الأمم المتحدة

A/58/373

الجمعية العامة

Distr.: General
17 September 2003
Arabic
Original: English/French/Russian/
Spanish

الدورة الثامنة والخمسون

البند ٦٩ 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

	الفقرات	الصفحة
أولا – مقدمة	١-٢	٢
ثانيا – الردود الواردة من الدول الأعضاء		٢
الاتحاد الروسي		٢
أوكرانيا		٦
بوليفيا		١٥
جورجيا		١٧
السلفادور		١٧
السنغال		١٨
كوبا		١٩

* A/58/150.

101003 101003 03-52338 (A)

أولا – مقدمة

١ – في الفقرة ٣ من القرار ٥٣/٥٧ المتعلق بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، دعت الجمعية العامة جميع الدول الأعضاء إلى مواصلة موافاة الأمين العام بآرائها وتقييماتها بشأن المسائل التالية: (أ) التقييم العام لمسائل أمن المعلومات؛ (ب) تعريف المفاهيم الأساسية المتصلة بأمن المعلومات، بما فيها التدخل دون إذن في نظم المعلومات والاتصالات السلكية واللاسلكية وموارد المعلومات أو إساءة استخدامها؛ (ج) مضمون المفاهيم الدولية ذات الصلة التي تهدف إلى تعزيز أمن النظم العالمية للمعلومات والاتصالات السلكية واللاسلكية. وفي الفقرة ٤ من القرار، طلبت الجمعية العامة إلى الأمين العام أن يبحث الأخطار القائمة والمحتملة في مجال أمن المعلومات والتدابير التعاونية التي يمكن اتخاذها للتصدي لها، وأن يجري دراسة بمساعدة فريق من الخبراء الحكوميين يتم إنشاؤه في عام ٢٠٠٤ ويعيَّن أعضاؤه على أساس التوزيع الجغرافي العادل، وكذلك بالتعاون مع الدول الأعضاء القادرة على تقديم تلك المساعدة، وأن يقدم تقريرا عن نتائج تلك الدراسة إلى الجمعية العامة في دورتها الستين.

٢ – وفي مذكرة شفوية مؤرخة ١٨ شباط/فبراير ٢٠٠٣، دُعيت جميع الدول الأعضاء إلى موافاة الأمين العام بآرائها وتقييماتها حول هذا الموضوع. وحتى هذا التاريخ، تم تلقي سبعة ردود ترد نصوصها مستنسخة في الفرع الثاني أدناه. وستصدر أي ردود أخرى في شكل إضافة لهذا التقرير.

ثانيا – الردود الواردة من الدول الأعضاء

الاتحاد الروسي

[الأصل: بالروسية]
[٢٨ نيسان/أبريل ٢٠٠٣]

المسائل المتصلة بعمل فريق الخبراء الحكوميين المعني بمشكلة أمن المعلومات

١ – وفقا لقراري الجمعية العامة ١٩/٥٦ المؤرخ ٢٩ تشرين الثاني/نوفمبر ٢٠٠١، و ٥٣/٥٧ المؤرخ ٢٢ تشرين الثاني/نوفمبر ٢٠٠٢، بشأن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، اللذين اعتمدا بتوافق الآراء، سيشهد عام ٢٠٠٤ تشكيل فريق خبراء حكوميين. وينص هذان القراران على تكليف فريق الخبراء الحكوميين بالنظر في الأخطار القائمة والمحتملة في مجال أمن المعلومات، وفي التدابير

التعاونية التي يمكن اتخاذها لمجابهتها، إجراء دراسة للمفاهيم الدولية، الرامية إلى تعزيز نظم المعلومات والاتصالات السلكية واللاسلكية العالمية، وتقديم تقرير عن نتائج هذه الدراسة إلى الجمعية العامة في دورتها الستين.

