and will last for 3 days: **16 – 18 October 2018**.

6. Languages

The languages of the event will be **English** and **French**.
Simultaneous interpretation will be provided.

7. Structure of the event and agenda

The event will be organized with a Plenary in the first morning with all participants, which will then split into parallel workshops organized under the three streams of the Forum:

- ► **POLICIES AND LEGISLATION (Room 1)**
- ► **INTERNATIONAL COOPERATION (Room 2)**
- ► **CAPACITY BUILDING (Room 3)**

Each workshop is expected to be chaired/ facilitated by one of the partnering organizations. Rapporteurs will present a brief outcome of the workshops in the Plenary of the last day, which will take place before the closing ceremony.

The agenda follows.

PROGRAMME OVERVIEW

TUE, 16 OCTOBER

8h00 – 9h00	***Registration and accreditation of participants***
9h00 – 10h00	**Welcome and Opening Ceremony** • *Alexander SEGER, Head of Cybercrime Division, Council of Europe* • *Takayuki OKU, Acting Head of Cybercrime Directorate, INTERPOL* • *Jason GRIMES, Deputy Head of Mission, British Embassy Addis Ababa* • *U.S. Mission to the African Union* • *Robert GILBERT, Cybercrime Expert, UNODC* • *Mrs. Anna BURYLO, Deputy Head of European Union Delegation to the African Union* • *H.E. Dr Amani ABOU-ZEID, Commissioner for Infrastructure and Energy, African Union*
10h00 – 10h30	**Coffee break**
10h30 – 11h30	**African Governments and the threat posed by cybercrime** Ministers' and senior officials' panel moderated by AUC • *Hon. Ebrima SILLAH, Minister of Information and Communication Infrastructure, the* ***Gambia*** • *Hon. Vincent Sowah ODOTEI, Deputy Minister for Communications of the Republic of* ***Ghana*** • *Hon. Mohamed Rahman SWARAY, Minister of Information and Communication,* ***Sierra Leone*** • *Hon. Foster OGOLA, Senator, National Assembly of* ***Nigeria*** • *Mrs. Rooba Yanembal MOORGHEN, Permanent Secretary Minister of Technology, Communication and Innovation,* ***Mauritius***
11h30 – 12h00	**Cybercrime legislation and policies in Africa** • *Moctar YEDALY, Head of Information Society Division,* ***African Union Commission*** • *Alexander SEGER,* ***Council of Europe*** • *Papa Assane TOURE, Primature,* ***Senegal***
12h00 – 12h15	**Tackling the cross-border nature of cybercrime** • *Takayuki OKU,* ***INTERPOL***
12h15 – 12h45	**Strengthening capacities of African criminal justice authorities on cybercrime and electronic evidence** Panel moderated by African Union Commission (30 min) • *Robert GILBERT,* ***UNODC*** • *Timothy FLOWERS,* ***U.S. Department of Justice*** • *Olaide OLUMIDE, Cybercrime Policy, Home Office,* ***United Kingdom*** • *Carlos BANDIN-BUJAN, Programme Manager, Directorate-General for Development and Cooperation,* ***European Union Commission***
12h45 – 13h00	**Information and organization on workshop sessions**
13h00 – 14h00	**Lunch**

TUE, 16 OCTOBER – AFTERNOON

DAY 1 Workshop sessions	*Room 1* *POLICIES AND LEGISLATION*	*Room 2* *INTERNATIONAL COOPERATION*	*Room 3* *CAPACITY BUILDING*
14h00 – 17h30 Coffee break between 15h30-16h00	Workshop 1 ***Cybercrime and cyber security policies - the global outlook and the African Continent*** *(Chair: African Union Commission)*	Workshop 2 ***International cooperation against cybercrime in Africa – challenges and opportunities*** *(Chair: INTERPOL)*	Workshop 3 ***Building capacities of African criminal justice authorities on cybercrime and electronic evidence*** *(Chair: GFCE)*

