الأمم المتحدة E/CN.15/2013/24

المجلس الاقتصادي والاجتماعي

Distr.: General
5 March 2013
Arabic
Original: English

لجنة منع الجريمة والعدالة الجنائية
الدورة الثانية والعشرون
فيينا، ٢٢-٢٦ نيسان/أبريل ٢٠١٣
البند ٧ من جدول الأعمال المؤقَّت*
اتجاهات الجريمة على الصعيد العالمي والمسائل المستجدَّة وتدابير التصدِّي في مجال منع الجريمة والعدالة الجنائية

تعزيز الأنشطة المتصلة بمكافحة الجريمة السيبرانية، بما في ذلك المساعدة التقنية وبناء القدرات

تقرير الأمين العام

ملخّص

أُعِدَّ هذا التقرير عملاً بقرار لجنة منع الجريمة والعدالة الجنائية ٧/٢٠، المعنون "تعزيز الأنشطة المتصلة بمكافحة الجريمة السيبرانية، بما في ذلك المساعدة التقنية وبناء القدرات". وهو يقدِّم ملخّصاً لأنشطة مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة فيما يخص تقديمَ المساعدة التقنية وبناء القدرات إلى الدول الأعضاء، بالإضافة إلى لمحةٍ عامةٍ عن الأنشطة التي قام بها المكتب لمساندة فريق الخبراء المعني بإجراء دراسة شاملة لمشكلة الجريمة السيبرانية، وخلاصةٍ وافيةٍ لمشروع الدراسة المتعلقة بالجريمة السيبرانية.

* E/CN.15/2013/1.

020413 V.13-80771 (A)

أولاً- مقدّمة

١- أُعِدَّ هذا التقرير عملاً بقرار لجنة منع الجريمة والعدالة الجنائية ٧/٢٠، المعنون "تعزيز الأنشطة المتصلة بمكافحة الجريمة السيبرانية، بما في ذلك المساعدة التقنية وبناء القدرات".

٢- وفي ذلك القرار طلبت اللجنة إلى مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة أن يتعاون مع الدول الأعضاء والمنظمات الدولية والإقليمية المعنية والقطاع الخاص، حسب الاقتضاء، على مواصلة تزويد الدول، بناءً على طلبها واستنادا إلى احتياجاتها الوطنية، بالمساعدة التقنية والتدريب، خصوصا فيما يتعلق بمنع الجرائم السيبرانية بكل أشكالها وكشف تلك الجرائم والتحري عنها وملاحقة مرتكبيها، دون المساس بالأعمال والنتائج التي تتمخّض عنها اجتماعات فريق الخبراء المعني بإجراء دراسة شاملة لمشكلة الجريمة السيبرانية وتدابير تصدي لها من جانب الدول الأعضاء والمجتمع الدولي والقطاع الخاص لها.

٣- كما أحاطت اللجنة علما بنتائج الاجتماع الأول لفريق الخبراء (انظر الوثيقة E/CN.15/2011/19)، وطلبت إلى مكتب المخدِّرات والجريمة أن يعزّز تعاونه مع الدول الأعضاء والمنظمات المعنية، مثل المنظمة الدولية للشرطة الجنائية (الإنتربول)، ومكتب الشرطة الأوروبي، والاتحاد الدولي للاتصالات، والمفوّضية الأوروبية، ومجلس أوروبا، ومنظمة شنغهاي للتعاون، وكومنولث الدول المستقلة، والقطاع الخاص، بما في ذلك شركات صنع الحواسيب وشركات تقديم خدمات الإنترنت، على مكافحة الجريمة السيبرانية.

ثانياً- عمل مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة، بالتعاون مع الدول الأعضاء، والمنظمات الدولية والإقليمية، والقطاع الخاص لتقديم المساعدة التقنية والتدريب للدول

٤- انتهى مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة في عام ٢٠١٢ من صياغة البرنامج العالمي المعني بالجريمة السيبرانية، الذي يعتمد نهجا كلّياً يركّز على: (أ) تقديم التدريب للمهنيين الممارسين في مجال إنفاذ القانون والعدالة الجنائية على تقنيات التحقيق ونهوج العدالة الجنائية في التصدي للجريمة السيبرانية؛ و(ب) منع الجريمة السيبرانية وزيادة الوعي بشأنها؛ و(ج) تعزيز التعاون على الصعيد الوطني والإقليمي والدولي في مواجهة الجريمة السيبرانية؛ و(د) جمع البيانات وإجراء البحوث والتحليلات عن الصلات بين الجريمة المنظمة والجريمة السيبرانية. وفي إطار هذا البرنامج، سوف يشجِّع المكتب على بناء القدرات على

نحو مستدام وطويل الأمد، من خلال عدّة سبل ومنها الدورات التدريبية، بالتعاون مع طائفة متنوّعة من الشركاء، منهم الاتحاد الدولي للاتصالات، والقطاع الخاص والخبراء الأكاديميون.

٥- وقد صُمِّمت جميع أنشطة البرنامج المعني بالجريمة السيبرانية لتؤدي إلى زيادة القدرات الوطنية المستدامة الطويلة الأمد على منع الجريمة السيبرانية ومكافحتها. وسوف يتولى تنفيذ الأنشطة في إطار البرنامج مكتب المخدِّرات والجريمة في المقام الأول بصفته الوكالة المنفِّذة، مع حصوله على دعم إضافي من الاتحاد الدولي للاتصالات وغيره من الشركاء ذوي الصلة، وذلك حسب الاقتضاء ووفقا للمجال المواضيعي والطلبات المقدمَّة من الحكومات والولاية المسنَدَة ذات الصلة.

٦- وفي أيار/مايو ٢٠١١، وقَّع مكتب المخدِّرات والجريمة على مذكّرة تفاهم مع الاتحاد الدولي للاتصالات لغرض التعاون على تقديم المساعدة التقنية في مجال الجريمة السيبرانية والأمن السيبراني، في إطار ولاية كلٍّ من المنظمتين.[(١)] وبموجب هذه المذكرة، عمل المكتب مع الاتحاد الدولي للاتصالات في تقديم المساعدة التقنية إلى الدول بناء على طلبها. وفي هذا السياق، يركّز المكتب على العناية بالجوانب المتعلقة بمنع الجريمة والعدالة الجنائية في التصدي للجرائم السيبرانية، على حين يركّز الاتحاد الدولي للاتصالات على تعزيز الأمن السيبراني، بطرائق منها حماية البُنى الأساسية الحيوية من الهجمات الحاسوبية.

٧- وقد طلب المجلس الاقتصادي والاجتماعي، في قراره ٢٠١١/٣٣ المعنون "المنع والحماية والتعاون الدولي في مجال مكافحة استعمال تكنولوجيات المعلومات الجديدة بغرض الاعتداء على الأطفال و/أو استغلالهم"، إلى مكتب المخدِّرات والجريمة أن يجري دراسة تسهِّل تحديدَ ووصف وتقييم آثار تكنولوجيات المعلومات الجديدة على الاعتداء على الأطفال واستغلالهم، مع مراعاة البيانات ذات الصلة التي جمعها فريق الخبراء. وطلب المجلس أيضاً في ذلك القرار إلى مكتب المخدِّرات والجريمة أن يصمِّم ويجري تقييما لاحتياجات الدول من التدريب على التحقيق في الجرائم التي تُرتكب تجاه الأطفال باستعمال تكنولوجيات المعلومات والاتصالات الجديدة، وأن يصمِّم أيضاً، استنادا إلى نتائج تلك الدراسة الاستقصائية، برنامجَ تدريبٍ ومساعدة تقنية من أجل مساعدة الدول الأعضاء على مكافحة تلك الجرائم بقدر أكبر من الفعالية.

٨- وخلال عام ٢٠١١ والنصف الأول من عام ٢٠١٢، بدأ مكتب المخدِّرات والجريمة في استعراض المؤلفات في هذا المجال لغرض إجراء الدراسة عن آثار تكنولوجيات المعلومات

(1) انظر www.itu.int/ITU-D/cyb/cybersecurity/docs/cybercrime.pdf.

الجديدة على الاعتداء على الأطفال واستغلالهم، وقام بخطوات تحضيرية فيما يتعلق بتقييم الاحتياجات التدريبية. ووفقاً لقرار المجلس الاقتصادي والاجتماعي ٢٠١١/٣٣، سوف يُقدَّم إلى اللجنة تقرير عن تنفيذ ذلك القرار، بما في ذلك الأنشطة ذات الصلة بالدراسة المشار إليها، لكي تنظر فيه خلال دورتها الثالثة والعشرين في عام ٢٠١٤.

٩- في نيسان/أبريل وأيار/مايو ٢٠١٢، نظَّم مكتب المخدِّرات والجريمة حلقات عمل في نيروبي لعشر دول في شرق أفريقيا والجنوب الأفريقي؛ وفي بيروت لـ١٢ بلدا في غرب آسيا؛ وفي بانكوك لـ١١ بلدا في جنوب شرق آسيا وجنوبها. وأتاحت حلقات العمل فرصةً للحصول على معلومات بشأن احتياجات المساعدة التقنية لدى تلك البلدان في مجال الجريمة السيبرانية. وأظهرت الحلقات وجود ما يلي: (أ) حاجة مستبانة إلى تدريب أساسي لواضعي السياسات وصانعي القرار بغية رفع أولوية المسائل المتعلقة بالجريمة السيبرانية؛ و(ب) الحاجة إلى المزيد من التطوير لآليات التعاون الدولي الرسمية وغير الرسمية على حد سواء بين الموظفين المسؤولين عن إنفاذ القوانين وأعضاء النيابات العامة؛ و(ج) الحاجة إلى تحسين فرص الوصول إلى برمجيات التحليل الجنائي وأجهزته الحاسوبية اللازمة لإجراء التحقيقات بشأن الجريمة السيبرانية؛ و(د) الحاجة إلى تعزيز الشراكات بين القطاعين العام والخاص من أجل تدعيم التدابير الرامية إلى منع الجريمة السيبرانية. وعلى أساس نتائج حلقات العمل، ينظر مكتب المخدِّرات والجريمة حاليا في خيارات تقديم المساعدة التقنية ضمن إطار البرنامج العالمي المعني بالجريمة السيبرانية وبالتعاون مع الشركاء ذوي الصلة، ومنهم الاتحاد الدولي للاتصالات، وكذلك لأجل بلدانٍ في شرق أفريقيا والجنوب الأفريقي.

١٠- وحضر ممثلون عن مكتب المخدِّرات والجريمة اجتماعات مع كبرى الجهات المقدِّمة للخدمات الإلكترونية على المستوى العالمي من أجل مواصلة مسار التقدم باتجاه دعم القطاع الخاص وإشراكه في البرنامج العالمي المعني بالجريمة السيبرانية. ويتوخّى البرنامج ضرورة التعاون الوثيق مع الشركاء في القطاع الخاص والمنظمات الحكومية الدولية ذات الصلة بغية تقديم دعم تعاوني لبرامج بناء القدرات. وقد صُمِّم البرنامج لتيسير علاقات العمل بين سلطات إنفاذ القانون والمكاتب المحلية للجهات الرئيسية المقدِّمة للخدمات الإلكترونية على المستوى العالمي، بما في ذلك قيام مقدِّمي الخدمات على المستوى العالمي بتقديم عروض إيضاحية للموظفين المسؤولين عن إنفاذ القانون المتخصّصين في الجريمة السيبرانية حول الإجراءات المؤسسية والمتطلبات المتعلقة بمراعاة الأصول القانونية وتيسير قيام مقدِّمي خدمات الأمن السيبراني على المستوى العالمي ببثّ المعلومات الاستراتيجية بشأن التهديدات إلى المسؤولين عن إنفاذ القانون.

