UNODC/CCPCJ/EG.4/2020/2

24 August 2020
Arabic
Original: English

تقرير عن اجتماع فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، المعقود في فيينا في الفترة من 27 إلى 29 تموز/يوليه 2020

أولا- مقدمة

1- طلبت الجمعية العامة في قرارها 230/65 إلى لجنة منع الجريمة والعدالة الجنائية أن تنشئ، وفقا للفقرة 42 من إعلان سلفادور بشأن الاستراتيجيات الشاملة لمواجهة التحديات العالمية: نظم منع الجريمة والعدالة الجنائية وتطورها في عالم متغير، فريق خبراء حكوميا دوليا مفتوح العضوية ينعقد قبل دورة اللجنة العشرين من أجل إجراء دراسة شاملة لمشكلة الجرائم 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.

2- وعقد الاجتماع الأول لفريق الخبراء في فيينا في الفترة من 17 إلى 21 كانون الثاني/يناير 2011. واستعرض فريق الخبراء واعتمد، في ذلك الاجتماع، مجموعة من المواضيع ومنهجية من أجل تلك الدراسة (E/CN.15/2011/19، المرفقان الأول والثاني).

3- وعقد الاجتماع الثاني لفريق الخبراء في فيينا في الفترة من 25 إلى 28 شباط/فبراير 2013. وأحاط فريق الخبراء علما في ذلك الاجتماع بمشروع الدراسة الشاملة لمشكلة الجريمة السيبرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها، الذي أعده مكتب الأمم المتحدة المعني بالمخدرات والجريمة (المكتب المعني بالمخدرات والجريمة)، بتوجيه من فريق الخبراء، عملا بالولاية المتضمنة في قرار الجمعية العامة 230/65، ومجموعة المواضيع ومنهجية الدراسة، وفق ما اعتمده فريق الخبراء في اجتماعه الأول.

4- وفي إعلان الدوحة بشأن إدماج منع الجريمة والعدالة الجنائية في جدول أعمال الأمم المتحدة الأوسع من أجل التصدي للتحديات 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 174/70، نوهت الدول الأعضاء بأنشطة فريق الخبراء، ودعت لجنة منع الجريمة والعدالة الجنائية إلى النظر في إصدار توصية بأن يواصل فريق الخبراء، مستندا إلى عمله، تبادل المعلومات عن التشريعات الوطنية، والممارسات الفضلى، والمساعدة التقنية، والتعاون الدولي، بغية دراسة الخيارات المتاحة

الرجاء إعادة استعمال الورق

لتعزيز التدابير القانونية أو غيرها من التدابير القائمة على الصعيدين الوطني والدولي للتصدي للجريمة السيبرانية واقتراح تدابير جديدة في هذا الشأن.

5- وعقد الاجتماع الثالث لفريق الخبراء في فيينا في الفترة من 10 إلى 13 نيسان/أبريل 2017. وفي ذلك الاجتماع، نظر فريق الخبراء، ضمن جملة أمور، في اعتماد ملخصي المقرر لمداولات الاجتماعين الأول والثاني لفريق الخبراء، ومشروع الدراسة الشاملة لمشكلة الجريمة السيبرانية والتعليقات الواردة بشأنها ومسارات العمل المقبلة في إعداد مشروع الدراسة. كما جرى تبادل المعلومات عن التشريعات الوطنية والممارسات الفضلى والمساعدة التقنية والتعاون الدولي.

6- وطلبت لجنة منع الجريمة والعدالة الجنائية، في قرارها 4/26، الذي اعتمدته في دورتها السادسة والعشرين المعقودة في أيار/مايو 2017، 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 سلفادور والدوحة. وطلبت أيضا في ذلك القرار إلى فريق الخبراء أن يواصل تبادل المعلومات عن التشريعات الوطنية، والممارسات الفضلى، والمساعدة التقنية، والتعاون الدولي، بغية دراسة الخيارات المتاحة من أجل تعزيز التدابير القانونية أو غيرها من التدابير القائمة على الصعيدين الوطني والدولي للتصدي للجريمة السيبرانية واقتراح تدابير جديدة في هذا الشأن.

7- وعقد الاجتماع الرابع لفريق الخبراء في فيينا في الفترة من 3 إلى 5 نيسان/أبريل 2018. وركز فريق الخبراء خلال الاجتماع على موضوعي التشريعات والأطر، والتجريم في سياق الجريمة السيبرانية. ونوقشت التطورات التشريعية والسياساتية في مجال التصدي للجريمة السيبرانية على الصعيدين الوطني والدولي. ونظر فريق الخبراء أيضا في سبل تجريم الأفعال التي تمثل جريمة سيبرانية على الصعيد الوطني. واعتمد فريق الخبراء خلال ذلك الاجتماع أيضا المقترح الذي قدمه الرئيس بشأن خطة عمل فريق الخبراء للفترة 2018-2021 (UNODC/CCPCJ/EG.4/2018/CRP.1).

8- وعقد الاجتماع الخامس لفريق الخبراء في فيينا في الفترة من 27 إلى 29 آذار/مارس 2019. وركز فريق الخبراء في ذلك الاجتماع على موضوعي إنفاذ القانون والتحقيقات، والأدلة الإلكترونية والعدالة الجنائية في سياق الجريمة السيبرانية. وناقش فريق الخبراء أيضا في ذلك الاجتماع، من بين جملة أمور، الجهود الوطنية الناجحة المبذولة لتنفيذ تدابير قانونية وإجرائية تهدف للتصدي للجريمة السيبرانية، والتدابير الرامية إلى استخدام أدوات استقصائية جديدة لجمع الأدلة الإلكترونية والتثبت من صحتها لأغراض الاستدلال في الإجراءات الجنائية. وركزت المناقشة أيضا على كيفية تحقيق التوازن بين الحاجة إلى تدابير فعالة في إطار إنفاذ القانون للتصدي للجريمة السيبرانية وحماية حقوق الإنسان الأساسية، وخاصة الحق في الخصوصية. وأعطى فريق الخبراء الأولوية للحاجة إلى بناء القدرات بصورة مستدامة بغرض تعزيز القدرات المحلية والتمكين من تبادل الممارسات والتجارب الجيدة في مجال التحقيق.

9- وسلمت الجمعية العامة، في قرارها 173/74 بأهمية العمل الذي يقوم به فريق الخبراء في مواصلة 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؛ ولاحظت الجمعية العامة مع التقدير أن فريق الخبراء سيضع، وفقا لخطة عمله للفترة 2018-2021، استنتاجات وتوصيات يمكن تقديمها إلى لجنة منع الجريمة والعدالة الجنائية؛ وسلمت بأن فريق الخبراء هو منبر مهم لتبادل المعلومات عن التشريعات الوطنية والممارسات الفضلى والمساعدة التقنية والتعاون الدولي؛ وطلبت إلى المكتب المعني بالمخدرات والجريمة أن يواصل جمع

المعلومات دوريا عن التطورات الجديدة والتقدم المحرز والممارسات الفضلى المستبانة، وأن يواصل إبلاغ هذه المعلومات إلى فريق الخبراء وإلى اللجنة؛ ودعت فريق الخبراء إلى أن يقوم، استنادا إلى ما ينهض به من أعمال ودون المساس بالمسائل الأخرى المندرجة في إطار ولايته، بتزويد المكتب المعني بالمخدرات والجريمة بالمشورة اللازمة، بما يشمل الجوانب المتعلقة بالبرنامج العالمي المعني بالجريمة السيبرانية، من أجل المساعدة في استبانة الاحتياجات ذات الأولوية القصوى في مجال بناء القدرات وتدابير التصدي الفعالة، وذلك دون المساس بوضع اللجنة بصفتها الهيئة الإدارية لبرنامج الجريمة التابع للمكتب.

10- وكان المكتب الموسع لفريق الخبراء قد وافق، من خلال إجراء الموافقة الصامتة، في 11 تشرين الثاني/نوفمبر 2019 على التاريخ الأصلي لعقد الاجتماع السادس لفريق الخبراء، وهو الفترة من 6 إلى 8 نيسان/أبريل 2020. وفي 18 كانون الأول/ديسمبر 2019، وافق المكتب الموسع، من خلال إجراء الموافقة الصامتة، على جدول الأعمال المؤقت للاجتماع السادس. وفي 12 آذار/مارس 2020، أُبلغ المكتب الموسع بأنه تقرر تأجيل الاجتماع بسبب القيود المفروضة المتعلقة بجائحة فيروس كورونا (كوفيد-19). وفي 15 نيسان/أبريل 2020 وافق المكتب الموسع، من خلال إجراء الموافقة الصامتة، على التاريخ الجديد للاجتماع السادس لفريق الخبراء، وهو من 27 إلى 29 تموز/يوليه 2020. وفي 22 حزيران/يونيه 2020، تمت الموافقة على عقد الاجتماع السادس في شكل هجين، بالحضور الشخصي وبالمشاركة عن بُعد.

ثانيا- قائمة التوصيات والاستنتاجات الأولية التي جمعها المقرر

11- وفقا لخطة عمل فريق الخبراء للفترة 2019-2021، أعد المقرر قائمة دقيقة بالاستنتاجات الأولية للدول الأعضاء وتوصياتها المقترحة، تركز على تعزيز تدابير التصدي العملية للجريمة السيبرانية، واستعان المقرر في هذا الشأن بالمساعدات اللازمة من الأمانة واستند في عمله إلى المناقشات والمداولات التي دارت في الاجتماع. ووفقا لخطة العمل، أدرجت القائمة المعدة في تقرير الاجتماع السادس، باعتبارها تجميعا للاقتراحات المقدمة من الدول الأعضاء، وذلك من أجل مواصلة مناقشتها في الاجتماع التقييمي المقرر عقده في موعد أقصاه عام 2021.

12- ووفقا لخطة العمل، سينظر فريق الخبراء، خلال اجتماعه التقييمي، في الاستنتاجات والتوصيات الأولية المتراكمة، ويجمعها في قائمة تضم الاستنتاجات والتوصيات المعتمدة بغية تقديمها إلى لجنة منع الجريمة والعدالة الجنائية. وقبل انعقاد الاجتماع التقييمي، سوف تعمم الاستنتاجات والتوصيات الأولية التي اقترحتها الدول الأعضاء على جميع الدول الأعضاء والمراقبين وسائر الجهات المعنية التماسا لتعليقاتها عليها، وستنشر تلك التعليقات لاحقا على الإنترنت قبل انعقاد الاجتماع التقييمي لكي تنظر الوفود فيها.

ألف- التعاون الدولي

13- تماشيا مع خطة عمل فريق الخبراء، تتضمن هذه الفقرة تجميعا أعده المقرر للاقتراحات التي قدمتها الدول الأعضاء في الاجتماع في إطار البند 2 من جدول الأعمال المعنون "التعاون الدولي". وهذه الاستنتاجات والتوصيات الأولية مقدمة من الدول الأعضاء، ولا يعني إدراجها أن فريق الخبراء قد أقرها، كما أن ترتيب عرضها لا يعني ضمنا ترتيبا لدرجة أهميتها:

(أ) فيما يتعلق بنطاق تعريف الجريمة السيبرانية لأغراض التعاون الدولي، ينبغي للبلدان أن تكفل تجريم الأفعال الإجرامية السيبرانية على نحو كاف، لا يشمل الجرائم التي ترتكب بواسطة الفضاء السيبراني فحسب، وإنما أيضا الجرائم الأخرى التي كثيرا ما ترتكب باستخدام الإنترنت والوسائل الإلكترونية (الجرائم التي

تُيسَّر بواسطة الفضاء السيبراني)، مثل الاحتيال السيبراني، والسرقة السيبرانية، والابتزاز، وغسل الأموال، والاتجار بالمخدرات والأسلحة، واستغلال الأطفال في المواد الإباحية،[1] والأنشطة الإرهابية؛

(ب) فيما يتعلق بآليات التعاون الدولي، تشجع الدول، في حال عدم وجود معاهدة ثنائية للمساعدة القانونية المتبادلة، على الانضمام إلى المعاهدات المتعددة الأطراف القائمة التي توفر أساسا قانونيا للمساعدة القانونية المتبادلة، مثل اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية واتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، أو على استخدام تلك المعاهدات المتعددة الأطراف. وفي حال عدم وجود معاهدة، يجوز لدولة أن تطلب من دولة أخرى التعاون على أساس مبدأ المعاملة بالمثل؛ وينبغي أيضا استخدام اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية كمعيار لبناء القدرات والمساعدة التقنية على الصعيد العالمي، ووجه الانتباه إلى المفاوضات الجارية بشأن البروتوكول الإضافي الثاني للاتفاقية الرامي إلى تعزيز التعاون عبر الحدود. وأعيد التأكيد على أن إمكانية تطبيق اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية محدودة نظرا لطبيعتها كصك إقليمي وحالة التصديق عليها، فضلا عن افتقارها إلى نهج كلي، وعدم مراعاتها للاتجاهات الراهنة في مجال الجريمة السيبرانية، وعدم ملاءمتها على نحو كامل بالنسبة للبلدان النامية. ووجه الانتباه إلى قرار الجمعية العامة 247/74 الذي قررت فيه

