UNODC/CCPCJ/EG.4/2017/2

Distr.: General
21 February 2017
Arabic
Original: English

فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية
فيينا، ١٠-١٣ نيسان/أبريل ٢٠١٧

مداولات الاجتماع الأول لفريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، المعقود في فيينا في الفترة من ١٧ إلى ٢١ كانون الثاني/يناير ٢٠١١

ملخَّص من إعداد المقرِّر

أولا- مقدِّمة

١- طلبت الجمعية العامة في قرارها ٦٥/٢٣٠ إلى لجنة منع الجريمة والعدالة الجنائية أن تنشئ، وفقاً للفقرة ٤٢ من إعلان سلفادور بشأن الاستراتيجيات الشاملة لمواجهة التحديات العالمية: نظم منع الجريمة والعدالة الجنائية وتطورها في عالم متغير، فريق خبراء حكوميًّا دوليًّا مفتوح العضوية ينعقد قبل دورة اللجنة العشرين من أجل إجراء دراسة شاملة عن مشكلة الجريمة السيبرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها، بما في ذلك 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 للتصدي للجريمة السيبرانية واقتراح تدابير جديدة في هذا الشأن.

٢- وعُقد الاجتماع الأول لفريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية في فيينا في الفترة من ١٧ إلى ٢١ كانون الثاني/يناير ٢٠١١. (للاطلاع على التقرير عن ذلك الاجتماع، انظر UNODC/CCPCJ/EG.4/2011/3). وعرض على الاجتماع مشروع جدول الأعمال المؤقَّت (UNODC/CCPCJ/EG.4/2011/1) ومشروع المواضيع المطروحة للنظر فيها في إطار دراسة شاملة بشأن تأثير الجريمة السيبرانية وتدابير التصدي لها (UNODC/CCPCJ/EG.4/2011/2) اللذان أعدتهما الأمانة العامة. واستعرض فريق الخبراء تقريراً إجرائيًّا قصيراً، ومجموعة من المواضيع الفنية المطروحة للنظر فيها في إطار الدراسة، ومنهجية

الرجاء إعادة استعمال الورق

الدراسة وإطارها الزمني الإرشادي، ورفع تقريراً في هذا الشأن إلى لجنة منع الجريمة والعدالة الجنائية في دورتها العشرين (انظر المرفقين الأول والثاني بالوثيقة E/CN.15/2011/19).

٣- واستُهل العمل على إعداد ملخَّص للمداولات الموضوعية ولكنَّ ذلك العمل لم يكتمل بسبب عدم توافر الموارد. ودعت اللجنة في قرارها ٧/٢٢ المؤرَّخ ٢٦ نيسان/أبريل ٢٠١٣ فريق الخبراء إلى إعداد الصيغة النهائية من التقريرين عن ملخَّص مداولاته أثناء اجتماعيه الأول والثاني، المعقودين في فيينا في الفترة من ١٧ إلى ٢١ كانون الثاني/يناير ٢٠١١ ومن ٢٥ إلى ٢٨ شباط/فبراير ٢٠١٣ على التوالي، واعتمادهما. وفي اجتماع المكتب الموسع لفريق الخبراء الذي عقد في ١ كانون الأول/ديسمبر ٢٠١٦، طلب الرئيس إلى المقرِّر وضع الصيغة النهائية للتقريرين عن ملخص مداولاته بحلول نهاية كانون الثاني/يناير ٢٠١٧، وأن يبقي الأمانة والرئيس على علم بالتقدُّم المحرز في عمله. وعملاً بذلك، استعرض المقرِّر، كريستوفر د. رام (كندا)، المذكرات الأصلية وعناصر مشروع الملخص وتسجيلات الاجتماع من أجل إعداد هذا الملخص ووضعه في صيغته النهائية.

٤- واستندت مداولات فريق الخبراء إلى جدول الأعمال بصيغته المعتمدة، ومشروع قائمة المواضيع الفنية، ومنهجية مقترحة للدراسة وُضعت أثناء الدورة. ويكمل هذا الملخص القرارات المتعلقة بنطاق الدراسة الموضوعي أو منهجيتها عن طريق استعراض كل من المسائل الموضوعية التي أثيرت والمعلومات التي قدمها الخبراء في الاجتماع الأول. ويتضمن الملخص آراء الخبراء الحكوميين الدوليين وغيرهم من الخبراء بشأن طائفة من المسائل، بما في ذلك المسائل الموضوعية التي تهم الدول الأعضاء، ومشروع قائمة المواضيع الفنية، وغيرها من المواضيع المقترح إدراجها في الدراسة، والمسائل الإجرائية والمنهجية المتصلة بإجراء الدراسة نفسها. ويجسد الملخص جدول أعمال الاجتماع، ولكن بالنظر إلى أنَّ العديد من المسائل أثيرت أكثر من مرة، يتبع الملخص قدر الإمكان نهجاً مواضيعيًّا.

ثانياً- ملخص المداولات

ألف- مشكلة الجريمة السيبرانية (البند ٢ من جدول الأعمال)

٥- ناقش الخبراء انتشار تكنولوجيات المعلومات والاتصالات والدور الذي تؤديه في بلدانهم، والكيفية التي ترتبط بها هذه العوامل بالجريمة السيبرانية. وأشار أغلب الخبراء إلى أنَّ الجريمة السيبرانية آخذة في الازدياد. كما أشاروا إلى أنَّ هناك صلات ملموسة ومعقَّدة بين (أ) انتشار التكنولوجيات وشيوع استخدامها، سواء داخل الدول الأعضاء أو على الصعيد الإقليمي، و(ب) تطور الجريمة السيبرانية. واعتبرت الجريمة السيبرانية مشكلة عالمية، وإن كانت لا تتخذ بالضرورة نفس الشكل. واتفق عدد كبير من المتكلمين على أنَّ تلك المشكلة تشكل شاغلاً عالميًّا. وأشار عدد من الخبراء إلى أنَّ التعقيد الذي تنطوي عليه أنماط الإجرام والإيذاء، وتدفق البيانات وعائدات الجريمة، بالإضافة إلى عوامل أخرى، تحدث آثاراً تختلف من دولة عضو إلى أخرى. ولوحظ أنَّ انتشار التكنولوجيات ومشكلة الجريمة السيبرانية التي تصاحبه

يثيران أيضاً أسئلة تتعلق بالسيادة الوطنية والاستقلال والحوكمة وحقوق الإنسان والثقافة. وذكر العديد من الخبراء ضرورة احترام الاستقلال السيادي والتنوع الثقافي، عند وضع تعاريف للجريمة السيبرانية، وأيضاً عند النظر في التدابير المحلية وعبر الوطنية والعالمية المتخذة للتصدي لها.

٦- وتكرر ذكر عدة جوانب من مشكلة الجريمة السيبرانية طوال الاجتماع:

(أ) تكنولوجيات المعلومات والشبكات الحاسوبية- أشار الخبراء إلى أنَّ تكنولوجيات المعلومات والشبكات الحاسوبية تمثل فرصة أمام الجهود الإنمائية الداخلية والدولية وهدفا تسعى إليه هذه الجهود في نفس الوقت، وتعتبر أيضاً وسيلة لتقديم المعونة الإنمائية والمساعدة التقنية وزيادة فعاليتهما إلى أقصى قدر ممكن. وقالوا إنَّ الجريمة السيبرانية، من هذا المنظور، تعتبر أيضاً أحد العوامل التي يمكن أن تهدد فرص التنمية. ومن ثم، يعد إيجاد سبل ووسائل للتصدي لتلك الجريمة أمرا ضروريا لجميع الدول الأعضاء. كما أشار الخبراء إلى أنَّ آثار الجريمة السيبرانية والأنشطة ذات الصلة يمكن أن تختلف في البلدان المتقدمة النمو عنها في البلدان النامية، ولكنَّ جميع الدول الأعضاء تشترك في حافز تعزيز التنمية وحمايتها من الجريمة السيبرانية. وبوجه أعم، أشار الخبراء إلى أنه بالنظر إلى أنَّ الشبكات الحاسوبية تتيح للمجرمين المقيمين في إحدى الدول استغلال الهياكل الأساسية في دولة أخرى واستهداف ضحايا مقيمين في تلك الدولة، فإنَّ هناك مصالح مشتركة في منع الجريمة السيبرانية ومكافحتها خارج سياق التنمية؛