١١- وفي شباط/فبراير ٢٠١٢، أُوفدت بعثة تقييم أوّلي إلى بنما، بناء على طلب الحكومة، وذلك لغرض مواصلة تطوير القدرة الوطنية على مكافحة الجريمة السيبرانية. وقد نُظمت بالاشتراك بين المقر الرئيسي لمكتب المخدِّرات والجريمة والمكتب الإقليمي للمكسيك وأمريكا الوسطى التابع له، وعملت مع فريق عامل حكومي يشمل عدة إدارات لاستعراض وتنقيح الإطار التشريعي الخاص بالجريمة السيبرانية. والفريق العامل يضمّ السلطات المحلية وقادة الرأي، بالإضافة إلى كيانات القطاع الخاص، وقد أُنشئ للعمل على صياغة تشريع بشأن الجريمة السيبرانية لصالح بنما. وعُقدت مشاورات للاتفاق على نهج موسّع وشامل لمكافحة الجريمة السيبرانية في ذلك البلد. وأعربت السلطات البنمية عن اهتمامها أيضاً بالنهج التعاوني القائم بين الاتحاد الدولي للاتصالات ومكتب المخدِّرات والجريمة، والدعم التي قد تحصل عليه لتعزيز دفاعها عن البُنى الأساسية الحيوية في هذا المجال في بنما.

١٢- وإضافةً إلى ذلك، وبغية مواصلة تدعيم التعاون وإذكاء الوعي بشأن الجرائم السيبرانية، عقد مكتب المخدِّرات والجريمة أيضاً في عام ٢٠١٢ حلقةَ عملٍ في جمهورية إيران الإسلامية، بناء على طلبها، لتقديم دورات تدريبية إلى ٨٠ موظفاً من الموظفين المسؤولين عن إنفاذ القانون وموظفي وزارة العدل حول الجريمة السيبرانية. كما عُقدت اجتماعات مع المكتب المحلي للإنتربول، والشرطة المختصة بالجريمة السيبرانية، والهيئات القضائية بغية تعزيز التعاون الدولي على مكافحة الجريمة السيبرانية.

ثالثاً- أنشطة مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة لتعزيز التعاون مع الدول الأعضاء والمنظمات الحكومية الدولية والقطاع الخاص

١٣- بغية المُضيّ قُدماً في تعزيز التعاون في مجال مكافحة الجريمة السيبرانية على جميع المستويات، واصل مكتب المخدِّرات والجريمة المشاركةَ بصفة مراقب في مشاورات اللجنة المعنية بالاتفاقية المتعلقة بجرائم الفضاء الحاسوبي التابعة لمجلس أوروبا، في إطار الاتفاقية المذكورة ومؤتمرها السنوي بشأن التعاون على مكافحة الجريمة السيبرانية - أوكتوبس (Octopus).

١٤- كما شارك مكتب المخدِّرات والجريمة بصفة شريك في مبادرة الكومنولث المعنية بالجريمة السيبرانية، حيث التمس المكتب سُبل تحسين التعاون بينه وبين الشركاء في المبادرة. علاوة على ذلك، شارك بصفة مراقب في الفريق الأوروبي للتدريب والتثقيف بشأن الجريمة السيبرانية، وتعاون مع منظمة الأمن والتعاون في أوروبا في سياق اجتماعها السنوي لخبراء الشرطة.

رابعاً- أنشطة مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة لمساندة فريق الخبراء المعني بإجراء دراسة شاملة عن مشكلة الجريمة السيبرانية[أ]

١٥- عُقد الاجتماع الأول لفريق الخبراء المعني بإجراء دراسة شاملة عن مشكلة الجريمة السيبرانية، في فيينا في الفترة من ١٧ إلى ٢١ كانون الثاني/يناير ٢٠١١، وفي ذلك الاجتماع قام فريق الخبراء باستعراض واعتماد مجموعة من المواضيع ومنهجية للدراسة (انظر الوثيقة E/CN.15/2011/19). وتقرَّر في إطار المنهجية توزيع استبيان على الدول الأعضاء والمنظمات الحكومية الدولية وممثلين عن القطاع الخاص والمؤسسات الأكاديمية. وتولّى مكتب المخدِّرات والجريمة جمع المعلومات وفقاً للمنهجية المتَّفق عليها، خلال الفترة الممتدة من شهر شباط/فبراير ٢٠١٢ إلى شهر تموز/يوليه ٢٠١٢.[٢]

١٦- وقد أُرسل مشروع استبيان إلى جميع الدول الأعضاء في حزيران/يونيه ٢٠١٢ التماساً لتعليقاتها عليه. وعقب تلقي التعليقات، وضع مكتب المخدِّرات والجريمة الصيغة النهائية للاستبيان وعمّمه من خلال بوابة شبكية لجمع البيانات. وللتأكد من الدول الأعضاء من صحة جوانب المعلومات المجموعة والمحلَّلة، أرسل المكتب إلى كل دولة موجزا عن الأحكام التشريعية الخاصة بالجريمة السيبرانية لديها للتعليق عليه وتصحيحه إن اقتضت الضرورة. وفي تشرين الثاني/نوفمبر ٢٠١٢، تشاور المكتب مع الخبراء الذين رشّحتهم كل مجموعة إقليمية بخصوص التحليل الأولي للنتائج المتحصّل عليها من الاستبيانات التي استكملتها الدول الأعضاء. وبناء على الردود على الاستبيانات الواردة من الدول الأعضاء والقطاع الخاص والمؤسسات الأكاديمية والمنظمات الحكومية الدولية، أعدّ المكتب مشروع دراسة لعرضها على فريق الخبراء للنظر فيها.

١٧- وعُقد الاجتماع الثاني لفريق الخبراء في الفترة من ٢٥ إلى ٢٨ شباط/فبراير ٢٠١٣.[٣] وخلال ذلك الاجتماع، عُني الفريق العامل بالنظر في الدراسة الشاملة عن مشكلة الجريمة السيبرانية التي أعدّها مكتب المخدِّرات والجريمة برعاية فريق الخبراء. ولاحظ فريق الخبراء أن

(أ) نص القسم "رابعا" كان قد صدر في وثيقة معلومات أساسية غير منقّحة تحريرياً (UNODC/CCPCJ/EG.4/2013/2)؛ وقد نُقِّح النص تحريرياً في هذا التقرير وفقا للمعايير المقررة لدى الأمانة.

(2) وردت معلومات من ٦٩ دولة عضواً، فيما يلي توزُّعها الإقليمي: أفريقيا (١١) والقارة الأمريكية (١٣) وآسيا (١٩) وأوروبا (٢٤) وأوقيانوسيا (٢). كما وردت المعلومات من ٤٠ منظّمة من القطاع الخاص و١٧ مؤسسة أكاديمية و١١ منظمة حكومية دولية. واستعرضت الأمانة أيضاً أكثر من ٥٠٠ وثيقة من مصادر مفتوحة.

(3) ترد حصيلة نتائج الاجتماع في الوثيقة UNODC/CCPCJ/EG.4/2013/3.

مداولاته، وكذلك الدراسة، تمثل تجميعا للآراء والنهوج المختلفة التي تتخذها الدول لمنع ظاهرة الجريمة السيبرانية ومكافحتها. وخلال المناقشات حول الدراسة عن الجريمة السيبرانية، لوحظ وجود دعم واسع لبناء القدرات وتقديم المساعدة التقنية، ولدور مكتب المخدِّرات والجريمة في هذا المجال. وقد أُعرب عن آراء متباينة بخصوص مضمون الدراسة والنتائج التي خلصت إليها والخيارات المعروضة فيها. وتباحث فريق الخبراء في سُبل المضي قدماً في هذا الصدد، وأوصى بأن تنظر اللجنة في الدراسة على نحو إضافي خلال دورتها الثانية والعشرين.

١٨- والخلاصة الوافية الواردة فيما يلي عن الدراسة الشاملة، أعدّها مكتب المخدِّرات والجريمة بناء على تكليف من فريق الخبراء. أما النتائج والخيارات الواردة في الدراسة والخلاصة الوافية فقد أعدّها المكتب بناء على المعلومات المقدَّمة والمستمدة من واقع التجربة، وليس القصد منها أن تكون توصيات.[٤]

ألف- خلاصة وافية للدراسة الشاملة عن مشكلة الجريمة السيبرانية التي أعدّها مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة

١- الموصولية العالمية والجريمة السيبرانية

١٩- في عام ٢٠١١، كان عدد الأشخاص الذين يستطيعون الوصول إلى شبكة الإنترنت لا يقل عن ٢,٣ بليون نسمة، أي قرابة ثلث مجموع سكان العالم. ويعيش ما نسبته أكثر من ٦٠ في المائة من جميع مستعمِلي الإنترنت في البلدان النامية، ولا يتجاوز عمر ٤٥ في المائة من مجموع مستعمِلي الإنترنت ٢٥ عاماً. وبحلول عام ٢٠١٧، من المتوقّع أن تناهز نسبة المشتركين في خدمة الإنترنت النقّالة ذات النطاق العريض ٧٠ في المائة من مجموع سكان العالم. وبحلول عام ٢٠٢٠، سوف يفوق عددُ الأجهزة المتصلة بالشبكة (أي ما يسمى "الأشياء المتصلة بالإنترنت") عددَ الناس بنسبة ستة إلى واحد، مما سيؤدي إلى تحوّل في المفاهيم الحالية للإنترنت. ففي عالم الغد المتّسم بالموصولية الفائقة، سوف يصعب تصوُّر وقوع "جريمة حاسوبية" وربما أيِّ جريمة أخرى لا تنطوي على أدلة إلكترونية مرتبطة بالموصولية بواسطة بروتوكول الإنترنت.

٢٠- وتتوقّف تعاريف الجريمة السيبرانية، في الأكثر، على الغرض من استخدام المصطلح. فالجرائم السيبرانية الأساسية تتمثل في عدد محدود من أفعال التعدّي التي تمسّ بسرية البيانات أو النظم الحاسوبية وسلامتها وتوافرها. أمَّا الأفعال المرتكبة بواسطة الحواسيب والرامية إلى

(4) النص الكامل للدراسة متاح باللغة الإنكليزية فقط، كما هو مذكور في الوثيقة E/CN.15/2013/CRP.5.