18h00 Cocktail Dinner organized by INTERPOL

WED, 17 OCTOBER

DAY 2 Workshop sessions	*Room 1* *POLICIES AND LEGISLATION*	*Room 2* *INTERNATIONAL COOPERATION*	*Room 3* *CAPACITY BUILDING*
09h30 – 13h00 Coffee break between 10h30-11h00	Workshop 4 ***Current status of cybercrime legislation in Africa. International standards – The Budapest Convention and the Malabo Convention*** *(Chair: Council of Europe)*	Workshop 5 ***International cooperation in the fight against cyber-enabled financial crimes in Africa*** *(Chair: U.S. Department of Justice)*	Workshop 6 ***Capacity Building Workshop – Strengthening collaboration between LEAs and Service Providers*** *(Chair: ICANN)*

13h00 – 14h00 Lunch

DAY 2 Workshop sessions	*Room 1* *POLICIES AND LEGISLATION*	*Room 2* *INTERNATIONAL COOPERATION*	*Room 3* *CAPACITY BUILDING*
14h00 – 17h30 Coffee break between 15h30-16h00	Workshop 7 ***The jurisdictional challenges of the Electronic Evidence in the cloud*** *(Chair: European Union)*	Workshop 8 ***International judicial cooperation – 24/7 Points of contact network and MLA authorities. Case studies, challenges and way forward*** *(Chair: Commonwealth Secretariat)*	Workshop 9 ***Child sexual exploitation and cyber violence in Africa – A regional outlook of ongoing initiatives and best practices*** *(Chair: UNODC)*

THU, 18 OCTOBER – MORNING

DAY 3 Workshop sessions	*Room 1* *POLICIES AND LEGISLATION*	*Room 2* *INTERNATIONAL COOPERATION*	*Room 3* *CAPACITY BUILDING*
09h30 – 13h00 Coffee break between 11h00-11h30	Workshop 10 ***Protecting fundamental rights and the rule of law in the fight against cybercrime – Legislative challenges and approaches in Africa*** *(Chair: African Union Commission)*	Workshop 11 ***The use of Information and Communications Technologies (ICT) to facilitate and support Terrorism – The Criminal justice perspective*** *(Chair: UNODC)*	Workshop 12 ***Cybercrime training strategies and curriculum building for law enforcement and criminal justice authorities*** *(Chair: INTERPOL)*

13h00 – 14h00 Lunch

THU, 18 OCTOBER – AFTERNOON

Plenary session, Room 1	
14h00 – 15h30	**Results of the Workshops** *Cybercrime Policies and Legislation (30 mins)* • *Cybercrime Policies in Africa* • *Legislation on cybercrime and electronic evidence in Africa* • *Jurisdictions in cyberspace and the evidence in the cloud* • *Human rights safeguards and data protection* *International Cooperation (30 mins)* • *Challenges and opportunities in international cooperation* • *Cross-border cyber-enabled financial crimes* • *24/7 POC and MLA* • *ICT to facilitate and support terrorism* *Capacity Building (30 mins)* • *Collaboration and synergies in capacity building activities* • *Collaboration with Service Providers* • *Child sexual exploitation and cyber violence* • *Cybercrime training strategies*
15h30 – 16h00	**Coffee break**
16h00 – 17h00	**International diplomacy and the challenges posed by cybercrime** *Senior-level panel of AU Diplomats and senior officials moderated by the African Union Commission*
17h00 – 17h45	**Final remarks and the way ahead** *International organizations* *African Union Commission*
17h45 – 18h00	**Closing ceremony** *African Union Commission*
End of Forum	

WORKSHOPS OVERVIEW

1	***Cybercrime and cyber security policies - the global outlook and the African Continent***
Room 1	*Tuesday, 16 October 2018, 14h00-17h30*

Background: *Cybercrime has become a major concern across the world, the large scale and sophistication of the cyber-attacks and the related monetary damage has been increasing at exponential rates for several years affecting governments , businesses and individuals .To address the policy challenges posed by criminal and malicious activities committed over ICT networks in a regional and continental and international compatible manner , there is a need for harmonized security frameworks and flexible mechanisms to enhance cooperation and exchange of information on cyber threats among concerned stakeholders. The definition of national strategies and consequent policies to tackle such issues has become a top priority in many African countries, and their adoption requires a strong commitment from national authorities and appropriate resources and capacities.*

Purpose: *To discuss the current status of Cybersecurity and Cybercrime policies in Africa, see how African countries deal with the complexity and international dimension of Cybersecurity policy making as well as international and regional debates over the creation of a global framework to fight transnational cybercrime. What new approaches or policies should be taken in account while drafting the national and regional legislations and how better align national laws with the international instruments and best practices?*

