الأمم المتحدة A/74/130

الجمعية العامة

Distr.: General
30 July 2019
Arabic
Original: English

الدورة الرابعة والسبعون

البند ١٠٩ من جدول الأعمال المؤقت*

مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية

مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية

تقرير الأمين العام

ملخَّص

أعدَّ هذا التقرير عملاً بقرار الجمعية العامة ٧٣/١٨٧، المعنون "مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية". وفي ذلك القرار، طلبت الجمعية العامة إلى الأمين العام أن يلتمس آراء الدول الأعضاء بشأن التحديات التي تعترضها في مجال مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، وأن يقدم تقريراً يستند إلى تلك الآراء إلى الجمعية العامة لكي تنظر فيه في دورتها الرابعة والسبعين.

ويحتوي هذا التقرير على معلومات عن آراء الدول الأعضاء المقدمة عملاً بالقرار المذكور أعلاه.

* A/74/150.

المحتويات

الصفحة

الصفحة

أولاً- مقدِّمة

١- طلبت الجمعية العامة إلى الأمين العام، في قرارها ١٨٧/٧٣ المعنون "مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية"، أن يلتمس آراء الدول الأعضاء بشأن التحديات التي تعترضها في مجال مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، وأن يقدم تقريراً يستند إلى تلك الآراء إلى الجمعية العامة لكي تنظر فيه في دورتها الرابعة والسبعين.

٢- وبناءً على هذا الطلب، دعت الأمانة الدول الأعضاء، في المذكرتين الشفويتين CU 2019/55/DTA/OCB/CMLS وCU 2019/90/DTA/OCB/CSS، المؤرَّختين ١٣ شباط/فبراير ٢٠١٩ و١٩ آذار/مارس ٢٠١٩، على التوالي، والصادرتين عن مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة (المكتب المعني بالمخدِّرات والجريمة/المكتب)، إلى تقديم معلومات عن التحديات التي تعترضها في مجال مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية. وأبلغت الأمانة الدول الأعضاء بأن هذه المعلومات سوف تُستخدم لإعداد تقرير عن تنفيذ القرار ١٨٧/٧٣ لتقديمه إلى الجمعية العامة للنظر فيه في دورتها الرابعة والسبعين. وأشارت الأمانة إلى أن الورقات الوطنية المقدمة لأغراض إعداد التقرير يجب ألا تتجاوز ١ ٠٠٠ كلمة، مع استثناء أي نصوص مقتبسة من أي قوانين أو تشريعات قد ترغب الدولة العضو في تقديمها. كما أشارت إلى أن القوانين و/أو التشريعات المرفقة بالردود ستتاح على بوابة إدارة المعارف المسماة بوابة الموارد الإلكترونية والقوانين المتعلقة بالجريمة (بوابة "شيرلوك")، لتكون مورداً إضافيًا للمعلومات.

٣- واستجابةً لهذه الدعوة، قدمت الدول الأعضاء التالية آراءها: الاتحاد الروسي، الأرجنتين، الأردن، أرمينيا، إسبانيا، أستراليا، إستونيا، إسرائيل، ألمانيا، إيران (جمهورية-إسلامية)، أيرلندا، إيطاليا، البرازيل، البرتغال، بوتسوانا، بوليفيا (دولة - المتعددة القوميات)، بيرو، بيلاروس، تايلند، تركيا، تشيكيا، الجمهورية العربية السورية، جمهورية كوريا الشعبية الديمقراطية، جنوب أفريقيا، جورجيا، رومانيا، سري لانكا، السلفادور، سلوفاكيا، سلوفينيا، سنغافورة، سويسرا، صربيا، الصين، طاجيكستان، العراق، غانا، فرنسا، الفلبين، فنزويلا (جمهورية-البوليفارية)، قطر، كندا، كوستاريكا، كولومبيا، لبنان، ليختنشتاين، ماليزيا، المغرب، المملكة العربية السعودية، المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية، منغوليا، ميانمار، النرويج، النمسا، نيكاراغوا، نيوزيلندا، الهند، هنغاريا، هولندا، الولايات المتحدة الأمريكية، اليابان.

٤- وتعكس الموجزات التالية التي أعدَّتها الأمانة والمعروضة أدناه هذه الآراء. وقد غطت الورقات المقدمة التحديات على كل من الصعيدين الوطني والدولي، وكذلك الإجراءات المتخذة للتصدي لها على الصعيدين كليهما، بما فيها الإجراءات المتخذة في إطار الآليات المتخصصة القائمة. وقدمت الدول الأعضاء معلومات عن التحديات المتصلة بالجوانب التقنية والتكنولوجية، وعرضت تجاربها وخبراتها في التصدي لها، كما أبرزت أهمية التعاون الدولي في مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية.

ثانياً- الردود الواردة من الحكومات

الأرجنتين

٥- أشارت الأرجنتين إلى أن أكبر التحديات التي تواجهها الدول في مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية تشمل ما يلي:

(أ) نطاق الصكوك الدولية. باستثناء اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، لم تُعتمد إلى الآن اتفاقيات دولية بشأن هذا الموضوع. وتسهم الأرجنتين بفاعلية في أنشطة لجنة اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، وتوصي بأن تنظر الدول التي لم تصبح بعد أطرافاً في تلك الاتفاقية في الانضمام إليها من أجل تعزيز تنفيذها وتوطيد الامتثال لها من جانب الدول غير الأعضاء في مجلس أوروبا. غير أن الأرجنتين، نظراً للطابع العالمي لظاهرة الجريمة السيبرانية والحاجة إلى وجود آليات للتصدي لها على الصعيد العالمي، تدعم العمليات المنفذة في إطار اتفاقية مجلس أوروبا وكذلك المناقشات الرامية إلى المضي قُدُماً صوب التفاوض - تحت مظلة الأمم المتحدة - بشأن إطار قانوني عالمي بشأن هذه المسألة؛

(ب) صعوبات الوصول إلى الأدلة الرقمية عبر الحدود. تتمثل الصعوبة الرئيسية التي صودفت في معظم الحالات في أن البيانات التي تُشكل أدلة تكون موجودة في ولاية قضائية مختلفة عن تلك التي تُتخذ فيها الإجراءات الجنائية، وأن هذه البيانات تكون، في جميع الحالات تقريباً، في حوزة شركات خاصة. ولا تُلبي الحلول المقترحة حتى الآن لهذه المشكلات - مثل 'قانون توضيح الاستخدام القانوني للبيانات فيما وراء البحار' في الولايات المتحدة (ساري المفعول) و'مبادرة الأدلة الإلكترونية' للاتحاد الأوروبي (قيد الإصدار) - احتياجات الدول الثالثة تلبية كاملة؛

(ج) قصور القدرة على قياس النتائج فيما يخص تبادل المعلومات والممارسات الجيِّدة. في العديد من الحالات، يصعب قياس النتائج من حيث تبادل الممارسات الجيِّدة والمعلومات المنصوص عليه في الاتفاقات؛

(د) الصعوبات في تحديث الإطار التنظيمي فيما يتعلق بالتقدُّم التكنولوجي. ينطوي تحديث الإطار التنظيمي الجنائي، من الناحيتين الموضوعية والإجرائية، على العديد من الصعوبات، التي تزداد شدتها في الدول ذات النظم القانونية المدونة؛

(هـ) انخفاض مستويات الوعي لدى السكان ولدى المنظمات. يتمثل أحد الجوانب الأساسية لمكافحة الجريمة في الجانب المتعلق بمنع الجريمة. وفي مجال الجريمة السيبرانية، يرتبط منع الجريمة ارتباطاً مباشراً بنشر الوعي، بين الأفراد والمنظمات، حول المخاطر والتهديدات المتعلقة باستخدام تكنولوجيات المعلومات والاتصالات. فمن الضروري وضع خطط توعية وطنية تبيَّن في إطارها تفاصيل الجهود والمبادرات، الخاصة والعامة على السواء، بطريقة تكفل الاتساق والاستخدام الأمثل للموارد؛

(و) مسؤولية القطاع الخاص. يضطلع القطاع الخاص بدور أساسي فيما يتعلق بالتحديات التي تفرضها الجريمة السيبرانية. وتتضمن مسؤولية الشركات جوانب مثل مكافحة

ومعالجة ما يهدد البيانات من أوجه ضعف تنطوي عليها المنصات والأجهزة واستخدام شبكات التواصل الاجتماعي للأغراض الإجرامية. وعلاوةً على التعاون الطوعي من جانب القطاع الخاص، من الضروري تحليل مدى الحاجة إلى قواعد امتثال إلزامية؛

(ز) تزايد المخاطر. إن انتشار استخدام الأجهزة "الذكية" المنخفضة التكلفة نسبيًّا والتي تتيح الوصول إلى الإنترنت دون مراعاة الحد الأدنى من مستويات الأمن يزيد من أسباب الهجمات المحتملة ونطاق الجريمة السيبرانية. وتستلزم مواجهة هذا التحدي تطبيق الدول لسياسات يكمل بعضها بعضاً واتباع الشركات لاستراتيجيات بشأن مسؤوليتها. وثمة مخاطر تنطوي عليها المشاريع التي تقودها الدول بهدف إيجاد آليات تمكِّن من فك تشفير المعلومات المستمدة من الأجهزة و/أو التطبيقات وآليات تمكِّن من إنشاء نقاط الدخول السرية. كما يلزم تقييم الأدوات التي تقترحها الهيئات القضائية المختلفة لاختراق المعلومات واستخراجها أو رصدها.

٦- وحددت الأرجنتين التحديات الرئيسية التي تواجهها في التحقيق في الجرائم التي ترتكب من خلال استخدام تكنولوجيات المعلومات والاتصالات وملاحقة مرتكبيها قضائيًّا على النحو التالي:

(أ) تدريب العناصر الفاعلة في نظام العدالة الجنائية؛

(ب) الحاجة إلى تزويد العاملين في الجهاز القضائي وأجهزة إنفاذ القانون بأدوات التحليل الجنائي الحاسوبية والتحقيقية المناسبة؛

(ج) عدم وجود تعاريف قانونية للسلوكيات الجنائية أو عدم تجريمها؛

(د) القواعد الإجرائية، بالنظر إلى الخصائص المحددة للأدلة الرقمية؛

(هـ) تحسين آليات التعاون الدولي؛

(و) تحسين درجة تعاون شركات القطاع الخاص (مقدِّمي خدمات الإنترنت).

٧- وذكرت الأرجنتين أيضاً أن التدريب في مجال الجريمة السيبرانية وفي مجال جمع الأدلة الرقمية هو التحدي الأكبر لها في ضمان فعالية الملاحقة الجنائية. وينبغي أن تُركَّز الجهود على توسيع نطاق معارف مشغلي النظم، ومن ثم تحسين تطبيق القوانين وتطبيق الصكوك الدولية السارية. إذ إنَّ ذلك سيكفل التصدي الفعَّال لهذه الجرائم كما أنه سيضمن احترام الحقوق الأساسية للأطراف في الإجراءات القانونية.

٨- وتُثمِّن الأرجنتين مساهمة المنظمات الدولية والإقليمية، مثل الأمم المتحدة (من خلال المكتب المعني بالمخدِّرات والجريمة)، ومنظمة الدول الأمريكية، والاتحاد الأوروبي، ومجلس أوروبا، في تبادل أفضل الممارسات والخبرات. وتعمل وزارة العدل حاليًّا على وضع قواعد إجرائية نموذجية للحصول على الأدلة الرقمية، لتكون هذه القواعد هي الأساس للتشريعات على المستوى الاتحادي ومستوى المقاطعات.

٩- والأرجنتين دولة اتحادية، أي أن نظام العدالة الاتحادي فيها يتعايش مع ٢٤ نظاماً قضائيًّا للمقاطعات. ويُصعب ذلك مواجهة الظواهر المعقدة والدولية، مثل الجريمة السيبرانية والأدلة الرقمية. وتتمثل إحدى الممارسات العظيمة الفائدة التي تنفذ في هذا الصدد في إنشاء وحدات مالية

متخصصة. وتنصب الجهود الجارية على ضمان تبنّي مختلف الولايات القضائية داخل الدولة لهذا النموذج، وتسريع وتيرة التحقيقات وتبادل المعلومات.

١٠- وسلّطت الأرجنتين أيضاً الضوء على التحدي الإضافي المتمثل في نقص الموارد المالية المطلوبة لمواجهة التحولات التي يلزم إجراؤها داخل النظام القضائي وأجهزة الأمن، والتي تشمل بذل جهود مستدامة على مستوى سياسات الدولة.

أرمينيا

١١- أفادت أرمينيا بأن هيئات الدولة والأجهزة الحكومية المعنية تتخذ بوتيرة مطردة تدابير للتصدي للمخاطر الآخذة في التطور الناشئة عن الاستخدام الإجرامي لتكنولوجيات المعلومات والاتصالات، ولتعزيز التشريعات القطاعية في هذا الصدد، بوسائل تشمل الحوار المستمر مع الكيانات المتخصصة التابعة للأمم المتحدة، ومنظمة الأمن والتعاون في أوروبا، والاتحاد الأوروبي ومجلس أوروبا، وكذلك من خلال تعزيز التعاون وتبادل المعلومات في إطار مركز مكافحة الإرهاب التابع لرابطة الدول المستقلة، ومنظمة معاهدة الأمن الجماعي، والمنظمة الدولية للشرطة الجنائية (الإنتربول).

١٢- وذكرت أرمينيا أنها تعتزم إنشاء فريق عامل مشترك بين الوكالات لوضع مفاهيم واستراتيجيات وطنية وخطط عمل في مجالي المعلومات والأمن السيبراني، للفترة ٢٠١٩-٢٠٢٠، على أن يضم الفريق العامل مسؤولين وخبراء حكوميين، ومؤسسات علمية وبحثية، ومنظمات مجتمع مدني وقطاع خاص، حسب الاقتضاء.

١٣- وذكرت أرمينيا أيضاً أنها انتهت من صوغ مشاريع القوانين المتعلقة بتعديل القانون الجنائي وقانون الإجراءات الجنائية على التوالي، ومن المتوقع اعتمادها في المستقبل القريب. وتتضمن هذه الحزمة من مشاريع القوانين تعديلات وملاحق للمواد المتعلقة بالجرائم المرتكبة باستخدام نظم حاسوبية. وأثناء عملية صوغ مشروع قانون الإجراءات الجنائية، عُقدت سلسلة من الاجتماعات مع ممثلي خبراء الشرطة في مجلس أوروبا.

١٤- وتُجري أرمينيا تقييمات دورية لمخاطر غسل الأموال وتمويل الإرهاب على المستوى الوطني. ففي عام ٢٠١٧، أُجري أحدث تقييم للفترة ٢٠١٤-٢٠١٧. وكشف التحديث التحليلي لتقرير عام ٢٠١٤ حول التقييم الوطني لمخاطر غسل الأموال وتمويل الإرهاب[(١)] عن بعض المخاطر المتعلقة بغسل الأموال والمرتبطة باستخدام تكنولوجيات المعلومات والاتصالات، إذ وُجد أن المنتجات الجديدة والآليات الجديدة لتسليم الأموال (مثل محطات نقاط البيع عبر الإنترنت، والخدمات المصرفية الإلكترونية، والخدمات المصرفية عبر الهواتف المحمولة، والمحافظ الرقمية) تُستخدم بقدر متزايد لإقامة علاقات تجارية أو إجراء معاملات معقدة وكبيرة بدرجة غير عادية.

(١) يتناول التقييم الوطني لمخاطر غسل الأموال وتمويل الإرهاب التهديدات والثغرات في القطاعات التي لُوحظ فيها حدوث تطورات مهمة، والتي يُقدم الخبراء توصيات بشأنها ضمن عملية التقييم المتبادل للنظام القائم في أرمينيا لمكافحة غسل الأموال وتمويل الإرهاب، التي تجريها لجنة الخبراء المعنية بتقييم تدابير مكافحة غسل الأموال وتمويل الإرهاب التابعة لمجلس أوروبا. ويُمكن الاطلاع على الخلاصة الوافية المتاحة على الرابط التالي: www.cba.am/Storage/EN/FDK/risk_assesment/NRA_Update_Executive_Summary(Public)_eng.pdf.

١٥- وأشارت أرمينيا إلى أن المنتجات والخدمات التي تنطوي على استخدام محطات نقاط البيع ونظم الخدمات المصرفية الإلكترونية تعاني من ثغرات فيما يتعلق باستبانة المخاطر التي قد تنشأ أثناء العلاقات التجارية. ومن هذه الثغرات، على وجه الخصوص، أنه بمجرد إقامة علاقة تجارية مع أحد العملاء واتخاذ تدابير العناية الواجبة الأولية المطلوبة للتعامل معه، يمارس العميل جميع أنشطته التجارية اللاحقة في بيئة إلكترونية، لا تتضمن تعامله وجها لوجه مع موظفي البنك المعنيين (مكتب خدمة العملاء). وتقل في هذه العلاقات فرص استبانة النشاط المشبوه. وعلاوةً على ذلك، يمكن استخدام البيانات المسروقة من البطاقات الصادرة عن بنوك أجنبية لتسجيل حسابات المحافظ الرقمية، التي تُفعل من خلال إدخال مجموعة من مُحددات هوية البطاقة الصالحة (الرقم وتاريخ الانتهاء ورقم التحقق من البطاقة). ومن ثم، قد يتمكن الجناة من الحصول على خدمات مالية دون المرور بإجراءات العناية الواجبة الإلزامية تجاه العملاء. ويمكن بعد ذلك استخدام المحافظ الرقمية المسجلة لتنفيذ تحويلات برقية متعددة تهدف إلى إخفاء منشأ عائدات الجريمة، وتؤدي لاحقاً إلى نقل الأرصدة المتاحة في الحسابات.

١٦- ومع مراعاة مسببات المخاطر وعواملها التي تم تحديدها، يتخذ مركز المراقبة المالية في المصرف المركزي في أرمينيا تدابير مناسبة لمنع هذه المخاطر وردعها، بما في ذلك من خلال إسناد مهام وإصدار تعليمات مناسبة لمؤسسات مالية معينة.

١٧- وخلال عام ٢٠١٨، استهلت شعبة مكافحة الجرائم المتصلة بالتكنولوجيات العالية، التابعة للإدارة العامة لمكافحة الجريمة المنظمة بجهاز الشرطة، ٧٩ قضية جنائية. ومن بين هذه القضايا، كانت ٧٠ قضية مرتبطة بجرائم التكنولوجيات العالية، وكانت ٩ قضايا مرفوعة على أساس مواد أخرى ومرتبطة ارتباطاً وثيقاً باستخدام تكنولوجيات المعلومات والاتصالات.

١٨- وتفيد نتائج دراسة أجراها جهاز الشرطة بحدوث زيادة في عدد الدعاوى الجنائية المقامة استناداً إلى المادة ١٨١ (السرقة المرتكبة باستخدام الحواسيب) والمادة ٢٥٤ (الاستيلاء غير القانوني على بيانات حاسوبية) من القانون الجنائي لأرمينيا. وأشارت الدراسة إلى وقوع الأفراد والكيانات الاعتبارية على السواء ضحايا للأفعال المشمولة بالمادة ١٨١، في حين أن أغلب ضحايا الجرائم المشمولة بالمادة ٢٥٤ هم من مستخدمي شبكات التواصل الاجتماعي أو خدمات البريد الإلكتروني. ويرتبط الكشف عن الجرائم، في المقام الأول، بأنها ترتكب في الخارج أو أن آثارها تخفى في منظومات خوادم موجودة في عدة دول. ومن ثم ففي هذه الحالات تكون التحقيقات معقدة نتيجة للاختلافات في التشريعات بين الدول. ومن ثم فإن جهاز إنفاذ القانون مقدم الطلب لا يحصل عموماً على المعلومات المطلوبة.

١٩- ووفقاً للأحكام ذات الصلة من اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، اتخذت جهة الاتصال الوطنية داخل جهاز الشرطة تدابير للكشف عن مستخدمي شبكات التواصل الاجتماعي غير الروسية. وتُجرى التحقيقات المتعلقة بالعمليات أو القضايا الجنائية من خلال شبكة نقاط

الاتصال "٧/٢٤". وحسبما ذكرت أرمينيا، فإن الشعبة الفرعية[٢] المتخصصة تقدم المشورة والمساعدة المهنية بشأن القضايا القطاعية إلى الشُّعب الفرعية الإقليمية لجهاز الشرطة عند الطلب (شفهيًّا أو كتابيًّا). وبالإضافة إلى ذلك، نُظمت دورة تدريبية ضمت رؤساء الشُّعب الفرعية الإقليمية لجهاز الشرطة، شُرحت خلالها بالتفصيل خصائص الجرائم الحاسوبية وعملية جمع الأدلة.

٢٠- وزار مسؤولون من الشُّعب الفرعية المتخصصة التابعة لجهاز الشرطة منظمات دولية معنية، وحضروا حلقات عمل وحلقات دراسية مُخصصة لدراسة أفضل الممارسات المتبعة في مكافحة الجريمة السيبرانية.[٣] واتُّخذت ترتيبات تنظيمية مناسبة في أرمينيا في إطار عملية "بروكسي" التابعة لمنظمة معاهدة الأمن الجماعي، والتي هدفت إلى مكافحة الاستخدام الإجرامي لتكنولوجيات المعلومات والاتصالات. ويُنفذ جهاز الشرطة أنشطة تهدف إلى التوعية بالمسائل والمشكلات المتعلقة بتكنولوجيات المعلومات والاتصالات.[٤]

٢١- وتعكف الشعبة الفرعية المتخصصة لجهاز الشرطة على مراقبة منطقة النطاق الأرميني على الإنترنت، والقطاع الأرميني من شبكات التواصل الاجتماعي الواسعة الانتشار، من أجل الكشف عن الجرائم. ولا تقتصر المراقبة على الكشف عن الجريمة السيبرانية وحسب (على سبيل المثال، فيروس "الفدية" (ransomware))، بل تشمل أيضاً الأفعال الإجرامية (مثل الابتزاز عن طريق الإكراه أو التهديد، والانتحار القسري) التي يقتصر دور الإنترنت فيها على كونه وسيطاً لارتكاب الجريمة وليس أداة مباشرة لارتكابها.

٢٢- وأفادت أرمينيا أيضاً بأنه من حيث أمن المعلومات، يشكل التحريض على التعصب القائم على الهوية، والعنف، والكراهية، وكراهية الأجانب، والممارسات المتطرفة والإرهابية، إلى جانب تمجيد مرتكبي أعمال الإبادة الجماعية، من خلال استخدام الإنترنت، وبخاصة عندما يجري تشجيع ذلك وتدبيره على مستوى الدولة، مصدر قلق بالغ، وينطوي على خطر دفع المجتمعات نحو التطرف وظهور المقاتلين الإرهابيين الأجانب. وفي الوقت نفسه، سلطت أرمينيا الضوء على أن حقوق الإنسان والحريات الأساسية، بما فيها الحقوق الجماعية، ينبغي كفالتها على نحو متساوٍ وغير تمييزي عبر الإنترنت وعلى أرض الواقع على السواء، بغض النظر عن الحدود[٥] وعن الوضع القانوني للأقاليم.

(٢) تنفذ الشُّعبة الفرعية المتخصصة أنشطة البحث العملياتية بمقتضى القانون ذي الصلة، حسب التكليفات الصادرة في إطار القضايا الجنائية، وتعالج الطلبات الواردة من المواطنين.

(٣) على وجه الخصوص، جرى عرض الأساليب المتقدمة لمكافحة الجريمة السيبرانية في إطار المشروع الثاني (تعزيز إصلاح النظام القضائي) والمشروع الثالث (تدابير الدعم لمكافحة الأشكال الخطيرة من الجريمة السيبرانية) لمرفق الشراكة الشرقية، وذلك خلال فعالية نظمها الاتحاد الأوروبي بالاشتراك مع مجلس أوروبا. وعلاوةً على ذلك، نوقش مشروع قانون الإجراءات الجنائية، وآفاق الإصلاحات التشريعية، والأسس القانونية للتعاون مع القطاع الخاص.

(٤) شملت الأنشطة إجراء مقابلات مع مختلف وسائل الإعلام، والمشاركة في مؤتمرات صحفية، وإصدار مجموعة واسعة من المواد الإعلامية، والإسهام في برامج تلفزيونية.

(٥) على النحو المنصوص عليه في المادة ١٩ من العهد الدولي الخاص بالحقوق المدنية والسياسية والذي تنطوي عليه تلك المادة ضمناً.

أستراليا

٢٣- أشارت أستراليا إلى أنها ترى أن الجريمة السيبرانية تتضمن الجرائم الموجهة ضد الحواسيب، وكذلك الجرائم الأكثر تقليدية التي تيسِّر الحواسيب ارتكابها. وأكدت أستراليا أيضاً على ضرورة تركيز المناقشات على المجالات التي تتوافر فيها الخبرة التقنية. والتحديات التي تمثلها الجرائم السيبرانية معقدة وآخذة في التطور، ويتطلب التصدي لها اهتماماً دائماً وتوجيهاً ومشورة من الخبراء التقنيين المتخصصين في الجريمة السيبرانية. وفي هذا السياق، تُثمن أستراليا للغاية عمل فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، الذي أنشئ عملاً بقرار الجمعية العامة ٢٣٠/٦٥. وترى أستراليا أن فريق الخبراء، المكلف بالولاية ذات الصلة من الأمم المتحدة لتبادل المعلومات والآراء بشأن الجرائم السيبرانية، ينبغي أن يظل المنبر الرئيسي لمناقشات الجريمة السيبرانية. وعلى نطاق أوسع، يضطلع المكتب المعني بالمخدِّرات والجريمة بولاية الأمم المتحدة ذات الصلة المتعلقة بمكافحة الجريمة عبر الوطنية والمخدِّرات. ونظراً لأن الجريمة السيبرانية جريمة عبر وطنية، فمن المناسب أن تظل مناقشات الجريمة السيبرانية متركِّزة في فيينا وتحت رعاية المكتب. وتتطلع أستراليا إلى تقرير فريق الخبراء الذي سيصدر في عام ٢٠٢١، بما في ذلك نتائجه وتوصياته بشأن التشريعات الوطنية، وأفضل الممارسات، والمساعدة التقنية، والتعاون الدولي.

٢٤- وفيما يتعلق بالبيانات الموجودة خارج البلد، أفادت أستراليا، مثل جميع الدول الأعضاء، بأن أجهزتها الوطنية المعنية بإنفاذ القانون تواجه تحديات في الوصول إلى البيانات والحصول عليها لمتابعة التحقيقات والملاحقات القضائية المتعلقة بالجرائم السيبرانية بفعالية. وقد كانت البيانات تُخزَّن عادةً داخل البلد وتتاح بموجب صلاحيات التحقيق الوطنية. أما في الوقت الحاضر فنظراً لتزايد إمكانية الاتصال العالمي وتزايد الاعتماد على نظم الحوسبة السحابية فإن البيانات توزع على مجموعة متنوعة من الخدمات، ومقدِّمي الخدمات، والأماكن، والولايات القضائية. وقد يصعب تحديد مكان البيانات ويتعذر الحصول عليها إلا من خلال عمليات تعاون قانوني دولي معقدة وبطيئة. ويعني الاستخدام المتزايد لخدمات الاتصالات باستخدام الإنترنت أن الصلاحيات التفويضية التقليدية للوصول إلى الاتصالات - المخولة للجهات الناقلة للاتصالات ولمقدِّمي خدمات نقل الاتصالات - لا تستوعب كمية البيانات المطلوبة للتحقيقات في الجرائم السيبرانية.

٢٥- وشددت أستراليا على أن الحلول التعاهدية، مثل اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، توفر أساساً راسخاً لتمكين أجهزة إنفاذ القانون من الوصول إلى البيانات الموجودة في دولة أخرى، وذلك، على سبيل المثال، عند الحصول على موافقة شخص مخول بالصلاحية القانونية للكشف عن البيانات، أو متى كانت المعلومات متاحة للجمهور. وتفرض القيود التي تتعدى هذه الظروف، بما في ذلك طلب موافقة سلطات الدولة، تحديات كبيرة أمام التحقيق في الجرائم السيبرانية وملاحقة مرتكبيها قضائيًّا.

٢٦- وتجهد آليات التعاون القانوني الدولي التقليدية، مثل المساعدة القانونية المتبادلة، لمواكبة الطلب، مما يتسبب في تأخر التحقيقات في الجرائم السيبرانية. ويمكن أن توفر أطر التعاون الدولي البديلة بين السلطات المختصة في الدول، وسلطات إنفاذ القانون، ومقدِّمي خدمات الاتصالات عند الاقتضاء ووفقاً للقانون الداخلي، حلولاً عملية وسريعة.

٢٧- وأفادت أستراليا بأنها استخدمت بنجاح المعاهدات المتعددة الأطراف، مثل اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية واتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، كأساس للتعاون القانوني الدولي، فضلاً عن ترتيباتها الثنائية والوطنية. كما أن الآليات الجديدة، مثل تلك المتوخاة في البروتوكول الإضافي الذي لا يزال قيد التفاوض لاتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية والمتعلق بالوصول عبر الحدود إلى البيانات، تراعي الطبيعة المستمرة التطور للجريمة السيبرانية، وسوف تُحسِّن بقدر كبير قدرة أجهزة إنفاذ القانون على الوصول إلى البيانات المطلوبة للتحقيقات في الجرائم السيبرانية. ومن خلال تعزيز كفاءة الوصول إلى البيانات، يمكن تحقيق توازن مناسب بين هدفي إنفاذ القانون وحماية البيانات.

٢٨- وفيما يتعلق بالضمانات وصلاحيات جهاز الشرطة، أشارت أستراليا إلى أن آليات الرقابة المناسبة ضرورية لتحقيق التوازن بين حماية حقوق الإنسان والحريات الأساسية، من ناحية، والحاجة المشروعة إلى قيام أجهزة إنفاذ القانون بممارسة صلاحيات التحقيق لمكافحة الجريمة السيبرانية، من ناحية أخرى. وفي أستراليا، تخضع صلاحيات إنفاذ القانون لقدر كبير من الإشراف، ولا سيما في ممارسة صلاحيات تنطوي على قدر أكبر من الاقتحام، مثل الوصول إلى محتوى الاتصالات المخزنة واعتراض المكالمات آنياً. وتشمل هذه الضمانات متطلبات ممارسة السلطة القضائية لصلاحياتها، ومتطلبات إبلاغ البرلمان، وحق المتهمين في الطعن في مقبولية الأدلة وحقهم في إعادة النظر في القرارات، وإشراف أمين مظالم الكومنولث على جميع الأوامر القضائية المتعلقة بالاتصالات. ويتطلب التأكد من أن صلاحيات الشرطة متوازنة ومتناسبة مع الضمانات إجراء تقييم ومراجعة مستمرين، مما قد يُشكل تحدِّياً في بعض الولايات القضائية.

٢٩- وفيما يتعلق بمسألة قابلية الأطر القانونية والعملياتية للتكييف، شدَّدت أستراليا على التزامها بالاحتفاظ بأطر تشريعية وطنية قابلة للتكييف تواكب التقدُّم التكنولوجي والسلوكي السريع. وتعترف أستراليا بالتحدي المتمثل في صوغ قوانين تتناول الجرائم السيبرانية المستقلة، والصلاحيات الإجرائية للتحقيق في الجرائم السيبرانية، ومقبولية الأدلة الإلكترونية، على أن تبقى تلك القوانين قابلة للتطبيق على التكنولوجيات والسلوكيات المتطورة. ولمعالجة هذه المسألة، تعمل أستراليا - على الصعيد الوطني وفي إطار جهودها الرامية لبناء القدرات - على صوغ تشريعات محايدة تكنولوجيًّا تراعي سلوكيات الجريمة السيبرانية وتكنولوجياتها المستقبلية.

٣٠- وذكرت أستراليا أن تشريعاتها ولوائحها مصوغة على غرار اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، التي هي الصك الدولي الرئيسي بشأن الجريمة السيبرانية، والتي توفر أساساً قويًّا على الصعيدين القانوني والعملياتي للتعاون الدولي على مكافحة الجريمة السيبرانية. ويبلغ عدد الأطراف في الاتفاقية ٦٣ طرفاً، أكثر من نصفهم دول غير أعضاء في الاتحاد الأوروبي. وذكرت أستراليا أنه، من واقع تجربتها، تتسم الاتفاقية بالعصرية والتقدمية والحياد التكنولوجي المتعمد، مما يسمح لها بالتطور والحفاظ على ملاءمتها للواقع مع ظهور تكنولوجيات جديدة. كما أنها وفرت الأساس للنُّهج التشريعية الوطنية في مختلف مناطق العالم، بما في ذلك لدول ليست أطرافاً في الاتفاقية في الوقت الحاضر.

٣١- ورأت أستراليا أيضاً أن من الضروري، بالإضافة إلى وضع الأطر الشاملة اللازمة لتجريم الأفعال الإجرامية السيبرانية، توفير تدريب مستدام ومستمر لموظفي إنفاذ القانون العاملين في خطوط المواجهة. وينبغي أن يشمل التدريب الجرائم التي تُسهَّل باستخدام التكنولوجيا، وجمع الأدلة الرقمية واستخدامها. وتعتبر أستراليا أن من المهم توفير دورات تدريبية محدَّثة ومستدامة لأجهزة إنفاذ القانون الأسترالية، وكذلك للشركاء الدوليين، ومواصلة تنفيذها من خلال برامج بناء القدرات.

٣٢- وتتطلب الجريمة السيبرانية، بحكم طبيعتها، تعاوناً وثيقاً مع الدول الأخرى. وتجد أستراليا صعوبة عندما لا يكون لدى الدول التي يجب أن تتعاون معها بشأن المسائل المتعلقة بالجرائم السيبرانية سوى قدرة محدودة على التصدي للجريمة السيبرانية أو ألا تكون لدى تلك الدول أطر قانونية وطنية شاملة للتصدي لها. وتتطلب معالجة هذا التحدي أن تُركز الدول على تعزيز وبناء القدرات اللازمة لمكافحة الجريمة السيبرانية، بوسائل من بينها التدريب المتخصص على مكافحة الجرائم السيبرانية. وأكدت أستراليا على أن تقديم المساعدة في مجال الإصلاح التشريعي مهم أيضاً للدول النامية. وتقدم أستراليا الدعم للدول في مجال بناء القدرات والمساعدة التقنية من أجل مساعدتها على بناء قدراتها التقنية. وتدعم أستراليا أيضاً العمل القيِّم الذي يقوم به البرنامج العالمي لمكافحة الجريمة السيبرانية التابع للمكتب المعني بالمخدِّرات والجريمة.

النمسا

٣٣- ذكرت النمسا، في معرض إفادتها عن التحديات العالمية في مكافحة الجريمة السيبرانية، أن الجريمة السيبرانية تُمثل تحدِّياً يتطور ويؤثر على كل دولة ويتطلب اتِّباع نهج كفء وفعال من أجل ما يلي:

(أ) زيادة عدد الدول التي لديها تشريعات محلية ملائمة ومتوافقة تتعلق بالجريمة السيبرانية وتدعم أيضاً آليات التعاون الدولي؛

(ب) بناء آليات التعاون، والثقة، والمهارات، اللازمة لتبادل البيانات من أجل التحقيق في الجرائم السيبرانية وملاحقتها قضائيًا والحد منها.

ويشمل ذلك، على سبيل المثال لا الحصر، التأكد من عدم وجود ملاذات آمنة لمرتكبي الجرائم السيبرانية، وزيادة قدرات سلطات إنفاذ القانون والسلطات القضائية على إجراء تحقيقات فعالة في الجرائم السيبرانية وملاحقة مرتكبيها وإدانتهم.

٣٤- وبغية ضمان وجود تشريعات شاملة تتعلق بالجرائم السيبرانية على مستوى الاتحاد الأوروبي، وافقت الدول الأعضاء في الاتحاد الأوروبي، بما فيها النمسا، على مجموعة من الصكوك التي توفر تعاريف مشتركة للجرائم الجنائية، وهي الصكوك التالية: توجيه بشأن الهجمات على نظم المعلومات، وتوجيه بشأن مكافحة الانتهاك الجنسي والاستغلال الجنسي للأطفال واستغلال الأطفال في مواد إباحية، والقرار الإطاري بشأن مكافحة الاحتيال وتزوير وسائل الدفع غير النقدية

المؤرَّخ ٢٨ أيار/مايو ٢٠٠١.[٦] وبالإضافة إلى ذلك، قدمت المفوضية الأوروبية، في ١٧ نيسان/أبريل ٢٠١٨، مقترحات تشريعية لتحسين الوصول عبر الحدود إلى الأدلة الإلكترونية في التحقيقات الجنائية.

٣٥- ومع ذلك، لا يمكن اعتبار الوصول إلى الأدلة الإلكترونية إلاَّ خطوة أولى، نظراً لعدم وجود نظام مشترك لحفظ البيانات على المستوى الأوروبي من شأنه يضمن توافر الأدلة الإلكترونية. ولذلك يتباين الإطار الزمني ومقدار الأدلة الإلكترونية تبايناً كبيراً بين الدول الأعضاء في الاتحاد الأوروبي، بل قد يعتمدان على رضى المنظمات. ومن الجدير بالذكر في هذا السياق الحالة الإشكالية لبروتوكول الاستفسارات عن أصحاب أسماء النطاقات (WHOIS)، التي لا تزال حتى الآن دون حل عملي. ومن المنتظر معالجة الحاجة إلى تحسين الوصول إلى الأدلة الإلكترونية في بروتوكول ثانٍ لاتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية.

٣٦- وأشارت النمسا إلى أن وكالة الاتحاد الأوروبي للتعاون في مجال إنفاذ القانون (اليوروبول) أنشأت في عام ٢٠١٣ المركز الأوروبي للجريمة السيبرانية (EC3)، الذي قدم مساهمةً كبيرةً في الجهود التي تبذلها الدول الأعضاء في الاتحاد الأوروبي لمكافحة الجريمة السيبرانية باستخدام نموذج مرن لمكافحة الجريمة. وأشارت النمسا إلى ضرورة إشراك المدعين العامين في قضايا الجرائم السيبرانية في أبكر مرحلة ممكنة، واعتبرت أن إنشاء شبكات متخصصة، مثل الشبكة القضائية الأوروبية للجريمة السيبرانية، مفيد في هذا الصدد.

٣٧- وفيما يتعلق بخيارات تعزيز تدابير التصدي الحالية واقتراح تدابير قانونية أو سبل أخرى جديدة للتصدي للجريمة السيبرانية على الصعيدين الوطني والدولي، أشارت النمسا إلى أن الجريمة السيبرانية مشكلة عالمية، وأن كل دولة بحاجة إلى مساعدة من الدول الأخرى لمكافحتها. واعتبرت النمسا أن اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية تُمثل نموذجاً للتشريعات الوطنية وإطاراً قيِّماً للتعاون الدولي، وأنها توفر صكًّا مرناً مفضَّلاً، حتى بالنسبة للأطراف غير الأعضاء في مجلس أوروبا. ولذلك لا تؤيد النمسا الدعوات إلى وضع صك دولي جديد بشأن الجريمة السيبرانية.

٣٨- وذكرت النمسا أن فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية هو الآلية الأساسية على مستوى الأمم المتحدة فيما يتعلق بموضوع الجريمة السيبرانية، وينبغي أن يظل كذلك، على الأقل حتى عام ٢٠٢١. وقد حقق فريق الخبراء نتائج، بما في ذلك فيما يتعلق بالإصلاحات التشريعية المستندة إلى المعايير الدولية القائمة، وخصوصاً فيما يتعلق ببناء القدرات. وينبغي إعداد تحديث لمشروع الدراسة الشاملة عن الجريمة السيبرانية الذي قُدِّم في عام ٢٠١٣، وهو ما سيتطلب خبرة فريق الخبراء.

(٦) لم يعد القرار الإطاري ساري المفعول. ففي ٢٩ أيار/مايو ٢٠١٩، استعيض عنه بتوجيه الاتحاد الأوروبي رقم 2019/713 (EU) الصادر عن البرلمان الأوروبي والمجلس بتاريخ ١٧ نيسان/أبريل ٢٠١٩ بشأن مكافحة الاحتيال وتزوير وسائل الدفع غير النقدية (*Official Journal of the European Union,* L 123, 10 May 2019)، الصفحات ١٨-٢٩.

٣٩- واقترحت النمسا أن يحقق المكتب المعني بالمخدِّرات والجريمة والدول الأعضاء تلك الأهداف، وأن تدعم الدول الأعضاء المكتب في التركيز على مجالات محددة يمكن أن يُحدث فيها تأثيراً حقيقيًّا في مكافحة تهديد الجريمة السيبرانية، وهي المجالات التالية:

(أ) رفع مستوى مهارات أجهزة الشرطة وإنفاذ القانون من خلال التدريب العام والمتخصص على السواء؛

(ب) تطوير المساعدة التقنية المقدمة إلى الدول النامية؛

(ج) إجراء تحليل للثغرات في مجال التعاون الدولي على تحديد المجالات ذات الأولوية؛

(د) دعم حملات التوعية العامة الرامية إلى تعزيز منع الجريمة، وبناء آليات تعاون بين المجتمع المدني وقطاع الأعمال مع أجهزة إنفاذ القانون؛

(هـ) تعزيز الآليات العملياتية القائمة، مثل شبكة نقاط الاتصال "٧/٢٤"؛

(و) جمع البيانات عن تهديدات الجريمة السيبرانية؛

(ز) قيام المكتب بدور مستودع لأفضل الممارسات ودراسات الحالة في التصدي للجريمة السيبرانية.

بيلاروس

٤٠- ذكرت بيلاروس أنها، بالنظر إلى تطور جرائم المخدِّرات المعاصرة واستخدام شبكة الإنترنت الخفية والعملات الرقمية المشفرة في الاتجار بالمخدِّرات، تعتقد أن إحدى أولويات الدول الأعضاء ينبغي أن تكون ضمان تبادل المعلومات، على المستوى فوق الوطني، بشأن وسائل ارتكاب الجرائم وأساليب الكشف عن الأنشطة الإجرامية التي تجري على شبكة الإنترنت الخفية؛ وجمع الأدلة الإلكترونية وضبطها؛ وتطوير واستخدام التقنيات الخاصة في التحقيق في الجرائم المرتكبة في الفضاء الافتراضي. ويمكن أن يكون تدريب ضباط إنفاذ القانون على آلية عمل شبكة الإنترنت الخفية والعملات الرقمية المشفرة أحد وسائل مواجهة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية. وشددت بيلاروس على أن من المهم وضع آلية قانونية دولية (توصيات) بشأن إجراءات ضبط الموجودات الرقمية المشفرة الإجرامية وتخزينها لحين اتخاذ المحكمة قراراً بشأنها.

٤١- وأشارت بيلاروس إلى أنها اعتمدت "مفهوم أمن المعلومات" في ١٨ آذار/مارس ٢٠١٩، وأنه ينص على مهام وأولويات استراتيجية في مجال أمن المعلومات ومكافحة الجريمة السيبرانية. ويستند المفهوم إلى المصالح الجيوسياسية لبيلاروس وإلى الاتفاقات الدولية بشأن التعاون في مجال ضمان أمن المعلومات على الصعيد الدولي، مع مراعاة الأحكام الرئيسية لقرارات الجمعية العامة، وكذلك توصيات منظمة الأمن والتعاون في أوروبا.

٤٢- وتعتقد بيلاروس أن وضع صك دولي عالمي في إطار الأمم المتحدة واعتماده من شأنه تسهيل تطوير التعاون بين الهيئات المختصة في الدول الأعضاء في مجال مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية.

بوليفيا (دولة-المتعددة القوميات)

٤٣- أشارت دولة بوليفيا المتعددة القوميات إلى أن التقدم التكنولوجي كان له تأثير على جميع جوانب النشاط البشري في البلاد وفي جميع أنحاء العالم، فضلاً عن تأثيره على الأمن فيما يتعلق باستخدام التكنولوجيات الجديدة. وقد أتاحت تكنولوجيات المعلومات والاتصالات تطور الجرائم التقليدية وانتشارها من خلال استخدام البرمجيات والتطبيقات وشبكات الاتصالات. وسهَّل اعتماد المؤسسات المالية على النظم الرقمية ارتكاب جرائم مثل الاحتيال. وبالمثل، أتاحت سهولة الوصول إلى الهواتف المحمولة دون تسجيل البيانات الشخصية إخفاء هوية مرتكبي الجرائم.

٤٤- وبالنسبة لجهاز الشرطة في دولة بوليفيا المتعددة القوميات، يُعد منع الجريمة وضمان أمن الاتصالات من الأولويات الرئيسية للجهاز. وقد أنشئت شعبة لمكافحة الجريمة السيبرانية ضمن القوة الخاصة لمكافحة الجريمة، التي هي وحدة متخصصة للكشف عن الجرائم المرتكبة باستخدام تكنولوجيات المعلومات والاتصالات. ويضم جهاز إنفاذ القانون الوطني وحدات مخصصة لمراقبة الصحافة وشبكات التواصل الاجتماعي. ويسعى رصد وسائل التواصل الاجتماعي إلى منع "فقاعات المعلومات" (الحد من المعلومات التي تهدف إلى التأثير سلباً على الرأي العام) وإلى منع الابتزاز والتهديدات والاتجار بالأشخاص والاحتيال والتنمر السيبراني والتمييز والجرائم الأخرى التي تهدد أمن الدولة.

٤٥- وأبلغت دولة بوليفيا المتعددة القوميات بأن الأطفال، وبخاصة أولئك الذين تتراوح أعمارهم بين ١٢ عاماً و١٨ عاماً، يتعرضون لمخاطر تتعلق باستخدام تكنولوجيات المعلومات والاتصالات، لأنهم يتعرضون لهذه التكنولوجيات الجديدة من سن مبكرة ويستخدمونها بانتظام للترفيه والاتصالات والحصول على المعلومات. بيد أن الأطفال لا يحصلون دائماً على فائدة تربوية أو تعليمية من تلك التكنولوجيات.

٤٦- وقدمت دولة بوليفيا المتعددة القوميات القائمة غير الشاملة التالية لأنواع إساءة استخدام تكنولوجيات المعلومات والاتصالات والجرائم الحاسوبية:

(أ) التحرش والإهانات والقذف والإقصاء الاجتماعي من خلال شبكات التواصل الاجتماعي ورسائل البريد الإلكتروني، وحتى من خلال مساحات التعليقات في أقسام الرأي في الصحف. وفي البيئات التي تبدو بريئة ظاهرياً، كما هو الحال في المدارس، تُشن حملات مجهولة المصدر، من خلال الفيسبوك على سبيل المثال، ضد بعض الأطفال؛ وتتعرض طالبات الجامعة للقذف، مثل اتهامهن بالبغاء، وتُبذل محاولات لتشويه سمعة الشركات على أساس معلومات خاطئة؛

(ب) عمليات الغش والاحتيال، وعلى سبيل المثال "التصيد الاحتيالي"، التي تحصل من خلالها المنظمات الإجرامية على معلومات سرية تتيح لها الدخول إلى الحسابات المصرفية وإفراغها.

وثمة مثال آخر هو توظيف الأشخاص عبر الإنترنت في وظائف للتغطية على الشبكات الضالعة في الاتجار بالأشخاص واستغلال الأطفال في المواد الإباحية. وبصفة عامة، يرتبط الاحتيال بالوصول إلى المعلومات السرية، وكذلك بإمكانية تغييرها؛

(ج) الرسائل الإلكترونية التطفلية. وهي لا تُشكل بالضرورة خرقاً للقانون ولكنها تمثل استخداماً غير سليم لقواعد البيانات لأغراض تجارية من جانب العديد من الشركات لتوسيع حملاتها التسويقية بغية الوصول إلى المستخدمين المحتملين. وقد تشمل الرسائل التطفلية حملات البغاء وغيرها من الحملات التي تُروج لأنشطة غير قانونية؛

(د) تبيع الجماعات الإجرامية، عبر الإنترنت، مواد الانتهاك الجنسي للأطفال، في شكل مقاطع فيديو وصور. وهذا انتهاك لاتفاقية حقوق الطفل والقانون الجنائي؛

(هـ) الملكية الفكرية. تُنتهك حقوق الأشخاص وحقوق المنظمات الابتكارية بطرائق متعددة، تشمل التقاط صور للنصوص المحمية (حقوق التأليف والطبع والنشر)؛

(و) المبيعات عبر الإنترنت، بما في ذلك وسطاء اليانصيب المزعومون ومسابقات اليانصيب المزعومة.

٤٧- وأفادت دولة بوليفيا المتعددة القوميات بأنه، إلى جانب تطور التكنولوجيات الحاسوبية، يجد المجرمون سبلاً مبتكرةً لارتكاب جرائم الاحتيال وغيرها من الجرائم بوتيرة أسرع من قدرة القوانين الجنائية على التصدي لها. وفي مواجهة ظاهرة آخذة في الازدياد، ينبغي النظر إلى الحاجة إلى الوقاية والحماية على أنها واجب الجميع، أي الدولة والشركات والمنظمات والمواطنين. وبهذا المعنى، تفرض الابتكارات التكنولوجية تحديات متعددة على المؤسسات المسؤولة عن التصدي لها، بما في ذلك ما يلي:

(أ) نقص وعي ومعرفة الجمهور باستخدام تكنولوجيات المعلومات والاتصالات، مما يجعلهم أكثر عرضة للجرائم المختلفة. ويتمثل أحد التحديات ذات الصلة في كيفية صوغ سياسات ملائمة من أجل زيادة المعرفة بالاستخدام السليم لهذه التكنولوجيات؛

(ب) وجود فراغ قانوني ناجم عن عدم المعرفة بالجرائم الجديدة المتعلقة بتكنولوجيات المعلومات والاتصالات، أو عن عدم سريان التشريعات القائمة عليها. ولذلك من الضروري مراجعة التشريعات وتحديثها؛

(ج) الحاجة إلى تعديل استراتيجيات التحقيق التقليدية وتدابير مكافحة الجريمة، من خلال استخدام أساليب جديدة في ضوء تطور الجرائم المتعلقة باستخدام تكنولوجيات المعلومات والاتصالات؛

(د) الحاجة إلى الانضمام إلى اتفاقات التعاون الدولي في مجال البحوث والضمان والحصول على الأدلة في مجال الجريمة السيبرانية. والعديد من دول أمريكا اللاتينية أطراف بالفعل في الاتفاقيات، وقد أحرزت مزيداً من التقدم في تطوير قدراتها التكنولوجية في مجال منع الجرائم المرتكبة باستخدام تكنولوجيات المعلومات والاتصالات والتحقيق فيها.

٤٨- وأشارت دولة بوليفيا المتعددة القوميات إلى أن إدماج التكنولوجيات الجديدة في نظم المؤسسات الحكومية يؤثر على الثقافة التنظيمية عن طريق تعديل الإجراءات وإدماج المعارف الجديدة المُكتسبة. ويتطلب العديد من التكنولوجيات المطورة في المؤسسات الأمنية والمطبقة فيها معارف محددة، مما قد يؤدي إلى فتح أبواب المؤسسات أمام أشخاص أو مؤسسات لا تنتمي بالضرورة إلى مجال الأمن، مثل الجامعات والمعاهد التقنية والمراكز البحثية وموردي البرمجيات. وفي الوقت الحاضر، تمتلك كل من قوات الشرطة والمواطنين أدوات تكنولوجية مختلفة للتعامل مع المشكلات الأمنية والأعمال الإجرامية، تُستخدم في بعض الحالات في منع الجريمة، وفي حالات أخرى كوسيلة مساعِدة للتحقيق في القضايا الجنائية. وبعض هذه العناصر منتشر على نطاق واسع، بين المواطنين والشرطة على السواء، في حين أن البعض الآخر أكثر تكلفة، ومن ثم يصعب على عامة الجمهور الحصول عليه.

