20 December 2010
Arabic
Original: English

فريق الخبراء المعني بالجريمة السيبرانية
فيينا، ١٧-٢١ كانون الثاني/يناير ٢٠١١

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

أولا- مقدِّمة

١- ناقشت الدول الأعضاء، أثناء مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، المعقود 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.

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

مشكلة الجريمة السيبرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدّي لتلك الجريمة، 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 ما يوجد من تدابير التصدّي للجريمة السيبرانية واقتراح تدابير جديدة للتصدّي لها).

٤- وبغية إعداد هيكل الدراسة، تم تحويل هذه الأبعاد الثلاثة (الجوانب الجوهرية والمنظور ومحور التركيز) إلى ١٣ موضوعا تتوافق مع الولاية المنصوص عليها في إعلان سلفادور. وصُنِّفت هذه المواضيع الثلاثة 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) الجرائم السيبرانية (الموضوع ١)؛

(ب) الإحصاءات (الموضوع ٢)؛

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

التدابير القانونية للتصدّي للجريمة السيبرانية (المواضيع ٤ إلى ٩)

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

(أ) مواءمة التشريعات (الموضوع ٤)؛

(ب) القانون الجنائي الموضوعي (الموضوع ٥)؛

(ج) آليات التحقيق (الموضوع ٦)؛

(د) التعاون الدولي (الموضوع ٧)؛

(هـ) الأدلة الإلكترونية (الموضوع ٨)؛

(و) المسؤولية (الموضوع ٩).

التصدّي للجريمة السيبرانية خارج دائرة التدابير القانونية (الموضوع ١٠)

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

تدابير التصدّي من جانب المجتمع الدولي (الموضوع ١١)

٨- يدعو إعلانُ سلفادور إلى تحليل ما تتخذه الدول الأعضاء والمجتمع الدولي والقطاع الخاص من تدابير للتصدّي للجريمة السيبرانية. ولئن كانت المسائلُ المتعلقة بالتدابير القانونية التي يتخذها المجتمع الدولي للتصدّي للجريمة السيبرانية مشمولة تحت عنوان التدابير القانونية، فإنَّ من شأن تناول هذه التدابير تحت عنوان منفصل خاص بها 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 من المجالات المعيَّنة التي ستتناولها الدراسة الشاملة.

تدبير التصدّي من جانب القطاع الخاص (الموضوع ١٣)

١٠- سبقت الإشارة أعلاه إلى أنَّ إعلان سلفادور يوصي أيضا بأن تتضمّن الدراسة الشاملة تحليلا لتدبير التصدّي التي يتخذها القطاع الخاص.

ثانيا- عرض مفصَّل للمواضيع

الموضوع ١- ظاهرة الجريمة السيبرانية

الخلفية

١١- يُستخدَم المصطلحان "الجريمة الحاسوبية"، وبصفة أكثر تحديدا "الجريمة السيبرانية"، لوصف فئة معيَّنة من السلوك الإجرامي. وتَتَّخذ الجرائمُ أشكالا مختلفة ابتداءً من أفعال ذات مضمون غير مشروع إلى بعض أشكال الجرائم الاقتصادية. وتَتَّصل بهذه الفئة من السلوك الإجرامي تحدياتٌ من ضمنها على السواء اتساعُ طائفة الجرائم المندرجة فيها والتطوّر الدينامي للأساليب الجديدة في ارتكاب الجرائم أيضا.

تطوُّر الجريمة الحاسوبية والجريمة السيبرانية

١٢- في ستينات القرن العشرين، عندما ظهرت النظم الحاسوبية العاملة بالترانزيستور وأصبحت الحواسيب تُلاقي مزيداً من الرواج،[١] تم التركيز في تجريم الأفعال المرتكَبة على الأضرار المادية التي تلحق بالنظم الحاسوبية والبيانات المخزَّنة فيها.[٢] واتَّسمت السبعينات 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 الثمانينات، زاد رواج الحواسيب الشخصية أكثر فأكثر، ولأول مرة في التاريخ، أصبحت طائفة واسعة من البنى التحتية البالغة 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، كان

---

(1) فيما يتعلق بالتحديات ذات الصلة، انظر Slivka/Darrow; Methods and Problems in Computer Security, Journal of Computers and Law, 1975, p. 217 et seq.

(2) McLaughlin, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, vol. 2, p. 217 et seq.

(3) Gemignani, Computer Crime: The Law in '80, Indiana Law Review, vol. 13, 1980, p. 681.

(4) McLaughlin, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, vol. 2, p. 217 et seq.

(5) Freed, Materials and cases on computer and law, 1971, p. 65.

(6) Bequai, The Electronic Criminals – How and why computer crime pays, Barrister, vol. 4, 1977, p. 8 et seq.

(7) Criminological Aspects of Economic Crimes, 12th Conference of Directors of Criminological Research Institutes, Council of Europe, Strasbourg, 1976, p. 225 et seq; Staff Study of Computer Security in Federal Programs; Committee on Governmental Operations, the 95th Congress 1 Session, United States Senate, February 1977.

(8) McLaughlin, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, vol. 2, p. 217 et seq; Bequai, Computer Crime: A Growing and Serious Problem, Police Law Quarterly, vol. 6, 1977, p. 22.

(9) Computer Abuse: The Emerging Crime and the Need for Legislation, Fordham Urban Law Journal, 1983, p. 73.

