الأمم المتحدة

A/CONF.203/14*

Distr.: General
14 March 2005
Arabic
Original: English

مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية

بانكوك، ١٨-٢٥ نيسان/أبريل ٢٠٠٥

البند ٣ من جدول الأعمال المؤقت**

التدابير الفعالة لمكافحة الجريمة المنظمة عبر الوطنية

حلقة العمل ٦: تدابير لمكافحة الجرائم المتصلة بالحواسيب***

ورقة معلومات خلفية****

ملخص

إن انتشار تكنولوجيا المعلومات والاتصالات الجديدة على نطاق العالم أدى إلى ظهور أشكال أخرى من الجرائم المتصلة بالحواسيب، والتي تشكل خطرا لا على سرية النظم الحاسوبية أو سلامتها أو توافرها فحسب، بل أيضا على أمن البنى الأساسية الحرجة. وفضلا عن ذلك، فإن الابتكارات التكنولوجية تسفر عن أنماط متمايزة من الابتكار الإجرامي، ومن ثم فإن الأخطار المختلفة التي تشكلها الجرائم المتصلة بالحواسيب تعكس التباينات بين الطائفة المتنوعة المسماة "الفجوة الرقمية". وعند مكافحة هذه الجرائم، يواجه المحققون والمدعون العامون والقضاة على السواء عددا من المشاكل المتعلقة بالتحاليل الجنائية تنجم جزئيا عن الطابع غير الملموس للأدلة الرقمية وسرعة اختفائها. وعلاوة على ذلك، فإن التحقيق في الجرائم المتصلة بالحواسيب وملاحقتها قضائيا غالبا ما يقتضيان تتبع النشاط الإجرامي وآثاره من خلال مجموعة متنوعة من مقدمي خدمات الإنترنت أو

* أعيد اصدارها لأسباب فنية.

** A/CONF.203/1.

*** يود الأمين العام أن يعرب عن تقديره للمعهد الكوري لعلم الإجرام والحكومة كندا للمساعدة التي قدماها في تنظيم حلقة العمل ٦.

**** تأخر تقديم هذه الوثيقة بسبب الحاجة إلى إجراء بحوث ومشاورات إضافية.

140405 V.05-83161 (A)

الشركات التي تقوم بذلك، ويتجاوز هذا التتبع أحيانا الحدود الوطنية، الأمر الذي يمكن أن يثير أسئلة صعبة تتعلق بالولاية القضائية والسيادة.

وتعقّد التحديات الخاصة بالجرائم المتصلة بالحواسيب يقتضي إقامة تعاون دولي، وهو ما يقتضي بدوره أن يكون لدى البلدان الأدوات القانونية والإجرائية والتنظيمية اللازمة. وعملا على إعداد طرائق فعالة لإقامة تعاون دولي ناجع لمكافحة الجرائم المتصلة بالحواسيب، تم الاضطلاع في السنوات الأخيرة بعدد من المساعي الإقليمية والأقاليمية، مما أسفر عن تحقيق عدة إنجازات هامة. وحتى تأتي هذه الجهود يلزم دعم مجموعة واسعة من البحوث في الجوانب المتنوعة التي تنطوي عليها مكافحة الجرائم المتصلة بالحواسيب للتشجيع على إقامة شراكة فعالة بين الحكومة والقطاع الخاص.

وتسلط هذه الورقة الضوء على التحديات التي تطرحها الجرائم المتصلة بالحواسيب حتى يتسنى للمشاركين في حلقة العمل ٦ النظر في التوصيات التي أعدتها الاجتماعات الإقليمية التحضيرية للمؤتمر الحادي العشر لمنع الجريمة والعدالة الجنائية، ورسم الطريق للتصدي لهذه الجرائم بشكل شامل وفعّال.

المحتويات

أولا- مقدمة

١- تغير تكنولوجيا المعلومات والاتصالات المجتمعات في شتى أنحاء العالم. فالابتكارات توجد أسواقا جديدة للسلع والخدمات. وهذه التكنولوجيا تحدث ثورة في أساليب العمل، فهي تحسّن الإنتاجية في الصناعات التقليدية، وتعيد تشكيل سرعة دوران رأس المال وتدفقه. غير أن التغييرات الاقتصادية ليست إلا أحد جوانب المعادلة، فالمجتمعات تشهد أيضا تغيرات ثقافية عميقة إذ إنها تعيد تشكيل وسائل الإعلام الجماهيري وتتشكل بفعل هذا الإعلام أيضا، وتتكيف مع النمو الانفجاري للإنترنت. وتضاعف عدد تكنولوجيا المعلومات والاتصالات على صعيد العالم يلقي أيضا ظلالا قاتمة، فهذه التكنولوجيا قد هيأت الظروف لأشكال جديدة من الاستغلال وأتاحت فرصا جديدة للأنشطة الإجرامية، وفي الواقع لأشكال جديدة من الجرائم.

٢- وقد اقترحت الاجتماعات الإقليمية التحضيرية الأربعة لمؤتمر الأمم المتحدة الحادي العشر لمنع الجريمة والعدالة الجنائية عددا من التوصيات لينظر فيها المؤتمر الحادي عشر: (أ) دراسة التجربة الراهنة والأطر والترتيبات القانونية الوطنية القائمة للتعاون بين الدول وكذلك بين الدول ومقدمي خدمات الإنترنت؛ (ب) بحث أنجع السبل لتعزيز التعاون وتبادل الخبرات والمعارف والدراية بين الحكومات والقطاع الخاص لوضع آليات وتفعيلها لمنع ومكافحة الجرائم المتصلة بالحواسيب وكفالة أمن الشبكات الحاسوبية ونظم الاتصالات، وكذلك كفالة وجود آليات ملائمة للتصدي لهذه الجرائم؛ (ج) استطلاع سبل ووسائل تعزيز قدرة الحكومات على استحداث وتطبيق أساليب تحري خاصة وكافية، وتعزيز قدرات الإدعاء، بما في ذلك إعداد وإنشاء برامج تدريبية شاملة لموظفي العدالة الجنائية؛ (د) التصدي لاستخدام التكنولوجيا الحاسوبية في استغلال النساء والأطفال، لا سيما فيما يتعلق بإنتاج المواد الإباحية والميل الجنسي إلى الأطفال؛ (هـ) دراسة جدوى إنشاء فرقة عمل عالمية خاصة بالإنترنت من أجل التعاون الدولي سعيا إلى مكافحة الجرائم المتصلة بالحواسيب؛ (و) النظر في اقتراح التفاوض بشأن اتفاقية جديدة لمكافحة الجرائم السيبرانية بغية وضع الأساس لاتخاذ إجراءات جماعية فعالة ضد هذا النوع من النشاط الإجرامي.[١]

إن وضع إطار مفاهيمي لمصطلح " الجرائم المتصلة بالحواسيب"، أو لما يشابهه من مصطلحات من قبيل "الجريمة السيبرانية"، موضوع مطروح على بساط البحث منذ ثلاثين عاما. ويرجع تاريخ النموذج الأولي إلى تقرير أعده معهد بحوث ستانفورد، ثم عاد ليظهر من جديد في شكل معدل طفيفا في عامي ١٩٧٩[٢] و١٩٨٩.[٣] واستُخدم مخطط التنظيم على

نطاق واسع في مقالات لاحقة عن الجريمة السيبرانية: الحاسوب موضوع الجريمة؛ أو الحاسوب أداة الجريمة؛ أو الحاسوب كوسيلة (الدور الرابع المقترح في عام ١٩٧٣، وهو الحاسوب كرمز، اختفى فيما يبدو في الثمانينات من القرن الماضي). وإعادة صياغة هذا النموذج المفاهيمي بشكل مفيد هو أن يُنظر إلى الجرائم المتصلة بالحواسيب باعتبارها سلوكا يحظره القانون و/أو فقه القضاء، وهو سلوك: (أ) يستهدف تكنولوجيات الحوسبة أو الاتصالات بعينها؛ (ب) أو يستخدم تكنولوجيات رقمية في ارتكاب الجريمة؛ (ج) أو ينطوي على الاستخدام العرضي للحاسوب فيما يتعلق بارتكاب جرائم أخرى، ومن ثم يكون الحاسوب مصدرا للدليل الرقمي.[٤] وقد حددت القوانين والمعاهدات، بما فيها الاتفاقية المتعلقة بجرائم الفضاء الحاسوبي لمجلس أوروبا،[٥] أنواعا مختلفة للجرائم المتصلة بالحواسيب (مثل جرائم انتهاك سرية النظم الحاسوبية أو سلامتها أو توافرها؛ والجرائم المتصلة بالمضمون؛ والجرائم المتصلة بالملكية الفكرية).

ثانيا- الجرائم المتصلة بالحواسيب

٣- ثمة عدد من أشكال الجرائم المتصلة بالحواسيب تستهدف تكنولوجيا المعلومات والاتصالات ذاتها، ويُشار إليها أحيانا بفئة الجرائم التي تنتهك سرية النظم الحاسوبية أو سلامتها أو توافرها. وتشمل هذه الجرائم أشكال سرقة خدمات الاتصالات والخدمات الحاسوبية باستخدام أساليب قرصنة متنوعة (رهنا بالتكنولوجيا المستخدمة، تشمل هذه الجرائم النفاذ غير المسموح به، وفك الشفرة أو كلمة المرور، والاستنساخ الرقمي، والاستيلاء على بطاقات الائتمان وهلم جرا). وقد تتعرض حواسيب خدمة الشبكة والمواقع الشبكية لهجمات ترمي إلى الحرمان من الخدمات. وتنجم هذه الجرائم في بعض الحالات عن هجمات متفرقة تُستخدم فيها العشرات أو المئات من الحواسيب المتواطئة بمثابة "حواسيب مدمرة" تقذف الطرف المستهدف بوابل من الطلبات يتزايد عددها بشكل يتعذر معه تلبيتها. وفي حالات أخرى يكون الحرمان من الخدمة نتيجة "عواصف جماعية" تنجم عن استنساخ جامح لديدان فائقة السرعة (برامج حاسوبية تستنسخ نفسها ذاتيا)، تستنسخ في دقائق مليارات من النسخ الذاتية — ويصدم هذا الحجم الهائل جزوع الألياف البصرية الأكثر سرعة ويحدث عطلا في النظم الضخمة للحواسيب المؤسسية. وقد تسببت الأوبئة العالمية الناجمة عن فيروسات الحاسوب في تعطل شبكات الأعمال والمستهلكين طوال العقدين السابقين، يتخللها بصورة دورية سلالات جديدة من الديدان والفيروسات الضارية والضارة بشكل خاص. وتبين الأمثلة الأخيرة طرفي التخصص: فمن ناحية نجد الديدان المصممة خصيصا

لمهاجمة مجموعة تتألف من مئات الملايين من أنظمة الحاسوب التي تستخدم النظم التشغيلية والتطبيقات الأكثر شيوعا، ومن ناحية أخرى نجد الديدان المصممة لمهاجمة تطبيقات الأمن المحكمة فقط المستخدمة في بضعة آلاف من المنصات فحسب.

أرسل شخصان مقيمان في ملبورن، أستراليا، ما بين ستة وسبعة ملايين رسالة إلكترونية على عناوين في أستراليا والولايات المتحدة الأمريكية، ووضعا رسائل عديدة على لوحات الرسائل لدى الشركات الرئيسية المقدمة لخدمات الإنترنت. وكان الغرض من هذه الرسائل التشجيع على شراء أسهم في شركة أمريكية تُباع أسهمها في الولايات المتحدة الأمريكية في الرابطة الوطنية للأسعار المؤتمتة للمتاجرين بالأوراق المالية (بورصة NASDAQ). وكانت هذه الرسائل، التي أرسلت بأسماء زائفة وأعيد إرسالها من خلال وحدات خدمة أخرى، تبشر بزيادة في سعر أسهم الشركة تصل إلى ٩٠٠ في المائة. وحدث بعد ذلك بفترة قصيرة زيادة في حجم تداول الأسهم بلغت عشرة أمثال، وتضاعف سعر السهم، وتوقف بعد ذلك تداول الأسهم ونفت الشركة البيانات الصادرة في الرسائل المختلفة.

لقد شرع هذان الشخصان في مخطط تقليدي يسمى "الضخ والتفريغ": كان يعلم أحد الشريكين، وهو مساهم في الشركة، أنه يقدم معلومات زائفة وعندما ارتفع سعر السهم باع أسهمه في الشركة لتحقيق الربح.

وانتهك هذان الشخصان القانون في كل من أستراليا والولايات المتحدة. وإضافة إلى التلاعب بالأسواق المالية، كان حجم حركة البريد الإلكتروني الناجمة عن رسائل الدعاية المذكورة كافيا ليشكل تشويشا على التشغيل المشروع للحاسوب. واتخذت اللجنة الأسترالية للأوراق المالية والاستثمار (ASIC) إجراءات استجابة للشكاوى المقدمة من الجمهور الأسترالي، وللمعلومات المقدمة من السلطات الأمريكية. وتم تتبع أثر مرتكبي الجريمة من خلال الرسائل الإلكترونية الموزعة عن طريق شبكات تجارية غير مشبوهة، ومن خلال العملية المالية المستخدمة لسداد خدمات الإنترنت.