(1) إن مصطلح "استغلال الأطفال في المواد الإباحية" راسخ بقوة في الصكوك القانونية الدولية المعتمدة في القرن الحادي والعشرين. ويعرف البروتوكول الاختياري الملحق باتفاقية حقوق الطفل بشأن بيع الأطفال واستغلال الطفل في البغاء وفي المواد الإباحية مصطلح "استغلال الأطفال في المواد الإباحية" في مادته 2 بأنه "تصوير أي طفل، بأي وسيلة كانت، يمارس ممارسة حقيقية أو بالمحاكاة أنشطة جنسية صريحة أو أي تصوير للأعضاء الجنسية للطفل لإشباع الرغبة الجنسية أساسا". وبالإضافة إلى ذلك، يكون على الدول، بموجب الفقرة (ج) من المادة 3 من البروتوكول الاختياري المذكور، تجريم الأجزاء التالية التي تتكون منها جريمة استغلال الأطفال في المواد الإباحية، وهي "إنتاج أو توزيع أو نشر أو استيراد أو تصدير أو عرض أو بيع أو حيازة مواد إباحية متعلقة بالطفل على النحو المعرف في المادة 2". وتشير اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، في الفقرة 2 من المادة 9 منها، إلى مصطلح "استغلال الأطفال في المواد الإباحية"، وتعرفه بأنه المواد الإباحية "التي تصور بصورة مرئية: (أ) قاصرا مشتركا في سلوك جنسي صريح؛ أو (ب) شخصا يظهر أنه قاصر منخرطا في سلوك جنسي صريح؛ أو (ج) صورا واقعية تمثل قاصرا مشتركا في سلوك جنسي صريح." وتتضمن الفقرة 2 من المادة 20 من اتفاقية مجلس أوروبا بشأن حماية الأطفال من الاستغلال الجنسي والاعتداء الجنسي مصطلح "استغلال الأطفال في المواد الإباحية"، وتعرفه بأنه "أي مواد تصور بصورة مرئية طفلا ينشغل في سلوك جنسي صريح حقيقي أو تمثيلي أو أي تصوير لأعضاء جنسية لطفل لأغراض جنسية في المقام الأول". وبموجب الفقرة 1 من المادة 20 من تلك الاتفاقية، تجرم أطراف الاتفاقية "إنتاج صور الأطفال الفاضحة، أو عرض أو توفير صور الأطفال الفاضحة، أو توزيع أو بث صور أطفال فاضحة، أو الحصول على صور أطفال فاضحة لصالح الشخص ذاته أو لصالح الغير، أو حيازة صور الأطفال الفاضحة، أو الحصول عن علم على طريق للنفاذ إلى صور فاضحة للأطفال من خلال تكنولوجيا المعلومات والاتصالات."

وقد أسهم ما سبق في استخدام مصطلح "استغلال الأطفال في المواد الإباحية" في التشريعات المحلية. ومن ثم، لا يزال هذا المصطلح مهما لتعريف الجريمة في كثير من البلدان. ومع ذلك، هناك اتجاه متزايد لدى هيئات إنفاذ القانون وأجهزة حماية الطفل للتساؤل عن مدى ملاءمة هذا المصطلح، واقتراح مصطلحات بديلة (انظر المبادئ التوجيهية المتعلقة بالمصطلحات والرامية إلى حماية الأطفال من الاستغلال والاعتداء الجنسيين، تحت العنوان *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse* (Bangkok, ECPAT International, 2016), pp. 38–40، الصادرة عن الفريق العامل المشترك بين الوكالات المعني بالاستغلال الجنسي للأطفال).

وبالتالي فعلى الرغم من أن مصطلح "استغلال الأطفال في المواد الإباحية" لا يزال يستخدم على نطاق واسع، ازداد استخدام مصطلح "المواد التي تصور الاعتداءات الجنسية على الأطفال" لوصف التمثيل الجنسي الصريح للأطفال، حيث اعتبر أن هذا المصطلح يجسد على نحو أدق الطابع الخطير للمحتوى، ويعارض فكرة إمكانية ممارسة تلك الأفعال بناء على موافقة الطفل. فعلى سبيل المثال، يدعم مشروع التخطيط الاستراتيجي العملي الشامل للشرطة لمكافحة المواد التي تنطوي على التعدي على الأطفال على الإنترنت مفهوما مفاده أن الصورة ذات الطابع الجنسي لطفل هي اعتداء على الطفل واستغلال له ولا ينبغي وصفها أبدا باعتبارها مواد إباحية. فـ"المواد الإباحية" مصطلح يستخدم للبالغين الذين يمارسون أفعالا جنسية بالتراضي وتوزع بشكل قانوني على الجمهور من أجل متعتهم الجنسية، في حين أن صور حالات التعدي على الأطفال ليست كذلك. فهي تنطوي على أطفال لا يستطيعون ولا يرغبون في الموافقة، وهم ضحايا لجريمة. وفي الواقع، فإنه من منظور إنفاذ القانون، تكون المواد التي تصور الاعتداءات الجنسية على الأطفال أدلة موثقة على وقوع جريمة الاعتداء الجنسي أو الاغتصاب (دراسة المكتب المعني بالمخدرات والجريمة لآثار تكنولوجيات المعلومات الجديدة فيما يتعلق بالاعتداء على الأطفال واستغلالهم، بعنوان *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children* (New York, 2015), p. 10).

الجمعية العامة إنشاء لجنة خبراء حكومية دولية مخصصة مفتوحة العضوية، تُمثَّل فيها جميع الأقاليم، لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية. وأعرب عدد من الوفود عن رأي مفاده أن من شأن وضع اتفاقية للأمم المتحدة أن ييسر كفاءة التعاون الدولي في مجال مكافحة الجريمة السيبرانية. ورأت وفود أخرى أنه ينبغي للأطر أو الصكوك الجديدة بشأن الجريمة السيبرانية ألا تخلق عقبات أو تتسبب في أن تتخلى الدول عن المعاهدات الحالية أو الالتزامات التي سبق أن قطعتها على نفسها، وكذلك الاتفاقات القائمة بالفعل، أو تعارض أيا مما سبق؛

(ج) من الضروري وجود شركاء استراتيجيين، مثل أعضاء المنظمات القائمة ومنها منظمة الدول الأمريكية أو مجموعة السبع أو المنظمة الدولية للشرطة الجنائية (الإنتربول)، في سياق التحقيق في الجرائم السيبرانية؛

(د) يتعين، في سياق التحقيقات والإجراءات القضائية، احترام سيادة الدول وولايتها القضائية. ولا ينبغي تقديم أي طلبات للاسترجاع المباشر للبيانات الموجودة في بلد آخر إلى أي منشأة تجارية أو إلى أفراد دون موافقة مسبقة من ذلك البلد؛

(هـ) ينبغي تحسين كفاءة التعاون الدولي عن طريق إنشاء آليات للاستجابة السريعة للتعاون الدولي وكذلك قنوات للاتصال بين السلطات الوطنية، من خلال موظفي الاتصال ونظم تكنولوجيا المعلومات، لجمع الأدلة عبر الحدود ونقل الأدلة الإلكترونية عبر الإنترنت؛

(و) ينبغي للدول أن تواصل تعزيز التعاون لحماية البنى التحتية الحيوية وتعزيز شبكات التعاون بين فرق التصدي للطوارئ الحاسوبية وفرق التصدي لحوادث الأمن الحاسوبي؛

(ز) ينبغي للدول أن تنظر في وضع بروتوكولات مبتكرة لتبادل المعلومات، بما في ذلك المعلومات الاستخبارية والأدلة على الأفعال الإجرامية، من أجل التعجيل بهذه الإجراءات؛

(ح) هناك حاجة إلى التأكيد مجددا على التزام جميع الدول الأعضاء بضمان سلامة وأمن تكنولوجيا المعلومات والاتصالات من خلال اقتصار استخدامها على الأغراض السلمية وتعزيز الجهود الدولية لمكافحة أي أنشطة خبيثة في الفضاء السيبراني في أوقات الأزمات الكبرى على كل من المستوى العالمي والإقليمي والمحلي؛

(ط) ينبغي أن تُسيَّر إجراءات التعاون الدولي على النحو الأمثل بحيث يقدم أقصى قدر من المساعدة لطلبات التعاون الدولي المتعلقة بحفظ الأدلة الإلكترونية، والحصول على سجلات الوقائع، ومعلومات تسجيل المستخدمين بطريقة لا تتعارض مع حقوق الإنسان والحريات الأساسية أو حقوق الملكية، في حدود الإمكانات المستمدة من الأطر القانونية المحلية؛

(ي) هناك حاجة إلى إعداد إجراءات مقبولة دوليا للتشغيل الموحد يمكن اتباعها في مسرح الجريمة فيما يتعلق بجمع البيانات وحفظها. ولتحقيق الاعتماد العالمي للممارسات الدولية الموحدة بشأن جمع الأدلة وتخزينها والتشارك فيها أهمية بالغة، لا سيما في سياق التحقيق في الجرائم السيبرانية والملاحقة القضائية لمرتكبي تلك الجرائم؛

(ك) تدعى البلدان إلى إيلاء اهتمام خاص لضرورة أن تكون تدابير التحقيق متناسبة، مع احترام الحريات الأساسية وأنظمة حماية البيانات الشخصية المرتبطة بالمراسلات الخاصة؛

(ل) ينبغي للتعاون الدولي في مجال مكافحة الجريمة السيبرانية أن يأخذ أيضا في الاعتبار النهوج التي تراعي الاعتبارات المتعلقة بنوع الجنس وعامل السن، واحتياجات الفئات المستضعفة؛

(م) ينبغي للدول أن تمتنع عن الانفراد باتخاذ تدابير غير قانونية لا تتفق مع القانون الدولي وميثاق الأمم المتحدة؛

(ن) فيما يتعلق بنطاق التعاون الدولي، تقدم المساعدة القانونية المتبادلة من خلال السلطات الوطنية فقط، في حين لا ينبغي أن يقتصر التعاون على الإدارات الحكومية، بل ينبغي أن يشمل أيضا القطاع الخاص، مثل مقدمي خدمات الإنترنت. وفي هذا السياق، أوصي بضرورة اعتماد أحكام تتيح التعاون المباشر مع مقدمي خدمات الإنترنت في ولايات قضائية أخرى فيما يتعلق بطلبات المعلومات عن المشتركين، وطلبات حفظ البيانات؛

(س) يجب أن تضمن الخيارات المتاحة للتصدي للجريمة السيبرانية وحماية المجتمعات دائما حماية حقوق الإنسان والضمانات الدستورية، وأن تعزز وجود فضاء سيبراني أكثر حرية وانفتاحا وأمنا ومرونة للجميع؛

(ع) تشجع البلدان على تحسين سبل التعاون مع الأوساط الصناعية، وتعزيز التعاون بين مقدمي الخدمات من القطاعين العام والخاص، ولا سيما بغرض التصدي للتحديات التي تطرحها المواد الإجرامية الضارة على الإنترنت؛

(ف) تكون للشركات الخاصة، ولا سيما مقدمي خدمات الإنترنت، مسؤولية مشتركة في منع الجرائم السيبرانية والتحقيق فيها؛ وينبغي لهذه الشركات أن تعجل استجاباتها لطلبات المساعدة القانونية وأن توسع من نطاقها، وأن تقدمها في البلدان التي توجد فيها، وأن تضمن أن يكون لديها قنوات مناسبة للتواصل مع السلطات المحلية؛

(ص) يجب تعزيز الشراكات بين القطاعين العام والخاص. ويجب إنشاؤها حيثما لا توجد، وينبغي للشركات الخاصة أن تشارك في الأفرقة العاملة (المنتديات المتعددة الأطراف) وأن تكون جزءا من الحوار بشأن تعزيز النهج المتبع إزاء الجرائم السيبرانية؛

(ق) يجب أيضا أن تشكل المنظمات غير الحكومية والأوساط الأكاديمية جزءا من الجهود الرامية إلى منع الجريمة السيبرانية والتصدي لها، نظرا إلى أنها تقدم منظورا شاملا متعدد الجوانب يستوعب الجميع، لتحقيق عدة أهداف منها ضمان حماية حقوق الإنسان، ولا سيما حرية التعبير والحق في الخصوصية؛

(ر) تدعى البلدان إلى الانضمام إلى شبكات الممارسين المعتمدة والتوسع في استخدامها وتعزيزها بغرض حفظ الأدلة الإلكترونية المقبولة وتبادلها، ومنها الشبكات العاملة على مدار الساعة (24/7) والشبكات المتخصصة في مجال الجريمة السيبرانية وقنوات الإنتربول من أجل التعاون الفوري المباشر بين أجهزة الشرطة، وكذلك إلى بناء شبكات مع الشركاء المتوائمين استراتيجيا بهدف تبادل البيانات المتعلقة بمسائل الجريمة السيبرانية والتمكين من الاستجابة السريعة والتقليل إلى أدنى حد من فقدان الأدلة الدامغة. وأوصي أيضا باستخدام التعاون المباشر بين أجهزة الشرطة وغير ذلك من أساليب التعاون غير الرسمي قبل استخدام قنوات المساعدة القانونية المتبادلة؛

(ش) ينبغي أن تقوم كل دولة بإنشاء نقطة اتصال فعلية تعمل على مدار الساعة (24/7)، مصحوبة بتوفير موارد مناسبة لتيسير حفظ البيانات الرقمية إلى جانب المساعدة الدولية المتبادلة التقليدية في المسائل الجنائية، وذلك بالاعتماد على النموذج الناجح لتجميد البيانات في إطار اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية؛

(ت) ينبغي للدول الأعضاء أن تتبادل المعلومات بشأن كيفية التصدي على المستوى المحلي للتحديات التي تواجه الحصول على الأدلة الرقمية في الوقت المناسب، لكي تستفيد الدول الأعضاء الأخرى من تلك التجارب وتزيد من كفاءة وفعالية عملياتها الخاصة؛

