Minute
Technical Meeting on Cybercrime of the Latin America and the Caribbean Crime Victimization Survey Initiative (LACSI)

Virtual Meeting
2 & 4 September 2020

Background

The *Technical Meeting on Cybercrime of the Latin America and the Caribbean Crime Victimization Survey Initiative (LACSI)* is organized by the Center of Excellence for Statistical Information on Government, Crime, Victimization and Justice (CoE), a joint project of the United Nations Office on Drugs and Crime (UNODC) and the National Institute of Statistics and Geography (INEGI) of Mexico.

UNODC, through the CoE, provides technical support for the implementation of Crime Victimization Surveys in the Latin American and Caribbean Region since 2013. These statistical projects are an important source of information for the report of the Sustainable Development Goals of the United Nations Agenda 2030. The LACSI Initiative promotes the use of a common methodology through an approved regional questionnaire (available in 4 languages: Spanish, English, French and Portuguese) in line with international standards. This Initiative is led by the UNODC and the CoE, and has the support of the Inter-American Development Bank (IDB), the Organization of American States (OAS) and the United Nations Development Programme (UNDP). The member countries of the Working Group have contributed to the construction of this regional instrument: Argentina, Belize, Chile, Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Haiti, Mexico, Panama and Peru.

The new cybercrime module is an effort to measure increasingly relevant criminal phenomena in the region. It was developed in 2019 and was presented at the 7th Technical Meeting of the Working Group of the LACSI Initiative in October 2019. As a result of this 7th Technical Meeting, it was agreed to further discuss the proposed module at a specialized meeting on cybercrime in the first half of 2020. Due to the global contingency situation for COVID-19, the Technical Meeting on Cybercrime, initially planned for April 2020 in the city of Santo Domingo, was postponed to September 2020 and was held virtually (for the agenda, see Annex 1).

An improved version of the Module (Version 04 August 2020) has been produced and circulated during the Technical Meeting on Cybercrime to receive comments from participants.

Objective of the technical meeting:

To understand the global, regional and national conceptual and policy overview of cybercrime with the aim of defining what behaviours should be measured through a household survey. This discussion, between experts from the National Statistics Offices and the Criminal Justice System Authorities of the member countries of the LACSI Initiative Working Group, as well as experts from other countries and international and regional organizations, is aimed at providing improvements to the Module on Cybercrime (Version 04 August 2020) of the aforementioned Initiative. The specific objectives were:

A. To briefly present the LACSI Initiative to the participants.
B. To share the knowledge of experts on the subject of cybercrime.
C. To present the international legal framework on the subject.
D. Present experiences in measuring cybercrime (Mexico, Peru, Saint Lucia)
E. Discuss the proposed Cybercrime Module (Version 04 August 2020) with participants to reach consensus.

A total of 35 people from the National Statistics Offices and the Criminal Justice System of Argentina, Colombia, Mexico, Peru, the Dominican Republic and Saint Lucia participated in this technical meeting; on behalf of the United Nations, the United Nations Office on Drugs and Crime (UNODC), the Economic Commission for Latin America and the Caribbean (ECLAC) and the United Nations Development Programme (UNDP) were present. The Inter-American Development Bank (IDB) and the Organization of American States (OAS) also took part in the meeting, as well as two international experts from the Cybercrime Research Institute and the Universistat Abat Oliba CEU (for the list of participants, see Annex 2).

A. Welcome & walk through

- *Mr. Enrico Bisogno, Chief of the Data Development and Dissemination Section, UNODC HQ*

  Mr. Bisogno welcomed the meeting participants and spoke about UNODC's activities in supporting Member States in their fight against cybercrime.
- *Ms. Salomé Flores, Coordinator of the Center of Excellence, UNODC Mexico*

  Ms. Flores presented the LACSI Initiative and spoke about the objectives of the meeting and the reasons why it is important to measure cybercrime.

B. Understanding cybercrime

- *Mr. Marco Gercke, Director of the Cybercrime Research Institute, Germany*

Mr. Gercke spoke of cybercrime as a crime that is an integral part of the daily lives of individuals and businesses and stressed that it is a constantly changing crime. He also said that cybercrime is not new, that it has been in our lives since the internet was invented, but that it has recently been considered a crucial issue. For further reference to the challenges related to this crime and the legal response, he provided the link to a study carried out in conjunction with the International Telecommunications Union: https://bit.ly/3382rah

- *Mr. José Ramón Agustina, Professor of Criminal Law and Criminology at Universitat Abat Oliba CEU, Spain*

From an academic perspective, Mr. Agustina indicated that there are six different approaches to understanding cybercrime and addressing its challenges. He also spoke of the hidden figure, the fallacies related to cybercrime and the importance of naming, measuring and classifying it. He also stressed that we now live in a dichotomy, a hybrid reality between physical space and virtual space. The dangerous thing about cyberspace is that it has no frontiers and that people do not take their safety in the world of the internet seriously. Finally, he highlighted the great challenge of the legal component and the lack of coordination between countries because cyberspace does not respect borders. For a better understanding, the expert provided a link where it is possible to find his publications on the subject: https://bit.ly/2R5gEPA

