الأمم المتحدة E/CN.15/2018/6

المجلس الاقتصادي والاجتماعي

Distr.: General
22 February 2018
Arabic
Original: English

لجنة منع الجريمة والعدالة الجنائية

الدورة السابعة والعشرون

فيينا، ١٤-١٨ أيار/مايو ٢٠١٨

البند ٥ من جدول الأعمال المؤقَّت*

المناقشة المواضيعية بشأن تدابير العدالة الجنائية لمنع الجريمة السيبرانية بجميع أشكالها والتصدِّي لها، بوسائل منها تعزيز التعاون على الصعيدين الوطني والدولي

دليل المناقشة المواضيعية بشأن تدابير العدالة الجنائية لمنع الجريمة السيبرانية بجميع أشكالها والتصدِّي لها، بوسائل منها تعزيز التعاون على الصعيدين الوطني والدولي

مذكِّرة من الأمانة

ملخَّص

دليل المناقشة المواضيعية هذا بشأن تدابير العدالة الجنائية لمنع الجريمة السيبرانية بجميع أشكالها والتصدِّي لها، بوسائل منها تعزيز التعاون على الصعيدين الوطني والدولي، أعدته الأمانة من أجل المناقشة المواضيعية التي ستجريها لجنة منع الجريمة والعدالة الجنائية في دورتها السابعة والعشرين، عملاً بمقرَّرها ١/١٨. وقد قرَّر المجلس الاقتصادي والاجتماعي، في مقرَّره ٢٤١/٢٠١٦، أن يكون الموضوع الرئيسي للدورة السابعة والعشرين للجنة "تدابير العدالة الجنائية لمنع الجريمة السيبرانية بجميع أشكالها والتصدِّي لها، بوسائل منها تعزيز التعاون على الصعيدين الوطني والدولي". وتعرض هذه المذكِّرة مجموعةً من المسائل المتعلقة بمجالات العمل المواضيعية المُقترحة في المناقشة المواضيعية، وتبيِّن بعض المسائل التي تُعين على تحديد شكل هذه المناقشة، وتقدِّم معلومات أساسية ذات صلة.

* E/CN.15/2018/1.

210318 210318 V.18-00971 (A)

أولاً- مقدِّمة

١- قرَّر المجلس الاقتصادي والاجتماعي، في مقرَّره ٢٤١/٢٠١٦، أن يكون الموضوع الرئيسي للدورة السابعة والعشرين للجنة منع الجريمة والعدالة الجنائية هو "تدابير العدالة الجنائية لمنع الجريمة السيبرانية بجميع أشكالها والتصدِّي لها، بوسائل منها تعزيز التعاون على الصعيدين الوطني والدولي".

٢- وأقرَّت اللجنة، في دورتها السادسة والعشرين المُستأنفة، المعقودة يومي ٧ و٨ كانون الأول/ديسمبر ٢٠١٧، مُقترح الرئيس المتعلق بطريقة تنظيم المناقشة المواضيعية في دورتها السابعة والعشرين وهي كالآتي: تجري المناقشة المواضيعية في جلسة تُعقد في الصباح وجلسة تُعقد بعد الظهر. وتُكرَّس الجلسة الصباحية لمناقشة الموضوع الفرعي "التحدِّيات الراهنة"، وجلسة بعد الظهر لمناقشة الموضوع الفرعي "التدابير الممكنة للتصدي لها".

٣- وقد أعدَّت الأمانة هذه المذكِّرة وفقاً لمقرَّر اللجنة ١/١٨ المُعنون "المبادئ التوجيهية للمناقشات المواضيعية التي تجريها لجنة منع الجريمة والعدالة الجنائية"، والذي قررت اللجنة فيه أن تستند مناقشات الموضوع البارز إلى دليل للمناقشة يتضمَّن قائمة بالمسائل التي يُتوخَّى من المشاركين تناولها.

ثانياً- معلومات أساسية: تمهيد السبيل إلى المناقشة المواضيعية

٤- أحدث التطور السريع للإنترنت وتكنولوجيا المعلومات تغييرات كبيرة في المجتمعات في سائر ربوع العالم، ولكنه أتاح أيضاً فرصاً جديدةً للجريمة. فالحواسيب والشبكات والبيانات يمكن أن ترتبط بالجريمة بمختلف أشكالها بأيِّ طريقة يمكن تصورها تقريباً، وهي أصبحت موضوع الجريمة وأدوات ارتكابها في الوقت ذاته، ممَّا أدى إلى ظهور دوافع وفرص جديدة لتوسع نطاق الجريمة. وغالباً ما تتسبب الإنترنت وتكنولوجيا المعلومات في إحداث خللٍ في التوازن بين المخاطر والمكاسب لدى مرتكبي الجرائم مع ترجيح كفة المكاسب. وإضافةً إلى ذلك، ونتيجةً للتصميم الرقمي الأساسي للإنترنت وكذلك لتوافر تكنولوجيا المعلومات والاتصالات عالميًّا، أصبحت الجريمة السيبرانية مرتبطةً بالجريمة المنظمة وكثيراً ما تكون ذات طبيعة عبر وطنية.(١)

٥- وقد أقرَّت الجمعية العامة، في قرارها ٢٣٠/٦٥، إعلان السلفادور بشأن الاستراتيجيات الشاملة لمواجهة التحدِّيات العالمية: نظم منع الجريمة والعدالة الجنائية وتطورها في عالم متغير، بالصيغة التي اعتمدها مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، وطلبت إلى لجنة منع الجريمة والعدالة الجنائية أن تنشئ، تماشياً مع الفقرة ٤٢ من إعلان السلفادور، فريق خبراء حكوميًّا دوليًّا مفتوح العضوية من أجل إجراء دراسة شاملة عن مشكلة الجريمة السيبرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها، بما في ذلك تبادل

(١) عولمة الجريمة: تقييم لخطر الجريمة المنظمة العابرة للحدود الوطنية (منشورات الأمم المتحدة، رقم المبيع E.10.IV.6)، الصفحة ٢٠٤؛ وتقرير المخدِّرات العالمي ٢٠١٧: مشكلة المخدِّرات والجريمة المنظمة، والتدفقات المالية غير المشروعة والفساد والإرهاب (منشورات الأمم المتحدة، رقم المبيع E.17.XI.11)، الصفحة ١٥.

المعلومات عن التشريعات الوطنية والممارسات الفضلى والمساعدة التقنية والتعاون الدولي، بغية دراسة الخيارات المتاحة لتعزيز التدابير القانونية أو غيرها من التدابير القائمة على الصعيدين الوطني والدولي للتصدي للجريمة السيبرانية واقتراح تدابير جديدة في هذا الشأن.

٦- وجُدِّدت ولاية الفريق تلك في إعلان الدوحة بشأن إدماج منع الجريمة والعدالة الجنائية في جدول أعمال الأمم المتحدة الأوسع من أجل التصدِّي للتحدِّيات الاجتماعية والاقتصادية وتعزيز سيادة القانون على الصعيدين الوطني والدولي ومشاركة الجمهور، الذي اعتمده مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية وأقرته الجمعية العامة في قرارها ١٧٤/٧٠.

٧- وعقد فريق الخبراء المعني بإجراء دراسة شاملة لمشكلة الجريمة السيبرانية ما مجموعه أربع دورات في الأعوام ٢٠١١ و٢٠١٣ و٢٠١٧ و٢٠١٨ على التوالي. وأحاطت لجنة منع الجريمة والعدالة الجنائية علماً، في قرارها ٧/٢٢ المؤرَّخ ٢٦ نيسان/أبريل ٢٠١٣، بالدراسة الشاملة عن الجريمة السيبرانية التي أعدها مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة (المكتب المعني بالمخدِّرات والجريمة) تحت إشراف فريق الخبراء وبالمناقشة التي دارت حول مضمونها خلال الاجتماع الثاني لفريق الخبراء، الذي عُقد في فيينا في الفترة من ٢٥ إلى ٢٨ شباط/فبراير ٢٠١٣، (انظر الوثيقة UNODC/CCPCJ/EG.4/2017/3) الذي أُعرب خلاله عن آراء مختلفة بشأن مضمون الدراسة واستنتاجاتها والخيارات المطروحة فيها؛ وطلب فيه إلى فريق الخبراء أن يواصل، بمساعدة من الأمانة، وحسب الاقتضاء، عمله للوفاء بولايته.

٨- وطلبت لجنة منع الجريمة والعدالة الجنائية (اللجنة)، في قرارها ٤/٢٦، الذي اعتمدته في دورتها السادسة والعشرين المعقودة في ٢٦ أيار/مايو ٢٠١٧، إلى فريق الخبراء أن يواصل عمله وأن يعقد في هذا السياق اجتماعات دورية ويعمل كمنتدى لإجراء مزيد من المناقشات بشأن المسائل الموضوعية المتعلقة بالجريمة السيبرانية، ومواكبة اتجاهاتها المتغيرة، بما يتماشى مع إعلاني السلفادور والدوحة، وطلبت أيضاً إلى فريق الخبراء أن يواصل تبادل المعلومات عن التشريعات الوطنية والممارسات الفضلى والمساعدة التقنية والتعاون الدولي، بغية دراسة الخيارات المتاحة لتعزيز التدابير القانونية أو غيرها من التدابير القائمة على الصعيدين الوطني والدولي للتصدِّي للجريمة السيبرانية واقتراح تدابير جديدة في هذا الشأن. وفي القرار نفسه، قرَّرت اللجنة أن يكرِّس فريق الخبراء اجتماعاته المقبلة للنظر على نحو منظَّم في كل من المسائل الرئيسية التي تتناولها الدراسة، دون المساس بالمسائل الأخرى المندرجة ضمن ولايته، آخذاً في اعتباره، حسب الاقتضاء، التبرعات المتلقاة عملاً بقرار اللجنة ٧/٢٢ ومداولاته في اجتماعاته السابقة.

