UNODC/CCPCJ/EG.4/2019/L.1/Add.1

Distr.: Limited
27 March 2019
Arabic
Original: English

فريق الخبراء المعني بإجراء دراسة شاملة
عن الجريمة السيبرانية
فيينا، ٢٧-٢٩ آذار/مارس ٢٠١٩

مشروع التقرير

إضافة

ثانياً- قائمة التوصيات والاستنتاجات الأولية (تابع)

ألف- إنفاذ القانون والتحقيقات

١- تمشياً مع خطة العمل، تتضمن هذه الفقرة تجميعاً للاقتراحات التي قدمتها الدول الأعضاء في الاجتماع في إطار البند ٢ من جدول الأعمال المعنون "إنفاد القانون والتحقيقات". وهذه الاستنتاجات والتوصيات الأولية مقدمة من الدول الأعضاء، ولا يعني إدراجها أنَّ فريق الخبراء قد أقرَّها.

ثالثاً- ملخَّص المداولات

ألف- إنفاذ القانون والتحقيقات (تابع)

٢- في المناقشة التي تلت ذلك، أولى فريق الخبراء الاهتمام لأمثلة عن الأنشطة الإجرامية المضطلع بها في البيئة الرقمية، مما يشكل صعوبات كبيرة للممارسين والمحققين في مجال العدالة الجنائية عند فتح أو إجراء التحقيقات وما يتبعها من ملاحقات قضائية. ومن الأمثلة التي ذكرت الاحتيال بالاتصال الحاسوبي المباشر، واستخدام الإنترنت لأغراض إرهابية، واستخدام الشبكة الخفية في ارتكاب أنشطة غير مشروعة، وكذلك الانتهاك والاستغلال الجنسيان للأطفال عن طريق إساءة استخدام تكنولوجيات المعلومات والاتصالات. وبالإضافة إلى ذلك، أُبلغ فريق الخبراء عن الترابط المفاهيمي بين الجريمة السيبرانية والأمن السيبراني، 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.

٣- وناقش اجتماع فريق الخبراء مجدَّداً مسألة ما إذا كان يلزم اعتماد صك قانوني شامل عالمي جديد بشأن الجريمة السيبرانية، أو أنه ينبغي للدول، بدلا من ذلك، أن تركز على التنفيذ الفعال للصكوك القائمة، بما في ذلك اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية (السيبرانية) (اتفاقية بودابست). فمن ناحية، دُفع بعدم ضرورة اعتماد صك قانوني شامل عالمي جديد بشأن الجريمة السيبرانية لأن اتفاقية بودابست توفر الإطار الملائم لوضع ما يناسب من تدابير محلية ودولية للتصدي للجريمة السيبرانية. وأشير إلى أن عدد الدول الأطراف في اتفاقية بودابست البالغ ٦٣ دولة طرفاً يبيّن أن الاتفاقية مفتوحة لانضمام الدول غير الأعضاء في مجلس أوروبا. وقيل إن الدول غير الأطراف في الاتفاقية تستلهم من الاتفاقية في مواءمة المعايير التشريعية المحلية الموضوعية والإجرائية على السواء. وقيل أيضاً 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 (٢٠١٤) والمدونة الدولية لقواعد السلوك في مجال أمن المعلومات الصادرة عن منظمة شنغهاي للتعاون.

٤- ومن ناحية أخرى، أُشير إلى أن 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 لم تنضم إليها جميع الدول في العالم. وشُدِّد على أن هذا الصك يتوخى وضعه في إطار عملية تقودها الأمم المتحدة ويمكن في إطارها وضع زمام الأمور في أيدي الدول الأعضاء التي تتولى المسؤولية عن تبسيط الجهود المبذولة للتصدي للجريمة السيبرانية، من خلال تقييم (أو الاستناد إلى) الصكوك القائمة مثل اتفاقية بودابست واتفاقية الاتحاد الأفريقي السالفة الذكر. وفي هذا السياق، أشير إلى قرار الجمعية العامة ١٨٧/٧٣ بشأن التحديات التي تواجهها الدول الأعضاء في "مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية" المؤرخ في ١٧ كانون الأول/ديسمبر ٢٠١٨، 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 وتقديم تقرير استناداً إلى تلك الآراء للنظر فيه في الدورة الرابعة والسبعين للجمعية العامة. وفي مداخلات أخرى، أُعرب عن رأي مفاده أن اتفاقية بودابست لا تتناول شواغل جميع الدول الأعضاء في الأمم المتحدة وأن تعديلها يقتضي عمليات معقدة، مما قد يكون غير مناسب بالنظر إلى الطبيعة المتطورة باستمرار للجرائم السيبرانية.