٢ - ويلاحظ الاتحاد الروسي أن أمن المعلومات الدولي يبقى من المسائل الهامة التي يتزايد الاحتياج إليها. ويفترض أن يشكل أمن المعلومات في الوقت الحاضر أحد الجوانب الهامة للأمن الوطني للدول، وأحد مكونات نظام مشترك للأمن الدولي والاستقرار الاستراتيجي. وترتبط استخدامات تكنولوجيات ووسائط المعلومات والاتصالات السلكية واللاسلكية ارتباطا مباشرا بصون الأمن العسكري والسياسي للبلدان على مستوى العالم، وتتطلب من ثم اتخاذ نهج عالمي شامل وبدون تمييز، يرتكز إلى مشاركة أكبر عدد ممكن من البلدان، في استعراض هذه المسألة، وتطبيق مبدأ المساواة في التمثيل الجغرافي.

٣ - وأفضل طريقة لكفالة هذا النهج هي العمل تحت إشراف الأمم المتحدة، إذ بوصفها منظمة دولية مركزية يتوفر فيها التمثيل الأفضل لمصالح جميع البلدان ولها دور تنسيقي في مجال نزع السلاح، تتيح فرصة إنشاء نظام متوازن وفعال للأمن العالمي.

٤ - ونحن نعتبر أن قرارات الجمعية العامة ٥٣/٧٠ المؤرخ ٤ كانون الأول/ديسمبر ١٩٩٨، و ٥٤/٤٩ المؤرخ ١ كانون الأول/ديسمبر ١٩٩٩، و ٥٥/٢٨ المؤرخ ٢٠ تشرين الثاني/نوفمبر ٢٠٠٠، و ٥٦/١٩ المؤرخ ٢٩ تشرين الثاني/نوفمبر ٢٠٠١، و ٥٧/٥٣ المؤرخ ٢٢ تشرين الثاني/نوفمبر ٢٠٠٢، كان لها دور فعال في فحص المجموعة الكاملة من قضايا أمن المعلومات الدولي، وكذلك في إعداد التوصيات ذات الصلة، وهي قرارات اُعتمدت كما جرت العادة بتوافق الآراء، ومن ثم فهي تعكس آراء المجتمع الدولي بأسره بشأن هذه المسألة، وتعكس كذلك مساهمات الدول المتعلقة بمسألة أمن المعلومات، والواردة في تقارير الأمين العام للأمم المتحدة (A/54/213، و A/55/140 و Corr.1 و Add.1، و A/56/164 و Add.1، و A/57/166 و Add.1).

٥ - ومما أدى دورا هاما في تحديد النهج الواجب اتباعه إزاء القضايا الراهنة المتصلة بأمن المعلومات الدولي الحلقة الدراسية التي نظمها حول هذا الموضوع معهد الأمم المتحدة لبحوث نزع السلاح بالاشتراك مع إدارة شؤون نزع السلاح التابعة للأمانة العامة للأمم المتحدة، وفقا للتوصيات الواردة في قرار الجمعية العامة ٥٣/٧٠ بشأن مسائل نزع السلاح وذلك في جنيف في آب/أغسطس ١٩٩٩ بمشاركة ممثلين عن أكثر من ٥٠ بلدا.

٦ - وأكدت الحلقة الدراسية الطبيعة الملحة لمسألة أمن المعلومات، وأوضحت أن الوقت قد حان لإدراجها في جدول الأعمال الدولي. وأتاحت الحلقة الدراسية أيضا فرصة لتحديد

النهج المختلفة تجاه استعراض جوهر المشكلة. إذ لا توجد في الوقت الراهن معايير أو أدوات دولية متعارف عليها ومناسبة، يمكن من خلالها استعراض مسائل أمن المعلومات، من وجهة نظر التدابير المتعلقة بتقليل المخاطر القائمة والمحتملة في هذا المجال على الصعيد العالمي.

٧ - وفي هذا الصدد، تتضح ضرورة دراسة المفاهيم والنُهج القائمة في هذا الشأن، بمشاركة أكبر عدد ممكن من البلدان، فضلا عن تحليل الأحكام القانونية الدولية، القائمة، المتعلقة بمختلف جوانب مسألة أمن المعلومات الدولي.