(ث) ينبغي للدول الأعضاء أن ترسي ممارسات تسمح بإرسال طلبات المساعدة القانونية المتبادلة وتلقيها بالوسائل الإلكترونية لتقليص فترات التأخير عند إرسال الوثائق من دولة إلى أخرى؛

(خ) ينبغي للبلدان أن تعزز التعاون فيما بين المؤسسات، وأن تحسن قابلية التشغيل المتبادل من خلال توحيد طلبات الحصول على المعلومات وإجراءات التوثيق، ومشاركة أصحاب المصلحة المتعددين؛

(ذ) ينبغي للبلدان أن تحسن تنفيذ القوانين الوطنية وأن تعزز تحسين التنسيق والتآزر على الصعيد المحلي من أجل جمع المعلومات والأدلة وتبادلها لأغراض الملاحقة القضائية؛

(ض) ينبغي للدول الأعضاء أن ترسي نظما محلية تجعل تبادل "معلومات المشتركين"، على النحو المبين في الفقرة 3 من المادة 18 من اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، أسرع وأكثر كفاءة؛

(أأ) ينبغي للدول أن تعزز تدابير تبادل المعلومات المالية أو النقدية، وتجميد الحسابات، ومصادرة الموجودات لضمان عدم تمتع المجرمين بفوائد الأنشطة الإجرامية؛

(بب) تشجع الدول على إنشاء أفرقة تحقيق مشتركة مع بلدان أخرى على المستوى الثنائي أو الإقليمي أو الدولي لتعزيز قدرات الإنفاذ؛

(جج) ينبغي للدول أيضا أن تتيح إمكانية التعامل الفعال مع الأدلة الإلكترونية ومقبولية تلك الأدلة أمام المحكمة، بما في ذلك عندما تكون مرسلة إلى ولاية قضائية أجنبية أو واردة منها. وفي هذا الصدد، تشجع البلدان على مواصلة جهود الإصلاح في مجال التشريعات المتعلقة بالجريمة السيبرانية والأدلة الإلكترونية، أو الشروع في تلك الجهود، باتباع الأمثلة والإصلاحات الإيجابية من جميع أنحاء العالم؛

(دد) يوصى بوضع أطر قانونية تشمل أيضا جوانب تتعلق بالولاية القضائية خارج الحدود الإقليمية على الأفعال التي تعد جرائم سيبرانية؛

(هه) ينبغي للبلدان أن تنقح الآليات الخاصة بالتخفيف من حدة النزاعات، وأن تتصدى للتحديات المتعلقة بإسناد الفعل إلى الفاعل في قضايا الجرائم السيبرانية والقدرة على التحقيق فيها؛

(وو) ينبغي للدول أن تعمل على توحيد ونشر الأدوات الإجرائية للتعجيل بإنتاج البيانات وتوسيع نطاق عمليات التفتيش (مثل أوامر توفير البيانات، وأوامر التعجيل في حفظها أو الوصول إليها عبر الحدود، إلخ.) وذلك لتيسير عمل سلطات إنفاذ القانون وتعاونها المباشر مع مقدمي خدمات الإنترنت وحل المشاكل المرتبطة بتتبع الأدلة الإلكترونية واستخدامها على النحو المناسب؛

(زز) ينبغي للدول أن تيسر وضع وتوحيد معايير تقنية قابلة للتشغيل المتبادل في مجال التحليل الجنائي الرقمي واسترجاع الأدلة الإلكترونية عبر الحدود؛

(حح) يوصى بالاستثمار في إنشاء سلطة مركزية قوية للتعاون الدولي في المسائل الجنائية لضمان فعالية آليات التعاون التي تنطوي على جرائم سيبرانية. ويوصى أيضا بإنشاء وحدات خاصة للتحقيق في الجرائم السيبرانية، وبأن تُعالجَ طلبات الحفظ المقدمة من دولة أخرى من خلال شبكة عاملة على مدار الساعة (24/7) (أو مباشرة مع مقدم الخدمة في بعض الحالات) للحفاظ على البيانات اللازمة في أسرع وقت ممكن. وقد يساعد زيادة فهم المعلومات اللازمة لنجاح طلب المساعدة القانونية المتبادلة في الحصول على البيانات بسرعة أكبر؛

(ط ط) من شأن وجود ترتيب رسمي مع منظمات مثل وكالة الاتحاد الأوروبي للتعاون في مجال إنفاذ القانون (اليوروبول)، والمركز الأوروبي للجريمة السيبرانية، ومركز الجريمة السيبرانية في الولايات المتحدة الأمريكية، ومركز مكافحة الجرائم السيبرانية في اليابان، والمركز الوطني لأمن الفضاء السيبراني في المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية، أن يساعد على تبادل المعلومات المتعلقة بأحدث التهديدات التي تطرحها الجرائم السيبرانية، وأساليب العمل، والتكنولوجيات الناشئة في مجال التحقيقات في الجرائم السيبرانية والوصول إلى بعضها البعض، والممارسات الفضلى، وما إلى ذلك؛

(يي) يتطلب التعاون الدولي الفعال وجود قوانين وطنية تستحدث إجراءات تمكن من التعاون الدولي. ومن ثم، يجب أن تسمح القوانين الوطنية بالتعاون الدولي بين أجهزة إنفاذ القانون؛

(كك) ينبغي للدول أن تتعاون بفعالية في مجال تسليم المطلوبين. وإذا كانت الدولة المتلقية الطلب تعتزم رفض تسليم المشتبه في ارتكابهم لجرائم سيبرانية، ينبغي لها، عند الطلب، أن تبذل قصارى جهدها للتشاور مع الدولة الطالبة لكي تتاح للدولة الطالبة الفرصة لإبداء رأيها وتقديم معلومات. وينبغي للدولة المتلقية الطلب أن تقدم أسباب الرفض إلى الدولة الطالبة؛

(لل) إلى جانب القوانين المحلية، يعتمد التعاون الدولي في مجال الجريمة السيبرانية على التعاون الرسمي القائم على المعاهدات وعلى المساعدة التقليدية المباشرة بين أجهزة الشرطة على حد سواء. وعند مناقشة صك جديد بشأن الجريمة السيبرانية، من المهم أن تتذكر البلدان أنه ينبغي للصك الجديد ألا يتعارض مع الصكوك القائمة، التي تمكن بالفعل من التعاون الدولي الآني. وبالتالي، ينبغي للبلدان أن تكفل أن يتفادى أي صك جديد بشأن الجريمة السيبرانية التضارب مع المعاهدات القائمة؛

(مم) ينبغي إعطاء أولوية لبناء القدرات المستدامة والمساعدة التقنية وزيادتها من أجل زيادة القدرات في جميع المجالات العملياتية وتعزيز قدرة السلطات الوطنية على التصدي للجريمة السيبرانية، بما في ذلك من خلال بناء الشبكات وعقد الاجتماعات والتدريبات المشتركة، وتبادل الممارسات الفضلى والمواد التدريبية ونماذج التعاون. وينبغي أن يشمل بناء القدرات والتدريب تدريبا شديد التخصص للممارسين، يشجع على وجه الخصوص على مشاركة الخبيرات، ويستجيب لاحتياجات المشرعين وواضعي السياسات من أجل تحسين معالجة المسائل المتعلقة بالاحتفاظ بالبيانات لأغراض إنفاذ القانون. وينبغي أيضا أن يركز بناء القدرات والتدريب على تحسين قدرات سلطات إنفاذ القانون والمحققين والمحللين في مجالات التحليل الجنائي، واستخدام البيانات المفتوحة المصدر في التحقيقات، وتسلسل العهدة فيما يتعلق بالأدلة الإلكترونية، وكذلك جمع وتبادل الأدلة الإلكترونية في الخارج. وينبغي التركيز كذلك في بناء القدرات والتدريب على تحسين قدرات القضاة وأعضاء النيابات العامة والسلطات المركزية والمحامين المتعلقة بالفصل في القضايا ذات الصلة والتعامل معها بفعالية؛

(نن) من الضروري وضع قواعد وأطر زمنية ملائمة للاحتفاظ بالبيانات/الحفاظ على البيانات، وإن أمكن توحيدها، لكفالة الحفاظ على الأدلة الإلكترونية أو الحصول عليها لدعم طلبات المساعدة القانونية المتبادلة الأخرى؛

(سس) للتعاون الدولي أهمية في جمع وتبادل الأدلة الإلكترونية في سياق التحقيقات عبر الحدود، وللاستجابة بسرعة وفعالية لطلبات المساعدة القانونية المتبادلة المتعلقة بحفظ الأدلة الإلكترونية والحصول عليها. وينبغي احترام مبدأي السيادة والمعاملة بالمثل في هذه العملية؛

(عع) يشجع المكتب المعني بالمخدرات والجريمة على مواصلة تقديم برامج بناء القدرات وبرامج التدريب في مجال مكافحة الجريمة السيبرانية إلى الخبراء الحكوميين الوطنيين من أجل تعزيز القدرات في مجال كشف الجرائم السيبرانية والتحقيق فيها. وينبغي لعملية بناء القدرات أن تلبي احتياجات البلدان النامية، وأن تركز على أوجه ضعف كل بلد من أجل تقديم مساعدة تقنية مصممة حسب الحاجة، وأن تشجع على تبادل أحدث المعارف خدمة لمصلحة الممارسين وأصحاب المصلحة؛

(فف) استحدث المكتب المعني بالمخدرات والجريمة أداة كتابة طلبات المساعدة القانونية المتبادلة من أجل مساعدة الممارسين في مجال العدالة الجنائية على صياغة طلبات المساعدة القانونية المتبادلة. كما وضع أيضا دليلا عمليا لطلب الأدلة الإلكترونية عبر الحدود، عنوانه *Practical Guide for Requesting*

Electronic Evidence Across Borders، وهو متاح عند الطلب للممارسين الحكوميين في الدول الأعضاء. ويمكن للبلدان أن تستفيد من استخدام هذه الأدوات الأساسية التي استحدثها المكتب؛

(صص) ينبغي أن تنظر لجنة منع الجريمة والعدالة الجنائية في توسيع نطاق خطة عمل فريق الخبراء إلى ما بعد عام 2021، باعتباره منتدى للممارسين لتبادل المعلومات بشأن الجريمة السيبرانية؛

(قق) رأى بعض المتكلمين أن التفاوض بشأن اتفاقية للأمم المتحدة لتعزيز التعاون في مكافحة الجريمة السيبرانية واعتمادها من شأنه أن ييسر تحسين كفاءة التعاون الدولي في مكافحة الجريمة السيبرانية؛

(رر) أوصي بأن يتولى خبراء المكتب المعني بالمخدرات والجريمة في فيينا تناول أي عملية صياغة لاتفاقية جديدة؛

(شش) أوصى بعض المتكلمين بأن تجدد لجنة منع الجريمة والعدالة الجنائية ولاية فريق الخبراء، وأن تتخذ قرارا بشأن خطة العمل لما بعد عام 2021، التي ينبغي أن تشمل أيضا الأشكال المستجدة للجريمة السيبرانية، ودراسة المسائل المتعلقة بالاعتداء الجنسي على الأطفال واستغلالهم جنسيا عبر الإنترنت؛

(تت) علاوة على ذلك، أوصي بألا تبدأ لجنة الخبراء الحكومية الدولية المخصصة المفتوحة العضوية، المنشأة عملا بقرار الجمعية العامة 247/74 لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، عملها إلا بعد أن ينتهي فريق الخبراء من وضع توصياته ويرسلها إلى لجنة منع الجريمة والعدالة الجنائية في عام 2021؛

(ثث) من جهة أخرى، أشار متكلمون آخرون إلى عدم الحاجة إلى أن يواصل فريق الخبراء عمله فيما بعد عام 2021، نظرا لاعتماد قرار الجمعية العامة 247/74. ومن شأن ذلك أن يتيح التركيز على تنفيذ هذا القرار والتفاوض على وضع اتفاقية جديدة، والاستفادة على أفضل وجه من الموارد المتاحة؛

(خخ) رحب ممثلو بعض الدول الأعضاء في بياناتهم باعتماد قرار الجمعية العامة 247/74. وأشير إلى أن عملية وضع الاتفاقية الجديدة، عملا بذلك القرار، ينبغي أن تكون شاملة وشفافة وأن تستند إلى توافق الآراء الذي يمكن أن تكون عمليات الأمم المتحدة السابقة المتعلقة بإبرام اتفاقية مكافحة الجريمة المنظمة عبر الوطنية واتفاقية الأمم المتحدة لمكافحة الفساد مثالا عليه؛

(ذذ) كانت هناك دعوات إلى المشاركة النشطة من جميع الدول الأعضاء في أعمال اللجنة المخصصة المتعلقة بوضع اتفاقية جديدة؛

(ضض) في الوقت نفسه، أشار متكلمون آخرون إلى ضرورة أن تراعي أي اتفاقية جديدة، من حيث المضمون، الأطر والصكوك القائمة وألا تتعارض معها. وأوصي بأن تدرج المسائل المتعلقة بجمع الأدلة عبر الحدود وأحكام التجريم واحترام السيادة في اتفاقية جديدة ممكنة؛

(أ أ أ) ينبغي للمجتمع الدولي أن يعطي الأولوية لتوفير بناء القدرات وغير ذلك من أشكال الدعم من أجل تعزيز قدرة السلطات الوطنية على التصدي للجريمة السيبرانية، ولا سيما جرائم الاعتداء الجنسي على الأطفال واستغلالهم جنسيا عبر الإنترنت؛