(ب) السرعة التي تتطور بها التكنولوجيات والجرائم الحاسوبية، ومدى ذلك التطور- يمثل هذان العاملان تحدياً أمام المشرِّعين ونظم إنفاذ القانون والعدالة الجنائية، ولا سيما في البلدان النامية. وقد أثيرت شواغل بشأن ضرورة ضمان أن تكون القوانين المحلية والصكوك الدولية وبرامج المساعدة التقنية جميعها محدَّثة، وأن تقدم المساعدة التقنية على أساس مستمر؛

(ج) الطابع عبر الوطني للشبكات الحاسوبية والجريمة السيبرانية- لاحظ الخبراء أنَّ الكيانات الرسمية المسؤولة عن التصدي للجريمة السيبرانية وحماية الضحايا والهياكل الأساسية تخضع لقيود السيادة والمحاملة القضائية والولاية الإقليمية، في حين لا يخضع لها المجرمون أنفسهم. وكثيراً ما أثيرت هذه النقطة، ليس في سياق إنفاذ القانون والتعاون الدولي فحسب، ولكن أيضاً فيما يتعلق بمجالات السياسات الأكثر عمومية، وتأثير حقوق الإنسان على الأشكال التي ينبغي أن يتخذها تجريم السلوك السيبراني، وتنظيم التكنولوجيات على الصعيدين الوطني أو العالمي لأسباب لا تتصل بالضرورة بالجريمة؛

(د) تعقُّد الجريمة السيبرانية، والسرعة التي ترتكب بها، والتحديات التي يشكلها هذان العاملان أمام التحقيقات والملاحقات الجنائية، سواء من حيث القدرات التحقيقية المحلية أو أطر التعاون الدولي القانونية أو غير القانونية- نوَّه الخبراء بأنَّ ضرورة إنشاء صلاحيات للتحقيق السريع أو المعجَّل والتوفيق بينها وبين ضمانات سيادة القانون يمثلان تحدياً يواجه المشرعين والمحققين المحليين؛

(هـ) التحديات التي تطرحها سرعة ارتكاب الجريمة السيبرانية وطابعها عبر الوطني- يثير هذان العاملان على نحو متزايد مشاكل تتعلق بسرعة اتخاذ التدابير عند التعامل مع الجريمة السيبرانية. ففي القضايا العابرة للحدود الوطنية، يجب الوصول سريعا إلى البيانات اللازمة، إلاَّ أنَّ اشتراط استخدام القنوات الرسمية للمساعدة القانونية المتبادلة ومراعاة ضمانات سيادة القانون القائمة في جميع الدول المعنية يؤديان إلى زيادة كبيرة في الوقت اللازم للحصول على البيانات؛

(و) انتشار التكنولوجيات في كل مكان والمسائل التي تثيرها في كل جانب من جوانب الحياة تقريباً- من أصغر قرية إلى أعلى مستوى من مستويات العلاقات الاستراتيجية العالمية والدولية، وفي أنشطة كل من القطاعين العام والخاص، هناك أثر لانتشار التكنولوجيات. وسلط الخبراء الضوء على العمل الذي تضطلع به حكوماتهم والجهود المبذولة على الصعيدين الإقليمي ودون الإقليمي. كما رحبوا بوضع تدابير تصد عالمية، وشددوا على الحاجة إلى تلك التدابير وعلى مشاركة الأمم المتحدة في وضعها وتنسيقها.

٧- وأثيرت مسألتان عامتان فيما يتعلق بتدابير التصدي للجريمة السيبرانية:

(أ) الحاجة إلى بيانات عالمية موثوقة وشاملة بشأن طبيعة المشكلة ومداها- تجسدت هذه المسألة في ولاية إجراء الدراسة، والمواد المتفق عليها بشأن المواضيع الفنية في الدراسة ومنهجيتها، التي اعتمدها فريق الخبراء في اجتماعه الأول. وتشمل التحديات المهمة في هذا الصدد النطاق البالغ الاتساع الذي تنطوي عليه المشكلة، والطائفة العريضة من مصادر المعلومات التي يتعين النظر فيها، والحاجة إلى تحديث البيانات وتحليلها على نحو مستمر بغية مراعاة التطورات الدينامية لهذه المشكلة؛

(ب) مسألة الأطر القانونية أو غير القانونية الرامية إلى تنظيم تدابير التصدي الدولية للجريمة السيبرانية والتنسيق بين تلك التدابير- أعرِب عن آراء متباينة في هذا الصدد. إذ رأى بعض الخبراء أنَّ هناك حاجة إلى وضع صك قانوني دولي شامل وعالمي جديد بشأن الجريمة السيبرانية من أجل تحقيق توافق عالمي في الآراء بشأن تدابير التصدي الفعالة وتوفير أساس قانوني دولي واضح لها. وأكد خبراء آخرون أنَّ استخدام النظم القانونية المحلية والدولية القائمة، وزيادة النهج المخصصة في مجال التعاون وتقديم المساعدة التقنية على أساس كل حالة على حدة سوف يكون أسلوبا أكثر فعالية.

٨- وفيما يتعلق بمعنى مصطلح "الجريمة السيبرانية"، شدد عدة خبراء على أنَّ وضع تعريف قانوني وحيد ليس ممكناً، في حين ساد اتفاق عام على الحاجة إلى اتباع نهج وصفي أو تصنيفي كأساس للدراسة قيد النظر وغيرها من البحوث، وكركيزة يقوم عليها التعاون الدولي الفعال. واتفق معظم الخبراء على أنَّ التصنيف الذي وضع في التسعينات من القرن الماضي والوارد في اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية يمثل نقطة انطلاق جيدة، بغض النظر عما إذا كانوا يدعمون الاتفاقية نفسها باعتبارها صكا قانونيا قابلا للتطبيق. فقد شمل ذلك التصنيف النظر في أنواع جديدة من الجريمة لم تصبح ممكنة إلاَّ بفضل التكنولوجيات الجديدة؛ واستخدام التكنولوجيات في ارتكاب جرائم كانت موجودة من قبل أو جرائم مماثلة، بطرائق جديدة في

بعض الأحيان؛ فضلاً عن أنَّ التكنولوجيات تستخدم في كثير من الأحيان من قبل الجماعات الإجرامية المنظمة أو الجماعات الإرهابية أو غيرها بغية تيسير ارتكاب الجرائم أو تفادي كشفها أو إخفاء الأدلة أو عائدات الجريمة.

٩- وأشار عدة خبراء إلى أنَّ احتمالات استخدام التكنولوجيات في ارتكاب جرائم كانت موجودة بالفعل واسعة جدًّا، مما لا يسمح باتباع أيِّ نهج يقوم على وضع قائمة بتلك الجرائم، سواء في الدراسة قيد النظر أو في تطبيقات أخرى. بيد أنه لوحظ أيضاً أنَّ قائمة واقعية بجرائم محدَّدة برزت مع مرور الوقت في المجالات التي ساد فيها توافق في الآراء على أنَّ ظهور أنماط جديدة من الجرائم ذات الصلة بالتكنولوجيا يمثل مشكلة خطيرة أو محددة قد تتطلب مواجهتها تعاوناً دوليًّا وتدابير تصد دولية منسقة. وأكثر الأمثلة التي ذكرت في هذا الصدد هي إنتاج المواد الإباحية القائمة على استغلال الأطفال ونشرها والأنواع الجديدة أو الموسعة من الاحتيال الجماعي.

١٠- وسُلط الضوء أيضاً على عدة تحديات سياساتية أو سياسية تقف عائقا أمام إمكانية التوصل إلى توافق في الآراء بشأن نطاق الجريمة السيبرانية بوصفها مشكلة عالمية، ومن تلك التحديات تزايد اعتماد الدول الأعضاء على التكنولوجيات والشبكات باعتبارها شكلا من أشكال الهياكل الأساسية الحيوية، وما يترتب على ذلك من ظهور الجريمة السيبرانية وغيرها من التهديدات بوصفها مسائل متعلقة بالأمن القومي أو الأمن السيبراني. ولوحظ أنَّ التداخل بين المسائل المتعلقة بالجريمة السيبرانية وتلك المتعلقة بالأمن السيبراني أمر حتمي. ومن بين التحديات الأخرى التي ذكرت أنه في حين لا يوجد توافق دولي في الآراء بشأن التعريف الدقيق لمصطلح "الإرهاب" أو نطاق ذلك المصطلح، فمن الواضح أنَّ بإمكان المنظمات الإرهابية أن تستخدم التكنولوجيات والشبكات، وأنها تستخدمها بالفعل. ويثير ذلك تحديات فيما يتعلق بكل من نطاق الدراسة قيد النظر والجهود المبذولة من أجل منع الجريمة السيبرانية والإرهاب ومكافحتهما بوجه عام. واتفق معظم الخبراء على أنَّ المشاكل المتعلقة بالأمن السيبراني والإرهاب قائمة ويلزم التصدي لها، ولكن اختلفت الآراء بشأن ما إذا كان من الملائم أو المجدي وضع تدابير رامية إلى التصدي لتلك التهديدات في سياق ولاية فريق الخبراء وإجراءات عمله.