(10) BloomBecker, The Trial of Computer Crime, Jurimetrics Journal, vol. 21, 1981, p. 428; Schmidt, Legal Proprietary Interests in Computer Programs: The American Experience, Jurimetrics Journal, vol. 21,

من شأن البدء في تربيط النظم الحاسوبية تمكين الجاني من الدخول إلى النظم الحاسوبية دون أن يكون موجودا في مسرح الجريمة.[١١] وأفضى استحداث الواجهة البينية البيانية (World Wide Web (الشبكة العالمية)) في التسعينات، التي أعقبها التزايد السريع في عدد مستخدمي الإنترنت، إلى ظهور أساليب جديدة من السلوك الإجرامي. فبعد أن كان توزيع المواد الإباحية عن 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 "التصيد الاحتيالي"،[١٣] و"الاعتداءات البوتنتية"[١٤] والاستخدامات

1981, p. 345 et seq. Denning, Some Aspects of Theft of Computer Software, Auckland University Law Review, vol. 4, 1980, p. 273 et seq; Weiss, Pirates and Prizes: The Difficulties of Protecting Computer Software, Western State University Law Review, vol. 11, 1983, p. 1 et seq; Bigelow, The Challenge of Computer Law, Western England Law Review, vol. 7, 1985, p. 401; Thackeray, Computer-Related Crimes, Jurimetrics Journal, 1984, p. 300 et seq.

(11) Yee, Juvenile Computer Crime – Hacking: Criminal and Civil Liability, Comm/Ent Law Journal, vol. 7, 1984, p. 336 et seq; Who is Calling your Computer Next? Hacker!, Criminal Justice Journal, vol. 8, 1985, p. 89 et seq; The Challenge of Computer-Crime Legislation: How Should New York Respond?, Buffalo Law Review, vol. 33, 1984, p. 777 et seq.

(12) Child Pornography, CSEC World Congress Yokohama Conference, 2001, p. 17; Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, United States. House of Representatives, 109th Congress, 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 من 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، ٢٠٠٩، الفصل ٢-٨-٤.

(14) نسبةً إلى مصطلح "Botnets" (بوتنت) وهو تعبير وجيز يشير إلى مجموعة حواسيب دُسَّ فيها برنامج يخضع لتحكُّم خارجي. وللاطلاع على مزيد من التفاصيل، انظر Wilson, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, p. 4.

المستجدة للتكنولوجيا مثل "بروتوكول نقل الصوت عبر الإنترنت" (VoIP)[١٥] و"الحوسبة السحابية"،[١٦] التي تخلق صعوبات أمام إنفاذ القانون.

نطاق الدراسة

١٣- 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 التي لم تُجرَّم بعد؛

(ج) استعراض الجرائم المُختَلطة (مثل التصيُّد الاحتيالي) واتجاهاتها في المستقبل؛

(د) حصر الحالات ذات الصلة؛

(هـ) تعريف الجريمة السيبرانية وأنماطها؛

(و) آليات منع الجريمة (تقنيا)؛

(ز) النظر في أهمية تعريف الجريمة السيبرانية؛

(ح) الاعتبارات المتعلقة بإمكانية إنهاء التجريم باعتبار ذلك حلا لبعض الجرائم السيبرانية.

الموضوع ٢- المعلومات الإحصائية

الخلفية

١٤- تُوفِّر إحصاءاتُ الجرائم أساساً لما يجريه صنّاع السياسات والأوساط الأكاديمية من مناقشات ومن عمليات لاتخاذ القرارات في هذا الصدد.[١٧] كما أنَّ من شأن الحصول على معلومات دقيقة عن حقيقة مدى انتشار الجريمة السيبرانية أن يمكِّن هيئات إنفاذ القانون من

(15) Simon/Slay, "Voice over IP: Forensic Computing Implications", 2006.

(16) Velasco San Martin, Jurisdictional Aspects of Cloud Computing, 2009; Gercke, Impact of Cloud Computing on Cybercrime Investigation, published in Taeger/Wiebe, Inside the Cloud, 2009, p. 499 et seq.

(17) Collier/Spaul, Problems in Policing Computer Crime, Policing and Society, 1992, vol. 2, p. 308، متاح على الموقع التالي: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf.

تحسين استراتيجياتها الخاصة بالتصدّي للجريمة السيبرانية، وردع الاعتداءات المحتملة وكفالة سنّ تشريعات أكثر ملاءمة وفعالية.

الوضعُ الراهن للإحصاءات المتعلقة بالجريمة السيبرانية

١٥- تُستَقَى المعلوماتُ المتعلقة بمدى انتشار الجرائم بوجه عام من الإحصاءات والدراسات الاستقصائية الخاصة بالجرائم.(١٨) ويطرح هذان النوعان من المصادر تحديات عند استخدامهما في وضع توصيات السياسات العامة. ففي المقام الأول، تُوضَع إحصاءات الجريمة عموما على المستوى الوطني، ولا تجسّد نطاق الانتشار على الصعيد الدولي. ولئن كان يمكن نظريا تجميع البيانات من مختلف الدول، فإنَّ هذا النهجَ لن يسفر عن معلومات موثوقة بسبب اختلاف التشريعات وممارسات تسجيل الإحصاءات.(١٩) فتجميعُ إحصاءات الجريمة الوطنية ومقارنتها يستلزمان حدّا مُعيَّناً من التوافق(٢٠) لا يتوفّر فيما يخص الجريمة السيبرانية. وحتى في الحالات التي تكون فيها الجرائم السيبرانية مسجَّلة، لا تكون بالضرورة مدرجة على حدة.(٢١)

١٦- وثانيا، لا يمكن للإحصاءات أن تجسّد إلا الجرائم المكتشفة والمبلغ عنها.(٢٢) وفيما يتصل بالجريمة السيبرانية على وجه الخصوص، هناك شواغل لأن عدد الحالات غير المبلغ عنها يبدو مرتفعا.(٢٣) وقد تخشى المؤسسات التجارية أن يؤثر هذا النوع من الدعاية السلبية على

(18) فيما يتعلق ببروز أهمية إحصاءات الجريمة، انظر: Osborne/Wernicke, Introduction to Crime Analysis, 2003, p.1 et seq، المتاح على الموقع التالي: www.crim.umontreal.ca/cours/cri3013/osborne.pdf.

