الأمم المتحدة

A/65/154

الجمعية العامة

Distr.: General
20 July 2010
Arabic
Original: English/Russian/Spanish

الدورة الخامسة والستون

البند ٩٤ 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

* A/65/150.

160810 120810 10-45840 (A)

أولا – مقدمة

١ – دعت الجمعية العامة في الفقرة ٣ من قرارها ٢٥/٦٤ جميع الدول الأعضاء إلى مواصلة موافاة الأمين العام بآرائها وتقييماتها بشأن المسائل التالية:

(أ) التقدير العام لمسائل أمن المعلومات؛

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

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

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

٢ – وعملا بذلك الطلب، أُرسلت مذكرة شفوية في ٢٧ شباط/فبراير ٢٠٠٩ إلى الدول الأعضاء تدعوها إلى تقديم معلومات عن هذا الموضوع. ويحتوي الفرع الثاني أدناه على الردود التي وردت. وستصدر أي ردود إضافية في شكل إضافات لهذا التقرير.

ثانيا – الردود الواردة من الحكومات

أوكرانيا

[الأصل: بالروسية]
[١٢ أيار/مايو ٢٠١٠]

التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي

١ – يتحدد الاهتمام بمشاكل أمن المعلومات بدور المعلومات المتزايد باطراد في المجالات المختلفة للأنشطة الحيوية للمجتمع. ومع إدخال تكنولوجيا المعلومات المتطورة في أنشطة الحياة اليومية للحكومة والمجتمع، يزداد احتمال حدوث مخاطر معلوماتية على نظم المعلومات والاتصالات السلكية واللاسلكية وموارد المعلومات المملوكة للهيئات الحكومية والمؤسسات التجارية من جانب العناصر الإجرامية والأفراد الذين يسعون إلى ارتكاب أفعال منافية للقانون.

٢ – ويُعزى نصف الجرائم الحاسوبية المسجلة في العالم إلى الحصول غير المأذون به على المعلومات الحاسوبية. وتتزايد معدلات الجريمة الحاسوبية ذات الدوافع المغرضة وتتزايد معها

الأضرار المادية التي تسببها. ويشهد الوقت الراهن ارتفاعا في معدلات الجريمة المرتكبة على يد الجماعات عبر الوطنية من قراصنة الحاسوب.

٣ - وتتسم الجريمة الحاسوبية بدرجة عالية من السرية، بحيث لا يصبح في الإمكان رسم صورة متكاملة لما ينتج عنها من انتهاكات قانونية، نظرا إلى أن كلا من الهيئات الحكومية والمؤسسات التجارية التي تتعرض لجرائم حاسوبية تسعى بكل السبل للتستر علي مثل هذه الحقائق ولا تميل إلى الكشف عن الأضرار التي تلحق بها وعن ضعف نظم حماية المعلومات لديها، تخوفا من فقدان سمعتها. ونتيجة لما ذُكر، فإن حدوث مثل هذه الأعمال الإجرامية لا يصل إلى العلن إلا لاما، مما يدل على أهمية وضع تدابير مشتركة ذات طبيعة وقائية وتحذيرية، بحيث ينبغي أن تُشكِّل تلك التدابير الأساس لنظام حماية المعلومات.

٤ - وفي العادة، فإن الجريمة الحاسوبية ما هي إلا مجرد خطوة أولى في سلسلة أعمال إجرامية تقود إلى أشكال أخرى من الأعمال الإجرامية التقليدية - مثل الاختلاس والابتزاز والغش وما إلى ذلك. ومع مرور كل يوم، تصبح الأعمال الإجرامية أكثر تطورا وحذقا وسرية وتترتب عليها أضرار اقتصادية وسياسية جسيمة في جميع بلدان العالم تقريبا. علاوة على ذلك، فإن معظم الخبراء يرون أن هناك صلة مباشرة بين السيادة المعلوماتية للدولة وبين مسائل الأمن الوطني.

٥ - وتظهر، أثناء مكافحة الجرائم التي تُرتكب في مجال تكنولوجيا المعلومات، مسائل عديدة ذات طابع قانوني، نظرا إلى أن الأدلة الحاسوبية تكون غير مادية وسريعة الزوال في كثير من الأحيان. كما أن صعوبة حل المشاكل التي تتميز بها الجريمة الحاسوبية تجعل التعاون على الصعيد الدولي أمراً ذا أهمية خاصة، مما يحتم على جميع البلدان في نهاية المطاف أن تمتلك موارد قانونية وإجرائية ومعيارية مناسبة ومتوافقة مع بعضها البعض.

٦ - وتقود الممارسة العملية للتحقيق في الجرائم الحاسوبية إلى معرفة أن تنسيق التعاون بين هيئات إنفاذ القانون التابعة لمختلف الدول هو أمر ضروري.

٧ - وهناك ممارسة عالمية تتمثل في تنفيذ تدابير مشتركة عند إجراء التحقيقات في الجرائم الحاسوبية. ويُشارك جهاز الأمن الأوكراني مشاركة فعالة في العمليات المشتركة لهيئات إنفاذ القانون والأجهزة الأمنية الخاصة بالعالم، التي تُنَفَّذ في إطار مكافحة استغلال الأطفال في المواد الإباحية، وأعمال الغش التي تُنفّذ عن طريق شبكة الإنترنت، والإرهاب الدولي.

٨ - وعلاوة على ذلك يتعين توحيد الجهود من أجل مواصلة تعزيز التعاون في مجال كفالة أمن المعلومات وخدمة المصالح المشتركة وتنفيذ تدابير لحمايتها، ويُفضّل أن يكون ذلك على أساس الاتفاقات الثنائية والمتعددة الأطراف. وفي رأينا، فإن النجاح في حل

مشاكل أمن المعلومات لن يتحقق إلا إذا تعاونت الهيئات الحكومية التابعة لمختلف الدول تعاونا فعالا، لا سيما وأن القاعدة القانونية اللازمة لذلك التعاون موجودة بالفعل.

٩ - وإذ يدرك جهاز الأمن الوطني الأوكراني ضرورة مجابهة مخاطر الجريمة الحاسوبية والإرهاب الحاسوبي، فقد أقام علاقات مع هيئات إنفاذ القانون والأجهزة الأمنية الخاصة بالدول الأجنبية.

١٠ - وتجدر الإشارة إلى أن الجرائم الحاسوبية تستهدف في أحيان كثيرة شبكات الحاسوب التابعة للهيئات الحكومية، ويتوقف النجاح في تتبع ومعاقبة مرتكبي هذه الجرائم على نوعية العلاقات القائمة على الصعيد الدولي، وكذلك على مدى استكمال القوانين الوطنية وفقا للظروف الراهنة.

١١ - وإذا ما وضعنا في الاعتبار النمو المطرد للجرائم الحاسوبية على نطاق العالم، ووجود روابط بين الجماعات الإجرامية من قراصنة الحاسوب بالبلدان المختلفة، وعدم ارتباط مخاطر الجرائم الحاسوبية بالحدود الدولية للبلدان، فإن التعاون الدولي في مجال مكافحة الجريمة الحاسوبية يتوسع بصفة مستمرة.

