Organized and funded by:

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

OAS REMJA

HEMISPHERIC FORUM ON INTERNATIONAL COOPERATION AGAINST CYBERCRIME

CONFERENCE PROGRAMME

SANTO DOMINGO,
5-7 DECEMBER 2017

OUTLINE

1. BACKGROUND

With the growing relevance of information and communication technologies for societies around the world and thus their vulnerability to threats such as cybercrime a major capacity building effort is required to enable criminal justice authorities to investigate, prosecute and adjudicate offences against and by means of computers as well as other offences entailing electronic evidence.

Given the scale of this challenge and the scarcity of resources, international organisations should join forces and develop synergies to support countries in a consistent and effective manner.

The Council of Europe and the European Union, for example, assist countries through a range of joint projects, including the GLACY+ project on Global Action on Cybercrime Extended. For both organisations GLACY+ helps create the necessary capacities to implement the Budapest Convention and to cooperate internationally within the framework of this treaty. The Dominican Republic as the first country of Latin America having become a Party serves as priority country and hub to share experience with others (www.coe.int/cybercrime).

The European Union

The European Union is supporting the organisation of this Hemispheric Forum on International Cooperation on Cybercrime through the joint EU-Council of Europe project on Global Action on Cybercrime Extended (GLACY+) financed under its Instrument Contributing to Peace and Stability.

The European Union has taken firm steps in recent years to enhance cybersecurity and to strengthen criminal justice action on cybercrime. Capacity building is a key element of the European Union's global response.

In 1999, the Meetings of Ministers of Justice or other Ministers of Attorney General of the Americas (REMJA), within the framework of the Organization of American States (OAS), established the Working Group on Cybercrime ("the Working Group") as the principal forum for international cooperation in the prevention, investigation and prosecution of cybercrime; facilitate the exchange of information and experiences among its members; and make necessary recommendations to enhance and strengthen cooperation among the OAS member states and with international organizations and mechanisms. The United States, through its Department of Justice (US/DoJ) serves as the Chair of the Working Group, which is supported by the OAS Department of Legal Cooperation of the Secretariat for Legal Affairs, in its capacity as the Technical Secretariat to the REMJA. This Working Group has taken leadership on the implementation of the recommendations adopted by the REMJA regarding cybercrime which includes adhering to the Convention on Cybercrime, also known as the Budapest Convention, by OAS member states, as well as adopt the legal and other measures required for its implementation. In addition, the US/DoJ and the Technical Secretariat have collaborated in carrying out over 34 cybercrime training workshops since 2004, involving more than 2200 Latin American and Caribbean judges, prosecutors and investigators.

In 1996, the U.S. Department of Justice (DOJ) created the Computer Crime & intellectual Property Section (CCIPS) with 5 federal prosecutors. Today, CCIPS has a staff of 45 prosecutors that prosecute and investigate cases involving exclusively electronic evidence. CCIPS is also the U.S. representative to the G7 24/7 High Tech Crime Network points of contact. Additionally, DOJ has at least one specialized (Computer Hacking & Intellectual Property-CHIP) prosecutor located in each of the 96 federal offices throughout the country. Each year, CCIPS gathers the CHIP prosecutors and holds a week long training to cover the new legal and technical challenges affecting cybercrime. A significant part of CCIPS' work is also aimed at international capacity building. More than 2,200 Latin American and Caribbean judges, prosecutors, and investigators, for example, have participated in 3-day cybercrime workshops through a joint effort between DOJ and the Organization of American States. CCIPS has held similar training in Asia and Africa.

The Caribbean Community (CARICOM) is a grouping of twenty countries: fifteen Member States and five Associate Members. CARICOM is the oldest surviving integration movement in the developing world. CARICOM rests on four main pillars: economic integration; foreign policy coordination; human and social development; and security.

Article 23 of the Revised Treaty of Chaguaramas provides for the Secretariat as the principal administrative organ of the Community with Headquarters in Georgetown, Guyana.

At the Twenty-Sixth (26th) Meeting of the Conference of Heads of Government held in July 2005 a new framework was designed with the objective(s): (1) to establish within CARICOM arrangements for managing the Regional Crime and Security Agenda and (2) To equate crime and security with other areas such as trade, health, agriculture and education.

