الأمم المتحدة E/CN.15/2011/19

المجلس الاقتصادي والاجتماعي

Distr.: General
2 March 2011
Arabic
Original: English

لجنة منع الجريمة والعدالة الجنائية
الدورة العشرون
فيينا، ١١-١٥ نيسان/أبريل ٢٠١١
البند ٦ من جدول الأعمال المؤقّت*
اتجاهات الجريمة على الصعيد العالمي والمسائل المستجدّة وتدابير التصدّي في مجال منع الجريمة والعدالة الجنائية

تقرير فريق الخبراء الحكومي الدولي المفتوح العضوية عن الدراسة الشاملة لمشكلة الجريمة السيبرانية وتدابير التصدّي لها من جانب الدول الأعضاء والمجتمع الدولي والقطاع الخاص

مذكّرة من الأمانة

١- عملاً بالفقرة ٩ من قرار الجمعية العامة ٦٥/٢٣٠، عقد فريق الخبراء الحكومي الدولي المفتوح العضوية، الذي شكّلته اللجنة وفقاً للفقرة ٤٢ من إعلان سلفادور بشأن الاستراتيجيات الشاملة لمواجهة التحديات العالمية: نظم منع الجريمة والعدالة الجنائية وتطوّرها في عالم متغيّر (قرار الجمعية العامة ٦٥/٢٣٠، المرفق) اجتماعه في فيينا من ١٧ إلى ٢١ كانون الثاني/يناير ٢٠١١. وأجرى فريق الخبراء، وفقا لولايته، مداولات بشأن مسألة:

إجراء دراسة شاملة لمشكلة الجريمة السيبرانية وتدابير التصدّي لها من جانب الدول الأعضاء والمجتمع الدولي والقطاع الخاص، بما في ذلك تبادل المعلومات عن التشريعات الوطنية والممارسات الفضلى والمساعدة التقنية والتعاون الدولي، بغية دراسة الخيارات

* E/CN.15/2011/1.

280211 V.11-80324 (A)

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

٢- وفي الفقرة ١١ من القرار ٦٥/٢٣٠، طلبت الجمعية العامة إلى فريق الخبراء الحكومي الدولي المفتوح العضوية أن يقدّم إلى لجنة منع الجريمة والعدالة الجنائية تقريرا عن التقدّم المحرز في عمله. ووفقا لذلك، استعرض فريق الخبراء واعتمد الوثيقتين الختاميتين المعنونتين "جمع المواضيع المطروحة للنظر في إطار دراسة شاملة بشأن تأثير الجريمة السيبرانية وتدابير التصدّي لها (المرفق الأول)، و"منهجية الدراسة" (المرفق الثاني)، اللتين قُدّمتا إلى اللجنة في دورتها العشرين كي تنظر فيهما.

٣- وعقب اعتماد جمع المواضيع المطروحة للنظر في إطار دراسة شاملة بشأن تأثير الجريمة السيبرانية وتدابير التصدِّي لها (المرفق الأول)، أصدر ممثل كولومبيا البيان التالي وطلب إدراجه في تقرير فريق الخبراء الحكومي الدولي المفتوح العضوية:

١- خلال اجتماع فريق الخبراء الحكومي الدولي المفتوح العضوية، أعربت وفود عديدة عن انشغالها إزاء إساءة الاستعمال المتكرر لتكنولوجيات المعلومات والاتصالات الجديدة في الأغراض الإرهابية. وفي هذا السياق، قدّم ممثل للأمانة عرضا عن عمل مكتب الأمم المتحدة المعني بالمخدرات والجريمة بشأن هذه المشكلة، ولا سيما إساءة استعمال الإنترنت. وإذا أُخذ في الحسبان أن دراسة الجريمة السيبرانية يتعيّن أن تكون كاملة وشاملة، فينبغي لها أن تتصدى لجميع الشواغل التي أُعرب عنها. وذلك يُضفي أهمية حاسمة على تضمين الدراسة جميع جوانب العلاقات بين الإرهاب والجريمة السيبرانية. فالمنظمات الإرهابية تستعمل هذه التكنولوجيات بطرق متنوّعة، من قبيل:

(أ) للأغراض الدعائية؛

(ب) لجمع المعلومات؛

(ج) كأداة تدريب؛

(د) لتنظيم الأنشطة غير المشروعة؛

(هـ) لنشر المعلومات لأغراض التجنيد والتحريض؛

(و) لأغراض ضمان خزن المعلومات وإرسالها؛

(ز) لمهاجمة الشبكات الحاسوبية نفسها.

٢- ولصالح تحقيق توافق في الآراء، تقبل كولومبيا اقتراحات وفد الأرجنتين بشأن هذا الموضوع، ولكنها تطلب ملاحظة ما يلي في تقرير اجتماع فريق الخبراء الحكومي الدولي المفتوح العضوية عن اجتماعه الأول:

(أ) فيما يتعلق بالفقرة ١٢ من جمع المواضيع المطروحة للنظر في إطار دراسة شاملة بشأن تأثير الجريمة السيبرانية وتدابير التصدّي لها (المرفق الأول)، تفهم كولومبيا أن حصر الأفعال المجرَّمة يشمل موضوع الإرهاب؛

(ب) وبالنسبة للعنوان السابق للفقرة ١٨ من هذه الوثيقة، تفهم كولومبيا أن تحديات مكافحة الجريمة السيبرانية تشمل أيضا موضوع الإرهاب؛

(ج) وتأمل كولومبيا أيضا أن تتضمن الدراسة النظر في إساءة استعمال الإرهابيين الممكن لأدوات يُمكن استعمالها في ارتكاب الجريمة السيبرانية، حسبما ذُكر في الفقرة ٢٥ من هذه الوثيقة.

المرفق الأول

جمع المواضيع المطروحة للنظر في إطار دراسة شاملة بشأن تأثير الجريمة السيبرانية وتدابير التصدّي لها

أولا- مقدّمة

١- ناقشت الدول الأعضاء، أثناء مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية في عام ٢٠١٠، مسألة الجريمة السيبرانية ببعض التعمّق وقرَّرت أن تدعو لجنة منع الجريمة والعدالة الجنائية إلى عقد اجتماع لفريق خبراء حكومي دولي مفتوح العضوية من أجل إجراء دراسة شاملة لمشكلة الجريمة السيبرانية وتدابير التصدّي لها. واعتمدت لجنة منع الجريمة والعدالة الجنائية تلك التوصية، ثم اعتمدها المجلس الاقتصادي والاجتماعي في قراره ١٨/٢٠١٠، كما اعتمدتها الجمعية العامة في قرارها ٢٣٠/٦٥.

٢- ووفقا للفقرة ٤٢ من إعلان سلفادور بشأن الاستراتيجيات الشاملة لمواجهة التحديات العالمية: نُظم منع الجريمة والعدالة الجنائية وتطوّرها في عالم متغيّر، ستبحث الدراسة الشاملة:

مشكلة الجريمة السيبرانية وتدابير التصدّي لتلك الجريمة التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص، بما يشمل تبادل المعلومات عن التشريعات الوطنية والممارسات الفضلى والمساعدة التقنية والتعاون الدولي، بغية دراسة خيارات لتعزيز التدابير القانونية أو التدابير الأخرى القائمة على الصعيدين الوطني والدولي للتصدّي للجريمة السيبرانية واقتراح تدابير جديدة في هذا الشأن.

٣- ومن ثم، فإنَّ الفقرة ٤٢ من إعلان سلفادور تحدِّد الجوانب الجوهرية المختلفة التي ينبغي أن تبحثها الدراسة (مشكلة الجريمة السيبرانية والتشريعات الوطنية والممارسات الفضلى والمساعدة التقنية والتعاون الدولي) وكذلك المنظور (التدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص) ومحور التركيز (النظر في الخيارات المتاحة لتعزيز التدابير القانونية أو التدابير الأخرى القائمة على الصعيدين الوطني والدولي للتصدّي للجريمة السيبرانية واقتراح تدابير جديدة في هذا الشأن).

٤- وبغية إعداد هيكل الدراسة، تم تحويل هذه الأبعاد الثلاثة (الجوانب الجوهرية والمنظور ومحور التركيز) إلى ١٢ موضوعا تتوافق مع الولاية المنصوص عليها في إعلان سلفادور. وصُنِّفت هذه المواضيع الاثنا عشر أدناه في فئات.

مشكلة الجريمة السيبرانية (المواضيع ١ إلى ٣)

٥- يبيِّنُ إعلانُ سلفادور أنَّ الدراسةَ ينبغي أن تتحرّى مشكلة الجريمة السيبرانية. وبُغيةَ تناول النطاق الكامل للمشاكل التي تطرحها الجريمة السيبرانية، حُدِّدت ثلاثة مجالات رئيسية لتحليلها تحليلا مفصّلا:

(أ) ظاهرة الجريمة السيبرانية (الموضوع ١)؛

(ب) المعلومات الإحصائية (الموضوع ٢)؛

(ج) التحديات التي تطرحها الجريمة السيبرانية (الموضوع ٣).

تدابير التصدّي القانونية للجريمة السيبرانية (المواضيع ٤ إلى ٩)

٦- يدعو إعلانُ سلفادور إلى إجراء دراسة تدابير التصدّي القانونية للجريمة السيبرانية، تشمل تبادل المعلومات عن التشريعات الوطنية والممارسات الفضلى والتعاون الدولي. وقد حُدِّدت، إضافة إلى الجوانب العامة لمواءمة التشريعات، مجالات معيَّنة لتدابير التصدّي القانونية للجريمة السيبرانية، هي:

(أ) النهوج المشتركة للتشريعات (الموضوع ٤)؛

(ب) التجريم (الموضوع ٥)؛

(ج) الصلاحيات الإجرائية (الموضوع ٦)؛

(د) التعاون الدولي (الموضوع ٧)؛

(هـ) الضمانات والشروط، بما في ذلك حماية حقوق الإنسان الأساسية والبيانات الشخصية؛

(و) احترام مبدأ تساوي الدول في السيادة وعدم التدخل في شؤون الدول الأخرى؛

(ز) الأدلة الإلكترونية (الموضوع ٨)؛

(ح) أدوار ومسؤوليات مقدِّمي الخدمة والقطاع الخاص (الموضوع ٩).