١١- ونظر الخبراء أيضاً في المشاكل المتعلقة بقياس المعدلات والاتجاهات في مجال الجريمة السيبرانية وتقييمها. وكان هناك اتفاق على الحاجة إلى معلومات دقيقة على الصعيدين الوطني والعالمي كي تكون بمثابة قاعدة من القرائن تستند إليها الإجراءات المتخذة في المستقبل، سواء في الدراسة قيد النظر أو بوجه أعم، وأثير عدد من التحديات المحددة، حيث أشار عدة خبراء إلى أنَّ المعلومات الإحصائية تقوم عموما على كل من حالات الإبلاغ والملاحقات القضائية، وكلاهما يستند إلى التعاريف القانونية للجرائم. وأشير إلى أنَّ ذلك يغفل السيناريوهات التي يكون فيها استخدام التكنولوجيات عنصرا وقائعيا في الجريمة وليس شرطاً قانونيًّا لوجودها، أو الحالات التي لم تكلل فيها جهود التحقيق أو الملاحقة القضائية بالنجاح، ولا يجسد بالضرورة مختلف النهج التي تتبعها الدول الأعضاء فيما يتعلق بالتجريم. ولوحظ أيضاً أنَّ الجرائم "المظلمة" أو التي لا يبلغ عنها تمثل مشكلة كبيرة بالنظر إلى أنَّ كثيرا من الجرائم السيبرانية لم تكتشف

قط، وفي بعض الحالات، لم يبلغ الضحايا عنها. واعتبر مقدمو الخدمات وغيرهم من كيانات القطاع الخاص مصدراً هامًّا للمعلومات في هذا المجال لأنهم أحياناً هم الذين يتلقون البلاغات عن وقوع مثل هذه الجرائم بدلاً من السلطات العامة، فضلاً عن قدرتهم على تقييم عدد بعض الجرائم أو مدى تفشيها بوسائل تقنية. كما أثير الافتقار إلى القدرات الإحصائية والهياكل الأساسية في البلدان النامية، بوصفه أحد التحديات التي تواجهها جهود المعونة الإنمائية والمساعدة التقنية وكذلك مسألة من المسائل التي يمكن أن تركز عليها تلك الجهود. وأشار الخبراء أيضاً إلى أنَّ التكنولوجيات تنتشر سريعاً وتسفر عن تحولات في العديد من أنشطة الحوكمة والأنشطة الاجتماعية والاقتصادية، الأمر الذي يثير تحديات أوسع نطاقاً فيما يتعلق بتقييم التكاليف المتكبدة وخطورة المشكلة بوجه عام، وتحديات أخرى ذات صلة بالمقارنات الإحصائية على مر الزمن.

باء- التدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي للجريمة السيبرانية، والخيارات المتاحة لتعزيز التدابير القانونية أو غيرها من التدابير القائمة على الصعيدين الوطني والدولي للتصدي للجريمة السيبرانية واقتراح تدابير جديدة في هذا الشأن (البندان ٣ و٤ من جدول الأعمال)

١٢- فيما يتعلق بتدابير التصدي القانونية وغيرها من التدابير القائمة على الصعيد الوطني، قدم العديد من الخبراء ملخصات توضح التدابير التشريعية التي اتخذتها بلدانهم، والتي يعود بعضها إلى عدة عقود خلت، مع اتساع نطاق الجريمة السيبرانية وتطورها. وأشار معظم الخبراء إلى أنَّ بلدانهم قد أدركت خطورة المشكلة، وأنها قد اتخذت إجراءات لمواجهتها في شكل تدابير تصد تشريعية وغير تشريعية. وذكرت نهج مختلفة في هذا الصدد، ولكن لوحظ أنَّ تلك النهج تجسد بوجه عام مزيجا من عمليات تعديل أو تحديث أحكام التجريم والصلاحيات التحقيقية القائمة بموجب القانون الوطني، وسن أحكام جديدة كلية عند الاقتضاء. واتفق معظم الخبراء على ضرورة حماية سلامة الشبكات الحاسوبية ومستخدميها من التهديدات الإجرامية الجديدة والمحددة مثل البرامجيات الحاسوبية الخبيثة وشبكات "البوتنِت"، ومن إمكانية الوصول إلى البيانات المخزنة أو الاتصالات أثناء سريانها بطرائق تنتهك الخصوصية الفردية أو السيادة الوطنية. كما كان هناك اتفاق على الحاجة إلى تجريم أفعال أو تحديث الأحكام الخاصة بها من أجل ضمان التصدي لمشاكل محددة مثل الاحتيال وإساءة استغلال الأطفال. وتشمل المسائل التي تكرر ذكرها فيما يتعلق بتدابير التصدي التشريعية ما إذا كان ينبغي للتعديلات أن تركز على تعديل الجرائم والصلاحيات القائمة، أم أن تتبع نهجا جديدة كلية، وعلى ضرورة صوغ مشاريع أحكام تشريعية على نحو "محايد تكنولوجيا" بحيث لا يتجاوزها الزمن أو تصبح غير قابلة للإنفاذ مع تطور التكنولوجيات.

١٣- وأشار كثير من الخبراء إلى أنَّ من المستصوب أن تكون هناك درجة من المواءمة أو أن تُتَّبع نُهُجٌ مشتركة في التجريم فيما يتعلق بتوفير أساس للتعاون الدولي، ولكن بعضهم أشار أيضاً إلى أنه قد لا يوجد بالضرورة توافق في الآراء بشأن كل جريمة من الجرائم الممكنة، وأكدوا

ضرورة احترام السيادة الوطنية والتنوع الثقافي. وأعرب الخبراء عن مجموعة من الآراء المختلفة بشأن ما إذا كان النهج الأفضل للتنسيق والتعاون الدولي هو المشاركة المفتوحة في وضع صك قانوني دولي جديد، أم استخدام اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية كأساس قانوني أو كمبادئ توجيهية في إطار "قانون غير ملزم"، أم استخدام صكوك أو مبادئ توجيهية قائمة أخرى، أو اتباع نهج مخصص إزاء التعاون وتبادل المعلومات والمساعدة التقنية بحسب كل حالة على حدة. غير أنَّ بعض الخبراء أشاروا إلى أنَّ هناك قيودا تحد من إمكانية المواءمة بالنظر إلى أنَّ العديد من الدول لديها بالفعل قوانين في هذا الصدد، وسيكون من الضروري تقاسم المعلومات بحيث يمكن لكل دولة أن تختار النهج الأمثل لها.

١٤- وأشار عدة خبراء إلى أنَّ مواءمة الجرائم والقوانين المنظمة للتحقيق مرتبطة إلى حد ما بقوانين حقوق الإنسان التي تؤثر على إمكانية الوصول إلى التكنولوجيات والشبكات واستخدامها، وبنطاق الجرائم المتعلقة بمجالات أخرى، مثل النهج المختلفة المتبعة في تنظيم الاستخدامات غير الإجرامية للتكنولوجيات ومقدمي الخدمات ووضع المعايير التقنية. فعلى سبيل المثال، أشير إلى أنَّ بعض أشكال المحتوى المتاح على شبكة الإنترنت مجرمة جنائيًّا في بعض الولايات القضائية، في حين أنها مشمولة بالحماية القانونية المكفولة لحرية المعلومات أو الحق في التعبير في بلدان أخرى. وذكر بعض الخبراء أنَّ هناك تبايناً فيما بين الجرائم العامة أو بين جرائم سيبرانية محدَّدة، مثل استخدام اختلاف أعمار الضحايا كأساس لتحديد الجرائم المرتكبة ضد الأطفال. وأثيرت أيضاً الاختلافات فيما بين أساليب ارتكاب الجرائم في الواقع الفعلي وظهور "الجريمة الموزعة" بمعنى ارتكاب جريمة معقدة على يد جماعات من المجرمين الموجودين في أماكن مختلفة، باعتبارها تحديا يواجه المشرعين والمحققين على حد سواء.