وكما جرت العادة في هذا النوع من الجرائم، طالبت اللجنة الأمريكية للأوراق المالية والبورصة برد ما سُلب وبإصدار أمر زجري مؤقت ودائم ضد مرتكبي الجريمة لمنعهما من معاودة هذا النشاط. وطُلب منهما رد ما حققاه من مكاسب غير مشروعة وتقديم وعد بعدم العودة إلى هذا السلوك مطلقا. وكانت السلطات الأمريكية واثقة في قدرة أستراليا على التعامل مع الملاحقة الجنائية في أستراليا. ووجهت اللجنة الأسترالية للأوراق المالية والاستثمار

١٩ تهمة جنائية للمتهمين. وأقر المتهمان بأنهما مذنبان لنشر معلومات زائفة أو مضللة ويمكن أن تشجع على شراء أوراق مالية، وللتشويش على الاستخدام المشروع للحاسوب، أو تعطيله أو عرقلته. وحُكم على المتهمين بالسجن عامين، وتم تعليق الحكم (بعد ثلاثة أشهر حبس بالنسبة إلى مرتكب الجريمة الرئيسي).

٤- وفي السياق المؤسسي، يتراوح نطاق المنع من الوصول إلى البيانات بين ظروف يمكن فيها استعادة البيانات (مثل هجوم يشنه موظف مستاء يتمثل في تشفير ملفات البيانات بشكل غير مسموح به)، وتدمير البيانات بحيث لا يمكن استعادتها (وهذا يعني عدم الاقتصار على مسح الملفات وإنما الحذف و/أو التدمير المادي لوحدات الدفع الصلبة أو وسائط التخزين الأخرى التي تتضمن الملفات). والشبكات الحاسوبية المحلية اللاسلكية، التي شهد استخدامها في المؤسسات زيادة كبيرة في السنوات الأخيرة، يمكن أن تتعرض لهجمات بهدف الحرمان من الخدمة (مثل التشويش المقصود) حتى عند تأمينها ضد النفاذ إليها بشكل غير مسموح به.[٦]

٥- ومن الضروري أيضا إدراك كيف يستخدم الحاسوب كوسيلة أو أداة لارتكاب الجرائم. فهناك مجموعة كبيرة من الجرائم المرتبطة بتغيير البيانات - ينطوي بعضها على ضرر إجرامي من قبيل التخريب الإلكتروني (مثل تشويه المواقع الشبكية)، ويشكل بعضها الآخر احتراف التزوير والتزييف. وثمة مواقع شبكية مخصصة "لصنع البطاقات" (بطاقات ائتمان مزورة) ويشمل ذلك توفير عملات وجوازات سفر مزورة بشكل متقن. وتشمل سرقة البيانات[٧] طائفة واسعة تتراوح بين قرصنة المعلومات والتجسس الصناعي، وانتهاك حقوق الطبع (سرقة الملكية الفكرية في شكل قرصنة البرمجيات وملفات الموسيقى MP3 والفيديو الرقمي وهلم جرا).[٨] وسرقة البيانات قد لا تكون مجرد جريمة اقتصادية، ولكن أيضا انتهاك للخصوصية وما يرتبط بها من حقوق الأشخاص في الجرائم الناشئة المتصلة بسرقة الهوية.

٦- وتنطوي أنواع كثيرة من الجرائم المتصلة بالحواسيب على سرقات اقتصادية مثل هجمات القرصنة، والهجوم على النظم المصرفية والمالية، فضلا عن الاحتيال الذي ينطوي على تحويل الأموال إلكترونيا. كما أعرب عن القلق إزاء غسل الأموال إلكترونيا والمسائل ذات الصلة مثل التهرب الضريبي.

٧- وتستخدم الحواسيب أيضا في تيسير مجموعة كبيرة من أعمال التدليس في مجال التسويق عن بعد والاستثمار، تتضمن ممارسات خادعة. والغش في المزادات هو أكثر أنواع

الغش المتصل بالحواسيب المبلغ عنه استنادا إلى شكاوى المستهلكين، إذ أنه يمثل ٦١ في المائة من شكاوى الغش المبلغ عنها وفقا لتقرير شامل أعد في الولايات المتحدة عن عام ٢٠٠٣.[٩] وتندرج أنواع أخرى من غش المستهلكين في الفئة الأعم "عدم تسليم السلع أو عدم الدفع" بعد إتمام المعاملات على الإنترنت. ويظل الغش في الأوراق المالية، المرتبط بالتلاعب في الاستثمارات المنخفضة القيمة في البورصة، نادرا إلى حد ما على مستوى المستهلك.

تمكن فتى كندي يبلغ من العمر ١٥ سنة من السيطرة على عدد من الحواسيب واستخدمها في شن هجمات متفرقة في شباط/فبراير ٢٠٠٠ ضد شركتي Yahoo وAmazon.com ومواقع أخرى بارزة في مجال التجارة الإلكترونية بهدف الحرمان من الخدمات. ومن خلال خفض سرعة النفاذ إلى هذه المواقع الشبكية أو تقييد النفاذ إليها، كلف هذا الفتى أصحاب هذه الشركات مئات الملايين من الدولارات بسبب ضياع الصفقات وعدم الاستفادة من السوق، فضلا عن تكاليف تحسين نظم الأمن. وبعد تفاخر هذا الفتى بهذه الهجمات في غرف الدردشة على الإنترنت، حدد مكتب التحقيقات الاتحادي الأمريكي في الولايات المتحدة هويته وأحال القضية إلى الشرطة الملكية الكندية الراكبة. وقليل من البلدان، إن وجد على الإطلاق، على استعداد لتسليم الأحداث. وفي هذه الحالة تحديدا، فإن تسليم الأحداث ممنوع بموجب القانون الكندي. وفي أيلول/سبتمبر ٢٠٠١، حُكم على الفتى بالسجن ثمانية أشهر في مركز لحبس الأحداث.

٨- "التصيد الاحتيالي" (أو رسائل الدعاية الساخرة) هو إعداد رسائل إلكترونية باستخدام صفحات الويب المقابلة وتصميمها بحيث تبدو كأنها مواقع موجودة للمستهلكين. وتوزع الملايين من هذه الرسائل الإلكترونية الاحتيالية، شأنها في ذلك شأن رسائل الدعاية الإلكترونية غير المرغوب فيها؛ غير أن هذه الرسائل لا تطلب بشكل مباشر شراء منتجات أو خدمات وإنما تعطي بالأحرى الإيحاء بأنها مرسلة من مصارف أو مزادات على الإنترنت أو من مواقع مشروعة أخرى، وتسعى إلى التحايل على المستخدمين لتحملهم على الرد وتقديم بيانات شخصية أو مالية أو بيانات تتعلق بكلمة المرور. وتُستخدم بعد ذلك هذه المعلومات الشخصية بشكل احتيالي لإجراء مشتريات (ويكون ذلك أحيانا بعد بيع المعلومات إلى طرف آخر).

٩- كما يجري على الإنترنت ارتكاب جرائم تقليدية مثل الابتزاز (التهديد بإفشاء معلومات خاصة بالممتلكات أو معلومات شخصية أو بإتلاف البيانات أو النظم) والتحرش. قُدمت أيضا للمحاكمة قضايا تتعلق بالتشنيع والتشهير وتمت محاكمتها بنجاح.

١٠- وتستخدم الحواسيب في مجموعة من الجرائم المتصلة بالمضمون تتضمن الحواسيب، لا سيما نشر المواد غير المشروعة أو الضارة. والمجتمع الدولي قلق بشكل خاص إزاء استخدام الأطفال في المنتجات الإباحية. فعلى الرغم من أن استخدام الأطفال في المنتجات الإباحية موجود منذ عقود طويلة (في شكل صور فوتوغرافية وفي المجلات والأفلام وأشرطة الفيديو)، فإن هناك نزعة متزايدة منذ الثمانينات من القرن الماضي إلى توزيع المنتجات الإباحية التي يستخدم فيها الأطفال من خلال مجموعة متنوعة من الشبكات الحاسوبية باستخدام مجموعة من خدمات الإنترنت تشمل المواقع الشبكية والمجموعات الإخبارية Usenet newsgroups، وغرف الدردشة على الإنترنت (Internet Relay Chat IRC)، وشبكات الند بالند (P2P).[١٠] وتستخدم هذه الشبكات في تيسير تبادل المعلومات، وتبادل صور أو أشرطة فيديو إباحية عن الأطفال، والمعاملات النقدية، ومعلومات تتعلق بالسياحة الجنسية التي تستهدف الأطفال. وتستغل نسبة معينة من المواد الإباحية الموزعة والخاصة بالأطفال في أغراض تجارية (عوضا عن تبادلها على أساس غير نقدي بين ذوي الميول الجنسية إلى الأطفال)، وترتبط بالجريمة المنظمة عبر الوطنية. وثمة منطقة رمادية أقل وضوحا تصبح فيها الأفعال غير القانونية مباحة بشكل عام، حيث استخدمت الإنترنت طوال الـ٢٥ عاما السابقة لتوزيع مواد إباحية، يعد كثير منها مشروعا في عدد كبير من الولايات القضائية، وكثير منها لأغراض تجارية، وغالبا ما يشار إليها باسم "الصناعة الترفيهية للكبار".[١١] غير أن ثمة حالات أخرى محددة بمزيد من الوضوح وعروضا معينة تشكل موادا إباحية (سواء كانت في شكل صور رقمية أو أشرطة فيديو) وتعد ماجنة من الناحية القانونية في كثير من البلدان، ويعد توزيع هذه المواد الماجنة جريمة. كما تستخدم الإنترنت في جرائم مضمون أخرى مثل توزيع مواد دعاية تشجع على الكراهية وكراهية الأجانب.[١٢]

من الحالات المعروفة جيدا في التسعينات من القرن الماضي الهجوم على سيتي بنك الذي شنه شاب من الاتحاد الروسي روسيا توصل إلى النفاذ بشكل غير مسموح به إلى وحدة خدمة المصرف في الولايات المتحدة. واستعان الشاب بعدد من المتواطئين لفتح حسابات في فروع المصرف في شتى أنحاء العالم، ثم أصدر تعليمات لحاسوب المصرف بتحويل أموال إلى تلك الحسابات. وعندما انكشف المخطط وتم تحديد هوية الفاعل

المزعوم، أُصدر أمر بالقبض عليه من المحكمة الاتحادية بالولايات المتحدة. ولم يكن هناك آنذاك معاهدة لتسليم المجرمين بين الاتحاد الروسي والولايات المتحدة، ولكن المتهم أرتكب خطأ بزيارة المملكة المتحدة لحضور معرض عن الحاسوب. وبموجب اتفاقات التسليم القائمة بين المملكة المتحدة والولايات المتحدة تمكنت السلطات البريطانية من تقديم المساعدة طالما كان للتهمة الموجهة إلى المتهم ما يقابلها في القانون البريطاني. وطلب المتهم أن تنظر المحكمة في قانونية توقيفه للطعن في تسليمه وساق حججا منها أن أمر تحويل الأموال قد صدر في الاتحاد الروسي، حيث توجد لوحة مفاتيح حاسوبه وليس في الولايات المتحدة. واعتبرت المحكمة أن الوجود المادي للمتهم في سانت بطرسون أقل أهمية من أنه كان يعمل على أقراص مغناطيسية موجودة في الولايات المتحدة. وعلاوة على ذلك، فإن التهم التي وجهت للمتهم كان لها مقابل واضح في القانون البريطاني الخاص بإساءة استخدام الحاسوب لعام ١٩٩٠؛ فلو كان المتهم يباشر عمله من المملكة المتحدة بدلا من الاتحاد الروسي لكان للمحاكم البريطانية الاختصاص القضائي. وتم تسليم المتهم إلى الولايات المتحدة حيث صدر حكم بإدانته وسجنه.

١١- ويولى اهتمام متزايد في السنوات الأخيرة للعلاقة بين الإرهاب والإنترنت، وإن كان يوجد في هذه الحالة أيضا مجموعة متنوعة من الأنشطة. فثمة دلالات تشير إلى استخدام الإنترنت في تيسير التمويل الإرهابي وكأداة لوجيستية لتخطيط الأعمال الإرهابية وتنفيذها. كما أن هناك مزيدا من التركيز على دور الإنترنت في نشر الدعاية الإرهابية وفي استخدامها في التجنيد. وهذه الأنشطة تختلف عن "الإرهاب السيبراني" الذي يعرّفه المركز الوطني لحماية البنية الأساسية بالولايات المتحدة بأنه "عمل إجرامي يرتكب عبر الحاسوب ويفضي إلى أعمال عنف و/أو الوفاة و/أو التدمير، ويولد الرعب بغرض إكراه حكومة ما على تغيير سياساتها".[١٣] وثمة مجالان متمايزان يثيران القلق هما: الهجوم على بيانات حرجة والهجوم على بنية أساسية حرجة.

١٢- ويتزايد الوعي بأهمية البنى الأساسية الإعلامية الحرجة، أي الشبكات التي تجعل من الممكن إجراء الاتصالات، بل والتي تستخدم أيضا لإدارة ومراقبة الجوانب الحاسمة الأهمية لبنى أساسية حرجة أخرى مثل الطاقة والنقل والغذاء والصحة العامة. وفي كثير من بلدان العالم يجوز أن تكون البنى الأساسية مملوكة للقطاع الخاص ومعرضة للهجوم بشكل خاص نظرا إلى أن كثيرا من نظم المراقبة الموزعة ونظم المراقبة الإشرافية واحتياز البيانات التابعة لهذه البنى الأساسية موصلة بالإنترنت ومن هنا يمكن تعطيلها. ونظرا إلى أوجه التكافل المتزايدة في المجتمعات الحديثة، فإن الهجوم السيبراني على هذه البنى الأساسية يمكن أن يكون له

انعكاسات فورية خطيرة على جميع النظم الاقتصادية والسياسية الوطنية، فضلا عن الآثار عبر الوطنية العميقة. ومن الأهمية بمكان التمكن من التصدي للهجوم على البنى الأساسية الإعلامية الحرجة (سواء كان الدافع هو الإرهاب أو غير ذلك من الأنشطة الإجرامية) من أجل الحد بأقصى درجة من خطورة احتمال أن يترتب على ذلك آثار متسلسلة على البنى الأساسية الحرجة الأخرى التي لا غنى عنها للمجتمع.