تحقيق مكاسب شخصية أو مالية أو إحداث أضرار، بما في ذلك أشكال الجرائم المتصلة بالهوية وبمحتوى الحواسيب (والتي تندرج كلها ضمن نطاق أوسع من معنى "الجريمة السيبرانية")، فلا يمكن تطويعها بسهولة لتنضوي ضمن تعاريف قانونية لمصطلح جامع. ومن ثم يلزم إيجاد تعاريف معيّنة للأفعال الأساسية التي تشكِّل جريمة سيبرانية، وإن كان تعريف الجريمة السيبرانية لا يتسم بنفس القدر من الأهمية فيما يخص الأغراض الأخرى، كتحديد نطاق صلاحيات الهيئات المختصة بالتحقيقات والتعاون الدولي، حيث يفضل التركيز على الأدلة الإلكترونية فيما يخص أيَّ جريمة، بدلاً من التركيز على تركيبة مفاهيمية واسعة واصطناعية "للجريمة السيبرانية".

٢- الصورة العالمية للجريمة السيبرانية

٢١- شهدت بلدان عديدة زيادة هائلة في الموصولية العالمية في وقت يتَّسم بتحوّلات اقتصادية وديمغرافية وبتزايد التفاوت في الدخل وتقييد الإنفاق في القطاع الخاص وانخفاض السيولة المالية. وعلى الصعيد العالمي، لاحظ موظّفو إنفاذ القانون المجيبون عن استبيان الدراسة ارتفاع مستويات الجرائم السيبرانية، حيث يستغل الأفراد والجماعات الإجرامية المنظمة الفرص الجديدة المتاحة لارتكاب الجرائم، بدافعٍ من تحقيق الأرباح والمكاسب الشخصية. وتشير التقديرات إلى أنَّ مصدر أكثر من ٨٠ في المائة من الجرائم السيبرانية هو شكل من أشكال النشاط المنظَّم، حيث تقوم الأسواق السوداء للجرائم السيبرانية على دورة تشمل إعدادَ البرامجيات الخبيثة والفيروسات الحاسوبية والتحكُّم بشبكات حواسيب مُصابة مُعدية ("اعتداءات البوت نت") وتلقُّف البيانات الشخصية والمالية وبيع البيانات والمتاجرة بالمعلومات المالية. و لم يعد مرتكبو الجرائم السيبرانية بحاجة إلى مهارات أو تقنيات معقّدة. ففي بيئة البلدان النامية على وجه الخصوص، ظهرت شبكات فرعية تضم شباناً ينخرطون في أفعال الاحتيال المالي بواسطة الحاسوب، بدأ كثيرون منهم بالضلوع في الجرائم السيبرانية في أواخر سنوات المراهقة.

٢٢- وعلى الصعيد العالمي، تتوزّع أفعال الجريمة السيبرانية في طائفة واسعة من الجرائم المرتكبة بدافع مالي والجرائم المتصلة بالمحتوى الحاسوبي، فضلاً عن أفعال التعدّي التي تمسّ بسرية النظم الحاسوبية وسلامتها وقابلية النفاذ إليها. غير أنَّ تصوّرات المخاطر والتهديدات النسبية تختلف بين الحكومات ومؤسسات القطاع الخاص. وفي الوقت الراهن، لا تمثّل إحصاءات الجرائم المسجّلة لدى الشرطة أساساً سليماً للمقارنات بين عدّة بلدان مع أنَّ هذه الإحصاءات غالباً ما تكون هامّة لوضع السياسات العامة على الصعيد الوطني. ويرى ثلثا

عدد البلدان أنَّ نظم إحصاءات الشرطة لديها غير كافية لتسجيل الجرائم السيبرانية. وتقترن معدّلات الجرائم السيبرانية المسجّلة لدى الشرطة بمستويات التنمية القطرية وقدرة الشرطة المتخصصة أكثر من اقترانها بمعدّلات الجرائم المرتكبة.

٢٣- وتمثّل الدراسات الاستقصائية عن الإيذاء الإجرامي أساساً أسلم للمقارنة. إذ تُظهر هذه الاستقصاءات أنَّ معدل حالات ضحايا الإيذاء الفردية من الجرائم السيبرانية أعلى بكثير من معدّل حالات ضحايا الإيذاء من أشكال الجرائم "التقليدية". كما أن معدلات ضحايا الإيذاء الاحتيالي بتزوير بطاقات الائتمان وانتحال الشخصية على الإنترنت والوقوع ضحية للاستجابة لمحاولات "تصيُّد احتيالي" ومحاولات الوصول دون إذن إلى حسابات البريد الإلكتروني تتراوح بين ١ و١٧ في المائة من نسبة السكان الذين يستعملون الإنترنت في ٢١ بلداً في جميع أنحاء العالم، مقارنةً بمعدلات ضحايا الإيذاء من السطو والسلب وسرقة السيارات التقليدية، والتي تقل عن ٥ في المائة من نسبة السكان في هذه البلدان نفسها. وكانت معدلات ضحايا الإيذاء بسبب الجرائم السيبرانية أعلى في البلدان التي تشهد مستويات نمو منخفضة، مما يُبرز الحاجة إلى تعزيز جهود منع الجرائم في هذه البلدان.

٢٤- وأبلغت مؤسسات من القطاع الخاص في أوروبا عن معدلات حالات إيذاء مماثلة — تراوحت بين ٢ و١٦ في المائة — وكانت تتعلق بأفعال انتهاك البيانات بسبب الاقتحام أو "التصيد الاحتيالي". والمجال الذي يُتاح فيه اختيار الأدوات الإجرامية لارتكاب الجرائم، ومنها مثلا "اعتداءات البوت نت"، مجال له بُعد عالمي. فقد كان أكثر من مليون عنوان فريد من عناوين بروتوكول الإنترنت تعمل على الصعيد العالمي كخوادم "بوت نت" للتحكُّم في شبكات الحواسيب ومراقبتها، في عام ٢٠١١. كذلك فإنَّ محتوى الإنترنت يمثل أيضاً مصدر قلق كبير للحكومات، فمن المواد المُراد حذفها منه المواد الإباحية المتعلقة بالأطفال، والخطابات المفعمة بالكراهية، ومواد التشهير بتشويه السمعة، وانتقاد الحكومات، مما يثير دواعي قلق بخصوص قانون حقوق الإنسان في بعض الحالات. ويُقدَّر أنَّ ما نسبته حوالي ٢٤ في المائة من إجمالي حركة الإنترنت العالمية ينطوي على انتهاك حقوق المؤلف (حقوق التأليف والنشر)، إذ تشمل تنزيل كثير من المواد من مواقع التشارك في الملفات بين النظراء من مستعمِلي الإنترنت (P2P)، وخصوصاً في بلدان في أفريقيا وأمريكا الجنوبية وغرب آسيا وجنوبها.

٣- التشريعات الخاصة بالجريمة السيبرانية

٢٥- تؤدي التدابير القانونية دوراً رئيسياً في منع ومكافحة الجريمة السيبرانية. وهذه التدابير ضرورية في جميع المجالات، بما في ذلك التجريمُ والصلاحيات الإجرائية والولاية القضائية

والتعاون الدولي ومسؤولية مقدّمي خدمات الإنترنت. وعلى الصعيد الوطني، تتعلق في أكثر الأحيان قوانينُ الجريمة السيبرانية، القائمة منها والجديدة (أو المخطَّط لها) على حدٍّ سواء، بالتجريم، مما يدّل على التركيز غالباً على تحديد أفعال جُرمية متخصّصة باعتبارها من أفعال الجرائم السيبرانية الأساسية. غير أنَّ البلدان باتت تُسلِّم أكثر فأكثر بالحاجة إلى تشريعات في مجالات أخرى. ومقارنةً بالقوانين القائمة، فإنَّ القوانين الجديدة أو المخطط لها الخاصة بالجريمة السيبرانية أصبحت تُعنى أكثر من ذي قبلُ بإجراءات التحقيق والولاية القضائية والأدلّة الإلكترونية والتعاون الدولي. أما على الصعيد العالمي، فقد رأى أقلّ من نصف عدد البلدان المجيبة عن الاستبيان أنَّ أطر القوانين الجنائية والإجرائية الخاصة بها كافية، وإن كانت تنطوي على تباينات إقليمية كبيرة. ففي حين أبلغ أكثر من ثلثي عدد البلدان في أوروبا عن وجود تشريعات كافية، كانت الصورة معكوسة بالنسبة إلى أفريقيا والقارة الأمريكية وآسيا وأوقيانوسيا، حيث رأى أكثر من ثلثي عدد البلدان أنَّ قوانينها كافية جزئياً فقط، أو غير كافية البتّة. وأشار أيضاً نصف عدد البلدان فحسبُ التي أبلغت عن أنَّ قوانينها غير كافية إلى قوانين جديدة أو مخطط لها، مما يسلّط الضوء على الحاجة الملحَّة إلى تعزيز التشريعات في مناطقها.

٢٦- وقد شهد العقد الماضي تطورات ذات دلالة هامة على صعيد إصدار الصكوك الدولية والإقليمية الرامية إلى التصدّي للجرائم السيبرانية. ومن تلك الصكوك ما هو مُلزِم وما هو غير مُلزِم. ويمكن تحديد خمس مجموعات من الصكوك، أُعدَّت في إطار هيئات أو استُمدت من هيئات هي: (أ) مجلس أوروبا أو الاتحاد الأوروبي، (ب) كومنولث الدول المستقلة أو منظمة شنغهاي للتعاون، (ج) منظمات حكومية دولية أفريقية، (د) جامعة الدول العربية، (ه) الأمم المتحدة. ويُلاحظ وجود إخصاب متبادل بالغ الدلالة بين هذه الصكوك، في مجالات منها على وجه الخصوص المفاهيم والنهوج التي وُضعت في اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية. ويظهر تحليل لمواد ١٩ صكاً من الصكوك المتعددة الأطراف ذات الصلة بالجريمة السيبرانية وجودَ أحكام أساسية مشتركة من جهة، وتبايناً كبيراً في المجالات الموضوعية المتناولة من جهة أخرى.

٢٧- وعلى الصعيد العالمي، بلغ عدد البلدان التي وقّعت أو صدّقت أو كليهما على صك ملزم بشأن الجريمة السيبرانية ٨٢ بلداً.[٥] وهذه الصكوك المتعددة الأطراف المتعلقة بالجريمة

(5) صك واحد أو أكثر من الصكوك التالية: اتفاقية المجلس الأوروبي المتعلقة بالجريمة السيبرانية، أو الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، (جامعة الدول العربية)، أو الاتفاق المتعلق بالتعاون بين الدول الأعضاء في كومنولث الدول المستقلة لمكافحة الجرائم في مجال المعلومات الحاسوبية، أو اتفاق التعاون في ميدان أمن المعلومات على الصعيد الدولي (منظمة شنغهاي للتعاون).