١٥- ولخص عدد من الخبراء النظم التشريعية الوطنية القائمة في بلدانهم فيما يتعلق بالتحقيق في الجريمة السيبرانية. وفي معظم الحالات، تشمل صلاحيات التحقيق صلاحيات عامة تنظم الأساليب المستخدمة مثل التفتيش والضبط، واعتراض الاتصالات، والقواعد والممارسات المتبعة في التحليل الجنائي والأدلة. وذكرت أيضاً الأحكام أو الاختلافات الأكثر تخصصا والموضوعة خصيصا من أجل التصدي للتحديات التي تواجه التحقيق في الجريمة السيبرانية. وتشمل تلك التحديات والتدابير فرض التزامات قانونية على مقدمي الخدمات تلزمهم بالاحتفاظ بالبيانات ومساعدة المحققين عن طريق استرجاع البيانات ذات الصلة واستخراجها من النظم المعقدة التي يستخدمونها، ومنح صلاحيات تحقيقية معجلة تجاوباً مع السرعة التي يمكن أن ترتكب بها الجرائم وإمكانية نقل الأدلة الرقمية أو محوها إذا علم المجرمون بأنَّ هناك تحقيقات تستهدفهم. وأشار الخبراء إلى أنَّ عددا من تقنيات التحقيق القائمة قد كيفت كي يمكن استخدامها في العثور على الأدلة الرقمية وضبطها والاحتفاظ بها على الأجهزة والشبكات. وذكر عدة خبراء أيضاً التحدي المتمثل في مواكبة التطور المستمر في التكنولوجيات والأساليب التي يستخدمها المجرمون من أجل تجنب كشفهم أو مراقبتهم، والحاجة إلى وضع صلاحيات وأساليب جديدة للتحقيق. وفي هذا السياق، لوحظ أنَّ بعض أشكال البرامجيات الحاسوبية الخبيثة يمكن أن تستخدم في إنفاذ القانون بنفس الطريقة التي

يستخدمها بها المجرمون، ولكن يمكن أن يثير استخدامها شواغل هامة ذات صلة بسيادة القانون أو حقوق الإنسان أو الولاية القضائية، تبعا للظروف.

١٦- وفي حين أنَّ نطاق الدراسة وولاية فريق الخبراء يركزان على التدابير المحلية والدولية الرامية للتصدي للجريمة السيبرانية باعتبارها جريمة جنائية أو مسألة من مسائل العدالة الجنائية، أشار عدد من الخبراء إلى أنَّ المجالات القانونية غير الجنائية لها أهمية حاسمة في فهم التدابير المحلية الرامية للتصدي للمشكلة وبناء توافق دولي في الآراء بشأن كيفية التصدي لها. ومن بين هذه المجالات أثير مجال حقوق الإنسان على الصعيدين الوطني والدولي، والذي أشار بعض الخبراء إلى أنَّ له أثرا مباشرا على نطاق التجريم وعلى الصلاحيات والممارسات التحقيقية الوطنية وعبر الوطنية. وفي هذا الصدد، بين الخبراء أنَّ استعداد العديد من الدول للتعاون وقدرتها القانونية على الاضطلاع به يتوقفان على وجود ضمانات مرضية متبادلة فيما يتعلق بسيادة القانون وحقوق الإنسان. وأثيرت أيضاً مسألة مدى اعتبار التدابير الأعم أو الأكثر استباقية فيما يتعلق بحقوق الإنسان، مثل القوانين أو المعايير المتصلة بحماية البيانات، عاملا في هذا الصدد. كما ذكر الخبراء طائفة من القوانين المحلية غير الجنائية التي تطبق على أنشطة مختلفة يضطلع بها القطاع الخاص أو الأفراد وتؤثر على كل من الهياكل الأساسية التي ترتكب فيها الجريمة السيبرانية وقدرة الشركات أو التزامها بالتعاون في مجالي المنع والتحقيق. وكان من بين الأمثلة التي تكرر ذكرها القوانين أو المعايير التقنية ذات الصلة بالخصوصية والهياكل الأساسية المتعلقة بحماية البيانات، والالتزام القانوني بالإبلاغ عن الجرائم أو التعاون مع سلطات إنفاذ القانون بمختلف السبل، والالتزامات القانونية أو الممارسات الطوعية فيما يتعلق بمسائل مثل التشفير والأمن التقني.

١٧- وفيما يتعلق بتدابير التصدي المحلية المقترحة أو الممكنة في المستقبل، سواء القانونية أو غير القانونية، كان هناك اتفاق عام على أنَّ تقدُّماً كبيراً قد أحرز في هذا الصدد في بضع دول أعضاء متقدمة النمو في الثمانينات والتسعينات من القرن الماضي، ثم بدأ في الانتشار على نطاق أعم. ووصف معظم الخبراء الجهود التشريعية وغير التشريعية المبذولة على مدار السنوات القليلة الماضية، وسلط العديد منهم الضوء على تطور الجهود الوطنية الرامية إلى بناء القدرات من أجل مواكبة التطورات التكنولوجية الجديدة. وسلط الضوء على إدماج الجهود الرامية إلى منع الجريمة السيبرانية ومكافحتها في مجالات غير جنائية مثل الحوكمة والتنمية التجارية والاستراتيجيات الإنمائية الوطنية. كما كان هناك اتفاق عام على الحاجة إلى المعونة الإنمائية والمساعدة التقنية من أجل ضمان ألاَّ تسهم الجريمة السيبرانية في إحداث "فجوة رقمية" بين الدول الأعضاء، أو أن تصبح عائقا أمام التنمية. كما اتفق عموماً على أنَّ الجهود الرامية إلى قمع الجريمة السيبرانية في البلدان التي تتمتع بقدرات قوية في مجالي القانون وإنفاذ القوانين لا ينبغي أن تسفر عن نقل هذه المشكلة عبر الوطنية والعالمية إلى بلدان أقل قدرة في هذا المجال. وقدم عدة خبراء معلومات عن جهود المساعدة التقنية الجارية على الصعيدين الوطني والإقليمي. وبين كل من الخبراء الوطنيين وممثلي القطاع الخاص أيضاً أنَّ ذلك النوع من أنشطة منع الجريمة وبناء القدرات يعد مجالاً يملك فيه القطاع الخاص الحافز لتقديم إسهامات ذات شأن كما يتمتع بالقدرة على القيام بذلك.

١٨- وفيما يتعلق بتدابير التصدي القانونية القائمة والمقترحة أو الممكنة، أعرب عن طائفة من الآراء التي انطوت على اختلافات كبيرة فيما يتعلق بالنهج الممكنة. حيث أعرب عن آراء مختلفة بشأن تجريم أشكال معينة من السلوك وبشأن صلاحيات التحقيق أو أساليبه، وأشار العديد من الخبراء إلى استصواب مواءمة القوانين واتباع نهج مشتركة في التجريم، قدر الإمكان، كأساس للتعاون الدولي والمساعدة التقنية على السواء. وأشير إلى أنَّ الجريمة السيبرانية تثير تحديات متشابهة في جميع أنحاء العالم، وأنَّ هناك مصلحة مشتركة في تقاسم الخبرات القانونية وتحديد الثغرات في التجريم أو إنفاذ القوانين التي يمكن أن يستغلها المجرمون وسدها.

١٩- وقدم عدد من الخبراء وعدة منظمات ملاحظات بشأن الأدوار الحالية والممكنة التي يمكن أن تضطلع بها المنظمات الدولية. وأشار الخبراء إلى أنَّ العديد من المنظمات الإقليمية ودون الإقليمية تعمل على وضع الأطر أو المعايير القانونية أو الحفاظ عليها، بما في ذلك اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، والاتفاق المتعلق بالتعاون بين الدول الأعضاء في كومنولث الدول المستقلة لمكافحة الجرائم في مجال المعلومات الحاسوبية (لعام ٢٠٠١)، واتفاق منظمة شنغهاي للتعاون في ميدان أمن المعلومات على الصعيد الدولي، ومعايير الاتحاد الأوروبي ولوائحه ذات الصلة. كما ذكرت مجموعة من أنشطة البحوث والتطوير والمساعدة التقنية أو بناء القدرات. وأشار الخبراء إلى أنَّ هناك حاجة إلى تنسيق الولايات والأنشطة فيما بين الكيانات والأنشطة التي تركز على الجرائم السيبرانية والمجالات ذات الصلة، بما في ذلك حقوق الإنسان والمجالات التجارية وغيرها من مجالات القانون الدولي العام والخاص واللوائح التنظيمية للتكنولوجيا. ورحب العديد من الخبراء بمبادرات المنظمات الإقليمية، غير أنَّ بعضهم بيَّن أنَّ الطابع العالمي الذي تتسم به الشبكات الحاسوبية والجريمة السيبرانية جعل مشاركة الأمم المتحدة مسألة أساسية، ولا سيما لجنة منع الجريمة والعدالة الجنائية ومكتب الأمم المتحدة المعني بالمخدرات والجريمة (المكتب). ورحب بعض الخبراء بالدراسة قيد النظر باعتبارها أول جهد رئيسي يبذل بشأن هذا الموضوع تحت رعاية اللجنة، في حين وجه خبراء آخرون الانتباه إلى الأنشطة السابقة التي اضطلعت بها اللجنة والجمعية العامة والهيئات الأخرى بشأن الجريمة السيبرانية أو الجرائم الحاسوبية.[(١)] وذكر عدة خبراء دليل الأمم المتحدة لمنع الجريمة المتصلة