قدرات منع الجريمة والعدالة الجنائية وتدابير التصدّي الأخرى للجريمة السيبرانية (الموضوع ١٠)

٧- لا يكتفي إعلانُ سلفادور بالإشارة إلى دراسة تدابير التصدّي القانونية للجريمة السيبرانية، بل يشير أيضا بصورة أعمَّ إلى سائر أنواع تدابير التصدّي للجريمة السيبرانية.

المنظمات الدولية (الموضوع ١١)

٨- يدعو إعلانُ سلفادور إلى تحليل تدابير التصدّي للجريمة السيبرانية التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص. ولئن كانت المسائل المتعلقة بتدابير التصدِّي القانونية للجريمة السيبرانية التي يتخذها المجتمع الدولي مشمولة تحت عنوان تدابير التصدّي القانونية، فإنَّ من شأن تناول التدابير التي يتخذها المجتمع الدولي تحت عنوان منفصل أن ييسّر تحليل الجوانب الأعم مثل العلاقة بين النهوج الإقليمية والدولية.

المساعدة التقنية (الموضوع ١٢)

٩- بالنظر إلى تأثير الجريمة السيبرانية على البلدان النامية، والحاجة إلى الأخذ بنهج موحَّد ومنسَّق لمكافحة الجريمة السيبرانية، سوف تعالج مسألة المساعدة التقنية باعتبارها مجالاً محدّداً ستتناوله الدراسة الشاملة.

ثانيا- عرض مفصَّل للمواضيع

الموضوع ١- ظاهرة الجريمة السيبرانية

الخلفية

١٠- يُستخدَم المصطلحان "الجريمة الحاسوبية"، وبصفة أكثر تحديدا "الجريمة السيبرانية"، لوصف فئة معيَّنة من السلوك الإجرامي. وتَتَّصل بهذه الفئة من السلوك الإجرامي تحدياتٌ من ضمنها على السواء اتساعُ نطاق الجرائم المندرجة فيها والتطوّر الدينامي للأساليب الجديدة في ارتكاب الجرائم.

تطوُّر الجريمة الحاسوبية والجريمة السيبرانية

١١- في ستينيات القرن العشرين، عندما ظهرت النظم الحاسوبية العاملة بالترانزيستور وأصبحت الحواسيب تُلاقي مزيداً من الرواج،[1] تم التركيز في تجريم الأفعال المرتكَبَة على

(1) فيما يتعلق بالتحديات ذات الصلة، انظر R. T. Slivka and J. W. Darrow, "Methods and problems in computer security", *Rutgers Journal of Computers and the Law*, vol. 5, No. 2 (1976), pp. 217-269.

الأضرار المادية التي تلحق بالنظم الحاسوبية والبيانات المخزَّنة فيها.[٢] واتَّسمت السبعينيات بالتحوُّل من جرائم الممتلكات التقليدية التي تمسُّ النظمَ الحاسوبية[٣] إلى أشكال جديدة من الجريمة،[٤] تشمل أمورا منها الاستخدام غير المشروع للنظم الحاسوبية،[٥] والتلاعب[٦] بالبيانات الإلكترونية.[٧] وأفضى الانتقال من المعاملات اليدوية إلى المعاملات الحاسوبية إلى نشوء شكل جديد من الجريمة – وهو الاحتيال الحاسوبي.[٨] وفي الثمانينيات، زاد رواج الحواسيب الشخصية أكثر فأكثر، ولأول مرة في التاريخ، أصبحت طائفة واسعة من البنى التحتية الحاسمة الأهمية معتمدة على التكنولوجيا الحاسوبية.[٩] وكان بين الآثار الجانبية لانتشار النظم الحاسوبية ازدياد الاهتمام بالبرامجيات الحاسوبية، وبدء ظهور أول شكل من أشكال قرصنة البرامجيات الحاسوبية والجرائم المتصلة ببراءات الاختراع.[١٠] وفضلا عن ذلك، أدّى البدء في ربط النظم الحاسوبية بعضها ببعض إلى تمكّن الجاني من الدخول إلى نظام

(2) McLaughlin, "Computer crime: the Ribicoff Amendment to United States Code, Title 18", *Criminal Justice Journal*, vol. 2, 1978, pp. 217 ff.

(3) Gemignani, "Computer crime: the law in '80", *Indiana Law Review*, vol. 13, 1980, p. 681.

(4) McLaughlin, "Computer crime: the Ribicoff Amendment".

(5) Freed, *Materials and Cases on Computer and Law* (n.p., 1971), p. 65.

(6) Bequai, "The electronic criminals: how and why computer crime pays", *Barrister*, vol. 4, 1977, pp. 8 ff.

(7) *Criminological Aspects of Economic Crime: Proceedings of the 12th European Conference of Directors of Criminological Research Institutes (November 1976)*, vol. XV, Collected Studies in Criminological Research (Strasbourg, Council of Europe, 1977), pp. 225 ff.; United States of America, *Staff Study of Computer Security in Federal Programs: Committee on Government Operations — United States Senate* (Washington, D.C., United States Government Printing Office, 1977).

(8) McLaughlin, "Computer crime: the Ribicoff Amendment" (انظر الحاشية ٢ أعلاه)؛ و Bequai, "Computer crime: a growing and serious problem", *Police Law Quarterly*, vol. 6, 1977, p. 22.

(9) E. A. Glynn, "Computer abuse: the emerging crime and the need for legislation", *Fordham Urban Law Journal*, vol. 12, No. 1 (1983-1984), p. 73.

(10) BloomBecker, "The trial of computer crime", *Jurimetrics Journal*, vol. 21, 1981, p. 428; W. Schmidt, "Legal proprietary interests in computer programs: the American experience", *Jurimetrics Journal*, vol. 21, 1981, pp. 345 ff.; M. Dunning, "Some aspects of theft of computer software", *Auckland University Law Review*, vol. 4, No. 3 (1982), pp. 273 ff.; Weiss, "Pirates and prizes: the difficulties of protecting computer software", *Western State University Law Review*, vol. 11, 1983, pp. 1 ff.; R. P. Bigelow, "The challenge of computer law", *Western England Law Review*, vol. 7, No. 3 (1985), p. 401; G. Thackeray, "Computer-related crimes: an outline", *Jurimetrics Journal*, vol. 25, No. 3 (1985), pp. 300 ff.

حاسوبي دون أن يكون موجودا في مسرح الجريمة.[١١] وأفضى استحداث الواجهة البينية البيانية (World Wide Web) في التسعينيات، التي أعقبها التزايد السريع في عدد مستخدمي الإنترنت، إلى ظهور أساليب جديدة من السلوك الإجرامي. فبعد أن كان توزيع مواد التعدِّي على الأطفال مثلا يتم عن طريق التبادل المادي للكتب وشرائط الفيديو، أصبح يجري من خلال المواقع الشبكية وخدمات الإنترنت.[١٢] ولئن كانت الجرائم الحاسوبية جرائم محلية عموما، فقد حوَّلت الإنترنت الجريمةَ الإلكترونية إلى جريمة عبر وطنية. وقد اتّسم العقدُ الأول من القرن الحادي والعشرين بانتشار أساليب جديدة ومعقَّدة للغاية في ارتكاب الجرائم، مثل "التصيُّد الاحتيالي"[١٣] و"الاعتداءات البوتنتية"[١٤] والاستخدامات المستجدة للتكنولوجيا مثل الاتصال عن طريق بروتوكول نقل الصوت عبر الإنترنت (VoIP)[١٥] و"الحساب الإلكتروني السحابي"،[١٦] مما يثير صعوبات أمام إنفاذ القانون.

(11) Yee, "Juvenile computer crime: hacking — criminal and civil liability", *Comm/Ent Law Journal*, vol. 7, 1984, pp. 336 ff.; "Who is calling your computer next? Hacker!", *Criminal Justice Journal*, vol. 8, 1985, pp. 89 ff.; A. M. Wagner, "The challenge of computer-crime legislation: how should New York respond?", *Buffalo Law Review*, vol. 33, No. 3 (1984), pp. 777 ff.

(12) "Child pornography", theme paper prepared for the Second World Congress against Commercial Sexual Exploitation of Children, Yokohama, Japan, 12-20 December 2001, p. 17; "Sexual exploitation of children over the Internet", report prepared for the use of the Committee on Energy and Commerce, United States, House of Representatives, 109th Congress, January 2007, p. 9.

(13) يصف مصطلح "phishing" (التصيُّد الاحتيالي) فعلا يُضطلع به لجعل الضحية تكشف عن معلومات شخصية/سرية. وكان هذا المصطلح يصف أصلا استخدام الرسائل الإلكترونية من أجل "تصيُّد" كلمات السر والبيانات المالية من بحر مستخدمي الإنترنت. واستخدام الحرفين "ph" مرتبط بأعراف شائعة للتسميات في أوساط مخترقي النظم الحاسوبية (hackers). وللاطلاع على مزيد من المعلومات في هذا الصدد، انظر: "فهم الجريمة السيبرانية: دليل للبلدان النامية"، الاتحاد الدولي للاتصالات (جنيف، ٢٠٠٩)، الفصل ٢-٨-٤.

(14) "Botnets" (بوتنت) هو تعبير وجيز يشير إلى مجموعة حواسيب دُسَّ فيها برنامج يخضع لتحكُّم خارجي. وللاطلاع على مزيد من التفاصيل، انظر: Clay Wilson, "Botnets, cybercrime, and cyberterrorism: vulnerabilities and policy issues for congress", Congressional Research Service Report RL32114, 2007, p. 4.

(15) M. Simon and J. Slay, "Voice over IP: forensic computing implications", paper prepared for the fourth Australian Digital Forensics Conference, Perth, 4 December 2006.

(16) Cristos Velasco San Martin, "Jurisdictional aspects of cloud computing", paper presented at the Council of Europe Octopus Interface Conference: Cooperation against Cybercrime, Strasbourg, 10-11 March 2009; M. Gercke, "Die Auswirkungen von Cloud Storage auf die Tätigkeit der Strafverfolgungsbehörden", in *Inside the Cloud: Neue Herausforderungen für das Informationsrecht*, J. Taeger and A. Wiebe, eds., Oldenburger Tagungsbände (Edewecht, Germany, Oldenburger Verlag für Wirtschaft, Informatik und Recht, 2009), pp. 499 ff.