(19) انظر في هذا السياق: Overcoming barriers to trust in crimes statistics, United Kingdom Statistics Authority, 2009, p. 9، المتاح على الموقع التالي: www.statisticsauthority.gov.uk/.../overcoming-barriers-to-trust-in-crime-statistics--england-and-wales---interim-report.pdf.

(20) انظر Alvazzi del Frate, Crime and criminal justice statistics challenges in Harrendorf/Heiskanen/Malby, International Statistics on Crime and Justice, 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, Oct. 2006, p. 3.

(22) فيما يتعلق بالتحديات ذات الصلة، انظر: Kabay, Understanding Studies and Surveys of Computer Crime, 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 Heise News بتاريخ ٢٧ تشرين الأول/أكتوبر ٢٠٠٧،

سمعتها.[٢٤] فحين تُعلن شركة أنَّ هناك من نجح في اختراق خادومها، قد يفقد الزبائن الثقة بها، فتترتّب على ذلك تكاليف أكبر حتى من 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 يجدون مبرّرا كافيا للإبلاغ عن الجرائم.[٢٦] وبما أنَّ أتمتة هجمات الجريمة السيبرانية تُمكِّن المجرمين السيبرانيين من وضع استراتيجية للحصول على أرباح كبيرة بشنّ 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

المتاح على الموقع التالي: www.heise-security.co.uk/news/80152. وانظر أيضا: Comments on Computer Crime – Senate Bill S. 240, Memphis State University Law Review, 1980, p. 660.

(24) انظر Mitchison/Urry, Crime and Abuse in e-Business, IPTS Report، المتاح على الموقع التالي: www.jrc.es/home/report/english/articles/vol57/ICT2E576.htm؛ و Collier/Spaul, Problems in Policing Computer Crime, Policing and Society, 1992, vol. 2, p. 310، المتاح على الموقع التالي: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf.

(25) انظر Collier/Spaul, Problems in Policing Computer Crime, Policing and Society, 1992, vol. 2, p. 310، المتاح على الموقع التالي: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf؛ و Smith, "Investigating Cybercrime: Barriers and Solutions", 2003, p. 2، المتاح على الموقع التالي: www.aic.gov.au/conferences/other/smith_russell/2003-09-cybercrime.pdf.

(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 على موقع 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 (SOCA)، والمتاحة على الموقع التالي: www.soca.gov.uk/downloads/massMarketingFraud.pdf.

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

١٧- سوف تتألّف الدراسة الخاصة بهذا الموضوع مما يلي:

(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 إحصاءات دقيقة؛

(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

١٨- يُولَى في الوقت الراهن كثيرٌ من الاهتمام لوضع استراتيجيات لتناول 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.

(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 معدلها الوسطي ١٠٠ ٥ دولار لكل حالة. وكان عدد الجرائم المبلغ عنها متدنيا للغاية، في حين كان المعدل الوسطي للخسائر المترتبة على هذه الجرائم مرتفعا.

تحديات التصدّي للجريمة السيبرانية

١٩- 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 نطاق الحماية بكلمات السر.[٣٠] ومن التحديات الأخرى صعوبة تعقّب أثر مرتكبي هذه الجرائم. ورغم أنَّ مستخدمي خدمات الإنترنت يخلفون آثارا متعددة، فإنه يمكن للمجرمين إعاقة 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

٢٠- سوف تتألّف الدراسة الخاصة بهذا الموضوع مما يلي:

(أ) حصر شامل للتحديات المتعلقة بمكافحة الجريمة السيبرانية؛

---

(29) انظر "Websense Security Trends Report 2004", p. 11; Information Security – Computer Controls over Key Treasury Internet Payment System, GAO 2003, p. 3; Sieber, Council of Europe Organised Crime Report 2004, p. 143.

(30) Ealy, "A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention", p. 9.

(31) للاطلاع على لمحة تاريخية وجيزة عن الإنترنت، بما في ذلك أصولها العسكرية، انظر: Leiner, Cerf, Clark, Kahn, Kleinrock; Lynch, Postel, Roberts, Wolff, "A Brief History of the Internet"، المتاح على الموقع التالي: www.isoc.org/internet/history/brief.shtml.

(32) Lipson, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues".

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

الموضوع ٤- مواءمة التشريعات

الخلفية

٢١- 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.

الاختلافات الوطنية والإقليمية

٢٢- إنَّ من أسباب الاختلافات في الأطر التشريعية الوطنية والإقليمية على السواء اختلاف وقع الجريمة السيبرانية باختلاف المناطق، كما يتبيَّن من مكافحة الرسائل الإلكترونية الاقتحامية (Spam).[٣٣] فقد برزت هذه الرسائل الاقتحامية 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، يمكن لبعض البلدان والمناطق أن تجرِّم نشر المواد التي يمكن اعتبارها محمية وفق مبدأ حرية القول[٣٥] في بلدان أخرى.[٣٦]

(33) "فهم الجريمة السيبرانية: دليل للبلدان النامية"، الاتحاد الدولي للاتصالات، ٢٠٠٩، الفصل ٢-٦-٧.

(34) انظر Spam Issue in Developing Countries, p. 4، المتاح على الموقع التالي: www.oecd.org/dataoecd/5/47/34935342.pdf.