(١) انظر قرار المجلس الاقتصادي والاجتماعي ٢٣/١٩٩٩، المعنون "عمل برنامج الأمم المتحدة لمنع الجريمة والعدالة الجنائية"، والوثيقتين E/CN.15/2001/4 وE/CN.15/2002/8؛ وتقرير الهيئة الدولية لمراقبة المخدرات لعام ٢٠٠١ (منشورات الأمم المتحدة، رقم المبيع A.02.XI.1)، الفقرات ٥-٨٣؛ وقرار الجمعية العامة ٥٥/٦٣ المؤرخ ٤ كانون الأول/ديسمبر ٢٠٠٠ وقرارها ٥٦/١٢١ المؤرخ ١٩ كانون الأول/ديسمبر ٢٠٠١؛ ومؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين، هافانا، ٢٧ آب/أغسطس - ٧ أيلول/سبتمبر ١٩٩٠: تقرير من إعداد الأمانة العامة (منشورات الأمم المتحدة، رقم المبيع A.91.IV.2)، الفصل الأول، الباب جيم، ومؤتمر الأمم المتحدة العاشر لمنع الجريمة والعدالة الجنائية، فيينا، ١٠-١٧ نيسان/أبريل ٢٠٠٠: تقرير من إعداد الأمانة العامة (منشورات الأمم المتحدة، رقم المبيع A.00.IV.8)، الفقرات ١٦١-١٧٤، ومؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية، بانكوك، ١٨-٢٥ نيسان/أبريل ٢٠٠٥: تقرير من إعداد الأمانة العامة (منشورات الأمم المتحدة، رقم المبيع A.05.IV.7)، الفقرات ٣٢٣-٣٤٠.

بالحواسيب ومكافحتها والذي وضع في عام ١٩٩٤، ورأوا أنه يمكن تحديثه وإعادة إصداره.[٢]

٢٠- وفيما يتعلق بإمكانية وضع صك قانوني دولي أو اتفاقية جديدة بشأن الجريمة السيبرانية، لم يعرب بعض الخبراء عن أيِّ رأي، في حين تبادل آخرون طائفة من الآراء المختلفة بشأن النهج الأمثل في هذا الصدد. وأشير إلى أنَّ المسألة كانت محور مناقشات سياسية، وأسفرت في نهاية المطاف عن التوصل إلى حل توافقي في مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية. وكانت نتائج تلك المناقشات، التي وردت في إعلان سلفادور، أساس الولاية المسندة إلى فريق الخبراء نفسه. وفي هذا السياق، أعرب بعض الخبراء عن قلقهم من أنَّ التركيز على طبيعة الإطار القانوني المحتمل فيما يتعلق بالإجراءات الدولية لمكافحة الجريمة السيبرانية قد تدفع الدول الأعضاء أو الخبراء إلى إغفال صعوبة التصدي للعديد من التحديات المحددة التي تنطوي عليها هذه التدابير أو الاستهانة بتلك الصعوبة، سواء في سياق صك قانوني أو في سياق آخر. وسلط الضوء أيضاً على أنَّ إعلان سلفادور يدعو إلى إجراء دراسة تستعرض الخيارات المتاحة من أجل تعزيز التدابير القائمة واقتراح تدابير جديدة. ويشمل ذلك تدابير قانونية وغير قانونية تهدف للتصدي للجريمة السيبرانية، سواء كانت ذات نطاق وطني أو دولي. كما أشير إلى أنَّ هناك حاجة إلى التوصل إلى نتيجة متوازنة من أجل النظر في جميع تدابير التصدي الممكنة بإنصاف.

٢١- وفيما يتعلق بالدراسة قيد النظر، رأى بعض الخبراء، من الناحيتين الإجرائية والمنهجية، أنها ينبغي أن تشمل النظر في جدوى وضع صك من هذا القبيل ومدى استصواب ذلك، وكذلك في محتوياته ومكوناته الممكنة. ورأى خبراء آخرون أنَّ الغرض من الجزء الأول من الدراسة هو جمع القرائن الوقائعية وتقديمها، وأنَّ النظر في تدابير التصدي القانونية مسألة يتعين على فريق الخبراء واللجنة وغيرهما من الهيئات السياسية النظر فيها بعد جمع القرائن. وساد اتفاق عام على أنَّ النظر في تلك المسألة في نهاية المطاف أمر يعنى به فريق الخبراء نفسه، وأنَّ الدراسة ينبغي أن تنظر في الخيارات المتاحة فيما يتعلق بالقواعد القانونية الفعالة، بما في ذلك الأسس الدولية العامة وغيرها من تدابير التصدي الرامية إلى مكافحة الجريمة السيبرانية (انظر E/CN.15/2011/19، المرفق الأول، الفقرة ٣٣ (ب)). وفي هذا السياق، دارت مناقشة أيضاً بشأن ما إذا كانت الإشارات إلى "صك قانوني دولي" تعني ضمناً الصكوك ذات الطابع العالمي، أم تشمل أيضاً الصكوك الموضوعة أو المتاحة للتصديق عليها أو الانضمام إليها على أساس إقليمي أو غير عالمي فحسب. وأكد بعض الخبراء أنَّ الصكوك غير العالمية المتفق عليها بين دولتين أو أكثر من الدول الأعضاء مثل اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية تظل صكوكاً قانونية دولية، في حين رأى آخرون أنَّ هذا المصطلح يشير إلى الصكوك ذات الطابع العالمي دون غيرها.

٢٢- ومن الناحية الموضوعية، أكد بعض الخبراء أنَّ الترتيبات المخصَّصة أو الصكوك القانونية الموضوعة على الصعيد الإقليمي، ولا سيما اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية،

(٢) استعراض السياسة الجنائية على الصعيد الدولي، الرقمان ٤٣ و٤٤ (منشورات الأمم المتحدة، رقم المبيع A.94.IV.5). وذكر الخبراء أن تحديث الدليل وإعادة إصداره سبق أن أوصت بهما الدراسة التي أجريت عامي ٢٠٠٠-٢٠٠١ بشأن الجريمة السيبرانية والدراسة التي أجريت في الفترة ٢٠٠٤-٢٠٠٧ بشأن الاحتيال الاقتصادي والجرائم المتعلقة بالهوية. انظر الوثيقة E/CN.15/2001/4، الفقرة ٥٢ (أ) '١' والوثيقة E/CN.15/2007/8، الفقرة ٣٧ (ز).

لا تمثل إجراء كافياً، وأنَّ هناك حاجة إلى صك قانوني يصاغ باستخدام عملية مفتوحة أمام الجميع، ويكون متاحاً للتصديق عليه أو الانضمام إليه على الصعيد العالمي تحت رعاية الأمم المتحدة. وكانت حجتهم أنَّ الطابع العالمي لتكنولوجيات المعلومات والاتصالات والجريمة السيبرانية يجعل من صوغ صك قانوني عالمي مسألة ملحة، وأشاروا إلى أنَّ هذه العمليات والصكوك لا تمثل نهجاً جديداً في التصدي للأشكال عبر الوطنية من الجريمة. كما سلط هؤلاء الخبراء الضوء على أهمية التوصل إلى توافق أساسي في الآراء بشأن تدابير التصدي للجريمة السيبرانية كأساس لوضع هذا الصك، وكذلك أهمية الأمم المتحدة بوصفها المحفل الوحيد الذي يمكن فيه التصدي للمسائل ذات الصلة بفعالية. كما أثير عدة شواغل محددة أخرى، بما في ذلك الحاجة إلى إجراء مفاوضات مفتوحة وبناء توافق في الآراء، وعدم استعداد بعض الدول الأعضاء للانضمام إلى اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية لأنها لم تشارك في التفاوض عليه كصك، وعدم قدرة بعض الدول الأعضاء على الانضمام إلى الاتفاقية لأسباب تتعلق بالسياسات أو بسبب المشاكل العملية المرتبطة بأحكام محددة في الاتفاقية ذاتها. وتتعلق تلك المشاكل بأحكام في الاتفاقية تسمح ببعض أشكال التحقيقات المباشرة عبر الحدود، ولا سيما إمكانية الوصول إلى البيانات مباشرة بناء على موافقة الأطراف من القطاع الخاص التي تحوز هذه البيانات أو تتحكم فيها دون اشتراط إخطار الدولة التي توجد البيانات المعنية ماديا في إقليمها أو الحصول على موافقة تلك الدولة. وذكر أولئك الخبراء أيضاً مشاكل مرتبطة بعدم وجود إطار مشترك قانوني أو متعلق بحقوق الإنسان، والاختلافات في السياسات والتقاليد أو الثقافة القانونية فيما يتعلق بعناصر التجريم. كما رأى بعض الخبراء الذين أيدوا صوغ صك قانوني دولي في عملية مفتوحة أنَّ اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية قد عفا عليها الزمن بالفعل، وأنها لا تتناول مسائل أخرى يرون أنه ينبغي النظر فيها أو إدراجها.