٥- وأشير إلى عملية التفاوض الجارية من أجل اعتماد بروتوكول إضافي ثانٍ لاتفاقية بودابست بهدف توفير قواعد واضحة وإجراءات أكثر فعالية بشأن 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؛ وإطار أوضح وضمانات أقوى للممارسات الحالية المتعلقة بالوصول إلى البيانات عبر الحدود؛ والضمانات، بما في ذلك متطلبات حماية البيانات.

٦- 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 للتعامل تحديداً مع الجريمة السيبرانية.

٧- وأطلع أعضاء الوفود والمناظرون فريقَ الخبراء على الجهود الوطنية الناجحة الرامية إلى وضع وتنفيذ تدابير قانونية وإجرائية للتصدي للجريمة الإلكترونية. ورأى البعض 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 سماع أصوات مختلف أصحاب المصلحة. وأشير إلى ضرورة ضمان اليقين والوضوح القانونيين على أساس مبدأ "لا جريمة ولا عقوبة إلا بنص"، فضلاً عن ضرورة استخدام صيغة "محايدة تكنولوجياً" في التشريعات الجديدة بحيث تظل مواكبة للتطورات السريعة في ميدان تكنولوجيات المعلومات والاتصالات.

٨- ودارت مناقشة أيضاً حول التحديات الناشئة عن النزاعات بشأن الولاية القضائية المعنية بالإنفاذ، وخصوصاً، على سبيل المثال، في الحالات التي 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 وبدرجة أقل على مكان وجود البيانات.

٩- وشدَّد فريق الخبراء أيضاً على الحاجة إلى وجود صلاحيات إجرائية مناسبة للحصول على الأدلة الإلكترونية المتعلقة بالجريمة السيبرانية وبأشكال الجريمة التقليدية كذلك، وبيَّن أن الأدلة الإلكترونية يمكن أن تشمل، ضمن أمور أخرى، معلومات عن المشتركين، وبيانات المحتوى وبيانات حركة الاتصالات. وأُشير إلى أنَّ المحققين يصادفون تطورات تكنولوجية جديدة، مثل البرامجيات المُخفية للهوية والتشفير العالي الدرجة والعملات الافتراضية، أثناء التحقيق في الجرائم التي تنطوي على أدلة إلكترونية، وبالنظر إلى ذلك، قد يتعين عليهم اعتماد استراتيجيات جديدة والنظر في كيفية استخدام أساليب التحري الخاصة والاستدلال الجنائي الرقمي عن بُعد لجمع هذه الأدلة الإلكترونية، مع ضمان مقبولية هذه الأدلة واستخدامها في المحاكم.

١٠- وركّزت المناقشة أيضاً على كيفية تحقيق التوازن بين الحاجة إلى تدابير فعّالة في إطار إنفاذ القانون للتصدي للجريمة السيبرانية وحماية حقوق الإنسان الأساسية، وخاصة الحق في الخصوصية. وكان القاسم المشترك، على سبيل المثال، أنّ القواعد المتعلقة بالاحتفاظ بالبيانات قد تمثل نهجاً عمليًّا لضمان قدرة مقدّمي 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 مفوض الأمم المتحدة السامي لحقوق الإنسان عن "الحق في الخصوصية في العصر الرقمي"، الذي قُدِّم إلى مجلس حقوق الإنسان عملاً بقرار الجمعية العامة ٦٨/١٦٧ (A/HRC/27/37).

