الأمن السيبراني

كان الاستخدام العمومي للإنترنت في عام 1988 لا يزال في مراحله الأولى، ولم تنص لوائح الاتصالات الدولية التي تم إعدادها في تلك السنة على أحكام صريحة بشأن الأمن السيبراني. غير أنها تضمنت (في المادة 9) إشارةً إلى تجنب "الضرر التقني"، كانت قد أضيفت لمواجهة انتشار أحد الأشكال الأولى من البرمجيات الضارة، وهي دودة موريس، في ذلك الوقت. وفي العقود التي تلت منذ ذلك الحين، تزايدت أهمية حماية الأمن السيبراني بصورة هائلة مما يستدعي النظر فيها مع استعراض لوائح الاتصالات الدولية. وقد طرحت مقترحات بإضافة أو تعديل مواد في المعاهدة بحيث يدرج فيها عناصر تتعلق بالأمن، بما في ذلك تدابير لمكافحة الرسائل الاقتحامية.

وفي نفس الوقت الذي يزداد فيه اعتمادنا على الإنترنت وغيرها من الشبكات لأغراض الخدمات والمعلومات الأساسية، يتزايد عدد الهجمات السيبرانية وتعقيدها. فتشير شركة McAfee المتخصصة في مجال الأمن السيبراني إلى أن عام 2011 شهد أكبر عدد من التهديدات المكتشفة على الإطلاق. فيقال إن عدد البرمجيات الضارة المنتشرة في جميع أنحاء العالم بلغ 70 مليون برمجية مختلفة على الأقل، وأضحت الهواتف الذكية أداة لنشرها. كما يفيد المحللون أن الرسائل الاقتحامية تمثل 70% على الأقل من رسائل البريد الإلكتروني.

وفي الوقت ذاته، أصبحت شبكات الطاقة الذكية، ونظم الحوسبة السحابية، وشبكات الأتمتة الصناعية، ونظم النقل الذكية، والحكومة الإلكترونية، والصيرفة الإلكترونية – على سبيل المثال على أنواع البنية التحتية الجديدة لا الحصر – أكثر ترابطاً وتشابكاً. فأي فشل في إحداها يمكن أن يؤثر على غيرها. فمع زيادة الملاءمة والكفاءة تزداد شدة التعرض للهجمات السيبرانية.[1]

ومع ذلك، لم يُتوصل بعد إلى أي تعريف مقبول عالمياً للأمن السيبراني. ويؤدي ذلك إلى عرقلة جهود الحماية، التي ينبغي أن تجري على المستويين الوطني والدولي على السواء، نظراً لطبيعة الشبكات والنظم الحاسوبية التي لا تعترف بالحدود في عالم اليوم.

وعادة ما تُعامل الأحداث المتعلقة بتكنولوجيات المعلومات والاتصالات في إطار قوانين العقوبات الوطنية القائمة، التي غالباً ما لا يجري تحديثها أو مواءمتها مع الاتجاهات العالمية. وليس لدينا إلى الآن أي معيار دولي مشترك لتعريف الجرائم ذات الصلة؛ هل يجب أن تشمل مثلاً قرصنة البرمجيات ونشر المواد الإباحية للأطفال؟ هل تشمل الاحتيال المالي إلى جانب هجمات قطع الخدمة؟ قد تكون الإجابة هي مواءمة القوانين المحلية وإنشاء إطار قانوني يمكن على أساسه تحقيق التعاون الدولي. غير أن البعض يرى أن هذا الأمر ليس ضرورياً، أو ينبغي إجراؤه على المستوى الإقليمي فحسب.

[1] انظر أيضاً مذكرة المعلومات الأساسية للمؤتمر العالمي للاتصالات الدولية حول حماية البنية التحتية الوطنية الأساسية.

ولا تعتبر القوانين هي التحرك الوحيد – أو الأسرع – لمواجهة الهجمات السيبرانية. فمن الممكن تكميل الحلول التقنية بمعايير تسهم في تحقيق قابلية التشغيل البيني والتطابق مع التدابير الأمنية. ولهذا الأمر أهمية بالغة نظراً لاعتماد الشبكات على بعضها البعض في عالم اليوم. وقد نشر قطاع تقييس الاتصالات في الاتحاد الدولي للاتصالات نحو 300 معيار يتعلق بالأمن السيبراني. ويوفر الاتحاد المساعدة إلى البلدان النامية في هذه المجال أيضاً، كما يقدم الدعم لإنشاء أفرقة استجابة للحوادث الحاسوبية (CIRT). ويتضمن البرنامج العالمي للأمن السيبراني[2] للاتحاد بنوداً حول تعزيز التعاون الدولي.

ويندرج هذا العمل ضمن مهمة الاتحاد المتمثلة في قيادة تنسيق الجهود الدولية الرامية إلى "بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات" – وهي المهمة التي أسندها إليه قادة العالم خلال القمة العالمية لمجتمع المعلومات في 2003 و2005.

[2] انظر www.itu.int/osg/cybersecurity/gca/.