٨ - ونحن نتوقع أن تدخل المباحثات الدولية المتعددة الأطراف بشأن هذه الإشكالية مرحلة نوعية جديدة عندما يتم تشكيل فريق الخبراء الحكوميين المعني بمسألة أمن المعلومات. فهذا الفريق سيتيح للمجتمع الدولي فرصة نادرة لدراسة مجموعة المسائل المذكورة أعلاه بأكملها.

٩ - ويرغب الاتحاد الروسي في المشاركة بشكل بنّاء في أعمال فريق الخبراء الحكوميين، كما يود أن يعرب، في هذا الصدد، عن بعض الآراء المتعلقة بالمسائل التي يمكن أن تشكل، من وجهة نظرنا، جدول أعمال للفريق.

١٠ - ويتعين قبل كل شيء، عند النظر في مسألة أمن المعلومات الدولي، أن تكون المنطلقات ذات فائدة للبشرية جمعاء، مثل كفالة التبادل العالمي للمعلومات بشكل حر وآمن ومتساو في الحقوق على الصعيد الدولي، استنادا إلى معايير ومبادئ القانون الدولي المتعارف عليها.

١١ - وسيكون من الضروري أن يأخذ هذا الفريق في اعتباره، عند تصريف أعماله، المساهمات المستلمة من الدول وفقا لقرارات الجمعية العامة للأمم المتحدة بشأن أمن المعلومات الدولي، فضلا عن المواد الأخرى التي قد تُقدم لينظر فيها أعضاء الفريق.

١٢ - ونحن نرى أن الفريق يستطيع تركيز مداولاته على النقاط الأساسية التالية:

١٣ - أولا: تحقيق توافق الآراء بشأن الآلية المفاهيمية المناسبة في مجال أمن المعلومات الدولي. وقد تشمل الواجبات الهامة لفريق الخبراء الدوليين، في هذه المرحلة، إعداد تقسيمات أساسية وقاعدية لشبكات وموارد ونظم المعلومات وهياكلها الأساسية، والأسلحة المعلوماتية، فضلا عن توضيح طبيعة ومؤشرات وتصنيفات الأخطار التي تهدد أمن المعلومات وتقسيمها إلى فئات.

١٤ - ثانيا: استعراض العوامل المؤثرة في حالة أمن المعلومات الدولي. ويُعتبر أمن المعلومات الدولي مجالا صعبا ومعقدا، يستدعي أن يتخذ المجتمع الدولي إزاءه نهجا شاملا يأخذ في

الاعتبار وجود أخطار إرهابية وإجرامية وعسكرية، في المجالين العسكري والمدني على السواء.

١٥ - وتتسم تكنولوجيات المعلومات والاتصالات، في مجتمع المعلومات العالمي الناشئ، بالترابط فيما بينها وباختراقها للحدود. ونتيجة لذلك، يبدو أمن المعلومات الدولي، في إطار مجتمع المعلومات العالمي، مرتبطا بشكل وثيق وتلقائي بمسائل تحديد مصادر الخطر وما إذا كانت محلية أو خارجية، وبمسائل السيادة الوطنية للدولة، ومسائل احترام حقوق وحريات الإنسان، لا سيما حقه في عدم التدخل في حياته الخاصة. ويمكن أن تشكل هذه المسائل وغيرها في هذا الصدد أساسا للمناقشات التي تجري أثناء سير أعمال فريق الخبراء الحكوميين.

١٦ - ويمكن أن تتمثل الخطوة التالية في تحديد ما يمكن اتخاذه من تدابير مقبولة للجميع، للحيلولة دون استخدام تكنولوجيات ووسائط المعلومات في تحقيق الأهداف الإرهابية والإجرامية الأخرى، فضلا عن منع استخدام الأسلحة المعلوماتية، وعلى وجه الخصوص عندما تستهدف الهياكل الأساسية للدولة. وفيما يبدو، يمكن أن تتمثل مهام هذه المرحلة في استعراض إمكانية إعداد إجراءات للإبلاغ المتبادل ووقف تأثير تكنولوجيا المعلومات عبر الحدود بطريقة غير مقننة، وإنشاء نظام دولي للرصد بغية تتبع الأخطار التي تبرز في مجال المعلومات، وإقامة آلية لمراقبة استيفاء شروط نظام أمن المعلومات الدولي، وكذلك آلية لتسوية المنازعات في مجال أمن المعلومات؛ وتهيئة الظروف لإنشاء نظام عالمي للمصادقة على تكنولوجيات ووسائط المعلومات والاتصالات السلكية واللاسلكية (بما في ذلك ما يتصل منها بالبرمجيات)، بغية كفالة أمن المعلومات تحديدا.