C. Internacional context

- *Ms. Nayelly Loya Marín, Global Programme on Cybercrime Coordinator, UNODC Office for Central America and the Caribbean (ROPAN)*

Ms. Loya spoke about the Global Programme on Cybercrime, its objective and global and regional scope. In addition, she indicated that there is still no internationally agreed definition of cybercrime, and that there is no UN Convention on the subject. She addressed the international perspective, explaining what is happening in cyberspace and what is being done to contrast this phenomenon. She also spoke about the activities being carried out in the region to combat this crime, about the Cybercrime Repository available to the public, as well as the opportunity to take a free online course of 14 modules available in English and Spanish (limited to certain modules). She closed her presentation by highlighting the classification that UNODC identifies through the Comprehensive Study on Cybercrime (UNODC, 2013).

D. Proposal for a module on cybercrime measurement for the LACSI Initiative

- Ms. Luisa Sánchez, Crime and Criminal Justice Researcher, Center of Excellence, UNODC Mexico

In this session the context of the Module within the LACSI Initiative and how UNODC classifies cybercrime in its International Classification of Crime for Statistical Purposes (ICCS) were discussed and presented. The digital security gap and the cybercrime included in the LACSI Initiative (cyberbullying, malware, email hacking, social media hacking, ransomware) were discussed in addition to presenting the structure of the Module, specifying the questions included for each crime included.

E. Country experiences on measuring cybercrime

In this session, countries with experience in measuring cybercrime presented their practice to the other participants:

- Saint Lucia: Saint Lucia National Crime Victimization Survey
  - Ms. Linn Lelia Brown, Statistician, Central Statistical Office (CSO)

- Mexico: Cyberbullying Module (MOCIBA)
  - Mr. Mario Santillana, National Institute of Statistics and Geography (INEGI)

- Perú: High Tech Crime Investigation
  - Ms. Cinthya Cárdenas Rondón, National Police of Peru (PNP)

F. Plenary discussion about the module proposal on cybercrime measurement of the LACSI Initiative

The CoE presented the following trigger questions on the conceptualisation of cybercrime included in the questionnaire, the methodological proposal contained in the module's questionnaire and the steps to be followed for its collection in the future. These questions are part of the *Format for SESSION 2: Plenary discussion about the module proposal on cybercrime measurement of the LACSI Initiative* (see Annex 3). They were addressed to the participants, with the aim of improving the Cybercrime Module (version 04 August 2020). This format was sent to participants prior to the start of the meeting and addresses the following issues:

- TOPIC 1: Module structure and methodology
- TOPIC 2: Types of cybercrimes to be measured
- TOPIC 3: Inclusion of context specific questions on cybercrime

Due to the comments received on the first day of discussions, the order in which the trigger questions were addressed during session 2 was changed.

1. **TOPIC 3: 3.1. Not all countries criminalize cybercrime / technology supported crimes. Could you tell us what types of cybercrime are criminalized in your country?**
   - Due to time contraints, the focus was put on the progress made by other international organisations on the topic. For example, the Latin American and Caribbean Cybersecurity Reports produced by the IDB and the OAS in 2016 (https://bit.ly/35ieEfl) and 2020 (https://bit.ly/2R81cTa) assess the risks faced by countries in the region and the capacities of states and societies to deal with cybercrime. The experiences of the countries in terms of the classification of cybercrimes will be compiled from the formats that the participants will send to the CoE, the Technical Secretary of the LACSI Initiative.

2. **TOPIC 2: 2.1 Do you have any suggestions or comments on the crimes already included in the module proposal?**
   Among the five behaviours that have already been piloted in the questionnaire of the Saint Lucia National Crime Victimization Survey (SLNCVS) are: cyberbullying, malware, email hacking, social media hacking and ransomware. Comments were received regarding some specific cybercrimes.
   - Cyberbullying definition: *"Someone sent or posted online and visible to others some text, image or video that was intended to embarrass or offend you personally, to hurt your feelings or cause some other emotional distress Exclude threatening or aggressive messages where you were the only recipient"*

Colombia (DANE) and UNODC ROPAN commented that, in order for there to be cyberbullying, and thus harm to the victim, it is not necessary for the act to be "visible to others".

- Hacking definition (Email/Social media): "*Someone gained access to your online email account(s) without your permission, and resulted in your contacts (e.g. friends/family) receiving an email from you that you didn't send.*" "*Someone gained access to your online social account(s) without your permission such as Facebook, Twitter, Instagram, LinkedIn, etc. and resulted in any messages or posts being made from your social media account(s) that you did not yourself send.*"
  Colombia (DANE) indicated that hacking can include additional means to those proposed such as blogs and social network accounts of a business nature. The CoE clarified that it is important to differentiate between personal accounts and institutional or corporate accounts because the border between both types of accounts delimits different behaviours (victimisation of individuals versus business victimisation). This point is linked to a discussion held the previous day about the limitations of a crime victimization survey, which conventionally collects information only among people of 18 years old and over, in order to capture all criminal behaviours carried out through digital means. On that occasion it was noted that many times children and teenagers are victims of cybercrime and that measurements that include their experiences are required.