(ببب) ينبغي للدول الأعضاء أن تتبادل المساعدة القانونية على أوسع نطاق ممكن بغرض الحصول على الأدلة الإلكترونية، بما في ذلك في الحالات التي تنطوي على استخدام تكنولوجيا المعلومات والاتصالات لارتكاب الأفعال الإرهابية أو تمويل الإرهاب، أو التحريض على ذلك؛ وأشير كذلك إلى أن كيانات القطاع الخاص تتحمل مسؤولية التعاون مع السلطات الوطنية في هذا الصدد؛

(ججج) ينبغي للدول الأعضاء أن تنظر في الاستثمار في قوات مركزية متخصصة في مجال الجريمة السيبرانية، وفي وحدات تكنولوجية إقليمية للتحقيقات الجنائية؛

(ددد) ينبغي للدول الأعضاء أيضا أن تنظر في إنشاء وحدات منفصلة لمكافحة الجريمة السيبرانية داخل السلطات المركزية المعنية بالمساعدة القانونية المتبادلة، لتكون أساسا للخبرة الفنية في مجال التعاون الدولي المعقد. ولن يكون لتلك الوحدات المتخصصة فائدة في الممارسة اليومية للمساعدة القانونية المتبادلة فحسب، وإنما ستتيح أيضا تقديم مساعدة مركزة في مجال بناء القدرات، مثل التدريب على تلبية احتياجات السلطات المحلية والأجنبية بشأن كيفية الحصول على المساعدة التي تنطوي على أدلة إلكترونية بسرعة وكفاءة، في إطار طلبات المساعدة القانونية المتبادلة في المسائل المتصلة بالشؤون السيبرانية؛

(هههه) ينبغي للدول الأعضاء أن تنظر في الاحتفاظ بقواعد بيانات إلكترونية تيسر الوصول إلى الإحصاءات المتعلقة بطلبات المساعدة القانونية المتبادلة الواردة والصادرة التي تتضمن أدلة إلكترونية، لضمان القيام باستعراضات للكفاءة والفعالية؛

(وو) ينبغي تذكير الدول الأعضاء بالاستفادة من السلطات المركزية في إحالة طلبات المساعدة القانونية المتبادلة وفي العمل مع السلطات المختصة لتنفيذ تلك الطلبات لضمان الامتثال للمعاهدات القائمة والحد من تأخر العملية؛

(زززز) فيما يتعلق بالحصول على بيانات من أجل إجراء التحقيقات المتعلقة بأفعال الجريمة السيبرانية، ينبغي للدول أن تستفيد من الصكوك الدولية المجربة والمختبرة، إذ إن هذه التحقيقات معقدة وتستلزم إطارا مؤسسيا أثبت قدرته على الصمود وقيمته المضافة. وسلط الضوء في هذا الصدد على اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية التي أرست معيارا في الحصول على الأدلة الإلكترونية على مر السنين، وأدت إلى تحقيق نتائج يومية بالنسبة لأجهزة إنفاذ القانون في جميع أنحاء العالم. وأوصي بأن تحد الدول من تنازع القوانين فيما يتعلق بالمتطلبات القانونية المنطبقة، بأن تأخذ في الاعتبار كنقطة للانطلاق، في حالة أوامر توفير البيانات المباشرة، تشريعات الدولة التي يوجد فيها مقدم خدمات الإنترنت المطالب بتوفير البيانات، أو تشريعات الدولة التي يكون المشتبه فيه من رعاياها؛

(حححح) يوصى بإنشاء إطار يوضح أنه في حالة عدم تحديد مكان تواجد البيانات (“loss of location”)، يتطلب قرار المضي في التحقيق بذل جهود لتحديد الإقليم المتأثر، والمكان الذي تكون فيه سلامة الشبكات المؤتمتة أمرا حيويا لكي يتسنى التشاور بشأن مسائل الولاية القضائية وأنسب طريقة لمواصلة التحقيقات؛

(ط ط ط) أوصي بأن ينطبق القانون الدولي، بما في ذلك مبادئ السيادة والسلامة الإقليمية وعدم التدخل في الشؤون الداخلية، على الفضاء السيبراني، وألا تستخدم تكنولوجيا المعلومات والاتصالات كأسلحة، وأن تدان الهجمات التي ترعاها الدول ويخضع المسؤولون عنها للمساءلة؛

(ييي) ينبغي للدولة المتلقية الطلب، رهنا بقانونها الداخلي، أن تقدم أقصى قدر من المساعدة في طلبات التحقيق وجمع الأدلة التي لا تتعلق بالحرية الشخصية أو حقوق الملكية، أو التي يكون لها أثر ضئيل على هذه الحقوق؛

(ككك) ينبغي للدول أن تنشئ آلية للتحرك السريع وقناة اتصال للمساعدة القضائية والتعاون في مجال إنفاذ القانون بغرض مكافحة الجريمة السيبرانية، وأن تنظر في إمكانية تبادل الوثائق القانونية والأدلة الإلكترونية عبر الإنترنت، مع دعمها بالتوقيعات الإلكترونية وغيرها من الوسائل التقنية؛

(للل) ينبغي للمجتمع الدولي أن يصـــوغ إجراء موحدا لأســـاليب التحري في الجرائم الســـيبرانية وأن يحسن اللوائح المتعلقة بالتزامات مقدمي خدمات الإنترنت بشأن حفظ السجلات في القوانين المحلية؛

(ممم) ينبغي للدول أن تمنع التحويلات الدولية للعائدات غير المشـــروعة المتأتية من الجرائم السيبرانية وأن تعزز التعاون الدولي في مجال استرداد الموجودات المتعلقة بالجرائم السيبرانية؛

(ننن) ينبغي للدول أن تحترم ســـيادة الدول الأخرى عند إرســـاء ولايتها القضـــائية على الجرائم الســـيبرانية، وألا تمارس على نحو مفرط الولاية القضـــائية خارج الحدود الإقليمية التي تفتقر إلى صـــلة كافية وحقيقية بالجريمة السيبرانية التي تجري ملاحقتها قضائيا. وتشجع الدول على تعزيز الاتصال والتشاور لتسوية النزاعات المتعلقة بالولاية القضائية؛

(سس‌س) من المهم ضـــمان الاســـتخدام الآمن والمأمون لتكنولوجيات المعلومات والاتصـــالات في توفير إمكانية الاتصال والتوعية للجميع في مختلف أنحاء العالم، بغض النظر عن حالة المناطق التي يقيم فيها المستخدمون.

باء - المنع

14- تماشـيا مع خطة عمل فريق الخبراء، تتضـمن هذه الفقرة تجميعا أعده المقرر للاقتراحات التي قدمتها الدول الأعضـــاء في الاجتماع في إطار البند 3 من جدول الأعمال المعنون "المنع". وهذه الاســـتنتاجات والتوصـــيات الأولية مقدمة من الدول الأعضـــاء، ولا يعني إدراجها أن فريق الخبراء قد أقرها، كما أن ترتيب عرضها لا يعني ضمنا ترتيبا لدرجة أهميتها:

(أ) ينبغي التسليم بأن المنع ليس مسؤولية الحكومات وحدها، وإنما يتطلب أيضا مشاركة جميع أصـــحاب المصـــلحة المعنيين، بما في ذلك ســـلطات إنفاذ القانون والقطاع الخاص، ولا ســـيما مقدمي خدمات الإنترنت والمنظمات غير الحكومية والمدارس والأوساط الأكاديمية، بالإضافة إلى الجمهور بوجه عام؛

(ب) أوصـي بأن يسـهل على الجمهور الوصـول إلى أدوات المنع، ومنها المنصـات الإلكترونية، والمقاطع الصوتية، والمعلومات البيانية التي تستخدم لغة مبسطة، ومنصات الإبلاغ؛

(ج) اعتبر من الضـروري وضـع سـلسـلة من السـياسـات العامة الطويلة الأجل المتعلقة بالمنع، وينبغي أن تشمل تلك السياسات تنظيم حملات للتوعية بشأن الاستخدام الآمن للإنترنت؛

(د) ينبغي إدراج الوعي بالأمن الســـيبراني كموضـــوع في التعليم الابتدائي والثانوي والعالي، للطلاب والمعلمين على حد سواء. وينبغي أن يكون ذلك، في الحالة المثلى، جزءا من اسـتراتيجية وطنية للأمن السـيبراني. وينبغي للدول أيضـا أن تتبادل الخبرات بشـأن كيفية اسـتخدام اسـتراتيجيات الأمن السـيبراني لمنع الجريمة السيبرانية. وبالإضافة إلى ذلك، ينبغي للدول أن تولي اهتماما خاصا لتدابير المنع الموجهة إلى أوساط الشباب، بما في ذلك من ارتكبوا جريمة للمرة الأولى، بهدف منع معاودة ارتكابهم للجرائم؛

(هـ) ينبغي للدول، عند منع الجريمة السـيبرانية ومكافحتها، أن تولي اهتماما خاصـا لمسـائل منع العنف الجنساني، وبخاصة العنف ضد النساء والفتيات وجرائم الكراهية، والقضاء على تلك الجرائم؛

(و) يجب أن تكون الأنشـــطة المتعلقة بالمنع اســـتباقية ومنتظمة ومســـتمرة ومناســـبة للفئات الضعيفة؛

(ز) يمكن للتقاطع والتعاون بين كيانات القطاعين العام والخاص فيما يتعلق بمجموعات البيانات الكبيرة أو مراكز البيانات الكبيرة أن يكونا من المجالات التي تتسم بالضعف الشديد، وبخاصة، على سبيل المثال لا الحصر، على نحو ما تبين في قطاع الصحة خلال الجائحة الحالية. وينبغي للدول أن تولي اهتماما خاصا لتنظيم الوصول إلى هذه البيانات على نحو قانوني وحمايتها من الهجمات السيبرانية؛

(ح) فيما يتعلق بالجهود في مجال المنع، ينبغي أن يتحمل مقدمو خدمات الإنترنت مزيدا من المسؤولية عن الاحتياطات الأمنية ("على نحو تلقائي") وعن منع الجريمة السيبرانية، وينبغي وضع معايير دولية بشأن محتوى معلومات السجلات والمدة التي يتعين على مقدمي الخدمات الاحتفاظ بها بتلك المعلومات. وعلاوة على ذلك، ينبغي أن تحدد بوضوح مسؤوليات مقدمي الخدمات فيما يتعلق باكتشاف الجرائم السيبرانية ومنعها وتعطيلها؛

(ط) هناك حاجة إلى إقامة شراكات بين القطاعين العام والخاص، بما في ذلك التعاون مع أصحاب المصلحة في مجال الأمن السيبراني وشركات التكنولوجيا الكبيرة في مجال تبادل المعلومات، من أجل منع الجريمة السيبرانية ومكافحتها؛

(ي) ينبغي للدول أن توفر التدريب للقضاة المتخصصين وغيرهم من القضاة الذين يتعاملون مع قضايا الجرائم السيبرانية، وأن تزود هيئات التحقيق بأدوات عالية الأداء لتتبع العملات المشفرة ومعالجة استخدامها لأغراض إجرامية؛

(ك) ينبغي للدول أن تزيد من استراتيجيات مكافحة استغلال المجموعات الإجرامية التقليدية للأدوات السيبرانية بغرض إخفاء اتصالاتها وأنشطتها؛

(ل) ينبغي وضع حلول تتيح التعاون المباشر بين السلطات الوطنية ومقدمي خدمات الإنترنت، مع الحفاظ على سيادة القانون وحقوق الإنسان، بما في ذلك متطلبات حماية البيانات؛

(م) ينبغي للدول أن تكفل حرية الصحافة عند وضع تدابير لمنع الجريمة السيبرانية؛

(ن) أوصي ببناء القدرات الجماعية للمؤسسات المختصة وتغيير ثقافة المنع بحيث تكون استباقية بدلا من أن تكون قائمة على رد الفعل. وأوصي أيضا بإنشاء آلية قوية لحفز وتيسير تبادل المعلومات الاستخبارية بشأن أساليب العمل الإجرامية المحتملة؛

(س) تشجع الدول الأعضاء على أن تواصل إدراج تدابير منع فعالة على الصعيدين الوطني والدولي، وأن تركز على الأنشطة الاستباقية مثل تعزيز الوعي بمخاطر الجريمة السيبرانية؛ وتوجه مثل تلك الحملات لتستهدف أساليب العمل من قبيل التصيد الاحتيالي أو البرمجيات الخبيثة (فيروسات الفدية "ransomware")، ومجموعات مختلفة مثل الشباب أو المسنين. وتشجع الدول الأعضاء أيضا على أن تواصل التركيز على ترجيح احتمال خضوع الجناة للملاحقة القضائية والعقاب، وتبذل جهودا لمنع الجريمة عن طريق كشف وعرقلة ما يجري من أنشطة غير مشروعة عبر الإنترنت. ويتعين على دوائر الشرطة والنيابات العامة أن تستثمر في التعريف بالتهديدات التي تطرحها الجرائم السيبرانية، والكشف عنها والتصدي لها. ولا غنى عن الشراكات بين القطاعين العام والخاص. ولا تتطلب أنشطة المنع هذه قوانين أو لوائح إضافية؛

(ع) نظرا لوجود "فجوة رقمية"، فإن بعض البلدان النامية تفتقر إلى القدرة على منع الجرائم السيبرانية وكشفها ومكافحتها، وتكون أضعف حالا في مواجهة التحديات التي تمثلها تلك الجرائم؛