٤٩- وخلصت دولة بوليفيا المتعددة القوميات إلى أن التقدُّم التكنولوجي يتيح نشوء ديناميات إجرامية جديدة، تجبر المؤسسات على أن تكيف، وتدمج في نظمها، استراتيجيات ابتكارية تمكِّنها من أن تبقى متقدمة قليلاً على العناصر الإجرامية وأن تدافع عن المجتمع وتحافظ على النظام العام عن طريق منع الجرائم والتحقيق فيها. ولذا فمن غير المتصور أن تفكر المؤسسات المسؤولة عن الأمن في مواجهة ظاهرة الإجرام دون استخدام الأدوات التكنولوجية. وتستطيع المؤسسات المسؤولة عن الأمن أن تستخدم الأدوات التكنولوجية لا داخلياً فحسب بل أيضاً لإشراك المواطنين في منع الجريمة.

بوتسوانا

٥٠- أشارت بوتسوانا إلى التحديات التالية في مجال مكافحة الجرائم، ولا سيما تلك المرتكبة بالاستعانة باستخدام تكنولوجيات المعلومات والاتصالات:

(أ) أن عدم مواءمة التشريعات المتعلقة بالجريمة السيبرانية وحماية البيانات بين مختلف الدول والولايات القضائية يجعل التحقيق في الأنشطة الإجرامية في الفضاء السيبراني أمراً بالغ الصعوبة؛

(ب) أن عدم وجود إطار دولي لتبادل معلومات الأمن السيبراني بين مختلف الأجهزة في البلدان المختلفة يمثل تحدِّياً فيما يخص حماية الشبكات والتحقيق في الأنشطة الإجرامية التي تشمل ولايات قضائية متعددة؛

(ج) من الممكن تطبيق الابتكارات التكنولوجية الجديدة، مثل الذكاء الاصطناعي وإنترنت الأشياء، في مجالات مثل الاستخدامات الزراعية والطبية وتحليل بيانات المناخ، لكن هذه الابتكارات تُوفر أيضاً وسيلة محتملة يمكن بها أو من خلالها شن الهجمات السيبرانية؛

(د) تتمثل إحدى العقبات أو التحديات الرئيسية الأخرى في بناء قدرات مختلف الأطراف الفاعلة، مثل أجهزة إنفاذ القانون ومقدِّمي الخدمات وواضعي السياسات والجهات التنظيمية، على التصدي لمسائل الأمن السيبراني؛

(هـ) وجود صعوبات في التعامل مع الشركات المتعددة الجنسيات التي تقدم خدمات داخل السوق المحلي دون ترخيص، مثل الفيسبوك والواتس آب وغوغل ومايكروسوفت ونتفلكس.

وتتسم عملية الحصول على المعلومات أو الأدلة المتعلقة بالجرائم التي ترتكب عبر شبكات هذه الشركات بالصعوبة؛

(و) بوتسوانا والعديد من الدول الأخرى ليست أطرافاً في الاتفاقيات القائمة المتعلقة بتكنولوجيات المعلومات والاتصالات والأمن السيبراني (على سبيل المثال، اتفاقية الاتحاد الأفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات الشخصية، واتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية)، مما يُصعب اللجوء للعدالة من خلال هذه الاتفاقيات. وتوفِّر اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية إطاراً قانونيًّا للتعاون الدولي في مجال الجريمة السيبرانية والأدلة الإلكترونية، وينبغي تشجيع البلدان على أن تصبح أطرافاً فيها؛

(ز) عمليات المساعدة القانونية المتبادلة بطيئة ومرهقة، مما يجعل العدالة مفتقرة إلى الكفاءة فيما يخص بوتسوانا وبلدان أخرى؛

(ح) لا يزال الكشف الطوعي عن الجريمة السيبرانية يشكل عقبة في العديد من الولايات القضائية. فعملية الحصول على المعلومات طويلة، ومستحيلة في بعض الحالات، ويرجع جانب من ذلك إلى عدم مواءمة قواعد الوصول إلى معلومات المشتركين بين الدول المختلفة. فما تفسره بوتسوانا بأنه جريمة أو تعتبره جريمة قد لا يكون كذلك في دولة أخرى.

٥١- وقدمت بوتسوانا التوصيات التالية:

(أ) توجد حاجة إلى التعاون والتضافر بين أجهزة مثل المكتب المعني بالمخدِّرات والجريمة والاتحاد الدولي للاتصالات والإنتربول بغية العمل سويًّا من أجل التصدي لتحديات استخدام المجرمين شبكات تكنولوجيات المعلومات والاتصالات لارتكاب جرائمهم. ويلزم توضيح دور مختلف الأجهزة في العمل على تحقيق الأمن السيبراني؛

(ب) ينبغي وضع إطار دولي لتبادل معلومات الأمن السيبراني بين الدول الأعضاء في الأمم المتحدة؛

(ج) يلزم إيجاد إطار دولي للسياسات والأنظمة لمعالجة مسألة الاستخدام السليم للتكنولوجيات الجديدة، بما فيها الذكاء الاصطناعي وإنترنت الأشياء؛

(د) ينبغي وضع برامج لبناء القدرات للدول الأعضاء؛

(هـ) ينبغي وضع إطار للشركات المتعددة الجنسيات لتوفير المعلومات والأدلة للدول الأعضاء وللمساعدة على التحقيق في الجرائم التي ترتكب داخل شبكات الشركات؛

(و) ينبغي تشجيع الأمم المتحدة على بحث الأساس المنطقي للموقف الذي يبدو متمنعاً والذي تتخذه البلدان فيما يتعلق بالتصديق على الاتفاقيات الإقليمية المتعلقة بتكنولوجيات المعلومات والاتصالات والأمن السيبراني؛

(ز) ينبغي اعتماد معيار لوضع إطار أبسط للمساعدة القانونية المتبادلة، لكي تعتمده الدول الأعضاء؛

(ح) وأخيراً، ثمة حاجة إلى معاهدة دولية لمعالجة قضايا الجرائم التي ترتكب في شبكة تكنولوجيات المعلومات والاتصالات. وينبغي أن توائم هذه المعاهدة التشريعات العالمية، ومبادئ تبادل المعلومات، والمعايير الدنيا لأمن المعلومات، وتقديم المساعدة في مسائل إنفاذ القانون (التحقيق وتسليم المطلوبين والملاحقة القضائية)، وأن تُقدم توجيهاً موجزاً بشأنها.

البرازيل

٥٢- ذكرت البرازيل أن سلطاتها تتعامل مع الجرائم السيبرانية منذ ظهور الإنترنت، وأن هذه الجرائم تتزايد من حيث عددها ومستوى تطورها. وقد تطلَّب انتقال الجرائم المختلفة إلى المنصات الرقمية بذل جهود كبيرة لتحديث التدابير التشريعية والقضائية المناسبة الخاصة بالتصدي للتهديدات الجديدة. كما أن النطاق الجغرافي لتلك الجرائم يشكل تحدِّياً للآليات التقليدية التي تقدم البرازيل من خلالها التعاون القانوني الدولي وتتلقاه. والتحديات هائلة، ومنها ما يلي: أن مقدِّمي خدمات الإنترنت، الذين يمتلكون المعلومات اللازمة للتحقيق في الجرائم السيبرانية وجمع الأدلة الإلكترونية، كثيراً ما يكون لديهم مقر مادي في بلد واحد ويقدمون خدماتهم في قارات مختلفة ويخزنون معلوماتهم على خوادم في أماكن أخرى على ظهر كوكب الأرض. وفي هذا السيناريو، يجهد مسؤولو إنفاذ القانون لتحديد الجهات التي تمتلك سلطة قضائية على البيانات وإمكانية الوصول المباشر إليها، وللاتصال بها حسب الأصول المرعية. كما أن معالجة طلبات التعاون الدولي، التي تُرسل عادةً في إطار معاهدات المساعدة القانونية المتبادلة، بطيئة للغاية، وتصبح أحياناً غير قابلة للتطبيق نظراً لسرعة التخلص من البيانات الرقمية.

٥٣- وأفادت البرازيل أيضاً بأنه متى اشتملت التحقيقات والولاية القضائية على عنصر دولي فإن سير الإجراءات القانونية للقضية يتباطأ في كثير من الأحيان بسبب الاختلافات حول معنى حماية الخصوصية، وهو ما ينعكس على المتطلبات الوطنية المختلفة بشأن الكشف عن البيانات. وهناك تحد آخر يواجه التعاون القانوني الدولي وهو السرعة البالغة التي تُزال بها الأدلة الرقمية، نظراً لأن الكم الهائل من المعلومات المتداولة على مستوى العالم والتكاليف المرتبطة بتخزينها تجعل الشركات لا تحتفظ بالبيانات إلا لمدة لا تزيد عما هو ضروري تماماً لأعمالها.

٥٤- وجريمة استغلال الأطفال في المواد الإباحية هي أكثر جريمة تواتراً من بين الجرائم العديدة المرتكبة في وسائل الإعلام الرقمية التي لاحق مسؤولو إنفاذ القانون في البرازيل مرتكبيها. وتبذل البرازيل أقصى ما تستطيع للتصدي لهذه الجريمة، سواءً من خلال الإنتربول أو مباشرة (ورد مليونا بلاغ من الولايات المتحدة، على سبيل المثال). ومن الجرائم المتكررة أيضاً غزو المواقع والتصيد الاحتيالي، وكلاهما يُمكِّن من الاحتيال المصرفي، الذي يتصدى له القطاع المالي البرازيلي بتدابير استباقية مُنظمة. وسرقة عملات البيتكوين والعملات الرقمية المشفرة (على سبيل المثال، من خلال فيروس WannaCry الذي ظهر في عام ٢٠١٧)، هما جريمتان أحدث ظهوراً وتشكلان كذلك صعوبات من حيث تصنيف الجريمة.

٥٥- وتُراعي البرازيل الطبيعة الفريدة للأدلة الرقمية والجريمة السيبرانية. وتنص المادة ١١ من الإطار المدني للإنترنت على وجوب تطبيق القانون البرازيلي في جمع البيانات وتخزينها ومعالجتها

عند وجود أحد الأجهزة الطرفية الحاسوبية على الأراضي البرازيلية. ولذلك يجب على الشركات الأجنبية التي لديها فروع في البرازيل أو التي تقدم خدمات للمستخدمين البرازيليين وتجمع البيانات التي حصلت عليها من هؤلاء المستخدمين أو تخزنها أو تحفظها أو تعالجها، أن تمتثل للقانون البرازيلي. ويسمح هذا الإطار للسلطات البرازيلية بالوصول المباشر إلى الأدلة والبيانات الإلكترونية التي تُجمع من الخدمات المقدمة في البلد. وتستند الولاية القضائية البرازيلية إلى مفهوم الخدمات المعروضة أو المقدمة في إقليمها الوطني.

٥٦- ورأت البرازيل أنه بالرغم من أن الإنترنت فضاء افتراضي بلا حدود فإن نقطة اتصالها بالعالم المادي تحدث في إقليم قائم ومحدود لدولة من الدول. ويمثل التوزيع الدولي المتماسك للولاية القضائية خطوة إلى الأمام في الملاحقة القضائية للجرائم السيبرانية. وقد أُدرج اختبار استهداف (مشابه لمبادرة الأدلة الإلكترونية للاتحاد الأوروبي[٧]) في القانون البرازيلي في عام ٢٠١٤. وحتى قبل المفاوضات حول معاهدة عالمية في هذا الشأن، استبقت البرازيل المواءمة بين التشريعات الوطنية في المستقبل باستخدامها الآلية القانونية المتمثلة في اختبار الاستهداف، التي تتجاهل مواقع الخوادم وجنسية الشركة المسؤولة عن إدارتها.

٥٧- وأفادت البرازيل بأن ثمة حاجة إلى توطيد التعاون والارتقاء بمستواه، إما من خلال استخدام شكل متقدم من أشكال تنفيذ معاهدات المساعدة القانونية المتبادلة الحالية، أو من خلال وضع معاهدات تكميلية بشأن الجريمة السيبرانية، مما سيكون له دور فعَّال في تسريع وتيرة التبادل الدولي للأدلة الرقمية، السريعة الزوال بطبيعتها. كما أن ما تتسم به الجريمة السيبرانية من كثرة المنصات والنظم والاستراتيجيات يستدعي تعزيز آليات التعاون التقني. ويجب أن تُتاح للخبراء وضباط الشرطة والمدعين العامين والقضاة المعنيين المزيد من الفرص للتعلم من التجارب والأساليب التي ثبت نجاحها لدى نظرائهم في الخارج.

٥٨- وذكرت البرازيل أيضاً أن التفاوض المتعدد الأطراف بشأن صك دولي تحت رعاية الأمم المتحدة قد يكون وسيلة لوضع معايير دنيا مشتركة لتبادل المعلومات والأدلة من أجل التصدي للجريمة السيبرانية، بالاستناد إلى الصكوك الدولية والإقليمية القائمة بالفعل. وينبغي تنظيم تلك المناقشات بدعم من المكتب المعني بالمخدِّرات والجريمة، في فيينا، حيث توجد بالفعل خبرة في مكافحة الجريمة السيبرانية، وحيث يناقش فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية هذه القضية بالفعل. ويمكن أن تتمثل الخطوة الأولى لوضع اتفاقية بشأن الجريمة السيبرانية في تشكيل فريق خبراء مفتوح العضوية للبدء في صوغ نص الاتفاقية.

(٧) القرار الإطاري لمجلس الاتحاد الأوروبي 2008/978/JHA المؤرَّخ ١٨ كانون الأول/ديسمبر ٢٠٠٨ بشأن مذكِّرة الأدلة الأوروبية لغرض الحصول على الأشياء والوثائق والبيانات لاستخدامها في المحاكمات في المسائل الجنائية (*Official Journal of the European Union,* L 350, 30 December 2008).

كندا

٥٩- ذكرت كندا أنها حدثت قوانينها مؤخّراً من أجل تحسين مكافحة الجريمة في القرن الحادي والعشرين، ولكن تلك القوانين مع ذلك لا تزال تواجه تحديات في هذا الصدد. و سلّطت كندا الضوء على طريقتين يعمل بهما المجتمع الدولي بالفعل على معالجة الظروف التي تنجم عنها تلك التحديات.

٦٠- فأولاً، من منظور العمليات، سلطت كندا الضوء على العمل المهم الذي يقوم به فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية. فالفريق مُكلف بإجراء دراسة شاملة عن مشكلة الجريمة السيبرانية وتدابير التصدي لها، بهدف بحث الخيارات المتاحة لتعزيز التدابير الحالية واقتراح تدابير قانونية وتدابير أخرى وطنية ودولية للتصدي للجريمة السيبرانية. وهذا العمل مستمر ويسترشد بخطة عمل تتوخى إنهاء الفريق لعمله في عام ٢٠٢١. وترى كندا أن عمل الفريق، الذي يوفر منتدى للاستفادة من مساهمات الخبراء في المناقشات حول موضوع الجريمة السيبرانية، وهو موضوع يتسم بطابع تقني للغاية، ضروري للمناقشات المقبلة في الأمم المتحدة حول التدابير المحتملة للتصدي للجريمة السيبرانية، بما في ذلك أبعاد ذلك العمل المتعلقة بالتعاون الدولي وببناء القدرات.

٦١- وثانياً، ومن وجهة نظر موضوعية، تؤيد كندا اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية تأييداً كاملاً، باعتبارها أفضل أداة دولية لمكافحة الجريمة السيبرانية. وتعالج الاتفاقية الطبيعة العالمية للاستخدام الإجرامي لتكنولوجيات المعلومات والاتصالات معالجة فعالة، من خلال توفير التعاون الدولي في مكافحة الجريمة السيبرانية، عن طريق الدول الأطراف فيها البالغ عددهم حاليًا ٦٣ دولة، بما في ذلك عدد كبير ومتزايد من الدول غير الأوروبية. والاتفاقية قابلة للتكييف بما يتناسب مع التحديات الناشئة، من خلال إصدار مذكرات إرشادية لمساعدة أطراف الاتفاقية على تطبيق الأحكام الحالية على الظواهر الجديدة في مجال الجريمة السيبرانية، وتكمِّلها شبكة نقاط الاتصال "٧/٢٤" وبرامج قوية لبناء القدرات. وتعمل أطراف الاتفاقية أيضاً على تحسين آليات التعاون الدولي، لأن التحقيقات الجنائية تتطلب بقدر متزايد الوصول إلى المعلومات المخزنة في ولايات قضائية أخرى. وتؤيد كندا الاتفاقية، وتعتقد اعتقاداً راسخاً أنها أفضل خيار متاح، إما كإطار ملزم قانوناً للدول الراغبة في الانضمام إليها والقادرة على ذلك، أو كنموذج لصوغ التشريعات الوطنية في الدول التي لا تنضم إليها.

٦٢- وفيما يتعلق بالتحديات الناشئة عن التطورات التكنولوجية الجديدة، أشارت كندا إلى أن الاتصالات لا تحدها حدود، فهي تتم في أي مكان وأي وقت ومن خلال أي مقدم خدمة أو أي جهاز. وهذا يؤثر قطعاً على إنفاذ القانون، إذ يجب على المحققين في كثير من الأحيان أن يراعوا طبيعة ترتيبات الشراكة وملكية الأصول وأماكن الكيانات، في بيئة معولمة. فما يبدو أنه خدمة واحدة للمستخدم النهائي يكون مؤلّفاً في كل الأحيان تقريباً من خدمات وتكنولوجيات متعددة وأشكال عديدة من الملكية والتوزيع، في ولايات قانونية متعددة.

٦٣- وعلاوةً على ذلك، ذكرت كندا أن السلوك الإجرامي المرتبط بتكنولوجيات المعلومات والاتصالات مستمر في التغير والتكيف؛ إذ تتزايد فيه دوافع الربحية والطابع العابر للحدود الوطنية، وفي كثير من الأحيان طابع التنظيم والتخصص. ويقسَّم النشاط الإجرامي إلى أفعال أصغر يقوم بها في كثير

من الأحيان مجرمون مختلفون يؤدي كل منهم دوراً واحداً في إطار المنظمة الإجرامية. وهذا التخصص لا يؤدي إلى زيادة تعقيد الجريمة وتطورها فحسب بل قد يوفر أيضاً حماية أوسع للمجرمين، لأن بعض مكونات الجريمة قد لا تُشكل جرائم جنائية في بعض الولايات القضائية. وفضلاً عن ذلك، يمكن أن تكون عناصر الجريمة موزعة على ولايات قضائية متعددة. ولا يقتصر أثر الاستفادة من الشبكات الموزعة التي تستخدم التكنولوجيات السيبرانية على استغلال مواطن الضعف في نظم العدالة الوطنية، بل هو يحوِّل أيضاً الولاية الإقليمية للدول وسيادتها إلى أداة تستخدم ضدها.

٦٤- وركَّزت كندا على التحديات التي تواجه تطبيق القوانين الوطنية عندما يكون انطباقها محدوداً إقليميًّا، فذكرت أن القوانين تقتصر عادةً على إقليم معين، مما يشكل تحدِّياً كبيراً نظراً لأن الحدود كثيراً ما تكون بلا أهمية في عالم يتسم بطابع رقمي متزايد. وتواصل تكنولوجيات المعلومات والاتصالات نموها وتطورها بوتيرة مذهلة، بينما تتفشى وتتطور الجريمة السيبرانية (التي تنطوي على إساءة استعمال تكنولوجيات المعلومات والاتصالات أو استغلالها). وتزيد الطبيعة السريعة الزوال والعابرة للأدلة الرقمية من تعقُّد المسألة؛ إذ يُمكن حذف هذه الأدلة أو نقلها بسرعة، بنقرة زر، من ولاية قضائية إلى أخرى. وفضلا عن ذلك، تنبع التعقيدات من مخاوف مهمة تتعلق بالخصوصية وحقوق الإنسان وكيفية استيعابهما في بيئة رقمية. وتوفر القوانين التقليدية بعض صلاحيات التحقيق، التي تظل مفيدة في مكافحة الجريمة السيبرانية، ولكن ثمة حاجة أيضاً إلى أدوات قانونية جديدة أو أكثر تطوراً لضمان إمكانية أن تواكب القدرة على التحقيق وتيرة استغلال المجرمين للتكنولوجيات.

٦٥- وأشارت كندا إلى أن التحديات المرتبطة بالحصول على المعلومات المطلوبة من الدول الأخرى تشمل، من منظور عملي، معرفة مكان وجود البيانات، وما إذا كانت متاحة أم لا، وما إذا كانت في شكلٍ مفهومٍ أم لا. ويعتمد هذا إلى حد ما على نوع البيانات الحاسوبية، فقد تُخزن بعض أنواع البيانات لضمان توافرها على المدى الطويل، بينما قد تُحذف أنواع بيانات أخرى، مثل بيانات حركة المرور، بوتيرة أسرع. وعلى الرغم من أن عمل شركات الاتصالات يمتد لأكثر من دولة فإن هذه الشركات تخضع عموماً لقوانين وطنية أو إقليمية، وقد تختلف آلية الوصول إلى البيانات أو حفظها من دولة إلى أخرى. وتشعر كندا بالقلق إزاء بعض نظم حفظ البيانات، نظراً لتداعياتها الكبيرة على الخصوصية، وعدم وجود دعم من الجمهور لها. وبالنسبة إلى كندا، فإن أنظمة الحفظ الخاصة بالتحقيقات، كما وردت في اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، تُقدم بديلاً حكيماً. كما أن المفاوضات حول البروتوكول الإضافي الثاني للاتفاقية سوف تُعزز آليات التعاون الدولي والحصول على الأدلة في بيئة الحوسبة السحابية.

٦٦- وفيما يتعلق بالتحديات التي يواجهها إطار التعاون الدولي الحالي، ارتأت كندا أن الحصول على الأدلة الرقمية، على الصعيدين المحلي والدولي على السواء، هو الركيزة الأساسية لنجاح التحقيق في الجريمة السيبرانية وأنواع الجرائم الخطيرة الأخرى وملاحقة مرتكبيها قضائيًّا. ومع ذلك فإن عواقب تجاوز الحدود من جانب واحد للحصول على الأدلة الرقمية، بغض النظر عن مدى أهمية هذه الأدلة، يمكن أن تؤدي إلى توتر العلاقات الدولية وتخل بصلاحية هذه الأدلة.

٦٧- وذكرت كندا أن معاهدات المساعدة القانونية المتبادلة تُستخدم أساساً للحصول على تلك المعلومات. غير أن كندا أشارت أيضاً إلى أن العمليات الحالية لا تُنفذ دائماً في الوقت المناسب بما يكفي لضرورات التحقيقات التي تنطوي على استخدام الأدلة الإلكترونية، كما أنها ليست مُصممة لتناسب الكم الهائل من الطلبات الناشئة عن هذا العدد من الجرائم المختلفة التي تترك آثاراً لأدلة رقمية. وبالنسبة لكندا، تمثل آليات المساعدة المتبادلة المنصوص عليها في اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية أفضل وسيلة حالياً لتفعيل التعاون الدولي بين طائفة متنوعة من الدول الأطراف. وعلاوةً على ذلك فإن المفاوضات حول البروتوكول الإضافي الثاني للاتفاقية سوف تزيد من تعزيز التعاون الدولي وتوفِّر الوصول إلى الأدلة الموجودة في بيئة الحوسبة السحابية على أساس تعاهدي.

الصين

٦٨- رحبت الصين باعتماد الجمعية العامة لقرارها ١٨٧/٧٣، المعنون "مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية"، مشيرة إلى أن الجمعية العامة أكدت في عدة قرارات بشأن منع الجريمة والعدالة الجنائية على تعزيز آليات التعاون الدولي في مكافحة الجريمة السيبرانية. وأوصت الصين بأن تُناقش الجمعية العامة موضوع الجريمة السيبرانية في كل دورة من دوراتها، بما في ذلك النظر في الإذن بإنشاء آليات حكومية دولية خاصة ذات صلة. وفي الوقت ذاته، أعربت الصين عن دعمها للمناقشة المستمرة للجريمة السيبرانية في إطار لجنة منع الجريمة والعدالة الجنائية. وأشارت الصين إلى أنها تدعم أيضاً عمل فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية من أجل مناقشة المسائل الموضوعية المتعلقة بمكافحة الجريمة السيبرانية مناقشة مستفيضة، وفقاً لخطة عمل الفريق للفترة ٢٠١٨-٢٠٢١، وتقديم توصيات واستنتاجات إلى لجنة منع الجريمة والعدالة الجنائية. وتشجع الصين أيضاً مختلف المنظمات الإقليمية أو الدولية على مناقشة قضايا الجريمة السيبرانية بنشاط والعمل معاً بشأن تدابير التصدي لها.

٦٩- وفيما يتعلق بالتشريعات الدولية، ارتأت الصين أن اتفاقية الجريمة المنظمة لا يمكن أن تستجيب بفعالية للمتطلبات الجديدة للتعاون الدولي للتصدي للجريمة السيبرانية. وتوجد بعض الاتفاقيات الإقليمية في مجال مكافحة الجريمة السيبرانية، مثل الاتفاقيات التي صاغها مجلس أوروبا ومنظمة شنغهاي للتعاون وجامعة الدول العربية والاتحاد الأفريقي. غير أن التشريعات الدولية لمكافحة الجريمة السيبرانية مجزأة بسبب الاختلافات في نطاق الدول الأعضاء المنضمين إليها وفي محتوى تلك الاتفاقيات. ولذلك ذكرت الصين أن المجتمع الدولي بحاجة ملحة إلى وضع إطار قانوني عالمي لمكافحة الجريمة السيبرانية، وإلى العمل سوياً لمواجهة وضع الجريمة الذي تتزايد خطورته بمرور الوقت، ولا سيما مواجهة التحديات الجديدة الناشئة عن التكنولوجيات الجديدة، مثل الحوسبة السحابية والذكاء الاصطناعي وإنترنت الأشياء والعملات الرقمية المشفرة. وتؤيد الصين الرأي القائل بأن تتفاوض جميع الدول بشأن اتفاقية عالمية لمكافحة الجريمة السيبرانية، مفتوحة العضوية أمام جميع البلدان، وأن تقر تلك الاتفاقية، وذلك تحت رعاية الأمم المتحدة وبالاستفادة من تجربة الاتفاقيات الإقليمية القائمة.

٧٠- وترى الصين أن الاتفاقية العالمية ينبغي أن تُنسِّق بفعالية بين القوانين والممارسات الوطنية الخاصة بمكافحة الجريمة السيبرانية، وأن تتصدى في الوقت المناسب للمشكلات الجديدة الناشئة عن التطور التكنولوجي، وأن توفر حلولاً مقبولة عالميًّا للحوكمة العالمية للجريمة السيبرانية. وفيما يتعلق بنطاق التطبيق، وبالإضافة إلى الجرائم المرتكبة ضد النظم الحاسوبية، ينبغي أن تنطبق الاتفاقية أيضاً على الجرائم المرتكبة أساساً من خلال استخدام الإنترنت وتكنولوجيا المعلومات، فضلاً عن الأنشطة التي تساعد على ارتكاب هذه الجرائم والتدبير لارتكابها. وعلى صعيد إنفاذ القانون والتحقيق، ينبغي أن تنص الاتفاقية على تدابير محددة الأهداف لإنفاذ القانون والتحقيق، وأن تضع ترتيبات لمسائل الشراكة بين القطاعين العام والخاص، مع توضيح التزامات مقدِّمي خدمات الشبكات ومشغليها المتعلقة بالتعاون على منع الجريمة السيبرانية والمساعدة على إنفاذ القانون والتحقيق. ومن حيث التعاون الدولي، ينبغي أن تنظم الاتفاقية الممارسة المتمثلة في الحصول على الأدلة الإلكترونية عبر الحدود، وأن تصمم آلية أكثر كفاءة لجمع الأدلة، استناداً إلى احترام سيادة الدول وحماية حقوق الشركات والأفراد، وأن تضع أحكاماً للجهاز القضائي تتسق مع خصائص الجريمة السيبرانية. وبالإضافة إلى ذلك، ينبغي أن تنص الاتفاقية على أحكام بشأن بناء القدرات والمساعدة التقنية وآليات منع الجريمة.

٧١- وفيما يتعلق بالتعاون الدولي، أشارت الصين إلى أنه قبل استحداث اتفاقية عالمية ينبغي تشجيع الدول على الاضطلاع بالتعاون العملي على مكافحة الجريمة السيبرانية على أساس الاحترام المتبادل والمساواة والمنفعة المتبادلة، وفقاً لاتفاقية الجريمة المنظمة والاتفاقيات الإقليمية والمعاهدات الثنائية. كما أشارت الصين إلى أن بعض الدول أقرت تشريعات وطنية لتجاوز قنوات المساعدة القضائية وقنوات التعاون في مجال إنفاذ القانون، وقامت من جانب واحد بالحصول على بيانات إلكترونية موجودة في الخارج، وهو ما أثر بدوره سلباً على المبادئ الأساسية للقانون الدولي، مثل السيادة وحماية حقوق الأفراد والشركات. وتواصل الصين السعي لتحقيق توازن بين احترام السيادة الوطنية وحماية حقوق الشركات والأفراد وتيسير التحقيقات وتحسين كفاءة الحصول على الأدلة من خلال تحسين إجراءات المساعدة القضائية والتعاون في مجال إنفاذ القانون وابتكار نماذج التعاون.

٧٢- وفيما يخص التدابير الوطنية، أكدت الصين أنه ينبغي للدول أن تتخذ تدابير مقابلة على الصعيد الوطني من أجل مكافحة الجريمة السيبرانية بفعالية، وبخاصة ما يلي:

(أ) تجريم استخدام الإنترنت لأغراض إرهابية، والأنشطة التي تساعد على ارتكاب الجريمة السيبرانية والتدبير لها؛

(ب) وضع نصوص قانونية تحدد التزامات مقدِّمي خدمات الإنترنت ومشغليها فيما يتعلق بالتعاون على منع الجريمة السيبرانية والمساعدة على إنفاذ القانون والتحقيق، وفي الوقت ذاته، توضيح حدود الالتزامات المذكورة أعلاه وكفالة الحقوق القانونية للمؤسسات المعنية والأفراد المعنيين؛

(ج) تعزيز القدرة اللازمة لأجهزة إنفاذ القانون والأجهزة القضائية للتحقيق في الجرائم السيبرانية، ولا سيما لتحسين مواجهة التحديات الناشئة عن التكنولوجيات الجديدة؛

(د) الإقرار بالأثر الإثباتي للبيانات الإلكترونية، والنص على تعريف ونطاق الأدلة الإلكترونية؛

(هـ) توضيح القواعد الخاصة بالحصول على الأدلة الإلكترونية وقبولها، والنص في التشريعات المحلية على وسائل مثل ضبط وسائط التخزين الأصلية وختمها، وجمعها في الموقع، والتفتيش والتجميد عن بُعد؛

(و) مراعاة السمات الخاصة للأدلة الإلكترونية عند تطبيق قواعد الإثبات التقليدية؛

(ز) تعزيز بناء قدرات المكلفين بالحصول على الأدلة الإلكترونية، وتزويد الفرق المهنية بالمعارف القانونية والقدرات التقنية، وصوغ معايير تقنية للحصول على الأدلة الإلكترونية.

كولومبيا

٧٣ وافقت كولومبيا على ضرورة تحسين التنسيق والتعاون بين الدول في مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، وذلك من خلال تقديم المساعدة التقنية إلى الدول النامية لتحسين تشريعاتها الوطنية، وتعزيز قدرة سلطاتها الوطنية على منع هذه الأنشطة الإجرامية والكشف عنها والتحقيق فيها وملاحقة مرتكبيها قضائيًا. ومع ذلك، رأت كولومبيا أن من المهم التمييز بين المسائل المتعلقة بالجريمة السيبرانية والتنظيم الواسع المحتمل لتكنولوجيات المعلومات والاتصالات، الذي من شأنه أن يتعدى التنظيم الجنائي للأفعال غير المشروعة. ولذا فمن المهم للغاية أن يكون هناك فهم واضح لمفهوم وضع أنظمة بشأن استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، ومفهوم أمن المعلومات والاتصالات في سياق الأمن الدولي. وتؤيد كولومبيا وجود شبكة إنترنت مجانية ومفتوحة وآمنة، وترى أن من الضروري أن تمتلك الدول الأدوات اللازمة لتمكينها من التعاون على مكافحة الجريمة السيبرانية، وتعزيز قدراتها الوطنية، وتوطيد تدابير الثقة المتبادلة بين الدول.

٧٤- وذكرت كولومبيا أن هناك تحديات كبيرة في مجال الجريمة السيبرانية، تشمل على سبيل المثال ما يلي: الهوية الرقمية؛ والتعاون مع مقدِّمي خدمات الإنترنت؛ والمسائل المتعلقة بالأدلة الرقمية، وأساليب الحصول عليها، وتخزينها، وتسلسل المسؤولية عنها، والتصديق عليها، والتحقق من صحتها؛ وحماية البيانات، والخصوصية، واحترام حقوق الأفراد وحرياتهم. وبالإضافة إلى ذلك، ترتبط الجرائم السيبرانية ارتباطاً وثيقاً بالجرائم الأخرى العابرة للحدود. ولذلك رأت كولومبيا أن هناك حاجة إلى فهم أعمق للجرائم، وأساليب العمل المستخدمة في ارتكابها، وما إلى ذلك، ولهذا السبب، من المهم تبادل الخبرات والممارسات الجيدة فيما بين الدول من أجل تحسين التدابير الوطنية والدولية لمواجهة هذه الجرائم. فالفجوة الرقمية تجعل بعض الدول أكثر عرضةً للخطر، ويفيد التعاون في هذا الصدد. ويجب تكييف التعاون القضائي الدولي (مثل المساعدة القانونية المتبادلة، وطلبات المساعدة القانونية المتبادلة، ومعاهدات المساعدة القانونية المتبادلة) بحيث يعمل بوتيرة أسرع. ولهذا الغرض، اقترحت كولومبيا وضع بروتوكولات ونماذج تُيسِّر فهم الدول للتعاون القضائي وتسري في إطار التحقيقات والعمليات القضائية.

٧٥- بيد أن كولومبيا رأت أيضاً أنه ينبغي مواصلة مناقشة المسائل المتعلقة بالجريمة السيبرانية، من وجهة نظر تقنية وسياسية، في إطار لجنة منع الجريمة والعدالة الجنائية ومن خلال فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية. وينبغي أن يكون هذا الفريق هو المنتدى الرئيسي، ولا ينبغي إنشاء أفرقة بديلة جديدة تحد من مشاركة البلدان. وقد اتفق فريق الخبراء على خطة عمل من المتوقع أن ينتج عنها في عام ٢٠٢١ تقرير يتضمن خيارات لتعزيز تدابير التصدي الحالية ويقترح تدابير قانونية و/أو تدابير أخرى جديدة.

٧٦- وأخيراً، رأت كولومبيا أن من غير الضروري البدء من نقطة الصفر في التفاوض على اتفاق جديد بشأن الجريمة السيبرانية. فبالنسبة لكولومبيا، من الضروري إعطاء الأولوية لبناء القدرات والتعاون على أساس المعاهدات القائمة، مثل اتفاقية الجريمة المنظمة واتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية.

كوستاريكا

٧٧- أشارت كوستاريكا إلى تاريخها الطويل في الاعتراف بحقوق الإنسان واحترامها وحمايتها. ولذلك فإن الصكوك الدولية التي وقَّعت وصدَّقت عليها لا تنتهك سيادة الدولة.

٧٨- وترى كوستاريكا أنه يجب على المدعين العامين والمحققين في قضايا الجرائم السيبرانية أن يحققوا، لدى مساعدة الضحية، توازناً بين حق الأفراد في الخصوصية والأمن العام؛ ويجب احترام هذه الضمانات عند جمع الأدلة، ولهذا الغرض، يجب تقديم طلب إلى القاضي لإصدار أوامر البحث أو رفع السرية المصرفية أو رفع السرية الضريبية، من بين أمور أخرى. وكل هذا مطلوب لتحقيق النجاح في التحقيقات وضمان مقبولية الأدلة أمام المحكمة.

٧٩- وتتمكن كوستاريكا، بصفتها دولة طرف في اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، من الحصول على تدريب مكثف للممارسين القانونيين، فضلاً عن إمكانية الوصول إلى شبكة نقاط الاتصال "٧/٢٤" وتبادل المعلومات مع مسؤولين آخرين من مناطق أخرى، من أجل الحصول على المعلومات ذات الصلة بالتحقيق وتبادلها آنياً والحصول على الأدلة الرقمية. وفضلا عن ذلك، ونظراً لأن كوستاريكا دولة طرف في اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، فقد أُدرجت في مشروع مجلس أوروبا والاتحاد الأوروبي المعروف باسم "برنامج العمل العالمي الممدَّد بشأن الجريمة السيبرانية" (GLACY+) (غلاسي+)، والذي شاركت بموجبه في ما يلي:

(أ) بعثة التقييم الأولي للمشروع، التي نُفذت في سان خوسيه في الفترة من ٢١ إلى ٢٤ أيار/مايو ٢٠١٨؛

(ب) البعثة الاستشارية بشأن التشريعات المتعلقة بالجريمة السيبرانية والأدلة الإلكترونية، والبعثة الاستشارية بشأن السياسة والاستراتيجية الوطنية المتعلقة بمكافحة الجريمة السيبرانية. وإعداد ومراجعة الإطار التشريعي المتعلق بالجريمة السيبرانية والأدلة الرقمية، وإعداد وتنقيح السياسة الوطنية المتعلقة بالجريمة السيبرانية، الذي نُفذ في سان خوسيه في الفترة من ٨ إلى ١١ تشرين الأول/أكتوبر ٢٠١٨؛

(ج) التدريب القضائي للمدربين بشأن الجريمة السيبرانية والأدلة الإلكترونية، المقدم للقضاة والمدعين العامين والمحامين في سان خوسيه في الفترة من ١١ إلى ١٥ شباط/فبراير ٢٠١٩؛

(د) دورة متقدمة في التدريب القضائي في مجال الجريمة السيبرانية والأدلة الإلكترونية، للقضاة والمدعين العامين وغيرهم من المسؤولين القضائيين (من ١٣ إلى ١٦ أيار/مايو ٢٠١٩)، وبعثة استشارية بشأن التشريعات الإجرائية المتعلقة بالجريمة السيبرانية والأدلة الإلكترونية (يومي ١٦ و١٧ أيار/مايو ٢٠١٩).

٨٠- وعلاوة على ذلك، دعم المشروع مشاركة كوستاريكا في الأنشطة التالية في الخارج:

(أ) حلقة عمل دولية حول استراتيجيات التدريب القضائي بشأن الجريمة السيبرانية والأدلة الإلكترونية، عقدت في سيبو، الفلبين، في الفترة من ١٢ إلى ١٤ كانون الأول/ديسمبر ٢٠١٧؛

(ب) المؤتمر الدولي المشترك لمجلس أوروبا ويوروجست بشأن التعاون القضائي في مجال الجريمة السيبرانية، المعقود في لاهاي، هولندا، يومي ٧ و٨ آذار/مارس ٢٠١٨؛

(ج) الاجتماع الرابع لفريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، المعقود في فيينا في الفترة من ٣ إلى ٥ نيسان/أبريل ٢٠١٨؛

(د) الدورة السابعة والعشرون للجنة منع الجريمة والعدالة الجنائية واجتماع اللجنة التوجيهية لمشروع "غلاسي+"، المعقودين في فيينا في الفترة من ١٤ إلى ١٨ أيار/مايو ٢٠١٨؛

(هـ) اجتماع اللجنة المعنية باتفاقية مكافحة الجريمة السيبرانية، والاجتماع العام التاسع عشر للجنة المذكورة، والاجتماع العام الثاني لفريق صياغة البروتوكول، ومؤتمر "الأخطبوط" بشأن التعاون على مكافحة الجريمة السيبرانية، والحلقة الدراسية حول شبكة نقاط الاتصال "٧/٢٤"، المعقودة في ستراسبورغ، فرنسا في الفترة من ٩ إلى ١٣ تموز/يوليه ٢٠١٨؛

(و) حلقة عمل دولية مشتركة لوحدات التحقيق في الجرائم السيبرانية والسلطات المركزية، عقدت في الفترة من ٢٧ إلى ٣١ آب/أغسطس ٢٠١٨؛

(ز) الاجتماع الرابع لرؤساء الوحدات للفريق العامل المعني بالجريمة السيبرانية، المعقود في ريو دي جانيرو، البرازيل، في الفترة من ٤ إلى ٦ أيلول/سبتمبر ٢٠١٨؛

(ح) المؤتمر المعني بالاقتصاد السري والجريمة السيبرانية، المعقود في ستراسبورغ، فرنسا، في الفترة من ٤ إلى ٧ أيلول/سبتمبر ٢٠١٨؛

(ط) الدورة السادسة لمؤتمر الإنتربول واليوروبول بشأن الجريمة السيبرانية، المعقود في سنغافورة في الفترة من ١٨ إلى ٢٠ أيلول/سبتمبر ٢٠١٨؛

(ي) الاجتماع العام العشرون للجنة المعنية باتفاقية مكافحة الجريمة السيبرانية، والاجتماع العام الثالث لفريق صياغة البروتوكول، واجتماع لجنة مشروع "غلاسي+"، المعقودة في ستراسبورغ، فرنسا، في الفترة من ٢٧ إلى ٣٠ تشرين الثاني/نوفمبر ٢٠١٨؛

(ك) مؤتمر العدالة الجنائية في الفضاء السيبراني، المعقود في بوخارست في الفترة من ٢٥ إلى ٢٧ شباط/فبراير ٢٠١٩؛

(ل) دورة الإنتربول لتنمية مهارات المدربين المعقودة في بوغوتا في الفترة من ٢٥ شباط/فبراير إلى ١ آذار/مارس ٢٠١٩؛

(م) الاجتماع الخامس لفريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، المعقود في فيينا في الفترة من ٢٧ إلى ٢٩ آذار/مارس ٢٠١٩.

٨١- وحاليًّا، صدق ٦٣ بلداً (من قارة أوروبا ومناطق أخرى) على اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، ولهذا تعتبرها كوستاريكا صكاً دولياً له سجل في مجال التنفيذ.

تشيكيا

٨٢- ذكرت تشيكيا أنها صدقت على اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية في عام ٢٠١٣، وأعقبت ذلك بالتصديق في عام ٢٠١٤ على البروتوكول الإضافي للاتفاقية، الذي يركز على تجريم الأفعال المتسمة بطابع العنصرية وكره الأجانب المرتكبة من خلال نظم حاسوبية، ويوسِّع نطاق الاتفاقية وأحكامها الموضوعية والإجرائية وأحكامها المتعلقة بالتعاون الدولي. وبمقدور أي دولة الانضمام إلى الاتفاقية وبروتوكولها الإضافي، وليس فقط الدول الأعضاء في مجلس أوروبا.

٨٣- وتعتقد تشيكيا بقوة أن اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية هي الصك الأكثر كفاءة وحداثة لمعالجة جميع التحديات الناشئة عن ظاهرة الجريمة السيبرانية في جميع أنحاء العالم. ولذلك ترحب تشيكيا بتزايد عدد الدول غير الأعضاء في مجلس أوروبا الذين انضموا إلى الاتفاقية أو نظروا في الانضمام إليها في الفترة الأخيرة، مما يؤكد على طابعها العابر للأقاليم والشامل للجميع وعلى شفافية إجراءات الانضمام إليها. ومن ثم، فبدلاً من صوغ صك جديد، الأمر الذي ستكون له نتائج عكسية بسبب طول عملية اعتماد اتفاقيات الأمم المتحدة والتصديق عليها، ينبغي أن يكون التركيز على التنفيذ الفعَّال للصكوك القانونية القائمة التي تمثلها اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، مع الأخذ في الاعتبار أيضاً مساهمتها الإيجابية في تنسيق المعايير التشريعية الوطنية.

٨٤- وتدعم تشيكيا الخبرات المتخصصة التي يكفل توافرها المكتب المعني بالمخدِّرات والجريمة، والنتائج المحددة التي يحققها، مثل الدليل العملي لطلب الأدلة الإلكترونية عبر الحدود، وتشيد بها. وينبغي أن يبقى التركيز منصباً على الجوانب المتعلقة بخبرة الخبراء في هذه المسألة، وهي خبرة توفرها مداولات فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، الذي يتخذ من فيينا مقراً له، وتنطوي على قيمة فريدة على مستوى الأمم المتحدة.

٨٥- وذكرت تشيكيا أن تعزيز القواعد الإجرائية بهدف مكافحة الجريمة السيبرانية أمر بالغ الأهمية؛ ولا تقل عنه في الأهمية ضمانات حقوق الإنسان وسيادة القانون، بما في ذلك حماية البيانات الشخصية.

٨٦- وأفادت تشيكيا بأنها، إدراكاً منها للعدد المتزايد من التهديدات المرتبطة بالجريمة السيبرانية ولطبيعتها العابرة للحدود بقدر متزايد، تركز على التوعية بالتهديدات السيبرانية والتدريب المتعلق بها، بما في ذلك بناء قدرات الموظفين المكلفين بإنفاذ القانون وتعيين موظفين جدد يملكون الخبرات اللازمة. وفي هذا السياق، تنظر تشيكيا نظرة إيجابية للغاية، من حيث التصدي للجريمة السيبرانية، للشبكة الوطنية للمدعين العامين، التي تعمل على الصعيد الإقليمي وتتخصص في مجال الجريمة السيبرانية، ولتشكيل وحدات شرطة متخصصة في الجريمة السيبرانية. وبالإضافة إلى ذلك، ذكرت تشيكيا أنها تركز على الأدلة الإلكترونية، التي يتزايد حجمها تزايداً ملحوظاً في الإجراءات الجنائية. وقد اعتمدت تشيكيا لائحة قانونية جديدة، تدخل حيز التنفيذ في ١ شباط/فبراير ٢٠١٩ وتضع قواعد صريحة للحفظ المعجل للبيانات الحاسوبية المخزنة المستخدمة في القضايا الوطنية وكذلك القضايا عبر الوطنية.

٨٧- وذكرت تشيكيا أن رقمنة العدالة من أولويات وزارة العدل التشيكية. وقد اعتمدت الحكومة الاستراتيجية المفاهيمية الوطنية لمكافحة الجريمة السيبرانية (تُدرج هذه المسألة في الاستراتيجية المفاهيمية الوطنية لمكافحة الجريمة المنظمة، التي تُحدَّث بانتظام وتصدرها وزارة الداخلية)، وتضع أهدافاً وتدابير محددة لاعتمادها في هذا المجال.

٨٨- وفيما يتعلق بالمساعدة القانونية المتبادلة، أشارت تشيكيا إلى التزايد المستمر في المعالجة الإلكترونية لطلبات المساعدة والعمليات ذات الصلة بها. وذكرت أنه تم تبسيط الإجراءات ذات الصلة من أجل تحقيق قدر أكبر من الكفاءة ومن التعاون السريع، بما في ذلك في مجال تبادل المعلومات بين الدول (على سبيل المثال، من خلال إنشاء قنوات اتصال غير رسمية أو نقاط اتصال داخل شبكة نقاط الاتصال "٧/٢٤" في إطار اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية).

٨٩- وأشارت تشيكيا إلى نفس التحديات المحتملة التي ذكرتها الدول الأخرى، وهي: زيادة إخفاء الهوية (التشفير كمعيار)، وتوافر البرمجيات الضارة والخدمات غير القانونية المدفوعة الأجر (الجريمة كخدمة)، وإمكانية إخفاء أرباح الجريمة في العملات الافتراضية، بالإضافة إلى إخفاء هوية ممتلكي هذه العملات. وأخيراً وليس آخراً، شدَّدت تشيكيا على أن نظام المساعدة القانونية الدولية المتبادلة المذكور أعلاه ليس كافياً للتعامل مع المسائل السيبرانية، لا سيما بسبب بطئه. فمتوسط الوقت اللازم لمعالجة طلب المساعدة القانونية المتبادلة المتعلق بمسائل سيبرانية يبلغ ٢١ شهراً (بين الدول الأعضاء في مجلس أوروبا). ولذا فمن المناسب البدء في مناقشة تعريف الولاية القضائية في الفضاء السيبراني، والوصول المباشر إلى الأدلة الإلكترونية الموجودة على خوادم في الخارج (أو في مكان غير معلوم). وثمة مجال للنقاش حول التعاون المباشر مع مقدِّمي الخدمات الأجانب. وتشارك تشيكيا، بصفتها دولة عضواً في الاتحاد الأوروبي ومجلس أوروبا، في مناقشات عديدة في هذا الصدد، وبخاصة فيما يتعلق بالأوامر الأوروبية المتعلقة بتوفير البيانات الإلكترونية وحفظها، والبروتوكول الإضافي الثاني لاتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية.

جمهورية كوريا الشعبية الديمقراطية

٩٠- رأت حكومة جمهورية كوريا الشعبية الديمقراطية أنه لا ينبغي استخدام تكنولوجيات المعلومات والاتصالات في الأنشطة الإجرامية بطريقة تهدد أو تنتهك الاستقرار السياسي والاقتصادي

والاجتماعي للدول. ورأت أن للتعاون والتنسيق بين الدول أهمية قصوى في منع استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية.

٩١- وأخذا في الاعتبار أن الصكوك القانونية لمنع ومكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية ليست كافية في جميع أنحاء العالم، رأت جمهورية كوريا الشعبية الديمقراطية أنه سيكون من اللازم إعداد قرار من الأمم المتحدة بشأن التعاون على منع استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية، بما يتوافق مع مصالح الدول.

٩٢- وأكدت حكومة جمهورية كوريا الشعبية الديمقراطية على أنه ينبغي مناقشة مسألة استخدام تكنولوجيات المعلومات والاتصالات في الأنشطة الإجرامية في اجتماع فريق الخبراء المفتوح العضوية ذي الصلة الذي تشارك فيه جميع الدول المعنية.

السلفادور

٩٣- رأت حكومة السلفادور أن غياب التشريعات هو التحدي الرئيسي الذي يقف أمام مكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية، وأشارت في هذا الصدد إلى الاعتبارات التالية:

(أ) عدم وجود ضوابط أو تشريعات تنظم توزيع الهواتف المحمولة واستخدام الإنترنت على جميع الناس بوجه عام، وبخاصة الهواتف التي تدفع قيمة مكالماتها مسبقاً، التي يمكن الحصول عليها بسهولة واستخدامها لأي غرض من الأغراض؛

(ب) عدم وجود تشريعات تسمح بالحصول على المعلومات عبر الإنترنت وآنياً بشأن سجلات الاستخدام وتخصيص عناوين بروتوكول الإنترنت العامة والخاصة التابعة لمختلف المشغلين الموجودين في البلد؛

(ج) عدم وجود لوائح تنظم استخدام الأجهزة التكنولوجية، مثل الطائرات الموجهة عن بعد، ومشوشات الإشارات، وأجهزة اعتراض الإشارات، والمعدات المصابة بالفيروسات، وغيرها من المعدات التي تسمح بارتكاب الجرائم السيبرانية؛

(د) عدم وجود لوائح تلزم إداريي الشبكات في المؤسسات العامة أو الخاصة أو غير الهادفة للربح بإنشاء سجلات لاتصالات عملائهم الداخليين وصيانتها وحفظها. ويمكن استغلال غياب هذه اللوائح في ارتكاب الجرائم التقليدية والجرائم السيبرانية.

إستونيا

٩٤- ذكرت إستونيا أن الجرائم السيبرانية واستخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية هما ظاهرتان متناميتان وتنشئان تحديات لكيانات إنفاذ القانون في جميع أنحاء العالم.

٩٥- وأشارت إستونيا إلى أن التعاون الدولي يكتسي أهمية قصوى نظراً إلى أن معظم الجرائم السيبرانية هي ذات طبيعة عابرة للحدود. وكثيراً ما تُخزن الأدلة الإلكترونية المتعلقة

بجريمة ما خارج البلد الذي يُجري التحقيق الجنائي. ومع ذلك، لا يكون التعاون الدولي فعالاً دائماً، وكثيرا ما لا يكون لدى البلدان القانون الموضـــوعي والإجرائي اللازم، أو لا تمتلك أجهزة إنفاذ القانون والقضاء القدرات الكافية.