١٢ - ولأغراض تنفيذ القرارات الصادرة عن مؤتمر القمة العالمي لمجتمع المعلومات (المرحلة الأولى - جنيف، ١٠-١٢ كانون الأول/ديسمبر ٢٠٠٣؛ والمرحلة الثانية، تونس، ١٦-١٨ تشرين الثاني/نوفمبر ٢٠٠٥)، اعتمد في أوكرانيا قانون بشأن ''المبادئ الأساسية لتطوير مجتمع المعلومات في أوكرانيا للفترة ٢٠٠٧-٢٠١٥''، تتمثل أولوياته الأساسية في الاندماج في الفضاء المعلوماتي العالمي وتطوير مجتمع المعلومات. وينص هذا القانون على تحسين أمن المعلومات في ظروف استخدام أحدث ما تم التوصل إليه في مجال تكنولوجيا المعلومات والاتصالات.

١٣ - بالإضافة إلى ذلك، جرى إعداد واعتماد خطة لتطوير الاتصالات السلكية واللاسلكية في أوكرانيا، وهي خطة ترمي إلى تنفيذ تدابير تنظيمية - تقنية، تهدف إلى كفالة التشغيل الآمن لجميع عناصر البنية التحتية للاتصالات السلكية واللاسلكية في أوكرانيا، وعلى وجه التحديد:

- تأسيس قاعدة معيارية قانونية من أجل معالجة المسائل التقنية والمتعلقة بالتشفير في مجال حماية المعلومات، وتنفيذها بشكل تدريجي، وجعلها متسقة مع المعايير الأوروبية والدولية؛

- وضع طرائق حديثة لحماية المعلومات مبنية على الوسائل التقنية الخاصة بحل المشاكل المعقدة المتعلقة بتوفير الحماية للمعلومات في شبكات الاتصالات السلكية واللاسلكية؛
- إقامة نُظُم للاعتراض المشروع للمعلومات في شبكات الاتصالات السلكية واللاسلكية في الحالات المنصوص عليها في القوانين؛
- تأسيس مركز تنسيق حكومي معني بالمسائل الأمنية في شبكات المعلومات والاتصالات السلكية واللاسلكية ذات الاستخدامات العامة، والمساعدة في تأسيس مراكز حكومية وغير حكومية تتميز بالكفاءة والقدرة على التصدي للحوادث التي تشهدها شبكات الاتصالات السلكية واللاسلكية.

١٤ - وتتشكل القاعدة المعيارية القانونية لحماية المعلومات في أوكرانيا أيضا من القوانين الأوكرانية التالية: ''قانون المبادئ الأساسية للأمن الوطني لأوكرانيا''، و ''قانون المعلومات''، و ''قانون حماية المعلومات في نُظُم المعلومات والاتصالات السلكية واللاسلكية'' (يشار إليها فيما بعد، بالقوانين)، وأوامر رئيس جمهورية أوكرانيا ومجلس وزرائها بشأن ''حالة الحماية التقنية للمعلومات في أوكرانيا ''، و ''قواعد توفير حماية المعلومات لنُظُم الإعلام والاتصالات ونُظُم المعلومات والاتصالات السلكية واللاسلكية'' (يشار إليها فيما بعد بالقواعد)، و ''نظام الربط بالشبكات العالمية لبث البيانات''، وعدد آخر من النُظم، بالإضافة إلى مجموعة كبيرة من القوانين التشريعية المسجلة لدى وزارة العدل، والتي تحكم مسائل ربط نظم المعلومات بالشبكات العالمية، وإصدار التراخيص لبعض أنواع الأنشطة المحددة، ونظام تقييم المنتجات في مجال حماية المعلومات، وما إلى ذلك.

١٥ - وتنص الصكوك التشريعية القانونية على أنه يجب ألا تستخدم لأغراض توفير الحماية اللازمة للمعلومات سوى نُظُم تكنولوجيا المعلومات والاتصالات السلكية واللاسلكية ذات الحماية (يشار إليها فيما بعد بنُظُم تكنولوجيا المعلومات والاتصالات السلكية واللاسلكية ذات الحماية)، أي تلك التي تشتمل على نُظُم متكاملة لحماية المعلومات (يشار إليها فيما بعد بالنُظُم المتكاملة لحماية المعلومات)، مثل مجموعة واحدة من الإجراءات القانونية والتنظيمية، وكذلك الموارد من برامجيات ومعدات تقنية قادرة على مجابهة المخاطر. ويشترط هنا أن تشتمل النُظُم المتكاملة لحماية المعلومات، وكذلك مجموعة وسائل الحماية المستخدمة فيها، على ما يؤكد امتثالها للمتطلبات الواردة في صكوك المعايير في مجال حماية المعلومات.

١٦ - ولأغراض تحديد مواصفات النُظُم المتكاملة لحماية المعلومات وفرادى وسائل حماية المعلومات، جرى في أوكرانيا وضع وتنفيذ زهاء ٥٠ من صكوك المعايير ذات الطابع التقني،

التي تُحدد معايير تقييم القدرة على حماية المعلومات وتصنيف نُظُم تكنولوجيا المعلومات والاتصالات السلكية واللاسلكية ذات الحماية، ونظام تنفيذ العمل في مجال الحماية، والمتطلبات فيما يتصل بفرادى وسائل الحماية والنُظُم المتكاملة لحماية المعلومات، تبعاً لتصنيفات نُظُم تكنولوجيا المعلومات والاتصالات السلكية واللاسلكية ذات الحماية، والغرض من المعلومات المُعالجة، ومجال استخدامها، ونوعها.

١٧ - وأنشئ في أوكرانيا كذلك نظام وطني غير حكومي لمعايير تقييم القدرة على حماية تكنولوجيا المعلومات. ويستند هذا النظام إلى مجموعة متكاملة من صكوك المعايير المتعلقة بحماية المعلومات في نُظُم تكنولوجيا المعلومات والاتصالات السلكية واللاسلكية ذات الحماية ضد إمكانية الحصول عليها بصورة غير مأذون بها، وتتسق تلك الصكوك مع الصكوك المماثلة في بلدان الاتحاد الأوروبي ومع المعايير الدولية، وبخاصة المعيار ISO IEC 15408.

١٨ - وبالإضافة إلى ذلك، يجري في أوكرانيا، على المستوى الوطني، إنشاء نظام من التدابير التنظيمية - التقنية التي تهدف إلى مكافحة الأنشطة غير المأذون بها فيما يتصل بنظم المعلومات والاتصالات السلكية واللاسلكية التابعة للسلطات الحكومية، وهيئات إنفاذ القانون، والجمارك، والضرائب، والمؤسسات الائتمانية - المالية، وغيرها، ولا سيما محاولات التدخل في عملها باستخدام إمكانيات شبكة الإنترنت العالمية.