السيبرانية إضافة إلى تأثيرها المباشر الذي يتمثل في العضوية فيها وتنفيذها رسمياً، لها تأثير غير مباشر على القوانين الوطنية، من خلال استخدامها كنموذج من جانب الدول غير الأطراف فيها، أو من خلال تأثيرها في تشريعات الدول الأطراف فيها على بلدان أخرى. وتتناسب العضوية في أيٍّ من الصكوك المتعددة الأطراف المتعلقة بالجريمة السيبرانية مع الزيادة المتصوَّرة في مدى كفاية القانون الجنائي والقانون الإجرائي الوطني، مما يدل على أنَّ الأحكام الحالية المتعددة الأطراف في هذه المجالات تُعتبر فعّالة عموماً. أما فيما يخص البلدان التي يفوق عددها الأربعين بلداً التي قدّمت معلومات، كانت اتفاقية المجلس الأوروبي المتعلقة بالجريمة السيبرانية هي الصك المتعدد الأطراف الذي استندت إليه على الأكثر لوضع تشريعات خاصة بالجرائم السيبرانية. وإجمالاً، استخدم حوالي نصف عدد هذه البلدان صكوكاً متعددة الأطراف مندرجة في "مجموعات" أخرى.

٢٨- وأبلغ ثلث عدد البلدان المجيبة عن الاستبيان عموماً بأنَّ تشريعاتها تتوافق بدرجة عالية، أو عالية جداً، مع تشريعات البلدان التي تُعتبر العلاقة بها هامّة لأغراض التعاون الدولي. غير أنَّ الوضع يتباين على الصعيد الإقليمي، إذ ترتفع درجات التوافق المبلّغ عنها في القارة الأمريكية وأوروبا. وقد يكون ذلك نتيجة لاستخدام بعض المناطق لصكوك متعددة الأطراف مصممة بطبيعتها لأداء دور في التوفيق بين التشريعات. وقد يعزى عدم الاتساق على المستوى الدولي وتنوّع القوانين الوطنية، من حيث تجريم الأفعال التي تعتبر جرائم سيبرانية والأسس التي تقوم عليها الولاية القضائية وآليات التعاون، إلى وجود صكوك متعددة بشأن الجريمة السيبرانية لها نطاق مواضيعي وجغرافي مختلف. وإن حالات التباين التي تعتري حالياً الصكوك والمناطق على حد سواء ناشئة عن الاختلافات القانونية والدستورية فيها، بما في ذلك ما يسود فيها من مفاهيم مختلفة بشأن الحقوق والخصوصية.

٤- التجريم

٢٩- جُمعت المعلومات بشأن القوانين الجنائية المتعلقة بالجرائم السيبرانية من خلال الاستبيان الخاص بالدراسة، وكذلك من خلال تحليل المصادر الرئيسية للتشريعات المتاحة التي جمعتها الأمانة.[٦] وأشار الاستبيان إلى ١٤ فعلاً يندرج عادةً ضمن مفاهيم الجرائم

(6) لقد حُلِّل المصدر الرئيسي لتشريعات ٩٧ دولة عضواً، بما في ذلك ٥٦ دولة أجابت عن الاستبيان، وكان توزّعها الإقليمي على النحو التالي: أفريقيا (١٥) والقارة الأمريكية (٢٢) وآسيا (٢٤) وأوروبا (٣٠) وأوقيانوسيا (٦).

السيبرانية.[٧] وتبيَّن من إجابات البلدان على الاستبيان أنَّ هذه الأفعال الـ١٤ مجرَّمة على نطاق واسع، باستثناء الجرائم المتعلقة بالرسائل الإلكترونية الاقتحامية، بصفة رئيسية، وكذلك إلى حد ما الجرائم المتعلقة بأدوات إساءة استعمال الحواسيب والعنصرية وكراهية الأجانب وإغواء أو "مراودة" الأطفال على الإنترنت. ويجسِّد هذا نوعاً من حدٍّ أساسي في توافق الآراء على ما يُعاقب عليه من السلوكيات الإجرامية السيبرانية. وأبلغت بلدان عن بعض الجرائم الإضافية غير المذكورة في الاستبيان؛ وهي تتعلق بصفة رئيسية بمحتوى الحواسيب، بما في ذلك تجريم المواد الفاحشة ولعب القمار على الإنترنت والأسواق غير المشروعة على الإنترنت من قبيل أسواق الاتجار بالمخدِّرات والبشر. وفيما يخص الأفعال الـ١٤ المذكورة، أبلغت بلدان بأنها تستند إلى الجرائم الخاصة بالفضاء السيبراني لتحديد الجرائم السيبرانية الأساسية التي تمس بسرية النظم الحاسوبية وسلامتها وقواعد النفاذ إليها. أما فيما يخص الأشكال الأخرى من الجرائم السيبرانية، فقد استُخدمت الجرائم العامة (غير الخاصة بالفضاء السيبراني) في أغلب الأحيان. غير أنه أُبلغ عن الأخذ بالنهجين فيما يخص الأفعال المرتكبة بواسطة الحواسيب والتي تشتمل على انتهاك السرية أو الاحتيال أو التزوير أو ارتكاب جرائم ذات صلة بالهوية.

٣٠- وعلى حين يوجد توافق رفيع المستوى في الآراء بشأن مجالات التجريم الواسعة، فإنَّ التحليل المفصّل للأحكام الواردة في التشريعات المرجعية يكشف عن نهوج متباينة. ذلك أنَّ الجرائم التي تنطوي على نفاذ غير مشروع إلى النظم الحاسوبية والبيانات تختلف باختلاف موضوع الجريمة (بيانات أو نظم أو معلومات) ومستوى التجريم، أي تجريم النفاذ بحد ذاته "فحسب" أو اقتضاء وجود نية أخرى كامنة في النفاذ، ومن ذلك مثلا التسبُّب بخسائر أو أضرار. وتختلف النية اللازم وجودها ليكون الفعل المرتكب جُرماً باختلاف النهوج المتّبعة في تجريم التدخُّل في النظم الحاسوبية أو البيانات الحاسوبية. فإنَّ معظم البلدان تقتضي أن يكون التدخُّل في النظم أو البيانات متعمَّداً ليعتبر جريمة، في حين تجرِّم بلدان أخرى التدخُّل دونما اكتراث فيها. أما فيما يتعلق بالتدخُّل في البيانات الحاسوبية، فيتراوح السلوك الذي يشكّل

(7) النفاذ غير المشروع إلى نظام حاسوبي؛ والنفاذ غير المشروع إلى بيانات الحواسيب أو اعتراض هذه البيانات أو احتيازها؛ والتدخل غير المشروع في البيانات أو النظم؛ وإنتاج أو توزيع أو حيازة أدوات لإساءة استعمال الحواسيب؛ وانتهاك تدابير حماية الخصوصية أو البيانات؛ والاحتيال أو التزوير بواسطة الحواسيب؛ وجرائم الهوية المرتكبة بواسطة الحواسيب؛ وجرائم حقوق المؤلف والعلامات التجارية المرتكبة بواسطة الحواسيب؛ والأعمال المرتكبة بواسطة الحواسيب والتي تتسبّب بضرر شخصي؛ والأعمال المرتكبة بواسطة الحواسيب والتي تنطوي على عنصرية أو كراهية للأجانب؛ وإنتاج أو توزيع أو حيازة المواد الإباحية المتعلقة بالأطفال بواسطة الحواسيب؛ وإغواء أو "مراودة" الأطفال بواسطة الحواسيب؛ وأعمال دعم الجرائم الإرهابية بواسطة الحواسيب.

تدخلاً فيها بين إتلاف البيانات أو حذفها وصولاً إلى تحويرها أو كبتها أو إدخالها أو نقلها. ويختلف تجريم التدخُّل غير المشروع تبعاً لما إذا كان الجُرم محصوراً بنقل البيانات غير العمومية، أو ما إذا كان الجُرم محصوراً بالتدخُّل "بواسطة الوسائل التقنية". ولا تجرِّم جميع البلدان أدوات إساءة استعمال الحواسيب. أمَّا في البلدان التي تجرِّمها، فتبرز الاختلافات تبعاً لما إذا كان الجُرم يشمل حيازةَ أو توزيع أو استعمال البرامجيات (كالبرامجيات الخبيثة) و/أو رموز النفاذ إلى الحواسيب (أي كلمات سر الضحية مثلا). ومن منظور التعاون الدولي، قد يكون لهذه الاختلافات تأثير على الاستنتاجات المتعلقة بازدواجية التجريم بين البلدان.

٣١- وقد أقرّت عدّة بلدان أحكاماً بشأن الجرائم الخاصة بالفضاء السيبراني فيما يتعلق بجرائم الاحتيال والتزوير والجرائم المتصلة بالهوية المرتكبة بواسطة الحاسوب، في حين قامت بلدان أخرى بتوسيع نطاق الأحكام العامة المتعلقة بالاحتيال أو السرقة، أو اعتمدت على أحكام الجرائم التي تشمل العناصر المكوّنة لها — كالنفاذ غير المشروع والتدخُّل في البيانات والتزوير، في حالة الجرائم ذات الصلة بالهوية. وجُرِّم على نطاق واسع عدد من الجرائم ذات الصلة بالمحتوى، وخصوصا الجرائم المتعلقة باستغلال الأطفال في المواد الإباحية. غير أنَّ الاختلافات تبرز بشأن تعريف مصطلح "الطفل"، والقيود المتعلقة بالمواد "البصرية" أو استبعاد المواد المصمَّمة بالمحاكاة، والأفعال المشمولة بها. وعلى الرغم من أنَّ الغالبية العظمى من البلدان تشمل في التجريم، على سبيل المثال، إنتاج وتوزيع المواد الإباحية المتعلقة باستغلال الأطفال، يظهر تباين أكبر في تجريم حيازة هذه المواد والوصول إلى مواقعها الشبكية. أما فيما يتعلق بانتهاك حقوق المؤلف والعلامات التجارية بواسطة الحواسيب، أبلغ أكثر البلدان عن تطبيق الجرائم الجنائية العامة على الأفعال المرتكبة عمداً وعلى نطاق تجاري.

٣٢- ودفع تزايد استعمال وسائل التواصل الاجتماعي ومحتوى الإنترنت الذي ينتجه المستعمِلون الحكومات إلى اتخاذ تدابير تنظيمية رقابية للتصدي لذلك، بما في ذلك اللجوءُ إلى القانون الجنائي، والدعوة إلى احترام الحق في حرية التعبير. وأبلغت البلدان المجيبة عن الاستبيان عن قيود مختلفة على التعبير، ومن ذلك القيود المفروضة على التشهير (تشويه السمعة) والتحقير والتهديد والتحريض على الكراهية وإهانة المشاعر الدينية والمواد الفاحشة والنيل من هيبة الدولة. ولا يتبدّى العنصر الاجتماعي الثقافي لبعض القيود في القانون الوطني فحسبُ، بل في الصكوك المتعددة الأطراف أيضاً. فبعض الصكوك الإقليمية المتعلقة بالجريمة السيبرانية تشمل على سبيل المثال جرائم واسعة النطاق بشأن انتهاك الآداب العامة وتداول المواد الإباحية وازدراء المبادئ أو القيم الدينية أو الأُسريّة.

