الأمم المتحدة

A/67/167*

الجمعية العامة

Distr.: General
23 July 2012
Arabic
Original: English/Russian/Spanish

الدورة السابعة والستون

البند ٩٠ من جدول الأعمال المؤقت**

التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي

التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي

تقرير الأمين العام

المحتويات

* أعيد إصدارها لأسباب فنية في ٨ نيسان/أبريل ٢٠١٣.

** A/67/150.

140812 130812 12-43412 (A)

أولاً – مقدمة

١ – دعت الجمعية العامة، في الفقرة ٣ من قرارها ٦٦/٢٤، جميع الدول الأعضاء إلى أن تواصل، آخذة في اعتبارها التقييمات والتوصيات الواردة في تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي (A/65/201)، موافاة الأمين العام بآرائها وتقييماتها بشأن المسائل التالية:

(أ) التقييم العام لمسائل أمن المعلومات؛

(ب) الجهود المبذولة على الصعيد الوطني لتعزيز أمن المعلومات وتشجيع التعاون الدولي في ذلك الميدان؛

(ج) مضمون المفاهيم المذكورة في الفقرة ٢ من القرار؛

(د) التدابير التي يمكن أن يتخذها المجتمع الدولي لتعزيز أمن المعلومات على الصعيد العالمي.

٢ – واستجابة لذلك الطلب، أُرسلت في ١٦ شباط/فبراير ٢٠١٢ مذكرة شفوية إلى الدول الأعضاء تدعوها إلى تقديم معلومات عن الموضوع. وترد في الفرع الثاني أدناه الردود التي تم تلقيها. وأي ردود أخرى يتم تلقيها ستصدر في شكل إضافات لهذا التقرير.

ثانيا – الردود الواردة من الحكومات

كولومبيا

[الأصل: بالإسبانية]
[٢١ أيار/مايو ٢٠١٢]

من المؤكد أن استخدام تكنولوجيا المعلومات والاتصالات أدى إلى حدوث تغييرات كبيرة في بلداننا وجلب منافع هامة لها. ومع ذلك، فإن هذه التطورات التكنولوجية زادت أيضا في استخدام التكنولوجيا للأغراض الإجرامية في مختلف أنحاء العالم، وهو ما يبرز الحاجة إلى اعتماد تدابير وضوابط عاجلة يمكنها أن تحمي الدولة من هذه التهديدات الجديدة.

ومن الشواغل المشتركة لجميع البلدان، زيادة القدرة على الإجرام في الفضاء الإلكتروني واستخدام التكنولوجيات الجديدة لتوليد تهديدات للحواسيب بالنظر إلى أن لهما أثرا كبيرا على أمن المعلومات، في المجالين العام والخاص على السواء، بما في ذلك المجتمع المدني، مما يبرز الحاجة إلى تنفيذ البروتوكولات والسياسات الأمنية الضرورية تنفيذا صارما

من أجل وضع ضوابط يمكنها أن تحمي الدولة وهياكلها الأساسية الحيوية من هذه التهديدات الجديدة.

وفي هذا السياق، وضعت كولومبيا في عام ٢٠٠٥ المعيار ٢٧٠٠١ للمنظمة الدولية لتوحيد المقاييس/اللجنة الكهربائية التقنية الدولية (ISO/IEC 27001)، كنظام إدارة يغطي السياسات والهيكل التنظيمي، والإجراءات، والعمليات، والموارد اللازمة لتنفيذ إدارة أمن المعلومات. والهدف من ذلك هو تطبيق معايير الجودة مثل مدونة أفضل الممارسات وأهداف الرقابة الواردة في المعيار ١٧٧٩٩ للمنظمة الدولية لتوحيد المقاييس/اللجنة الكهربائية التقنية الدولية (ISO/IEC 17799)، الذي يركز على حماية خصائص السرية والسلامة والتوافر، كما هو موضح أدناه:

- السرية: منع استخدام المعلومات من قِبل جهات غير مرخص لها من أفراد أو عمليات.
- السلامة: حماية دقة وكمال أي شيء ذي قيمة بالنسبة لمنظمة معينة.
- التوافر: كفالة وصول الكيانات المرخص لها إلى المعلومات وإمكانية استخدامها لها.

وتتجلى فوائد المعيار ٢٧٠٠١ للمنظمة الدولية لتوحيد المقاييس/اللجنة الكهربائية التقنية الدولية (ISO/IEC 27001) في ما يلي:

(أ) وضع منهجية واضحة ومحكمة التنظيم لإدارة أمن المعلومات؛

(ب) الحد من خطر تعرض المعلومات للضياع أو السرقة؛

(ج) وصول المستخدمين الآمن إلى المعلومات؛

(د) الاستعراض المستمر للمخاطر التي تهدد المعلومات والضوابط الأمنية ذات الصلة؛

(هـ) القدرة على القيام بعمليات فحص خارجية وداخلية دقيقة من شأنها تحديد نقاط الضعف المحتملة في نظم أمن المعلومات؛

(و) ضمان الامتثال للتشريعات والأنظمة الموجودة المتعلقة بإدارة المعلومات؛

(ز) زيادة وعي الناس بمسائل أمن المعلومات.

وسعيا لتعزيز الأطر القانونية والتشغيلية لأمن المعلومات، سن كونغرس جمهورية كولومبيا في ٥ كانون الثاني/يناير ٢٠٠٩ القانون رقم ١٢٧٣ الذي عدل القانون الجنائي، واستحدث مصلحة جديدة محمية قانونيا، هي حماية المعلومات والبيانات، وكفل الحماية الشاملة للنظم التي تستخدم تكنولوجيات المعلومات والاتصالات، إلى جانب تضمنه أحكاما أخرى.

وينقسم هذا القانون المهم إلى فصلين يتعلقان بـ ''الهجمات على سرية وسلامة وتوافر البيانات والنظم الحاسوبية'' و ''جرائم الهجمات على الحواسيب وغيرها من الجرائم''.

وينص الفصل الأول على ما يلي:

- الدخول غير المشروع إلى نظام حاسوب: يعاقب بالسجن لمدة تتراوح بين ثمانية وأربعين (٤٨) وستة وتسعين (٩٦) شهرا وغرامة مالية تتراوح بين ١٠٠ و ٠٠٠ ١ مرة الأجر الشهري القانوني الأدنى الساري. كل شخص يدخل دخولا تاما أو جزئيا، بدون ترخيص أو تجاوزا للترخيص الممنوح، إلى نظام حاسوبي محمي أو غير محمي بإجراء أمني، أو يظل داخل النظام المذكور ضد رغبة أي شخص له الحق المشروع في أن يمنع ذلك.
- التعطيل غير المشروع لعمل النظم الحاسوبية أو لشبكات الاتصالات السلكية واللاسلكية: يعاقب بالسجن لمدة تتراوح بين ثمانية وأربعين (٤٨) وستة وتسعين (٩٦) شهرا وغرامة مالية تتراوح بين ١٠٠ و ٠٠٠ ١ مرة الأجر الشهري القانوني الأدنى الساري، كل شخص يمنع أو يعيق، بدون ترخيص، الاشتغال أو الوصول العادي لنظام حاسوبي أو لبيانات حاسوبية موجودة فيه أو لشبكة اتصالات سلكية أو لاسلكية، ما لم يكن الفعل جرما موجبا لعقوبة أشد.
- اعتراض بيانات الحاسوب: يعاقب بالسجن لمدة تتراوح بين ستة وثلاثين (٣٦) واثنين وسبعين (٧٢) شهرا كل شخص يقوم، بدون أمر قضائي مسبق، باعتراض بيانات حاسوبية في نقطة المنشأ أو عند المقصد أو داخل نظام حاسوبي، أو باعتراض الانبعاثات الكهرومغناطيسية من نظام حاسوب يرسلها.
- إلحاق ضرر بحاسوب: يعاقب بالسجن لمدة تتراوح بين ثمانية وأربعين (٤٨) وستة وتسعين (٩٦) شهرا وغرامة مالية تتراوح بين ١٠٠ و ٠٠٠ ١ مرة الأجر الشهري القانوني الأدنى الساري كل شخص يقوم بدون ترخيص بتدمير بيانات حاسوبية أو نظام لتجهيز البيانات، أو أجزائه أو عناصره المنطقية، أو بإلحاق ضرر بها، أو محوها، أو إفسادها، أو تغييرها أو محوها.