Additional proposals included the establishment of the following bodies:

1. "A Council of Ministers with responsibility for National Security and Law Enforcement (CONSLE) as a separate and distinct body of CARICOM, reporting to the Conference of Heads of Government through the Prime Minister with responsibility for Crime and Security, and

2. "An Implementation Agency for Crime and Security (IMPACS), the nerve centre of this Management Framework and an institution of CARICOM with primary responsibility for the implementation of the regional crime and security agenda, reporting directly to the Council of Ministers.

The Framework formally came into operation in March 2006 when the CARICOM Secretariat convened the first meeting of the Council of Ministers responsible for National Security and Law Enforcement (CONSLE). In 2006, the Community was the recipient of the HIPCAR project which provided nine (9) pieces of legislation- including one on cybercrime. Adoption of the legislation has been slow due to many extenuating circumstances. There is intention to intensify these efforts in 2018.

There are several ongoing activities in CARICOM on cybercrime– including the development of the CARICOM Cybercrime Action Plan, the Declaration of St Philip, Barbados, on Caribbean Collaboration on Cyber Security, which was ratified in 2013; the CARICOM Cybercrime Strategy and the creation of National Cyber Security Incident Response Teams (CIRTS).

The Dominican Republic had its first "cybercrime investigation" in mid-2003, which evidenced the need for specific cybercrime legislation and an investigative unit. The first unit, the Cybercrime Investigation Division (DIDI) was created in the end of 2003 within the National Department of Investigations, an agency with the mission of protecting the President, elected officials and dealing with national security and terrorism. In 2004 began the drafting of a cybercrime-specific legislation, which was drafted in line with the Budapest Convention drafting guidelines. In November 2004 the Cybercrime Investigation Department (DICAT) was created within the Criminal Investigations Directorate of the National Police to deal with all aspects of cybercrime.

The cybercrime law, 53-07 was enacted in April 2007, fully in-line with the Budapest Convention. In 2008 the Council of Europe invited Dominican Republic to accede to the Budapest Convention. The country acceeded in 2013, becoming, this way, the first country in the hemisphere to be a party to the convention. In 2013 also the Specialized Cybercrime Prosecution Service (PEDATEC) was created within the General Attorney's Office; this service has currently specialized attorneys in all 34 judicial districts.

The Dominican Republic is now a priority country and regional hub in the GLACY+ capacity building project, assisting the C-PROC office in reaching out to all countries in Latin America and the Caribbean.

2. EXPECTED OUTCOMES

The outcomes of the Forum are expected to be threefold:

✓ Representatives of participating countries will be in a better position to benefit from the support by different international organisations to the strengthening of their criminal justice capacities on cybercrime and electronic evidence, including instruments fo international cooperation.

✓ 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.

✓ Representatives of participating countries will be able to exchange best practices amongst each other and create a network of contacts that will allow them to perform a more efficient working environment through the exchange of information regarding common tasks; the strengthening of their capacities to face new challenges in criminal law investigations that have a cybercrime component and evaluation of electronic evidence; the promotion and improvement of regional cooperation protocols between internet service providers and criminal investigators; and the strengthening of regional mechanisms in criminal matters.

3. PARTICIPANTS

Governments of countries of Latin America and the Caribbean have nominated officials that are involved in matters related to cybercrime and electronic evidence representing law enforcement, prosecution services, judiciary, relevant ministries (such as Justice and Interior) or legislators. Private sector organisations are also participating.

4. LOCATION

This forum will take place at the Convention Center of the Ministry of Foreign Affairs (MIREX) in Santo Domingo, Dominican Republic and will last for 3 days.

PROGRAMME OVERVIEW

TUE, 5 DECEMBER

08h00 – 09h00.	REGISTRATION AND ACCREDITATION OF PARTICIPANTS
PLENARY SESSIONS	ROOM1
09h00 – 10h00.	OPENING CEREMONY (English/Spanish) 1. Council of Europe 2. European Union 3. Organization of American States 4. US Department of Justice 5. CARICOM Secretariat 6. Government of the Dominican Republic
10h00 – 10h30.	COFFEE BREAK
10h30 – 11h45	Capacity building on cybercrime in the Americas: "How international and regional organizations and other authorities can support you" (10 minutes each) 1. **Major Michael JONES**, Chief of Operations, CARICOM IMPACS 2. **Adrian ACOSTA**, Digital Crime Officer, INTERPOL 3. **Wouter VEENSTRA**, Deputy Head, Global Forum on Cyber Expertise (GFCE), Secretariat 4. **Captain (N) Errington R. SHURLAND,** Executive Director, Regional Security System 5. **Alvaro Proaño CARRIÒN,** Mayor de Policia, AMERIPOL, Colombia 6. **Normand WONG,** Counsel, Criminal Law Policy, Department of Justice, Canada
11h45 – 12h45.	Key note speakers (15 minutes each): 1. Building a cybercrime strategy (CoE); **Alexander SEGER, Council of Europe** 2. The use of cyber networks in the fight against cybercrime **Adrian ACOSTA, Digital Crime Officer, INTERPOL** 3. The Project "Republica Digital" and the National Cybersecurity Policy **Zoraima CUELLO, Vice-Minister of Presidency, Dominican Republic**
12h45 – 13h00.	Information and organization on workshop sessions.
13h00 – 14h00.	LUNCH