Chair: Moctar Yedaly, **African Union Commission**

Rapporteur: African Union Commission

Panel:

- **General Introduction**
- **Cybercrime and cyber security strategies in Africa - the general outlook**
  - World Bank
  - U.S. Department of Justice
- **Case studies and good practices**
  - Ghana
  - Morocco
  - Uganda
- **Challenges in implementing national strategies**
  - Panel discussion
- **Discussion and the way forward**

Reference materials	

2	***International cooperation against cybercrime in Africa – challenges and opportunities***
Room 2	*Tuesday, 16 October 2018, 14h00-17h30*

Background: *We often say that we need to work together to fight against cybercrime, but what is the challenges behind such claim? New possibilities were opened for criminal activity, and the criminal networks operate globally using the new technologies. The increasing reliance on the Internet, combined with economic growth and development of technology, has introduced new risks and vulnerabilities. Law enforcement agencies still face the challenges to respond effectively in the cross-border investigation. From cyber-dependant crimes such as ransomware and Crime-as-a-service, to traditional financial or telecom fraud, countries cannot conduct successful investigation without support from other parties.*

Purpose: *We would like to confirm the common understanding on the need for international cooperation. How do we cooperate, what are the challenges, and how can we do better? Through this workshop, we will identify (1) needs for cooperation with international, public, private partners, (2) capacity gaps in engaging in international cooperation, (3) to discuss how best synergize the cooperative network.*

Chair: Takayuki OKU, Director of Cybercrime Directorate, **INTERPOL**

Rapporteur: Dong Uk KIM, Project Manager – Cybercrime Directorate, **INTERPOL**

Panel:

- ► **International Cooperation against Cybercrime in Africa (Need and Challenges) [40 mins]**
  - – Country Situation Reports on Challenges [Kenya, Cote d'Ivoire, Gambia]
  - – Progress of Regional Efforts [Rwanda]
- ► **International Cooperation in Africa : a Survey [40 mins]**
  - – Current Situations and Challenges
  - – Questionnaires to be prepared, collected by INTERPOL
- ► **Building the Future Opportunities [40 mins]**
  - – INTERPOL Operational Activities in Africa [INTERPOL]
  - – Cooperation with CSIRT [ngCERT]
  - – Grounds for international cooperation [Council of Europe]
- ► **Discussions : How to enhance international cooperation in Africa [40 mins]**
  - – Panel discussion

Reference materials	

3	***Building capacities of African Criminal Justice Authorities on Cybercrime and Electronic Evidence***
Room 3	*Tuesday, 16 October 2018, 14h00-17h30*

Background: *For countries to be able to fight cybercrime in an effective and successful manner there are many topics to be addressed. This ranges from raising awareness on the importance of fighting cybercrime, by conducting needs assessments, drafting legislation, building specialized law enforcement units and training of judiciaries.*

Important in this regard is also for countries to engage in efficient regional and international cooperation. This entails not just operational cooperation between LEA's but also sharing experiences with neighboring countries to support capacity building against cybercrime.

The aim of this workshop is to share insights of several countries and international organizations providing capacity building against cybercrime, to learn about the different approaches, the topics they are focused on, the working methods they use and obviously their practical results.

Purpose: *(1) To provide insight on multiple capacity building initiatives by different organizations and countries (2) To share experiences of several African countries reaping the benefits of capacity building against cybercrime (3) To discuss good practices, problematic areas and the way ahead.*

Chair: Wouter VEENSTRA, , Manager Outreach & Partnerships, **GFCE** Secretariat

Rapporteur: Wouter VEENSTRA, , Manager Outreach & Partnerships, **GFCE** Secretariat

Panel:

- ▶ **UNODC (20 min)**
  - Mr. Robert GILBERT, Cybercrime Expert at UNODC
  - Discussion

- ▶ **Implementing the Commonwealth Cyber Declaration (20 min)**
  - Ms. Olaide OLUMIDE - Deputy Programme Manager, Commonwealth Cybersecurity Programme
  - Discussion