١٣- ولم يتم بعد التوصل إلى حل للتحديات التي يطرحها توافر أجهزة تشفير قوية على نطاق واسع، الأمر الذي أثار اهتماما دوليا في السنوات الخمس الماضية، فضلا عن أن الجيل الجديد من أجهزة التشفير الكمي يلوح الآن في الأفق.(١٤) وعلى الرغم من أن التشفير أمر لا غنى عنه لقطاع الأعمال والتجارة الإلكترونية، فإن المجرمين يستخدمونه أيضا. ومعضلة "الاستخدام المزدوج للتكنولوجيا" تتجاوز تقنية إخفاء المعلومات لتشمل مجموعات متنوعة من البرمجيات المتوافرة بالمجان على الشبكة على أساس الند بالند، ويعززها التشفير القوي المقاوم بدرجة كبيرة للمراقبة (مثل Freenet). وهذه التكنولوجيات تعزز حرية التعبير ويمكن أن تسهم في دعم الحريات الديمقراطية، ولكن يمكن أيضا أن يستخدمها المجرمون لإخفاء اتصالاتهم أو لتوزيع مواد غير قانونية.

ثالثا- الفجوة الرقمية والجرائم المتصلة بالحواسيب

١٤- عندما تنتشر تكنولوجيا المعلومات والاتصالات أنحاء مختلفة من العالم، فإن انتشارها لا يكون متماثلا. فبينما تشهد إحدى المناطق انتشار الكبلات الليفية عالية القدرة، فإن منطقة أخرى قد تشهد زيادة حثيثة في عدد الهاتف المحمول والشبكات اللاسلكية. واختلاف أنماط التكيف التكنولوجي قد يعرض المناطق لأشكال مختلفة من الضعف، وتظهر أنواع محددة من الجرائم المتصلة بالحواسيب للاستفادة من الظروف المختلفة.

١٥- وكان التغيير كبيرا: زيادة مذهلة في عدد أجهزة تكنولوجيا المعلومات والاتصالات (يوجد في الخدمة حاليا زهاء مليارين من الحواسيب والأجهزة الأخرى التي تعمل بمشغلات دقيقة)، وزيادة أسية في التوصيلية، وثورة في التقدم في الحوسبة مثل الاختراقات العملية في تصغير الأجهزة وزيادة سرعتها وسعتها للتخزين، ووصول نظم ذكية والروبوطية، وتحسين التفاعل بين الإنسان والحاسوب. ومع ذلك فإن هذا التحول التكنولوجي لا يقتصر على الانتشار في البيئة، إذ أنه يربط بين الناس والأشياء والمعلومات بشكل غير مسبوق، وإنما يحمل في طياته أيضا جيلا جديدا من الأخطار الرقمية والضعف إزاءها، ويقتضي إعادة التفكير بشكل جذري في أسلوب رؤية الجريمة في القرن الحادي والعشرين.

١٦- وإدراكا لذلك، شجعت الجمعية العامة في عام ٢٠٠٢ على بذل جهود دولية جديدة لمساعدة الدول الأعضاء في التصدي للجرائم المتصلة بالحواسيب. وفي "خطط العمل لتنفيذ إعلان فيينا بشأن الجريمة والعدالة: مواجهة تحديات القرن الحادي والعشرين"، المرفقة بقرار الجمعية العامة ٥٦/٢٦١ المؤرخ ٣١ كانون الثاني/يناير ٢٠٠١، قسما خاصا بعنوان "إجراءات العمل على مكافحة الجرائم المتصلة بالتكنولوجيا العالية والحواسيب"، يقدم توصيات ذات توجه عملي في مجال السياسات بشأن منع ومكافحة هذه الجرائم. كما دعت الجمعية في قرارها ٥٧/١٧٠ المؤرخ ١٨ كانون الأول/ديسمبر ٢٠٠٢ لجنة منع الجريمة والعدالة الجنائية أن تأخذ في الاعتبار، عند صياغة توصيات بشأن المؤتمر الحادي عشر عملا بقرار الجمعية ٥٦/١١٩ المؤرخ ١٩ كانون الأول/ديسمبر ٢٠٠١، التقدم المحرز في متابعة إعلان وخطة عمل فيينا.

١٧- وكان الاعتراف بوجود الفجوة الرقمية إحدى دعائم إسهام الأمم المتحدة في مطلع القرن الحادي والعشرين. وقد حدد السياق العام إعلان الأمم المتحدة بشأن الألفية المعتمد في قرار الجمعية العامة ٥٥/٢ المؤرخ ٨ أيلول/سبتمبر ٢٠٠٠. وفي إطار الغاية ٨ من الأهداف الإنمائية للألفية، المرفقة بتقرير الأمين العام المعنون "الدليل التفصيلي لتنفيذ إعلان الأمم المتحدة بشأن الألفية" (الوثيقة A/56/326)، يرد الهدف ١٨: "التعاون مع القطاع الخاص لإتاحة فوائد التكنولوجيات الجديدة، وبخاصة تكنولوجيا المعلومات والاتصال". ويتضمن إعلان المبادئ، الذي اعتمده مؤتمر قمة مجتمع المعلومات، المعقود في جنيف في الفترة ١٠-١٢ كانون الأول/ديسمبر ٢٠٠٣ رؤية مشتركة لمجتمع المعلومات (الوثيقة A/C.3/59/3، الفصل الأول، الباب ألف): "إننا ندرك تماما أيضا أن فوائد ثورة تكنولوجيا المعلومات توزع اليوم بشكل متفاوت بين البلدان المتقدمة النمو والبلدان النامية وفيما بين المجتمعات. ونحن ملتزمون التزاما تاما بتحويل هذه الفجوة الرقمية إلى فرصة رقمية للجميع، وخاصة لهؤلاء المعرضين للتخلف عن الركب ولمزيد من التهميش".[١٥]

في نهاية عام ٢٠٠٤ بلغ عدد من لديهم الفرصة للنفاذ إلى الإنترنت في الصين ٩٤ مليونا أو زهاء ٧,٢ في المائة من عدد سكان هذا البلد، ومنهم ٤٥,٥ في المائة يستخدمون النطاق العرض. وكان يقدر عدد المضيفين بما مجموعه ٤١,٦ مليون، وعدد عناوين مقدمي خدمات الإنترنت بما مجموعه ٦٠ مليونا، وأسماء المجالات بما مجموعه ٠٧٧ ٤٣٢، وعدد المواقع الشبكية في الصين بـ ٩٠٠ ٦٦٨.[١٦] وبمعدل نمو سنوي يقارب ١٨ في المائة،

سيتجاوز عدد مستخدمي الإنترنت الصينيين عددهم في أمريكا الشمالية بحلول عام ٢٠٠٨، ولكنه يتجاوز الآن بالفعل عددهم في اليابان وفي جمهورية كوريا مجتمعين. وفي عام ١٩٩٩، لم يكن هناك سوى ٨,٩ مليون مستخدم، ثم زاد هذا العدد إلى ٣٣,٧ مليون في عام ٢٠٠١. وزاد عدد المضيفين من ٣,٥ مليون في عام ١٩٩٩ إلى ٣٣,٧ مليون في عام ٢٠٠١.

١٨- وبنهاية عام ١٩٨٥، تجاوز عدد مضيفي الإنترنت ٠٠٠ ٢، وفي عام ١٩٨٩ بلغ عددهم ٠٠٠ ١٠٠، وفي عام ٢٠٠٠ تجاوز٠٠٠ ٣٠٠. وبلغ هذا العدد مليون في منتصف عام ١٩٩٢، و ١٠ ملايين في أواخر عام ١٩٩٥ أو بداية عام ١٩٩٦، و ١٠٠ مليون في أواخر عام ٢٠٠٠، وبلغ ما يربو على ١٦٢ مليونا[١٧] في تموز/يوليو ٢٠٠٢. وفي عام ٢٠٠٢، لم يكن لدى العالم النامي سوى ٤,١ مستخدم للإنترنت و ٣,٣ حاسوب لكل ١٠٠ نسمة، بينما كان في العالم المتقدم النمو ٣٣,٣ مستخدم للإنترنت و ٣٦,٢ حاسوب لكل ١٠٠ نسمة (E/2004/62 وCorr.1). وكان خمس سكان العالم الذين يعيشون في البلدان ذات الدخل الأكبر لديهم ٨١,٩ في المائة من مجموع الحواسيب في العالم، ويمثلون ٧٦,٢ في المائة من مستخدمي الإنترنت، و٩٧,٥ من مضيفي الإنترنت في العالم.[١٨]

١٩- ولا يوجد في معظم البلدان النامية قطاع للاتصالات قادر على دعم هذه النظم الدينامية والحديثة والفعالة للمعلومات والاتصالات. وفي عام ٢٠٠٠، أفادت الأمم المتحدة أن ٤,٥ في المائة فقط من سكان العالم لديهم فرصة للنفاذ إلى الشبكة، قياسا بنسبة ٤٤ في المائة من سكان أمريكا الشمالية و١٠ في المائة من الأوروبيين النفاذ إليها، بينما تتراوح معدلات النفاذ في أفريقيا وآسيا وأمريكا الجنوبية بين ٠,٣ و ١,٦ في المائة.[١٩] وأكثر من ٩٨ في المائة من عرض نطاق برتوكول الإنترنت العالمي، على المستوى الإقليمي، يستخدم حاليا للاتصال من أمريكا الشمالية وإليها. وتستأثر ٥٥ بلدا بنسبة ٩٩ في المائة من الإنفاق العالمي على إنتاج تكنولوجيا المعلومات (E/200/52، الفقرتان ٥٠ و ٥١). وثمة اتجاه واضح نحو الاقتصادات القائمة على المعرفة، غير أن عوامل أخرى غير التنمية، مثل هيكل خدمات الاتصالات وتكاليف الحصول عليها، تؤثر على معدلات النفاذ والاستخدام.

٢٠- ومع ذلك، فبينما تبدأ فوائد تكنولوجيا المعلومات والاتصالات في الانتشار على نحو أوسع من ذي قبل، سيلزم أيضا إذكاء الوعي بالأخطار المتزامنة مع هذا الانتشار وبأوجه الضعف المرتبطة بالجرائم المتصلة بالحواسيب. فالفجوة الرقمية لا تشير فقط إلى الفوارق

الاقتصادية بين البلدان المتقدمة النمو والبلدان النامية والبلدان ذات الاقتصادات الانتقالية،[٢٠] وإنما تكشف أيضا أنماطا مختلفة في الأخطار وأوجه الضعف الناجمة عن الجرائم السيبرانية. فتكنولوجيا المعلومات والاتصالات تُعتمد في أوقات مختلفة في المناطق المختلفة لا لمجرد وجود تفاوتات بين البلدان الغنية والبلدان الفقيرة ولكن بسبب عوامل من قبيل الجغرافيا الإقليمية. ففي بعض البلدان ذات التضاريس الجبلية مثلا قد تكون تكلفة وضع كبلات تحت الأرض للاتصالات رادعة، بينما يؤدي تركيب نظم الأبراج والهوائيات الميكروويفية للترحيل إلى فعالية تبني شبكات لاسلكية للهاتف. وبهذا الشكل، فإن نمط تكنولوجيا المعلومات والاتصالات في بلد أو منطقة قد يكون مختلفا تماما عنه في منطقة مجاورة أو بلد مجاور. ويؤدي التباين في الأخذ بالابتكارات التكنولوجية إلى اختلاف أنماط الابتكارات الإجرامية، ومن ثم اختلاف الأخطار الناجمة عن الجرائم المتصلة بالحواسيب.

٢١- ومن الممكن استخدام أي بلد نام لديه الحد الأدنى من البنى الأساسية للاتصالات كمنطقة حشد لشن هجمات، أو كبلد عبور توجه من خلاله الهجمات، خاصة إن لم يكن لدى ذلك البلد أي عقوبات قانونية تثني عن ارتكاب جرائم حاسوبية أو تكفل الملاحقة القضائية لهذه الأفعال. وبالنسبة إلى البلدان النامية، قد تؤدي أنواع التكنولوجيات التي عممت في أول الأمر وتمت المحافظة عليها إلى أخطار جديدة على المنطقة بعينها. وقد يقول البعض إن هياكل تكنولوجيا المعلومات الناشئة والتي لا تزال هشة قد تكون معرضة للخطر بشكل غير تناسبي إلى حين أن تصبح النظم أكثر قوة ومعايير الأمن أكثر صلابة.[٢١]

٢٢- ويمكن أن يكون نوع ونطاق الحواسيب والشبكات المناظرة في البيئات المؤسسية أو الحكومية مختلفا تماما عن بيئة المستهلك أو المقيم. ونظرا إلى أن تبني تكنولوجيا المعلومات والاتصالات يبدأ في الزيادة بين عامة الناس، فإن مجموعات مستهدفة جديدة تأخذ في الظهور وتصبح معرضة لمجموعات محددة من الجرائم المتصلة بالحواسيب تتراوح بين الإصابة بالفيروسات واقتحام الحواسيب من جهة، وأشكال مختلفة من غش المستهلكين من جهة أخرى. ومع تبني البلدان لتكنولوجيا المعلومات والاتصالات تتعرض قطاعات مختلفة من المجتمع لأنواع مختلفة من الجرائم المتصلة بالحواسيب.

