UNODC/CCPCJ/EG.4/2019/2

Distr.: General
12 April 2019
Arabic
Original: English

تقرير عن اجتماع فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، الذي عُقد في فيينا في الفترة من ٢٧ إلى ٢٩ آذار/مارس ٢٠١٩

أولاً- مقدِّمة

١- طلبت الجمعية العامة في قرارها ٦٥/٢٣٠ إلى لجنة منع الجريمة والعدالة الجنائية (اللجنة) 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 لمشكلة 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. واستعرض فريق الخبراء واعتمد، في ذلك الاجتماع، مجموعة من المواضيع ومنهجية من أجل تلك الدراسة (الوثيقة E/CN.15/2011/19، المرفقان الأول والثاني).

٣- وعُقد الاجتماع الثاني لفريق الخبراء في فيينا في الفترة من ٢٥ إلى ٢٨ شباط/فبراير ٢٠١٣؛ وأُحيط فيه الفريق علماً بالدراسة الشاملة لمشكلة الجريمة السيبرانية والتدابير التي تتَّخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدِّي لها، التي أعدَّها مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة (المكتب)، بتوجيه من فريق الخبراء، عملاً بالولاية المتضمَّنة في قرار الجمعية العامة ٦٥/٢٣٠، وحسب مجموعة المواضيع المراد بحثها في إطار الدراسة الشاملة ومنهجية تلك الدراسة، التي اعتمدها فريق الخبراء في اجتماعه الأول. وأُعرب عن آراء مختلفة بشأن مضمون الدراسة ونتائجها والخيارات التي تقدمها (انظر الوثيقة UNODC/CCPCJ/EG.4/2013/3).

٤- وفي إعلان الدوحة بشأن إدماج منع الجريمة والعدالة الجنائية في جدول أعمال الأمم المتحدة الأوسع من أجل التصدِّي للتحديات الاجتماعية والاقتصادية وتعزيز سيادة القانون على الصعيدين الوطني والدولي ومشاركة الجمهور، الذي اعتمده مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية وأقرَّته الجمعية العامة في قرارها ١٧٤/٧٠، نوَّهت الدولُ الأعضاء بأنشطة فريق الخبراء، ودعت اللجنةَ إلى النظر في إصدار توصية بأن يواصل فريق الخبراء، في إطار عمله، 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.

٥- وعُقد الاجتماع الثالث لفريق الخبراء في فيينا في الفترة من ١٠ إلى ١٣ نيسان/أبريل ٢٠١٧. وفي ذلك الاجتماع، نظر فريق الخبراء، ضمن جملة أمور، في اعتماد ملخَّصَيْ المقرِّر لمداولات الاجتماعين الأول والثاني لفريق الخبراء، ومشروع الدراسة الشاملة عن مشكلة الجريمة السيبرانية والتعليقات الواردة بشأنها ومسارات العمل المقبلة في إعداد مشروع الدراسة. كما تبادل فريق الخبراء المعلومات عن التشريعات الوطنية والممارسات الفضلى والمساعدة التقنية والتعاون الدولي.

٦- وطلبت اللجنة، في قرارها ٤/٢٦، الذي اعتمدته في دورتها السادسة والعشرين المعقودة في أيار/مايو ٢٠١٧، إلى فريق الخبراء أن يواصل عمله وأن يعقد في هذا السياق اجتماعات دورية ويعمل كمنتدى لإجراء مزيد من المناقشات بشأن المسائل الموضوعية المتعلقة بالجريمة السيبرانية، ومواكبة اتجاهاتها المتغيرة، بما يتماشى مع إعلاني سلفادور والدوحة. وطلبت أيضاً 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 القائمة للتصدي للجريمة السيبرانية واقتراح تدابير جديدة وطنية ودولية في المجال القانوني أو في مجالات أخرى.

٧- وعُقد الاجتماع الرابع لفريق الخبراء في فيينا في الفترة من ٣ إلى ٥ نيسان/أبريل ٢٠١٨. وركَّز فريق الخبراء خلال ذلك الاجتماع على التشريعات والأطر والتجريم في إطار الجريمة السيبرانية. ونوقشت التطورات التشريعية والسياساتية في مجال التصدي للجريمة السيبرانية على الصعيدين الوطني والدولي، وأولي الاعتبار لسبل تجريم الجريمة السيبرانية على الصعيد الوطني. واعتمد فريق الخبراء خلال ذلك الاجتماع أيضاً المقترح الذي قدمه الرئيس بشأن خطة عمل فريق الخبراء للفترة ٢٠١٨-٢٠٢١ (UNODC/CCPCJ/EG.4/2018/CRP.1).

٨- وحدَّد المكتب الموسَّع في اجتماعه المعقود في ٢ تشرين الثاني/نوفمبر ٢٠١٨ موعد انعقاد الاجتماع الخامس لفريق الخبراء. واتَّفق المكتب الموسَّع، في الاجتماع نفسه، على جدول الأعمال المؤقَّت للاجتماع الخامس.

ثانياً- قائمة التوصيات والاستنتاجات الأولية

٩- وفقاً لخطة عمل فريق الخبراء للفترة ٢٠١٨-٢٠٢١، سوف يُعدُّ المقرِّر، في اجتماعي فريق الخبراء في عامي ٢٠١٩ و٢٠٢٠، قائمة بالاستنتاجات الأولية للدول الأعضاء وتوصياتها المقترحة،

التي ينبغي أن تكون دقيقة وتركِّز على تعزيز تدابير التصدي العملية للجريمة السيبرانية، وسوف يستعين المقرِّر في هذا الشأن بالأمانة ويستند في عمله إلى مناقشات ومداولات فريق الخبراء. ووفقاً لخطة العمل، تُدرج تلك القائمة المعدَّة في التقريرين عن الاجتماعين، باعتبارها تجميعاً للاقتراحات المقدَّمة من الدول الأعضاء لمواصلة مناقشتها في الاجتماع التقييمي الذي سيُعقد في موعد أقصاه عام ٢٠٢١. ووفقاً لخطة العمل، سينظر فريق الخبراء، خلال اجتماعه التقييمي، في الاستنتاجات والتوصيات الأولية، ويجمعها في قائمة تضم الاستنتاجات والتوصيات المعتمدة بغية تقديمها إلى اللجنة. وقبل انعقاد الاجتماع التقييمي، سوف تُعمَّم الاستنتاجات والتوصيات الأولية التي اقترحتها الدول الأعضاء على جميع الدول الأعضاء والمراقبين وسائر الجهات المعنية التماساً لتعليقاتها عليها، وستُنشر تلك التعليقات لاحقاً على الإنترنت قبل انعقاد الاجتماع التقييمي لكي تنظر الوفود فيها.

ألف- إنفاذ القانون والتحقيقات

١٠- تماشياً مع خطة العمل، تتضمن هذه الفقرة تجميعاً للاقتراحات التي قدمتها الدول الأعضاء في الاجتماع في إطار البند ٢ من جدول الأعمال المعنون "إنفاذ القانون والتحقيقات". وهذه الاستنتاجات والتوصيات الأولية مقدمة من الدول الأعضاء، ولا يعني إدراجها أنَّ فريق الخبراء قد أقرَّها، كما أن ترتيب عرضها لا يعني ضمناً ترتيباً لدرجة أهميتها:

(أ) اقترحت بعض الدول الأعضاء أنه نظراً للطابع المتطور والمعقد وعبر الوطني للجريمة السيبرانية، سيكون من السابق لأوانه مناقشة معايير مشتركة في التعاون الدولي. ولذلك، ينبغي للدول الأعضاء أن تسعى إلى إرساء تدابير دولية جديدة لمكافحة الجريمة السيبرانية من خلال النظر في التفاوض على صك قانوني عالمي جديد بشأن الجريمة السيبرانية في إطار الأمم المتحدة. وينبغي النظر في هذا الصك مع مراعاة جملة أمور منها شواغل ومصالح جميع الدول الأعضاء ومشروع اتفاقية الأمم المتحدة بشأن التعاون في مكافحة الجريمة السيبرانية المُقدَّم إلى الأمين العام في ١١ تشرين الأول/أكتوبر ٢٠١٧ (مرفق الوثيقة A/C.3/72/12)؛

(ب) من جانب آخر، رأت دول أعضاء أخرى أن النظر في إعداد صك قانوني عالمي جديد غير ضروري ولا ملائم لأن أفضل طريقة لتذليل التحديات التي تفرضها الجريمة السيبرانية وصعوبات تدريب المحققين والمدعين العامين والقضاة تدريباً كافياً هي بناء القدرات، والتواصل والتعاون النشيطان فيما بين أجهزة إنفاذ القانون، واستخدام الأدوات القائمة، مثل اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية (اتفاقية بودابست). وبناء على ذلك، ينبغي للدول الأعضاء أن تواصل استخدام و/أو الانضمام إلى الصكوك القانونية المتعددة الأطراف القائمة المتعلقة بالجريمة السيبرانية، مثل اتفاقية بودابست التي يعتبرها العديد من الدول أنسب دليل لوضع ما يناسب من تشريعات محلية، موضوعية وإجرائية على السواء، بشأن الجريمة السيبرانية وتيسير التعاون الدولي على مكافحتها؛