3. **TOPIC 2: 2.2 Do you consider essential the inclusion of other types of cybercrimes? The following crimes were proposed:**
   - Impersonation: *"creation of a false profile, but with the identity of another person who is intended to impersonate." and Identity theft: "It occurs when the person impersonating the identity does so by having stolen the person's Internet access data and social networks".*
     The Dominican Republic (Ministry of Interior and Police and ONE), Peru (INEI) and Colombia (DANE) were in favour of including these two crimes in the new version of the Module. To avoid misunderstandings, Colombia and Peru suggested revising the two definitions so that they are mutually exclusive and understandable. UNDP stressed that in these two crimes it is crucial to investigate the relationship with the offender, as in the two cybercrimes the impact on victims can be very different.
   - Fake news: *"They are a form of news consisting of deliberate disinformation or hoaxes spread via traditional news media or online social media. The news is then often reverberated as misinformation in social media but occasionally finds its way to the mainstream media as well.* ***Fake news is written and published usually with the intent to mislead in order to damage an agency, entity, or person, and/or gain financially or politically, often using sensationalist, dishonest, or outright***

fabricated headlines to increase readership. *By presenting false facts as if they were real, they are seen as a threat to the credibility of serious media and professional journalists, as well as a challenge to the public receiver".*

IDB stressed that fake news affect the whole population and their measurement would not be accurate. Moreover, there is no direct relationship between perpetrator and victim. UNDP recognized the complexity of this topic as it is challenging to distinguish whether the victim is the individual or the person as part of an organized group or a country. ECLAC agreed that we are all victims of fake news and added that there is also a problem in defining the concept since, possibly, all news has a false component and a true component. ECLAC representative suggested focusing on the intentionality of deceiving with a false news item.

Colombia (DANE) stressed that fake news is not a personal crime, but it could be investigated by the occurrence or the perception that people have about the occurrence of this and its impact. The Dominican Republic (ONE) also indicated that it is a crime that is very difficult to measure and delimit.

Considering the interest in this topic, it was proposed to measure it in another section of the LACSI questionnaire (for example, in section B of Perception, to obtain a measurement of the perception of this phenomenon or to measure its impact on those who were exposed to fake news).

UNODC ROPAN stressed the importance of distinguishing and using the terms "misinformation" - without intent to deceive - and "disinformation" - as a deliberate act of disinformation.

- Grooming: The Dominican Republic (Ministry of Interior and Police) expressed interest in including this crime. The challenge of measuring it was stressed considering that international recommendations suggest to interview respondents of 18 years and over in a crime victimization survey. With this methodological challenge, the respondents who are most vulnerable to this type of crime would be excluded from the measurement. In the case of Colombia (DANE), it was indicated that this problem would not exist, since the target population of its crime victimization survey is people aged 15 years and older.
- Phishing: The Dominican Republic (Ministry of Interior and Police) expressed interest in including this crime. Colombia (DANE) agreed to include phishing. Peru (INEI) suggested a revision of the definition of phishing, to avoid misunderstandings. The CoE stressed that both grooming and phishing are a type of modus operandi for achieving a crime, through deception. Therefore, a question could be included to ask how the victim was tricked into falling for any of the crimes measured in the module.
- Sextortion: *"A form of blackmail in which sexual information or images are used to extort sexual favors from the victim. Social media and text messages are often the source of the sexual material and the threatened means of sharing it with others. An example of*

this type of sextortion is where people are extorted with a nude image of themselves they shared on the Internet through sexting."

The Dominican Republic (Ministry of Interior and Police) expressed interest in including this crime.

- Additional comments:

  Colombia (DANE) and UNDP reminded that it is necessary not to lose sight of the length of the Module, which is part of an already considerably long questionnaire. The Dominican Republic (ONE) stressed that these numerous definitions increase the complexity and challenges for the training and coaching of staff involved in data collection. To solve this problem of length, the Dominican Republic (Ministry of Interior and Police) suggests dividing the modules according to age group to focus on measuring the main groups affected by each cybercrime.

