

Distr.: General
30 March 2001
Arabic
Original: English

المجلس الاقتصادي والاجتماعي



لجنة منع الجريمة والعدالة الجنائية

الدورة العاشرة

فيينا، ٨-١٧ أيار/مايو ٢٠٠١

البند ٤ من جدول الأعمال المؤقت*

التعاون الدولي على مكافحة الجريمة عبر الوطنية

استنتاجات الدراسة عن التدابير الفعالة لمنع ومكافحة الجريمة ذات الصلة بالتكنولوجيا الراقية والحواسيب

تقرير الأمين العام

ملخص

هذا التقرير مقدم استجابة، جزئياً، لطلب المجلس الاقتصادي والاجتماعي، في قراره ٢٣/١٩٩٩ المؤرخ ٢٨ تموز/يوليه ١٩٩٩، أن يجري الأمين العام دراسة عن التدابير الفعالة التي يمكن اتخاذها على الصعيدين الوطني والدولي لمنع ومكافحة الجرائم ذات الصلة بالحواسيب. ويعرض هذا التقرير فحواً أولاً للموضوع ويوصي بالاضطلاع بدراسة أكثر تفصيلاً وإحالتها إلى لجنة منع الجريمة والعدالة الجنائية في دورتها الحادية عشرة لكي تنظر فيها بصفقتها مسألة عالية الأولوية. كما يوصي التقرير بأن تنظر اللجنة أثناء دورتها الحادية عشرة في مجموعة من الخيارات بشأن اتخاذ مزيد من الإجراءات، بما في ذلك احتمال صوغ صك دولي لمكافحة الجريمة ذات الصلة بالحواسيب، والخيارات بشأن وضع استراتيجية قصيرة الأجل، بما في ذلك إنشاء برنامج عالمي للأمم المتحدة لمكافحة الجريمة ذات الصلة بالتكنولوجيا الراقية والحواسيب. كما يقدم هذا التقرير معلومات عن أنشطة منظمات دولية وحكومية-دولية أخرى ذات صلة ويحاول الاستجابة لبعض الشواغل التي أثارها الدول الأعضاء كل على حدة.

المحتويات

الصفحة	الفقرات	
٣	١	مقدمة..... أولاً-
٣	٣٤-٢	الخلفية..... ثانياً-
٣	١٢-٢	ألف- بحث المشكلة من جانب منظمات دولية-حكومية أو دولية أخرى ..
٦	١٣	باء- أنشطة الأمم المتحدة.....
٨	٢٩-١٤	جيم- طبيعة الجريمة ذات الصلة بالحواسيب والتكنولوجيا الراقية: تحديد أولي للأشكال.....
١١	٣٤-٣٠	دال- تقدير نطاق وتكاليف الجريمة ذات الصلة بالحواسيب والتكنولوجيا الراقية.....
١٣	٥٥-٣٥	ثالثاً- الاستنتاجات والتوصيات: وضع سياسات عالمية لمنع ومكافحة الجريمة ذات الصلة بالحواسيب والتكنولوجيا الراقية.....
١٣	٣٥	ألف- ضرورة معالجة الجريمة ذات الصلة بالحواسيب والتكنولوجيا الراقية كموضوع منفصل.....
١٣	٣٩-٣٦	باء- ضرورة مساعدة البلدان النامية.....
١٥	٤١-٤٠	جيم- ضرورة النظر في اتخاذ تدابير دولية ووطنية وذات صلة بالقطاع الخاص.....
١٥	٤٩-٤٢	دال- دور الأمم المتحدة.....
١٧	٥٠	هاء- عناصر دراسة مفصلة.....
١٨	٥٥-٥١	واو- خيارات وتوصيات محددة للاضطلاع بمزيد من العمل بشأن الجريمة ذات الصلة بالتكنولوجيا الراقية والحواسيب.....

أولاً - مقدمة

على معلومات أو معارف محضة. وهذا يثير مضاعفات كبيرة في مجالات مثل حقوق الإنسان والتنمية الاجتماعية والاقتصادية المستدامة. وسيكون من الهام أن تصبح مكافحة الجريمة عنصراً من تلك البرامج والعكس بالعكس. كما أن تكنولوجيا المعلومات والبنية الهندسية لشبكات الحواسيب والاتصالات تمثل بقدر كبير نتاج تطور القطاع الخاص، ولا بد من أن تراعى في وضع تدابير لمكافحة الجريمة ذات الصلة بالتكنولوجيا الرقابة والحواسيب عوامل مثل الجدوى التجارية والقدرة التنافسية الاقتصادية للتكنولوجيات المعنية.

ثانياً - الخلفية

ألف - بحث المشكلة من جانب منظمات دولية - حكومية أو دولية أخرى

٢- إن القلق المتزايد الذي تبديه الدول إزاء طبيعة هذه المشكلة ونطاقها، وضرورة اتخاذ تدابير عالمية ناجعة لمكافحةها، يدلّ عليهما عدد المحافل التي جرى فيها بحث هذه المشكلة.

١ - مجلس أوروبا

٣- أوشك مجلس أوروبا على الانتهاء من وضع نص اتفاقية بشأن الجريمة السيبرانية،^(١) وستتناول هذه الاتفاقية الأفعال الجنائية ذات الصلة بالعبث بالنظم والوصول إلى البيانات دون إذن والاحتيال والتزوير الإلكترونيين والمحتوى المناهض للقانون وجرائم الملكية الفكرية. ويتناول مشروع النص سلطات التحري، بما في ذلك تعقب الاتصالات والبحث عن الأدلة الإلكترونية وضبطها والحفاظ عليها. كما أنه سيعرّف التعابير الأساسية وسيضع معايير للمساعدة القانونية المتبادلة وسائر أشكال التعاون الدولي. وسيمثل هذا النص، عند اتمامه بنجاح، المحاولة الأولى لوضع صك دولي شامل لمكافحة الجريمة ذات الصلة بالحواسيب. وقد لقي مشروع النص المكتمل ردود فعل متباينة. فقد كان في نظر الحكومات والخبراء وأجهزة إنفاذ القوانين بوجه عام تطوراً

١- مازالت مشكلة النشاط الإجرامي الذي تستخدم فيه تكنولوجيات عصرية للحواسيب والشبكات الحاسوبية والاتصالات تمثل تحدياً هاماً لأوساط العدالة الجنائية وإنفاذ القوانين لدى الدول الأعضاء. ويمكن اعتبار ذلك التحدي متكوّناً من عدد من العناصر الواضحة، على النحو المبين أدناه:

(أ) التحدي عالمي. في الماضي، كان معظم مستخدمي التكنولوجيات العصرية، ومن ثمّ معظم الجناة والضحايا، يوجدون في البلدان المتقدمة. وقد تمّ تبين توسيع إمكانية الوصول إلى هذه التكنولوجيات لتشمل البلدان النامية بصفتها أولوية رئيسية، من أجل ضمان تحوّل مجتمع المعلومات العالمي إلى عامل يدعم التنمية بدلاً من أن يكون عائقاً آخر أمامها.^(١) وستكون البلدان النامية مستضعفة أمام الجرائم الحاسوبية وجرائم الاتصالات ويمكن أن تستبعد من شبكات الحواسيب والاتصالات بواسطة منع الجريمة أو تكنولوجيات الأمن إذا لم تكن قادرة على المشاركة في وضع وتنفيذ سياسات لمكافحة الجريمة؛

(ب) التحدي حيوي. تفضي سرعة تطور التكنولوجيات الجديدة إلى تطور الابتكارات الإجرامية بالسرعة ذاتها، وتفضي الطبيعة العالمية للتكنولوجيات إلى الانتشار السريع للتقنيات الإجرامية الجديدة. لذلك، فإنّ من الأساسي رصد كل من التطور المشروع والابتكار الإجرامي من أجل جعل الردود المحلية والدولية مواكبة للمستجدات، خصوصاً في البلدان التي لديها موارد تقنية محدودة. والعملية مدفوعة في المقام الأول بالتطور التكنولوجي، ولذلك فهي مفتوحة؛

(ج) التحدي متعدد المجالات. يمثل تطوّر تكنولوجيات شبكات الحواسيب والاتصالات أساس الانتقال الكبير من الأنشطة الاجتماعية والاقتصادية التي تنطوي على مجهود بدني وتنتج سلعاً إلى الأنشطة التي تنطوي

الإلكتروني عبر الحدود وتعقب الاتصالات وضرورة التعاون بين الحكومات ومؤسسات القطاع الخاص ذات الصلة.

٦- وفي كانون الأول/ديسمبر ١٩٩٧، اعتمدت مجموعة الـ ٨ خطة عمل من ١٠ نقاط بشأن الجريمة السيبرانية تضمنت استعراض التشريعات، والتدابير الرامية إلى ضمان توفر موظفين متدربين ومجهزين لإنفاذ القوانين، والنظر في مسائل الجريمة السيبرانية عند التفاوض على اتفاقات تخص المساعدة القانونية، والنظر في طرائق الحفاظ على الأدلة الإلكترونية وجعلها متاحة للإجراءات الجنائية الأجنبية، وتحسين التعاون مع الصناعات، والمعايير القضائية وغيرها من المعايير التقنية بشأن الأمن الحاسوبي، واستخدام الأدلة الإلكترونية في الإجراءات القانونية.^(٤)

٧- وفي سنة ١٩٩٩، اعتمدت مجموعة الـ ٨ بعض المبادئ الأساسية الأولية بشأن أجهزة إنفاذ القوانين التي تسعى إلى الوصول إلى البيانات الإلكترونية المخزنة في الدول الأجنبية.^(٥) وأتفق بوجه عام على أن البيانات يمكن الوصول إليها بحرية إذا كانت متاحة للعموم، مثلما هي الحال فيما يخص المواقع الشبكية المفتوحة مثلاً، أو عندما يتم الحصول على موافقة شخص له صلاحية قانونية للوصول إلى البيانات وإفشائها. وفيما يتعلق بالبيانات التي هي ليست متاحة للعموم يواجه المفتشون معضلة. فإذا هم لم ينسخوا البيانات بسرعة، محابها الجناة عادة. أما إذا نسخوها دون أن يطلبوا الإذن أولاً من الدولة التي توجد فيها تلك البيانات، ظهرت مسائل جادة فيما يتعلق بسيادة تلك الدولة وحماية حقوق الأشخاص الذين لهم مصلحة في البيانات المضبوطة. وتشمل المبادئ التي اتفقت عليها مجموعة الـ ٨ طلباً بشأن التعجيل بالمساعدة القانونية المتبادلة. وهكذا، يُطلب من الدولة التي توجد فيها البيانات أن تتخذ خطوات عاجلة للحفاظ عليها ريثما تقدّم مساعدة رسمية أكثر لضمان ضبطها وإفشائها للدولة الطالبة. عندئذ يُنفذ نقل البيانات إلى الدولة الطالبة بواسطة إجراءات تقليدية أكثر وضمانات بشأن المساعدة القانونية المتبادلة.

إيجابياً، بالرغم من أن العديد يرون أن البعض من أصعب المسائل لم يجز تناولها. واتخذت جماعات عديدة ذات مصلحة موقفاً مفاده أنه لا ينبغي إخضاع الشبكات الدولية للوائح تنظيمية، ووجهت هذه الجماعات انتقادات شديدة إلى الصكّ معتبرة إياه محاولة لتوسيع نطاق السلطات المحلية لإنفاذ القوانين على حساب حرمة الشخصية للفرد وغير ذلك من المصالح.

٤- وقد أجرت المفاوضات بشأن نص الصكّ لجنة من الخبراء معنية بالجريمة في الحيز السيبراني، كانت قد أنشئت في شباط/فبراير ١٩٩٧ عقب عدّة دراسات سابقة عن المشكلة.^(٣) وإضافة إلى أعضاء اللجنة العاديين، دعي إلى المشاركة في وقائع اللجنة خبراء من كندا والولايات المتحدة الأمريكية واليابان، وانضمت دول أخرى إلى تلك المداورات أثناء سير المفاوضات. وأنتجت اللجنة ٢٥ صيغة متتالية لمشروع النص طوال مدة ولايتها التي انتهت في كانون الأول/ديسمبر ٢٠٠٠. وقد أحيل النص النهائي إلى اللجنة البرلمانية لمجلس أوروبا، وسيحال بعد ذلك إلى اللجنة الأوروبية المعنية بمشاكل الجريمة لكي تستعرضه في حزيران/يونيه ٢٠٠١، وفي حال الموافقة عليه سيحال بعد ذلك إلى لجنة وزراء مجلس أوروبا لاعتماده.

٢- مجموعة الـ ٨

٥- عقب المناقشات التي أجرتها مجموعة البلدان الصناعية السبع الكبرى والاتحاد الروسي (مجموعة الـ ٨) بشأن المشاكل الناشئة عن الجريمة عبر الوطنية في اجتماعها على مستوى القمة الذي عقد في هاليفاكس، كندا، في حزيران/يونيه ١٩٩٥، أنشأت هذه المجموعة فريق ليون لكبار الخبراء المعنيين بالجريمة المنظمة عبر الوطنية، وشمل هذا الفريق فريقاً فرعياً من الخبراء بشأن الجريمة ذات الصلة بالحواسيب. وقد اجتمع الفريق الفرعي بانتظام منذ سنة ١٩٩٧ وأنتج عدداً من المبادرات. وتمثلت أهم الشواغل التي بحثتها في المشاكل التي تطرحها عمليات التنفّيش

إلى منع الجريمة من خلال تثقيف المستهلكين وإدماج عناصر أمنية في التكنولوجيات الجديدة التي يجري استحداثها.