١٧ - ويتعين التفكير في إمكانية إيجاد وسائل للتعاون على المستوى الدولي فيما بين أجهزة إنفاذ القانون، بشأن منع ووقف انتهاكات القانون في مجال المعلومات، لا سيما ما يتصل منها بالكشف عن مصادر الاعتداءات المعلوماتية؛ كما يتعين النظر في مسألة مواءمة التشريعات الوطنية لفرادى البلدان، وعلى وجه الخصوص المسائل التنظيمية المتعلقة بأمن المعلومات، ليتسنى وضع تصنيف موحد لانتهاكات القانون في مجال أمن المعلومات، وكذلك تحديد التبعات التي قد تنشأ عن ارتكاب أفعال مصنفة كأفعال إجرامية.

١٨ - ويُقتَرح أيضا تقييم إمكانية تقديم المساعدة على الصعيد الدولي، إلى البلدان التي تقع ضحية هجمات معلوماتية، بهدف تخفيف آثار الأضرار التي تلحق بتنفيذ مهام الأعمال العادية، لا سيما ما يلحق منها بالهياكل الأساسية الحيوية للدولة.

١٩ - وربما يأتي المستقبل بما يستدعي العمل من أجل إعداد صك قانون دولي متعدد الأطراف ومقبول لدى الجميع، يهدف إلى تعزيز نظام الأمن الدولي من الناحية القانونية،

وتتحمل بموجبه الدول والكيانات الأخرى الخاضعة للقانون الدولي مسؤولية دولية عن الأنشطة التي تجري في مجال المعلومات، سواء قامت هي بتنفيذها، أو نفذت في أقاليم خاضعة لولايتها القانونية.

٢٠ - ويرى الاتحاد الروسي أن الفكرة الأساسية وراء إقامة نظام عالمي لأمن المعلومات الدولي، ربما تمثلت في التزام الأطراف بعدم القيام بأعمال في مجال المعلومات، يكون الهدف منها هو إلحاق الضرر بشبكات أو نظم أو موارد أو أنشطة المعلومات التابعة لدولة أخرى، أو بالهياكل الأساسية التابعة لها، أو تخريب النظم السياسية والاقتصادية والاجتماعية، أو التأثير النفسي في قطاعات واسعة من السكان، بهدف زعزعة استقرار المجتمع والدولة.

أوكرانيا

[الأصل: بالروسية]
[٢٧ أيار/مايو ٢٠٠٣]

١ - التقييم العام للمسائل المتعلقة بأمن المعلومات

١ - تعتبر عملية العولمة الجارية على الصعيد الدولي، وإدخال تكنولوجيات المعلومات الجديدة، وظهور مجتمع المعلومات عوامل تؤكد كلها أهمية أمن المعلومات باعتباره عنصرا من عناصر الأمن القومي.

٢ - وتنشأ عن وضع الهياكل الأساسية للمعلومات وتطوير تكنولوجيات المعلومات الجديدة وإدخالها إلى دولة من الدول مخاطر تحدق بأمن المعلومات. ومن أعظمها التهديدات المتعمدة التي قد تنجم عن اختلافات موضوعية أو ذاتية بين مصالح أفراد معنيين من النواحي الروحية أو الفكرية أو المادية وعن سبل الوفاء بتطلعاتهم، مما يؤدي أحيانا إلى ظهور حالات صراع.