(ج) بما أن الجريمة السيبرانية لها طابع عبر وطني والغالبية العظمى من الجرائم السيبرانية على الصعيد العالمي ترتكبها مجموعات منظمة، ينبغي للدول الأعضاء أيضاً زيادة استخدام اتفاقية الجريمة المنظمة عبر الوطنية من أجل تيسير تبادل المعلومات والأدلة في التحقيقات الجنائية بشأنها؛

(د) ينبغي للدول الأعضاء أن تروج للتعاون الدولي على مكافحة الجريمة السيبرانية وتشرع فيه بالاستفادة من الصكوك القائمة وبإبرام اتفاقات ثنائية تستند إلى مبدأ المعاملة بالمثل، وبتقديم الدعم، بالتعاون مع مكتب الأمم المتحدة، لعملية إنشاء الشبكات وتبادل المعلومات فيما بين السلطات القضائية وسلطات إنفاذ القوانين على نحو منتظم؛

(هـ) ينبغي أن تطور البلدان خبرات ضباط الشرطة في التحقيق في الجرائم السيبرانية من خلال تزويدهم بالتدريب الذي تقدمه العديد من البلدان وكذلك المكتب وغيره من الشركاء، والذي يرمي إلى تعزيز القدرات على كشف الجريمة السيبرانية والتحقيق فيها ومكافحتها. وينبغي لعملية بناء القدرات في هذا المجال أن تسعى بوجه خاص إلى تلبية احتياجات البلدان النامية، والتركيز على أوجه ضعف كل بلد من أجل ضمان تقديم مساعدة تقنية مصممة حسب الحاجة، والتشجيع على تبادل أحدث المعارف خدمة لمصلحة الجهات المستفيدة منها؛

(و) تشجَّع الدول على مواصلة منح المكتب الولايات والمساندة المالية اللازمة لكي يتمكن من تحقيق نتائج ملموسة في مشاريع بناء القدرات في هذا المجال؛

(ز) ينبغي للبلدان أن تخصص موارد لتطوير خبراتها في مجال التحقيق في الجرائم السيبرانية، ولإقامة الشراكات التي تستخدم آليات التعاون في الحصول على الأدلة الدامغة؛

(ح) ينبغي للدول الأعضاء أن تواصل جهودها الرامية إلى تطوير الوحدات والأجهزة والهياكل المتخصصة بمكافحة الجريمة السيبرانية داخل هيئات إنفاذ القانون وأجهزة النيابة العامة والجهاز القضائي، بحيث تحصل على الخبرات والمعدات اللازمة للتصدي للتحديات التي تفرضها الجريمة السيبرانية ولجمع الأدلة الإلكترونية في الإجراءات الجنائية وتبادل المعلومات عنها واستخدامها؛

(ط) بما أن تعطيل أسواق الجريمة السيبرانية يتطلب وضع استراتيجيات متوسطة وطويلة الأجل لإنفاذ القانون تتضمن التعاون مع الشركاء الدوليين، فإن تلك الاستراتيجيات ينبغي لها أن تكون استباقية، ويفضل أن تستهدف الجماعات المنظمة التي ترتكب الجرائم السيبرانية والتي قد يكون لديها أعضاء في بلدان متعددة؛

(ي) ينبغي للبلدان أن تواصل سن تشريعات موضوعية تتناول الأشكال الجديدة والمستجدة للجريمة السيبرانية تصوغها بلغة محايدة تكنولوجياً لضمان مواكبتها للتطورات المستقبلية في مجال تكنولوجيا المعلومات والاتصالات؛

(ك) لا بد للقوانين الإجرائية المحلية من أن تواكب التقدم التكنولوجي وأن تضمن تزويد أجهزة إنفاذ القانون بالموارد الكافية لمكافحة جرائم الإنترنت. وينبغي صوغ القوانين ذات الصلة على نحو يراعي المفاهيم التقنية المطبقة ويفي بالاحتياجات العملية للمحققين في الجرائم السيبرانية ويتسق مع ضمانات اتباع الأصول القانونية الواجبة ويحقق المصالح المتعلقة بالخصوصية ويضمن الحريات المدنية وحقوق الإنسان ويمتثل لمبدأي التناسب والولاية الاحتياطية ويكفل الإشراف القضائي. وينبغي للدول الأعضاء أيضاً أن تخصص الموارد اللازمة لسن التشريعات المحلية بحيث تأذن بما يلي:

'١' تقديم طلبات للتعجيل في حفظ البيانات الحاسوبية إلى الشخص المسيطر على البيانات – أي مقدمي خدمات الإنترنت والاتصالات – من أجل الحفاظ على سلامة البيانات وصونها لفترة زمنية محددة نظراً لاحتمال فقدان تلك البيانات؛

'٢' تفتيش وحجز البيانات المخزنة في الأجهزة الرقمية، التي كثيراً ما تكون أهم دليل لإثبات تهمة ارتكاب جريمة إلكترونية؛

'٣' إصدار أوامر لإبراز بيانات حاسوبية قد تتسم بدرجة أقل من حماية الخصوصية، مثل بيانات حركة المرور وبيانات المشتركين؛

'٤' الجمع الآني لبيانات حركة المرور والمحتوى في القضايا المناسبة؛

'٥' التعاون الدولي من جانب سلطات إنفاذ القانون المحلي؛

(ل) بما أنَّ التحقيقات في الجرائم السيبرانية تتطلب درجة من الإبداع والحنكة التقنية وتآزر جهود الشرطة والمدعين العامين، ينبغي للبلدان أن تشجع على التعاون الوثيق بين الشرطة والمدعين العامين في مرحلة مبكرة من التحقيقات من أجل جمع أدلة كافية لتوجيه الاتهام إلى الأشخاص المحددين؛

(م) ينبغي للمحققين أن يوجهوا موظفي إنفاذ القانون عند إجراء التحقيقات في قضايا الجرائم السيبرانية لضمان احترام معايير الأصول القانونية الواجبة؛

(ن) ينبغي لأجهزة إنفاذ القانون المحلية الاتصال بمقدمي خدمات الإنترنت المحليين وموظفي المجموعات الصناعية الخاصة الأخرى والتواصل معهم. فهذا التواصل يدعم التحقيقات التي تجريها أجهزة إنفاذ القانون عبر زيادة الثقة والتعاون فيما بين الجهات المعنية؛

(ص) ينبغي للبلدان اتباع نهوج مرنة بشأن أُسس الولاية القضائية المعمول بها في مجال الجريمة السيبرانية، بما في ذلك الاعتماد بدرجة أكبر على المكان الذي تُقدَّم فيه خدمات تكنولوجيا المعلومات والاتصالات بدل الاعتماد على مكان وجود البيانات؛

(ع) ينبغي للبلدان أن تستثمر في التوعية بالجريمة السيبرانية لدى عامة الجمهور والقطاع الخاص المعني من أجل معالجة مشكلة انخفاض معدلات الإبلاغ عن الجريمة السيبرانية مقارنة بأنواع أخرى من الجرائم؛

(ف) ينبغي للدول الأعضاء أن تعزز الشراكات بين القطاعين العام والخاص لمكافحة الجريمة السيبرانية، بوسائل منها سن التشريعات وإنشاء قنوات حوار لهذا الغرض، من أجل تعزيز التعاون بين سلطات إنفاذ القانون ومقدمي خدمات الاتصالات والأوساط الأكاديمية وذلك بهدف تعزيز المعارف وزيادة فعالية تدابير التصدي للجريمة السيبرانية؛

(ص) ينبغي للدول أن تتخذ التدابير الرامية إلى تشجيع مقدمي خدمات شبكة الإنترنت على القيام بدور في منع الجريمة السيبرانية ودعم أنشطة إنفاذ القانون والتحقيق، بوسائل منها

إدراج أحكام بشأن التزامات مقدمي الخدمات في تشريعاتها المحلية، وأن تحدد بوضوح نطاق هذه الالتزامات وحدودها من أجل حماية الحقوق والمصالح المشروعة لمقدمي الخدمات؛

(ح) ينبغي للدول أن تعزز أنشطة التحقيق وإنفاذ القانون المتصلة بالتعاون والتحريض على ارتكاب الجريمة السيبرانية والإعداد لها بغية التصدي بفعالية للسلسلة الكاملة للجريمة السيبرانية؛

(ط) ينبغي للدول أن تواصل تعزيز بناء القدرات وتعزيز قدرة السلطات القضائية وسلطات إنفاذ القوانين على التحقيق في الجرائم السيبرانية ومقاضاة مرتكبيها. وينبغي أن تركز أنشطة بناء القدرات على التحديات المتزايدة التي تطرحها الحوسبة السحابية والشبكة الخفية وغيرها من التكنولوجيات الناشئة الأخرى. وعلاوة على ذلك، تشجَّع الدول على تقديم المساعدة إلى البلدان النامية في مجال بناء القدرات.