٢٣- وأكد خبراء آخرون أنَّ صوغ صك قانوني دولي جديد على أساس مفتوح مسألة غير ممكنة بالنظر إلى إلحاح المشكلة وحجم بعض المسائل التي سيتعين حلها على أساس توافق الآراء. وأشاروا إلى أنَّ هذه المسألة قد أثيرت في مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية وفي مناسبات سابقة، ورأوا أنَّ مواقف الدول بشأن طائفة من المسائل ذات الصلة بالسيادة الوطنية والقانون المحلي متباينة إلى درجة لا تسمح بصوغ صك مفيد وفعال في غضون فترة زمنية معقولة. وأعربوا عن أملهم في أن تساعد الدراسة على توضيح أوجه التشابه والاختلاف في النهج المتبعة في القوانين الوطنية ومدى إمكانية التوصل إلى توافق في الآراء. وقالوا إنَّ النهج الأفضل، في رأيهم، هو التركيز على احتياجات المساعدة التقنية الأكثر إلحاحاً واستحداث وسائل تعاون غير رسمية تتيح إجراء التحقيقات بصورة عاجلة. وأكدوا أنَّ السيادة والولاية القضائية وحقوق الإنسان يمكن أن تكون عوامل مؤثرة، ولكن قد لا يمكن بالضرورة تجاوز التحديات المرتبطة بها. ورأوا أيضاً أنَّ المشكلة الرئيسية التي تقف عائقا أمام إنفاذ القانون هي الافتقار إلى القدرات الوطنية والقنوات غير الرسمية المناسبة، وأنَّ ذلك ينبغي أن يكون محور التركيز في المستقبل. وأفاد هؤلاء الخبراء أيضاً بأنَّ درجة التعقيد التي تنطوي عليها الجريمة السيبرانية والسرعة التي يمكن أن ترتكب بها تشيران إلى أنَّ هناك حاجة إلى وضع نهج مرنة تختلف بحسب الحالة، ولا سيما فيما يتعلق بأساليب التحقيق المسموح بها في بعض الولايات

القضائية دون غيرها. وفي هذا الصدد، أعربوا عن رأي مفاده أنَّ بناء الثقة المتبادلة بين سلطات إنفاذ القانون من خلال الوسائل المتاحة، مثل منظومات الشبكات العاملة على مدار الساعة طوال أيام الأسبوع، مسألة هامة. كما أعربوا عن قلقهم من أنَّ محاولة وضع صك قانوني دولي شامل جديد بشأن الجريمة السيبرانية سوف تستغرق وقتا طويلا، وأنَّ نجاحها غير مضمون. وعلى هذا الأساس، رأوا أنه ما دامت هناك حاجة إلى إطار قانوني دولي، فإنَّ أفضل خيار هو استخدام اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، التي وضعت في إطار مجلس أوروبا ولكن باب الانضمام إليها مفتوح أمام الدول الأخرى. وذكر عدد من الخبراء أنَّ اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية تمثل أيضاً أداة قيمة باعتبارها من خيارات "القانون غير الملزم" في إرشاد الدول الأعضاء كأساس يستند إليه في أحكام التجريم أو صلاحيات التحقيق أو الأدلة الإلكترونية أو غير ذلك من القوانين، حتى وإن كانت هذه الدول غير مستعدة للانضمام للاتفاقية وتنفيذها بالكامل أو غير قادرة على ذلك.

٢٤- وبوجه عام، ركزت المناقشات بشأن إمكانية وضع صك قانوني دولي عالمي وشامل على مدى استصواب وضع صك من هذا القبيل أو مدى جدواه، بدلا من التركيز على ما قد يحتويه ذلك الصك أو المسائل المحددة التي يحتمل أن تثار في المفاوضات بشأنه. وأشار عدة خبراء إلى أنَّ المسألة الأخيرة تشكل عنصراً هامًّا في الدراسة التي ستحدد المسائل والتحديات القائمة وتقترح نهجا لحلها. وأثار أحد الخبراء تفاصيل أكثر تحديداً، مقترحاً إمكانية اتباع الشكل الأساسي لاتفاقية الأمم المتحدة لمكافحة الفساد فيما يتعلق بمسائل مثل التجريم والمنع والمساعدة التقنية والتعاون الدولي وحماية السيادة الوطنية. وأشار خبير آخر إلى أنه في حين أنَّ المناقشات بشأن مسألة الإرهاب على الصعيد العالمي يمكن أن تتسم بالصعوبة، ستكون هناك على الأقل إمكانية للنظر في توسيع نطاق هذا الصك ليشمل جرائم إرهابية محددة أو جرائم ذات صلة، وأنه يرجح أنَّ بعض استخدامات الجماعات الإرهابية للتكنولوجيا سوف تكون مشمولة بأحكام تستهدف الجريمة السيبرانية بوجه عام.

٢٥- وذكرت أيضاً في هذا السياق اتفاقية الجريمة المنظمة. واعتبر بعض الخبراء أنَّ الاتفاقية تمثل أداة مفيدة، بالنظر إلى أنَّ معظم الدول الأعضاء قد صدقت عليها أو انضمت إليها. وعلاوة على ذلك، يبدو أنَّ قدرا كبيرا من الجريمة السيبرانية له "طابع عبر وطني" وينطوي على وجود "جماعة إجرامية منظمة" خلفه، ومن ثم، فهو يفي بمتطلبات المادة ٣ بشأن نطاق انطباق الاتفاقية. وأشار خبراء آخرون إلى أنَّ نطاق الاتفاقية لا يشمل سيناريوهات الجريمة السيبرانية التي لا تشارك في ارتكابها الجماعات الإجرامية المنظمة، فضلا عن أنَّ الاتفاقية لم تتناول الأشكال المتخصصة من التعاون الدولي والتي قد تكون لازمة في قضايا الجريمة السيبرانية. كما أثيرت شكوك بشأن مدى خطورة بعض أشكال الجريمة السيبرانية، وما إذا كانت تفي بعتبة "الجريمة الخطيرة" اللازمة لتطبيق تلك الاتفاقية بحسب التعريف الوارد في الفقرة (ب) من المادة ٢. وأعرب عن طائفة من الآراء المماثلة فيما يتعلق بتطبيق صكوك مكافحة الإرهاب والفائدة المرجوة من ذلك فيما يتعلق بالسيناريوهات التي يهاجم فيها الإرهابيون التكنولوجيات أو الشبكات أو يستخدمونها لأغراض أخرى.