٣٣- وفي هذا الصدد يؤدي القانون الدولي لحقوق الإنسان مفعوله كسيف ودرع معاً، إذ إنه يقتضي تجريم أشكالٍ تعبيرٍ متطرّفة (محدودة)، ويحمي في الوقت نفسه أشكالَ تعبيرٍ أخرى. ومن ثم يتعيّن على الدولِ التي هي أطراف في الصكوك الدولية لحقوق الإنسان ذاتِ الصلة بالموضوع فرض بعض المحظورات على حرية التعبير، بما في ذلك التحريض على الإبادة الجماعية والكراهية التي تشكّل تحريضاً على التمييز الجائر أو العداء أو العنف، والتحريض على الإرهاب وبث الدعاية للحرب. ومن جهة أخرى، ثمة "هامش تقدير" يتيح لغيرها من البلدان المجال لتعيين حدود للتعبير المقبول بما يتماشى مع ثقافاتها وتقاليدها القانونية. ومع ذلك، فإنَّ من شأن القانون الدولي لحقوق الإنسان أن يتدخّل عند نقطة معينة. فعلى سبيل المثال، إن تطبيق القوانين الجنائية المتعلقة بالتشهير وعدم احترام السلطة والإهانة على التعبير على الإنترنت، سيواجه صعوبات عالية الدرجة لإثبات تناسب التدابير وملاءمتها واتِّسامها بأقل قدر من التدخُّل. وعندما يكون المحتوى غير قانوني في بلد ما، ولكن يكون إنتاجه ونشره قانونياً في بلد آخر، سيتعيّن على الدول أن تركّز في تدابير العدالة الجنائية على الأشخاص الذين ينفذون إلى مواقع المحتوى الذي يعدّ غير قانوني ضمن ولايتها القضائية الوطنية، بدلاً من التركيز على المحتوى المنتَج خارج البلد.

٥- إنفاذ القانون والتحقيقات

٣٤- أبلغ أكثر من ٩٠ في المائة من البلدان المجيبة عن الاستبيان بأنَّ أفعال الجريمة السيبرانية تصل إلى علم السلطات المسؤولة عن إنفاذ القانون في أكثر الأحيان من خلال التبليغات المقدّمة من الضحايا الأفراد أو الضحايا من الشركات. وقدَّرت البلدان المجيبة عن الاستبيان أنَّ نسبة التأذّي الفعلي من الجرائم السيبرانية المبلّغ عنها إلى الشرطة تبدأ صعوداً من واحد في المائة. وتشير دراسة استقصائية عالمية للقطاع الخاص إلى أنَّ ٨٠ في المائة من الضحايا الأفراد للجرائم السيبرانية الأساسية لا يبلِّغون الشرطة عن الجريمة. ويُعزى تدني الإبلاغ عن هذه الجرائم إلى عدم الوعي بالإيذاء وآليات الإبلاغ، وإلى شعور الضحايا بالخجل والحرج، وإلى تخوُّف الشركات من المخاطر المتصوَّرة التي قد تهدد سمعتها. وأبرزت السلطات في جميع مناطق العالم المبادرات الرامية إلى تعزيز الإبلاغ عن تلك الجرائم، بما في ذلك عن طريق نظم الإبلاغ بالاتصال الحاسوبي المباشر وبالخطوط الهاتفية المباشرة وحملات التوعية العمومية والتواصل مع القطاع الخاص وتعزيز مدى التواصل وتبادل المعلومات مع الشرطة. غير أنَّ تدابير التصدِّي للجريمة السيبرانية التي تتخذ لمواجهة حوادث معينة يجب أن تقترن بتحقيقات تكتيكية على المدى المتوسط والبعيد، تركّز على أسواق الجريمة ومدبري

المخططات الإجرامية. وتنخرط سلطات إنفاذ القانون في البلدان المتقدمة النمو في هذا المجال، بما في ذلك من خلال الوحدات السرية التي تستهدف المخالفين على مواقع الشبكات الاجتماعية وغرف الدردشة والرسائل الفورية ومواقع تبادل الملفات بين النظراء (P2P). وتنشأ التحديات التي ينطوي عليها التحقيق في الجرائم السيبرانية عن الابتكارات الإجرامية التي يقوم بها الجُناة والصعوبات في الحصول على الأدلة الإلكترونية والقيود على الموارد الداخلية والقدرات والإمدادات اللوجستية. وغالباً ما يلجأ المشتبه بهم إلى تقنيات إخفاء الهوية والتشويش، وتصل التقنيات الجديدة بسرعة إلى أوساط واسعة من المجرمين من خلال أسواق الجرائم عبر الإنترنت.

٣٥- وتتطلّب التحقيقات التي تجريها سلطات إنفاذ القانون في الجرائم السيبرانية مزيجاً من تقنيات عمل الشرطة التقليدية منها والجديدة. وعلى حين يمكن تنفيذ بعض إجراءات التحقيق بواسطة الصلاحيات التقليدية، فإنه يصعب تكييف العديد من القواعد الإجرائية التي تستند إلى نهج يقوم في توجّهه على الحيّز المكاني للأشياء لجعلها تستند إلى نهج يشمل تخزين البيانات الإلكترونية وتدفّق البيانات في الوقت الحقيقي. وأشار الاستبيان الخاص بالدراسة إلى عشرة إجراءات للتحقيق في الجرائم السيبرانية، بدءاً من البحث العام والمصادرة وصولاً إلى الصلاحيات المتخصصة، كحفظ البيانات الحاسوبية.[٨] وأبلغت البلدان في أكثر الأحيان عن وجود صلاحيات عامة (غير خاصة بالفضاء السيبراني) في كل مستويات التحريات؛ كما أبلغ عدد من البلدان أيضاً عن تشريعات خاصة بالفضاء السيبراني، ولا سيما لضمان التعجيل في حفظ البيانات الحاسوبية والحصول على بيانات المشتركين المخزنة. وأبلغت بلدان عديدة عن عدم وجود صلاحيات قانونية لاتخاذ تدابير متقدّمة، مثل التحاليل الجنائية الحاسوبية عن بُعد. وفي حين أنه يمكن توسيع نطاق الصلاحيات الإجرائية التقليدية لتشمل الأوضاع الخاصة بالفضاء السيبراني، فقد يؤدي اتّباع نهج من هذا النحو في العديد من الحالات إلى أوجه عدم يقين قانوني وتحديات بشأن مشروعية جمع الأدلة، وبالتالي مقبوليتها. وعموماً، ثمة قواسم مشتركة أساسية في النهوج الوطنية المتّبعة في صلاحيات التحقيق في الجرائم السيبرانية أقل من القواسم المشتركة الأساسية في تجريم العديد من الجرائم السيبرانية.

(8) البحث عن المعدات أو البيانات الحاسوبية ومصادرتها؛ والأمر بالحصول على معلومات عن المشتركين؛ والأمر بالحصول على بيانات حركة الاتصالات المخزّنة؛ والأمر بالحصول على بيانات المحتوى المخزّنة؛ وجمع بيانات حركة الاتصالات في الوقت الحقيقي؛ وجمع بيانات المحتوى في الوقت الحقيقي؛ والتعجيل في حفظ البيانات الحاسوبية؛ واستخدام أدوات التحاليل الجنائية الحاسوبية عن بُعد؛ والنفاذ عبر الحدود إلى نظم أو بيانات حاسوبية.

٣٦- وبصرف النظر عن الشكل القانوني لصلاحيات التحقيق، تستخدم جميع السلطات المجيبة عن الاستبيان أساليب البحث والمصادرة للاستحواذ الفعلي على المعدات الحاسوبية والحصول على البيانات الحاسوبية. وتستخدم غالبية البلدان أيضاً أوامر قضائية للحصول على البيانات الحاسوبية المخزنة من مقدّمي خدمات الإنترنت. ومن ناحية ثانية، خارج أوروبا، أبلغ حوالي ثلث عدد البلدان عن تحديات في إلزام الأطراف الثالثة التي لها علاقة بالتحقيق بتقديم المعلومات. ويستخدم حوالي ثلاثة أرباع عدد البلدان إجراءات تحقيق متخصصة، كجمع البيانات في الوقت الحقيقي أو التعجيل في حفظها. ويتطلب استخدام إجراءات التحقيق عادةً حدًّا أدنى من الأدلة الأولية أو تقريراً يبلّغ عن وقوع جريمة سيبرانية. أمَّا الإجراءات التي هي أكثر تدخلاً، كتلك التي تشتمل على جمع البيانات في الوقت الحقيقي أو النفاذ إلى محتوى البيانات، فتستلزم مستويات معيارية أكثر صرامة، كوجود دليل على ارتكاب جريمة خطيرة أو دليل على وجود سبب محتمل أو أسس معقولة على ذلك.

٣٧- ويُعدّ التفاعل بين سلطات إنفاذ القانون ومقدّمي خدمات الإنترنت علاقة معقّدة بصفة خاصة. ذلك أنَّ لدى مقدّمي الخدمات المعلومات الخاصة بالمشتركين والفواتير وبعض سجلات الاتصال ومعلومات عن المواقع (كبيانات أبراج الاتصالات اللاسلكية الخاصة بمقدّمي خدمات الهواتف الجوالة) ومحتوى الاتصالات؛ وقد تمثّل كل هذه العناصر أدلّة إلكترونية مهمة عن جريمة معيّنة. وتختلف الالتزامات القانونية الوطنية والسياسات العامة المتّبعة في القطاع الخاص بشأن الاحتفاظ بالبيانات وإفشائها اختلافاً كبيراً حسب البلد وأوساط الصناعة ونوع البيانات. وقد أبلغت البلدان في معظم الأحيان عن اللجوء إلى أوامر قضائية للحصول على أدلة من مقدّمي الخدمات. ولكن سلطات إنفاذ القانون قد تتمكّن في بعض الحالات من الحصول مباشرةً على بيانات المشتركين المخزّنة وبيانات حركة الاتصالات وحتى بيانات المحتوى. وفي هذا الصدد، أبلغ كثير من مؤسسات القطاع الخاص عن عدم الاقتصار على الأخذ بسياسة عامة أولية تقتضي مراعاة الأصول القانونية للإفشاء عن البيانات، بل الأخذ أيضاً بنهج طوعي يتمثل في الاستجابة في بعض الظروف للطلبات المباشرة التي تقدمها سلطات إنفاذ القانون. كما إنَّ العلاقات غير الرسمية بين سلطات إنفاذ القانون ومقدّمي الخدمات، والتي أُبلغ عن وجودها في أكثر من نصف مجموع عدد البلدان المجيبة عن الاستبيان، تساعد في عملية تبادل المعلومات وبناء الثقة. وأشارت الردود إلى أنَّ هناك حاجة إلى تحقيق التوازن بين الحفاظ على الخصوصية ومراعاة الأصول القانونية من جهة، وبين إفشاء الأدلة في الوقت المناسب من جهة أخرى لضمان عدم تحوُّل القطاع الخاص إلى "معرقل" للتحقيقات.