رابعا- عبر الحدود: الجريمة العابرة للحدود والتحاليل الجنائية الحاسوبية

٢٣- يجب مواجهة عدد من المشاكل المرتبطة بالتحاليل الشرعية عند التحقيق في الجرائم المتصلة بالحاسوب. وجزء من المشكلة المواجهة في إعادة تكوين حادث ينطوي على جريمة سيبرانية يتمثل في أن شطرا كبيرا من الأدلة غير ملموس وسريع الزوال. وعوضا عن الأدلة

المادية، تبحث التحقيقات في الجرائم السيبرانية عن آثار رقمية غالبا ما تكون سريعة الزوال وقصيرة العمر. وأحد أسباب سرعة زوالها هو أن بعض أنواع العناوين الإلكترونية والمعلومات المتعلقة بالمسارات (أي "بيانات حركة المرور") لا تخزن بشكل دائم. وربما لا تبقى هذه المعلومات إلا في ذاكرة النظام الحاسوبي لمدة قصيرة ثم تحل محلها مسالك معلومات أخرى.

٢٤- غير أن التكنولوجيات الجديدة لا تخلق مشاكل جديدة فحسب، ولكنها تخلق أيضا فرصا جديدة للمحققين إذ أنها تسمح بإعادة تكوين القنوات الرقمية. ففي ظروف كثيرة يجوز أن تخزن بيانات حركة المرور وأشكال أخرى من معلومات إدارة الشبكة في سجلات بدلا من مسحها. أما في شبكات الإنترنت وشبكات الحواسيب الأخرى، فإن مجموعة متنوعة من معلومات إدارة الشبكة تخزن عادة لتحليلها فيما بعد للمساعدة في حسابات الشبكة، وتحديد عولية الخدمة، وعولية أجهزة الشبكة، والسجل الزمني للأخطاء، واتجاهات الأداء، والتنبؤ بالقدرات. وإضافة إلى هذه الأغراض، قد يكون هناك أيضا استخدامات لهذه البيانات لأغراض التسويق وتحديد ملامح المستهلكين (مثل طلبات الحصول على صفحات في المواقع الشبكية للبيع بالتجزئة للمساعدة على تحديد المنتجات الأكثر رواجا أو أنماط التسوق أو ملامح المستهلكين).

٢٥- بيد أن هناك عددا من الاعتبارات تحدد ما إن كانت بيانات حركة المرور أو المعلومات المشابهة ستخزن. وأحد هذه العوامل على سبيل المثال هو نوع الخدمة. فخدمة النفاذ إلى الشبكة (باستخدام بروتوكول خدمة التحقق عن بعد للمستخدمين الثنائيين (RADIUS) مثلا) قد تخزن بعض أنواع المعلومات الخاصة بالمشترك وبعض بيانات المرور للسماح للمشتركين بالنفاذ إلى الإنترنت. وهذا هو النمط السائد بشكل خاص في الخدمات الموقوتة والتي يجب أن تسجل متى دخل المشترك على الشبكة ومدة استخدامه لها. وعلى النقيض، فإن هذه المعلومات تكون ضئيلة جدا فيما يتعلق بالخدمات التي تغفل الهوية أو تعزز الخصوصية.[٢٢]

٢٦- والبريد الإلكتروني، الذي يرجع تاريخه إلى بدايات الإنترنت (كان متاحا على شبكة ARPANET في عام ١٩٧١) يتضمن عادة في عنوان التطبيق معلومات عن العنوان وبيانات أخرى خاصة بحركة المرور.[٢٣] وينشئ بعض هذه المعلومات برنامج عميل المستخدم النهائي، والبعض الآخر عن طريق وحدة خدمة البريد الإلكتروني (باستخدام بروتوكول نقل البريد البسيط SMTP).

٢٧- وأشهر خدمة للإنترنت هي على الأرجح شبكة ويب العالمية، ويستخدم معظمها نظام أسماء المجالات (DNS) لإقامة علاقة بين أسماء المجالات (اسم مكان وجود المواقع على الشبكة) وعناوين بروتوكول الإنترنت (العنوان العددي الذي تنتقل منه وإليه مجموعات الرسائل). ويمكن أن تخزن وحدات خدمة الشبكة كميات كبيرة من بيانات حركة المرور بشأن الصفحات التي تم طلبها وهوية الذي طلبها (أي عن طريق أي عنوان من عناوين مقدمي الخدمات). وهذه الممارسة أكثر شيوعا في وحدات الخدمة التجارية حيث سريعا ما تصل بيانات الدخول إلى مستويات الجيغا بايت، ومن ثم يمكن أن يكون تخزينها مكلفا.

٢٨- ويجوز أن تجمّع خدمات نقل الملفات المعلومات الخاصة بالمشترك في سجلات، أو قد لا يجوز ذلك، رهنا بالتنفيذ. وكان يجري نقل الملفات فيما مضى باستخدام بروتوكول نقل الملفات (FTP) على الرغم من أن عمليات نقل الملفات بشكل مأمون يجري تشفيرها بشكل متزايد باستخدام برمجية (Secure Shell) SSH. وعوضا عن وحدات خدمة الملفات المركزية، ظهر في الآونة الأخيرة نموذج الند بالند (P2P) الذي يسمح بتقاسم الملفات بين أعداد كبيرة من المستخدمين (موارد لا مركزية موزعة عبر شبكات مؤلفة من كيانات عابرة منها على سبيل المثال Napster, KaZaA, Morpheus, Gnutella, Freenet). ويتيح بعض أنواع نموذج الند بالند الحصول بسهولة على بيانات حركة المرور، بينما تصمم أنواع أخرى تحول دون تحليل حركة المرور.

٢٩- وتشمل خدمات أخرى المجموعة الإخبارية البالغ عددها نحو ١٠٠ ٠٠٠ على شبكة Usenet، وتتناول كل موضوع يمكن تصوره تقريبا. ويمكن النفاذ إلى هذه المجموعات من خلال شبكة عالمية ذات وحدات خدمة للتخزين والإحالة تستخدم بروتوكول نقل أخبار الشبكة (NNTP) – وقد تتوافر بعض البيانات عن حركة المرور من وحدة الخدمة بينما تكون بيانات أخرى على الحاسوب الشخصي المحلي. كما أن هناك أشكال كثيرة من الدردشة الآنية من غرف الدردشة على الإنترنت (IRC) إلى الرسائل اللحظية (Instant Messaging).

٣٠- ويجري عموما تناول خدمات الإنترنت المختلفة من خلال أجهزة شبكية مختلفة (مثل وحدات التوجيه ووحدات الخدمة). ورهنا بتشكيل موقع مقدم الخدمة، يمكن تخزين سجلات مختلفة في أجهزة كثيرة مختلفة، ويحتمل أن تكون تحت سيطرة كيانات قانونية مختلفة وتقع، في بعض الحالات، في ولايات قضائية مختلفة.

٣١- ونظرا إلى نطاق الخدمات المحتملة وبيئات الأسواق المختلفة ومجموعة عوامل منها تكلفة الاحتفاظ بالبيانات،[٢٤] يمكن القول بأنه لا يوجد موقف موحد لقطاع الأعمال أو الصناعة بشأن جمع البيانات الخاصة بحركة المرور وبالمشتركين والاحتفاظ بها. ومن البديهي أن الاحتفاظ ببعض البيانات الخاصة بحركة المرور وبالمشتركين يمكن أن ييسر تتبع أثر المجرمين على الإنترنت من قبل أجهزة إنفاذ القانون. وقد اعتمد عدد من البلدان مؤخرا تشريعات تفرض الاحتفاظ بالبيانات. وحتى في حالة عدم وجود قوانين تقضي بالاحتفاظ ببيانات حركة المرور، فمن الأهمية القصوى أن يفهم المحققون الجنائيون نطاق الممارسات المحاسبية والإدارية لشبكات مقدمي خدمات الإنترنت لتحديد ما مدى إمكانية تلبية متطلبات أجهزة إنفاذ القانون عن طريق الممارسات الروتينية لمقدمي خدمات الإنترنت.[٢٥] وتعاون مقدمي خدمات الإنترنت قد يكون نفيسا عندما تسعى السلطات إلى التحقيق في جريمة حاسوبية وملاحقة مرتكبيها.

٣٢- وغالبا ما تقتضي فعالية التحقيق والملاحقة القضائية تتبع أثر النشاط الإجرامي من خلال مجموعة متنوعة من مقدمي خدمات الإنترنت أو الشركات المقدمة لتلك الخدمات مع توصيل الحواسيب بالإنترنت. وحتى ينجح المحققون في ذلك، فعليهم أن يتتبعوا أثر قناة الاتصالات بالحواسيب المصدرية وحاسوب الضحية أو بأجهزة أخرى تعمل مع مقدمي خدمات وسطاء في بلدان مختلفة. ولتحديد مصدر الجريمة، غالبا ما يتعين على أجهزة إنفاذ القانون الاعتماد على السجلات التاريخية التي تبين متى أجريت توصيلات مختلفة ومن أين ومن الذي أجراها. وفي أحيان أخرى، قد يتطلب أيضا إنفاذ القانون تتبع أثر التوصيل وقت إجرائه. وعندما يكون مقدمو الخدمات خارج نطاق الولاية القضائية الإقليمية للمحقق، وهو ما يحدث في أغلب الأحيان، فإن أجهزة إنفاذ القانون تحتاج إلى المساعدة من نظرائها في ولايات قضائية أخرى. وتوضع عادة تدابير المساعدة القانونية المتبادلة التقليدية بل والعاجلة للحصول على بيانات تاريخية وآنية في الحالات التي لا تنطوي إلا على بلدين (بلد الضحية وبلد الجاني مثلا). وعندما يوجه المجرم الاتصالات عبر ثلاثة أو أربعة أو خمسة بلدان، فإن عملية المساعدة القانونية تستغرق فترات متعاقبة قبل أن تحصل أجهزة إنفاذ القانون على البيانات من كل مقدم للخدمات في قناة الاتصالات الأكثر اتساعا، مما يضاعف من احتمالات عدم توافر البيانات أو ضياعها، واستمرار عدم تحديد هوية المجرم وتمتعه بالحرية لارتكاب أعمال إجرامية أخرى.[٢٦]

٣٣- ومن أجل المساعدة في التحقيق بشأن الجرائم المتصلة بالحاسوب، أنشأ الفريق الفرعي التابع لمجموعة الـ٨ والمعني بالجرائم المتصلة بالتكنولوجيا الراقية في عام ١٩٩٧ نقاط

اتصالات تعمل ٢٤ ساعة يوميا بشأن القضايا الدولية المتصلة بالتكنولوجيا الراقية الجرائم المتصلة بالحواسيب، وهي قائمة بوحدات الجرائم الحاسوبية متاحة لأجهزة إنفاذ القانون الأخرى ٢٤ ساعة يوميا على مدار الأسبوع (٧/٢٤"). وشبكة الاتصالات، التي تضم حاليا ٤٠ بلدا، هي أيضا جزء لا يتجزأ من اتفاقية مجلس أوروبا المتعلقة بجرائم الفضاء الحاسوبي، والتي توفر مجموعة من أدوات التحقيق لمكافحة أي جريمة ترتكب ضد أي نظام حاسوبي و/أو من خلاله.

٣٤- ومع انتشار الفيروسات والديدان والقراصنة الذين يستغلون ضعف النظم، يلزم أيضا وجود آليات تمكّن من التصدي الفوري لذلك. ولذا أنشئت فرق التصدي للطوارئ الحاسوبية (CERTs) في عشرات البلدان في العالم. وتتمثل المهام الرئيسية لهذه الفرق فيما يلي:

(أ) تقديم نظرة شاملة عن طرائق شن الهجمات وعن أوجه الضعف إزاءها، وعن تأثير الهجمات على نظم وشبكات المعلومات؛ وتقديم معلومات عن اتجاهات وخصائص الحوادث وأوجه الضعف إزاءها؛

(ب) إنشاء بنية أساسية من مهنيين متخصصين بشكل متزايد في مجال الأمن يتمتعون بكفاءة متزايدة، ويتصدون على وجه السرعة للهجمات الموجهة إلى النظم الموصلة بالإنترنت، وبمقدرتهم حماية نظمهم مما يخل بأمنهم؛

(ج) تقديم طرائق لتقييم أمن النظم الشبكية وقدرتها على الاستمرار، وتحسينهما وصيانتهما؛

(د) العمل مع البائعين على تحسين أمن المنتجات المجهزة بحالتها.[٢٧]

٣٥- فإذا كان مرتكب الهجوم في بلد ما، وشُن الهجوم من حواسيب موجودة في بلد آخر، ووقعت الآثار المترتبة على ذلك في بلد ثالث، فمن البديهي أن هناك، علاوة على سرعة زوال البيانات، تحديات قانونية تنجم عن مشاكل الحدود والولايات القضائية. وتؤكد التحقيقات في الجرائم المتصلة بالحواسيب وملاحقتها قضائيا أهمية المساعدة القانونية المتبادلة. غير أن مسائل السيادة لا تمثل إلا قضية من القضايا التي تنشأ في حالات البحث والضبط عبر الحدود. ودون مساعدة قانونية متبادلة على نحو ملائم يحتمل أن يجري موظفو إنفاذ القانون في إحدى الدول التي تسعى إلى الحصول على معلومات في حواسيب موجودة في دولة أخرى عمليات بحث عابرة للحدود غير مرخص بها في النظم الحاسوبية. بيد أنه قبل النظر حتى في المساعدة القانونية المتبادلة يلزم النظر في التشريعات المحلية. فالتعاون الدولي يتطلب في

نهاية المطاف مع ذلك أن يكون لدى البلدان بالفعل قوانين قادرة على التصدي للجرائم الحاسوبية.