١٩ - ووفقا للقواعد الواردة في الفقرتين الفرعيتين ١٠ و ١١ من المادة ١٦ من القانون الأوكراني بشأن ''الدائرة الحكومية للاتصالات المتخصصة وحماية المعلومات بأوكرانيا''، وبهدف تحسين تنسيق أعمال الهيئات الحكومية المعنية بالكشف عن مخاطر المعلومات في نُظُم الإعلام والاتصالات ونُظُم المعلومات والاتصالات السلكية واللاسلكية، فضلا عن إزالة الآثار الناجمة عن تنفيذ تلك المخاطر، وتحقيق التعاون الدولي في هذه المسائل، قامت الدائرة الحكومية للاتصالات المتخصصة وحماية المعلومات بأوكرانيا بإنشاء وتشغيل القسم المناسب لذلك، وهو فريق الاستجابة للطوارئ الحاسوبية في أوكرانيا (CERT-UA).

٢٠ - وامتثالاً للتوجهات العالمية لتطوير شبكات هياكل الاستجابة السريعة، فإن فريق الاستجابة للطوارئ الحاسوبية يمثل فريقا للتصدي لحالات الطوارئ الحاسوبية. ويجري تنسيق أنشطة مثل هذه الهياكل على الصعيد الدولي من خلال المنظمة الدولية المسماة 'منتدى أفرقة التصدي للحوادث التي تهدد الأمن' (FIRST).

٢١ - وبتاريخ ١٣ تموز/يوليه ٢٠٠٩، حصل القسم المختص بالدائرة الحكومية للاتصالات المتخصصة وحماية المعلومات بأوكرانيا، وهو فريق الاستجابة للطوارئ الحاسوبية

في أوكرانيا (CERT-UA) (www.cert.gov.ua)، على وضع العضوية الكاملة بمنتدى أفرقة التصدي للحوادث التي تهدد الأمن.

٢٢ - وفي إطار قيامه بأنشطته لعام ٢٠٠٩، تلقى فريق الاستجابة للطوارئ الحاسوبية في أوكرانيا (CERT-UA) ٤٦١ بلاغا من أفرقة الاستجابة للطوارئ الحاسوبية (CERT-OB) في ٣٠ بلدا من بلدان العالم هي (الاتحاد الروسي، وإسبانيا، وأستراليا، وإستونيا، وإسرائيل، وألمانيا، وإيطاليا، وباكستان، والبرتغال، وبلجيكا، وبولندا، وتايوان، وتركيا، وجمهورية كوريا، والدانمرك، ورومانيا، والصين، وفرنسا، وفنلندا، وكندا، وليتوانيا، وماليزيا، والمملكة العربية السعودية، والنرويج، والنمسا، والهند، وهنغاريا، وهولندا، والولايات المتحدة الأمريكية، واليابان) بشأن أنشطة غير مأذون بها بقطاع أوكرانيا من شبكة الإنترنت (نشر البرامجيات المسببة للضرر، وهجمات لحجب الخدمة، وغير ذلك من المحاولات للقيام بأنشطة غير مأذون بها).

٢٣ - ولا بد من إضافة أنه، تم في أوكرانيا وضع الأسس التشريعية والقانونية، ونُظِّم العمل المتعلق بتوفير التعاون بين الدائرة الحكومية للاتصالات المتخصصة وحماية المعلومات بأوكرانيا وهيئات إنفاذ القانون، بهدف تنفيذ تدابير تتعلق بضمان أمن موارد المعلومات الحكومية في نُظُم تكنولوجيا المعلومات والاتصالات السلكية واللاسلكية ذات الحماية، وتعزيز فعالية نظام التصدي للأنشطة غير المأذون بها فيما يتصل بموارد المعلومات المذكورة.

٢٤ - وهكذا، فإنه تتوفر لدى أوكرانيا اليوم القدرة على تنفيذ الأعمال الخاصة بحماية المعلومات في جميع مراحل إنشاء نُظُم تكنولوجيا المعلومات والاتصالات السلكية واللاسلكية ذات الحماية، والنُظُم المتكاملة لحماية المعلومات التي تشتمل عليها نُظُم تكنولوجيا المعلومات والاتصالات السلكية واللاسلكية ذات الحماية، بغض النظر عن نوع ودرجة حرجية المعلومات التي تجري معالجتها، وعن نوع نُظُم تكنولوجيا المعلومات والاتصالات السلكية واللاسلكية ذات الحماية ودرجة تعقيدها. ومن ثم، فإن جميع النُهُج الأساسية لصياغة متطلبات حماية موارد المعلومات في نُظُم تكنولوجيا المعلومات والاتصالات السلكية واللاسلكية ذات الحماية، والتخطيط والإعداد لها، وتقييم قدرتها على الحماية، وتوفيرها، تتفق في عمومها مع النُهُج التي تتبعها الهيئات الحكومية المسؤولة عن الأمن في الدول الأعضاء في الأمم المتحدة والبلدان الأعضاء في الاتحاد الأوروبي.

٢٥ - ولأغراض توفير الأنشطة التثقيفية المتعلقة بتأهيل الخبراء في مجال أمن المعلومات وهندسة الحاسوب، أُسس معهد لحماية المعلومات تابع للجامعة الحكومية لتكنولوجيا المعلومات والاتصالات، ليعمل كمؤسسة تعليمية وعلمية متفرعة عن الجامعة.

بنما

[الأصل: بالإسبانية]
[٢١ حزيران/يونيه ٢٠١٠]

١ - توجد في جمهورية بنما مؤسسات تتصدى لإساءة استخدام شبكة الإنترنت لأغراض إجرامية بما في ذلك الأعمال الإرهابية، ولهذا، لدينا مجلس الأمن القومي ومعهد الطب الشرعي والعلوم الجنائية - قسم الجرائم.

٢ - ويقوم مجلس الأمن القومي بالعمل الاستخباري ضد أنشطة الجريمة المنظمة، بما في ذلك الإرهاب، في حالة وقوع هجوم محتمل على الممتلكات والسلامة الإقليمية.

٣ - ويقوم قسم الجرائم من معهد الطب الشرعي والعلوم القانونية الذي أنشئ بموجب القانون ٦٩ المؤرخ ٢٧ كانون الأول/ديسمبر ٢٠٠٧، من ناحيته بأعمال التحقيق في جرائم الفضاء الحاسوبي.

٤ - ويجرم قانوننا للعقوبات استخدام الإنترنت لأغراض إرهابية، حيث تنص مادته ٢٨٩ على أن ''من يستخدم الإنترنت لتعليم سبل جمع أو تجنيد الأشخاص للقيام بأعمال لأغراض إرهابية يعاقب بالسجن لمدة تتراوح من خمسة إلى عشرة أعوام''.

٥ - وهناك أيضا قوانين أخرى تجرم استخدام شبكة الإنترنت لأغراض إجرامية، ويعاقب على هذا الاستخدام جنائيا ومدنيا وإداريا، ويحكم القانون ١٤ المؤرخ ١٨ أيار/مايو الفصل الثامن والفصل ١ ''للجرائم المرتكبة ضد أمن المعلومات''، ويحكم القانون ٥١ المؤرخ ٢٢ تموز/يوليه ٢٠٠٨ ''الوثائق الإلكترونية والتوقيعات الالكترونية وتقديم الخدمات وغير ذلك من ترتيبات تطوير التجارة الإلكترونية''، أما القانون ٣٨ المؤرخ ٨ شباط/فبراير ١٩٩٦ فيحكم قواعد تنظيم الاتصالات السلكية واللاسلكية في جمهورية بنما.