٩٦- وذكرت إستونيا أن اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية هي، في الوقت الحالي، الصـك الوحيد الملزم قانوناً وذي الأثر العالمي لمكافحة الجريمة السيبرانية. وقد استخدم العديد من البلدان في العالم التي لم تنضم إلى الاتفاقية أحكام تلك الاتفاقية بشأن القانون الموضوعي والإجرائي كليهما وبشـــأن التعاون الدولي كنموذج. ونظراً لأن العديد من البلدان قبلت تلك المعايير وتحقّق بالفعل مستوى معين من المواءمة، فهناك حاجة وإمكانية لإرساء مزيد من التعاون. وتوفر الاتفاقية، بصـفتها صـكًّا دوليًّا ملزماً قانوناً وقائماً بالفعل، معايير ينبغي لذلك أن تتبعها أيضـاً البلدان التي ليس لديها الإطار القانوني اللازم.

٩٧- وترى إســـتونيا أن اتفاقية مجلس أوروبا المتعلقة بالجريمة الســـيبرانية هي أداة فعالة لجمع الأدلة الإلكترونية وتبادلها. ونظراً لأنه يمكن أيضـاً اسـتخدام أحكام القانون الإجرائي للاتفاقية وتدابير الاتفاقية للتعامل مع الجرائم الجنائية الأخرى المتعلقة بالبيانات الحاســـوبية أو الأدلة الإلكترونية، فهي أكثر من مجرد صـك بشـأن الجرائم الإلكترونية. وبالإضـافة إلى ذلك، فبما أنه يمكن اســـتخدام أحكام الاتفاقية للتعامل مع الأدلة الإلكترونية المتعلقة بأي جريمة جنائية، فقد أصـبحت أكثر فائدة وقيمة للدول. ومن ناحية أخرى، أصـبحت الأدلة الإلكترونية والوصـول إليها من أكبر التحديات التي تقف أمام ســـلطات إنفاذ القانون لدى إجراء التحقيقات الجنائية. ونظراً إلى أن الأدلة الإلكترونية تخزن في بلدان أخرى في كثير من الأحيان، فيتعين اســـتخدام تدابير التعاون الدولي وقنواته. وعلى الرغم من أن التعاون الدولي القائم على اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية وغيرها من الصكوك، مثل اتفاقية الجريمة المنظمة، يعمل بصورة مرضية، فإن هناك حاجة لتحسينه وجعله أكثر فعالية.

٩٨- وأشارت إستونيا إلى أنه لعدة سنوات جرت مناقشات بشأن البروتوكول الإضافي الثاني الملحق باتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية. وقد انطلقت المفاوضـات بشـأنه مؤخراً. وسيوفر البروتوكول الإضـافي، الذي سيكون مفتوحاً أمام الدول الأطراف في الاتفاقية، أدوات إضـافية لسـلطات إنفاذ القانون والجهاز القضـائي من أجل تحسـين التعاون الدولي وتوفير قواعد وضـمانات أكثر وضـوحاً. ولذلك، ذكرت إستونيا أن الاتفاقية وأهميتها وتغطيتها على الصـعيد العالمي ستزداد في المستقبل، ويمكن لمزيد من البلدان أن تستفيد منها.

٩٩- وسـلطت إسـتونيا الضـوء على المناقشـات التي جرت بشـأن مكافحة الجريمة السـيبرانية وبناء القدرات على مســـتوى المكتب المعني بالمخدِّرات والجريمة. ومنذ عام ٢٠١١، يناقش فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية التدابير الممكنة للتصدي للجريمة السيبرانية، بما في ذلك كيفية ضـمان تنفيذ الصـكوك الدولية الحالية على نحو أفضـل. وقد أصـبح فريق الخبراء منصـة مفيدة وفعالة للدول لمناقشـة المشـاكل والتحديات ذات الصـلة بالجرائم السـيبرانية وتبادل أفضـــل الممارســـات. وعلى الرغم من عدم توافق الآراء حتى الآن بشـــأن العديد من القضـــايا،

فقد كان هناك تأييد قوي لبناء القدرات. ويواصل فريق الخبراء عمله حالياً وفقاً لخطة العمل المتفق عليها، ويُتوقع أن يقدم استنتاجاته وتوصياته بحلول عام ٢٠٢١.

١٠٠- ورأت إستونيا أن من السابق لأوانه بدء مناقشات موازية وإعداد تقارير موازية على مستوى الأمم المتحدة. فنظراً لأن الموارد محدودة، يجب استخدامها بأكثر طريقة فاعلية؛ ولذلك ينبغي أن يواصل فريق الخبراء الحالي عمله ويكمله في إطار ولايته وخطة عمله. ومع ذلك، كما بدا جلياً من خلال المناقشات الحالية بالفعل، فقد ظهرت إلى الوجود مواضيع فرعية ومواضيع جديدة متعلقة بالجرائم السيبرانية، وتحقيقات إلكترونية، وأدلة إلكترونية، وقد يؤدي ذلك إلى مواصلة فريق الخبراء عمله لما بعد عام ٢٠٢١.

فرنسا

١٠١- أفادت فرنسا بأنها أكدت، في سياق نداء باريس من أجل سيادة الثقة والأمن في الفضاء السيبراني، إلى جانب أكثر من ٦٠ دولة أخرى وعدة مئات من المنظمات الدولية وممثلي المجتمع المدني والقطاع الخاص، دعمها لفضاء سيبراني مفتوح وآمن ومستقر وميسر وسلمي يكون فيه القانون الدولي منطبقاً، بما في ذلك حقوق الإنسان. ومن بين الشروط لتحقيق هذا الهدف مكافحة استخدام الوسائل الرقمية للأغراض الإجرامية.

١٠٢- وفي هذا المجال، ذكرت فرنسا أن لديها نظاماً وطنياً قوياً في مجال مكافحة الجريمة السيبرانية، من حيث القانون المطبق حالياً، وتدابير الوقاية، والموارد المخصصة للمحققين والقضاة لمكافحة هذه الظاهرة بفعالية. وتنبع الآلية جزئياً من اقتباس أحكام اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، التي توفر إطاراً قانونياً دولياً مناسباً ومرناً للتصدي لظاهرة الجريمة السيبرانية عن طريق تعزيز النظم التشريعية الوطنية، ولكن كذلك عن طريق تمهيد الطريق لإقامة التعاون الدولي. وهذه الأحكام إضافية إلى الأحكام المنصوص عليها في اتفاقية الجريمة المنظمة فيما يتعلق بجميع أشكال الجريمة المنظمة عبر الوطنية.

١٠٣- وذكرت فرنسا أنها، على الرغم من هذا الإطار القانوني الدولي المعتمد والنظام الوطني القوي، لا تزال تواجه بعض الصعوبات في مكافحة الجريمة السيبرانية. ويجري تناول هذه الصعوبات في إطار اجتماعات فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، وهي كما يلي:

(أ) عدم تكييف القوانين الوطنية والوسائل المتخصصة في عدد من البلدان لمكافحة الجريمة السيبرانية، ولا سيما، في بعض البلدان، غياب التشريعات الوطنية (في القانون الموضوعي والقانون الإجرائي على السواء) المكيفة لتناسب مسألة الجريمة الإلكترونية، وغياب التدريب والموارد المكيفة، فيما يخص المحققين والجهات الفاعلة في سلسلة الإجراءات الجنائية، لمكافحة الجريمة السيبرانية بفعالية. ومن أجل المساعدة على تعزيز الآليات في هذا المجال، تشارك فرنسا بنشاط في عدد من برامج بناء القدرات، على أساس ثنائي ولكن أيضاً على مستوى الاتحاد الأوروبي ومستوى مجلس أوروبا؛

(ب) غياب التعاون من جانب القطاع الخاص وبعض الولايات القضائية الأجنبية بشأن نقل البيانات، وحتى بشأن حفظ أوامر التجميد في التحقيقات وإجراءات المحاكم. ولا يزال تعاون

مقدِّمي الخدمات جزئيًا في هذه المرحلة (٦٠ في المائة في المتوسط، ولكنه متفاوت جداً حسب الشركاء). ومن الضروري أن يستجيب مقدِّمو الخدمات للطلبات التي ترسلها السلطات المختصة في الدول في سياق التحقيقات والإجراءات الجنائية، دون جعل هذه الا ستجابة مشروطةً بالجنسية المرفقة بعنوان بروتوكول الإنترنت. ومن أجل تحسين هذا الوصول إلى الأدلة الإلكترونية، تشارك فرنسا بنشاط في المفاوضات داخل الاتحاد الأوروبي بشأن اقتراحين تشريعيين قدمتهما المفوضية الأوروبية في ٢٧ نيسان/أبريل ٢٠١٨ ، وهما مشروع لوائح تنظيمية تحدد أحكام وشروط الحصول على الأدلة الإلكترونية ومشروع توجيه يُلزم مقدِّمي الخدمات بتعيين ممثل قانوني مفوض بتلقي الأوامر القضائية والرد عليها. وتشارك فرنسا أيضاً في الفريق العامل المكلف بصوغ البروتوكول الإضافي الملحق باتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية والذي يتناول هذه المسألة أيضاً؛

(ج) التحدي الدائم المتمثل في التكيف مع التكنولوجيات الجديدة، ولا سيما العملات المشفرة، التي تخضع لتنظيم جزئي فقط، مما يؤدي إلى مخاطر كبيرة تتمثل في إخفاء هوية أصحاب التدفقات المالية، ومع الشبكة الخفية، والتشفير، وإنترنت الأشياء. وتجري مناقشة الممارسات الجيدة وتبادلها من أجل تحسين فهم هذه الظواهر، في إطار فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، وعلى نطاق أوسع داخل المكتب المعني بالمخدِّرات والجريمة، وتود فرنسا أن تؤكد على القيمة التنفيذية لهذه المناقشات وعمليات التبادل.

جورجيا

١٠٤- أفادت جورجيا بأنها أجرت منذ عام ٢٠٠٨ إصلاحات أساسية على تشريعاتها الموضوعية والإجرائية وصكوكها المتعلقة بالسياسات من أجل مكافحة الجريمة السيبرانية بفعالية. وتمت مواءمة جميع الإصلاحات الرئيسية مع اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، التي انضمت إليها جورجيا في عام ٢٠١٢.

١٠٥- واعتبرت جورجيا صعوبات الوصول إلى البيانات عبر الحدود تحدِّياً رئيسيًّا في مكافحة الجريمة السيبرانية. وذكرت أن آليات المساعدة القانونية المتبادلة التقليدية عفا عليها الزمن إلى حد بعيد، في وجه الحوسبة السحابية التي تتطور باستمرار. ورأت جورجيا أن إلغاء القيود على الوصول إلى البيانات عبر الحدود أو تخفيفها بطريقة أخرى هو إصلاح لا مفر منه بغية زيادة فعالية التحقيق في الجرائم السيبرانية وملاحقة مرتكبيها. ومع ذلك، يجب أن تنفذ الدول هذه الإصلاحات من خلال صكوك متعددة الأطراف، ويجب أن تكون الصلاحيات الإجرائية المشتركة بين الولايات القضائية مصحوبة بضمانات قوية. واعتبرت جورجيا أن صوغ البروتوكول الإضافي الثاني الملحق باتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية فرصة مهمة في هذا الصدد.

١٠٦- وأفادت جورجيا بأنها شاركت في السنوات الأخيرة في عدد من مشاريع بناء القدرات التي نفذها و/أو دعمها مجلس أوروبا (مشاريع الشراكة الشرقية) والاتحاد الأوروبي وحكومة الولايات المتحدة. وفي إطار هذه المشاريع، تم تدريب المئات من المهنيين العاملين في مجالي إنفاذ القانون والقضاء، واعتمدت الحكومة عدداً من الوثائق السياساتية التي استنارت بخبرات متعددة الجنسيات في مجال الجرائم السيبرانية والأدلة الإلكترونية والأمن السيبراني.

١٠٧- وفيما يتعلق بالقانون الموضوعي، أفادت جورجيا بتجريمها الوصول غير القانوني إلى الأجهزة واعتراض سبيلها، والتدخل في البيانات والنظم، فضلاً عن إساءة استخدامها، وذلك بموجب المواد من ٢٨٤ إلى ٢٨٦ من القانون الجنائي لعام ١٩٩٩، واتساقاً مع المواد من ٢ إلى ٦ من اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية. وتمت دون أي تحديات كبيرة ملاحقة مرتكبي جميع الجرائم ذات الصلة بالفضاء السيبراني باعتبارهم ارتكبوا جرائم تقليدية. فعلى سبيل المثال، تشهد جريمة الاحتيال السيبراني تزايداً في الآونة الأخيرة، ولم تجد المحاكم الجورجية أي صعوبات في تطبيق تشريعات الاحتيال التقليدية على هذه الحالات.

١٠٨- وفيما يتعلق بالقانون الإجرائي، أفادت جورجيا بأنها نفذت في تشريعاتها، منذ عام ٢٠١٠، جميع الصلاحيات الإجرائية المنصوص عليها في اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، بما في ذلك أوامر توفير الوثائق والبيانات، وجمع بيانات حركة الاتصالات في الوقت الحقيقي، واعتراض المحتوى، في حين كان العديد من الصلاحيات الأخرى موجوداً بالفعل في تشريعاتها. وفي غضون ذلك، اعتمدت جورجيا ضمانات إجرائية قوية، بما في ذلك اشتراط التفويض القضائي فيما يتعلق بجميع الصلاحيات الإجرائية المنطوية على اقتحام الخصوصية، وشرط التناسب، والحد من استخدام صلاحيات إجرائية معينة (لا تُستخدم إلا في حالات الجرائم الخطيرة)، وشرط استخدام أقل خيار اقتحاماً من بين الصلاحيات الإجرائية المتاحة.

١٠٩- وفيما يتعلق بتعاون مقدِّمي خدمات الإنترنت الأجانب، أُشير إلى أن وكالات إنفاذ القانون الجورجية تسعى بنجاح للحصول على معلومات المشتركين من مختلف شركات الإنترنت العالمية (فيسبوك وآبل ومايكروسوفت، إلخ.)، فيما يتعلق بالخدمات المقدمة في جورجيا. وعلى سبيل المثال، كانت جورجيا من بين أفضل ١٠ بلدان في العالم من حيث معدل الكشف عن البيانات، حيث بلغ معدل الكشف عن البيانات في الفيسبوك ٩٤ في المائة فيما يتعلق بالطلبات الخاصة بالإجراءات القانونية خلال الفترة ٢٠١٧-٢٠١٨. وفي عام ٢٠١٨ استحدثت جورجيا أمراً دولياً لتوفير الوثائق والبيانات، خول للقضاة في جورجيا إصدار أمر بتوفير الوثائق والبيانات بشأن الأشخاص الموجودين أو الكيانات الموجودة خارج الولاية القضائية الإقليمية لجورجيا إذا استُوفيت الشروط التالية مجتمعة: موافقة الشخص موضوع الأمر على الكشف الطوعي عن البيانات الإلكترونية؛ وسماح البلد الذي يستضيف الكيان الأجنبي بإجراء هذا الكشف، من خلال قوانينه أو من خلال سياساته التنفيذية. ويجب أن يحصل المدعي العام على هذه الأوامر من المحكمة، ويجب أن تُحال من خلال مسؤول مفوض من قبل النائب العام. ولا تترتب عن عدم الامتثال لمثل هذه الأوامر أي مسؤولية قانونية. ووفقاً للمادة ١٨ من اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، استخدمت جورجيا الأوامر الدولية لتوفير الوثائق والبيانات فيما يتعلق بفيسبوك ومقدِّمي خدمات دوليين آخرين فيما يتعلق بالخدمات المقدمة في جورجيا.

ألمانيا

١١٠- أشارت ألمانيا إلى التطور التكنولوجي الذي أدى إلى إحداث تغيرات مستمرة في المجتمع. فذكرت أنه يهيئ فرصاً جديدة يستفيد منها كل فرد، بل أيضاً المجتمع ككل. ومن ناحية

أخرى، ينشـــئ التقدم التكنولوجي تحديات جديدة، حيث تُســـتخدم الإمكانات التكنولوجية للتواصل والتصرف بسرعة وعلى نطاق عالمي لأغراض غير مشروعة. ولذلك، رأت ألمانيا أن من المهم مواجهة هذه التحديات ومحاربة السلوك الإجرامي. وهذا يتطلب إطاراً قانونيًّا وطنيًّا متطوراً بما فيه الكفاية، مع إقامة تعاون فعال أيضاً عبر الحدود الوطنية.

١١١- وترى ألمانيا أن أي حل على المستوى الدولي ينبغي أن يكون مصـمما خصيصـاً لمواجهة التحديات المحددة الناجمة عن تكنولوجيات المعلومات والاتصالات، وينبغي أن يعالج الحل مسائل سرية نظم المعلومات وسلامتها والوصول إليها (ما يسمى الجرائم السيبرانية الأساسية). ولن يكون من المجدي أو المرغوب فيه محاولة وضـع أحكام تنطبق على جميع الجرائم التي ترتكب باسـتخدام الحاسـوب أو عبر الإنترنت. ويجب أن تكون الأحكام المتعلقة بالجرائم السـيبرانية الأسـاسـية مرنة بما فيه الكفاية لمواكبة التطورات التكنولوجية. ومن ناحية أخرى، هناك حاجة إلى آليات لتبادل البيانات عبر الحدود للتحقيق في الجرائم السيبرانية وملاحقة مرتكبيها ومعاقبتهم.

١١٢- وشـددت ألمانيا على أن اتفاقية مجلس أوروبا المتعلقة بالجريمة السـيبرانية مناسـبة تماما للتصـدي بفعالية للتحديات القائمة في مجال مكافحة الجريمة السـيبرانية. وفي هذا الصـدد، أثبتت الاتفاقية أنها أداة مناسبة لمكافحة الجريمة السيبرانية، وهي مفتوحة أيضـاً أمام البلدان الثالثة. ولاحظت ألمانيا أن الاتفاقية تحظى بقبول واســع من جانب العديد من الدول باعتبارها صــكاً دولياً رئيســياً في مكافحة الجريمة السـيبرانية، وقد اسـتخدمتها السـلطات في ألمانيا أيضـاً كمرشـد للتشـريعات المحلية. ولا يزال تعريف الاتفاقية المحايد تكنولوجيًّا للجرائم مواكباً للزمن. وترى ألمانيا أن ذلك التركيز بصــفة عامة على الجرائم التي ترتكب ضــد ســرية نظم المعلومات وســلامتها وإمكانية الوصــول إليها هو، على وجه التحديد، ما ســاهم في المسـتوى العالي لقبول الاتفاقية على الصـعيد العالمي. ولذلك ترى ألمانيا أن من الضـروري الحفاظ على فهم لمفهوم الرجوع إلى مجموعة أسـاسـية من الجرائم السـيبرانية. وفي المقابل، ينبغي توخي الحذر عند توسيع نطاق "الجريمة السيبرانية" لتشمل أشكال السلوك التي لا تُستخدم فيها أجهزة الحاسوب إلا كوسيلة لارتكاب جرائم عامة. فمن الممكن ارتكاب أي جريمة تقريباً باستخدام أجهزة الحاسوب، لكن هذا لا يجعلها "جريمة سيبرانية".

١١٣- وأشــارت ألمانيا إلى أن التكيف مع آخر التطورات ينبغي أن يســتند إلى اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، كما هو الحال حاليًّا فيما يخص التفاوض بشأن البروتوكول الإضـافي الثاني، في مجال تأمين الأدلة الإلكترونية. وسيهدف البروتوكول الثاني إلى تحسين التعاون بين الأطراف في مجال تعقب الجرائم الســيبرانية وفي مجال تأمين الأدلة الإلكترونية. ولذلك، لا تدعم ألمانيا الدعوات لوضــع صك دولي جديد بشأن الجريمة السيبرانية.

١١٤- وفضلاً عن ذلك فإن فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية يقوم بإعداد دراســة شــاملة عن تحديات مكافحة الجريمة الســيبرانية. وتُجرى مناقشــات فنية حول تحديات الجريمة السيبرانية منذ عام ٢٠١١ ضمن فريق الخبراء المذكور. وترى ألمانيا أن فريق الخبراء هو العملية الرئيسية على مسـتوى الأمم المتحدة بشـأن موضـوع الجريمة السـيبرانية وينبغي أن يظل كذلك. وينبغي تفادي العمليات الموازية المتعلقة بقرارات الجمعية العامة والازدواجية المحتملة للجهود، حيثما أمكن ذلك.

١١٥- وأكدت ألمانيا أنه ينبغي إيلاء اهتمام خاص لتنفيذ تشريعات الجريمة السيبرانية وإحراز تقدم فعال على أرض الواقع، بما في ذلك من خلال تقديم المساعدة التقنية. ولا يوجد افتقار إلى المعايير الدولية الملائمة، وقد وضعت الدول الأعضاء أيضاً، في إطار القانون الجنائي، تشريعات موضوعية بشأن الجرائم السيبرانية، من أجل تنفيذ المعايير القائمة. ويتمثل التحدي الذي ينبغي أن يواجهه الآن فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية في كيفية تزويد الكيانات المعنية بإنفاذ القانون بإطار قانوني سليم وبالموارد اللازمة لتأمين الأدلة الإلكترونية، وفي الوقت نفسه، تقييد صلاحيات إنفاذ القانون من خلال شروط وضمانات تستند إلى سيادة القانون وحماية الحقوق والحريات الأساسية.

غانا

١١٦- أفادت غانا بأنَّ لديها حاليًّا تشريعين رئيسيين بشأن الأدلة السيبرانية والإلكترونية، وهما: قانون الاتصالات الإلكترونية لعام ٢٠٠٨ (القانون رقم ٧٧٥) وقانون المعاملات الإلكترونية لعام ٢٠٠٨ (القانون رقم ٧٧٢).

١١٧- وعلى الرغم من أن النائب العام هو المدعي الرئيسي في جميع الجرائم الجنائية في غانا، فهناك أجهزة أخرى، مثل الشرطة، تلاحق مرتكبي الجرائم تحت سلطة النائب العام. غير أن مكتب النائب العام يلاحق مرتكبي القضايا التي تحيلها إليه الشرطة. وتحيل الشرطة إلى هذا المكتب عدداً أقل من القضايا المتعلقة بالجرائم السيبرانية أو الجرائم المرتكبة باستخدام الحاسوب، ولذلك لوحظت بعض المشكلات والنكسات في ملاحقة مرتكبي هذه القضايا.

١١٨- وأفادت غانا بأن الشرطة، التي هي هيئة التحقيق الرئيسية، تفتقر إلى الأدوات اللازمة، لأن جميع أدوات مختبر التحليل الجنائي لمكافحة الجريمة السيبرانية قد انتهت صلاحيتها. ولذلك تحال التحقيقات إلى مختبرات التحليل الجنائي الخاصة، مع ما يرتبط بذلك من تكلفة، وتحال هذه التكلفة في كثير من الأحيان إلى المدعي. وفي معظم الأحيان يؤثر عدم دفع تكلفة الفحص تأثيراً سلبيًّا على المحاكمة. وعندما تُدفع التكلفة في نهاية المطاف، تحتاج الشرطة إلى وقت طويل لتحصيل المبلغ المطلوب. ومن شأن التأخير في الدفع أن يؤثر على إصدار التقرير في الوقت المناسب، مفضياً إلى تأخير المحاكمة. ومختبر الجرائم السيبرانية هو المختبر الوحيد الذي يخدم البلد بأسره، إلا أنه يفتقر إلى الموظفين الأكفاء اللازمين، مما يؤثر كثيراً على مخرجاته.

١١٩- وأفادت غانا بأنَّ لديها حاليًّا قرارين متباينين من المحكمة العليا بشأن الوصول إلى محتويات أي جهاز إلكتروني. فوفقًا لأحد القرارين، لا تحتاج وكالة مكلفة بإنفاذ القانون إلى مذكرة قضائية للوصول إلى محتويات الجهاز المشتبه فيه؛ ويركز القرار الآخر على ضرورة الحصول على مذكرة قضائية للوصول إلى المحتويات. ولتحقيق الانسجام والوضوح بين هذين القرارين المتعارضين، أُحيلت القضية إلى محكمة الاستئناف العليا في غانا لتحسم فيها.

١٢٠- ويمكن أن تحدث الجريمة السيبرانية، بحكم طبيعتها، عبر عدة حدود دولية. ولهذا السبب، يمكن أن تكون معلومات هامة لازمة لملاحقة القضية بنجاح متاحة في ولاية قضائية أخرى. وأكدت غانا أن الحصول على هذه المعلومات يمكن أن يكون مستحيلاً أو بطيئاً في كثير من

الأحيان. وفي غياب معاهدة للمساعدة القانونية المتبادلة بين الأطراف، قد لا يكون الحصول على المعلومات ممكناً. وفي حالة وجود معاهدة لتبادل المساعدة القانونية، تكون عملية نقل المعلومات بطيئة وبيروقراطية في كثير من الأحيان، مما يتسبب في تأخير التحقيقات ثم النظر في القضية.

هنغاريا

١٢١- أفادت هنغاريا بأن عدد ضحايا إساءة استخدام تكنولوجيات المعلومات والاتصالات ازداد على الصعيدين الوطني والدولي. وبوجه عام، يفضِّل المجرمون استخدام التطبيقات المستندة إلى الإنترنت (مثل فايبر وسناب شات ومسنجر وواتس آب وآي ميسج)، على استخدام التكنولوجيا القائمة على النظام العالمي للاتصالات المتنقلة، ولا توجد حاجة إلى خبرة خاصة لاستخدام هذه التطبيقات. وترى هنغاريا أن هذا يشكل تحدِّياً للشرطة ووكالات إنفاذ القانون الأخرى.

١٢٢- وأشارت هنغاريا أيضاً إلى أن تكنولوجيات المعلومات والاتصالات الحديثة تُستخدم كوسيلة لارتكاب جرائم مثل الاحتيال عبر الإنترنت ونشر المواد الإباحية المتعلقة بالأطفال عبر الإنترنت والاتجار بالمخدِّرات الاصطناعية عبر الإنترنت. وتُستخدم وسائل التواصل الاجتماعي أيضاً في الوصول بسهولة إلى الأطفال وارتكاب جرائم الاستغلال الجنسي، في شكل صور أو مقاطع فيديو. وبالإضافة إلى ذلك، تُستغل الشبكة الخفية لشراء الأسلحة والمخدِّرات والمستندات المزورة، بصفة غير مشروعة ومع إخفاء الهوية. وتُستخدم عملة البيتكوين لسداد ثمن تلك المنتجات غير المشروعة والخطرة. وعلاوة على ذلك، يمكن أن تشكل تقنية الطباعة الثلاثية الأبعاد تهديداً ناشئاً فيما يتعلق بإنتاج الأسلحة أو قطع غيارها.

١٢٣- وشدَّدت هنغاريا كذلك على أن معظم الجرائم المتصلة بتكنولوجيا المعلومات والاتصالات لها سمات دولية، ويشترك فيها في كثير من الأحيان أكثر من بلدين. ويسبب ذلك صعوبات للسلطات عندما يُشترط الحصول على إنابة قضائية لتبادل المعلومات بين تلك الدول. وقد تواجه السلطات صعوبات عند التحقيق في الجرائم ذات الصلة، وذلك، على سبيل المثال، لأن استخدام خدمات الشبكات الخاصة الافتراضية يزيد من صعوبة تحديد بيانات المستخدمين الشخصية الصحيحة. ومن ثم فهناك حاجة إلى بذل مزيد من الجهود في مجال الوقاية.

١٢٤- وترى هنغاريا أنه سيتعين على مقدِّمي خدمات الإنترنت الوطنيين التعاون الوثيق مع القطاع العام، بما فيه الشرطة. ونظراً لعدم وجود معايير دولية بشأن التزامات مقدِّمي خدمات الإنترنت فينبغي للسلطات الوطنية أن توائم ما على مقدِّمي الخدمات هؤلاء من التزامات بشأن تسجيل المعلومات وتخزينها وتبادلها (الاحتفاظ بالبيانات) فيما يتعلق بالاتصالات، بما في ذلك نوع البيانات، وأدنى وأقصى مدة للحفاظ على البيانات، وتفاصيل الاتصال. وينبغي أيضاً توحيد الحد الأدنى من المعلومات المشترط لإرسال طلب من الشرطة إلى مقدِّمي خدمات الإنترنت، لأن مقدِّمي الخدمات يتوقعون عادةً توفير معلومات لمعالجة الطلب أكثر مما تملكه السلطات.

١٢٥- وتوصي هنغاريا باعتبار نقاط الاتصال "٧/٢٤" التي تحددها كل دولة عضو على حدة في إطار اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية ممارسة جيدة. كما اقترحت استخدام قناة اتصالات الإنتربول لتبادل المعلومات.

١٢٦- وأبلغت هنغاريا بأن تشفير وسائل الاتصال التقنية الشخصية مفيد في منع الجريمة السيبرانية. غير أن المجرمين يستغلون التشفير لإخفاء هويتهم ومكان وجودهم. ويمثل فك التشفير تحدِّياً آخر للشرطة. وسيكون من الضروري زيادة الوعي حول الأمن السيبراني في القطاعين العام والخاص. وعلاوة على ذلك فإن تحسين البنية التحتية لتكنولوجيا المعلومات في المؤسسات وتدريب موظفي القطاعين العام والخاص أمران ضروريان لتحسين القدرات على المستوى الوطني.

١٢٧- وسلطت هنغاريا الضوء على أن التعاون الجيد بين مختلف الدول أمر لا غنى عنه لحل القضايا بنجاح. ولليوروبول دور مهيمن في أوروبا في مجال التعاون. ويمكن استخدام اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية باعتبارها ممارسة جيدة من حيث الحصول على الأدلة الإلكترونية من مقدِّمي الخدمات في البلدان الأخرى.

١٢٨- ونظراً لأن الجريمة السيبرانية تمثل تحدِّياً آخذاً في التطور يؤثر على كل بلد، اعتبرت هنغاريا المتطلبات التالية ضرورية لمواجهتها بكفاءة:

(أ) الزيادة إلى أقصى حد ممكن من عدد البلدان التي لديها تشريعات محلية ملائمة ومتوافقة متعلقة بالجرائم السيبرانية تدعم التعاون الدولي؛

(ب) بناء آليات التعاون، والثقة، والمهارات، اللازمة لتبادل البيانات لأغراض التحقيق في الجرائم السيبرانية وملاحقة مرتكبيها والحد منها؛

(ج) التأكد من عدم وجود ملاذات آمنة للمجرمين، وزيادة قدرات سلطات إنفاذ القانون والسلطات القضائية، وخصوصاً في مجال تأمين الأدلة الإلكترونية.

١٢٩- وفيما يتعلق بالمساعدة التقنية، ذكَّرت هنغاريا بمشروع الدراسة الشاملة عن الجريمة السيبرانية، مشيرة إلى وجود توافق واسع في الآراء على ضرورة بذل جهود لبناء القدرة على التصدي للجريمة السيبرانية. وذكرت أن البرنامج العالمي المعني بالجريمة السيبرانية والتابع للمكتب المعني بالمخدِّرات والجريمة قائم بالفعل، وتكتسي مشاركة جميع الدول الأعضاء فيه أهمية كبرى. وهناك أيضاً عدد من البرامج الأخرى لبناء القدرات تدعمها هنغاريا، مثل البرامج التي يديرها مجلس أوروبا والاتحاد الأوروبي. وبالنسبة لهنغاريا، هناك حاجة إلى ضمان أن تكون جميع مشاريع بناء القدرات محددة الأهداف ومنسقة بفعالية من أجل تفادي الازدواجية، وأن تكون مصمَّمة ومرتبة زمنيًّا على نحو مناسب لتلبية احتياجات التعاون الدولي وضمان تحقيق نتائج مستدامة، وأن تُقيّم بفعالية لقياس أثرها.

١٣٠- وفيما يتعلق بخيارات تعزيز التدابير الوطنية والدولية الحالية للتصدي للجريمة السيبرانية واقتراح حلول جديدة، رأت هنغاريا أن اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية تمثل نموذجاً صالحاً للتشريعات الوطنية وإطاراً قيماً للتعاون الدولي. وبما أن الاتفاقية مفتوحة أمام الدول غير الأعضاء في مجلس أوروبا للانضمام إليها فهي توفر أداة مرنة للقيام بهذه المهمة (أي وضع تدابير التصدي الوطنية وتعزيز التعاون الدولي). ولا تؤيد هنغاريا الدعوات لوضع صك دولي جديد بشأن الجريمة السيبرانية.

١٣١- وترى هنغاريا أن فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية هو العملية الرئيسية على مستوى الأمم المتحدة بشأن الجريمة السيبرانية، وينبغي أن يظل كذلك، على الأقل حتى عام ٢٠٢١. وقد حقق الفريق نتائج، بما في ذلك بشأن الإصلاحات التشريعية، على أساس المعايير الدولية القائمة، وكذا من حيث بناء القدرات. وقد أظهرت السنوات الست الماضية تقدماً جيداً فيما يتعلق بالإصلاحات التشريعية، ولا سيما في الحالات التي استخدمت فيها البلدان المعايير الدولية القائمة. ووضع العديد من المنظمات برامج لبناء القدرات. وتلزم مواصلة هذه الجهود وتوسيع نطاقها.

١٣٢- وتقترح هنغاريا أن تدعم الدول الأعضاء المكتب المعني بالمخدِّرات والجريمة في العمل على اتخاذ الإجراءات التالية لمكافحة تهديد الجريمة السيبرانية:

(أ) تحسين مهارات الشرطة ومهارات أجهزة إنفاذ القانون، من خلال التدريب العام والمتخصص؛

(ب) تقديم المساعدة التقنية في البلدان النامية؛

(ج) تحليل الفجوات في التعاون الدولي، لتحديد المجالات ذات الأولوية؛

(د) دعم حملات توعية الجمهور الرامية إلى تعزيز منع الجريمة وبناء تعاون المجتمع المدني وقطاع الأعمال مع أجهزة إنفاذ القانون؛

(هـ) تعزيز الآليات التشغيلية القائمة، مثل شبكة نقاط الاتصال "٧/٢٤"؛

(و) جمع البيانات عن تهديدات الجرائم السيبرانية؛

(ز) القيام بدور مستودع للممارسات الفضلى ودراسات الحالات الإفرادية في مجال التصدي للجريمة السيبرانية.

الهند

١٣٣- أشارت الهند إلى الزيادة المطردة في الجرائم السيبرانية، والتي تثير قضايا وتحديات جديدة لأجهزة إنفاذ القانون. وذكرت أن الجرائم السيبرانية تختلف كثيراً عن الجرائم التقليدية، من حيث طبيعتها ونطاقها ووسائلها وأدلتها وأنشطتها. ومن ثم فإن تبادل المعلومات في الوقت الحقيقي أو شبه الحقيقي ضروري لجمع الأدلة اللازمة لتقديم مرتكبي الجرائم السيبرانية إلى العدالة. والأفعال الإجرامية المتعلقة بالجرائم السيبرانية معقدة تقنيًا وقانونيًا. وليست للفضاء السيبراني والجريمة السيبرانية حدود مادية، ومن ثم فإن التعاون الدولي أساسي للتحقيق وجمع البيانات والأدلة والمعاقبة، في جملة أمور.

١٣٤- وأفادت الهند بأنه، وفقا لمكتبها الوطني لسجلات الجريمة، سُجلت ٦٢٢ ٩ جريمة متعلقة بالجرائم السيبرانية في عام ٢٠١٤، و٥٩٢ ١١ جريمة في عام ٢٠١٥، و٣١٧ ١٢ جريمة في عام ٢٠١٦. وخلال عام ٢٠١٦، كان الدافع وراء ٤٨,٦ في المائة من قضايا الجرائم السيبرانية المبلغ عنها تحقيق مكاسب غير مشروعة (٩٨٧ ٥ قضية من أصل ٣١٧ ١٢ قضية)، يليها الانتقام (٨,٦ في المائة، أو ١ ٠٥٦ قضية)، وخدش حياء النساء (٥,٦ في المائة، أو ٦٨٦ قضية).

١٣٥- وأشارت الهند كذلك إلى الإطار القانوني والمؤسسي الوطني للجرائم السيبرانية، وذلك بالإشارة إلى أن قانون تكنولوجيا المعلومات لعام ٢٠٠٠، بصيغته المعدلة في عام ٢٠٠٨، وقانون العقوبات الهندي، يوفران الإطار القانوني للتعامل مع التجارة الإلكترونية والأمن السيبراني والجرائم السيبرانية والإرهاب السيبراني. كما أن القوانين الوطنية واسعة النطاق للغاية، وتتناول معظم القضايا المتعلقة بالجرائم السيبرانية.

١٣٦- وأشارت الهند أيضاً إلى أن الأنواع المختلفة من إساءة استخدام تكنولوجيات المعلومات والاتصالات في شكل جرائم سيبرانية "أساسية" وجرائم سيبرانية مدعومة بتكنولوجيات المعلومات والاتصالات تفرض تحديات متفاوتة تتعين معالجتها. وتشمل إساءة استعمال تكنولوجيات المعلومات والاتصالات عمليات اقتحام المواقع الإلكترونية وتشويهها، والفيروسات أو الأكواد الخبيثة، وهجمات الحرمان من الخدمة، والهجمات الموزَّعة المواقع للحرمان من الخدمة، والاختراق، والتصيُّد الاحتيالي، والإرهاب السيبراني، واستغلال الأطفال في المواد الإباحية، والابتزاز الجنسي، وانتحال الهوية، والمطاردة السيبرانية والمضايقة السيبرانية، والأخبار الزائفة والدعاية، والمقامرة غير المشروعة، وبيع الأدوية والمخدِّرات المزيفة، والتجسس السيبراني، وما إلى ذلك.

١٣٧- وأشارت الهند إلى أن الجرائم السيبرانية تُرتكب باستخدام أدوات تكنولوجيا المعلومات والاتصالات الحديثة، مثل البرمجيات الخبيثة ("malware")، وشبكات السيطرة على الأجهزة الإلكترونية (botnets)، وتوجيه الرسائل الطبقي "onion routing"، وحتى الهواتف المحمولة العادية التي تستخدم لأغراض الاستدراج الموجَّه.

١٣٨- وأشارت الهند إلى التحديات التالية التي تعيقها فيما يتعلق بمواجهة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية:

(أ) أن استخدام أشكال عديدة من البرمجيات الخبيثة وشبكات السيطرة على الأجهزة الإلكترونية (البوتنيت) يتيح للمجرمين تجنب الضوابط التقنية، من قبيل برامج مكافحة الفيروسات (antivirus software) وبرامج تنقية محتويات الإنترنت (Internet filters)، وكذلك تجنب اكتشاف المجرمين من قبل أجهزة إنفاذ القانون؛

(ب) استخدام هذه التكنولوجيات مع التشويش وإخفاء الهوية والقدرة الحسابية ومنع تعقب مصدر الجريمة أو مرتكبها؛

(ج) أن خدمات الشبكات الخاصة الافتراضية تسمح بالاتصال عبر الإنترنت مع إخفاء الهوية؛

(د) الأدوات المتعددة التي تسمح للمجرمين بإخفاء هوياتهم على الإنترنت أو بعدم إمكانية تعقبهم. ومن بين هذه الأدوات، تشكل شبكات السيطرة على الأجهزة الإلكترونية (البوتنيت) التحدي الأكبر، لعدد من الأسباب؛

(هـ) أن التصدي للجريمة السيبرانية يتطلب معرفة قانونية متخصصة، ومجموعات من مهارات التحقيق، وأدوات التحليل الجنائي، والحنكة التحليلية؛

(و) فيما يتعلق بالتحديات القانونية، أن الطبيعة عبر الوطنية للجريمة السيبرانية تؤدي إلى تعقُّد البت في الولاية القضائية، مما يجعل التحقيق والملاحقة القضائية أمراً صعباً. ويؤدي الافتقار إلى مواءمة التشريعات فيما بين البلدان إلى صعوبات في التحقيق في جرائم الإرهاب السيبراني ومحاكمة مرتكبيها.

١٣٩- وركزت الهند على التحديات القائمة على الصعيد الدولي والتي تعوق التعاون على مكافحة إساءة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، وأشارت إلى ما يلي:

(أ) أن الوقت عامل جوهري في التحقيقات في الجرائم السيبرانية، ولذلك يلزم تحديد إطار زمني لتقديم الأدلة الرقمية فيما يخص التعاون المتعدد الأطراف بين الدول؛

(ب) أن معاهدات المساعدة القانونية المتبادلة تركز في المقام الأول على سيناريوهات ما بعد الجريمة، في حين أن تبادل المعلومات السريع ضروري لمكافحة الجريمة السيبرانية، على خلاف الجرائم التقليدية. وهناك حاجة أيضاً إلى تعاون دولي في مجال منع الجريمة السيبرانية؛

(ج) أن معاهدات المساعدة القانونية المتبادلة لا تحتوي على شرط بشأن تلبية متطلبات الحالات العاجلة، وهو مطلب رئيسي لمكافحة الجرائم السيبرانية، وهذا الجانب يحتاج إلى مناقشة؛

(د) أن التعاون الدولي في مجال الأمن السيبراني ضروري بالنظر إلى الانتشار الواسع النطاق لاستخدام تكنولوجيات التحكم والقيادة، وشبكات السيطرة على الأجهزة الإلكترونية (البوتنيت)، والشبكة العميقة؛

(هـ) أن قوانين حماية الخصوصية تعرقل تبادل المعلومات.

إيران (جمهورية-الإسلامية)

١٤٠- فيما يتعلق بالتحديات في مجال مواجهة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، أفادت جمهورية إيران الإسلامية بأن عدم امتثال مقدِّمي خدمات الإنترنت والشبكات الاجتماعية الأجنبية يمثل مشكلة أولى. وذكرت أن الإنترنت ووسائل التواصل الاجتماعي تساهم بقدر كبير في تحسين حياة الإنسان، إلا أن تكنولوجيات الاتصالات السلكية واللاسلكية الملتحمة والقابلة للنقل والمتاحة في كل مكان وزمان عبر الإنترنت ووسائل التواصل الاجتماعي دفعت المجرمين، وخاصة الجماعات الإجرامية المنظمة، إلى استخدام هذه التكنولوجيات بقدر متزايد للأغراض الإجرامية. ويؤدي مقدمو خدمات الإنترنت والشبكات الاجتماعية دوراً لا غنى عنه في منع ومكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، وتحديداً في مجال جمع الأدلة الإلكترونية وحفظها، فضلاً عن إنفاذ القانون.

١٤١- وترى جمهورية إيران الإسلامية أن تدابير التصدي العادلة والمرنة تعتمد اعتماداً كبيراً على تنظيم الأنشطة التي تجري في وسائل التواصل الاجتماعي. وتنظم السلطات الوطنية الأنشطة التي تجري في وسائل التواصل الاجتماعي المملوكة للقطاع الخاص الإيراني تنظيماً جيداً، بما يتسق مع القانون الإجرائي الخاص بالجرائم الحاسوبية. ويمكن لسلطات إنفاذ القانون الكشف عن الأنشطة الإجرامية التي تجري في الفضاء السيبراني، وجمع الأدلة الإلكترونية وحفظها، والتحقيق الفعال في استخدام

تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية وملاحقة مرتكبيه. إلاَّ أنَّه، نظراً لطبيعة الجريمة السيبرانية التي تتجاوز الحدود الإقليمية، تواجه السلطات تحديات خطيرة في ملاحقة مرتكبي الجرائم التي ترتكب باستخدام الخوادم الموجودة في بلدان أخرى والمملوكة للقطاعات العامة أو الخاصة الأجنبية. وفي معظم الحالات، لا تتعاون خدمات الشبكات الاجتماعية الأجنبية في المسائل الجنائية. ويمثل عدم امتثال هذه الهيئات لطلبات الدول للتعاون تحدِّياً لمنع الجريمة ومكافحتها على نحو فعال، ويعرِّض سيادة القانون للخطر على المستويين الوطني والدولي.

١٤٢- وفيما يتعلق بالتدابير القسرية الانفرادية، أفادت جمهورية إيران الإسلامية بأنها، بحكم موقعها في منطقة تعاني من الجريمة المنظمة، تواجه عقبات دولية أمام التعاون على المستوى الدولي في المسائل الجنائية، لا سيما في مجال مواجهة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية. وذكرت أن التدابير القسرية الانفرادية، التي تضر بالتصدي الجماعي لهذه الجرائم، تخل بتعاون البلدان مع سلطات إنفاذ القانون الإيرانية في التحقيق في الجرائم وملاحقة مرتكبيها، ولا سيما الجرائم المرتكبة من خلال استخدام تكنولوجيات المعلومات والاتصالات، وكذلك في نقل الأدوات التكنولوجية اللازمة للحفاظ على الأدلة الإلكترونية وإجراء فحوص التحليل الجنائي الرقمية. وتؤدي التدابير القسرية الانفرادية، باعتبارها انتهاكاً صارخاً للمبادئ الأساسية للقانون الدولي المنصوص عليها في ميثاق الأمم المتحدة، إلى عرقلة التعاون الفعال على مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، وليس ذلك فحسب، بل تضعف أيضاً سيادة القانون، وبذلك تشجع المجرمين على مواصلة أنشطتهم غير المشروعة. ولا تزال إزالة العوائق الدولية ضرورية، ليس فقط لمكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية مكافحة فعالة ولكن أيضاً لضمان الأمن الجماعي للدول. وجمهورية إيران الإسلامية ملتزمة بمحاربة الجريمة المنظمة. وهي تدعم التعاون الدولي على مكافحة الجريمة السيبرانية الذي ييسره المكتب المعني بالمخدِّرات والجريمة، وتؤكد على الحاجة إلى تعزيز المساعدة التقنية في هذا المجال.

١٤٣- وفيما يتعلق بعدم وجود إطار دولي شامل للجميع، أكدت جمهورية إيران الإسلامية على الحاجة إلى إطار قانوني دولي بشأن الجريمة السيبرانية. وذكرت أنه، في الوقت الراهن، لا يزال الافتقار إلى إطار دولي سليم وشامل للجميع بشأن الجريمة السيبرانية يمثل تحدِّياً في مجال مواجهة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية. وتتطلب طبيعة الجريمة السيبرانية تصدياً مرناً وجماعيًّا يناسب السياق المحدد، من خلال صك دولي، مع مراعاة الحاجة إلى مواكبة تطور التكنولوجيا وأساليب العمل الجديدة للجماعات الإجرامية المنظمة. وتفتقر الصكوك الحالية المتعلقة بالجريمة السيبرانية والتي وضعها عدد محدود من الدول إلى المتطلبات اللازمة لهذا التصدي، الأمر الذي بدوره يجعلها غير قابلة للتطبيق على المستوى الدولي.

١٤٤- وأثنت جمهورية إيران الإسلامية على العمل الواسع النطاق والقيم الذي يقوم به المكتب المعني بالمخدِّرات والجريمة، لا سيما فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، وأعربت عن تقديرها له. وأشارت إلى أنها ما زالت تدعم جهود المكتب في هذا المسعى وتعتقد أن اعتماد اتفاقية عالمية بشأن الجريمة السيبرانية تحت رعاية الأمم المتحدة سيحقق مصالح الدول على

أفضل وجه وسيخفف من التحديات المواجهة في مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية.

١٤٥- وفيما يتعلق بالإطار القانوني الخاص بالجريمة السيبرانية، أشارت جمهورية إيران الإسلامية إلى أن الجرائم التقليدية التي يسهِّل استخدام الفضاء السيبراني ارتكابها، أو يُمكِّن منه، يُعاقب عليها، داخل أراضيها، بموجب قانون العقوبات الإسلامي. بيد أن مجلس الشورى الإسلامي (البرلمان) وضع واعتمد تشريعاً بشأن الفضاء السيبراني من أجل منع ومكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، وتحديداً الجريمة السيبرانية، بطريقة فعالة ومرنة. ويتناول التشريع أيضاً الأدلة الإلكترونية، نظراً لدورها الذي لا غنى عنه في ملاحقة مرتكبي الجرائم السيبرانية.

١٤٦- ومن حيث القوانين الجنائية الموضوعية، أشارت جمهورية إيران الإسلامية إلى قانون التجارة الإلكترونية لعام ٢٠٠٤. وبموجب هذا القانون، اعتُرف بالعقود الإلكترونية وبتدابير حماية الأجهزة للأسرار التجارية، وتم تجريم إساءة استخدام البيانات الشخصية، وانتهاك حقوق المستهلك، والكشف عن المعلومات التجارية السرية في المعاملات الإلكترونية، وكذلك الاحتيال والتزوير باستخدام الحاسوب. وذُكر أن قانون جرائم الحاسوب لعام ٢٠٠٩ تضمن أحكاما بشأن التجريم ومسؤولية الأشخاص الاعتباريين. وتم بموجب هذا القانون، من بين أمور أخرى، تجريم الوصول إلى البيانات والنظم الحاسوبية دون إذن، وبث محتوى إباحي، والعمل ضد سلامة وسرية البيانات، والسرقة والاحتيال المتعلقين بالحاسوب. ويعاقب القانون على هذه الجرائم بالغرامة والسجن لمدة تصل إلى ١٥ سنة. وتعتبر المادة ٢٦ ارتكاب الجرائم السيبرانية بطريقة منظمة أو على نطاق واسع أو استهداف النظم الحاسوبية الخاصة بالخدمة العامة ظروفًا مشدِّدة. ويخضع هذا القانون حاليًّا للتدقيق لتكييفه مع أساليب العمل الجديدة للمجرمين وتزويد سلطات إنفاذ القانون بإطار قانوني مرن.

١٤٧- ومن حيث القانون الإجرائي، أشارت جمهورية إيران الإسلامية إلى القانون الإجرائي المتعلق بالجرائم السيبرانية، الذي كان سابقاً جزءاً من قانون جرائم الحاسوب لعام ٢٠٠٩، والذي دُمج لاحقاً في قانون الإجراءات الجنائية مع إدخال تعديلات طفيفة عليه. ويغطي هذا التشريع مسائل مثل الاختصاص القضائي، والفروع المتخصصة المعنية بالتحقيق، وملاحقة مرتكبي الجرائم السيبرانية، وشروط وإجراءات البحث عن الأدلة الإلكترونية والبيانات والنظم الحاسوبية وضبطها. ويكفل القانون مراعاة الأصول القانونية وحماية الخصوصية. ولا تسمح المادتان ٦٧١ و٦٧٢ بإصدار أوامر المحكمة بشأن البحث عن البيانات وضبطها إلا عندما تكون هناك أسباب قوية ومعقولة لإصدار الأمر، الذي يجب تنفيذه بحضور المالك القانوني. ويمنع القانون أي عملية ضبط تنطوي على التسبب في أضرار في الممتلكات أو تؤدي إلى تعطيل الخدمة العامة، كما هو منصوص عليه في المادة ٦٧٩.

العراق

١٤٨- أشار العراق إلى أن استخدام الإنترنت هو أحد خصائص الحضارة الحديثة، ومقياس للتنمية والاندماج في الحضارة الإنسانية والتفاعل مع البلدان الأخرى. ونتيجة لذلك، تحدث حاليًّا ثورة في أساليب التبادل العلمي والثقافي. وقد أصبح الإنترنت قناة ضخمة للمعرفة، تساهم في ربط وتماسك المجتمعات والأفراد بما يتجاوز الحدود الجغرافية والمحدِّدات السياسية والاجتماعية

والمذاهب الفكرية، وفي تقارب الحضارات وتبادل الأفكار بين الجنسيات واللغات والأديان. وهذا يؤدي إلى النظر في القيم والمبادئ التي يجب أن تحكم محتوى الإنترنت، ولا يزال موضوعاً مهماً ومثيراً للجدل. وفي حين أن البلدان النامية لا تشكل سوى نسبة مئوية صغيرة من مستخدمي الإنترنت في العالم فإن قضية المحتوى ذات أهمية كبيرة لهذه البلدان، بسبب أثرها على مجتمعاتها. وعلى الرغم من أن إحدى قيم الإنترنت هي المساواة والحرية فإن خصوصية مجتمعات البلدان النامية تتطلب أن تأخذ الحكومات هذه الخصوصية في الاعتبار وتحاول حمايتها من التوجهات والثقافات المتعددة.