(ف) شُجِّع المكتب المعني بالمخدرات والجريمة بقوة على مواصلة تقديم المساعدة التقنية، عند الطلب، لمنع ومكافحة الجريمة السيبرانية؛

(ص) ينبغي أن تكون الأدوات الدولية التي تعد مستقبلا بشأن منع الجريمة السيبرانية متاحة للجميع في مختلف أنحاء العالم، دون أي تمييز على أساس وضع البلد أو الإقليم الذي يكون الشخص من رعاياه أو من المقيمين فيه؛

(ق) ينبغي حماية حقوق الإنسان الأساسية والحريات الأساسية في كل مكان، بما في ذلك في المجال الرقمي والفضاء السيبراني، بغض النظر عن الحدود ودون أي تدخل أو تقييد؛

(ر) الفضاء السيبراني والجريمة السيبرانية لا تحدهما الحدود الإقليمية ولا يعترفان بأي حدود أو قيود مادية أخرى. ومن ثم، ينبغي للمجتمع الدولي أن يظل متحدا من أجل كبح التهديدات السيبرانية؛

(ش) الفضاء السيبراني مجال فريد وعالمي، وفي غياب مدونة دولية لقواعد السلوك، ينبغي بذل المزيد من الجهود لوضع قواعد ومبادئ ومعايير للسلوك المسؤول من قبل الدول في الفضاء السيبراني. وفي هذا السياق، ينبغي لجميع الدول الأعضاء أن تنبذ التهديد باستعمال القوة أو استخدامها ضد البنى التحتية الأساسية الحيوية للدول الأخرى؛

(ت) تشجع الدول الأعضاء على أن تواصل إدراج تدابير منع فعالة على الصعيدين الوطني والدولي، وتركز على الأنشطة الاستباقية مثل تعزيز الوعي بمخاطر الجريمة السيبرانية وترجيح احتمال خضوع الجناة للملاحقة القضائية والعقاب، وأن تبذل جهودا لمنع وقوع المزيد من الجرائم بكشف ما يجري من أنشطة إلكترونية غير مشروعة وعرقلتها؛

(ث) تتميز ممارسات الأمن السيبراني عن الجهود المبذولة لمكافحة الجريمة السيبرانية. وينبغي للدول أن تضع استراتيجية وطنية لمكافحة الجريمة السيبرانية، تتضمن تشريعات أو سياسات وطنية لمنع الجريمة السيبرانية، وكذلك استراتيجية وطنية للأمن السيبراني. وينبغي أن تشمل مجالات التركيز في الاستراتيجيات الوطنية المتعلقة بالجرائم السيبرانية منع الجريمة السيبرانية، والشراكات بين القطاعين العام والخاص، والقدرات في مجال العدالة الجنائية، والتوعية من خلال نشر قرارات المحاكم؛

(خ) ينبغي للبلدان أن تجمع طائفة واسعة من البيانات للمساعدة على فهم الاتجاهات بغرض وضع وتشكيل سياسات الجريمة السيبرانية وتدابير التصدي العملياتية لمكافحة الجريمة السيبرانية؛

(ذ) ينبغي للجهود المبذولة لوضع استراتيجيات لمنع الجرائم السيبرانية أن تراعي أيضا حماية حقوق الإنسان؛

(ض) ينبغي أن تكون "قدرات العدالة الجنائية" مجالا آخر من مجالات التركيز في الاستراتيجيات الوطنية لمكافحة الجرائم السيبرانية. وينبغي أن يكون تقديم المساعدة إلى البلدان النامية أولوية من أجل تعزيز قدرات أجهزة إنفاذ القانون في مجال منع الجريمة السيبرانية؛

(أأ) ينبغي للدول الأعضاء أن تستفيد من المساعدة في مجال بناء القدرات المقدمة من البرنامج العالمي المعني بالجريمة السيبرانية التابع للمكتب المعني بالمخدرات والجريمة وغيره من المبادرات، ومنها برامج مجلس أوروبا الموسعة المتعلقة بالتدابير العالمية لمكافحة الجريمة السيبرانية؛

(بب) ينبغي للدول أن تضع أو تعزز برامج دعم لضحايا الجرائم السيبرانية؛

(جج) ينبغي للدول أن تجري دراسات استقصائية لقياس أثر الجريمة السيبرانية على المنشآت التجارية، بما في ذلك التدابير المنفذة وتدريب الموظفين وأنواع الحوادث السيبرانية التي تؤثر عليها والتكاليف المرتبطة بالتعافي من الحوادث السيبرانية ومنعها؛

(دد) ينبغي للدول أن تدعم المنشـــآت التجارية والمجتمعات المحلية في التوعية بمخاطر الجرائم السيبرانية واستراتيجيات التخفيف من آثارها وتعزيز الممارسات السيبرانية، التي من شأنها أن تحقق فوائد نهائية كبيرة في مجال المنع؛

(هه) ينبغي دراسة أساليب عمل مرتكبي الجرائم السيبرانية المعاصرين بعناية من خلال تحليل المعلومات الاستخبارية والبحوث الجنائية من أجل استغلال الموارد الحالية على نحو أكثر فعالية واكتشاف مواطن الضعف؛

(وو) ينبغي للدول أن تنظر في إنشاء منصة للتنسيق بغرض تعزيز التبادل الفوري للبيانات المتعلقة بالحوادث والاتجاهات الجديدة المستبانة في مجال الجريمة السيبرانية. وينبغي للدول أيضا أن تنظر في إنشاء مراكز للرصد الجنائي بغرض رصد التهديدات والاتجاهات المتعلقة بالجرائم السيبرانية؛

(زز) ينبغي للبلدان أن تنظر في بذل جهود محددة ومصممة خصيصا لحماية الأطفال على الإنترنت. وينبغي أن يشمل ذلك ضمان وجود أطر قانونية وترتيبات عملية وترتيبات للتعاون الدولي على الصعيد المحلي للتمكين من الإبلاغ عن الاعتداء الجنسي على الأطفال واستغلالهم جنسيا عبر الإنترنت، والكشف عن هذه الحالات والتحقيق فيها وردعها وملاحقة مرتكبيها قضائيا؛

(حح) إن قطاع الصناعة شريك رئيسي في منع الجريمة السيبرانية. وينبغي للبلدان أن تنظر في تنفيذ آليات للتعاون مع القطاع الصناعي، بما في ذلك بشأن الإحالة إلى السلطات الوطنية المختصة، وإزالة المواد الإجرامية الضارة، ومنها المواد التي تصور الاستغلال الجنسي للأطفال والمواد التي تصور أفعال العنف البغيضة؛

(طط) ينبغي إصدار إرشادات منتظمة بشأن منع الحوادث واطلاع المستخدمين والمنظمات وأصحاب المصلحة الآخرين عليها لتمكينهم من منع الحوادث السيبرانية التي قد تؤدي إلى أنشطة إجرامية؛

(يي) ينبغي أن تكون هناك منهجية وإجراءات موحدة لتبادل المعلومات الآنية القائمة على الأدلة لمنع الجريمة السيبرانية؛

(كك) ينبغي وضع آلية لتسجيل جميع الخدمات على الإنترنت وتنفيذ الحد الأدنى من المعايير الأمنية الأساسية من خلال اللوائح المحلية؛

(لل) ينبغي للدول أن تنظر في استخدام الذكاء الاصطناعي لتصميم النظم التي تقوم بإعادة تشكيل نفسها تلقائيا في مواجهة الهجمات؛

(مم) أوصي بإنشاء قاعدة بيانات عالمية بشأن الانتهاكات المتعلقة بالعملات المشفرة واستغلال المجرمين للبيانات على نطاق واسع، فضلا عن إجراء استعراض استراتيجي منسق على الصعيد العالمي للتهديدات التي تشكلها الجرائم الجنائية المرتكبة على الشبكة الخفية؛

(نن) ينبغي تشجيع المبادرات الإقليمية والدولية الرامية إلى تعزيز الأمن السيبراني، ولا سيما تبادل المعلومات عن الهجمات السيبرانية الواسعة النطاق؛

(سس) لعل الدول تنظر في إنشاء نظام دولي لتبادل المعلومات عن التهديدات السيبرانية بغرض تبادل ودراسة التكنولوجيات وأساليب العمل المتعلقة بالتهديدات الجديدة؛

(عع) تشجع الدول على إنشاء نظام متعدد المستويات لحماية الأمن السيبراني بغرض اعتماد تكنولوجيات مختلفة لأمن المعلومات وتدابير لإدارة مختلف مرافق المعلومات والاتصالات، وضمان حماية البنية التحتية الحيوية من الجرائم السيبرانية؛

(فـف) ينبغي للدول أن تشرك خبيرات في مجال منع الجرائم السيبرانية والتحقيق فيها؛

(صص) ينبغي الجمع بين الخبرات الوطنية والإقليمية في مجال المنع من أجل إنشاء مستودع متعدد الأطراف يتيح نشر الممارسات الجيدة في سياقات مختلفة؛

(قق) ينبغي تعزيز التدابير الرامية إلى منع انتشار خطاب الكراهية والتطرف والعنصرية؛

(رر) ينبغي زيادة الوعي وتقديم المساعدة التشريعية بشأن الأطر التنظيمية الرامية إلى مكافحة التنمر السيبراني والتهديد بالعنف أو الاعتداء عبر الإنترنت؛

(شش) ينبغي بناء القدرات وتوفير التعاون في مجال منع الجريمة السيبرانية مع الجهات الفاعلة والمنظمات الإقليمية الأخرى (مثل منظمة الدول الأمريكية) ومع منتديات أصحاب المصلحة المتعددين مثل المنتدى العالمي للخبرة السيبرانية؛

(تت) تشجع الدول على أن تغتنم الفرصة للتفاوض على اتفاقية جديدة بشأن مكافحة الجرائم السيبرانية من أجل صياغة معايير موحدة في مجال المنع بغية تنسيق الإجراءات في مختلف البلدان على نحو أكثر فعالية؛

(ثث) أوصي بأن تستثمر الدول في بناء القدرات بغرض رفع مستوى مهارات الموظفين على كامل نطاق نظام العدالة الجنائية كتدبير فعال للمنع له تأثير رادع بالنسبة للجريمة السيبرانية؛

(خ خ) ينبغي أن ييسر المكتب المعني بالمخدرات والجريمة تبادل الممارسات الفضلى بشأن تدابير المنع الفعالة والناجحة لمكافحة الجريمة السيبرانية.

ثالثا- ملخص المداولات (ملخص مقدم من الرئيس)

15- أعدت الأمانة، على ضوء ما جرى في الاجتماع، ملخص المداولات التالي بعد الاجتماع بالتنسيق الوثيق مع الرئيس، عملا بتنظيم الأعمال المقترح للاجتماع، الذي عمم على المكتب الموسع لفريق الخبراء في 13 تموز/يوليه 2020، ووافق عليه فريق الخبراء في افتتاح الاجتماع. ولم يخضع ملخص المداولات هذا للمناقشة، ومن ثم فهو لم يعتمد أثناء الاجتماع. وأصبح التقرير من ثم ملخصا مقدما من الرئيس، على النحو المبين في الأقسام ألف إلى جيم أدناه.

ألف- التعاون الدولي

16- نظر فريق الخبراء، أثناء جلساته الأولى والثانية والثالثة المعقودة يومي27 و28 تموز/يوليه 2020، في البند 2 من جدول الأعمال المعنون "التعاون الدولي".

17- وتولى تيسير المناقشة المناظرون التالية أسماؤهم: جورج ماريا تينديزوا (نيجيريا)، وغانتشيان جانغ (الصين)، وأمرونكي ليلاكانويت (تايلند)، وماركو كينَّبو (إستونيا)، وفاديم سوشيك (الاتحاد الروسي)، وبيدرو جانيس (الأرجنتين)، وستيفن ماكجلين (أستراليا)، وشيري إل. شيبرد-برات (الولايات المتحدة).

18- وأثناء المناقشة، أشار المتكلمون إلى الزيادة السريعة في الجريمة السيبرانية، وكذلك في ضوء التحديات التي تطرحها جائحة كوفيد-19، وشددوا على أهمية تعزيز التعاون الدولي من أجل التصدي بفعالية لآفة الجرائم التي ترتكب وتيسر بواسطة الفضاء السيبراني والتي لها طابع عبر وطني وتنطوي على مستويات عالية من التطور الإجرامي والتكيف مع الظروف والأولويات المتغيرة. وفي هذا الصدد، أشار العديد من المتكلمين إلى الإجراءات و/أو الإصلاحات الوطنية المتخذة من أجل وضع وتنفيذ استراتيجيات وسياسات بشأن

الجريمة السيبرانية؛ وسن تشريعات بشأن الجريمة السيبرانية و/أو تطوير التشريعات القائمة بشأنها؛ وتنفيذ أدوات جديدة للتحقيق بغرض جمع الأدلة الإلكترونية؛ والعمل، استنادا إلى تدابير داخلية قوية وقدرات محسنة وبنية تحتية محسنة، على تعزيز التعاون الدولي على مكافحة الجريمة السيبرانية.

19- وأشار المتكلمون إلى أن التحديات التي يطرحها الافتقار إلى مواءمة أحكام التجريم، والثغرات في الصلاحيات الإجرائية لسلطات إنفاذ القانون والعدالة الجنائية، والتنازع في الولاية القضائية عند تأمين الأدلة الإلكترونية، تدعو إلى تجديد التزام الدول الأعضاء بتنفيذ التعاون الإقليمي والدولي الفعال والقوي في مجال مكافحة الجريمة السيبرانية. وفي هذا الصدد، سلط الضوء على أنه على الرغم من الدور الحيوي للتعاون الدولي في التصدي للجريمة السيبرانية ومنعها، فإنه ينبغي تعزيزه بالاقتران مع مراعاة مبدأي السيادة واحترام القوانين الوطنية، وفي حال عدم وجود معاهدة سارية، المعاملة بالمثل، وكذلك مع مراعاة تفاوت مستويات القدرة والموارد لدى الدول الأعضاء، ولا سيما البلدان النامية.