نطاق الدراسة

١٢- ستركّز الدراسة التي ستُجرى لهذا الموضوع على ظاهرة الجريمة السيبرانية ذاتها، ولن تشمل تدابير التصدّي لها:

(أ) تحليل ظاهرة الجريمة السيبرانية مع أخذ الأفعال التي تشملها الأطر القانونية القائمة في الاعتبار؛

(ب) حصر الأفعال المجرَّمة؛

(ج) حصر السلوكيات التي لم تُجرَّم بعد؛

(د) استعراض الجرائم المركَّبة (مثل التصيُّد الاحتيالي) واتجاهاتها في المستقبل؛

(هـ) حصر القضايا ذات الصلة؛

(و) النظر في أهمية تعريف الجريمة السيبرانية.

الموضوع ٢- المعلومات الإحصائية

الخلفية

١٣- تُوفِّر إحصاءاتُ الجرائم أساساً لما يقوم به مقررو السياسات والأوساط الأكاديمية من مناقشات ومن اتخاذ لقرارات في هذا الصدد.[١٧] كذلك فإن الحصول على معلومات دقيقة عن المدى الحقيقي لانتشار الجريمة السيبرانية يُمكن أن يمكِّن هيئات إنفاذ القانون من تحسين استراتيجياتها الخاصة بالتصدّي للجريمة السيبرانية وردع الاعتداءات المحتملة وكفالة سنّ تشريعات أكثر ملاءمة وفعالية.

الوضعُ الراهن للإحصاءات المتعلقة بالجريمة السيبرانية

١٤- تُستَقَى المعلوماتُ المتعلقة بمدى انتشار الجرائم بوجه عام من الإحصاءات والدراسات الاستقصائية الخاصة بالجرائم.[١٨] ويطرح هذان النوعان من المصادر تحديات عند استخدامهما

(17) P. A. Collier and B. J. Spaul, "Problems in policing computer crime", *Policing and Society*, vol. 2, No. 4 (1992), p. 308.

(18) فيما يتعلق بالأهمية الناشئة لإحصاءات الجريمة، انظر: D. A. Osborne and S. C. Wernicke, *Introduction to Crime Analysis: Basic Resources for Criminal Justice Practice* (Binghamton, New York, Haworth Press, 2003), pp. 1 ff.

في إعداد توصيات السياسات العامة. فبادئ ذي بدء، تُوضَع إحصاءات الجريمة عموما على المستوى الوطني، ولا تجسّد نطاق الانتشار على الصعيد الدولي. ولئن كان يمكن نظريا تجميع البيانات بين مختلف الدول، فإنَّ هذا النهجَ لن يسفر عن معلومات موثوقة بسبب اختلاف التشريعات وممارسات التسجيل.[١٩] فتجميعُ إحصاءات الجريمة الوطنية ومقارنتها يستلزمان درجة ما من التوافق[٢٠] لا تتوفّر فيما يخص الجريمة السيبرانية. وحتى في الحالات التي تكون فيها الجرائم السيبرانية مسجَّلة، لا تكون بالضرورة مدرجة بشكل منفصل.[٢١]

١٥- وثانيا، لا يمكن للإحصاءات أن تجسّد إلا الجرائم المكتشفة والمبلغ عنها.[٢٢] وفيما يتصل بالجريمة السيبرانية على وجه الخصوص، هناك مخاوف من أن عدد الحالات غير المبلغ عنها قد يكون مهماً.[٢٣] وقد تخشى المؤسسات التجارية أن يؤثّر هذا النوع من الدعاية السلبية على سمعتها.[٢٤] فحين تُعلن شركة أنَّ هناك من نجح في اختراق خادومها، فقد يفقد

(19) انظر في هذا السياق: *Overcoming Barriers to Trust in Crimes Statistics: England and Wales*, Monitoring Report No. 5, interim report (London, United Kingdom Statistics Authority, December 2009), p. 9، المتاح على الموقع التالي: www.statisticsauthority.gov.uk.

(20) A. Alvazzi del Frate, "Crime and criminal justice statistics challenges", in *International Statistics on Crime and Justice*, S. Harrendorf, M. Heiskanen and S. Malby, eds., HEUNI Publication Series, No. 64 (Helsinki, European Institute for Crime Prevention and Control, affiliated with the United Nations, 2010), p. 168، المتاح على الموقع التالي: www.unodc.org/documents/data-and-analysis/Crime-statistics/International_Statistics_on_Crime_and_Justice.pdf.

(21) "Computer crime", Parliamentary Office of Science and Technology, *Postnote*, No. 271, October 2006, p. 3.

(22) فيما يتعلق بالتحديات ذات الصلة، انظر: M. E. Kabay, "Understanding studies and surveys of computer crime", June 2009، المتاح على الموقع التالي: www.mekabay.com/methodology/crime_stats_methods.pdf.

(23) "طلب مكتب التحقيق الاتحادي في الولايات المتحدة من الشركات ألا تسكت عن هجمات التصيُّد الاحتيالي والهجمات على نظم المعلومات والاتصالات فيها، بل أن تبلغ السلطات بذلك لكي تحسن معرفتها بالأفعال الإجرامية التي تتم على الإنترنت". وقال مارك ميرشون، رئيس مكتب التحقيقات الاتحادي بالنيابة في نيويورك إنَّ "ما يسبب مشكلة لنا هو أنَّ بعض الشركات تقلق دون شك من الدعاية السلبية أكثر من قلقها من نتائج نجاح هجمات الاختراق الحاسوبي". انظر "FBI wants to know more about hacker attacks", *Heise News* بتاريخ ٢٧ تشرين الأول/أكتوبر ٢٠٠٦، المتاح على الموقع التالي: www.h-online.com/security/news/item/FBI-wants-to-know-more-about-hacker-attacks-731717.html. وانظر أيضا: "Comments on computer crime: Senate Bill S. 240", *Memphis State University Law Review*, 1980, p. 660.

(24) انظر N. Mitchison and R. Urry, "Crime and abuse in e-business", in *IPTS Report*, No. 57, 2001, pp. 18-22؛ و"Collier and Spaul, "Problems in policing computer crime (انظر الحاشية ١٧ أعلاه)، صفحة ٣١٠.

الزبائن الثقة بها، مما يترتّب عليه تكاليف قد تتجاوز حتى الخسائر الناجمة عن الاختراق. ولكن إذا لم يجر الإبلاغ عن الجرائم وملاحقة مرتكبيها قضائياً، فقد يعمد الجناة إلى تكرارها. وقد لا يعتقد الضحايا أنَّ هيئات إنفاذ القانون ستتمكّن من معرفة هوية الجناة،[٢٥] وربما لا يجدون مبرّرا كافيا للإبلاغ عن الجرائم.[٢٦] وبما أنَّ أتمتة هجمات الجريمة السيبرانية تُمكِّن المجرمين السيبرانيين من وضع استراتيجية لجني أرباح كبيرة عن طريق شنّ العديد من الهجمات السيبرانية التي تستهدف مبالغ صغيرة (الأمر الذي يحدث في حالات الاحتيال المتعلقة بالرسوم المدفوعة مقدما)،[٢٧] فإنَّ التأثير المحتمل لعدم الإبلاغ عن الجرائم قد يكون كبيرا. وعندما لا يخسر الضحايا إلا مبالغ صغيرة، فقد يفضّلون عدم إبلاغ هيئات إنفاذ القانون بالجرائم بالنظر إلى ما تستغرقه الإجراءات ذات الصلة من وقت. وفي الممارسة العملية، كثيرا ما تنطوي الحالات المبلغ عنها على مبالغ طائلة.[٢٨]

نطاق الدراسة

١٦- سوف تتألّف الدراسة الخاصة بهذا الموضوع مما يلي:

(25) انظر Collier and Spaul, "Problems in policing computer crime" (انظر الحاشية ١٧ أعلاه)، صفحة ٣١٠؛ و R. G. Smith, "Investigating cybercrime: barriers and solutions", paper prepared for the Association of Certified Fraud Examiners, Pacific Rim Fraud Conference, Sydney, 11 September 2003, p. 2، المتاح على الموقع التالي: www.aic.gov.au/about_aic/research_programs/staff/smith_russell.aspx.

(26) في واقع الأمر، تقتصر الصحف ومحطات البث التلفزيوني في تغطيتها الإعلامية للتحقيقات الناجحة المتصلة بالإنترنت على القضايا المثيرة للاهتمام مثل الكشف عن أحد مرتكبي جرائم الاستغلال الجنسي للأطفال من خلال تفكيك التعديلات التي أُدخلت على صور المشتبه فيه المتلاعب فيها وتوضيح ملامحه. وللاطلاع على مزيد من المعلومات عن القضية وتغطيتها، انظر المقال المعنون "Interpol in Appeal to find Paedophile Suspect" في صحيفة نيويورك تايمز بتاريخ ٩ تشرين الأول/أكتوبر ٢٠٠٧، المتاح على الموقع التالي: www.nytimes.com/2007/10/09/world/europe/09briefs-pedophile.html?_r=1&oref=slogin؛ وكذلك المعلومات المتاحة في موقع المنظمة الدولية للشرطة الجنائية (الإنتربول) على العنوان التالي: www.interpol.int/Public/THB/vico/Default.asp.

(27) انظر الوثيقة المعنونة "International crackdown on mass marketing fraud revealed", 2007، التي وضعتها وكالة مكافحة الجريمة المنظمة الخطيرة، المملكة المتحدة.

(28) في عام ٢٠٠٦، ورد في التقرير عن جرائم الإنترنت الصادر عن المركز الوطني المعني بجرائم ذوي الياقات البيضاء في الولايات المتحدة (NW3C) أنَّ ١.٧ في المائة فقط من إجمالي الخسائر المبلغ عنها بدولارات الولايات المتحدة كانت تتعلق برسائل احتيال نيجيرية، لكن هذه الحالات المبلغ عنها أسفرت عن خسائر متوسطها ٥ ١٠٠ دولار لكل حالة. وكان عدد الجرائم المبلغ عنها متدنّيا للغاية، في حين كان متوسط الخسائر المترتبة على هذه الجرائم مرتفعا.

(أ) جمع أحدث الإحصاءات والدراسات الاستقصائية والتحليلات التي تتناول مدى انتشار الجريمة السيبرانية ونطاقها؛

(ب) تقييم الإحصاءات لإعداد توصيات بشأن السياسات العامة؛

(ج) استبانة العقبات المحتملة في جمع الإحصاءات الدقيقة؛

(د) استبانة البلدان التي تقوم تحديدا بجمع إحصاءات عن الجرائم السيبرانية؛

(هـ) تقييم الحاجة إلى جمع معلومات إحصائية عن الجريمة السيبرانية وفوائد جمعها؛

(و) فحص التقنيات المحتملة التي يمكن استخدامها في جمع هذه المعلومات؛

(ز) مناقشة النموذج المحتمل للسلطة المركزية التي تودع لديها المعلومات الإحصائية.