٣ - وتشمل المخاطر الرئيسية المحدقة بأمن المعلومات ما يلي:

- التلاعب بالمعلومات (من قبيل تضليل الجمهور أو إخفاء المعلومات أو تحريفها)؛
- انتهاك الأساليب المحددة لتبادل المعلومات أو الوصول إلى موارد المعلومات دون إذن أو فرض القيود على الوصول إليها دون مبرر، أو جمع المعلومات أو استخدامها بشكل غير مشروع؛
- تدمير فضاء المعلومات التابع للدولة أو استخدامه في أعمال مناوئة لها؛

- إرهاب الإعلام، على سبيل المثال، من خلال نشر الفيروسات الحاسوبية، ووضع برامج وأجهزة التنصت، وتركيب أجهزة التقاط الترددات اللاسلكية لاستقبال المعلومات من المباني أو المرافق التقنية، واستخدام نظم المعلومات والاتصالات السلكية واللاسلكية وموارد المعلومات بشكل غير مشروع، ونشر المعلومات الكاذبة وما إلى ذلك.

٤ - ومن بين النتائج المباشرة المترتبة على الاستخدام السلبي للمعلومات التضليل الذي يؤدي إلى تحريف معلومات الدولة وموارد معلوماتها و/أو تدميرها وكذلك عجز النظم الحكومية أو الصناعية أو المالية أو الأكاديمية أو الثقافية الهامة عن أداء وظيفتها، وتكون النتيجة هي فقدان السيادة على المعلومات.

٥ - ويتضح من بحث المسائل المتعلقة بأمن المعلومات أنه، بالاضافة إلى المشاكل العامة، هناك مشاكل تتعلق بالحفاظ على نوعية موارد المعلومات ونطاقها، ووضع استراتيجيات استخدامها بالتوازي مع تكنولوجيا المعلومات، وإنشاء هياكل أساسية كافية للمعلومات وصون أمن المعلومات في إطار نظم المعلومات والاتصالات السلكية واللاسلكية ومكافحة الأنشطة السلبية التي تؤثر في الفرد والمجتمع والدولة ككل.

٦ - وقد يؤدي عدم كفاية الحماية المتاحة لموارد المعلومات بالدولة إلى تكبد أضرار اقتصادية فادحة من جراء هبوط قيمة قطاع تجارة تكنولوجيا المعلومات والتكنولوجيا الصناعية وتدنيه، فضلا عن الأضرار الكبرى التي تلحق بالأمن القومي ككل من جراء الأعطال التي يحتمل أن تعرقل السير العادي لنظم الاتصال والرصد والإدارة، وتسرب المعلومات المتعلقة بأسرار الدولة وما شابهها.

٧ - ويتوقف أمن المعلومات على مدى اتخاذ تدابير لحماية المعلومات في جميع المراحل. ويهدف أمن المعلومات إلى كفالة سلامة النظم وضمان دقة المعلومات ومصداقيتها والتخفيف من حدة الآثار التي قد تنجم عن تحريف المعلومات أو تدميرها.

٨ - ومن بين سمات العالم الحديث استخدام نظم المعلومات المحلية والعالمية، في مختلف ميادين الأنشطة الاجتماعية والحكومية، للإسراع بتبادل المعلومات والحصول على مختلف موارد المعلومات.

٩ - وقد أتاح استخدام هذه النظم على نطاق واسع، لا سيما في ميادين النشاط المتصلة بإدارة شؤون الدولة، فرصا حقيقية للوصول دون إذن إلى موارد المعلومات الحكومية ونظم مراقبتها لنشر معلومات خاطئة والإخلال بمصداقية المعلومات وإمكانية الوصول إليها، وما إلى ذلك.

١٠ - ويتوقف الاستقرار في الميادين السياسية والاقتصادية والعسكرية والمالية وغيرها من ميادين النشاط الحكومي على مدى موثوقية نظم المعلومات والاتصالات السلكية واللاسلكية وفعاليتها. فحيثما ينشأ فضاء للمعلومات تكتسي موثوقية وحماية نظم المعلومات والاتصالات السلكية واللاسلكية التي تخدم مصالح الإدارة الحكومية أهمية واعتبارا بشكل خاص. فالوصول إلى نظم المعلومات لا يتيح توافر معلومات قيمة فحسب بل قد يتيح، من خلال ما يوفره من سبل للإخلال بالنظم أو عرقلتها، تجميد الأنشطة كليا أو جزئيا في قطاعات هامة إن لم يكن في جميع قطاعات الاقتصاد، والتأثير سلبا في موارد المعلومات ونشر معلومات محظورة بموجب القانون، وما إلى ذلك.