20- وأشير إلى أنه منذ الاجتماع السابق لفريق الخبراء، حدثت تطورات في اللجنة الثالثة التابعة للجمعية العامة أضافت بعدا آخر إلى الحوار الدولي بشأن الجرائم السيبرانية، وهو اعتماد الجمعية العامة للقرار 247/74، الذي قررت فيه الجمعية العامة إنشاء لجنة خبراء حكومية دولية مخصصة مفتوحة العضوية، تُمثَّل فيها جميع الأقاليم، لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية.

21- وأعرب عدد من المتكلمين عن رأي مفاده أن وضع اتفاقية لمكافحة الجريمة السيبرانية في إطار الأمم المتحدة من شأنه أن ييسر كفاءة التعاون الدولي في مجال مكافحة الجريمة السيبرانية، وأنه سيكون أنسب وسيلة للتصدي للجريمة السيبرانية على الصعيد الدولي. وشددوا في هذا الصدد على أن صكا عالميا جديدا لمكافحة الجريمة السيبرانية سوف يراعي جملة أمور منها شواغل ومصالح جميع الدول الأعضاء، ولا سيما البلدان النامية، وسيسهم في سد الثغرات القانونية في هذا المجال. ورأى بعض هؤلاء المتكلمين أن اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية محدودة نظرا لطبيعتها كصك إقليمي وحالة التصديق عليها، وافتقارها إلى نهج كلي، إذ إنها لا تراعي الاتجاهات الراهنة في مجال الجريمة السيبرانية، ولا تلائم البلدان النامية على نحو كامل.

22- وأعرب متكلمون آخرون عن تفضيلهم للاستفادة على أفضل وجه ممكن من الصكوك أو الأطر والآليات الدولية القائمة، مثل اتفاقية مكافحة الجريمة المنظمة واتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية والإنتربول. وفيما يتعلق باتفاقية الجريمة المنظمة على وجه الخصوص، شدد بعض المتكلمين على أنها يمكن أن تكون أداة مفيدة جدا للتعاون الدولي في مجال مكافحة الجريمة السيبرانية. وأكدت إحدى المتكلمات أن بلدها أرسل وتلقى طلبات عديدة للمساعدة استندت إلى أحكام تلك الاتفاقية كأساس قانوني للتعاون الدولي الذي يشمل الأدلة الإلكترونية في قضايا الجرائم السيبرانية. وأشارت المتكلمة نفسها، تأييدا كذلك لاستخدام ذلك الصك، إلى أنه في معظم القضايا الكبرى، تنشأ الجرائم السيبرانية في إطار شكل من أشكال الجريمة المنظمة، مثل الأنشطة في "الأسواق" الخفية، ومن خلال مرتكبي جرائم في أكثر من بلد واحد، وأن عدد قضايا الجرائم السيبرانية المتعلقة بالجماعات الإجرامية المنظمة كثيرا ما يفوق عدد الحالات التي يكون فيها القراصنة الأفراد هم العناصر الإجرامية الرئيسية.

23- ورأى عدد من المتكلمين أن اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية توفر إطارا ملائما لوضع ما يناسب من تدابير محلية ودولية للتصدي للجريمة السيبرانية. وأشار هؤلاء المتكلمون إلى وجود 65 دولة طرفا في الاتفاقية، منها 21 دولة من غير الأعضاء في مجلس أوروبا، ومن ثم فإن الاتفاقية استخدمت كأساس للتعاون الدولي الفعال ونموذج لوضع تشريعات وطنية ومعيار لبناء القدرات والمساعدة التقنية. وأضافوا أن هذه الاتفاقية ستظل الاتفاق المتعدد الأطراف الاستباقي الأهم بشأن الجريمة السيبرانية في المستقبل المنظور، حيث إنها متاحة للبلدان التي تسعى إلى إيجاد مسار فوري لإجراء إصلاحات تشريعية بشأن

الجريمة السيبرانية، وتعزيز القدرة على إنفاذ القانون، وزيادة التعاون الدولي، دون المساس بالمناقشات المقبلة بشأن صك جديد في إطار الأمم المتحدة. غير أن أحد المتكلمين أشار إلى أن الاتفاقية تواجه أيضا تحديات تتعلق بضعف التنفيذ في بعض الولايات القضائية، ولذلك فإنه ينبغي اعتبار تدابير التصدي المستندة إلى أحكامها في حالة تطور مستمر.

24- وأشير إلى عملية التفاوض الجارية من أجل اعتماد بروتوكول إضافي ثان لاتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية بهدف توفير قواعد واضحة وإجراءات أكثر فعالية بشأن الأحكام التي تجعل التعاون الدولي أكثر فعالية وسرعة؛ والأحكام التي تتيح التعاون المباشر مع مقدمي الخدمات في ولايات قضائية أخرى فيما يتعلق بطلبات المعلومات عن المشتركين، وطلبات حفظ البيانات، والطلبات الطارئة؛ والإطار والضمانات القوية للممارسات التي تنطوي على إمكانية الوصول إلى البيانات عبر الحدود، بما في ذلك متطلبات حماية البيانات.

25- واسترعى بعض المتكلمين انتباه فريق الخبراء إلى الخبرات في مجال التعاون الدولي المكتسبة في إطار المنظمات الإقليمية، مثل منظمة الدول الأمريكية، والشبكات الإقليمية، مثل مجتمع الشرطة في القارة الأمريكية، بينما ذكر أحد المتكلمين أن بلده يواصل العمل عن كثب مع المنظمة الأفريقية للتعاون بين أجهزة الشرطة (أفريبول) لمكافحة الجريمة السيبرانية.

26- ومع مراعاة المناقشات الجارية بغرض التوصل إلى اتفاق بشأن الخطوط العريضة وطرائق عمل الأنشطة الأخرى التي تضطلع بها لجنة الخبراء الحكومية الدولية المخصصة المعنية بوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، جرى التشديد على أن الاتفاقية الجديدة ينبغي أن تهدف إلى اتباع نهج شامل وإلى تصديق/انضمام أكبر عدد ممكن من الدول إليها، باتباع المثالين الناجحين لاتفاقية الجريمة المنظمة واتفاقية مكافحة الفساد. وكانت هناك دعوة أيضا إلى أن تكون عملية وضع الاتفاقية شفافة وشاملة وقائمة على التوافق في الآراء، وأن تسترشد بنتائج وتوصيات فريق الخبراء، وتراعي التقدم الذي يكون المجتمع الدولي قد أحرزه بالفعل، وكذلك الحاجة إلى تعزيز وجود شبكة إنترنت مجانية ومفتوحة وآمنة وحماية حقوق الإنسان على الإنترنت، بما في ذلك حماية البيانات ذات الطابع الشخصي والحق في الخصوصية. وأشار بعض المتكلمين إلى أن أي اتفاقية جديدة ينبغي أن تصاغ على أساس التوافق في الآراء، وأن تراعي الأطر والصكوك القائمة وألا تتعارض معها أو تكون ازدواجا لها؛ وينبغي ألا تخلق عقبات أو تتسبب في أن تتخلى الدول عن الالتزامات التي سبق أن قطعتها على نفسها أو تعارضها.

27- وأشار بعض المتكلمين إلى أنه مع التقدم المحرز في مجال التكنولوجيا السحابية، يتزايد حجم تخزين الأدلة الإلكترونية على خوادم خارج الولاية القضائية الإقليمية للدول الأعضاء. ونظرا للطابع عبر الوطني والمتقلب لمثل هذه الأدلة الإلكترونية، أشير إلى التعاون المباشر الذي يركز أساسا على تبادل المعلومات الاستخبارية باعتباره أداة مفيدة جدا لمعالجة المسائل المتعلقة بضيق الوقت والتحديات التي تفرضها الظروف الطارئة من خلال تقصير المدة اللازمة لتفعيل قنوات المساعدة القانونية المتبادلة. وذكر أن التعاون المباشر لا يزال يعتمد على الثقة المتبادلة، وإن كان سيستفيد أيضا من توحيد الطلبات والتعجيل بحفظ البيانات، وكذلك زيادة تواتر استخدام الآليات القائمة بالفعل، مثل المنظومة العالمية للاتصالات الشرطية المأمونة (I-24/7) التي أنشأتها الإنتربول، فضلا عن شبكات أفرقة التصدي لحوادث الأمن الحاسوبي، الخاصة والعامة على حد سواء. وعلاوة على ذلك، قد تكون هناك حاجة إلى وضع بروتوكولات مبتكرة لتبادل المعلومات والأدلة من أجل التعجيل بهذه الإجراءات.

28- وأشير إلى أن من الخطوات الرئيسية في الجريمة السيبرانية والتحقيقات الرقمية عبر الحدود الحفاظ على سلامة الأدلة الإلكترونية وضمان صحتها ومقبوليتها كدليل في الإجراءات الجنائية ذات الصلة، مع اعتبار أن المسائل المتعلقة بتسلسل العهدة ونُسَخ الأدلة الجنائية أساسية. ومن هذا المنظور، لوحظ أنه ينبغي إيلاء

الأولوية لتحسين أساليب التحري الخاصة، لا لجمع الأدلة الإلكترونية فحسب، بما في ذلك على الشبكة الخفية، وإنما أيضا لإجراء التحقيقات المالية. وفي هذا الصدد، ذكر أحد المتكلمين أن تدابير مكافحة غسل الأموال وتمويل الإرهاب، وكذلك تدابير استرداد الموجودات، ينبغي أن تكون جزءا أساسيا من تدابير أجهزة إنفاذ القانون في مجال التصدي للجريمة السيبرانية. وأشار متكلمون آخرون إلى التحديات التي تطرحها العملات المشفرة في مجال التحقيق في التدفقات غير المشروعة المتعلقة بعائدات الجريمة وملاحقة المسؤولين عنها قضائيا. وسلط عدد من المتكلمين الضوء على ضرورة وأهمية استكشاف السبل والوسائل الكفيلة بتمكين الممارسين في مجال العدالة الجنائية وإنفاذ القانون من توظيف التكنولوجيات المتطورة، مثل الذكاء الاصطناعي وتكنولوجيات المعلومات والاتصالات، بما في ذلك البيانات الضخمة، والاستفادة الكاملة منها في مكافحة الجريمة السيبرانية.

29- وفي مجال المساعدة القانونية المتبادلة، اعتبر التنفيذ السريع لطلبات المساعدة القانونية المتبادلة أحد أهم الشروط اللازمة لفعالية تدابير مكافحة الجريمة السيبرانية وغيرها من الجرائم التي تنطوي على أدلة إلكترونية. وأشار بعض المتكلمين إلى العوامل التي تؤثر سلبا على كفاءة المساعدة القانونية المتبادلة في مجال الجريمة السيبرانية، بما في ذلك مختلف المقتضيات القانونية ونهوج التجريم التي تعيق الوفاء بشرط التجريم المزدوج، وكذلك عدم وجود محتوى وشكل موحد للطلبات ذات الصلة.

30- وللتعجيل بإجراءات التعاون الدولي وتبسيط عمليات المساعدة القانونية المتبادلة، اقترح وضع نظام منفصل للحصول على معلومات عن المشتركين. وفي هذا الصدد، أشير إلى أنه في سياق المناقشات الجارية بشأن البروتوكول الإضافي الثاني الملحق باتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، يجري النظر في تدابير الحصول على معلومات المشتركين على نحو أسرع.

31- وأشار أحد المتكلمين إلى التدابير الرئيسية التي يمكن للبلدان اتخاذها لتقليص المدة اللازمة لتنفيذ طلبات المساعدة القانونية المتبادلة، بما في ذلك بناء القدرات والمتطلبات القطرية الخاصة بطلبات المساعدة القانونية المتبادلة، من أجل تقليص وقت الاستجابة وتيسير تنفيذ الطلب دون اتصالات إضافية موسعة للحصول على معلومات إضافية؛ واستخدام قنوات الاتصال المباشرة بين السلطات المركزية بدلا من القنوات الدبلوماسية الرسمية.

32- وشدد بعض المتكلمين على الحاجة إلى تحديث الممارسة المتعلقة بالمساعدة القانونية المتبادلة وتبسيطها والتعجيل بها من خلال إرسال طلبات التعاون الدولي إلكترونيا، وهي ممارسة جرى اتباعها مؤخرا في بعض البلدان الإيبيرية-الأمريكية. واقترح في هذا الصدد أن ترسل السلطات المركزية وغيرها من السلطات المختصة طلبات المساعدة، سواء كانت رسمية أو فيما بين المؤسسات، عن طريق البريد الالكتروني، وكذلك طلبات الحفظ، باستخدام الشبكات العاملة على مدار الساعة (24/7).

33- وأشار بعض المتكلمين إلى إمكانية الوصول عبر الحدود الوطنية إلى البيانات الحاسوبية المخزنة، مُذكِّرين بأن اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية تتضمن حكما محددا (المادة 32) بشأن ذلك، وشددوا على ضرورة تنفيذ التدابير ذات الصلة بعناية من أجل تحقيق التوازن بين الحاجة إلى إجراء تحقيقات وحماية حقوق الإنسان وسيادة الدول.