- استخدام البرامجيات الخبيثة: يعاقب بالسجن لمدة تتراوح بين ثمانية وأربعين (٤٨) وستة وتسعين (٩٦) شهرا وغرامة مالية تتراوح بين ١٠٠ و ٠٠٠ ١ مرة الأجر الشهري القانوني الأدنى الساري كل شخص يقوم بدون ترخيص بإنتاج برامجيات خبيثة أو برامج حاسوبية ضارة أخرى أو الاتجار بها، أو اقتنائها، أو توزيعها، أو بيعها، أو إرسالها، أو جلبها إلى البلاد أو إخراجها منها.

- انتهاك البيانات الشخصية: كل يعاقب بالسجن لمدة تتراوح بين ثمانية وأربعين (٤٨) وستة وتسعين (٩٦) شهرا وغرامة مالية تتراوح بين ١٠٠ و ٠٠٠ ١ مرة الأجر الشهري القانوني الأدنى الساري كل شخص يحصل بدون ترخيص، سواء لمصلحته الخاصة أو لمصلحة طرف ثالث، على شفرات شخصية أو بيانات شخصية واردة في ملفات أو محفوظات أو قواعد بيانات أو وسائط مماثلة، أو يقوم بجمعها، أو استخراجها، أو عرضها، أو بيعها، أو تبادلها، أو إرسالها أو شرائها، أو اعتراضها، أو كشفها، أو تغييرها أو استخدامها.

- تزوير المواقع من أجل التقاط البيانات الشخصية: يعاقب بالسجن لمدة تتراوح بين ثمانية وأربعين (٤٨) وستة وتسعين (٩٦) شهرا وغرامة مالية تتراوح بين ١٠٠ و ٠٠٠ ١ مرة الأجر الشهري القانوني الأدنى الساري كل شخص يقوم، بنية الإجرام وبدون ترخيص محدد، بتصميم برامج، أو تطويرها، أو الاتجار بها، أو بيعها، أو تشغيلها، أو إرسال صفحات شبكية، أو روابط إلكترونية، أو نوافذ منبثقة، ما لم يكن الفعل جرما موجبا لعقوبة أشد.

وينص الفصل الثاني على ما يلي:

- السرقة باستخدام الحواسيب أو الوسائل المماثلة: يتعرض للعقوبات المنصوص عليها في المادة ٢٤٠ من القانون الجنائي، وهي أحكام بالسجن تتراوح بين ثلاث (٣) وثماني (٨) سنوات كل شخص يقوم، بعد تجاوز الإجراءات الأمنية للحاسوب، بالأفعال المبينة في المادة ٢٣٩ الخاصة بالتلاعب بنظام حاسوبي، أو شبكة إلكترونية أو شبكة لبث المعلومات عن بُعد أو ما شابهها أو ينتحل صفة مستخدم بالنسبة لنظم التحقق من الهوية والترخيص القائمة.

- تحويل أصول دون موافقة: يعاقب بالسجن لمدة تتراوح بين ثمانية وأربعين (٤٨) ومائة وعشرين (١٢٠) شهرا وغرامة مالية تتراوح بين ٢٠٠ و ٥٠٠ ١ مرة الأجر الشهري القانوني الأدنى الساري كل شخص يقوم، من أجل الربح وباستخدام حاسوب أو جهاز مماثل، بتحويل، بدون موافقة، لأي أصل على حساب طرف

ثالث، ما لم يكن الفعل جرما موجبا لعقوبة أشد. وتطبق نفس العقوبة على كل من يبرمج أو ينزل أو يمتلك أو يقدم برامجيات لغرض ارتكاب الجريمة المذكورة أعلاه، أو الاحتيال.

وكان القانون رقم ١٢٧٣ لعام ٢٠٠٩، بدون شك، خطوة هامة جدا إلى الأمام في مكافحة الجرائم المرتبطة بالحاسوب في كولومبيا؛ ومع ذلك، فإن نشأة أنواع وأنماط مختلفة من الجريمة المنظمة، والجرائم الإلكترونية على وجه الخصوص، اضطرت كولومبيا لتنفيذ استراتيجية شاملة لمحاربة الجرائم الإلكترونية مع التركيز على الدفاع عن الفضاء الإلكتروني وأمن الفضاء الإلكتروني، مما جعل العمل المشترك بين الوكالات أهم عامل في تحقيق الأهداف المتوخاة من مفهوم أمن المعلومات.

وفي هذا الإطار، استهلت الحكومة الكولومبية، في تموز/يوليه ٢٠١١، سياستها الوطنية للدفاع عن الفضاء الإلكتروني وأمن الفضاء الإلكتروني المبنية على ثلاث ركائز أساسية:

- اعتماد إطار مناسب مشترك بين المؤسسات للوقاية والتنسيق والرصد وصياغة التوصيات للتصدي لأي تهديدات ومخاطر تنشأ.
- توفير التدريب المتخصص في أمن المعلومات وتوسيع خطوط التحقيق الخاصة بالدفاع عن الفضاء الإلكتروني وأمن الفضاء الإلكتروني.
- تعزيز التشريع الخاص بتلك المسائل والتعاون الدولي، وتسريع انضمام كولومبيا إلى العديد من الصكوك الدولية.

ومن أجل تنفيذ المبادئ الاستراتيجية المذكورة أعلاه بشكل شامل، صممت كولومبيا وأنشأت أربع سلطات:

(أ) الأولى هي اللجنة المشتركة بين القطاعات، المسؤولة عن رسم الرؤية الاستراتيجية لإدارة المعلومات ووضع مبادئ توجيهية لسياسات إدارة الهياكل الأساسية العامة لتكنولوجيا المعلومات وأمن الفضاء الإلكتروني والدفاع عن الفضاء الإلكتروني؛

(ب) الثانية هي الفريق الكولومبي للتصدي للطوارئ الحاسوبية، وهي وكالة التنسيق الوطنية المعنية بمسائل أمن الفضاء الإلكتروني والدفاع عن الفضاء الإلكتروني؛

(ج) الثالثة هي القيادة المشتركة للفضاء الإلكتروني التابعة للقوات المسلحة، المكلفة بمنع ومكافحة أي تهديد أو هجوم إلكتروني يؤثر على القيم والمصالح الوطنية؛

(د) وأخيرا، تم إنشاء مركز الشرطة المعنية بالجرائم الإلكترونية؛ وهو مسؤول عن أمن الفضاء الإلكتروني في كولومبيا، وتوفير المعلومات والدعم والحماية من الجرائم الإلكترونية.

وسوف تمكّن هذه المؤسسات كولومبيا من تنفيذ ولايات السياسة الوطنية للدفاع عن الفضاء الإلكتروني وأمن الفضاء الإلكتروني وتطويرها والتصدي على نحو شامل وفعال لهذا النوع الجديد من الجرائم المتنامي بشكل كبير في جميع أنحاء العالم.

ولم تقم كولومبيا بوضع السياسة العامة للدفاع عن الفضاء الإلكتروني وأمن الفضاء الإلكتروني فحسب؛ بل اتخذت أيضا عددا من المبادرات القطاعية المهمة لصياغة سياسات فعالة في مجال أمن المعلومات. وترد تفاصيل أهم هذه المبادرات أدناه:

المبادرة	الوكالة الرائدة	النطاق
نموذج أمن المعلومات لاستراتيجية الحكومة الإلكترونية	برنامج الحكومة الإلكترونية – وزارة تكنولوجيا المعلومات والاتصالات	يشير هذا النموذج الأمني إلى مجموعة السياسات الاستراتيجية التي تشكل الأساس لأهداف الحكومة الإلكترونية، مثل ''حماية المعلومات الشخصية'' و ''مصداقية برنامج الحكومة الإلكترونية والثقة فيه''. ويحدد العوامل التالية باعتبارها عناصر أساسية لأمن المعلومات بالنسبة للوكالات الحكومية: (أ) توافر المعلومات والخدمات؛ (ب) سلامة المعلومات والبيانات؛ (ج) سرية المعلومات.
توصيات مقدمة إلى الحكومة لتنفيذ استراتيجية وطنية الأمن الفضاء الإلكتروني	لجنة تنظيم الاتصالات السلكية واللاسلكية	في هذه الوثيقة، تقدم لجنة تنظيم الاتصالات توصيات إلى الحكومة بشأن استراتيجية وطنية لأمن الفضاء الإلكتروني وتقترح أدوات مناسبة للتعاون والتعامل بين الحكومة وجميع مستويات القطاع الخاص؛ وتحدد طرق ردع الجرائم الإلكترونية؛ وتوصي بوضع وتنفيذ أطر قانونية تتعلق بالأمن الحاسوبي تتسق مع المعايير الدولية؛ وتقدم توصيات من أجل استحداث نظم لمعالجة الحوادث الأمنية على الشبكة، بما في ذلك رصد تلك الحوادث وتحليلها والتصدي لها؛ وتقترح مبادئ توجيهية لإعمال ثقافة وطنية خاصة بأمن الفضاء الإلكتروني من أجل تحسين مستويات حماية الهياكل الأساسية الحيوية للمعلومات في كولومبيا.
مركز تنسيق أمن الحواسيب الكولومبي الخاص بمقدمي خدمات الإنترنت	الرابطة الكولومبية لتكنولوجيا المعلومات والاتصالات السلكية واللاسلكية	مركز تنسيق أمن الحواسيب الكولومبي على اتصال مباشر مع مراكز أمن الشركات المنتسبة إليه (أكبر مقدمي خدمات الإنترنت في كولومبيا). وهو قادر على تنسيق معالجة وتسوية الطلبات والبلاغات المتعلقة بمشاكل أمن الحواسيب.

وفضلا عن القدرات الوطنية في مجال أمن المعلومات، من المهم الإشارة إلى سلسلة تدابير ينبغي، من وجهة نظر كولومبيا، أن تتخذ على المستوى الدولي لتعزيز أمن المعلومات:

- تعزيز قنوات الاتصال بين الدول الأعضاء في الأمم المتحدة من أجل تنسيق الجهود في المكافحة عبر الوطنية للجرائم التي تؤثر على المعلومات والبيانات.

- صياغة صكوك دولية وإقليمية تركز على التعريف القانوني للأفعال المعاقَب عليها التي تهدد أمن الفضاء الإلكتروني والدفاع عن الفضاء الإلكتروني في كل دولة.
- صياغة وتدوين بروتوكولات للتصدي لحوادث الحواسيب، مما يؤدي إلى وضع سياسات عالمية خاصة بأمن المعلومات.
- تعزيز الأنشطة الوقائية والتشريعية في ما يتعلق بالفئات الناشطة في قرصنة الحواسيب، وخاصة في الجامعات والكليات، من أجل الحد من انخراط الشباب في هذه التنظيمات التي تهدد التطور العادي للهياكل الأساسية الرقمية للدول.
- توحيد التشريعات مع التركيز على الوقاية والمساعدة ومتابعة الأنشطة المتعلقة بأمن المعلومات.
- تعزيز وتنفيذ التكنولوجيا، مع التركيز على اعتماد أفضل الممارسات في مجال إدارة أمن المعلومات. ومن المهم الإشارة هنا إلى ضرورة وضع خطط للاستثمار في التكنولوجيا المتطورة، إلى جانب توفير الدعم الحكومي لمشاريع التنمية التكنولوجية.
- توفير الفرص من أجل تبادل المعلومات والمعارف في ما يتعلق بالمعايير العالمية الخاصة بهذه المسألة.

تشريعات جمهورية كولومبيا في مجال أمن المعلومات

القانون/القرار	الموضوع
القانون رقم ٥٢٧ (١٩٩٩) (التجارة الإلكترونية)	يحدد وينظم الوصول إلى رسائل البيانات والتجارة الإلكترونية والتوقيعات الرقمية واستخدامها، وينشئ سلطات التصديق ويتضمن أحكاما أخرى.
القانون رقم ٥٩٩ (٢٠٠٠)	يصدر بموجبه القانون الجنائي، الذي يبقي على تجريم ''الانتهاك غير القانوني للاتصالات''، ويؤكد قانونية حقوق التأليف والنشر ويشمل بعض الأفعال المرتبطة بشكل غير مباشر بالجريمة الحاسوبية، مثل عرض أو بيع أو شراء أجهزة قادرة على اعتراض الاتصالات الخاصة بين الأشخاص. ويعرف الدخول غير المشروع إلى نظام حاسوبي (المادة ١٩٥)، ويقضي بتغريم كل من يدخل على نحو غير مشروع إلى نظام حاسوبي محمي بتدابير أمنية أو يظل داخل النظام المذكور ضد رغبة أي شخص له الحق الشرعي في منعه.
القانون رقم ٩٦٢ (٢٠٠٥)	يسن أحكاما لتبسيط الإجراءات الإدارية لوكالات الدولة وكياناتها وللأفراد الذين يؤدون وظائف عامة أو يقدمون الخدمات العامة. وينص على حافز من أجل استخدام التكنولوجيا المتكاملة للحد من مدد الانتظار وتكاليف الإجراءات الإدارية.
القانون رقم ١١٥٠ (٢٠٠٧)	يقدم تدابير لتعزيز كفاءة وشفافية القانون رقم ٨٠ (١٩٩٣) ويسن أحكاما عامة أخرى متعلقة بالمشتريات العامة. ويحدد على وجه الخصوص إمكانية قيام الإدارة العامة بإصدار القرارات والوثائق الإدارية وبإرسال الإخطارات إلكترونيا، ولذلك فهو يتوخى استحداث نظام إلكتروني للمشتريات العامة.

القانون/القرار	الموضوع
القانون رقم ١٢٧٣ (٢٠٠٩)	يعدل القانون الجنائي، ويستحدث مصلحة جديدة محمية قانونيا، هي ''حماية المعلومات والبيانات''، ويضمن الحماية الشاملة للنظم التي تستخدم تكنولوجيا المعلومات والاتصالات، إلى جانب أحكام أخرى.
القانون رقم ١٣٤١ (٢٠٠٩)	يحدد مبادئ ومفاهيم مجتمع المعلومات وإطار تكنولوجيا المعلومات والاتصالات، وينشئ الوكالة الوطنية للاتصالات اللاسلكية، ويحتوي على أحكام أخرى.
القرار رقم ٢٢٥٨ (٢٠٠٩) للجنة تنظيم الاتصالات	يتعلق بأمن الشبكة لمقدمي الخدمات الشبكية وخدمات الاتصالات السلكية واللاسلكية. ويعدل هذا القرار المادتين ٢٢ و ٢٣ من القرار رقم ١٧٣٢ (٢٠٠٧) للجنة تنظيم الاتصالات والمادتين ١-٨ و ٢-٤ من قرارها رقم ١٧٤٠ (٢٠٠٧). ويضع هذا النظام الشرط القاضي بأن على مقدمي الخدمات الشبكية و/أو خدمات الاتصالات السلكية واللاسلكية الذين يتيحون الوصول إلى شبكة الإنترنت أن يستخدموا نماذج أمنية، وفقا للخصائص والاحتياجات المحددة لشبكتهم، تساعد على تحسين أمن الدخول إلى شبكاتهم، وذلك تمشيا مع الأطر الأمنية التي حددها الاتحاد الدولي للاتصالات، متقيدين بمبادئ سرية البيانات، وسلامة البيانات وتوافر عناصر الشبكة، والمعلومات، والخدمات، والتطبيقات، وكذلك تدابير التحقق من الهوية، والدخول، وعدم التنصل. ويحدد أيضا المتطلبات الواجب توافرها في مقدمي الخدمات الشبكية وخدمات الاتصالات السلكية واللاسلكية في ما يتعلق بحرمة الاتصالات وأمن المعلومات.
التعميم رقم ٠٥٢ (٢٠٠٧) (هيئة الإشراف المالي بكولومبيا)	يحدد المتطلبات الدنيا للأمن والجودة لمعالجة المعلومات عبر وسائل الإعلام وقنوات توزيع المنتجات والخدمات للعملاء والمستخدمين.