قطر

[الأصل: بالإنكليزية]
[٢٥ أيار/مايو ٢٠١٠]

١ - تعرب دولة قطر عن اقتناعها بضرورة استخدام تكنولوجيا المعلومات والاتصالات وفقا لميثاق الأمم المتحدة والمبادئ الأساسية للعلاقات الدولية. ثم إنه يجب ضمان حرية تدفق المعلومات دون الإخلال بالسيادة الوطنية مع المحافظة على الأمن واحترام الفروق الثقافية والسياسية والأخلاقية بين الأمم.

٢ - وتقوم الجهود المبذولة على المستوى الوطني على المصلحة وأمن الاتصالات وبذل قصارى الجهود لتعزيزها من حين لآخر لمواكبة تقدم الاتصالات على المستويين الوطني والدولي.

٣ - ويمكن إجمال الجهود الوطنية فيما يلي:

- وضع استراتيجيات وسياسات أمنية وسن قوانين تحظر استخدام التكنولوجيا لأغراض لا تتفق مع أهداف حماية الاستقرار الأمني؛
- إنشاء آلية لتعزيز أمن المعلومات بغية كفالة حماية الهياكل الأساسية للمعلومات الحساسة في قطر؛
- يسعى مكتب أمن الإنترنت والمعلومات لرصد الشبكات الحكومية والشبكة الوطنية بغية التصدي للمخاطر الإلكترونية التي تهدد دولة قطر؛
- ترمي إدارة حوادث الإنترنت وتنسيق الجهود لتسويتها إلى كفالة تسوية المسائل المتصلة بالإنترنت بعد الإبلاغ عنها بأسرع وقت ممكن. وهذا ما يتم القيام به في قطر من خلال الفريق القطري للاستجابة لحالات الطوارئ الحاسوبية؛
- القيام بدور فعال بقدر أكبر في مجال المعلومات والتوعية لتحسين مستوى المهارات والمؤهلات التقنية للموظفين في المؤسسات القطرية؛
- تقديم الدعم إلى القطريين في التعامل مع المسائل المتصلة بالإنترنت؛
- متابعة آخر أوجه التقدم في ميدان العلوم التكنولوجية الحديثة المتصلة بأمن وسلامة الإنترنت وكفالة وتقييم المنتجات التقنية وأمنها وخدماتها؛
- النهوض بالعلاقات الدولية بغية معالجة المسائل المتصلة بالإنترنت. قد شاركت دولة قطر في منتدى أفرقة التصدي للحوادث والأمن وعملية ميريديان.

٤ - وترد فيما يلي أهم التدابير التي يمكن أن يتخذها المجتمع الدولي لتعزيز أمن المعلومات على المستوى الوطني:

- ينبغي أن تواصل الأمم المتحدة قيادة المناقشة، وتقدم توضيحات بشأن استخدام تكنولوجيا المعلومات والاتصالات السلكية واللاسلكية في المعدات الإلكترونية وما إذا كانت مبادئ القانون الدولي القائمة كافية لتوفير إطار مناسب لتحديد السلوك اللائق على الإنترنت بشأن الأعمال العدوانية؛
- إنشاء لجنة دولية مخصصة لأمن المعلومات السلكية واللاسلكية وتقديم دراسات شاملة تتصل بهذا الموضوع؛
- تشجع دولة قطر جميع الدول الأعضاء على إنشاء أفرقة للتصدي للطوارئ الحاسوبية على المستوى الوطني؛
- إذكاء الوعي من خلال ندوات واجتماعات تعقد على المستويين المحلي والدولي؛
- تشجيع الدول على التعاون بغية مكافحة التجسس والقرصنة الإلكترونية؛
- استخدمات معدات مشفرة ومؤمنة لنقل المعلومات والوثائق لتأمين السرية في تبادلها؛
- نظم لحماية التحديث وعقد حلقات عمل منتظمة لتقييم آخر المستجدات العلمية في مجال النهوض بأمن المعلومات.

كوبا

[الأصل: بالإسبانية]
[٢٧ أيار/مايو ٢٠١٠]

١ - تؤيد كوبا جميع مظاهر القلق المعبر عنه في نص القرار ٢٥/٦٤ بخصوص استخدام تكنولوجيا الإعلام ووسائطه في أغراض لا تتسق مع تحقيق الاستقرار والأمن الدوليين، وتؤثر سلبا على السلامة الإقليمية للدول، وهو ما يضر بأمنها في الميدانين المدني والعسكري. وترى كوبا أن القرار كان محقا في تشديده على ضرورة منع استخدام موارد المعلومات وتكنولوجياتها في أغراض إجرامية أو إرهابية.

٢ - وتؤكد كوبا مجددا أن الاستعمال العدائي للاتصالات السلكية واللاسلكية الذي يرمي علنا أو سرا إلى تقويض النظام القانوني والسياسي للدول، يمثل انتهاكا للقواعد الدولية المعترف بها في هذا المجال، ومظهرا سلبيا وعديم المسؤولية لاستعمال تلك الوسائط قد تؤدي آثاره إلى إحداث توترات وحالات تضر بالسلام والأمن الدوليين، وهو ما يؤدي بدوره إلى تقويض المبادئ والمقاصد المكرسة في ميثاق الأمم المتحدة.

٣ - وتنوه كوبا، مع القلق، إلى أن نظم المعلومات والاتصالات السلكية واللاسلكية إذا ما صُممت و/أو استُخدمت بغرض إلحاق أضرار بالمرافق الأساسية لدولة من الدول، فإنها قد تتحول إلى سلاح وتشكل بذلك خطرا على السلام والأمن الدوليين.

٤ - وفي هذا السياق، تكرر جمهورية كوبا إدانتها التي سبق أن أعربت عنها في مختلف المحافل الدولية لما تقوم به الإدارات المتعاقبة في الولايات المتحدة الأمريكية من تصعيد عدواني في حربها الإذاعية والتلفزيونية ضد كوبا، وهو ما يشكل انتهاكا سافرا للمعايير الدولية الناظمة للمجال اللاسلكي.

٥ - ولم تلحظ حكومات الولايات المتحدة الأمريكية الضرر الذي يمكن أن يلحق بالسلام والأمن الدوليين جراء ما يصار إليه من حالات خطيرة من قبيل استخدام طائرة عسكرية لبث إشارات تلفزيونية باتجاه كوبا دون موافقتها.

٦ - ويشكل العدوان اللاسلكي التي تشنه الولايات المتحدة الأمريكية ضد كوبا انطلاقا من الأراضي الأمريكية انتهاكا لمبادئ القانون الدولي التي تنظم العلاقات بين الدول ولقواعد الاتحاد الدولي للاتصالات وأنظمته التي تحدد قواعد السلوك التي يجب أن تتقيد بها البلدان الأعضاء في هذه الوكالة المتخصصة التابعة لمنظومة الأمم المتحدة.