٩- وفي سياقٍ أوسع، وعلى النحو المُجسَّد في خطة التنمية المستدامة لعام ٢٠٣٠ التي اعتمدتها الجمعية العامة في قرارها ١/٧٠، ثمة اعترافٌ متزايدٌ بأنَّ الحدَّ من النزاعات والجريمة والعنف والتمييز وضمان عدم التهميش والحوكمة الرشيدة وسيادة القانون تمثل كلها عوامل رئيسية لرفاهة الشعوب وضرورية لتحقيق التنمية المستدامة. والهدف ١٦ من أهداف التنمية المستدامة ("التشجيع على إقامة مجتمعات مسالمة لا يُهمش فيها أحد من أجل تحقيق التنمية المستدامة، وإتاحة إمكانية وصول الجميع إلى العدالة، وبناء مؤسسات فعالة وخاضعة للمساءلة وشاملة للجميع على جميع المستويات") مهم للغاية في ذلك الشأن. والهدف ١٦ مرتبطٌ بمكافحة

الجريمة السيبرانية، التي تعمل، إلى جانب الأشكال الأخرى من الجريمة، بما في ذلك الجريمة المنظمة، على تقويض الحوكمة الرشيدة و سيادة القانون وتهديد الأمن والنمو، فضلاً عن زعزعة الاستقرار في الدول الأعضاء (انظر الفقرة ٤ من الوثيقة E/CN.7/2016/CRP.1-E/CN.15/2016/CRP.1).

١٠- وسيجري تناول جوانب الجريمة السيبرانية، ضمن مسائل أخرى، خلال مؤتمر الأمم المتحدة الرابع عشر لمنع الجريمة والعدالة الجنائية، المزمع عقده في اليابان، في نيسان/أبريل ٢٠٢٠، وذلك في سياق حلقة العمل الرابعة الخاصة بالمؤتمر التي ستتناول موضوع "الاتجاهات الراهنة للجريمة، والتطورات الأخيرة والحلول المستجدة، لا سيما التكنولوجيات الجديدة بوصفها وسائل وأدوات لمكافحة الجريمة".

١١- وفي ضوء هذه الخلفية، تتوخى المناقشة المواضيعية، المزمع تنظيمها في إطار الدورة السابعة والعشرين للجنة، تقييم التطورات الأخيرة. وستكون المناقشة المواضيعية بمثابة منتدى لإجراء المزيد من المناقشات وتبادل الآراء والخبرات بين الدول الأعضاء. ولتيسير المناقشة المواضيعية، حُدِّدت ثمانية مجالات عمل مواضيعية ذات صلة بالجريمة السيبرانية، بما فيها المجالات المندرجة صراحةً في الموضوع الرئيسي. ويُناقَش كل مجالٍ من المجالات الثمانية المذكورة على حدة في القسم الثالث أدناه، مع تكريس عناوين فرعية منفصلة للتحديات الراهنة وتدابير التصدِّي الممكنة (على النحو المتفق عليه خلال الدورة السادسة والعشرين المستأنفة للجنة، انظر الفقرة ٢ أعلاه) وقائمة إرشادية بالمسائل أو النقاط للمناقشة.

ثالثاً- المجالات المواضيعية: مسائل للمناقشة

ألف- أنواع الجريمة السيبرانية وما يتصل بها من تهديدات

التحدِّيات الراهنة

١٢- "الجريمة السيبرانية" ليست مصطلحاً قانونيًّا أو مصطلح استدلال جنائي، ولا تعرِّف أو تصف فئةً واضحةً من الأعمال الإجرامية. وثمة اتفاقٌ عام على قائمة أساسية من التجاوزات والجرائم المرتبطة تحديداً بالحواسيب، ولكن خارج هذا الإطار، لم يُتوصَّل بعدُ إلى توافقٍ عالميٍّ في الآراء بشأن معنى هذا المصطلح. وهذا الوضع ناتجٌ عن الطابع العالمي للحواسيب وتعدد استخداماتها، فضلاً عن التطور السريع لتكنولوجيا المعلومات والاتصالات وطرائق استخدامها منذ أواخر خمسينيات القرن الماضي.

١٣- وحسب السياق، يُمكن أن يشير مصطلح "الجريمة السيبرانية" إلى الجرائم المرتكبة باستخدام تكنولوجيا المعلومات والاتصالات أو الجرائم المرتكبة ضد منشآت تكنولوجيا المعلومات والاتصالات ومستخدميها في حد ذاتهم أو السياقات الجنائية التي يكون فيها لتكنولوجيا المعلومات والاتصالات دورٌ غير مباشر أو داعم.[٢] ويُستخدم مصطلح "الجريمة السيبرانية" للإشارة إلى مجموعة كبيرة من الجرائم، بما في ذلك الجرائم المرتكبة ضد نظم الحاسوب وبياناته (مثل القرصنة

(٢) Christopher Ram, "Cybercrime" in *Routledge Handbook of Transnational Criminal Law*, Neil Boister and Robert J. Currie, eds. (New York, Routledge, 2015), p. 379.

الحاسوبية)، والتزوير والاحتيال المتصلان بالحواسيب (مثل تصيد البيانات الاحتيالي)، والجرائم ذات الصلة بالمحتوى (مثل نشر مواد متعلقة بالاعتداء على الأطفال جنسيًّا)،[٣] والجرائم المتعلقة بحقوق التأليف والنشر (مثل نشر المواد المقرصنة).

١٤- وزاد الاستخدام المتنامي لتكنولوجيا الحاسوب والتوجه نحو رقمنة البيانات من أهمية البيانات الحاسوبية. ونتيجةً لذلك، أصبحت البيانات الحاسوبية عُرضةً لهجمات متكررة تتراوح بين اعتراض البيانات والتجسس عليها. وظهر الآن اقتصادٌ رقميٌّ غير نظامي يتسم بالتعقيد، سلعته البيانات. وللبيانات الشخصية والمالية المسروقة، المُستخدمة مثلاً للنفاذ إلى الحسابات المصرفية وبطاقات الائتمان، أو للحصول، عن طريق الاحتيال، على تسهيلات ائتمانية، قيمةٌ نقديةٌ. وتُفضي هذه الأوضاع إلى ارتكاب مجموعةٍ من الأنشطة الإجرامية، بما فيها تصيُّد البيانات الاحتيالي والتوجيه الاحتيالي نحو المواقع الإلكترونية وتوزيع البرامجيات الحاسوبية الخبيثة وقرصنة قواعد بيانات الشركات، وهي أنشطة تدعمها بنيةٌ متكاملةٌ من مبرمجي الشفرات الخبيثة ومضيفي المواقع المتخصصة والأفراد القادرين على استئجار شبكات حواسيب مصابة ببرامجية خبيثة لشن هجمات آلية.

١٥- وما زال تطوير البرمجيات الخبيثة وتوزيعها يمثلان على نحو خاص الركن الأساسي لمعظم قضايا الجرائم السيبرانية. ومنذ أواخر عام ٢٠١٣، أصبح فيروس الفدية (cryptoware) (وهو فيروس فدية يستخدم التشفير) البرامجية الخبيثة الأبرز من حيث الخطورة والتأثير. وحسب توجه سارقي المعلومات، أصبحت حملات نشر فيروس الفدية تستهدف بشكل متزايد الكيانات في القطاعين العام والخاص.[٤]

١٦- ويسعى المجرمون على الدوام إلى إيجاد سبل وتكنولوجيات لجعل نماذج أعمالهم أكثر فعالية ولزيادة هوامش أرباحهم. وتحد الطبيعة المجهولة للمعاملات على شبكة الإنترنت وكذا استخدام العملات المشفرة من إمكانية كشف سلطات إنفاذ القانون عن الملابسات الإجرامية. والاستخدام المتزايد للشبكات الخصوصية الافتراضية وبرامج التخفي (Onion routers) وترجمة العناوين الشبكية الواسعة النطاق يحد من قدرة المُحقِّقين على إسناد الأدلة.

١٧- ولا تزال معدلات الجريمة السيبرانية في تزايد تماشياً مع توسع شبكة الإنترنت، ممَّا يفاقم حالة ضعف مستخدمي الإنترنت لتبلغ مستويات جديدة. وإضافةً إلى ذلك، يُعد التهديد الذي تفرضه الجريمة السيبرانية بمختلف أشكالها تهديداً متعدد الأبعاد، وهو لا يستهدف المواطنين فحسب، بل يستهدف أيضاً الشركات والحكومات بوتيرة آخذة في التسارع. وتمثل أدوات الجريمة السيبرانية تهديداً أمنيًّا مباشراً وتضطلع بدورٍ لا ينفك يزداد أهمية في تسهيل ارتكاب معظم أشكال الجريمة المنظمة والإرهاب.

(٣) انظر مكتب الأمم المتحدة المعنى بالمخدِّرات والجريمة، *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children* (دراسة عن آثار تكنولوجيات المعلومات الجديدة على الاعتداء على الأطفال واستغلالهم جنسيًّا)، (فيينا، ٢٠١٥).

(٤) مكتب الشرطة الأوروبي، *European Union Serious and Organised Crime Threat Assessment: Crime in the Age of Technology* (تقييم أخطار الجرائم الخطيرة والمنظمة في إطار الاتحاد الأوروبي: الجريمة في عصر التكنولوجيا) (لاهاي، ٢٠١٧)، الصفحة ٣٠.

تدابير التصدِّي الممكنة

١٨- إنَّ حجم المشكلة غير المسبوق المقترن بالأنواع المتعددة من التصرفات التي توصف بأنها جرائم سيبرانية يهدد قدرة السلطات على التصدِّي لها بفعالية وكفاءة. وفي الوقت نفسه، يمكن للفضاء الإلكتروني أن يُتيح فرصاً وأدوات للكشف عن الجريمة السيبرانية. فقد ينتُج عن استخدام تكنولوجيا المعلومات والاتصالات عددٌ من القرائن وخيوط التحقيق لفائدة نظام العدالة الجنائية. وبات لدى السلطات بيانات عن الأنشطة الإجرامية أكثر من أيِّ وقتٍ مضى، ويتسنى لها الآن أن تُسخِّر هذه المعلومات بطرائق تعزز من فعالية الاستخبارات والتحقيقات من حيث التكلفة. ومن الأمثلة المثيرة للاهتمام مثال الاستغلال الإجرامي للعملات المشفرة. وهذه العملات المشفرة باتت متاحةً بفعل تقنية سلسلة السجلات المغلقة. وبالرغم من الفجوات القانونية والفنية التي تكتنف هذه التقنية حاليًّا، إلا أنَّ العديد من خصائصها قد تجعلها أداةً مُجديةً لإنفاذ القانون، من خلال تتبع أنماط المعاملات المشبوهة وتعقب الأدلة (انظر الفقرة ١٦٤ من الوثيقة E/CN.15/2018/CRP.1).