باء- الأدلة الإلكترونية والعدالة الجنائية

١١- تماشياً مع خطة العمل، تتضمن هذه الفقرة تجميعاً للاقتراحات التي قدمتها الدول الأعضاء في الاجتماع في إطار البند ٣ من جدول الأعمال المعنون "الأدلة الإلكترونية والعدالة الجنائية". وهذه الاستنتاجات والتوصيات الأولية مقدمة من الدول الأعضاء، ولا يعني إدراجها أنَّ فريق الخبراء قد أقرَّها، كما أن ترتيب عرضها لا يعني ضمناً ترتيباً لدرجة أهميتها:

(أ) ينبغي للدول الأعضاء أن تطور وتنفذ الصلاحيات القانونية والقواعد المتعلقة بالولاية القضائية وغيرها من الأحكام الإجرائية لضمان التحقيق بفعالية على الصعيد الوطني في الجريمة السيبرانية والجرائم التي ييسرها استخدام التكنولوجيا، وتحقيق التعاون الفعال في القضايا عبر الوطنية، مع مراعاة الحاجة إلى تدابير فعَّالة في إطار إنفاذ القانون ومراعاة السيادة الوطنية وحماية الحق في الخصوصية وحقوق الإنسان الأخرى. وقد يشمل ذلك ما يلي:

'١' تعديل قواعد الإثبات لكفالة جمع الأدلة الإلكترونية وحفظها، والتأكد من صحتها، واستخدامها في الإجراءات الجنائية؛

'٢' اعتماد أحكام على الصعيدين الوطني والدولي لتتبع الاتصالات؛

'٣' اعتماد أحكام تنظم عمليات التفتيش المحلية والعابرة للحدود؛

'٤' اعتماد أحكام بشأن اعتراض الاتصالات المنقولة عبر الشبكات الحاسوبية والوسائط المماثلة؛

'٥' سن قوانين موضوعية وإجرائية محايدة تكنولوجياً لتمكين البلدان من التصدي للأشكال الجديدة والمستجدة من الجريمة السيبرانية؛

'٦' مواءمة التشريعات الوطنية؛

'٧' سن تشريعات جديدة أو تعزيز التشريعات القائمة لإتاحة الاعتراف بمقبولية الأدلة الإلكترونية وتحديد نطاقها؛

(ب) ينبغي للدول الأعضاء أن تعزز الجهود الرامية إلى بناء قدرات الموظفين المكلفين بإنفاذ القوانين، بمن في ذلك الموظفون الذين يعملون في أجهزة متخصصة لإنفاذ القانون والمدعون العامون والقضاة، لكي يكتسبوا كحد أدنى المعارف التقنية الأساسية المتعلقة بالأدلة الإلكترونية ويتمكنوا من الاستجابة بفعالية وسرعة لطلبات المساعدة في تتبع الاتصالات واتخاذ سائر التدابير اللازمة الأخرى للتحقيق في الجرائم السيبرانية؛

(ج) ينبغي للدول الأعضاء أن تعزز بناء القدرات من أجل تحسين التحقيقات، وزيادة فهم الجريمة السيبرانية والمعدات والتكنولوجيات المتاحة لمكافحتها، وتمكين المدعين العامين والقضاة والسلطات المركزية الوطنية من البت في هذه الجريمة ومقاضاة مرتكبيها على النحو الملائم؛

(د) ينبغي للدول الأعضاء أن تعزز الجهود الرامية إلى بناء قدرات السلطات المركزية المعنية بالتعاون الدولي بشأن الشروط والإجراءات المتعلقة بالمساعدة القانونية المتبادلة، بما في ذلك من خلال توفير التدريب على صوغ طلبات شاملة تتضمن معلومات كافية للحصول على الأدلة الإلكترونية؛

(هـ) ينبغي للدول الأعضاء أن تنظر في اتباع نهج "فريق الادعاء" الذي يجمع بين مهارات وموارد مختلف الأجهزة، ويضم المدعين العامين وموظفي التحقيق وأخصائيي التحليل الجنائي بهدف إجراء التحقيقات. ويسمح هذا النهج للمدعين العامين بالتعامل مع هذه الأدلة الإلكترونية وتقديمها؛

(و) لا ينبغي أن تتوقف مقبولية الأدلة الإلكترونية على المكان الذي جُمعت فيه الأدلة، سواء من داخل الولاية القضائية للبلد أو خارجها، شريطة ألاَّ يوجد ما يمس بموثوقية الأدلة وأن تكون هذه الأدلة قد جُمعت بشكل قانوني، على سبيل المثال، بموجب معاهدة للمساعدة القانونية المتبادلة، أو الاتفاق المتعدد الأطراف، أو بالتعاون مع البلد صاحب الولاية القضائية؛

(ز) ينبغي للدول الأعضاء أن تتخذ التدابير الضرورية لسن تشريع يضمن مقبولية الأدلة الإلكترونية، مع مراعاة أن مقبولية الأدلة، بما في ذلك الأدلة الإلكترونية، هي من المسائل التي ينبغي لكل بلد أن يتناولها وفقاً للقانون المحلي؛

(ح) ينبغي للدول الأعضاء أن تعزز التعاون الدولي فيما بين أجهزة إنفاذ القانون والمدعين العامين والسلطات القضائية ومقدمي خدمات الإنترنت من أجل سد الثغرة بين السرعة التي ينشط بها مرتكبو الجرائم السيبرانية وسرعة اتخاذ تدابير إنفاذ القانون. ولدى القيام بذلك، ينبغي للدول الأعضاء أن تستخدم الأطر القائمة، مثل الشبكات العاملة على مدار الساعة (24/7) والتعاون من خلال المنظمة الدولية للشرطة الجنائية (الإنتربول)، فضلاً عن معاهدات المساعدة القانونية المتبادلة، لتعزيز التعاون الدولي الذي ينطوي على أدلة إلكترونية. وينبغي للدول الأعضاء أن تواصل مواءمة وتبسيط العمليات المتعلقة بالمساعدة القانونية المتبادلة ووضع نموذج مشترك للتعجيل بهذه العمليات لجمع الأدلة الإلكترونية ونقلها في الوقت المناسب عبر الحدود؛

(ط) تشجَّع الدول الأعضاء على زيادة تبادل الخبرات والمعلومات، بما في ذلك التشريعات والإجراءات الوطنية، والممارسات الفُضلى بشأن التحقيق في الجرائم السيبرانية

عبر الحدود، والمعلومات عن الجماعات الإجرامية المنظمة والتقنيات والأساليب التي تستخدمها تلك الجماعات؛

(ي) ينبغي للدول الأعضاء أن تُنشئ شبكةً تضم جهات التنسيق بين أجهزة إنفاذ القانون والسلطات القضائية والمدعين العامين؛

(ك) ينبغي للدول الأعضاء أن تقيم إمكانية تكليف فريق الخبراء أو خبراء المكتب، بمساهمة من الدول الأعضاء، بإجراء تقييم سنوي لاتجاهات الجريمة السيبرانية والتهديدات الجديدة، وجعلها في متناول الجمهور؛

(ل) ينبغي للمكتب أن يدعم توسيع نطاق أنشطة التفتيش لاستبانة الأشكال والأنماط الجديدة للإجرام، وآثار الجريمة في المناطق الرئيسية والتطورات الحاصلة في بيئة الاتصالات السلكية واللاسلكية، بما في ذلك توسع نطاق إنترنت الأشياء، واعتماد تكنولوجيا سلسلة كتل البيانات والعملات المشفرة واستخدام الذكاء الاصطناعي بالاقتران مع التعلم الآلي؛

(م) ينبغي للمكتب، من خلال البرنامج العالمي المعني بالجريمة السيبرانية، أن يقوم، حسب الاقتضاء ورهناً بتوافر الموارد، بتعزيز ودعم وتنفيذ مشاريع التعاون التقني والمساعدة التقنية. و ستجمع هذه المشاريع بين الخبراء في منع الجريمة وأمن الحوا سيب والتشريعات والملاحقة القضائية وتقنيات التحقيق وما يتصل بها من مسائل، والدول التي تلتمس المعلومات أو المساعدة في تلك المجالات؛

(ن) ينبغي للمكتب أن يضع برنامجاً تعليمياً يركِّز على زيادة المعرفة وإذكاء الوعي بالتدابير الرامية إلى مكافحة الجريمة السيبرانية، لا سيما في مجال جمع الأدلة الإلكترونية، لفائدة السلطات القضائية وسلطات الادعاء في الدول الأعضاء؛

(ص) ينبغي للدول الأعضاء أن تواصل العمل على تعزيز التعاون في جمع الأدلة الإلكترونية، من خلال جملة تدابير منها:

'١' تبادل المعلومات بشأن التهديدات التي تطرحها الجريمة السيبرانية؛

'٢' تبادل المعلومات بشأن الجماعات الإجرامية السيبرانية، بما في ذلك التقنيات والأساليب التي تستخدمها؛

'٣' تشجيع التعاون والتنسيق المعزَّزين بين أجهزة إنفاذ القانون والمدعين العامين والسلطات القضائية؛

'٤' تبادل الاستراتيجيات والمبادرات الوطنية الرامية إلى التصدي للجريمة السيبرانية، بما في ذلك التشريعات والإجراءات الوطنية من أجل مقاضاة مرتكبي الجريمة السيبرانية؛