٣- المنظمات الدولية أو الدولية-الحكومية الأخرى

١١- إن مسألة الجريمة ذات الصلة بالتكنولوجيا الراقية والحواسيب مسألة تناولتها أيضاً منظمات أخرى دولية-حكومية ودولية، وذلك بصفتها موضوعاً مستقلاً وكذلك في سياق اعتبارات أخرى ذات صلة بالجريمة مثل غسل الأموال والجريمة المنظمة عبر الوطنية. وقد بدأ الكومنولث يبحث تلك المسائل في سنة ١٩٩٨، مدرجاً هذا الموضوع في جدول أعمال اجتماع لوزراء القانون بالكومنولث في أيار/مايو ١٩٩٩. فقد أنشأ ذلك الاجتماع فريقاً عاملاً من الخبراء المعنيين بالجريمة الحاسوبية وذات الصلة بالحاسوب لكي يصوغ تشريعات نموذجية لبلدان الكومنولث، لكنه أرجأ العمل بشأن هذا المشروع إلى حين الانتهاء من إعداد اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية. واستؤنف العمل في تموز/يوليه ٢٠٠٠ ويجري الآن إعداد مشروع تشريعات نموذجية. كما تكفل الكومنولث بتوزيع مواد بشأن التطورات الدولية على الدول الأعضاء فيه، وباستعراض مخططات الكومنولث التي تتناول الجناة الهاربين والمساعدة القانونية المتبادلة لضمان تقديم أشكال التعاون الضرورية، في إطار هذه المخططات، إلى المجال الجديد المتمثل في الجريمة ذات الصلة بالتكنولوجيا الراقية.

١٢- وأصبحت الانترنت أيضاً نشيطة في هذا المجال، فقد أنشأت مجموعة من الأفرقة العاملة الإقليمية المعنية بجرائم تكنولوجيا المعلومات. ونزعت البحوث التي أجرتها الانترنت والمواد التي أنتجتها إلى تجسيد احتياجات وشواغل أجهزة إنفاذ القوانين، وتشمل المواد التي أنتجتها لكي تُستخدم في تدريب المحققين كتيباً إرشادياً للمحققين الجدد ودليلاً أكثر تفصيلاً بشأن الجرائم ذات الصلة بالحواسيب يبين أفضل الممارسات والتقنيات لصالح المحققين المُحتكين. وتدرك الانترنت أيضاً الحاجة إلى استعمال وسائط التكنولوجيا الراقية لتعميم المعلومات على أجهزة إنفاذ القوانين، وهي

٨- كما جرى النظر في المبادئ الأساسية لتعقب الاتصالات على الشبكات الحاسوبية. فمعظم موفري هذه الخدمات يحتفظون بسجلات إلكترونية لمصدر ومقصد اتصالات مثل البريد الإلكتروني، ولكن لفترات زمنية محدودة. ولا يمكن الوصول إلى السجلات التي يمكن استعمالها لتعقب الاتصالات وتبين مستعملي النظم المعنيين في معظم البلدان إلا باللجوء إلى عمليات تفتيش وضبط خاضعة للمراجعة القضائية. وهذا لا يمثل عقبة جادة أمام تعقب معظم الاتصالات المحلية، أما في حالات الاتصالات عبر الحدود فتزداد حالات التأخير بسبب الحاجة الإضافية إلى تقديم طلبات في هذا الخصوص من خلال قنوات المساعدة القانونية المتبادلة. وهذه المشكلة معروفة لدى الجناة المتطورين الذين يستغلونها بتوجيه اتصالاتهم عبر أعداد كبيرة من البلدان المختلفة بين المصدر والمقصد، أو بتوجيهها عبر بلدان تفتقر إلى القوانين أو البنية التحتية التي تمكن من التعقب الناجح، وذلك من أجل إخفاء المصدر أو المقصد الحقيقي لاتصالاتهم.

٩- ولتيسير التعاون السريع بين أجهزة إنفاذ القوانين في الحالات عبر الوطنية، أوصى فريق ليون بإنشاء شبكة من الصلات في كل دولة بحيث يمكن التوجه إليها بطلب ٢٤ ساعة في اليوم وسبعة أيام في الأسبوع لتوفير المساعدة على التحقيق من جهات مختصة. وتألفت هذه الشبكة في البداية من الدول الأعضاء في مجموعة الـ ٨ لكنها وُسّعت الآن لكي تضم ١٩ بلداً، ونقلت المسؤولية التشغيلية إلى المنظمة الدولية للشرطة الجنائية (الانتربول).

١٠- وبغية جمع المؤسسات الحكومية بمؤسسات القطاع الخاص، عقدت مجموعة الـ ٨ عدّة مؤتمرات بشأن التعاون مع الصناعة.^(٦) ويشمل ممثلو الصناعة بوجه عام الشركات التي تنشئ أجهزة وبرامجيات الحواسيب والاتصالات وغيرها من عناصر البنية التحتية للحواسيب والاتصالات، والشركات التي تعرض خدمات على المستخدمين الأفراد. وُبحث في هذه المناقشات مسائل تتصل برغبة الشركات في التعاون مع أجهزة إنفاذ القوانين وقدرتها على ذلك، والحاجة

وملاحقة مرتكبيها قضائياً. ودُعيت لجنة منع الجريمة والعدالة الجنائية إلى التكفل بوضع تلك التوصيات السياسية، آخذة في الاعتبار العمل الجاري القيام به في المحافل الأخرى. وبعد ذلك، طلبت الجمعية العامة في قرارها ٦٠/٥٥ المؤرخ ٤ كانون الأول/ديسمبر ٢٠٠٠ إلى اللجنة أن تواصل النظر في النتائج والتوصيات المحسّدة في إعلان فيينا وتقرير المؤتمر العاشر، وطلبت إلى الأمين العام أن يضع، بالتشاور مع الدول الأعضاء، مشروع خطط عمل لكي تنظر فيها اللجنة في دورتها العاشرة؛

(و) وأجرى معهد آسيا والشرق الأقصى لمنع الجريمة ومعاملة المجرمين التابع للأمم المتحدة، إضافة إلى مشاركته في إعداد حلقة العمل التي عقدت أثناء المؤتمر العاشر والتي تعلقت بالجرائم ذات الصلة بالشبكات الحاسوبية، مجموعة من الاجتماعات وحلقات العمل لتبني المسائل ووضع جدول أعمال للأنشطة القادمة. وأجرى هذا المعهد دراسة استقصائية للدول الأعضاء بشأن المسائل التي تنطوي على الجرائم ذات الصلة بالحوسيب، وتستصدر نتائج هذه الدراسة قريباً. كما يعكف المعهد في الوقت الحالي على جمع ونشر المواد التي استعملتها الأمم المتحدة والأفراد المشاركون في حلقة العمل التي عقدت أثناء المؤتمر العاشر. وتتمحور خطط المعهد في المستقبل حول إعداد وتعميم معلومات عملية للتحقيق في الجريمة ذات الصلة بالحوسيب وملاحقة مرتكبيها قضائياً؛

(ز) وسيكون معروضاً على اللجنة في دورتها العاشرة تقرير للأمين العام عن مشاريع خطط عمل لتنفيذ إعلان فيينا بشأن الجريمة والعدالة: مواجهة تحديات القرن الحادي والعشرين (E/CN.15/2001/5). ويتناول تقرير الأمين العام أيضاً الجريمة ذات الصلة بالتكنولوجيا الرقابة والحوسيب، وهو يتضمّن مجموعة من التوصيات السياسية والتدابير المحددة التي يمكن اتخاذها لزيادة القدرة، على الصعيدين المحلي والدولي، على منع هذا النوع من الجرائم والتحرر عنه وملاحقة مرتكبيها قضائياً. وتستند تلك

المتصلة بالحوسيب ومكافحتها^(١٢) لكي يكون مورداً للمحققين وواضعي السياسات، وأتيح هذا الدليل على نطاق واسع على الانترنت؛

(د) وأدرجت أيضاً مسألة الجريمة ذات الصلة بالحوسيب في جدول أعمال مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين، الذي عقد في فيينا من ١٠ إلى ١٧ نيسان/أبريل ٢٠٠٠. وأثناء المؤتمر العاشر، نظم معهد آسيا والشرق الأقصى لمنع الجريمة ومعاملة المجرمين التابع للأمم المتحدة حلقة عمل ليوم واحد حول هذا الموضوع^(١٣). وتكونت حلقة العمل من مناقشات قامت بها أربعة أفرقة حول المواضيع التالية: علم الإجرام فيما يتعلق بالجريمة ذات الصلة بالحوسيب؛ والمشاكل المترتبة بتفتيش الشبكات الحاسوبية وضبطها؛ والمشاكل المترتبة بتعقب الاتصالات على الشبكات الحاسوبية؛ والعلاقات بين أجهزة إنفاذ القانون وصناعتي الحاسوب والانترنت. وقام خبراء رائدون في تلك المجالات باطلاع المشاركين على المسائل الراهنة والتقدم المحرز في المناقشات التي دارت في مجلس أوروبا ومجموعة الـ ٨ وغيرها من المحافل. وقد شارك في حلقة العمل عدّة ممثلين عن الصناعة إضافة إلى ممثلي الدول المشاركة. وأصدرت حلقة العمل عدّة توصيات، منها الدعوة إلى زيادة التعاون بين الحكومات والصناعة وتحسين التعاون الدولي على تعقب الجناة واتخاذ مزيد من الإجراءات من جانب الأمم المتحدة فيما يتعلق بتوفير التعاون التقني والمساعدة التقنية^(١٤)؛

(هـ) كما تناول إعلان فيينا بشأن الجريمة والعدالة: مواجهة تحديات القرن الحادي والعشرين، الذي اعتمده المؤتمر العاشر^(١٥) وأقرته الجمعية العامة في قرارها ٥٩/٥٥، المؤرخ ٤ كانون الأول/ديسمبر ٢٠٠٠، الجريمة ذات الصلة بالتكنولوجيا الرقابة والجريمة ذات الصلة بالحوسيب. ففي الفقرة ١٨ من إعلان فيينا، قررت الدول الأعضاء وضع توصيات سياسية إجرائية المنحى بشأن منع ومكافحة الجريمة ذات الصلة بالحوسيب، وتعهدت بالعمل على تعزيز قدرتها على منع هذه الجرائم والتحقيق فيها

شبكات الاتصالات أو أشكال أخرى من التكنولوجيا
العصرية؛

التوصيات والتدابير إلى المواد التي يتناولها هذا التقرير
بالبحث؛

(ي) وعقب اعتماد الاتفاقية، نظمت حلقة عمل أخرى حول موضوع "التحدي الذي تمثله الجريمة السيرانية المتعدمة الحدود"، وشكلت حلقة العمل هذه جزءاً من ندوة حول سيادة القانون في القرية العالمية - مسألتنا السيادة والعالمية، وذلك في إطار المؤتمر السياسي الرفيع المستوى للتوقيع على اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والبروتوكولين الملحقين بها، الذي عقد في باليرمو، إيطاليا، في الفقرة من ١٢ إلى ١٥ كانون الأول/ديسمبر ٢٠٠٠. وكان من بين المواضيع التي جرى تناولها الجريمة ذات الصلة بالحواسيب وغير ذلك من أشكال الإجرام عبر الوطني التي أصبحت التدابير المتخذة بشأنها والمتجذرة حصراً في القانون الداخلي تُعتبر بشكل متزايد غير وافية بالغرض. ولوحظ أن هذه الجريمة آخذة في الانتشار مع انتشار التكنولوجيا التي تعتمد عليها ومع ازدياد سهولة ارتكاب جرائم عبر الحدود. واعتبر سن تشريعات على المستوى الوطني واعتماد صك دولي شامل عنصرين هامين للعثور على حل، ولكن، أشير أيضاً إلى أن هنالك شواغل بشأن خطر وضع لوائح تنظيمية قبل الأوان. وأفيد بأنه يمكن أيضاً معالجة المشكلة جزئياً بواسطة المنع، وذلك باستخدام أشياء مثل الأمن التقني والتعليم ووضع معايير أخلاقية لاستخدام التكنولوجيا الجديدة. واقترحت حلقة العمل أيضاً تقسيم مجموعة الجرائم السيرانية إلى الفئات الأساسية التالية: الوصول دون إذن إلى الحواسيب أو النظم الحاسوبية؛ وتدمير البيانات أو تحويرها؛ والتدخل في الاستخدام المشروع للحواسيب أو النظم الحاسوبية؛ وسرقة الممتلكات غير الملموسة؛ والحصول على قيمة بواسطة الاحتيال.