١٩- ويتمتع المحققون الماهرون في المجال الرقمي، بفضل الجهود المعززة الرامية إلى بناء قدراتهم، بالقدرة على الحصول على الأدلة الإلكترونية على ارتكاب الجرائم السيبرانية، وإن حرص مرتكبوها على عدم ترك أيِّ آثار رقمية أو مسحوا تلك الآثار. فرهناً بمدة الاحتفاظ بالبيانات، توفر سجلات الاتصال ببروتوكول الإنترنت (IP) أثراً تعقُّبيًّا كاملاً لجميع اتصالات الإنترنت وأوقاتها ومصادرها ووجهاتها.

٢٠- وإضافةً إلى ذلك، دفع اعتماد المجتمع المتزايد على الإنترنت والتواصل عبر الحاسوب بأجهزة إنفاذ القانون إلى وضع أدوات للتحقيق في الجرائم المرتكبة على شبكة الإنترنت أو استخدام البرامجيات للكشف عن الأنماط الإجرامية مثلاً. كما تستخدم أجهزة إنفاذ القانون مواقع التواصل الاجتماعي لتحسين علاقاتها مع الجماعات المحلية ولطلب التعاون من الجمهور في التحقيقات الجنائية.

٢١- ولذا، فمن الضروري أن تنظر الدول في وضع استراتيجيات متعددة التخصصات للتصدي للتحديات ولتحسين قدرتها على التحقيق في القضايا التي تنطوي على جرائم سيبرانية ومحاكمة مرتكبيها بنجاح وفعالية. وقد تتراوح الاستراتيجيات المتعددة التخصصات بين اتخاذ تدابير تنظيمية ومبادرات لوضع سياسات من أجل منع الجريمة السيبرانية وتدريب السلطات المختصة، على النحو المُبيَّن أدناه.

نقاط للمناقشة

٢٢- لعلَّ اللجنة تودُّ أن تنظر في النقاط التالية بغرض مناقشتها لاحقاً:

(أ) ما هي الدروس المستفادة من تحليل الأنماط المتغيرة في الجريمة السيبرانية؟

(ب) ما هي الطريقة الأفضل للاستفادة من هذه الدروس في وضع تدابير تنظيمية فعالة للتصدي للجريمة السيبرانية، واستراتيجيات رامية إلى وضع سياسات لمكافحتها على الصعيد الوطني؟

(ج) ما هو أثر مختلف أنواع الجريمة السيبرانية على قدرة الدول الأعضاء على الاحتفاظ بسجلات للجرائم ذات الصلة بشكل منهجي وتبادل المعلومات لأغراض إنفاذ القانون على الصعيدين الوطني والدولي، بما في ذلك المعلومات عن ضلوع الجماعات الإجرامية المنظمة في هذه الجرائم وأساليب عمل تلك الجماعات والتقنيات المستخدمة في كشف أشكال الجريمة السيبرانية؟

(د) إلى أيٍّ مدى يمكن للتعاريف الواردة في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية للمصطلحين "جماعة إجرامية منظمة" و"جماعة ذات هيكل تنظيمي" أن تنطبق على الفضاء الإلكتروني، بما في ذلك القضايا التي يتفاعل فيها مرتكبو الجريمة، المحميون بإمكانية حجب الهوية في الغالب، دون معرفة الطرف الآخر؟

باء- التدابير القانونية المتخذة ضد الجريمة السيبرانية: جوانب التجريم

التحدِّيات الراهنة

٢٣- لدى تقييم التحدِّيات الراهنة التي تواجه وضع تدابير قانونية للتصدي للجريمة السيبرانية، من المفيد ألاَّ يغيب عن الأذهان أنَّ هذه التحدِّيات نشأت وتفاقمت على مر السنين. فعلى مر عصور التاريخ، أدت الخدمات الحاسوبية وتكنولوجيا الإنترنت إلى نشوء أشكال جديدة للجريمة فور ظهورها. ومن الأمثلة عن ذلك تطور الشبكات الحاسوبية منذ سبعينيات القرن الماضي والنفاذ الأول غير المرخص للشبكات الحاسوبية الذي حدث بعد ذلك بفترة وجيزة. وبالمثل، ظهرت أول جرائم برامجية بعد فترة قصيرة من ظهور الحواسيب الشخصية في ثمانينيات القرن الماضي، عندما كانت الحواسيب الشخصية تُستخدم لنسخ المنتجات البرامجية. وفي أواخر التسعينيات من ذلك القرن، أصبحت الشبكات جزءاً بالغ الأهمية من الهياكل الأساسية لتكنولوجيا المعلومات والاتصالات، ممَّا أدى إلى تزايد القلق بشأن بعض أشكال الجريمة السيبرانية التي تهدد هذه الشبكات. وهذا أفضى بدوره إلى استخدام تكنولوجيا الأمن السيبراني والتوجه، بوجه خاص، نحو تجريم بعض أشكال الهجمات التي تُشن ضد الهياكل الأساسية الحيوية أو فرض عقوبات مُشددة عليها.(٥)

٢٤- وبصرف النظر عن نشوء تعاريف ومفاهيم جديدة استناداً إلى التكنولوجيا المتغيرة بسرعة، ثمة سؤالٌ ملحٌّ عمَّا إذا كان ينبغي التعامل مع الجريمة السيبرانية كظاهرة جديدة واستحداث جرائم جديدة بالكامل متصلة بها، أم محاولة تطبيق التعاريف القائمة للجرائم وتوسيع نطاقها أو تعديلها لدى الضرورة. وقد سنَّت بعض البلدان تشريعات جديدة تتعامل مع الاحتيال الحاسوبي بوصفه جريمةً خاصةً، في حين صنَّفت بلدان أخرى النسخ غير المشروع للبيانات

(٥) انظر على سبيل المثال Aunshul Rege-Patwardhan, "Cybercrimes against critical infrastructures: a study of online criminal organization and techniques", *Criminal Justice Studies: A Critical Journal of Crime, Law and Society*, vol. 22, No. 3 (2009), p. 261; Luca Montanari and Leonardo Querzoni, eds., *Critical Infrastructure Protection: Threats, Attacks and Countermeasures* (March 2014). وانظر أيضاً Security Council resolution 2341 (2017) on the threats to international peace and security cause by terrorist acts.

أو إتلافها، أو الحيلولة دون النفاذ إلى البيانات أو سوء استخدامها، كجرائم جديدة لأنَّ التعاريف الحالية لا تشمل إلا الممتلكات الملموسة. وفي مثالٍ آخر، صُنِّف انتحال الهوية كجريمة منفصلة في بعض الولايات القضائية.

٢٥- أمَّا إذا فُضِّل إدخال تعديلات على التشريعات الجنائية القائمة من قبل، فغالباً ما تصطدم الهيئات التشريعية بالإجراءات المُطوَّلة لدى استعراض القانون وتحديثه. ومن ثم، يتمثل التحدي الرئيسي في الفجوة الزمنية التي تفصل بين اكتشاف أشكال جديدة للإجرام وسن التعديلات التشريعية اللازمة لمواجهتها. وما يزال هذا التحدي مهمًّا وذا صلة أكثر من أيِّ وقتٍ مضى مع تسارع تكنولوجيا المعلومات والاتصالات.

تدابير التصدِّي الممكنة

٢٦- إنَّ التشريعات الجنائية المناسبة هي أساس التحقيق في الجريمة السيبرانية وملاحقة مرتكبيها قضائيًّا. ومن ثم، ينبغي أن يتحلى واضعو القوانين بالقدرة على الاستجابة لتطور تكنولوجيا المعلومات والاتصالات ورصد فعالية الأحكام القانونية الحالية باستمرار. ويُعد التحليل الدقيق للتشريعات الحالية أمراً ضروريًّا للكشف عن الثغرات المحتملة ومعالجة الصعوبات الناجمة عنها والتي تحول دون استيفاء شرط التجريم المزدوج في سياق التعاون الدولي. ويجوز للمُشرِّعين أن يستفيدوا من الصكوك المتعددة الأطراف، المُلزمة منها وغير المُلزمة.

٢٧- ولضمان حصول أثر مستدام، قد يستلزم الأمر صوغ القوانين الجديدة والتعديلات على القوانين القائمة صياغةً مرنةً وحياديةً تكنولوجيًّا، مع مراعاة ضرورة اليقين والدقة القانونيين. وينبغي أن تتناول القوانين ضرورة الحصول على المعلومات في الوقت المناسب وعبر الحدود الوطنية. وأخيراً، قد يحتاج المُشرِّعون إلى قدرٍ كافٍ من التدريب والتوجيه لكي يتمكنوا من وضع أحكام سليمة وسن قوانين فعالة.

نقاط للمناقشة

٢٨- لعلَّ اللجنة تودُّ أن تنظر في النقاط التالية بغرض مناقشتها لاحقاً:

(أ) ما هي الدروس المُستفادة من الجهود المبذولة على الصعيد الوطني لوضع التشريعات وإنفاذها بغية مكافحة الجريمة السيبرانية ولإدماج تلك التشريعات في الإطار الأوسع للاستراتيجية الوطنية لمكافحة الجريمة السيبرانية؟

(ب) هل توفِّر القوانين الوطنية أساساً قانونيًّا كافياً لكشف جميع الجرائم المتصلة بالجريمة السيبرانية والتحقيق فيها وملاحقة مرتكبيها قضائيًّا على نحو فعَّال؟ وما هي الثغرات التي ينبغي سدها؟

(ج) ما هو تأثير الصكوك المتعددة الأطراف الحالية على نطاق الأُطر القانونية الوطنية الرامية إلى مكافحة الجريمة السيبرانية؟ هل تحقق التقارب بين التدابير القانونية الوطنية بفضل تلك الصكوك؟ وإذا كان الأمر كذلك، فإلى أيِّ مدى؟

(د) هل لتنوع النُّهج الوطنية في تجريم الجرائم السيبرانية تأثيرٌ على نطاق التعاون الدولي، بالنظر إلى وجود اشتراط التجريم المزدوج؟