WORKSHOP SESSIONS	ROOM1 (English/Spanish)	ROOM 2 (English/Spanish)
14h00 – 17h30. (Coffee break between) 15h30 – 16h00.	WORKSHOP 1 COUNCIL OF EUROPE Capacity building and the Budapest Convention on Cybercrime; support the elaboration of strategies on cybercrime and collection of e-evidence	WORKSHOP 2 INTERPOL Interpol's role in international police cooperation and coordination with private sector
20h00	SOCIAL DINNER ORGANIZED BY THE GOVERNMENT OF DOMINICAN REPUBLIC (TBC)	

WED, 6 DECEMBER

WORKSHOP SESSIONS	ROOM 1 (English/Spanish)	ROOM 2 (English/Spanish)
9h30 – 13h00. (Coffee break between) 10h30-10h45.	**WORKSHOP 3** INTERPOL Capacity building and obligatory certification of police officers in digital evidence and cybercrime investigations	**WORKSHOP 4** OAS/USDoJ TOR, The Dark Web and Bitcoin: The Technical Background Needed and an Example of a Successful Investigation and Prosecution
13h00 – 14h00.	LUNCH	

WORKSHOP SESSIONS	ROOM 1 (English/Spanish)	ROOM 2 (English/Spanish)
14h00 – 17h00. (Coffee break between) 15h30 – 16h00.	**WORKSHOP 5** Council of Europe Access to evidence in the cloud	**WORKSHOP 6** Other International / regional organizations and other countries (Part 1) International community in the fight against cybercrime

THU, 7 DECEMBER

WORKSHOP SESSIONS	ROOM 1 (English/Spanish)	
9h30 – 13h00. (Coffee break between) 10h30-11h00.	**WORKSHOP 7** OAS/USDoJ Procedural and Substantive Laws: how courts evaluate admissibility of digital evidence	**WORKSHOP 8** Other International / regional organizations and other countries (Part 2) International community in the fight against cybercrime
13h00 – 14h00.	LUNCH	

WORKSHOP SESSIONS	ROOM 1 (English/Spanish)
14h00 – 17h30.	FINAL PLENARY • Results of workshops • Final remarks and way forward (COE, OAS, CARICOM IMPACS, CARICOM Secretariat, INTERPOL, USDoJ, Canada and European Union) CLOSING CEREMONY Government of Dominican Republic
17h30.	END OF CONFERENCE

DETAILED PROGRAMME

TUE, 5 DECEMBER

08h00 – 09h00. REGISTRATION AND ACCREDITATION OF PARTICIPANTS

WORKSHOP SESSIONS ROOM 1 (English/Spanish)

09h00 – 10h00. **OPENING CEREMONY**
(English/Spanish)

1. Council of Europe
2. European Union
3. Organization of American States
4. US Department of Justice
5. CARICOM Secretariat
6. Government of the Dominican Republic

10h00 – 10h30. COFFEE BREAK

10h30 – 11h45 Capacity building on cybercrime in the Americas:How international and regional organizations and other authorities can support you" (10 minutes each)

1. **Major Michael JONES**, Chief of Operations, CARICOM IMPACS
2. **Adrian ACOSTA**, Digital Crime Officer, INTERPOL
3. **Wouter VEENSTRA**, Deputy Head, Global Forum on Cyber Expertise (GFCE), Secretariat
4. **Captain (N) Errington R. SHURLAND,** Executive Director, Regional Security System
5. **Alvaro Proaño CARRIÒN,** Mayor de Policia, AMERIPOL, Colombia
6. **Normand WONG,** Counsel, Criminal Law Policy, Department of Justice, Canada

11h45 – 12h45. Key note speakers (15 minutes each):

1. Building a cybercrime strategy (CoE);
   Alexander SEGER, Council of Europe
2. The use of cyber networks in the fight against cybercrime
   Adrian ACOSTA, Digital Crime Officer, INTERPOL
3. The Project "Republica Digital" and the National Cybersecurity Policy
   Zoraima CUELLO, Vice-Minister of Presidency, Dominican Republic

12h45 – 13h00. Information and organization on workshop sessions.