٣٨- وتنطوي التحقيقات في الجرائم السيبرانية دائماً على اعتبارات تتعلق بالخصوصية بموجب القانون الدولي لحقوق الإنسان. وتنصّ معايير حقوق الإنسان على أنَّ القوانين يجب أن تكون واضحة بما فيه الكفاية لتعطي دلالة كافية عن الظروف التي تخوِّل للسلطات استخدام إجراءات التحقيق، وأنَّه يجب أن تكون هناك ضمانات وافية وفعالة لمكافحة إساءة استخدام تلك الإجراءات. وأفادت بلدان بأنَّ قوانينها الوطنية تحمي حقوق الخصوصية، كما أبلغت عن مجموعة من القيود والضمانات في إطار التحقيقات. ولكن عندما تكون التحقيقات عبر الحدود الوطنية، يستتبع تباين مستويات حماية الخصوصية عدم القدرة على التنبؤ بقدرات سلطات إنفاذ القانون الأجنبية على الحصول على البيانات، وبالثغرات التي قد تنطوي عليها نظم حماية الخصوصية في الولاية القضائية المعنية.

٣٩- وقد بدأ أكثر من ٩٠ في المائة من البلدان التي أجابت عن الاستبيان بإنشاء بُنى تنظيمية متخصصة للتحقيق في الجرائم السيبرانية والجرائم التي تنطوي على أدلّة إلكترونية. لكن هذه البُنى التنظيمية تفتقر في البلدان النامية إلى ما يكفي من الموارد والقدرات. ولدى البلدان الأقل نمواً عدد أقل بكثير من أفراد الشرطة المتخصصين، أيْ بمعدل يبلغ نحو ٠,٢ لكل ١٠٠ ٠٠٠ مستعمِل من مستعملي الإنترنت ضمن البلد المعني، في حين يكون هذا المعدّل أعلى بضعفين إلى خمسة أضعاف في البلدان التي تفوقها تقدماً. وأُبلغ بأنَّ سبعين في المائة من الموظفين المتخصصين المكلفين بإنفاذ القوانين في البلدان الأقل نمواً يفتقرون إلى المهارات والمعدات الحاسوبية، ولا يتلقى إلا نصفهم تدريباً أكثر من مرة واحدة في السنة. كما أبلغ أكثرُ من نصف عدد البلدان المجيبة عن الاستبيان في أفريقيا وثلث عدد البلدان في القارة الأمريكية بأنَّ الموارد المتاحة لسلطات إنفاذ القانون للتحقيق في الجرائم السيبرانية غير كافية. وعلى الصعيد العالمي، يُرجّح أن تكون الصورة أسوأ من ذلك. فلم يرد على الاستبيان على سبيل المثال إلا ٢٠ في المائة من البلدان الخمسين الأقل نمواً في العالم. وأبلغ جميع البلدان المجيبة عن الاستبيان في أفريقيا وأكثر من ٨٠ في المائة من البلدان المجيبة في القارة الأمريكية وآسيا وأوقيانوسيا بأنها بحاجة إلى مساعدة تقنية. وكان أكثر المجالات ذكراً باعتباره يستلزم مساعدة تقنية هو أساليب التحقيق العامة المتعلقة بالجرائم السيبرانية. وقد أشار ٦٠ في المائة من البلدان التي تحتاج إلى المساعدة إلى أنَّ وكالات إنفاذ القانون فيها بحاجة إلى هذا النوع من المساعدة.

٦- الأدلة الإلكترونية وتدابير التصدِّي في مجال العدالة الجنائية

٤٠- إنَّ الأدلة هي الوسيلة إلى إثبات الوقائع ذات الصلة بذنب أو براءة الفرد الذي يمثُل للمحاكمة. والأدلة الإلكترونية هي كل المواد الإثباتية التي توجد في شكل إلكتروني أو رقمي؛

ويمكن أن تكون مخزّنة أو عابرة؛ كما يمكن أن توجد في شكل ملفات حاسوبية أو مواد مرسلة أو سجلات أو بيانات وصفية أو بيانات شبكية. وتهتم التحاليل الجنائية الرقمية باستعادة المعلومات، التي كثيراً ما تتسم بسرعة زوالها وسهولة إصابتها بالتلف والفيروسات، ولكنها قد تكون قيّمة لأغراض الأدلة. وتتضمن تقنيات التحاليل الجنائية إنشاء نسخ "مطابقة تماماً" من المعلومات المخزنة والمحذوفة، واستخدام برامج "منع الكتابة" من أجل ضمان عدم تحريف المعلومات الأصلية، واستخدام خوارزميات "تجزئة" للملفات المشفّرة، أو استخدام التوقيعات الرقمية، بغية إظهار أي تعديلات تدخل على المعلومات. وأبلغ معظم البلدان تقريباً بأنَّ لديها بعض القدرات في مجال التحاليل الجنائية الرقمية. غير أنَّ العديد من البلدان المجيبة عن الاستبيان، من جميع المناطق، أشار إلى عدم كفاية عدد المحقّقين المتخصصين في التحاليل الجنائية وإلى تباين القدرات على الصعيد الاتحادي وصعيد الولايات، وإلى الافتقار إلى أدوات التحليل الجنائي، وتراكم الأعمال غير المنجزة بسبب الكميات الهائلة من البيانات اللازم تحليلها. وأبلغ نصف عدد البلدان بأنَّ المشتبه بهم يلجأون إلى التشفير، مما يجعل الحصول على هذا النوع من الأدلة بدون رمز التشفير صعباً ويستغرق وقتاً طويلاً. وفي معظم البلدان، تقع مهمة تحليل الأدلة الإلكترونية على عاتق سلطات إنفاذ القانون. غير أنه يتعيّن على المدّعين العامين معاينة وفهم الأدلة الإلكترونية من أجل إقامة الحجة عند المحاكمة. وقد أبلغت البلدان كلها في أفريقيا وثلث عدد البلدان في مناطق أخرى بعدم كفاية الموارد المتاحة للمدّعين العامين للقيام بذلك. وعادة ما تكون المهارات الحاسوبية لدى المدّعين العامين أقل مستوى من المهارات الحاسوبية لدى المحقّقين. وعلى الصعيد العالمي، أبلغ نحو ٦٥ في المائة من البلدان المجيبة عن الاستبيان بوجود نوع من التخصص في الجرائم السيبرانية لدى المدّعين العامين. ولم يبلِّغ سوى ١٠ في المائة من البلدان عن وجود دوائر قضائية متخصصة. ويتولّى النظر في الأغلبية العظمى من قضايا الجرائم السيبرانية قضاة غير متخصصين، ممن لا يتلقون في ٤٠ في المائة من البلدان المجيبة عن الاستبيان أيّ نوع من التدريب المتصل بالجرائم السيبرانية. ومن ثم، يعدُّ تدريب القضاة في مجال قانون الجرائم السيبرانية وجمع الأدلة واكتساب المهارات الحاسوبية الأساسية والمتقدمة جانباً ذا أولوية خاصة.

٤١- ولا يعمد أكثر من ٦٠ في المائة من البلدان المجيبة عن الاستبيان إلى التمييز قانونياً بين الأدلة الإلكترونية والأدلة المادية. وعلى حين تتباين النهوج المتّبعة، فإنَّ بلداناً عديدة تعتبر هذه الممارسة جيدة، لأنها تضمن مقبولية الأدلة الإلكترونية بالتساوي مع جميع الأنواع الأخرى من الأدلة. ولا يعترف عدد من البلدان خارج أوروبا بالأدلة الإلكترونية على الإطلاق، مما يجعل الملاحقة القضائية لمرتكبي الجرائم السيبرانية وسائر الجرائم المثبتة بأدلةٍ من المعلومات الإلكترونية غير مجدية. وليس لدى بعض البلدان عموماً قواعد إثبات منفصلة

خاصة بالأدلة الإلكترونية، لكن عدداً من البلدان أشار إلى مبادئ ومنها مثلاً الخاصة بأفضل دليل وبمدى وجاهة الأدلة وبعدم قبول الرواية عن الغير وبموثوقية الأدلة وسلامتها؛ وهي كلها مبادئ قد تنطبق بشكل خاص على الأدلة الإلكترونية. وسلّطت بلدان عديدة الضوء على التحديات التي تُواجَه في إسناد الأفعال المرتكبة إلى الشخص المعين، وعلّقت بأنَّ ذلك غالباً ما يتوقّف على الأدلة الظرفية.

٤٢- وتدل التحدِّيات التي تواجه المحققين في أجهزة إنفاذ القانون والمدّعين العامين على أنَّ معدّلات "الإحضار أمام العدالة" أدنى بالنسبة لمرتكبي الجرائم السيبرانية من غيرهم من الجناة. ولوحظ أنَّ عدد المشتبه بارتكابهم جرائم مسجّلة لدى الشرطة في قضايا المواد الإباحية المتعلقة باستغلال الأطفال قابل للمقارنة بعدد المشتبه بارتكابهم جرائم جنسية أخرى. ولكنَّ عدد المشتبه بارتكابهم جرائم مسجّلة لدى الشرطة متعلقة بالنفاذ غير المشروع والاحتيال أو التزوير بواسطة الحواسيب لا يتجاوز ٢٥ لكل ١٠٠ جريمة. ولم يتمكّن إلا عدد قليل جداً من البلدان من توفير البيانات بشأن الأشخاص الذين تمت مقاضاتهم أو إدانتهم. لكن إحصاءات الجرائم السيبرانية في بلد واحد أظهرت أنَّ نسبة الأشخاص الذين أُدينوا بارتكاب الجرائم السيبرانية المسجّلة أقل بكثير من نسبة الأشخاص المدانين بارتكاب سائر الجرائم التقليدية.

٧- التعاون الدولي

٤٣- أبلغت البلدان التي أجابت عن الاستبيان بأنَّ ٣٠ إلى ٧٠ في المائة من الجرائم السيبرانية تشتمل على بُعد عابر للحدود الوطنية، وتنطوي من ثم على مسائل متعلقة بالتحقيقات عبر الحدود الوطنية والسيادة والولاية القضائية والأدلة الواقعة خارج نطاق الولاية القضائية ومتطلبات التعاون الدولي. وينشأ البُعد العابر للحدود الوطنية الذي تتّسم به الجريمة السيبرانية عندما يكون للجريمة المعنية عنصر جوهري أو أثر خطير الشأن في إقليم آخر، أو عندما يكون أحد جوانب تنفيذ الجريمة قد تم في إقليم آخر. وينصّ القانون الدولي على عدد من الأسس المتعلقة بالولاية القضائية بشأن الأفعال المعنية، بما في ذلك أشكال الولايات القضائية المستندة إلى الإقليم والمستندة إلى الجنسية. وتوجد بعض هذه الأسس أيضاً في الصكوك المتعددة الأطراف المتعلقة بالجرائم السيبرانية. وفي حين ترى كل البلدان الأوروبية أنَّ قوانينها الوطنية توفّر إطاراً كافياً لتجريم الأفعال التي تندرج في عداد الجرائم السيبرانية والمرتكبة خارج نطاق الولاية القضائية وكذلك لملاحقة مرتكبيها قضائياً، فقد أبلغ نحو ثلث إلى أكثر من نصف عدد البلدان في مناطق أخرى من العالم عن عدم كفاية الأطر القائمة في هذا المجال. وفي بلدان عديدة، تجسّد الأحكام الفكرة القائلة بأنَّه ليس من

الضروري أن تقع "كل عناصر" الجريمة داخل البلد من أجل تأكيد ولايته القضائية الإقليمية. ويمكن تحديد الروابط الإقليمية بالإشارة إلى عناصر الفعل المعني أو آثاره، أو موقع النظم أو البيانات الحاسوبية المستخدمة في ارتكابه. وتجري عادةً تسوية تنازع الولايات القضائية من خلال المشاورات الرسمية وغير الرسمية بين البلدان. ولا تكشف إجابات البلدان حالياً عن أيّ حاجة إلى أشكال إضافية من الولاية القضائية تُفرض على بُعدٍ مفترض يخصّ "الفضاء السيبراني"؛ فغالباً ما تكون أشكال الولاية القضائية المستندة إلى الإقليم والمستندة إلى الجنسية قادرة دائماً على ربط الجريمة السيبرانية المرتكبة ربطاً كافياً بدولة واحدة على الأقل.