جيم- الصلاحيات الإجرائية والأدلة الإثباتية الإلكترونية

التحدِّيات الراهنة

٢٩- إنَّ للصلاحيات التحقيقية الوطنية دوراً رئيسيًّا في جمع الأدلة الإثباتية الإلكترونية. ويكشف فحص الصلاحيات التحقيقية على الصعيد الوطني تنوعاً كبيراً في النُّهُج المتبعة في استخدام الأدلة الإثباتية الإلكترونية للتحقيق في الجريمة. وترتبط تلك النُّهج بنطاق تفسير الصلاحيات الموجودة سابقاً لتنطبق على البيانات مثل الأدلة غير الملموسة والسلطة القانونية القائمة التي تتخذ تدابير تدخُّلية خاصة، مثل تحقيقات التحليل الجنائي عن بُعد. وبالرغم من اختلاف الصلاحيات القانونية، فإنه ينبغي إتاحة مجموعة من التدابير التحقيقية المُحددة لجمع الأدلة الإثباتية الإلكترونية. وقد تتضمن هذه التدابير التعجيل في حفظ البيانات الحاسوبية وإصدار الأوامر بالحصول على بيانات المحتوى المُخزَّنة والأوامر بالحصول على بيانات حركة الاتصالات المخزَّنة والأوامر بالحصول على معلومات المشتركين وجمع بيانات المحتوى في الوقت الحقيقي وجمع بيانات حركة الاتصالات في الوقت الحقيقي والبحث عن المعدات أو البيانات الحاسوبية ومصادرها والنفاذ عبر الحدود إلى نظم أو بيانات حاسوبية واستخدام أدوات التحاليل الجنائية الحاسوبية عن بُعد. ويمكن إيجاد أمثلة عن القوانين الوطنية المعنية بالتدابير التحقيقية في مستودع معلومات المكتب المعني بالمخدِّرات والجريمة المتعلقة بالجريمة السيبرانية وفي بوابة الموارد الإلكترونية والقوانين المتعلقة بالجريمة (شيرلوك). وينبغي أن تواكب الصلاحيات التحقيقية مسار التكنولوجيات الحديثة، وأن تكون مدعومة بأطر قانونية ومؤسسية تعزز وتيسِّر التنسيق والتعاون الفعالين وفي الوقت المناسب بين القطاع الخاص والأجهزة الحكومية ذات الصلة، على الصعيد الوطني والإقليمي والعالمي، مع الحرص على مراعاة حقوق الإنسان. ومن الضروري للغاية أن تتضمن تلك الأُطر عنصراً قويًّا مراعياً لحقوق الإنسان، إذ إنَّ تكنولوجيا المعلومات والاتصال تؤثر على مجالات من قبيل الخصوصية وحرية التعبير.

٣٠- وفي أفضل الحالات، تكون الأدلة الإثباتية الإلكترونية مقبولةً لدى المحكمة. غير أنَّ الأهمية المتزايدة التي تكتسيها الأدلة الإثباتية الإلكترونية في الدعاوى الجنائية تفرض تحديات لم تُعرف من قبلُ. فهي، على سبيل المثال، سهلة الإتلاف للغاية ويمكن تعديلها أو حذفها بسهولة. ونتيجةً لذلك، يُعتبر الحفاظ على سلامة الأدلة الإثباتية الإلكترونية من الخطوات الأساسية في التحليل الجنائي الحاسوبي. كما أنَّ حماية سلامة البيانات أمرٌ ضروريٌّ لضمان مصداقية الأدلة الإثباتية ودقتها. وإضافةً إلى ذلك، ولضمان مقبولية الأدلة الإثباتية الإلكترونية، ينبغي أن تُجمع هذه الأدلة من خلال الإجراءات المعمول بها التي تراعي حقوق الإنسان.

٣١- وعلاوةً على ذلك، لكي تتمكَّن سلطات إنفاذ القانون من جمع الأدلة الإثباتية الإلكترونية المتعلقة بالجريمة السيبرانية والتحقيق فيها بفعالية، أصبح للتعاون مع الجهات الفاعلة ذات الصلة الأخرى، مثل الجهات الفاعلة من القطاع الخاص، أهميةً خاصةً خلال السنوات الماضية. وبصفة

عامة، يضطلع مقدمو خدمات الاتصالات بدور مهم في إتاحة الوصول إلى الأدلة الإثباتية الإلكترونية. ويمكن أن تؤثر القوانين الوطنية المتعلقة بالخصوصية على قدرة مقدِّمي الخدمات على تبادل المعلومات مع السلطات في إطار تحقيقٍ ما.

تدابير التصدِّي الممكنة

٣٢- نظراً للطابع المتغير للأدلة الإثباتية الإلكترونية، فإنه يلزم وضع بعض المعايير والشروط للتعامل مع هذه الأدلة الإثباتية الإلكترونية وضمان صحتها وسلامتها. وتتضمن تلك المعايير والشروط قواعد وإجراءات عامة، مثل حفظ سجلات القضايا واستخدام تكنولوجيا مقبولة على نطاق واسع وإشراك خبراء مؤهلين في التحقيقات.

٣٣- ويقتضي عددٌ متزايدٌ من التحقيقات في الجرائم السيبرانية، بما في ذلك القضايا التي تشمل الإساءة للأطفال واستغلالهم، أدلة إثباتية إلكترونية تحتفظ بها أطرافٌ ثالثة. لذا، فمن الضروري للغاية أن تعمل قطاعات الصناعة والحكومات معاً لوضع آليات تتيح لأجهزة إنفاذ القانون الحصول على البيانات في الوقت المناسب في الحالات الطارئة. وينبغي أن تُقرَن هذه الآليات بإجراءات قانونية عادلة وشفافة لغرض إجراء التحقيقات الروتينية.

٣٤- وقد انعقد في فيينا يومي ١٢ و١٣ شباط/فبراير ٢٠١٨ اجتماعٌ لفريق خبراء بشأن النفاذ القانوني إلى البيانات الرقمية عبر الحدود، نُظِّم بالاشتراك مع المكتب المعني بالمخدِّرات والجريمة والمديرية التنفيذية للجنة مكافحة الإرهاب، وبالتعاون مع الرابطة الدولية للمدعين العامين. وتمثل هدف الاجتماع في إرساء الأسس لوضع دليلٍ لفائدة السلطات المركزية والمدعين العامين والمحققين من أجل الحصول على الأدلة الإثباتية الإلكترونية من ولايات قضائية أجنبية في إطار إجراء تحقيقات عبر الحدود بشأن مكافحة الإرهاب وما يتصل به من جرائم منظمة. وأتاح الاجتماع فرصةً لتبادل القوانين والأدلة الوطنية وأمثلة عن حالات واقعية بيَّنت الممارسات الفضلى والدروس المستفادة من الحصول على الأدلة الإثباتية الإلكترونية من مقدِّمي خدمات الاتصال الخاضعين لولايات قضائية أجنبية.

نقاط للمناقشة

٣٥- لعلَّ اللجنة تودُّ أن تنظر في النقاط التالية بغرض مناقشتها لاحقاً:

(أ) ما هي التحدِّيات التي تواجهها السلطات التحقيقية لدى محاولتها استيفاء الشروط المتعلقة باستخدام تقنيات تحقيقية محددة وجمع الأدلة الإثباتية الإلكترونية وتبادلها من أجل الكشف عن الجريمة السيبرانية والتحقيق فيها وملاحقة مرتكبيها قضائيًّا، وما هي الممارسات الفضلى في مواجهة هذه التحدِّيات؟

(ب) ما هي الخبرة المُكتسبة في الدول الأعضاء في مجال قبول هذه الأدلة الإثباتية في المحاكم؟

(ج) ما أثر التعاون مع القطاع المالي في جمع الأدلة الإلكترونية المتعلقة بعائدات الجريمة السيبرانية (ناقلو الأموال غير المشروعة، مثلاً)؟

(د) ما هي التحدِّيات الرئيسية، من منظور سيادة القانون وحقوق الإنسان، التي تواجه الاستخدام والتنفيذ الفعالين للتقنيات المرتبطة بالتحقيق في الجرائم السيبرانية وملاحقة مرتكبيها قضائيًا؟

(هـ) ما هي الدروس المستفادة من الجهود المبذولة من أجل تعزيز التعاون بين سلطات إنفاذ القانون ومقدِّمي خدمات الاتصال لتأمين الأدلة الإثباتية الإلكترونية بغية الكشف عن الجريمة السيبرانية والتحقيق فيها وملاحقة مرتكبيها قضائيًا؟

دال- مسائل الولاية القضائية

التحدِّيات الراهنة

٣٦- ينص القانون الدولي على عدد من الأسس المتعلقة بالولاية القضائية بشأن الجرائم السيبرانية، ويتمثل شكلاها الرئيسيان في الولاية القضائية المستندة إلى الإقليم والولاية القضائية المستندة إلى الجنسية. ويمكن إيجاد بعض هذه الأسس أيضاً في الصكوك المتعددة الأطراف المتعلقة بالجرائم السيبرانية. وباتت الولاية الإقليمية الموسَّعة أو الموضوعية تستند اليوم في الأغلب إلى وقوع ركن من أركان الجريمة، أو آثار تلك الجريمة في إقليم دولة ما، أو وجود رابط وثيق آخر بذلك الإقليم. ويجب على الدول أيضاً أن تحدد البلد الأكثر قدرة على ملاحقة الجناة المزعومين قضائيًا استناداً إلى عوامل مثل موقع الأدلة الإثباتية أو موقع الجناة.

٣٧- ومن شأن تطبيق بلدان مختلفة لمجموعة من الأسس القضائية أن يدفع بأكثر من بلد واحد إلى تأكيد ولايته القضائية على نفس الجريمة السيبرانية. ويزداد خطر التنازع بين الولايات القضائية بشكل أكبر إذا طُبِّق مبدأ الولاية الإقليمية على الحالات التي تكون فيها البنية التحتية المستخدمة في ارتكاب الجريمة هي وحدها الموجودة في البلد المعني، وليس الجاني أو الضحية.

٣٨- وتفرض الحوسبة السحابية عدداً من التحدِّيات على العدالة الجنائية، لا سيما فيما يتعلق بالقانون المنطبق وولاية الإنفاذ الجنائية. وغالباً ما لا يكون واضحاً لسلطات العدالة الجنائية في أيِّ ولاية قضائية خُزِّنت البيانات وما هو النظام القانوني الساري عليها. فقد يكون لمقدم الخدمة مقرٌّ في إحدى الولايات القضائية ولكنه يخضع للنظام القانوني في ولاية قضائية ثانية، في حين تُخزَّن البيانات في ولاية ثالثة. وقد تُحفظ نفس البيانات في عدة ولايات قضائية باستخدام تقنيات تعرف بالنسخ المتطابق، أو قد تنتقل بين الولايات القضائية، ممَّا يُفاقم من تعقيد هذه المسائل.