13h00 – 14h00. LUNCH BREAK

WORKSHOP SESSIONS — ROOM 1 (English/Spanish)

14h00 – 17h30.

(Coffee break between) 16h00-16h15.

WORKSHOP 1:
COUNCIL OF EUROPE: Capacity building and the Budapest Convention on Cybercrime; support the elaboration of strategies on cybercrime and e-evidence

The "culture of security" is the ultimate component of a country's development in digital capacity. The cybersecurity culture addresses the level where governments and its citizens acknowledge the risks existing in the cyberspace by default and how to manage those risks through a set of good security practices. In this workshop, experts and participants will discuss and agree on the main elements for building a cyber-strategy: Strategic foundations, Policy and Governance, Resourcing, Risk management, Resilience, Cybercrime, key Partnerships and Cybersecurity culture and workforce.

The added aim of this workshop is also to identify the main features of the Budapest Convention in the fight against Cybercrime, including the accession process and the existing capacity building projects being implemented in the region, as well in enhancing the capacity of Prosecutors and Judges in the fight against Cybercrime and in handling electronic evidence.

Moderator/s: Claudio PEGUERO, General of Brigade, Director of Plan and Development, National Police and National Coordinator to the GLACY+ Project, Dominican Republic;

Rapporteur: Daniela DUPUY, Specialized Prosecutor on Cybercrime, Buenos Aires, Argentina;

- Topic: How to reflect Cybercrime and Electronic Evidence in a Cyber Strategy in LATAM Countries
  Speaker: Francisco NEIRA BASSO, Chief ICT Officer, International Consultant, Cybercrime Expert, Council of Europe (30 min + 30 min for discussion)

- Topic: Features provided by the Budapest Convention in the fight against Cybercrime.
  Speaker: Betty SHAVE, International Consultant, Expert on Cybercrime, Council of Europe (30 min + 30 min for discussion)

- Topic: Ideas and strategies for a capacity building programme for operators of the criminal justice system in LATAM countries.
  Speaker: Marcos SALT, International Consultant, Expert on Cybercrime, Council of Europe (30 min + 30 min for discussion)

Conclusions: Ingredients for success.
Speaker: Claudio PEGUERO, Dominican Republic (15 min)

WORKSHOP SESSIONS — ROOM 2 (English/Spanish)

14h00 – 17h30.

(Coffee break between) 16h00-16h15.

WORKSHOP 2:
INTERPOL's role in international police cooperation and coordination with private sector

Cybercrime is a fast-growing area of crime. More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide.

Most cybercrimes are transnational in nature, therefore INTERPOL is the natural partner for any law enforcement agency looking to investigate these crimes on a cooperative level. By working with private industry, INTERPOL is able to provide local law enforcement with focused cyber intelligence, derived from combining inputs on a global scale.

Moderator/s: Milos MIJOMANOVIC, Digital Crime Officer, INTERPOL;
Rapporteur: Dong Uk KIM, Project Manager, INTERPOL;

- Topic: Interpol coordinated cybercrime operations: America's cyber surge
  Speaker: Adrian ACOSTA (30 min + 30 min for discussion)

- Topic: Case Study: Operational Case
  Speaker: Victor CHANENKO, Head of Cybercrime Department of the Federal Police, Argentina and Horacio AZZOLI, Head of the Specialized Unit in Cybercrime (UFECI), Argentina (30 min + 30 min for discussion)

- Topic: Case Study
  Speaker: Edgar Martin VARGAS CARPIO, Head of National Police in Peru, AMERIPOL, Colombia (30 min + 30 min for discussion)

Conclusions: Ingredients for success.
Speaker: Milos MIJOMANOVIC, Interpol (15 min)

WEDNESDAY, 6 DECEMBER

WORKSHOP SESSIONS — ROOM 1 (English/Spanish)

09h30 - 13h00

(Coffee break between) 10h30-10h45.