٧ - فكل أسبوع، تخصص محطات إرسال توجد في أراضي الولايات المتحدة الأمريكية لكوبا آلاف الساعات من البث التلفزيوني على ٣٤ موجة متوسطة، وقصيرة وموجات تلفزيونية. ففي أواخر شهر أيار/مايو ٢٠١٠، بلغت ساعات البث الأسبوعي غير المشروع الموجه نحو كوبا ١٥٦ ٢ ساعة. وهناك عدة محطات من محطات الإرسال هذه مملوكة أو موالية لمنظمات مرتبطة بعناصر إرهابية معروفة تقيم في أراضي الولايات المتحدة الأمريكية وتعمل ضد كوبا من هناك بموافقة تامة من سلطات الولايات المتحدة الأمريكية.

٨ - وهذه البرامج الإذاعية والتلفزية غير المشروعة، لا تبث أخبارا، وإنما هي على النقيض من ذلك، تزوّر الأخبار وتبث أراجيف لزرع البلبلة. ويعتمد الكونغرس الأمريكي لهذه الأعمال كل سنة ميزانية تزيد على ٣٠ مليون دولار من الأموال الاتحادية. ومنذ إنشاء المحطتين، أنفقت حكومة الولايات المتحدة ٦٥٩,٨ مليون دولار على هذا الغرض.

٩ - وتشكل هذه البرامج الاستفزازية ضد كوبا انتهاكات للمبادئ الدولية التالية:

- المبادئ الأساسية للاتحاد الدولي للاتصالات الواردة في ديباجة دستوره والمتعلقة بالأهمية المتزايدة التي تكتسيها الاتصالات السلكية واللاسلكية من أجل صون السلام وتحقيق التنمية الاقتصادية والاجتماعية لجميع الدول بهدف تيسير العلاقات السلمية والتعاون الدولي بين الشعوب وبلوغ التنمية الاقتصادية والاجتماعية من خلال الأداء السليم للاتصالات السلكية واللاسلكية. ويتسم محتوى البرامج التلفزيونية التي تبثها حكومة الولايات المتحدة ضد كوبا بطابع تخريبي يهدف إلى زعزعة الاستقرار والتضليل ويتعارض مع المبادئ المذكورة؛

- الحكمان CS 197 و CS 198 من دستور الاتحاد الدولي للاتصالات، اللذان ينصان على ضرورة إنشاء وتشغيل جميع المحطات، كيفما كانت أهدافها، على نحو لا يحدث تشويشا يضر بالاتصالات أو الخدمات اللاسلكية التابعة لدول أعضاء أخرى؛

- الاتفاق الصادر عن الجلسة العامة التاسعة للمؤتمر العالمي للاتصالات اللاسلكية المعقودة 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 موجاتها 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 قيامها بتخصيص تردداتها

الخاصة الترددات المخصصة والمسجلة باعتراف دولي لتتجنب بذلك إحداث أي تشويش ضار؛

- الفقرة الفرعية ٤ من المادة ٤٢ من أنظمة الاتصالات اللاسلكية للاتحاد، التي تحظر على المحطات المنشأة على متن طائرات تعمل في البحر أو فوق البحر تقديم أي خدمات للبث الإذاعي؛

- 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 ميغاهيرتز، وطالب إدارة الولايات المتحدة الأمريكية باتخاذ التدابير المناسبة لوقفه. علاوة على ذلك، دأب مجلس أنظمة الاتصالات اللاسلكية منذ أيلول/سبتمبر ٢٠٠٦ على مطالبة إدارة الولايات المتحدة الأمريكية باتخاذ تدابير ترمي إلى إزالة التشويش على موجة التردد ٥٠٩ ميغاهيرتز دون أن يتلقى أي رد حتى الآن. وفي ٢٠ آذار/مارس ٢٠٠٩، اختتم المجلس اجتماعه الخمسين وأكد مجددا في موجز قراراته (الوثيقة RRBO9-1/5) عدم مشروعية البث وطالب إدارة الولايات المتحدة الأمريكية باتخاذ التدابير اللازمة من أجل وضع حد لحالات التشويش على الخدمات التلفزيونية لكوبا؛

- الفقرة الفرعية ٣ من المادة ٢٣ من أنظمة الاتصالات اللاسلكية للاتحاد، التي تقيّد الإرسال التلفزيوني خارج الحدود الوطنية.

١٠ - وأقر تقرير أصدره مكتب المراجعة التابع لحكومة الولايات المتحدة الأمريكية (وهي هيئة رسمية في الولايات المتحدة) في كانون الثاني/يناير ٢٠٠٩ بأن برنامج الإرسال الإذاعي والتلفزيوني لحكومة الولايات المتحدة الأمريكية الموجه ضد كوبا ينطوي على انتهاكات للقواعد الدولية وللقانون المحلي:

- ورد فيه أن الاتحاد الدولي للاتصالات اللاسلكية قرر في عام ٢٠٠٤ وعام ٢٠٠٦ أن البرامج التلفزيونية على القناتين ١٣ و ٢٠ تحدث تشويشا ضارا للمحطات الكوبية وأن وزارة الخارجية لم تفعل شيئا للرد على مطالبة الاتحاد. وورد في التقرير أيضا أن المؤتمر العالمي للاتصالات الإذاعية المعقود في تشرين الثاني/نوفمبر ٢٠٠٧ أفتى بأن البث الموجه من طائرة في الولايات المتحدة باتجاه كوبا مخالف لأنظمة الاتحاد الدولي للاتصالات اللاسلكية؛

- اعترف التقرير بأنه، رغم أن قوانين الولايات المتحدة الأمريكية تحظر البث الداخلي لهذا النوع من البرامج الإذاعية والتلفزيونية على حد سواء، فإنه يمكن التقاطها في

أراضي الولايات المتحدة الأمريكية وبخاصة في ميامي، وهي البرامج التي رصد في المحطات المتعاقد معها بث إعلانات سياسية فيها بمقابل ولقطات إشهارية ذات طابع جنسي. وبالإضافة إلى ذلك ذكر التقرير أن البرامج الموجهة ضد كوبا لا تستوفي معايير الاتزان والموضوعية الصحفية، وأنه يلاحظ فيها استخدام لغة تحريضية وتهجمية؛

١١ - وتذكّر كوبا كذلك بأن المؤتمر العالمي للاتصالات اللاسلكية الذي انعقد في جنيف، سويسرا، في الفترة من ٢٢ تشرين الأول/أكتوبر إلى ١٦ تشرين الثاني/نوفمبر ٢٠٠٧ قد أقرّ نص الاستنتاجات الذي يصف عمليات البث الموجهة من طائرات في الولايات المتحدة باتجاه كوبا بأنها مخالفة لأنظمة الاتصالات اللاسلكية. وتنص الاستنتاجات التي أيدتها الجلسة العامة حرفيا على أنه ''لا يمكن اعتبار قيام محطة إذاعية تعمل على متن طائرة وتبث موجاتها باتجاه إقليم إدارة أخرى دون موافقتها عملا يتماشى مع أنظمة الاتصالات اللاسلكية''؛