جيم- طبيعة الجريمة ذات الصلة بالحواسيب
والتكنولوجيا الراقية: تحديد أولي للأشكال

١٤- تتطلب ظاهرة الجريمة ذات الصلة بالتكنولوجيا الراقية والحواسيب تبين الجرائم الجديدة تماماً وتعديل وصف

(ح) وتخطط الجمعية العامة علماً، في قرارها ٥٥/٦٣ المؤرخ ٤ كانون الأول/ديسمبر ٢٠٠٠، بقيمة الجهود المبذولة لمكافحة إساءة استخدام تكنولوجيا المعلومات. وستشمل تلك الجهود ما يلي: القضاء على الملاذات الآمنة للجنة؛ والتعاون مع أجهزة إنفاذ القوانين في القضايا الدولية؛ وتبادل المعلومات؛ وتدريب الموظفين وتجهيزهم؛ وحماية السرية، والحفاظ على البيانات المتعلقة بالتحريات الجنائية وسرعة الوصول إلى تلك البيانات؛ والإبقاء على نظم وافية بغرض المساعدة القانونية المتبادلة؛ والتوعية العامة بالمشكلة؛ وتصميم نظم للمعلومات لمنع الجريمة وتيسير التحريات عنها؛ وأخذ ضرورة حماية الحريات الفردية والحرمة الشخصية في الاعتبار مع الحفاظ على قدرة الحكومات على مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية. وقررت الجمعية أيضاً الإبقاء على مسألة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية في جدول أعمال دورتها السادسة والخمسين؛

(ط) واعتمدت الجمعية العامة، بمقتضى قرارها ٥٥/٢٥ المؤرخ ١٥ تشرين الثاني/نوفمبر ٢٠٠٠، اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والبروتوكولين الملحقين بها (القرار ٥٥/٢٥، المرفقات الأولى إلى الثالث). ولا تنطبق الاتفاقية في الحالات التي لا تكون فيها الجرائم المرتكبة جرائم خطيرة، أو في الحالات التي لا تنطوي فيها جماعة إجرامية منظمة، أو في الحالات التي لا تنطوي على عنصر عبر وطني في أي من الجرائم المرتكبة،^{١٦} مما يستبعد بعض الجرائم الإلكترونية. لكنها ستنتطبق في الحالات التي يستخدم فيها الجناة شبكات الحواسيب أو الاتصالات لدعم أشكال من الجريمة المنظمة عبر الوطنية تقليدية أكثر. وتدعو الفقرة ١ (ح) من المادة ٢٩ بالتحديد إلى اتخاذ تدابير محلية وتوفير المساعدة التقنية لمكافحة الجريمة المنظمة عبر الوطنية التي ترتكب باستخدام الحواسيب أو

منع اقتحام الحرمة الشخصية للمستخدمين المشروعين الذين يمكن الوصول إلى بياناتهم، وكذلك لأن الوصول دون إذن كثيراً ما يصحب جرائم أخرى أو يتدخل في الاستخدام المشروع للنظام.

(ب) استخدام النظم الحاسوبية دون إذن

١٨- يتداخل استخدام النظم الحاسوبية دون إذن مع الوصول دون إذن، لأنه لا بد من استخدام النظم للتمكن من الوصول. ولكن، حالما يتم التمكن من الوصول، تستخدم النظم أيضاً لارتكاب جرائم أخرى أو لإخفاء هوية الجاني الحقيقية. وفي العادة يُجرّم الاستخدام دون إذن بحجة أن استخدام وقت الحاسوب أو مرافقه يمثل سلعة ثمينة لا يدفع الجناة رسمها، خاصة وأنها في بعض الأحيان لا تتاح للمستخدمين المشروعين الذين يدفعون رسوماً.

(ج) قراءة البيانات أو نسخها أو أخذها دون إذن

١٩- كما هي الحال فيما يتعلق بالسرقة التقليدية، يتمثل الضرر الناجم عن قراءة البيانات أو نسخها أو أخذها دون إذن في الخسارة في القيمة التي تلحق بالضحية واكتساب الجاني قيمة غير مشروعة. غير أن هذين الجانبين منفصلان فيما يتعلق بالبيانات، إذ أنه يمكن نسخ البيانات دون نقلها من مكانها. وهذا الفعل يمكن تجريمه أيضاً بصفته شكلاً من أشكال انتهاك الحرمة الشخصية.

(د) إنشاء أو نشر برامج معادية

٢٠- تتدخل الفيروسات والديدان وغيرها من البرامج الحاسوبية في عمليات النظم الحاسوبية، وذلك باستهلاك قدرتها على الحوسبة والتخزين. وفي معظم الحالات، تنتشر هذه الفيروسات بواسطة البريد الإلكتروني أو نقل الأقراص الملوثة، بحيث سرعان ما يفقد الجناة التحكم في نطاق الضرر الناجم حالما يطلق البرنامج. كما أن العديد من البرامج المعادية تلحق ضرراً فعلياً بالبيانات، وذلك بمحو الملفات أو

الجرائم القائمة لضمان شمولها إساءة استخدام التكنولوجيات الجديدة. فقد أصبح من اللازم بحث الأشكال الجديدة من السلوك الضار بهدف تحديد ما إذا كان تطبيق القانون الجنائي مناسباً كرد فعل وما إذا كان ينبغي تجريم السلوك المعني فعلاً. وقد بدأ يظهر توافق دولي في الآراء بشأن جوهر أخطر أنماط السلوك وأكثرها ضرراً، ولكن مازالت هنالك بعض المجالات التي تعالجها بعض الدول وليس كلها كجريمة. وأكبر مثالين على ذلك هما مشاكل الملكية الفكرية، ومنها مثلاً نسخ البرمجيات أو البيانات دون إذن، ومشكلة ما يوصف بأنه محتوى منافي للقانون.

١٥- وقد تسبب استغلال التكنولوجيات الجديدة لأغراض إجرامية في ظهور أشكال جديدة تماماً من الجرائم. وفي حالات أخرى، ترتكب أشكال من الجريمة تقليدية أكثر بطرائق جديدة تزيد في فوائدها للجناة وتقلل من مجازفاتهم. وثمة فئة أساسية ثالثة من النشاط الإجرامي تتمثل في لجوء الجناة إلى استخدام التكنولوجيات استخداماً أعم لتنظيم أنفسهم والاتصال فيما بينهم وحماية أنشطتهم من المراقبة. وتشمل مجالات التصنيف الأساسية الأخرى التصنيف حسب ما إذا كانت الجرائم مرتكبة لغرض الكسب الاقتصادي أو المادي لصالح الجناة أو لدوافع أخرى، وما إذا كانت الجرائم تنطوي على جرائم مرتكبة ضد نظم الحواسيب والاتصالات أو على استخدام تلك التكنولوجيات للإيقاع بالآخرين كضحايا.

١٦- ويرد أدناه وصف للأنواع الأساسية من الجرائم ذات الصلة بالتكنولوجيا الرقمية والحواسيب.

١- الجرائم المرتكبة ضد التكنولوجيات ومستخدميها

(أ) الوصول دون إذن إلى الحواسيب أو النظم الحاسوبية

١٧- في معظم الحالات، يُعامل الوصول دون إذن إلى الحواسيب أو النظم الحاسوبية كجريمة وذلك حرصاً على

حرية التعبير أو الكلام ، في تقييد مدى قدرة دول عديدة على تجريم بعض أشكال المحتوى.

(ب) الاختطاف ذو الصلة بالانترنت

٢٣- لقد بدأ الجناة من مشتبه الأطفال في استخدام الانترنت كوسيلة للتمكن من الوصول إلى الأطفال دون الكشف عن هوياتهم الحقيقية. فالحوار يبدأ في غرف الدردشة الإلكترونية وحالما يكسب الجاني ثقة الطفل، يدبر مقابلة شخصية ويختطف الضحية. وقد ألقى القبض على عدد من الجناة من قبل موظفين معينين بإنفاذ القوانين كانوا يقدمون أنفسهم بصفتهم أطفالاً على الانترنت. وفي بعض الحالات، كان الجناة يحثون الضحايا على إلغاء الملفات التي تتضمن تدويناً لمخاطبتهم من أجل إخفاء الدليل على الاختطاف.

(ج) الاحتيال

٢٤- تشمل فئة الاحتيال معظم الجرائم التي توجه فيها الأموال إلكترونياً وجهة خاطئة أو التي يتلقى فيها مستخدمو التكنولوجيا معلومات خاطئة لحرمانهم من الأموال أو قيمة الأصول. وهذه الجرائم يمكن أن يرتكبها أشخاص داخلون مُطلعون كالموظفين أو أشخاص خارجيون يتمكنون من الوصول دون إذن إلى نظم خصوصية أو يدرجون معلومات خاطئة في النظم العمومية. ويتوقع أن يزداد الاحتيال وغيره من الجرائم الاقتصادية زيادة كبيرة مع انتشار التجارة الإلكترونية. وثمة مشكلة متزايدة في هذا المجال هي استخدام التكنولوجيا للتلاعب بالأسواق المالية.

(د) التجسس التجاري أو الصناعي

٢٥- إن تزايد اعتماد الشركات على النظم الحاسوبية لإنشاء ونقل المعلومات جعل منها أيضاً أهدافاً للتجسس الصناعي. ويمكن القيام بهذا التجسس بالتمكن من الوصول دون إذن من الخارج، أو من قبل أشخاص داخلين مُطلعين

تشويهاها. وهذا الضرر الذي يمكن أن يكون كبيراً يتمثل في فقدان عمليات النظم وفقدان بيانات قيّمة، وفي تكاليف إزالة نقل البرامج وإعادة تشغيل وظائف النظم.

(هـ) تخريب الحواسيب

٢١- يمكن أن يكون الضرر ناجماً مباشرة عن فعل الجناة الذين تمكنوا من الوصول دون إذن، إما عن قصد أو عن غير قصد، عندما كانوا يحاولون استخدام النظام أو إخفاء حقيقة تمكنهم من الوصول. وهذه الجرائم يرتكبها في بعض الأحيان أشخاص داخلون مُطلعون يملكون الإذن بالوصول إلى النظام المعني. وتشمل هذه الفئة العمليات الهجومية لتعطيل الخدمة، التي يتمكن الجاني في إطارها من الوصول دون إذن إلى عدد كبير من الحواسيب المشبكة ويستخدمها لإرسال وابل من البيانات العشوائية إلى النظام المستهدف بحيث يحمل الهدف حمولة مفرطة ويتسبب في تعطيله. وهذا يمكن أن يشكل مجرد تخريب أو يمكن استخدامه كأسلوب تضليلي لإخفاء جرائم أخرى بشلّ آليات الأمن التقنية. كما يمكن استخدام برامج معادية كالفيرسات للقيام بأفعال تخريبية محددة، ولكن يمكن تمييزها عن أفعال الجناة المباشرة لأنها حالما تنتشر تمارس في العادة أثرها الضار دون تمييز.

٢- الجرائم التقليدية التي ترتكب باستخدام تكنولوجيا الحواسيب أو الاتصالات

(أ) الجرائم التي تنطوي على محتوى منافي للقانون

٢٢- تتمثل الجرائم التي تنطوي على محتوى منافي للقانون في استخدام النظم الحاسوبية لإنتاج أو توزيع صور أو نصوص أو معلومات أخرى تخضع لعقوبات جنائية. وثمة تباين بين أنواع المحتوى الذي يجرم في مختلف الدول. فمعظم الدول تجرم في الوقت الحالي إنشاء أو توزيع مواد خليعة عن الأطفال، ولكن ثمة توافق أقل في الآراء بشأن المواد التي تعتبر داعرة أو إباحية أو تجديفية أو داعية إلى الكراهية. وتتسبب حماية مبادئ حقوق الإنسان التي يكفلها الدستور، بما فيها

تكنولوجيا مثل التشفير. وفي بعض الحالات، قد يُلجأ أيضاً إلى جرائم أخرى مثل القمار أو الاحتيال.^(١٧)

٣- استخدام التكنولوجيا لدعم أنشطة إجرامية أخرى

٢٩- بوجه عام، تتيح شبكات الحواسيب والاتصالات العصرية وغيرها من التكنولوجيا من هذا القبيل للتنظيمات الإجرامية نفس المزايا التي تتيحها لأوساط الأعمال التجارية المشروعة. وتشمل المزايا الاتصالات العالمية السريعة والموثوقة والقليلة التكلفة التي هي في معظم الحالات في مأمن أكثر من الوسائل التقليدية من أن يُعترض سبيلها أو تُراقب من الخارج. فطبيعة الشبكات وتطور سرعة وحجم البيانات التي يجري نقلها يجعل من الصعب على أجهزة إنفاذ القوانين أن تعترض سبيل الاتصالات كل على حدة. والمنتجات الأمنية المكرسة، ومنها برامج الجدران النارية وبرامج التشفير، تحمي الاتصالات الإجرامية من أن يُعترض سبيلها أو تُفتَح بنفس الفعالية التي تحمي بها الاتصالات المشروعة. كما يمكن لتكنولوجيا الشبكات في بعض الحالات أن تدعم تماماً أشكالاً جديدة من التنظيم الإجرامي. وأشيع الأمثلة على ذلك الحناة من مشتبه الأطفال الذين يستطيعون تحديد مواقع بعضهم البعض وتقاسم مواد إباحية عن الأطفال ويحافظون في الوقت ذاته على سرية هويتهم، ويمكن أن يتعاونوا بطرائق غير مشمولة بالمفاهيم أو التعاريف الحالية للجريمة المنظمة. كما تستطيع التنظيمات الإجرامية التقليدية أكثر أن تعثر على فرص جديدة للتعرف على جناة من مناطق أو بلدان أخرى والتعاون معهم.