١١- وأكّد فريق الخبراء مجدداً أهمية التعاون الدولي في التحقيق في الجرائم السيبرانية وملاحقة مرتكبيها قضائيًّا عبر الحدود. وسُلِّم بأنّ عدد طلبات المساعدة القانونية المتبادلة للحصول على أدلة إلكترونية أو الحفاظ عليها يتزايد بسرعة، وأنّ الطرائق الحالية للتعاون، وبوجه خاص عمليات تبادل المساعدة القانونية التي تستغرق وقتاً طويلاً، ليست كافية لمواجهة التحديات التي تواجه الوصول السريع والناجح إلى البيانات، بسبب الطبيعة المتقلبة التي تتّسم بها هذه الأدلة التي يمكن نقلها أو حذفها "بنقرة على زر في لوحة مفاتيح حاسوب".

١٢- وذُكرت ممارسات مختلفة بوصفها أمثلة لتحفيز التعاون الدولي في الحالات المنطوية على أدلة إلكترونية، وخصوصاً على المستوى العملياتي، بما في ذلك ما يلي: إرسال طلبات المساعدة القانونية المتبادلة مباشرة فيما بين 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 (أفرقة التحقيق 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 والمعروفة باسم "الشبكة ٧/٢٤"؛ والإكثار من استخدام سبل التعاون المباشر بين أجهزة الشرطة، بما في ذلك عن طريق المساعدة المقدَّمة من الإنتربول، لأغراض جمع المعلومات الاستخبارية. وأُشير أيضاً إلى المركز الأوروبي لشؤون الجريمة السيبرانية الذي أنشأه مكتب الشرطة الأوروبي (اليوروبول) في عام ٢٠١٣ بهدف تعزيز تدابير الاتحاد الأوروبي الرامية إلى التصدي للجريمة السيبرانية.

١٣- وتطرق فريق الخبراء أيضاً إلى مسألة الوصول إلى البيانات عبر الحدود. وأشير إجمالاً إلى أن ممارسات الدول والإجراءات المستخدمة، فضلاً عن الشروط والضمانات الإجرائية، تختلف اختلافاً كبيراً بين مختلف الأطراف. وعلاوة على ذلك، جرى التأكيد على الحقوق الإجرائية للمشتبه فيهم، واعتبارات الخصوصية، وحماية البيانات الشخصية، ومشروعية الوصول إلى البيانات المخزنة في خوادم موجودة في الولايات القضائية الأخرى، فضلاً عن احترام السيادة الوطنية.

١٤- وشدَّد فريق الخبراء على أهمية بناء القدرات المستدامة من أجل تعزيز الفعالية والمهارات لدى جميع السلطات المختصة على الصعيد العملي من أجل التصدي للتحديات التي تطرحها

الجريمة السيبرانية. وفي هذا السياق، أشار متكلمون إلى فائدة تبادل الممارسات الجيدة والخبرات فيما بين الممارسين، ليس داخل الدول فحسب، بل أيضاً مع الدول الأخرى. 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. وجرى التأكيد في هذا الصدد على أن الأدلة الإلكترونية أصبحت متعاظمة الانتشار في التحقيق في الجرائم التقليدية أيضاً، لذا لا بد من وضع هياكل متخصصة للتحقيق في هذه الجرائم وتزويدها بالخبرة والمعارف والمهارات التشغيلية المحددة.

١٥- وناقش فريق الخبراء كذلك تعاون السلطات الوطنية مع القطاع الخاص، ولا سيما مع مقدمي خدمات الاتصالات، 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، فإن من المسلم به أيضاً أن هناك حاجة إلى بذل مزيد من الجهود لكفالة مستوى مماثل من التعاون في القضايا العابرة للحدود الوطنية. وفي هذا الصدد، أُشير إلى "مخاطر ازدواجية الامتثال" بالنسبة لمقدمي خدمات الاتصال، أي كيفية موازنة استجاباتهم وفقاً للمتطلبات القانونية للدول المعنية.

رابعاً- تنظيم الاجتماع

باء- البيانات (تابع)

١٦- أدلى بكلمات خبراء من الدول التالية: إيطاليا، بوركينا فاسو، الجزائر، سري لانكا، شيلي، الصين، فرنسا، كندا، كولومبيا، الكويت، موريتانيا، الهند، هولندا، النرويج، اليابان.

١٧- وأدلى بكلمة أيضاً الاتحاد الأوروبي، وهو منظمة حكومية دولية.