34- وشدد العديد من المتكلمين على أهمية بناء الشبكات من أجل تعزيز التعاون الدولي للتصدي للجريمة السيبرانية. ولوحظ أن الشبكات العاملة على مدار الساعة (24/7)، التي تضم جهات اتصال مسؤولة في كل بلد مشارك، تؤدي دورا حيويا في تيسير التعاون، ولا سيما فيما يتعلق بحالات الطوارئ. كما تيسر هذه الشبكات الطلبات المتعلقة بحفظ البيانات التي كثيرا ما تصبح موضوع طلب المساعدة القانونية المتبادلة في مرحلة لاحقة؛ ويتم التعامل مع طلبات الحفظ هذه في العادة خلال أيام، إن لم يكن ساعات. وسلم على نطاق واسع بأن احتمال تأخر التحقيقات المتعلقة بالجرائم السيبرانية – حيث يمكن حذف الأدلة بسرعة وفقدان البيانات أو

تعديلها – يجعل العضوية في الشبكات العاملة على مدار الساعة (24/7) وإمكانية التواصل مع موظفي الاتصال ضرورية. ولهذا السبب، اتفق المتكلمون على أنه ينبغي للسلطات المركزية وغيرها من السلطات المختصة أن تنشئ علاقات وأن تزيد من تعزيز الثقة المتبادلة من خلال الاتصال المباشر والمشاورات المباشرة، وكذلك من خلال الشبكات الإقليمية والدولية في مجال القضاء والمسائل الجنائية أو الشبكات المتخصصة لمكافحة الجريمة السيبرانية. ومن الأمثلة التي ذكرت في هذا الصدد شبكة التعاون القضائي في جنوب شرق آسيا (SeaJUST network) المؤسسة حديثا، وشبكة Cybernet (وهي شبكة تابعة لرابطة المدعين العامين الإيبيرية–الأمريكية تضم جهات الاتصال المتخصصة من أعضاء النيابة العامة والوزارات في جميع الدول الأعضاء في الرابطة)؛ وشبكة التعاون في المجالات الجنائية التابعة للرابطة.

35- ورأى بعض المتكلمين أن الهياكل أو الوحدات المتخصصة في الجرائم السيبرانية داخل السلطات المركزية يمكن أن تشكل أساسا للخبرة في مجال التعاون الدولي المعقد. ويمكن لهذه الهياكل أو الوحدات المتخصصة أن توفر ما يلزم من موارد وخبرة في مجال التفعيل اليومي لنظام المساعدة القانونية المتبادلة، كما تسمح بتوفير تدريب مركز للسلطات المحلية والأجنبية بشأن كيفية الحصول على المساعدة والأدلة الإلكترونية في الوقت المناسب وبطريقة فعالة في القضايا المتصلة بالفضاء السيبراني.

36- وسلط العديد من المتكلمين الضوء على أهمية تعزيز وتوطيد التعاون بين السلطات الوطنية والقطاع الخاص، وبخاصة مقدمي خدمات الاتصالات ومقدمي خدمات الإنترنت، من أجل تعزيز الحفاظ على البيانات والوصول إليها، وتيسير التصدي للجرائم السيبرانية في الوقت المناسب، وبخاصة في القضايا عبر الوطنية. واقترح وضع إطار مرجعي أو دليل لتيسير التوصل إلى فهم مشترك بين الجانبين للمتطلبات والعمليات. وشدد على ضرورة وضع أحكام تتيح التعاون المباشر مع مقدمي الخدمات في ولايات قضائية أخرى فيما يتعلق بطلبات المعلومات عن المشتركين، وطلبات حفظ البيانات. وأعرب عن الأمل في أن يوفر البروتوكول الإضافي الثاني الملحق باتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، الذي يجري التفاوض بشأنه، حلا أكثر اكتمالا للتعاون المباشر مع كيانات القطاع الخاص.

37- وشدد أحد المتكلمين على أن الإنتربول تؤدي دورا فريدا في تيسير التعاون المباشر بين أجهزة الشرطة، من خلال المكاتب المركزية الوطنية في كل بلد، والمنظومة العالمية للاتصالات الشرطية (I-24/7) وإشعاراتها وقواعد بياناتها؛ وأن البرنامج العالمي المعني بالجريمة السيبرانية التابع للإنتربول، على وجه الخصوص، أنشأ منبرا تحليليا سيبرانيا وقدرات على التعاون من أجل تبادل المعارف والتنسيق العملياتي.

38- وأولى العديد من المتكلمين الأولوية إلى الحاجة إلى بناء قدرات مستدامة داخل النظم الوطنية لإنفاذ القانون والعدالة الجنائية، بما في ذلك بناء قدرات الممارسين من السلطات المركزية العاملين في مجال التعاون الدولي. وأشير إلى أن بناء القدرات يمثل أمرا أساسيا، وبخاصة للبلدان النامية، من أجل تطوير الموارد البشرية والبنى التحتية والمعدات، وسد الفجوة الرقمية مع البلدان المتقدمة.

39- وكان هناك اتفاق واسع النطاق على أن أنشطة بناء القدرات والمساعدة التقنية المقدمة استنادا إلى الصكوك القائمة أدوات قيمة وفعالة لمكافحة الجريمة السيبرانية، وأنه ينبغي من ثم مواصلة تطويرها ومنحها الأولوية، مع احترام أولويات الدول الأعضاء. وفي هذا الصدد، أعرب عدد من المتكلمين عن دعمهم، كجهات مانحة أو متلقية للمساعدة، للبرنامج العالمي المعني بالجريمة السيبرانية التابع للمكتب المعني بمكافحة المخدرات وغيره من برامج أو أطر المساعدة التقنية، مثل تلك المقدمة من الإنتربول، وبرامج مجلس أوروبا الموسعة المتعلقة بالتدابير العالمية لمكافحة الجريمة السيبرانية، وبرنامج الأمن السيبراني في سياق إعلان "بو" بشأن الأمن الإقليمي لمنتدى جزر المحيط الهادئ.

40- وفيما يتعلق بدور المكتب المعني بالمخدرات والجريمة، ركز العديد من المتكلمين على تشجيع المكتب على مواصلة توفير برامج بناء القدرات والتدريب على مكافحة الجريمة السيبرانية إلى خبراء من ذوي الاختصاص بغرض تعزيز القدرات الوطنية على كشف الجرائم السيبرانية والتحقيق فيها وتيسير تبادل الممارسات الفضلى بشأن تدابير المنع الفعالة والناجحة لمكافحة الجريمة السيبرانية. وشدد على وجه الخصوص على الحاجة إلى تدريب جهات فاعلة مختلفة في مجالات العدالة الجنائية وإنفاذ القانون، بما في ذلك القضاة وأعضاء النيابة العامة وموظفو الأمن؛ وإنشاء وحدات متخصصة للتحقيق في جرائم الفضاء السيبراني وملاحقة مرتكبيها قضائيا، والهيكل المناسب لتلك الوحدات؛ وضمان الوصول إلى أحدث التقنيات في مجال التحقيقات في الجرائم السيبرانية والتحليل الجنائي الرقمي. وأشار بعض المتكلمين إلى أنه ينبغي لمبادرات بناء القدرات ذات الصلة أن تلبي احتياجات البلدان النامية، وأن تركز على أوجه ضعف كل بلد من أجل تقديم مساعدة تقنية مصممة حسب الحاجة، وأن تشجع على تبادل أحدث المعارف خدمة لمصلحة الممارسين وأصحاب المصلحة.

41- وأشار أحد المتكلمين إلى أهمية تدريب موظفي إنفاذ القانون والأعمال التي تضطلع بها أكاديمية الجرائم السيبرانية التابعة لوكالة الاتحاد الأوروبي للتدريب على إنفاذ القانون والأكاديمية الدولية لإنفاذ القانون. وشدد أيضا على أهمية التعاون الدولي في مجال التدريب والتثقيف. وأعرب بعض المتكلمين عن تأييدهم لتوفير التدريب للقضاة المتخصصين وغيرهم من القضاة الذين يتعاملون مع قضايا الجرائم السيبرانية، وتزويد هيئات التحقيق بأدوات عالية الأداء لتتبع العملات المشفرة ومعالجة استخدامها لأغراض إجرامية.

42- وسلط بعض المتكلمين الضوء على الابتكارات، مثل إدماج نميطة خاصة بالأدلة الإلكترونية في أداة المكتب المعني بالمخدرات والجريمة لكتابة طلبات المساعدة القانونية المتبادلة المُحدَّثة التي قد تساعد في تبسيط عمليات المساعدة القانونية المتبادلة التي تنطوي على أدلة إثباتية إلكترونية. وبالمثل، أشير إلى الدليل العملي لطلب الأدلة الإلكترونية عبر الحدود، وعنوانه *Practical Guide for Requesting Electronic Evidence Across Borders* كجزء من دور المكتب في تقديم المساعدة التقنية للدول الأعضاء.

43- وشدد عدد من المتكلمين على أنه ينبغي للدول الأعضاء أن تمتنع عن الانفراد باتخاذ تدابير غير قانونية لا تتفق مع القانون الدولي وميثاق الأمم المتحدة وتحول دون تحقيق التنمية الاقتصادية والاجتماعية التامة لسكان البلدان المتضررة. وذكر أن هذه التدابير القسرية الانفرادية أعاقت التعاون مع سلطات إنفاذ القانون الوطنية في التحقيق في الجرائم المرتكبة من خلال استخدام تكنولوجيات المعلومات والاتصالات وملاحقة مرتكبيها قضائيا، وكذلك في نقل الأدوات التكنولوجية اللازمة للحفاظ على الأدلة الإلكترونية وإجراء فحوص التحليل الجنائي الرقمية.

44- وأعرب بعض المتكلمين عن قلقهم بشأن الهجمات السيبرانية التي تشنها بعض الدول الأعضاء أو الجماعات التي ترعاها الدول على قطاعات البنى التحتية الحيوية، ومنها قطاع الصحة، وشددوا على ضرورة إدانة مثل هذا الإجراء بقوة وخضوع المسؤولين عنه للمساءلة. وأعرب متكلم آخر عن قلقه البالغ بشأن الواقع الجديد الذي أوجدته جائحة كوفيد-19 في قطاع الصحة، الذي أصبح هدفا مباشرا وضحية عرضية للهجمات على الأمن السيبراني، بالإضافة إلى التحديات الهائلة التي تجري مواجهتها في مجال الرعاية الصحية.

45- ورأى بعض المتكلمين أنه ينبغي للجنة منع الجريمة والعدالة الجنائية أن تنظر في تمديد خطة عمل فريق الخبراء إلى ما بعد عام 2021 من أجل الاحتفاظ بمنتدى للخبراء والممارسين لتبادل المعلومات عن الجريمة السيبرانية، بما في ذلك لغرض دراسة النهوج المتبعة إزاء الاعتداء الجنسي على الأطفال واستغلالهم جنسيا عبر الإنترنت، وغير ذلك من أشكال الجريمة السيبرانية المستجدة. وأكد متكلمون آخرون أنه لا يوجد ما يدعو، بعد إتمام تنفيذ خطة عمل فريق الخبراء في الاجتماع التقييمي المقرر عقده في عام 2021، إلى تمديد

ولاية الفريق، في ضـــوء قرار الجمعية العامة 247/74 والحاجة إلى التركيز على تنفيذ ذلك القرار، والتفاوض على الاتفاقية الجديدة، والاستفادة على أفضل وجه من الموارد المتاحة.

46- وأشـــار أحد المتكلمين إلى أنه على الرغم من وجود اختلافات بين ولاية فريق الخبراء وقرار الجمعية العامة 247/74، ينبغي تركيز الاهتمام على أوجه التقارب والتكامل. وفي ضوء ذلك، ينبغي أن يجسد التعاون الدولي وبناء القدرات، اللذان أحرز فريق الخبراء تقدما بشأنهما، كركيزتين من ركائز الأعمال التي ستضطلع بها اللجنة المخصصة المكلفة بالتفاوض بشأن الاتفاقية الجديدة في المستقبل.

47- وشدد متكلم آخر على أنه لا ينبغي أن تبدأ اللجنة المخصصة عملها إلا بعد أن ينتهي فريق الخبراء من وضع توصياته ويرسلها إلى لجنة منع الجريمة والعدالة الجنائية في عام 2021.

باء- المنع

48- نظر فريق الخبراء، أثناء جلستيه الرابعة والخامسة المعقودتين يومي 28 و29 تموز/يوليه 2020، في البند 3 من جدول الأعمال المعنون "المنع".

49- وتولى تيسير المناقشة المناظرون التالية أسماؤهم: دستينو بيدرو (أنغولا)، ولايون هان (الصين)، وبينجابورن واتشارافوتيشي (تايلند)، وهوراشيو أزولين (الأرجنتين)، وكلاوديو بيغيرو (الجمهورية الدومينيكية)، وبيدرو فيرديلهو (البرتغال).

50- وخلال المناقشة، أشير إلى أن منع الجريمة السيبرانية أصبح عنصرا هاما من عناصر السياسات والاستراتيجيات الوطنية الرامية إلى منع ومكافحة الهجمات والتهديدات السيبرانية وتقليل مواطن الضعف في البنية التحتية السيبرانية والتمكن من إدارة جميع المخاطر ذات الصلة بصورة فعالة. وجرى النظر في منع الجريمة السيبرانية في إطار نهج شامل لمكافحة الجريمة السيبرانية يمكن تنفيذه على نطاق واسع لجعل الإنترنت وتكنولوجيات الاتصالات ذات الصلة متاحة دائما وأكثر أمانا للمستخدمين، وكذلك تعزيز التعاون في جميع القطاعات وعلى جميع المستويات بين الجهات الفاعلة المعنية على الصعيدين الوطني والدولي.

