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 4: PROVISIONS ON CRIMINALIZATION

PLENARY (ROOM M-3)

MAY 31, 2022

Thank you Madame Chair,

CARICOM wishes to highlight the following in relation to the provisions contained in the Chapter on Criminalization. We will respond to the first group of questions posed by you.

1. What kinds of [mental/fault] elements (for example, [malicious/dishonest] intent) should be captured when considering the offences of [illegal/unlawful/unauthorized] access and interception? Should the convention consider putting in place legal protections for cybersecurity researchers and other professionals working in cybersecurity (including, inter alia, penetration testers)?

2. Do you think that any of the proposed conducts must result or be intended to result in a specific or serious harm, or material damage, in order to be considered as an offence? How should "harm" be defined?

3. Should the infringement of security measures be considered as a condition for establishing some conducts as an offence, and if so under which circumstances?

4. Could we consider the proposed provisions on "Obstruction of a computer, programme or data", "Attack on a site design" and "disruption of information and communications technologies networks", as forms of [illegal] [unlawful] [unauthorized] interference?

5. How do you think the convention should deal with the question of "unauthorised access to or interference with a critical information infrastructure"?

Madame Chair,

INTEGRITY OFFENCES

Firstly, CARICOM believes that the inclusion of the core cyber dependent/related crimes, where the information and communication system is the target of the criminal conduct, is critical. As we outlined in our opening statement, these consist of Illegal/ Unauthorized Access/ Modification/ Interception and System Interference, Data Interference and the Misuse of Devices.

We further believe that these represent overarching provisions which are capable of addressing the main threat vectors within the computer crimes ecosystem without the use of specific categorizations of the threats. It is a fact that the specific threats within the cyber domain changes frequently, from Malware, Spam, to Ransomware, and Identity Theft. CARICOM forms the view that in most instances these egregious activities, regardless of the specific classification, can be covered through one or more of these provisions which are being recommended.

Madame Chair,

ILLEGAL ACCESS - THE CRIMINAL ACT & THE MENTAL ELEMENT

In CARICOM's view, it is important that this new instrument establishes that the foundation of these offences is the absence of the lawful authority to access the information and communication system and that the act is done intentionally. This is consistent with the approach to criminal offences which potentially attract stringent sanctions and penalties.

CARICOM recommended in its submissions on the Chapter on Criminalization the inclusion of the terms "intentionally" and "wilfully" within the substantive criminal offences. This was deliberately done.

Madame Chair,

Before we carefully examine the mental element, CARICOM notes that there are not many criminal cases in common law jurisdictions which have dealt with the issue of cybercrimes and which have sought to explain the parameters of the offence of "Illegal Access".

It has been judicially decided that the offence of unauthorized access, was to protect the integrity of computer systems and criminalize the breaking into and 'hacking' of them. Therefore, what is criminalized is a person's actual deliberate unauthorized interference with the data or program in a computer.

It is CARICOM's view that the instrument should encourage Member States, when introducing the offence of Illegal Access to include this highest form of mens rea which is a direct intention to access, knowing that you do not have the authorization. This should be expressly stated as the standard before criminal liability can be

invoked. The lower standards of recklessness or negligence may be problematic in cases where stringent and harsh sanctions of imprisonment are contemplated due to the serious nature of these offences.

CARICOM's recommendation of the use of the terminology, "intentionally and without right", ensures that there is a preservation of the usual common law defences, such as, accident, duress, and lack of intention, as well as the usual justifications such as in the interest of furthering a criminal investigation or to safeguard the public interest, including the interest of national security.

Madame Chair,

You have asked Member States to consider the issue of legal protections for cyber security professionals. This area of the discourse has always been contentious as the IT community has consistently maintained a strident position in seeking to engage in particular exercises. For this reason, security professionals may be best addressed in the domestic law of the particular Member State based on their own context and particular nuances and their own internal posture with the IT and cyber security professionals within their jurisdiction. It may be difficult to achieve consensus on this very delicate point.

Madame Chair,

CARICOM considers that there should be some flexibility afforded to Member States to include the following qualifications:

1. Member States may be afforded the flexibility to include a qualification in respect of imposing a requirement for a breach of a security measure by the individual accessing the information and communication system before criminal charges may be laid;
2. Based on the domestic context, it may be appropriate to also allow Member States the flexibility to include a requirement that there is an intention to obtain computer data by unauthorised mean or other dishonest intent;
3. Further, the new instrument may take the approach of offering flexibility to Member States on the issue of the need to prove harm as a requirement before criminal charges may be laid for Illegal Access. However, a requirement for harm may operate to strip the provision of its strength in safeguarding the integrity and confidentiality of ICT's, and the data stored thereon.

UNAUTHORIZED/ ILLEGAL INTERCEPTION

It is important that the new convention includes a provision which treats with the illegal/ unauthorized interception of data. The purpose of this provision is to protect the right to privacy of data communication. It is justified on the basis of the right to privacy as enshrined in Article 17 of International Covenant on Civil and Political Rights. Interception for the purposes of the recommended offence includes listening to, monitoring or surveillance of the

content of communications via technical means. The recommended offence would apply to "non-public" transmissions of data.

CARICOM therefore recommends that the mental element required to prove this offence should be the same as obtains for the offence of ill Illegal Access.

DATA INTERFERENCE & SYSTEM INTERFERENCE

Madame Chair,

It is also important for the new instrument to include provisions which address the intentional damage or interference to data as well as ICT systems. As it concerns the former, the protected legal interest is the integrity of the computer data on such systems. As it concerns system interference the protected legal interests are the users or operators of such information and communication system.

Madame Chair,

You will note that CARICOM's contribution to these offences are technology neutral. The recommendation is not necessarily to attach a classification to forms of data interferences or system interferences which are being criminalized but to create a provision which addresses the underlying mischief. Hence, should the classification and manner of interference change, the relevance and applicability of the provision will remain intact.

However, as it concerns data interference and system interference, CARICOM posits that when treating with the data interference, the Ad Hoc Committee may consider that it may be useful to give Member States the flexibility of only imposing appropriate criminal sanctions where the conduct results in harm.

"Harm" should not be defined by the instrument but left to the Member State which elects to insert this qualification to so define.

TREATMENT OF SYSTEM INTERFERENCE WITH CRITICAL INFRASTRUCTURE

Madame Chair,

CARICOM is of the belief that when the Convention treats with "System Interference", Member States should be allowed to reserve the right to create a scale of punitive measures which may be adjusted based on the type of ICT system which is compromised. This is important as an ICT which sits at the core of a critical infrastructure is different from a private computer system. Interference with the former could cripple a nation and therefore Member States should be allowed to approach this offence in a manner to ensure that the penalty is commensurate with the impact of the act.

MISUSE OF DEVICES

In addition to the above offences of Unauthorized Access, Interception, Data Interference and System Interference, the new

instrument should include a provision which establishes a separate and distinct offence regarding the creation, manufacture of or production, sale, procurement for use, importation, exportation, distribution or otherwise making available or possession of devices, software, computer programs, password, access code or similar data for the purpose of the commission of any of the above offences. (Unauthorized Access, Unauthorized Interception, Data Interference, System Interference).

Madame Chair,

CARICOM thanks you for the opportunity to make contributions in respect of the first group of questions posed in relation to the negotiation segment on the Chapter on Criminalization.