دال- تقدير نطاق وتكاليف الجريمة ذات الصلة بالحواسيب والتكنولوجيا الراقية

٣٠- مع ازدياد توسع نطاق شبكات الحواسيب والاتصالات وزيادة تعقيدها، ازداد بقدر كبير عدد الناس الذين يستخدمونها ودرجة اعتمادهم عليها. وقد أشار الأمين

يستخدمون التكنولوجيا لجمع معلومات قيمة وإرسالها إلى المنافسين دون أن يفتضح أمرهم.

هـ) جرائم الملكية الفكرية

٢٦- إن قدرة التكنولوجيا الجديدة على تخزين المعلومات ونقلها ونسخها يجعل نسخ المعلومات واستخدامها دون إذن مثار قلق كبير. غير أن هذه الأفعال لا تعاملها كل الدول بصفتها أفعالاً إجرامية. فبعضها يتناولها كمسألة مدنية بين الأطراف المعنيين مباشرة.

و) القمار

٢٧- إن تطوير البنية التحتية لدعم التجارة الإلكترونية الصغيرة الحجم أتاح أيضاً إمكانية القمار بواسطة الانترنت. وتدرج هذه المسألة ضمن القانون الجنائي عندما يستخدم القمارون مواقع شبكية في الولايات القضائية التي يمارس فيها القمار بطريقة مشروعة في ولايات قضائية تجرم ذلك. وبصرف النظر عن الاعتبارات الأخلاقية، كثيراً ما يُنظم القمار قانونياً لتوليد إيرادات ضريبية وضمان الإشراف لاستبعاد الجريمة المنظمة وحماية القمارين من اللعب الذي ينطوي على خداع. وفي الآونة الأخيرة، أصبح القمار بواسطة الانترنت يعتبر أيضاً وسيلة ممكنة لممارسة عمليات غسل الأموال.

ز) غسل الأموال

٢٨- من المتوقع أن يتيح التزايد المتواصل في التجارة الإلكترونية وغيرها من ضروب النشاط التجاري بواسطة الشبكات الحاسوبية فرصاً عديدة لغسل الأموال. وبوجه عام، تمكن التكنولوجيا الجناة من إخفاء هوياتهم ومواقعهم الحقيقية واستغلال الاختلافات بين الولايات القضائية باستخدام حسابات أجنبية أو ولايات قضائية متعددة، وإخفاء الطبيعة الحقيقية لصفقاتهم التجارية باستخدام

بلايين دولار، ويقدر أنه أصاب قرابة ٤٥ مليون حاسوب في كامل أنحاء العالم. وفي حادثة أخرى تمثلت في هجمات لتعطيل الخدمة، أُرسِل إلى مواقع شبكية وابل من البيانات الضخمة التي لا معنى لها، مما تسبّب في تعطيل ١٢٠٠ موقع منها مواقع منظمات إخبارية ومواقع للتجارة الإلكترونية، وذلك في أقل من ساعتين. وفي معظم الحالات تتضاعف الخسائر الناجمة عن بعض الحوادث، وخصوصاً تلك التي تنطوي على فيروسات، وذلك عندما يعمد جناة آخرون إلى نسخ الفيروس وإدخال تغييرات لإخفاء طبيعته عن المستخدمين أو برامجيات التصفية ثم يعيدون نشره.^(٢٠)

٣٢- ومن الصعب القيام بتحديد كمي للخسائر الحالية، لكن هذه الخسائر تشمل التكاليف المباشرة المترتبة على إصلاح النظم والبرامجيات، وفقدان إمكانية الوصول إلى المستخدمين أو عرض الخدمات عليهم وما يترتب على ذلك من ضرر لاحق، وفقدان بيانات قيمة والخسائر في الإيرادات المتأتبة من تشغيل المواقع. وتقتضي هذه الجرائم أيضاً استحداث تدابير أمنية وقائية أخرى والإبقاء عليها، مما يزيد في عامل التكلفة. كما أن الزيادات الإجمالية في هذه الجرائم والطبيعة المدهشة لبعض الجرائم المعنية يولّد أيضاً تدابير سياسية جوهرية ولكن لا يمكن التنبؤ بها لتعزيز مكافحتها في إطار القانون الجنائي، وتشديد العقوبات، واتخاذ احتياطات تقنية من جانب منتجي البرامجيات والمعدات الحاسوبية والشركات التي تعرض على الزبائن وصلهم الشبكي. وثمة تكلفة أخرى مستترة مترتبة على هذه الأحداث وهي الخوف من الجريمة السيبرانية الذي يمكن أن يضعف استخدام التكنولوجيا أو يُثني الحكومات والسكان في البلدان النامية عن استخدامها على أنجع وجه.

٣٣- ومن الصعب أيضاً البحث عن تحليل موثوق فيه لطبيعة ونطاق الجرائم ذاتها. فالمسائل تظل مفتوحة فيما يتعلق بما إذا كان ينبغي تجريم بعض أشكال السلوك، وبكيفية تعريفها وتصنيفها في تلك الحالة. كما يتوقف أي نظام تصنيف جزئي على التكنولوجيا المعنية، وهذا يؤثر أيضاً مسائل تعريفية. فتكنولوجيا مثل الشبكات الحاسوبية

العام، في تقريره إلى جمعية الأمم المتحدة للألفية، إلى أن عدد مستخدمي الانترنت في مطلع التسعينات وصل إلى ١٤٣ مليون مستخدم حتى سنة ١٩٩٨ وأن من المتوقع أن يرتفع عدد المستخدمين إلى ٧٠٠ مليون في سنة ٢٠٠١. وقد بلغت قيمة التجارة الإلكترونية، وهي ظاهرة أحدث عهداً، ما مجموعه ٢,٦ بليون دولار سنة ١٩٩٦ ويتوقع أن تصل إلى ٣٠٠ بليون دولار في سنة ٢٠٠٢.^(١٨) وثمة إحصاءات شاملة قليلة تتعلق بالجرائم ذات الصلة بالتكنولوجيا الرقابة والحواسيب لكن الأدلة غير المتينة وهذه الإحصاءات المتوفرة توحي بأن نطاق هذا النوع من الجرائم أخذ في الازدياد مع ازدياد عدد الجناة والضحايا المحتملين على خط الحاسوب.^(١٩) ويبدو أن نطاق الأنشطة الإجرامية أخذ في الانتشار أيضاً بسبب ما تتيحه التكنولوجيا من فرص إجرامية جديدة وعتور الجناة على سبل جديدة لاستغلالها. وما يثير قلقاً خاصاً في الوقت الراهن هو سرعة توسع التجارة الإلكترونية وبنيتها التحتية الداعمة، ومن المرجح أن يكون هذا التوسع مصحوباً بزيادات لاحقة في الجرائم الاقتصادية ذات الصلة بالحواسيب، ومنها الاحتيال والتلاعب بالأسواق المالية وغسل الأموال.

٣١- وبتزايد درجة الاعتماد على الشبكات، يزداد أيضاً الضرر الذي يمكن أن ينجم عن الأفعال الإجرامية. وأصبحت معظم البلدان الصناعية، التي يوجد فيها أكبر قدر من الاعتماد على الشبكات، تعتبر الآن شبكات الاتصالات والحواسيب والبنية التحتية الداعمة لها أهدافاً محتملة للإرهاب. وما زالت الهجمات على النظم الحاسوبية لأسباب استراتيجية أو سياسية نادرة، لكن الأفعال الإجرامية التي تقوم على دوافع أخرى تتسبب بانتظام في ضرر واسع النطاق، بل إن هذا الضرر يتجاوز في بعض الأحيان أقصى ما كان الجناة ينوون إحداثه. ومن بين الأمثلة الحديثة العهد على ذلك إنشاء ونشر فيروس "ميليسا" ("Melissa") في آذار/مارس ١٩٩٩ الذي تسبّب في ضرر مباشر تزيد تكلفته على ١٠ ملايين دولار في الولايات المتحدة الأمريكية وحدها، كما قدر الضرر الذي تسبّب فيه فيروس "I love you" في أيار/مايو ٢٠٠٠ بخسائر تتراوح بين ٧ و ١٠

ثالثاً - الاستنتاجات والتوصيات: وضع سياسات عالمية لمنع ومكافحة الجريمة ذات الصلة بالحواسيب والتكنولوجيا الرقمية

ألف - ضرورة معالجة الجريمة ذات الصلة بالحواسيب والتكنولوجيا الرقمية كموضوع منفصل

٣٥- تتصل الأنشطة الإجرامية التي يتناولها هذا التقرير بالتكنولوجيات الأساسية، وهي تشترك في العديد من الخصائص. وبعض هذه الأنشطة جديدة أنشأها أو حدّتها التكنولوجيات ذاتها، بينما تعد الأخرى أشكالاً من الجريمة تقليدية أكثر تأثرت تأثراً كبيراً بتلك التكنولوجيات. والعديد من المسائل السياساتية الأساسية، ومنها إقامة توازن مناسب بين حقوق الإنسان وسلطات التحري وبين المصالح المحلية والدولية، وهي مشتركة بين كل أشكال الجرائم ذات الصلة بالتكنولوجيا العصرية والحواسيب. وعلى مستوى عملي أكثر، فإن المشاكل التي يواجهها المحققون والمدعون العامون، ومنها تحديد أماكن الجناة وهويتهم وضبط الأدلة الحاسوبية أو الإلكترونية والحفاظ عليها وإثبات صحتها واستخدامها في المحكمة، هي نفس المشاكل جوهرياً بصرف النظر عن طبيعة الجرائم ذاتها. لذلك يُوصى بأن يعالج هذا المجال بصفته موضوعاً منفصلاً لأغراض البحث وأي مناقشات متعددة الأطراف تدور في المستقبل. ولكن، ينبغي الإشارة إلى أن العديد من مواطن القلق الناشئة، ومنها نشر المواد الإباحية عن الأطفال والاحتيال وسائر الجرائم المالية، ستطلب أيضاً إسهام خبراء على اطلاع بالجنة المعنيين وطرائقهم المحددة.

باء - ضرورة مساعدة البلدان النامية

٣٦- إن العديد من المناقشات السياساتية حول النظم الحاسوبية والجرائم ذات الصلة بالحواسيب دارت حتى الآن داخل وبين البلدان التي توجد لديها قطاعات للتكنولوجيا الرقمية متطورة جداً. ولهذه البلدان مصالح كبيرة يمكن أن تتأثر سلباً من الجرائم ذات الصلة بالحواسيب. ولهذه البلدان

ونظم البث الكابلية والنظم الهاتفية الخلوية والتقليدية بدأت تتحول بسرعة إلى نظم لا يمكن التمييز بينها نظراً لانتشار استخدامات الشبكات الحاسوبية وتحوّل عدد متزايد من النظم التقليدية إلى استخدام التكنولوجيات الرقمية. ومن الأمثلة الراهنة على ذلك ما يسمّى جهاز "بالم" للتحكم اليدوي الذي يجمع بين جوانب الخدمات الهاتفية الخلوية والبث الشبكي والوصول إلى شبكات الحواسيب. وهذا سيمثل تحدياً للباحثين ومحلي السياسات وصانعي النصوص القانونية في المستقبل المنظور، كما أنه أفضى إلى صدور نداءات لاستخدام مفاهيم ولغة محايدة تكنولوجياً لضمان تجنّب الفجوات وحالات التضارب.

٣٤- ويشكل جمع احصاءات دقيقة أيضاً مشاكل حتى عندما تكون الجرائم مستبانة بوضوح. ويعتقد معظم الخبراء أن الأشكال المعهودة من الجرائم ذات الصلة بالحواسيب مبلغ عنها قليلاً جداً لأن الضحايا قد لا يدركون أنهم أوقع بهم كضحايا أو قد لا يدركون أن السلوك المعني جريمة أو قد يقررون عدم التظلم لأسباب تتعلق بالحرج أو بموثوقية الشركة. وتنشأ مشاكل أخرى بسبب الإيذاء الجماعي الذي تتسبب فيه جرائم مثل نشر الفيروسات، لأن أعداد الضحايا هي ببساطة أكبر من أن تحدّد أو تحصى، ولأن هذه البرامج يمكن أن تستمر في الإيقاع بضحايا جدد بعد إلقاء القبض على الجناة ومعاقبتهم بزمن طويل. وثمة عامل آخر سيعقّد جمع الإحصاءات عن الجريمة الوطنية ومقارنتها وهو أن الجرائم عبر الوطنية ذات الصلة بالحواسيب هي بحكم طبيعتها تُرتكب أو تكون لها آثار في دولتين على الأقل، وفي بعض الحالات في دول عديدة، مما يترتب عليه احتمال تعدّد حالات الإبلاغ أو عدم الإبلاغ البتة.