كوبا

[الأصل: بالإسبانية]
[٢١ أيار/مايو ٢٠١٢]

إن الاستخدام العدائي للاتصالات السلكية واللاسلكية الذي يرمي سراً أو علانية إلى تقويض النظام القانوني والسياسي للدول، يشكل انتهاكا للقواعد الدولية المعترف بها في هذا المجال، من شأنه أن يؤدي إلى نشوء توترات وأوضاع غير مؤاتية للسلام والأمن الدوليين.

وتشاطر كوبا تماما القلق الذي أعرب عنه قرار الجمعية العامة ٦٦/٢٤ بخصوص استخدام تكنولوجيات المعلومات ووسائلها في أغراض لا تتفق مع تحقيق الاستقرار والأمن الدوليين وتؤثر سلبا على السلامة الإقليمية للدول، مما يقوِّض أمنها في المجالين المدني والعسكري. ويشدد هذا القرار أيضا بصورة ملائمة على ضرورة منع استخدام موارد المعلومات وتكنولوجياتها في أغراض إجرامية أو إرهابية.

وفي هذا الصدد، تكرر كوبا إدانتها لما تقوم به الإدارات المتعاقبة للولايات المتحدة من تصعيد عدواني لحربها الإذاعية والتليفزيونية ضد كوبا مما ينتهك المعايير الدولية السارية التي تحكم المجال اللاسلكي. ويشن هذا العدوان دون مراعاة الأضرار التي قد تلحق بالسلام والأمن الدوليين من جراء خلق أوضاع خطيرة، من قبيل استخدام طائرة عسكرية لبث إشارات تليفزيونية باتجاه كوبا دون موافقتها.

وخلال عام ٢٠١١، سُجِّل ما متوسطه ٢ ١٩٣ ساعة من ساعات الإرسال غير المشروع ضد كوبا، التي بُثَّت على ٣٠ ترددا من الولايات المتحدة كل أسبوع. والعديد من محطات البث هذه مملوك لمنظمات ترتبط بعناصر إرهابية معروفة تعيش في كوبا وتعمل ضدها انطلاقا من أراضي الولايات المتحدة، أو تقدِّم خدمات لتلك المنظمات، وهي تبث برامج تحرض فيها على التخريب، والقيام بهجمات سياسية واغتيالات، وغير ذلك من أشكال الإرهاب الإذاعي.

ويشكِّل بث هذه البرامج الاستفزازية ضد كوبا انتهاكا للمبادئ الدولية التالية:

- المبادئ الأساسية للاتحاد الدولي للاتصالات، الواردة في ديباجة دستوره. ويتسم محتوى البرامج التليفزيونية التي تبثها حكومة الولايات المتحدة ضد كوبا بطابع تخريبي، ويرمي إلى زعزعة الاستقرار والتضليل ويتعارض مع تلك المبادئ.
- الحكمان CS 197 و CS 198 من دستور الاتحاد الدولي للاتصالات، اللذان ينصَّان على أن جميع المحطات، أيا كانت أهدافها، يجب إنشاؤها وتشغيلها فعليا بحيث لا تحدث تشويشا يضر بالخدمات اللاسلكية أو الاتصالات التابعة لدول أعضاء أخرى.
- الاتفاق الصادر عن الجلسة العامة التاسعة للمؤتمر العالمي للاتصالات السلكية المعقود في تشرين الثاني/نوفمبر ٢٠٠٧، الذي ينص في فقرته الفرعية (ز) من الفقرة ٦-١ على أنه ”لا يمكن اعتبار قيام محطة إذاعية تعمل على متن طائرة وتبث برامجها حصرا باتجاه إقليم إدارة أخرى دون موافقتها عملا يتماشى مع أنظمة الاتصالات اللاسلكية“.
- الفقرة الفرعية ٣ من المادة ٨ من أنظمة الاتصالات اللاسلكية للاتحاد، التي تنص على أنه يجب على الإدارات الأخرى أن تراعي عند تحديد تردداتها الخاصة الترددات المخصصة والمسجلة باعتراف دولي تلافيا لإحداث أي تشويش ضار.
- الفقرة الفرعية ٤ من المادة ٤٢ من أنظمة الاتصالات اللاسلكية، التي تحظر تشغيل خدمات للبث الإذاعي على متن طائرات تعمل في البحر أو فوق البحر.

- قرار مجلس أنظمة الاتصالات اللاسلكية الذي أقر في اجتماعه الخامس والثلاثين المعقود في كانون الأول/ديسمبر ٢٠٠٤، بوقوع تشويش ضار للخدمات الكوبية من جراء البث على موجة التردد ٢١٣ ميغاهرتز، وطالب إدارة الولايات المتحدة باتخاذ التدابير المناسبة لوقفه. وعلاوة على ذلك، ما برح مجلس أنظمة الاتصالات اللاسلكية منذ أيلول/سبتمبر ٢٠٠٦ يطلب من حكومة الولايات المتحدة اتخاذ تدابير ترمي إلى إزالة التشويش على موجة التردد ٥٠٩ ميغاهرتز، دون أن يتلقى أي رد حتى الآن. وأكد المجلس مجددا، في موجز قرارات اجتماعه الخمسين الذي اختتم في ٢٠ آذار/مارس ٢٠٠٩ (الوثيقة RRBO9-1/5)، عدم مشروعية البث وطالب حكومة الولايات المتحدة باتخاذ كل التدابير اللازمة من أجل وضع حد لهاتين الحالتين من التشويش على الخدمات التليفزيونية في كوبا.

- الفقرة الفرعية ٣ من المادة ٢٣ من أنظمة الاتصالات اللاسلكية، التي تقيِّد الإرسال التليفزيوني خارج الحدود الوطنية. وأقر تقرير أصدره في كانون الثاني/يناير ٢٠٠٩ مكتب المحاسبة العام التابع لحكومة الولايات المتحدة الأمريكية، وهو وكالة حكومية رسمية، بأن برنامج الإرسال الإذاعي والتليفزيوني لحكومة الولايات المتحدة الموجه ضد كوبا يشكل انتهاكا للقواعد الدولية وللقانون المحلي.

واعتمد المؤتمر العالمي للاتصالات اللاسلكية، الذي انعقد في جنيف عام ٢٠٠٧، استنتاجات خلصت إلى أنّ عمليات البث الموجهة من طائرات في الولايات المتحدة باتجاه كوبا تنتهك أنظمة الاتصالات اللاسلكية. ونصَّت الاستنتاجات المعتمدة في الجلسة العامة على أنه ”لا يمكن اعتبار قيام محطة إذاعية تعمل على متن طائرة وتبث برامجها حصراً باتجاه إقليم إدارة أخرى دون موافقتها عملا يتماشى مع أنظمة الاتصالات اللاسلكية“.

ولهذه الاستنتاجات قوة القانون بالنسبة لعمل الاتحاد الدولي للاتصالات. وبذلك يكون المؤتمر العالمي للاتصالات اللاسلكية قد أيد القرار الصادر في عام ١٩٩٠ عن المجلس الدولي السابق لتسجيل الترددات، والذي ينص على أن توجيه البث التليفزيوني من على متن منطاد مبرمج من بُعد باتجاه الإقليم الوطني الكوبي يشكِّل انتهاكا للأنظمة.

واعتمد مجلس النظم الإذاعية التابع للاتحاد الدولي للاتصالات في اجتماعه الرابع والخمسين المعقود في تموز/يوليه ٢٠١٠، القرار التالي:

بعد دراسة دقيقة لتقرير المدير وبيان مقدم من كوبا (الوثيقة RRB10-2/3 (Add.1))، لاحظ المجلس مع الأسف استمرار التشويش على

محطات البث في كوبا بسبب البث من الولايات المتحدة، وقرر الإبقاء على قراراته السابقة بالنسبة لهذه المسألة.

وأشار المجلس أيضا إلى الطلب المقدم إلى ”المكتب، بوصفه أمينا تنفيذيا للمجلس“ بإثارة موضوع التشويش الضار على محطات البث VHF/UHF المملوكة لكوبا في مؤتمر المفوضين المقبل. وأقر بالحق السيادي لكل حكومة في إثارة أي مسألة في مؤتمر المفوضين، وأكد أن ممثلي مجلس النظم الإذاعية الاثنين في مؤتمر المفوضين لعام ٢٠١٠، وأمينه التنفيذي سيكونون على استعداد لتقديم أي معلومات مناسبة، وإسداء المشورة اللازمة في مؤتمر المفوضين المقبل.