خامسا- التشريعات الوطنية: الشرط الأساسي اللازم

٣٦- تنتشر أحيانا بعض أنواع الجرائم المتصلة بالحواسيب مثل العدوى عبر الحدود الوطنية. وفي حالات أخرى تتسرب عناصر الجريمة عبر الحدود في إطار إستراتيجية حذرة ومتعمدة للتعتيم والتضليل. وزيادة كثافة تكنولوجيات المعلومات والاتصالات لجني فوائد مجتمع المعلومات تؤدي أيضا إلى زيادة تواتر الجرائم المحلية المتصلة بالحواسيب. ومن هنا فإن من مصلحة الأمن الاقتصادي والأمن العام للبلدان أن تسن تشريعات محلية لمكافحة الجرائم المتصلة بالحواسيب.

٣٧- لقد تطورت القوانين الوطنية على مدى قرون بينما تطورت الإنترنت على مدى عقود فقط. وغني عن القول ان القانون يواصل التكيف مع تغير المجتمع. وربما تحتاج التشريعات المحلية إلى التحديث للتصدي للجرائم المتصلة بالحواسيب. وقد قدم سيبير قائمة مؤلفة من ست موجات رئيسية للتشريعات المعنية بالجرائم الحاسوبية التي اعتمدتها البلدان منذ السبعينات من القرن الماضي:[٢٨] (أ) حماية البيانات وحماية الخصوصية؛ (ب) القانون الجنائي للتصدي للجرائم الاقتصادية المتصلة بالحواسيب؛ (ج) حماية الملكية الفكرية؛ (د) الحماية من المضمون الضار وغير القانوني؛ (ه) قانون الإجراءات الجنائية؛ (و) لوائح قانونية بشأن تدابير من قبيل التشفير والتوقيعات الرقمية.[٢٩]

٣٨- ويلزم وجود عدد من العناصر للتصدي للجرائم المتصلة بالحواسيب، هي: (أ) كفالة تحديد الجرائم في القانون؛ (ب) إنشاء سلطات تحري قانونية لمكافحة الجرائم السيبرانية؛ (ج) العمل على تحقيق ذلك على نحو يوفر الضمانات التي تحمي حقوق الإنسان الأساسية والحريات الأساسية.

ألف- الجرائم الرئيسية

٣٩- أعدت قوائم شاملة بالجرائم ضد سرية النظم الحاسوبية وسلامتها وتوافرها.[٣٠] وهناك أيضا عدد من الجرائم المتصلة بالمضمون (مثل إنتاج وتوزيع مواد إباحية خاصة بالأطفال أو بكراهية الأجانب) مدرجة في الجرائم المتصلة بالحواسيب.

أفاد مكتب الإشراف على أمن المعلومات بوزارة الأمن العام في الصين أنه تم تسجيل ما يقل قليلا عن ٥٠٠٠ جريمة حاسوبية في عام ٢٠٠١، بزيادة عن عام ٢٠٠٠ الذي بلغ عدد الجرائم فيه ما يقرب من ٢٩٠٠ جريمة، وعن عام ١٩٩٩ الذي بلغ عدد الجرائم فيه زهاء ٤٠٠ جريمة. وفي منتصف عام ٢٠٠٢، أبلغ المكتب عن ما يربو قليلا على ٣٠٠٠ حالة، ويُقدر أنه سيلزم التعامل مع ٣٥٠ حالة اقتحام للنظام وما يزيد على ٨٠٠ حالة إتلاف حاسوبي بحلول نهاية عام ٢٠٠٢.[٣١] وعدد الحالات التي حددها المكتب يتزايد بمعدل مذهل، على الرغم من عدم الإبلاغ عن كثير منها أو عدم ملاحظته. ومعظم مرتكبي هذه الجرائم من الشباب (يتراوح عمرهم بين ١٨ و٣٠ سنة)، وتُشن معظم الهجمات من مقاهي إنترنت حجب فيها المجرمون هويتهم بالنفاذ عبر http أو Sock proxy عن طريق عناوين زائفة لمقدمي الخدمات أو باستخدام التشفير أو تقنية إخفاء الرسائل. وتم بناء على ذلك اتخاذ تدابير أكثر صرامة بشأن تسجيل مقاهي الإنترنت ومراقبتها في الصين.

٤٠- وأثيرت مجموعة من الأسئلة عندما حاولت البلدان تكييف الأحكام المخصصة للسلع المادية وحاولت استخدامها في عالم السلع الرقمية "غير الملموس" و"السريع الزوال".

٤١- ويلزم توخي الحذر عند صياغة الأحكام من أجل تجنب تجريم أفعال قد تكون مشروعة. فهناك خط رفيع بين الجانب الخاص والجانب العام عند تحديث القانون الجنائي. ومن الممكن أن تصبح الأحكام المصيغة بعبارات محددة عتيقة عند ظهور تكنولوجيات أحدث. وبناء على ذلك، فمن المستصوب استخدام عبارات "محايدة من الناحية التكنولوجية".

باء- السلطات الإجرائية

٤٢- لقد تعين على كثير من البلدان في السنوات الأخيرة التصدي لمسائل تتعلق بتعريف "الوثائق"، نتيجة لزيادة انتشار السجلات الإلكترونية. بل أن مصطلحات أساسية من قبيل مفهوم "المكان" موضع البحث قد تصبح تحديات قانونية عندما تكون البيانات موزعة عبر شبكة حاسوبية (أي أن البحث قد يكون عن حاسوب في مكتب ما في أحد الأماكن ولكن البيانات قد تكون مخزنة في حاسوب في مكان مادي آخر – على الرغم من وجوده "افتراضيا" أمام المستخدم والمحققين).

٤٣- ومن المفيد عند إعداد سلطات إجرائية التمييز بين ثلاثة أنواع من المعلومات: (أ) المضمون الفعلي للاتصالات الإلكترونية، (ب) بيانات حركة المرور، (ج) معلومات عن المشتركين. ولعل من المستصوب التمييز بين هذه الأنواع الثلاثة لأنها قد تبعث على توقعات مختلفة بشأن الخصوصية، أو حماية البيانات، أو تستهل حقوق إنسانية وحريات أساسية أخرى.

٤٤- ومن التحديات القانونية الأولى وضع تعريف لمصطلح "بيانات حركة المرور" و "معلومات عن المشتركين". وتُعرّف اتفاقية مجلس أوروبا المتعلقة بجرائم الفضاء الحاسوبي[٣٢] مثلا "بيانات حركة المرور" بأنها: "أي بيانات حاسوبية تتعلق باتصال عن طريق نظام حاسوبي، وتنشأ عن نظام حاسوبي يشكل جزءا من سلسلة الاتصالات، وتشير إلى مصدر الاتصال ومقصده ومسلكه وتوقيته وتاريخه وحجمه ومدته ونوع الخدمة الأصلية" (المادة ١). وتُعرّف الاتفاقية "المعلومات عن المشتركين" بأنها: "أي معلومات، مدرجة في شكل بيانات حاسوبية أو أي شكل آخر، ويحتفظ بها مقدم الخدمات، وتتعلق بالمشتركين في الخدمات التي يقدمها، وتختلف عن البيانات المتعلقة بحركة المرور أو بالمضمون، ويمكن بموجبها تحديد:

"أ- نوع خدمة الاتصالات المستخدمة، والأحكام التقنية المتصلة بها ومدة الخدمة؛

"ب- هوية المشترك، وعنوانه البريدي أو الجغرافي، ورقم هاتف الخدمة وأرقام النفاذ الأخرى، والمعلومات الخاصة بالفواتير والسداد، المتاحة على أساس اتفاق أو ترتيب الخدمة؛

"ج- أي معلومات أخرى عن موقع تركيب أجهزة الاتصال المتاحة على أساس اتفاق أو ترتيب الخدمة" (الفقرة ٣ من المادة ١٨).

٤٥- وتناول دليل الأمم المتحدة لمنع الجريمة المتصلة بالحواسيب ومكافحتها[٣٣] مسألة التعاريف، كما تصدى لها القرار الإطاري بشأن الهجمات ضد نظم المعلومات الصادر عن مجلس الاتحاد الأوروبي، فضلا عن تناولها في تشريعات وطنية.[٣٤]

٤٦- وفي التشريعات المحلية لكثير من البلدان قد تجتذب أنواع معينة من المضامين مزيدا من الحماية الدستورية في ضوء مفاهيم من قبيل "الاتصالات الخاصة" و "حرية التعبير". ولعل من الضروري من الناحيتين القانونية والإجرائية، والوضع هكذا، التمييز بين مضامين بعض أنواع اتصالات الإنترنت (الاتصالات الخاصة غير العامة) عن بيانات حركة المرور. ومن

الممكن في بعض السياقات أن تكون عناصر معينة من بيانات حركة المرور والمعلومات الخاصة بالمشتركين[٣٥] مرتبطة بأحكام حماية البيانات لأنها تشكل معلومات أساسية تتعلق بالأشخاص، الأمر الذي قد يستدعي حماية الخصوصية.

٤٧- وتجدر الإشارة إلى أن عملية جمع البيانات والاحتفاظ بها بعد ذلك مليئة بالمصالح والقيم المتضاربة لأصحاب المصالح المختلفين، وقد يكون من المستصوب السعي إلى إقامة توازن بين المصالح المشروعة المختلفة. وتُحدد عملية جمع البيانات في بعض الولايات القضائية على نحو صارم بموجب ممارسات عادلة خاصة بالمعلومات، تكون أحيانا مدرجة في تشريعات خاصة بحماية البيانات أو بالخصوصية تنص على عدم جمع البيانات إلا لأغراض محدودة، ولا تستخدم إلا لأغراض منصوص عليها، وبموافقة مدروسة، ورهنا بضمانات أخرى مفروضة على استخدامها (مثل التحقق من سلامة المعلومات، ومعرفة الجداول الزمنية لتدميرها، والنفاذ إلى المواضيع).[٣٦]

٤٨- وتثير تكنولوجيات التخزين والإحالة عادة أسئلة قانونية متميزة في تلك الولايات القضائية التي لديها نظم قضائية مختلفة للتعامل مع مراقبة المضمون في الوقت الحقيقي (مثل أحكام "استراق الأسلاك") على خلاف البحث والضبط. وفيما يتعلق بالجرائم المتصلة بالحواسيب، ربما يمثل ذلك مشكلة للبريد الإلكتروني الذي قد يتطلب إذنا لمراقبة المضمون في الوقت الحقيقي عندما تكون رسالة البريد الإلكتروني متحركة، ولكنها قد تتطلب أمرا بالبحث والضبط إذا كانت ساكنة (أي مخزنة في وحدة خدمة البريد الإلكتروني أو على المحرك الصلب للمستخدم النهائي). ومادامت الرسالة الإلكترونية لا تتغير جوهريا في كلتا الحالتين، فقد تنشأ شواغل نظرا إلى اللجوء إلى أداتين قانونيتين مختلفتين، مع احتمال وجود حدين قانونيين مختلفين.

٤٩- وثمة عدد من الأدوات القانونية المعدة للمساعدة في التحقيقات المتصلة بالحواسيب، بما في ذلك أوامر الحفظ والتقديم. وأمر الحفظ هو آلية مستعجلة تطلب من مقدم الخدمات أن يقوم بتخزين وحفظ البيانات القائمة الخاصة بمعاملة ما أو بعميل ما. وهذه الآلية الإجرائية مهمة في سياق الأدلة الإلكترونية نظرا إلى أن مسح هذه الأدلة أو تدميرها يمكن أن يكونا أسهل من مسح أو تدمير الأدلة المادية. وأمر الحفظ هو في جوهره أمر"بعدم المسح". وأمر الحفظ[٣٧] أمر مؤقت بطبيعته ويصدر عندما تعتزم أجهزة إنفاذ القانون تأمين السلطة القانونية اللازمة للحصول على البيانات (مثل أمر ضبط البيانات أو أمر التقديم للإفراج عن البيانات).

٥٠- و يطلب أمر التقديم من أمين الوثائق تقديم الوثائق أو إتاحتها لأجهزة إنفاذ القانون في غضون فترة زمنية محددة. وأوامر التقديم مماثلة لمذكرات البحث، وإن كان أمين الوثائق هو الذي يجري عمليات البحث بدلا من الشرطة في حالة أمر التقديم. وهذا النوع من الأوامر أقل إزعاجا حيث إن أمين الوثائق غالبا ما يكون في وضع أفضل لمعرفة مكان وجود الوثائق المعنية. ومن الشائع في أوساط الأعمال الحالية أن تخزن المؤسسات البيانات خارج نطاق الولاية القضائية التي تعمل فيها، ويكون ذلك في أغلب الأحيان للاستفادة من رخص تكاليف تخزين البيانات. وقد تكون مذكرة البحث غير ملائمة في هذه الظروف، بينما تمكّن أوامر التقديم مالك البيانات أو أمين البيانات من استرجاع الوثائق أو السجلات.

سادسا- نحو إيجاد حلول من خلال التعاون الدولي

٥١- قد يكون من الضروري أيضا اعتماد قوانين وطنية مكيفة للتصدي للجرائم السيبرانية، للاستجابة بفعالية للطلبات المقدمة من دول أجنبية لالتماس المساعدة أو للحصول على المساعدة من بلدان أخرى. وتوافق القوانين الوطنية مع قوانين الدول الأخرى هدف مهم عند إعداد تشريعات للتصدي للجرائم المتصلة بالحواسيب. ومن أجل احترام الحقوق السيادية للدول وتيسير التعاون الدولي، فإنه يلزم في نهاية المطاف استطلاع الإمكانيات التي تتيحها الآليات الرسمية الدولية مثل الاتفاقيات. وحتى تؤدي المساعدة القانونية المتبادلة وظيفتها بشكل فعال ينبغي أن تكون الجرائم الرئيسية والسلطات الإجرائية في إحدى الولايات القضائية متوافقة مع تلك الموجودة في الولايات القضائية الأخرى.