١١ - ويعتبر كفالة أمن المعلومات المتضمنة في نظم المعلومات والاتصالات السلكية واللاسلكية عاملا من العوامل الرئيسية وشرطا لازما لضمان أمن المعلومات وكفالة السيادة الوطنية وسيادة الدولة وتحقيق التنمية الاجتماعية المستقرة.

١٢ - وتشمل المخاطر الرئيسية المحدقة بالمعلومات المتضمنة في نظم المعلومات والاتصالات السلكية واللاسلكية في الوقت الراهن ما يلي:

- الإخلال بسير نظم المعلومات والاتصالات السلكية واللاسلكية الهامة؛
- ارتكاب أعمال متعمدة أو غير متعمدة تؤدي إلى الإخلال بسرية المعلومات ومصداقيتها وإمكانية الحصول عليها؛
- التدخل دون إذن في نظم المعلومات (من خلال نشر الفيروسات الحاسوبية، وتركيب برامج وأجهزة التنصت واستخدام أجهزة التقاط المعلومات من المباني والمرافق التقنية، والتقاط المعلومات وحل شفراتها، ونشر المعلومات الخاطئة، والتقاط الترددات اللاسلكية للتدخل في نظم الكلمات السرية الرئيسية، وتشويش خطوط الاتصال ونظم المراقبة، وما إلى ذلك).

١٣ - ولا يمكن أن توفر نظم المعلومات والاتصالات السلكية واللاسلكية، ولا سيما تلك المستخدمة في الإدارة الحكومية، حماية موثوقة من الانتهاكات الجنائية إلا بإنشاء نظام مركب لحماية المعلومات يشمل استخدام تقنيات شفرية واتخاذ تدابير تقنية، وكذا طائفة من النهج التنظيمية والتقنية.

١٤ - وينبغي إيلاء اهتمام خاص لمسألة ربط الشبكات الحاسوبية بشبكات المعلومات الدولية.

١٥ - ولا يمكن لأوكرانيا أن تصبح عضوا كاملا في المجتمع الدولي دون تعزيز التعاون مع الشبكات العالمية لتبادل المعلومات من قبيل شبكة الإنترنت. فهذه النظم توفر طائفة واسعة من خدمات المعلومات والاتصالات السلكية واللاسلكية الحديثة التي يعلن العديد منها توفير حماية المعلومات.

١٦ - وفي الوقت ذاته، يشكل الكم الهائل من الأجهزة المستخدمة في تلك النظم، وسماتها التي يصعب بل يستحيل تقييمها دون الرجوع إلى رموز برمجتها، تهديدا خطيرا لأمن المعلومات والمعاملات المالية والمدفوعات الإلكترونية. وثمة حالات لا حصر لها تهورت فيها مصارف فاستخدمت تكنولوجيات مستوردة قد تتيح لخبير اختراق نظامها في ١٠ دقائق.

١٧ - ويجب إيلاء الاهتمام للمخاطر التي تنشأ عندما يتم ربط حواسيب خدمة الشبكة والشبكات المحلية بالشبكات العالمية دون إعداد مسبق. ومن اليسير على قراصنة الحاسوب، من الناحية العملية، أن يخترقوا أي شبكة حاسوبية محلية مرتبطة بشبكة إنترنت إذا لم تزود بآليات الحماية اللازمة.