١٢ - وقد تم الاتفاق على هذه الاستنتاجات على مستوى الجمعية العامة للمؤتمر، وهي تكتسي قوة القانون بالنسبة لعمل الاتحاد. وبذلك يكون المؤتمر العالمي للاتصالات اللاسلكية قد أيد الإعلان الصادر في عام ١٩٩٠ عن المجلس الدولي لتسجيل الترددات، الذي كان قائما آنذاك، والذي ينص على أن توجيه البث التلفزيوني من على متن منطاد مبرمج من بُعد باتجاه الإقليم الوطني الكوبي يشكل انتهاكا للأنظمة؛

١٣ - وقد تبدّى العداء الذي تناصبه حكومة الولايات المتحدة الأمريكية لكوبا في الحصار الاقتصادي والتجاري والمالي الذي تفرضه عليها منذ قرابة ٥٠ عاما، وهو الحصار الذي يؤثر أيضا على مجال المعلومات والاتصالات السلكية واللاسلكية:

- لا يحق لكوبا الاستفادة من الخدمات التي يعرضها عدد كبير من المواقع على شبكة الإنترنت، حيث أنه يحظر دخولها بمجرد ما يتبين أن النطاق الكوبي هو مصدر الاتصال؛
- دون سابق إشعار، قام مكتب مراقبة الممتلكات الأجنبية في الآونة الأخيرة بحظر أسماء النطاقات .com المرتبطة بكوبا؛
- بسبب قوانين الحظر الاقتصادي والتجاري والمالي الذي تفرضه عليها حكومة الولايات المتحدة الأمريكية، لا تستطيع كوبا، أن تصل البلد بكابلات الألياف الضوئية التي تحيط بالأرخبيل الكوبي، مما يضطرها إلى تسديد تكاليف الخدمات الساتلية مع ما ينطوي عليه ذلك من قيود تعزى إلى مدى توافق النطاق الترددي،

وعقبات خطيرة تعرقل الحصول على التكنولوجيات اللازمة، وارتفاع تكاليف التوصيل؛

- تستخدم الإنترنت في شن حملات تشهير ضد كوبا لأغراض هدامة، وتشويه سمعة البلد.

١٤ - ويقوض هذا الموقف الذي تتخذه الولايات المتحدة الأمريكية الإرادة والنتائج والروح التي سادت بين دول العالم بأسره عندما اجتمعت في سويسرا وتونس بمناسبة عقد مؤتمري القمة العالميين المعنيين بمجتمع المعلومات في عامي ٢٠٠٣ و ٢٠٠٥ تباعا.

١٥ - وقد حث هذان المؤتمران الدولَ بقوة على أن تقوم، في سعيها إلى بناء مجتمع المعلومات، باتخاذ خطوات لمنع وتجنب أية تدابير انفرادية لا تتفق مع القانون الدولي وميثاق الأمم المتحدة قد تعرقل التحقيق الكامل للتنمية الاقتصادية والاجتماعية للسكان في البلدان المعنية أو تعوق رفاههم.

١٦ - وتكتسي المناقشة التي تجري في الجمعية العامة للأمم المتحدة بشأن التقدم المحرز في ميدان تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي أهمية بالغة تزداد كل يوم. فالتدابير المشار إليها آنفا بالتفصيل التي تتخذها الولايات المتحدة الأمريكية ضد كوبا إنما تؤكد ضرورة إجراء هذه المناقشة والحاجة الملحة إلى اتخاذ تدابير لوضع حد لمثل هذه المظاهر.

١٧ - وتؤيد كوبا بحزم العملية الجارية في الجمعية العامة للأمم المتحدة، وستواصل كوبا بذل قصارى جهودها للإسهام في التطوير السلمي لتكنولوجيا المعلومات والاتصالات في العالم واستخدامها لما فيه خير البشرية جمعاء، وهي على استعداد للتعاون مع باقي البلدان، بما فيها الولايات المتحدة الأمريكية، لإيجاد الحلول الكفيلة بتذليل العقبات التي تحول دون تحقيق هذين الهدفين.

المكسيك

[الأصل: بالاسبانية]
[أيار/مايو ٢٠١٠]

تقييم عام لمشاكل أمن المعلومات

١ - المؤسسات المصرفية والمؤسسات والمالية، وكذلك الوحدات الإدارية التابعة للحكومة الاتحادية المعنية بمواضيع السلامة العامة والأمن الوطني هي المنظمات التي تبذل في البلد أكثر الجهود في مجال أمن المعلومات. وهناك وحدة لمكافحة جرائم الفضاء الحاسوبي وشرطة لمكافحة هذه الجرائم تتبع الإدارة الاتحادية للسلامة العامة المعنية بمكافحة جرائم الفضاء الحاسوبي المخلة بالأمن العام.

٢ - ومن ناحية أخرى، فإنه بالرغم من وجود جهود متفرقة تبذلها السلطات الثلاث في مجال مكافحة جرائم الفضاء الحاسوبي، لا توجد سياسة للحكومة الاتحادية توجه استراتيجيات مكافحة هذه الجرائم في البلد، وثمة حاجة إلى تعزيز التشريعات القائمة في هذا المجال، ويحتاج القضاة إلى المزيد من الأدوات التي من شأنها أن تساعدهم على التصدي لهذه الجرائم والمعاقبة عليها، وتستدعي الحاجة أيضا استكمال القواعد التي تحكم عمل مقدمي خدمات الإنترنت لكي يحتفظوا بسجل لنشاطهم في برنامجهم، ويبلغوا عن أي حادث محتمل. ومن ناحية أخرى، هناك حاجة لوضع اتفاقات داخلية وإيجاد اتفاقات تعاون مع الدول الأخرى للتصدي لجرائم الفضاء الحاسوبي والإرهاب الإلكتروني التي تهدد الأمن القومي.

التدابير الجاري اتخاذها على المستوى الوطني لتعزيز أمن المعلومات والمساهمة في التعاون الدولي في هذا المجال

٣ - هناك جهود تبذلها المكسيك فيما يتعلق بإيجاد اليقين القانوني في إطار سياق أمن المعلومات من قبيل الجهود التالية:

(أ) إدراج قواعد بشأن بعض جرائم الفضاء الحاسوبي في القوانين التالية: قانون العقوبات الاتحادي، القانون الجنائي لمنطقة العاصمة الاتحادية، القانون الاتحادي للإجراءات الجنائية، وقانون كوليما لحماية البيانات، والقوانين الجنائية لولايات أغواكلينتس، وتاباسكو، وتارناليبس؛

(ب) في ٣٠ نيسان/أبريل ٢٠٠٩، صدر في الجريدة الرسمية للاتحاد المرسوم الذي يضيف الجزء التاسع والعشرين - سين من المادة ٧٣ من دستور الولايات المتحدة المكسيكية،

الذي يعطي لكونغرس الاتحاد صلاحية إصدار تشريعات لحماية البيانات الشخصية التي توجد بحوزة الأفراد؛

(ج) في ١ حزيران/يونيه ٢٠٠٩، صدر المرسوم الذي يضيف إلى المادة ١٦ من الدستور فقرة ثانية، تقر بأن لكل شخص الحق في التمتع بحماية بياناته الشخصية، والوصول إلى هيئة العفو الدولية، وتصحيح وإلغاء هذه البيانات، وكذلك الاعتراض عليها بالشروط التي يحددها القانون الذي سيضع الاستثناءات من المبادئ التي تحكم معالجة البيانات لأسباب تتعلق بالأمن القومي، والأحكام المتعلقة بالنظام العام، والأمن والصحة العامين، أو لحماية حقوق الأطراف الثالثة؛