(35) فيما يتعلق بمبدأ حرية القول، انظر: Tedford/HerbeckHaiman, Freedom of Speech in the United States, 2005; Barendt, Freedom of Speech, 2007; Baker; Human Liberty and Freedom of Speech; Emord, Freedom, Technology and the First Amendment, 1991؛ وبشأن أهمية المبدأ المتعلق بالمراقبة الإلكترونية، انظر: Woo/So, The case for Magic Lantern: September 11 highlights the need for increasing surveillance, Harvard Journal of Law & Technology, vol. 15, No. 2, 2002, p. 530 et seq; Vhesterman, Freedom of Speech in Australian Law; A Delicate Plant, 2000; Volokh, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, vol. 33, 2001, p. 57 et seq، المتاح على الموقع التالي: www.law.ucla.edu/volokh/harass/religion.pdf؛ و Cohen, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007، المتاح على الموقع التالي: www.fas.org/sgp/crs/misc/95-815.pdf.

٢٣- 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 ومواءمة التشريعات بغية منع توفير ملاذات آمنة للمجرمين.[٣٩]

نطاق الدراسة

٢٤- سوف تتألّف الدراسة الخاصة بهذا الموضوع مما يلي:

(أ) تحليل جوانب النجاح والقصور في الجهود المبذولة لمواءمة التشريعات الخاصة بالجريمة السيبرانية؛

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

(ج) تحليل مدى تأثير الاختلافات في المعايير القانونية على التعاون الدولي؛

---

(36) إنَّ الشواغل المتعلقة بحرية التعبير تفسر عدم اعتبار بعض الأفعال العنصرية أفعالا غير مشروعة في الاتفاقية المتعلقة بالجريمة السيبرانية، في حين أنها مجرمة في البروتوكول الإضافي الأول. انظر Explanatory Report to the First Additional Protocol, No. 4.

(37) فيما يتعلق بنطاق الهجمات عبر الوطنية التي أسفرت عن أفدح الأضرار، انظر: Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 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: Putnam/Elliott, International Responses to Cyber Crime, in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, p. 35 et seq، المتاح على الموقع التالي: http://media.hoover.org/documents/0817999825_35.pdf؛ و Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, p. 1 et seq، المتاح على الموقع التالي: http://media.hoover.org/documents/0817999825_1.pdf.

(39) فيما يتعلق بمبدأ ازدواجية التجريم في التحقيقات الدولية، انظر: United Nations Manual on the Prevention and Control of Computer-Related Crime, p. 269، المتاح على الموقع التالي: www.uncjin.org/Documents/EighthCongress.html؛ وانظر: Schjolberg/Hubbard, Harmonizing National Legal Approaches on Cybercrime, 2005, p. 5، المتاح على الموقع التالي: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

(د) استبانة الأساليب التي يمكن الأخذ بها في صياغة التشريعات على نحو يكفل المرونة اللازمة للحفاظ على التقاليد القانونية الأساسية في سياق عملية المواءمة.

الموضوع ٥- النص على الجرائم السيبرانية

الخلفية

٢٥- يتطلّب التحقيق في الجريمة السيبرانية وملاحقة مرتكبيها بصورة فعّالة تجريم أفعال جديدة إذا كانت بعض السلوكيات المعينة غير مشمولة بالفعل بالتشريعات القائمة. فوجود تشريعات مناسبة ضروري ليس فقط من أجل إجراء تحقيقات وطنية، بل لأنه يمكن أن يؤثّر أيضا على التعاون الدولي، كما أُشير إلى ذلك أعلاه.

القانون الجنائي الموضوعي

٢٦- 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. لكن بعض النهوج تذهب إلى أبعد من ذلك، وتجرم الأفعال المتعلقة مثلا بإنتاج وتوزيع الأدوات (مثل البرامجيات أو الأجهزة) التي يمكن أن تستخدم لارتكاب جرائم سيبرانية، والأفعال المرتبطة باستغلال الأطفال في المواد الإباحية أو "المراودة" أو نشر خطابات كراهية.

نطاق الدراسة

٢٧- 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 النص على الجرائم السيبرانية؛

(ب) تقييم الممارسات الفضلى فيما يتصل بالتجريم؛

(ج) تحليل الاختلافات في النهوج التي تأخذ بها بلدان القانون العام وبلدان القانون المدني في النص على الجرائم السيبرانية.

الموضوع ٦- إجراءات التحقيق

الخلفية

٢٨- 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

٢٩- 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.

٣٠- وقد اعتمدت بعض الدول تدابير تتجاوز تلك الأحكام القياسية لمعالجة تحديات خاصة مثل اعتراض الاتصالات التي تتم باستخدام بروتوكول نقل الصوت عبر الإنترنت

(40) فيما يتعلق بالنهوج المستندة إلى المستخدمين في مكافحة الجريمة السيبرانية، انظر: Görling, The Myth Of User Education, 2006، المتاح على العنوان التالي: www.parasite-economy.com/texts/StefanGorlingVB2006.pdf. وانظر أيضا التعليقات التي قدمها جان بيير شوفينمان، وزير الداخلية الفرنسي، خلال مؤتمر مجموعة الثمانية 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 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"، الاتحاد الدولي للاتصالات، ٢٠٠٩، الفصل ٣-٢-٧.