٣٩- وعلاوةً على ذلك، ليس من الواضح ما إذا كان مقدم الخدمات الحاسوبية السحابية هو نفسه مراقب البيانات الخاصة بمستخدم ما أو مجهزها، ومن ثم، ليس من الواضح ما هي القواعد التي تسري عليها. ومن دواعي الغموض كذلك مسألة ما إذا كانت البيانات مُخزَّنة أم عابرة ومن ثم ما إذا كان يتعين إصدار أوامر الإبراز أو أوامر التفتيش والحجز أو أوامر الاعتراض أو أوامر جمع البيانات آنيًا وعلى أساس أيِّ ولاية قضائية. وفضلاً عن ذلك، تتسبب الطبيعة غير المركزية

للحوسبة السحابية بمشاكل للتحليل الجنائي والبحوث عبر الإنترنت جرّاء هيكلية السحابة (التشغيل المتعدد للبيانات وتوزيعها وتصنيفها)، وبسبب التحدِّيات القانونية المتصلة بسلامة وصحة عملية جمع البيانات أو مراقبة الأدلة أو ملكية البيانات أو الولاية القضائية.(٦)

تدابير التصدِّي الممكنة

٤٠- يمكن لعدة دول، في حالات عديدة، أن تطالب بالولاية القضائية على الجرائم السيبرانية، ومن المهم إجراء مشاورات لاتخاذ القرار بشأن الدولة التي ينبغي أن تلاحق الجناة قضائيًّا. وقد ينطوي ذلك القرار على مسائل قانونية ودبلوماسية وعملية مثل المطالبات بالولاية القضائية وغيرها من المطالبات القانونية التي تقدمها كل دولة وكذا مسألة تحديد ما إذا كان يمكن تسليم الجناة إلى الدولة التي ترغب في ملاحقتهم قضائيًّا، والاعتبارات العملية من قبيل الكلفة وغيرها من العقبات التي تعترض طريق نقل الأدلة الإثباتية من دولة إلى أخرى، مع ضمان قبول هذه الأدلة الإثباتية في المحكمة وأن تُقدَّم الأدلة الإثباتية أمام المحكمة على نحوٍ فعال. وعادةً ما تُحلُّ النزاعات المتعلقة بالولاية القضائية، حيثما نشأت، من خلال المشاورات المباشرة وغير المباشرة بين البلدان. فإذا ما تقرر أن تتولى الملاحقة القضائية دولة من عدة دول محتملة، يمكن أن تُنقل إليها الولاية القضائية للدول الأخرى بصورة فعلية. ويوفر نقل الإجراءات الجنائية، بوصفه شكلاً منفصلاً من أشكال التعاون الدولي، السياق وإطار العمل للقيام بذلك.(٧)

٤١- وقد جرى العمل أيضاً على تعزيز التعاون الإقليمي والدولي من أجل تأمين الأدلة الإثباتية الإلكترونية على الصعيد المتعدد الأطراف. ففي حزيران/يونيه ٢٠١٧، وافقت اللجنة المعنية بالاتفاقية المتعلقة بجرائم الفضاء الحاسوبي التابعة لمجلس أوروبا على إعداد بروتوكول ثانٍ مُلحقٍ بالاتفاقية المتعلقة بجرائم الفضاء الحاسوبي بُغية توفير قواعد واضحة وإجراءات أكثر فعاليةً لتأمين الأدلة الإثباتية الإلكترونية "في السحاب" في تحقيقات جنائية محددة. وقد أقرَّت اللجنة الاختصاصات يوم ٨ حزيران/يونيه ٢٠١٧ ومن المقرر إجراء مفاوضاتٍ بشأنها في الفترة من أيلول/سبتمبر ٢٠١٧ إلى كانون الأول/ديسمبر ٢٠١٩.

نقاط للمناقشة

٤٢- لعلَّ اللجنة تودُّ أن تنظر في النقاط التالية بغرض مناقشتها لاحقاً:

(أ) ما هي المعايير التي تحكُم الولاية القضائية لأغراض تنفيذ إجراءات العدالة الجنائية في قضايا الجريمة السيبرانية؟ وكيف يجري تطبيق تلك المعايير على السياقات الحاسوبية السحابية حيث تكون البيانات في أغلب الأحيان غير "ثابتة"؟

---

(٦) مجلس أوروبا، اللجنة المعنية باتفاقية الجريمة السيبرانية، "Criminal justice access to data in the cloud: challenges" (وصول أجهزة العدالة الجنائية إلى البيانات الموجودة في السحابة: التحدِّيات)، ورقة مناقشة أعدها الفريق المعني بالأدلة الموجودة في السحابة، التابع للجنة المعنية باتفاقية الجريمة السيبرانية، ٢٦ أيار/مايو ٢٠١٥، (٢٠١٥) ١٠، الصفحات من ١٠ إلى ١٤.

(٧) انظر ورقة المعلومات الأساسية التي أعدتها الأمانة عن الاعتبارات العملية والممارسات الجيِّدة والصعوبات القائمة في مجال نقل الإجراءات الجنائية، بصفته شكلاً منفصلاً من أشكال التعاون الدولي في المسائل الجنائية (CTOC/COP/WG.3/2017/2).

(ب) ما هي التجربة التي اكتُسبت من إجراء المشاورات بهدف حل النزاعات المتعلقة بالولاية القضائية على الجرائم السيبرانية؟ وما هي التحدِّيات والممارسات الفضلى وكذا الدروس المستفادة في هذا الشأن؟

هاء- التعاون والتنسيق بين الوكالات على الصعيد الوطني

التحدِّيات الراهنة

٤٣- تُعد استراتيجيات أصحاب المصلحة المتعددين فيما يخص الجريمة الإلكترونية عنصراً حيويًّا في مكافحة الجريمة السيبرانية. والتحدِّيات القانونية والتقنية والمؤسسية التي تفرضها الجريمة السيبرانية هي تحديات بعيدة المدى ولا يمكن معالجتها إلا باتباع استراتيجية متماسكة متأصلة في المبادرات القائمة وفي دور مختلف أصحاب المصلحة. ولكي تكون مكافحة الجريمة السيبرانية فعالة، فإنها تتطلب هياكل تنظيمية متطورة للغاية تتفادى التداخل بين الاختصاصات وتكون صلاحياتها محددةً تحديداً واضحاً، وهذا من شأنه أن يوفر جوًّا من التنسيق بين جميع الأطراف المعنية حتى تتمكن من اتخاذ إجراءات متضافرة. وبدون الهياكل المناسبة، سيكون من الصعب للغاية تنفيذ سياسات قوية ومبادرات برنامجية.

٤٤- ويُعد ردع الجريمة السيبرانية أيضاً جزءاً لا يتجزأ من الاستراتيجيات الوطنية لضمان الأمن السيبراني وحماية البنية التحتية الحيوية للمعلومات. ويشمل ذلك، على وجه الخصوص، اعتماد تشريعات لمكافحة إساءة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية وأغراض أخرى، ولمواجهة الأنشطة الرامية إلى المساس بسلامة البنية التحتية الوطنية الحرجة. وردع الجريمة السيبرانية مسؤولية مشتركة تقع على عاتق السلطات الحكومية والقطاع الخاص وعلى المواطنين، وهي مسؤولية تتطلب من الجميع تضافرَ الأعمال لمنع حوادث الأمن السيبراني والاستعداد لها والرد عليها والتعافي منها. أمَّا وضع استراتيجية وطنية لمكافحة الجريمة السيبرانية ومن ثَم تنفيذُها فأمرٌ يتطلب نهجاً شاملاً يشمل التعاون والتنسيق بين الجهات المعنية على المستوى المؤسسي.

٤٥- بيد أنَّ التنسيق المؤسسي يطرح عدداً من الصعوبات، يتصل معظمها بالموارد والقدرات المتاحة تحت تصرف كل بلد. وهناك عدة عوامل أخرى ينبغي أن تُراعَى، من بينها مدى الدعم الذي يقدمه القطاع الخاص، على سبيل المثال من خلال الشراكات بين القطاعين العام والخاص، أو التنظيم الذاتي وتدابير الحماية الذاتية السارية في القطاع الخاص.

تدابير التصدِّي الممكنة

٤٦- برزت فكرة إنشاء الشراكات بين الوكالات كممارسة شائعة على المستوى الاستراتيجي لمكافحة الجرائم السيبرانية، ومنها الجرائم التي تيسرها التكنولوجيا ضد الأطفال. وردًّا على التحدِّيات المتعددة الجوانب التي تعترض مكافحةَ الجريمة السيبرانية، يحتاج مقدمو خدمات الاتصالات والمؤسسات العامة، مثل سلطات إنفاذ القانون والسلطات القضائية الجنائية، إلى إقامة شراكات بين القطاعين العام والخاص تتيح تعزيز الثقة وإقامة حوارات متبادلة. وعلى صعيد أعم، تحتاج الدول إلى اتخاذ تدابير تنظيمية تتجاوز القانون الجنائي وتحفِّز القطاع الخاص على المشاركة

في منع الجريمة مشاركةً فعَّالة. وقد يكون مثل هذا النهج مفيداً في خلق بيئة تستشعر التهديدات الناشئة وتفضي إلى مواجهتها.

٤٧- ويمكن أن يكون إنشاء أفرقة عمل تستهدف الجريمةَ المنظَّمة الميسرة بالإنترنت أداةً مفيدة لاتخاذ إجراءات متضافرة ضد الجريمة السيبرانية. وينبغي لأفرقة العمل تلك أن تتفاعل مع البيئة الإجرامية المتطورة، وقد يؤدي وجودها، مثلاً، إلى إنشاء أفرقة أكثر استدامة لتبادل المعلومات ووضع ترتيبات أكثر تخصيصاً لتنفيذ عمليات محددة مثل تفكيك شبكات البرامجيات الخبيثة للتحكم في الأجهزة الإلكترونية (البوتنيت). وفي جميع الحالات، تحتاج السلطات إلى المرونة لإشراك مجموعة متنوعة من أصحاب المصلحة، كأجهزة إنفاذ القانون والقطاع الخاص والأوساط الأكاديمية وفئات المستخدمين، والتنسيق معهم بكفاءة لتحقيق النتيجة المرجوة.

