THE SECOND SESSION OF THE AD HOC COMMITTEE TO ELABORATE A COMPREHENSIVE INTERNATIONAL CONVENTION ON COUNTERING THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES FOR CRIMINAL PURPOSES

STATEMENT BY
MRS. ANDREA MARTIN-SWABY
DEPUTY DIRECTOR OF PUBLIC PROSECUTIONS AND HEAD OF JAMAICA'S CYBERCRIMES AND DIGITAL FORENSICS UNIT

ON BEHALF OF
THE CARIBBEAN COMMUNITY
(CARICOM)

AGENDA ITEM 5: GENERAL PROVISIONS

PLENARY (ROOM M-3)

JUNE 6, 2022

Madame Chair,

Jamaica is pleased to deliver this statement on behalf of the 14 member states of the Caribbean Community. CARICOM wishes to thank you and the Secretariat team for the work done thus far during this session of the committee. The questions on General provisions will now be addressed:

1. How can we best ensure a fit for purpose convention considering the diverse range of technological means used to perpetrate the range of offences to be criminalized under this convention?

2. How can we ensure that the convention remains fit for purpose considering future technological developments?

Madame Chair,

It is important that the Convention remains fit for purpose to treat with the constant evolution of crimes involving the use of ICT's. A focus on the core elements of the mischief being addressed should be the focus of the criminalization provisions as opposed to seeking to focus on the current threats within the ICT space.

CARICOM has taken note that over the last two decades the types of threats have been given several titles such as spam, malware, phishing, ransomware, DDOS attacks, smishing etc. The focus of the new instrument should not be to criminalize every known threat according to its classification or title. Several of these offences can be covered under one or more of the core/general

offences. Nevertheless, where it is determined that there is a threat that is unique in nature that cannot be accommodated under any of the categories of the integrity offences, or the scope and effect of the threat is significantly altered by the use of ICT's, we may consider the inclusion of this threat.

However, due to the dynamic nature of the technological era, it would be impossible to criminalize every classified threat. Each country, based on their unique context may include additional offences which are not named in the Convention. Moreover, as is normally the practice, each State can amend their domestic law to ensure it reflects technological advancements concerning ICT crimes.

3. Do you think that a chapter on general provisions, following the same structure as in UNCAC and UNTOC, could be possible for this convention? (In their chapter on general provisions, the two aforementioned conventions contain a provision on "statement of purpose", "use of terms", "scope of application" and "protection of sovereignty"). If not, what provision should be added or removed and why?

CARICOM believes that the Chapter on General Provisions should follow a similar structure as in the UNTOC and UNCAC to maintain consistency in respect of UN instruments.

4. Should the statement of purpose contain more than three main ideas (these being, in broad terms, measures to prevent and

combat [use of ICTs for criminal purposes] [cybercrime], related international cooperation and related technical assistance)? What other elements would Member States be interested in including in the statement of purpose? On which of these additional elements could Member States reach consensus?

CARICOM believes that consideration should be given to including asset recovery within the statement of purpose. However, CARICOM is cognizant that other instruments such as UNTOC and UNCAC included Chapters on Asset recovery although it was not mentioned in the statement of purpose. CARICOM will listen to the views of other member states in this regard.

5. Is a reference to the protection of human rights necessary in the statement of purpose, if an article exclusively on this matter is included in the convention, as proposed by some Member States?

CARICOM is not of the view that the inclusion of language protecting of human rights is necessary in the statement of purpose as the Article titled "Conditions and Safeguards" which is included in the Chapter governing Procedural Measures and Law Enforcement would include human rights safeguards. CARICOM recommended that this article should state as follows;

" *Each State Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Article are subject to conditions and safeguards provided for under its domestic law, which shall provide for the protection of human rights and liberties, including rights arising*

pursuant to obligations it has undertaken under the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments".

CARICOM believes that this is sufficient as the purpose of this Convention is to combat the use of ICT's for criminal purposes. Accordingly, the purpose of this Convention should focus exclusively on elements which are core to the fight against ICTs for criminal purposes. These include measures that prevent and combat cybercrimes.

However, CARICOM accepts and appreciates that in implementing the purposes of this Convention, law enforcement will be given the powers of compelling the expedited preservation of data, the production of data and search and seizure warrants. We acknowledge that the exercise of these powers will be applicable to several offences.