51- وأبرز عدد من المتكلمين أنه ينبغي للدول الأعضاء، في سياق وضع استراتيجيات واسعة النطاق لمنع الجريمة السيبرانية، أن تراعي التزاماتها الدولية في مجال حقوق الإنسان. وردد متكلمون آخرون رأيا مفاده أن صياغة الاستراتيجيات والمقترحات المتعلقة بمنع الجريمة السيبرانية ينبغي أن تستند إلى رؤية شاملة تراعي التمايز وعدم الاتساق من حيث الأثر على مختلف الفئات السكانية داخل البلد، وكذلك على البلدان المختلفة، لا سيما بالنظر إلى الفجوة الرقمية بين البلدان المتقدمة النمو والبلدان النامية، وافتقار بعض البلدان النامية إلى القدرة على منع الجرائم السيبرانية وكشفها ومكافحتها، وكونها أضعف حالا في مواجهة التحديات التي تمثلها تلك الجرائم.

52- ولوحظ أن التعاون بشأن الأمن السيبراني في بعض الولايات القضائية يختلف عن البرامج الرامية إلى دعم التحقيقات المتعلقة بالجرائم السيبرانية، وأنه رغم أن هذا التعاون وسياسات الإنفاذ الرامية إلى مكافحة الجريمة السيبرانية يعتبران في كثير من الأحيان وجهين لعملة واحدة، فإن تلك السياسات هي مسؤولية تتحملها الحكومة وحدها، في حين أن الأمن السيبراني هو مسؤولية مجموعة من الجهات الفاعلة في القطاعين العام والخاص. وعلاوة على ذلك، أفيد بأن المنظمات العامة والخاصة تواصل تعزيز التوعية في أوساط المنشآت التجارية من خلال برامج تهدف إلى تحسين مهارات موظفي تكنولوجيا المعلومات في المنشآت التجارية في مجال الأمن السيبراني.

53- واعتبر العديد من المتكلمين أن استراتيجيات أصحاب المصلحة المتعددين فيما يخص الجريمة السيبرانية هي عنصر وقائي حيوي في مجال مكافحة الجريمة السيبرانية. وشدد على أن التحديات القانونية

والتقنية والمؤسسية التي تفرضها الجريمة السيبرانية هي تحديات بعيدة المدى ولا يمكن معالجتها إلا باتباع استراتيجيات متماسكة وشاملة تستند إلى المبادرات القائمة والأدوار التي يضطلع بها سائر أصحاب المصلحة. ومن هذا المنظور، شُدد على ضرورة تعزيز وزيادة مشاركة جميع الجهات الفاعلة ذات الصلة في منع الجريمة السيبرانية، ولوحظ أنه يمكن للمنظمات الإقليمية والقطاع الخاص والأوساط الأكاديمية توفير دعم أساسي، لا سيما للبلدان النامية، من أجل تحقيق ثقافة أمن سيبراني عالمية.

54- وأكد العديد من المتكلمين ضرورة أن تقيم المؤسسات العامة، مثل سلطات إنفاذ القانون والسلطات القضائية الجنائية ومقدمي خدمات الاتصالات، شراكات بين القطاعين العام والخاص قائمة على الثقة والاطمئنان المتبادلين للتصدي للتحديات المتعددة الجوانب التي تعترض مكافحة الجريمة السيبرانية. وشدد على أهمية وجود شراكات جيدة بين القطاعين العام والخاص، وبخاصة الشراكات المتعلقة بالكشف عن الجرائم والإبلاغ عنها، وتوفير المعلومات عن مواقع المشتبه فيهم والضحايا، وتوفير البيانات الأخرى، حسب الاقتضاء. ومن منظور الشراكات، أشير أيضا إلى ضرورة أن يتحمل مقدمو الخدمات مزيدا من المسؤولية عن الاحتياطات الأمنية كتدابير لدرء الجريمة السيبرانية. وينبغي تحديد هذه المسؤوليات بوضوح. وشدد أيضا على أن أي حلول تتيح التعاون المباشر بين السلطات الوطنية ومقدمي خدمات الإنترنت ينبغي أن تستند إلى سيادة القانون وحقوق الإنسان، بما في ذلك متطلبات حماية البيانات.

55- واسترعى بعض المتكلمين انتباه فريق الخبراء إلى أن مسؤولية حماية البيانات التي تمكن من احترام الحق في الخصوصية لا تقع على عاتق الدول وحدها بل تقع أيضا على عاتق الشركات والجهات الفاعلة الأخرى، وهي مسألة تعتبر أساسية في مجال منع الجريمة السيبرانية، مثلها مثل الحق في حرية التعبير وحرية الصحافة. وذُكِر قطاع الصناعة باعتباره شريكا رئيسيا في منع الجريمة السيبرانية يمكنه العمل مع السلطات العامة بشأن مسائل مثل إحالة القضايا إلى السلطات الوطنية المختصة وإزالة المواد الإجرامية الضارة، بما في ذلك المواد التي تصور اعتداءات جنسية على أطفال والمواد التي تصور أفعال عنف بغيضة.

56- وسلط الضوء على دور المنظمات غير الحكومية والأوساط الأكاديمية في سياق الاستراتيجيات الشاملة التي تستوعب الجميع بشأن منع الجرائم السيبرانية والتحقيق فيها، والتي تراعي حماية حقوق الإنسان، ولا سيما حرية التعبير والخصوصية.

57- وأعرب كثير من المتكلمين عن تفضيلهم لتدابير المنع الفعالة المتخذة على الصعيدين الوطني والدولي التي تشمل ملاحقة الجناة قضائيا ومعاقبتهم، وبذل جهود لمنع وقوع المزيد من الجرائم، بكشف ما يجري من أنشطة إلكترونية غير مشروعة وعرقلتها. واعتبر هذا الجانب عنصرا هاما من عناصر سياسات المنع لما له من أثر رادع، ونوقش هذا الجانب بالاقتران مع ضرورة الاستثمار في بناء القدرات لرفع مستوى مهارات الموظفين على كامل نطاق نظام العدالة الجنائية، بما في ذلك الخبيرات، اللائي ينبغي إشراكهن على الصعيد الوطني في منع الجرائم السيبرانية والتحقيق فيها.

58- وسلط الضوء على أهمية حملات إذكاء الوعي والحملات التعليمية، لا سيما تلك التي تتناول المخاطر الناشئة والمخاطر التي تستهدف فئات معينة مثل الأطفال، بوصفها عنصرا هاما من عناصر سياسات منع الجريمة السيبرانية. وفي هذا السياق، شدد على ضرورة إيلاء الأولوية لتشجيع "ثقافة الأمن السيبراني" من أجل تعزيز وعي جميع الجهات الفاعلة بالمخاطر والتهديدات الجنائية التي تشكلها الجريمة السيبرانية، وكذلك من أجل الوصول إلى فهم مشترك للتدابير الأمنية وتدابير المنع اللازمة.

59- وشدد على ضرورة إدراج الوعي بالأمن السيبراني، وبخاصة مخاطر الجريمة السيبرانية والجانب الخفي من الإنترنت، كموضوع في التعليم الابتدائي والثانوي والعالي، للطلاب والمعلمين على حد سواء.

وأضيف أن ذلك ينبغي أن يكون، في الحالة المثلى، جزءا من استراتيجية وطنية للأمن السيبراني. وشدد بعض المتكلمين على ضرورة منع انتشار خطاب الكراهية والتطرف والعنصرية، فضلا عن التنمر السيبراني والعنف عبر الإنترنت، بما في ذلك العنف الجنساني والعنف ضد المجموعات المستضعفة، إما من خلال مبادرات تثقيفية أو تبسيط الأطر التنظيمية القائمة، أو كليهما. وبالإضافة إلى ذلك، رأى أحد المتكلمين أنه ينبغي للدول أن تولي اهتماما خاصا للتدابير الوقائية الموجهة إلى أوساط الشباب، بما في ذلك من ارتكبوا جريمة للمرة الأولى، بهدف منع معاودة ارتكابهم للجرائم.

60- وألقى أحد المتكلمين الضوء على الحاجة إلى أدوات لضمان أمن التجارة الرقمية، نظرا إلى أنه ينبغي إدراج هذا الموضوع في خطة التنمية الأوسع نطاقا للبلدان التي لم تستفد بعد استفادة كاملة من طريقة التجارة هذه في السلع والخدمات.

61- وأشير إلى تحليل المعلومات الاستخبارية والبحوث الجنائية كأداتين مهمتين لمنع الجريمة السيبرانية. وأشير إلى تحليل مقادير هائلة من المعلومات المفتوحة المصدر (cyberpatrols) كوسيلة لتحديد التهديدات وأوجه الضعف، وتحليل نطاقها وتأثيرها والاستجابة في مرحلة مبكرة من خلال إنذارات وأدلة وتدريب.

62- وأشار أحد المتكلمين إلى ما تضطلع به الإنتربول من أعمال مع الشركاء من القطاعين العام والخاص لوضع استراتيجيات سليمة بشأن الجريمة السيبرانية، بما في ذلك عن طريق تنظيم حملات توعية على الصعيد العالمي لدعم كيانات إنفاذ القانون في التغلب على التحديات التي تواجهها في مكافحة الجرائم السيبرانية وعدم الإبلاغ عن تلك الجرائم بالقدر الكافي.

63- وأبلغ أحد المتكلمين عن العمل المضطلع به في إطار مشروع "لا مزيد من الفدية"، وهو مبادرة مشتركة بين سلطات إنفاذ القانون وشركات أمن تكنولوجيا المعلومات بغرض تفكيك أعمال الجريمة السيبرانية المتصلة بالفدية ومساعدة ضحايا فيروسات الفدية لاسترجاع البيانات المشفرة من دون الدفع للمجرمين. وأشار المتكلم نفسه إلى الشبكة الأوروبية لمنع الجريمة من أجل تبادل الممارسات الفضلى في مجال سياسات الأمن السيبراني والسياسات المتعلقة بالسلامة.

جيم- مسائل أخرى

64- نظر فريق الخبراء أثناء جلسته السادسة المعقودة في 29 تموز/يوليه 2020، في البند 4 من جدول الأعمال، المعنون "مسائل أخرى". ولم تثر أي مسائل في إطار هذا البند من جدول الأعمال.

رابعا- تنظيم الاجتماع

ألف- افتتاح الاجتماع

65- افتتح الاجتماع الدكتور ماشاباني (جنوب أفريقيا)، رئيس فريق الخبراء، الذي فوض أندريه ريبل (البرازيل)، نائب رئيس فريق الخبراء، لرئاسة الاجتماع نيابة عنه.

باء- إقرار جدول الأعمال والمسائل التنظيمية الأخرى

66- اعتمد فريق الخبراء، في جلسته الأولى، المعقودة في 27 تموز/يوليه 2020، جدول الأعمال المؤقت التالي:

1- المسائل التنظيمية:

(أ) افتتاح الاجتماع؛

(ب) إقرار جدول الأعمال.

2- التعاون الدولي.

3- المنع.

4- مسائل أخرى.

5- اعتماد التقرير.

جيم- الكلمات

67- تكلم خبراء من الدول الأعضاء التالية: الاتحاد الروسي، أذربيجان، الأرجنتين، أرمينيا، إسبانيا، أستراليا، إستونيا، إسرائيل، إكوادور، ألمانيا، إندونيسيا، إيطاليا، باراغواي، البرازيل، البرتغال، بولندا، بيرو، تايلند، الجزائر، الجمهورية الدومينيكية، جمهورية إيران الإسلامية، جمهورية فنزويلا البوليفارية، جنوب أفريقيا، رومانيا، شيلي، الصين، العراق، غواتيمالا، فرنسا، الفلبين، فييت نام، كندا، كوبا، كولومبيا، لبنان، ماليزيا، مصر، المكسيك، المملكة المتحدة، منغوليا، النرويج، النمسا، نيجيريا، نيوزيلندا، الهند، هندوراس، هنغاريا، هولندا، الولايات المتحدة، اليابان، اليونان.

68- وألقى كلمة خبير من دولة فلسطين، وهي دولة غير عضو تتمتع بمركز مراقب.[2]

69- وتكلم أيضا ممثلو المنظمات الحكومية الدولية التالية: مجلس أوروبا والاتحاد الأوروبي والإنتربول. وألقى كلمة مراقب من جامعة بيجين التربوية.

دال- الحضور

70- حضر الاجتماع ممثلون عن 93 دولة عضوا، ودولة غير عضو تتمتع بمركز مراقب، ومعهد تابع لشبكة برنامج الأمم المتحدة لمنع الجريمة والعدالة الجنائية، ومنظمات حكومية دولية، والقطاع الخاص.

71- وعممت في الاجتماع قائمة مؤقتة بأسماء المشاركين (UNODC/CCPCJ/EG.4/2020/INF/1).

هاء- الوثائق

72- عرض على فريق الخبراء، بالإضافة إلى التعليقات من الدول الأعضاء الواردة وفقا لخطة العمل للفترة 2018-2021، جدول الأعمال المؤقت المشروح (UNODC/CCPCJ/EG.4/2020/1).

خامسا- اعتماد التقرير

73- اعتمد فريق الخبراء، في جلسته السادسة المعقودة في 29 تموز/يوليه 2020، هذا التقرير.

(2) ألقى المراقب عن دولة فلسطين كلمة أيضا نيابة عن مجموعة الـ77 والصين.