WORKSHOP 3:
INTERPOL capacity building and obligatory certification of police officers in digital evidence and cybercrime investigations

Cybercrime is rapidly getting progressed and diversified due to its technical development and sophisticated crime operandi. On top of that, Criminal organizations turning increasingly to the Internet to facilitate their activities and maximize their profit in the shortest time. The crimes themselves are not necessarily new – such as theft, fraud, illegal gambling, sale of fake medicines – but they are evolving in line with the opportunities presented online and therefore becoming more widespread and damaging. Police training plays a key role in INTERPOL's overall mission to promote international police co-operation. INTERPOL works to enhance and certificate the capacity of police in participating member countries, by equipping them with the knowledge and skills needed to meet today's policing challenges. The wide range of initiatives is designed to bridge the gap between national and international policing.

Moderator/s: Adrian ACOSTA, INTERPOL;

Rapporteur: Dong Uk KIM, INTERPOL;

- Topic: Regional capacity building programme: "Cyber-Americas"
  Speaker: Milos MIJOMANOVIC, Interpol (30 min + 30 min for discussion)
- Topic: Completion of cybercrime capacity building programme in the Republic of Argentina
  Speaker: Diosnel ALARCON (30 min + 30 min for discussion)
- Topic: Country example: Capacity building and certification - Guatemala
  Speaker: Diego TEOS, Head of Cybercrime Unit of National Police, Guatemala
  (30 min + 30 min for discussion)

Conclusions: Ingredients for success.
Speaker: Adrian ACOSTA (15 min)

WORKSHOP SESSIONS — ROOM 2 (English/Spanish)

09h30 - 13h00

(Coffee break between) 10h30-10h45.

WORKSHOP 4:
ORGANIZATION OF AMERICAN STATES AND UNITED STATES DEPARTMENT OF JUSTICE (OAS/USDoJ): TOR, The Dark Web and Bitcoin: The Technical Background needed and an Example of a Successful Investigation and Prosecution

Nowadays, crime in cyberspace can be committed anonymously with ease and at times without detection by the victim. Cyberspace allows criminals to extend their reach across national borders and poses a strain on resources for prosecutors and investigators. What happens when an extra layer of anonymity is added to the mix? In this workshop, experts will discuss the TOR network (also known as the "onion"), how to investigate cases in it, what is the Dark Web, the tools needed to trace criminals and the currency (bitcoin) that criminals use to purchase and sell goods in it. Participants will also be provided the opportunity to interact with the prosecutor who was part of the team who successfully investigated and prosecuted Ross Ulbricht also known as "Dread Pirate Roberts", the creator of Silk Road.

Moderator/s: Rodolfo ORJALES, USDoJ;

Rapporteur: Laura MARTINEZ, OAS;

- Topic: The Dark Web and Bitcoin
  Speaker: Licurgo YUNEZ, Head of DICAT, National Police, Dominican Republic
  (60 min + 30 min for discussion)
- Topic: Case study – Silk Road
  Speaker: Tim HOWARD, U.S. Attorney's Office, Southern District of New York
  (Silk Road Prosecutor) (60 min + 30 min for discussion)

Conclusions: Ingredients for success.
Speaker:Rodolfo ORJALES, USDoJ (15 min)

13h00 – 14h00. LUNCH BREAK

WORKSHOP SESSIONS ROOM 1 (English/Spanish)

14h00 – 17h30.

(Coffee break between) 16h00-16h15.

WORKSHOP 5:
COUNCIL OF EUROPE: Access to evidence in the cloud

The Cybercrime Convention Committee (T-CY), at its 12th plenary (2-3 December 2014), established a working group to explore solutions for access to evidence in the cloud for criminal justice purposes, including through mutual legal assistance ("Cloud Evidence Group"). This decision was motivated by the recognition that in the light of the proliferation of cybercrime and other offences involving electronic evidence, and in the context of technological change and uncertainty regarding jurisdiction, additional solutions are required to permit criminal justice authorities to obtain specified electronic evidence in specific criminal investigations.

In this workshop participants will get familiar with the recommendations issued by the Cloud Evidence Group, difficulties, constraints but also the usefulness of the investigation in the "Cloud".