الموضوع ٣- تحديات الجريمة السيبرانية

الخلفية

١٧- يُولَى في الوقت الراهن كثيرٌ من الاهتمام لوضع استراتيجيات تتناول التحديات المحدَّدة المرتبطة بالجريمة السيبرانية. وثمة نوعان من الأسباب التي تدعو إلى وضع هذه الاستراتيجيات: أولا، أنَّ بعض الأدوات اللازمة للتحقيق في الجريمة السيبرانية جديدة وتستلزم بالتالي بحوثا مكثَّفة، وثانيا، أنَّ التحقيقات في الجرائم التي تنطوي على استخدام التكنولوجيا الشبكية تكون محفوفة بعدة تحديات فريدة من نوعها غير مسبوقة في التحقيقات التقليدية.

تحديات مكافحة الجريمة السيبرانية والأخطار ذات الصلة

١٨- إنَّ قائمة التحديات التقنية والقانونية الفريدة المتصلة بالجريمة السيبرانية طويلة. ويُشار كمثال واحد على ذلك إلى إمكانية ارتكاب جرائم سيبرانية باستخدام أجهزة برامجية لا تتطلب معرفة تقنية متعمقة، مثل الأدوات البرامجية الحاسوبية[٢٩] المصمَّمة للعثور على منافذ مفتوحة أو لكسر الحماية بكلمات السر.[٣٠] ومن التحديات الأخرى صعوبة تعقّب

(29) "Websense", *Security Trends Report 2004*, p. 11; United States of America, General Accounting Office, *Information Security: Computer Controls over Key Treasury Internet Payment System*, GAO-03-837 (Washington, D.C., 2003), p. 3; U. Sieber, "The threat of cybercrime", in *Organised Crime in Europe: The Threat of Cybercrime — Situation Report 2004* (Strasbourg, Council of Europe Publishing, 2005), p. 143.

(30) K. Ealy, "A new evolution in hack attacks: a general overview of types, methods, tools, and prevention", SANS Institute, 2003, p. 9.

أثر مرتكبي هذه الجرائم. ورغم أنَّ مستخدمي خدمات الإنترنت يخلفون آثارا متعددة، فإنه يمكن للمجرمين عرقلة التحقيقات بتمويه هويتهم. فعلى سبيل المثال، إذا ارتكب أشخاصٌ جرائمَ باستخدام مرافق طرفية عمومية لخدمات الإنترنت أو شبكات لاسلكية مفتوحة، فقد يصعب تحديد هويتهم. ومَنشَأُ التحدي الأعمّ الذي يعترض سبيل التحقيق في الجريمة السيبرانية هو أنَّ الإنترنت تُوفِّر، من الناحية التكنولوجية، القليل من أدوات المراقبة التي يمكن أن تستخدمها سلطات إنفاذ القانون. فقد صُمِّمت الإنترنت أصلا كشبكة عسكرية[٣١] تستند إلى بنية شبكية لا مركزية، الهدف منها هو الحفاظ على القدرة التشغيلية الرئيسية حتى في حال تعرُّض عناصر من الشبكة لهجمات. ولم يكن هذا النهج اللامركزي مصمَّما أصلا لتيسير التحقيقات الجنائية أو منع الهجمات من داخل الشبكة، كما أنَّ تدابير التحقيق التي تستلزم وسائل للمراقبة تثير تحديات فريدة في هذا السياق.[٣٢]

نطاق الدراسة

١٩- سوف تتألّف الدراسة الخاصة بهذا الموضوع مما يلي:

(أ) حصر شامل للتحديات المتعلقة بمكافحة الجريمة السيبرانية؛

(ب) موجز بالممارسات الفضلى، التقنية والقانونية على السواء، المستخدمة لتذليل هذه التحديات.

الموضوع ٤- النهوج المشتركة للتشريعات

الخلفية

٢٠- وضعت بلدان ومنظمات إقليمية متنوعة في السنوات العشرين الماضية تشريعات وأطرا قانونية للتصدّي للجريمة السيبرانية. ولئن نشأت بعض التوجهات المشتركة على هذا الصعيد، فإنَّ الاختلافات في التشريعات الوطنية لا تزال كبيرة.

(31) للاطلاع على لمحة تاريخية وجيزة عن الإنترنت، بما في ذلك أصولها العسكرية، انظر: B. Leiner and others, "A brief history of the Internet"، المتاح على الموقع التالي: www.isoc.org/internet/history/brief.shtml.

(32) H. F. Lipson, *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues* (Pittsburgh, Carnegie Mellon University, Software Engineering Institute, 2002).

الاختلافات الوطنية والإقليمية

٢١- إنَّ من أسباب الاختلافات في الأطر التشريعية الوطنية والإقليمية على السواء اختلاف وقع الجريمة السيبرانية باختلاف المناطق، كما يتبيَّن من مكافحة الرسائل الإلكترونية التطفلية (Spam).[٣٣] فقد برزت الرسائل التطفلية هذه باعتبارها مسألة أكثر خطورة في البلدان النامية منها في البلدان الغربية بسبب ضآلة الموارد المتاحة لمكافحتها وارتفاع تكلفتها مقارنة بالبلدان الأخرى.[٣٤] وفيما يتعلق بالمحتوى غير المشروع، قد يجرم بعض البلدان والمناطق نشر مواد يمكن اعتبارها محمية وفق مبدأ حرية التعبير[٣٥] في بلدان أخرى.[٣٦]

(33) "فهم الجريمة السيبرانية: دليل للبلدان النامية" (انظر الحاشية ١٣ أعلاه)، الفصل ٢-٦-٧.

(34) انظر Organization for Economic Cooperation and Development, "Spam issues in developing countries", document DSTI/CP/ICCP/SPAM(2005)6/FINAL, 26 May 2005, p. 4، المتاح على الموقع التالي: www.oecd.org/dataoecd/5/47/34935342.pdf.

(35) فيما يتعلق بمبدأ حرية القول، انظر: T. L. Tedford and D. A. Herbeck, *Freedom of Speech in the United States*, 5th ed. (State College, Pennsylvania, Strata, 2005)؛ و E. Barendt, *Freedom of Speech* (Oxford, Oxford University Press, 2007)؛ و C. E. Baker; *Human Liberty and Freedom of Speech* (New York, Oxford University Press, 1989)؛ و J. W. Emord, *Freedom, Technology and the First Amendment* (San Francisco, Pacific Research Institute for Public Policy, 1991)؛ وبشأن أهمية المبدأ المتعلق بالمراقبة الإلكترونية، انظر: C. Woo and M. So, "The case for Magic Lantern: September 11 Highlights — the need for increasing surveillance", *Harvard Journal of Law and Technology*, vol. 15, No. 2 (2002), pp. 530 ff.؛ و M. Chesterman, *Freedom of Speech in Australian Law: A Delicate Plant* (Aldershot, Hampshire, Ashgate, 2000)؛ و E. Volokh, "Freedom of speech, religious harassment law, and religious accommodation law", *Loyola University Chicago Law Journal*, vol. 33, 2001, pp. 57 ff.، المتاح على الموقع التالي: www.law.ucla.edu/volokh/harass/religion.pdf؛ و H. Cohen, "Freedom of speech and press: exceptions to the First Amendment", Congressional Research Service Report 95-815, 2009، المتاح على الموقع التالي: www.fas.org/sgp/crs/misc/95-815.pdf.

(36) إنَّ الشواغل المتعلقة بحرية التعبير (على سبيل المثال، التعديل الأول على الدستور الأمريكي) هي التي تفسر عدم اعتبار بعض الأفعال العنصرية أفعالا غير مشروعة في الاتفاقية المتعلقة بالجريمة السيبرانية (مجلس أوروبا، مجموعة المعاهدات الأوروبية، الرقم ١٨٥)، في حين أنها مجرمة في البروتوكول الإضافي لاتفاقية الجريمة الإلكترونية المتعلق بتجريم أعمال العنصرية وكراهية الأجانب المرتكبة بواسطة النظم الحاسوبية (مجلس أوروبا، مجموعة المعاهدات الأوروبية، الرقم ١٨٩). انظر كذلك التقرير التفسيري للبروتوكول الإضافي المتاح على الموقع التالي: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

٢٢- وبالنظر إلى أنَّ الجريمة السيبرانية هي جريمة عبر وطنية بمعنى الكلمة،[٣٧] فإنَّ التعاون الدولي يمثل متطلبا جوهريا لإجراء تحقيقات وملاحقات قضائية ناجحة.[٣٨] ويستلزم التعاون الدولي الفعال مستوى معينا من الفهم المشترك للمسائل المعنية واعتماد نهوج مشتركة فيما يخص التشريعات بغية منع توفير ملاذات آمنة للمجرمين.[٣٩]

٢٣- سوف تتألّف الدراسة الخاصة بهذا الموضوع مما يلي:

(أ) تحليل الجهود المبذولة لاعتماد نهوج مشتركة في التشريعات الخاصة بالجريمة السيبرانية؛

(ب) عناصر أخرى فيما يتعلق باعتماد نهوج مشتركة في التشريعات الخاصة بالجريمة السيبرانية، بما في ذلك الجدّية المتصوَّرة لتطبيق قواعد حقوق الإنسان وتأثيرها؛

(ج) حصر السبل التي تنفّذ بها البلدان المعايير القانونية التي تضعها المنظمات الإقليمية وإجراء تحليل لتحديد الأساليب التي يمكن أن تساعد في كفالة اتساق النهوج المعتمدة؛

(د) تحليل مدى تأثير الاختلافات في التشريعات القانونية على التعاون الدولي.

(37) فيما يتعلق بنطاق الهجمات عبر الوطنية التي أسفرت عن أفدح الأضرار، انظر: A. D. Sofaer and S. E. Goodman, "Cyber crime and security: the transnational dimension", in *The Transnational Dimension of Cyber Crime and Terrorism*, A. D. Sofaer and S. E. Goodman, eds., Hoover National Security Forum Series (Stanford, California, Hoover Institution Press, 2001), p. 7، المتاح على الموقع التالي: http://media.hoover.org/documents/0817999825_1.pdf.