- ▶ **GLACY+ (30 min)**
  - Mr. Matteo LUCCHETTI, Programme Manager Cybercrime, Council of Europe
  - Dr. (Mrs.) Yanembal MOORGHEN, Permanent Secretary, Ministry of Technology, Communication and Innovation, Mauritius
  - Discussion

- ▶ **From Training to Action: Collaborations between the United States and Ghana in Cyber Investigations (30 min)**
  - Mr. Timothy C. FLOWERS, Sr. Trial Attorney, Computer Crime and Intellectual Property Section, U.S. Department of Justice
  - Mr. Albert ANTWI-BOASIAKO, Cyber Security Advisor, Ministry of Communication of Ghana
  - Discussion

- ▶ **GFCE: From awareness to implementation (20 min)**
  - Mr. Wouter VEENSTRA, Manager Outreach & Partnerships, GFCE Secretariat
  - Discussion

- ▶ **ECOWAS (20 min)**
  - Mr. Mawuli AMOA, Program Officer – Telecommunications and Networks, ECOWAS Commission
  - Discussion

- ▶ **Discussion on the way forward**

Reference materials	Commonwealth Cyber Declaration GFCE Delhi Communiqué GLACY+ Project

4	***Current status of cybercrime legislation in Africa. International standards – The Budapest Convention and the Malabo Convention***
Room 1	*Wednesday 17 October, 09h30 – 13h00*

Background: *Over 80% of African countries had reforms of legislation on cybercrime and electronic evidence in place or underway at the beginning of 2018, based on findings from the background desktop study on the state of cybercrime legislation, completed by the Council of Europe. Many of these governments use the Malabo and the Budapest Conventions as guidelines in the process of drafting specific legislation, consistent with human rights and rule of law requirements. The aim of this workshop is to review the progress made so far throughout the African continent, including examples of good practices, problematic areas and lessons to be drawn.*

Purpose*: (1) To discuss the current status of cybercrime legislation in the African Continent, progress made, issues encountered (2) To assess the status of adoption and implementation of international and regional standards in the field. (3) To discuss good practices, problematic areas and the way ahead.*

Chair: Alexander SEGER, Head of the Cybercrime Division, **Council of Europe**

Rapporteur: Zahid JAMIL, Council of Europe Expert

▶ **Cybercrime legislation in Africa: State of play [60 min]**

- The Malabo Convention
  - Moctar YEDALY, African Union Commission
- The Budapest Convention on Cybercrime
  - Alexander SEGER, Council of Europe
- The journey towards the Budapest Convention: United Kingdom
  - Daniel GRUBB, UK
- Overview of progress made
- Discussion

▶ **Substantive criminal law: examples of good practice [40 min]**

- Benchmarks: what is required?
- Country example [Cape Verde]
  - Mrs. Angela Cristina MARQUES RODRIGUES, Juiz Criminal, Conselho Superior da Magistratura Judicial, Cape Verde
- Discussion

▶ **Procedural powers to secure electronic evidence [40 min]**

- Benchmarks: what is required?
- Country examples [Ghana]
  - Mr.Albert ANTWI-BOASIAKO, National Cyber Security Advisor, Ministry of Communications, Ghana
- Discussion

▶ **Panel Discussion: How to ensure completion of legislative reforms in Africa? [40 min]**

- Mr. Cecil O. MASIGA, Senior Official – Ministry of Transport and Communications, Botswana
- Mr. Khumbuzo NKUNIKA, Assistant Director – Ministry of Transport and Communications, Zambia

Reference materials	*Malabo Convention* *Budapest Convention*

5	***International cooperation in the fight against cyber-enabled financial crimes in Africa***
Room 2	*Wednesday, 17 October 2018, 9h30-13h00*

Background: *The workshop will focus on all those forms of criminal activities aimed at getting illicit financial gain by the instrumental use of information and communication technologies. In this category one can easily identify many forms of Internet-related scams, frauds, ransomware attacks, but also targeted phishing attacks such as the so-called Business Email Compromise.*
They have represented an increasingly concerning issue all over the world in the past years, and have caused consistent financial losses to many organizations, both in the public and in the private sector, also in many African countries. Once more, international cooperation is essential to address these issues, surely between criminal justice authorities of the affected countries, but also with private parties – and specifically with the financial sector.