Moderator/s: Alexander SEGER, CoE;

Rapporteur: Betty SHAVE, United States;

- Topic: Criminal Justice challenges regarding access to evidence in the cloud
  Speaker: Francisco NEIRA BASSO, Chief ICT Officer, International Consultant, Cybercrime Expert, Council of Europe (30 min + 30 min for discussion)
- Topic: Cooperation with service providers
  Speaker: Enrique GUTIERREZ, Lead LATAM Investigations, Corporate External Legal Affairs, Microsoft (30 min + 30 min for discussion)
- Topic: Judicial challenges of the transborder access to data lodged in the cloud: case analysis
  Speaker: Marcos SALT, Professor, University of Buenos Aires, Faculty of Law, International Consultant, Council of Europe (30 min + 30 min for discussion)

Conclusions: Ingredients for success.
Speaker:Alexander SEGER, CoE (15 min)

WORKSHOP SESSIONS ROOM 2 (English/Spanish)

14h00 – 17h30.

(Coffee break between) 16h00-16h15.

WORKSHOP 6:
International community in the fight against cybercrime (Part 1)

In accordance with different worldwide sources, cybercrime is costing the world economy up to $500bn a year. Notwithstanding, international cooperation between the different international and regional actors as well as with countries with capacity to make the difference, remain, still, dangerously inadequate.

Therefore, the developments of an international and national level call of consciousness are the grounds for effective actions. There is a need is to reassess and renew as much as possible the current international legal frameworks, to offer a forum for broader international discussion expressing an outlook towards increasing and advancing international law-enforcement and judicial cooperation among the national authorities and between international and regional organizations. These developments should consider the influences of the novel and emerging issues in respect of international law-enforcement and judicial cooperation in criminal matters, with recommendations on capacity-building, which should show an equal concern for the situation in countries at different stages of development so as to avoid a chaotic future.

This workshop brings countries with capacity building programmes, international and regional organizations aligned in a congregation of efforts to show the respective covered areas and on how they can bring benefits to the countries that need their support.

Moderator/s: Wayne M. CAINES, Minister of National Security, Bermuda
Rapporteur: Cesar MOLINE, INDOTEL, Dominican Republic;

- Topic: Cybersecurity and our environment
  Speaker: Anselm CHARLES, ICT Manager (Ag.) CARICOM IMPACS Speaker
  (30 min + 15 min for discussion) - TBC

- Topic: CARICOM Secretariat
  Speaker: Jennifer BRITTON, Deputy Programme Manager – ICT4D,
  CARICOM Secretariat (30 min + 15 min for discussion)

- Topic: How to balance police powers with the need to protect privacy in legislation
  Speaker: Normand WONG, Counsel, Criminal Law Policy, Department of Justice,
  Canada (20 min + 10 min for discussion)

- Topic: How to deal with jurisdiction-related issues when the police need to obtain data that is located in a foreign jurisdiction
  Speaker: Normand WONG, Counsel, Criminal Law Policy, Department of Justice,
  Canada (20 min + 10 min for discussion)

Conclusions: Ingredients for success.
Speaker:Wayne M. CAINES, Minister of National Security, Bermuda (15 min)

THURSDAY, 7 DECEMBER

WORKSHOP SESSIONS	ROOM 1 (English/Spanish)

09h15 - 13h00.

(Coffee break between) 10h45-11h15.

WORKSHOP 7:
OAS/USDoJ: Procedural and Substantive Laws: how courts evaluate admissibility of digital evidence
What are the laws that can help prosecuting cybercrime? What are the international agreements and requirements needed to request evidence from other countries? This workshop will aim to address the aforementioned questions and the existing challenges for law enforcement and prosecutors when presenting electronic evidence to a judge. Furthermore, the workshop will also discuss the need for a harmonization and update of criminal laws against cybercrime in order to facilitate admissibility of digital evidence in courts.

Moderator/s: Rodolfo ORJALES, USDoJ;

Rapporteur: Laura MARTINEZ, OAS;

- Topic: International Cooperation: The Formal (bi-lateral treaties) and informal ways to obtain digital evidence in the United States
  Speaker: Rodolfo ORJALES, Department of Justice, Computer Crime Section
  (60 min + 30 min for discussion)

- Topic: Procedural Laws
  Speaker: Marcos SALT, Professor, University of Buenos Aires, Faculty of Law
  (60 min + 30 min for discussion)

Conclusions: Ingredients for success.
Speaker:Rodolfo ORJALES, USDoJ (15 min)

WORKSHOP SESSIONS	ROOM 2 (English/Spanish)

09h15 - 13h00.

(Coffee break between) 10h45-11h15.