'٥' تبادل أفضل الممارسات والخبرات المتصلة بالتحقيق في الجرائم السيبرانية عبر الحدود؛

'٦' إنشاء شبكة مكوَّنة من جهات الاتصال تضم سلطات إنفاذ القانون والسلطات القضائية والمدعين العامين؛

'٧' مواءمة وتبسيط العمليات المتعلقة بالمساعدة القانونية المتبادلة ووضع نموذج مشترك للتعجيل بهذه العمليات من أجل جمع الأدلة الإلكترونية ونقلها في الوقت المناسب عبر الحدود؛

'٨' عقد حلقات عمل وحلقات دراسية من أجل تعزيز قدرة سلطات إنفاذ القانون والسلطات القضائية على صوغ طلبات جمع الأدلة في المسائل المتصلة بالجريمة السيبرانية، في إطار معاهدات المساعدة القانونية المتبادلة؛

'٩' وضع معايير للجوانب الإجرائية المتصلة بجمع الأدلة الرقمية ونقلها وتوحيدها؛

'١٠' وضع نهج مشترك لترتيبات تبادل المعلومات مع مقدمي الخدمات فيما يتعلق بالتحقيق في الجرائم السيبرانية وجمع الأدلة؛

'١١' العمل مع مقدمي الخدمات من خلال الشراكات بين القطاعين العام والخاص من أجل تحديد طرائق التعاون في مجال إنفاذ القانون والتحقيق في الجرائم السيبرانية وجمع الأدلة عليها؛

'١٢' وضع مبادئ توجيهية لمقدمي الخدمات لمساعدة أجهزة إنفاذ القانون في التحقيقات في الجرائم السيبرانية، بما في ذلك فيما يتعلق بصيغة الأدلة والمعلومات الرقمية ومدة حفظها؛

'١٣' تعزيز القدرات التقنية والقانونية لأجهزة إنفاذ القانون والقضاة والمدعين العامين من خلال برامج بناء القدرات وتنمية المهارات؛

'١٤' تقديم المساعدة إلى البلدان النامية في تعزيز قدراتها في مجال التحليل الجنائي السيبراني، بما في ذلك من خلال إنشاء مختبرات للتحليل الجنائي السيبراني؛

'١٥' عقد حلقات عمل وحلقات دراسية لزيادة الوعي بأفضل الممارسات في التصدي للجريمة السيبرانية؛

'١٦' إنشاء هيئة دولية للتحقق من أدوات التحليل الجنائي الرقمية واعتمادها وإعداد الأدلة الإرشادية وتعزيز قدرات أجهزة إنفاذ القانون والتدابير القضائية للتصدي للجريمة السيبرانية؛

(ع) ينبغي للبلدان أن تستثمر في بناء وتعزيز قدرات التحليل الجنائي الرقمي، بما في ذلك توفير التدريب والتأهيل الأمني، فضلاً عن نظم إدارة أمن المعلومات لدعم الملاحقات القضائية الناجحة في الجرائم السيبرانية عن طريق فحص الأجهزة الإلكترونية من أجل جمع الأدلة بطريقة موثوقة؛

(ف) ينبغي توفير تدريب متخصِّص بشأن الجريمة السيبرانية لموظفي الجهاز القضائي في النظم القانونية التي تستخدم النموذج القائم على التحقيق الذي يكون فيه موظفو الجهاز القضائي هم أيضاً المحقِّقون؛

(ص) بعض القضاة ليسوا على دراية بالأدلة الرقمية، ونتيجة لذلك، يخضع هذا النوع من الأدلة في كثير من الأحيان لمعايير أعلى فيما يتعلق بالتوثيق والقبول. ومع ذلك، ينبغي إيلاء الاعتبار إلى عدم وجود أسباب عملية لفرض معايير أعلى فيما يتعلق بسلامة الأدلة الرقمية مقارنة بالأدلة التقليدية. فاحتمال تحوير الأدلة الرقمية أو تلفيقها ليس أكبر من احتمال القيام بذلك مع الأدلة الأخرى. بل يمكن القول إنه من الصعب أن تُحوَّر أو تُلفَّق الأدلة الرقمية بسبب إمكانية استخدام خوارزميات رياضية مختلفة مثل "قيمة البعثرة" للتوثُّق من التحوير أو اثباته؛

(ق) ينبغي للدول أن تحسِّن فعالية التنسيق المشترك بين الهيئات المحلية وتعزيز أوجه التآزر فيما بينها، بما في ذلك تبادل المعلومات والاستخبارات الموثوق بها مع القطاع الخاص ومنظمات المجتمع المدني وسائر أصحاب المصلحة من أجل تيسير التعاون والتآزر الدوليين على نحو فعال؛

(ر) ينبغي للدول أن تسن تشريعات جديدة أو تعزز التشريعات القائمة بحيث تمكِّن من الاعتراف بمقبولية الأدلة الإلكترونية وتحديد نطاقها؛

(ش) لعل الدول تنظر في تصنيف البيانات التالية على أنها أدلة إلكترونية في تشريعاتها المحلية: بيانات حركة المرور مثل سجلات الوقائع، وبيانات المحتوى مثل الرسائل الإلكترونية، وبيانات المشتركين مثل معلومات تسجيل المستخدمين، وغيرها من البيانات المُخزَّنة والمُجهَّزة والمُرسَلة في شكل رقمي والتي تبرز أثناء ارتكاب الجريمة ويمكن عندئذ استخدامها لإثبات وقائع تلك الجريمة؛

(ت) تشجَّع الدول على تعزيز بناء القدرات على جمع الأدلة الإلكترونية، وإنشاء الأفرقة المهنية وتزويدها بالخبرة القانونية والتقنية على السواء، وتعزيز التعاون وتبادل الخبرات والتدريب في هذا الصدد. ويشجع المكتب على الاضطلاع بدور في هذه الجهود؛

(ث) تشجَّع الدول على أن تنشئ في تشريعاتها المحلية ذات الصلة أساليب جمع الأدلة الإلكترونية، مثل مصادرة وسائط التخزين الأصلية والحفاظ عليها، وجمع الأدلة في الموقع، وجمع الأدلة والتحقُّق منها عن بُعد. وتشجَّع الدول الأعضاء على تجميد الأدلة الإلكترونية لمنع الإضافة أو الحذف أو التعديل عن طريق تدابير مثل حساب تدقيق المجموع للتأكد من صحة الأدلة الإلكترونية، وغلق الحسابات المفتوحة على التطبيقات الشبكية، واعتماد آلية الحماية ضد الكتابة على الأدلة؛

(خ) تشجَّع الدول على وضع قواعد ومعايير تقنية فيما يتعلق بجمع الأدلة الإلكترونية؛

(ذ) ينبغي للدول أن تكفل أن تُجمع الأدلة الإلكترونية بالامتثال للإجراءات القانونية الواجبة؛

(ض) ينبغي للدول أن تضع في تشريعاتها المحلية قواعد لتقييم موثوقية الأدلة الإلكترونية وسلامتها ومشروعيتها وأهميتها، وأن تأخذ في الاعتبار الخصائص الفريدة للأدلة الإلكترونية عند تطبيق قواعد الأدلة الأصلية والإثبات بالسماع واستبعاد الأدلة غير القانونية؛

(ظ) عند جمع الأدلة الإلكترونية في الخارج، ينبغي للدول أن تحترم سيادة الدول التي تتواجد فيها البيانات، والامتثال للإجراءات القانونية الواجبة، واحترام الحقوق المشروعة للأشخاص والكيانات ذات الصلة. وينبغي للدول أيضاً أن تمتنع عن الاستخدام المنفرد لتدابير التحقيق التقني التدخلية أو الهدامة في هذا الصدد؛

(غ) تشجَّع الدول على التشاور مع الدول الأخرى من أجل مواصلة تحسين المساعدة القضائية الدولية والتعاون في مجال الإنفاذ عن طريق الاستفادة المثلى من الإجراءات والأساليب ذات الصلة، بغية تيسير التحقيق في الجرائم السيبرانية وجمع الأدلة الإلكترونية؛

(أأ) ينبغي للدول أن تنظر في اعتماد أحكام نموذجية دولية بشأن صلاحيات التحقيق المتعلقة بجمع الأدلة الإلكترونية واستكشاف إمكانية التفاوض على صك عالمي ملزم قانوناً بشأن مكافحة الجريمة السيبرانية في إطار الأمم المتحدة. ويمكن أن يتضمن هذا الصك أحكاماً مقبولةً عالمياً بشأن جمع الأدلة الإلكترونية عبر الحدود.

ثالثاً- ملخَّص المداولات

ألف- إنفاذ القانون والتحقيقات

١٢- نظر فريق الخبراء، أثناء جلساته الأولى والثانية والثالثة المعقودة يومي ٢٧ و٢٨ آذار/مارس ٢٠١٩، في البند ٢ من جدول الأعمال المعنون "إنفاذ القانون والتحقيقات".