٤٨- وقد غيَّرت الإنترنت تركيز أنشطة تنظيم تكنولوجيا المعلومات والاتصالات الحكومي داخل الحكومات. فوَجدت الهيئات التي تنظم قطاع تكنولوجيا المعلومات والاتصالات نفسَها منخرطةً بالفعل في مجموعة من أنشطة التصدِّي للجريمة السيبرانية. وينطبق الأمر بوجه خاص على مجالات مثل تنظيم المحتوى وسلامة الشبكات وحماية المستهلك، نظراً لتعرض المستخدمين للخطر. ومن ثم، فإنَّ سبب تدخل الهيئات التنظيمية هو أنَّ الجريمة السيبرانية تقوض تطوير صناعة تكنولوجيا المعلومات والاتصالات وتطور الأطراف التي تقدم المنتجات والخدمات ذات الصلة. ويمكن النظر إلى الواجبات والمسؤوليات الجديدة لهيئات تنظيم تكنولوجيا المعلومات والاتصالات في مجال مكافحة الجريمة السيبرانية كجزء من الاتجاه الأوسع نحو تحويل النماذج المركزية لتنظيم الجرائم السيبرانية إلى هياكل مرنة.[٨]

نقاط للمناقشة

٤٩- لعلَّ اللجنة تودُّ أن تنظر في النقاط التالية بغرض مناقشتها لاحقاً:

(أ) ما هي التحدِّيات الناشئة على الصعيد الوطني أمام تعزيز القدرات المؤسسية والتنسيق بين الوكالات للتصدي للجريمة السيبرانية؟

(ب) هل اكتُسبت أيُّ خبرات في وضع أُطُر أو مبادئ توجيهية نموذجية من أجل التعاون بين أصحاب المصلحة على الصعيد الوطني بغية منع الجريمة السيبرانية ومكافحتها؟ وإذا ما اكتُسبت هذه الخبرات بالفعل، فكيف تُعزِّز هذه الأُطر أو المبادئ التوجيهية التعاون الراهن؟

واو- التعاون الدولي

التحدِّيات الراهنة

٥٠- تُحدِّد الصكوك القائمة، إضافة إلى تجريمها لأعمال الجريمة السيبرانية ومنح الصلاحيات الإجرائية ذات الصلة، آليات للتعاون الدولي في التحرِّي عن الجرائم السيبرانية وملاحقتها قضائيًّا عبر

(٨) الاتحاد الدولي للاتصالات، *Understanding Cybercrime: Phenomena, Challenges and Legal Response* (فهم الجريمة السيبرانية: الظواهر والتحدِّيات وتدابير التصدِّي القانونية) (جنيف، ٢٠١٢)، الصفحة ١٠١.

الحدود. ويمثل التعاون الدولي على مكافحة الجريمة السيبرانية تحدياً متنامياً لسلطات العدالة الجنائية وإنفاذ القانون. وعلى الرغم من أنَّ مكان وجود بيانات حاسوبية معيَّنة قد يكون من الناحية النظرية قابلاً للتحديد في نقطة زمنية معيَّنة، إلاَّ أنَّ ظهور الحوسبة السحابية وتقاسم البيانات وتخزينها بين النظراء يعني أنَّ البيانات يمكن أن تكون موجودةً في نسخ متعدِّدة وأن تكون موزَّعةً في أجهزة وأماكن متعدِّدة، كما يمكن أن تُنقَل إلى موقع جغرافي آخر في غضون ثوانٍ قليلة.(٩)

٥١- ونظراً لعدم استقرار الأدلة الإثباتية الإلكترونية، يقتضي التعاون الدولي بشأن مسائل الجريمة السيبرانية استجابةً سريعة وقدرةً على طلب إجراءات تحقيقية متخصصة، بما في ذلك حفظ البيانات وتوفيرها من قِبل مقدِّمي الخدمات من القطاع الخاص. وتشمل التحدِّيات الشائعة لدى طلب تلك البيانات من ولاية قضائية أخرى حالات التأخير في الاستجابة للطلبات، وعدم الالتزام والمرونة من جانب السلطة التي تُطلب منها الأدلة الإثباتية، والشكل الذي تُقدَّم به الأدلة الإثباتية إلى الولاية القضائية الطالبة وما إذا كان يمكن أن تُستخدم في الإجراءات الجنائية، واختلاف تعاريف الجرائم الجنائية بين الدول المتعاونة.(١٠)

٥٢- وقد اتفق معظم الخبراء، خلال الاجتماع الثاني الذي عقده فريق الخبراء المعني بإجراء دراسة شاملة لمشكلة الجريمة السيبرانية في عام ٢٠١٣، على ضرورة تعزيز التعاون الدولي وتسريع خُطاه من أجل التصدِّي لمشكلة الجريمة السيبرانية، لا سيما أنَّ هذه المشكلة آخذة في التوسع وأنَّ تزايد الاعتماد على التكنولوجيات في الأغراض المشروعة يجعل خطر الجريمة السيبرانية أكثر شدةً. وإلى جانب ذلك، أُبديت آراء متباينة بشأن النهج الاستراتيجي الأفضل وبشأن أولويات التصدِّي للمشاكل المتصلة بالجريمة السيبرانية.(١١) وفي ذلك السياق، ثار جدلٌ بشأن ما إذا كان من الضروري استحداث صكٍّ قانوني عالمي جديد يُعنى بمكافحة الجريمة السيبرانية وذلك بُغية معالجة جملة أمور منها جوانب التعاون الدولي على الصعيد العالمي أو أنه يتعين على المجتمع الدولي، عوضاً عن ذلك، أن يستمر في الاعتماد على الصكوك المتعددة الأطراف الحالية، بما في ذلك اللجنة المعنية بالاتفاقية المتعلقة بجرائم الفضاء الحاسوبي التابعة لمجلس أوروبا. ولا يزال هذا الموضوع محل نقاش دون التوصل إلى توافقٍ في الآراء حتى الساعة.

تدابير التصدِّي الممكنة

٥٣- يمكن إدخال المزيد من التحسينات على آليات التعاون الدولي من خلال النظر في كيفية تسريع عمليات المساعدة القانونية المتبادلة. كما يمكن تعزيز التعاون بين أجهزة إنفاذ القانون ومواصلة الحوار المتعدد الأطراف في مجال تيسير الوصول إلى البيانات الحاسوبية عبر الحدود الوطنية.

(٩) ورقة معلومات أساسية عن حلقة العمل ٣ بشأن تعزيز تدابير منع الجريمة والعدالة الجنائية للتصدِّي للأشكال المتطوِّرة للجريمة، مثل الجرائم الإلكترونية (السيبرانية) والاتِّجار بالممتلكات الثقافية، بما في ذلك الدروس المستفادة والتعاون الدولي (A/CONF.222/12)، الفقرة ٣٢.

(١٠) ورقة معلومات أساسية من إعداد الأمانة عن جمع وتبادل الأدلة الإثباتية الإلكترونية (CTOC/COP/WG.3/2015/2)، الفقرة ١٩.

(١١) مداولات فريق الخبراء المعني بإجراء دراسة شاملة لمشكلة الجريمة السيبرانية خلال اجتماعه الثاني المنعقد في فيينا من ٢٥ إلى ٢٨ شباط/فبراير ٢٠١٣، ملخص المقرر الخاص، الفقرة ٢٥ من الوثيقة UNODC/CCPCJ/EG.4/2017/3.

ويمكن، على سبيل المثال، إنشاء نظام منفصل لتيسير الوصول إلى معلومات المشتركين، على النحو المبيَّن في الفقرة ٣ من المادة ١٨ من الاتفاقية المتعلقة بجرائم الفضاء الحاسوبي التابعة لمجلس أوروبا، للتمييز بين أنواع البيانات الملتمسة. ومن شأن هذا النظام أن يساهم في جعل المساعدة القانونية المتبادلة في المسائل المتعلقة بالجريمة السيبرانية والأدلة الإثباتية الإلكترونية أكثر فعالية.(١٢)

٥٤- وقد تساعد الابتكارات، مثل إدماج نميطة خاصة بالأدلة الإلكترونية في أداة المكتب المعني بالمخدِّرات والجريمة لكتابة طلبات المساعدة القانونية المتبادلة المُحدَّثة، في تبسيط عمليات المساعدة القانونية المتبادلة التي تنطوي على أدلة إثباتية إلكترونية. ولكن، وبالتوازي مع ذلك، قد يتعيَّن على أجهزة إنفاذ القانون، بصورة متزايدة، أن تعثر على سبل ريادية للتعاون في التحرِّيات عبر الوطنية عن الجرائم السيبرانية. وربما كان من المهم جدًّا في هذا الشأن إشراك كيانات مثل المجمَّع العالمي للابتكار، التابع للإنتربول، والمركز الأوروبي لشؤون الجريمة السيبرانية، التابع لمكتب الشرطة الأوروبي (اليوروبول)، في تنسيق التحرِّيات عبر الوطنية ودعمها، بوسائل منها تسهيل تقاسم المعلومات بين سلطات إنفاذ القانون الوطنية.

٥٥- وقد تشمل الحلول الأخرى ما يلي: إنشاء وحدات مستقلة معنية بالجريمة السيبرانية داخل السلطات المركزية، ورصد الممارسات العملية الفُضلى واستعراضها في المسائل المتعلقة بالمساعدة القانونية المتبادلة للتأكد من مسألتي التجاوب والفعالية، من خلال جملة أمور منها إجراء إحصاءات عن طلبات المساعدة القانونية المتبادلة التي تنطوي على أدلة إثباتية إلكترونية؛ واستخدام أكبر للتعاون المباشر بين أجهزة الشرطة بوصفه سبيلاً مكملاً مفيداً للأساليب المتبعة في تبادل المساعدة القانونية بُغية ضمان الاستجابة في الوقت المناسب لطلبات المساعدة العاجلة؛ وتركيز التدريب وتكثيفه من أجل تعزيز المساعدة القانونية المتبادلة؛ والتعاون المباشر بين أجهزة الشرطة وغيره من أشكال التعاون الدولي بشأن الجريمة السيبرانية والأدلة الإثباتية الإلكترونية؛ وتشجيع تبادل المعلومات والخبرات في أوساط شبكات نقاط الاتصال على مدار الساعة (٧/٢٤)؛ وتخصيص الموارد للسلطات الوطنية المكلفة بمهمة تنفيذ طلبات المساعدة القانونية المتبادلة، وتعزيز التنسيق بينها وبين السلطات المركزية لغرض الاستجابة في الوقت المناسب.