4. **TOPIC 1: 1.1 Do you think that this cybercrime module should be included as a core or annex crime within the LACSI questionnaire? And why?**
   - In favour of it being a core crime: UNODC ROPAN agrees that this Module should be parto f the core questionnaire within the LACSI Initiative as the results could feed into the discussions that will be initiated and maintained in the United Nations convention on the misuse of Information and Communication Technologies (ICT). The Dominican Republic (Ministry of Interior and Police and NSOs) recalled that it is important to have data to create a law for the prosecution of cybercrimes. It is important to have a way to foster a common classification, to facilitate international cooperation. The OAS stressed the importance of making this topic visible and beginning to collect data on cybercrime.
   - In favour of it being an annex crime: Peru (INEI) expressed its reservation that this Module be part of the core questionnaire of the LACSI Initiative since the legislation of each country is variable. UNDP suggests that although ideally this Module should be parto f the core questionnaire, its inclusion should be at the discretion of countries to encourage better resource allocation according to internal information priorities. Colombia (DANE) stressed that, considering the list of crimes already considered as core in the LACSI Initiative and the additional burden that the inclusion of the Module could mean, it would be important to keep it as discretionary for each country. However, the importance and relevance that cybercrime has taken on in recent years and more recently during the COVID-19 pandemic must be recognised. The DANE representative also proposed reaching an agreement that it should be a core crime, but that the cybercrimes to be included could be evaluated.

5. **TOPIC 1: 1.2 Do you have any comments, for example, on the structure of the module, the formulation of the questions or the Language used, among others?**

- Colombia (DANE) presented very detailed comments regarding the structure of the Module. The DANE representative mentioned some of them (such as, for example, the importance of adding the technological device from which the crime occurred; the open questions included in the module could represent a challenge when it comes to systemizing the information; the inclusion of an initial filter question to verify that the informant has connected to the internet for personal reasons; establishing a list of damages in case of malware; the DANE representative suggested that the concept of health included in the questions should explicitly mention that it encompasses both physical and mental health, among others). These comments will be sent by mail to the Technical Secretary of the LACSI Initiative, the CoE.
- UNDP agreed with Colombia's comments (DANE) regarding possible victimization of the informant by more than one cybercrime. It was also suggested to inquire about the devices where the victimization occurred in the last 12 months. It was also suggested to include a measurement of the economic impact and also on the confidence in the authorities in charge of mitigating this impact.
- Dominican Republic (Ministry of Interior and Police) asked about technical assistance and training in case a country decides to pilot and implement this Module.
- UNODC ROPAN stressed that the responsibility of private companies working in cyberspace must be considered, in addition to the responsibility of the authorities, in pursuing these cybercrimes. This should be reflected in the Module.

6. **TOPIC 3: 3.2 Being a victim of a cybercrime can have several impact on the victim's habits and it is considered essential to measure this. Do you think that measuring the changes in the informant's habits should be included? If so, where in the LACSI questionnaire?**

- Colombia (DANE), Dominican Republic (Ministry of Interior and Police) and UNDP expressed interest in measuring the effects of cybercrime on people's lives within the Module. It was stressed that, in the case of cyber-crime, there could be effects/consequences in the frequentation of websites, in the use of devices, in the handling of passwords, for example. It is proposed to include this measurement before that of the effects on physical and psychological health, to avoid possible biases.
- OAS indicated that it would be important to know if from cases of cyberbullying, malware, hacking or ransomware, the person changed his/her behaviour. This could be asked in the questions for ALL cybercrime section or discussed if the question should be asked for any particular situation. For example, in the case of cyberbullying, the person could have decided to stop posting comments or photos, or stop using social networks.

Agreements

Ms. Flores, the Coordinator of the Centre of Excellence summarized the main agreements resulting from the discussion among the participants of the two days of the technical meeting:

- Definition of cyberbullying: Both cyberbullying visible and invisible to other people should be included in the concept.
- Definition of social media hacking: It was agreed to include blogs as a social media that could be hacked, although the initial proposal to keep the hacking of personal accounts and institutional and/or corporate social network accounts separate was maintained.
- Definitions of impersonation and identity theft: it was suggested that these definitions be improved to make them clearer and mutually exclusive.
- Fake news: it was agreed not to include it as a crime, due to its complexity in measuring the extent of its occurrence, but the importance of the issue is noted. A question will be generated in Section B of Perception of the LACSI Initiative, considering the difference between the concepts of "misinformation" and "disinformation". There will be an attempt to use an as neutral definition as possible, although the challenge of separating the concept of fake news from its political meaning/association is acknowledged. There will also be an attempt to identify areas or sectors to which this news is linked and to identify the means by which these types of news are received.
- Core or annex crime: Most participants noted that this Module could be annex within the LACSI Initiative. However, the CoE will seek to promote this tool with the countries of the region.
- Crimes to be included: in order to give countries the opportunity to meet their internal need of information and also allocate resources in an efficient way, the decision on the number and type of cybercrimes to be measured will be left to the discretion of the countries.
- Structure and methodology of the Module: the Technical Secretariat of the LACSI Initiative, the CoE, will implement the very specific comments received during the discussions: in particular, answer options will be adjusted to have a broad concept of the health effects of cybercrime (including mental health), and it will be taken into account that the reporting of these behaviours is often made to companies that provide technological services and not to the authority.
- Evident demand to extend this work of measuring cybercrime: from the two days of work, the importance of making a particular design for the population that is a victim of cybercrime but that is not usually part of the target population of a victimization survey of people: children and companies. The CoE committed itself to look for potential partner agencies with experience of working with these target populations (e.g. business

chambers or the United Nations Children's Fund - UNICEF). The opportunity of suggesting the participation of other institutions or potential partners remains open to meeting participants.