١٣- وتولى تيسير المناقشة المناظرون التالية أسماؤهم: السيد شينكو وو (الصين)؛ والسيدة إيوانا ألباني (رومانيا)؛ والسيد مارتن غيرشانيك (الأرجنتين)؛ والسيد بيدرو فيرديلهو (البرتغال)؛ والسيد أنطون كورديكوف (الاتحاد الروسي).

١٤- وفي المناقشة التي تلت ذلك، نظر فريق الخبراء في أمثلة عن الأنشطة الإجرامية المضطلع بها في البيئة الرقمية والتي تشكل صعوبات كبيرة للممارسين والمحققين في مجال العدالة الجنائية عند فتح وإجراء التحقيقات وما يتبعها من ملاحقات قضائية. ومن الأمثلة التي ذُكرت الاحتيال بالاتصال الحاسوبي المباشر، واستخدام الإنترنت لأغراض إرهابية، واستخدام الشبكة الخفية في ارتكاب أنشطة غير مشروعة، والانتهاك والاستغلال الجنسيان للأطفال عن طريق إساءة استخدام تكنولوجيات المعلومات والاتصالات. وبالإضافة إلى ذلك، أُبلغ فريق الخبراء عن الترابط المفاهيمي بين الجريمة السيبرانية والأمن السيبراني والتباينات بينهما، فضلاً عن التوجهات والتحديات المتصلة بالجريمة السيبرانية، بما في ذلك هجمات فيروس الفدية؛ وأساليب الاستدراج الموجَّه المستخدمة في الاحتيال (التصيد الاحتيالي العام أو الموجه، والتصيد الإلكتروني الصوتي، وسرقة الهوية من خلال إرسال الروابط الإلكترونية الخبيثة)؛ واستخدام منصة Cobalt Strike لشن هجمات إلكترونية ضد النظم المصرفية؛ وإنترنت الأشياء؛ وتعدين العملات المُشفَّرة والهجمات الإلكترونية بغرض تعدين العملات المشفَّرة؛ واستنساخ البطاقات المصرفية وما يتصل بذلك من جرائم.

١٥- ونوقش مرة أخرى موضوع ما إذا كان صك قانوني عالمي شامل بشأن الجريمة السيبرانية ضرورياً أو ما إذا كان ينبغي للدول أن تركز بدلاً من ذلك على التنفيذ الفعال للصكوك القائمة، بما في ذلك اتفاقية بودابست. فدفع بعض المتكلمين بعدم ضرورة اعتماد صك قانوني شامل عالمي جديد بشأن الجريمة السيبرانية لأن اتفاقية بودابست توفر إطاراً ملائماً لوضع ما يناسب من تدابير محلية ودولية للتصدي للجريمة السيبرانية. وأشير إلى أن ٦٣ دولة طرفاً قد انضمت إلى اتفاقية بودابست، مما يدل على أنها مفتوحة لانضمام الدول غير الأعضاء في مجلس أوروبا. وقيل إن بعض الدول غير الأطراف في الاتفاقية تستلهم من الاتفاقية في مواءمة المعايير التشريعية المحلية الموضوعية والإجرائية على السواء. وأشير أيضاً إلى إن مفهوم "مواءمة المعايير الوطنية" لا يشمل فقط حالات التقارب والتعاريف المشتركة، بل أيضاً الحالات التي تكون فيها المعايير الدولية مفيدة في وضع الأنظمة الوطنية. وأُشير إلى التكامل بين اتفاقية بودابست والصكوك الإقليمية الأخرى، مثل اتفاقية الاتحاد الأفريقي المتعلقة بأمن الفضاء الإلكتروني وحماية البيانات الشخصية، المعتمدة في عام ٢٠١٤، والمدونة الدولية لقواعد السلوك في مجال أمن المعلومات الصادرة عن منظمة شنغهاي للتعاون.

١٦- وفي حين دفع متكلمون آخرون بأن صكاً قانونياً عالمياً جديداً بشأن الجريمة السيبرانية داخل إطار الأمم المتحدة هو أمرٌ ضروري للتصدي للتحديات التي يفرضها التطور السريع لتكنولوجيا الإنترنت والتي لا تغطيها الآليات القائمة التي، في كل الأحوال، لم تنضم إليها جميع الدول في العالم. وشُدِّد على أن ذلك الصك يُتوخى وضعه كجزء من عملية تقودها الأمم المتحدة ويمكن في إطارها وضع زمام الأمور في أيدي الدول الأعضاء التي تتولى المسؤولية عن تبسيط الجهود المبذولة للتصدي للجريمة السيبرانية، بالاستفادة من الصكوك القائمة مثل اتفاقية بودابست واتفاقية الاتحاد الأفريقي السالفة الذكر أو بالاستناد إليها. وفي هذا السياق، أشير إلى قرار الجمعية العامة ١٨٧/٧٣، المؤرخ ١٧ كانون الأول/ديسمبر ٢٠١٨، بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، وإلى الولاية الواردة فيه التي يلتمس الأمين العام بموجبها آراء الدول الأعضاء بشأن التحديات التي تواجهها في مجال مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، ويقدم تقريراً استناداً إلى تلك الآراء لتنظر الجمعية العامة فيه في دورتها الرابعة والسبعين. وأعرب أيضاً عن رأي مفاده أن اتفاقية بودابست ليست شفافة أو شاملة بما يكفي وأنها لا تعالج شواغل جميع الدول الأعضاء، وأنها أنشأت عمليات معقدة وغير شفافة من أجل تعديل نصها، مما قد يكون غير مناسب بالنظر إلى الطبيعة المتطورة باستمرار للجرائم السيبرانية.

١٧- وأشير إلى عملية التفاوض الجارية من أجل اعتماد بروتوكول إضافي ثانٍ لاتفاقية بودابست بهدف توفير قواعد واضحة وإجراءات أكثر فعالية بشأن بعض أو جميع المسائل التالية: 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.

١٨- وشُدِّد أيضاً على أن اتفاقية الجريمة المنظمة يمكن أن تُستخدم كأداة مفيدة للتصدي للتحديات التي تفرضها الجريمة السيبرانية ولا سيما بالنظر إلى الطابع عبر الوطني لتلك التحديات. واقتُرح النظر في التفاوض على بروتوكول إضافي لاتفاقية الجريمة المنظمة يتناول الجريمة السيبرانية على وجه الخصوص.

١٩- وأطلع أعضاءُ الوفود والمناظرون فريقَ الخبراء على الجهود الوطنية الناجحة الرامية إلى تنفيذ تدابير قانونية وإجرائية للتصدي للجريمة الإلكترونية. ورأى بعض المتكلمين أن اتفاقية بودابست وما يصاحبها من مشاريع لبناء القدرات هي اللبنات الأساسية في هذا المجال. ونُظر بتعمق في مسألة الإصلاحات التشريعية على الصعيد الوطني، بما في ذلك نطاق تلك الإصلاحات. ووُجِّه الانتباه إلى الحاجة إلى الاضطلاع بعمليات شاملة وتشاركية لضمان مراعاة آراء مختلف أصحاب المصلحة. وأشير إلى ضرورة ضمان اليقين والوضوح القانونيين على أساس مبدأ "لا جريمة ولا عقوبة إلا بنص"، وضرورة استخدام صيغة "محايدة تكنولوجياً" في التشريعات الجديدة بحيث تظل مواكبة للتطورات السريعة في ميدان تكنولوجيات المعلومات والاتصالات.

٢٠- ودارت مناقشة أيضاً حول التحديات الناشئة عن النزاعات بشأن الولاية القضائية المعنية بالإنفاذ، وخصوصاً، على سبيل المثال، في الحالات التي قد يكون فيها لمقدم الخدمة مقرٌّ في إحدى الولايات القضائية، ويكون المتحكم في البيانات موجوداً في بلد آخر أو تكون البيانات مخزَّنة في ولاية قضائية أخرى أو في ولايات قضائية متعددة. وأُشير إلى أنَّ ظهور الحوسبة السحابية يثير تحديات عملية وقانونية إضافية أمام التحقيقات الجنائية. وأُشير أيضاً إلى أنَّ اتباع نهوج مرنة بشأن أُسس الولاية القضائية المعمول بها في مجال الجريمة السيبرانية قد يكون مفيداً، مثل نهج الاعتماد بدرجة أكبر على المكان الذي تُقدَّم فيه خدمات تكنولوجيا المعلومات والاتصالات بدل الاعتماد على مكان وجود البيانات.

٢١- وشدَّد فريق الخبراء أيضاً على الحاجة إلى وجود صلاحيات إجرائية مناسبة للحصول على الأدلة الإلكترونية، بما في ذلك البيانات والبيانات الوصفية المتعلقة بالجريمة السيبرانية وكذا بأشكال أخرى من الجريمة. وقد تشمل هذه الأدلة الإلكترونية معلومات عن المشتركين، أو بيانات المحتوى، أو بيانات حركة المرور. وأُشير إلى أنَّ المحققين يصادفون تطورات تكنولوجية جديدة، مثل البرامجيات المُخفية للهوية والتشفير العالي الدرجة والعملات الافتراضية، أثناء تحقيقهم في الجرائم التي تنطوي على أدلة إلكترونية، وبالنظر إلى ذلك، قد يتعين عليهم اعتماد استراتيجيات جديدة والنظر في كيفية استخدام أساليب التحري الخاصة والتحليل الجنائي الرقمي عن بُعد لجمع تلك الأدلة الإلكترونية، مع ضمان مقبولية الأدلة واستخدامها في المحاكم. وأُعطيت الأولوية لتعزيز الدور التنسيقي الذي تضطلع به السلطات الوطنية المختصة مثل المحامين أو مكاتب المدعين العامين المتخصصين.