Purpose: *The aim of this workshop is to assess the current situation in Africa as compared to the international scenario and to discuss possible approaches aimed at reducing connected risks.*

Chair: Timothy FLOWERS, Senior Trial Attorney, Computer Crime and Intellectual Property Section at Main Justice, **U. S. Department of Justice**

Rapporteur: Timothy Flowers, U.S. Department of Justice

Panel:

► **General Introduction** – Issues at stake, global trends and threats for African countries
- Timothy FLOWERS, U.S. Department of Justice

► **Case studies – Successful investigations**
- Timothy FLOWERS, U.S. Department of Justice

► **Commonwealth**
- Shadrach HARUNA, Commonwealth Secretariat

► **The situation in Africa**
- Alhagie MBOW, Member of the Parliament, The Gambia
- Kwesi Korankye AMOAH, Executive Director, Economic and Organised Crime Office, Ghana
- Henry KAYIZA, CID Cybercrime, Uganda Police
- Ratjindua TJIVIKUA, Head of Cybercrime Investigations, Namibia

► **Possible solutions**
- Keong Min YOON, Legal Consultant, The World Bank
- George Maria TYENDEZWA, Head of Cybercrime Prosecution Unit, Federal Ministry of Justice – on behalf of Nigeria Electronic Fraud Forum

► **Discussion and the way forward**

Reference materials	

6	***Capacity Building Workshop – Strengthening collaboration between LEAs and Service Providers***
Room 1	*Wednesday, 17 October 2018, 9h30-13h00*

Background: *The importance of the Internet to any economy in this information age is not debatable and governments across the globe are increasingly focusing on the use of ICTs in all facets of the economic agenda. Thus, government participation in the policy making processes that would influence the way the internet would work tomorrow is critical. But we also know that the increasing ubiquity of the Internet and ICTs has also come with its good share of challenges, more so, cybercrimes. Today, more and more cases presented before courts of law either have a Cyber / ICTs element, or need the intervention of ICTS. And Law Enforcement Agencies have found themselves directly impacted. Are LEA's ready for law enforcement in the age of ICTs?.*

Purpose: *This workshop will discuss the current realities LEAs face in investigating, enforcing and prosecuting cyber / ICTs related crimes in a borderless environment. It will also highlight prevailing cyber laws in Africa and some specific country cases as well as a judicial perspective on how such cases are determined. Most importantly, it will also explore how best LEAs, ISPs and the industry could collaborate in efforts to fight cyber-crimes.*

Chair: Bob OCHIENG, Manager, Stakeholder Engagement – Africa, **ICANN**

Rapporteur: Bob OCHIENG, Manager, Stakeholder Engagement – Africa, **ICANN**

Panel:

- ► **Background setting [10 min]**
  - – Bob OCHIENG, ICANN
- ► **The law enforcement perspective [20 min]**
  - – Balbine MANGA, AVOCATE, Expert Cyber-legislation cybercriminalité et Gouvernance de l'internet, Cameroon
- ► **The judicial perspective – Cooperation with multi-national service providers [20 min]**
  - – Philippe VAN LINTHOUT, Investigating Judge, Belgium
- ► **The use of AFRINIC's WHOIS database to combat cybercrime [20 min]**
  - – Alan BARRETT, CEO of AFRINIC
- ► **Collaboration with Facebook [20 min]**
  - – Emilar GANDHI, Public Policy Manager, Facebook
- ► **Discussion: how to improve collaboration between LEAs and private parties in cybercrime investigations in Africa? [90 min]**
  - – Introductory remarks
  - – Panel discussion

Reference materials	►

7 *The jurisdictional challenges of Electronic Evidence in the cloud*

Room 1 *Wednesday, 17 October 2018, 14h00-17h30*

Background: The proliferation of cybercrime and other offences involving electronic evidence, technological change such as cloud computing and related uncertainty regarding data location and jurisdiction, pose major challenges to law enforcement authorities and the rule of law in cyberspace. Additional solutions are required to permit criminal justice authorities to obtain specified electronic evidence in specific criminal investigations. Such solutions are currently being developed by the Council of Europe (proposed Additional Protocol to the Budapest Convention) and the European Union (e-evidence proposals) or have been adopted such as the US CLOUD act.

Purpose: To review the significant of challenges and the relevance of solutions for Africa.