WORKSHOP 8:
International community in the fight against cybercrime (Part 2)
In accordance with different worldwide sources, cybercrime is costing the world economy up to $500bn a year. Notwithstanding, international cooperation between the different international and regional actors as well as with countries with capacity to make the difference, remain, still, dangerously inadequate.

Therefore, the developments of an international and national level call of consciousness are the grounds for effective actions. There is a need is to reassess and renew as much as possible the current international legal frameworks, to offer a forum for broader international discussion expressing an outlook towards increasing and advancing international law-enforcement and judicial cooperation among the national authorities and between international and regional organizations. These developments should consider the influences of the novel and emerging issues in respect of international law-enforcement and judicial cooperation in criminal matters, with recommendations on capacity-building, which should show an equal concern for the situation in countries at different stages of development so as to avoid a chaotic future.

This workshop brings countries with capacity building programmes, international and regional organizations aligned in a congregation of efforts to show the respective covered areas and on how they can bring benefits to the countries that need their support.

Moderator/s: Francisco NEIRA BASSO, Council of Europe;
Rapporteur: Esther AGELAN, Judge of the Supreme Court of Dominican Republic, Santo Domingo;

- Topic: Global Programme on Cybercrime of the United Nations Office of Drugs and Crime (UNODC), video presentation.
  Speaker: Neil WALSH, Head of UNODC Global Programme on Cybercrime, Vienna, Austria and Bertha Nayelly LOYA MARIM, Deputy Head of Office for UNODC in El Salvador (15 min)

- Topic: RSS Digital Forensics Lab
  Speaker: Candacy MAYNARD, Lab Manager, Regional Security System (RSS)
  (30 mim + 15 min for discussion)

- Topic: The GLACY+ Project of the Council of Europe (Global Action on Cybercrime Extended) (30 min + 15 min for discussion)
  Speaker: Manuel DE ALMEIDA PEREIRA, Project Manager GLACY+, Council of Europe (TBD)

- Topic: Cyber Capacity Building by the GFCE: Putting principles into practice
  Speaker: Wouter VENSTRA, Deputy Head, Global Forum on Cyber Expertise (GFCE), Secretariat (30 min + 15 min for discussion)

Conclusions: Ingredients for success.
Speaker:Francisco NEIRA BASSO, Council of Europe (15 min)

13h00 – 14h00. LUNCH BREAK

PLENARY SESSIONS ROOM1 (LANGUAGES: ENGLISH/FRENCH/SPANISH/PORTUGUESE)

14h00 – 17h00.

(Coffee break between)
16h00-16h15.

Results of workshops (15 minutes each rapporteur – 120 minutes)

WS 1: COUNCIL OF EUROPE: Developing a cyber-strategy for LATAM Countries; features provided by the Budapest Convention and Capacity building on Cybercrime. (Rapporteur: Daniela DUPUY).

WS 2: INTERPOL: Interpol's role in international police cooperation and coordination with private sector. (Rapporteur: Dong Uk KIM).

WS 3: INTERPOL: Capacity building and obligatory certification of police officers in digital evidence and cybercrime investigations. (Rapporteur: Dong Uk KIM).

WS 4: OAS/USDoJ: TOR, The Dark Web and Bitcoin: The Technical Background needed and an Example of a Successful Investigation and Prosecution. (Rapporteur: Laura MARTINEZ).

WS 5: COUNCIL OF EUROPE: Access to evidence in the Cloud. (Rapporteur: Betty SHAVE).

WS 6: International Community in the fight against Cybercrime (Part 1):
Rapporteur: Cesar MOLINE).

WS 7: OAS/USDoJ: OAS/USDoJ: Procedural and Substantive Laws: how courts evaluate admissibility of digital evidence. (Rapporteur: Laura MARTINEZ).

WS 8: International Community in the fight against Cybercrime (Part 2):
(Rapporteur: Esther AGELAN).

Final remarks and way forward (COE, OAS, CARICOM IMPACS, CARICOM Secretariat, INTERPOL, USA, Canada and European Union) – 5 minutes each

CLOSING CEREMONY: Government of Dominican Republic (15 minutes)

17h00. END OF CONFERENCE

WITH THE SUPPORT OF:

GFCE Global Forum on Cyber Expertise

Canada

COMUNIDAD DE POLICÍAS DE AMÉRICA AMERIPOL

IMPLEMENTATION AGENCY FOR CRIME AND SECURITY IMPACS

INTERPOL

CARICOM