Follow-up

- Participants committed to review the new module proposal (Version 04 August 2020) and send comments/observations (Annex 3: Template for SESSION 2: Discussion on the LACSI Initiative's module proposal on measuring cybercrime) by September 30th.
- The CoE will take into account the comments received and apply them to generate a new version of the Module that will be ready at the end of October.
- The CoE, as Technical Secretary of the LACSI Initiative, will share the new version of the Cybercrime Module with participants at the end of October for final approval. In case no comments are received, a silent approval will take place.
- The CoE will publish the new version of the Module on its website, in the four languages of the LACSI Initiative (English, Spanish, French and Portuguese).
- The CoE will organize the 8th Technical Meeting of the LACSI Initiative Working Group in November 2020. The meeting will be held virtually. At this meeting, in addition to officially approving the module within the LACSI Initiative, other proposals in the fields related to the disease by COVID-19 and experimental measurements of criminal incidence will be added.
- Countries that would like to pilot the cybercrime module can contact the CoE at unodc-mexico.cde.estadistica@un.org
- Countries requiring technical assistance to implement the Cybercrime Module may contact the CoE and make a formal request at: unodc-mexico.cde.estadistica@un.org

Annex 1

AGENDA

Technical Meeting on Cybercrime of the
Latin America and the Caribbean Crime Victimization Survey Initiative (LACSI)

2 & 4 September 2020
Virtual meeting

SESSION 1: Wednesday, 2 September 2020

9:00 – 11:30 hrs MEX/PANAMA | 10:00 – 12:30 hrs NYC/CARACAS | 11:00 – 13:30 hrs BUENOS AIRES

08:15 – 09:00	**Event platform: https://portal-v3.voiceboxer.com/account/login (simultaneous translation available)**
09:00 – 09:30	**Welcome & walk through** • Enrico Bisogno, Chief of the Data Development and Dissemination Section, UNODC HQ • Ms. Salomé Flores, Coordinator of the Center of Excellence, UNODC Mexico • Background & meeting objectives • Dynamics of the technical meeting • Introduction of participants
9:30 – 10:15	**Understanding cybercrime** **Moderates:** Enrico Bisogno, Data Development and Dissemination Section, UNODC HQ • Cybercrime Research Institute (15 min) ○ Mr. Marco Gercke, Director, Germany *Q&A (5 min)* • Universitat Abat Oliba CEU (15 min) ○ Mr. José Ramón Agustina, Professor, Spain *Q&A (5 min)*
10:15 – 10:25	**Break**
10:25 – 10:45	**International context** • Global Programme on Cybercrime (15 min) ○ Ms. Nayelly Loya Marín, Global Programme on Cybercrime Coordinator, UNODC Panama *Q&A (5 min)*
10:45 – 11:00	**Proposal for a module on cybercrime measurement for the LACSI Initiative** **Presents:** Ms. Luisa Sánchez, Center of Excellence, UNODC Mexico (15 min) • Information needs in the Latin America and the Caribbean region • Review of the module structure and how it complements the measurement of other crimes included in the LACSI Initiative (bank fraud, threats, extortion) *Q&A (10 min)*
11:00 – 11:10	**Break**
11:10 – 12:00	**Country experiences on measuring cybercrime**

	Moderates: Ms. Salomé Flores, Coordinator of the Center of Excellence, UNODC Mexico • Saint Lucia: Saint Lucia National Crime Victimization Survey – module on cybercrime results (15 min) ○ Ms. Linn Lelia Brown, Statistician, Central Statistical Office (CSO) • Mexico: Cyberbullying Module (MOCIBA) (15 min) ○ Mr. Mario Santillana, National Institute of Statistics and Geography (INEGI) • Perú: High Tech Crime Investigation (15 min) ○ Ms. Cinthya Cárdenas Rondón, National Police of Peru (PNP) ***Q&A (10 min)*** **ON PREPARATION FOR SESSION 2:** • Based on the presentations of the experts and the countries' experiences, reflect and assess the proposed module on cybercrime using the discussion format (documents sent by email on Monday, August 31). • **Reflections and comments will be discussed in session 2.**

SESSION 2: Friday, 4 September 2020

9:00 – 11:30 hrs MEX/PANAMA | 10:00 – 12:30 hrs NYC/CARACAS | 11:00 – 13:30 hrs BUENOS AIRES