٢٢- وركَّزت المناقشة أيضاً على كيفية تحقيق التوازن بين الحاجة إلى تدابير فعَّالة في إطار إنفاذ القانون للتصدي للجريمة السيبرانية وحماية حقوق الإنسان الأساسية، وخاصة الحق في الخصوصية. وقيل إنَّ القواعد المتعلقة بالاحتفاظ بالبيانات قد تمثل نهجاً عمليًّا لضمان قدرة مقدِّمي خدمات الاتصالات على الاضطلاع بدور أكبر في التصدي للجريمة السيبرانية من خلال تعزيز التعاون مع

أجهزة إنفاذ القانون، شريطة أن يراعي تنفيذ هذه القوانين الضمانات الإجرائية وإجراءات حماية الخصوصية الواجبة. وأُشير إلى تقرير مفوضية الأمم المتحدة لحقوق الإنسان عن "الحق في الخصوصية في العصر الرقمي" (A/HRC/27/37)، الذي قُدِّم إلى مجلس حقوق الإنسان عملاً بقرار الجمعية العامة ١٦٧/٦٨.

٢٣- وأكَّد فريق الخبراء مجدداً أهمية التعاون الدولي في التحقيق في الجرائم السيبرانية وملاحقة مرتكبيها قضائيًّا عبر الحدود. وأشار بعض المتكلمين إلى أن عدد طلبات المساعدة القانونية المتبادلة للحصول على أدلة إثبات إلكترونية وحفظها يتزايد بسرعة، وأنَّ طرائق التعاون التقليدية، وبوجه خاص الإجراءات المتعلقة بتبادل المساعدة القانونية التي رأى البعض أنها تستغرق وقتاً طويلاً، لا تسهل الوصول السريع إلى البيانات. وأشار متكلمون آخرون إلى أن المساعدة القانونية المتبادلة لا تزال أداة بالغة الأهمية لتبادل البيانات عبر الحدود. وأشار بعض المتكلمين أيضاً إلى أن بناء القدرات والتدريب بشأن الاحتياجات المتعلقة بالمساعدة القانونية المتبادلة، بما في ذلك صوغ طلبات شاملة تتضمن معلومات كافية للحصول على الأدلة الإلكترونية، تمثل عناصر رئيسية لكفالة الوصول في الوقت المناسب إلى البيانات. وبالإضافة إلى ذلك، أوصت بعض البلدان باستخدام الشبكات العاملة على مدار الساعة (24/7) لطلب حفظ البيانات بشكل فوري بسبب الطبيعة المتقلبة التي تتَّسم بها هذه الأدلة التي يمكن نقلها أو حذفها بنقرة زر في لوحة مفاتيح حاسوب.

٢٤- وأُشير إلى ممارسات مختلفة بوصفها أمثلة على الكيفية التي يمكن بها تعزيز التعاون الدولي فيما يتعلق بالأدلة الإلكترونية، ولا سيما على المستوى العملياتي. وشملت تلك الأمثلة إرسال طلبات المساعدة القانونية المتبادلة مباشرةً إلى السلطات المختصة للدول المتعاونة؛ والإكثار من استخدام أدوات التعاون الدولي المصمَّمة خصيصاً للحفاظ على سلامة الأدلة الإلكترونية مثل التعجيل في حفظ البيانات الحاسوبية، والتحقيقات المشتركة، واستخدام الوسائل الإلكترونية في إرسال طلبات المساعدة القانونية المتبادلة، مع الإشارة تحديداً إلى الفائدة المحتملة التي يمكن أن تُستمد في هذا الصدد من مبادرة الإنتربول بشأن إرسال طلبات المساعدة القانونية المتبادلة عن طريق مراسلات إلكترونية مؤمَّنة، وتبادل المعلومات بين جهات الاتصال التابعة لشبكة الاتصالات العاملة على مدار الساعة (24/7)، والإكثار من استخدام سبل التعاون المباشر بين أجهزة الشرطة، بما في ذلك عن طريق المساعدة المقدَّمة من الإنتربول، لأغراض جمع المعلومات الاستخبارية. وأشير أيضاً إلى المركز الأوروبي للجريمة السيبرانية، الذي أنشأته وكالة الاتحاد الأوروبي للتعاون في مجال إنفاذ القانون في عام ٢٠١٣ بهدف تعزيز تدابير إنفاذ القانون للتصدي للجريمة السيبرانية داخل الاتحاد الأوروبي.

٢٥- وتطرق فريق الخبراء أيضاً إلى مسألة الوصول إلى البيانات عبر الحدود. وبوجه عام، لوحظ أن الممارسات والإجراءات التي تستخدمها الدول والشروط والتدابير الاحترازية المتصلة بتلك الممارسات والإجراءات متباينة تبايناً كبيراً. وأُعرب عن القلق بشأن المشاكل القانونية المحتملة الناجمة عن بعض الممارسات المتعلقة بالوصول إلى البيانات عبر الحدود. وعلاوة على ذلك، جرى التأكيد على الحقوق الإجرائية للمشتبه فيهم، واعتبارات الخصوصية، وحماية البيانات الشخصية، ومشروعية الوصول إلى البيانات المخزنة في خوادم موجودة في ولايات قضائية أخرى، واحترام مبدأ السيادة الوطنية.

٢٦- وشدَّد فريق الخبراء على أهمية بناء القدرات المستدامة من أجل تعزيز الفعالية والمهارات لدى جميع السلطات المختصة على الصعيد التنفيذي من أجل التصدي للتحديات التي تطرحها الجريمة السيبرانية. وفي هذا السياق، أشار متكلمون إلى فائدة تبادل الممارسات الجيدة والخبرات فيما بين الممارسين، ليس داخل كل دولة فحسب، بل أيضاً فيما بين الدول. وأشار بعض المتكلمين إلى تعزيز التدريب وبناء القدرات، بالتوازي مع تطوير الهياكل أو الوحدات المتخصصة في الجرائم السيبرانية داخل دوائر النيابة العامة وسلطات إنفاذ القانون. وفي هذا الصدد، جرى التشديد على أن استخدام الأدلة الإلكترونية قد بات شائعاً بصورة متزايدة في التحقيق في الأشكال الأخرى للجريمة، ولذلك من الضروري وضع هياكل متخصصة تقدم الخبرة والمعارف والمهارات التنفيذية للتحقيق في تلك الجرائم.

٢٧- وناقش فريق الخبراء كذلك أهمية تعزيز وتوطيد التعاون بين السلطات الوطنية والقطاع الخاص، وبخاصة مقدمي خدمات الاتصالات ومقدمي خدمات الإنترنت، من أجل تعزيز الحفاظ على البيانات والوصول إليها. ولئن أُبرزت الأهمية المتزايدة لهذا التعاون على الصعيد المحلي، ولا سيما في القضايا المستعجلة التي تنطوي على جرائم خطيرة، فقد سُلِّم أيضاً بالحاجة إلى بذل مزيد من الجهود لكفالة مستوى مماثل من التعاون في القضايا العابرة للحدود الوطنية. وفي هذا الصدد، أشير إلى احتمال حدوث تضارب في المتطلبات بالنسبة لمقدمي خدمات الاتصالات ومقدمي خدمات الإنترنت، ويتمثل ذلك تحديداً في كيفية الموازنة بين تجاوبهم مع الطلبات المقدمة والمتطلبات القانونية للدول المعنية.

٢٨- وأبلغ العديد من المتكلمين عن التدابير الوطنية المتخذة من أجل وضع وتنفيذ استراتيجيات وسياسات بشأن الجريمة السيبرانية؛ وسن تشريعات بشأن الجريمة السيبرانية و/أو تطوير التشريعات القائمة بشأنها؛ واستخدام أدوات استقصائية جديدة لجمع الأدلة الإلكترونية والتثبت من صحتها لأغراض الاستدلال في الإجراءات الجنائية، مع مراعاة ضمانات حقوق الإنسان؛ وتطبيق ترتيبات مؤسسية ترمي إلى ضمان المزيد من الكفاءة في استخدام الموارد في التصدي للجريمة السيبرانية؛ وتعزيز التعاون الدولي على مكافحة الجريمة السيبرانية. وأشار أحد المتكلمين إلى أن الاختلافات القائمة بين الأمن السيبراني والجريمة السيبرانية تمثل الاعتبارات الرئيسية التي ينبغي مراعاتها عند هيكلة تدابير التصدي الوطنية وتحديد الاختصاصات المؤسسية بشأن تلك المسائل.