(38) فيما يتعلق بالحاجة إلى التعاون الدولي في مكافحة الجريمة السيبرانية، انظر: T. L. Putnam and D. D. Elliott, "International responses to cyber crime", in *Transnational Dimension of Cyber Crime and Terrorism*, A. D. Sofaer and S. E. Goodman, eds., Hoover National Security Forum Series (Stanford, California, Hoover Institution Press, 2001), pp. 35 ff.، المتاح على الموقع التالي: http://media.hoover.org/documents/0817999825_35.pdf؛ و Sofaer and Goodman, "Cyber crime and security: the transnational dimension".

(39) فيما يتعلق بمبدأ ازدواجية التجريم في التحقيقات الدولية، انظر: "United Nations Manual on the Prevention and Control of Computer-Related Crime", *International Review of Criminal Policy*, Nos. 43 and 44, 1994 (United Nations publication, Sales No. E.94.IV.5), para. 269، المتاح على الموقع التالي: www.uncjin.org/Documents/EighthCongress.html؛ وانظر: Judge Stein Schjolberg and Amanda M. Hubbard, "Harmonizing national legal approaches on cybercrime", paper prepared for the International Telecommunication Union, WSIS Thematic Meeting on Cybersecurity, Geneva, 28 June-1 July 2005, p. 5.

الموضوع ٥- التجريم

الخلفية

٢٤- يتطلّب التحقيق في الجريمة السيبرانية وملاحقة مرتكبيها بصورة فعّالة تجريم أفعال جديدة إذا كانت سلوكيات معينة غير مشمولة أصلاً بالتشريعات القائمة. فوجود تشريعات مناسبة ضروري ليس فقط من أجل إجراء تحقيقات وطنية، بل لأنه يمكن أن يؤثّر أيضا على التعاون الدولي، كما أُشير إليه أعلاه.

القانون الجنائي الموضوعي

٢٥- تشمل معظم الأطر الإقليمية الشاملة التي وُضعت للتصدّي للجريمة السيبرانية مجموعة من أحكام القانون الجنائي الموضوعي المصمَّمة لسد الثغرات الموجودة في التشريعات الوطنية في ذلك المجال. وتشمل الأحكام القياسية في هذه الأطر تجريم الوصول غير المشروع إلى البيانات واعتراضها والتدخل فيها بصورة غير مشروعة، والتدخل غير المشروع في النظم، وأعمال الاحتيال والتزوير الحاسوبية. ويمكن أن تذهب بعض النهوج إلى أبعد من ذلك، وتجرم الأفعال المتعلقة مثلا بإنتاج وتوزيع الأدوات (مثل البرامجيات أو الأجهزة) التي يمكن أن تستخدم لارتكاب جرائم سيبرانية أو للأغراض الإرهابية، والأفعال المرتبطة بالتعدِّي على الأطفال أو الاستمالة أو نشر خطاب الكراهية.

نطاق الدراسة

٢٦- سوف تستند الدراسة الخاصة بهذا الموضوع إلى نتائج دراسة الموضوع ١ المتعلق بظاهرة الجريمة السيبرانية، وسوف تتناول ما يلي:

(أ) حصر النهوج الوطنية والإقليمية المتبعة في تجريم الجرائم السيبرانية، بما في ذلك فيما يتعلق بالمشاركة فيها ومحاولة ارتكابها؛

(ب) تقييم الممارسات الفضلى فيما يتصل بالتجريم؛

(ج) تحليل الاختلافات في النهوج التي تأخذ بها مختلف النظم والتقاليد القانونية في تجريم الجرائم السيبرانية.

الموضوع ٦- الصلاحيات الإجرائية

الخلفية

٢٧- تحتاج هيئات إنفاذ القانون، من أجل إجراء تحقيقات فعالة، إلى إجراءات تحقيق تمكنها من اتخاذ التدابير اللازمة لتحديد هوية الجناة وجمع الأدلة المطلوبة للدعوى الجنائية.(٤٠) ويمكن أن تكون هذه التدابير هي نفسها التدابير المستخدمة في التحقيقات التقليدية غير المرتبطة بالجريمة السيبرانية. ولكن، بالنظر إلى أنه ليس من الضروري أن يكون الجاني حاضرا في مسرح الجريمة أو حتى على مقربة منه، فإنَّ من المرجح أن تُجرى التحقيقات في الجرائم السيبرانية بطريقة مختلفة عن التحقيقات التقليدية.(٤١)

تدابير التحقيق

٢٨- إضافةً إلى الأحكام المتعلقة بالجرائم السيبرانية الرئيسية، تتضمن أيضا معظم الأطر الإقليمية الشاملة التي وُضِعت للتصدّي للجريمة السيبرانية مجموعة من الأحكام المصمَّمة خصيصا لتيسير التحقيقات في الجرائم السيبرانية. وتتضمّن الأحكام القياسية إجراءات محدَّدة للتفتيش والضبط، والتعجيل في صون البيانات الحاسوبية، والكشف عن البيانات المخزونة، واعتراض بيانات المحتويات، وجمع البيانات عن حركة المعلومات.

٢٩- وتواجه هيئات إنفاذ القانون في المرحلة الحالية تكنولوجيات مطوَّرة حديثا ذات تأثير سلبي على أساليب التحقيق التقليدية. والكثير من تلك التحديات لم يتم التصدِّي لها بعد.

(40) فيما يتعلق بالنهوج المستندة إلى المستخدمين في مكافحة الجريمة السيبرانية، انظر: S. Görling, "The myth of user education", paper prepared for the Virus Bulletin Conference, Montreal, 11-13 October 2006، المتاح على العنوان التالي: www.virusbtn.com/conference/vb2006/abstracts/Gorling.xml. وانظر أيضا التعليقات التي قدمها جان بيير شوفينمان، وزير الداخلية الفرنسي، خلال أحد مؤتمرات مجموعة الثمانية بشأن الأمن والثقة في الفضاء السيبراني، عُقد في باريس في عام ٢٠٠٠: "بصورة أعم، علينا أن نثقف مستخدمي الإنترنت. فيتعين أن يفهموا جميعا ما الذي يمكنهم أو لا يمكنهم القيام به على الإنترنت، وعلينا أن نحذرهم من الأخطار المحتملة. فمع تزايد استخدام الإنترنت، علينا بطبيعة الحال أن نضاعف جهودنا في هذا الصدد".

(41) بالنظر إلى البروتوكولات المستخدمة في اتصالات الإنترنت وإمكانية استخدام الإنترنت في جميع أنحاء العالم، لا توجد حاجة تذكر إلى الوجود المادي في المكان الذي تقدم فيه الخدمات فعليا. وبالنظر إلى استقلال مكان الفعل عن مسرح الجريمة، يعد الكثير من الأفعال الجنائية المتعلقة بالإنترنت جرائم عبر وطنية. وفيما يتعلق باستقلالية مكان الفعل ونتائج الجريمة، انظر: "فهم الجريمة السيبرانية: دليل للبلدان النامية" (انظر الحاشية ١٣ أعلاه)، الفصل ٣-٢-٧.

نطاق الدراسة

٣٠- سوف تتألّف الدراسة الخاصة بهذا الموضوع مما يلي:

(أ) حصر أمثلة الحالات التي أبرزت التحقيقات في إطارها الحاجة إلى تدابير تحقيق خاصة بالجريمة السيبرانية؛

(ب) حصر مختلف الأحكام المتعلقة بالتحقيقات الواردة في الأُطر القانونية الإقليمية والوطنية؛

(ج) تقديم لمحة عامة عن احتياجات هيئات إنفاذ القانون الراهنة لأحكام تحقيق معيَّنة تتعلق بالجريمة السيبرانية للتصدي للتحديات التي تستحدثها التكنولوجيات الجديدة؛

(د) تحليل الاختلافات في نهج وضع أحكام التحقيق المتعلقة بالجريمة السيبرانية في مختلف النظم والتقاليد القانونية.

الموضوع ٧- التعاون الدولي

الخلفية

٣١- يتزايد عدد الجرائم السيبرانية ذات البعد الدولي،[٤٢] ولا سيما لأنَّ وجود مرتكبي هذه الجرائم في مكان وجود الضحية لم يعد لازما في كثير من الأحيان بالنظر إلى أنهم يرتكبون جرائمهم من خلال شبكة الإنترنت عبر الوطنية. وبسبب هذا الانفصال بين مكان الضحية ومكان الجاني وقدرة الجناة على التنقل، أصبح من الضروري أن تتعاون هيئات إنفاذ القانون والسلطات القضائية دوليا وأن تساعد الدولة صاحبة الاختصاص القضائي.[٤٣] ويمثل التعاون الدولي الفعال أحد أهم التحديات الرئيسية في مكافحة تلك الجريمة الآخذة في العولمة بشكليها التقليدي والسيبراني على السواء. وقد يكون التعاون الدولي صعبا بسبب الاختلافات القائمة في التشريعات والممارسات بين الدول وكذلك بسبب العدد المحدود نسبيا من المعاهدات والاتفاقات

(42) فيما يتعلق بالبعد عبر الوطني للجريمة السيبرانية، انظر: Mike Keyser, "The Council of Europe Convention on Cybercrime", *Journal of Transnational Law and Policy*, vol. 12, No. 2 (2003), p. 289، المتاح على الموقع التالي: www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf؛ و Sofaer and Goodman, "Cyber crime and security: the transnational dimension" (انظر الحاشية ٣٧ أعلاه)، pp. 1 ff.

(43) انظر في هذا السياق: *Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime and the Protocols Thereto* (منشورات الأمم المتحدة، رقم المبيع E.05.V.2)، ص ٢١٧، المتاح على الموقع التالي: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

المتاحة للدول بشأن التعاون الدولي.[٤٤] وعلاوة على ذلك، فإن ما ينبغي اعتباره مسألة دولية فيما يتعلق بالجريمة السيبرانية أمر ينبغي مناقشته والاتفاق عليه.