٢٦- وأثيرت أيضاً عدة تحديات محدَّدة فيما يتعلق بأطر التعاون الدولي القانونية القائمة أو الممكنة في المستقبل، بما في ذلك الحاجة إلى وضع حلول فعالة لبعض المشاكل العامة المبينة في الفقرة ٧ من هذا التقرير. وفيما يخص التعاون الدولي بوجه عام، أعرب عن طائفة من الآراء فيما يتعلق بكيفية تقديم هذا التعاون في الوقت المناسب، سواء بموجب الصكوك القانونية الدولية والإقليمية القائمة، مثل اتفاقية الجريمة المنظمة واتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، أو استناداً إلى مختلف الأسس الثنائية وغير الرسمية. وأثار عدد من الخبراء شواغل فيما يتعلق بالحاجة إلى التوصل إلى توافق في الآراء بشأن معايير التحليل الجنائي ذات الصلة بجمع البيانات الرقمية وحفظها ونقلها وتوثيقها واستخدامها كأدلة في الدعاوى الجنائية أو الدعاوى القانونية الأخرى. وأشار بعض الخبراء أيضاً إلى أنَّ الاختلافات في القوانين الوطنية المتعلقة بجواز استخدام أساليب مثل اعتراض الاتصالات واختراق الأنشطة الإجرامية أو انتحال شخصية المجرمين أو "الإيقاع" بهم يمكن أن تثير شواغل فيما يتعلق بالسيناريوهات التي تنطوي على تحقيقات على شبكة الإنترنت أو تؤثر على ولايات قضائية أخرى. وأشار خبراء آخرون إلى أنه قد تنشأ خلافات فيما يتعلق بمتطلبات حقوق الإنسان المنصوص عليها في القوانين الوطنية، واستخدموا كمثال على ذلك الاختلافات في تدابير حماية الخصوصية المطبقة على البيانات المستخدمة في توجيه الاتصالات وتعقبها وعلى المضمون الفعلي الذي تنطوي عليه تلك الاتصالات.

٢٧- وفيما يتعلق بإجراءات التحقيق العابرة للحدود الوطنية، رأى عدد من الخبراء، ولا سيما من لهم خلفية في مجال إنفاذ القانون، أنَّ قنوات المساعدة القانونية المتبادلة التقليدية ضرورية في القضايا عبر الوطنية، ولكنها لم تعد كافية في القضايا ذات الصلة بالجريمة السيبرانية. وأكدوا أنَّ السرعة التي بات يمكن للمجرمين ارتكاب الجريمة السيبرانية بها، ثم حذف الأدلة الإلكترونية على الجريمة أو إخفاؤها، تتطلب صلاحيات وأساليب تحقيقية أسرع وأكثر مباشرة. وساد اتفاق عام على أنَّ مسألة السرعة تثير مشكلة خطيرة آخذة في الاتساع، ولكن العديد من الخبراء سلطوا الضوء أيضاً على ضرورة احترام السيادة الوطنية والمساواة والاستقلالية والولاية القضائية الإقليمية. واحتجت المجموعة الأخيرة من الخبراء بأنه على الرغم من أنَّ آليات المساعدة القانونية المتبادلة قد تكون أكثر فعالية، فإنَّ وظيفتها الأساسية هي حماية السيادة ومنع التحايل على متطلبات سيادة القانون الأساسية في كل دولة، بما في ذلك المتطلبات التي تنفذ ضمانات حقوق الإنسان والضمانات الإجرائية. وكان ذلك أيضاً أحد الشواغل المحددة التي أثيرت فيما يتعلق باتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية. ورأى أحد الخبراء أنَّ الاتفاقية ذهبت أبعد من اللازم فيما يتعلق بالسماح بالوصول إلى البيانات عبر الحدود الإقليمية، في حين أعرب خبير آخر عن أمله في أن تعدل الأحكام ذات الصلة كي تسمح بالمزيد من الوصول إلى البيانات عبر الحدود الإقليمية. ورأى الخبراء في مجال إنفاذ القانون عموما أنَّ الفجوة بين الأطر الزمنية القصيرة التي تجرى فيها التحقيقات والأطر الزمنية الأطول التي يجري فيها التعاون الدولي هي أخطر تحد يواجه التحقيق في قضايا الجريمة السيبرانية المرتكبة عبر الحدود الوطنية وملاحقة مرتكبيها قضائيًّا. كما أشار عدة خبراء إلى أنَّ المشاكل تزداد خطورة باطراد مع ظهور تطورات مثل "الحوسبة السحابية" التي تزيد من عدد الولايات

القضائية المختلفة التي يحتمل أن تكون ضالعة في هذه القضايا، وتجعل أماكن مرتكبي الجرائم أقل وضوحاً ويصعب التأكد منها في غضون الفترات الزمنية القصيرة المتاحة. كما أثار الخبراء شواغل أكثر عمومية بشأن الحاجة إلى التوصل إلى صيغ أو تفاهمات عملية بشأن كيفية توزيع المسؤولية عن عناصر التحقيق والملاحقة القضائية بين مختلف الولايات القضائية التي تطالب بها في السيناريوهات التي تشمل عدداً من الدول المختلفة.

٢٨- وسلط عدة خبراء وممثلين عن القطاع الخاص الضوء على أهمية المنع. وذكر في هذا الصدد كل من الوسائل التقنية، مثل استخدام التطبيقات الأمنية لحماية سلامة النظم والبيانات، والوسائل الاجتماعية، مثل تثقيف مستخدمي النظم وإدراج عناصر الجريمة السيبرانية في البرامج المدرسية والجامعية ذات الصلة. وأشار خبراء إلى أنَّ ما تتسم به بعض أنشطة الجريمة السيبرانية من نطاق بالغ الاتساع وطابع مستمر، بما في ذلك البريد الإلكتروني الطفيلي وشبكات "البوتنت"، يضفي أهمية على وجود القدرة على التدخل أثناء استمرار ارتكاب فرادى الجرائم ضد ضحايا جدد، والتي يكون مصدرها في كثير من الأحيان أجهزة مؤتمتة. واعتبر أنَّ القدرة على تعقب البرامجيات الحاسوبية الخبيثة وإزالتها من الأجهزة المصابة مسألة ضرورية، سواء كتدبير وقائي لمنع ارتكاب الجرائم أو تدبير تحقيقي يهدف إلى التصدي لها. ومن بين التدابير ذات الصلة ذكرت إمكانية إنشاء الصلاحيات والقدرات اللازمة لمنع أو "إسقاط" المواقع الإلكترونية التي تستخدم في ارتكاب الجرائم أو التي تنشر محتوى غير قانوني أو برامجيات حاسوبية خبيثة. وجرت أيضاً مناقشة بشأن مسائل القانون الجنائي وحقوق الإنسان والولاية القضائية والمسائل التقنية التي يثيرها تدبير من هذا القبيل. وأوضح بعض الخبراء أنَّ تدبيرا كهذا يتطلب صلاحيات قانونية وكذلك قدرة تقنية على تتبع البرامجيات الحاسوبية الخبيثة وإزالتها. ولاحظ آخرون أنَّ مشغلي الهياكل الأساسية من القطاع الخاص يمكن أن يضطلعوا بدور هام سواء في تطوير النظم المقاومة للبرامجيات الحاسوبية الخبيثة أو في إزالة تلك البرمجيات. وأشير إلى أنَّ التعاون بين القطاعين العام والخاص عبر الحدود أمر مهم لأنَّ شبكات "البوتنت" لها طابع عبر وطني.

٢٩- وفي سياق إعلان سلفادور والتكليف الصادر بإعداد الدراسة، أثيرت الأدوار الهامة التي يضطلع بها القطاع الخاص والحاجة إلى التعاون الفعال بين القطاعين العام والخاص. وأثار عدد من الخبراء وممثلي القطاع الخاص مسائل تتعلق بالتعاون بين القطاعين العام والخاص. وأشير إلى أنَّ نطاق أنشطة القطاع الخاص وتطورها في مختلف البيئات التقنية والتنظيمية يجعل تعريف مصطلحات رئيسية مثل "مقدم الخدمات" للأغراض القانونية أمرا صعبا، غير أنَّ ذلك لا يمثل بالضرورة عقبة أمام وضع ممارسات تعاون جيِّدة. ومن منظور القطاع الخاص، أشير إلى أنَّ الوفاء بالاحتياجات القانونية في مختلف البلدان يشكل تحدياً كبيراً يواجه الشركات ذات الأنشطة الدولية. كما أشير إلى أنه في حين أنَّ الحكومات تميل إلى اعتبار القطاع الخاص كياناً واحداً، إلاَّ أنه فعليا يتألف من طائفة هائلة الاتساع من الكيانات المختلفة من حيث المهام والقدرات، الأمر الذي تترتب عليه آثار هامة عند طلب مختلف أشكال المساعدة أو التعاون.

٣٠- وأبرز عدة خبراء ضرورة تحديد الجهود الناجحة في هذا المجال والاستفادة منها، وضرورة إذكاء الوعي في أوساط العاملين في مجال إنفاذ القانون بما يمكن للقطاع الخاص أن يقوم به وما ليس في وسعه. وذكر الخبراء أنَّ التعاون ممكن ومستصوب في طائفة واسعة نسبيا من المجالات

المحددة، بما في ذلك المنع، والتعاون في التحقيقات، وجمع المزيد من المعلومات العامة بشأن تطورات الجريمة واتجاهاتها، وتدريب المحققين وخبراء التحليل الجنائي على التكنولوجيات الجديدة فور استحداثها والبدء في تسويقها. ومن المسائل المحددة التي ذكرها الخبراء فيما يتعلق بالتعاون في التحقيقات بين القطاعين العام والخاص مدى انطباق الضمانات القانونية عند مشاركة الشركات الخاصة في أنشطة التحقيق. وشملت المسائل ذات الصلة تطبيق الرقابة القضائية وضمانات حقوق الإنسان وحماية السيادة الوطنية في حال كانت أنشطة التحقيق تنطوي على شركات أو أنشطة عبر وطنية، ومقبولية المعلومات التي يجري الحصول عليها كأدلة.