وفي الآونة الأخيرة، أسند المؤتمر العالمي للاتصالات اللاسلكية، في شباط/فبراير ٢٠١٢، إلى مدير مكتب الاتصالات اللاسلكية التابع للاتحاد الدولي للاتصالات ولاية لمتابعة هذه المسألة وتقديم تقرير إلى المؤتمر المقبل، المقرر عقده في عام ٢٠١٥، عن التشويش الذي تسببه الولايات المتحدة في الخدمات الإذاعية بسبب أفعالها العدوانية اللاسلكية.

وهكذا أكد المؤتمر صلاحية الاستنتاج المعتمد في اجتماعه السابق، الذي أقر بعدم شرعية البث الإذاعي والتليفزيوني الموجه من الولايات المتحدة إلى كوبا على متن الطائرات.

ويتجلى العداء الذي تناصبه حكومة الولايات المتحدة الأمريكية لكوبا في الحظر الاقتصادي والتجاري والمالي الذي تفرضه عليها منذ أكثر من خمسين عاما والذي يؤثر أيضا على مجال المعلومات والاتصالات السلكية واللاسلكية:

- تضرر قطاع تكنولوجيات الاتصالات والمعلومات بشدة من الحظر، فقد حُسبت الخسائر في الفترة بين عامي ٢٠١٠ و ٢٠١١ بمقدار ٣٩٤ ٣٩٦ ٧ من دولارات الولايات المتحدة.
- لا يمكن لكوبا الاستفادة من الخدمات التي يقدمها عدد كبير من المواقع الشبكية، بحيث ينطبق منع دخولها بمجرد أن يتبين أن الاتصال يجري من عنوان على شبكة الإنترنت مخصص لنطاق كوبي ينتهي بالحرفين (cu).
- باستخفاف ونفاق كاملين، لا تزال الولايات المتحدة تتهم كوبا زورا بمنع مواطنيها من الدخول إلى الشبكة العالمية، بينما الواقع مختلف جدا وهو أن كوبا لا يمكنها الاتصال بواسطة كابلات الألياف الضوئية التي تحيط بالأرخبيل الكوبي، بسبب قوانين الحظر الذي تفرضه عليها الولايات المتحدة، مما يضطرها إلى تسديد تكاليف الخدمات الساتلية الباهظة.

- في ٦ تشرين الأول/أكتوبر ٢٠١٠، أقرت شبكة تويتر للتواصل الاجتماعي بمسؤوليتها الكاملة عن منع توجيه رسائل من كوبا عبر الهواتف المحمولة إلى قاعدتها. وبالمثل، أقرت في نيسان/أبريل ٢٠١١ بأنه يجري تقييد إمكانية الاستفادة من بعض أدوات الشبكة في كوبا بدعوى أن الدخول يتم من بلد خاضع للحظر.
- وابتداء من شباط/فبراير ٢٠١١، أوقفت الشركة المالية Synivere تسديد المدفوعات إلى شركة الاتصالات الكوبية ETECSA لتغطية تكاليف خدمة ''التجوال'' المقدمة في الهواتف المحمولة، بدعوى أن المصرف الذي تتعامل معه لا يستطيع القيام بمعاملات مع كوبا، وأدى ذلك إلى عدم تحصيل مبلغ ٢,٦ مليون دولار، وغير ذلك من الصعوبات.

والمناقشة التي تجري في الجمعية العامة بشأن التطورات في ميدان تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي هي مناقشة في محلها وذات أهمية كبيرة. وتؤكد الإجراءات من قبيل تلك المشار إليها أعلاه التي تتخذها حكومة الولايات المتحدة ضد كوبا ضرورة إجراء هذه المناقشة والحاجة الملحَّة إلى اتخاذ تدابير لوضع حد لهذه الإجراءات.

وأيدت كوبا قرار الجمعية العامة ٦٦/٢٤ وستواصل الإسهام في التطوير السلمي لتكنولوجيات المعلومات والاتصالات في العالم واستخدامها لما فيه خير البشرية جمعاء.

بنما

[الأصل: بالإسبانية]
[١٠ تموز/يوليه ٢٠١٢]

أضحت اقتصادات القرن الحادي والعشرين تعتمد اعتمادا متزايداً على قطاع الخدمات، ويتجلى ذلك بشكل خاص في اقتصادات العالم المتقدم. والتجارة الإلكترونية هي أحدث أشكال هذا القطاع الاقتصادي، فهي تيسر المعاملات التجارية وتتيح إيصال السلع والخدمات إلى جميع أنحاء العالم بتكاليف أقل ووقت أقصر. أما الحكومة الإلكترونية فهي مرادف التجارة الإلكترونية الذي تعتمده الدول والذي يتيح لها تلبية قسط كبير من احتياجات المواطنين بسرعة وكفاءة عن طريق مختلف التكنولوجيات (الشبكية والمحمولة).

ونظراً لانتشار استخدام تكنولوجيا المعلومات والاتصالات في التجارة والحكومة الإلكترونيتين، لا بد من بذل الجهود لضمان تلبية هذه التكنولوجيات الحد الأدنى من احتياجات عملاء الدولة والمواطنين إلى سرية المعلومات وسلامتها وتوافرها. غير

أن الكثير من الجهود المبذولة حاليا يركز على تقديم حلول تقنية لمشاكل ذات طابع عام، مما يستوجب التصدي للمشكلة من زوايا مختلفة.

ونحن نعتقد أن على الدول الراغبة في تعزيز التجارة والحكومة الإلكترونيتين أن تضطلع بمهمة أولى هي وضع أُطر قانونية تستند إلى المعايير الدولية التي سبق أن اعتمدتها الدول الأخرى والتي تحظى بقبول واسع، وأن تهيئ في الوقت ذاته بيئة غير مؤاتية للمجرمين والإرهابيين الذين يستخدمون هذه الموارد في أنشطتهم. والبلدان التي تعتمد تدابير حمائية قانونية وتقنية بمقدورها هي وحدها التي تجني ثماراً اقتصادية نتيجة إيجادها بيئة مؤاتية للتجارة والحكومة الإلكترونيتين.

وفي الوقت ذاته، ينبغي الاستمرار في بذل الجهود لتطوير التكنولوجيات ووضع السياسات التي تدافع عن فضاء الدول الإلكتروني حيث تتلاقى مصالح بلدان مختلفة، وذلك من خلال وضع استراتيجيات وطنية في مجال أمن الفضاء الإلكتروني يمكن تنفيذها ضمن أُطر زمنية واقعية ومحددة بوضوح. وهذه الاستراتيجيات، فضلا عن إسهامها في إحلال السلام العالمي، ينبغي توجيهها لصون استقرار البلدان وأمنها القومي.

وقد اتخذت بنما التدابير التالية على المستوى الوطني لتعزيز أمن المعلومات والإسهام في التعاون الدولي:

(أ) إنشاء الفريق المعني بالتصدي لحوادث الأمن الحاسوبي بموجب الأمر التنفيذي رقم ٧٠٩ المؤرخ ٢٦ أيلول/سبتمبر ٢٠١١؛

(ب) تعديل القانون الموضوعي (القانون الجنائي) لإدراج أفعال إجرامية جديدة تتعلق بجرائم الفضاء الإلكتروني وتقديمه فيما بعد إلى الجمعية الوطنية لتعتمده (القانون رقم ٣٣٧)؛

(ج) مناقشة قانون الإجراءات الجنائية وتعديله بغية تضمينه الأفعال الإجرامية الجديدة التي أُدرجت في القانون الجنائي؛

(د) إنشاء فريق عامل يُعنى بمناقشة مسؤولية مقدمي خدمات الإنترنت عن أمن المعلومات وترأسه الهيئة الوطنية للتجديد الحكومي والهيئة الوطنية للخدمات العامة. كما تناقش هيئات التنظيم الوطنية في منطقة أمريكا الوسطى تنفيذ نتائج المداولات التي يجريها الفريق على المستوى الإقليمي (اللجنة التقنية للاتصالات في أمريكا الوسطى/الاتحاد الدولي للاتصالات)؛

(هـ) إنشاء فريق عامل يُعنى بالتعامل مع الأدلة الرقمية ويرأسه مكتب المدعي العام بالاشتراك مع الهيئة الوطنية للتجديد الحكومي؛