١٤٩- وشدد العراق على أن تقارب الشعوب له أيضاً تأثير على عولمة الجريمة والسلوك الإجرامي، بما في ذلك الجرائم التي تمس المجتمعات المحافظة في البلدان النامية. ومن ثم فهناك حاجة إلى وضع لوائح بشأن أخلاقيات الإنترنت تتناسب مع خصوصيات كل مجتمع على حدة. ولذا فمن شأن وضع المواثيق أن يحدد محتوى للإنترنت ينطبق على كل بلد أو منطقة على حدة وفقاً للمعايير الأخلاقية المناسبة، ولن يكون هذا المحتوى متاحاً بالضرورة للجميع.

١٥٠- وسلط العراق الضوء على أنه، في العقد السابق، انتشر استخدام التطبيقات القائمة على الإنترنت انتشاراً هائلاً. ولذلك أصبح من الضروري ضبطها وتنظيمها. وبعض التطبيقات الحديثة (للترفيه أو الألعاب) يتطلب من المشتركين السماح بالوصول إلى سلسلة من المعلومات الشخصية. ونظراً لأن مستوى الوصول إلى المعلومات المتوفرة على الشبكة يحدِّد مستوى خصوصية المستخدمين على نفس الشبكة فإن العراق يشجع مصممي ومروجي التطبيقات على وضع معايير تتطلب منهم إظهار دليل على الغرض من الوصول إلى المعلومات أو الأجهزة. وهناك نهج آخر يتمثل في جعل متطوعين يقومون بتقييم التطبيقات على أساس معايير متفق عليها، من أجل زيادة الثقة في التطبيقات السليمة وتقليل الثقة في التطبيقات الخبيثة.

١٥١- وأبلغ العراق بأن من المعروف أن الأخبار تنتشر بسرعة على الإنترنت بين جمهور واسع قد لا يكون قادراً على التحقق من مصدر تلك الأخبار أو لا يهتم به. ويجب تشجيع الشركات على التعامل مع الأخبار بدقة وموضوعية وعدم نشر أخبار أو مقاطع فيديو مزيفة تزيد من الكراهية بين المجتمعات. وقد يكون مطلوباً أيضاً، لا سيما في الوقت الراهن، تقليل مصادر مقاطع الفيديو والوسائط الصوتية والمكتوبة التي تحض على الكراهية. وسيكون من المفيد أيضاً تعزيز التعاون بين الجهات التي ترعى وسائط الأخبار ووسائل التواصل الاجتماعي والفرق التطوعية المعنية بتقييم الأخبار والتي تقوم بتحليل الأخبار واستكشاف مصداقيتها.

١٥٢- وفيما يتعلق بالمخاطر التي يتعرض لها الأطفال على الإنترنت، أشار العراق إلى أن مجتمع المعلومات يوفر عالماً رقميًّا فوريًّا بنقرة على لوحة مفاتيح. ويمكن الوصول إلى مستوى غير مسبوق من الخدمات والمعلومات من خلال أجهزة الحاسوب أو الأجهزة المحمولة المزودة بإمكانية الوصول إلى الإنترنت. وتتناقص بسرعة حواجز مثل تكاليف الأجهزة وإمكانية الوصول إلى الإنترنت. وتوفر هذه التطورات للأطفال والشباب فرصاً لا مثيل لها ليصبحوا "مواطنين رقميين" في عالم الإنترنت الذي لا حدود له أو قيود. وتتضمن المخاطر ونقاط الضعف الموجودة على الإنترنت والمتعلقة باستخدام الإنترنت للأطفال والشباب ما يلي:

(أ) التعرض للمحتوى غير المشروع والضار، مثل المواد الإباحية، والمقامرة، ومواقع إيذاء النفس، ومشاهد العنف والإرهاب وغير ذلك من المحتوى غير اللائق، والاتصال بالمستخدمين الآخرين. وفي معظم الحالات، لا يتخذ مشغلو المواقع التي تحتوي على هذا المحتوى تدابير فعالة لتقييد وصول الأطفال؛

(ب) الاستهداف من خلال الرسائل التطفلية والإعلانات لترويج المنتجات الموجهة إلى فئات عمرية واهتمامات معينة؛

(ج) الاستخدام الخارج عن الإرادة والمفرط للإنترنت وللألعاب التي تتاح عبر الإنترنت؛

(د) التخويف والمضايقة والتهديد والابتزاز؛

(هـ) التعرض للتطرف والعنصرية وغيرهما من أنواع الكلام والصور التمييزية؛

(و) تمويه سن الشخص؛

(ز) إساءة استخدام البيانات الشخصية والكشف عن المعلومات الشخصية الذي يؤدي إلى خطر الأذى الجسدي وانتهاك حقوق الشخص نفسه أو حقوق الآخرين، من خلال قرصنة المحتوى (خاصة الوسائط) وتحميله دون إذن، بما في ذلك الصور غير اللائقة.

١٥٣- وركز العراق على قضايا الأمن العام، فأكد على أن شركات الإنترنت الكبرى تقدم خدمات وفرصاً عظيمة للتنمية الاجتماعية والاقتصادية. ولا تكون المنصات القائمة على الإنترنت مناسبة للتنمية الاجتماعية والاقتصادية إلا عندما يعرض مستخدموها أنفسهم بصدق. بيد أنهم عندما يستخدمون اسماً مجهولاً أو مزيفاً، وهو أمر شائع جداً في وسائل التواصل الاجتماعي، فقد يسيئون استخدام هذه الخدمات ويقومون بأنشطة إجرامية مثل نشر خطاب الكراهية وإيديولوجيات الإرهاب ورسائل التهديد والابتزاز. ويشكل ذلك تحدِّياً صعباً في مجال الأمن العام بالنسبة لحكومات البلدان النامية، خاصةً عندما تفتقر إلى التقنيات الرفيعة المستوى وتسعى إلى الحصول على التعاون من شركات الإنترنت. ويمكن لهذه الشركات جمع المعلومات العامة والشخصية لعملائها، كجزء من عملية إدارة حساباتهم، ويمكنهما من خلال هذه المعلومات رصد مواقعهم الجغرافية وأرقام هواتفهم وغيرها من المعلومات المفيدة، ويمكنهما مكافحة الجرائم وإنقاذ الأرواح. وهذا يتطلب من أصحاب المصلحة تحمل نصيبهم من المسؤولية، بتعاون وثيق بينهم، لمواجهة هذه التحديات وضمان توفير خدمات مستمرة وأكثر أماناً من أجل تحقيق أهداف التنمية المستدامة.

١٥٤- وأشار العراق أيضاً إلى التحديات الأخرى التي تُواجه في مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، وتشمل هذه التحديات ما يلي: عدم وجود اتفاقية عالمية بشأن الجريمة السيبرانية؛ وصعوبة فهم الأدلة الرقمية، أو فهم جزء منها، وسهولة إتلافها أو إخفائها؛ وكون الجرائم السيبرانية تتجاوز الحدود الجغرافية، إلى جانب وجود مسافة جغرافية بين المجرم والضحية؛ وافتقار السلطات المختصة إلى التدريب المناسب وبناء القدرات اللازمين لمكافحة الجريمة السيبرانية؛ وكون الخبرة والدراية في مجال التحقيق في الجرائم السيبرانية من قبل المنظمات غير الحكومية والكيانات الحكومية الأخرى لا تُستخدم على نحو كاف؛ وعدم توفر بنية تحتية

إلكترونية كافية لمكافحة الجريمة السيبرانية؛ وصعوبة الحد من الطريقة التي ترتكب بها الجريمة السيبرانية أو التضييق عليها.

١٥٥- وخلص العراق إلى أن هناك حاجة متزايدة وملحة إلى زيادة التعاون بين أصحاب المصلحة بغية ضمان مستقبل رقمي آمن.

أيرلندا

١٥٦- أشارت أيرلندا إلى مشروع الدراسة الشاملة عن الجريمة السيبرانية، الذي لوحظ فيه وجود توافق واسع في الآراء على أن ضرورة بذل جهود لبناء القدرات لمكافحة الجرائم السيبرانية. وذكرت أنه، في الواقع، كان هناك اتفاق واسع النطاق في الاجتماع الخامس الذي عقده مؤخراً فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية على أن عدم كفاية القدرات ربما يمثل في الوقت الحالي أهم تحدٍ في التعامل الفعال مع الجريمة السيبرانية.

١٥٧- وسلطت أيرلندا الضوء على أن هناك تحدِّياً كبيراً فيما يتعلق ببناء القدرات ينشأ من أن أي جريمة قد تنطوي على عنصر سيبراني، وخاصة فيما يتعلق بالأدلة الإلكترونية. ولذا فمن الضروري أن يتمتع جميع المحققين والمدعين العامين والقضاة بالخبرة ذات الصلة في هذا المجال. ومن المهم أيضاً إعداد الممارسين المتخصصين، عند الاقتضاء. ومما يؤكد هذا التحدي أن الطبيعة الدولية للجريمة السيبرانية تعني أن الافتقار إلى القدرة الكافية في دولة واحدة يمكن أن يؤثر سلباً على القدرة على مكافحة الجريمة ليس في تلك الدولة فحسب بل في أي دولة.

١٥٨- وللتغلب على هذه التحديات، أشارت أيرلندا إلى أن من المهم مواصلة وتوسيع نطاق برامج بناء القدرات على المستويين الوطني والدولي. ويجب أن تكون مشاريع بناء القدرات هذه محددة الأهداف ومنسقة بفعالية لتجنب ازدواجيتها وضمان استدامتها. كما ينبغي تصميمها بطريقة مناسبة فيما يتعلق بالمتطلبات المحددة للنظم القانونية المختلفة للدول واحتياجاتها للتعاون الدولي. وأخيراً، ينبغي تقييم هذه المشاريع تقييماً دقيقاً بغية الاستفادة من هذا التقييم في المشاريع المستقبلية.

١٥٩- وأقرت أيرلندا بما للمنتدى الذي يوفره فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية من قيمة لتبادل المعارف والخبرات فيما يتعلق بالتحديات التي تطرحها الجريمة السيبرانية. وعلى وجه الخصوص، أشارت أيرلندا إلى أن طبيعة فريق الخبراء كمنتدى للخبراء، وليس كمنتدى سياسي، كانت مفتاح نجاح فريق الخبراء. ولذلك تعتقد أيرلندا أن فريق الخبراء ينبغي أن يظل هو العملية الرئيسية على مستوى الأمم المتحدة بشأن الجريمة السيبرانية.

١٦٠- وأشارت أيرلندا كذلك إلى أن التحديات الرئيسية التي تصادف فيما يتصل بالجريمة السيبرانية لا تتعلق بالإطار القانوني الدولي في هذا المجال. ولذلك أكدت أيرلندا أنها لا تؤيد مقترحات وضع صك دولي جديد بشأن الجريمة السيبرانية. وذكرت أن اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، التي هي أول صك دولي ملزم في مجال مكافحة الجريمة السيبرانية، أثبتت أنها مرنة إزاء البيئة التكنولوجية المتغيرة على الدوام وأنها عالمية في نطاقها. وتتجلى الطبيعة العالمية للاتفاقية في مشاركة ٦٣ دولة طرفاً من جميع المجموعات الإقليمية الخمس للأمم المتحدة، وفي أن

عدداً كبيراً من الدول التي ليست أطرافاً في الاتفاقية تنفذ قوانين بشأن الجريمة السيبرانية مصممة على غرار الاتفاقية. وفي هذا الصدد، ذكرت أيرلندا أن الأحكام الموضوعية للاتفاقية منفذة إلى حد بعيد في القانون الأيرلندي، وأن أيرلندا ملتزمة بالتصديق على الاتفاقية في أقرب فرصة ممكنة.

١٦١- وأعربت أيرلندا عن دعمها الكامل للجهود الجارية للتفاوض حول بروتوكول إضافي ثان ملحق باتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية بشأن تعزيز التعاون الدولي، مما سيزيد من تحسين الاتفاقية ويساعد على ضمان أن تبقى أهم صك دولي بشأن الجريمة السيبرانية.

إسرائيل

١٦٢- أكدت إسرائيل أنه بالنظر إلى أن المنصات المملوكة ملكية خاصة لشركات تكنولوجيا المعلومات يمكن أن تستخدم أيضاً في النشاط الإجرامي، فإن أحد أهم التحديات التي تواجهها الدول اليوم هو التفاعل بين الدولة والشركات الخاصة. وفي هذا الصدد، هناك حاجة إلى النظر في إطار عمل مناسب ومتوازن لتمكين الشركات من تقديم خدمات موثوقة لعملائها، مع الحفاظ على خصوصيتهم وحرية التعبير وتشجيع الابتكار، من ناحية، وإيجاد إطار مناسب للتعاون مع سلطات إنفاذ القانون في حالات النشاط الإجرامي، من الناحية الأخرى.

إيطاليا

١٦٣- أفادت إيطاليا بأن الشرطة الوطنية الإيطالية، من خلال دائرة شرطة البريد والاتصالات، مسؤولة عن منع الجريمة السيبرانية ومكافحتها. ويتولى المركز الوطني لجرائم تكنولوجيا المعلومات وحماية البنية التحتية الحيوية، الذي يعمل على مدار الساعة وطوال أيام الأسبوع، والذي أنشئ ضمن دائرة شرطة البريد والاتصالات، المسؤولية الحصرية عن منع ومكافحة جرائم تكنولوجيا المعلومات (ذات الطابع المشترك أو المنظم أو الإرهابي) المرتكبة ضد البنية التحتية الحيوية. ويُنجز المركز هذه المهمة بنجاح من خلال المراقبة المستمرة للإنترنت. ويوفر المركز المذكور خدمات الحماية السيبرانية على أساس الاتفاقات المبرمة بين إدارة الأمن العام والكيانات التي تدير البنية التحتية الحيوية (شراكة بين القطاعين العام والخاص). ويتضمن المركز أيضاً نقطة الاتصال الإيطالية لحالات الطوارئ التقنية والتشغيلية المتعلقة بالأحداث الإجرامية عبر الوطنية.

١٦٤- وفيما يتعلق بالإرهاب السيبراني، أفادت إيطاليا بأن دائرة شرطة البريد والاتصالات مسؤولة عن منع ومكافحة التحريض على الإرهاب الجهادي عبر الإنترنت، وخاصة من خلال مراقبة الإنترنت بدعم من الوسطاء اللغويين والثقافيين وبالتعاون مع المديرية المركزية لشرطة المنع وقسم التحقيقات العامة والعمليات الخاصة بالشرطة. وعلاوة على ذلك، وعلى الرغم من اختصاصات الشرطة الوطنية وقوات الدرك (Carabinieri Corps) والشرطة المالية الإيطالية "Guardia di Finanza"، وهي الجهات المكلفة بأنشطة التحقيق في مجال الإرهاب والتخريب، فإن دائرة شرطة البريد والاتصالات تقوم باستمرار بتحديث قائمة المواقع الإلكترونية المستخدمة لأغراض إرهابية. وعلاوة على ذلك، تقوم الشرطة المالية الإيطالية، من خلال وحدة الاحتيال التكنولوجي الخاصة، باكتشاف

ومنع ومكافحة الجرائم المرتكبة باستخدام الأدوات السيبرانية في مسائل التهرب الضريبي، والجرائم الجمركية، وعمليات الاحتيال المتعلقة بموارد الاتحاد الأوروبي، وجرائم العملة والتزوير.

١٦٥- وعلى المستوى الأوروبي، تعمل دائرة شرطة البريد والاتصالات كنقطة اتصال وطنية لوحدة اليوروبول المعنية بإحالة محتويات الإنترنت، والمسؤولة عن تلقي تقارير الدول الأعضاء عن محتوى الدعاية الإرهابية الجهادية عبر الإنترنت.

١٦٦- وفيما يتعلق بالقطاع المصرفي، كُلفت دائرة شرطة الاتصالات البريدية، بناءً على توجيه من وزير الداخلية، بمهمة منع ومكافحة الجريمة السيبرانية التي تُستخدم فيها تقنيات معينة للتصيد الاحتيالي أو الاختراق أو تُستخدم فيها البرمجيات أو المعدات التكنولوجية من أجل سرقة واستنساخ واستخدام الهويات الرقمية ورموز استخدام الخدمات المصرفية عبر الإنترنت وبطاقات الدفع المستخدمة في المعاملات الإلكترونية، لأغراض احتيالية.

١٦٧- وفيما يتعلق بالعملات المشفرة، أشارت إيطاليا إلى أن هذه العملات كثيراً ما تُستخدم كوسيلة للدفع لشراء السلع والخدمات. وتتميز هذه المعاملات بسرية هوية المُصدرين والمستفيدين الحقيقيين على السواء، مما يشجع على استخدامها لأغراض غير مشروعة (في إطار التصيد الاحتيالي وفيروسات التشفير من نوع فيروسات طلب الفدية، على سبيل المثال).

١٦٨- وأشارت إيطاليا إلى أن مركزاً وطنيًّا لمكافحة استغلال الأطفال في المواد الإباحية على الإنترنت أنشئ في دائرة شرطة البريد والاتصالات. ويقوم المركز باستمرار بتحديث قائمة سوداء لإرسالها إلى مقدِّمي خدمة الإنترنت لكي يتمكنوا من منع مستخدمي الإنترنت في إيطاليا من الوصول إلى الفضاءات الافتراضية المحتوية على مواد الاعتداء الجنسي على الأطفال الصادرة من بلدان أخرى. ويعتمد المركز أيضاً على تعاون جميع الجهات الفاعلة المؤسسية والاجتماعية المشاركة في تثقيف القاصرين وحمايتهم بغرض تنفيذ استراتيجيات مشتركة لمكافحة هذه الظواهر وتطوير البحوث والتقنيات الجديدة لدعم التحقيقات. وتستند منهجيات التحقيق المبتكرة التي تتبناها دائرة شرطة البريد والاتصالات إلى أكثر التقنيات السرية تطوراً من أجل إحباط أنظمة إخفاء الهوية ومن أجل التمكن من تحديد هوية الأشخاص المعنيين والقاصرين الذين يتعرضون للإساءة. وتوجَّه التحقيقات أيضاً إلى الشبكات الاجتماعية، التي تُظهر أشكالًا جديدة من الاستدراج وأحداث التنمر الإلكتروني، فضلاً عن جرائم التشهير عبر الإنترنت (معظمها ضد الأشخاص ذوي المسؤوليات المؤسسية) والمطاردة والمضايقة والتهديدات والتحريض على الكراهية.

اليابان

١٦٩- ركزت اليابان، أولاً، على تحدٍ متميز ناشئ عن طبيعة الجريمة السيبرانية. فالجرائم السيبرانية تتسم بطابع سرية الهوية إلى حد بعيد ولا تترك سوى القليل من الأثر. وعلاوة على ذلك، لا تقف أمام الجرائم السيبرانية أي قيود إقليمية أو زمنية، ويمكن أن تسبب أضراراً فورية لعدد لا يحصى من الضحايا. ولذلك، يمكن للمجرمين ارتكاب الجرائم السيبرانية بسهولة من خلال استغلال البلدان الضعيفة التي ليست لديها تدابير مضادة فعالة، واستخدام هذه البلدان كأساس للقيام بأنشطة الجريمة السيبرانية ضد ضحايا في جميع أنحاء العالم. ومن ثم فإن أحد التحديات المشتركة بين المجتمع الدولي

يتمثل في سد هذه الفجوة في القدرات بحيث تكون لدى كل بلد تدابير مضادة ملائمة ومناسبة لمكافحة الجرائم السيبرانية لكي لا يُترك للمجرمين أي مجال للمناورة.

١٧٠- وترى اليابان أن التحدي المذكور أعلاه يتفاقم من خلال جانبين هما الافتقار إلى الأطر القانونية والافتقار إلى بناء القدرات. ويمثل الافتقار إلى أطر قانونية صارمة بشأن كل من القانون الموضوعي والإجرائي لمكافحة الجريمة السيبرانية في بعض الدول الأعضاء تحدِّياً كبيرا. فعلى سبيل المثال، تشكل البلدان التي لا يوجد لديها تشريع كاف لتجريم استحداث الفيروسات الحاسوبية، أو الدول التي ليس لديها تشريع يتيح الحفاظ على بيانات الإنترنت، تحدِّياً خطيرًا في مكافحة الجريمة السيبرانية. ومن أجل مواجهة هذا التحدي، ينبغي للمجتمع الدولي أن يساعد الدول الأعضاء على سن تشريعات جديدة قادرة على معالجة الأشكال الجديدة والناشئة للجريمة السيبرانية وعلى الصمود أمام مرور الزمن.

١٧١- وترى اليابان أن أكثر السبل شمولاً وفعالية من حيث التكلفة لتحقيق هذا الهدف هي استخدام الأطر القانونية الدولية القائمة. وسيؤدي هذا لا إلى تفادي ازدواجية العمل فحسب، بل أيضاً سيمكِّن الدول الأعضاء من سن تشريعات ذات معايير مقبولة بالفعل على نطاق واسع. وسيسد ذلك الفجوة بين الدول الأعضاء، كما سييسر التعاون الدولي (على سبيل المثال، سيتم الوفاء بمبدأ التجريم المزدوج على نحو أفضل بين الدول الأعضاء ذات الأطر القانونية المماثلة). وفي هذا الصدد، حظيت اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية بقبول واسع من المجتمع الدولي، وهي توفر نقطة بداية مشتركة. وقد أثبت سن القوانين بما يتوافق مع هذه الاتفاقية فعاليته في اليابان. فعلى سبيل المثال، تم بنجاح تطبيق جريمة "إنشاء سجلات كهرومغناطيسية للأوامر غير المأذون بها" (المادة ١٦٨-٢ من القانون الجنائي)، التي اشتُرعت في عام ٢٠١١ اتساقاً مع الاتفاقية، على أشكال جديدة وناشئة من الجرائم السيبرانية، مثل إنشاء برمجيات طلب الفدية، لم تكن متوخاة في وقت الاشتراع.

١٧٢- وأكدت اليابان أنه حتى في حالة وجود أطر قانونية متينة فإن عدم قدرة وكالات إنفاذ القانون والجهاز القضائي على الاستفادة منها من شأنه أن يعيق بصورة خطيرة أي جهود لمكافحة الجريمة السيبرانية. وتمثل قدرة أجهزة إنفاذ القانون على اكتشاف الأدلة الإلكترونية والتحقيق فيها وجمعها أمراً لا غنى عنه في هذا الصدد. ويجب أن يفهم الجهاز القضائي أيضاً أساليب عمل مرتكبي الجرائم السيبرانية وأن يفهم الأدلة الإلكترونية فهماً صحيحاً بهدف اتخاذ قرار صحيح بشأن مقبولية هذه الأدلة ومصداقيتها. وترى اليابان أنه، على مستوى المجتمع الدولي، ما زال توفير بناء القدرات وتقديم المساعدة التقنية للدول الأعضاء المحتاجة قاصراً.

١٧٣- وأفادت اليابان بأنها تقدم برامج بناء القدرات إلى البلدان المحتاجة من خلال جملة أمور من بينها برامج التدريب الخاصة بكل بلد على حدة، بما في ذلك بعض البرامج التي تديرها الوكالة اليابانية للتعاون الدولي، ومعهد آسيا والشرق الأقصى لمنع الجريمة ومعاملة المجرمين، والحوار حول الجرائم السيبرانية بين اليابان ورابطة دول جنوب شرق آسيا. ويتمثل أحد التحديات الشائعة في تمكين البلدان المستفيدة من البرامج من أن تواصل، بنفسها وباستدامة، جهودها الرامية إلى بناء القدرات.

وفي هذا الصـــدد، تعاونت حكومة اليابان مع مجمع الإنتربول العالمي للابتكار منذ عام ٢٠٠٦ لتزويد البلدان بالمساعدة اللازمة لتشجيعها في جهودها الرامية إلى بناء القدرات.

١٧٤- وشددت اليابان على الحاجة إلى مواصلة مناقشات الخبراء، وأكدت على أن أكثر وسيلة فعالية لاستبانة التحديات المتعلقة بالتشريع وبالافتقار إلى القدرة على تقديم المساعدة التقنية من أجل مكافحة الجريمة السيبرانية هي الاستماع إلى آراء الخبراء وتجاربهم. فالخبراء يستطيعون تقديم صورة حديثة عن مسألة الجريمة السيبرانية من خلال مراعاة طبيعتها المستمرة في التطور وكذلك التحديات الجديدة والناشئة. وستوفر المناقشات بين الخبراء فهماً أفضل لحجم المشكلة الكامل، بهدف تحديد المجالات التي ينبغي للمجتمع الدولي أن يركز فيها جهوده.

١٧٥- وأشارت اليابان إلى أن فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية الكائن في فيينا، الذي يضم خبراء معنيين من جميع أنحاء العالم ويوفر المكان المثالي لمناقشة وتحديد الاتجاهات والتحديات الحديثة وطريق المضي قدماً. ويناقش فريق الخبراء حالياً الموضوعات ذات الصلة على أساس سنوي، بناءً على خطة عمل متعددة السنوات تم اعتمادها بتوافق الآراء بين جميع الدول الأعضاء. ومن المتوقع أن يواصل الفريق عمله ويجري عملية تقييم في عام ٢٠٢١. وستمكن هذه العملية المجتمع الدولي من استبانة التحديات العديدة وكذلك الخطوات الواجب اتخاذها. وينبغي أن تستند أي مناقشة حول الجريمة السيبرانية إلى مدخلات محددة وقائمة على الأدلة من الخبراء. ولذلك، ينبغي اعتبار النتائج التي يتوصل إليها فريق الخبراء أساس المناقشات في المستقبل. ولدى حكومة اليابان اعتقاد راسخ بأنه ينبغي إجراء المناقشات حول الجريمة السيبرانية في فريق الخبراء، في فيينا. وبعبارة أخرى، فإن أي حركة تعرقل جهود فريق الخبراء، مثل نقل المناقشات حول الجريمة السيبرانية بعيداً عن فيينا إلى منتدى يشارك فيه عدد قليل من الخبراء، سوف تضعف بصورة خطيرة قدرة المجتمع الدولي على مكافحة الجريمة السيبرانية.

الأردن

١٧٦- ذكر الأردن التحديات التالية باعتبارها التحديات الرئيسية المتعلقة بمكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض غير المشروعة أو الإجرامية:

(أ) وجود برمجيات وبرامج مجانية تخفي هويات المستخدمين وتجعل من الصعب تعقبهم وكشفهم؛

(ب) توافر المعلومات وسهولة الحصول عليها وإمكانية اكتساب المعرفة باستخدام الأدوات الإجرامية والخبرة في استخدامها من مواقع مجانية عديدة على مواقع الشبكة العالمية؛

(ج) الشبكة الخفية، التي تشكل مرتعا خصبا للأعمال غير المشروعة بما في ذلك استئجار أشخاص للقيام بعمليات القتل، وتجارة المخدِّرات، والإتجار بالأشخاص، واستغلال الأطفال، الأمر الذي يجعل عملية رصد هذه المواقع ومراقبتها مهمة صعبة، بسبب استخدام التشفير لمنع كشف هوية المستخدمين؛

(د) بطء الإجراءات وتبادل المعلومات في قضايا الجرائم السيبرانية التي تقع في عدة دول، لاسيما بالنظر إلى أن الجريمة السيبرانية تتطلب سرعة الإجراءات والمعالجة؛

(هـ) عدم تجاوب بعض منصات التواصل الاجتماعي وعدم تعاونها بخصوص تبادل المعلومات مع أجهزة إنفاذ القانون؛

(و) الحاجة إلى بناء القدرات من خلال برامج تدريبية دولية وتبادل الخبرات مع الدول المتقدمة النمو في مسائل الجريمة السيبرانية.

لبنان

١٧٧- أفاد لبنان بأن عام ٢٠١٨ كان عاماً حافلاً في مكافحة استخدام تكنولوجيا المعلومات للأغراض الإجرامية، على مستوى السلطة التنفيذية والسلطة البرلمانية والسلطة القضائية. وفي مؤشر الأمن السيبراني العالمي (٢٠١٨) الصادر عن الاتحاد الدولي للاتصالات، أتى لبنان في المرتبة ١٢٤ عالمياً، في حين بلغ معدلها على مؤشر استخدام الإنترنت ٦٥ (مؤشر تنمية تكنولوجيا المعلومات والاتصالات الصادر عن الاتحاد الدولي للاتصالات (٢٠١٧)).

١٧٨- وتولي حكومة لبنان أهمية كبيرة لمسألة الأمن السيبراني. وقد أشار بيان وزاري صراحة إلى تعزيز الإجراءات والتدابير الخاصة بحماية الفضاء السيبراني اللبناني والبنية التحتية المعلوماتية والبيانات الشخصية للأفراد والمؤسسات، وتعتزم الحكومة متابعة هذا الأمر بالاقتران مع مشروع الحكومة الإلكترونية المعنون "الحكومة الرقمية". وقد أنشئت وزارة جديدة (وزارة الدولة لشؤون التكنولوجيا) في الحكومة الجديدة.

١٧٩- وعلاوة على ذلك، اتخذ رئيس الوزراء قراراً في نهاية عام ٢٠١٨ بتشكيل فريق وطني للأمن السيبراني، بمشاركة ممثلين عن الوزارات والإدارات ذات الصلة. وكُلِّف الفريق بوضع استراتيجية وطنية للأمن السيبراني في لبنان وإنشاء هيئة وطنية للتعامل مع هذه المسألة. وتشمل الاستراتيجية الوطنية التي يجري وضعها خمسة مسائل رئيسية. وبعد فترة تحضيرية، بدأ العمل على وضع الخطة في ١٥ تشرين الثاني/نوفمبر ٢٠١٨ ومن المقرر أن ينتهي العمل خلال الشهرين التاليين.

١٨٠- وأفاد لبنان أيضاً بأن لجان برلمانية، بما في ذلك لجنة تكنولوجيا المعلومات ولجنة الإعلام والاتصالات، عقدت عدة جلسات برلمانية لتقييم الوضع الراهن وتقديم توصيات في هذا المجال.

١٨١- وعلى الصعيد التشريعي، صدر بتاريخ ١٠ تشرين الأول/أكتوبر ٢٠١٨ القانون رقم ٢٠١٨/٨١ المتعلق بالمعاملات الإلكترونية وحماية البيانات ذات الطابع الشخصي، وأصبح نافذا منذ ١٧ كانون الثاني/يناير ٢٠١٩. وهو يعالج مواضيع متعددة ومتجانسة، منها حماية البيانات ذات الطابع الشخصي والجرائم المتعلقة بالنظم والبيانات المعلوماتية. كما ينقح القانون بعض أحكام القانون الجنائي المتعلقة بالجرائم السيبرانية. وعلاوة على ذلك، يتناول القانون المسائل المتعلقة بالأدلة الإلكترونية، ويفرض على مقدِّمي خدمات الإنترنت حفظ بيانات العملاء لمدة ثلاث سنوات.

١٨٢- وأفاد لبنان أيضاً بأنه، فيما يتعلق بوزارة العدل، تم تدريب ٢٠ قاضياً، بدعم من مجلس أوروبا والاتحاد الأوروبي في إطار مشروع سايبر ساوث (CyberSouth)، على التعامل مع الأدلة الإلكترونية.

وفي وقت تقديم الرد الوطني، كانت المراسيم التشريعية لوزارة العدل قيد الإعداد لتنفيذ القانون رقم ٢٠١٨/٨١.

١٨٣- وأشار لبنان إلى التحديات التالية باعتبارها بعض التحديات التي تواجهها وزارة العدل على الخصوص والدولة اللبنانية بصفة عامة في هذا المجال:

(أ) عدم صدور المراسيم التطبيقية اللازمة لتفعيل القانون رقم ٢٠١٨/٨١؛

(ب) غموض أو عدم كفاية بعض النصوص القانونية الواردة في القانون رقم ٢٠١٨/٨١، وبخاصة من حيث حماية البيانات الشخصية وتحديد ولاية قضائية متخصصة للبت في الأمور المستعجلة دون النص على إنشاء هيئة تتحقق من التزام ممارسي التجارة الإلكترونية بتقديم البيانات الإلزامية (المادة ٣١)، أو فيما يخص الحماية من الإعلانات الترويجية (المادة ٣٢)؛

(ج) عدم توفر الخبرة لدى جميع القضاة للتعامل مع الجرائم الإلكترونية أو الأدلة الإلكترونية، وكذلك ضرورة تطوير قدرات القضاة والعاملين في الأجهزة الأمنية وتزويدهم بما يلزم من تدريب ومعدات للتمكن من مجاراة إمكانات المجرمين وقدراتهم التقنية؛

(د) عدم رقمنة المحاكم وربطها بكل الوزارات والمؤسسات التي تتعامل معها؛

(هـ) الحاجة إلى اعتماد استراتيجيات وسياسات وطنية بشأن الأمن السيبراني على المستوى الوطني وإنشاء مؤسسات وطنية تعنى بتنفيذ هذه السياسات والاستراتيجيات؛

(و) صعوبة التعامل مع الإجراءات المنصوص عليها في لائحة الاتحاد الأوروبي التنظيمية العامة لحماية البيانات، التي تمنع أفراد الشرطة القضائية من الوصول مباشرة إلى عناوين بروتوكول الإنترنت، بينما كانت هذه العناوين متاحة سابقاً؛

(ز) ضعف النظم الموحدة التي يستخدمها مقدمو الخدمات، مثل نظام ترجمة العناوين الشبكية الخاص بعناوين بروتكول الإنترنيت، الذي تستخدمه وزارة الاتصالات؛

(ح) قدرة المجرمين على إخفاء هويتهم الحقيقية من خلال استخدام برمجيات خاصة (مثل VPN وTOR وغيرها)، وصعوبة معرفة مكانهم الفعلي، واستخدامهم تقنيات التشفير لإخفاء المعاملات. ويحول هذا كله دون تمكن الأجهزة الأمنية المختصة من فك التشفير والكشف عن المعلومات والبيانات الخاصة بالمجرمين، التي يستخدمونها فيما يتعلق بجرائمهم الفعلية والمعتزمة؛

(ط) تعدد الأجهزة المرتبطة ارتباطاً مباشراً بتكنولوجيا المعلومات والإنترنت، حيث أصبح بإمكان كل جهاز تقريباً (ثلاجة، سيارة، وغيرهما) الارتباط بشبكة إنترنت الأشياء دون مراعاة أنظمة الحماية اللازمة قبل طرح هذه الأجهزة في الأسواق؛

(ي) عدم وجود خطة استراتيجية للتحول الرقمي في لبنان ومخطط تنفيذي خاص بها؛

(ك) عدم اعتماد معايير أمن المعلومات والسياسات المعترف بها عالميا في مختلف الإدارات والمؤسسات العامة؛

(ل) عدم نشر ثقافة الوعي بين أفراد المجتمع حول المخاطر السيبرانية وكيفية حماية المعلومات الشخصية والبيانات وحول خطر الاختراق والسرقة وكيفية اعتماد أفضل الممارسات وحماية هذه المعلومات والبيانات؛

(م) ظاهرة الشبكة الخفية، التي تسمح للمجرمين ببيع وشراء السلع والمواد على نحو غير مشروع وممارسة أنشطتهم الإجرامية بطريقة سرية، لا سيما تجارة المخدِّرات، وبيع الأسلحة، وتبادل المواد الإباحية الخاصة بالأطفال، والبرمجيات الخبيثة، والبيانات الشخصية للأفراد؛

(ن) ظاهرة العملات الافتراضية والرقمية التي تسمح للأفراد والجماعات الإرهابية بشراء وبيع المواد الإجرامية بطريقة سرية، دون إمكانية تتبع مصادر هذه الأموال أو الكيانات التي حولت إليها؛

(س) عدم وجود إطار للتعاون الدولي (اتفاقية، معاهدة) لتبادل المعلومات بين الدول فيما يتعلق بالأدلة الرقمية ومكافحة الجرائم السيبرانية؛

(ع) ضرورة تبادل المعلومات وتضافر الجهود بين مختلف الأجهزة الأمنية ومؤسسات القطاعين العام والخاص؛

(ف) بطء عملية التواصل مع مقدِّمي الخدمات المحليين والدوليين؛

(ص) عدم الإبلاغ عن كل الجرائم السيبرانية، وخاصة تلك التي تسبب بعض الإحراج، كالجرائم المتعلقة بالتحرش الجنسي والابتزاز؛

(ق) استعمال المجرمين لتقنيات معقَّدة، مثل تقنية "الهجمات الموزَّعة" التي تشن من خلال إطلاق الهجمات من عدة خوادم حول العالم أو استخدام بعض الأجهزة "الذكية" التي اخترقوها سابقاً كمنصة لإطلاق هجمات على أهداف أخرى.

ليختنشتاين

١٨٤- أشارت ليختنشتاين إلى أن الجريمة السيبرانية آخذة في الازدياد وأن المجتمع الدولي يواجه مجموعة متنوعة من التحديات في هذا الشأن، بما في ذلك في مجالات التحقيق في هذا النشاط الإجرامي والملاحقة القضائية لمرتكبيه. وبالنسبة لليختنشتاين، يشكل التصيد الاحتيالي، و"الاحتيال باسم الرؤساء التنفيذيين"، وقرصنة البريد الإلكتروني، والاعتراض غير المشروع للبيانات، أكبر التحديات في الوقت الحالي. وتتطلب هذه التحديات استجابة تنفيذية وتشريعية حازمة على المستوى الوطني وتحسين التعاون على المستوى الدولي. ومع ذلك، تشعر ليختنشتاين بالقلق إزاء الميل نحو تنظيم الفضاء السيبراني وكذلك تجريم الأفعال الإجرامية السيبرانية والتحقيق فيها وملاحقة مرتكبيها بطرائق تنتهك حقوق الإنسان والحريات الأساسية، بما في ذلك الحق في الخصوصية. وأشارت ليختنشتاين إلى أنه يجب مراعاة التزامات الدول بموجب القانون الدولي، ولا سيما قانون حقوق الإنسان، في جميع الأوقات، بما في ذلك عند تنظيم الفضاء السيبراني وعند تجريم الجرائم السيبرانية والتحقيق فيها وملاحقة مرتكبيها.

١٨٥- وأفادت ليختنشتاين بأن تشريعاتها الوطنية بشأن الجريمة السيبرانية تستند إلى اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية. وخلال عمليات التنقيح الرئيسية الأخيرة لقانونها الجنائي في عامي ٢٠٠٩ و٢٠١١، كانت تلك الاتفاقية هي الإطار المرجعي الدولي الرئيسي لاستحداث أحكام جديدة متعلقة بالفضاء السيبراني. وقد صدقت ليختنشتاين على الاتفاقية في عام ٢٠١٦ وما زالت الاتفاقية هي الإطار للتعديلات التشريعية المستقبلية.

١٨٦- وأعربت ليختنشتاين عن دعمها لتعزيز القانون الدولي الرامي إلى تنظيم الأنشطة التي تجري في الفضاء السيبراني، بناءً على مبادئ الشفافية والاحتوائية للجميع والتعاون، وبما يتفق تماماً مع معايير حقوق الإنسان الحالية. وقد صدقت دول من جميع المناطق على اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، وتسهل الاتفاقية إلى حد بعيد التعاون بين الدول، من خلال مواءمة القوانين، ووضع الإجراءات، وتحديد نقاط الاتصال. وأعربت ليختنشتاين عن دعمها لزيادة التعاون الدولي على أساس تلك الاتفاقية، وعارضت وضع معايير قانونية متوازية أو متباينة في مجال الجريمة السيبرانية، وهو موقف أعربت عنه، إلى جانب شواغل أخرى، في تصويتها ضد قرار الجمعية العامة ١٨٧/٧٣.

ماليزيا

١٨٧- أشارت ماليزيا إلى أن الجرائم السيبرانية أصبحت أكثر تعقُّداً، نظراً لتطور تكنولوجيات مثل إنترنت الأشياء والحوسبة السحابية والذكاء الاصطناعي، وخدمات من قبيل برنامج حماية الخصوصية المسمى أونيون روتر (Onion Router) والشبكة الخفية. وهذه التكنولوجيات هي سلاح ذو حدين: فهي تجلب مزايا للدول والحكومات، ولكن تجلبها أيضاً لمرتكبي جرائم معينة. ونتيجة لذلك، تواجه الحكومات المزيد من التحديات في مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية.

١٨٨- وأشارت ماليزيا إلى أن البيئة السيبرانية أعطت ميزة لمرتكبي الجرائم، بسبب عنصرين هما استخدام اسم مستعار وإخفاء الهوية، وأثارت تحديات أمام أجهزة إنفاذ القانون في تحديد هوية مرتكب الجريمة وربطها بفرد محدد. كذلك يفرض الاستخدام الواسع النطاق للتشفير، الذي يحقق فائدة هائلة في ضمان السرية والسلامة، تحديات أمام أجهزة إنفاذ القانون فيما يتعلق بجمع الأدلة حول الجرائم السيبرانية. ويتمتع المجرمون أيضاً بفوائد التكنولوجيا للقيام بأنشطتهم الإجرامية. وفضلا عن ذلك، هناك العديد من التطبيقات والأدوات، بما في ذلك أدوات مكافحة التحليل الجنائي، متوفرة على الإنترنت ويمكن تنزيلها بسهولة ويمكن إساءة استخدامها للأغراض الإجرامية.

١٨٩- وعلاوة على ذلك، أشارت ماليزيا إلى أن ظهور الحوسبة السحابية، على سبيل المثال، أتاح للمجرمين الفرصة لتخزين المعلومات في البيئات السحابية. وتخلق طبيعة الحوسبة السحابية في حد ذاتها تحديات جديدة لأجهزة إنفاذ القانون، من حيث اكتشاف الأدلة الرقمية واحتيازها. فاكتشاف الأدلة الرقمية واحتيازها من المنصات السحابية النائية التي يتحكم فيها مقدمو الخدمات اختلافًا كبيرًا عن اكتشافها في الموقع أو على الصعيد المحلي. ولذلك، يتطلب الحصول على البيانات من البيئات السحابية أدوات وتقنيات ونهوجاً مختلفة.

١٩٠- وترى ماليزيا أن هناك حاجة إلى التصـــدي للتحديات التي يواجهها الموظفون المعنيون في التعامل مع الأدلة الرقمية ومع الأدلة المتعلقة بالحفاظ على تسلسل العهدة وضمان العمليات الشاملة والبنية التحتية المناسبة لتحسين مستوى مقبولية الأدلة في المحاكم. والكفاءة التقنية لدى الأشخاص المعنيين بالتعامل مع الأدلة الرقمية ضرورية لتجنب الإخلال بالأدلة وتلويثها. فعلى سبيل المثال، تواجه أجهزة إنفاذ القانون والمدعون العامون تحديات ليس فقط في الحفاظ على الخبراء الحاليين بل أيضـــاً في الحصول على موارد جديدة للاضطلاع بالتحقيقات في الجرائم السيبرانية. وإلى جانب ذلك، هناك حاجة إلى رفع مستوى مهارات وكفاءات القضاة والمدعين العامين وتعزيز معارفهم بشأن أساسيات تكنولوجيات المعلومات والاتصالات والأمن السيبراني، بما في ذلك معرفة المصطلحات المتعلقة بالنظم الحاسوبية والشبكات. ومن ثم فهناك حاجة إلى تدريب خاص للقضاة والمدعين العامين بشأن الأمن السيبراني والجرائم السيبرانية وتكنولوجيا الإنترنت.

١٩١- وترى ماليزيا أن الأدلة الإلكترونية سريعة التلاشي ويمكن تعديلها أو حذفها ببساطة. ولذا فإن الوقت عنصر مهم جدًّا في جمع الأدلة. وأفادت ماليزيا أيضاً بأن نقص الموارد البشرية لدى وكالات إنفاذ القانون يشكل تحدِّياً آخر تواجهه السلطات الوطنية. بل إن بعض وكالات إنفاذ القانون لا يوجد لديها فريق مكرس للتركيز على التحقيقات في الجرائم السيبرانية. وتوجد الأدلة الإلكترونية عادة في بنية تحتية يمتلكها القطاع الخاص، أي شركات الاتصالات ومقدمو خدمات الإنترنت، الذين تتنوع قدراتهم على استبقاء الأدلة الرقمية وحفظها.

١٩٢- وفيما يتعلق بالتحقيقات في الجرائم السيبرانية، شددت ماليزيا على أنه يتعين على أجهزة إنفاذ القانون الحصول على الأدلة الرقمية عبر الحدود من خلال قناة رسمية، وهي المساعدة القانونية المتبادلة، لكي تكون الأدلة مقبولة في المحكمة. وقد يستغرق تلقي الردود من خلال هذه المساعدة وقتاً طويلاً للغاية، مما قد يطيل إجراءات المحكمة. وبالإضافة إلى ذلك، لا تزال طلبات الحصول على الأدلة خارج الولاية القضائية تخضع لمسألة ازدواجية التجريم.

١٩٣- وأشارت ماليزيا أيضاً إلى مسألة أخرى تواجهها الحكومة في مكافحة إساءة استعمال تكنولوجيات المعلومات والاتصالات من جانب المجرمين، وهي تحدي جعل القانون يتصدى على نحو كافٍ لتقنيات الجريمة السيبرانية المتطورة الحالية. وبالإضافة إلى ذلك، سلطت ماليزيا الضوء على أن تشريعاتها الوطنية تُلزم من يعدُّون الوثائق بالتحقق من مصادرهم أو التصديق على الأدلة في المحكمة. بيد أن عدم رغبة بعض الشـــهود، مثل مقدِّمي الخدمات العالميين، على الإدلاء بشهادتهم في المحكمة فيما يتعلق بصحة الوثيقة أو مصدر المعلومات تؤدي إلى عدم الملاحقة.

منغوليا

١٩٤- شددت منغوليا على أن استخدام الإنترنت كان يتزايد بسرعة في العقد الماضي بسبب التحسن في جودته وسرعته ونطاقه. ونتيجة لذلك، يتزايد يوميًّا عدد الجرائم والانتهاكات المرتبطة بالإنترنت. ويتعرض الأفراد والكيانات التجارية كثيراً للهجوم من قبل الجماعات الإجرامية الأجنبية عن طريق منصات الإنترنت.

١٩٥- وأشارت منغوليا إلى ثلاثة عناصر أساسية في مكافحة الجريمة السيبرانية وهي: تعقُّب الإنترنت والتتبع الرقمي؛ التحليل؛ التعاون الدولي. وهناك حاجة إلى زيادة القدرة على مكافحة الجرائم السيبرانية والوفاء بالمعايير الدولية في مكافحة هذه الجريمة.

١٩٦- وأشارت منغوليا إلى أنه يجب إيلاء اهتمام خاص للجرائم السيبرانية، التي تنطوي على هجمات سيبرانية متنوعة، ومخططات هرمية، وتصيُّد احتيالي، والاتجار غير المشروع عبر الإنترنت، والتهديدات عبر الإنترنت، ونظام البطاقات، والاحتيال عبر الإنترنت، واستغلال الأطفال في المواد الإباحية، وجرائم الملكية الفكرية القائمة على الإنترنت.

١٩٧- وأفادت منغوليا بأن هيكل وتنظيم وحدات مكافحة الجرائم السيبرانية في الدول الأخرى ينقسم إلى ثلاث فئات: (أ) مكافحة الجريمة السيبرانية ضد الحواسيب والشبكات والنظم؛ (ب) مكافحة الجريمة السيبرانية المرتكبة باستخدام الحواسيب والشبكات والنظم؛ (ج) تتبع البصمات الرقمية وتعزيزها والبحث فيها. غير أن البلد يفتقر، على المستوى الوطني، إلى الموارد البشرية اللازمة لمكافحة الجريمة السيبرانية، لأن هناك إحجاماً عن بناء القدرات وإعداد الموارد البشرية في هذا المجال. فعلى سبيل المثال، توجد في الاتحاد الروسي مدرسة مخصصة لأمن الشبكات بغرض إعداد القوى العاملة التي ستقوم في المستقبل بمكافحة الجريمة السيبرانية. ولا تمتلك منغوليا حالياً مؤسسة مخصصة لإعداد القوى العاملة اللازمة لمكافحة الجريمة السيبرانية في المستقبل. ولذا فمن أجل مكافحة هذه الجريمة في المستقبل بمساعدة وتعاون من البلدان التي تقود مكافحة الجريمة السيبرانية، شددت منغوليا على الحاجة إلى تدريب القوى العاملة اللازمة للمستقبل وبناء قدراتها، وبالإضافة إلى ذلك، تدريب وإعداد الموظفين الحاليين بانتظام لكي تكون لديهم القدرة الكافية على مكافحة الجريمة السيبرانية.

١٩٨- وأشارت منغوليا كذلك إلى أن عناوين بروتوكول الإنترنت تؤدي دوراً حاسم الأهمية في التحقيق في الجرائم السيبرانية والانتهاكات السيبرانية. غير أنه، لأسباب مالية وتكنولوجية وبرامجية، يوفر مقدمو خدمة الإنترنت في منغوليا عنواناً واحداً من عناوين بروتوكول الإنترنت للعديد من المستخدمين، وبذلك يصعب تحديد الوقت والتاريخ المحددين اللذين حدث فيهما السلوك المعني. ونتيجة لذلك فمن الصعب جداً تتبُّع الفرد الذي ارتكب الجريمة السيبرانية أو الانتهاك السيبراني. ومن أجل الحصول على الترخيص ذي الصلة من لجنة تنظيم الاتصالات، يُشترط على مقدِّمي خدمة الإنترنت امتلاك القدرة التكنولوجية اللازمة للتأكد من أن العنوان الواحد من عناوين بروتوكول الإنترنت لا يتشارك فيه أكثر من ٢٠ شخصاً. إلا أن منغوليا اعتبرت تنفيذ هذا النظام غير كافٍ وغير فعال. ولذلك فمن دون حل المشكلة المتعلقة بعنوان بروتوكول الإنترنت، يكاد يكون من المستحيل التحقيق في الجرائم السيبرانية بسرعة.

١٩٩- وعلاوة على ذلك، أكدت منغوليا أن هناك حاجة لتوضيح بعض المصطلحات المستخدمة في القانون الجنائي. فعلى سبيل المثال، تحتاج المصطلحات الواردة في المادة ٢٦ من القانون الجنائي لمنغوليا، مثل مصطلحات "الأجهزة الإلكترونية" و"الشبكات المحمية" و"الهجمات غير المشروعة"، إلى مزيد من التوضيح؛ وهناك صعوبة في استخدامها في الممارسة العملية حيث لا يوجد أي توضيح أو تفسير لهذه المصطلحات في القوانين والتشريعات الأخرى. وتتسم قواعد ولوائح دول

أخرى فيما يتعلق بالجرائم السيبرانية بأنها شاملة للغاية. وعناصر هذه الجريمة المنصوص عليها في القانون الجنائي واضحة؛ ولذلك لا يوجد مجال للالتباس أو إساءة تفسير المواد ذات الصلة.

٢٠٠- ويستخدم مواطنو منغوليا في الغالب منصات اجتماعية قائمة على الإنترنت مثل فيسبوك وتويتر وإنستغرام وياهو!، وكلها مؤسسة بموجب قوانين ولوائح دول مختلفة. ولذلك، لا يمكن للسلطات الوطنية الحصول على الوثائق اللازمة للتحقيقات في الجرائم السيبرانية من هذه الكيانات المؤسسة في الخارج. وهناك وثيقة للتعاون بين أجهزة الشرطة مبرمة بين منغوليا والولايات المتحدة فيما يتعلق بطلب الحصول على الوثائق. ومع ذلك فمن الضروري، على أساس قوانين الولايات المتحدة، من أجل الحصول على الوثائق ذات الصلة، الحصول على أمر قضائي بتوفير الوثائق، وهذا يجعل التعاون متعذراً.

٢٠١- وترى منغوليا أن هناك حاجة إلى اعتماد برنامج وطني لمكافحة الجريمة السيبرانية. فمن خلال اعتماد مثل هذا البرنامج، سيكون بالوسع تنفيذ إجراءات سياساتية لمكافحة الجريمة السيبرانية بطريقة مرحلية ومستدامة. ويمكن لمنغوليا تحسين الحالة الراهنة للوائح التنظيمية المتعلقة بالجريمة السيبرانية وإنشاء وحدة مخصصة لمكافحة هذه الجريمة.