٢٩- وأعرب العديد من المتكلمين عن تأييدهم لعمل فريق الخبراء باعتباره المنتدى العالمي الشامل الأوحد والأنسب لتيسير النقاش وتبادل الآراء بين الدول الأعضاء حول التشريعات الوطنية والممارسات الفضلى والمساعدة التقنية والتعاون الدولي بغية تدارس الخيارات القائمة لتدعيم التدابير القانونية وغيرها من التدابير المتخذة على الصعيدين الدولي والوطني للتصدي للجريمة السيبرانية. وأُشير أيضاً إلى القيمة التي تضيفها اللجنة في هذا الشأن. وذُكر أن فريق الخبراء لديه ولاية فريدة تجعل منه منبراً للمناقشات بشأن هذا الموضوع؛ على أن هذا لا ينبغي أن يستبعد بالضرورة المبادرات الأخرى الرامية إلى إنشاء نظام حوكمة عالمي شامل لمكافحة الجريمة السيبرانية.

٣٠- وأُعرب عن التأييد لما يضطلع به المكتب من أعمال في مجال المساعدة التقنية وبناء القدرات بهدف وضع تدابير متسقة للتصدي للجريمة السيبرانية.

٣١- وعلاوة على ذلك، أعرب بعض المتكلمين أيضاً عن تقديرهم لصدور الدليل العملي لطلب الأدلة الإلكترونية عبر الحدود، الذي تشارك في إعداده وإصداره المكتب والمديرية التنفيذية للجنة مكافحة الإرهاب والرابطة الدولية للمدعين العامين، والذي أتيح للدول الأعضاء ومسؤولي العدالة الجنائية لديها من خلال بوابة الموارد الإلكترونية والقوانين المتعلقة بالجريمة التابعة للمكتب. وبما أن الدليل قد صدر في إطار من التعاون مع الدول الأعضاء ومنظمات دولية وإقليمية و شركات تقديم خدمات الاتصالات، مثل فيس بوك وغوغل وميكرو سوفت وأُوبر، فهو يتضمن معلومات عن الخطوات التي يمكن اتباعها على الصعيد الوطني لجمع الأدلة الإلكترونية وحفظها وتبادلها في ضوء الهدف العام الرامي إلى ضمان كفاءة ممارسات تقديم المساعدة القانونية المتبادلة.

باء- الأدلة الإلكترونية والعدالة الجنائية

٣٢- نظر فريق الخبراء أثناء جلستيه الرابعة والخامسة المعقودتين في ٢٨ و٢٩ آذار/مارس ٢٠١٩، في البند ٣ من جدول الأعمال، المعنون "الأدلة الإلكترونية والعدالة الجنائية".

٣٣- وتولى تيسير المناقشة المناظرون التالية أسماؤهم: السيد شاوفاوي تسي (الصين)؛ والسيد ماركو كينَّبو (إستونيا)؛ والسيدة كاميلا بوش (شيلي)؛ والسيد جيوسبي كوراسانيتي (إيطاليا)؛ والسيد فاديم سميخنوف (الاتحاد الروسي)؛ والسيدة بريوني ديلي ويتوورث (أستراليا).

٣٤- وخلال المناقشة التي أعقبت ذلك، أُشير إلى الدور المزدوج للأدلة الإلكترونية. فمن ناحية، أُقر بأن استخدام التكنولوجيا والبنية التحتية الرقمية أتاحت مزيداً من الفرص لمرتكبي الجرائم الخطيرة والمنظمة المعتمدة على الفضاء الإلكتروني والتي يتيح الفضاء الإلكتروني ارتكابها لتوسيع نطاق أنشطتهم غير المشروعة واستهداف المزيد من الضحايا ومضاعفة أرباحهم. ومن ناحية أخرى، جرى التأكيد أيضاً على أن الأدلة الإلكترونية أصبحت متزايدة الأهمية في الكشف والتحقيق والملاحقة القضائية لجميع أنواع الجريمة.

٣٥- وأشار العديد من المتكلمين إلى تزايد أهمية الأدلة الإلكترونية في الإجراءات الجنائية، ووصفوا النهوج الوطنية المختلفة لتحديد نطاق تلك الأدلة. وأشار بعض المتكلمين إلى عدم وجود تعريف متفق عليه عموماً للأدلة الإلكترونية على الصعيد الدولي، في حين أن وضع قواعد بشأن هذه الأدلة ومقبوليتها على الصعيد الوطني هو من اختصاص الدول الأعضاء. ولفت المتكلمون الانتباه إلى الحاجة إلى تشريعات إجرائية تمنح سلطات إنفاذ القانون المختصة صلاحية جمع الأدلة الإلكترونية بشكل فعال، مع مراعاة السرية والخصوصية وحقوق الإنسان ومراعاة الأصول القانونية والضمانات القانونية الأخرى. وأشير إلى أن صلاحيات التحقيق التقليدية يمكن أن تشمل الصلاحيات الإجرائية وصلاحيات التحقيق العامة كما تشمل تقنيات تحقيق رقمية محددة.

٣٦- واتُفق على أن من الخطوات الرئيسية في الجريمة السيبرانية والتحقيقات الرقمية هي الحفاظ على سلامة الأدلة الإلكترونية وضمان صحتها ومقبوليتها كدليل في الإجراءات الجنائية ذات الصلة. وفي هذا السياق، أشير إلى المعايير والإجراءات والمتطلبات الوطنية للتعامل مع الأدلة

الإلكترونية. وأبرز فريق الخبراء مجدداً ضرورة بناء القدرات والمعارف التقنية للسلطات المختصة للتعامل بفعالية وكفاءة مع التحديات ذات الصلة.

٣٧- ونظر فريق الخبراء في العوامل المهمة عند تقييم مقبولية الأدلة الإلكترونية. وشُدِّد على أهمية الامتثال لمبدأ التناسب عند استخدام أساليب التحري الخاصة في التحقيقات في الجرائم السيبرانية، بما في ذلك استخدام العملاء السريين وتحقيقات التحليل الجنائي عن بُعد، ولا سيما بشأن الشبكة الخفية. وأشير إلى أن هذا المبدأ قد اختُبر في العديد من النظم القانونية المحلية من جانب السلطة القضائية التي تُشرف على التحقيقات ومن جانب المحكمة، حسب الاقتضاء؛ ويمكن تحديد الأهمية على أساس مدى خطورة الجرم المعني، أو عدد الأشخاص الذين انتُهكت حقوقهم في الخصوصية بسبب استخدام أساليب التحري الخاصة؛ وأنواع البيانات الحاسوبية المعنية؛ وما إذا كانت ثمة تدابير بديلة أقل تقييداً متاحة؛ وما إذا كان ثمة قدر من العدالة الإجرائية في عملية صنع القرارات؛ وما إذا كان الأشخاص المتضررون قد حصلوا على فرص كافية للانتصاف القانوني.

٣٨- ووُجِّه الانتباه إلى ظهور تشفير مدمج في البرمجيات والتطبيقات، مما يجعل الوصول إلى البيانات والأدلة الإلكترونية صعباً ويستغرق وقتاً طويلاً في غياب مفاتيح فك التشفير المناسبة. وقُدِّمت اقتراحات عملية بشأن كيفية التغلب على هذه المسألة، شملت التعاون مع البلدان الأخرى التي قد تكون لها القدرة على الوصول إلى المعلومات المشفرة، واستخدام المركز الأوروبي المعني بالجرائم السيبرانية والتعاون مع الأوساط الصناعية المعنية التي يمكن أن تضع آليات تتيح الحصول على البيانات المشفرة في الوقت المناسب.

٣٩- وأُشير أيضاً إلى استخدام الذكاء الاصطناعي في التحقيقات، مع الإشارة بصفة خاصة إلى نظام التعرف على سمات الوجه وانتهاكات حقوق التأليف والنشر. وقيل، بوجه عام، إن الذكاء الاصطناعي قد يوفر حلولاً للتمكين من الاستخدام الأكثر فعالية للوقت والموارد عند دراسة كميات كبيرة من البيانات الهامة لدى البحث عن الأدلة الإلكترونية.

٤٠- ونوقشت مسألة معلومات المشتركين بوصفها أكثر البيانات التي تسعى سلطات العدالة الجنائية للحصول عليها لدى إجراء التحقيقات الجنائية في الجرائم السيبرانية وغيرها من القضايا التي تنطوي على أدلة إلكترونية. وفي هذا الصدد، أشار العديد من المتكلمين إلى التحديات المتعلقة بمعلومات المشتركين المتصلة بعنوان شبكي محدد استُخدم لارتكاب جريمة جنائية. ولوحظ أنه على الرغم من أن العناوين الشبكية الثابتة هي عناوين مستقرة وتُسنَد لمشترك معيَّن طيلة فترة ترتيبات الخدمات، وعلى الرغم من أن مقدمي الخدمات يمكنهم البحث عن هذه المعلومات في قاعدة بيانات المشتركين، إلاَّ أن مقدمي الخدمات يمكنهم إسناد عنوان شبكي واحد لعدة مشتركين. ولذلك فمن الضروري تحديد المشترك الذي أُسند إليه عنوان شبكي في وقت معين. وأُشير أيضاً إلى أن هذا التخصيص الدينامي للعناوين الشبكية يُعزى إلى العدد المحدود للعناوين الشبكية في الصيغة الرابعة لبروتوكول الإنترنت. ويمكن حل هذه المشكلة لدى استكمال الانتقال إلى الصيغة السادسة لبروتوكول الإنترنت أو عندما تبلغ عملية الانتقال مرحلةً أكثر تقدُّماً.