(و) إرسال طلب رسمي للحصول على المساعدة التقنية من منظمة الدول الأمريكية فيما يتعلق بوضع استراتيجية البلدان الأمريكية في مجال أمن الفضاء الإلكتروني؛

(ز) قيام مركز التنسيق التابع لمنظمة الدول الأمريكية/فريق التصدي للطوارئ الحاسوبية، بتيسير دورة تدريبية عن كيفية التعامل مع الحوادث، وقد أُجريت الدورة في بنما في نيسان/أبريل؛

(ح) تقييم الاقتراح المقدم من مكتب الأمم المتحدة المعني بالمخدرات والجريمة والمتعلق بوضع برنامج لبناء قدرة بنما على مكافحة الجريمة الإلكترونية؛

(ط) المشاركة بانتظام في اجتماعات وزراء العدل أو غيرهم من الوزراء، أو المدعين العامين في الأمريكتين وفي اجتماعات لجنة البلدان الأمريكية لمناهضة الإرهاب التابعة لمنظمة الدول الأمريكية؛

(ي) تقديم طلب رسمي للانضمام إلى اتفاقية الجرائم الإلكترونية، وذلك بمقتضى المذكرة الشفوية المؤرخة ٣١ كانون الثاني/يناير ٢٠١٢ الموجهة من وزارة الخارجية إلى كارلوس أروسينيما، سفير بنما في بروكسل.

وفيما يتعلق بالتدابير التي يمكن أن يتخذها المجتمع الدولي تعزيزاً لأمن المعلومات على الصعيد العالمي، نرى أنه ينبغي النظر في التوصيات التالية:

(أ) اعتماد إطار قانوني مشترك من شأنه أن يتيح للدول التعاون فيما بينها عن طريق تبادل المساعدة القانونية السريعة استنادا إلى إجراءات متفق عليها دوليا؛

(ب) وضع استراتيجيات وطنية وإقليمية في مجال أمن الفضاء الإلكتروني؛

(ج) تشجيع التبادل المنتظم للمعلومات فيما بين الدول عن طريق الأفرقة الوطنية المعنية بالتصدي للحوادث بغية تيسير تدفق المعلومات، ولا سيما المعلومات المتعلقة بمحاكمة المجرمين والإرهابيين؛

(د) وضع برامج للتوعية العامة باللوائح المحلية والدولية السارية في كل دولة.

قطر

[الأصل: بالإنكليزية]
[١٨ أيار/مايو ٢٠١٢]

تقوم الجهود الوطنية التي تبذلها دولة قطر في ميدان أمن المعلومات على اتّباع نهج شامل يراعي أمن الأصول المعلوماتية وأمن الأفراد الذين يستخدمونها. وتتفق هذه الاستراتيجية مع رؤية قطر الوطنية لعام ٢٠٣٠ التي تشدد على التنمية البشرية والاجتماعية والاقتصادية باعتبارها ركيزة أساسية، والتي تقودها مبادرات دولية من قبيل جدول أعمال أمن الفضاء الإلكتروني العالمي الذي وضعه الاتحاد الدولي للاتصالات ومبادئ حماية الهياكل الأساسية الحيوية للمعلومات التي وضعتها مجموعة الثمانية.

وفريق مواجهة الطوارئ الحاسوبية التابع للبرنامج الوطني لأمن الفضاء الإلكتروني في قطر (فريق مواجهة الطوارئ الحاسوبية هو إحدى مبادرات مركز التدريب العالي لأمن المعلومات)، وهو مؤسسة تمولها الحكومة تحت رعاية المجلس الأعلى للاتصالات وتكنولوجيا المعلومات، يشكل في الوقت الراهن حجر زاوية أساسيا في برنامج عمل قطر في مجال أمن الفضاء الإلكتروني، الذي يشمل فرعين يُعنى أحدهما بحماية الهياكل الأساسية الحيوية للمعلومات والآخر بضمان تأدية الكيانات الحكومية المعنية بتكنولوجيا المعلومات والاتصالات لرسالتها.

ويعمل الفريق القطري لمواجهة الطوارئ الحاسوبية مع الهيئات الحكومية ومنظمات القطاعين العام والخاص والمواطنين القطريين لضمان رصد التهديدات والأخطار الإلكترونية واحتوائها. وتشمل الممارسات الراسخة التي يتبعها الفريق لتحديد مصدر التهديدات الإلكترونية أحدث ما توصل إليه العلم من وسائل رقمية للتحقيق العدلي وتحليل البرامجيات الخبيثة، وقدرات نظام رصد التهديدات الإلكترونية، بالإضافة إلى قنوات لتحسين الجاهزية والاستجابة الأمنيتين من خلال تنظيم برامج تدريبية على سيناريوهات من هذا القبيل. وفيما يلي وصف موجز لمهام الفريق:

جمع معلومات أمنية عن التهديدات الإلكترونية

مركز العمليات الأمنية – يستخدم المحللون الأمنيون أدوات مطوّرة داخليا (نُظم رصد التهديدات) لإنذار الهيئات الحكومية والمؤسسات الحيوية بشكل استباقي بشأن التهديدات الإلكترونية ويزودونها بأدوات القضاء على تلك التهديدات.

نظام رصد التهديدات – هذا النظام هو أداة مطورة داخليا تجمع المعلومات الأمنية المتعلقة بالتهديدات الإلكترونية والواردة من عدد من المصادر، وتحللها لكشف الأثر الذي تحدثه الحواسيب أو المواقع الإلكترونية المصابة بفيروسات والتخفيف من حدته.

مختبر تحليل البرامجيات الخبيثة

يهدف المعمل إلى بناء القدرة الوطنية على قياس تهديدات البرامجيات الخبيثة وتحليلها وتوفير الحماية منها. وفي الوقت الراهن، يصدر المعمل تقريرا مفصلا عن تأثير البرامجيات الخبيثة على الآلات المصابة؛ ونوع النظام المستهدف؛ ومصدر البرامجيات الضارة الموجودة في البلد؛ وأي عملية اتصال يجريها الحاسوب المصاب بالحاسوب المركزي. ويساعد المختبر أيضا على قياس مدى أهمية كل فيروس بغرض تقييم الخطر المرتبط به والتهديد الذي يطرحه حسب حجمه، ويتعقب كافة البرامج الضارة باستخدام ما هو متاح في الأسواق من آلات مضادة للفيروسات.

التعامل مع الحوادث التي يتعرض لها القطاع العام

يهدف الفريق القَطَري لمواجهة الطوارئ الحاسوبية إلى تقليص عدد الآلات المصابة في دولة قطر إلى أدنى حد عن طريق توفير الدعم الأساسي إلى القطاعين العام والحيوي. ومن أجل بلوغ هذا الهدف وتوفير التوجيه الصحيح، وسّعت قطر نطاق خدمات مواجهة الحوادث بحيث تغطي مستخدمي خطوط الاشتراك الرقمية غير المتماثلة عن طريق إنشاء بوابة إلكترونية للتعامل مع الحوادث التي يتعرض لها القطاع العام. وتوفر البوابة خطوات متنوعة وتوجيهات وأدوات برامجية أساسية تتيح فحص الفيروس والقضاء عليه باستخدام الآلات المترلية المربوطة بخطوط الاشتراك الرقمية غير المتماثلة.

التدريب في مجال أمن الفضاء الإلكتروني

ينظم الفريق القَطَري لمواجهة الطوارئ الحاسوبية دورات تدريبية وحلقات عمل في مجال أمن الفضاء الإلكتروني لفائدة العاملين في مجال تكنولوجيا المعلومات من المؤسسات الحكومية والدول الأعضاء الأخرى في مجلس التعاون لدول الخليج العربية.

التوعية بأمن الفضاء الإلكتروني

يرسي الفريق القَطَري أساساً للمعارف البشرية بالقضايا التي تمس أمن الفضاء الإلكتروني وأفضل الممارسات فيه، مع التركيز على موظفي الشركات الكبرى.