٥٢- والمجتمع الدولي يبدأ الآن فقط في مواجهة التحديات المتعددة المستمرة في الظهور في هذا المجال. فالهجمات العنيفة بهدف الحرمان من الخدمة التي تستخدم مئات الحواسيب المتواطئة في بضعة بلدان لمهاجمة مواقع شبكية تجارية في بلد آخر؛ أو الأضرار الكبيرة التي يسببها فيروس أو ديدان تكتسح ثلثي العالم تثير أسئلة جوهرية مثل أين ارتكبت الجريمة ومن الذي يقيم الدعوى؟ وثمة مسألة حاسمة أخرى ستتمثل فيما إن كانت الإجراءات الفعالة ستتوقف في نهاية الأمر على استعداد الدول وقدرتها على الالتزام بالتحقيق والملاحقة القضائية؟ ومن البديهي أن الجرائم عبر الوطنية المتصلة بالحواسيب مستعدة لاستغلال الثغرات الناجمة عن الاختلافات في الأطر القانونية وفي قدرة نظم العدالة الجنائية. وقد ينظر البعض إلى الأمر على أنه انتقاص من السيادة، بينما سيتمسك البعض الآخر بأن العالم يشهد تحولا في السيادة حيث تبدأ مجتمعات المعلومات في الظهور في شتى أنحاء العالم.

٥٣- وسريعا ما توجه هذه السيناريوهات الانتباه إلى تعقد قضية تسليم المجرمين، التي يمكن أن تثير هي ذاتها عددا من المشاكل. في حالة انعدام التوافق العملي للجرائم الرئيسية فمثلا قد تعرّف الجريمة على نحو لا يسمح بتلبية متطلبات التجريم المزدوج. وفي الوقت ذاته، ثمة قبول متنام بأن السلوك الأساسي أو العناصر الأساسية للجريمة هي التي يجب أن تكون متوافقة حيثما يقتضي الأمر تطبيق التجريم المزدوج، لا مجرد الشكل الذي صيغت به الجريمة في البلدان ذات الصلة. غير أنه حتى عندما لا يشكل التجريم المزدوج مشكلة في حالة محددة، فإنه قد لا ينظر إلى الجرائم المتصلة بالحواسيب على أنها جرائم خطيرة بالقدر الكافي (من حيث الأحكام الخاصة بالعقوبات مثلا) للوفاء بشروط تسليم المجرمين.

٥٤- بيد أنه على الرغم من التحديات، فقد تم تحقيق عدد من الإنجازات الهامة منذ عام ٢٠٠٠ عند انعقاد مؤتمر الأمم المتحدة العاشر المتعلق بمنع الجريمة ومعاملة المجرمين، من بينها صكان قانونيان جديدان هما اتفاقية مجلس أوروبا المتعلقة بجرائم الفضاء الخارجي واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، وهي اتفاقية عالمية النطاق، ولكنها تتعامل بشكل غير مباشر مع الجرائم السيبرانية عندما تقوم بها مجموعات إجرامية منظمة.

٥٥- وعلى المستوى الدولي، فإن كيانات مثل مكتب الأمم المتحدة المعني بالمخدرات والجريمة، والمنظمة الدولية للشرطة الجنائية، ومنظمة التعاون والتنمية في الميدان الاقتصادي (OECD)، ومجموعة الـ ٨ المؤلفة من بلدان فرادى، وهيئات إقليمية مثل الاتحاد الأوروبي، ومجلس أوروبا، ومنظمة الدول الأمريكية، ورابطة أمم جنوب شرق آسيا، ورابطة التعاون الاقتصادي لآسيا والمحيط الهادئ، تقدم الخبرة السياسية والتقنية اللازمة لتعزيز التعاون الدولي. وعلى عكس ما كان سائدا منذ بضع سنوات، فإنه أصبح من الممكن الآن التحدث عن توافق دولي في الآراء حول مكافحة الجرائم السيبرانية، لا سيما الأشكال عبر الوطنية التي غالبا ما تتخذها. ومن ثم فإن هناك أخيرا "مناخا أخلاقيا" إيجابيا لاتخاذ إجراءات متضافرة، سواء من خلال تدابير مدنية أو جنائية أو إدارية، ويقر هذا التعاون بما يسميه علماء علم الاجتماع بـ "المجتمعات ذات المصير المشترك".[٣٨]

٥٦- وقد فتحت الاتفاقية المتعلقة بجرائم الفضاء الخارجي للتوقيع في ٢٣ تشرين الثاني/نوفمبر ٢٠٠١، ووقعت عليها ٣٠ دولة وصدقت عليها ٨ دول (ويمكن أن توقع على الاتفاقية دول من خارج أوروبا ووقعت عليها بالفعل أربع دول غير أوروبية (كندا، واليابان، وجنوب أفريقيا، والولايات المتحدة). ودخلت الاتفاقية حيز النفاذ في ١ تموز/يوليه ٢٠٠٤. وهي تطلب من الدول الأطراف أن تنسق قوانينها الوطنية التي تعرّف الجرائم الرئيسية التي تشمل: الجرائم ضد سرية البيانات والنظم الحاسوبية وسلامتها وتوافرها، فضلا

عن الجرائم المتصلة بالحواسيب مثل التزوير والتدليس الحاسوبي، والجرائم المتصلة بانتهاك حقوق الطبع، وجرائم الإباحة الجنسية المتعلقة بالأطفال المرتكبة عبر نظام حاسوبي. وإضافة إلى ذلك، تنص الاتفاقية على مجموعة مهمة من السلطات الإجرائية منها أوامر التقديم وأوامر الحفظ المقصود بها تيسير التحقيقات والملاحقة القضائية في سياق الشبكات الحاسوبية العالمية. كما أنها تتضمن أحكاما لإنشاء نظام حثيث وفعال للتعاون الدولي. وأخيرا، فإن مسألة "جرائم الكراهية" على الإنترنت أدت إلى وضع بروتوكول إضافي للاتفاقية المتعلقة بجرائم الفضاء الخارجي لتجريم الأفعال القائمة على العنصرية أو كراهية الأجانب المرتكبة من خلال نظم حاسوبية،[٣٩] والتي فتحت للتوقيع في ٢٨ كانون الثاني/يناير ٢٠٠٣. ووقعت على البروتوكول الإضافي ٢٠ دولة وصدقت عليه دولتان.

٥٧- وفي عام ٢٠٠٢ اعتمد وزراء العدل لدول الكومنولث قانونا نموذجيا بعنوان قانون الحواسيب والجرائم المتصلة بالحواسيب.[٤٠] وهذا القانون النموذجي، الذي يربطه باتفاقية المتعلقة بجرائم الفضاء الحاسوبي إطار مشترك، يزود أجهزة إنفاذ القانون بأدوات ناجعة وحديثة لمكافحة الجرائم السيبرانية. ويمكن للمدعين العامين والمحققين والمشرعين تقييم المواد المعدة دوليا مثل المبادئ التوجيهية، والأدلة القانونية والتقنية، وأفضل الممارسات، والتشريعات النموذجية لمساعدة السلطات في إعداد تشريعات محلية.

٥٨- وتشارك الأمم المتحدة بنشاط منذ مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين (١٩٩٠) في التصدي لمختلف جوانب التطورات المتصلة بالحواسيب.[٤١] وفي عام ١٩٩٤ نُشر "دليل الأمم المتحدة لمنع الجريمة المتصلة بالحواسيب ومكافحتها"[٤٢] بمساعدة جوهرية ومالية كبيرة من حكومة كندا ومن عدد من الخبراء قدمتهم حكومات ومنظمات غير حكومية أخرى.

٥٩- وفي عام ٢٠٠٠، عقدت خلال المؤتمر العاشر حلقة عمل بشأن "الجرائم المتصلة بشبكات الحواسيب".[٤٣] وفي عام ٢٠٠١، قدم الأمين العام إلى لجنة منع الجريمة والعدالة الجنائية استنتاجات خلصت إلى دراسة عن التدابير الفعالة لمنع ومكافحة الجريمة ذات الصلة بالتكنولوجيا الراقية والحواسيب (E/CN.15/2001/4).

٦٠- وفي عام ٢٠٠٤، ونتيجة للمرحلة الأولى من مؤتمر القمة العالمي لمجتمع المعلومات (WSIS)، أنشأ الأمين العام رسميا الفريق العامل المعني بإدارة الإنترنت للنظر في رسائل الدعاية غير المرغوب فيها، والأمن السيبراني، والقضايا الأخرى المتصلة بالإنترنت تحضيرا للمرحلة

الثانية لمؤتمر القمة العالمي لمجتمع المعلومات الذي سيعقد في تونس في تشرين الثاني/نوفمبر ٢٠٠٥.

٦١- والجرائم المتصلة بالإنترنت ظاهرة دولية تتطلب حلا دوليا. وللتوصل إلى هذا الحل، ينبغي للمجتمع الدولي أن يستعرض بدقة الوسائل المتاحة له بالفعل لتعزيز التعاون الدولي. كما ينبغي له أن يسعى إلى زيادة معرفته وفهمه للمظاهر المختلفة للظاهرة، وللتحديات التي تطرحها هذه المظاهر، والسبل الممكنة والمستصوبة لمنع هذه الظاهرة ومكافحتها.

سابعا- التعاون في البحث في الجرائم المتصلة بالحواسيب

٦٢- إن مهمة توفير قاعدة أدلة لتطوير السياسات في المستقبل مسألة لا تخلو من التحديات. والبحث في الجرائم المتصلة بالحواسيب أول مراحلها. ولعل أشخاصا مطلعين ومؤسسات، في القطاعين العام والخاص، لا يرغبون لأسباب تجارية أو سياسية أو أمنية في تقاسم معرفتهم مع الباحثين. والمعلومات التي تسلك طريقها إلى السجل العام قد تكون في أغلب الأحيان غير كاملة أو غير دقيقة. وعلى الرغم من هذه المعوقات، فمن المهم إعداد قاعدة معارف حتى يمكن للجهود المبذولة لتضييق الفجوة الرقمية أن تحدث أثرا.

٦٣- ولا بد من استخدام مجموعة واسعة من طرائق البحث والنهج المقارنة لتوفير بيانات أساسية عن مدى انتشار وخطورة أنواع مختلفة من الجرائم السيبرانية. وإضافة إلى ذلك، فالبحوث التي تتناول فعالية القوانين الجديدة، واستراتيجيات حفظ الأمن، والملاحقة القضائية، من خلال استعراض الحالات ودراسات التناقص، حاسمة الأهمية. ويجب ألا تقتصر البحوث على بيانات الشرطة أو المحاكم، فهذان المصدران يجب أن يكونا أكثر تحديدا وانتظاما. وتشمل المجالات التي تتطلب بشكل عاجل إجراء بحوث سلوك الضحية والجاني، فضلا عن البقاء على علم بالتطورات التشريعية والتطورات الخاصة بإنفاذ القانون عبر العالم.[٤٤]

ثامنا- التعاون بين القطاع العام والقطاع الخاص في التصدي للجرائم المتصلة بالحواسيب

٦٤- ثمة اعتراف متزيد من قبل الحكومة وممثلي القطاع الخاص بالضرورة القصوى لتوثيق التعاون في سعيهما للتصدي للجرائم المتصلة بالحواسيب. فليس بوسع حكومة بمفردها أو مجموعة من الحكومات، ولا بوسع شركة بمفردها أو قطاع صناعة بأكمله أن ينجح في

ذلك. ولكن يجب أن يكون هناك بالأحرى شراكة قوية بين القطاعين العام والخاص قوامها الانفتاح وتبادل الاتصالات بقوة. ولعل من الواضح أن كيانات القطاع الخاص تقوم، وستواصل القيام، بدور حيوي في إعداد تكنولوجيات للمساعدة في منع الجرائم السيبرانية والتحقيق فيها. وبغض النظر عن الحلول التكنولوجي، فبوسع القطاع الخاص أن يقوم بدور هام أيضا، في مساعدة صانعي السياسات في تحديد أولويات وحلول تشريعية. وإضافة إلى ذلك، فقد أثبتت التجربة أن إقامة شراكة قوية بين الحكومة وقطاع الصناعة يمكن أن ييسر إنفاذ القانون ضد المجرمين السيبرانيين بمزيد من الفعالية.

٦٥- ومن المشجع تكاثر الشراكات بين القطاعين العام والخاص. وطالما اعترف أعضاء مجموعة الـ٨ بأن التصدي الفعال للجرائم السيبرانية يتطلب تعاونا غير مسبوق بين الحكومة وقطاع الصناعة، واتخذوا خطوات هامة في هذا الاتجاه، منها استضافة مؤتمرات بين ممثلي الحكومة وقطاع الصناعة لمناقشة الاهتمامات المشتركة والحلول الممكنة.[٤٥] وبالمثل، تبذل الأمم المتحدة، ورابطة التعاون الاقتصادي لآسيا والمحيط الهادئ، ومنظمة التعاون والتنمية في الميدان الاقتصادي، ومنظمات متعددة الأطراف جهودا متزايدة لإشراك القطاع الخاص في هذه الأنشطة.