(تقنية فويب).[٤٢] ولئن أدرجت معظم الدول في تشريعاتها أحكاما بشأن تدابير التحقيق – مثل التنصّت على الهواتف – تمكّنها من اعتراض الاتصالات عبر الخطوط الأرضية وعبر الهواتف النقّالة،[٤٣] فإنّ هذه التدابير لا تكفي عادة للتمكّن من اعتراض الاتصالات التي تتم بتقنية فويب. ويجري اعتراض المكالمات الهاتفية التقليدية عادة من خلال الشركات التي توفّر خدمات الاتصالات.[٤٤] وبتطبيق المبدأ ذاته على تقنية فويب، تستعين هيئات إنفاذ القانون في هذا الشأن بمقدمي خدمات الإنترنت وخدمات تقنية فويب. أما إذا كانت خدمة الاتصالات الصوتية عبر الإنترنت تستند إلى تكنولوجيا الاتصال بين النظراء، فقد لا يتمكن مقدمو الخدمات من اعتراض الاتصالات.[٤٥]

نطاق الدراسة

٣١- سوف تتألّف الدراسة الخاصة بهذا الموضوع مما يلي:

(أ) إيراد أمثلة عن حالات أبرزت التحقيقات في إطارها الحاجة إلى تدابير تحقيق خاصة بالجريمة السيبرانية؛

---

(42) يُستخدم مصطلح "بروتوكول نقل الصوت عبر الإنترنت" (VoIP) لوصف تقنية نقل الاتصالات الصوتية باستخدام شبكات النقل التجميعي للبيانات مع البروتوكولات ذات الصلة. وللاطلاع على مزيد من المعلومات، انظر: Swale, Voice Over IP: Systems and Solutions, 2001; Black, "Voice Over IP", 2001.

(43) فيما يتعلق بأهمية اعتراض الاتصالات وإيجاد حلول تقنية، انظر: Karpagavinayagam/State/Festor, "Monitoring Architecture for Lawful Interception in VoIP Networks, in Second International Conference on Internet Monitoring and Protection", ICIMP 2007. وفيما يتعلق بالتحديات التي يمثلها اعتراض بيانات الاتصالات، انظر: SwaleChochliouros/Spiliopoulou/Chochliouros, "Measures for Ensuring Data Protection and Citizen Privacy Against the Threat of Crime and Terrorism – The European Response", in Janczewski/Colarik, "Cyber Warfare and Cyber Terrorism", 2007, p. 424.

(44) فيما يتعلق بالاختلافات بين الاتصالات عبر شبكات التبديل الهاتفية العامة (PSTN) وباستخدام بروتوكول نقل الصوت عبر الإنترنت (تقنية فويب)، انظر: Seedorf, "Lawful Interception in P2P-Based VoIP Systems", in Schulzrinne/State/Niccolini, Principles, Systems and Applications of IP Telecommunication. Services and Security for Next Generation Networks, 2008, p. 217 et seq.

(45) فيما يتعلق باعتراض وكالات إنفاذ القانون للاتصالات الصوتية عبر الإنترنت، انظر Bellovin and others, "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP"; Simon/Slay, "Voice over IP: Forensic Computing Implications", 2006; Seedorf, "Lawful Interception in P2P-Based VoIP Systems", in Schulzrinne/State/Niccolini, Principles, Systems and Applications of IP Telecommunication. Services and Security for Next Generation Networks, 2008, p. 217 et seq.

(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؛

(د) تحليل الاختلافات في نهج وضع أحكام التحقيق المتعلقة بالجريمة السيبرانية في بلدان القانون العام وبلدان القانون المدني.

الموضوع ٧- التعاون الدولي

الخلفية

٣٢- يتزايد عدد الجرائم السيبرانية ذات البعد الدولي،[٤٦] 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.[٤٧] 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 المتاحة للدول بشأن التعاون الدولي.[٤٨]

---

(46) فيما يتعلق بالبعد عبر الوطني للجريمة السيبرانية، انظر: Keyser, The Council of Europe Convention on Cybercrime, Journal of Transnational Law and Policy, vol. 12, No. 2, p. 289، المتاح على الموقع التالي: www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf. و Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, p. 1 et seq، المتاح على الموقع التالي: http://media.hoover.org/documents/0817999825_1.pdf.

(47) انظر في هذا السياق: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, p. 217، المتاح على الموقع التالي: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

(48) Gabuardi, Institutional Framework for International Judicial Cooperation: Opportunities and Challenges for North America, Mexican Law Review, vol. I, No. 2, p. 156، المتاح على الموقع التالي: http://info8.juridicas.unam.mx/pdf/mlawrns/cont/2/cmm/cmm7.pdf.

صكوك التعاون الدولي

٣٣- توجد أربعة مصادر رئيسية تمثل الأساس القانوني اللازم للتعاون الدولي الرسمي بأشكال من قبيل تسليم المطلوبين والمساعدة القانونية المتبادلة في المسائل الجنائية والتعاون لأغراض المصادرة.

٣٤- أولا، قد تمثّل الأحكام المتعلقة بالتعاون الدولي جزءا من الاتفاقات الدولية والإقليمية التي تعالج نوعا معيّنا من الجرائم الدولية، مثل اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية،[٤٩]،[٥٠] واتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية.[٥١] وثانيا، توجد معاهدات إقليمية متعلقة بالتعاون الدولي مثل الاتفاقات متعلقة بتسليم المطلوبين أو المساعدة القانونية المتبادلة في المسائل الجنائية الخاصة بمجلس أوروبا والبلدان الأمريكية والجماعة الإنمائية للجنوب الأفريقي. ويتمثّل المصدر الثالث في الاتفاقات الثنائية المتعلقة بتسليم المطلوبين أو المساعدة القانونية المتبادلة. وتتضمّن تلك الاتفاقات عموما معلومات محدَّدة تتعلق بأنواع الطلبات التي يمكن تقديمها، وتحدّد الإجراءات ذات الصلة وأساليب الاتصال، وكذلك حقوق وواجبات الدولة مقدِّمة الطلب والدولة متلقية الطلب.[٥٢] والمصدر الرابع للتعاون الدولي هو القانون الوطني الذي قد يجيز التعاون الدولي على أساس المعاملة بالمثل، أو على أساس كل حالة على حدة.