ويعمل الفريق على حماية الهياكل الأساسية الحيوية نظراً إلى أن عددا من القطاعات الصناعية، مثل المالية والطاقة، وتكنولوجيا المعلومات والاتصالات، له أهمية حيوية في المحافظة على اقتصاد قطر وشعبها وحكومتها. ومن ثم، فهو يرمي إلى حماية نظم المعلومات التي تقوم عليها تلك القطاعات الحيوية، وذلك على النحو التالي:

- وضع استراتيجيات وطنية للحماية، وتحديد أفضل الممارسات والأُطر والأدوات، وتوعية أصحاب المصلحة
- تقديم المساعدة المباشرة لمالكي الهياكل الأساسية للمعلومات الحيوية ومشغليها في تحسين وسائل حماية شبكات الإشراف على البيانات والحصول عليها
- فهم قضايا القطاع الصناعي والقطاعات التابعة له وتنفيذ استراتيجيات حماية خاصة بكل قطاع
- العمل مع المؤسسات الدولية المعنية بحماية الهياكل المعلوماتية الأساسية بغية التوصل إلى حلول عبر وطنية
- قياس نُضج المؤسسات المعنية بحماية الهياكل الأساسية المعلوماتية في البلد وتقييم ما تحرزه من تقدم.

وعلاوة على ذلك، يواصل برنامج أمن الفضاء الإلكتروني التابع للمجلس الأعلى للاتصالات وتكنولوجيا المعلومات العمل مع الهيئة التشريعية على سن قوانين ووضع معايير تكفل التحسين المستمر للضمانات الوطنية في التصدي للتهديدات الناشئة المعاصرة.

ويوصي المجلس الأعلى المجتمع الدولي بوضع واعتماد التدابير الممكنة التالية:

- القيام، في غضون خمس سنوات، بإنشاء أُطر قانونية دولية متسقة على الصعيد الإقليمي في جميع البلدان
- القيام، في غضون ثلاث سنوات، بتشكيل أفرقة تعنى بمواجهة الحوادث الحاسوبية في كافة البلدان التي ليس لديها في الوقت الراهن أفرقة من هذا القبيل
- القيام، في غضون خمس سنوات، بوضع استراتيجيات وطنية في مجال أمن الفضاء الإلكتروني تكون متوائمة مع مبادئ التعاون الدولي، وتشمل حماية الهياكل الأساسية الحيوية للمعلومات
- وضع مناهج دراسية تتعلق بأمن الفضاء الإلكتروني وترمي إلى بناء قدرات مختلف الفئات المعنية وتوعيتها، كالحكومات والأوساط الأكاديمية والقطاع الخاص والمدارس

- التشديد على أهمية إتاحة برامج لتوعية الأطفال والشباب في مجال السلامة على شبكة الإنترنت.

تركيا

[الأصل: بالإنكليزية]
[٣١ أيار/مايو ٢٠١٢]

تتوغل تكنولوجيات المعلومات والاتصالات بشكل سريع في الحياة اليومية والعمليات التجارية على حد سواء. وتخزن بيانات مختلفة ذات أهمية حيوية للأفراد والمؤسسات والحكومات بشكل رقمي في الفضاء الإلكتروني وترسل من خلاله. وعلى الرغم من الفوائد التي تقدمها التكنولوجيا، فهي تنطوي على بعض المخاطر، من حيث عدم قدرتها على الحفاظ على سرية وسلامة البيانات المخزنة رقمياً، وعلى توافر نظم المعلومات. إن الثغرات في نظم المعلومات والاتصالات – التي تنشأ عن خلل في التصميم، والتشكيل والتشغيل، وعن عدم كفاية القدرات التقنية ونقص التدريب أو الوعي بمسائل الأمن لدى الموظفين والمستخدمين – توفر بيئة مناسبة لظهور هذه المخاطر.

ومن أجل تجنب المخاطر أو التخفيف من حدتها ولمعالجة الثغرات، تتزايد على الصعيدين الوطني والمؤسسي أهمية الجهود المبذولة لتطوير أمن الفضاء الإلكتروني. وفي هذا الصدد، يعتبر بناء القدرات التقنية والإدارية، وزيادة الوعي بمسائل الأمن لدى الموظفين التنفيذيين، والعاملين والمستخدمين في المؤسسات العامة والخاصة جزءاً أساسياً من هذه الجهود.

وقد ترسخ الوعي لدى المسؤولين التنفيذيين في المستويات العليا من الحكومة التركية بضرورة تعزيز أمن المعلومات الوطنية. وبالإضافة إلى ذلك، فإن هيئة المعلومات والاتصالات في تركيا تركز بشكل خاص على أبحاث للتوصل إلى أفضل الممارسات وللتعرف على التهديدات الناشئة في الفضاء الإلكتروني، وعلى تنظيم وتنفيذ تدريبات وطنية في مجال أمن الفضاء الإلكتروني، وتعزيز القدرات المؤسسية والتقنية في مجال التصدي لحالات الطوارئ وإجراء مراجعات منتظمة لمشغلي الاتصالات الإلكترونية من أجل ضمان العمل بالسياسات والعمليات والبرامج والضوابط الملائمة لمعالجة حوادث أمن الاتصالات الإلكترونية بشكل سليم.

ويُعترف بأهمية بحث المفاهيم الدولية المتعلقة بالتهديدات العالمية، وبحث الثغرات الخاصة لنظم المعلومات، وأفضل الممارسات من حيث آليات تبادل المعارف المتخصصة مع المنظمات الدولية الأخرى، وذلك من أجل تعزيز أمن النظم العالمية للمعلومات والاتصالات السلكية واللاسلكية.

ومن الممكن أن تثبت أهمية الاتفاقيات المتعددة الأطراف التي تتناول التعاون في مجال حوادث أمن المعلومات والاتصالات في الفضاء الإلكتروني، ونهج الأدلة العدلية المستخدم فيها، وكذلك تبادل المعلومات عن قواعد بيانات البرامجيات الخبيثة، باعتبارها أدوات مفيدة في تعزيز أمن المعلومات على الصعيد العالمي.

أوكرانيا

[الأصل: بالروسية]
[٣١ أيار/مايو ٢٠١٢]

تقييم عام لمسائل أمن المعلومات

أدى الإدخال السريع لتكنولوجيات المعلومات والاتصالات في جميع مجالات الحياة وعولمة وصلات المعلومات إلى تحول الأنشطة غير المشروعة في جميع أنحاء العالم إلى الفضاء الإلكتروني. وأصبحت الجرائم الحاسوبية، المسماة أيضاً جرائم الفضاء الإلكتروني، والتي لا تعرف الحدود الدولية، لا تشكل فقط تهديداً لحقوق الأفراد وحرياتهم، بل تهدد أيضاً المصالح الوطنية للدول وأمنها.

وشهدت السنوات الأخيرة ازدياداً ملحوظاً في الهجمات الحاسوبية على الهياكل الأساسية الوطنية الحيوية، وتضر هذه الهجمات بالدول بتشويهها للمعلومات الهامة وبتعطيلها عمليات الإنتاج في المصانع وتوريد الخدمات العامة والطاقة وشبكات المواصلات.

وأجري في عام ٢٠١١ تقييم لجرائم الفضاء الإلكتروني في دول معينة تعرضت فيها نظم المعلومات في هيئات ووكالات حكومية لهجمات قراصنة الحاسوب مما عرقل أنشطتها، وكشف التقييم أن الهجمات الإلكترونية تشكل تهديدا كبيرا على المجتمع، وأنه لا يمكن التنبؤ بعواقبها.

الجهود المبذولة على الصعيد الوطني لتعزيز أمن المعلومات وتشجيع التعاون الدولي في هذا الميدان

لقد تصدت بعض البلدان المتقدمة لهذه التهديدات بإنشاء نظم وطنية لمكافحة جرائم الفضاء الإلكتروني تترأسها هيئة تنسيق وحيدة. ويمكّن هذا النهج من تضافر القوى والموارد على نحو فعال بين الكيانات الحكومية وغير الحكومية ذات الصلة، وذلك لمواجهة وإبطال المخاطر التي تتهدد أمن الفضاء الإلكتروني.