Chair: Carlos BANDIN-BUJAN, Programme Manager Security, Nuclear Safety, Directorate-General for Development and Cooperation, **European Union Commission**

Rapporteur: Philippe VAN LINTHOUT, Investigating Judge, Co-President of the association of Investigating Judges, Court of First Instance of Antwerp, **Belgium**

Panel:

▶ **Crime and evidence in the cloud : challenges and issues [60 min]**

- Introductory presentation
- Access to evidence in the cloud: territoriality and enforcement jurisdiction
- The effectiveness of mutual legal assistance
- Cooperation with the private sector: opportunities and limitations
  - Philippe VAN LINTHOUT, Belgium
  - Emilar GANDHI, Public Policy Manager, Facebook

▶ **Towards solutions [60 minutes]**

- Introductory presentation
- US CLOUD act
  - Timothy FLOWERS, U.S. Department of Justice
- European Union E-evidence proposals
  - Carlos BANDIN-BUJAN, European Commission
- Solutions within the context of the Budapest Convention
  - Alexander SEGER, Council of Europe

▶ **Discussion: what way ahead for Africa? [60 minutes]**

- Panel discussion [**Ghana**, **Nigeria**, **Senegal**]
  - Albert ANTWI-BOASIAKO, Ministry of Communications, Ghana
  - George-Maria TYENDEZWA, Federal Ministry of Justice, Nigeria
  - Papa Assane TOURE, Primature, Senegal

Reference materials	▶ Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters; ▶ Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings; ▶ Enhanced international cooperation on cybercrime and electronic evidence: Towards a Protocol to the Budapest Convention ▶ Negotiations of the Additional Protocol to the Buda[pest Convention ▶ US CLOUD Act

8	***International judicial cooperation – 24/7 Points of contact network and MLA authorities. Case studies, challenges and way forward***
Room 2	*Wednesday, 17 October 2018, 14h00-17h30*

Background: *The increasing reliance on internet for businesses and social transactions and the ubiquitous nature of electronic evidence in most criminal cases, have heighten the need for Law enforcement agencies and prosecution services to deal with identification of cybercriminals in foreign jurisdictions or with acquisition of data that are located abroad. Due to the volatility and fleeting nature of this form of evidence, there is an increasing need to structure cooperation in a manner that would be efficient and effective for criminal justice.*

Jurisdiction is traditionally structured on territorial basis. Thus nations guide their sovereign power zealously. However, sovereignty, a fundamental principle of statehood, is one of the major tools in the armoury of the criminals – who use the barriers of sovereignty to shield themselves and evidence of their crimes from detection. They often take advantage of differences between legal systems, the clash of bureaucracies, the protection of sovereignty and, many times, the incapacity of law enforcement and nations to work together to overcome their differences, to foster their crimes. The scale and volume of these crimes, the technical complexity of identifying the perpetrators and, where identified, the challenges of bringing them to justice remain issues of critical and urgent concern to the law enforcement community.

This is aggravated by the ease and speed at which this crime is committed across borders and the slow bureaucratic criminal justice response. However, with the increasing wave of trans-border crime and its attendant consequences on varied economies, serious consideration and attention are being increasingly given to the issue of how international co-operation can be structured to provide effective action against criminals.

Regional blocks have aligned and restructured their cross border cooperation, relating to cybercrime and electronic evidence to meet the urgency required. Such changes have been given prominence in the Budapest Convention 24/7 network for parties to the Convention and its additional protocol. Countries that are yet to be party to the Convention have also administratively structured cooperation informally through law enforcement cooperation mechanism, such as INTERPOL or regional prosecutorial cooperation, complementing formal cooperation through central authorities, to ensure quick, efficient and effective cooperation.

These forms of cooperation have proved successful particularly for parties to Budapest Convention. Those outside the Budapest convention are developing as product of necessity but need to be fostered, strengthened and anchored by legislation for effectiveness. However, challenges such as cumbersome administrative procedures, necessity to cope with very varied legislations, policy frameworks and different levels of collaboration provided by private sectors persist. These challenges are multiple with countries without formal 24/7 network.