نطاق الدراسة

٣٥- سوف تتألّف الدراسة الخاصة بهذا الموضوع مما يلي:

(أ) استبانة التحديات المتعلقة بالتعاون الدولي في قضايا الجرائم السيبرانية؛

---

(49) فيما يتعلق بالاتفاقية، انظر: Smith, An International Hit Job: Prosecuting Organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009, vol. 97, p. 1118، المتاح على الموقع التالي: www.georgetownlawjournal.org/issues/pdf/97-4/Smith.PDF.

(50) Inter-American Convention on Mutual Assistance in Criminal Matters, 1992, Treaty Series, OAS, No. 75. ويرد نص الاتفاقية وقائمة الدول الموقّعة والمصدِّقة عليها في الموقع التالي: www.oas.org/juridico/english/sigs/a-55.html.

(51) Council of Europe Convention on Cybercrime, ETS 185.

(52) انظر في هذا السياق معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية، ١٩٩٩، قرار الجمعية العامة ٤٥/١١٧؛ والأدلة التشريعية لتنفيذ اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والبروتوكولات الملحقة بها، ٢٠٠٤، ص. ٢١٧، المتاح على الموقع التالي: \\unvcl01-d2\data02\Data\TES\tesshar\OUT\RTU\dtsearch\01crime\TOC\Legislative guides\04-50411_A.pdf.

(ب) حصر أحكام التعاون الدولي المتعلقة بالتحقيقات والملاحقات القضائية بشأن الجرائم السيبرانية؛

(ج) حصر الأمثلة على الممارسات الفضلى الواردة في الاتفاقات الثنائية؛

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

(هـ) تحديد دور الوسائل غير الرسمية للتعاون من قبيل تبادل المعلومات الاستخباراتية؛

(و) تقديم لمحة عامة عن الطلبات الراهنة الصادرة عن السلطات المعنية فيما يتعلق بالتعاون الدولي.

الموضوع ٨- الأدلة الإلكترونية

الخلفية

٣٦- بالنظر إلى أنَّ المعلومات تخزَن باطراد 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[٥٣] والتكلفة المنخفضة نسبيا[٥٤] لتخزين الوثائق الرقمية مقارنة بتخزين الوثائق المادية إلى زيادة عدد الوثائق الرقمية.[٥٥] واليوم، يوجد كم كبير من البيانات المخزنة بشكل رقمي فقط.[٥٦] ونتيجة لهذه الزيادة، أصبحت الوثائق الإلكترونية مثل الوثائق النصية وأفلام الفيديو

(53) انظر: Abramovitch, A brief history of hard drive control, Control Systems Magazine, EEE, 2002, vol. 22, Issue 3, p. 28 et seq؛ و Coughlin/Waid/Porter, The Disk Drive, 50 Years of Progress and Technology Innovation, 2005، المتاح على الموقع التالي:
www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf.

(54) Giordano, Electronic Evidence and the Law, Information Systems Frontiers, vol. 6, No. 2, 2006, p. 161; Willinger/Wilson, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law and Technology, 2004, vol. X, No. 5.

(55) Lange/Minster, Electronic Evidence and Discovery, 2004, p. 6.

(56) Homer, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, vol. 1, No. 1, p. 1، متاح على الموقع التالي:
www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf

الرقمية والصور الرقمية[٥٧] تؤدي دورا في التحقيقات المتعلقة بالجريمة السيبرانية والإجراءات ذات الصلة بها في المحاكم.[٥٨]

القواعد المتعلقة بالأدلة الإلكترونية

٣٧- يثير استخدام الأدلة الإلكترونية عددا من التحديات على السواء في مرحلتي جمعها وقبولها كَبَيِّنات.[٥٩] 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 شهود العيان. وفي هذه الحالات، تغدو إمكانية النجاح في التعرف على هوية الجاني وملاحقته قضائيا مرهونة بجمع الأدلة الإلكترونية وتقييمها بصورة صحيحة.[٦٠]

٣٨- وتؤثّر الرقمنة أيضا على طريقة تعامل هيئات إنفاذ القانون والمحاكم مع الأدلة.[٦١] ففي حين يكفي عرض الوثائق التقليدية في المحكمة، قد تتطلب الأدلة الرقمية تطبيق إجراءات

(57) فيما يتعلق بمقبولية الصور الرقمية وموثوقيتها، انظر: Kwiatkowski, Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images, Journal of Law and Policy, p. 267 et seq.

(58) Harrington, A Methodology for Digital Forensics, T.M. Cooley J. Pac. and Clinical L., 2004, vol. 7, p. 71 et seq; Casey, Digital Evidence and Computer Crime, 2004, p. 14. وفيما يتعلق بالأطر القانونية القائمة في مختلف البلدان، انظر: Rohrmann/Neto, Digital Evidence in Brazil, Digital Evidence and Electronic Signature Law Review, 2008, No. 5؛ و Wang, Electronic Evidence in China, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; Bazin, Outline of the French Law on Digital Evidence, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; Makulilo, Admissibility of Computer Evidence in Tanzania, Digital Evidence and Electronic Signature Law Review, 2008, No. 5. Winick, Search and Seizures of Computers and Computer Data, Harvard Journal of Law and Technology, 1994, vol. 8, No. 1, p. 76; 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.

(59) Casey, Digital Evidence and Computer Crime, 2004, p. 9.

(60) فيما يتعلق بضرورة إضفاء الطابع الرسمي على التحاليل الجنائية الحاسوبية، انظر: Leigland/Krings, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, vol. 3, No. 2.

(61) فيما يتعلق بصعوبات التعامل مع الأدلة الرقمية بتطبيق الإجراءات والمذاهب التقليدية، انظر: 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, p. 57 et seq.