النامية لتقييم مصالحها من التكنولوجيات ذاتها وكيف يمكن أن تتأثر تلك المصالح بالجرائم ذات الصلة بالحواسيب والجهود الرامية إلى مكافحتها. وهذا يجعل من المساعدة في المراحل الأولى عاملاً هاماً جداً. وما انفكت بعض البلدان تشارك بنشاط منذ بعض الوقت، غير أن العديد من البلدان ما زالت لا تألف التكنولوجيات ولم تول اهتماماً كبيراً للمسائل التقنية والقانونية والسياساتية التي ستنشأ. وحتى مع المساعدة، يستغرق إيجاد هذه الخبرة الفنية وقتاً. لذلك، فإن من الهام أن تبدأ هذه المساعدة بأسرع وقت ممكن وأن تتواصل فترة طويلة بما فيه الكفاية لضمان المشاركة الفعلية طالما كانت المناقشات جارية. وعلى المدى الأطول، ستكون هنالك حاجة أيضاً إلى المساعدة التقنية الجارية لضمان الفعالية التشغيلية. وسيطلب استمرار تطور التكنولوجيات والجرائم التي تتوقف عليها بذل جهود عالمية لرصد التطورات الجديدة واستحداث ردود فعل ناجعة وتعميمها بالقدر الكافي من السرعة الذي يمكن أجهزة إنفاذ القوانين والمدعين العامين من التقدم بنفس السرعة التي يتقدم بها الجناة بل وحتى من تجاوزهم.

٣٩- لذلك، يوصى ببذل جهود عاجلة لتقدير الاحتياجات إلى المساعدة التقنية لدى البلدان النامية التي تطلبها والوفاء بتلك الاحتياجات في أسرع وقت ممكن. وينبغي إجراء هذا التقدير في سياق استراتيجيات التنمية الإلكترونية لدى تلك البلدان والاستخدام العالمي المتزايد لتكنولوجيات نظم الحواسيب والاتصالات ومنع الجريمة. كما ينبغي القيام بذلك بالتشاور مع شركات القطاع الخاص المسؤولة عن هذه التكنولوجيات، وبتلقي المساعدة من هذه الشركات حيثما أمكن ذلك. وستتضمن عناصر التقدير الهامة إجمالاً تبين التكنولوجيات البالغة الأهمية وتحديد الأولويات.

استثمارات واسعة النطاق في التكنولوجيات من القطاعين العام والخاص، كما أن لديها سكانا يعتمدون بشكل متزايد على استخدام الشبكات الحاسوبية. غير أن مصالح البلدان النامية مطروحة أيضاً. فالتكنولوجيات الجديدة تمثل فرصة كبيرة للنهوض بمصالح البلدان النامية في المجالين الاجتماعي والاقتصادي وغيرهما من المجالات،^(٢١) لكنها يمكن أن تزيد أيضاً في تفاقم التباينات الموجودة حالياً إذا لم تتمكن تلك البلدان من استغلال تلك الفرصة استغلالاً كاملاً. وفي ذلك الخصوص، يمكن أن تصبح الجرائم ذات الصلة بالحواسيب وجهود البلدان المتقدمة وصناعات التكنولوجيا الراقية الرامية إلى مكافحة تلك الجرائم عقبة أمام التنمية إذا لم تستطع البلدان النامية المشاركة الفعلية في المناقشات. فإسهام هذه البلدان ضروري لتبيين وتوضيح مصالحها على نحو كامل، وتبين الاحتياجات إلى المساعدة التقنية وغيرها في مختلف مراحل العملية، واتخاذ تدابير مجدية في كل المجتمعات لمنع الجريمة ومكافحتها، وضمان التنفيذ الكامل والفعلي لتلك التدابير.

٣٧- وسيكون من الضروري تحقيق تنفيذ عالمي تقريباً للتدابير الناجعة لمكافحة الجريمة، لأن التكنولوجيات الجديدة يمكن أن يستغلها المجرمون دون أن يتعرضوا لأي قيود تقريباً من تلك التي تفرضها الحدود الوطنية على الجناة التقليديين. ففي حين توجد عوامل تقيد الجناة التقليديين مثل البعد الجغرافي والتدابير الرقابية الجمركية وضرورة الوصول الجسدي إلى ضحاياهم، يستطيع الجناة الإلكترونيون ممارسة عملياتهم عن بعد مفلتين فعلاً من العقاب، وذلك من أو عبر أي ولاية قضائية تفتقر إلى تشريعات وافية بالعرض أو إلى الرغبة في إنفاذ تلك التشريعات أو القدرة على إنفاذها. وسيكون التمثيل الواسع والمشاركة الفعلية أساسيين لضمان جدوى السياسات والتدابير التي توضع لكل البلدان ورغبة كل البلدان في تنفيذها بفعالية وقدرتها على ذلك.

٣٨- وسيطلب ضمان المشاركة الفعلية الحصول على المساعدة من البلدان المتقدمة في عدة مراحل من العملية. ففي البدء، ستكون هناك حاجة إلى معلومات من البلدان

والمساعدة على تطوير تكنولوجيات محددة يمكن أن تحدث فوائد اجتماعية، ولكن لا تكون بالضرورة مجدية تجارياً. وبشكل أعم، خلص المجلس إلى أن الدور الأساسي للأمم المتحدة يتمثل في تحقيق التوافق في الآراء والشراكات فيما بين أصحاب المصلحة في هذه العملية، بما فيهم الحكومات والمؤسسات الأكاديمية وشركات القطاع الخاص. والهدف من تحقيق توافق الآراء هو حشد الخبرات الفنية والموارد اللازمة لضمان إمكانية وصول الجميع إلى تكنولوجيات المعلومات الجديدة، وفرصة الاستفادة منها.

٤٣- وتمثل الجريمة ذات الصلة بالتكنولوجيا الراقية والحوسيب عقبة هامة أمام إمكانية الوصول إلى ما يصفه المجلس بأنه اقتصاد عالمي قائم على المعرفة وجني فوائده المحتملة، وستكون مهمة تحقيق توافق الآراء بالقدر ذاته من الأهمية في مجال مكافحة الجريمة. وثمة من قبل اتفاق عام على ضرورة اتخاذ تدابير فعلية لمكافحة الجريمة فيما بين الدول التي لديها قدر كبير من الاستثمارات في التكنولوجيات وتعتمد عليها اعتماداً كبيراً، لكن ذلك ما هو إلا بداية العملية. فاستحداث تدابير محددة سيقتضي تقييم وتسوية العديد من المسائل الاقتصادية والاجتماعية والثقافية والقانونية. وسوف يتعين دعم عمليتي وضع وتنفيذ العديد من التدابير لمكافحة الجريمة بتحقيق توافق عالمي تقريباً وبوضع معايير وافية بالعرض بشأن القدرة التقنية في كل بلد تقريباً إذا أريد لهذه التدابير أن تبرهن على فعاليتها. ولا ينبغي أن يقتصر التوافق المذكور على البلدان وحكوماتها فحسب، بل ينبغي أن يشمل أيضاً شركات القطاع الخاص المتعددة الجنسيات أيضاً.

٤٤- وفي المستقبل العاجل، من الهام جمع وتعميم المعلومات الدقيقة عن طبيعة ونطاق المشكلة وآراء الدول الأعضاء في ما ينبغي القيام به لمعالجة المشكلة، وذلك لتمكين الدول من النظر في الخيارات وإرشاد الأمم المتحدة إلى الطريقة التي ينبغي لها أن تتصرف بها. وقد شرعت المنظمات الدولية الحكومية المذكورة في هذا التقرير، وكذلك بعض الحكومات على أساس فردي، في عملية تقاسم الخبرة الفنية

جيم- ضرورة النظر في اتخاذ تدابير دولية ووطنية وذات صلة بالقطاع الخاص

٤٠- يسلم الخبراء بشكل عام بأن الطابع الدولي لتكنولوجيات الحوسيب والاتصالات العصرية أفضى إلى أشكال جديدة من الجريمة عبر الوطنية والمتعددة الجنسيات. فمفهوم الحيز السبراني والسهولة التي يمكن بها لأفعال إجرامية في موقع جغرافي أن تؤثر في مواقع أخرى يجعلان من الأساسي تحقيق تكامل بين كل من التدابير الوطنية والدولية. فبدون هذا التكامل، قد لا تكون التدابير المضادة فعالة لمكافحة الجريمة، ويمكن أن تترتب عليها عواقب مناوئة مثل ثني السكان عن استخدام التكنولوجيات الجديدة أو إضعاف حقوق الإنسان أو إيجاد تباينات في القدرة التنافسية الصناعية أو التنمية الصناعية.

٤١- كما يجعل الدور البارز الذي تقوم به الصناعة في تطوير التكنولوجيات وصيانتها من الهام إدماج تدابير القطاعين العام والخاص. وتؤيد أوساط القطاع الخاص بوجه عام مكافحة الجريمة بشكل فعال، ولكن لا بد من التوفيق بين دوافعها، التي هي بالأحرى تجارية لا سياسية، وطرائقها التي هي تقنية بدلاً من أن تكون قانونية في طبيعتها، وإدماجها كلما أمكن ذلك مع الجهود التي تبذلها الحكومات على الصعيدين المحلي والدولي.

دال- دور الأمم المتحدة

٤٢- كجزء من التحضير لجمعية الأمم المتحدة للألفية، دعي المجلس الاقتصادي والاجتماعي إلى النظر في دور تكنولوجيا المعلومات في مجالي التنمية والتعاون الدولي. وخلص المجلس إلى أن تطوّر وانتشار تكنولوجيات المعلومات الجديدة هما قائمان بذاتهما إلى حد كبير، لكن بإمكان الأمم المتحدة أن تساعد في هذه العملية بطرائق هامة.^(٢٢) وتشمل هذه الطرائق مساعدة البلدان النامية على مواكبة التطورات الجديدة، خصوصاً في المناطق أو المجالات المواضيعية التي لا يرحح أن تفي التطورات المدفوعة بالسوق باحتياجاتها،

البرنامج. وترد مناقشة هذه التوصية بالتفصيل في الباب وادناه.

٤٨- وفي الأمد الأبعد، يرى العديد من الخبراء أن أقل ما يجب القيام به لإرساء السياسات والسلطات والإجراءات وآليات التعاون الدولي اللازمة للتصدي بفعالية للجريمة عبر الوطنية ذات الصلة بالحواسيب هو وضع صك قانوني عالمي شامل لمكافحة الجريمة ذات الصلة بالتكنولوجيا الراقية والحواسيب. غير أن الآراء متباينة بشأن السرعة التي يمكن بها وضع هذا الصك. فكما سبقت الإشارة إليه في الباب باء اعلاه، من الضروري إشراك مجموعة أوسع من البلدان في مرحلة مبكرة من العملية. وثمة أيضاً مسائل رئيسية سيتعين حلها عند صوغ هذا الصك، ومنها مثلاً المسائل المتعلقة بالسيادة الوطنية وتطبيق ضمانات قضائية وغيرها بشأن حقوق الإنسان ودور شركات القطاع الخاص في التدابير الرامية إلى تعزيز أمن الحواسيب ومكافحة الجريمة. ويجب أخذ تلك المسائل في الاعتبار عند تقييم الخيارات المتعلقة بكل من عملية صوغ الصك وشكله ومحتواه الممكنين. وبوجه عام، سيكون الصك الذي يحتوي على أحكام أوسع نطاقاً وأكثر إلزاماً أنجع، ولكن سيستغرق التفاوض بشأنه وقتاً أطول وستجد دول عديدة تنفيذه أصعب وأكثر استغراقاً للوقت. ولا يمكن وضع استنتاجات في المرحلة الراهنة، ولكن يوصى بأن يُطلب من فريق الخبراء أن ينظر في الخيارات الإجرائية والمضمونية فيما يتعلق بوضع صك دولي وأن يصوغ توصيات كجزء من تقريره إلى اللجنة في دورتها الحادية عشرة.

٤٩- وثمة عامل آخر ينبغي النظر فيه وهو أن الجريمة ذات الصلة بالتكنولوجيا الراقية والحواسيب آخذة في الازدياد بسرعة من حيث تواترها ونطاقها الجغرافي وتعقدتها التقني، وهو نسق يبدو على الأرجح أنه سيتواصل، بالتوازي مع سرعة تطور وانتشار وسائط جديدة للحواسيب والشبكات والاتصالات. ويوحى هذا التوقع بأنه، بينما يمكن أن يمثل الصك القانوني العالمي رداً هاماً في الأمد الطويل، فقد تكون هنالك حاجة أيضاً إلى تدابير ناجعة في المستقبل العاجل.

التشريعية والادعائية والتقنية والمتعلقة بإنفاذ القوانين التي كانت قد اكتسبتها مع دول أخرى، وذلك على نحو عام وكذلك في سياق حالات مفردة من الجرائم عبر الوطنية الكبرى. وينبغي التوسع في ذلك، من حيث النطاق وكذلك من حيث عدد البلدان المشاركة، لكن القيام بذلك يستوجب إجراء تقدير دقيق للاحتياجات الراهنة والموارد المتاحة للاستجابة لتلك الاحتياجات.

٤٥- لذلك، يوصى بأن يوعز إلى المركز المعني بمنع الإحرام الدولي التابع لمكتب مراقبة المخدرات ومنع الجريمة بالأمانة العامة أن يضطلع بدراسة أكثر تفصيلاً للمشكلة لكي يجيلها إلى لجنة منع الجريمة والعدالة الجنائية في دورتها الحادية عشرة. وسيرد أدناه مزيد من المناقشة لجوهر الموضوع الممكن لهذه الدراسة، ولكن ينبغي أن تتضمن الدراسة على الأقل استقصاء للاحتياجات الأساسية لدى الدول الأعضاء ومدى استعدادها لتقديم المساعدة من خلال توفير الموارد المالية والخبرة التقنية وآرائها بشأن الطريقة التي يمكن بها إعداد ردّ عالمي على هذه المشكلة والشكل الذي ينبغي أن يتخذه ذلك الرد.