وكان هذا أحد الاعتبارات الرئيسية التي روعيت في استعراض النهج المتبعة إزاء تقييم التهديدات والتحديات الجديدة، بما فيها التي تهم مجال أمن المعلومات، وتنظيم مناسبات رفيعة المستوى للدول بشأن إقامة نظام وحيد على الصعيد الوطني لمكافحة جرائم الفضاء الإلكتروني، ووضع مشروع قانون بشأن أمن الفضاء الإلكتروني، وإقامة وتعزيز التعاون مع أجهزة المخابرات ووكالات إنفاذ القانون الأجنبية.

وفي حزيران/يونيه ٢٠١١، أوقفت إدارة الأمن في أوكرانيا الأنشطة الإجرامية لمجموعة من قراصنة الحاسوب وذلك بالتعاون مع وكالات من ١١ دولة (ألمانيا، ورومانيا، والسويد، وفرنسا، وقبرص، وكندا، ولاتفيا، وليتوانيا، والمملكة المتحدة، وهولندا، والولايات المتحدة الأمريكية). وقد استخدمت تلك المجموعة برامجيات خبيثة نشرتها عبر شبكة الإنترنت لسرقة أكثر من ٧٢ مليون دولار من مؤسسات مصرفية أجنبية.

وفي تشرين الأول/أكتوبر ٢٠١١، نظمت إدارة الأمن في أوكرانيا الجولة السنوية من محادثات خبراء أوكرانيا ومنظمة حلف شمال الأطلسي المتعلقة بالدفاع عن الفضاء الإلكتروني، التي عقدت في يالطا، بأوكرانيا. وأكدت نتيجة المحادثات من جديد موقف أوكرانيا من ضرورة زيادة تطوير نظام أمن المعلومات بمشاركة القطاعين العام والخاص، وباستخدام الدروس المستفادة من الدول الأخرى.

وبمبادرة من إدارة الأمن، ستناقش مسألة إنشاء لجنة على حدة معنية بأمن الفضاء الإلكتروني في الاجتماع الثاني والثلاثين لرؤساء وكالات الخدمات الخاصة والأمن وهيئات إنفاذ القانون في رابطة الدول المستقلة.

مضمون المفاهيم المذكورة في الفقرة ٢ (قرار الجمعية العامة ٦٦/٢٤)

تُعرَّف في التشريعات الأوكرانية التهديدات الرئيسية التالية للأمن القومي، بما في ذلك أمن المعلومات:

- تقييد حرية المواطنين في التعبير والحصول على المعلومات.

- جرائم الفضاء الإلكتروني والإرهاب الإلكتروني.
- إفشاء أسرار الدولة أو أي معلومات سرية أخرى يحميها القانون، أو إفشاء معلومات سرية تمتلكها الدولة أو تستخدم لتلبية الاحتياجات الوطنية ولتحقيق مصالح المجتمع والدولة.
- محاولات التلاعب بانطباعات الجماهير، بوسائل منها نشر المعلومات المضللة أو الناقصة أو المتحيزة.

التدابير التي يمكن أن يتخذها المجتمع الدولي لتعزيز أمن المعلومات على الصعيد العالمي

الطريقة الرئيسية التي تمكِّن المجتمع الدولي من تعزيز أمن المعلومات هي إيجاد بيئة مواتية تسمح لكل دولة بضمان أمن المعلومات الخاص بها وتطوير تعاون فعال في هذا الصدد.

ولوضع آليات تتصدى بفعالية للتهديدات القائمة والمحتملة لأمن المعلومات، ينبغي للمجتمع الدولي اتخاذ التدابير التالية:

- الأخذ بآليات استشارية للتعاون في مجال الدفاع عن الفضاء الإلكتروني، وذلك لتسهيل تبادل الخبرات في ما يتعلق بصياغة التشريعات واللوائح في هذا المجال.
- إنشاء نظم لتبادل المعلومات بشأن رصد الفضاء الإلكتروني وللإخطار المبكر بالهجمات الإلكترونية وتبادل المعلومات عن جوانبها التقنية، وتتبع مصادر الهجمات والتدابير المضادة الفعالة.
- التعاون في معالجة الآثار الضارة الناجمة عن الهجمات الإلكترونية، وتبادل الدروس المستفادة، واستحداث حلول تكنولوجية وصياغة توصيات تنظيمية بشأن ردع الهجمات الإلكترونية.
- وضع صكوك قانونية دولية تحدد مصطلحات وقواعد موحدة، مثل مدونة لقواعد السلوك على شبكة الإنترنت.

ونظراً لضرورة التصدي لهذه التهديدات، ينبغي للشركاء من أجهزة المخابرات ووكالات إنفاذ القانون العمل بشكل مشترك في المجالات التالية:

- وضع آليات من أجل التبادل السريع بين أجهزة المخابرات للمعلومات المتعلقة بأنشطة الجماعات الإجرامية المنظمة، بما في ذلك الجماعات الإرهابية التي تهدف إلى

التدخل غير المأذون به في موارد معلومات الهياكل الأساسية الوطنية لشبكة الإنترنت أو نظم معلومات المكاتب أو المؤسسات الحكومية.

- تبادل المعلومات عن الجرائم المتعلقة بالدخول غير المأذون به إلى النظم الحاسوبية للمؤسسات المالية، بما في ذلك دخولها بغرض تزوير بطاقات مصرفية، أو التدخل غير المأذون به في أداء النظم الحاسوبية المصرفية بغرض سرقة معلومات سرية أو إعاقة العمليات.

- التعاون أثناء العمليات لتعقب الأشخاص الذين يرتكبون جرائم الفضاء الإلكتروني باستخدام الهياكل الأساسية الوطنية لشبكة الإنترنت وتوثيق أنشطتهم غير المشروعة.

- تبادل الخبرات والممارسات السائدة حالياً في مجال فحص البرامجيات والمعدات الحاسوبية (الأدلة العدلية في جرائم الفضاء الإلكتروني)، عند التحقيق في الجرائم المرتكبة باستخدام تكنولوجيا الحاسوب، وتبادل أساليب وتقنيات فحص تجهيزات الحواسيب من أجل توثيق الأنشطة الإجرامية.

- وضع برامج تدريب مشتركة للعاملين في أجهزة المخابرات وبرامج للتدريب الداخلي لخبرائها.

- حضور الندوات والحلقات الدراسية والمؤتمرات المشتركة المتعلقة بمكافحة جرائم الفضاء الإلكتروني.

ويمكن أن يتمثل أحد أشكال التعاون في وضع نظام لرصد موارد الهياكل الأساسية الوطنية لشبكة الإنترنت من أجل ضمان الكشف المبكر عن التهديدات، ونظام لتحديد أفضل الأدوات التي يتعين استخدامها لإبطال تلك التهديدات.

وقد يكون إنشاء مراكز استجابة وطنية للحوادث الحاسوبية وإقامة تعاون وثيق في ما بينها إحدى الآليات الممكنة لتنسيق أنشطة أمن الفضاء الإلكتروني التي تقوم بها هيئات الدولة وشركات الاتصالات السلكية واللاسلكية والجهات الفاعلة الأخرى المعنية بالهياكل الأساسية الوطنية لتكنولوجيا المعلومات والاتصالات، والرامية إلى منع الاستخدام غير المشروع للحواسيب وتكنولوجيا المعلومات.

ويمكن أن تشمل المهام الرئيسية لهذه المراكز الوطنية ما يلي:

- استقاء المعلومات عن التهديدات الحالية لأمن الفضاء الإلكتروني وتحليلها وتجميعها في قواعد البيانات ذات الصلة.

- رصد وكشف الآليات والموارد الموجودة على شبكة الإنترنت، التي تتعارض عملياتها مع اللوائح التي تنظم استخدام الهياكل الأساسية الوطنية لشبكة الإنترنت.
- وضع توصيات لمستخدمي شبكة الإنترنت بهدف حماية مصالح الأفراد والمجتمع والدولة في مجال المعلومات وتوصيات بشأن تقديم الخدمات الاستشارية والدعم التقني للمستخدمين.
- تلقي التقارير العاجلة عن هجمات قراصنة الحاسوب، وتقديم المساعدة العاجلة لوقفها والقيام على الفور بإخطار مستخدمي شبكة الإنترنت ونظم المعلومات الأخرى (بما في ذلك النظم المحلية ونظم الشركات) بالمخاطر التي تتهدد أمن الفضاء الإلكتروني.
- التعاون وتبادل المعلومات مع المراكز المماثلة في البلدان الأخرى.