خاصة، وقد لا تكون هذه الإجراءات مناسبة لتحويل تلك الأدلة الرقمية إلى أدلة تقليدية من قبيل النسخ المطبوعة من الملفات.[٦٢]

نطاق الدراسة

٣٩- سوف تتألّف الدراسة الخاصة بهذا الموضوع مما يلي:

(أ) حصر الأحكام المتعلقة بالتعامل مع الأدلة الإلكترونية ومقبوليتها؛

(ب) تحليل الاختلافات في النهوج، واستبانة المبادئ المشتركة فيما يخص الأدلة الإلكترونية في بلدان القانون العام وبلدان القانون المدني.

الموضوع ٩- مسؤولية متعهِّدي خدمات الإنترنت

الخلفية

٤٠- إنَّ ارتكابَ جريمة سيبرانية، حتى وإن كان الجاني يعمل بمفرده، يمس تلقائيا بعدد من الأشخاص والمؤسسات التجارية. فبالنظر إلى بنية الإنترنت، يتطلب نقل رسالة إلكترونية بسيطة خدمات عدد من المتعهِّدين، مثل متعهِّدي خدمات البريد الإلكتروني، ومتعهِّدي خدمات الوصول إلى الإنترنت، ومتعهِّدي وحدات التوجيه التي تحيل الرسالة الإلكترونية إلى متلقيها.[٦٣] والوضع مشابه فيما يتعلق بتنزيل الأفلام التي تحتوي على مواد إباحية يُستغل فيها الأطفال. فعملية تنزيل الأفلام تشمل متعهِّد المحتوى الذي يحمِّل الصور (موقع شبكي مثلا)، والمتعهِّد المضيف الذي يوفِّر وسيطة التخزين للموقع الشبكي، ومتعهِّد وحدات التوجيه التي تحيل الملفات إلى المستخدمين، وأخيرا متعهِّد خدمات الوصول الذي يمكِّن المستخدم من استعمال الإنترنت.

(62) انظر: Vacca, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 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, p. 291 et seq.

(63) فيما يتعلق بهيكل الشبكة ونتائج مشاركة متعهِّدي الخدمات، انظر: Black, Internet Architecture: An Introduction to IP Protocols, 2000؛ و Zuckerman/McLaughlin, Introduction to Internet Architecture and Institutions, 2003، المتاح على الموقع التالي: http://cyber.law.harvard.edu/digitaldemocracy/internetarchitecture.html.

دور متعهِّد خدمات الإنترنت

٤١- إنَّ تعذُّر ارتكاب الجريمة السيبرانية دون مشاركة متعهِّدي الخدمات، إضافة إلى أنَّ متعهِّدي الخدمات هؤلاء لا يملكون القدرة في الكثير من الحالات على منع ارتكاب الجرائم السيبرانية، يثير تساؤلات بشأن ما إذا كان ينبغي الحد من مسؤولية متعهِّدي خدمات الإنترنت.[٦٤] والإجابة على هذا السؤال حاسمة فيما يتعلق بالتطور الاقتصادي للبنى التحية لتكنولوجيا المعلومات والاتصالات.

٤٢- وكثيرا ما تعتمد الجهود التي تبذلها هيئات إنفاذ القانون على تعاون متعهِّدي خدمات الإنترنت. ويثير ذلك بعض الشواغل، لأنَّ الحدَّ من مسؤولية متعهِّدي خدمات الإنترنت عن الأفعال التي يرتكبها مستخدمو خدماتهم قد يؤثّر على التعاون والدعم الذي يقدمونه في إطار التحقيقات في الجرائم السيبرانية وفي منع الجرائم السيبرانية فعليا.

نطاق الدراسة

٤٣- سوف تتألّف الدراسة الخاصة بهذا الموضوع مما يلي:

(أ) حصر النهوج المتبعة في تنظيم مسؤولية متعهِّدي خدمات الإنترنت بتحديد الفوارق بين مختلف أنواعهم؛

(ب) دراسة مفهوم محدودية مسؤولية متعهِّدي خدمات الإنترنت؛

(ج) قدرة متعهِّدي خدمات الإنترنت على مساعدة هيئات إنفاذ القانون ومنع الجريمة السيبرانية.

الموضوع ١٠- التصدّي للجريمة السيبرانية خارج دائرة التدابير القانونية 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.

---

(64) للاطلاع على التمهيد للمناقشة، انظر: Elkin-Koren, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, vol. 9, 2005, p. 15 et seq، المتاح على الموقع التالي: www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

سبل التصدّي بغير التدابير القانونية

٤٥- تشمل سبل التصدّي للجريمة السيبرانية خارج دائرة التدابير القانونية مثلا إقامة البنى التحتية اللازمة للتحقيق في الجرائم وملاحقة مرتكبيها (مثل توفير المعدات والموظفين)، وتدريب الخبراء القائمين على مكافحة الجريمة السيبرانية، وتثقيف مستخدمي الإنترنت، وإيجاد حلول تقنية لمنع الجريمة السيبرانية أو التحقيق فيها.

نطاق الدراسة

٤٦- سوف تتألّف الدراسة الخاصة بهذا الموضوع مما يلي:

(أ) تقديم لمحة عامة عن مختلف النهوج المتبعة في التصدّي للجريمة السيبرانية خارج دائرة التدابير القانونية؛

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

(ج) تحليل العلاقات بين مختلف تدابير التصدّي للجريمة السيبرانية خارج دائرة التدابير القانونية وإمكانيات اعتمادها بطريقة جامعة.