صكوك التعاون الدولي

٣٢- توجد مصادر مختلفة للأساس القانوني اللازم للتعاون الدولي الرسمي، مثل تسليم المطلوبين والمساعدة القانونية المتبادلة في المسائل الجنائية والتعاون لأغراض المصادرة. وقد تُشكِّل الأحكام المتعلقة بالتعاون الدولي جزءا من الاتفاقات الدولية والإقليمية، بما في ذلك اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.[٤٥]

نطاق الدراسة

٣٣- سوف تتألّف الدراسة الخاصة بهذا الموضوع مما يلي:

(أ) حصر النهوج القانونية المحلية لتعريف المسائل الدولية بالنسبة لإنفاذ القانون الجنائي بشأن الإنترنت؛

(ب) دراسة الخيارات فيما يتعلق بالقواعد القانونية الفعّالة، بما في ذلك القواعد الدولية العامة، وغيرها من تدابير مكافحة الجريمة السيبرانية؛

(ج) استبانة التحديات المتعلقة بالتعاون الدولي الفعال، وخصوصا تسليم المطلوبين والمساعدة القانونية المتبادلة، في قضايا الجرائم السيبرانية، بما في ذلك تطبيق ازدواجية التجريم والاختلافات في تدابير التحقيق؛

(د) حصر الأحكام الوطنية والدولية التي تتناول التعاون الدولي والمتعلقة بالتحقيقات والملاحقات القضائية في مجال الجرائم السيبرانية؛

---

(44) Carlos A. Gabuardi, "Institutional framework for international judicial cooperation: opportunities and challenges for North America", *Mexican Law Review*, vol. 1, No. 2 (2009), p. 156، المتاح على الموقع التالي: http://info8.juridicas.unam.mx/pdf/mlawrns/cont/2/cmm/cmm7.pdf.

(45) الأمم المتحدة، مجموعة المعاهدات، المجلد ٢٢٢٥، الرقم ٣٩٥٧٤؛ فيما يتعلق بالاتفاقية، انظر: Jennifer M. Smith, "An international hit job: prosecuting organized crime acts as crimes against humanity", *Georgetown Law Journal*, vol. 97, 2009, p. 1,118، المتاح على الموقع التالي: www.georgetownlawjournal.org/issues/pdf/97-4/Smith.PDF.

(هـ) حصر الأمثلة على الممارسات الفضلى الواردة في المعاهدات والترتيبات الثنائية والمتعددة الأطراف، بما في ذلك الدروس المستفادة من عمل شبكة نقاط الاتصال التي تعمل على مدار الساعة طوال أيام الأسبوع؛

(و) حصر قضايا الجرائم السيبرانية التي تنطوي على تعاون دولي؛

(ز) تحديد دور الوسائل غير الرسمية للتعاون من قبيل تبادل المعلومات الاستخباراتية وما يرتبط بذلك من تحديات؛

(ح) تقديم لمحة عامة عن الاحتياجات الراهنة للسلطات المعنية فيما يتعلق بالتعاون الدولي؛

(ط) استبانة ما هو جار من برامج تدريبية وتبادل للخبرات وأنشطة في مجال بناء القدرات وتقديم المساعدة التقنية، وبلورة أفكار للاضطلاع بالمزيد منها في المستقبل، بغية تعزيز القدرات في مجال العدالة الجنائية وتمكين البلدان من التعاون على المستوى الدولي.

الموضوع ٨- الأدلة الإلكترونية

الخلفية

٣٤- بالنظر إلى أنَّ المعلومات تخزَن باطّراد في شكل رقمي، أصبحت الأدلة الإلكترونية مهمة في التحقيقات المتعلقة بالجرائم السيبرانية والتحقيقات التقليدية على السواء. وأصبحت التكنولوجيا الحاسوبية والشبكية جزءا من الحياة اليومية في البلدان المتقدمة النمو، وهي تنحو هذا المنحى باطّراد في البلدان النامية أيضا. وقد أفضت زيادة قدرة التخزين في الأقراص الصلبة[٤٦] والتكلفة المنخفضة نسبيا[٤٧] لتخزين الوثائق الرقمية مقارنة بتخزين الوثائق المادية إلى زيادة عدد الوثائق الرقمية.[٤٨] واليوم، يوجد كم كبير من البيانات المخزنة بشكل رقمي

(46) D. Abramovitch, "A brief history of hard drive control", *IEEE Control Systems Magazine*, vol. 22, No. 3 (2002), pp. 28 ff.؛ و T. Coughlin, D. Waid and J. Porter, "The disk drive: 50 years of progress and technology innovation — the road to two billion drives"، *Computer Technology Review*, April 2005 المتاح على الموقع التالي:
www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf.

(47) S. M. Giordano, "Electronic evidence and the law", *Information Systems Frontiers*, vol. 6, No. 2 (2006), p. 161; S. D. Willinger and R. M. Wilson, "Negotiating the minefields of electronic discovery", *Richmond Journal of Law and Technology*, vol. 10, No. 5 (2004).

(48) Lange/Minster, Electronic Evidence and Discovery, p. 6.

فقط.[٤٩] ونتيجة لهذه الزيادة، أصبحت الوثائق الإلكترونية مثل الوثائق النصية وأفلام الفيديو الرقمية والصور الرقمية[٥٠] تؤدي دورا في التحقيقات المتعلقة بالجريمة السيبرانية والإجراءات ذات الصلة بها في المحاكم.[٥١]

القواعد المتعلقة بالأدلة الإلكترونية

٣٥- تثير الأدلة الإلكترونية عددا من التحديات على السواء في مرحلتي جمعها وقبولها كأدلة.[٥٢] فخلال عملية جمع الأدلة، يتعيَّن على المحققين أن يستوفوا إجراءات ومتطلبات معيَّنة، كالمعاملة الخاصة اللازمة لحماية سلامة البيانات. ويلزم أن تتوفّر لهيئات إنفاذ القانون تدابير محدَّدة لإجراء التحقيقات بنجاح. وتَوفُّر هذه التدابير مهمٌ بوجه خاص في حال عدم وجود أشكال الأدلة التقليدية مثل البصمات أو أقوال الشهود. وفي هذه الحالات، تغدو

(49) Chet Hosmer, "Proving the integrity of digital evidence with time", *International Journal of Digital Evidence*, vol. 1, No. 1 (2002), p. 1، المتاح على الموقع التالي: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

(50) فيما يتعلق بمقبولية الصور الرقمية وموثوقيتها، انظر: Jill Witkowski, "Can juries really believe what they see? New foundational requirements for the authentication of digital images", *Washington University Journal of Law and Policy*, vol. 10, 2002, pp. 267 ff.

(51) Michael Harrington, "A methodology for digital forensics", *Thomas M. Cooley Journal of Practical and Clinical Law*, vol. 7, 2004, pp. 71 ff؛ و Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 2nd ed. (London, Academic Press, 2004), p. 14. وفيما يتعلق بالأطر القانونية القائمة في مختلف البلدان، انظر: C. A. Rohrmann and J.S.A. Neto, "Digital evidence in Brazil", *Digital Evidence and Electronic Signature Law Review*, No. 5, 2008؛ و M. Wang, "Electronic evidence in China", *Digital Evidence and Electronic Signature Law Review*, No. 5, 2008؛ و P. Bazin, "An outline of the French Law on digital evidence", *Digital Evidence and Electronic Signature Law Review*, No. 5, 2008؛ و A. B. Makulilo, "Admissibility of computer evidence in Tanzania", *Digital Evidence and Electronic Signature Law Review*, No. 4, 2007؛ و R. Winick, "Search and seizures of computers and computer data", *Harvard Journal of Law and Technology*, vol. 8, No. 1 (1994), p. 76؛ و F. Insa, "Situation report on the admissibility of electronic evidence in Europe", in *Syllabus to the European Certificate on Cybercrime and E-Evidence*, 2008, p. 213.

(52) Casey, *Digital Evidence and Computer Crime* (انظر الحاشية ٥١)، ص ٩.

إمكانية النجاح في التعرف على هوية الجاني وملاحقته قضائيا مرهونة بجمع الأدلة الإلكترونية وتقييمها بصورة صحيحة.[٥٣]

٣٦- وتؤثّر الرقمنة أيضا على طريقة تعامل هيئات إنفاذ القانون والمحاكم مع الأدلة.[٥٤] ففي حين يكفي عرض الوثائق التقليدية في المحكمة، قد تتطلب الأدلة الرقمية تطبيق إجراءات خاصة، وقد لا تكون هذه الإجراءات مناسبة لتحويل تلك الأدلة الرقمية إلى أدلة تقليدية من قبيل النسخ المطبوعة من الملفات.[٥٥]

نطاق الدراسة

٣٧- سوف تتألّف الدراسة الخاصة بهذا الموضوع مما يلي:

(أ) حصر الأحكام والضمانات والمعايير المتعلقة بجمع الأدلة الإلكترونية وصونها وتخزينها وتحليلها ومقبوليتها؛

(ب) تحليل الاختلافات في النهوج، واستبانة المبادئ المشتركة فيما يخص الأدلة الإلكترونية في النظم والتقاليد القانونية المختلفة؛

(ج) جمع الممارسات الفضلى فيما يتعلق بالتدريب المتخصص وبناء القدرات وتبادل التكنولوجيا؛

(د) تحليل آلية تبادل الأدلة الرقمية عبر الحدود.

(53) فيما يتعلق بضرورة إضفاء الطابع الرسمي على التحاليل الجنائية الحاسوبية، انظر: R. Leigland and A. W. Krings, "A formalization of digital forensics", *International Journal of Digital Evidence*, vol. 3, No. 2 (2004).

(54) فيما يتعلق بصعوبات التعامل مع الأدلة الرقمية بتطبيق الإجراءات والمذاهب التقليدية، انظر: R. Moore, "To view or not to view: examining the plain view doctrine and digital evidence", *American Journal of Criminal Justice*, vol. 29, No. 1 (2004), pp. 57 ff.

(55) انظر: John R. Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 2nd ed. (Hingham, Massachusetts, Charles River Media, 2005), p. 3. وفيما يتعلق بالمناقشة السابقة بشأن النسخ المطبوعة، انظر: Robinson, The admissibility of computer Printouts under the business records exception in Texas, *South Texas Law Journal*, vol. 12, 1970, pp. 291 ff.

الموضوع ٩- أدوار ومسؤوليات مقدِّمي الخدمات والقطاع الخاص

الخلفية

٣٨- يتوقّف منع الجرائم السيبرانية والتحقيق فيها على عدد من العناصر المختلفة. وارتكابَ جريمة سيبرانية، حتى وإن كان الجاني يعمل بمفرده، يشمل تلقائياً عدداً من الأشخاص والمؤسسات التجارية. فبالنظر إلى بنية الإنترنت، يتطلب نقل رسالة إلكترونية بسيطة خدمات عدد من مقدِّمي الخدمات، مثل مقدِّمي خدمات البريد الإلكتروني، ومقدِّمي خدمات الوصول إلى الإنترنت، ومقدِّمي أجهزة التوجيه التي تحيل الرسالة الإلكترونية إلى متلقيها. والوضع مشابه فيما يتعلق بتنزيل الأفلام التي تحتوي على مواد يُستغل فيها الأطفال. فعملية تنزيل الأفلام تشمل مقدِّم المحتوى الذي يحمِّل الصور (موقع شبكي مثلا)، والمقدِّم المضيف الذي يوفِّر وسيطة التخزين للموقع الشبكي، وأجهزة التوجيه التي تحيل الملفات إلى المستخدمين، وأخيرا مقدِّم خدمات الوصول الذي يمكِّن المستخدم من استعمال الإنترنت.