٢٠٢- وفي هذا العصر الذي تتطور فيه تكنولوجيا المعلومات بسرعة، يتسم تحسين الأمن السيبراني الوطني ومكافحة الجرائم السيبرانية بأهمية حاسمة. وقد جاءت منغوليا في المرتبة ٨٤ في مؤشر الأمن السيبراني العالمي (٢٠١٨) الصادر عن الاتحاد الدولي للاتصالات. ومع نمو تكنولوجيا المعلومات، تصبح الجريمة السيبرانية أكثر تعقُّداً، وتشمل أنواعاً جديدة من الجرائم. ومن المستحيل القضاء على الجرائم السيبرانية المرتكبة على الإنترنت. ومع ذلك فمنغوليا قادرة، من خلال استخدام القوانين واللوائح ذات الصلة، على التصدي لتلك الجرائم، عن طريق المنع والقمع معاً.

٢٠٣- وعلاوة على ذلك، ذكرت منغوليا أن الأسباب الرئيسية لوقوعها ضحية للجرائم السيبرانية هي أن الجمهور لا يدرك الأخطار، وأن هناك افتقاراً إلى المعارف والأخبار وإلى التحذيرات الكافية بشأن الجريمة السيبرانية. ولذلك شددت منغوليا على الحاجة إلى بناء القدرات ونشر الوعي بالمخاطر المحتملة للجرائم السيبرانية على الإنترنت. ومن المهم إنفاذ التقيد الصارم بالمتطلبات التقنية، ومراقبة تنفيذ اللوائح ذات الصلة، وحل المشاكل القصيرة الأجل المتعلقة بعناوين بروتوكول الإنترنت وغيرها من الصعوبات، وزيادة مسؤولية مقدِّمي خدمات الإنترنت، من أجل منع الجرائم السيبرانية وقمعها وكشفها ومكافحتها.

٢٠٤- وأشارت منغوليا إلى أن من الواضح من الوضع الراهن أن أجهزة إنفاذ القانون ينبغي أن تكون مستعدة جيداً لمنع هذه الجرائم ومكافحتها. ولذا فمن الضروري تدريب وتثقيف العاملين وزيادة قدرة هذه الوكالات بكل طريقة ممكنة على مكافحة الجريمة السيبرانية. ومن الضروري أيضاً إنشاء مختبر مسؤول عن الكشف عن البصمات الرقمية وتعزيزها والبحث فيها وتحليلها، وزيادة عدد الوحدات العاملة في مكافحة الجريمة السيبرانية.

٢٠٥- وتعتقد منغوليا أن هناك حاجة إلى وضع صك قانوني دولي لمكافحة الجرائم التي تنطوي على استخدام تكنولوجيات المعلومات والاتصالات وللتصدي لتلك الجرائم.

المغرب

٢٠٦- أشار المغرب إلى أن العالم المعاصر يعيش ثورة في تكنولوجيات المعلومات والاتصالات، بما في ذلك أجهزة الحاسوب المتطورة وبرامج معالجة المعلومات التي تطورها الشركات الضخمة. وقد تأثرت هذه العملية بالعولمة وسهولة نقل المعلومات، مما أدى إلى تقليص المسافات بين النظم القانونية والقضائية. وأدت عناصر العولمة هذه إلى عولمة الجريمة وكذلك عولمة أساليب ارتكابها. وعلى الرغم من مزايا تكنولوجيا المعلومات فقد اقترنت بسلسلة من العواقب السلبية الخطيرة بسبب إساءة استخدامها والانحرافات عن أغراضها المقصودة، وذلك أساساً من خلال الهجمات ضد القيم والمصالح الأساسية للأفراد والمؤسسات والدول. وقد ظهر عدد من الجرائم التي ترتكب من خلال استخدام الإنترنت ووسائل الإعلام الإلكترونية، مما يسهل بدوره ارتكابها والتهرب من إقامة العدل (من حيث تحديد هويات الجناة وأماكنهم على حد سواء).

٢٠٧- ووفقاً للتحقيقات التي أجرتها أجهزة الشرطة القضائية اللامركزية في هذا الصدد، أفاد المغرب بأن التحديات التي تواجه التصدي للجريمة السيبرانية ترتبط عموماً بما يلي:

(أ) إخفاء الهوية: استخدام الخوادم الوكيلة والشبكة الخفية؛

(ب) الطابع عبر الوطني: تخزين الأدلة في خوادم موجودة خارج الأراضي الوطنية؛

(ج) الاستخدام المتواتر لتشفير البيانات؛

(د) الاستغلال الإجرامي للعملة المشفرة؛

(هـ) التطور المستمر لأساليب التشغيل المستخدمة؛

(و) الصعوبات في الوصول إلى البيانات المتعلقة بحركة مستخدمي تطبيقات أو مواقع معيَّنة مستضافة في الخارج؛

(ز) التخطيط لتوفير التدريب المستمر على مكافحة الجريمة السيبرانية للعاملين في التحقيقات المتعلقة بالجريمة السيبرانية والأدلة الرقمية، بغية مواكبة التقدم الهائل في التكنولوجيا؛

(ح) اقتناء أجهزة وبرمجيات متخصصة مناسبة وكفؤة لإجراء التحقيقات المتعلقة بالجرائم السيبرانية؛

(ط) أن مستخدمي تكنولوجيات المعلومات والاتصالات ينبغي أن يخضعوا لبرنامج توعية بشأن مخاطر عدم الامتثال لتدابير الحماية؛

(ي) تفعيل هياكل الحماية وتدابير التصدي للتهديدات المتصلة بالفضاء السيبراني الخاصة برابطة الدول المستقلة؛

(ك) التعاون والتنسيق بين الدول بشأن توضيح المسائل القانونية وتنفيذ القوانين ذات الصلة، وكذلك بشأن آليات التحقيق وإجراء التحقيقات المشتملة على الأدلة الرقمية بكفاءة.

٢٠٨- وأشار المغرب إلى أن المجتمع الدولي تصدى للجريمة السيبرانية من خلال الصكوك المعيارية واعتماد الاتفاقيات ذات الصلة وعقد العديد من المؤتمرات. وكان على المغرب أيضاً،

بحكم موقعه الاستراتيجي، أن يعتمد تشريعات للتعامل مع ظاهرة المعلوماتية وأن يقيم شراكات، لا سيما مع الاتحاد الأوروبي، كانت مفيدة للغاية.

٢٠٩- وقد سن المشرِّع المغربي تشريعات جنائية مناسبة لخصوصية استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، وفقا للمبادئ العامة للعدالة الجنائية. وتشمل هذه التشريعات القانون رقم ٠٣-٠٧، بشأن مراقبة نظم المعالجة الآلية للمعطيات، الذي اعتُمد في عام ٢٠٠٣ كجزء من القانون الجنائي (الفصول ٦٠٧/٣ إلى ٦٠٧/١١). وهذا القانون هو الإطار الأساسي لمكافحة الجريمة السيبرانية في المغرب، وأحكامه مستمدة من الاتفاقيات الدولية، وخاصة اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية والبروتكول الإضافي الملحق بها، من خلال المرسوم الملكي رقم ١-١٤-٨٥ الصادر في ١٢ أيار/مايو ٢٠١٤ بتنفيذ القانون رقم ١٣٦-١٢ بالموافقة على اتفاقية الجريمة السيبرانية. كما استُلهم هذا القانون من مشروع القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات.

٢١٠- وصادق المغرب أيضاً على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الموقعة في القاهرة في ٢١ كانون الأول/ديسمبر ٢٠١٠، وذلك بموجب المرسوم رقم ٤٦-١٣-١ المؤرَّخ ١٣ آذار/مارس ٢٠١٣، بتنفيذ القانون رقم ١٢-١٧، المنشور في الجريدة الرسمية رقم ٦١٤٠ في ٤ نيسان/أبريل ٢٠١٣.

٢١١- وتنص المادة ٣ من القانون رقم ١٠٨-١٣، بشأن القضاء العسكري، على بعض المتطلبات المتعلقة بالجرائم التي تدخل في اختصاص المحكمة العسكرية، مما يسمح لتلك المحكمة أيضاً بالفصل في الجرائم السيبرانية.

٢١٢- وبفضل القوانين الوقائية التي تهدف إلى حماية البيانات الشخصية أو التبادل الإلكتروني للبيانات، مثل المرسوم الملكي رقم ١-٠٧-١٢٩ المؤرَّخ ٣٠ تشرين الثاني/نوفمبر ٢٠٠٧، بتنفيذ القانون رقم ٥٣-٠٥ بشأن التبادل الإلكتروني للمعطيات القانونية، والمرسوم الملكي رقم ١-٠٩-١٥ المؤرَّخ ١٨ شباط/ فبراير ٢٠٠٩، بتنفيذ القانون رقم ٠٩-٠٨، بشأن حماية البيانات الشخصية، أصبح المغرب قبلة للمستثمرين في مجال تكنولوجيا المعلومات والاقتصاد الرقمي.

٢١٣- وينص القانون رقم ٩٦-٢٤ بشأن البريد والمراسلات، الصادر بالمرسوم الملكي رقم ١-٩٧-١٦٢ في ١ آب/ أغسطس ١٩٩٧، بصيغته المعدَّلة والمتمَّمة، والمرسوم رقم ٤٤٤-٠٨-٢ المؤرَّخ ٢١ أيار/مايو ٢٠٠٩، على إنشاء مجلس وطني لتكنولوجيات الإعلام والاقتصاد الرقمي، مسؤول عن تنسيق السياسات الوطنية وتقييم تنفيذها.

٢١٤- كما يوفر مشروع قانون بشأن الجريمة المعلوماتية المنظمة، بموجب المواد ١٨٧ و٤٤٨/١ و٤٤٨/٢ منه، العديد من الأدوات للتصدي لهذه الجريمة.

٢١٥- وعلى المستوى المؤسسي، أُنشئت فرقة عمل ضمن الشرطة القضائية لمكافحة الجريمة السيبرانية. وفي جهاز الأمن الوطني المغربي، أُنشئت وحدتان لمكافحة الإرهاب من أجل مكافحة الجرائم المتعلقة بنظم المعلومات، على مستوى التحقيق ومستوى تتبع المجرمين من خلال الإنترنت.

وأنشأت وزارة الدفاع الوطني مديرية الجرائم السيبرانية للتصدي للجرائم السيبرانية وتتبُّع آثارها ومكافحتها بالتنسيق مع مختلف الإدارات الأمنية الوطنية والدولية.

٢١٦- وعلى الرغم من هذه الجهود، أكد المغرب أنه لا يزال هناك الكثير من التحديات في مكافحة هذه الجريمة. ويصعب على التشريعات الاستجابة للتطور السريع للجرائم السيبرانية، فعلى سبيل المثال، لا يوجد إطار قانوني للجرائم المرتكبة من خلال الشبكات الاجتماعية. ويرتبط معظم الأحكام القانونية الحالية بمستخدمي وسائل التواصل الاجتماعي، ولا يتضمن أي متطلبات لإثبات مسؤولية مقدِّمي خدمات الشبكات وإلزامهم بحذف أو حظر أو إيقاف أو تعطيل الوصول إلى المحتوى الإلكتروني غير المشروع. ومما يفاقم من ذلك أن معظم مقدِّمي ومديري هذه المنصات موجودون خارج الولاية القضائية للبلد.

٢١٧- وسلط المغرب الضوء على أن التعاون الدولي على مكافحة الجريمة السيبرانية يشكل أيضاً تحدِّياً فيما يتعلق بالاتصال بمقدِّمي خدمات الاتصالات الموجودين في ولايات قضائية أخرى، الأمر الذي يتطلب اعتماد صك دولي يتيح التعاون المباشر معهم لضمان إمكانية توصيل البيانات عبر الحدود.

٢١٨- ومن ناحية أخرى، سلط المغرب الضوء أيضاً على أن التصدي للجريمة السيبرانية يمثل تحدِّياً أكبر على مستوى تعزيز قدرة أجهزة إنفاذ القانون. ويتطلب التطور الكبير والمتواصل لأساليب الجريمة السيبرانية، مثل الجرائم المتصلة بالإنترنت، والهجمات السيبرانية، وهجمات التصيد الاحتيالي، والتصيد الإلكتروني، والوصول إلى الإنترنت، والعملات الافتراضية، والحوسبة السحابية، والتشفير، أن تغير هيئات التحقيق استراتيجياتها في مجال البحث والتحقيق والاستدلال الجنائي، وتوفير أدلة إلكترونية مقبولة وذات حجية في نظر الجهاز القضائي.

ميانمار

٢١٩- أشارت ميانمار إلى أن مكافحة الجريمة السيبرانية أمر حيوي لحماية الأمن السيبراني الوطني والبنية التحتية الوطنية للمعلومات. وذكرت أن هناك حاجة ملحة لوضع تشريعات وطنية ملائمة، تتوافق مع المعايير الدولية، لتحقيق أقصى قدر من الفعالية في مكافحة الجرائم السيبرانية. وينبغي تزويد أجهزة إنفاذ القانون بالصكوك القانونية والأدوات التقنية والبنية التحتية والمهام المناسبة اللازمة لإجراء تحقيقات فعالة وملاحقات قضائية ناجحة.

٢٢٠- وعلاوة على ذلك، شددت ميانمار على أن إيجاد استراتيجيات وحلول بشأن خطر الجرائم السيبرانية يمثل تحدِّياً كبيراً للبلدان النامية. وفيما يتعلق بالاختلافات الإقليمية، ينقل مرتكبو مواقع المحتوى غير المشروع أنشطتهم إلى بلد لا يجرِّم المحتوى غير المشروع، من أجل تجنب التحقيقات الجنائية. وهذه التحركات إلى البلدان الأجنبية هي أحد التحديات التي تواجه أجهزة إنفاذ القانون، لأن الخادوم يوجد خارج أراضي البلد. ويستغل المجرمون هذه الاختلافات الإقليمية استغلالاً تامًّا ولا ينشرون أو يوزعون أو يتيحون أو يخزنون المحتوى غير القانوني والصور المسيئة على محركات الأقراص الصلبة المحلية، بل يقومون بذلك على خادوم خارجي يمكنهم الوصول إليه عبر الإنترنت. وبناءً على ذلك فإن التعاون الدولي أمر حاسم الأهمية لاستبانة المجرمين والتغلب على الصعوبات

الناشئة عن الاختلافات الإقليمية. وينبغي مراعاة كل من الاتساق مع القوانين الوطنية القائمة والتواؤم مع المعايير الدولية عند اعتماد سياسات الأمن السيبراني الوطنية وإنشاء الأطر القانونية المناسبة.

٢٢١- وأبلغت ميانمار عن التحديات التالية التي تواجهها الدولة في صوغ سياسة الأمن السيبراني والصكوك القانونية اللاحقة:

(أ) يلزم اعتماد إطار سياساتي وطني شامل وتشريعات مناسبة بشأن مكافحة الجريمة السيبرانية تتوافق مع الممارسات والإجراءات الدولية. وتحتاج الدولة إلى جعل استراتيجيات الأمن السيبراني ومكافحة الجرائم السيبرانية متوافقة مع المعايير الدولية؛

(ب) من الضروري إجراء تحليل شامل للقوانين الوطنية الحالية بغية تحديد أي فجوات محتملة وتداخل محتمل بين التشريعات المتعلقة بالفضاء السيبراني وغيرها من التشريعات. وتستغرق مراجعة القوانين ذات الصلة بالتفصيل وقتاً طويلاً، كما تحتاج إلى تطبيق معايير مهنية عالية ومراعاة المفاهيم القائمة على الممارسات الدولية وتبادل وجهات النظر؛

(ج) تدعو الحاجة إلى إنشاء وكالة لإنفاذ القانون لضمان أن يكون الأمن الوطني وسيادة القانون ممثلين للحقوق الأساسية للمواطنين. وفي الوقت نفسه، يتعين إنشاء مركز للاعتراض المشروع للرسائل بغية الاضطلاع بمراقبة الاتصالات من خلال اعتماد إجراءات تشغيل قياسية للاعتراض المشروع تستند إلى المبادئ والمعايير الدولية لحماية البيانات وحماية الخصوصية؛

(د) ينبغي إنشاء فرق للتصدي للحوادث السيبرانية والهجمات السيبرانية (أي فرق للتصدي لحالات الطوارئ الحاسوبية، وفرق للتصدي للحادثات الحاسوبية، وفرق للتصدي لحادثات الأمن الحاسوبي) تكون مؤهلة جيداً لإدارة الأزمات السيبرانية وإجراء تقييمات للتهديدات ومواطن الضعف. ومن المفترض أن تقوم هذه الفرق بنشر المعلومات الأمنية وإسداء المشورة الأمنية بشأن حادثات الفضاء السيبراني والمخاطر السيبرانية والهجمات السيبرانية، والمخاطر التي يمكن أن يتعرض لها الجمهور من جرّاء هذه الهجمات السيبرانية، ودعم أجهزة إنفاذ القانون من خلال تقديم المساعدة التقنية اللازمة لهذه الأجهزة لتكون قادرة على إجراء تحقيقات فعالة؛

(ه) ينبغي أن تدعم الدولة الصناديق المخصصة لاتخاذ تدابير الحماية التقنية بغية جعل الإنترنت مأمونة وآمنة وضمان سلامة الإنترنت وحماية الشبكات، بما في ذلك بتوفير البنى الأساسية والمرافق والمعدات اللازمة لتنفيذ تدابير الحماية وأنشطة السلامة هذه؛

(و) من المهم لدى تكييف الأطر التشريعية السيبرانية الوطنية بهدف تنظيم التحقيقات الجنائية مراعاة ضمانات حقوق الإنسان عند استخدام البيانات الشخصية؛

(ز) تحتاج القطاعات الخاصة التي تقوم بجمع بيانات المستخدمين أو تخزينها أو تبادلها إلى معايير واضحة ودقيقة بشأن حماية البيانات وحماية الخصوصية؛

(ح) ينبغي أن يتلقى مستخدمو الإنترنت معلومات محددة تحديداً جيداً عن الأمن السيبراني وطبيعة الجريمة السيبرانية وأنواعها والحالة المعقدة والمتعددة الجوانب للهجمات السيبرانية. وعلاوة على ذلك، ينبغي دعم حملات توعية المستخدمين ودعم التدريب، كما ينبغي الارتقاء

بمستوى الإلمام بالبيئة الرقمية حيثما يتم توطين تكنولوجيات المعلومات والاتصالات المربوطة شبكيًّا على الصعيد العالمي لفائدة المستخدمين على الصعيد الوطني.

٢٢٢- وفي ميانمار، يكثر حدوث حالات الاحتيال والتشهير على الإنترنت. وتتعلق الحالات الشائعة المرتكبة عبر الإنترنت باستخدام المعلومات والاتصالات عبر الإنترنت للتحريض على أعمال الشغب العرقية والدينية وتهديد العاملين في الحكومة وفي المنظمات. وما يواجه ميانمار أساساً هو استخدام وسائل التواصل الاجتماعي في الأعمال الإرهابية وفي الدعاية وفي الهجمات الشخصية. ولا تحصل السلطات في التحقيقات الجنائية على معلومات محددة أو تعاون من مقدِّمي خدمات الإنترنت.

٢٢٣- وعلاوة على ذلك، أبلغت ميانمار بأنه في الحالات التي يتعين فيها طلب معلومات المشتركين من شركات التواصل الاجتماعي الأجنبية، ترفض الشركات الطلبات على أساس أن هذه الطلبات لا تندرج في إطار الإجراءات الموحدة. ونتيجة لذلك، تواجه ميانمار صعوبات في التحقيقات.

٢٢٤- وأشارت ميانمار أيضاً إلى صعوبات عديدة في التحقيقات تنجم عن نقص الموارد المتاحة للتقنيين، ونقص معارف مستخدمي الإنترنت، وضعف الأثر القانوني الملزم للقوانين والإجراءات. ومع تطور التكنولوجيا، وإمكانية الوصول إلى الخدمات المصرفية عبر الهواتف المحمولة، أصبحت الهجمات السيبرانية توجَّه الآن إلى مستخدمي الهواتف المحمولة.

٢٢٥- ورأت ميانمار أن الآليات القانونية القائمة غير كافية لمكافحة الجرائم المرتكبة من خلال استخدام تكنولوجيات المعلومات والاتصالات. وأفادت بأنه يجري صوغ القانون السيبراني والسياسات المتصلة به المتعلقة بمسائل الحكومة الإلكترونية والتجارة الإلكترونية والأمن السيبراني، وينفذ هذا المشروع تحت قيادة وزارة النقل والاتصالات، بمشورة من شركة استشارية خارجية.

٢٢٦- وأشارت ميانمار إلى أن حل المشكلة يمكن أن يتم من خلال وضع واعتماد اتفاقية في إطار الأمم المتحدة، لأن التعاون الدولي ضروري.

٢٢٧- وتوافق ميانمار على أن التصدي لاستخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية يتطلب مناقشة دائمة ومفتوحة، بمشاركة جميع الدول المهتمة. ويمكن توفير منصة لهذه المناقشة من خلال فريق عامل مفتوح العضوية تابع للأمم المتحدة، مع تفويضه لوضع أي وثائق ذات صلة واتخاذ القرارات على أساس أغلبية الأصوات. وتوافق ميانمار كذلك على أن فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية يركز في المقام الأول على القضايا المتعلقة بمكافحة جرائم المعلومات.

هولندا

٢٢٨- أشارت هولندا إلى أن أوساط الشرطة والعدالة على الصعيد الدولي تتشاطر المسؤولية عن الحيلولة دون تحوُّل الإنترنت إلى ملاذ آمن للمجرمين، ويجب ألا يُسمح للجريمة بأن تؤتي أُكلَها. والصكوك القانونية الفعالة التي تحترم حقوق الإنسان الأساسية ضرورية في مكافحة الجريمة السيبرانية. ويمكن تحديد صكوك مختلفة، وطنية وإقليمية ودولية. فأولاً، عززت دول عديدة قدرتها الوطنية على مكافحة الجريمة السيبرانية. بيد أنه توجد تباينات دولية في القانون الجنائي والخبرات

والمعدات، وهذا يُصَعِّب التصدي لظاهرة بهذا الطابع العابر للحدود ومكافحتها. ولا يمكن التصدي لهذه الظاهرة إلا عبر تعزيز جهود بناء القدرات داخل الدول وفيما بينها. فيمكن، من خلال إنشاء شبكة دولية واسعة مكونة من أجهزة إنفاذ القانون المقتدرة، توجيه ضربة كبيرة للجريمة السيبرانية المنظمة. أما النوع الثاني من الصكوك فهو الصك الإقليمي. وهذه الصكوك إقليمية لأنها غير متاحة للبلدان الواقعة خارج الإقليم المعني. ومن الأمثلة عن هذا النوع من المبادرات مبادرة الأدلة الإلكترونية للاتحاد الأوروبي، وأُطر عمل منظمة شنغهاي للتعاون، والمنظمات الأفريقية الحكومية الدولية، وجامعة الدول العربية. وثالثاً، توجد صكوك دولية مفتوحة أمام الدول في جميع أنحاء العالم. ومن هذه الصكوك اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، التي تضم ٦٣ طرفاً (وهو رقم آخذ في الازدياد)، وثمة حوالي ٧٠ دولة إضافية تتخذ من الاتفاقية تشريعا نموذجيا، وكذلك اتفاقية الجريمة المنظمة وبروتوكولاتها. ونظرا لكون هولندا واحدة من أوائل الدول الموقعة والمصدقة على اتفاقية مجلس أوروبا، فقد جنت منافع الاتفاقية من حيث تحقيق نتائج ملموسة في مجال التحقيقات الجنائية، من خلال تكييف القانون الوطني ليلائم إمكانيات التعاون الموسعة مع الدول الأطراف الأخرى. وأبرزت هولندا أيضاً فوائد الإطار الذي تتيحه اتفاقية الجريمة المنظمة.

٢٢٩- وذكرت هولندا أن أهم الاحتياجات العملية لأجهزة إنفاذ القانون في الفضاء السيبراني وأكثرها إلحاحاً هي: أولاً، التمكين من الوصول إلى الأدلة الإلكترونية عبر الحدود، وثانياً، التعاون الدولي في مجال التحقيقات الجنائية. ولا يكفي التعاون الثنائي والمساعدة القانونية المتبادلة في قضايا الجرائم العابرة للحدود والجرائم سريعة التطور. وبات الوصول إلى الأدلة الإلكترونية في الوقت الراهن ضرورةً فيما يتعلق بجميع أنواع الجرائم، بالنظر إلى استخدام تكنولوجيا المعلومات والاتصالات، لا سيما مع ظهور العديد من المرافق الجديدة، مثل وسائل التواصل الاجتماعي وإرسال الرسائل على شبكة الإنترنت، التي أدت إلى ازدياد لا مثيل له في البيانات الرقمية. ولا يمكن تحسين التعاون الدولي إلا إذا كانت لدى أجهزة إنفاذ القانون القدرة والإمكانية اللازمتان للمشاركة، على سبيل المثال، في إجراء تحقيق مشترك. ويجري بالفعل تطوير ومناقشة مناهج مبتكرة للوصول إلى الأدلة الإلكترونية عبر الحدود، مثل إصدار أمر بتوفير الأدلة أو البحث الموسَّع في الشبكة. وتشهد المفاوضات الحالية بشأن صوغ بروتوكول إضافي لاتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية على الرغبة المشتركة للعديد من الدول في تكييف الإطار القائم من أجل تحقيق التعزيز الفعال للعدالة الجنائية في الفضاء السيبراني.

٢٣٠- وذكرت هولندا أن التحدي الكبير في مواجهة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية يتمثل في تمكين الصكوك الحالية من تفعيل كامل إمكاناتها وعدم تحويل الموارد والطاقة الشحيحة أصلاً لتصب في عملية طويلة الأمد سعياً إلى وضع إطار جديد يتجاوز الحدود الوطنية. واتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية هي نتيجة ملموسة قائمة تُثبت قيمتها الإضافية يومياً. وتتمتع أجهزة إنفاذ القانون والسلطات القضائية في بلدان تمتد من الولايات المتحدة إلى سري لانكا ومن اليابان إلى السنغال بإمكانية الاستفادة من الفرص المختلفة التي تتيحها الاتفاقية، محققة نتائج محددة في التحقيقات الجنائية. والبروتوكول الإضافي للاتفاقية هو خطوة جارية بالفعل في إطار الجهود التي يلزم بذلها على الدوام لمواكبة التطورات وتقديم حلول حديثة.

٢٣١- ومع مرور الوقت، بُذلت جهود كبيرة في مجال بناء القدرات، إلا أنه لا يزال يلزم القيام بالكثير من العمل، وهذا هو التحدي الكبير الثاني. ويمكن تحقيق ذلك على أساس ثنائي أو بالاشتراك مع مكتب برنامج الجريمة السيبرانية التابع لمجلس أوروبا ومع المكتب المعني بالمخدِّرات والجريمة. وفيما يخص الأمم المتحدة، يتبوأ بالفعل فريق الخبراء المعني بإجراء دراسة شاملة عن الجرائم السيبرانية مركزاً مثالياً ليكون منصة لتبادل وجهات النظر وأفضل الممارسات. وأفادت هولندا عن حدوث تحسن كبير داخل فريق الخبراء، خلال المشاورات المتعمقة التي جرت في السنوات السابقة والسنة الحالية، في تنفيذ خطة عمله لعام ٢٠١٧. وتتوقع هولندا أن تؤدي هذه العملية إلى تكوين صورة عامة أكثر حداثة وواقعية في عام ٢٠٢١ عن تحديات العدالة الجنائية في الفضاء السيبراني، إضافة إلى تقديم توصيات توجيهية بشأن المستقبل.

٢٣٢- ودعت هولندا إلى مواصلة التحسين الذي أُدخل في عام ٢٠١٧ على عمل فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، وتوقعت أن تتحقق أفضل النتائج بالتركيز على تقديم المساعدة التقنية من أجل تيسير نقل الممارسات الفضلى وبناء القدرات في جميع أنحاء العالم. ودعت هولندا إلى المشاركة في المفاوضات الحالية التي أثبتت فائدتها وحققت نتائج، ودعت الدول الأخرى إلى عدم تحويل الموارد والإمكانات بعيداً عن هذه المفاوضات عبر إطلاق مبادرات جديدة.

نيوزيلندا

٢٣٣- أشارت نيوزيلندا إلى أن العزلة الجغرافية للبلد حمتها عبر التاريخ من بعض المخاطر. إلا أن الطابع العابر للحدود الذي تتصف به الجريمة السيبرانية يعني أن بُعد المسافة لا يوفر للبلد أي حماية. وتشمل التحديات الخاصة التي تواجهها نيوزيلندا في مكافحة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية ما يلي:

(أ) الصورة غير الكاملة عن الجريمة السيبرانية في نيوزيلندا وفي جميع أنحاء العالم؛

(ب) صعوبة حساب تكاليف الجرائم السيبرانية؛

(ج) صعوبة اكتشاف الجرائم السيبرانية والتحقيق فيها وملاحقة مرتكبيها قضائيًّا؛

(د) المسائل الناشئة عن المسؤوليات المشتركة بين الحكومة والمنظمات غير الحكومية والقطاع الخاص والأفراد.

٢٣٤- وأبلغت نيوزيلندا بأنها ركزت، في تصديها للجريمة السيبرانية، على أن تكون التشريعات المناسبة للغرض المنشود منها، واتباع نهج مشترك، وإذكاء الوعي والتثقيف، والتعاون الدولي. وقد اُستخرجت المعلومات المقدمة لأغراض هذا التقرير من الخطة الوطنية للتصدي للجريمة السيبرانية (٢٠١٥)، المتاحة عبر الإنترنت.

٢٣٥- لا توجد صورة مكتملة للجرائم السيبرانية. فهذه الجرائم يمكن تمييزها عن "الجرائم التقليدية" من خلال التحديات التي تفرضها طبيعتها العالمية على أجهزة إنفاذ القانون. ويمكن للأفراد والجماعات خلف البحار العمل أينما يكون الاتصال بالإنترنت متاحاً. وتتخذ الأغلبية الساحقة لمرتكبي هذه الجرائم مقراتها في الخارج، كما أنهم منظمون للغاية. ولا يتم الإبلاغ، في

جميع أنحاء العالم، عن العديد من حالات الجرائم السيبرانية. وفي بعض الحالات، لا يعلم الضحايا أنهم تضرروا. ويشعر ضحايا آخرون بحرج بالغ يمنعهم من الإبلاغ عن الجريمة، أو لا يعرفون الجهة التي يمكن إبلاغها عن الجريمة، أو لا يعتقدون أن أجهزة إنفاذ القانون يمكن أن توفر سبل الانتصاف لهم. وإذا حصل الضحايا على انتصاف من قبل مقدم خدمات أو من مؤسسة مالية، فقد لا يُبلغون أيضاً عن الجريمة. وأخيرا، قد تتردد الأعمال التجارية في الكشف عن الخسائر أو الانتهاكات خشية الضرر الذي قد يلحق بسمعتها.

٢٣٦- ويصعب حساب تكاليف الجرائم السيبرانية، كما أن من الصعب تقدير التكاليف غير المباشرة الناجمة عنها، بما في ذلك تكاليف الفرص الضائعة، تقديراً كميًّا. وبالنسبة للعديد من المنشآت الصغيرة والمتوسطة الحجم، يمكن أن تؤدي الجرائم السيبرانية إلى "الحرمان من ممارسة العمل التجاري"، فقد لا يُسرَق أي شيء ولكن الهجوم يمكن أن يقيد قدرة هذه المؤسسات على الاضطلاع بالتداول التجاري. كما تتكبد الأعمال التجارية والأفراد تكاليف لحمايتها من الجرائم السيبرانية ومعالجة الأضرار (إن لزم الأمر). كما يمكن أن تتيح الجرائم السيبرانية أيضاً تنظيم وارتكاب جرائم مادية، مثل الاحتيال والابتزاز وإثارة الاضطراب والاعتداء الجنسي وغيره من الاعتداءات العنيفة. كما قد تؤدي الجرائم السيبرانية إلى وقوع أضرار اجتماعية من خلال الإحراج والإزعاج، وفي الحالات الأكثر خطورة، قد تؤدي إلى الأذى البدني أو العاطفي. وعلى الرغم من أن الخسائر المالية الناجمة عن الجرائم السيبرانية يمكن أن تكون صغيرة في الحالات الفردية، فإن الآثار الواقعة على ثقة الجمهور واطمئنانه يمكن أن تكون مدمِّرة مع مرور الوقت. وتُدر الجرائم السيبرانية عائدات مرتفعة بتكلفة منخفضة، وتسبب مخاطر منخفضة بقدر معتدل للجاني. وقد تتسبب الآلاف من رسائل البريد الإلكتروني التطفلية في خسائر صغيرة لكل ضحية على حدة، إلا أنها تتسبب في خسارة أكبر بكثير لنيوزيلندا ككل.

٢٣٧- ومن الصعب كشف الجرائم السيبرانية والتحقيق فيها وملاحقة مرتكبيها قضائيًّا. فالعنصر العالمي للجريمة السيبرانية يجعل من الصعب العثور على مرتكبها والوصول إلى الأدلة ذات الصلة بها. ويمكن أن يكون تبادل المعلومات والتعاون بين البلدان المختلفة ضعيفاً، وحتى في حالة وجود علاقات تعاونية قوية، قد تكون الإجراءات التي تنص عليها معاهدة المساعدة القانونية المتبادلة بطيئة ومرهقة للغاية. وقد تتطلب القضايا قدرا غير متناسب من جهود التحقيق، مما يقلل من توافر الموارد اللازمة لتلبية الاحتياجات الأخرى. كما يمكن أن تكون الدولة التي يعمل منها مرتكب الجريمة مفتقرة إلى القدرة اللازمة لإجراء التحقيق أو الحفاظ على الأدلة.

٢٣٨- ومما يزيد من تعقيد التحقيقات إمكانية العمل على شبكة الإنترنت مع إخفاء شبه كامل للهوية. فإسناد الفعل إلى الفاعل في الحادثات السيبرانية صعب للغاية، وخصوصاً عندما ينشأ الهجوم في الخارج. وهذا يجعل الجريمة السيبرانية تحدِّياً ليس فقط من حيث التحقيق فيها بل أيضاً من حيث الملاحقة القضائية لمرتكبيها. إذ يمكن استغلال الخوادم الوكيلة وقنوات مثل شبكة "تور" (Tor) وشبكات النظراء من طرف المجرمين الذين يحاولون إخفاء هويتهم تحت طبقات التشفير. وكثيرا ما تُستخدم هذه الشبكات لتسهيل النشاط الإجرامي، وتفرض تحديات على أجهزة إنفاذ القانون. كما أن هذه الشبكات ومواقع الشبكة الخفية تبيع الجرائم السيبرانية باعتبارها نوعاً من الخدمات، من قبيل تأجير قراصنة مواقع الإنترنت أو توفير حزم الأدوات البسيطة. وتقلل هذه التطورات

من الحواجز التي تحول دون ارتياد عالم الجرائم السيبرانية. ولذلك يمكن لمجموعة من الجهات الفاعلة غير الماهرة أن يكون لها تأثير ضار نسبيًّا. ومن الناحية الأخرى، أخذت الخطوط الفاصلة بين الجهات الفاعلة الإجرامية والجهات الفاعلة الحكومية (التي يمكن أن يتصرف بعضها أيضاً بقصد إجرامي) تنطمس مع انتشار النشاط وتزايد تعقُّد الأساليب. ومع تطور التكنولوجيا واستراتيجيات الكشف، تتطور أيضاً الجهات الفاعلة، مما يصعِّب على الجهات المتصدية مواكبة هذا التطور ولا يُحجِم المجرمون عن استخدام تكنولوجيا إخفاء الهوية، بما في ذلك استخدام برمجيات مثل "تور"، لمحاولة إخفاء المواقع التي توفر مواد استغلال الأطفال وتجارة المخدِّرات.

٢٣٩- واستجابة نيوزيلندا للجريمة السيبرانية هي استجابة مشتركة بين الحكومة والمنظمات غير الحكومية والقطاع الخاص والأفراد. وتقع على عاتق مجموعة من الهيئات الحكومية في نيوزيلندا مسؤوليات سياساتية وتشغيلية تتصل بالجريمة السيبرانية. وقد تطورت هذه الأدوار أساساً بصورة طبيعية وليس وفقا لخطة ما. فالجريمة السيبرانية مشكلة مشتركة، على كل من المنظمات غير الحكومية والمجتمع المدني والقطاع الخاص الاضطلاع بدور في منعها والتصدي لها. ويمكن أن تؤدي هذه المسؤولية المشتركة إلى نشوء تحديات. فسوف يُبلَّغ عن بعض الحوادث إلى جهات متعددة، وقد يُحوَّل الضحايا من هيئة إلى أخرى في محاولة لتحديد أفضل جهة لإيجاد الحل. كما يمكن أن تختلف الاستجابات أيضاً داخل كل من الهيئات. وقد أحرزت نيوزيلندا تقدماً في هذا المجال من خلال إنشاء فريق مواجهة الطوارئ الحاسوبية في نيوزيلندا (CERT NZ) في عام ٢٠١٦، وهو هيئة توفِّر مزيدا من الوضوح بشأن المكان الذي ينبغي الإبلاغ إليه عن حادثات الفضاء الإلكتروني، وتفرز هذه الحادثات وتحولها إلى الهيئات المعنية بكفاءة أكبر، وتوفِّر مشورة ذات طابع عملي أكبر وفي توقيت أنسب للهيئات والأعمال التجارية والأفراد. كما يقوم العديد من شركات القطاع الخاص بالتصدي للجريمة السيبرانية كجزء من الخدمة الأساسية التي تقدمها للعملاء. وهناك مجال للحكومة لتحسين التجربة التي يتعرض لها ضحايا الجرائم السيبرانية، إلى جانب اكتساب فهم أفضل للمسألة وإذكاء الوعي بها.

نيكاراغوا

٢٤٠- ترى نيكاراغوا أن الأحكام الجزائية الحالية غير كافية لمكافحة الجرائم المرتكبة باستخدام تكنولوجيا المعلومات والاتصالات. فقد وقع العديد من الدول ضحية لهذه الجرائم. ولذلك، فإن نيكاراغوا مقتنعة بضرورة تناول هذا الموضوع من طرف الأمم المتحدة، بغية وضع واعتماد اتفاق دولي بشأن التعاون والتنظيم في هذا الموضوع.

٢٤١- وبالمثل، اعتبرت نيكاراغوا أن من المناسب إنشاء فريق عامل مفتوح العضوية في أقرب وقت ممكن، بغية المضي قُدماً في صوغ صك تنظيمي دولي بشأن الجرائم المرتكبة باستخدام تكنولوجيات المعلومات والاتصالات.

النرويج

٢٤٢- أشارت النرويج إلى مساهمتها الوطنية التي أُرسلت إلى المكتب المعني بالمخدِّرات والجريمة في ٤ آذار/مارس ٢٠١٩ حول التدابير والمبادرات الرامية إلى مكافحة الجريمة السيبرانية فيما يتعلق بعمل فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية.(٨)

٢٤٣- وقد صدَّقت النرويج على اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية في عام ٢٠٠٥، وتتابع عملية وضع البروتوكول الإضافي الثاني عن كثب. وتدعم النرويج فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية باعتباره العملية الرئيسية على مستوى الأمم المتحدة فيما يتعلق بموضوع الجريمة السيبرانية، حتى عام ٢٠٢١ على الأقل.

٢٤٤- وذكرت النرويج أنه، مع تطور التهديدات في مجال الجريمة السيبرانية، يجب توسيع نطاق تدابير التصدي للتحديات، لأن الافتقار إلى تدابير فعالة قد يشكل تهديدا لسيادة القانون. فقد أصبحت الأدلة الإلكترونية ذات أهمية متزايدة في القضايا الجنائية. وغالبا ما تخزن هذه البيانات في الخارج، بحيث يصعب تحديد مكانها والحصول عليها. والتعاون عامل أساسي على الصعيدين الوطني والدولي في هذا الصدد. ونظرا لكون أجهزة إنفاذ القانون مقيدة بالحدود الوطنية، يلزم إيجاد أطر عمل دولية أكثر فعالية. وفي الوقت نفسه، يجب أن يكون في صميم الجهود المبذولة الالتزام بالحقوق الأساسية والتحلي بدرجة عالية من الوعي بالتدابير الوقائية عند وضع صكوك دولية جديدة.

٢٤٥- وأكدت النرويج أنها ستضمن توافر القدرات والكفاءات والقدرة التقنية الكافية لمواجهة الأنواع الجديدة والمتغيرة باستمرار من الجرائم. وأشارت النرويج إلى الحاجة إلى زيادة فهم التهديدات التي تواجَه في المجال الرقمي باعتبار ذلك في صميم عملها الوطني. كما أن من المهم رؤية التحديات الجديدة في سياق الجريمة التقليدية. فالجريمة السيبرانية ليست نوعاً منفصلاً من الجرائم، بل هي عنصر مشترك يوجد في العديد من أنواع الجرائم، بما في ذلك الجريمة المنظمة العابرة للحدود الوطنية والإرهاب. والعمل المتضافر بين الحكومات والقطاع الخاص جزء أساسي من الحل.

٢٤٦- وسلطت النرويج الضوء كذلك على أن السلطات النرويجية ستضمن، وفقا للاستراتيجية السيبرانية الدولية للنرويج (٢٠١٧)، التنسيق الوثيق بين الهيئات التي تمثل النرويج في المجالات التي تم فيها وضع سياسات وإقامة تعاون على الصعيد الدولي بشأن الأمن السيبراني فيما يتعلق بالجريمة السيبرانية والتصدي للحادثات السيبرانية. وستدعم النرويج، في إطار الجهود الدولية المستمرة لمكافحة الجريمة السيبرانية، النُّهج التعاونية الرامية إلى إيجاد حلول جيدة، مع التمسك بالقيم الديمقراطية وحماية حقوق الإنسان العالمية.

بيرو

٢٤٧- أفادت بيرو بأنه، في عام ٢٠١٦، أعد مصرف التنمية للبلدان الأمريكية، بالتنسيق مع منظمة الدول الأمريكية، تقرير عام ٢٠١٦ بشأن الأمن السيبراني في أمريكا اللاتينية والكاريبي. وبعد تقييم

(٨) متاحة على الرابط www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Compilation_12March.pdf.

٤٩ مؤشـــرا تناولت مجالات مختلفة (الســـياســـية والاســـتراتيجية، والثقافة والمجتمع، والتعليم، والأطر القانونية، والتكنولوجيات)، حُددت أربعة تحديات رئيسية لبيرو، وهي على النحو التالي:

(أ) تعزيز قدرات الحماية السيبرانية لدى القوات المسلحة؛

(ب) تعزيز القدرات التقنية لشـــعبة التحقيق في جرائم التكنولوجيا العالية على التعامل مع الأدلة الإلكترونية؛

(ج) تعزيز الوعي الاجتماعي بالأمن السيبراني؛

(د) تحسين قدرات أساتذة الجامعات وتوفير التدريب للشركات.

٢٤٨- وطبقا لتقرير الاستخبارات الأمنية الصادر عن شركة مايكروسوفت (*Microsoft Security Intelligence Report*) (لعام ٢٠١٧)، كانت ١٦,٩ في المائة من الحواسيب في بيرو موبوءة ببرمجيات خبيثة، مقارنة بالمعدل العالمي البالغ ٧,٨ في المائة. وعلى غرار ذلك، فإن الإصـــابة من خلال فيروســـات طروادة (Trojans) (٨,١٣ في المائة) والديدان الحاســـوبية (worms) (٥,٧ في المائة) والفيروسات (٠,٩٢ في المائة) في بيرو أعلى من المتوسط العالمي.

٢٤٩- وفي دراســـة حديثة، أشـــارت أمانة الحكومة الرقمية برئاســـة مجلس وزراء بيرو إلى أن ٢٢,٦ في المائة من كيانات الإدارة العامة ليســـت لديها القدرات للازمة لتنفيذ نظامها المعمم للأمن الرقمي. وقد أُبديت الأسباب التالية:

(أ) عدم توفر الموارد الاقتصادية الكافية اللازمة للتنفيذ؛

(ب) عدم توفر عدد كاف من الموظفين (٥٠,٩ في المائة)؛

(ج) عدم توفر المعرفة بقدر كاف لبدء التنفيذ (٢٢,٦ في المائة)؛

(د) أن هذه ليست مسألة ذات أولوية بالنسبة للقطاع الذي تعمل فيه (١٦ في المائة).

٢٥٠- ولمخاطر أمن المعلومات أثر سلبي شديد على الأصول الحيوية للمنظمات، تترتب عليه تكاليف اقتصـادية وسـلبية تتكبدها هذه الكيانات. وفي العديد من الحالات، تنقطع إجراءات العمل الرئيسـية أو تتوقف بينما يجري ابتزاز المنظمات أو تخويفها لتدفع مبالغ كبيرة من المال لاسترجاع المعلومات.

٢٥١- وفيما يتعلق بالتحديات ذات الأولوية، رأت حكومة بيرو أن من الضـــروري تأســـيس مكتب متخصـص تابع للمدعي العام يتولى معالجة الجرائم الحاسـوبية، ومن الضـروري أيضـاً توفير قدر أكبر من التدريب لموظفي الضـرائب بشـأن هذه المسـألة، وإنشـاء مؤسـسـة مسـؤولة عن منع الجرائم السيبرانية في أوساط المواطنين. وقد سُجلت زيادة كبيرة في عدد الشكاوى المتعلقة بالجرائم الحاسوبية، لا سيما تلك التي تتخذ شكل الاحتيال الحاسوبي. وتتمثل التحديات الرئيسية التي يجب مواجهتها فيما يلي:

(أ) الاحتيال الحاسـوبي باسـتخدام معلومات البطاقات المصـرفية أو "الكاردينغ"، الذي تسـتخدم فيه المنظمات الإجرامية المعلومات السـرية الواردة في البطاقات المصـرفية لإجراء عمليات شراء عبر الإنترنت من متاجر الإنترنت التي توجد النطاقات الشبكية والخوادم الخاصة بها في الخارج.

وهذا يصعِّب الحصول على المعلومات في الوقت المناسب من خلال الامتثال لقوانين كل بلد التي تنص على المعلومات التي يتعين على كل شركة تقديمها؛

(ب) سرقة الهوية من خلال الشبكات الاجتماعية، كنتيجة للحرية التي تتيح للمستخدمين إنشاء حساب وتصفح الإنترنت دون الإفصاح عن هويتهم، وحتى إنشاء أسماء مختلفة تُستخدم بطريقة غير مشروعة؛

(ج) إغواء الأطفال، الذي تتظاهر فيه المنظمات الإجرامية بأنها أطفال، من أجل حث ضحاياها على خلع ملابسهم أمام كاميرات الفيديو الخاصة بالحواسيب المحمولة أو الحواسيب المنضدية. وفي حالات أخرى، يتم عقد لقاءات وجهاً لوجه، يجري خلالها الحصول على مواد الاعتداء الجنسي على الأطفال لكي تُباع وتُتبادل مع المتحرشين بالأطفال الآخرين، على الصعيدين الوطني والدولي، بما في ذلك من خلال تطبيقات مثل واتس اب؛

(د) الابتزاز والسلب من جانب الأشخاص ضد شركاء حياتهم السابقين، من خلال استخدام مقاطع فيديو أو صور ذات طابع جنسي، يهدد هؤلاء بنشرها على الإنترنت. وقد يكون ذلك لأغراض مختلفة، مثل الحصول على منفعة اقتصادية أو استئناف العلاقة؛

(هـ) هجمات القراصنة النشطاء المتمثلة في شن حملات تهدف إلى التأثير على صورة المؤسسة مع الاستفادة من الشبكات التي تخفي الهويات، مثل شبكة "تور"، والتي تتيح شن الهجمات من بلدان آسيوية، مما يجعل كشفها أمرا مستحيلاً. وعلى غرار ذلك، تُشَنُّ الهجمات على المعلومات المؤسسية لأغراض تجارية، بغية الحصول على معلومات مستفيضة من الكيانات لأغراض إجرامية. وهناك أيضاً إمكانية أن تقوم وسائل الإعلام بشن هجمات سيبرانية أو تجسس سيبراني من أجل الوصول إلى المواد التي تستحق النشر باعتبارها أخبار هامة.

الفلبين

٢٥٢- أشارت الفلبين إلى أن الجريمة السيبرانية قضية اجتماعية خطيرة، ولاحظت أن الفضاء السيبراني يعتبر بُعدا جديدا (يضاف إلى الأرض والجو والماء) يتعين على الحكومة تنظيمه ويتعين على أجهزة إنفاذ القانون مد ولاياتها إليه من أجل التعامل معه. وبغية ضمان سلامة الناس وأمنهم، أقرت الحكومة بضرورة تزويد أجهزة إنفاذ القانون بما يلزمها من خلال التشريعات التالية: قانون منع الجرائم السيبرانية لعام ٢٠١٢ (قانون الجمهورية رقم ١٠١٧٥)، وقانون التجارة الإلكترونية لعام ٢٠٠٠ (قانون الجمهورية رقم ٨٧٩٢)، وقانون مكافحة الصور الجنسية والتلصص الجنسي لعام ٢٠٠٩ (قانون الجمهورية رقم ٩٩٩٥) ، وقانون مكافحة استغلال الأطفال في المواد الإباحية لعام ٢٠٠٩ (قانون الجمهورية رقم ٩٧٢٥)، وقانون مكافحة الاتجار بالأشخاص لعام ٢٠٠٣ (قانون الجمهورية رقم ٩٢٠٨)، وقانون إصدار لائحة أجهزة الوصول إلى البيانات لعام ١٩٩٨ (قانون الجمهورية رقم ٨٤٨٤) وقانون خصوصية البيانات لعام ٢٠١٢ (قانون الجمهورية رقم ١٠١٧٣).

٢٥٣- وقد انضمت الفلبين إلى اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية في ٢٠ شباط/فبراير ٢٠١٨، واستجابت للطلبات الدولية المتعلقة بحفظ البيانات، وتوفير معلومات المشتركين الخاصة بالمستخدمين، وجمع البيانات الحاسوبية وبيانات الأعمال التجارية، وضبط أسماء النطاقات.

٢٥٤- وفي هذا السياق، تعتبر القوانين الوطنية أن التخصص هو مفتاح النجاح في التحقيق مع مرتكبي الجرائم السيبرانية وملاحقتهم قضائيًا. وبموجب قانون منع الجرائم السيبرانية لعام ٢٠١٢، أنشئت الهيئات المتخصصة التالية للتصدي للجرائم السيبرانية والمسائل ذات الصلة بها:

(أ) مكتب الجريمة السيبرانية التابع لوزارة العدل: وهو السلطة المركزية بموجب قانون منع الجرائم السيبرانية والمعني بضمان تنفيذ اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، بما في ذلك المسائل المتعلقة بالمساعدة الدولية المتبادلة وتسليم المطلوبين؛

(ب) مركز التحقيق في الجرائم السيبرانية والتنسيق بشأنها: وهو هيئة مشتركة بين الأجهزة تعمل تحت الإشراف الإداري لوزارة تكنولوجيا المعلومات والاتصالات، بموجب القانون الجمهوري رقم ١٠٨٤٤ لعام ٢٠١٥، والمسؤول عن تنسيق السياسات بين الهيئات ذات الصلة ووضع خطة الأمن السيبراني الوطنية وإنفاذها؛

(ج) قسم الجريمة السيبرانية التابعة للمكتب الوطني للتحقيقات: أعيد تنظيم هذا القسم من أجل التحسين الفعال لقدراته في مجالات التصدي للجرائم السيبرانية والتحاليل الجنائية الرقمية والأمن السيبراني، وفقا لما ينص عليه قانون الجرائم السيبرانية. وقد أنشأ هذا القسم ثلاثة مراكز إقليمية للجرائم السيبرانية، وحصل على أدوات وبرامج جديدة ومحدَّثة خاصة بالتحاليل الجنائية، مع توفير التدريب المناسب للمحللين الجنائيين التابعين له؛

(د) فريق مكافحة الجرائم السيبرانية التابع للشرطة الوطنية: أنشئ بالتوازي مع تسعة مكاتب إقليمية لمكافحة الجريمة السيبرانية في جميع أنحاء البلد. وقد أعد أربع دورات متخصصة في مكافحة الجرائم السيبرانية، يحتاجها ضباط الشرطة الذين يتخصصون في الجرائم السيبرانية.