08:15 – 09:00	**Event platform: https://portal-v3.voiceboxer.com/account/login (simultaneous translation available)**
9:00 – 10:30	**Plenary discussion about the module proposal on cybercrime measurement of the LACSI Initiative** **Moderates:** Ms. Luisa Sánchez, Center of Excellence, UNODC Mexico • Participants comments about the UNODC proposal related to: ○ Structure and methodology of the module ○ Types of cybercrimes to be measured ○ Inclusion of cybercrime context-specific questions
10:30 – 10:45	**Break**
10:45 – 11:15	**Technical Meeting agreements** **Moderates:** Ms. Salomé Flores, Coordinator of the Center of Excellence, UNODC Mexico • Topics that the module will cover • Countries volunteering for module pilot test
11:15 – 11:30	**Technical Meeting closure** • Next steps of the LACSI Initiative • Closure

More information:

- *Latin America and the Caribbean Crime Victimization Survey Initiative (LACSI)*
- LACSI Initiative Conceptual Framework (English) (Spanish)
- Meeting minute of the 7th LACSI Technical Meeting – October 22 and 23, 2020 | Mexico City (English) (Spanish)
- VicLab talks (recorded in English and Spanish, subtitles available)

Annex 2

List of participants

N°	Country	Participant	E-mail	Institution	Position
1	Argentina	Horacio Azzolin	HAzzolin@mpf.gov.ar	Ministerio Público Fiscal (Unidad Especializada en Ciberdelincuencia)	Fiscal de la Procuración General de la Nación
2	Colombia	Diana Carolina Peña	dcpenab@dane.gov.co	DANE	Coordinadora GIT Capital Social
3	Colombia	Horacio Coral Díaz	hcorald@dane.gov.co	DANE	Asesor
4	Colombia	Rodrigo Javier Acevedo Nieto	rodrigo.acevedo6500@correo.policia.gov.co	Policía Nacional de Colombia (Dirección de Investigación Criminal e Interpol - DIJIN)	Mayor en el Centro Cibernético Policial de la Dirección de Investigación Criminal e INTERPOL
5	Mexico	Mario Santillana	alberto.santillana@inegi.org.mx	INEGI	Director General Adjunto de Modelos de Información Gubernamental y Encuestas Nacionales de Gobierno, Victimización Seguridad y Justicia
6	Peru	Aníbal Sánchez Aguilar	anibal.sanchez@inei.gob.pe	INEI	Subjefe de Estadística
7	Peru	Juan Trejo	Juan.Trejo@inei.gob.pe	INEI	
8	Peru	Cinthya Julissa Cárdenas Rondón	cjjcinthya@gmail.com	Policía Nacional del Perú (PNP)	Capitán en la División de Investigación de Delitos de Alta Tecnología de la Dirección de Investigación Criminal
9	Peru	Luis Alberto Loayza Ramírez	lloayzar@gmail.com	Policía Nacional del Perú (PNP)	Jefe de la División de Estadística de la dirección de Tecnologías de la Información y Comunicaciones (DIRTIC)
10	Peru	Marco Antonio Vilchez Asenjo	vilchezasenjo@gmail.com	Policía Nacional del Perú (PNP)	Jefe del Dpto de Análisis de la DIVEST DIRTIC
11	Peru	Roger Chipa Sierra	rogerchipa@gmail.com	Policía Nacional del Perú (PNP)	Jefe del Dpto de Procesamiento de la DIVEST
12	Dominican Republic	Dangela Ramirez	dramirezg@mip.gob.do	Ministerio de Interior y Policía	Directora de asuntos internos

13	Dominican Republic	Maridalia Rodríguez	maridalia.rodriguez@one.gob.do	ONE	Encargada del departamento de Articulación Sectorial del SisTOPIC Estadístico Nacional
14	Dominican Republic	Ivan Féliz Vargas	ifeliz@pgr.gob.do	Procuraduría General de la República	Procurador General de Corte de Apelación, Titular de la Procuraduría Especializada para Delitos de Alta Tecnología
15	Saint Lucia	Linn Lelia Brown	linn.brown@govt.lc	Central Statistical Office (CSO)	Statistician (Demography)
16	(CDMX)	Salomé Flores	salome.flores@un.org	CoE	Oficial Nacional de Programas
17	(CDMX)	Luisa Sánchez	luisa.sanchez@un.org	CoE	Investigadora en Delincuencia y Justicia Penal
18	(CDMX)	Giada Greco	giada.greco@un.org	CoE	Técnico en Estadísticas Delictivas
19	(CDMX)	Javier Tun	javier.tunchim@un.org	CoE	Especialista en gestión del conocimiento
20	(CDMX)	Héctor Duarte	hector.duerte@un.org	CoE	Especialista de estadísticas delictivas
21	(CDMX)	Justo Rojas	rojasjusto@gmail.com	CoE	Asistente técnico en estadísticas delictivas
22	(CDMX)	Víctor Merchand	victor.merchand@un.org	UNODC	Specialist Information Technology Strategies
23	(Washington)	Ariel Nowersztern	ARIELN@IADB.ORG	IDB	Especialista en Ciberseguridad
24	(Washington)	José Antonio Mejía	JoseAM@IADB.ORG	IDB	Modernisation of the State Lead Specialist
25	(Chile)	Xavier Mancero	xavier.mancero@cepal.org	ECLAC	Senior statistician
26	(Chile)	Pablo VIllatoro	pablo.villatoro@cepal.org	ECLAC	Senior statistics assistan
27	(Washington)	Kerry-Ann Barrett	KABarrett@oas.org	OAS	Cybersecurity Policy Specialist
28	(Washington)	Karen Bozicovich	KBozicovich@oas.org	OAS	Chief of the Public Security Information and Knowledge Section
29	(Panama)	Marcela Smutt	marcela.smutt@undp.org	UNDP	Chief Technical Specialist
30		Pablo Gordillo	juan.gordillo@undp.org	UNDP	Project Coordinator
31	(El Salvador)	Nayelly Loya Marín	bertha.loya@un.org	UNODC	Cybercrime Programme Coordinator