٤١- ونوقشت أيضاً مسألة التمييز بين أنواع البيانات المطلوبة وأثرها على فعالية آليات التعاون الدولي في الوقت المناسب للحصول على الأدلة الإلكترونية. وبحثت بعض الحلول منها تعزيز التعاون في مجال إنفاذ القانون، ومواصلة الحوار المتعدد الأطراف بشأن الوصول إلى البيانات الحاسوبية عبر الحدود الوطنية، وإنشاء نظام مستقل للحصول على معلومات عن المشتركين، على النحو المحدد في الفقرة ٣ من المادة ١٨ من اتفاقية بودابست.

٤٢- وأشار العديد من المتكلمين إلى التحديات التي تطرحها العملات المشفرة في التحقيقات في الجرائم السيبرانية. وأُبلغ فريق الخبراء عن دورة تدريب المدربين على التحقيق في قضايا العملة المشفرة التي نظمها المكتب. وتمثل الهدف من تلك الدورة التدريبية في تحسين قدرة موظفي إنفاذ القانون والمُحللين والمدعين العامين والقضاة فيما يتصل بالعملات المشفرة، بما في ذلك قدرتهم على تعقُّب العملات الافتراضية (البت كوين) في التحقيقات المالية، وتحديد الموارد المعلوماتية، والتعاون بشأن الدعاوى القضائية الدولية.

٤٣- وناقش بعض المتكلمين، في إطار البند ٣، المسائل المتعلقة بالولاية القضائية. وأشير بوجه خاص إلى التطورات الأخيرة في الاجتهاد القضائي الوطني فيما يتعلق بتفسير مبدأ الإقليمية في الحالات التي تكون فيها البيانات الحاسوبية المخزنة في خوادم سحابية في ولايات قضائية أخرى.

٤٤- واتفق المتكلمون على أن التعاون الدولي أمر بالغ الأهمية من أجل جمع وتبادل الأدلة الإلكترونية في سياق التحقيقات عبر الحدود. وشدِّد على أنه ينبغي للدول أن تستفيد استفادةً كاملةً من اتفاقية الجريمة المنظمة المتعددة الأطراف والمعاهدات والترتيبات الإقليمية الثنائية ذات الصلة بشأن الجريمة السيبرانية من أجل تعزيز التعاون الدولي بشأن المساعدة القضائية وإنفاذ القانون في القضايا ذات الصلة بهذه المسألة، مع احترام مبادئ السيادة والمساواة والمعاملة بالمثل. وسُلِّط الضوء بوجه خاص على أهمية تعزيز التواصل من أجل تبادل الخبرات والتجارب ابتغاء التصدي للتحديات التي تطرحها المتطلبات الوطنية المتباينة بشأن مقبولية الأدلة وسلامتها وصحتها.

٤٥- 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. وأُشير إلى أن بناء القدرات يمثل أمراً أساسياً، وبخاصة للبلدان النامية، من أجل تطوير الموارد البشرية والهياكل الأساسية والمعدات، وكذلك من أجل سد الفجوة الرقمية مع البلدان المتقدمة. واتُّفق إجمالاً على أنَّ عملية بناء قدرات موظفي أجهزة إنفاذ القانون والعدالة الجنائية ستكون عمليةً مستمرةً ومتواصلةً، نظراً للتطور السريع للتكنولوجيا والابتكارات الإجرامية. ومن ثم، فقد أشارت الأغلبية الساحقة من المتكلمين إلى أن المساعدة التقنية والتعاون شرطان مسبقان هامان لتعزيز القدرات المحلية والتمكين من تبادل الممارسات والتجارب الجيدة في مجال التحقيق وتعميم التقنيات الجديدة.

٤٦- وفي هذا الصدد، أشار عدد من المتكلمين إلى التحديات التي تطرحها الموارد المحدودة في مجال التحليل الجنائي، والافتقار إلى أدوات التحليل الجنائي ومعداته التي غالباً ما تكون باهظة الثمن،

والكم الهائل للبيانات المجمعة لأغراض التحليل الجنائي. وأُبلغ كذلك عن التحديات المواجَهة في تعيين موظفين مهرة بما فيه الكفاية.

جيم- مسائل أخرى

٤٧- نظر فريق الخبراء أثناء جلسته السادسة المعقودة في ٢٩ آذار/مارس ٢٠١٩، في البند ٤ من جدول الأعمال، المعنون "مسائل أخرى".

٤٨- وطلب أحد المتكلمين معلومات عن التقرير المتعلق بمكافحة استخدام تكنولوجيات المعلومات والاتصالات، الذي سيقدم إلى الجمعية العامة في دورتها الرابعة والسبعين، عملاً بقرار الجمعية العامة ١٨٧/٧٣. وردًّا على ذلك، أشار ممثل عن الأمانة إلى الولاية الواردة في القرار، وأكَّد على أن الأمانة قد أرسلت مذكرات شفوية إلى الدول الأعضاء في ١٣ شباط/فبراير ٢٠١٩ تدعوها فيها إلى تقديم معلومات عن التحديات التي تواجهها في مجال مكافحة استخدام تكنولوجيات المعلومات والاتصالات لأغراض إجرامية، وتبلغها بأن تلك المعلومات ستُستخدم لإعداد التقرير. وحُدِّد الموعد النهائي لتقديم التعليقات الوطنية في يوم الجمعة ١٢ نيسان/أبريل ٢٠١٩. وبعد انقضاء ذلك الموعد النهائي، تُجمِّع الأمانة التعليقات الواردة بغية وضع الصيغة النهائية للتقرير في أيار/مايو ٢٠١٩.

رابعاً- تنظيم الاجتماع

ألف- افتتاح الاجتماع

٤٩- افتتح الاجتماع نائب رئيس فريق الخبراء، أندريه ريبل (البرازيل)، بصفته رئيساً للاجتماع الخامس لفريق الخبراء.

باء- الكلمات

٥٠- تكلَّم خبراء من الدول الأعضاء التالية: الاتحاد الروسي، الأرجنتين، الأردن، أرمينيا، إسبانيا، أستراليا، إستونيا، إكوادور، ألمانيا، الإمارات العربية المتحدة، إندونيسيا، إيران (جمهورية- الإسلامية)، إيطاليا، باراغواي، البرازيل،، بوركينا فاسو، بيرو، بيلاروس، تايلند، الجزائر، الجمهورية الدومينيكية، جنوب أفريقيا، جورجيا، سلوفاكيا، سري لانكا، شيلي، صربيا، الصين، فرنسا، الفلبين، فييت نام، كندا، كوستاريكا، كولومبيا، الكويت، ماليزيا، المغرب، المكسيك، المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية، موريتانيا، النرويج، النيجر، نيجيريا، الهند، هولندا، الولايات المتحدة الأمريكية، اليابان.

٥١- وتكلم أيضاً ممثلا المنظمتين الحكوميتين الدوليتين التاليتين: مجلس أوروبا والاتحاد الأوروبي.

جيم- إقرار جدول الأعمال والمسائل التنظيمية الأخرى

٥٢- أقرَّ فريق الخبراء في جلسته الأولى، المعقودة في ٢٧ آذار/مارس ٢٠١٩، جدول الأعمال المؤقَّت التالي:

١- المسائل التنظيمية:

(أ) افتتاح الاجتماع؛

(ب) إقرار جدول الأعمال.

٢- إنفاذ القانون والتحقيقات.

٣- الأدلة الإلكترونية والعدالة الجنائية.

٤- مسائل أخرى.

٥- اعتماد التقرير.

دال- الحضور

٥٣- حضر الاجتماع ممثلون عن ١٠٥ دول أعضاء، ومعهد تابع لشبكة برنامج الأمم المتحدة لمنع الجريمة والعدالة الجنائية، ومكتب المخدِّرات والجريمة، ومنظمات حكومية دولية والقطاع الخاص.

٥٤- وترد في الوثيقة UNODC/CCPCJ/EG.4/2019/INF/1/Rev.1 قائمة بأسماء المشاركين.

هاء- الوثائق

٥٥- إضافةً إلى مشروع الدراسة الشاملة لمشكلة الجريمة السيبرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدِّي لها، عُرضت على فريق الخبراء الوثيقتان التاليتان:

(أ) جدول الأعمال المؤقَّت المشروح (UNODC/CCPCJ/EG.4/2019/1)؛

(ب) اقتراح الرئيس بشأن خطة عمل فريق الخبراء للفترة ٢٠١٨-٢٠٢١، استناداً إلى قرار لجنة منع الجريمة والعدالة الجنائية ٤/٢٦ (UNODC/CCPCJ/EG.4/2018/CRP.1).

خامساً- اعتماد التقرير

٥٦- اعتمد فريق الخبراء تقريره (UNODC/CCPCJ/EG.4/2019/2) في جلسته السادسة المعقودة في ٢٩ آذار/مارس ٢٠١٩.