٣٩- وبينما كثيرا ما يجري التركيز على كفالة وجود التشريعات المناسبة، فإن قطاع الصناعة الخاص يواصل أداء دور هام في منع الجريمة السيبرانية والمساعدة في التحقيقات ذات الصلة على السواء. بيد أن مشاركته في التحقيقات المتصلة بالجريمة السيبرانية محفوفة بعدد من التحديات.

المسائل القانونية

٤٠- إنَّ تعذُّر ارتكاب الجريمة السيبرانية دون مشاركة مقدِّمي الخدمات، إضافة إلى أنَّ مقدِّمي الخدمات ليست لديهم القدرة في الكثير من الأحيان على منع ارتكاب الجرائم السيبرانية، يثير تساؤلات بشأن ما إذا كان ينبغي الحد من مسؤولية مقدِّمي الخدمات. والإجابة على هذا السؤال حاسمة بالنسبة للتطور الاقتصادي للبنى التحية لتكنولوجيا المعلومات والاتصالات.

٤١- وكثيرا ما تعتمد الجهود التي تبذلها هيئات إنفاذ القانون على تعاون مقدِّمي خدمات الإنترنت. ويثير ذلك بعض الشواغل، لأنَّ فرض مسؤولية على مقدِّمي الخدمات عن الأفعال التي يرتكبها مستخدمو خدماتهم أو الحد من تلك المسؤولية قد يؤثّر على التعاون والدعم الذي يقدمونه في إطار التحقيقات في الجرائم السيبرانية وفي منع تلك الجرائم فعليا.

دور قطاع الصناعة

٤٢- إنَّ دورَ قطاع الصناعة في معالجة مسألة الجريمة السيبرانية معقَّدٌ؛ وقد يتدرّج من وضع حلول وتنفيذها لحماية خدماته هو من إساءة الاستعمال في ارتكاب الجرائم إلى حماية

المستخدمين ودعم التحقيقات. وكثيرا ما تكون تدابير الحماية الذاتية التي يعتمدها قطاع الصناعة مكوَّناً منطقياً من استراتيجيات تجارية شاملة، ولا تتطلّب عموما أساسا قانونيا محدَّدا ما دامت لا تنطوي على تدابير مكافحة فاعلة غير قانونية. ولا تمثّل تدابير الحماية التي تتخذ بالنيابة عن المستخدمين مشكلات كذلك، شريطة أن تتخذ بموافقة المستخدم. بيد أنّ إشراك قطاع الصناعة في التحقيقات الجنائية أثار تحديات في العديد من البلدان، وتم في هذا الصدد اعتماد نهوج مختلفة. فقد عمدت بعض البلدان إلى إشراك قطاع الصناعة في التحقيقات الجنائية على أساس طوعي بحت، ووضعت مبادئ توجيهية لتيسير التعاون بين قطاع الصناعة وهيئات إنفاذ القانون. وثمة بلدان أخرى اعتمدت نهجا مختلفا فرضت فيه على قطاع الصناعة التزامات قانونية بالتعاون مع هيئات إنفاذ القانون في التحقيقات الجنائية.

نطاق الدراسة

٤٣- سوف تتألّف الدراسة الخاصة بهذا الموضوع مما يلي:

(أ) النهوج والممارسات فيما يخص مسؤولية مقدِّمي الخدمات، بما في ذلك التمييز بين الأنواع المختلفة من مقدِّمي الخدمات؛

(ب) رسم خريطة دور القطاع الخاص، بما في ذلك مقدِّمو الخدمات، وطبيعته ووظائفه؛

(ج) الممارسات التي يتبعها القطاع الخاص في مجال منع الجريمة السيبرانية والتحقيق فيها؛

(د) الممارسات ذات الصلة بالتعاون بين القطاع الخاص وهيئات إنفاذ القانون في منع الجريمة السيبرانية والتحقيق فيها؛

(هـ) قدرة مقدِّمي الخدمات الوطنيين ومتعدِّدي الجنسيات على مساعدة هيئات إنفاذ القانون على منع الجريمة السيبرانية والتحقيق فيها؛

(و) تخصيص تكاليف الجريمة السيبرانية؛

(ز) تقييم مَواطن القوة والضعف في النهوج القائمة.

الموضوع ١٠- منع الجريمة وقدرات العدالة الجنائية وتدابير التصدّي الأخرى للجريمة السيبرانية

الخلفية

٤٤- كثيرا ما يركّز النقاش حول كيفية التصدّي للجريمة السيبرانية على التدابير القانونية، في حين تأخذ استراتيجيات مكافحة الجريمة السيبرانية عموما بنهج أكثر شمولا.

سبل التصدّي الأخرى

٤٥- إلى جانب التدابير القانونية، تشمل سبل التصدّي الأخرى للجريمة السيبرانية اعتماد تدابير لمنع الجريمة وتطوير البنى التحتية اللازمة للتحقيق في الجرائم وملاحقة مرتكبيها (مثل توفير المعدات والموظفين)، وتدريب الخبراء القائمين على مكافحة الجريمة السيبرانية، ووضع الممارسات الفضلى، وتثقيف مستخدمي الإنترنت، وإيجاد الحلول التقنية لمنع الجريمة السيبرانية أو التحقيق فيها.

نطاق الدراسة

٤٦- سوف تتألّف الدراسة الخاصة بهذا الموضوع مما يلي:

(أ) تقديم لمحة عامة عن النهوج الأخرى المتبعة في التصدّي للجريمة السيبرانية؛

(ب) تدابير منع الجريمة السيبرانية؛

(ج) تحديد الوسائل الكفيلة بقياس مدى نجاح هذه النهوج؛

(د) تحليل العلاقات بين تدابير التصدّي المختلفة وإمكانيات اعتماد توليفات منها؛

(هـ) الدور الممكن للأوساط الأكاديمية، وخصوصا من خلال تطوير المناهج الملائمة وإجراء البحوث بشأن ظاهرة الجريمة السيبرانية.

الموضوع ١١- المنظمات الدولية

الخلفية

٤٧- في سبعينيات وثمانينيات القرن العشرين، كانت أغلبية النهوج القانونية المتعلقة بالتصدّي للجريمة السيبرانية توضع على الصعيد الوطني. وفي التسعينيات، بدأت معالجة مسألة الجريمة السيبرانية في إطار المنظمات الإقليمية والدولية، بما في ذلك من خلال الجمعية العامة، التي

اعتمدت على مرّ السنين عدة قرارات بشأن الجريمة السيبرانية،[٥٦] والكومنولث (القانون النموذجي بشأن الجريمة السيبرانية والتوسيع المحتمل لنطاق خطة هراري لكي تشمل البيانات الإلكترونية) ومجلس أوروبا (الاتفاقية المتعلقة بالجريمة السيبرانية) والاتحاد الأوروبي (القرار الإطاري بشأن الاعتداء على نظم المعلومات والاتفاقية التي وضعها المجلس وفقا للمادة ٣٤ من معاهدة الاتحاد الأوروبي بشأن المساعدة المتبادلة في المسائل الجنائية بين الدول الأعضاء في الاتحاد الأوروبي) وكومنولث الدول المستقلة (اتفاق عام ٢٠٠١ بشأن التعاون بين بلدان كومنولث الدول المستقلة لمكافحة الجرائم في مجال المعلومات الحاسوبية) ومنظمة الدول الأمريكية، ومنظمة شنغهاي للتعاون. وقد قامت منظمات دولية، بما فيها الاتحاد الدولي للاتصالات، الذي اضطلع بأنشطة في إطار البرنامج العالمي للأمن السيبراني، ومكتب الأمم المتحدة المعني بالمخدرات والجريمة بجمع بيانات وإعداد دراسات.

مواءمة المعايير

٤٨- لقد ثبت نجاح وضع معايير مفردة موحدة وحيدة فيما يتعلق بالبروتوكولات التقنية، ويثير ذلك تساؤلاً بشأن كيفية تجنب التعارض بين مختلف النهوج الدولية.[٥٧] وقد اعتُمد أكثر النهوج شمولاً في اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية وقانون الكومنولث النموذجي بشأن الجريمة السيبرانية، حيث يشملان القانون الجنائي الموضوعي والقانون الإجرائي والتعاون الدولي. ويُمكن في إطار هذا الموضوع دراسة الأُطر القائمة لتحديد نطاقها ومَواطن قوتها وضعفها وأي ثغرات محتملة فيها.

نطاق الدراسة

٤٩- سوف تتألّف الدراسة الخاصة بهذا الموضوع مما يلي:

(أ) حصر الممارسات الفضلى المتبعة في المنظمات الإقليمية والدولية، بما فيها الأمم المتحدة؛

(ب) استبانة مَواطن القوة والضعف في النهوج القائمة؛

(ج) تحليل الثغرات في النهوج القانونية الدولية القائمة.

---

(56) على سبيل المثال، قرارات الجمعية العامة ٤٥/١٢١، و٥٥/٦٣، و٥٦/١٢١، و٦٠/١٧٧.

(57) للاطلاع على التفاصيل، انظر: M. Gercke, "National, regional and international legislative approaches in the fight against cybercrime", *Computer Law Review International*, 2008, pp. 7 ff.

الموضوع ١٢- المساعدة التقنية

الخلفية

٥٠- خلافا لما يُعتقد أحيانا، ليست الجريمة السيبرانية مشكلة تمس بصورة رئيسية البلدان المتقدمة. ففي عام ٢٠٠٥، تجاوز عدد مستخدمي الإنترنت في البلدان النامية عددهم في البلدان الصناعية للمرة الأولى.(٥٨) وبما أنَّ أحد الأهداف الأساسية لاستراتيجيات مكافحة الجريمة السيبرانية هو الحيلولة دون وقوع مستخدمي الإنترنت ضحية للجريمة السيبرانية، فإنَّه لا يمكن التقليل من أهمية مكافحة الجريمة السيبرانية في البلدان النامية. ومن المهم أيضا أن تُؤخذ في الاعتبار مسألةُ الاختلاف الممكن في وقع الجريمة السيبرانية على البلدان النامية والبلدان المتقدمة النمو. ففي عام ٢٠٠٥، نشرت منظمة التعاون والتنمية في الميدان الاقتصادي تقريرا يحلل أثر الرسائل الإلكترونية التطفلية على البلدان النامية،(٥٩) خُلِص فيه إلى أنَّ البلدان النامية كثيرا ما تفيد بأنَّ مستخدمي الإنترنت فيها يعانون أكثر من غيرهم في البلدان المتقدمة النمو من آثار تلك الرسائل وإساءة استخدام الإنترنت.