32	(Spain, Barcelona)	José Agustina	jagustinas@uao.es	Universitat Abat Oliba CEU	Catedrático de Derecho penal y Criminología
33	(Vienna)	Enrico Bisogno	enrico.bisogno@un.org	UNODC HQ	Chief of Data Development Unit
34	(Vienna)	Fatma Ismetova Usheva	fatma.usheva@un.org	UNODC HQ	Data Analyst
35	(Germany, Cologne)	Marco Gercke	gercke@cybercrime.de	Cybercrime Research Institute (CRI)	Director

Annex 3

Format for SESSION 2: Plenary discussion about the module proposal on cybercrime measurement of the LACSI Initiative (Friday, September 4, 2020)

Participant's name and surname:

Institution / Country:

The topics to discuss during the session will be the following. For each topic, you can add any other question that you consider pertinent to discuss in the Working Group:

TOPIC 1: Module structure and methodology

1.1. Do you think that this cybercrime module should be included as a *core crime* or *annex crime* within the LACSI questionnaire? Yes/No and why? ***Core crime:*** those crimes that are considered a priority to be measured (and that, when adopting the LACSI Initiative, each country will have to measure) ***Annex crime:*** those crimes whose inclusion is totally discretionary and depends a lot on the reality of the countries and the resources allocated to carrying out the survey
Insert your answer here:

1.2. Do you have any comments, for example, on the structure of the module, the formulation of the questions or the language used, among others? Please indicate the corresponding question number in the module and your specific proposal.
Insert your answer here:

TOPIC 2: Types of cybercrimes to be measured

2.1. Do you have any suggestions or comments on the crimes already included in the module proposal?
Insert your answer here:

2.2. In the cybercrime world, there are other cybercrimes that could be included in the module, such as: Impersonation / Identity theft, Fake news, Grooming, Sextortion, among others.
Which ones do you consider essential to include and why, considering the regional and country context? In methodological terms, please take into consideration that this module will be included in a household survey, recommended for people aged 18 years and over.

Impersonation: creation of a false profile, but with the identity of another person who is intended to impersonate.
Identity theft: occurs when the person impersonating the identity does so by having stolen the person's Internet access data and social networks.
Fake news: Also known as junk news, pseudo-news, alternative facts, false news or hoax news is a form of news consisting of deliberate disinformation or hoaxes spread via traditional news media (print and broadcast) or online social media. Digital news has brought back and increased the usage of fake news, or yellow journalism. The news is then often reverberated as misinformation in social media but occasionally finds its way to the mainstream media as well. Fake news is written and published usually with the intent to mislead in order to damage an agency, entity, or person, and/or gain financially or politically, often using sensationalist, dishonest, or outright fabricated headlines to increase readership. By presenting false facts as if they were real, they are seen as a threat to the credibility of serious media and professional journalists, as well as a challenge to the public receiver.
Phishing: obtaining confidential information in a fraudulent way where the scammer, known as a phisher, uses social engineering techniques, posing as a trusted person or company in an apparent official electronic communication, usually an email, or some other instant messaging system, social networks, following a malware.
Grooming: a criminal form of harassment that involves an adult who comes into contact with a child or adolescent with the aim of gradually gaining their trust and then engaging them in sexual activity. It is a process in which a bond of trust is created between the victim and the harasser. This tries to isolate the minor little by little, and this is achieved by detaching them from their support network (family, teachers, friends, etc.) and creating an atmosphere of secrecy and intimacy. The abuser sends, through a technological means, sexual material to the boy or girl. In addition, it is usually made to pass as a minor and adapts the language to the age of the victim.
Sextortion: A form of blackmail in which sexual information or images are used to extort sexual favors from the victim. Social media and text messages are often the source of the sexual material and the threatened means of sharing it with others. An example of this type of sextortion is where people are extorted with a nude image of themselves they shared on the Internet through sexting.

Insert your answer here:

TOPICA 3: Inclusion of cybercrime context-specific questions

3.1. Not all countries criminalize cybercrime / technology-supported crimes. Could you tell us what types of cybercrime are criminalized in your country? If that's the case, please indicate the corresponding law(s).