(د) هناك فريق للاستجابة لحوادث الأمن الحاسوبي التابع للجامعة الوطنية المستقلة للمكسيك يعالج المشاكل الأمنية في الأوساط الأكاديمية، ويقدم الدعم والمشورة التقنية إلى السلطات الحكومية في المكسيك المعنية بالتصدي لجرائم الفضاء الحاسوبي؛

(هـ) يحتفظ بشرطة لجرائم الفضاء الحاسوبي ضمن جهاز الشرطة الاتحادية تتولى متابعة التحقيقات في الجرائم المخلة بالأمن العام؛

(و) يجري داخل الحكومة الاتحادية إعداد تقرير تنفيذي بشأن جوانب الضعف في الفضاء الحاسوبي لإبلاغ السلطات العليا والحكومة الاتحادية بما يستجد على المستوى العالمي من أحداث في هذا الفضاء، واتخاذ ودعم مبادرات تعزز أمن الفضاء الحاسوبي في المكسيك؛

(ز) يجري الإعداد داخل الحكومة الاتحادية لإنشاء فريق للتصدي لحوادث الأمن الحاسوبي بغية تنسيق جهود التصدي لجرائم الفضاء الحاسوبي على المستويين الداخلي والخارجي؛

(ح) جوانب الضعف في الفضاء الحاسوبي من المواضيع المطروحة على جدول الأعمال الوطني للمخاطر؛

(ط) يضطلع ببرامج لتوعية عموم الناس تنسقها وحدة عامة وخاصة لمكافحة جرائم الفضاء الحاسوبي؛

(ي) حضور مختلف المحافل ووضع اتفاقات ودية مع الدول الأخرى للتصدي لجرائم الفضاء الحاسوبي.

التدابير التي يمكن أن يتخذها المجتمع الدولي لتعزيز أمن المعلومات العالمية

٤ - فيما يلي تدابير تعزيز أمن المعلومات على الصعيد العالمي:

(أ) وضع التشريعات المناسبة أو تحديث القائم منها إذا لزم الأمر لحماية المعلومات في مجال الفضاء الحاسوبي؛

(ب) تدريب القضاة على مواضيع الفضاء الحاسوبي بغية تأهيلهم للبت في جرائم الفضاء الحاسوبي وإصدار الأحكام المناسبة في هذا الصدد؛

(ج) إنشاء أفرقة وطنية للاستجابة لحوادث الأمن الحاسوبي تنسق جهود التصدي لهذه الحوادث في حالات الحوادث الكبيرة وتكون مراكز تنسيق مع البلدان الأخرى؛

(د) ترك قنوات الاتصال مفتوحة باستمرار بين المراكز الوطنية المذكورة للتنسيق فيما بينها في حالة وقوع أي حادث إقليمي أو عالمي؛

(هـ) إقامة منتديات لتبادل الخبرات وتدريب أفرقة الأمن من أعضاء المجتمع الدولي؛

(و) تنفيذ الاتفاقيات الدولية بشأن التعاون في مكافحة جرائم الفضاء الحاسوبي من أجل الإسراع في التحقيقات وتشكيل جبهة مشتركة.

المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية

[الأصل: بالإنكليزية]
[٢ حزيران/يونيه ٢٠١٠]

١ - يسر المملكة المتحدة أن تستجيب لقرار الجمعية العامة ٢٥/٦٤ بشأن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي

٢ - إننا نعتبر هذا الموضوع على أنه من المواضيع الأكثر أهمية، كما نعتبره حيويا لفرادى الدول، ولتجارتها، ولحماية مواطنيها، فضلا عن أهميته وحيويته في السياق الأوسع للأمن الدولي. وتكرس المملكة المتحدة جهدا كبيرا لجعل الفضاء الحاسوبي مكانا آمنا لجميع الأمم، ونحن نرحب بالأنشطة الدولية في هذا المجال، لأننا نعتقد بأنه ينبغي على جميع الدول أن تتعاون في العمل على تهيئة بيئة آمنة ومرنة في الفضاء الحاسوبي.

تقدير عام لقضايا أمن المعلومات

٣ - إننا نعتقد بأن الفضاء الحاسوبي الآمن هو أمر بالغ الأهمية بالنسبة لعالم اليوم. فالمواطنون، والتجارة، والبنية التحتية الوطنية الحيوية، والحكومة يعتمدون جميعهم بشكل متزايد على شبكة الإنترنت. ومن المرجح أن تكون لأي حادث يؤثر سلبا على خدمات الإنترنت داخل دولة ما عواقب على تلك الدولة، وربما تكون تلك العواقب ذات طبيعة قاسية. وهناك حقيقة مؤسفة تتمثل في احتمال وجود عددٍ من الجهات الفاعلة المُهَدِّدَة، سواء من خارج أو من داخل أي دولة من الدول، والتي قد تحاول تعطيل خدمة الإنترنت أو التلاعب بها، لأي سبب من عدة أسباب مختلفة.

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

٤ - تواصل المملكة المتحدة العمل محليا ودوليا من أجل الترويج لفضاء حاسوبي أكثر أمنا. لقد قمنا على الصعيد المحلي بنشر استراتيجيتنا الوطنية للأمن الحاسوبي في حزيران/يونيه ٢٠٠٩. وتدعم هذه الوثيقة الجهود الوطنية في مجال أمن المعلومات. وتدعو الاستراتيجية إلى إنشاء منظمتين جديدتين، هما مكتب الأمن الحاسوبي ومركز عمليات الأمن الحاسوبي. وقد أُنشئت المنظمتان الاثنتان وهما توصلان النمو. وهناك ثلاثة أفرقة للاستجابة للطوارئ الحاسوبية تديرها حكومة المملكة المتحدة، وهي تقدم خدمة متخصصة لشبكات البنية التحتية الوطنية البالغة الأهمية بالمملكة المتحدة وللشبكات العسكرية وغيرها من الشبكات

الحكومية. وعلى الصعيد الدولي فإننا نقوم أيضا بدور نشط في هذا العمل. وتشتمل مشاركتنا على صعيد الأمم المتحدة على العضوية في فريق الخبراء الحكوميين. لقد شاركنا في تقديم قرار الأمم المتحدة بشأن إرساء ثقافة عالمية لأمن الفضاء الحاسوبي واستعراض الجهود الوطنية الرامية إلى حماية الهياكل الأساسية الحيوية للمعلومات. ونتمتع بالعضوية في الهيئات ذات الصلة التابعة للاتحاد الدولي للاتصالات. ونشارك في أنشطة منظمة الأمن والتعاون في أوروبا. وقد بدأ الاتحاد الأوروبي، بدعمنا ومشاركتنا الكاملتين، يعمل على العديد من المبادرات في مجال حماية البنية التحتية الوطنية الحساسة بالاتحاد الأوروبي. وقد ساهمنا في مشاركة الاتحاد الأوروبي في أعمال المنتدى الإقليمي لرابطة أمم جنوب شرق آسيا (آسيان) بشأن الأمن الحاسوبي. وبالمثل فإننا نشارك في عدد من الأنشطة ضمن إطار حلف شمال الأطلسي كجزء من حماية الشبكات المملوكة لتلك المنظمة. وكانت المملكة المتحدة منذ أمد بعيد أمة رائدة ضمن إطار ميريديان (www.meridian2007.org)، ومنتدى أفرقة التصدي للحوادث التي تهدد الأمن (www.first.org)، ومجموعة أفرقة الاستجابة للطوارئ الحاسوبية بالحكومات الأوروبية (www.egc-group.org).