٢٥٥- وتقوم القوات المسلحة الفلبينية، بقيادة نائب رئيس أركان دائرة الاتصالات والإلكترونيات ونظم المعلومات، بوضع خطة استراتيجية للفضاء السيبراني لتوفير خارطة طريق لإيجاد منظمة كاملة القدرة في مجال الفضاء السيبراني بحلول عام ٢٠٢٢.

٢٥٦- ومجلس مكافحة غسل الأموال هو وحدة الاستخبارات المالية في البلد، ومكلف بتنفيذ قانون مكافحة غسل الأموال، بصيغته المعدلة بموجب قوانين الجمهورية رقم ٩١٩٤ و١٠١٦٧ و١٠٣٦٥، بالإضافة إلى القانون الجمهوري رقم ١٠١٦٨، المعروف أيضاً باسم قانون منع وقمع تمويل الإرهاب لعام ٢٠١٢.

٢٥٧- وفي كانون الثاني/يناير ٢٠١٧، ساهم الجهاز القضائي أيضاً في الجهود المبذولة لمكافحة الجريمة السيبرانية، من خلال تعيين محاكم مختصة في الجريمة السيبرانية للبت في القضايا المشمولة بقانون منع الجرائم السيبرانية لعام ٢٠١٢، إضافة إلى تعيينها بصفة محاكم تجارية.

٢٥٨- وأبلغت الفلبين أيضاً بأنه، على الصعيد الوطني، أنشئت آليات التعاون التالية المشتركة بين الهيئات:

(أ) اللجنة الفرعية المعنية بالجريمة السيبرانية، التابعة للجنة التنسيق الوطنية لإنفاذ القانون، والتي تعزز التنسيق بين الهيئات لمكافحة الجريمة السيبرانية والأنشطة الأخرى المتصلة بها من خلال تقديم المساعدة إلى حملات مكافحة الجريمة السيبرانية التي تقوم بها دول أخرى، مثل تيسير الحصول إلى المعلومات واعتقال الأشخاص المتورطين في الجرائم السيبرانية؛

(ب) المجلس المشترك بين الهيئات لمكافحة الاتجار بالأشخاص، الذي يصدر القواعد واللوائح التنظيمية للتنفيذ الفعال للقانون الجمهوري رقم ٩٢٠٨، أو قانون مكافحة الاتجار بالأشخاص لعام ٢٠٠٣، بصيغته المعدلة بموجب القانون الجمهوري رقم ١٠٣٦٤، أو القانون الموسَّع لمكافحة الاتجار بالأشخاص لعام ٢٠١٢. ويرأس هذا المجلس وزير العدل، الأمر الذي يؤدي بدوره إلى زيادة سرعة تنسيق المشاريع والبرامج المعنية بالمعالجة الفعالة للمسائل المتعلقة بالاتجار بالأشخاص. ويوصي المجلس بتدابير لتعزيز المساعدة المتبادلة بين البلدان الأجنبية، من خلال ترتيبات ثنائية و/أو متعددة الأطراف، بغية منع وقمع الاتجار الدولي بالأشخاص؛

(ج) المجلس المشترك بين الهيئات لمكافحة استغلال الأطفال في المواد الإباحية، الذي يرأسه وزير الرعاية الاجتماعية والتنمية الاجتماعية، والمؤلف من هيئات حكومية أخرى ومنظمات غير حكومية معنية، ويضع خططاً وبرامج شاملة ومتكاملة لمنع وقمع أي شكل من أشكال مواد الاعتداء الجنسي على الأطفال، ويضطلع برفع دعاوى قضائية ضد الأفراد أو الهيئات أو المؤسسات أو المنشآت التي تنتهك أحكام قانون مكافحة استغلال الأطفال في المواد الإباحية لعام ٢٠٠٩ (قانون الجمهورية رقم ٩٧٧٥).

٢٥٩- وفيما يتعلق بالممارسات الجيدة في إنفاذ القانون والتحقيق، أقرت الفلبين بأهمية استخدام الهيئات المتخصصة في مجالي إنفاذ القانون والتحقيق. وترى الفلبين أن التعاون بين الهيئات أمر أساسي لفعالية إنفاذ القانون وفعالية التحقيق في القضايا، تحت قيادة اللجنة الفرعية المعنية بالجريمة السيبرانية والتابعة للجنة التنسيق الوطنية لإنفاذ القانون، والمجلس المشترك بين الهيئات لمكافحة الاتجار بالأشخاص، والمجلس المشترك بين الهيئات لمكافحة استغلال الأطفال في المواد الإباحية.

٢٦٠- وأُشير أيضاً إلى أن الإنتربول هي آلية أخرى تستخدمها أجهزة إنفاذ القانون، ويقوم المكتب المركزي الوطني للإنتربول في مانيلا بدور هيئة التنسيق الرئيسية لتعاون الشرطة على الصعيدين الوطني والدولي على التصدي للجرائم عبر الوطنية. والتعاون الوثيق مع أجهزة إنفاذ القانون والهيئات الحكومية الأخرى وأجهزة إنفاذ القانون الأجنبية ضروري للتحقيق مع مرتكبي الجرائم السيبرانية وتتبُّعهم وملاحقتهم قضائيًا.

٢٦١- وقد استضاف المركز الفلبيني المعني بالجريمة العابرة للحدود، وهو أمانة المكتب المركزي الوطني للإنتربول في مانيلا، بالاشتراك مع مجلس مكافحة غسل الأموال، الاجتماع العملياتي للإنتربول بشأن قضية الأموال المسروقة من مصرف بنغلاديش، وهي من أكبر قضايا غسل الأموال.

٢٦٢- وفيما يتعلق بالممارسات الجيدة في مجال الأدلة الإلكترونية والممارسات الجنائية، أفادت الفلبين بأن الأجهزة المتخصصة تستخدم التحاليل الجنائية الرقمية لتتبُّع مرتكبي الجرائم السيبرانية والتحقيق معهم ومقاضاتهم. وقد أصبح قانون منع الجرائم السيبرانية لعام ٢٠١٢، الذي اعتمد في ١٢ أيلول/سبتمبر ٢٠١٢، سارياً في ١٨ شباط/فبراير ٢٠١٤. وبالاقتران مع استخدام قواعد الأدلة الإلكترونية الصادرة عن المحكمة العليا، أصبح النظر في قضايا الجرائم السيبرانية في محاكم الجرائم السيبرانية أكثر فعالية.

٢٦٣- وأطلق مركز التحقيق والتنسيق في الجرائم السيبرانية خطة الأمن السيبراني الوطنية ٢٠٢٢ في ٢ أيار/مايو ٢٠١٧، التي أُقر فيها بالحاجة الملحة لحماية كل مستخدم للإنترنت في الفلبين، وحماية الهياكل الأساسية الحيوية الوطنية للمعلومات، والشبكات الحكومية، والمؤسسات الصغيرة والمتوسطة الحجم وسائر الشركات والمؤسسات.

٢٦٤- وحتى مع الجهود التي تبذلها الحكومة لمكافحة الجريمة السيبرانية، إلى جانب الهيئات المتخصصة، وسن قوانين لمكافحة الجريمة السيبرانية، وإنشاء محاكم للجرائم السيبرانية، واستخدام قواعد الأدلة الإلكترونية، لا تزال هناك حاجة إلى توفير التدريب للمتخصصين والخبراء على كيفية استخدام هذه الأدوات. وينبغي الاستفادة من بناء القدرات المستمر، لا سيما المقدم من الجهات الراعية، سواء كانت محلية أو أجنبية. وزيادة على ذلك، ينبغي إجراء عمليات تقدير وتقييم للجرائم السيبرانية والأمن السيبراني دورياً بغية تحديد اتجاه الفلبين فيما تبذله من جهود.

البرتغال

٢٦٥- أفادت البرتغال بأن تكنولوجيا المعلومات والاتصالات تهيئ فرصاً جديدة للمجرمين، وتؤدي إلى ارتفاع معدَّل الجرائم المرتكبة في العالم الرقمي وعبره وتنوعها. وذكرت أن هذه الجرائم لها أثر متزايد على استقرار الهياكل الأساسية الحيوية للدول والمؤسسات وعلى رفاه الأفراد، بسبب تأثيرها على التمتع الكامل بحقوق الإنسان والحريات المدنية. كما أن استخدام التكنولوجيات والإنترنت لنشر المحتوى الإرهابي، ولترويج خطاب الكراهية وترويج التطرف والتشدد، وكذلك لارتكاب جرائم خطيرة أخرى مثل الاعتداء الجنسي على الأطفال والاتجار بالأشخاص وغسل الأموال، كلها أمثلة على شواغل الدول في العصر الرقمي.

٢٦٦- وأشارت البرتغال إلى أن الدول تواجه صعوبات في التحقيقات الجنائية نتيجة لاستخدام تكنولوجيات التشفير، وصعوبة الحصول على الأدلة الإلكترونية وحفظها، ومسألة ممارسة الولاية القضائية في الفضاء السيبراني، وغياب التعاون الدولي في هذا المجال. ويلبي استخدام التشفير حاجة مشروعة للخصوصية وممارسة الحقوق الأساسية، كما يلبي احتياجات الأعمال التجارية والسلطات العامة؛ وقد استثمرت الشركات في تطوير أدوات توفر حماية أفضل لخصوصية عملائها، مصرحة بأن الجهود المبذولة لإضعاف التشفير يمكن أن تجعل المعلومات الخاصة مكشوفة لمن قد يسيئون استخدامها. وتُعتبر المعالجة الآمنة للبيانات عنصراً مهماً لحماية البيانات الشخصية، والتشفير معترف به كتدبير أمني في اللائحة التنظيمية رقم ٦٧٩/٢٠١٦ للبرلمان الأوروبي ومجلس الاتحاد الأوروبي. إلاَّ أنَّ تكنولوجيات التشفير، في حين تحافظ على أمن البيانات أو المعلومات، تتيح أيضاً فرصا جيدة للمجرمين.

٢٦٧- وهناك تحدٍ آخر يواجه التحقيقات والملاحقات القضائية، وهو كيفية الحصول على الأدلة الإلكترونية المخزَّنة في النظم الحاسوبية وتأمينها، بالنظر إلى حجمها ودرجة تعقُّدها. ويمكن تقديم الخدمات القائمة على الشبكات من أي مكان، دون الحاجة إلى وجود هياكل مادية أو مرافق أو موظفين في الدولة المعنية. ومن ثم فكثيراً ما تُخزن الأدلة ذات الصلة على خوادم خارج الدولة التي تقوم بالتحقيق، وفي ولاية قضائية أجنبية واحدة أو عدة ولايات قضائية أجنبية، أو حتى في ولاية قضائية غير معروفة، وقد تشارك فيها جهات متعددة الجنسيات تقدم الخدمات.

٢٦٨- وبسبب عدم وجود ارتباط بين سلطات التحقيق القائمة في الولايات القضائية المختلفة، تستوجب طلبات التعاون القضائي غالباً الحصول على الأدلة الإلكترونية عبر الحدود، وغالبا ما يتم توجيهها إلى دول تضم عددا كبيرا من مقدِّمي الخدمات ولكن ليست لها علاقة محددة بالإجراءات ذات الصلة. وقد يستغرق الحصول على الأدلة من خلال التعاون القضائي فترات زمنية طويلة، قد لا تعود خلالها هذه الأدلة متاحة. وتكمن الصعوبة الأخرى في عدم وجود إطار واضح للتعاون مع مقدِّمي الخدمات من القطاع الخاص، مع تباين النُّهج الوطنية بشأن هذا التعاون.

٢٦٩- وأشارت البرتغال إلى منع ومكافحة التحريض على الإرهاب ونشر المحتوى الإرهابي وترويج التطرف والتشدد على الإنترنت وعبر سائر تكنولوجيات المعلومات والاتصالات، باعتبار هذه تحديات أخرى تواجهها الدول على المستوى الدولي.

٢٧٠- ومسألة مكافحة الجرائم المرتكبة من خلال تكنولوجيا المعلومات والاتصالات والجريمة السيبرانية هي مسألة ذات أهمية استراتيجية للبرتغال، الملتزمة بشدة بهذه المكافحة. وقد اعتُمد قانون بشأن الجرائم الحاسوبية (القانون رقم ١٩٩١/١٠٩) في عام ١٩٩١ ونُقح في عام ٢٠٠٩ (القانون رقم ٢٠٠٩/١٠٩ (قانون الجرائم السيبرانية)). وتخضع الاستراتيجية الوطنية للأمن في الفضاء السيبراني (٢٠١٥) للمراجعة حاليًا، ومن المتوقع نشر استراتيجية وطنية جديدة في غضون الأشهر المقبلة. ويشار إلى مسألتي استخدام تكنولوجيا المعلومات والاتصالات والجريمة السيبرانية على أنهما من أهم المسائل في الاستراتيجيتين القديمة والجديدة كلتيهما.

٢٧١- وأبلغت البرتغال أيضاً بإجازة قانون بشأن الاحتفاظ بالبيانات المولَّدة أو المعالجة فيما يتعلق بتوفير خدمات الاتصالات الإلكترونية المتاحة للجمهور أو شبكات الاتصالات العامة. وهذا القانون مهم بصفة خاصة للتحقيق الجنائي في الجرائم الخطيرة، من قبيل الإرهاب والجريمة المنظمة.

٢٧٢- واعتبرت البرتغال أن وجود إطار قانوني محلي مناسب وعصري، ينص على أدوات وصلاحيات إجرائية مناسبة، ومن ثم يسمح لسلطات إنفاذ القانون والمدعين العامين بفحص الأدلة الرقمية وجمعها مع احترام حقوق وضمانات المشتبه فيهم والضحايا على حد سواء، هو عامل أساسي لمحاربة الجريمة السيبرانية.

٢٧٣- وأنشأت البرتغال وحدات متخصصة تابعة لأجهزة إنفاذ القانون والقضاء في البلد. ففي دائرة الادعاء العام، أنشئ مكتب الجرائم السيبرانية في عام ٢٠١١، وفي الشرطة الجنائية، أنشئت الوحدة الوطنية لمكافحة الجريمة السيبرانية والجريمة التكنولوجية، التي تعمل وتنسق على الصعيد الوطني. ودائرة

الادعاء العام مسؤولة عن التحقيقات الجنائية، والشرطة الجنائية هي سلطة إنفاذ القانون ذات الاختصاص الحصري للتحقيق في الجرائم السيبرانية والجرائم المرتكبة عبر استخدام تكنولوجيا المعلومات والاتصالات، وتعمل تحت إشراف المدعي العام المسؤول، كما هو محدد في قانون تنظيم التحقيقات الجنائية (القانون رقم ٢٠٠٨/٤٩). ويزيد هذا التخصص من كفاءة التحقيقات، ويضمن تدابير التصدي المتسقة والتنسيق الدولي. والتعاون الدولي مهم للحصول على الأدلة من أي بلد آخر، وينبغي بذل الجهود، لا سيما على مستوى الأمم المتحدة، لبناء القدرات وزيادة التعاون.

٢٧٤- وفيما يتعلق بالتحديات الأخرى، أشارت البرتغال إلى أن الجرائم السيبرانية واستخدام تكنولوجيا المعلومات والاتصالات لارتكاب الجرائم أمران لا تحدهما الحدود الإقليمية؛ لأنهما يرتكبان على الصعيد العالمي. وتُستخدم الخدمات العالمية (مثل خدمات البريد الإلكتروني والشبكات الاجتماعية والخدمات السحابية) في كل مكان، وقد تُستخدم أيضاً لأغراض إجرامية تستهدف ضحايا من العديد من الدول المختلفة. وبينما تدرك بعض الدول الحاجة إلى السرعة في معالجة القضايا التي تنطوي على أدلة رقمية فإن دولاً أخرى تصر على استخدام أدوات تقليدية، من قبيل طلبات المساعدة القانونية المتبادلة، لا تسمح بتلبية المتطلبات أو مواجهة التحديات الراهنة في الوقت المناسب. ولا توجد أية لوائح تنظيمية دولية شاملة قائمة، ولا توفر الأطر الوطنية حلولاً متنوعة، ومن ثم فهناك حاجة إلى نهج جديد.

٢٧٥- وذكرت البرتغال أيضاً أن الأطراف في اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية تقوم بصوغ بروتوكول إضافي للاتفاقية. ومن المتوقع أن يوفر هذا البروتوكول توجيهات واضحة لأجهزة إنفاذ القانون والسلطة القضائية بشأن الوصول إلى البيانات عبر الحدود وتحسين التعاون غير الرسمي وتبادل المعلومات وسير إجراءات المساعدة القانونية المتبادلة من أجل الحصول على البيانات المخزنة في ولايات قضائية أخرى، مع الاحترام الكامل للحقوق والحريات الأساسية.

٢٧٦- وعلى مستوى الاتحاد الأوروبي، يجري التفاوض حول وضع لائحة تنظيمية وتوجيه بشأن الأدلة الإلكترونية، سيتيحان تأمين الأدلة الإلكترونية وجمعها وتحسين التعاون في هذا المجال.

قطر

٢٧٧- قالت قطر إن إساءة استخدام موارد وتكنولوجيات المعلومات، بما في ذلك من خلال الجرائم السيبرانية والقرصنة الإلكترونية، تشهد زيادة، مما يؤثر على أمن البلدان واستقرارها. وقد استُعرضت الآثار الضارة لاستخدام موارد أو تكنولوجيات المعلومات على التنمية والسلام والاستقرار وحقوق الإنسان استعراضاً مفصَّلاً في مختلف القرارات الصادرة من كيانات الأمم المتحدة. وتؤثر الجرائم المرتكبة في العالم الرقمي، وتنوعها المتزايد، واستخدام هذه التكنولوجيات والوسائل لأغراض تتعارض مع هدف الحفاظ على الاستقرار والأمن الدوليين، تأثيراً سلبيًّا على سلامة الهياكل التحتية للدول، وتضر بأمنها ميدانيًّا.

٢٧٨- وهناك حاجة إلى تعزيز التدابير القانونية على الصعيدين الوطني والدولي من أجل التصدي للجريمة السيبرانية، واقتراح تدابير جديدة لمكافحة الجريمة السيبرانية والكشف عنها والتحقيق فيها ومقاضاة مرتكبيها. ومن الضروري تكثيف الجهود الدولية المبذولة لمنع استخدام الموارد الإجرامية

أو تكنولوجيات المعلومات لأغراض إجرامية وإرهابية. ومن أجل صون السلام والاستقرار وتهيئة بيئة منفتحة وآمنة ومستقرة وسلمية لتكنولوجيا المعلومات والاتصالات، أكدت قطر من جديد دعمها لفريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، ودعت إلى استمراره.

٢٧٩- وأفادت قطر بأنها تسعى إلى تعزيز أمن المعلومات داخل الدولة وتشجيع التعاون الدولي على مكافحة الجريمة السيبرانية، لا سيما وأنها كانت ضحية القرصنة الإلكترونية، التي شكلت غطاءً لإحداث أزمة إقليمية مصطنعة ألحقت أضراراً بالغة بالأمن والاستقرار على الصعيدين الإقليمي والدولي. وتولي قطر اهتماماً خاصًّا لتطوير تشريعاتها وتعزيز العمل الدولي المشترك الرامي إلى منع الجرائم السيبرانية والكشف عنها ومقاضاة مرتكبيها.

٢٨٠- وقد أصدرت قطر القانون رقم (١٤) لعام ٢٠١٤ لمكافحة الجرائم الإلكترونية، الذي يشكل خطوة متقدمة في سبيل تعزيز التشريعات والإجراءات الوطنية لمكافحة الجريمة السيبرانية. ويتضمن القانون فصولاً تُعرف الجرائم السيبرانية، مثل جرائم التعدي على نظم وبرامج و شبكات المعلومات، وجرائم الاحتيال والتزوير الإلكترونيين، وجرائم انتهاك حقوق الملكية الفكرية. وينص القانون على أحكام بشأن إجراءات التحقيق وجمع الأدلة والتزامات مقدمي الخدمات والتزامات أجهزة الدولة والتعاون الدولي، بما في ذلك المساعدة القانونية المتبادلة وتسليم المجرمين.

٢٨١- وخلصت قطر إلى أن الجريمة السيبرانية، بوصفها شكلاً مستجداً من أشكال الجريمة المنظمة عبر الوطنية، تمثل تحدياً متنامياً ومتغيراً، وتستلزم استجابات جماعية منسقة ومتزايدة تستند إلى مبدأ المصلحة المشتركة والمسؤولية المشتركة. وفي هذا السياق، تسعى قطر إلى تعزيز تعاونها مع المكتب المعني بالمخدِّرات والجريمة من أجل بناء القدرات الوطنية وتعزيز أمن الشبكات الحاسوبية ودعم التعاون الإقليمي والدولي من أجل توفير بيئة سيبرانية آمنة وقوية.

رومانيا

٢٨٢- قالت رومانيا إن التكنولوجيا، إذ تتقدم، تؤدي دوراً مهماً في مجموعة واسعة من الأنشطة الإجرامية، مع إحداث أثر وتأثير كبيرين على بيئة الإنترنت. ويمثل مصطلح "الجريمة السيبرانية" مجموعة واسعة من التهديدات الإجرامية، مثل توزيع فيروسات الفدية (ransomware) وغيرها من البرامجيات الضارة، والاحتيال الذي ينطوي على مدفوعات غير نقدية، واستخدام الإنترنت في تجارة مواد الاستغلال الجنسي للأطفال.

٢٨٣- ووصفت رومانيا "الجريمة المعتمِدة على الفضاء السيبراني" بأنها أي جريمة لا يمكن ارتكابها إلا باستخدام الحواسيب أو الشبكات الحاسوبية أو غيرها من أشكال تكنولوجيا المعلومات والاتصالات. أما "الجرائم المُيسَّرة بالفضاء السيبراني" فيمكن ارتكابها إما على الإنترنت أو خارجها. والدور الذي تؤديه الإنترنت هو زيادة مدى هذه الجرائم ونطاقها الجغرافي وسرعة ارتكابها. ويشكل الاستغلال الجنسي للأطفال عبر الإنترنت أسوأ جانب من الجرائم المُيسَّرة بالفضاء السيبراني. وعلاوةً على ذلك، تستضيف الشبكة الخفية عدداً متزايداً من المنتديات المخصصة تحديداً لإنتاج مواد الاستغلال الجنسي للأطفال وتبادلها وتوزيعها. وبالإضافة إلى ذلك،

تتيح الإنترنت مجموعة واسعة من التطبيقات، مثل التشارك في الملفات بين الأقران وتخزين البيانات الآمن، تسهل ارتكاب هذه الجرائم.

٢٨٤- وأشارت رومانيا إلى الاحتيال الذي يتعلق بمدفوعات غير نقدية باعتباره تهديداً آخر عالي التنظيم وشديد التخصص ولا ينفك يتطور، ويتكيف مع التدابير المضادة والتقنيات الحديثة. ويتضمن هذا التهديد نوعين مختلفين من الجرائم: الاحتيال ببطاقة غير موجودة، الذي يُرتكب أساساً على الإنترنت، أو الاحتيال ببطاقة موجودة، الذي عادةً ما يحدث في متاجر التجزئة والآلات المصرفية. ويسيطر المجرمون أيضاً على نظم تشغيل الآلات المصرفية للحصول على الأموال النقدية بسهولة أكبر.

٢٨٥- وتفيد تقارير بأنه يمكن أيضاً استخدام المنصات التجارية عبر الإنترنت من أجل التجارة في سلع وخدمات غير مشروعة. وتتيح الأسواق غير المشروعة القائمة على الإنترنت، أي على الشبكة الظاهرة والشبكة الخفية على حد سواء، أدوات، من قبيل مجموعات أدوات الجرائم السيبرانية أو الوثائق المزيفة، يمكن استخدامها لارتكاب جرائم أخرى.

٢٨٦- وذُكر أيضاً أن البيانات المسروقة هي سلعة أخرى تشيع المتاجرة بها عبر الإنترنت وتُستخدم لاحقاً من أجل تعزيز الاحتيال. وعادةً ما تكون هذه البيانات مالية، مثل بيانات بطاقة دفع مسروقة أو بيانات تسجيل دخول إلى حساب مصرفي مسروقة. وقد تتضمن أيضاً بيانات تمتد من قوائم التفاصيل الشخصية الكاملة والوثائق المستنسخة إلى قوائم البريد الإلكتروني وتسجيلات الدخول إلى الحسابات عبر الإنترنت.

٢٨٧- وقالت رومانيا إن المجرمين يستفيدون من كل قناة اتصال متاحة، لا للاتصالات الداخلية فحسب بل أيضاً للاتصال بالضحايا المحتملين، على سبيل المثال، من خلال حملات التصيد الاحتيالي للبريد الإلكتروني أو وسائل التواصل الاجتماعي. ويستخدم المجرمون أيضاً تطبيقات آمنة وخدمات مماثلة لإخفاء أنشطتهم الإجرامية. ويشكل تزايد استفادة المجرمين من خدمات التشفير ومن الجهات الفاعلة الشريرة الأخرى عقبة خطيرة أمام الكشف عن جميع أنواع الجرائم والتحقيق فيها ومقاضاة مرتكبيها، بما في ذلك جريمة الإرهاب.

٢٨٨- كما أن أشكال الدفع الجديدة، مثل العملات المشفرة والدفع عبر الإنترنت والمنصات المصرفية، أتاحت للمجرمين سبلاً جديدة لتمويل أعمالهم التجارية الإجرامية وتوسيع نطاقها. وتشكل سرعة معالجة المعاملات عبر ولايات قضائية عدة وانتشار أدوات التشفير وإخفاء الهوية بعض أهم العقبات التي تواجَه في التحقيقات المالية. والبيتكوين هي العملة الأكثر استخداماً في المدفوعات بين المجرمين فيما يتعلق بالجرائم السيبرانية. وهي مقبولة في معظم الأسواق القائمة على الشبكة الخفية والمحلات الآلية التي تبيع بالبطاقات، ولكن يتزايد استخدامها في الجرائم المرتكبة خارج الفضاء السيبراني، مثل دفع الفدية في عمليات الاختطاف.

٢٨٩- وسلطت رومانيا الضوء على أن الجريمة السيبرانية في البلد تطورت بطريقة مماثلة لتطور ظواهر إجرامية عالمية أخرى، على النحو المبين في تقارير اليوروبول خلال الفترة ٢٠١٤-٢٠١٧. وكانت جماعات إجرامية مؤسسة في رومانيا نشطة بصورة ملحوظة في مجال الجرائم السيبرانية.

ومع مرور الوقت، أصبحت رومانيا أيضاً هدفاً لهذه الجرائم، التي تشكل تهديداً للأمن القومي بالمعنى الواسع، بما يشمل النظام المالي.

٢٩٠- وأفادت رومانيا بأنها بذلت جهوداً كبيرة لاعتماد تشريعات إجرائية شاملة لتغطية مختلف جوانب الإجراءات الجنائية الخاصة بجمع الأدلة الإلكترونية، بما يتوافق مع الضمانات وسبل الانتصاف المتعلقة بسيادة القانون، واستناداً إلى اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية. وقد صدقت رومانيا على هذه الاتفاقية في عام ٢٠٠٣. ويغطي التشريع الوطني الذي يجرِّم الأنشطة غير المشروعة، على النحو المنصوص عليه في المواد من ٢ إلى ٩ من الاتفاقية، مجموعة كبيرة من أنواع سوء السلوك، بما يتيح للوحدات المتخصصة التحقيق في الحالات ذات الصلة. وما زالت هذه الأحكام - بعد مرور ١٥ عاماً على سنِّها - تنطبق على الأشكال الجديدة من الجرائم السيبرانية. وتقدِّم المذكرات التوجيهية التي اعتمدتها اللجنة المعنية باتفاقية الجريمة السيبرانية إرشادات إضافية بشأن العناصر التي تشكل هذه الجريمة.

٢٩١- وحسبما سبق الإبلاغ به، أُنشئت في عام ٢٠٠٤، ضمن مكتب النيابة العامة في رومانيا، مديرية التحقيق في الجريمة المنظمة والإرهاب. وعلاوةً على ذلك، أُنشئت في إطار جهاز الشرطة مديرية مكافحة الجريمة المنظمة، باعتبارها كياناً متخصصاً لدعم أنشطة مديرية التحقيق في قضايا الجريمة المنظمة والإرهاب. وفي الأعوام الخمسة الماضية، أُجريت تحقيقات بشأن أكثر من ٨٠٠ ٢٨ قضية من قضايا الجرائم المعتمِدة على الفضاء السيبراني أو الجرائم التي يتيح الفضاء السيبراني ارتكابها.

٢٩٢- وأشارت رومانيا إلى مثال على هذه الجرائم، وهو أنشطة "الاستنساخ" (skimming) المستخدمة لسرقة بيانات البطاقات المصرفية، والتي تتعلق بأنشطة تقوم بها جماعات إجرامية في العديد من الولايات القضائية المختلفة (تصنيع الأجزاء، وتجميع الأجزاء، والاحتيال الفعلي). وتنطبق على هذه الأنشطة أحكام المادة ٣٦٥ من القانون الجنائي. وفيما يتعلق بأساليب العمل، ما زالت تقنيات الاستدراج الموجَّه (social engineering)، والتصيد الاحتيالي الموجَّه (spear-phishing)، واستعمال المستويات المتعددة من خوادم القيادة والسيطرة، ومسح نقاط الضعف (vulnerability scanning)، تشكل بعض التقنيات الأكثر استخداماً. ومن التحديات الكبيرة التي تواجه إنفاذ القانون تزايد استخدام الأدوات المفتوحة المصدر من جانب مجموعة واسعة من الجهات الفاعلة، بما يجعل من الصعب عزو النشاط غير القانوني إلى أشخاص معينين أو مجموعات معينة. وذكرت رومانيا أن هجمات البرامجيات الضارة مشمولة بالتشريعات الوطنية في المادة ٢٠٧ (الابتزاز) والمادتين ٣٦٢ و٣٦٣ من القانون الجنائي.

٢٩٣- وأشارت رومانيا إلى أن أساليب الاستدراج الموجَّه المستخدمة في ارتكاب جريمة الاحتيال (التصيد الاحتيالي العام (phishing)، والتصيد الاحتيالي الموجَّه (spear-phishing)، والتصيد الاحتيالي الصوتي (vishing)، والتصيد الاحتيالي عن طريق خدمة الرسائل القصيرة (smishing))، بالإضافة إلى تقنيات الهجوم عبر وسيط وتقنيات الهجوم عبر المتصفحات، المستخدمة في أغلب الأحيان لاختلاس تحويلات الأموال، هي أشكال شائعة للجرائم السيبرانية في رومانيا. وهي مُجرَّمة بموجب المادتين ٣٢٥ و٢٤٩ من القانون الجنائي (بحسب القضية المحددة، يمكن توجيه تُهم إضافية، مثل إساءة استعمال الأجهزة أو التدخل في البيانات). ويتم التحقيق في استخدام

منصة Cobalt Strike لشن هجمات على النظام المصرفي بموجب أحكام المواد ٣٦٠ و٣٦٢ و٣٦٣ و٣٦٦ و٢٤٩ من القانون الجنائي.

٢٩٤- وتخضع أنشطة تعدين العملات المُشفَّرة (cryptocurrency mining) ومعظم أنشطة اختطاف العملات المشفَّرة (crypto-jacking) للتحقيق بموجب المادتين ٣٦٠ و٣٦٦ من القانون الجنائي. كما تخضع أنشطة الاستنساخ العميق لبيانات البطاقات المصرفية (deep insert skimming) للتحقيق بموجب المادتين ٣٦٠ و٣٦٦ من القانون الجنائي.

٢٩٥- وخلصت رومانيا إلى أن وضع إطار قانوني شامل يستند إلى اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية وإنشاء مؤسسات متخصصة قد ساعدا على معالجة المشكلة التي لا تنفك تتغير المتمثلة في الجريمة السيبرانية والأدلة الإلكترونية. وفي هذه المرحلة، هناك حاجة إلى موارد إضافية ومزيد من التدريب وبناء القدرات. ولن تكون المناقشات بشأن معاهدات دولية جديدة في هذا المجال مفيدة، وقد تُضعف الجهود المبذولة.

الاتحاد الروسي

٢٩٦- أشار الاتحاد الروسي إلى أن تحدي مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية أصبح، من حيث أبعاده ونطاقه، منذ فترة طويلة، تهديداً عالميًّا يؤثر على جميع بلدان العالم دون استثناء. وفي الوقت الحاضر، ليس لدى المجتمع العالمي نهج موحد إزاء هذه المسألة. وعلى المستوى الدولي، يتفاقم الوضع بسبب عدم وجود إطار قانوني دولي شامل للتعاون، وحتى عدم وجود أساس مصطلحي مشترك. وعلى المستوى الإقليمي، استحدث عدد من المنظمات واعتمد صكوكاً ذات صلة، غير أن قدرة هذه الصكوك على معالجة هذه الجرائم بفعالية ما زالت غير كافية.

٢٩٧- وذكر الاتحاد الروسي أن عدداً من الدول يروج لاتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية بوصفها حلاً ممكناً. غير أن هذا الصك غير كافٍ لمواجهة التهديدات الحالية. فقد وُضعت هذه الاتفاقية في نهاية التسعينات، وهي لذلك لا تنظم الكثير من "اختراعات" المجرمين العصرية. كما أنها تتيح إمكانية انتهاك مبدأ سيادة الدول ومبدأ عدم التدخل في الشؤون الداخلية للدول الأخرى. ومن ثم لا يزال هناك خطر إضفاء الشرعية على قيام دوائر خاصة في مجموعة محدودة من البلدان بجمع البيانات الشخصية الخاصة بالمستخدمين في جميع أنحاء العالم دون ضوابط، فضلاً عن استمرار الاتجاه الذي حدده عدد من الدول من أجل توطيد المكاسب التكنولوجية لتلك الدول في فضاء المعلومات والحفاظ على "فجوة رقمية" بين البلدان المتقدمة والبلدان النامية.

٢٩٨- وأكد الاتحاد الروسي أنه يشجع على وضع مبادئ وقواعد عالمية تتشارك فيها جميع الأطراف المهتمة وتضع الأساس للتعاون الدولي الفعال على مكافحة الجريمة السيبرانية. ويمكن أن يكون هذا الصك هو اتفاقية لمكافحة الجرائم المتعلقة باستخدام تكنولوجيات المعلومات والاتصالات، تبرم تحت رعاية الأمم المتحدة، وتراعي الواقع الراهن ومبدأ المساواة في السيادة ومبدأ عدم التدخل في الشؤون الداخلية للدول. ويمكن لمشروع اتفاقية الأمم المتحدة للتعاون

في مكافحة الجريمة الإلكترونية، الذي قدمته روسيا وعمم بصفة وثيقة رسمية (A/C.3/72/12)، أن يشكل أساساً لهذا العمل. ويعتقد الاتحاد الروسي أن هذا المشروع سيصبح "حافزاً للتفكير"، وسيثير مناقشة هذا الموضوع في المنتديات الدولية الرئيسية، ولا سيما الأمم المتحدة، وسيوطد ويركز جهود المجتمع الدولي الرامية إلى وضع حلول عملية في هذا الصدد.

٢٩٩- ويرى الاتحاد الروسي أنه، بالنظر إلى الطبيعة العالمية لظاهرة الجريمة المعلوماتية، لا يكفي حصر مناقشة المسائل في إطار منتدى فيينا الخاص بالأمم المتحدة - أي فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية. فولاية فريق الخبراء يقتصر معظمها على مناقشة الجوانب التقنية لهذه المسألة. وفي هذا السياق، يُعتبر البحث عن حل سياسي وبناء توافق في الآراء هو المهمة الأساسية.

٣٠٠- ولبلوغ هذه الغاية، يؤكد الاتحاد الروسي على أنه ينبغي تنفيذ أحكام قرار الجمعية العامة ١٨٧/٧٣، بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، تنفيذاً صارماً. ويتمثل حل آخر في إطلاق منتدى دائم داخل الجمعية العامة ليناقش، على أساس نهج متكامل ومتوازن، جميع جوانب التعاون الدولي على مكافحة الجريمة السيبرانية، بهدف إيجاد حل سياسي وبناء توافق الآراء، مع مراعاة الاحتياجات العاجلة للدول في هذا المجال وتيسير تبادل أفضل الممارسات في هذا الصدد. ويتمثل أحد الخيارات المتعلقة بهذا المنتدى في إنشاء فريق عامل مفتوح العضوية للأمم المتحدة معني بالجريمة السيبرانية، تُسند إليه ولاية إعداد وتنفيذ أي وثائق ذات صلة تصدرها الدول الأعضاء.

المملكة العربية السعودية

٣٠١- أشارت المملكة العربية السعودية إلى العقبات التالية أمام مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية:

(أ) ضعف تعاون شركات المنصات الرقمية مع السلطات القانونية وسلطات إنفاذ القانون في جميع أنحاء العالم؛

(ب) غياب الهوية الرقمية في العالم الافتراضي، واستخدام محددات هوية وبيانات وهمية وانتحال هوية أشخاص آخرين على الإنترنت، ولا سيما على وسائل التواصل الاجتماعي؛

(ج) تباين التشريعات والقوانين الجنائية للدول الأعضاء؛

(د) الافتقار إلى التنسيق والتعاون والمساعدة بين البلدان بشأن مكافحة الجريمة السيبرانية؛

(هـ) عدم كفاية الضوابط على تقديم الخدمات الإلكترونية (الشبكات، والموارد، والبيئات السحابية، والخدمات، وغيرها) في بلدان كثيرة؛

(و) الافتقار، في بلدان كثيرة، إلى نظم المعلومات المتطورة التي تتيح رصد العمليات المشبوهة وتحديد مصادرها ومَن يقف وراءها؛

(ز) ضعف القدرات البشرية والتقنية والمؤسسات الحكومية والخاصة والأفراد في مجال الأمن السيبراني؛

(ح) غياب تشريعات دولية لتجريم وتتبع استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، وهي تشريعات يمكن أن تسهم في الجهود الدولية المبذولة في سبيل مكافحة هذه الجرائم؛

(ط) الحاجة إلى تطوير مؤهلات العاملين في مجال أمن المعلومات من خلال برامج تدريبية متخصصة؛

(ي) التعدد والتنوع بين البلدان في التشريعات والقوانين التي تعاقب على السلوك الإجرامي في مجال تكنولوجيا المعلومات؛

(ك) تهدف منصات التجارة على شبكة الإنترنت إلى تحقيق الربح فحسب. وبالإضافة إلى ذلك، تتيح هذه المنصات أرضية خصبة للبرامجيات الحاسوبية والتطبيقات التي تستخدم التكنولوجيا لإخفاء المستخدمين وارتكاب الجرائم السيبرانية؛

(ل) اتساع نطاق الجرائم المرتكبة باستخدام تكنولوجيا المعلومات وإمكاناتها العابرة للحدود، مما يؤدي إلى ضعف التنسيق والاتصال بين الدول من أجل مكافحة هذه الجرائم؛

(م) استبدال العملات التقليدية بعملات رقمية يسهِّل على الجماعات الإجرامية إخفاء الكثير من معاملاتها المالية على الإنترنت؛

(ن) ضعف الوعي بالاستخدام الآمن والأمثل لتكنولوجيا المعلومات والإنترنت؛

(س) ضرورة مشاركة المملكة العربية السعودية في التشريعات الدولية الرامية إلى مكافحة إساءة استخدام التكنولوجيا؛

(ع) الحاجة إلى تكثيف الوقاية من خلال زيادة الوعي في المجتمعات بشأن الأساليب التي تستخدمها العصابات الإجرامية الناشطة على الإنترنت.

صربيا

٣٠٢- أفادت صربيا بأن تنظيم واختصاصات مكتب المدعي الخاص المعني بجرائم التكنولوجيا العالية في صربيا منصوص عليهما في قانون تنظيم واختصاصات السلطات الحكومية المعنية بمكافحة الجريمة السيبرانية، الذي دخل حيز النفاذ في ٢٥ تموز/يوليه ٢٠٠٥، وقانون إدخال تعديلات على قانون تنظيم واختصاصات السلطات الحكومية المعنية بمكافحة الجريمة السيبرانية، الذي دخل حيز النفاذ في ١ كانون الثاني/يناير ٢٠١٠. وبناءً على ذلك فإن مكتب المدعي الخاص هو المختص في إقليم صربيا بتناول القضايا التي تنطوي على الجرائم المذكورة أعلاه.

٣٠٣- وأشارت صربيا إلى إطارها التشريعي والاستراتيجي، الذي يشمل ما يلي:

(أ) قانون تنظيم واختصاصات السلطات الحكومية المعنية بمكافحة الجريمة السيبرانية؛

(ب) قانون التصديق على اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية؛

(ج) قانون التصديق على البروتوكول الإضافي ل اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، المتعلق بتجريم الأعمال المتسمة بطابع العنصرية وكراهية الأجانب المرتكبة بواسطة النظم الحاسوبية؛

(د) قانون التصديق على اتفاقية مجلس أوروبا بشأن حماية الأطفال من الاستغلال الجنسي والاعتداء الجنسي؛

(هـ) القانون الجنائي؛

(و) قانون الإجراءات الجنائية؛

(ز) قانون الاتصالات الإلكترونية؛

(ح) قانون أمن المعلومات؛

(ط) استراتيجية مكافحة الجريمة ذات الصلة بالتكنولوجيا العالية للفترة ٢٠١٩-٢٠٢٣؛

(ي) استراتيجية تطوير مجتمع المعلومات في صربيا حتى عام ٢٠٢٠؛

(ك) التقييم الاستراتيجي للأمن العام في جمهورية صربيا.

٣٠٤- وتشدد الإصلاحات الأخيرة التي أُدخلت على التشريعات المحلية على أهمية اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية وبروتوكولها الإضافي.

٣٠٥- وفي أيلول/سبتمبر ٢٠١٨، اعتمدت الحكومة الاستراتيجية الوطنية المتعلقة بمكافحة الجريمة السيبرانية وخطة العمل التي ترافقها. وعلاوة على ذلك، أنشأت وزارة العدل أفرقة عاملة من أجل تعديل القانون الجنائي وقانون الإجراءات الجنائية. ولهذا الغرض، استهل ممثلون عن مكتب المدعي العام ومكتب المدعي الخاص المعني بالجريمة ذات الصلة بالتكنولوجيا العالية بعثة خبراء في آذار/مارس ٢٠١٩ ضمن مشروع iPROCEEDS (استهداف عائدات الجريمة على الإنترنت في جنوب شرق أوروبا وتركيا) المشترك بين الاتحاد الأوروبي ومجلس أوروبا. وكانت مهمتهم إجراء تحليل متعمق للثغرات القانونية الموجودة في التشريعات الوطنية، وتقييم مدى امتثال تلك التشريعات ل اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، وتوجيه الاتحاد الأوروبي رقم 2013/40/EU بشأن الهجمات ضد نُظم المعلومات والاستعاضة عن القرار الإطاري للمجلس ٢٠٠٥/٢٢، وغيرهما من معايير الاتحاد الأوروبي والمعايير الدولية. وسيؤدي التحليل الذي سيعدونه إلى تقديم مقترحات لتعديل القوانين، سعياً إلى تحقيق المواءمة الكاملة.

٣٠٦- وأشارت صربيا إلى أن الخبرة المكتسبة في الأعوام الخمسة عشر الماضية أظهرت أن بناء القدرات والتخصص على المستوى الوطني، استناداً إلى الاتفاقات الدولية القائمة، مثمر جداً ويُحدث فرقاً. ومن المشكوك فيه ما إذا كانت المناقشات بشأن معاهدات دولية جديدة في هذا المجال مفيدة.

٣٠٧- وفيما يتعلق بالإطار المؤسسي والقدرات الإدارية، ذكرت صربيا المؤسسات التالية المختصة بالتصرف في مجال الجريمة السيبرانية:

(أ) مكتب المدعي الخاص المعني بجرائم التكنولوجيا العالية؛

(ب) المحكمة العليا في بلغراد؛

(ج) إدارة مكافحة وقمع جرائم التكنولوجيا العالية، التابعة لوزارة الداخلية؛

(د) السلطات المختصة الأخرى في الدولة.

٣٠٨- ومن حيث الإحصاءات والتحليل، أفادت صربيا بأن إجمالي عدد القضايا المدرجة في سجل مكتب المدعي الخاص المعني بجرائم التكنولوجيا العالية في عام ٢٠١٨ بلغ ٣ ٠٢٢ قضية، منها ٣٢٢ قضية أُدرجت في السجل تتعلق بجناة بالغين معروفين؛ و١ ٣٠٦ قضايا أُدرجت في السجل تتعلق بجناة غير معروفين، و١ ٣٩٤ قضية أُدرجت في السجل تتعلق بجرائم جنائية أخرى، ويشكل ذلك زيادة بنسبة ٢٧,٤٦ في المائة مقارنة بعام ٢٠١٧.

٣٠٩- وتبعاً لذلك، وحسبما أفادت به صربيا أيضاً، لوحظت تطورات إيجابية هامة في تطبيق خطوات إجرائية متنوعة في شتى مراحل الإجراءات الجنائية، مثل توجيه تهم جنائية ضد ٣٢٤ من الجناة المعروفين، بزيادة قدرها ٢٨,٥٧ في المائة؛ وزاد تطبيق إرجاء الملاحقة القضائية بنسبة ٨٥,٧١ في المائة، وزاد تطبيق اتفاق تفاوضي لتخفيف العقوبة بنسبة ١٠٥ في المائة. وهذه الزيادة الكبيرة هي نتيجة لزيادة في عدد الأشخاص المبلغ عنهم والقضايا المبلغ عنها، وزيادة في الموارد البشرية لمكتب المدعي الخاص، وزيادة في بناء قدرات السلطات المختصة.

٣١٠- وفيما يتعلق بالممارسات الجيدة، ذكرت صربيا الأمثلة التالية على قضايا دولية شاركت فيها السلطات المتخصصة المعنية بالجرائم السيبرانية في صربيا ونجحت القضايا بسبب تنفيذ اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية وأحكامها المتعلقة بالتعاون الدولي المنفذة في القانون الصربي:

(أ) عملية "Shadow Web"، في شباط/فبراير ٢٠١٨. تمت السيطرة على أحد أكبر المنتديات الإجرامية، المسمى "In Fraud"، والذي يتعامل في معلومات بطاقات الائتمان المسروقة. وقد قُبض على مواطن صربي ووُجهت إليه تُهم جنائية؛

(ب) عملية "Power Off"، في نيسان/أبريل ٢٠١٨. تمت السيطرة على أكبر خدمة إجرامية للهجمات الموزَّعة الخاصة بحجب الخدمة في العالم، وهي "Webstresser". وقُبض على مواطنَين صربيَين اثنين ووُجهت إليهما تُهم جنائية. وشاركت في العملية السلطات المختصة في إسبانيا وألمانيا وإيطاليا وصربيا وكرواتيا وكندا والمملكة المتحدة والنمسا وهولندا والولايات المتحدة، بالإضافة إلى هونغ كونغ، الصين. وبدأ المدعي الخاص المعني بجرائم التكنولوجيا العالية التحقيقات مع شخصين مشتبه بهما، وضُبطت للمرة الأولى عملة مشفرة لدى أحد المشتبه بهما؛

(ج) عملية "The Dark Overlord"، في أيار/مايو ٢٠١٨. وتتعلق بجماعة إجرامية سرقت بيانات شخصية وابتزت أصحابها.

٣١١- وأفادت صربيا بأنَّ التعاون الدولي من جانب مكتب المدعي الخاص في عام ٢٠١٨ كان ناجحاً بصفة خاصة. وشارك مكتب المدعي الخاص في أعمال الفريق المعني بالجرائم العابرة للحدود التابع لاتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية وفي الأنشطة ذات الصلة بإعداد

المزيد من التوصيات والمبادئ التوجيهية المتصلة بتطبيق الاتفاقية. كما شارك مكتب المدعي الخاص في عمل الفريق بشأن صوغ البروتوكول الإضافي الثاني للاتفاقية. وبالإضافة إلى ذلك، أُدرج مكتب المدعي الخاص في المشروع الممدَّد المتعلق بالتدابير العالمية لمكافحة الجرائم السيبرانية والمسمى "GLACY+"، المشترك بين مجلس أوروبا والاتحاد الأوروبي، وفي أنشطة دولية أخرى. وفي عام ٢٠١٨، شارك ممثلون عن مكتب المدعي الخاص في مشروع التعاون بين القطاعين العام والخاص في مجال الجريمة السيبرانية في منطقة الشراكة الشرقية، المسمى "EAP III" والتابع لمجلس أوروبا، والموُجَّه نحو ما يسمى "جيرة" الاتحاد الأوروبي، وكذلك في مشروع تعزيز التشريعات والقدرات المؤسسية في مجال الجريمة الإلكترونية والأدلة الإلكترونية في منطقة الجيرة الجنوبية، المسمى "Cyber@South"، والذي يستهدف بلدان شمال أفريقيا وغربها والبلدان الآسيوية الواقعة على شاطئ البحر الأبيض المتوسط، ومشروع استهداف عائدات الجريمة على الإنترنت في جنوب شرق أوروبا وتركيا في إطار أداة تقديم المساعدة في مرحلة ما قبل الانضمام، المسمى "iPROCEEDS@IPA"، والذي أُدرجت فيه بلدان من جنوب شرق أوروبا وتركيا. ودعت الشبكة القضائية الأوروبية للجرائم السيبرانية مكتب المدعي الخاص إلى المشاركة في اجتماعاتها في لاهاي. كما شارك ممثلو مكتب المدعي الخاص في عمل فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية.

سنغافورة

٣١٢- أشارت سنغافورة إلى التحديات التي تواجهها والمشتركة مع ولايات قضائية أخرى. وتشمل هذه التحديات زيادة تطور أساليب المجرمين الذين يسعون إلى استغلال إمكانية الوصول الأكبر الناتجة من العولمة وظهور التكنولوجيا وانتشارها لتحقيق غايات إجرامية.

٣١٣- وأفادت سنغافورة بأن استخدام الفضاء السيبراني نما بقدر كبير خلال العقد الماضي. ويعود ذلك إلى انخفاض تكاليف التكنولوجيا و سهولة الحصول عليها، مما أدى إلى زيادة في قضايا الجرائم السيبرانية (الأفعال المجرَّمة بموجب قانون إساءة استعمال الحاسوب في البلد، وكذلك الجرائم التي تُستخدم فيها أجهزة الحوسبة أو شبكات الحوسبة كأدوات لارتكاب جريمة تقليدية). وفي هذا الصدد، رصدت قوات الشرطة السنغافورية زيادةً في عدد عمليات الاحتيال من خلال الإنترنت وعدد الضحايا الذين يقعون فريسة لتكتيكات جديدة يستخدمها محتالون دوليون يستعملون تكنولوجيات المعلومات والاتصالات، تمتد من الأساليب المتطورة من قبيل القرصنة الحاسوبية إلى استخدام تكنولوجيا انتحال الهويات الهاتفية (call-spoofing). وبسبب مدى انتشار الجرائم التي يتيح الفضاء السيبراني ارتكابها واتساع نطاق تلك الجرائم في كل الولايات القضائية، يمكن أن تترسخ هذه الجرائم في أي مكان، ويكون الكشف عنها واقتلاعها وإزالتها أكثر صعوبة. وقد بذلت سنغافورة جهوداً على الصعيد الوطني والإقليمي والدولي، ترد تفاصيلها أدناه، للتصدي لهذا التحدي المعقد.