٦٦- وفي كانون الأول/ديسمبر ٢٠٠٤، أعلن ممثلون لعدد من الصناعات وأجهزة إنفاذ القانون الدولي إنشاء شبكة تصيد (PhishNet) رقمية، وهي عملية تعاونية لإنفاذ القانون تجمع بين رواد الصناعة في مجال التكنولوجيا، والخدمات المصرفية والمالية، وشركات البيع بالمزادات على الإنترنت، وأجهزة إنفاذ القانون للتطرق لمسألة "التصيد"، وهو شكل مدمر ومتزايد من سرقة الهوية على الإنترنت. وتنشئ شبكة التصيد الرقمية خطا واحدا وموحدا للاتصال بين الصناعة وإنفاذ القانون حتى يتسنى جمع البيانات الحرجة لمكافحة التصيد وتقديمها لأجهزة إنفاذ القانون في الوقت الحقيقي. وبينما تركز مجموعات صناعية أخرى على تحديد مواقع التصيد على الشبكة وتقاسم أفضل الممارسات والمعلومات الخاصة بالقضايا، فإن شبكة التصيد الرقمية هي أول مجموعة من نوعها تركز على مساعدة أجهزة إنفاذ القانون الجنائي ومساعدتها في القبض على المسؤولين عن ارتكاب جرائم ضد المستهلكين من خلال التصيد، وملاحقتهم قضائيا. وتجمع شبكة التصيد الرقمية بين رواد الصناعة من تسعة من أكبر عشرة مصارف أمريكية ومقدمي خدمات مالية، وأربعة من أكبر خمسة مقدمي خدمات الإنترنت، وخمس من شركات التجارة والتكنولوجيا الرقمية، وتعمل مع أكبر أجهزة لإنفاذ القانون الاتحادي والدولي.

٦٧- وشكّل عدد من كيانات القطاع الخاص على مدى السنوات القليلة الماضية فريقا مع جامعة هونغ كونغ لعقد عدد من المؤتمرات الهامة بشأن الجرائم السيبرانية. وقد جمعت تلك الاجتماعات كبار موظفي العدالة وإنفاذ القانون من آسيا والمحيط الهادئ، فضلا عن أكاديميين بارزين وممثلين لمنظمات متعددة الأطراف رائدة منها الأمم المتحدة، ومجلس أوروبا، والمنظمة الدولية للشرطة الجنائية، ورابطة التعاون الاقتصادي لآسيا والمحيط الهادئ. وشملت مجالات النقاش التحديات التي يطرحها أمن الشبكات، والأخطار التي تهدد التجارة الإلكترونية مثل رسائل الدعاية غير المرغوب فيها، والتصيد، والأشكال الأخرى من التدليس والقرصنة على الإنترنت.

٦٨- وقد عمل المسؤولون عن إنفاذ القانون من جميع أنحاء العالم طوال السنوات القليلة الماضية إلى جانب عدد من الشركات المعروفة للتحقيق في حالات المدلسين على الإنترنت والمجرمين السيبرانيين، بمن فيهم عدد من أشهر الجهات الموجهة لرسائل الدعاية غير المرغوب فيها، وملاحقتهم قضائيا.

٦٩- وعلى الرغم من هذا التقدم المحرز، فإنه يمكن فعل المزيد لمواصلة زيادة مستوى التعاون بين الحكومة وقطاع الصناعة، ولتوفير مزيد من التنظيم والانتظام في الحوار والشراكة بين القطاعين العام والخاص.

تاسعا- التوصيات

٧٠- لعل المؤتمر الحادي عشر يرغب في النظر في التوصيات التالية، التي تمت صياغتها في اجتماعي خبراء استضافهما المعهد الكوري لعلم الإجرام بسيول، مع مراعاة التوصيات ذات الصلة المقدمة من الاجتماعات الإقليمية التحضيرية الحادي عشر:

(أ) يلزم التركيز بشكل واسع وشامل للتصدي لمشاكل الجرائم السيبرانية التي تتجاوز القانون الجنائي، والإجراءات الجنائية، وإنفاذ القانون. وينبغي أن يشمل هذا التركيز مقتضيات التشغيل المأمون للاقتصاد السيبراني الذي يعظم الثقة في الأعمال التجارية، والخصوصية الفردية، فضلا عن استراتيجيات تعزيز وحماية الابتكار والقدرة على توليد الثروة والفرص التي تتيحها تكنولوجيا المعلومات والحوسبة، بما في ذلك آليات الإنذار المبكر والتصدي في حالات حدوث هجمات سيبرانية. وفيما وراء منع الجرائم المتصلة بالحواسيب وملاحقتها قضائيا يتبدى التحدي الأكبر المتمثل في إيجاد ثقافة عالمية للأمن السيبراني، وتلبية

احتياجات جميع المجتمعات، بما فيها البلدان النامية وهياكلها الناشئة التي لا تزال هشة الخاصة بتكنولوجيا المعلومات؛

(ب) ينبغي زيادة تطوير التعاون الدولي على جميع الصعد. وينبغي للأمم المتحدة، نظرا إلى طابعها العالمي، ومع تحسين آليات التنسيق الداخلي حسبما نادت بذلك الجمعية العامة، أن تقوم بدور رائد في الأنشطة الحكومية الدولية لكفالة تشغيل الفضاء الحاسوبي وحمايته حتى لا يقوم مجرمون أو إرهابيون بإساءة استخدامه أو استغلاله. وينبغي على وجه الخصوص أن تؤدي الأمم المتحدة دورا مفيدا في النهوض بنهج عالمية لمكافحة الجرائم السيبرانية، وبإجراءات التعاون الدولي بغية تلافي الآثار السلبية للجرائم السيبرانية وتخفيف آثارها على البنى الأساسية الحرجة، والتنمية المستدامة، وحماية الخصوصية، والتجارة الإلكترونية، والخدمات المصرفية، والتبادلات التجارية؛

(ج) ينبغي تشجيع الدول كافة على تحديث قوانينها الجنائية في أقرب وقت ممكن من أجل التصدي للطابع الخاص للجرائم السيبرانية. وفيما يتعلق بالأشكال التقليدية للجرائم المرتكبة باستخدام التكنولوجيات الحديثة، يمكن إجراء هذا التحديث بتوضيح أو حذف الأحكام التي لم تعد كافية تماما، مثل القوانين التي تعجز عن التصدي لتدمير أو سرقة الأشياء غير الملموسة، أو بوضع أحكام جديدة للجرائم الجديدة، من قبيل النفاذ غير المسموح به إلى الحواسيب أو شبكات الحواسيب. وينبغي أن يشمل هذا التحديث القوانين الإجرائية للتتبع الاتصالات مثلا، وقوانين أو اتفاقات أو ترتيبات المساعدة القانونية المتبادلة لحفظ البيانات على وجه السرعة مثلا. ولتحديد قوة التشريعات الجديدة، ينبغي تشجيع الدول على أن تستلهم بأحكام اتفاقية مجلس أوروبا المتعلقة بجرائم الفضاء الحاسوبي؛

(د) وينبغي أن تعمل الحكومات والقطاع الخاص والمنظمات غير الحكومية يدا بيد لرأب الفجوة الرقمية، وإذكاء الوعي العام بشأن أخطار الجرائم السيبرانية واتخاذ التدابير المضادة الملائمة، وتعزيز قدرة العاملين في مجال العدالة الجنائية، بمن فيهم موظفو إنفاذ القانون والمدعون العامون والقضاة. وتحقيقا لهذا الغرض، ينبغي أن تشمل الإدارات القضائية الوطنية ومعاهد التعليم القانوني مناهج شاملة عن الجرائم المتصلة بالحواسيب في برامجها التعليمية؛

(هـ) وينبغي أن يولي المؤتمر الحادي عشر اهتماما كبيرا لتقرير الأدوات العملية الراهنة وتحسينها وتوسيع نطاقها من أجل تقاسم المعلومات على الصعيد الدولي، وآليات الإنذار المبكر والتصدي، وتدابير الحد من الأضرار في مكافحة الجرائم السيبرانية، باستخدام المنظمة الدولية للشرطة الجنائية، وآليات التحذير ٢٤/٧ لمجموعة الـ٨، والاتفاقية المتعلقة

بجرائم الفضاء الحاسوبي، وفرق التصدي للطوارئ الحاسوبية (CERTs)، ومنتدى فرق التصدي للحوادث والأمن (FIRST)، التي لا تزال تقتصر على بلدان معينة معظمها من البلدان المتقدمة النمو. وينبغي توفير هذه الأدوات دوليا من أجل تقاسم المعارف والمعلومات فيما يتعلق بوسائل وسبل الاعتراف بالأنواع الجديدة من الجرائم السيبرانية والحماية منها وتجنبها والتعامل معها، ومن أجل إطلاع الجمهور على آليات التصدي الفعالة. وإضافة إلى ذلك، ينبغي التركيز بشكل خاص على توفير هذه الأدوات العملية للبلدان النامية وتقديم التدريب المتصل بها؛

(و) وينبغي أن تقوم سياسات مكافحة الجرائم السيبرانية على أساس الأدلة، وأن تخضع لعملية تقييم صارمة لكفالة كفاءتها وفعاليتها. ولذا ينبغي بذل جهود متضافرة ومنسقة على الصعيد الدولي لإنشاء آليات تمويل لتيسير البحوث العملية وكبح أنواع كثيرة من الجرائم السيبرانية الناشئة حديثا. بيد أن كفالة تنسيق البحوث دوليا وإتاحة نتائجها على نطاق واسع لا يقل أهمية عن ذلك؛

(ز) وينبغي أن يرفع مكتب الأمم المتحدة المعني بالمخدرات والجريمة نتائج حلقة العمل المعنية بتدابير مكافحة الجرائم المتصلة بالحواسيب، والتي ستعقد خلال المؤتمر الحادي عشر، إلى المرحلة الثانية من مؤتمر القمة العالمي لمجتمع المعلومات الذي سيعقد في تونس العاصمة، في عام ٢٠٠٥، لينظر فيها.

الحواشي

(١) D. B. Parker, S. Nycum and S. S. Oüra, *Computer Abuse* (Menlo Park, California, Stanford Research Institute, 1973).

(٢) Donn B. Parker, *Computer Crime: Criminal Justice Research Manual* (Washington, D.C., United States Department of Justice, 1979).

(٣) Donn B. Parker, *Computer Crime: Criminal Justice Research Manual* (Washington, D.C., United States Department of Justice, 1989).

(٤) Russell G. Smith, Peter N. Grabosky and Gregor F. Urbas, *Cyber Criminals on Trial* (Cambridge, Cambridge University Press, 2004).

(٥) مجلس أوروبا، مجموعة المعاهدات الأوروبية، الرقم ١٨٥.

(٦) في بعض البلدان التي يستعمل فيها مستخدمو الإنترنت المقيمون الشبكات المحلية اللاسلكية، استخدمت الشبكات غير المؤمنة للنفاذ إلى الإنترنت بشكل غير مسموح به لأغراض متعددة. وغالبا ما يرتبط ذلك بما يسمى "قيادة الحرب" (استخدام حاسوب محمول في سيارة لتحديد نقاط النفاذ اللاسلكي أو "البقاع الساخنة" والنفاذ إليها).

(٧) لا يشير مفهوم السرقة في بعض البلدان إلا إلى السلع الملموسة ويتضمن حرمان الشخص من شيء ملموس؛ ومن ثم فإن هذا المفهوم لا يتسع ليشمل سلعة غير ملموسة ولا يغطي عملية استنساخ ملفي رقمي. ولا تتعامل بعض البلدان مع هذه الأفعال بتوقيع جزاءات جنائية أو عقوبات، ولكن تعتبر بالأحرى أن القانون المدني، بما في ذلك نظم حقوق الطبع، تغطيها.

(٨) تستخدم برمجية الند بالند التي أعدها Bram Cohen's Bit Torrent بشكل متزايد لتقاسم ملفات البيانات الكبيرة للأغراض المشروعة (مثل توزيع برمجيات من مصادر مفتوحة، أو ألعاب حاسوبية، أو "اختيار الأقران" للبرمجة التلفزيونية) وجانب قراصنة الفيديو. وللإطلاع على عرض عام لقرصنة الفيديو، انظر مقال Clive Thompson بعنوان "The Bit Torrent effect" في مجلة *Wired* بتاريخ ١٣كانون الثاني/يناير ٢٠٠٥؛ ومقال Jeff Howe بعنوان "The shadow Internet" الصادرين في مجلة *Wired* بتاريخ ١٣كانون الثاني/يناير ٢٠٠٥.

(٩) تقرير عن الغش على الإنترنت في عام ٢٠٠٣: ١ كانون الثاني/يناير-٣١ كانون الثاني/ديسمبر ٢٠٠٣ (المركز الوطني لجرائم أصحاب الأعمال، ومكتب التحقيقات الاتحادي، الولايات المتحدة).

(١٠) انظر Michael D. Mehta, Don Best and Nancy Poon, "Peer-to-peer sharing on the Internet: an analysis of how Gnutella networks are used to distribute pornographic material". *Canadian Journal of Law and Technology*, vol. 1, No. 1 (January 2002); and United States of America, General Accounting Office, *File Sharing Programs: Peer-to-peer Networks Provide Ready Access to Child Pornography*, GAO-03-351 (واشنطن، مقاطعة كولومبيا، شباط/فبراير ٢٠٠٣).

(١١) Dick Thornburgh and Herbert S. Lin, eds., *Youth, Pornography and the Internet* (Washington, D.C., National Academy Press, 2003).

(١٢) للإطلاع على عرض عام للقوانين السارية في ٢٤ بلدا، والتي تتصدى للمواد المشجعة على العنصرية وكراهية الأجانب ومعادة السامية، انظر الوثيقة المتعلقة بالموضوع التي نُظر فيها في مؤتمر منظمة الأمن والتعاون في أوروبا بشأن معاداة السامية، (CIO.GAL/25/04/Rev.1) المعقود في برلين من ٢٨ إلى ٢٩ نيسان/أبريل ٢٠٠٤.

(١٣) Scott Berinato, "The truth about cyberterrorism", *CIO Magazine*، ١٥ آذار/مارس ٢٠٠٢.

(١٤) للحصول على معلومات بشأن المنتجات المتوافرة تجاريا والتي تستخدم أسلوب التشفير الكمي لتشفير البيانات في النظم القائمة على الألياف البصرية أو الشبكات اللاسلكية، انظر مقال Gary Stix المعنون "Best-Kept Secrets"، *Scientific American*، كانون الثاني/يناير ٢٠٠٥.