٥ - ويتاح تنزيل الاستراتيجية الوطنية لأمن الحاسوب بالمملكة المتحدة من الصفحة الشبكية لمكتب مجلس الوزراء على الموقع www.cabinetoffice.gov.uk.

التدابير التي يمكن اتخاذها من جانب المجتمع الدولي لتعزيز أمن المعلومات على الصعيد العالمي

٦ - إننا نشجع جميع الدول على إنشاء الأفرقة الوطنية للاستجابة للطوارئ الحاسوبية. كما نشجع جميع الدول على سن تشريعات محلية فعالة بشأن الجرائم الحاسوبية. ونحن نعتقد أنه في حين أن الجريمة الإلكترونية ليست هي النشاط الخبيث الوحيد في الفضاء الحاسوبي، إلا أنها الأكثر انتشارا، وأن الحد من النشاط الإجرامي يعود بالفائدة على الجميع. ونحن نعتقد بأن اتفاقية مجلس أوروبا بشأن الجريمة الحاسوبية يمثل أداة مناسبة لمكافحة الجريمة الإلكترونية على الصعيد الدولي. وبالإضافة إلى ذلك، فإننا نعتقد بأن مجموعة الأدوات التي استنبطها الاتحاد الدولي للاتصالات، والتي يتم الترويج لها في الأمم المتحدة، توفر أساساً جيداً يمكن للدول أن تستند إليه في إجراء تقييم ذاتي لمدى استعدادها لمواجهة الهجمات المحتملة على الهياكل الأساسية الوطنية الحيوية. ونرحب بالجهود التي تتم داخل العديد من المحافل للترويج لأفضل الممارسات في مجال أمن المعلومات.

المفاهيم الدولية ذات الصلة

٧ - إن المفهوم الدولي الأساسي هو مفهوم القانون الدولي. وهناك نقاش واسع، لا سيما في المؤتمرات الالكترونية، حول إمكانية تطبيق القانون الدولي الحالي على الفضاء الحاسوبي. لقد درست المملكة المتحدة هذا الموضوع، وفي رأينا فإن المبادئ القائمة للقانون الدولي، سواءً تلك المعنية باستخدام القوة أو تلك المعنية بقانون النزاعات المسلحة، توفر إطار ملائما يمكن من خلاله تحديد وتحليل استخدام الفضاء الحاسوبي في سياق الأعمال العدائية.

اليونان

[الأصل: بالإنكليزية]
[٢٨ حزيران/يونيه ٢٠١٠]

١ - أصبحت مسائل أمن المعلومات تعالج على نطاق أوسع مما كان في الماضي. وأكيد أن النية تتجه إلى اتخاذ تدابير للتصدي للمخاطر الحديثة الملازمة لاكتساب الشبكات والنظم طابع العولمة. والنظر جار في اتخاذ تدابير تحافظ على حرية تدفق المعلومات لتطبيقها على الصعيد الوطني وفي السياق العابر للحدود الوطنية.

٢ - ويجري اتباع المفاهيم الدولية والمتعددة الجنسيات الحالية والقيام بدراسات بشأنها. وثمة حاجة إلى تقديم التوجيه بشأن تقييم المخاطر. وينبغي أيضا تناول موضوع الحماية السيبرية. وينبغي الاحتفاظ بالحقوق السيادية الوطنية في أمن هذه المعلومات في أي تقاسم عالمي لهذه المعلومات.

٣ - وغني عن القول إنه ينبغي أن تواصل جميع الدول الأعضاء إبلاغ الأمين العام بآرائها وتقييماتها بشأن المسائل ذات الصلة. وفي هذا الصدد، يجدر بالذكر النقاط التالية:

(أ) جميع مسائل أمن المعلومات عموما ما تحظى بتقدير كبير؛

(ب) دراسة وتطبيق سبل الحفاظ على التدفق الحر للمعلومات والعمل من أجل تحقيق المستويات المطلوبة من سريتها - نزاهتها - توافرها، والأخذ بتلك السبل داخل الحدود الوطنية وفي السياق العابر للحدود الوطنية؛

(ج) ينبغي صياغة مفاهيم توصيل الشبكات التي توفر القدرات المستحدثة والمتقاسمة على الصعيدين الوطني والدولي والاتفاق عليها . ويجب أن يتوافر تقييم لمخاطر توصيل الشبكات والتوجيه الدولي الواضح في هذا الصدد. وبالإضافة إلى ذلك، وبما أن الحماية السيبيرية تشكل أحد مصادر القلق البالغ جدا بالنسبة لكل دولة، فإن هناك حاجة إلى التعاون وإعمال روح الكفاءة والاقتصاد. وأخيرا وليس آخرا، لا يمكن تجاهل حاجة البلد إلى الحفاظ على سيادته والحفاظ على قاعدة معلومات خاصة به، ويجب مراعاة هذا الأمر في صياغة أي من المفاهيم المذكورة؛

(د) يمكن أن تكون التدابير التي ينبغي أن يتخذها المجتمع الدولي لتعزيز أمن المعلومات على المستوى العالمي على نحو ما يلي:

'١' ينبغي أن تكون المفاهيم الدولية ذات الصلة مفصلة ومتفقا عليها؛

'٢' يمكن اقتراح خطة توجيهية بشأن هياكل أساسية عامة منسقة تغطي مسائل التشريع الأساسي، من أجل تزويد عدد من المستخدمين المرخص لهم بالتدابير اللازمة في مجال أمن مناولة جميع المراسلات والرسائل إلكترونيا، وتوفير طرق الاتصال المتعددة؛

'٣' ينبغي مواءمة وتوسيع المفاهيم التي تتبعها التحالفات المتعددة الجنسيات ومجموعات الدول الصغيرة بما يجعلها قابلة للتطبيق على المستوى العالمي. ويمكن أن يذهب الاتفاق على تحديد الخطر وأثره السلبي إلى أبعد من هندسة تدابير متطورة يتم استحداثها، حيث إن هذه التدابير قد يستخدمها الخصوم أيضا؛

'٤' بالتوازي مع كل ما سبق، ينبغي أن تفهم سيادة البلد على أنها هي المرجعية الأساسية لكل محاولة للعولمة. وينبغي وضع مفهوم دولي لتحديد مداخل تبادل المعلومات الوطنية في ظل سيناريوهات تعكس مستوى التكامل المطلوب، واستخدامها كدليل في جميع الجهود المبذولة على المستويات الوطنية والمتعددة الجنسيات والدولية.