Purpose: *The purpose of this session through case studies and discussions, is to identify the need for the efficacy of the 24/7 network, assess (1) the challenges in providing cross border assistance in criminal matters between central authorities and criminal justice agencies in Africa and in other regions; (2) regional and international best practices; (3) the way forward.*

Structure: *The Workshop is structured into two parts. The first part, comprised of Comsec, CoE, Interpol, UK and one individual expert, runs for one and a half hours. The second part will discuss country experiences and is comprised of some contact persons sharing their experiences on the best practice and challenges will run for one hour. The half an hour will be devoted to Q/A session..*

Chair: Shadrach HARUNA, **Commonwealth Secretariat**

Rapporteur: Olaide OLUMIDE, **UK Home Office**

Panel:

► **International cooperation between criminal justice authorities – a Case study [30 min]**

- Introductory presentation
- The shutdown of the Avalanche botnet
    - Zahid JAMIL, Barrister-at-law, Pakistan

► **The 24/7 networks and other international cooperation instruments [60 min]**

- INTERPOL
    - Dong Uk KIM, Digital Crime Officer
- Commonwealth Secretariat
    - Shadrach HARUNA, Commonwealth Secretariat
- Council of Europe
    - Matteo LUCCHETTI, Program Manager Cybercrime
- The case of UK
    - Daniel GRUBB, Cyber Policy, Home Office

► **Experiences, best practices and challenges [60 min]**

- ngCERT, Nigeria
- Emmanuel MUGABI, Uganda
- Morocco

► **Q&A [30 min]**

-

Reference materials	

9	***Child sexual exploitation and cyber violence in Africa – A regional outlook of ongoing initiatives and best practices***
Room 3	*Wednesday, 17 October 2018, 14h00-17h30*

Background: *The scourge of online sexual exploitation and abuse of children is on the rise. In many instances the children being abused are from developing countries while the abusers are based in developed countries. The emergence of the use of live streaming child sex abuse has provided a greater challenge for Law Enforcement agencies. Cooperation between ISP's and LE is the only way the scourge of Online Child sexual exploitation will be overcome.*

Purpose: *(1) To discuss the current Criminal Justice response to Child sexual exploitation and cyber violence (2) How to address the issues from a practical and legislative perspective. (3) To discuss good practices, problematic areas and the way ahead.*

Chair: Kelvin LAY, Law Enforcement Expert (International Consultant), **UNODC**

Rapporteur: Kelvin LAY, Law Enforcement Expert (International Consultant), **UNODC**

Panel:

► **The use of the Internet for Child sexual exploitation: State of play [60 min]**

- Case studies-best practice (Kenya)
- Social Media Platforms Dissemination of CSAM
- ISP's and cooperation with Law Enforcement
- International Cooperation
- Discussion

► **Hunting the Predators-Online investigations [40 min]**

- OSINT
- Undercover Investigations-Human Rights
- Discussion

► **Technical Challenges of Investigating Child sexual Exploitation [40 min]**

- Encryption and Live Streaming
- Restrictions of MLA's/International Cooperation
- Lack of skilled personnel to carry out investigations

► **Discussion: How to ensure a coordinated response to Child Sexual Exploitation and Cyber violence [40 min]**

- Panel discussion: [Kenya, Uganda, Ethiopia]

Reference materials	

10	***Protecting fundamental rights and the rule of law in the fight against cybercrime – Legislative challenges and approaches in Africa***
Room 1	*Thursday, 18 October 2018, 9h30-13h00*

Background: *The large-scale theft of personal data, computer intrusions, bullying, harassment and other forms of cyber violence, or sexual violence against children online, are attacks against human rights. Hate speech, xenophobia and racism may contribute to radicalisation leading to violent extremism. Attacks against computers used in elections and election campaigns are attacks against democracy. Daily attacks against critical information infrastructure affect national security and economic and other national interests as well as international peace and stability. Moreover, evidence in relation to fraud, corruption, murder, rape, terrorism, the sexual abuse of children and, in fact, any type of crime may take the form of electronic evidence, which is volatile, often intangible and often in other jurisdictions. And accessing such evidence also has implications for human rights and the rule of law.*

Purpose: *(1) To discuss the challenges to human rights and the rule of law posed by cybercrime in Africa (2) To review progress made in Africa on related adapting legislative frameworks to the new digital environment (3) To discuss the way forward to raise awareness on Digital rights.*

Chair: Moctar YEDALY, **African Union Commission**

Rapporteur: Moctar YEDALY, **African Union Commission**

Panel:

- ► **Cybercrime and threats to fundamental rights [World Bank, Cipesa, Academia]**

  - – Introduction and general remarks
  - – The international landscape
  - – The situation in Africa

- ► **Upholding human rights and the rule of law in the field of cybercrime [ICANN, Internet Society]**

  - – Introduction and general remarks
  - – The global outlook
  - – Protection of Personal Data in cybercrime investigation and prosecution
  - – The situation in Africa

- ► **Panel discussion**

Reference materials	Malabo convention African Chart on Human Rights – African Union Internet Governance and digital economy – Personal Data Protection Guidelines for Africa.

11	***The use of Information and Communications Technologies (ICT) to facilitate and support Terrorism – The Criminal justice perspective***
Room 2	*Thursday, 18 October 2018, 9h30-13h00*

Background: It is widely understood that the Internet has changed societies irrevocably, for good and for bad. While the many benefits of the Internet are self-evident, it may also be used to facilitate communication within terrorist organizations and to transmit information on, as well as material support for, planned acts of terrorism, all of which require specific technical knowledge for the effective investigation of these offences.

Purpose: (1) To discuss the current Criminal Justice response to ICT enabled terrorism (2) To assess the status of adoption and implementation of international and regional standards in the field. (3) To discuss good practices, problematic areas and the way ahead.

Chair: Robert GILBERT, Cybercrime Expert, **UNODC**

Rapporteur: Robert GILBERT, Cybercrime Expert, **UNODC**

Panel:

▶ **The use of the Internet for Terrorist purposes: State of play [60 min]**

- Case studies-recent examples
- Social Media Platforms and Radicalisation
- Terrorist Financing
- Execution
- Discussion

▶ **The use of the Internet in Counter-Terror investigations [40 min]**

- OSINT
- Undercover Investigations-Human Rights implications
- Discussion

▶ **Technical Challenges of Investigating Terrorist Attacks [40 min]**

- Lack of skilled personnel
- Collaboration or non-collaboration of Internet Service Providers (ISP's)
- Encryption
- Restrictions of MLA's/International Cooperation
- Possibilities of direct access to information (Article 32 Budapest Convention)
- Forced collaboration – the territoriality question (Yahoo – Skype case)

▶ **Discussion: How to ensure a coordinated response to ICT enabled Terror [40 min]**

- Panel discussion: [Somalia, Kenya, Uganda]

Reference materials	

12	***Cybercrime training strategies and curriculum building for law enforcement and criminal justice authorities***
Room 3	*Thursday, 18 October 2018, 9h30-13h00*

Background: *With the pervasive use of information technology in everyday life of general public, the day-to-day tasks of any law enforcement or judiciary officers may include components of electronic evidence and Internet investigations. The knowledge and skills on IT investigation is required not only for the members of cybercrime units, but also for any other officers in other branches of the law enforcement agencies. However, such courses are seldom taught in training institutions of the LEA.*

Purpose: *What are the knowledge and skills that LE needs? Does patrol officers need to know what IP address is, or how to deal with mobile phones? Can we train the existing officers, or do we need to recruit technical officers? Through this workshop, we aim to (1) identify the need and challenges in training, (2) present models of training development, and (3) discuss how to develop and deliver sustainable training for the law enforcement officers.*

Chair: Takayuki OKU, Director of Cybercrime Directorate, **INTERPOL**

Rapporteur: Dong Uk KIM, Project Manager – Cybercrime Directorate, **INTERPOL**

Panel:

- **Cybercrime Training Needs and Challenges [40 mins]**
  - Country Situation Reports [Botswana, Nigeria]
  - Challenges in Developing Training [INTERPOL]
  - Discussions
- **Cybercrime Training Strategy: a Survey [40 mins]**
  - Current Situations and Challenges
  - Strategies for Cybercrime Training for LE
  - Questionnaires to be prepared, collected by INTERPOL
- **Building the Future Opportunities [40 mins]**
  - CERT's role in cybercrime training [Nigeria]
  - Progress Report on Judicial Training [Council of Europe]
  - Developing Standard Cybercrime Curriculum [INTERPOL]
- **Discussions : How to enhance international cooperation in Africa [40 mins]**
  - Panel discussion

Reference materials	