٤٦- و يوصى كذلك بإنشاء فريق خبراء دولي حكومي مفتوح العضوية لكي يستعرض الدراسة ويعدّ الخيارات والتوصيات لانعام النظر فيها واتخاذ إجراءات بشأنها في الدورة الحادية عشرة للجنة. وكما لوحظ أعلاه، من الهام أن تشارك مجموعة كاملة من البلدان في كل مراحل العملية. ومن الهام أن يكون فريق الخبراء هذا متألفاً من أعضاء من مناطق مختلفة قدر الإمكان، وأن يتضمن بوجه خاص ممثلين من البلدان النامية. لذلك يوصى بدعم هذه المشاركة بتبرعات من دول أخرى إلى أقصى حد ممكن.

٤٧- ويوصى كذلك بإنشاء برنامج عالمي لمكافحة الجرائم ذات الصلة بالتكنولوجيا الراقية والحواسيب بعد الانتهاء من الدراسة والحصول على آراء فريق الخبراء، كما يوصى بأن تقدم الدول المهتمة تبرعات لإنشاء ودعم هذا

(د) ينبغي إدراج الآراء والمساعدة الصادرة عن عناصر من القطاع الخاص مع تسليط الضوء على الجوانب التالية:

١٠٠٠ ينبغي أن تبحث الدراسة وتُنظر في آراء ومساهمات الصناعات المسؤولة عن تطوير وتشغيل التكنولوجيات ذات الصلة، بما في ذلك المعدات والبرامجيات الحاسوبية وشبكات الحواسيب والاتصالات؛

١٠٠١ ينبغي أن تبحث الدراسة أيضاً في آراء المنظمات غير الحكومية ذات الصلة. وقد كانت المنظمات المكرّسة لقضايا مثل حرية التعبير وحماية الحرمة الشخصية بالغة الأهمية في المحاولات التي بذلت من قبل لإيجاد سلطات تحر فعالة. كما أنّها وُلدت معارضة سياسية للجهود التي قامت بها مجموعة الـ ٨ ومجلس أوروبا في ذلك المجال؛

(هـ) ينبغي أن تنظر الدراسة في المسائل المدرجة خارج نطاق مكافحة الجريمة، ومنها التنمية المستدامة وحماية الحرمة الشخصية وحرية التعبير وغير ذلك من الحقوق الأساسية وكذلك المصالح التجارية وغيرها. فتلك المصالح وغيرها من المصالح الأساسية وثيقة الصلة بالتطور التكنولوجي ومن المرجح أن تتأثر بازدياد الجرائم ذات الصلة بالحواسيب وكذلك بتزايد الجهود التي تبذلها الحكومات والمجتمع الدولي لمنع تلك الجرائم ومكافحتها؛

(و) ينبغي أن تقيّم الدراسة مدى الإجماع بصفة عامة وكذلك في سياق عوامل ذات صلة بالإحصاءات، مثل أشكال الإجماع المحددة والجغرافيا وغيرها من الظروف الاجتماعية والاقتصادية. وقد جرى من قبل بحث الصعوبات المعترضة في جمع وتحليل المعلومات الإحصائية الدقيقة. ولكن ينبغي أن تتوفر معلومات موثوقة أكثر لتوفير فهم موحد للنطاق التقني لهذا المجال ولدراسة

لذلك يوصى بأن يُطلب أيضاً من فريق الخبراء أن يضع مزيداً من الخيارات بشأن استراتيجية عالمية قصيرة الأمد لمكافحة الجريمة ذات الصلة بالتكنولوجيا الراقية والحواسيب، مع التركيز على مجالات مثل المساعدة العامة والمساعدة القانونية والتقنية الخاصة بمجالات محددة؛ ووضع معايير تقنية لأشياء مثل جمع الأدلة الإلكترونية وحفظها والتأكد من صحتها وإفشائها؛ وإنشاء جهات مركزية أو جهات اتصال بشأن طلبات المساعدة. وفي ذلك المضمار، ينبغي أن يؤخذ في الاعتبار العمل الذي بدأت تضطلع به المنظمات المذكورة في الباب الفرعي ألف من الباب الثاني من هذا التقرير.

هـ- عناصر دراسة مفصلة

٥٠- في الحالة المعرفية الراهنة، مازال مجال الجريمة ذات الصلة بالحواسيب يثير أسئلة أكثر من الأجوبة التي يقدمها، وثمة حاجة إلى القيام بمزيد من الدراسات لتحديد جوهر الموضوع وتحديد المصالح التي يؤثر فيها وكيفية تأثيره فيها وتبيين الخيارات السياسية للمستقبل. وينبغي أن تتضمن الدراسة على الأقل ما يلي:

(أ) ينبغي استقصاء آراء الدول في طبيعة المشكلة ونطاقها وردود الفعل المحلية والدولية الممكنة عليها؛

(ب) ينبغي استشارة الدول التي تمثل نطاقاً كاملاً من الخصائص الصناعية والقانونية والاجتماعية والاقتصادية؛

(ج) ينبغي النظر في كل الجرائم المحلية والدولية. ومع أن دولاً عديدة ستعتبر بعض المسائل اهتمامات محلية صرفة، فإن طبيعة التكنولوجيات تقيم تميزات تقليدية بين الجريمة المحلية وعبر الوطنية. وسيلاقى الباحثون وواضعو السياسات والمفاوضون في كثير من الأحيان صعوبة في التمييز بين الجرائم المحلية وعبر الوطنية مما يؤيد فكرة اتباع نهج متكامل، خصوصاً في المراحل الأولية من العملية؛

٢٠٠٠ طبيعة الجناة ودوافعهم. إن الجناة الذين يرتكبون جرائم أحدثتها التكنولوجيات الجديدة يمثلون مجال دراسة جديداً نسبياً. أما دوافع الجناة التقليديين أكثر مثل مشتهي الأطفال أو مرتكبي الاحتيال أو المتجرين بالمخدرات على الصعيد الدولي فهي محدّدة جيداً. ويستوجب تكيف هؤلاء الجناة مع التكنولوجيات الجديدة القيام ببحث في هذه الظاهرة من منظور الجريمة ذات الصلة بالحواسيب؛

٢٠٠١ الجوانب الجغرافية للجرائم. ستختلف الجوانب الجغرافية عن تلك المتعلقة بالجرائم التقليدية بشكل أكثر، وذلك على الأقل من جانبين رئيسيين. أما الجانب الأول فهو وجود "نطاقين جغرافيين" مركّبين فوق بعضهما البعض. فسيكون من الهام بحث الموقع المادي الفعلي للجناة وعوامله الموضوعية المحددة، ومنها الظروف الاجتماعية أو الاقتصادية أو الثقافية. ولكن، سيكون من الهام أيضاً بحث الجغرافيا الإلكترونية - أي الاعترافات ذات الصلة بالحيز السيرياني الذي كثر الحديث عنه - التي تؤثر في أنماط الإجماع.

واو- خيارات وتوصيات محدّدة للاضطلاع بمزيد من العمل بشأن الجريمة ذات الصلة بالتكنولوجيا الراقية والحواسيب

١- صك دولي ممكن لمكافحة الجريمة ذات الصلة بالتكنولوجيا الراقية والحواسيب

٥١- بعد الانتهاء من إعداد دراسة، يوصى بأن يشير فريق الخبراء على اللجنة بالمسائل والخيارات ذات الصلة بما إذا كان من الممكن والمستحسن صوغ صك دولي لمكافحة

نماذج الجرائم التي تظهر فيه. كما ينبغي التقليل من التقصير في الإبلاغ عن هذه الجرائم بزيادة توعية الناس بأنواع السلوك المعنية وبأنها تعامل أو ينبغي أن تُعامل كجرائم. كما أن من الهام جمع بيانات أولية لإيجاد دعم سياسي للإجراءات المحلية والدولية الفعالة لمكافحة تلك الجرائم؛

(ز) ينبغي أن تنظر الدراسة في تعريف وتصنيف الجرائم ذات الصلة بالتكنولوجيا الراقية والحواسيب. ويتسق التصنيف المستخدم في هذا التقرير مع أعمال أخرى في هذا المجال، وهو يمكن أن يصلح كأساس لإنعام النظر في هذه المسألة، ولكن من الضروري القيام ببحث أكثر دقة وتفصيلاً لوضع إطار يحظى بقبول كل الحكومات والجماعات ذات المصلحة والخبراء في هذا الميدان. فتلك أولوية عاجلة، حيث إن من الضروري وضع تعاريف وتصنيفات لتحقيق الاتساق في جمع الاحصاءات والبحوث التي سيُستند إليها في وضع مزيد من السياسات. وسيقتضي تحديد النماذج على نحو مجد دراسة العوامل في عدة مجالات رئيسية، منها التالية:

١٠٠٠ التكنولوجيا ذات الصلة. إن مجال الجريمة ذات الصلة بالتكنولوجيا الراقية والحواسيب مدفوع بقدر كبير بطبيعة ونطاق التكنولوجيا المعنية، التي تتطور وتتلاقى بسرعة. ولذلك السبب، استخدمت العبارة العامة "الجريمة ذات الصلة بالتكنولوجيا الراقية والحواسيب" في هذا التقرير وفي أعمال أخرى حول هذا الموضوع. وثمة حاجة إلى القيام ببحوث لاستقصاء كامل نطاق التكنولوجيا المعنية واقتراح خيارات للقيام بتصنيف عام يشملها كلها. كما أن هنالك حاجة إلى القيام ببحث أكثر تفصيلاً في التطورات التكنولوجية المحددة وأنواع النشاط الإجرامي التي تتوقف عليها. ونظراً لسرعة تطور التكنولوجيا، ينبغي أن تؤخذ في الاعتبار لا التكنولوجيا الحالية فحسب، بل والتطورات المحتملة أيضاً؛

والدولية للتغيرات. ويمكن أن تشمل الخيارات تفويض بعض السلطات التشريعية إلى هيئة من الخبراء تمثل الدول الأطراف وتُنشأ لهذا الغرض، واستخدام البروتوكولات لمعالجة مسائل محددة عند نشوئها واللجوء إلى صياغة واسعة نسبياً ومحايدة تكنولوجياً أو تدابير أخرى؛

(د) كيفية إدماج المصالح ذات الصلة، ومنها الحرمة الشخصية وحرية التعبير وغيرها من المصالح التجارية والمتعلقة بحقوق الإنسان في صك دولي. فمع أنّ جوهر الموضوع يقتضي أن ينصب تركيز الصك المعتمد على مكافحة الجريمة ومنعها، يجب النظر أيضاً في مصالح أخرى أثناء صياغة الصك وكذلك في محتواه الموضوعي.

٢- استراتيجية قصيرة الأجل لمعالجة الجريمة ذات الصلة بالتكنولوجيا الرقابة والحاسب

٥٢- كما أشير إليه أعلاه، تمثل الجريمة ذات الصلة بالتكنولوجيا الرقابة والحاسب مشكلة ملحة قد تقتضي رد فعل دولياً متضافراً في الامدين القصير والطويل. ويوصى بأن تستعرض الدراسة التدابير التي يمكن اتخاذها في المستقبل العاجل وبأن يصوغ فريق الخبراء توصيات بشأن استراتيجية قصيرة الأجل لكي تنظر فيها اللجنة في دورتها الحادية عشرة. ويمكن أن تشمل عناصر هذه الاستراتيجية ما يلي:

(أ) جمع المعلومات عن الجريمة ذات الصلة بالتكنولوجيا الرقابة والحاسب والردود الممكنة عليها، وتعميم هذه المعلومات على كل الدول الأعضاء من أجل اطلاع كل الدول التي لم تشارك بعد في المناقشات بأسرع وقت ممكن. وستشكل الدراسة المقترحة عنصراً أساسياً من المجموعات المتكاملة من المعلومات، ولكن تتوفر أيضاً مواد أخرى، منها ما يلي:

١٠٠ يمكن تحديث دليل الأمم المتحدة لمنع الجريمة المتصلة بالحاسب ومكافحتها، الذي نشر سنة ١٩٩٤، وإعادة إصداره؛

الجريمة ذات الصلة بالتكنولوجيا الرقابة والحاسب. وستشمل تلك المسائل ما يلي:

(أ) مسألة ما إذا كان ينبغي أن يكون الصك، إذا تقرر إعداد، وصائياً أو ملزماً قانونياً. ويمكن أن يسعى الصك المعتمد إلى إرساء اشتراطات إلزامية بشأن أشياء كالأفعال الإجرامية وسلطات التحري وآليات التعاون الدولي، أو يمكن أن يكتفي بمجرد توفير مبادئ توجيهية لمساعدة الدول على استحداث تدابير فعالة وترويج التوحيد الدولي للقوانين والإجراءات. وسينطوي الحل الوسط بين هذين الخيارين، الذي تشكل اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية مثلاً عليه، على وضع صك تنشئ بعض أحكامه التزامات ملزمة، بينما تتضمن الأحكام الأخرى مبادئ توجيهية أعم أو تترك مسألة تنفيذها لتقدير الدول الأطراف؛