٣١٤- ففيما يتعلق بالجهود الوطنية، أفادت سنغافورة بأنه في ٢٠ تموز/يوليه ٢٠١٦، أعلن وزير الشؤون الداخلية ووزير الشؤون القانونية عن خطة عمل سنغافورة الوطنية الخاصة بالجرائم

السيبرانية، وذلك في مؤتمر "آر إس أي" (RSA) لآسيا والمحيط الهادئ واليابان. وتتمثل رؤية خطة العمل الوطنية الخاصة بالجرائم السيبرانية في ضمان إتاحة بيئة آمنة و سليمة على الإنترنت لسنغافورة مع ا ستمرار نمو أنشطة المجرمين على الفضاء السيبراني من حيث النطاق والتعقُّد والخطورة في جميع أنحاء العالم. وتتضمن الخطة تفاصيل عن الاستراتيجية المتعددة الجوانب للحكومة لمكافحة الجرائم السيبرانية من خلال ما يلي:

(أ) توعية الجمهور وتمكينه لكي يبقى بأمان في الفضاء السيبراني؛

(ب) تعزيز القدرات والإمكانيات في مجال مكافحة الجريمة السيبرانية؛

(ج) تعزيز التشريعات وإطار العدالة الجنائية؛

(د) تكثيف الشراكات والمشاركات الدولية.

٣١٥- ومن حيث الجهود الإقليمية والدولية، أشارت سنغافورة إلى الدور المفيد الذي تؤديه المنظمات الدولية والإقليمية والشراكات بين أصحاب المصلحة المتعددين في بناء القدرات، وتعزيز المعلومات، وتبادل أحدث الاتجاهات والتطورات وأفضل الممارسات، والتعاون الدولي، في مجال مكافحة الجريمة السيبرانية العابرة للحدود.

٣١٦- وتشمل البرامج الإقليمية الرئيسية اجتماع وزراء رابطة أمم جنوب شرق آسيا المعني بالجريمة المنظمة عبر الوطنية واجتماع كبار مسؤولي رابطة أمم جنوب شرق آسيا المعني بالجريمة المنظمة عبر الوطنية. وقد أطلقت سنغافورة، بوصفها الراعية المتطوعة لرابطة أمم جنوب شرق آسيا بشأن الجرائم السيبرانية، مبادرات جديدة لزيادة قدرات الدول الأعضاء في الرابطة على مكافحة الجريمة السيبرانية، مثل استضافة مؤتمر رابطة أمم جنوب شرق آسيا + ثلاثة بشأن الجرائم السيبرانية واجتماع المائدة المستديرة الخامس لكبار المسؤولين في الرابطة بشأن الجريمة السيبرانية، في تموز/يوليه ٢٠١٨. كما ركزت رابطة أمم جنوب شرق آسيا جهودها على تعزيز معارف المدعين العامين وقدراتهم بشأن مباشرة قضايا الجرائم السيبرانية، وعُقد اجتماع المائدة المستديرة للمدعين العامين بشأن الجرائم السيبرانية الخاص برابطة أمم جنوب شرق آسيا في سنغافورة في أيلول/سبتمبر ٢٠١٨. وهذه فعاليات سنوية ستنظم أيضاً في عام ٢٠١٩.

٣١٧- وأفادت سنغافورة بأنها تعمل عن كثب مع الإنتربول من أجل النهوض بالتعاون الإقليمي والدولي لمكافحة الجريمة السيبرانية. وقد عُينت سنغافورة في منصب نائب رئيس الفريق العامل الأوروبي الآسيوي التابع للإنتربول والمعني بالجرائم السيبرانية للفترة من ٢٠١٧ إلى ٢٠١٩. وبالإضافة إلى ذلك، أطلقت سنغافورة، بدعم من الإنتربول، مبادرة إنشاء مكتب رابطة أمم جنوب شرق آسيا المعني بالجريمة السيبرانية، الذي أُطلق في تموز/يوليه ٢٠١٨ في المجمَّع العالمي للابتكار التابع للإنتربول، والذي يقع في سنغافورة. ويستخدم هذا المكتب موارد الإنتربول ليقود العمليات المشتركة التي تركز على رابطة أمم جنوب شرق آسيا والرامية إلى مكافحة الجريمة السيبرانية. وشاركت سنغافورة أيضاً في عملية "الطفرة السيبرانية" لرابطة أمم جنوب شرق آسيا، التي يقودها المجمَّع العالمي للابتكار التابع للإنتربول والتي نفذت في شباط/فبراير ٢٠١٧. وشملت العملية الناجحة للغاية سبعة بلدان من رابطة

أمم جنوب شرق آسيا وسبع شركات من القطاع الخاص، وكشفت عن حوالي ٠٠٠ ٩ خادوم مخترَق ومئات المواقع الإلكترونية المصابة بالبرمجيات الضارة.

٣١٨- وفضلا عن ذلك فسنغافورة شريك داعم لمؤتمر الإنتربول العالمي (INTERPOL World)، وهو مؤتمر دولي يعقد كل سنتين في سنغافورة ويجتمع فيه القطاعان العام والخاص من أجل الحوار وإيجاد فرص التعاون لمواجهة التحديات المقبلة فيما يتعلق بشؤون الأمن وعمل الشرطة. ويتيح هذا الحدث الفريد منتدى قيِّماً لأصحاب المصلحة المعنيين لمناقشة تحديات الجرائم السيبرانية في العالم وتلقي تحديثات من الخبراء بشأن أحدث التهديدات والاتجاهات والحلول.

٣١٩- وتشارك سنغافورة مشاركةً نشطةً في عمليات الإنفاذ الدولية العابرة للولايات القضائية بشأن الجرائم السيبرانية. وشاركت سنغافورة في عملية "أفالانش" (Avalanche) التي قادها مكتب التحقيقات الاتحادي للولايات المتحدة واليوروبول ومكتب الشرطة الجنائية الاتحادية الألمانية في عام ٢٠١٦، ومرة أخرى في عام ٢٠١٧. وهدفت العملية إلى تفكيك شبكة عالمية من الحواسيب المصابة تستخدمها شبكة إجرامية لسرقة معلومات الحسابات المصرفية ومعلومات الهويات الشخصية والقيام بأنشطة غسل الأموال، بالإضافة إلى نظام "أندروميدا" Andromeda، الذي هو أحد أقدم نُظم البرمجيات الضارة الموجودة. وتشارك سنغافورة بنشاط أيضاً في المنصات الدولية التي تركز على رفع مستوى التعاون العالمي وتبادل أفضل الممارسات في مجال إنفاذ القانون. وتشمل هذه المنصات أول مناقشة مائدة مستديرة وطنية بشأن الجريمة السيبرانية عقدها المكتب المعني بالمخدِّرات والجريمة، في إندونيسيا يومي ٢ و٣ تموز/يوليه ٢٠١٨، وحلقة عمل خبراء العملات المشفرة التي عقدها المكتب في سنغافورة من ١٢ إلى ١٤ آذار/مارس ٢٠١٩، واجتماع فريق الخبراء المعني بالجريمة السيبرانية التابع للإنتربول، والمؤتمر المشترك بين الإنتربول واليوروبول المعني بالجرائم السيبرانية.

٣٢٠- وخلصت سنغافورة إلى أن التحديات التي تواجهها الدول الأعضاء في مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية هي تحديات متعددة الجوانب. ومن الواضح أن الجريمة السيبرانية هي مسألة يفيد فيها استمرار المناقشة وتعزيز التعاون الدولي والتضافر على الصعيدين الإقليمي والدولي بين الدول الأعضاء وأصحاب المصلحة المعنيين، بما في ذلك في الأمم المتحدة. وسنغافورة ملتزمة بالتعاون الدولي والإقليمي على مكافحة الجريمة السيبرانية، وتتطلع إلى المشاركة، عند الإمكان، في الجهود المبذولة في بناء القدرات. وعلاوة على ذلك، ستواصل سنغافورة دعم التعاون وتبادل المعلومات لمواجهة هذه التحديات.

سلوفاكيا

٣٢١- أفادت سلوفاكيا بأنها تولي مكافحة الجريمة السيبرانية اهتماماً كبيراً وتعتبر هذه المكافحة تحدياً مهمًّا. ومن أجل التصدي بفعالية لمسألة الجريمة السيبرانية، يجب تلبية جانبين أساسيين: جانب قانوني وجانب تقني. فأولاً، من الضروري وجود تشريع محلي مناسب. ولا بد من استكمال أحكام القانون الجنائي الموضوعية بأحكام إجرائية مناسبة. وترى سلوفاكيا أنه من المهم ضمان توسيع نطاق الأحكام الإجرائية التقليدية، مثل تفتيش المنازل وتسليم الأشياء أو ضبطها أو

مصادرها، لتشمل أيضاً البيانات المستمدة من أي وسيلة لحفظ البيانات يتم ضبطها. وعليه، ففيما يتعلق بتفتيش البيانات الحاسوبية، من الضروري وجود أحكام إجرائية إضافية لضمان إمكانية الحصول على البيانات الحاسوبية بصورة قانونية وبطريقة تتسم بنفس فعالية تفتيش أي جهاز محسوس ناقل للبيانات وضبطه. وبناءً على ذلك، يجب أن تتضمن القوانين المحلية أحكاماً تسمح لسلطات الدولة بتفتيش البيانات الحاسوبية المخزنة وضبطها. ويجب ضمان أن تكون لدى كل الدول أحكام مناسبة لمنع مرتكبي الجرائم من التخفي تفادياً للمثول أمام العدالة.

٣٢٢- وتعتبر سلوفاكيا أن اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، التي تنص، في جملة أمور، على أحكام تتعلق بالتفتيش والمصادرة، وإصدار أوامر بشأن البيانات الحاسوبية وحفظ البيانات، هي مثال ممتاز لنموذج يحتوي على مجموعة واسعة من الصلاحيات الإجرائية. وقد صدَّقت سلوفاكيا على تلك الاتفاقية في عام ٢٠٠٨، وتعتبرها المعيار الدولي الأفضل الذي يحتوي على أحكام موضوعية وإجرائية مناسبة ويتيح التعاون الدولي الفعال. وفي ضوء ما تقدم، ترى سلوفاكيا أن التنفيذ الناجح للصلاحيات الإجرائية المنصوص عليها في الاتفاقية المذكورة، وكذلك الإرادة السياسية الواضحة، عاملان ضروريان لوضع إطار قوي لغرض الحصول على الأدلة.

٣٢٣- وعلاوةً على ذلك، ترى سلوفاكيا أن أهمية الفقرة ١ (أ) من المادة ١٨ من اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، التي تنص على إصدار أوامر تقديم المعلومات، تتمثل في أنها أثبتت جدواها حقيقة على مرِّ الزمن. والعنصر الرئيسي ليس مكان البيانات، بل هو وجود جهة تسيطر على البيانات أو تحتفظ بها في إقليم معين. ويتيح هذا النهج حلولاً في معظم الحالات، حتى في عصر الحوسبة السحابية. واستناداً إلى ما سبق، لا ترى سلوفاكيا ضرورة لإعداد صك دولي جديد بشأن الجريمة السيبرانية، وتشجع البلدان التي ليست طرفاً في اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية على الانضمام إليها.

٣٢٤- وأشارت سلوفاكيا أيضاً إلى أن كل جريمة جنائية تقريباً قد تنتج عنها أدلة إلكترونية. وتسمح اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية بجمع الأدلة الإلكترونية بشأن جميع أنواع الجرائم، مما يجعل هذا الصك أكثر أهمية. ويترتب على ذلك أنه ينبغي إعلام كل قاضٍ أو مدعٍ عام بكيفية استخدام الوسائل المتاحة لتأمين الأدلة الإلكترونية. وتُعتبر الأنشطة التثقيفية وبرامج بناء القدرات على الصعيدين الوطني والدولي في هذا الصدد ضرورية. وترى سلوفاكيا أن برامج بناء القدرات يجب أن تكون محددة الأهداف، ويجب تجنب ازدواجها إن أمكن ذلك.

٣٢٥- وأشارت سلوفاكيا أيضاً إلى الجوانب التقنية، بالإضافة إلى الجوانب القانونية. وذكرت أن الدول ينبغي أن تضع في اعتبارها أن أحد العوامل الرئيسية لنجاح التحقيقات المتعلقة بالجريمة السيبرانية والجرائم التي ترتكب باستخدام الفضاء السيبراني يتمثل في الأنواع المختلفة من التخصص (الشبكات المحلية للمدعين العامين والقضاة المعنيين بالجرائم السيبرانية، والسلطات القضائية المتخصصة المعنية بالجرائم السيبرانية، وما إلى ذلك)، فضلاً عن التدريب المنتظم لسلطات إنفاذ القانون والسلطات القضائية من أجل ضمان تطبيق الصلاحيات الإجرائية تطبيقاً صحيحاً ومواكبة التطورات الجارية. وإقامة الشبكات وتبادل أفضل الممارسات ضروريان داخل الدول وعلى المستوى الدولي.

٣٢٦- ومن أجل ضمان التخصص واستمرار تحديث الخبرات، أنشأت سلوفاكيا ضمن رئاسة قوات الشرطة إدارة خاصة للجرائم الحاسوبية. وتساعد هذه الإدارة على زيادة فعالية مكافحة الجرائم الحاسوبية والجرائم المرتكبة عبر الإنترنت، وتعالج حاليًّا في المقام الأول الهجمات السيبرانية على نظم المعلومات، والاستغلال الجنسي للأطفال عبر الإنترنت، والاحتيال المتعلق بالمدفوعات غير النقدية، والمحتوى غير المشروع على الإنترنت (بما في ذلك المحتوى الإرهابي)، وتتضمن مهامها البحث عن الجرائم السيبرانية ورصدها (بما في ذلك الكشف على عمليات الإنترنت السرية). وتقدم هذه الإدارة أيضاً التعاون إلى المدعين العامين عند الحاجة إلى المساعدة الفنية. ويسير التعاون بصورة جيدة جدًّا. وتقيم الإدارة أيضاً حواراً مع الأوساط الدولية للشرطة المعنية بالجريمة السيبرانية، وكذلك مع القطاع الخاص، وبخاصة مع مقدمي خدمات الإنترنت، في سلوفاكيا وفي الخارج على حد سواء، لأن بيانات الأفراد كثيراً ما تكون في حيازة كيانات خاصة أو خاضعة لسيطرتها، ومن الضروري مناقشة تعقيدات التعاون وتحدياته.

٣٢٧- وعلاوة على ذلك، أُنشئت الشبكة الوطنية للمدعين العامين لمكافحة الجريمة السيبرانية في عام ٢٠١٧. وتتمثل مهمتها الرئيسية في تقديم معلومات عملية وتبادل الخبرات بين أعضاء الشبكة ومع المدعين العامين الآخرين بشأن الجرائم السيبرانية، فيما يتعلق بالقضايا الوطنية وقضايا التعاون الدولي.

٣٢٨- وعلى المستوى الوطني، أُنشئ فريق متعدد التخصصات من الخبراء معني بالجرائم السيبرانية. ويجمع الفريق بين خبراء من جميع السلطات الحكومية الهامة والقطاع الخاص، ويعقد مناقشات بشأن مسائل من بينها كيفية تعديل القوانين المتصلة بالكشف عن البيانات لأغراض الإجراءات الجنائية بحيث لا تكون هناك حاجة إلى أمر من المحكمة (في سلوفاكيا، يلزم الحصول على أمر من المحكمة لتحديد هوية مستخدم رقم الهاتف أو عنوان بروتوكول الإنترنت). وعليه، تعتبر سلوفاكيا أن إنشاء شبكات متخصصة على الصعيدين الوطني والدولي تجمع بين الممارسين الذين يتعاملون مع الجرائم السيبرانية أمراً مفيداً.

٣٢٩- وأكدت سلوفاكيا أنها ملتزمة بمكافحة الجريمة السيبرانية. وبالنظر إلى الطبيعة العالمية للجريمة السيبرانية، أكدت سلوفاكيا أنها تقدِّر كثيراً إمكانية المشاركة في فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، فتبادل أفضل الممارسات وتبادل الآراء مع الخبراء من جميع أنحاء العالم في إطار فريق الخبراء المذكور مفيد للغاية، وينبغي أن يظل فريق الخبراء هو العملية الرئيسية على مستوى الأمم المتحدة بشأن موضوع الجريمة السيبرانية حتى عام ٢٠٢١ على الأقل.

سلوفينيا

٣٣٠- أقرت سلوفينيا بأنه، مع التطور السريع في تكنولوجيا المعلومات، تدخل خدمات ومعدات وأجهزة جديدة إلى السوق، إلى جانب أساليب عمل جديدة يتعبها المجرمون. وهذا يستلزم تكيفاً سريعاً ومناسباً من جانب سلطات إنفاذ القانون، الأمر الذي لا يمكن كفالته إلا إذا كان هناك تعاون فعال ووثيق مع القطاع الخاص وهيئات البحوث. ويستلزم هذا التعاون تبادلاً آمناً وسريعاً للمعلومات والدراية وتقنيات وأساليب التحقيق، فضلاً عن تدريب الموظفين المستمر. وبالنظر إلى

الاتجاهات السائدة، من المتوقع حدوث زيادة في الجرائم الجنائية التي تُرتكب باستخدام تكنولوجيات المعلومات العصرية والرقمية والافتراضية أو غيرها من التكنولوجيات.

٣٣١- وقد لاحظت الشرطة السلوفينية أن مرتكبي الجرائم الجنائية في الفضاء السيبراني يزدادون مهارة من الناحية التكنولوجية وتزداد دقة تنظيمهم؛ ويعملون على الصعيد الدولي، ويتركون قدراً أقل من الآثار والأدلة التي يمكن استخدامها ويمكن أن تسهِّل التعرف عليهم. ويحدث كل هذا بسرعة كبيرة، وعدد الضحايا آخذ في الازدياد، وتستغرق استعادة الحالة الطبيعية وقتاً أطول بكثير. ولا تتخذ الآثار المتروكة، في معظمها، سوى الشكل الرقمي، وتكون في كثير من الأحيان موزعة على بلدان أو قارات كثيرة، مما يؤثر سلباً على مدة التحقيقات الجنائية ونجاحها. ويتمثل تحدٍ آخر أفادت به سلوفينيا في الحجم المتزايد من البيانات التي تخضع للفحص والتحليل في كل تحقيق، وكذلك في أن المزيد من الشركات المصنِّعة للأجهزة الإلكترونية يستخدم كقاعدة افتراضية تشفير البيانات القوي. وهذا يمنح المجرمين درجة عالية من السرية ويزيد كثيراً من صعوبة الكشف والوقاية.

٣٣٢- وبالنظر إلى تطور الإنجازات التكنولوجية واستغلالها، تواجه البيئة الدولية تحديات لا يمكن التغلب عليها إلا من خلال تعزيز التعاون والمعاملة بالمثل في مجال وضع ممارسات جديدة لمنع المخاطر والحد منها، واستحداث نُهج وأدوات وآليات جديدة، ومن خلال المزيد من الإجراءات المتبادلة والتضامن في الوقاية على مستوى العمليات. ويستلزم التشتت الدولي للأدلة ولعمليات مرتكبي الانتهاكات الأخذ بأشكال تحقيق جديدة وتحسين التشريعات والمؤهلات والمعدات.

جنوب أفريقيا

٣٣٣- أشارت جنوب أفريقيا إلى التحديات المرتبطة بصكوك القانون المدني والجنائي القائمة المتعلقة باستخدام تكنولوجيات المعلومات والاتصالات، فأفادت بأن لديها تشريعات لمكافحة أفعال الجرائم السيبرانية، تتضمن مشروع قانون الجرائم السيبرانية (سيصبح قريباً قانوناً برلمانيًّا)، وقانون الإجراءات الجنائية، وقانون الاتصالات والمعاملات الإلكترونية، وقانون التعاون الدولي في المسائل الجنائية، وقانون حماية المعلومات الشخصية. وعلاوة على ذلك، قالت جنوب أفريقيا إن غياب توافق دولي في الآراء بشأن المسائل والمفاهيم الرئيسية، بما في ذلك طبيعة التهديدات السيبرانية وأبعادها، وعدالة إجراءات ونتائج الأطر الرسمية، وتجريم سلوكيات محددة باعتبارها جرائم سيبرانية، كل ذلك يطرح تحديات في مجال مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية. وتتجاوز هذه التحديات نطاق العناصر التعريفية، التي تختلف اختلافاً كبيراً.

٣٣٤- وأشارت جنوب أفريقيا أيضاً إلى التنسيق والتعاون بين الدول في مجال مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية. فذكرت أنه، رغم توافر عدد من الآليات القائمة لتعزيز التنسيق والتعاون، مثل المساعدة القانونية المتبادلة، ونقاط الاتصال المعيَّنة، والالتزامات الواقعة على عاتق مقدمي خدمات الاتصالات الإلكترونية والمؤسسات المالية، وكذلك سرعة قيام مختلف مقدمي الخدمات بالكشف عن بيانات حركة المرور الإلكترونية، تبقى هناك تحديات في التصدي للجريمة السيبرانية. واعتُبرت المسائل التالية تحديات هامة: طول عملية المساعدة القانونية

المتبادلة؛ تعدد الوكالات التي تضطلع بولايات مختلفة، مما يجعل التنسيق المركزي صعباً؛ آلية التنسيق وتنفيذ التدابير المقترحة التي لا تحظى بدعم كامل من مختلف أصحاب المصلحة. وفي حين أن الصكوك الإقليمية القائمة قد تنجح في معالجة التهديدات السيبرانية من خلال إتاحة التعاون بين أطراف الاتفاقيات، فإن التحدي الأكبر يكمن في أنها قد لا تكافح الجريمة السيبرانية بفعالية على الصعيد العالمي، لأن الدول غير الأطراف في الاتفاقية قد لا تتعاون معاً. ويشكل غياب تعريف متفق عليه عالمياً للجريمة السيبرانية تحدِّياً، ولذلك وضع كل بلد على حدة تعريفاً خاصًّا به، مما يؤدي إلى بروز تحديات عندما يتعلق الأمر بالمساعدة القانونية المتبادلة أو التعاون الدولي، بما في ذلك تسليم المطلوبين وإتاحة الأدلة الإلكترونية. ومن أجل تنفيذ القوانين المتعلقة بالجريمة السيبرانية تنفيذاً فعالاً، ولا سيما عند وجود حاجة إلى التعاون مع دول أخرى، من المهم ضمان وجود بعض المواءمة بين القوانين، الأمر الذي يستلزم اتفاقاً على تعريف الجريمة السيبرانية. وهناك الكثير من الصكوك الإقليمية الملزمة أو غير الملزمة التي تهدف إلى معالجة مسألة الجريمة السيبرانية، لكن قد لا ترغب بلدان كثيرة، بسبب توجهاتها السياسية وجداول أعمالها الدولية وظروفها الاجتماعية والاقتصادية، في التصديق على أي من الصكوك الإقليمية القائمة.

٣٣٥- وفيما يتعلق بالمساعدة التقنية، أشارت جنوب أفريقيا إلى أنه رغم وجود اتفاقات ثنائية ومتعددة الأطراف (مثل أحكام اتفاقية الجريمة المنظمة بشأن المساعدة القانونية المتبادلة وتسليم المطلوبين ونقل السجناء المحكوم عليهم ومصادرة الأصول)، يبدو أن الاتفاقات الإقليمية والقاريَّة تحل محل الاتفاقات الثنائية والمتعددة الأطراف من حيث تأدية الوظيفة. والتعاون الدولي فيما يتعلق بالجرائم السيبرانية محدود في معظم الحالات ولا يشمل الإجراءات اللازمة لأمور من بينها الحفاظ على الأدلة، أو إتاحة بيانات حركة المرور الإلكترونية على أساس مستعجل، أو ضمان توافر الأدلة.

٣٣٦- وترى جنوب أفريقيا أن هناك تحديات قائمة أخرى تتمثل في تباين القوانين الوطنية للبلدان واشتمالها على أوصاف متباينة للجريمة السيبرانية؛ وتباين الإجراءات المتصلة بالتعاون الدولي؛ والإجراءات الرسمية الواجب اتباعها فيما بين البلدان قبل أن تكون الأدلة مقبولة في المحاكم؛ وقوانين الخصوصية، وما إلى ذلك.

٣٣٧- وتعتبر جنوب أفريقيا أن عدم وجود هياكل وطنية في مختلف البلدان تتمتع بسلطات تنسيقية من أجل تنسيق طلبات المساعدة المتبادلة يعوق فعالية المساعدة القانونية المتبادلة. ويؤدي تعدد الصكوك الإقليمية الرامية إلى التصدي للجرائم السيبرانية إلى التجزؤ وإلى التعاون القائم على التقوقع بين البلدان، ولا تنجح هذه الصكوك في كفالة التعاون الدولي المناسب. ويشكل غياب صك معترف به عالميًّا على مستوى الأمم المتحدة يتناول التعاون الدولي في مسائل الجريمة السيبرانية عاملاً هامًّا يسهم في عدم فعالية التعاون الدولي في هذا المجال.

٣٣٨- وجنوب أفريقيا مقتنعة بأنه ينبغي تعزيز دور المكتب المعني بالمخدِّرات والجريمة، ولا سيما لجنة منع الجريمة والعدالة الجنائية، في مجال إتاحة بناء القدرات. وتتمثل مشكلة في افتقار سلطات وطنية كثيرة إلى التمويل اللازم للتدريب المتخصص الذي يمكِّنها من التحقيق الفعال في قضايا الجرائم السيبرانية المعقدة. وعلى غرار ذلك، من الصعب استبقاء الموظفين ذوي الخبرة والمدرَّبين، بسبب الطلب عليهم في القطاع الخاص. وهناك افتقار واسع الانتشار إلى برامج

التدريب الأساسية والمتوسطة في مؤسسات التدريب على إنفاذ القانون، ونادراً ما يُمنح المحققون ذوو الخبرة فرصة حضور الدورات التدريبية أو حلقات العمل المتقدمة، بسبب كمية العمل المسند إليهم. وحتى مع أفضل النوايا والتدابير المقترحة، تجعل القيود المتصلة بالميزانية والقدرات من الصعب تنفيذ التدابير المقترحة، وغالباً ما تقتصر القدرات والموارد المتاحة على ولاية الوكالة المعنية ولا يمكن بالضرورة استخدامها لمساعدة الوكالات الأخرى. وفضلا عن ذلك، لا توجد أطر أو مبادئ توجيهية رسمية للتعاون بين أصحاب المصلحة المعنيين في مجال الجريمة السيبرانية.

إسبانيا

٣٣٩- أبلغت إسبانيا بأنَّ الجريمة السيبرانية الناتجة من تنامي استخدام تكنولوجيات المعلومات والاتصالات هي أحد الأخطار المهدِّدة الرئيسية وواحد من أهم التحديات التي تواجه الدول كلها، وذلك أيضاً بسبب تنوُّع المنهجيات الإجرامية التي تستخدمها جماعات الجريمة المنظمة. فالمجرمون يستفيدون من منصَّات الاتصالات ومن تكنولوجيات المعلومات والاتصالات الجديدة من أجل استحداث نماذج أعمال تجارية غير مشروعة جديدة، ومنها مثلاً استخدام الشبكة الخفية بغية التمكُّن من ارتكاب جرائم أخرى (كالاتجار بالأسلحة النارية والنقود المزيفة)، واستخدام البرامجيات الحاسوبية الخبيثة المتطورة (مثلاً برامجيات طلب الفدية) ونظام التحكم في البنى التحتية المصرفية، وما يُسمى أسلوب "المتعهِّد الإجرامي المنفرد"، الذي يعرض خدمات غير مشروعة. وتشكِّل كل الأمثلة المذكورة أعلاه تحديات تواجه المسؤولين الأمنيين والمجتمع بأسره.

٣٤٠- كذلك فإنَّ اتساع انتشار الوصول إلى الإنترنت وسرعة تزايده، وازدياد عدد الأجهزة التي توفِّر الموصولية، هي عوامل من شأنها أن تؤدي إلى زيادة في عدد ضحايا الجريمة السيبرانية المحتملين. وبالمثل، إذا وضع في الاعتبار تزايد معدَّل النمو السكاني في البلدان النامية (وبالدرجة الرئيسية في أفريقيا)، وتقديرات النمو في عدد الذين يستخدمون الإنترنت في تلك البلدان، فإنَّ من السهل توقُّع حدوث زيادة كبيرة في استخدام الإنترنت لارتكاب الجرائم، وتحديداً الجرائم الاقتصادية. غير أنه، كما أن المجرمين يتعلمون كيف يستفيدون من التكنولوجيات الجديدة لتطوير أساليب عمل جديدة، يمكن كذلك لسلطات الشرطة أن تستخدم الابتكارات التكنولوجية لاستحداث تدابير جديدة للتحقيق في التهديد الذي تشكِّله الجريمة المنظمة والخطيرة ومكافحته.

٣٤١- واعتبرت إسبانيا أنَّ تضمين القانون الوطني مقتضيات بشأن إجراء التحريات المستترة في الإنترنت يمثل أداة رئيسية في مكافحة الجرائم المنظمة والجرائم الخطيرة، التي تُرتكب من خلال استخدام تكنولوجيات المعلومات والاتصالات. وهذا هو الحال أيضاً فيما يخص الاستخدام التدريجي للتكنولوجيات الجديدة، مثل الطائرات المسيَّرة، والبرامجيات الحاسوبية المحددة التوجيه، والخدمات السحابية، والوصول السريع إلى الشبكات الاجتماعية.

٣٤٢- وفي إسبانيا، تشكِّل تدابير مكافحة الجرائم التي تُخطَّط وتُنفَّذ عبر الإنترنت، وعموماً من خلال تكنولوجيات المعلومات والاتصالات، جانباً مهماً من الاستراتيجية الأمنية الوطنية، التي نُشرت في كانون الأول/ديسمبر ٢٠١٣ ويجري حالياً تحديثها. ونتيجة لذلك، تُعدُّ مكافحة الجريمة السيبرانية جزءاً من هدف أوسع نطاقاً هو جعل استخدام الفضاء السيبراني مأموناً، على

أســـاس نموذج متكامل. وهذا يشـــمل التنســـيق والتعاون بين الإدارة العمومية والقطاع الخاص والمواطنين، وفي الوقت نفســـه إدماج المبادرات الدولية ضـــمن النظام القانوني الداخلي والدولي. ويجري تحقيق هذا النهج بطرائق مختلفة.

٣٤٣- فأولاً، بالنسبة إلى الإصلاحات التشريعية، حقق القانونان الأساسيان ١/٢٠٠٥ و٢/٢٠١٥، في عام ٢٠١٥، إصـــلاحاً مهمًّا لقانون العقوبات الإســـباني، مســـتلهم من اللوائح التنظيمية الأوروبية (التوجيـــه ٤٠/٢٠١٣ والتوجيـــه ٩٣/٢٠١١، والقرار الإطـــاري DM 2008/919/JAI، وغيرهـــا)، ومن اتفاقية مجلس أوروبا المتعلقة بالجريمة الســـيبرانية واتفاقية مجلس أوروبا بشـــأن حماية الأطفال من الاستغلال الجنسي والاعتداء الجنسي. ويتضمن هذان الصكَّان تعاريف لجرائم جديدة، الأمر الذي ألهم القيام بإصلاحات واسعة النطاق للأحكام ذات الصلة من قانون العقوبات، ومنها مثلاً الأحكام المتعلقة بالهجمات الحاســـوبية، والتحرش الجنســـي بالقُصَّـــر، واســـتغلال الأطفال في المواد الإباحية، والملكية الفكرية، وجرائم الكراهية، والاحتيال الحاسوبي، وجرائم الإرهاب. وفي عام ٢٠١٥ أيضاً، اعتُمد من خلال القانون الأساسي ١٣/٢٠١٥ إصلاح هام لقانون الإجراءات الجنائية، استُلهم من اتفاقية مجلس أوروبا المتعلقة بالجريمة الســـيبرانية، تضـــمَّن تنظيم تدابير تكنولوجية هامة متصـــلة بتســـجيل البيانات وحزمها والحفاظ عليها. وبغية تسهيل تفسير هذه التطورات التشريعية، نشر مكتب النائب العام للدولة تعميمات ذات صلة.

٣٤٤- وثانياً، فيما يتعلق بالتدابير التشـــريعية، كانت دائماً لدى كل أجهزة الشـــرطة الوطنية والمستقلة ذاتياً في إسبانيا، منذ أكثر من ٢٠ سنة، وحدات متخصصة تتكوَّن من موظفين ذوي مؤهلات عالية في البحوث التكنولوجية، ولديهم معارف وخبرات تمكنهم من مكافحة اســـتخدام تكنولوجيات المعلومات والاتصـــالات للأغراض الإجرامية. وتتيح هذه الخبرة لســـلطات الشـــرطة الاســـتفادة من التكنولوجيات الجديدة، مثل تكنولوجيا البيانات الضـــخمة، وكذلك الأجهزة المســـتندة إلى الشـــبكة العالمية والتي يمكن إدخالها في منتجات كالملابس والمجوهرات والأحذية من أجل التحقيق في الجرائم واستبانة هوية المشتبه فيهم.

٣٤٥- واستحدث مكتب المدعي العام الإسباني أيضاً تخصصاً في مجال الجريمة السيبرانية. ومنذ عام ٢٠١١، نشرت الشبكة الوطنية للمدَّعين العامين، المكرسة تحديداً للملاحقة القضائية للجرائم الســـيبرانية، قرابة ١٥٠ مدعياً عامًّا على الأراضـــي الوطنية، في عواصـــم المقاطعات البالغ عددها ٥٠ عاصـــمة، وفي عدد من المدن المختارة. وتحافظ الوحدات المتخصـــصـــة التابعة لمكتب المدَّعي العام والشرطة على اتصال دائم بغيرها من الهيئات ذات المسؤولية عن الأمن السيبراني، من أجل كفالة التنسيق الوافي فيما بينها وجعل استخدام الفضـاء السيبراني مأموناً للجميع. وتشـمل هذه الهيئات الهيئة الإســـبانية لحماية البيانات، والمركز الوطني لحماية البنى التحتية الحيوية، والمعهد الوطني للأمن الســـيبراني، والمركز الوطني لعلوم التشـــفير، والقيادة المشـــتركة للدفاع الســـيبراني، وكذلك منظمات وكيانات من القطاع الخاص، مثل الكيانات المصرفية أو الكيانات المسؤولة عن خدمات الاتصالات وغيرها من الخدمات الضرورية.

٣٤٦- واعتبرت إسبانيا أنَّ من المهم مواصلة دعم تدريب الوحدات المتخصصة المعنية بمكافحة الجريمة السيبرانية، وكذلك زيادة مواردها البشرية والمادية. كما نال تدريب الباحثين والموظفين القانونيين، وفي المقام الأول القضاة والمدَّعون العامون، عناية في السنوات الأخيرة، وقُدِّم على مستويين:

(أ) الإعداد الشامل بشأن المعارف الأساسية والضرورية، الذي يُقدَّم لجميع المهنيين المعنيين بمكافحة الجريمة؛

(ب) التدريب المتخصص للوحدات أو المجموعات التي تُعنى تحديداً بالجريمة السيبرانية.

٣٤٧- وذكرت إسبانيا أنَّ التعاون الدولي مهم في التصدي للتحدِّي المشترك الذي تشكِّله الجريمة السيبرانية لجميع الدول. وتشمل الأمثلة على مشاركة البلد في جهود التعاون الدولي المشاركة الناشطة في شبكة نقاط الاتصال "٧/٢٤" المنشأة بمقتضى المادة ٣٥ من اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية؛ وفي الشبكة الأوروبية القضائية لمكافحة الجريمة السيبرانية؛ وفي الشبكة الأوروبية للمدَّعين العامين المتخصصين في الملكية الفكرية. وبالمثل، يعزز مكتب المدعي العام الإسباني الشبكة الإيبيرية - الأمريكية للمدَّعين العامين المتخصصين "سايبريد" (CibeRed) ويشارك فيها.

٣٤٨- وأبلغت إسبانيا بأنها عضو ناشط في لجنة اتفاقية الجريمة السيبرانية التابعة لاتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، وفي الأفرقة العاملة المعنية بإعداد البروتوكول الإضافي الثاني للاتفاقية، الذي يهدف إلى تحسين التعاون والتضافر الدوليين مع متعهِّدي تشغيل النُّظُم السيبرانية وتوريدها ومع كيانات القطاع الخاص. وتشارك إسبانيا في العديد من التحقيقات العابرة للحدود الوطنية، مع البلدان الأوروبية وبلدان أمريكا اللاتينية، باتباع أساليب تعاون متقدمة، ومنها مثلاً فرق التحقيق المشتركة. وهي تشارك أيضاً في التدريب في بلدان أخرى، بما في ذلك بصفة مدرِّب.

سري لانكا

٣٤٩- أكَّدت سري لانكا أنها ما فتئت تشارك بنشاط في فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، الذي استعرض مؤخَّراً الفصلين الخامس والسادس من مشروع الدراسة الشاملة عن الجريمة السيبرانية، الصادر في شباط/فبراير ٢٠١٣. وسوف يركِّز فريق الخبراء في اجتماعه المقبل على الفصلين الأخيرين السابع والثامن (التعاون الدولي والمنع).

٣٥٠- وذكرت سري لانكا أنها ترغب في توضيح الصلة بين المعلومات الملتمسة من خلال قرار الجمعية العامة ١٨٧/٧٣ والعمل الجاري في المكتب المعني بالمخدِّرات والجريمة بشأن الدراسة الشاملة عن الجريمة السيبرانية، وما إذا كان ثمة ازدواجية مع العمل الذي يقوم به فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية.

٣٥١- ومن حيث التشريعات الوطنية بشأن الجريمة السيبرانية، أبلغت سري لانكا بأنَّ قانون الجرائم الحاسوبية، رقم ٢٤ لعام ٢٠٠٧، هو الأداة التشريعية الرئيسية في مكافحة الجريمة السيبرانية. وبالإضافة إلى ذلك فإنَّ قانون الاحتيالات بواسطة أجهزة دفع النقود، رقم ٣٠ لعام ٢٠٠٦، يعالج على وجه التحديد مسائل حيازة أو استخدام الأجهزة المغشوشة أو غير المأذون بها الخاصة بدفع النقود.

٣٥٢- وقد أصبحت سري لانكا دولة طرفاً في اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، في عام ٢٠١٥؛ وبذلك أثبتت بوضوح التزامها القوي بمواءمة وتحسين قوانينها الوطنية وفقاً لأفضل المعايير الدولية المتاحة التي تحكم مكافحة الجريمة السيبرانية. وسري لانكا ملتزمة أيضاً بتحسين أساليب التحقيق وتعزيز مقدرة مسؤولي العدالة الجنائية على اتباع أساليب أكثر فعالية في إنفاذ القانون.

٣٥٣- وفي حين أنَّ الأحكام القانونية الموضوعية المضمَّنة في المواد من ٣ إلى ١٠ من قانون الجرائم الحاسوبية المذكور تستند إلى المواد من ٢ إلى ٨ من اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، فإنَّ المادة ٩ مجسدة جزئيًا في المادة ٢٨٦-ألف من قانون العقوبات (المعدَّل)، رقم ٢٢ لعام ١٩٩٥. ويعالج قانون الملكية الفكرية، رقم ٣٦ لعام ٢٠٠٣، الجرائم المشمولة بالمادة ١٠ من اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية.

٣٥٤- وبغية التصدي للتحديات المستجدة في مجال الجريمة السيبرانية، شرعت سري لانكا في إعادة النظر في تدابير العدالة الجنائية الوطنية في مجال حماية سلامة الأطفال في الإنترنت. وتبعاً لذلك، أقرَّت سري لانكا مؤخَّراً تعديلاً للمرسوم الخاص بالمنشورات الفاضحة لكي يتناول على نحو شامل الجرائم المتصلة باستغلال الأطفال في المواد الإباحية. وسيُستحدث من خلال هذا التعديل فصل جديد عنوانه "استغلال الأطفال في المواد الإباحية باستخدام النظم الحاسوبية".

٣٥٥- ومن حيث تدابير إنفاذ القانون ذات الصلة بالجرائم السيبرانية والأدلة الإلكترونية، تنص الأحكام الإجرائية الواردة في الجزء الثاني من قانون الجرائم الحاسوبية على اعتراض المعلومات الأساسية عن المشتركين وبيانات حركة المرور الحاسوبية وجمعها في الوقت الحقيقي وتقديم طلبات حفظ البيانات. وتخضع هذه الأحكام لضمانات تتسق مع المادة ١٥ من اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية.[٩]

٣٥٦- وبمقتضى المادة ١٨ من ذلك القانون، يُشترط على أجهزة إنفاذ القانون استصدار أمر قضائي من قاضٍ من أجل الحصول على المعلومات الأساسية عن المشتركين التي تكون في حيازة مقدِّمي خدمات النُّظُم. ولا بد من استيفاء اشتراط مماثل من أجل اعتراض الاتصالات. كما أن أوامر الحفاظ على البيانات بمقتضى المادة ١٩ من القانون توجب على أي شخص مسؤول عن نظام حاسوبي أو نظام معلومات أن يحافظ على البيانات ويتيحها عندما تطلبها أجهزة إنفاذ القانون. غير أنَّ المدة مقيَّدة بفترة سبعة أيام. ولا يمكن الحصول على تمديد فترة الحفاظ على البيانات إلا من خلال أمر من المحكمة.

٣٥٧- والإشراف القضائي على هذه التدابير الإجرائية يحمي مقدِّمي الخدمات من الطلبات غير الضرورية أو التعسُّفية من جانب أجهزة إنفاذ القانون، مع كفالة تقديمهم المساعدة إلى موظفي

(٩) بمقتضى قانون الجرائم الحاسوبية، تستوجب تدابير التحقيق الاقتحامية، ومنها مثلاً تفتيش الحواسيب واحتجازها أو اعتراض الاتصالات، الحصول على أمر قضائي يصدر عن قاضٍ (المادة ١٨). وينص دستور سري لانكا في الفصل الثالث منه على عدد من الحقوق الأساسية ويكفلها. وسريّ لانكا طرف في عدد من المعاهدات الدولية الخاصة بحقوق الإنسان، ومنها مثلاً العهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية، والعهد الدولي الخاص بالحقوق المدنية والسياسية، واتفاقية حقوق الطفل، واتفاقية مناهضة التعذيب وغيره من ضروب المعاملة أو العقوبة القاسية أو اللاإنسانية أو المهينة.

إنفاذ القانون على مكافحة الجريمة بفعالية. ولم تؤثر هذه الضمانات الواردة في التشريعات الوطنية سلباً على كفاءة التحقيقات الجنائية أو فعاليتها؛ بل إنها من الناحية الأخرى أوجدت قدراً أكبر من الثقة لدى الضحايا ولدى منشآت الأعمال (وبخاصة المصارف ومؤسسات القطاع المالي) بشأن الإبلاغ عن حادثات الجريمة السيبرانية، وأوجدت ثقة أيضاً لدى مقدِّمي خدمات الاتصالات السلكية واللاسلكية فيما يخص التعاون مع أجهزة إنفاذ القانون. ويمكن التنويه بذلك على أنه إحدى الممارسات الفضلى بالنسبة إلى البلدان النامية.

٣٥٨- وضمن جهاز الشرطة، أُنشئت وحدة متخصصة معنية بالتحقيقات في الجرائم السيبرانية، ولديها فرعان في المقاطعات. وتؤدي هذه الوحدة وظيفة نقطة الاتصال "٧/٢٤" في إطار اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية. وقد تم تحسين مستواها مؤخَّراً، وأُنجزت بنجاح تحقيقات بشأن أكثر من ٧٥٠ قضية، بفضل الخبرة التي اكتسبها الموظفون الوطنيون من خلال تدابير بناء القدرات المشار إليها أدناه.

٣٥٩- وشدَّدت سري لانكا على أنَّ الحصول على الأدلة الإلكترونية من مقدِّمي الخدمات الأجانب أمر حيوي للتحقيقات والملاحقات القضائية بشأن الأفعال الجُرمية المشمولة في الجريمة السيبرانية. ولأنَّ الأدلة توجد في ولايات قضائية مختلفة، فإنَّ الحاجة إلى اتباع طرائق تحقيق أكثر فعاليةً، مقترنة بتدابير فعالة بشأن التعاون الدولي، ذات أهمية قصوى. ويُعالج موضوع التعاون الدولي في المسائل القضائية الجنائية بمقتضى قانون المساعدة المتبادلة في المسائل الجنائية، رقم ٢٥ لعام ٢٠٠٢. وقد أُدرج هذا القانون بإشارة مرجعية في قانون الجرائم الحاسوبية؛ ثم عُدِّل القانون رقم ٢٥ لعام ٢٠٠٢، في عام ٢٠١٨، بالقانون رقم ٢٤ لعام ٢٠١٨، المحتوي على سمات من اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية.

٣٦٠- ومن حيث تدابير بناء القدرات، ركَّزت سلسلة من البرامج بشأن الجرائم السيبرانية والأدلة الإلكترونية، شملت الجهاز القضائي وإدارة النيابة العامة ووحدات الشرطة، على تعزيز أساليب إنفاذ القانون والتحقيق. ويُضطلع بهذه البرامج في إطار مشروع مدعوم من الاتحاد الأوروبي ومجلس أوروبا. وقد عزَّزت هذه التدابير الخاصة ببناء القدرات مقدرة موظفي أجهزة إنفاذ القانون الوطنية على اتباع إجراءات عمل موحَّدة أكثر فعالية، استناداً إلى الممارسات والخبرات الجيدة، وكذلك إلى الدروس المستفادة من دول أخرى أطراف في اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية.

٣٦١- وأبلغت سري لانكا بأن الحكومة اعتمدت في تشرين الأول/أكتوبر ٢٠١٨ استراتيجية شاملة بشأن الأمن السيبراني. وبناءً عليه، تعكف سري لانكا الآن على صوغ تشريعات بشأن الأمن السيبراني وحماية البيانات. وتقود هاتين المبادرتين وزارة البنى التحتية الرقمية وتكنولوجيا المعلومات، بدعمٍ من فرق التصدي للطوارئ الحاسوبية، وهيئة تكنولوجيا المعلومات والاتصالات، ومصرف سري لانكا المركزي، وغير ذلك من أصحاب المصلحة الرئيسيين. وقد أدرجت الوزارةُ القطاعَ الخاص في هذه الجهود، وسوف تتَّبع الحكومة نهجاً يحتوي الجميع من خلال التشاور مع أصحاب المصلحة الرئيسيين في استعراض مشاريع التشريعات الجديدة.

سويسرا

٣٦٢- لاحظت سويسرا أنَّ تطور تكنولوجيات المعلومات والاتصالات، بينما يتيح فرصاً لم يسبق لها مثيل للأفراد والمؤسسات ومنشآت الأعمال والتجارة، فهو يمثِّل في الوقت نفسه تحدِّيات، وخصوصاً في مجال العدالة الجنائية، ومن ثم سيادة القانون. وفي حين أنَّ الجريمة السيبرانية، بالمعنى الدقيق لهذا المصطلح، أي الأفعال الجُرمية التي تُرتكب بواسطة النظم الحاسوبية، بما في ذلك الأفعال الجُرمية التي تترك أدلة في النُّظُم الحاسوبية، آخذة في التطور، وفي حين أنَّ الأدلة على هذه الأفعال الجرمية يتزايد تخزينها في خوادم حاسوبية موجودة في ولايات قضائية أجنبية، قد تكون متعددة ومتغيرة وغير معلومة، وذلك على سبيل المثال في "الفضاء الحاسوبي"، فإنَّ سلطات إنفاذ القانون مقيَّدة بحدود أراضي الدول ولا بدَّ لها من احترام سيادتها.

٣٦٣- ولاحظت سويسرا بقلق محدودية فعالية المساعدة القانونية المتبادلة في الحصول على الأدلة الإلكترونية السريعة الزوال، وحالات فقدان (المعرفة عن) أماكن البيانات، وكذلك كون الدول تعول بقدر متزايد على الوصول الأحادي الجانب عبر الحدود إلى البيانات في غياب قواعد دولية في هذا الشأن.

٣٦٤- وشدَّدت سويسرا، بوصفها دولة طرفاً في اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، على أهمية هذه الاتفاقية. وترى سويسرا أن هذه الاتفاقية تسهِّل التعاون بقدرٍ كبير، من خلال مواءمة القوانين ووضع الإجراءات وتعيين جهات الاتصال. واستناداً إلى هذه الاتفاقية، من الضروري تسهيل التعاون الدولي وزيادته.

٣٦٥- وستظل مسألة ما إذا كان مقدِّم الخدمات موجودا أو يعرض خدمة على نحو كافٍ في إقليم دولة طرف ما، ومن ثم يخضع للولاية القضائية لتلك الدولة، مسألة حاسمة الأهمية في السنوات المقبلة. وستكون هذه المسألة هامة لا من حيث القانون الجنائي فقط بل أيضاً من حيث قانون الضرائب وقانون حقوق التأليف والطبع والنشر، على سبيل المثال.

٣٦٦- وشدَّدت سويسرا على أنَّه يجب التقيد بالتزامات الدول بمقتضى القانون الدولي، وخصوصاً قانون حقوق الإنسان، في جميع الأوقات، بما في ذلك عند التنظيم الرقابي للفضاء السيبراني وعند تجريم أفعال الجريمة السيبرانية والتحقيق فيها والملاحقة القضائية لمرتكبيها. ويجب أن توضع في الاعتبار مبادئ حماية البيانات وغيرها من ضمانات سيادة القانون وأن تُتَّبع، وخصوصاً عند بحث ومناقشة سبل جديدة للتعاون الدولي وللتحقيقات العابرة للحدود الوطنية.

الجمهورية العربية السورية

٣٦٧- أكَّدت الجمهورية العربية السورية أن خطر الجريمة المعلوماتية (السيبرانية) يستفحل يوماً بعد يوم، وذلك مع تنامي استخدام تكنولوجيات المعلومات والاتصالات من قبل الشبكات الإجرامية والجماعات الإرهابية لتحقيق أغراضها الإجرامية والإرهابية. وهذا يؤثِّر في استقرار البلدان وفي بُناها التحتية ومؤسساتها، وبخاصة في النسيج الاجتماعي والثقافي والتطور الاقتصادي والتنموي. كما أن توسع الفجوة الرقمية بين الدول يقوض حتماً قدرة العديد من الدول على منع هذه الجرائم ومكافحتها وملاحقة مرتكبيها.

٣٦٨- وترى الجمهورية العربية السورية أن مما لا شك فيه أنَّ ارتفاع معدَّلات الجرائم المرتكبة في العالم الرقمي وازدياد عددها كان له تأثير كبير في انتشار الجرائم الإرهابية حول العالم، وبخاصة الجرائم المرتكبة من قِبل التنظيم الإرهابي في الجمهورية العربية السورية والعراق. ويسهِّل الفضاء الرقمي غير المراقب وغير القابل للتتبع على الإرهابيين ارتكاب جميع أشكال الجرائم، من قتل واتجار بالأشخاص، واتجار بالممتلكات الثقافية، ونهب المعالم والمواقع الدينية، واستخدام الإنترنت لأغراض الاعتداء على الأطفال واختطافهم وتجنيدهم من أجل استخدامهم في الأعمال القتالية والإرهاب، وكذلك أفعال العنصرية والتحريض على الكراهية أو الاقتتال الطائفي أو العرقي أو المذهبي، وكذلك اقتراف الانتهاكات الجسيمة الأخرى للقوانين والاتفاقيات والقرارات الدولية ذات الصلة، مما يستدعي التصدي الجدي على الصعيد الدولي.

٣٦٩- وقد اتخذت الجمهورية العربية السورية العديد من التدابير من أجل مكافحة خطر الجرائم الإلكترونية واستخدام الفضاء الرقمي من قِبل الجماعات الإرهابية لارتكاب أبشع الجرائم الإرهابية العابرة للحدود الوطنية، وشملت تلك التدابير تعزيز الأُطر القانونية. وفي هذا الصدد، أصدرت الحكومة المرسوم التشريعي رقم ١٧ لعام ٢٠١٢ بشأن مكافحة الجرائم المعلوماتية، وتشريع استخدام الدليل الجنائي الرقمي بغية زيادة فعالية مكافحة الجرائم التقليدية التي تنطوي على استخدام تكنولوجيات المعلومات والاتصالات. وأُصدر القانون رقم ٩ لعام ٢٠١٨، الذي يتضمَّن إحداث نيابة عامة ومحاكم متخصصة في قضايا جرائم المعلوماتية والاتصالات، وذلك بغية زيادة الوعي بخطورة هذه الجرائم وبناء القدرات وحماية الضحايا في البلد.