٣١- وسلط عدد من الخبراء الضوء على أهمية المساعدة التقنية وتبادل المعلومات، سواء بموجب صك قانوني دولي شامل أو على أساس الاحتياجات الأكثر إلحاحاً وبحسب وسائل تقديم المساعدة. وأشير إلى أنَّ المسألة نفسها قد اعتبرت أولوية منفصلة ومحددة في إعلان سلفادور. وشدد عدة خبراء على أنَّ هناك حاجة ملحة إلى المساعدة التقنية ولا يمكن تأجيلها أو التأخر في تقديمها رهن الانتهاء من الدراسة الجارية. وأشير أيضاً إلى أنَّ طبيعة المشكلة تتطلب أن يكون تبادل المعلومات على أساس المعاملة بالمثل. وذكر بعض الخبراء أنَّ المساعدة التقنية ذات الصلة بالجريمة السيبرانية تتصل أيضاً بمسائل أعم بما في ذلك الاستراتيجيات الإنمائية وطائفة من الجهود أو المشاريع المحددة. وأشارت الأمانة إلى أنَّ مكتب الأمم المتحدة المعني بالمخدرات والجريمة قد أسندت إليه ولاية تطوير المساعدة التقنية وتقديمها ولا يحتاج سوى إلى ما يلزم من الموارد الخارجة عن الميزانية لبدء العمل. وأعرب خبراء يمثلون منظمات حكومية دولية أخرى عن استعدادهم للتعاون في جهود المساعدة التقنية.

٣٢- وأثيرت عدةَ مرات أثناء الدورة مسألتا نطاق الدراسة والعمل المقبل بشأن الجريمة السيبرانية وعلاقتهما بمسائل أعمَّ تتصل بأمن الفضاء الإلكتروني والإرهاب. وفيما يتعلق بالمسائل المتصلة بالإرهاب، توصل الخبراء في نهاية المطاف إلى توافق في الآراء على أنه ينبغي للدراسة أن تتفادى الدخول في تحقيقات واسعة النطاق أو مفتوحة فيما يتعلق بالإرهاب. وبقدر ما أثير أثناء الدورة، ينبغي التركيز على الجريمة السيبرانية ذاتها في سياق الإرهاب (انظر E/CN.15/2011/19، الفقرة ٣). وأوضح عدة خبراء بوجه أعم أنَّ التطورات في مجالي الأمن السيبراني والإرهاب سوف تشكل تحديات وتهيئ فرصاً للتآزر الممكن فيما يتعلق بالأنشطة المقبلة التي يمكن أن تسفر عنها الولاية الحالية المسندة إلى فريق الخبراء والدراسة نفسها. ولوحظ أنه في حين أنَّ الدول الأعضاء قد تولي الاعتبار، فيما يتعلق بوضع السياسات، للتهديدات الأخطر مثل الأمن السيبراني، فإنَّ معظم الأنشطة الفعلية ذات الصلة سوف تكون في نطاق الجرائم القائمة المحددة أو العامة، أو العمل الممكن في المستقبل بشأن الجريمة السيبرانية. وأبديت ملاحظات مماثلة فيما يتعلق بالإرهاب السيبراني. وأشير إلى أنَّ معنى مصطلح "الإرهاب السيبراني" ليس واضحاً تماماً، وأنه لا يوجد توافق دولي في الآراء بشأن نطاق مصطلح "الإرهاب". بيد أنَّ هذا الأمر لا يمنع بالضرورة إحراز تقدم في التوصل إلى توافق في الآراء بشأن المشاكل أو الأنشطة المحددة وتنفيذه. وأشير أيضاً إلى أنَّ العديد من الأنشطة المضطلع بها لدعم الجماعات الإرهابية على شبكة الإنترنت تكون مشمولة ضمن جرائم أعم.

جيم- دراسة شاملة عن الجريمة السيبرانية (البند ٥ من جدول الأعمال)

٣٣- يرد توثيق الاتفاق الذي توصل إليه فريق الخبراء في اجتماعه الأول في مرفقات تقريره الإجرائي المقدَّم إلى لجنة منع الجريمة والعدالة الجنائية (انظر UNODC/CCPCJ/EG.4/2011/3 و E/CN.15/2011/19). وفي سياق النظر في الخيارات الممكنة بشأن الدراسة، أعرب عن عدد من المسائل والنهج. وقدمت الأمانة تقديرات بشأن تكاليف إصدار وثيقة دراسة مكونة من نحو ١٥٠ إلى ٢٠٠ صفحة وتكاليف عقد الاجتماعات المقبلة لفريق الخبراء. كما أشير إلى أنه في حين أنَّ الميزانية العادية قد غطت تكاليف الاجتماع الأول، فإنَّ الاضطلاع بمزيد من العمل من جانب فريق الخبراء وداخل مكتب الأمم المتحدة المعني بالمخدرات والجريمة يتوقف على تقديم مساهمات خارجة عن الميزانية. وجرت مناقشة بشأن الخيارات الأخرى، بما في ذلك استخدام أفرقة فرعية أصغر حجماً وأقل تكلفة، غير أنَّ المجتمعين توصلوا إلى اتفاق عام على أنَّ الدراسة لا بد أن تظل تحت سيطرة فريق الخبراء ذاته من أجل ضمان أن تظل أنشطة الرقابة على الأعمال والنتائج مفتوحة وحكومية دولية على حد سواء. وأكد معظم الخبراء أنَّ المسائل المثارة تتطلب النظر فيها على المستوى الحكومي، وأنَّ العملية يجب أن تظل مفتوحة أمام جميع الدول الأعضاء. ومع ذلك، اتفق على أنه بإمكان كل مجموعة إقليمية أن تعين بحد أقصى ستة خبراء حكوميين يمكن للأمانة أن تتشاور معهم بشأن مسائل محدَّدة بحسب الحاجة. وأعرب عن الثقة في حياد الأمانة بوصفها الوكالة الرئيسية المسؤولة عن إجراء البحوث وتقديم التقارير بشأنها، وشدد على أنَّ النتائج النهائية سوف تخضع للاستعراض من قبل فريق الخبراء الحكومي الدولي المفتوح العضوية قبل إحالتها إلى لجنة منع الجريمة والعدالة الجنائية.

دال- الاستنتاجات والتوصيات، واعتماد التقرير، واختتام الاجتماع (البنود من ٦ إلى ٨ من جدول الأعمال)

٣٤- كما ذُكر أعلاه، اعتمد فريق الخبراء التقرير الإجرائي القصير الذي أعدته الأمانة، بالإضافة إلى مجموعة المواضيع الفنية التي ستشملها الدراسة والمنهجية التي ستتبعها استناداً إلى ما رآه الفريق وعدله أثناء الاجتماع. وفيما عدا ذلك، لم تقترح أو ينظر في أيِّ استنتاجات أو توصيات محددة.[٣] واتفق على أنَّ التقارير المتعلقة بنتائج اجتماعات مكتب فريق الخبراء سوف تصدر وتوزع من خلال المجموعات الإقليمية. وأشار المقرِّر إلى أنه بالإضافة إلى النصوص الموضوعية والمنهجية المعتمدة، سيعد تقرير يلخص مداولات فريق الخبراء ويعمم للموافقة عليه حالما يمكن معالجته وتوزيعه بجميع اللغات الرسمية الست.[٤]

---

(٣) ترد معلومات إضافية بشأن البنود من ٦ إلى ٨ في تقرير اجتماع فريق الخبراء الحكومي الدولي المفتوح العضوية المعني بإجراء دراسة شاملة عن مشكلة الجريمة السيبرانية المعقود في فيينا في الفترة من ١٧ إلى ٢١ كانون الثاني/يناير ٢٠١١ (E/CN.15/2011/19).

(٤) كما ذكر في الفقرة ٢ أعلاه، لم يجرِ ذلك بعد الاجتماعين الأول (٢٠١١) والثاني (٢٠١٣) بسبب عدم توافر الموارد.