(ب) العلاقة التي ستكون للصك المعتمد باتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، إن كانت ستكون هنالك أي علاقة بينهما. وبوجه عام يمكن أن تكون الاتفاقية المذكورة بمثابة سابقة لبعض الأحكام، بينما قد لا تكون بعض الأحكام الأخرى مناسبة لجوهر موضوع الجريمة ذات الصلة بالتكنولوجيا الرقابة والحاسب. فحصر نطاق الاتفاقية في أنشطة "الجماعات الإجرامية المنظمة"، مثلاً، سيستبعد جزءاً كبيراً من الجرائم ذات الصلة بالتكنولوجيا الرقابة والحاسب، لأن هذه الجرائم يرتكبها أفراد أو جماعات من الأفراد الذين لا يندرجون ضمن التعريف المبين في الاتفاقية.^(٢٣) لذلك، يبدو أنّ من غير الممكن صوغ بروتوكول آخر ملحق بالاتفاقية بشأن هذا النوع من الجرائم؛^(٢٤)

(ج) كيفية الحفاظ على حداثة الصك بعد الانتهاء من صوغه. فكما لوحظ في مقدمة هذا التقرير، يتميز هذا المجال الذي هو قيد البحث بدنامية تطوّر التكنولوجيات والأنشطة الإجرامية ذات الصلة بها، وسيكون من الهام ضمان مواكبة أي إطار لإدماج التدابير المحلية

(د) ينبغي التشجيع على إنشاء جهات مركزية أو نقاط اتصال في كل دولة من الدول الأعضاء. وذلك سيشمل نقاط الاتصال بشأن تقديم المساعدة العاجلة في التحريات عن الجرائم ذات الصلة بالحواسيب^(٢٦) لكنه سيشمل أيضاً جهات اتصال أعم لغرض جمع المعلومات عن التطورات في كل دولة وعن تلقي وتعميم المعلومات الواردة من المجتمع الدولي؛

(هـ) ستكون هنالك حاجة إلى رصد قدر كبير من الموارد المالية والتقنية. ويمكن أن تكون هذه المساعدة على شكل تبرعات إلى صندوق الأمم المتحدة لمنع الجريمة والعدالة الجنائية أو توفير الخبرة الفنية أو المواد لبرنامج عالمي لمكافحة الجرائم ذات الصلة بالتكنولوجيا الرقمية والحواسيب أو لمشاريع محددة من مشاريع الأمم المتحدة. فالطابع العالمي للتكنولوجيات وقابلية استغلالها بسهولة من قبل الجناة في أي مكان كانوا يُوفران حوافز للدول التي لديها موارد مالية أو تقنية لكي تساعد غيرها من الدول. كما أن للصناعات التي تطوّر وتشغل شبكات الحواسيب والاتصالات موارد مالية وتقنية يمكن استغلالها، وكذلك حوافز للمساهمة، لأنّ أشكالاً عديدة من الجرائم ذات الصلة بالحواسيب تهدّد الجدوى التجارية لمنتجاتها.

٣- وضع برنامج عالمي لمكافحة الجرائم ذات الصلة بالتكنولوجيا الرقمية والحواسيب

٥٣- تشير الأدلة المتوفرة إلى أن هنالك قدراً كبيراً من النشاط في مجالي البحث والتطوير المتعلقين بوضع سياسات وتدابير قانونية وتقنية، لكن التنسيق العام بين هذه الأنشطة قليل. ويختلف نطاق النشاط من بلد إلى آخر. ويشارك في هذه الأنشطة عددٌ من المنظمات الدولية-الحكومية والمنظمات غير الحكومية وكذلك عدّة وكالات وإدارات تابعة للأمم المتحدة، وهي موضع انشغال كبير لدى الشركات التجارية والجماعات غير الحكومية ذات المصلحة. وثمة بالأحرى تركيز في الاهتمام وفي تخصيص الموارد على مسائل محدّدة تهمّ الحكومات أو المنظمات المعنية مباشرة، مما

٢٤ يمكن نشر وتعميم وقائع ومواد حلقة العمل المعنية بالجرائم ذات الصلة بشبكات الحواسيب، التي عقدت أثناء مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين^(٢٥)؛

٣٠ يمكن تعميم المواد الصادرة عن منظمات دولية حكومية أخرى، وخصوصاً مجلس أوروبا والانتربول وفريق ليون الذي أنشأته مجموعة الـ ٨، تعميماً أوسع نطاقاً؛

٤٤ يمكن عقد حلقات عمل أو حلقات دراسية أو جلسات توجيهية مع المسؤولين في الدول المهتمة، مع إمكانية مشاركة ممثلين من القطاع الخاص؛

(ب) يمكن جعل المواد ذات الصلة بتدريب المحققين والمدعين العامين متاحة أكثر. ولم تنتج الأمم المتحدة مواد من هذا القبيل، لكن عدداً من الدول الأعضاء فعلت ذلك من أجل استخدام تلك المواد في تدريب موظفيها، وفي بعض الحالات من أجل استخدامها في مشاريع المساعدة التقنية المقدمة إلى دول أخرى؛

(ج) ستكون هنالك حاجة إلى المساعدة التقنية المباشرة في بعض الدول. ويمكن أن تشمل هذه المساعدة تدريب القضاة والمدعين العامين والمحققين والخبراء التقنيين والقضائيين الذين يمكن أن يصبح العديد منهم في موضع يؤهلهم لتدريب الآخرين. وفي بعض الحالات، يمكن إدماج هذه المشاريع مع مشاريع إنمائية عامة أخرى تهدف إلى مساعدة الدول على حيازة واستخدام تكنولوجيات جديدة لتحقيق تنميتها. وكما لوحظ أعلاه، سيكون من الهام أن يصبح منع الجريمة ومكافحتها جزءاً أساسياً ثابتاً في تلك المشاريع إذا أُريد تجنب الآثار المناوئة التي تلحق بالتنمية من جراء الجرائم ذات الصلة بالحواسيب؛

الإنسان والتنمية، بهدف إدراج موضوع الجريمة ذات الصلة بالحواسيب في برامج أخرى، حسبما هو مناسب، وضمان إدماج مساهمات برامج أخرى في وضع استراتيجيات لمنع الجريمة ومكافحتها؛

(ز) تنسيق الأنشطة مع منظمات دولية حكومية أخرى ومع الحكومات والوكالات الناشطة في مجال الجريمة ذات الصلة بالتكنولوجيا الراقية والحواسيب؛

(ح) تنسيق الأنشطة مع الجماعات غير الحكومية ذات المصلحة وشركات القطاع الخاص وتنظيم الموارد النقدية والخبرة التقنية المقدمة من الشركات كجزء من استراتيجية عالمية لمكافحة الجريمة ذات الصلة بالتكنولوجيا الراقية والحواسيب.

٤- قائمة حصرية أولية بالمسائل المضمونية لكي ينظر فيها

٥٥- سيتعين التطرق إلى العديد من المسائل المضمونية ذاتها بصفقتها عناصر من استراتيجيات قصيرة الأجل وكذلك طويلة الأجل. واستناداً إلى المداولات التي دارت سابقاً في الأمم المتحدة وغيرها من المحافل المشار إليها في هذا التقرير، تستوجب المسائل المضمونية التالية أن ينظر فيها:

(أ) تبين السلوك المؤذي الذي ينطوي على استخدام تكنولوجيا جديدة وتجرىم أفعال جديدة أو تعديل مفهوم الأفعال المجرمة حالياً لكي تشمل تجريم ذلك السلوك؛

(ب) وضع مبادئ لمعالجة تعقب الاتصالات على الصعيد عبر الوطني، بما في ذلك إنشاء صلاحيات للحصول على بيانات المرور والحفاظ عليها وإفشائها؛^(٢٧)

(ج) وضع مبادئ تنظم عمليات التفتيش الإلكتروني عبر الحدود، المتعمدة وغير المتعمدة؛

يزيد في احتمال وجود فجوات أو حالات من التضارب في البحوث. وتوجد الأمم المتحدة، بحكم طبيعتها العالمية، في موضع فريد لبحث وتنسيق الأنشطة في المجال الذي هو قيد النظر. ويوصى بوضع برنامج عالمي لمكافحة الجرائم ذات الصلة بالتكنولوجيا الراقية والحواسيب بعد الانتهاء من استقصاء احتياجات الدول الأعضاء وآرائها. ويوصى أيضاً بأن تقدم الدول تبرعات لإرساء هذا البرنامج العالمي وتشغيله.

٥٤- وينبغي للجنة في دورتها الحادية عشرة أن تنظر في النطاق المرجعي الممكن للبرنامج العالمي، وذلك بعد الحصول على نتائج الدراسة وآراء فريق الخبراء. ويمكن أن تشمل ولاية البرنامج العالمي الأنشطة المبيّنة في الفقرة ٥٢ أعلاه وكذلك الأنشطة التالية:

(أ) تبين الدول الأعضاء التي تطلب المساعدة وتحليل احتياجاتها المحددة؛

(ب) وضع مواد لمساعدة صانعي السياسات والمشرعين وأجهزة إنفاذ القوانين والمدعين العامين وسائر المسؤولين ذوي الصلة في معالجة الحالات المحلية وعبر الوطنية؛

(ج) جمع المواد التي تعدها جهات أخرى وتجميعها معاً وتعميمها؛

(د) تقديم المساعدة القانونية والتقنية وغيرها من ضروب المساعدة إلى الدول التي تطلبها، رهناً بتوافر الموارد الكافية؛

(هـ) وضع قائمة حصرية بالخبرة التقنية المتوفرة من الأفراد والأجهزة الراغبين في تقديم المساعدة إلى الدول التي تطلب ذلك؛

(و) تنسيق الأنشطة مع الوكالات والإدارات الأخرى التابعة للأمم المتحدة، وخصوصاً في مجالي حقوق

هنالك حاجة إلى هذه البرامج والمواد لمساعدة الدول على المشاركة بفعالية في وضع سياسات عالمية وكذلك لضمان تمتع السلطات المحلية بالقدر الوافي من التدريب والتجهيز بحيث يتسنى لها أن تردّ بفعالية وسرعة على طلبات الحصول على المساعدة في التحري في الجرائم عبر الوطنية ذات الصلة بالحوسيب؛

(ك) جمع وتحليل وتقاسم المعلومات عن التطورات التكنولوجية الجديدة والحناءة وأساليبهم وعن الطرائق الناجعة لمنع هذه الجرائم والتحري عنها وملاحقة مرتكبيها قضائياً؛

(ل) تدريب الخبراء المعنيين بإنفاذ القوانين وتجهيزهم ومدّهم بالموارد لضمان قدرتهم على ممارسة أعمالهم بفعالية في مجال التحري في الجرائم وملاحقة مرتكبيها قضائياً في الحالات المحلية، وقدرتهم على التعاون بفعالية مع دول أخرى في الحالات عبر الوطنية؛

(م) ضرورة تقييم وتوضيح دور القطاع الخاص وعلاقته بالحكومات، على كلا الصعيدين المحلي والدولي. وتشمل العناصر أو الجوانب المحددة من هذه العلاقة التي تستوجب النظر فيها ما يلي:

١٠ ضرورة إقامة توازن بين التدابير الناجعة لمكافحة الجريمة والموقفات التقنية والتجارية التي تعترض وضعها وتنفيذها. وينبغي للصناعات أن تأخذ مسألة مكافحة الجريمة بعين الاعتبار أثناء مرحلة تصميم تكنولوجيات جديدة، ولكن يجب على أجهزة إنفاذ القوانين أن تسلّم بأن بعض التدابير قد لا تكون ممكنة تقنياً أو قد تمثل تغيرات من شأنها أن تجعل التكنولوجيات غير منتجة أو غير قادرة على المنافسة. ولا ينبغي أن تؤثر متطلبات مكافحة الجريمة في الجدوى الأساسية للتكنولوجيات الجديدة أو

(د) وضع مبادئ موحدة لمعالجة اعتراض سبيل الاتصالات التي تُجرى على شبكات الحواسيب وما شابهها من الوسائط؛

(هـ) تقدير المصالح المتعلقة بالسرية والحرمة الشخصية، التي هي ملازمة لأشكال مختلفة من عمليات خزن البيانات ونقلها من أجل استحداث تدابير رقابية إجرائية بشأن ضبط البيانات واعتراض سبيلها بما يتماشى مع تلك المصالح. ومعظم الدول تضع قيوداً قليلة أو لا تضع قيوداً البتة على إمكانية وصول أجهزة إنفاذ القوانين إلى المواقع الشبكية المفتوحة أو الاتصالات على الشبكة العالمية مثلاً، لكنها تنزع إلى وضع قيود على ضبط البيانات من مصادر أكثر خصوصية؛

(و) وضع معايير أو ممارسات موحدة لتبين الأفراد الذين يستخدمون خدمات شبكات الحواسيب أو وسائط الاتصالات، مع موازنتها بضرورة مراعاة الحرمة الشخصية وكتمان الهوية؛

(ز) وضع مبادئ موحدة لتعديل الممارسات القضائية والقواعد القانونية بشأن الإثبات لضمان إمكانية الحفاظ على الأدلة الحاسوبية والتأكد من صحتها واستخدامها في الإجراءات الجنائية؛

(ح) وضع مبادئ موحدة لحماية الحقوق الأساسية عند وضع سياسات وتدابير دولية لمكافحة الجرائم ذات الصلة بالتكنولوجيا الرقابة والحوسيب وكذلك عند تنفيذ هذه التدابير في حالات محددة؛

(ط) وضع مبادئ موحدة تنظم سرية البيانات وكما لها، وموازنة هذه المبادئ أو توفيقها مع ضرورة اتخاذ تدابير ناجعة لمكافحة الجريمة؛

(ي) وضع وتمويل برامج و مواد للمساعدة التقنية لصالح الدول التي تطلب تلك المساعدة. وستكون

٤٤ ضرورة إجراء تقييم عالمي للدور المحتمل للقطاع الخاص في مكافحة الجريمة. وهذه مسألة معقدة بدأت تواجه العديد من موفري الخدمات الذين يشاطرون الاهتمام العام بمكافحة الجريمة على نحو فعال، لكنهم يدركون المخاطر والصعوبات التي تنشأ إذا ما أصبحوا عنصراً بديلاً أو مكماً لأجهزة الدولة لإنفاذ القوانين. وتواجه الصناعات ضغوطاً متزايدة بشأن إدماج تدابير أمنية في تكنولوجيا جديدة قد لا تكون مجدية تجارياً أو قد تؤثر في المصالح الأساسية لزيابتهائها.^(٢٨) كما أنها تواجه ضغوطاً من الحكومات لمراقبة أو استبعاد المحتوى الذي يعتبر غير مشروع أو غير مناسب، أو لمساعدة أجهزة الدولة لإنفاذ القوانين على إجراء تحرياتها الجنائية. وتثير هذه الضغوط مسائل أخلاقية وقانونية وسياساتية معقدة ينبغي استكشافها على المستويين الوطني والعالمي، بهدف تحقيق أكبر قدر من الاتساق العالمي.