Insert your answer here:

3.2. Being a victim of a cybercrime can have big impact on the victim's habits and it is considered essential to measure it. Do you think that measuring the changes in the informant's habits should be included? If so, where in the LACSI questionnaire?
Insert your answer here:

3.3. Do you have other suggestions? Do you have any other suggestions or additional comments to the module?
Insert your answer here:

Annex 4

Q&As to experts

Mr. José Ramón Agustina, Professor of Criminal Law and Criminology, Universitat Abat Oliba CEU, Spain

1. **(Trad.) "Shouldn't the capacities of the police for searching and investigating cybercrime also be strengthened? I think the issue of cybercrime victimization is important, but I also think it is important to strengthen the administrative record, as well as the capacity to respond and investigate. In this sense, are there special lines for reporting this type of crime in the countries, attended by specialized police personnel? (Ms. Karen Bozicovich / OAS):**

   (Trad.) Yes, in fact, the capacities of the police for recording and investigating cybercrime should also be strengthened. I think it would be very important to encourage the collaboration of researchers and experts from the academic world (specialized in statistics, criminology and cyber security) with police forces. In my country it is not easy, as there is a high level of distrust on the part of the police to let anyone in from outside. In this context of collaboration, multidisciplinary work teams should be created so that records can be used to extract information for police intelligence and, in turn, to carry out well-coordinated criminological investigations in which the profiles of offenders and victims, the dynamics of crime, the assessment of damage, the reaction measures adopted, the vulnerabilities of the victim, etc., are fully known. As I said in my paper, the concept of cybercrime is criminological and covers very different legal forms or figures of crime. Therefore, the register should make it possible to indicate whether ICTs have played an essential role in the commission of the crime, whatever it may be. Likewise, of course, police should be trained and special lines should be set up to report this type of crime. Right now, in the police forces in my country, as far as I know, there are only specialised units for the judicial police, but neither immediate attention to victims nor preventive training in schools is there a quality effort to tackle such an important problem. Without doubt, it is a question of investing many more personnel, economic and material resources.

2. **(Trad.) "What interesting experiences do you know about civic/social education on cybercrime and what to do if you are a victim?" (Ms. Karen Bozicovich / OAS):**

(Trad.) In Spain we have the INCIBE and Is4k (they have online access to materials). There are several important research groups that are working on the criminological analysis of cybercrime, such as CRIMINA, directed by Dr. Fernando Miró. I think there is a need to work much more on the problem from a victimology perspective. In this regard, I am attaching an article that we published in the *Revista Española de Pedagogía*: https://revistadepedagogia.org/lxxvii/no-273/retos-educativos-ante-los-riesgos-emergentes-en-el-ciberespacio-claves-para-una-adecuada-prevencion-de-la-cibervictimizacion-en-menores/101400073259/

3. **(Trad.) "Thank you very much for the excellent presentation. I would like to know if: is there any experience you can share about processes of inter-institutional articulation and interaction (entities that, due to their legal framework, participate in the design and execution of public policies, on cybersecurity) for the identification of demands, generation and exchange of statistical data related to the topic?" (Ms. Maridalia Rordíguez, ONE, Dominican Republic)**

(Trad.) In terms of experiences with inter-institutional collaboration processes in cybersecurity, the general feeling is that, beyond effective measures, there is little coordination in the public sphere. Those who invest in cybersecurity are mainly private companies that see the problem and furthermore have to defend themselves without the State, as it lacks the means. The focus is clearly on prevention and we are all very poorly aware at all levels. I recently participated in a training day for public administrations, as obviously cyber-fraud and cyber-attacks on public bodies are very important. We will soon publish a book with the experiences.

Ms. Nayelly Loya Marín, Global Programme on Cybercrime Coordinator, UNODC Office for Central America and the Caribbean (ROPAN)

1. **(Trad.) "Regarding information and education, are you working with journalists and media (traditional and non-traditional)?" (Ms. Karen Bozicovich / OAS)**

   (Trad.) Yes, with the purpose of educating through them, but also so that they better understand and address the phenomenon. This includes workshops with traditional media, as well as podcasts and in various digital formats.

2. **(Trad.) "Do you have an assessment tool to evaluate/diagnose the capacities of criminal justice systems to prevent/investigate/prosecute cybercrime?" (Ms. Karen Bozicovich / OAS)**

   (Trad.) Yes, in conjunction with the World Bank and other system agencies, a tool was developed that can be accessed here: http://www.combattingcybercrime.org/

3. **"Will there be a schedule of meetings for that group on the new treaty? (Ms. Kerry-Ann Barret / OAS)**

   (Trad.) Due to COVID19, the session has been postponed by the United Nations General Assembly and must now be convened on a date not decided upon before 1 March 2021. It is at this organizational session that Member States will decide how, where and when substantive sessions will be held.