المساعدة التقنية

٥١- يتطلب البعد عبر الوطني للجريمة السيبرانية من جميع البلدان أن تعمل بطريقة فعّالة ومنسّقة. وللبلدان المتقدمة النمو والبلدان النامية مصلحة مشتركة في توفير المساعدة التقنية. ومنع توفير ملاذات آمنة لمرتكبي الجرائم السيبرانية من التحديات الرئيسية في سياق مكافحة الجريمة السيبرانية.(٦٠) ومن ثم، أصبح بناء القدرات في البلدان النامية لتمكينها من مكافحة الجريمة السيبرانية مهمة رئيسية من مهام المجتمع الدولي.

٥٢- وتتجسّد أهمية المساعدة التقنية في إعلان سلفادور الذي اعتمده مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية المعقود في عام ٢٠١٠، الذي أوصى بأن يقدِّم مكتب

(58) انظر: Development Gateway's Special Report, *Information Society – The Next Steps* (2005).

(59) "Spam issues in developing countries" (انظر الحاشية ٣٤ أعلاه).

(60) عولجت هذه المسألة في عدد من المنظمات الدولية. وينص قرار الجمعية العامة ٥٥/٦٣ على أنه "ينبغي للدول أن تكفل عدم توفير قوانينها وممارساتها ملاذا آمنا للذين يسيئون استعمال تكنولوجيا المعلومات لأغراض إجرامية". والنص الكامل للقرار متاح على الموقع التالي: http://www.unodc.org/pdf/crime/a_res_55/res5563a.pdf. وتشدِّد المبادئ وخطة العمل لمكافحة جريمة التكنولوجيا المتطورة المعتمدة في اجتماع وزراء العدل والداخلية في مجموعة الثمانية، الذي عُقد في واشنطن العاصمة في ١٠ كانون الأول/ديسمبر ١٩٩٧، على "ضرورة القضاء على الملاذات الآمنة لمن يسيئون استخدام تكنولوجيا المعلومات".

الأمم المتحدة المعني بالمخدرات والجريمة إلى الدول، بناءً على طلبها، المساعدة التقنية في مجال مكافحة الجريمة السيبرانية. واقتُرِح فيه أيضا النظر في إعداد خطة عمل بشأن بناء القدرات على الصعيد الدولي توضع بالتعاون مع جميع الشركاء المعنيين. وينبغي أن تبقى المساعدة التقنية محدَّثة وأن تقدَّم على أساس مستمر.

نطاق الدراسة

٥٣- سوف تتألف الدراسة الخاصة بهذا الموضوع مما يلي:

(أ) استبانة العناصر والمبادئ الأساسية للمساعدة التقنية في سياق معالجة الجريمة السيبرانية؛

(ب) حصر الدورات التدريبية القائمة في مجال الجريمة السيبرانية على المستوى الوطني والإقليمي والدولي؛

(ج) استبانة الممارسات الفضلى المتبعة في تقديم جوانب المساعدة التقنية المتصلة بالجريمة السيبرانية.

المرفق الثاني

منهجية الدراسة

١- بغية النهوض بولاية فريق الخبراء فيما يتعلق بالدراسة، تم إعداد البنية المبيَّنة أدناه لتيسير إجراء الدراسة التي سيُضطلع بها تحت رعاية فريق الخبراء.

٢- وسوف يكون من حق كل بلد تقديم آرائه التي سيجري تجسيدها في الدراسة.

٣- وسوف يكلَّف مكتب الأمم المتحدة المعني بالمخدرات والجريمة بإعداد الدراسة، بما في ذلك إعداد استبيان وجمع البيانات وتحليلها وإعداد مشروع لنص الدراسة. وتحقيقا لتلك المهمة، سيستند المكتب إلى خبراته الداخلية وإلى القدرات المتاحة من مختلف فروعه المواضيعية (شعبة شؤون المعاهدات، فرع البحوث وتحليل السياسات). ولذلك الغرض، لا بد من إتاحة الموارد الملائمة من خارج الميزانية بما يمكِّن المكتب من أداء تلك الوظائف بكفاءة. ولمساعدة الأمانة على ضمان أخذ الخبرات والنظم والاحتياجات التكنولوجية الرئيسية في الحسبان على النحو المناسب، تقدِّم كل مجموعة إقليمية إلى الأمانة أسماء خبراء حكوميين (لا يتعدّون الستّة) مشفوعة بمعلومات عن كيفية الاتصال بهم ومجالات خبراتهم. وسوف تستعين الأمانة بمشورة الخبراء كمورد مساعد حسب الاقتضاء وعلى أساس كل حالة على حدة.

٤- وسوف تقدِّم الأمانة إلى مكتب فريق الخبراء بانتظام معلومات محدَّثة عن العملية وتستشيره بشأنها، وتتولى تعميم محاضر المشاورات على الدول الأعضاء. ولا يُقصد بإعداد قائمة الخبراء تشكيل أي فريق خبراء محدود العضوية أو أجهزة أخرى موازية أو فرعية لفريق الخبراء.

٥- ولأغراض جمع المعلومات، سيتولى المكتب إعداد استبيان لتوزيعه على الدول الأعضاء والمنظمات الحكومية الدولية وكيانات القطاع الخاص (انظر الإطار الزمني الإرشادي أدناه) يتألف من أداة استقصائية وحيدة تستند إلى الخطوط العريضة المتضمَّنة في ورقة المفاهيم/العمل للاجتماع الأول لفريق الخبراء، بصيغتها المعدَّلة، وإلى توصيات الاجتماع الأول لفريق الخبراء كما وردت في تقريره.

٦- وفي مرحلة ثانية، سوف تقوم الأمانة، حسب الاقتضاء، وآخذة الحاجة لإيجاد تمثيل متوازن للمناطق المختلفة في الاعتبار، باستشارة ممثلين من القطاع الخاص، بمن فيهم ممثلو مقدِّمي خدمات الإنترنت ومستخدمي الخدمات وغيرهم من الجهات الفاعلة المعنية؛ وممثلون من الأوساط الأكاديمية، من البلدان المتقدمة النمو والبلدان النامية على السواء؛ وممثلون من المنظمات الحكومية الدولية ذات الصلة.

الإطار الزمني الإرشادي

كانون الثاني/يناير ٢٠١١: التوجّهات والمبادئ التوجيهية في مجال السياسات التي يوفرها الاجتماع الأول لفريق الخبراء. اعتماد مواضيع الدراسة ومنهجيتها وإطارها الزمني.

شباط/فبراير – نيسان/أبريل ٢٠١١: تحديد هوية الخبراء الذين سيساعدون مكتب الأمم المتحدة المعني بالمخدرات والجريمة في إجراء الدراسة (انظر أعلاه). تسليم الأسماء إلى مكتب فريق الخبراء. الإبلاغ بأسماء الخبراء الحكوميين عن طريق المجموعات الإقليمية.

نيسان/أبريل ٢٠١١: الدورة العشرون للجنة منع الجريمة والعدالة الجنائية. توزيع مشروع الاستبيان الذي أعدّه المكتب لجمع المعلومات. طلب الملاحظات/التعليقات من الدول الأعضاء. مشاورات بالاتصال الحاسوبي المباشر لتلقّي التعليقات من أعضاء فريق الخبراء. إقرار اللجنة بنتائج الاجتماع الأول لفريق الخبراء والعمل المستقبلي، حسبما اقتُرح في الاجتماع الأول.

منتصف حزيران/يونيه ٢٠١١: آخر موعد لتسليم التعليقات على الاستبيان.

منتصف تموز/يوليه ٢٠١١: وضع الاستبيان في صيغته النهائية وتوزيعه على الدول الأعضاء. وسيُرسل الاستبيان أيضا عن طريق رسائل منفصلة إلى المنظمات الحكومية الدولية وممثلين من القطاع الخاص والمؤسسات الأكاديمية من أجل دعوتهم لتوفير المعلومات والردّ على أسئلة الاستبيان التي تقع في نطاق اهتمامهم. وفيما يتعلق بالقطاع الخاص بصورة خاصة، سيتم توفير الضمانات بأن أي بيانات يُتحصّل عليها ستبقى سرية ولن يُذكر مصدرها في حال نشرها.

منتصف تموز/يوليه – أواخر كانون الأول/ديسمبر ٢٠١١: جمع البيانات وتصنيفها (خمسة أشهر ونصف، مع رسالة تذكير في منتصف الفترة ترسلها الأمانة في أوائل تشرين الأول/أكتوبر ٢٠١١).

أوائل كانون الأول/ديسمبر ٢٠١١: الاجتماع الثاني لفريق الخبراء، بالتزامن مع الدورة العشرين المستأنفة للجنة الجريمة. إحاطة بالتقدم المحرز. تقرير مؤقت لعلم لجنة الجريمة في دورتها الحادية والعشرين (نيسان/أبريل ٢٠١٢).

نيسان/أبريل ٢٠١٢: تقديم التقرير المرحلي المؤقت إلى لجنة الجريمة في دورتها الحادية والعشرين.

منتصف كانون الثاني/يناير ٢٠١٢ – تموز/يوليه ٢٠١٢: تحليل البيانات وصياغة مشروع نص الدراسة. وضع الصيغة النهائية لمشروع نص الدراسة.

آب/أغسطس ٢٠١٢: توزيع مشروع نص الدراسة على أعضاء فريق الخبراء لضمان التحضير للاجتماع الثالث لفريق الخبراء في حينه.

تشرين الأول/أكتوبر ٢٠١٢: الاجتماع الثالث لفريق الخبراء لاستعراض مشروع الدراسة وتنقيحه واعتماده.

نيسان/أبريل ٢٠١٣: تسليم الدراسة إلى لجنة الجريمة في دورتها الثانية والعشرين للنظر فيها.