٤٤- أما أشكال التعاون الدولي فتشمل تسليم المطلوبين وتبادل المساعدة القانونية والاعتراف المتبادل بالأحكام الأجنبية والتعاون غير الرسمي بين أجهزة الشرطة. ونظراً لطبيعة الأدلة الإلكترونية التي تتسم بسهولة زوالها وتغيّرها، يتطلّب التعاون الدولي في المسائل الجنائية المتعلقة بالجرائم السيبرانية اتخاذ تدابير التصدِّي في الوقت المناسب والتمكُّن من طلب تنفيذ إجراءات تحقيق متخصصة، ومنها مثلاً حفظ البيانات الحاسوبية. ويُعدُّ استخدام الأشكال التقليدية من التعاون الأسلوب السائد في الحصول على الأدلة من خارج نطاق الولاية الإقليمية في قضايا الجرائم السيبرانية، حيث أبلغ أكثر من ٧٠ في المائة من البلدان عن استخدام طلبات المساعدة القانونية المتبادلة الرسمية لهذا الغرض. وفي إطار هذا النوع من التعاون الرسمي، يستند استخدام حوالي ٦٠ في المائة من الطلبات إلى الصكوك الثنائية باعتبارها الأساس القانوني للتعاون. وتُستخدم الصكوك المتعددة الأطراف في ٢٠ في المائة من الحالات. وأُفيد بأنَّ أوقات الاستجابة للطلبات المعنية تستغرق أشهراً، لكل من طلبات تسليم المطلوبين والمساعدة القانونية المتبادلة؛ وهي فترة زمنية تطرح تحدِّيات على صعيد جمع الأدلة الإلكترونية السريعة الزوال والتغيُّر. وأفاد ٦٠ في المائة من البلدان في أفريقيا والقارة الأمريكية وأوروبا و٢٠ في المائة من البلدان في آسيا وأوقيانوسيا عن وجود قنوات للطلبات العاجلة؛ غير أنَّ تأثير القنوات على زمن الاستجابة غير واضح. وأبلغ ثلثا البلدان المجيبة تقريباً بأنَّ أساليب التعاون غير الرسمي ممكنة، لكن عدداً قليلاً من البلدان كان لديه سياسة عامة لاستخدام مثل هذه الآليات. وتوفِّر المبادرات المتعلقة بالتعاون غير الرسمي وبتسهيله، كالشبكات العاملة ٢٤ ساعة طيلة الأسبوع، إمكانيات مهمة لتسريع وقت الاستجابة؛ لكنها غير مستخدمة بقدرٍ كافٍ، إذ اقتصر استخدامها على نحو ثلاثة في المائة من العدد الإجمالي لقضايا الجرائم السيبرانية التي تناولتها سلطات إنفاذ القانون في مجموعة البلدان المبلِّغة.

٤٥- وقد صُمِّمت أساليب التعاون الرسمية وغير الرسمية لإدارة عملية موافقة الدولة على إجراء سلطات إنفاذ القانون الأجنبية تحقيقات تمسّ بسيادتها. غير أنَّ المحقّقين باتوا يطلعون

باطّراد، عن علم أو عن غير علم، على بيانات تندرج خارج إطار الولاية القضائية لبلدهم خلال عملية جمع الأدلة، دون الحصول على موافقة الدولة التي تقع فيها البيانات فعلياً. وتحدث هذه الحالة خصوصاً نتيجة لتقنيات الحوسبة السحابية التي تنطوي على تخزين البيانات في مراكز بيانات متعددة في مواقع جغرافية مختلفة. فإنَّ "موضِع" البيانات، وإن أمكنت معرفته من الناحية التقنية، أصبح اصطناعياً أكثر فأكثر، حتى أنه كثيراً ما توجّه طلبات المساعدة القانونية المتبادلة التقليدية إلى البلد الذي يوجد فيه مقدّم الخدمات، بدلاً من البلد الذي يقع فيه مركز البيانات فعلياً. وقد تحصل سلطات إنفاذ القانون الأجنبية مباشرةً على البيانات التي تتجاوز حدود ولايتها الإقليمية عندما يستفيد المحققون من وجود رابط مباشر قائم انطلاقاً من جهاز المشتبه به، أو عندما يستخدم المحقّقون وثائق تفويض قانونية بشأن الحصول على البيانات. كذلك قد يحصل المحققون المكلّفون بإنفاذ القوانين، في بعض الأحيان، على البيانات من مقدِّمي الخدمات خارج الولاية الإقليمية وذلك من خلال تقديم طلب مباشر غير رسمي؛ مع أنَّ مقدّمي الخدمات يطلبون عادةً مراعاة الأصول القانونية. ولكن هذه الحالات غير مشمولة على النحو المناسب في الأحكام القائمة بالنفاذ إلى البيانات "عبر الحدود"، المنصوص عليها في اتفاقية المجلس الأوروبي المتعلقة بالجريمة السيبرانية والاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وذلك بسبب التركيز على "موافقة" الشخص الذي يتمتع بالسلطة القانونية لإفشاء البيانات، والمعرفة المفترضة لموقع البيانات وقت النفاذ إليها أو استلامها.

٤٦- وقد يفضي هذا الوضع على صعيد التعاون الدولي إلى ظهور مجموعات من البلدان لديها الصلاحيات والإجراءات اللازمة لتتعاون فيما بينها، ولكن مع بقاء هذه الصلاحيات والإجراءات محصورة، بالنسبة لجميع البلدان الأخرى، بالوسائل "التقليدية" للتعاون الدولي التي لا تأخذ في الاعتبار خصوصيات الأدلة الإلكترونية والطابع العالمي للجرائم السيبرانية. وهذا هو الحال خصوصاً فيما يتعلق بالتعاون في إجراءات التحقيق. ويعني عدم وجود نهج مشترك، بما في ذلك في إطار الصكوك الحالية المتعددة الأطراف بشأن الجرائم السيبرانية، أنَّ طلبات اتخاذ إجراءات، مثل الحفظ العاجل للبيانات خارج البلدان الملزَمة دولياً بضمان مثل هذه الخدمة وتوفيرها عند الطلب، قد لا تُنفّذ بسهولة. ومن شأن إدراج هذه الصلاحية في مشروع اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني أن يحقّق بعض التقدُّم في سدّ هذه الثغرة. أمَّا على الصعيد العالمي، فإنَّ التباين في نطاق الأحكام المتعلقة بالتعاون في الصكوك المتعددة الأطراف والثنائية، وعدم فرض أجل ملزم للاستجابة للطلبات، وعدم الاتفاق على إتاحة سُبل النفاذ المباشر إلى البيانات التي توجد خارج الولاية القضائية، وتعدُّد شبكات

سلطات إنفاذ القانون غير الرسمية، والتباين في ضمانات التعاون، أمور تمثل تحديات كبيرة في وجه التعاون الدولي الفعَّال فيما يتعلق بالأدلة الإلكترونية في المسائل الجنائية.

٨- منع الجرائم السيبرانية

٤٧- ينطوي منع الجريمة على استراتيجيات وتدابير تسعى إلى التقليل من احتمالات حدوث جرائم والتخفيف من آثارها الضارة التي قد تلحق بالأفراد والمجتمع. وقد أبلغ زهاء ٤٠ في المائة من البلدان المجيبة عن الاستبيان عن وجود قانون وطني أو سياسة عامة وطنية لديها بشأن منع الجرائم السيبرانية. وهناك حالياً مبادرات قيد الإعداد في بلدان أخرى تبلغ نسبتها ٢٠ في المائة. وأبرزت البلدان أنَّ الممارسات الجيدة في مجال منع الجرائم السيبرانية تتضمن إصدار التشريعات، والقيادة الفعّالة، وتنمية القدرات في مجال العدالة الجنائية وإنفاذ القانون والتعليم والتوعية، وإنشاء قاعدة معرفية قوية، والتعاون بين الحكومة والمجتمعات المحلية والقطاع الخاص وكذلك على الصعيد الدولي. وأبلغ أكثر من نصف عدد البلدان عن وجود استراتيجيات بشأن الجرائم السيبرانية. وفي حالات عديدة، أُدرجت الاستراتيجيات الخاصة بالجرائم السيبرانية بشكل وثيق ضمن استراتيجيات للأمن السيبراني. وتضمَّن حوالي ٧٠ في المائة من جميع الاستراتيجيات الوطنية المبلّغ عنها مكوّنات بشأن زيادة الوعي والتعاون الدولي والقدرات في مجال إنفاذ القانون. ولأغراض التنسيق، يُبلَّغ في أغلب الأحيان عن وكالات إنفاذ القانون والملاحقة القضائية باعتبارها هي المؤسسات الرائدة المعنية بالجرائم السيبرانية.

٤٨- وتظهر عملياً الدراسات الاستقصائية، بما في ذلك في البلدان النامية، أنَّ معظم الأفراد من مستعمِلي الإنترنت يتخذون حالياً الاحتياطات الأمنية الأساسية. وقد أبرزت الحكومات وهيئات القطاع الخاص والمؤسسات الأكاديمية المجيبة عن الاستبيان أهمية استمرار حملات زيادة الوعي العام، بما في ذلك حملات التوعية بالتهديدات الناشئة، والحملات التي تستهدف جمهوراً محدداً، كالأطفال. ويكون تثقيف المستعمِلين أكثر فعاليةً عندما يقترن بوجود نظم تساعدهم على تحقيق أهدافهم بطريقة آمنة. فإذا كانت التكلفة التي يتكبّدها المستعمِل أعلى من المنفعة المباشرة التي يحصل عليها، فإنَّ ذلك لن يوفّر حافزاً كبيراً للأفراد على اتّباع الإجراءات الأمنية. وأفادت كيانات القطاع الخاص أيضاً بأنه يجب دمج توعية المستعمِلين والموظفين في نهج كُلّي بشأن الأمن. وتتضمن المبادئ الأساسية والممارسة الجيدة المُشار إليها المساءلة عن العمل في مجال التوعية وعن السياسات العامة والممارسات المتّبعة في إدارة المخاطر والقيادة على مستوى مجالس الإدارة وتدريب الموظفين. وقد أجرى ثلثا عدد المجيبين من القطاع الخاص تقييماً لمخاطر الجرائم السيبرانية، وأبلغ معظمهم عن استعمال

تقنيات من تكنولوجيا الأمن السيبراني كالجدران النارية الواقية وحفظ الأدلة الرقمية واستبانة ماهية المحتوى وكشف التسلل والإشراف على النظم ومراقبتها. ولكن أُعرب عن دواعي قلق لأنَّ الشركات الصغيرة والمتوسطة الحجم إمَّا أنها لا تقوم بخطوات كافية لحماية النظم وإما أنها تتصور بشكل خاطئ أنها لن تكون هدفاً لهذه الجرائم.