Therefore, it is important that human rights safeguards be introduced into the instrument. CARICOM believes that it is adequate to include these human rights safeguards in the Chapter which addresses Procedural rules and investigative powers. In this Chapter the balance between law enforcement powers and the protection of rights ought to be outlined.

6. Should clauses/articles on electronic evidence be limited to the offences established in the convention? Should the scope of application of the convention take into account the scope of

application defined for procedural measures, and/or for international cooperation?

CARICOM believes that the provisions on electronic evidence should not be limited to the offences established in the Convention. One of the main features of this new instrument will be that the scope of the procedural measures is not restricted to the offences created under the new instrument.

These investigative tools of preservation of data, production of data and search and seizure of computer material will be applicable to any criminal investigation which involves the collection of computer material.

This unique scope and reach of the new instrument should be highlighted in the General Provisions.

In relation to International Cooperation being referred to in the scope of the instrument, CARICOM acknowledges that this issue was not mentioned in the Scope of the UNTOC and UNCAC, although these Conventions each contain a chapter on international cooperation. As such, CARICOM is open to hearing the views of other Member States on this issue.

7. Should the scope of application include a clause on freezing, seizure, confiscation and return of the proceeds of the offences established by the convention, as proposed by some Member States?

Yes Madame Chair, the UNCAC and UNTOC both include references to the freezing, confiscation and return of the proceeds of the offences established by those Conventions. Including this provision in our instrument would preserve consistency in the approach of the United Nations. Further, it would acknowledge a key aspect of transnational organized crime, the tainted proceeds of the criminal conduct.

8. Would the language in articles 4 of UNTOC and UNCAC cover all concerns from Member States with regard to the protection of sovereignty? Are considerations of sovereignty different in the context of the use of ICTs than in other – traditional – contexts?

CARICOM, believes that the language in article 4 of the UNTOC and UNCAC are sufficient in addressing the issue of the respect for sovereignty.

However, CARICOM notes that ICT crimes, by their nature, are transnational organized crimes, which may involve multiple jurisdictions. By its nature, the crime can be committed in one territory and have its impact in another. Victims may be in an entirely different jurisdiction than where the perpetrators may be physically located. In this regard, they are different from traditional offences.

For this reason, the proposed Article on jurisdiction will have to address this issue carefully as was done in the UNTOC (see article 15) and UNCAC (article 42). However, in the General provisions,

what is included in UNTOC and UNCAC is sufficient regarding the outline of the principle of sovereignty.

9. Among the long list of terms proposed for including as definitions under the convention, could you propose a key list of terms that the Ad Hoc Committee has to consider as a priority (in the understanding that a final Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, second session 30 May - 10 June 2022 Page 8 of 12 list would need to be made after a review of the finally agreed provisions, especially on crime types, procedural measures and international cooperation)?

- Child
- Child sexual exploitation/child sexual abuse
- Computer data
- Computer systems
- Confiscation
- Freezing
- Information and Communication Technology systems
- Public Communication networks
- Intercept
- Intimate image
- Proceeds
- Seizure
- Service provider

- Sexual activity
- Subscriber information
- Content Data
- Traffic data

10. Do you think that the AHC has to first define these terms, or that definitions should only be addressed after the substantive articles of the convention are negotiated? What would be the best stage in the negotiating process to discuss definitions in a focused manner?

CARICOM submits that the above-mentioned words and terms should be defined after there is agreement on the substantive provisions of the Convention. It may not be worthwhile to define terms at this stage, as there is no certainty that they will be used in the Convention. After the substantive articles are negotiated, we can proceed to negotiating the definitions of key words and terms that will be used in the Convention.

11. Do Member States wish to consider, at this stage, the differences between "computer systems" and "ICT devices" and their impact on the scope of application of the convention?

Madame chair you have specifically asked what is the difference between "computer system" and "ICT device". CARICOM wishes to highlight that the new instrument will treat with the use of ICT's.

ICT devices encompass a wider range of apparatus than computer devices. The broad terminology of ICT devices not only include computer devices and systems, but also antiquated technologies

such as landline telephones, radio and devices which are used for television broadcast.

The use of the terminology "ICT's" as opposed to "computer devices" will operate to future proof this new Convention since it will encompass radio, television, cellular phones, computer and network hardware and software and anything capable of facilitating communication as well as any device which is capable of automatically processing data.

CARICOM will await further discourse by member states in this regard in assessing the views concerning the extent to which both terms are similar and where they differ.