الحواشي

(١) انظر "بناء الجسور الرقمية" في تقرير الأمين العام إلى جمعية الأمم المتحدة للألفية (A/54/2000)، الفقرات ١٥٠ - ١٦٧. انظر أيضاً تقرير الأمين العام عن التنمية والتعاون الدولي في القرن الحادي والعشرين: دور تكنولوجيا المعلومات في إطار اقتصاد عالمي قائم على المعرفة (E/2000/52)، الأبواب من الثالث إلى الخامس).

(٢) اللجنة الأوروبية المعنية بمشاكل الجريمة، لجنة الخبراء المعنية بالجريمة في الحيز السيبراني، "مشروع الاتفاقية المتعلقة بالجريمة السيبرانية" ("Draft Convention on Cyber-crime" (PC-CY(2000), draft No 25, rev.5) وهي متاحة على الانترنت على العنوان <http://conventions.coe.int/treaty/en/projects/cybercrime25.htm>.

في قدرتها على المنافسة، لكن تكاليف الجريمة ومنع الجريمة يجب أن يصبح جزءاً من التقييمات الإجمالية لنسبة الفائدة إلى التكلفة بشأن كل من الحكومات والصناعات، وينبغي تخصيص التكاليف، حسبما هو مناسب، من الأرباح التي تولدها التكنولوجيات التي تدعم الجرائم؛

٢٤ ضرورة تعاون الحكومات والصناعات على نحو فعال لتحقيق أقصى قدر من الفوائد وتقليل التكاليف التي ينطوي عليها ذلك إلى أدنى قدر. وهذا يشمل تبين ووضع تقنيات أمنية فعالة وتقنيات فعالة أخرى بشأن منع الجريمة، وإدماج هذه التقنيات في التكنولوجيات الجديدة في أبكر مرحلة ممكنة من إنشائها، وتدريب وإعداد أجهزة إنفاذ القوانين والنيابة العامة فيما يتعلق بالتكنولوجيات الجديدة قبل أن يتمكن الجناة المحتملون من الوصول إليها. فالتقدم التكنولوجي للصناعات ذات الصلة يجعلها هامة، إن لم تكن أساسية، لضمان نجاح برامج المساعدة التقنية، وستكون المصالح التجارية للصناعات ذاتها، في حالات عديدة، مبرراً لمشاركتها في هذه البرامج؛

٣٤ ضرورة إنشاء نُظُم وإجراء عمليات بطرائق تدعم القيام بتحريات جنائية ومنع الجريمة على نحو فعال، على أن تُراعى في ذلك أيضاً ضرورة حماية حرمة الشخصية وغيرها من حقوق مستخدمي التكنولوجيات. وتشمل الأمثلة على ذلك تشغيل نُظُم قادرة على الاحتفاظ بأدلة الاتصالات لفترات معقولة تحسباً لاحتمال ظهور حاجة إليها في التحريات، وضرورة التمكن من تحديد هوية الزبائن.

(١٢) أنظر العددين ٤٣ و ٤٤ من المحلة الدولية للسياسات الجنائية (منشورات الأمم المتحدة، رقم المبيع E.94.IV.5).

(١٣) أنظر قراري الجمعية العامة ٩١/٥٢ المؤرخ ١٢ كانون الأول/ديسمبر ١٩٩٧ و ١١٠/٥٣ المؤرخ ٩ كانون الأول/ديسمبر ١٩٩٨. أنظر أيضاً الفقرات ١٦١-١٧٤ من الوثيقة مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين، فيينا، ١٠-١٧ نيسان/أبريل ٢٠٠٠: تقرير من إعداد الأمانة العامة (منشورات الأمم المتحدة، رقم المبيع A.00.IV.8).

(١٤) أنظر الفقرة ١٤ من الوثيقة A/CONF.187/L.10.

(١٥) أنظر الفصل الأول من تقرير مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين...

(١٦) أنظر المادتين ٢ (استخدام المصطلحات) و ٣ (نطاق الانطباق) من الاتفاقية (المرفق الأول من القرار ٢٥/٥٥).

(١٧) هذه الجرائم بحثتها في الآونة الأخيرة فرقة العمل للإجراءات المالية عن غسل الأموال، التابعة لمنظمة التعاون والتنمية في الميدان الاقتصادي. أنظر الفقرات ٥-١٨ من تقرير فرقة العمل عن "أنماط غسل الأموال للفترة ٢٠٠٠-٢٠٠١" (باريس، منظمة التعاون والتنمية في الميدان الاقتصادي، شباط/فبراير ٢٠٠١).

(١٨) الفقرة ١٥٢ من الوثيقة A/54/2000.

(١٩) على سبيل المثال، أفاد مدير مكتب المباحث الاتحادي للولايات المتحدة، في كلمة عن الجريمة السيبرانية ألقاها أمام اللجنة القضائية لمجلس شيوخ الولايات المتحدة في ٢٨ آذار/مارس ٢٠٠٠، بأن عدد القضايا التي ينظر فيها مجلس المباحث الاتحادي تضاعف من ٥٤٧ إلى ١١٥٤ قضية، بالرغم من أنه ليس واضحاً ما إذا كان ذلك يعود إلى الارتفاع في عدد الجرائم أو في حالات الإبلاغ عنها أو كليهما. أنظر: بيتر غرابوسكي، "الجريمة عبر الحاسوب: عرض عام من وجهة نظر علم الإجرام"، منتدى حول الجريمة والمجتمع، المجلد ١ (٢٠٠١)، ص ٣٨.

(٢٠) اعترف مختص في البرمجة من الولايات المتحدة عمره ٣١ عاماً بأنه أنشأ فيروس "ميليسا" ("Melissa")، واعترف طفل كندي في الخامسة عشرة من العمر بأنه مذنب في ٥٦ تهمة جنائية تتعلق بالهجمات لتعطيل الخدمة. ولم توجه التهمة إلى أحد في قضية فيروس "I love you"، ولكن يعتقد ان الفيلين هي منشأ هذا

(٣) ترد الاستنتاجات المستخلصة من الدراسات مبيّنة في توصيتي مجلس أوروبا R(89)9 و R(95)13. ولجنة الخبراء أنشأتها لجنة الوزراء التابعة لمجلس أوروبا في الاجتماع ٥٨٣ لنواب الوزراء في ٤ شباط/فبراير ١٩٩٧.

(٤) أنظر مرفق البلاغ الصادر عن اجتماع وزراء العدل والداخلية لمجموعة الـ ٨، الذي عقد في واشنطن العاصمة في ١٠ كانون الأول/ديسمبر ١٩٩٧.

(٥) أنظر الفقرة ١٧ والمرفق ١ من البلاغ الصادر عن المؤتمر الوزاري لمجموعة البلدان الـ ٨ بشأن مكافحة الجريمة المنظمة عبر الوطنية، الذي عقد في موسكو يومي ١٩ و ٢٠ تشرين الأول/أكتوبر ١٩٩٩.

(٦) عقد الاجتماعان في باريس من ١٥ إلى ١٧ أيار/مايو ٢٠٠٠ وفي برلين من ٢٤ إلى ٢٦ تشرين الأول/أكتوبر ٢٠٠٠. ويعتزم عقد اجتماع آخر في طوكيو في أيار/مايو ٢٠٠١.

(٧) في الفقرة ١٤ من القرار ٢٣/١٩٩٩، يطلب المجلس إلى الأمين العام أن يجري دراسة عن التدابير الفعالة التي يمكن اتخاذها على الصعيدين الوطني والدولي لمنع ومكافحة الجرائم ذات الصلة بالحواسيب، تتضمن استقصاء عن استحسان وضع أدلة عملية ومبادئ توجيهية وتوصيات، وأن يقدم تقريراً عن استنتاجات الدراسة إلى لجنة منع الجريمة والعدالة الجنائية في دورتها العاشرة.

(٨) أنظر قراري الجمعية العامة ١٠٩/٤٥ و ٤٥/٤٥/١٢١ المؤرخين ١٤ كانون الأول/ديسمبر ١٩٩٠ ووثيقة مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين، هافانا، ٢٧ آب/أغسطس - ٧ أيلول/سبتمبر ١٩٩٠: تقرير من إعداد الأمانة العامة (منشورات الأمم المتحدة، رقم المبيع A.91.IV.2)، الفصل الأول، الباب جيم، ص - ١٨٩.

(٩) أنظر الفقرات ٣٧٠-٣٨٥ من الوثيقة A/CONF.169/16/Rev.1.

(١٠) أنظر الفقرتين ٨ و ١٨ من المادة ١٨ من المرفق الأول بقرار الجمعية العامة ٢٥/٥٥ المؤرخ ١٥ تشرين الثاني/نوفمبر ٢٠٠٠.

(١١) أنظر الباب الأول من الفصل الأول من التقرير عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين ...

تكون محكمة مختصة أو هيئة عمومية أخرى قد قضت بأن المحتوى ذاته غير مشروع.

الفيروس. وقد تم توزيع مجموعة واسعة من التقديرات للأضرار الناجمة عن كل حادثة من هذه الحوادث، لكن التكاليف الحقيقية لن تُحدّد على الأغلب أبداً. والأرقام المذكورة كدليل على النطاق العام للخسائر وعلى مستوى القلق السياسي بشأن الخطر الذي تمثله الجرائم على ذلك النطاق.

(٢١) أنظر الأبواب الثالث إلى الخامس من الوثيقة E/2000/52.

(٢٢) أنظر الفقرات ٧٩-٩٩ من الوثيقة E/2000/52.

(٢٣) أنظر المادتين ٢ و ٣ من الاتفاقية (المرفق الأول من القرار ٢٥/٥٥).

(٢٤) تتضمن البروتوكولات الثلاثة الراهنة كلها الأحكام المتعلقة بنطاق وانطباق الاتفاقية، مع ما تقتضيه الحال من تغييرات. ونظراً لأن العديد من أحكام الاتفاقية صيغت على أساس أنها لن تنطبق إلا على الحالات التي تخصّ جماعات إجرامية منظمة، فسيكون من الصعب تطبيقها على الحالات التي تخصّ الجرائم ذات الصلة بالحواسيب التي يرتكبها أفراد.

(٢٥) يعكف معهد آسيا والشرق الأقصى لمنع الجريمة ومعاملة المجرمين التابع للأمم المتحدة، الذي نظم حلقة العمل هذه، في الوقت الحالي على إعداد تلك المواد لنشرها.

(٢٦) هذه العملية كانت قد بدأتها مجموعة الـ ٨ وتبعتها الانترنتبول.

(٢٧) يشير تعبير "بيانات المرور" بوجه عام إلى البيانات التي يخزنها موفرو الخدمات والتي تدوّن مصدر الاتصالات الإلكترونية ومقصدتها. وهذا يمكن أن يشمل كلا من المصدر الأول والمقصد النهائي وكذلك المصادر والمقاصد المؤقتة داخل الشبكة الحاسوبية. ويتصل بذلك التعبير مفهوم آخر هو بيانات "المنخرطين" أو "المستخدمين"، ويستخدم موفرو الخدمات هذا المفهوم لتحديد هوية الزبائن الأفراد.

(٢٨) من الأمثلة الحديثة على ذلك إصدار محكمة فرنسية أمراً تطالب فيه شركة الانترنت "ياهو" (Yahoo! Inc.) باستحداث طرائق تقنية لإقفال باب الوصول أمام منخرطيها في فرنسا إلى المواقع الشبكية للبيع بالمراد العلني لأشياء تذكارية نازية. فبيع هذه الأشياء محظور في فرنسا، لكنه مشروع في الولايات القانونية الأخرى التي توجد فيها هذه المواقع. وموفرو الخدمات راغبون بوجه عام في اتخاذ هذه الإجراءات - بالقدر الممكن تقنياً - ولكن فقط عندما