(١٥) للإطلاع على تحليل لجوانب تكنولوجيا المعلومات والاتصالات في الأهداف الإنمائية للألفية، انظر تقرير الاتحاد الدولي للاتصالات *World Telecommunication Development Report 2003: Access Indicators for the Information Society*، الطبعة السابعة (٢٠٠٣). وتقدم هذه الدراسة تقييما هاما للأهداف الإنمائية للألفية ذات الصلة بتكنولوجيا المعلومات والاتصالات، ويبدو أن المؤشر الرقمي للنفاذ مبشر بشكل خاص.

(١٦) مركز معلومات شبكة الإنترنت بالصين، تقرير المسح الإحصائي الخامس عشر بشأن تطور الإنترنت في الصين، (كانون الثاني/يناير ٢٠٠٥)، (الموقع *www.cnnic.net.cn*) (الذي تمت زيارته في ٢٥ كانون الثاني/يناير ٢٠٠٥).

(١٧) Internet Systems Consortium (http://www.isc.org).

(١٨) معلومات مستقاة من قاعدة بيانات مؤشرات الاتحاد الدولي للاتصالات، الطبعة الثامنة (٢٠٠٤).

(١٩) دراسة الحالة الاقتصادية والاجتماعية في العالم، ٢٠٠٠ (منشور الأمم المتحدة، رقم المبيع E.00.II.C.1).

(٢٠) للإطلاع على تحليل إحصائي لتعقد الفجوة الرقمية، انظر الإطار المفاهيمي المقدم في الدراسة *Monitoring the Digital Divide ... and Beyond,* (2003).

(٢١) لوحظ أنه من المفارقة أن هذه الظروف تنشئ على مستوى مختلف "فجوة رقمية"، بالضبط بعد أن كادت هذه الفجوة لأن تندمل، وربما تفضي إلى تقويض الثقة في قطاع الأعمال على المستوى المحلي، أو تقويض الجاذبية إلى إجراء الاستثمارات اللازمة.

(٢٢) الفرق الرئيسي بين خدمة غفل وخدمة ذات اسم مستعار هي أن الخدمة ذات الاسم المستعار تحتفظ بهوية (اسم مستعار مثلا أو اسم غفل) لمدة معينة (ومن ثم فقد تكون هناك علاقة أقوى بين الهوية التي تحمل اسما مستعارا وهوية المشترك وهوية "العالم الحقيقي"). ومن ناحية أخرى، فإن الخدمة الغفل في شكلها المحض هي أساسا خدمة مكتملة أو ذات معاملة واحدة. وثمة أنواع مختلفة من الخدمات الغفل أو ذات الأسماء المستعارة، ويقدم معظمها خادم بروكسي proxy أو سلاسل أو شبكات مشتركة للنفاذ إلى خدمة أو أكثر من خدمات الإنترنت مثل خدمات إعادة إرسال البريد الإلكتروني، أو التجول على الشبكة، أو غرف الدردشة على الإنترنت، أو المجموعات الإخبارية Usenet newsgroups. وهناك أيضا درجات من إغفال الهوية أو استعارة الأسماء لا تتوقف فقط على عوامل مثل برمجية التشفير الأساسية أو برمجية التثبت من الهوية، وإنما تتوقف على طبيعة وأمن وحدة أو وحدات خدمة إغفال الهوية، وإجراءات إنشاء الاسم الغفل، وفي حالة خدمات الدفع، على آليات إعداد الفواتير.

(٢٣) David H. Crocker, rev., *Standard for the Format of ARPA Internet Text Messages*, RFC 822 (13 August 1982).

(٢٤) في حلقة العمل المعنية بالاحتفاظ بالبيانات، والمعقودة في إطار الحوار بين الحكومات وقطاعات الصناعة في مجموعة الثمانية بشأن سلامة الفضاء السيبراني والثقة فيه (برلين، تشرين الأول/أكتوبر ٢٠٠٠) تم تحديد الآثار المالية التالية للاحتفاظ بالبيانات: حجم السجلات المخزنة؛ استرجاع البيانات ذات الصلة؛ الهندسة والتطوير؛ تكاليف الإدارة والتشغيل والتدريب؛ توفير الأمن والخصوصية؛ المسؤولية عن تناول البيانات وتقديمها لإنفاذ القانون؛ التكاليف المرتبطة بالفرص وبثقة المستهلك.

(٢٥) قد يحتفظ مقدمو الخدمة بالبيانات لمدد زمنية مختلفة، رهنا بنماذج الأعمال والخدمات والتكنولوجيا. فيحتفظ ببعض البيانات لأغراض إعداد الفواتير، بينما يحتفظ ببيانات أخرى لمراجعة أداء النظام. وتتباين الأطر الزمنية من بضع ثوان إلى فترات أطول قد تكون مطلوبة أو مسموح بها بموجب التشريع الوطني، لأغراض غير إنفاذ القانون. كما يُحتفظ بأنواع مختلفة من بيانات حركة المرور لفترات زمنية مختلفة، فسجلات النفاذ إلى الشبكة (RADIUS أو TACACS+) مثلا لها متطلبات تجارية ومتطلبات خاصة بتخزين البيانات مختلفة عن سجلات بروتوكول نقل أخبار الشبكة (NNTP)، وربما تكون متوافرة نتيجة لذلك، في ظروف معينة، لفترات أطول. غير أن المضمون لا يحتفظ به ولا يتوافر عادة.

(٢٦) توصيات لتتبع أثر الاتصالات الشبكية عبر الحدود الوطنية في التحقيقات بشأن الإرهاب والأعمال الإجرامية (http://canada.justice.gc.ca/en/news/g8/doc2.html).

(٢٧) انظر مركز التنسيق التابع لفرقة التأهب للطوارئ الحاسوبية، التقرير السنوي العام ٢٠٠٣ (www.cert.org)؛ ومنتدى فرق التصدي للحوادث والأمن (www.first.org).

(٢٨) Ulrich Sieber, *Legal Aspects of Computer-Related Crime in the Information Society: COMCRIME Study* (١ كانون الثاني/يناير ١٩٩٨).

(٢٩) تم تطبيق نموذج سيبير الخاص بالموجات الرئيسية الست للتشريعات الوطنية على التجربة الأسترالية في منشور Russell G. Smith و Peter N. Grabosky و Gregor F. Urbas المعنون *"Cyber Criminals on Trial"* (كامبردج، مطبعة جامعة كامبردج، ٢٠٠٤).

(٣٠) منظمة التنمية والتعاون في الميدان الاقتصادي، *Computer-Related Crime: Analysis of Legal Policy, ICCP Series No.10, (1986)*. انظر أيضا التوصية رقم R (89) 9، التي اعتمدتها لجنة وزراء مجلس أوروبا في ١٣ أيلول/سبتمبر ١٩٨٩.

(٣١) التقرير القطري المقدم من الصين إلى مؤتمر آسيا والمحيط الهادئ المعني بالجرائم السيبرانية وأمن المعلومات، الذي نظمته اللجنة الاقتصادية والاجتماعية لآسيا والمحيط الهادئ ووزارة الإعلام والاتصالات بجمهورية كوريا في سيول في الفترة ١١-١٣ تشرين الثاني/نوفمبر ٢٠٠٢. وقد يكون عدد المجرمين كبيرا بالنظر إلى أنه تم القبض على ٥٢ مشتبها فيه في حي واحد من أحياء بيجين (دائرة إدعاء منطقة هايديان) بين عام ٢٠٠١ وأيار/مايو ٢٠٠٤ — ٤٨,٤ في المائة منهم بسبب القرصنة.

(٣٢) مجلس أوروبا، مجموعة المعاهدات الأوروبية، الرقم ١٨٥.

(٣٣) *International Review of Criminal Policy* (الاستعراض الدولي للسياسات الجنائية)، العددان ٤٣ و٤٤ (منشور الأمم المتحدة، رقم المبيع E.94.IV.5).

(٣٤) يقدم قانون تنظيم السلطات التحققية في المملكة المتحدة ٢٠٠٠ تعريفا لبيانات حركة المرور في المادة ٢-٩، وإن كان هذا التعريف يشمل أيضا "المعلومات عن المشتركين". ويرد مفهوم لبيانات حركة المرور في تعاريف الولايات المتحدة لمصطلح "جهاز تسجيل أرقام الهاتف" و "جهاز التصيد والتتبع" (United States Code, title 18, sect. 3127) وتم تحديثه من خلال قانون توحيد ودعم أمريكا بتوفير الأدوات المناسبة اللازمة لاعتراض الإرهاب وإعاقته لعام ٢٠٠١ (PATRIOT).

(٣٥) فيما يتعلق بالمعلومات عن المشتركين، قد يكون هناك بالفعل في عدد من البلدان لوائح في مجال الاتصالات الهاتفية (معلومات عن اسم الزبون وعنوانه).

(٣٦) تشمل الصكوك الدولية الهامة، على سبيل المثال، اتفاقية مجلس أوروبا لحماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية لعام ١٩٨١ (مجلس أوروبا، مجموعة المعاهدات الأوروبية، رقم ١٠٨) أو المبادئ التوجيهية لمنظمة التعاون والتنمية في الميدان الاقتصادي لعام ١٩٨٠ التي تنظم حرمة الحياة الخاصة ونقل البيانات الشخصية عبر الحدود. وقد سعت هذه الصكوك إلى وضع مبادئ يجب بمقتضاها الحصول على المعلومات الشخصية بشكل عادل؛ والاقتصار في استخدامها على الغرض المحدد أولا؛ وأن تكون كافية للغرض وذات صلة به وغير مفرطة؛ ودقيقة ومحدثة؛ ويمكن الوصول بها إلى الموضوع؛ وتُحفظ بشكل سري؛ وتدمر بعد تحقيق الغرض. كما تم تعزيز درجة الالتزام في بعض الولايات القضائية، مثلا من خلال توجيهات الاتحاد الأوروبي لحماية البيانات ١٩٩٥ — التوجيه 95/46/EC ، و١٩٩٧ — التوجيه 97/66/EC). وبناء على ما سبق، طبقت بلدان أوروبية عديدة قوانين أكثر صرامة لحماية البيانات للامتثال لالتزاماتها القانونية للوفاء بمعايير التوجيه. ويوجد أيضا خارج نطاق أوروبا صكوك تتضمن أحكاما مشابهة للتعامل مع البيانات الشخصية، مثل القانون الكندي لحماية البيانات الشخصية والوثائق الإلكترونية.

(٣٧) لاحظ أن "حفظ البيانات" يكفل عدم مسح المعلومات المحددة الموجودة والمتعلقة بأحد المشتركين. وعلى العكس من ذلك فإن "الاحتفاظ بالبيانات" مطلب عام مقصود بد إجبار جميع مقدمي خدمات الإنترنت على جمع مجموعة متنوعة من البيانات تتعلق بجميع المشتركين، والاحتفاظ بها.

(٣٨) Roderic Broadhurst, “Content crimes: criminality and censorship in Asia”, paper presented at Octopus Interface: the Challenge of Cybercrime، ستراسبورغ، فرنسا، ١٥-١٧ أيلول/سبتمبر ٢٠٠٤.

(٣٩) مجلس أوروبا، مجموعة المعاهدات الأوروبية، الرقم ١٨٩.

(٤٠) يمكن الإطلاع على القانون النموذجي على صفحات شعبة الشؤون القانونية والدستورية بأمانة الكومنولث على الشبكة على العنوان التالي: (http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/{DA109CD2-5204-4FAB-AA77-86970A639B05}_Computer%20Crime.pdf).

(٤١) عقد المؤتمر حلقة عمل عن "حوسبة إدارة العدالة الجنائية" (A/CONF.144/14). وقد أصدرت المنظمة منذ عام ١٩٩٢ "دليل حوسبة نظم المعلومات في ميدان العدالة الجنائية" (منشور الأمم المتحدة، رقم المبيع E.92.XVII.6). وعقد المؤتمر التاسع حلقة عمل أخرى عن "التعاون والمساعدة الدوليان في مجال إدارة نظام العدالة الجنائية: حوسبة عمليات العدالة الجنائية، وتنمية معلومات العدالة الجنائية وتحليلها واستخدامها في السياسات" (A/CONF. 169/13). (انظر أيضا معهد آسيا والشرق الأقصى لمنع الإجرام ومعاملة المجرمين التابع للأمم المتحدة، التحدي العالمي لجرائم التكنولوجيا الراقية: حلقة العمل بشأن الجرائم المتصلة بشبكات الحواسيب، ومؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين، ١٥ نيسان/أبريل ٢٠٠٠، فيينا، النمسا (وطوكيو، نيسان/أبريل ٢٠٠١)).

(٤٢) *International Review of Criminal Policy* (الاستعراض الدولي للسياسات الجنائية)، العددان ٤٣ و٤٤ (منشور الأمم المتحدة، رقم المبيع E.94.IV.5).

(٤٣) انظر ورقة معلومات أساسية من أجل حلقة العمل بشأن الجرائم المتصلة بشبكات الحواسيب (A/CONF.187/10).

(٤٤) Peter Grabosky and Roderic Broadhurst, “The future of cyber-crime in Asia”, *Cybercrime: the Challenge in Asia*, Roderic Broadhurst and Peter Grabosky, eds. (Hong Kong University Press, 2005), pp. 347-360.

(٤٥) انظر “G8 Berlin Meeting: Government/Industry Dialogue on Safety and Confidence in Cyberspace (Summary and Assessment)” (available at http://www.mofa.go.jp/policy/economy/summit/2000/lyon.html); and Kuriko Miyake, “G8 concludes Tokyo high-tech crime meeting” (available at http://archives.cnn.com/2001/TECH/internet/05/31/g8.cyber.crime.idg).