نقاط للمناقشة

٥٦- لعلَّ اللجنة تودُّ أن تنظر في النقاط التالية بغرض مناقشتها لاحقاً:

(أ) كيف يمكن تقليص الوقت المطلوب لتنفيذ إجراءات المساعدة القانونية المتبادلة في القضايا التي تنطوي على جرائم سيبرانية وأدلة إثباتية إلكترونية؟ وما هي الممارسات الفُضلى في مجال التعاون المباشر بين أجهزة الشرطة عند نقل الأدلة الإثباتية الإلكترونية إلى الخارج؟ وأين تكمن التحدِّيات لدى القيام بذلك؟

(١٢) انظر الصفحة ١٣ من الوثيقة المعنونة "Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY" (2016) 5 (وصول أجهزة العدالة الجنائية إلى الأدلة الإثباتية الإلكترونية الموجودة في السحابة: توصيات لكي تنظر فيها اللجنة المعنية باتفاقية الجريمة السيبرانية)، وهي وثيقة أعدتها اللجنة المعنية باتفاقية الجريمة السيبرانية، التابعة لمجلس أوروبا.

(ب) ما هي الأمثلة التي يمكن للدول أن تقدمها عن الكيفية التي زاد بها تعزيز تبادل المعلومات على الصعيدين الوطني والدولي من القدرة على الكشف عن المخاطر وتقييمها والاستجابة للطلبات بصورة فعالة وفي وقت مناسب؟

(ج) كيف ينبغي إعداد الطلبات الدولية للاحتفاظ بالأدلة الإثباتية الإلكترونية وإرسالها ومعالجتها؟ وما هي الخبرات المُكتسبة من التعاون بين القطاعين العام والخاص في هذا الصدد؟

زاي- منع الجريمة السيبرانية

التحدِّيات الراهنة

٥٧- إنَّ التكاليف وأوجه التعقد المرتبطة بالتحقيق في قضايا الجرائم السيبرانية وملاحقة مرتكبيها قضائيًّا توحي بثمار هائلة محتملة للتعاون في مجال منع الجريمة السيبرانية. وعلى نحو خاص، تضطلع الشراكات بين القطاعين العام والخاص بدورٍ محوري في منع الجريمة السيبرانية. ويمكن أن يكون لمقدِّمي الخدمات دور في منع الجريمة السيبرانية من خلال ما يلي: (أ) تخزين بيانات المستخدمين التي يمكن لموظفي إنفاذ القانون الذين في حوزتهم إذن بالتفتيش الحصول عليها لاستخدامها في التحقيق في الجريمة السيبرانية؛ (ب) الغربلة الفعالة للاتصالات عبر شبكة الإنترنت ومحتوياتها بهدف منع الجرائم السيبرانية قبل ارتكابها. غير أنَّ هذين التدبيرين يفرضان، لدى تحليلهما في سياق حرية التعبير، العديد من التحدِّيات.

٥٨- وعند مناقشة دور مقدِّمي الخدمات في منع الجريمة السيبرانية، ينبغي مراعاة حدودهم بوصفهم هيئات تابعة للقطاع الخاص. فمن ناحية أولى، يواجه موظفو إنفاذ القانون وكذا الزبائن تقلب سياسات مقدِّمي الخدمات وعدم إمكانية التنبؤ بها. فقد يغير مقدمو الخدمات سياساتهم من طرف واحدفي أيِّ وقت ودون أن يُخطروا أجهزة إنفاذ القانون بذلك مسبقاً. وإضافةً إلى ذلك، لا تتباين السياسات والممارسات بشكل كبير بين مقدم خدمات وآخر فحسب، بل بين دولة عضو وأخرى أيضاً. فقد يستجيب أحد مقدِّمي الخدمات للعديد من الطلبات المقدمة من بلد ما، في حين أنه لا يستجيب لأيِّ طلب مقدم من بلد آخر أو يستجيب لعدد قليل منها، وقد يفعل مقدم خدمات آخر العكس تماماً.(١٣)

٥٩- ومن ناحية ثانية، قد تتأثر تحقيقات الشرطة في الجرائم السيبرانية بضمانات حماية البيانات التي تقتضي حذف البيانات الشخصية التي لم تَعُد مطلوبة للأغراض التي جُمعت من أجلها. ومن ثم، قد تمثل قوانين الاحتفاظ بالبيانات نهجاً عمليًّا لضمان قدرة مقدِّمي الخدمات على الاضطلاع بدورٍ أكبر في منع الجريمة السيبرانية من خلال تعزيز التعاون مع أجهزة إنفاذ القانون، إلا أنَّ من المهم أن تُنفَّذ هذه القوانين مع مراعاة الضمانات الإجرائية وإجراءات حماية الخصوصية

(١٣) مجلس أوروبا، اللجنة المعنية باتفاقية الجريمة السيبرانية، "Criminal justice access to data in the cloud: Cooperation with 'foreign' service providers" (T-CY (2016)2) (وصول أجهزة العدالة الجنائية إلى البيانات الموجودة في السحابة: التعاون مع مقدِّمي الخدمات "الأجانب")، الصفحة ٢٢.

الواجبة. وينبغي مراعاة المعايير واللوائح التنظيمية الخاصة بحماية البيانات، بما فيها لائحة الاتحاد الأوروبي العامة لحماية البيانات.(١٤)

٦٠- وتواجه الأوساط الأكاديمية تحدياً كبيراً يتمثل في سد الثغرات العديدة القائمة والتي لا تنفك تظهر في المعارف المتعلقة بالجريمة السيبرانية، لا سيما الاعتداء على الأطفال واستغلالهم جنسيًّا من خلال تكنولوجيا المعلومات والاتصالات. ويمكن للمؤسسات الأكاديمية، رهناً بتوافر التمويل المستدام، أن تضطلع بأدوار متعددة في منع الجريمة السيبرانية، بوسائل منها تعليم المختصين وتدريبهم وتطوير القوانين والسياسات والعمل على وضع المعايير والحلول التقنية.

تدابير التصدِّي الممكنة

٦١- تشمل الممارسات الفُضلى في مجال منع الجريمة السيبرانية سن التشريعات والقيادة الفعالة وتطوير القدرات المرتبطة بالعدالة الجنائية وإنفاذ القانون وإنشاء قاعدة معارف متينة وتعزيز التعاون بين الحكومة والمجتمعات والقطاع الخاص والدول. ومن المهم للغاية تقديم المساعدة في وضع تقنيات المنع وصقلها وتبادل الدروس المستفادة والممارسات الفُضلى والتشارك في المعلومات اللازمة لوضع هذه التقنيات وإكسابها فعالية.

٦٢- وسبق أن أُشير إلى أهمية حملات إذكاء الوعي والحملات التعليمية، لا سيما تلك التي تتناول المخاطر الناشئة والمخاطر التي تستهدف فئات معينة مثل الأطفال، بوصفها عنصراً من عناصر سياسات منع الجريمة السيبرانية.(١٥) وتتضمن مبادرة التعليم من أجل العدالة، وهي عنصر أساسي من عناصر البرنامج العالمي لتنفيذ إعلان الدوحة التابع للمكتب المعني بالمخدِّرات والجريمة، إعداد مواد خاصة بمكافحة الجريمة السيبرانية للأطفال والشباب وتعميمها على الطلبة في المستويات التعليمية الابتدائية والثانوية والجامعية.

٦٣- ويمكن أن يضطلع المجتمع المدني بدورٍ حيوي في مساعدة الأطفال على فهم مخاطر الإنترنت والتعامل معها، وهي مساعدة تكتسي أهميةً بالغةً في الجهود الرامية إلى منع إيذاء الأطفال واستغلالهم باستخدام تكنولوجيا المعلومات والاتصالات. وتمكِّن المبادرات التعليمية الأطفال وأسرهم ومقدِّمي الرعاية الآخرين من فهم المخاطر المرتبطة بتكنولوجيا المعلومات والاتصالات وتقييمها بشكل صحيح.(١٦)

٦٤- وثمة عددٌ من نماذج الشراكات بين القطاعين العام والخاص، التي تعزز منع الجريمة السيبرانية، مثل الشراكات بين سلطات إنفاذ القانون ومقدِّمي خدمات الاتصال. ويعتمد العديد من هذه الشراكات على تبادل المعلومات على أساس قواعد واضحة، والثقة، والعضوية المحدودة،

(١٤) لائحة الاتحاد الأوروبي ٦٧٩/٢٠١٦ التابعة للبرلمان الأوروبي والمجلس المؤرخة في ٢٧ نيسان/أبريل ٢٠١٦، المعنية بحماية الأشخاص الطبيعيين لدى معالجة البيانات الشخصية وبحرية تنقل هذه البيانات، وكذا التوجيه الملغي 95/46/EC (الجريدة الرسمية للاتحاد الأوروبي، القانون رقم ١١٩، ٤ أيار/مايو ٢٠١٦، الصفحات من ١ إلى ٨٨).

(١٥) انظر الدراسة المعنونة: "*Study on the Effects of New Information Technologies*" (دراسة بشأن آثار تكنولوجيات المعلومات الجديدة)، الصفحة ٥٤.

(١٦) المرجع نفسه، الصفحة ٥٤.

وتشجيع المنافع المتبادلة، والاستجابة. وعلاوةً على ذلك، سيتعاظم دور القطاع الخاص في عمليات كشف المواد المسيئة وحجبها قبل وصول المستخدمين إليها، بما فيها المواد المتصلة بالإساءة الجنسية للأطفال على شبكة الإنترنت.(١٧)

٦٥- ويتمثل نهج واضح وتطلعي للحكومات في العمل بالشراكة مع الجهات التي سوف تؤثر في مجال الأعمال والبيئة التشغيلية في المستقبل بحيث تتمكن جميع الأطراف المعنية من استباق التغيرات في السلوكيات الإجرامية وطرائق إساءة استخدام التكنولوجيا على نحو أفضل. وفي هذا السياق، لا بد من الاستمرار في تطوير فهم معمق لسلوك المجرم السيبراني المعاصر باستخدام تحليل الاستخبارات وإجراء بحوث في علم الجريمة واستخدام تقنيات تحديد المواصفات النمطية، وذلك بُغية استغلال الموارد الحالية على نحوٍ أكثر فعالية وتحديد خصائص تكنولوجيات الاتصالات المستقبلية المعرضة للاستغلال الإجرامي على نحو استباقي.