٤٩- وتؤدي الأُطر التنظيمية الرقابية دوراً مهماً في منع الجرائم السيبرانية فيما يتعلق بالقطاع الخاص عموماً وبمقدّمي الخدمات خصوصاً. وقد اعتمد حوالي نصف عدد البلدان قوانين لحماية البيانات تحدِّد المتطلبات اللازمة لحماية البيانات الشخصية واستخدامها. وتتضمن بعض هذه القوانين متطلبات محدَّدة خاصة بمقدّمي خدمات الإنترنت وغيرهم من مقدّمي خدمات الاتصالات الإلكترونية. وعلى حين تتطلّب قوانين حماية البيانات حذف البيانات الشخصية عندما لا تعود لازمة، فقد وضع بعض البلدان استثناءات لأغراض التحقيقات الجنائية، تُلزِم مقدّمي خدمات الإنترنت بتخزين أنواع معينة من البيانات لفترة زمنية محدَّدة. ولدى العديد من الدول المتقدمة أيضاً قواعد تلزم المنظمات بإبلاغ الأفراد والجهات التنظيمية الرقابية عن الانتهاكات المتعلقة بالبيانات. ويتحمّل مقدّمو خدمات الإنترنت عادةً مسؤولية محدودة باعتبارهم "مجرّد قنوات" لمرور البيانات. وتزداد هذه المسؤولية في حال قيامهم بتعديل المحتويات المرسَلة، وكذلك في حال كونهم على علم، فعلياً أو استدلالياً، بنشاط غير قانوني. ومن جهة أخرى، تقل هذه المسؤولية في حال مسارعتهم إلى اتخاذ الإجراءات اللازمة إثر إبلاغهم بنشاط غير قانوني. وعلى حين تتوافر لمقدِّمي خدمات الإنترنت إمكانيات تقنية لفرز محتويات الإنترنت، فإنَّ فرض قيود على النفاذ إلى شبكة الإنترنت يخضع لإمكانية التوقّع ومتطلبات التناسب مع مستوى التهديد، وهما شرطان واردان في القانون الدولي لحقوق الإنسان الذي يحمي حقوق التماس المعلومات وتلقيها وتناقلها.

٥٠- وتتَّسم الشراكات بين القطاع العام والقطاع الخاص بأهمية محورية لمنع الجرائم السيبرانية. وقد أبلغ أكثر من نصف مجموع البلدان عن وجود هذه الشراكات. وقد أُقيمت أعداد من هذه الشراكات على نحو متساوٍ بمقتضى اتفاقات غير رسمية وعلى أسس قانونية أيضاً. وفي أكثر الأحيان تكون هيئات القطاع الخاص مشمولة في علاقات الشراكة، تليها المؤسسات الأكاديمية، والمنظمات الدولية والإقليمية. وتُستخدَم الشراكات غالباً من أجل تيسير تبادل المعلومات عن التهديدات والاتجاهات، وكذلك تُستخدم من أجل تنفيذ أنشطة وإجراءات وقائية في حالات محددة. وفي سياق بعض الشراكات بين القطاع العام والقطاع الخاص، أخذت كيانات القطاع الخاص بنهج استباقي للتحقيق في الجرائم السيبرانية واتخاذ إجراءات قانونية بشأنها. وتُكمّل هذه الإجراءات تلك التي تتخذها سلطات إنفاذ القانون،

ويمكن أن تساعد في تخفيف الضرر على الضحايا. كما إنَّ المؤسسات الأكاديمية تؤدي مجموعة متنوعة من الأدوار في منع الجرائم السيبرانية، من خلال عدة سُبل ومنها تثقيف المهنيين وتدريبهم ووضع القوانين والسياسات العامة والعمل على تطوير المعايير والحلول التقنية. وتستضيف الجامعاتُ الخبراءَ في مجال الجرائم السيبرانية وبعضَ الأفرقة المعنية بمواجهة الطوارئ الحاسوبية ومراكز البحوث المتخصصة، وتيسّر ما يضطلعون به من أعمال.

باء- موجز النتائج الرئيسية من الدراسة

٥١- فيما يلي النتائج الرئيسية المستخلصة من الدراسة الشاملة عن الجريمة السيبرانية:

(أ) إنَّ التنافر في الإجراءات على الصعيد الدولي وتنوّع القوانين الوطنية الخاصة بالجرائم السيبرانية قد يعزيان إلى وجود صكوك متعددة ذات نطاق موضوعي وجغرافي مختلف. ومع أنَّ تلك الصكوك تعبِّر شرعياً عن الاختلافات الاجتماعية والثقافية والإقليمية القائمة، فإنَّ أوجه التباين في مدى الصلاحيات الإجرائية والأحكام المتعلقة بالتعاون الدولي قد تفضي إلى نشوء "مجموعات" متعاونة من البلدان، مما لا يتناسب دائماً مع الطابع العالمي للجرائم السيبرانية؛

(ب) إنَّ التعويل على الوسائل التقليدية للتعاون الدولي الرسمي في مسائل الجرائم السيبرانية لا يمكّن حالياً من الاستجابة في الوقت المناسب لمقتضيات الحصول على الأدلّة الإلكترونية السريعة الزوال والتغيُّر. وبما أنَّ عدداً متزايداً من الجرائم يشتمل على أدلّة إلكترونية توجد في أماكن جغرافية متباعدة التوزّع، فإنَّ ذلك يصبح مشكلة ليس بشأن الجرائم السيبرانية فقط، وإنما بشأن كل الجرائم عموماً؛

(ج) في عالم الحوسبة السحابية ومراكز البيانات، تستدعي الضرورةُ إعادة تحديد مفهوم دور "موضع" الأدلة، لأهداف عدّة ومنها التوصُّل إلى توافق في الآراء بشأن المسائل المتعلقة بحصول سلطات إنفاذ القانون مباشرةً على المعلومات الموجودة خارج نطاق ولايتها القضائية؛

(د) إنَّ تحليل الأطر القانونية الوطنية المتاحة يشير إلى عدم كفاية التنسيق فيما يتعلق بالجرائم السيبرانية "الأساسية" وصلاحيات التحقيق ومقبولية الأدلة الإلكترونية. ويمثّل القانون الدولي لحقوق الإنسان مرجعاً خارجياً هاماً فيما يتعلق بمسائل التجريم والأحكام الإجرائية؛

(هـ) إنَّ سلطات إنفاذ القانون والمدّعين العامين والسلطات القضائية في البلدان النامية تحتاج إلى دعم ومساعدة تقنيين على نحو شامل ومستدام وطويل الأمد من أجل التحقيق في الجرائم السيبرانية ومكافحتها؛

(و) إنَّ أنشطة منع الجرائم السيبرانية في جميع البلدان تتطلب تعزيز الشراكات بين القطاع العام والقطاع الخاص وإدماج الاستراتيجيات الخاصة بالجرائم السيبرانية ضمن منظور أوسع للأمن السيبراني، وذلك من خلال نهج كلي يشتمل على مواصلة زيادة الوعي في هذا الصدد.

جيم- موجز الخيارات الواردة في الدراسة

٥٢- استندت الخيارات المعروضة في الدراسة التي أعدها مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة إلى المعلومات المستمدّة من ردود البلدان على سؤال من أسئلة الاستبيان الخاص بالدراسة حول الخيارات التي يمكن النظر فيها لتعزيز التدابير القانونية أو غيرها من التدابير القائمة على الصعيدين الوطني والدولي للتصدي للجرائم السيبرانية واقتراح تدابير جديدة في هذا الشأن، وكذلك إلى النتائج الرئيسية المستخلصة من الدراسة. وتبيّنت الدراسة أن هذه الخيارات يمكن أن تتضمَّن واحداً أو أكثر من واحد من الخيارات التالية:[٩]

(أ) صوغ أحكام نموذجية دولية بشأن تجريم الأفعال الأساسية التي تمثل جرائم سيبرانية، وذلك بغية دعم الدول في القضاء على الملاذات الآمنة من خلال اعتماد عناصر مشتركة للجرائم؛

(ب) صوغ أحكام نموذجية دولية بشأن صلاحيات التحقيق الخاصة بالأدلّة الإلكترونية، بغية دعم الدول في ضمان وجود الأدوات الإجرائية الضرورية للتحقيق في الجرائم التي تشتمل على أدلّة إلكترونية؛

(ج) صوغ أحكام نموذجية بشأن الولاية القضائية، من أجل توفير أسس فعّالة مشتركة للولاية القضائية في المسائل الجنائية الخاصة بالجرائم السيبرانية؛

(د) صوغ أحكام نموذجية بشأن التعاون الدولي فيما يتعلق بالأدلّة الإلكترونية، بغية إدراجها في الصكوك الثنائية أو المتعددة الأطراف، بما في ذلك إعداد معاهدة نموذجية منقّحة بشأن تبادل المساعدة في المسائل الجنائية، بما يتوافق مع الاقتراحات الواردة في دليل المناقشة الخاص بمؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية؛

(هـ) صوغ صك متعدد الأطراف بشأن التعاون الدولي فيما يتعلق بالأدلّة الإلكترونية في المسائل الجنائية، بغية توفير آلية دولية للتعاون الجيد التوقيت من أجل حفظ الأدلّة الإلكترونية والحصول عليها؛

(9) يرد المزيد من التفاصيل حول هذا في الوثيقة UNODC/CCPCJ/EG.4/2013/2.

(و) صوغ صك شامل متعدد الأطراف بشأن الجرائم السيبرانية، بغية إقرار نهج دولي في مجالات التجريم والصلاحيات الإجرائية والولاية القضائية والتعاون الدولي؛

(ز) تعزيز الشراكات على الصعد الدولية والإقليمية والوطنية، بما في ذلك الشراكات مع القطاع الخاص والمؤسسات الأكاديمية، من أجل تقديم مساعدة تقنية معزّزة من أجل منع الجرائم السيبرانية ومكافحتها في البلدان النامية.

خامساً- توصيات لتعزيز الأنشطة المتصلة بمكافحة الجريمة السيبرانية، بما في ذلك المساعدة التقنية وبناء القدرات

٥٣- لعلَّ اللجنةَ تودّ أن تطلب إلى مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة، استنادا، من ضمن جملة أمور، إلى أنشطته المجملة في القسم ثانيا من هذا التقرير، مواصلة تقديم المساعدة التقنية إلى الدول الأعضاء فيما يتعلق بمواجهة الجريمة السيبرانية، وتحثُّ الدولَ الأعضاء على تقديم موارد من خارج إطار الميزانية لذلك الغرض من أجل ضمان بناء القدرات المستدامة طويلة الأمد لمواجهة الجريمة السيبرانية في الدول النامية.