الموضوع ١١- المنظمات الدولية

الخلفية

٤٧- في سبعينات وثمانينات القرن العشرين، كانت أغلبية النهوج القانونية المتعلقة بالتصدّي للجريمة السيبرانية توضع على الصعيد الوطني. وفي التسعينات، بدأت معالجة مسألة الجريمة السيبرانية في إطار المنظمات الإقليمية والدولية، وشمل ذلك تناولها من خلال الجمعية العامة لها، التي اعتمدت على مدى السنوات عدة قرارات بشأن الجريمة السيبرانية،[٦٥] وكذلك في إطار الكومنولث (القانون النموذجي الخاص بالجريمة السيبرانية)، ومجلس أوروبا (الاتفاقية المتعلقة بالجريمة السيبرانية)، والاتحاد الأوروبي (القرار الإطاري بشأن الاعتداء على نظم المعلومات).

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

مواءمة المعايير

٤٨- لقد ثبت نجاح المعايير المفردة الموحدة فيما يتعلق بالبروتوكولات التقنية، فأثار ذلك التساؤلات بشأن كيفية تجنب التضارب بين مختلف النهوج الدولية.[٦٦] وقد اعتُمد النهج الأشمل في اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية وقانون الكومنولث النموذجي بشأن الجريمة السيبرانية، بالنظر إلى أنهما يشملان القانون الجنائي الموضوعي والقانون الإجرائي والتعاون الدولي. فيمكن 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؛

(ب) استبانة مَواطن القوة والضعف في النهوج القائمة؛

(ج) تحليل الثغرات في النهوج القانونية الدولية القائمة.

الموضوع ١٢- المساعدة التقنية

الخلفية

٥٠- خلافا لبعض المعتقدات السائدة أحيانا، لا تعد الجريمة السيبرانية مشكلة تمس البلدان المتقدمة بصورة رئيسية. ففي عام ٢٠٠٥، تجاوز عدد مستخدمي الإنترنت في البلدان النامية عددهم في البلدان الصناعية للمرة الأولى.[٦٧] 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

(66) للاطلاع على التفاصيل، انظر: Gercke, National, Regional and International Legislative Approaches in the Fight Against Cybercrime, Computer Law Review International, 2008, p. 7 et seq.

(67) انظر: "Development Gateway's Special Report, Information Society – Next Steps?", 2005، المتاح على الموقع التالي: http://topics.developmentgateway.org/special/informationsociety.

الميدان الاقتصادي تقريرا يحلل أثر الرسائل الإلكترونية الاقتحامية على البلدان النامية،[٦٨] 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 منسقة. ومنع توفير ملاذات آمنة لمرتكبي الجرائم السيبرانية من التحديات الرئيسية في سياق مكافحة الجريمة السيبرانية.[٦٩] ومن ثم، أصبح بناء القدرات في البلدان النامية لتمكينها من مكافحة الجريمة السيبرانية مهمة رئيسية من مهام المجتمع الدولي. ويتجسد ذلك في إعلان سلفادور الذي اعتمده مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية المعقود في عام ٢٠١٠، الذي أوصى بأن يقدِّم مكتب 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.

نطاق الدراسة

٥٢- سوف تتألف الدراسة الخاصة بهذا الموضوع مما يلي:

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

(ب) استبانة الممارسات الفضلى المتبعة في تقديم جوانب المساعدة التقنية المتصلة بمسألة الجريمة السيبرانية.

---

(68) انظر: "Spam Issue in Developing Countries"، المتاح على الموقع التالي: www.oecd.org/dataoecd/5/47/34935342.pdf.

(69) عولجت هذه المسألة في عدد من المنظمات الدولية. وقد ذكرت الجمعية العامة ٥٥/٦٣ في قرارها 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. وقد شددت خطة عمل مجموعة الثمانية المؤلفة من ١٠ نقاط على "وجوب القضاء على الملاذات الآمنة لمن يسيئون استخدام تكنولوجيا المعلومات".

الموضوع ١٣- القطاع الخاص

الخلفية

٥٣- يتوقف منع الجرائم السيبرانية والتحقيق فيها على عدد من العناصر المختلفة. فكثيرا ما يجري التركيز على كفالة وجود التشريعات المناسبة، ولكن قطاع الصناعة الخاص يظل يؤدي دورا هاما في منع الجريمة السيبرانية والمساعدة في التحقيقات ذات الصلة على السواء. لكن مشاركته في التحقيقات المتصلة بالجريمة السيبرانية محفوفة بعدد من التحديات.

دور قطاع الصناعة

٥٤- إنَّ دورَ قطاع الصناعة في معالجة مسألة الجريمة السيبرانية معقَّدٌ وقد يتدرج من وضع الحلول وتنفيذها إلى حماية خدماته الخاصة من إساءة استعمالها في ارتكاب الجرائم إلى حماية المستخدمين ودعم التحقيقات. وكثيرا ما تكون تدابير الحماية الذاتية التي تعتمدها دوائر الصناعة عنصرا منطقيا من استراتيجيات تجارية شاملة، ولا تتطلّب عموما أساسا قانونيا محدَّدا ما دامت لا تنطوي على تدابير مضادة فعلية غير قانونية. ولا تمثّل تدابير الحماية التي تتخذ بالنيابة عن المستخدمين مشكلات كذلك، شريطة أن تتخذ بموافقة المستخدم. بيد أنَّ إشراك قطاع الصناعة في التحقيقات الجنائية طرح 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

٥٥- سوف تتألّف الدراسة الخاصة بهذا الموضوع مما يلي:

(أ) حصر الممارسات الفضلى المتبعة لدى القطاع الخاص في مجال منع الجريمة السيبرانية والتحقيق فيها؛

(ب) تحليل متطلبات قطاع الصناعة وإنفاذ القانون؛

(ج) تقييم مَواطن القوة والضعف في النهوج القائمة.