نقاط للمناقشة

٦٦- لعلَّ اللجنة تودُّ أن تنظر في النقاط التالية بغرض مناقشتها لاحقاً:

(أ) ما هي الأمثلة التي يمكن للدول أن تقدمها عن استراتيجيات المنع الفعالة المتخذة في أوساط الجهات المعنية لمكافحة الجريمة السيبرانية؟ وكيف يجري تعريف النجاح وتقييمه؟

(ب) كيف يمكن للأوساط الأكاديمية والقطاع الخاص والمنظمات غير الحكومية أن تساهم بالصورة الأمثل في تطوير المعارف والتشريعات والسياسات في مجال الجريمة السيبرانية وتبادلها؟

(ج) ما هي الخبرات التي اكتسبتها الدول الأعضاء فيما يتعلق بتحقيق التوازن بين حماية البيانات وإجراء التحقيقات في الجرائم السيبرانية على نحوٍ فعال؟

حاء- بناء القدرات والمساعدة التقنية

التحدِّيات الراهنة

٦٧- يُعدُّ بناء القدرات على مستوى أجهزة إنفاذ القانون ونُظم العدالة الجنائية الوطنية أمراً بالغ الأهمية. ففي حين شرعت أغلب البلدان في وضع هياكل متخصصة في التحقيق في الجرائم السيبرانية والجرائم التي تنطوي على أدلة إثباتية إلكترونية، لا تزال تلك الهياكل، في بلدان أخرى، تفتقر إلى التمويل وتعاني من نقص في القدرات. وبما أنَّ الدليل الإثباتي الإلكتروني ضروري للتحقيق في الجرائم السيبرانية، فقد يتعيَّن على سلطات إنفاذ القانون أن تميِّز بوضوح بين الجهات المعنية بالتحقيق في الجرائم السيبرانية وتلك المعنية بمختبرات التحليل الجنائي الرقمي، وأن تحدِّد بوضوح تسلسل سير عملهما. وقد يحتاج موظفو الخطوط الأمامية في أجهزة إنفاذ القانون، بصورة متزايدة، إلى اكتساب واستخدام مهارات أساسية، مثل المهارات اللازمة لإنتاج صورة طبق الأصل لجهاز تخزين إلكتروني لأغراض الاستدلال الجنائي.

(١٧) انظر، على سبيل المثال، تقرير شركة *Netclean* لعام ٢٠١٧، المتاح على الرابط التالي: https://www.netclean.com/netclean-report-2017.

٦٨- ويتضح إجمالاً أنَّ عملية بناء قدرات موظفي أجهزة إنفاذ القانون والعدالة الجنائية ستكون عمليةً مستمرةً ومتواصلةً، نظراً للتطور السريع للتكنولوجيا والابتكارات الإجرامية.

تدابير التصدِّي الممكنة

٦٩- تُعدُّ المساعدة التقنية والتعاون أمرين مهمين للتمكين من تبادل أفضل للممارسات والخبرات في مجال التحقيق وتعميم تقنيات جديدة. ولعلَّ الدول الأعضاء تودُّ تعزيز تبادل نهج جديدة في التحقيق في عمليات الاحتيال المالي المعقدة على الإنترنت والاتجار بالمخدِّرات على شبكة الإنترنت أو استخدام العملات الافتراضية لغرض غسل الأموال، ومن ثم، تمكين سلطات إنفاذ القانون في مختلف البلدان من الحصول سريعاً على المهارات اللازمة لمكافحة مخاطر الجريمة السيبرانية الناشئة.

٧٠- وقد يُسهِّل إنشاء الهياكل أو الوحدات المتخصصة في الجريمة السيبرانية داخل أجهزة إنفاذ القانون على الدول تركيز مواردها المحدودة في مكان واحد بُغية وضع تقنيات متخصصة في مجال التحقيق وجمع الأدلة الإثباتية الإلكترونية المناسبة وتحليلها، بوسائل منها إجراء فحوص التحليل الجنائي الرقمي. وفي الوقت نفسه، قد توفر هذه الهياكل أو الوحدات التدريب لأجهزة إنفاذ القانون المحلية وتنسق التدابير الوطنية للتصدي للجريمة السيبرانية وتسهل التعاون فيما بين الشركاء المشاركين في التحقيقات وتستهدف أشكال الجريمة الإلكترونية التي قد تثير قلق الدولة على نحو خاص.

٧١- والمكتب المعني بالمخدِّرات والجريمة مُكلَّفٌ، من خلال برنامجه العالمي المعني بالجريمة السيبرانية، بمساعدة الدول الأعضاء على مكافحة الجرائم السيبرانية من خلال بناء القدرات وتقديم المساعدة التقنية، وذلك وفقاً لقرار الجمعية العامة ٦٥/٢٣٠ ولقراري لجنة منع الجريمة والعدالة الجنائية ٢٢/٧ و٢٢/٨. ويقدم المكتب المعني بالمخدِّرات والجريمة مساعدة تقنية مُركَّزة من أجل بناء القدرات ومنع الجريمة السيبرانية وإذكاء الوعي وتعزيز التعاون والتحليل المتصل بالجريمة السيبرانية، لا سيما في البلدان النامية. كما أنه يقدم، عند الطلب وفي نطاق ولايته، المساعدة التشريعية للدول الأعضاء التي تحتاج إليها.

٧٢- وقد أعد المكتب المعني بالمخدِّرات والجريمة، على سبيل المثال، دورةً لتدريب المُدربين في مجال التحقيق في العملات المشفرة، وهو يوفر تدريباً بهذا الشأن في العديد من المناطق. ويتمثل هدف التدريب في تحسين قدرة موظفي إنفاذ القانون والمُحللين والمدعين العامين والقضاة فيما يتصل بالعملات المشفرة، وتعقُّب العملات الافتراضية (البت كوين) في التحقيقات المالية، وتحديد الموارد المعلوماتية، والتعاون بشأن الدعاوى القضائية الدولية.

نقاط للمناقشة

٧٣- لعلَّ اللجنة تودُّ أن تنظر في النقاط التالية بغرض مناقشتها لاحقاً:

(أ) ما هي جوانب التدابير والاستراتيجيات المتعلقة بالجريمة السيبرانية التي تحظى بالأولوية في المساعدة التقنية وبناء القدرات، لا سيما بالنظر إلى الطبيعة المتغيرة للجريمة السيبرانية والمخاطر الجديدة والناشئة المرتبطة بها؟

(ب) ما هي الدروس المستفادة من تبادل الممارسات الفضلى في مجال التحقيق ومن التجارب ومن تعميم التقنيات الجديدة كمثالٍ عن التعاون في مجال المساعدة التقنية؟

(ج) كيف يمكن تحقيق وتعزيز أوجه التآزر والتحالف بالشكل الأمثل بين المنظمات الدولية التي تقدم المساعدة التقنية في المسائل المرتبطة بالجريمة السيبرانية من أجل تقديم خدمات ملموسة ومستدامة لبناء القدرات لفائدة الدول الأعضاء التي تحتاج إلى المساعدة؟

رابعاً- سد الثغرات الراهنة وسبيل المضي قُدُماً

٧٤- تتزايد الجهود التي يبذلها المجتمع الدولي من أجل فهمٍ واستجابةٍ أفضل لمخاطر الجريمة السيبرانية. ومع ذلك، ثمة حاجة ماسة للمزيد من العمل لأنَّ تحديات لا يستهان بها لا تزال قائمة لدى وضع وتنفيذ تدابير شاملة ومنسقة ومستدامة وفعالة للتصدي للجريمة السيبرانية.

٧٥- و ستعمل اللجنة، من خلال تيسير المناقشة المواضيعية في إطار دورتها السابعة والعشرين، وأثناء مداولاتها بشأن البند المعني من جدول الأعمال، بمثابة منبرٍ لتبادل المعلومات والممارسات الفضلى والدروس المستفادة، و ستضع تدابير فعالة وتروج للصكوك أو المعايير الدولية ذات الصلة بمكافحة الجريمة السيبرانية.

٧٦- ولعلَّ اللجنة تودُّ، لدى نظرها في اتخاذ المزيد من الإجراءات لمواجهة التحدِّيات التي تفرضها الجريمة السيبرانية والمضي قُدماً في وضع تدابير مناسبة للتصدي لها، أن تركز النقاش على جوانب الأطر القانونية والمؤسسية الحالية التي يُعتقد أنها تمثل أشد المخاطر، وعلى المجالات ذات الأولوية التي تواجه فيها الدول الأعضاء أكبر التحدِّيات.

٧٧- ولعلَّ اللجنة تودُّ أن تنظر في أن توصي بمواصلة الدول الأعضاء تعزيز الجهود الرامية إلى بناء قدراتها وتقوية أُطرها القانونية، لا سيما لدى استعراض السياسات والقوانين والأُطر المؤسسية الحالية والممارسات التي من شأنها أن تعزز قدرتها على التصدِّي للمخاطر الحالية والناشئة المرتبطة بالجريمة السيبرانية.

٧٨- ولعلَّ اللجنة تودُّ أيضاً أن تحدد وتضع أولويات بمجالات المساعدة التقنية التي قد يضطلع فيها المكتب المعني بالمخدِّرات والجريمة، بالتعاون والتنسيق الوثيقين مع الجهات الفاعلة الأخرى، وعلى أساس الولايات ذات الصلة، بهدف تقديم دعم أفضل للدول الأعضاء في تنفيذ سياساتها وقوانينها الوطنية وتحسين قدراتها المؤسسية على التصدِّي للتحديات الراهنة والناشئة المرتبطة بالجريمة السيبرانية.

٧٩- ولعلَّ اللجنة تودُّ كذلك أن تدعو المكتب المعني بالمخدِّرات والجريمة إلى مساعدتها في البقاء على تواصل مع سائر الهيئات الدولية الحكومية التي تُعنى بالجريمة السيبرانية وتدابير العدالة الجنائية بغية منع هذه الجريمة ومكافحتها، بما فيها مؤتمر الأطراف في اتفاقية الجريمة المنظمة وفريقه العامل المعني بالتعاون الدولي، كل حسب ولايته وعند الاقتضاء.