١٨ - وقد اقترنت الوسائل والسبل الجديدة المتاحة لنقل المعلومات بين البلدان، وبخاصة زيادة شعبية الأشكال الجديدة المتوفرة لإنشاء المشاريع عن طريق استخدام شبكة إنترنت (التجارة الإلكترونية)، والتطبيق التدريجي لنظم المراقبة الإلكترونية، باستخدام التكنولوجيات الحاسوبية على نطاق واسع وباتساع نطاق المعلومات المتاحة في شكل إلكتروني. ونتيجة لذلك، باتت مواد وصلات المعلومات تعتمد أكثر فأكثر على درجة الحماية المتاحة لتلك المعلومات التي تستهدفها العناصر السلبية في المجتمع ومن يتعاون معهم. ويتيح عدم اتساق نظم وآليات الحماية القائمة إمكانية حقيقية للقيام دون إذن بالوصول إلى المعلومات التي تم إنشاؤها أو تجهيزها أو تحويلها أو تخزينها في شكل إلكتروني، أو باستخدام تلك المعلومات أو عرقلتها أو تحريفها.

١٩ - ويكتسي مشكل التدخل في موارد المعلومات الحكومية أهمية كبرى في جميع أنحاء العالم. وإذا كانت المسألة الجوهرية قبل التسعينات هي حماية الدولة من التجسس الأجنبي، فإن مشكلة مكافحة ما يسمى بالجريمة الحاسوبية بات في السنوات الأخيرة أكثر إلحاحا بسبب انتشار تكنولوجيا المعلومات على نطاق واسع في جميع ميادين الحياة المجتمعية. ولا أدل على ذلك من أن الجريمة الحاسوبية أصبح يعترف بها دوليا كشكل جديد من أشكال الجريمة الفكرية. وعلاوة على ذلك، فإن هذا النوع من الجريمة لا ترتكبه جماعات إجرامية منظمة فحسب بل كذلك أفراد ومنظمات إرهابية.

٢٠ - وما يجتذب المجرمين بوجه خاص نظم المعلومات التي تستخدمها أجهزة الحكومة، وأجهزة إنفاذ القانون، ومصالح الجمارك والضرائب، ومؤسسات المال والائتمان، والجيش. ففي أوكرانيا، كشفت وكالات إنفاذ القانون في أكثر من مناسبة عمليات غير قانونية استخدمت فيها بطاقات بلاستيكية في نظم الدفع الدولية وعمليات دفع إلكترونية صورية هدفها الحصول بطريقة غير قانونية على الأموال أو التدخل بدون إذن في أنشطة الشبكات الحاسوبية عن طريق شبكة إنترنت، وما إلى ذلك.

٢ - تعريف المفاهيم الأساسية لأمن المعلومات، بما في ذلك التدخل غير المأذون في نظم المعلومات أو الاتصالات السلكية واللاسلكية أو في موارد المعلومات أو استخدامها على نحو غير مشروع

٢١ - يؤدي التطوير المكثف لتكنولوجيات المعلومات والاتصالات السلكية واللاسلكية إلى تفاقم مشكلة كفالة أمن المعلومات، بما في ذلك مسألة التدخل غير المأذون في نظم المعلومات أو الاتصالات السلكية واللاسلكية أو استخدامها على نحو غير مشروع ومسألة حماية موارد المعلومات.

٢٢ - وفي هذا السياق لا بد من فهم مصطلح ''أمن المعلومات'' بوصفه نوعا من الحماية لمجال المعلومات الخاص بالدول الذي يتيح تحقيق مصالحها الوطنية ومراعاة حقوق الفرد والمجتمع والدولة.

٢٣ - وفي ضوء المخاطر الاجتماعية التي لا يستهان بها المصاحبة للأنشطة غير المشروعة المذكورة آنفا وأهمية عمل نظم المعلومات والاتصالات السلكية واللاسلكية على نحو يتسم بالكفاءة، يعرف القانون الجنائي الأوكراني الجرائم المرتبطة باستخدام الحواسيب والنظم أو الشبكات الحاسوبية ويحدد العقوبات المنصوص عليها مقابل ارتكاب هذه الجرائم، على النحو التالي تحديدا:

- التدخل غير المشروع في عمل الحواسيب أو النظم أو الشبكات الحاسوبية: الأعمال التي تسفر عن تشويه المعلومات الحاسوبية أو وسائل نقل تلك المعلومات أو تدميرها أو عن نشر فيروسات الحاسوب عن طريق برامج حاسوبية أو غيرها من الوسائل التقنية بغرض الدخول على نحو غير مشروع إلى الحواسيب أو النظم أو الشبكات الحاسوبية؛