٣٧٠- وفي التطبيق العملي للتشريعات، واجهت السلطات المختصة مشاكل عديدة وتحديات جمة، بالنظر إلى أنَّ هذا النوع من الجريمة لا حدود له بطبيعته، مما يجعل التحقيقات الجنائية أكثر تعقُّداً على سلطات إنفاذ القانون. وتشمل هذه التحديات مجابهة احتكار بلدان متقدمة النمو لشبكة الإنترنت العالمية، وتسييس العمل، وعدم التعاون في مجال مشاطرة سلطات الجمهورية العربية السورية في الأدلة والمعلومات عن الأشخاص الذين يرتكبون الأنشطة الإجرامية عبر الإنترنت. وإضافةً إلى ذلك، أبلغت الجمهورية العربية السورية بأنَّ الحصار المطبق عليها والتدابير القسرية اللاشرعية الأحادية الجانب المفروضة عليها من جانب الولايات المتحدة وبلدان أخرى والاتحاد الأوروبي، تحتكر تكنولوجيات الاتصالات، كل ذلك حد ويحد من حصول السلطات المعنية في البلد على التكنولوجيات والأدوات اللازمة لمكافحة هذه الأنشطة الإجرامية.

٣٧١- وترى الجمهورية العربية السورية أن صكوك القانون الجنائي المستخدمة حاليًّا على الصعيدين الدولي والإقليمي غير كافية لمواجهة استخدام تكنولوجيات المعلومات والاتصالات غير المشروع في العمليات الإجرامية والإرهابية. ولا توجد في الوقت الحالي اتفاقية دولية في هذا السياق، ما عدا اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، التي لا تشمل استخدام تكنولوجيات المعلومات في الأعمال الإرهابية.

٣٧٢- وفي ضوء ما تقدَّم، وبغية تعزيز مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، توصي الجمهورية العربية السورية بما يلي:

(أ) تقيُّد الدول الصارم بالتزاماتها الدولية وتنفيذ قرارات مجلس الأمن ذات الصلة بمكافحة الإرهاب؛

(ب) تعزيز التعاون الإقليمي والدولي الفعال، بما في ذلك من خلال تبادل المعلومات، ووضع آلية مرنة متَّفق عليها لتبادل المعلومات والأدلة الرقمية؛

(ج) التوصُّل إلى اتفاق مبدئي بين الدول الأعضاء بشأن سُبُل بحث الحلول في مجال مكافحة الجرائم المرتكبة باستخدام تكنولوجيات المعلومات والاتصالات، وذلك من أجل إتاحة المجال لإنشاء فريق عامل مفتوح العضوية تابع للأمم المتحدة في نيويورك يضمن مشاركة كل الدول المعنية في مناقشة هذا الموضوع؛

(د) وضع صك قانوني دولي ملزِم بشأن التعاون الدولي في هذا المجال بما يتوافق مع مصالح الدول الأعضاء، على أن يوضع في الاعتبار أنَّ صكوك القانون الجنائي القائمة غير كافية لمكافحة جرائم تكنولوجيات المعلومات والاتصالات؛

(هـ) سدُّ "الفجوة الرقمية" من خلال تخلِّي الدول عن احتكارها للتكنولوجيا الإلكترونية وأدواتها، بعد أن ثبت عدم مقدرتها على تأمين الحماية الكاملة من عواقب إساءة استخدام تكنولوجيات المعلومات والاتصالات، وذلك برفع القيود المفروضة على نقل هذه التكنولوجيا والأدوات إلى كل البلدان دون تمييز؛

(و) تعزيز إجراءات الوقاية والمنع عبر التعاون والمشاركة الفاعلة من جميع الدول؛

(ز) تعجيل الاستجابة لطلبات التعاون الدولي، وبخاصةٍ لغرض تأمين الأدلة الرقمية والحفاظ عليها، وتحديد أُطر زمنية لهذه الاستجابة؛

(ح) النظر في إنشاء منصة إلكترونية عالمية تفاعلية، تشترك فيها الجهات الحكومية المعنية في كل من الدول الأعضاء. ومن شأن هذه المنصة أن تسهِّل تبادل المعلومات عن قضايا الجرائم السيبرانية العابرة للحدود الوطنية، وكذلك تقديم الإرشادات بشأن الاستخدام الآمن لقواعد البيانات الإلكترونية، بالإضافة إلى إتاحة برامج متخصصة للمساعدة على منع الجرائم السيبرانية وإحباط الانتساب إلى أوساط الإجرام السيبراني، فضلا عن توفير مبادئ توجيهية أخرى تكفل الاستجابة السريعة بما يتلاءم مع تعقُّد التكنولوجيا المستخدمة في هذه الجرائم؛

(ط) بناء القدرات الوطنية وتقديم المساعدة التقنية من أجل تحسين مهارات السلطات المختصة للتصدي بفعالية لتحديات الجريمة السيبرانية والتحديات المقترنة بالأدلة الرقمية، بما في ذلك عن طريق دعم الجهود الوطنية الرامية إلى تطوير ونشر البنى التحتية الخاصة بالإنترنت بغية تحسين القدرات على مكافحة الجرائم السيبرانية، ودعم التدريب والتوعية بشأن المسائل التقنية ورقمنة حفظ السجلات؛

(ي) توفير التجهيزات اللازمة للحصول على الأدلة الرقمية، ودعم تدريب عدد كاف من المحققين الرقميين المؤهلين والمدرَّبين على أساليب التحقق في الجرائم السيبرانية واستخلاص الأدلة الرقمية المتصلة بها؛

(ك) وضع معايير رقابية ملزِمة بشأن استخدام الفضاء الرقمي، تأخذ في الاعتبار تحقيق التوازن بين حرية الإنترنت والخصوصية وأمن الدول، وكذلك استحداث أُطر عمل لمواجهة إساءة استخدام الفضاء الرقمي. وعلى سبيل المثال؛ فرض رقابة على مواقع تبادل العملات الافتراضية ("البيتكوين") التي يمكن أن تُستخدم لغسل الأموال وتمويل الإرهاب، وكذلك منصات شبكات التواصل الاجتماعي التي تُستخدم في التحريض على الجريمة؛

(ل) تعزيز الشراكة بين الجهات الحكومية المعنية وشركات القطاع الخاص، ومنها مثلاً شركات تقديم خدمات الإنترنت وشبكات الأجهزة الخلوية وغيرها، من أجل إتاحة المعلومات المخزنة لديها عند طلبها، وفقاً لضوابط قانونية وقضائية، بغية استكمال التحقيق في جرائم المعلوماتية واستخلاص الأدلة.

طاجيكستان

٣٧٣- أشارت طاجيكستان إلى أنَّ انتشار تكنولوجيات المعلومات والاتصالات وتطور البنى التحتية للمعلومات قد أسهما في إيجاد مجتمع المعلومات. وحسبما تبيِّن الممارسة المتبعة في العالم، أدى عصر المعلومات إلى توسيع آليات العنف السياسي، مُضيفاً إلى الأساليب المادية المتبعة في الإقناع والتلاعب بالوعي وغير ذلك من الطرائق المعلوماتية الخاصة بالتأثير على وعي الجمهور.

٣٧٤- وقدَّمت طاجيكستان التوصيات التالية:

(أ) ينبغي تشجيع الحكومات على توفير المعلومات والتدريب المهني على نحو وافٍ للعاملين في أجهزة إنفاذ القانون التابعة لها، وتزويدهم بالموارد الوافية للقيام بالتحقيق الفعال في الجرائم ذات الصلة باستخدام الإنترنت وغيرها من تكنولوجيات المعلومات والاتصالات؛

(ب) ينبغي للحكومات أن تشجِّع سلطاتها المسؤولة عن إنفاذ القانون على اكتساب المهارات المتخصصة التي تسهِّل التحقيق في الجرائم السيبرانية وتتيح لها إجراء التحقيقات الجنائية بنجاح؛

(ج) يجب على الحكومات أن تعمل على نحو جماعي من أجل كفالة تبادل المعلومات بفعالية فيما بين الهيئات وعلى الصعيد الأقاليمي، وإزالة العقبات التي تُواجَه في القيام بالتحقيقات بشأن الجرائم السيبرانية في بعض البلدان، وإدخال التغييرات اللازمة على التشريعات والممارسات والإجراءات المتَّبعة بغية الإسراع في تبادل المعلومات، ومعالجة الطلبات الواردة من مختلف موارد المعلومات، وإحالة الأدلة الرقمية؛

(د) من الضروري تنظيم دورات تدريبية خاصة منتظمة من أجل كفالة التدريب المهني السليم للعاملين في سلطات إنفاذ القانون في مجال مكافحة الجريمة السيبرانية واستخدام الإنترنت وغيرها من تكنولوجيات المعلومات والاتصالات؛

(هـ) يُعتبر من الضروري إعداد واعتماد اتفاقية عالمية في إطار الأمم المتحدة بشأن التعاون على مكافحة الجرائم ذات الصلة باستخدام تكنولوجيات المعلومات والاتصالات، تلبي مصالح جميع الدول الأعضاء.

تايلند

٣٧٥- أبلغت تايلند بأنَّ الجرائم السيبرانية النمطية التي تُواجَه في البلد تشمل الاختراق الحاسوبي، والاحتيال عبر الإنترنت، والتسلل الحاسوبي، والمطاردة السيبرانية، وسرقة الهوية على الإنترنت، والتعدي على الأطفال على الإنترنت، وبث المحتويات المسيئة، ونشر الشيفرات الخبيثة، والهجمات بفيروسات طلب الفدية. ويلتمس المجرمون دائماً الثغرات في التكنولوجيا من أجل إخفاء هويتهم، بما في ذلك من خلال اتِّباع نهوج ابتكارية كاستخدام عملات فك التشفير (العملات المشفَّرة) في نظام سلسلة كتل البيانات من أجل غسل الأموال.

٣٧٦- وأبلغت تايلند أيضاً بأنَّ صعوبة جمع الأدلة الرقمية تُواجَه في معظم قضايا الجريمة السيبرانية. وهذا يُعزى إلى أنَّ الأدلة الهامة في الملاحقة القضائية لمرتكبي الجرائم السيبرانية تكمن في مسار حركة البيانات الحاسوبية التي تكون في حيازة مقدِّمي خدمات الإنترنت ومقدِّمي خدمات وسائط التواصل الاجتماعي، ومنها مثلاً الفيسبوك، ولاين، وإنستغرام، ووي تشات، وواتس آب، التي كثيراً ما تكون مسجَّلة في بلدان أجنبية وغير مُرغمة على تقديم المساعدة والتعاون وفقاً للقانون التايلندي الخاص بالجرائم ذات الصلة بالحاسوب. ولذلك فإنَّ أجهزة إنفاذ القانون قد تحتاج إلى الحصول على تلك الأدلة من خلال القناة الرسمية التي هي معاهدات المساعدة القانونية المتبادلة. وهذه العملية تستهلك وقتاً طويلاً، وقد تصبح عسيرة في الممارسة العملية. كما أنَّ المعلومات المحصَّلة من خلال قنوات التعاون غير الرسمية، على الرغم من فائدتها، قد تكون غير مناسبة كأدلة تُبرز أمام المحكمة.

٣٧٧- وبالإضافة إلى ذلك فإنَّ بعض التكنولوجيات الجديدة، ومنها مثلاً التشفير، قد تحول دون الوصول إلى البيانات. وبعض الهواتف المحمولة "الذكية" قد لا يمكن فتح قفلها من دون موافقة مالكي الأجهزة، مما يحول دون الوصول إلى نُظمها التشغيلية. ويُضاف إلى ذلك أنَّ الافتقار إلى أدوات وبرامجيات التحليل الجنائي الرقمية بسبب تكلفتها العالية يمثل مشكلة شائعة يواجهها اختصاصيو التفتيش الجنائي الحاسوبي، والأدوات المتاحة مجاناً وبرامجيات المصادر المفتوحة محدودة القدرة في مجال التفتيش الجنائي الحاسوبي.

٣٧٨- وأبلغت تايلند أيضاً بأنَّ أجهزة إنفاذ القانون قد لا يكون لديها فهم كاف بشأن الأدلة الرقمية والتكنولوجيات المصرفية المالية العصرية. وقد يفتقر العديد من الموظفين إلى الخبرات اللازمة في قراءة البيانات المالية أو التماس الأدلة الظرفية، بما في ذلك عن طريق تقنيات التحقيق السيبراني العصرية. ومن ثم فإنَّ من اللازم توفير التدريب بشأن الجريمة السيبرانية للمدَّعين العامين وسائر موظفي إنفاذ القانون، وإيجاد منصَّة للتشارك في المعارف وأفضل الممارسات المتَّبعة.

٣٧٩- ومع أنَّ قانون الجرائم ذات الصلة بالحاسوب يفرض واجباً على مقدِّمي الخدمات بأن يحتفظوا ببيانات الحركة الحاسوبية وأن يقدموا المعلومات المطلوبة إلى السلطة المختصة، فإنَّ بعض مقدِّمي الخدمات لا يمتثلون لذلك على نحو تام دائماً. ويقضي بعضهم وقتاً في تقديم المعلومات المطلوبة بسبب ضخامة عدد الطلبات. ويمانع بعضهم في الإفصاح عن البيانات بسبب قلقهم بشأن خصوصية زبائنهم.

٣٨٠- وأكَّدت تايلند أنَّ تزايد استخدام تكنولوجيات المعلومات والاتصالات، ومعه وصول عدد أكبر من الأجهزة إلى خدمات الإنترنت، جعل البُنى التحتية الحاسمة الأهمية لدى الدول والمنشآت

معرضة للمخاطر. وفي حين أنَّ هذه الأجهزة من الممكن أن تكون متضررة وتم الإخلال بها من الناحية التكنولوجية، فإنه لا بدَّ من أن يظل نظام المعلومات مستقراً وآمناً تماماً. ومن ثم فإنَّ التعاون بين جميع الهيئات المعنية وجميع أصحاب المصلحة المعنيين لازم من أجل حماية هذا النظام. ومن الصعب أيضاً أن تُستبان بوضوح النية التي تنطوي عليها الطلبات التي يتلقاها مقدِّمو خدمات النظم.

٣٨١- وفي تايلند، يمثل قانون الجرائم ذات الصلة بالحاسوب (القانون رقم B.E.2550) (٢٠٠٧) القانون الرئيسي الذي يتناول مسائل الملاحقة القضائية لمرتكبي الجرائم السيبرانية. وهو يُستخدم مقترناً بقوانين أخرى تقرِّر الأفعال الجرمية الجنائية ذات الصلة بالجريمة السيبرانية، ومنها مثلاً القانون الجنائي وقانون مكافحة الاتِّجار بالأشخاص وقانون المخدِّرات وقانون حقوق التأليف والطبع والنشر وقانون منع وقمع الضلوع في منظمة إجرامية عابرة للحدود الوطنية. ولا بدَّ من أن يكون سن القوانين ذات الصلة مصحوباً ببرامج لبناء قدرات الموظفين المعنيين على المستوى العملي، ومن بينهم موظفو إنفاذ القانون، وأن يكون مصحوباً كذلك بآليات تنسيق فعالة. وثمة حاجة عاجلة إلى رفع مستوى الإلمام بالتكنولوجيا الرقمية ومستوى الوعي والفهم لدى أصحاب المصلحة المعنيين وإعدادهم لتنفيذ هذه القوانين.

٣٨٢- وفيما يتعلق بحماية حقوق الأفراد، ومن بينهم الأطفال، أبلغت تايلند بأنَّ الأشخاص الضالعين في جرائم الاتجار بالأشخاص، والتنمُّر السيبراني، وعمليات الاحتيال عبر الإنترنت، بما في ذلك حِيل الغش، يستغلون التكنولوجيات الجديدة للتواصل مباشرةً مع الأفراد واكتساب ثقتهم لتحقيق أغراض إجرامية. وفي الوقت نفسه، يزداد بث المعتقدات المتطرِّفة والسلبية عبر الإنترنت. وتشمل التحديات الرئيسية ما يلي:

(أ) تحقيق الفعالية في تنفيذ القوانين واللوائح التنظيمية القائمة؛

(ب) التنسيق بين الهيئات المعنية، ومن ذلك مثلاً التنسيق بين موظفي أجهزة إنفاذ القانون ومتعهِّدي الخدمات المالية وأصحاب المصلحة المعنيين؛

(ج) مشاركة أصحاب المصلحة المتعددين المعنيين في تعزيز وحماية حقوق الأفراد.

٣٨٣- وترى تايلند أن التحقيق في الجرائم ذات الصلة يتعين أن يضع في الاعتبار مشاعر الضحايا وظروفهم، ومن ثم فهو يتطلب اتباع نهج خاص بالسياق المعيَّن ويستند إلى حقوق الإنسان. ومن ضمن الذين هم في حالات هشاشة، تبرز فئة الأطفال باعتبارهم هدفاً للتنمر السيبراني والمطاردة السيبرانية وألعاب الإنترنت والرسائل الجنسية ومواد التعدي الجنسي على الأطفال واستدراج الأطفال عبر الإنترنت والابتزاز الجنسي. وينبغي توجيه انتباه خاص إلى مواقع وسائط التواصل الاجتماعي، ومنها مثلاً فيسبوك وإنستغرام وتويتر.

٣٨٤- وخلصت تايلند إلى أنه لا يمكن لأيِّ بلد أن يمنع الجريمة السيبرانية ويقمعها وحده. ولذلك فإنَّ التعاون الدولي والحوار بين الدول الأعضاء مهمان جدًّا؛ وتشارك تايلند في فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، الذي هو المنصة الوحيدة في هذا الشأن. وتأمل تايلند أن يتم تمديد الولاية المسندة إلى فريق الخبراء وعمله إلى ما بعد عام ٢٠٢١.

تركيا

٣٨٥- أكَّدت تركيا أنَّ تكنولوجيات المعلومات والاتصالات تُستخدم في شبكة واسعة تشمل القطاعين العام والخاص والبُنى التحتية الحيوية والأفراد، وقد أصبحت واسعة الانتشار على الصعيدين الوطني والدولي كليهما. ونتيجة لذلك، باتت تكنولوجيات المعلومات والاتصالات تؤدي دوراً هامًّا في النمو المستدام والتنمية المستدامة. بيد أنه كلما ازداد استخدام هذه التكنولوجيات أصبح المجتمع أكثر اعتماداً عليها، وعُرضةً للمخاطر التي تسببها. ويواجه الأفراد والشركات والبنى التحتية الحيوية والدول مشاكل خطيرة بسبب الحادثات السيبرانية. وقد تُسبِّب أوجه الضعف الأمني في نُظُم المعلومات والاتصالات انقطاع الخدمة في هذه النظم أو تُعرِّضها للاستغلال، أو قد تؤدي في النهاية إلى خسائر في الأرواح أو خسائر اقتصادية واسعة النطاق، أو اضطراب في النظام العام، و/أو تعرِّض الأمن الوطني للخطر. ومن الناحية الأخرى، يقدم الفضاء السيبراني مزايا عدة لمرتكبي الهجمات على تكنولوجيات المعلومات والاتصالات، ومنها مثلاً إخفاء الهوية وإمكانية الإنكار. ومن العسير كشف مموِّلي ومنظِّمي الهجمات السيبرانية المستمرة والمتطورة التي تستهدف نُظُم المعلومات. وهذا الوضع يجعل مكافحة التهديدات والمهاجمين مهمةً صعبةً.

٣٨٦- وضمن هذا السياق، يتسم التعاون الدولي على الصعيد الوطني، الذي يشمل أصحاب المصلحة المعنيين، كالقطاعين العام والخاص والجامعات والمنظمات غير الحكومية والأفراد، بأهمية حاسمة، ولكن التعاون الدولي والتشارك في المعلومات يتسم بنفس الأهمية. ومن ثم فإنَّ واحداً من الأهداف الا ستراتيجية الرئيسية في الا ستراتيجية وخطة العمل الوطنيتين بشأن الأمن السيبراني هو مكافحة الجرائم السيبرانية. وفي هذا الصدد، تؤيد تركيا الأنشطة المنفذة على الصعيد الدولي ضمن مفهوم مكافحة الجريمة السيبرانية وتسهم فيها.

٣٨٧- وقد وقَّعت تركيا على اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، في عام ٢٠١٠. ثم أُدمجت الاتفاقية في القانون الداخلي من خلال سنِّ قانون الموافقة على التصديق على اتفاقية الجريمة السيبرانية، في عام ٢٠١٤. وإضافةً إلى ذلك فإنَّ المسائل ذات الصلة بالأمن السيبراني تخضع للتنظيم في إطار قانون العقوبات التركي.

٣٨٨- وأشارت تركيا إلى أنه بسبب تزايد اتساع انتشار استخدام الإنترنت وتكنولوجيات المعلومات والاتصالات الدائمة التقدُّم، أصبح الفضاء السيبراني بؤرة لكل شيء؛ تجتذب أنواعاً كثيرة من الجهات الفاعلة المعادية. وتتزايد صعوبةً استبانةُ هوية المجرمين السيبرانيين، بسبب تعدُّد طبقات بنية الإنترنت والخوادم الوكيلة المستخدمة للوصول إليها. ويتيح الاستخدام الخبيث لهذه التكنولوجيات الوسائل اللازمة لارتكاب أفعال الجريمة السيبرانية، ووسيطاً مريحاً للتواصل من جانب الجماعات الإرهابية. وتستخدم التنظيمات غير المشروعة تكنولوجيات المعلومات والاتصالات لترويج ونشر رسائلها الدعائية، وجمع المعلومات، وجمع الأموال، وتجنيد الأعضاء الجدد، وقيادة الأنشطة المنظّمة، والتشارك في المعلومات، وتخطيط أعمال الإرهاب وتنسيقها. وتميل الجماعات الإرهابية إلى استخدام التطبيقات والأدوات التي تتيح قنوات مشفَّرة للتواصل أو لتخطيط أو تنسيق أعمالها العدوانية. ويجعل هذا الوضع من العسير على أجهزة إنفاذ القانون استبانة هوية الإرهابيين واستبانة أنشطتهم.

٣٨٩- وترى تركيا أنَّ تعزيز أمن المعلومات على الصعيد العالمي وتطوير الثقافة الأمنية للمجتمع الدولي مسألتان حاسمتا الأهمية لكل أصحاب المصلحة المعنيين. كما أن تعزيز التشريعات الدولية والاتفاقات الدولية الثنائية أو المتعددة الأطراف عامل هام أيضاً. وفي هذا الخصوص، تعتقد تركيا أنَّ استحداث تدابير تيسِّر منع استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، وتعزيز آليات التعاون الدولي في هذا الميدان، من شأنهما أن يسهما في استبانة هوية الإرهابيين وكبحهم واستبانة أنشطتهم وإحباطها.

٣٩٠- ومن الناحية الأخرى، يمكن أن يُعتبر بث المحتوى غير المشروع عبر الإنترنت مشكلة خطيرة تفرز تحديات أمام ضمان الأمن السيبراني. كما أن الاعتداءات الخبيثة التي تقوم بها التنظيمات الإرهابية على القيم الإنسانية المشتركة وعلى الحق في الحياة في جميع أنحاء العالم، وكذلك المحتوى الذي يُبثُّ عبر الإنترنت كأدوات دعائية، يُبرزان أهمية منع استخدام الإنترنت لأغراض غير قانونية. وضمن هذا السياق، ينبغي أن تُعتبر مكافحة بث المحتوى غير القانوني في الإنترنت مسؤولية لا تقع على عاتق الدول وحدها بل تقع أيضاً على عاتق شركات الإنترنت العالمية، التي هي أكبر الجهات الفاعلة في ساحة الإنترنت. ولذلك ينبغي للجهات الفاعلة في الإنترنت أن تعمل بالتعاون مع الدول المعنية لغرض القيام بعناية بمنع الأنشطة الإجرامية التي تنفذها جميع التنظيمات الإجرامية على منصاتها.

٣٩١- وترى تركيا كذلك أنه بالنظر إلى أنَّ كل الجماعات الإرهابية تستخدم الفضاء السيبراني للقيام بأنشطة إجرامية ذات دوافع متباينة، فثمة حاجة ماسة إلى استجابة وسطاء الإنترنت العالميين بأقصى ما يمكن من السرعة والحساسية لطلبات إزالة المحتوى غير المشروع المتصل بهذه الجماعات الإرهابية. ويتسم التنفيذ الحازم والمستمر للقرارات بشأن هذا المحتوى بأهمية كبرى؛ وإلا فإنَّ الاستخدام الخبيث للإنترنت من جانب الجماعات الإرهابية يمكن أن يؤدي إلى أضرار لا يمكن تداركها. وفي هذا الصدد، يتسم التعاون من جانب مقدِّمي المحتوى والاستضافة المعنيين بأهمية حيوية لكفالة التعاون التام. كما أن امتثال مقدِّمي الخدمات العالميين لطلبات إزالة المحتوى، وفقاً للتشريعات والأوامر القضائية على الصعيدين الوطني والدولي، من شأنه أن يساعد كثيراً على مكافحة المحتوى غير المشروع الذي يبث على منصَّات الإنترنت.

المملكة المتحدة لبريطانيا العظمى وإيرلندا الشمالية

٣٩٢- ذكرت المملكة المتحدة أنَّ مفهوم "استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية" من شأنه أن يُفسَّر لأغراض التصدي له بأنه بديهي (وبأنه أوسع نطاقاً من نطاق الجريمة السيبرانية)، مع أنَّ التأطير الواسع للمسألة لا يسمح بتقديم إجابة واضحة في هذا الصدد. كما أن التحديات التي تعترض التصدي لاستخدام تكنولوجيات المعلومات والاتصالات في الجرائم تتبدى بطرائق شديدة التنوع والتعقُّد تبعاً لعدد من العوامل المتباينة. وتشمل هذه العوامل دوافع الجُناة، والسمات المقابلة و/أو حالات الهشاشة المقابلة لدى الضحايا، والأساليب والوسائل التكنولوجية التي يطبِّقها الجناة، بما في ذلك الأساليب المحددة الخاصة بتمويه أنشطتهم؛ وكذلك، بما يجسد كل ما سبق ذكره، ما إذا كانت الجريمة تشتمل على اقتحام للشبكة أو النظام أم تتعلق بمحتوى إجرامي (مثلاً المواد التي تصور استغلال الأطفال جنسيًّا).

٣٩٣- وبالنظر إلى هذه التباينات وشيوع تكنولوجيات المعلومات والاتصالات في كل الجرائم المعاصرة، إما في شكل أدلة رقمية أو عندما يُمثِّل محتوى تكنولوجيا المعلومات والاتصالات جريمة في حد ذاته، فإنَّ مفهوم "استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية" محدود من حيث مدى فائدته التشخيصية. وقد أبدت المملكة المتحدة ملاحظة مفادها أنَّ "العامل الرقمي" في الجريمة بات حقيقة واقعة منذ وقت غير قصير، يتجسد فيها إدراج المجرمين استخدام تكنولوجيات المعلومات والاتصالات في صلب أنشطتهم من أجل توسيع نطاق وفرص ارتكاب الجرائم، وزيادة استخدام الإنترنت والتعويل عليها في المجتمعات قاطبة. ومن ثم يمكن أن يقال إن التحديات الناتجة عن ذلك أمام أجهزة إنفاذ القانون لا تنفصل عن بعض التحديات الأعم والهائلة العدد التي تواجهها المجتمعات في التصدي لكثير من الجرائم المعاصرة عموماً.

٣٩٤- وعلى الرغم من هذه المسائل التعريفية، أشارت المملكة المتحدة إلى عدد من التحديات الاستراتيجية التي تعترض كل قدرات الدول الأعضاء على القيام بالتحقيق على وجه التحديد في الجرائم التي تنطوي على مكوِّن يتعلق باستخدام تكنولوجيات المعلومات والاتصالات وحل تلك الجرائم، ومن تلك التحديات ما يلي:

(أ) عدم كفاية الإمكانات أو القدرات التقنية اللازمة لإجراء التحقيقيات الرقمية، بما في ذلك عدم توافر الموظفين ذوي المهارات المهنية الوافية في تكنولوجيات المعلومات والاتصالات؛ أو وجود صعوبات في إعادة تدريب أولئك الموظفين، وخصوصاً الموظفين العاملين في أجهزة إنفاذ القانون الوطنية؛

(ب) عدم وجود قوانين موضوعية وطنية في عدد من الولايات القضائية لتجريم الأفعال الجرمية ذات الصلة باستخدام تكنولوجيات المعلومات والاتصالات، ولتشكيل أساس للتعاون الدولي من خلال الاعتراف المتبادل بهذه الجرائم (ازدواجية التجريم)؛

(ج) عدم وجود قوانين إجرائية وطنية، تشتمل على ضمانات ونظم رقابية مناسبة بشأن حقوق الإنسان، من أجل إتاحة التحقيق في الجرائم ذات الصلة باستخدام تكنولوجيا المعلومات والاتصالات وإمكانية قبول الأدلة الرقمية في المحاكم؛

(د) وجود تحديات في قياس المدى والتأثير غير المباشر للجرائم المتصلة باستخدام تكنولوجيات المعلومات والاتصالات، وما ينتج عن ذلك من تحديات في مجال زيادة الوعي لدى الجمهور بأضرارها وفي التشجيع على الإبلاغ عن هذه الجرائم؛

(هـ) التحديات في تشجيع الجمهور على الوعي وعلى اتباع السلوك الذي يراعي الأمن السيبراني و/أو الوعي بالجرائم ذات الصلة بتكنولوجيات المعلومات والاتصالات، من أجل الحد من هشاشة الجمهور تجاه هذه الجرائم، و/أو إدراك حالات وقوع هذه الجرائم من أجل الإبلاغ عنها؛

(و) التحديات العامة الناشئة من البلدان التي تتسم بضعف سيادة القانون فيها، أو الولايات القضائية غير المتعاونة التي تؤوي المجرمين السيبرانيين، وهي تحديات تجسد الطابع العابر للحدود لهذه الجرائم وكون هذه الجرائم تتجاوز الحاجة إلى موطئ قدم مادي في البلدان الضحايا؛

(ز) التحديات الناشئة من الوسائل التكنولوجية التي يستخدمها المجرمون لتمويه أنشطتهم بمزيد من الفعالية، بما في ذلك استخدام تكنولوجيات مثل الشبكة الخفية والتشفير والشبكات الخصوصية الافتراضية والعملات الافتراضية، كما هو مشار إليه في التقييم الاستراتيجي الوطني الذي اضطلعت به الهيئة الوطنية المعنية بالجريمة في عام ٢٠١٨.

٣٩٥- وقد ذُكر بإجمال عدد من التحديات المشار إليها أعلاه ذات الصلة بالمملكة المتحدة على وجه الخصوص في المذكرة الخطية المقدَّمة إلى الاجتماع الخامس لفريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، بشأن موضوعي إنفاذ القانون والتحقيقات والأدلة الإلكترونية والعدالة الجنائية.(١٠)

٣٩٦- وخارج إطار هذين الموضوعين، يظل التحدي الذي يواجه في فهم الجريمة المعتمِدة على الفضاء السيبراني تحدِّياً متميزاً. وقد حدَّدت المملكة المتحدة ثغرة معلومة بين تجارب الجمهور في مجال الجريمة السيبرانية، من ناحية، والإبلاغ عنها، من الناحية الأخرى، وذلك من خلال المقارنات بين الاستقصاءات الموجهة إلى الجمهور والإحصائيات الرسمية للإبلاغ عن الجرائم.

٣٩٧- وتواجه المملكة المتحدة أيضاً تحدِّيات تتعلق بالولايات القضائية غير المتعاونة. وقد لاحظت الهيئة الوطنية المعنية بالجريمة، في التقييم الاستراتيجي الوطني لعام ٢٠١٨، أنَّ "جماعات الجريمة السيبرانية، وكثيرة منها تقوم بعملياتها على الصعيد الدولي وناطقة باللغة الروسية، لا تزال تشكِّل تهديداً لمصالح المملكة المتحدة". وفي حالات كثيرة، تكون هذه الجماعات موجودة مادياً في ولايات قضائية لا تسمح بتسليم المواطنين بشأن هذه الجرائم، أو التي لا يكون فيها التعاون ضد هذه الجماعات متيسراً دائماً.

٣٩٨- وتعتقد المملكة المتحدة أنَّ فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية يتيح فرصة فريدة لمواصلة استكشاف حلول قائمة على التوافق في الآراء للتصدي للجريمة السيبرانية في الدول الأعضاء. وعلى وجه الخصوص فإن وضعية الفريق بوصفه منتدى خبراء، مسندة إليه ولاية النظر على نحو منهجي في مجموعة واسعة من المواضيع، ملائمة على نحو مثالي لضمان إجراء مناقشات بشأن اتخاذ تدابير للتصدي للجريمة السيبرانية تأخذ في الحسبان مجموعة شاملة من وجهات النظر والحلول الممكنة. ولذلك تعتقد المملكة المتحدة أنَّ من المهم كفالة الاعتراف بعملية فريق الخبراء بوصفها المنصة الرئيسية للمناقشات عن الجريمة السيبرانية، برعاية لجنة منع الجريمة والعدالة الجنائية وبالاتساق مع الولاية المسنَدة إلى تلك اللجنة بشأن النظر في مسائل أخرى ذات صلة بالجريمة. وعلاوةً على ذلك، تشجع المملكة المتحدة المكتب المعني بالمخدِّرات والجريمة والدول الأعضاء على الاستفادة التامة من فريق الخبراء، بوصفه منصَّة للمناقشات التقنية من جانب الخبراء، للاسترشاد به في عمل برنامج المساعدة التقنية الذي يضطلع به المكتب بشأن الجريمة السيبرانية.

٣٩٩- وتعتقد المملكة المتحدة أيضاً أنَّ اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية هي أنجع إطار يمكن أن يُستند إليه في مواصلة بناء التوافق في الآراء على الصعيد الدولي ومواءمة النُّهوج

(١٠) متاح في الموقع الشبكي www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Compilation_12March.pdf.

المتَّبعة بشأن الجريمة السيبرانية. فهذه الاتفاقية، التي تضم ٦٣ طرفاً، تحظى بتوافق آراء واسع النطاق عبر العديد من المناطق، وقد أثبتت أنها تتوافق مع البيئات القانونية والمؤسسية المتنوعة. كما أنَّ الاتفاقية، من خلال اللجنة المعنية بالجريمة السيبرانية، التي تيسِّر الحوار بين الأطراف في الاتفاقية، تنطوي على آلية متينة تكفل لها القدرة على أن تضع في الاعتبار التطورات التي تحدث في فضاء الجريمة السيبرانية، ومواكبة التحديات المستجدَّة والتكنولوجيات الجديدة. ولذلك توصي المملكة المتحدة بأن تتخذ الدول الأعضاء التي لم تصبح بعدُ أطرافاً في الاتفاقية الخطوات اللازمة لطلب الانضمام إليها، رهناً بكفالة تطبيق ضمانات سليمة بشأن حقوق الإنسان وبوجود القوانين الإجرائية الوطنية ذات الصلة. أما في الأحوال التي لا توجد فيها بالفعل هذه الأحكام القانونية الوطنية فإنَّ لدى مجلس أوروبا برامج خاصة ببناء القدرات اللازمة للانضمام إلى الاتفاقية؛ ومن ثم تعتقد المملكة المتحدة أنه ينبغي للدول الأعضاء أن تتواصل مع مجلس أوروبا من أجل تحديد مدى توافر برامج المساعدة التقنية هذه لهذه الأغراض، عن الاقتضاء.

الولايات المتحدة الأمريكية

٤٠٠- أبلغت الولايات المتحدة بأنها تواجه أربعة تحديات رئيسية، أولها الضغط الذي يُمارس من أجل الحد من مساهمات الخبراء في السياسات الدولية. ففي حين أنَّ أساليب إنفاذ القانون التقليدية قابلة لتكييفها لمكافحة الجريمة السيبرانية، فإنَّ التحديات المواجَهة معقَّدة وماضية في التطور. ومن ثم فإنَّ أي نقاشات عن السياسات في إطار الأمم المتحدة بشأن الجريمة السيبرانية ينبغي أن تفيد من المدخلات والمشورة المباشرة من الخبراء التقنيين. أما الضغط الذي يمارسه بعض الحكومات لإطلاق نقاشات سياسية بشأن معاهدات عالمية جديدة، على الرغم من عدم وجود تأييد بتوافق الآراء لاتِّباع هذا النهج، فهو يستهلك الموارد القيِّمة ويضعف مقدرة الخبراء على إسداء مشورة مجدية بشأن كيفية التغلُّب على التحديات الأساسية التي تواجهها الدول الأعضاء عند التحقيق في قضايا الجريمة السيبرانية وملاحقة مرتكبيها قضائياً. والمدخلات التي يسهم بها الخبراء ضرورية لفهم مسائل معقَّدة مثل يلي:

(أ) حماية حرية التعبير؛

(ب) القيود المناسبة على سلطة الدولة؛

(ج) التنفيذ الفعال للأطر والآليات القائمة؛

(د) توفير التدريب والمساعدة التقنية للبلدان النامية في الوقت المناسب.

٤٠١- وقد تبدَّت هذه المشكلة أثناء اعتماد قرار الجمعية العامة ١٨٧/٧٣، حيث أدى انقسام في التصويت إلى إطلاق نقاشات سياسية جديدة في الجمعية العامة على نحو يضعف مقدرة فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، المنشأ عملاً بقرار الجمعية العامة ٢٣٠/٦٥، على القيام بالولاية المسندة إليه. كما أن القرار ١٨٧/٧٣ يعرقل جهود فريق الخبراء من خلال وضع تقرير آخر قبل أن يكمل فريق الخبراء خطة عمله، وتقديم ذلك التقرير في محفل لا يشارك فيه في العادة خبراء إنفاذ القانون. وينبغي للدول الأعضاء أن تساند مساهمة ومشاركة خبراء إنفاذ القانون والعدالة الجنائية والقطاع الصناعي الخاص والمجتمع المدني في عمليات صنع السياسات في الأمم

المتحدة. وينبغي أيضاً للدول الأعضاء أنْ تكفل تنظيم النقاشات السياساتية على أساس المشورة المقدَّمة من الخبراء الوطنيين، الذين هم في "خط المواجهة" في ميدان مكافحة الجريمة السيبرانية.

٤٠٢- ويتعلق التحدِّي الثاني بتطور الجريمة السيبرانية والتنظيمات الإجرامية العابرة للحدود الوطنية. فقد وسَّعت التنظيمات الإجرامية العابرة للحدود الوطنية نطاق التهديدات التي تسببها الجريمة السيبرانية، وذلك باستغلال تكنولوجيات المعلومات والاتصالات، بما في ذلك الشبكة الخفية، لا من أجل تسهيل الهجمات فحسب، بل أيضاً من أجل إيجاد أسواق على الإنترنت للبيانات المسروقة. وتقوم الدول الأعضاء بخطوات للتصدي لذلك، تشمل زيادة الانضمام إلى اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية. وبالاستفادة من تلك الاتفاقية، عزَّزت بلدان من جميع المناطق (ومنها بلدان نامية وبلدان متقدمة النمو) القوانين الوطنية، وحسَّنت مقدرتها على التعاون مع غيرها من البلدان بطرائق تحدُّ أيضاً من مقدرة التنظيمات الإجرامية العابرة للحدود الوطنية على استغلال بنية تكنولوجيات المعلومات والاتصالات الوطنية التي لديها من أجل الأغراض الإجرامية.

٤٠٣- ويخص التحدِّي الثالث محدودية القدرات الوطنية وتقادم الأطر القانونية الوطنية. وتواجه الولايات المتحدة تحديات في العمل مع الشركاء على الملاحقة القضائية لمرتكبي الجرائم السيبرانية حيثما لا تكون لدى تلك البلدان سوى قدرات محدودة و/أو لا تكون قد حدَّثت أُطرها القانونية وسلطاتها التحقيقية الوطنية من أجل التصدي للجريمة السيبرانية. وفي حين تعوِّل بعض البلدان على القوانين الجنائية العامة فإنَّ القوانين التي تخص الجريمة السيبرانية تحديداً هي الأفضل. وعلى الرغم من عدم وجود تعريف متَّفق عليه للجريمة السيبرانية، يوجد اتفاق عام على السلوكيات غير المشروعة التي تشكل قائمة أساسية بالجرائم. ولدى المجتمع الدولي خبرة تمتد لأكثر عقد من الزمن، تشمل العديد من النظم القانونية المختلفة، في صوغ قوانين فعالة عصرية شاملة بشأن الجريمة السيبرانية. ويمكن صوغ تلك القوانين على نحو محايد من حيث التكنولوجيا، بحيث يتم تجنب الحاجة إلى إدخال تعديلات متواترة. وقد كانت اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية مصدر الإلهام الرئيسي لصكوك أخرى، وهي تشكل نموذجاً للقوانين الوطنية لبلدان ذات تقاليد ثقافية وقانونية متباينة، بما في ذلك بعض الدول الأعضاء التي لا تنظر حاليًّا في الانضمام إلى الاتفاقية. وتكون الجهود التي تبذلها الولايات المتحدة، إلى جانب غيرها من البلدان، من أجل الملاحقة القضائية لمرتكبي الجرائم السيبرانية أكثر نجاحاً عند العمل مع بلد يطبِّق قوانين تخص الفضاء السيبراني تحديداً.

٤٠٤- وتواجه الولايات المتحدة أيضاً تحديات في العمل مع البلدان التي نجحت في اعتماد قوانين تخص الجريمة السيبرانية ولكنْ قد تكون ذات قدرة محدودة على تنفيذ إطارها القانوني أو قد لا تكون قد اتخذت الخطوات اللازمة للقيام بذلك في الممارسة العملية. وإضافةً إلى ذلك، لا تزال الولايات المتحدة تواجه تحديات جسيمة في تلقي المساعدة من بعض الدول الأعضاء على استبانة هوية الجُناة وتوقيفهم وملاحقتهم قضائيًّا في الولايات القضائية لتلك الدول، وعلى الإذن لسلطاتها بالتعاون على الصعيد الدولي في قضايا الجريمة السيبرانية. وعلى سبيل المثال، هناك حاجة عاجلة إلى توفير التدريب المتخصِّص في مجال الأدلة الإلكترونية لسلطات العدالة الجنائية، وهذا هو السبب في أن الولايات المتحدة جهة مانحة للبرنامج العالمي المعني بالجريمة السيبرانية التابع للمكتب المعني بالمخدِّرات والجريمة، وكذلك البرامج التدريبية التي ترعاها منظمة الدول الأمريكية ومجلس أوروبا والآسيان والجماعة

الاقتصادية الأفريقية. وتوصي الولايات المتحدة بأن تعمِّق الدول الأعضاء تركيزها على هذه البرامج، وخصوصاً لصالح البلدان النامية. وينبغي للدول الأعضاء أن تعطي الأولوية لتقديم المساعدة بشأن الإصلاح التشريعي وبناء القدرات، بغية كفالة ترجمة القوانين الجديدة إلى إجراءات عملية.

٤٠٥- ويتعلق التحدي الرابع بالصعوبات التي تواجه في الحصول على الأدلة الإلكترونية. فعلى غرار الدول الأعضاء الأخرى، تواجه الولايات المتحدة تحدِّيات في الحصول على الأدلة الإلكترونية، التي أخذت تشيع في كل التحقيقات في مجال إنفاذ القانون، من الولايات القضائية الأجنبية، من أجل مكافحة الجريمة السيبرانية. وعلى وجه التحديد، تواجه الولايات المتحدة تحديات في الحصول على المساعدة من الدول الأعضاء التي تفتقر إلى الصلاحيات القانونية أو إلى القدرة على الاستجابة الفعالة لطلبات الحصول على الأدلة الإلكترونية.

٤٠٦- وعلى الصعيد الداخلي، تواجه الولايات المتحدة تحديات في تنفيذ آلاف الطلبات الواردة من ولايات قضائية أخرى للحصول على الأدلة الإلكترونية، وذلك في كثير من الأحيان لأنَّ تلك البلدان لا تدرك اشتراطات الولايات المتحدة في هذا الصدد، أو لا تقدم معلومات كافية للوفاء بالمعايير القانونية الخاصة بالولايات المتحدة. فقصور طلبات الحصول على المساعدة القانونية المتبادلة يتطلب من سلطات الولايات المتحدة التماس التوضيحات والمعلومات الإضافية من الشركاء الدوليين، مما يؤخِّر تلبية الطلبات. وينبغي للدول الأعضاء أن تعمل على سدِّ هذه الثغرات بتمكين السلطات المركزية والمختصة، من خلال تزويدها بموارد كافية وتدريب واف، اتساقاً مع التزاماتها بمقتضى صكوك مثل اتفاقية الجريمة المنظمة. والعمل جار أيضاً مع المكتب المعني بالمخدِّرات والجريمة على توفير أدوات جديدة للسلطات المركزية والمختصة. وتوصي الولايات المتحدة، علاوةً على ذلك، بزيادة أنشطة بناء القدرات من أجل الدول الأعضاء بشأن متطلبات وإجراءات المساعدة القانونية المتبادلة، بما في ذلك توفير التدريب على إعداد الطلبات الوافية التماساً للأدلة الإلكترونية.

٤٠٧- وأخيراً فمن أجل الحصول على الأدلة الإلكترونية، تستخدم الدول الأعضاء المعاهدات الثنائية للمساعدة القانونية المتبادلة، وكذلك الاتفاقيات المتعددة الأطراف، مثل اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية واتفاقية الجريمة المنظمة، كأساس قانوني للتعاون. ويشارك أيضاً أكثر من ٨٠ بلداً بنشاط في شبكة نقاط الاتصال "٧/٢٤" المعنية بجرائم التكنولوجيا العالية، التابعة لمجموعة البلدان السبعة، من أجل تسهيل تلبية طلبات الحفاظ على البيانات وغيرها من الطلبات. وتوصي الولايات المتحدة بأن تنظر الدول الأعضاء في الانضمام إلى هذه المعاهدات والشبكات واستخدامها في مكافحة الجريمة السيبرانية.

فنزويلا (جمهورية-البوليفارية)

٤٠٨- سلَّمت حكومة جمهورية فنزويلا البوليفارية بتنامي استخدام تكنولوجيات المعلومات والاتصالات، وبأنَّ دور المجتمع الدولي في استخدام هذه التكنولوجيات يمكن أن يسهم في بلوغ الأهداف التنموية المتَّفق عليها دوليًّا، بما في ذلك الأهداف الواردة في خطة التنمية المستدامة لعام ٢٠٣٠، وفي التصدي للتحديات الجديدة.

٤٠٩- وأكدت جمهورية فنزويلا البوليفارية أهمية إزالة العقبات التي تعرقل الحدَّ من الفجوات الرقمية، وخصوصاً الفجوات التي تعترض التحقيق التام للتنمية الاقتصادية والاجتماعية والثقافية للبلدان ورفاهية سكانها، وعلى وجه الخصوص في البلدان النامية. وشدَّدت على وجوب إنهاء استخدام تكنولوجيات المعلومات والاتصالات، بما فيها شبكات التواصل الاجتماعي، الذي ينتهك القانون الدولي ويضر بمصالح الدول الأعضاء.

٤١٠- وشجعت جمهورية فنزويلا البوليفارية على العمل المشترك الذي يقوم به المجتمع الدولي بغية كفالة الوصول إلى مجتمع المعلومات، و شجعت أيضاً على احترام المساواة بين الجنسين وتمكين المرأة، واحترام الهوية الثقافية، والتنوُّع الثقافي والعرقي واللغوي، والتقاليد والديانات، والقيم الأخلاقية.

٤١١- وأبلغت جمهورية فنزويلا البوليفارية بأنها تهدف إلى تحقيق استخدام ومعالجة المعلومات على نحو مسؤول من جانب وسائط الإعلام، وفقاً لمدونات قواعد السلوك والأخلاقيات المهنية. فلوسائط الإعلام بجميع أشكالها دور مهم في مجتمع المعلومات، وينبغي أن تؤدي تكنولوجيات المعلومات والاتصالات دوراً مسانداً في هذا الصدد. وأكدت جمهورية فنزويلا البوليفارية مجدداً الحاجةَ إلى الحدِّ من اختلالات التوازن الدولية التي تؤثر في وسائط الإعلام، وبخاصةٍ فيما يتعلق بالبُنى التحتية والموارد التقنية وتنمية الموارد البشرية.

٤١٢- ورأت جمهورية فنزويلا البوليفارية أن استخدام وسائط الإعلام كأداة للدعاية العدوانية ضد البلدان النامية بهدف تقويض حكوماتها مسألة تدعو إلى القلق. وفي هذا الصدد، سلطت جمهورية فنزويلا البوليفارية الضوء على الحاجة إلى تعزيز وسائل الاتصال البديلة ومصادر الاتصالات الحرة والتعدُّدية والمسؤولة التي تعكس الظروف الواقعية والمصالح الخاصة لبلدان العالم النامي وشعوبه.

٤١٣- ومن هذا المنطلق، فإن جمهورية فنزويلا البوليفارية، إدراكاً منها لكون صكوك القانون الجنائي الدولية غير كافية حاليًّا لمكافحة الجرائم المتصلة بتكنولوجيات المعلومات والاتصالات، ترى أنَّ من الضروري وضع اتفاقية في إطار الأمم المتحدة بشأن التعاون في هذا المجال، يُوافق عليها المجتمع الدولي وتستند أساساً إلى توافق في آرائه، وتُشجَّع فيها الدول الأعضاء على بناء مجتمع معلوماتي مسؤول وعلى المساعدة على اتخاذ التدابير اللازمة لاجتناب اتخاذ أي تدبير أُحادي الجانب لا يتوافق مع القانون الدولي وميثاق الأمم المتحدة ويحول دون تحقيق التنمية الاقتصادية والاجتماعية التامة لسكان البلدان المتضررة ويعرقل رفاههم، والامتناع عن اتخاذ أي تدبير من هذا النوع.

٤١٤- ورأت جمهورية فنزويلا البوليفارية، أن هذا القلق بشأن إمكانية استخدام تكنولوجيات المعلومات والاتصالات في النزاعات الدولية والعمليات المستترة وغير المشروعة والهجمات على بلدان ثالثة من قِبل الأفراد والتنظيمات والدول عن طريق استخدام النُّظُم الحاسوبية انطلاقاً من بلدان أخرى يتطلب اتخاذ تدابير ضمن إطار الأمم المتحدة من أجل إحراز تقدُّم في وضع وثيقة تساعد على تنظيم هذا الاستخدام وعلى التعاون في هذا المجال.

٤١٥- وبالنظر إلى القلق المتأتِّي من القدرة المعبَّر عنها من جانب بعض الحكومات على التصدي لهذه الهجمات باللجوء إلى الأسلحة التقليدية، أكدت جمهورية فنزويلا البوليفارية مجدَّداً أنَّ أنجع طريقة لمنع التهديدات الجديدة والتصدي لها هي من خلال التعاون المشترك بين جميع الدول،

وبذلك اجتناب تحوُّل الفضاء السيبراني إلى تهديد بالعمليات العسكرية. واعتبرت جمهورية فنزويلا البوليفارية أنَّ من الأولويات تعزيز الحوار والمناقشات الجارية بين الدول الأعضاء بغية التشارك في الممارسات الجيدة وفي الخبرات الوطنية أو الإقليمية، مع إيلاء الاهتمام بصفة خاصة للبلدان النامية. وبالمثل، أعربت جمهورية فنزويلا البوليفارية عن تأييدها لمقترح إنشاء فريق عامل حكومي دولي، برعاية الأمم المتحدة، يتولى البحث عن الحلول وتسوية الخلافات، بناءً على المساواة بين الدول.

٤١٦- وسلَّمت جمهورية فنزويلا البوليفارية أيضاً بأنَّ استخدام تكنولوجيات المعلومات والاتصالات غير المشروع يمكن أن يكون له تأثير ضار على البُنى التحتية والأمن الوطني والتنمية الاقتصادية لأيِّ دولة عضو، ولذلك شدَّدت على الحاجة إلى زيادة الجهود الدولية الرامية إلى التصدِّي لهذه المشكلة.