الاتحاد الدولي للاتصالات

المؤتمر العالمي لتنمية الاتصالات
إسطنبول 2002

المؤتمر العالمي لتنمية الاتصالات
لعام 2002

إسطنبول، تركيا، 18 – 27 مارس 2002

الوثيقة A-141
20 مارس 2002
الأصل: بالإنكليزية

البند 3 من جدول الأعمال **اللجنة 4**

هنغاريا

مقترحات بشأن أعمال المؤتمر

الجرائم الإلكترونية

تقدم سلطة الاتصالات في هنغاريا هذه الوثيقة إلى المؤتمر العالمي لتنمية الاتصالات – 2002 للنظر فيها.

مقدمة

من السمات المميزة لمجتمع المعلومات أن تكنولوجيا المعلومات الحديثة تتغلغل في كل مجالات الحياة تقريباً بطريقة تتيح زيادة فعالية الإدارة والأعمال المكتبية والتجارة والاتصال. ولكن المجتمع الجديد لا يحصل على المزايا وحسب، فقد بدأت العيوب تظهر في الأفق أيضاً. وكما يحدث في أي مجال من مجالات الحياة التي تتصارع فيها المصالح الاقتصادية أو يمكن فيها الحصول على مزايا اقتصادية عن طريق الجريمة ظهرت هذه الأفعال الإجرامية في هذا المجال أيضاً باستخدام التكنولوجيا الجديدة. والأفعال الإجرامية المرتبطة بالحاسوب لا تطال جميع البلدان بالتساوي. وهي تسبب متاعب كثيرة خاصة في تلك البلدان التي بلغت التكنولوجيا فيها مرحلة من التطور والتي أصبحت فيها الوسائل والأدوات الجديدة جزءاً لا يتجزأ من حياة المجتمع.

وبالتوازي مع تطور الظروف التكنولوجية لمجتمع المعلومات بدأت مسألة الجرائم الإلكترونية تمس أعداداً متزايدة من الناس: فنحن نتعايش مع فيروسات الحاسوب وبدأت فيروسات البريد الإلكتروني في الانتشار. ولم يمض وقت طويل حتى أصبحت مواقع شهيرة مثل "ياهو" أو "أمازون" أو موقع "إيليندر" في هنغاريا في قلب هجوم المخترقين. والضرر المعنوي والمادي الذي يصيب مقدمي الخدمة ضرر كبير. ولم تقف الخسارة عند حد مقدمي الخدمة بل إن المستعملين أيضاً قد يجدون أنفسهم بين الضحايا بسبب انضمامهم إلى الشبكة. ولذلك فإننا نحتاج بشدة إلى حل لقمع الجرائم الإلكترونية.

الاقتراح

لكي نتمكن من مكافحة هذه الجرائم يجب أن نعرف أولاً ما هو المعنى الحقيقي للجرائم الإلكترونية وحجم الضرر الذي تسببه.

الخطوة 1: المتابعة الإحصائية للجرائم الإلكترونية

ليس من السهل أن نراقب الأفعال الإجرامية نظراً لأن مرتكبيها يفعلون كل ما يستطيعون لإخفاء سلوكهم غير القانوني ولإخفاء شخصياتهم. وهناك بعض الظواهر الخاصة بالإضافة إلى العوامل الشكلية المشوِّهة التي نعرفها في العادة وهو أمر يزيد من صعوبة مراقبة الأفعال الإجرامية المرتبطة بالحاسوب.

- توضيح ومتابعة الجريمة المرتبطة بالحاسوب يزداد صعوبة لأن التكنولوجيا تعطي لمرتكبي الجريمة إمكانية الاختفاء: إذ يمكن ارتكاب الفعل باستعمال كلمات مرور وعلامات هوية تخص أشخاصاً آخرين. والشبكات الإلكترونية تعبر حدود الدول الأمر الذي يجعل الجرائم الإلكترونية ممكنة بحيث يستطيع مرتكب الجريمة أن يخرق القانون في بلد بينما هو في بلد آخر. وبالإضافة إلى ذلك نجد أن بعض مرتكبي الجرائم من الصغار الذين لا يتعرضون للعقوبة.

- تسعى الأطراف المتضررة (مثل البنوك) إلى التغطية على هذه الأفعال للحفاظ على سمعتها الطيبة.

- يجعل الطابع الجديد لهذه الجرائم من الصعب رصدها إحصائياً. فلم يتم بعد تشكيل ممارسة قضائية موحدة تتعلق بهذه الأفعال الإجرامية الجديدة. ولذلك لا نجد غرابة في وجود تأخير كبير في التصرفات القانونية حيال الجرائم الإلكترونية.

الخطوة 2: التوصل إلى التنظيم الملائم – أفضل الممارسات

ظلت مسألة التنظيم القانوني للمشاكل التي يثيرها مجتمع المعلومات في مركز الاهتمام بالفعل منذ سنوات. ويتوالى إدخال التعديلات اللازمة في القوانين القائمة لمعالجة هذه الأوضاع الجديدة في الحياة كما يجري إعداد قوانين جديدة. ويجري تشكيل استراتيجيات وتوقعات جديدة ولكن الاهتمام بالجرائم الإلكترونية أقل من اللازم مقارنة بحجم الضرر الذي تسببه هذه الجرائم.

وحتى إذا افترضنا أن الأدوات القانونية القائمة كافية لمعالجة الجرائم التي تُرتكب بواسطة أدوات المعلومات التكنولوجية فإن هذه الجرائم تحتاج مزيداً من الفحص. ويعني ذلك أن الحماية منها تتطلب وسائل تكنولوجية وتنظيمية تختلف عادة عن تلك الوسائل التي تتطلبها جرائم مشابهة ولكنها تُرتكب بأدوات أخرى. وبالتوازي مع التنظيم القانوني يجب علينا أن نتوصل أولاً وقبل كل شيء إلى حل القضايا التكنولوجية والتنظيمية المتعلقة بالأمن لكي يمكن منع هذه الجرائم.