- سرقة المعلومات الحاسوبية أو الاستيلاء عليها أو الحصول عليها بالابتزاز أو عن طريق الخداع أو إساءة استغلال منصب رسمي؛

- انتهاك قواعد تشغيل الحواسيب أو النظم أو الشبكات الحاسوبية الآلية من قبل شخص مسؤول عن تشغيل تلك الحواسيب أو النظم أو الشبكات: الأعمال التي تسفر عن سرقة المعلومات الحاسوبية أو وسائل حماية تلك المعلومات أو تشويهها أو تدميرها، أو عن النسخ غير المشروع للمعلومات الحاسوبية، أو عن تعطيل كبير لعمل الحواسيب أو النظم أو الشبكات الحاسوبية.

٢٤ - وباختصار، يجوز تعريف مصطلح ''الجريمة الحاسوبية'' بأنه الفعل غير المشروع الذي يتعدى على الإجراءات المتبعة لتشغيل نظم تكنولوجيا المعلومات أو إجراءات الوصول إليها أو الذي يضر بسلامة المعلومات أو سريتها أو إمكانية الوصول إليها وبحقوق المواطنين وحرياتهم خلال عمليات تكنولوجيا المعلومات.

٣ - مضمون المفاهيم الدولية الرامية إلى تعزيز أمن النظم العالمية للمعلومات والاتصالات السلكية واللاسلكية

٢٥ - سيُسجل القرن الحادي والعشرون في التاريخ بوصفه الفترة التي شهدت مولد مجتمع المعلومات العالمي وتطوره والتي وحدت بين العمليات المادية وعمليات تكنولوجيا المعلومات أو مدت نطاق الأولى إلى الثانية، والتي ساعدت على تحقيق تحسن ذي شأن في إنتاجية العمل والرفاه الاجتماعي. وهناك بلدان عديدة أخذت تنشئ بالفعل الأسس التنظيمية والتقنية للهياكل الأساسية الوطنية والعالمية. وتتناول الأمم المتحدة مسألة إعمال الحق في الوصول إلى وسائل الاتصال والمعلومات الأساسية في الإعلان العالمي لحقوق الإنسان.

٢٦ - وتجربة البلدان المتقدمة النمو في مجال إيجاد حلول فعالة لمشاكل نشر تكنولوجيا المعلومات في النصف الثاني من التسعينات، التي جمعتها رسميا منظمات دولية (الاتحاد الدولي للاتصالات السلكية واللاسلكية، المنظمة الدولية لتوحيد المقاييس/اللجنة الإلكترونية - التقنية الدولية، المعهد الأوروبي لمعايير الاتصالات السلكية واللاسلكية) والعديد من المنظمات الوطنية لتوحيد المقاييس، تدل على الحاجة إلى إنشاء هياكل أساسية متعددة المستويات (على الصعيدين الوطني والإقليمي) لتكنولوجيا المعلومات، وجمعها بعد ذلك في الهيكل الأساسي العالمي لتكنولوجيا المعلومات.

٢٧ - ومشاركة أوروبا في الهيكل الأساسي العالمي لتكنولوجيا المعلومات لا تعني إنشاء هياكل أساسية وطنية للمعلومات داخل المنطقة الأوروبية وحسب، بل أيضا المساعدة على بناء تلك الهياكل الأساسية في فرادى البلدان من أجل المصلحة المشتركة لكل بلد في أوروبا ككل. وبدلا عن الحديث عن ''هيكل أساسي أوروبي للمعلومات''، يفضل الأوروبيون استخدام مصطلح ''مجتمع المعلومات الأوروبي''. ولبنات بناء مجتمع المعلومات الأوروبي هي

الخدمات الأساسية والإضافية التي تقدمها شبكاته. ويمكن تعزيز الشبكات الأوروبية القائمة باستحداث قناة معلومات أوروبية فائقة السرعة وعريضة النطاق، تجمع في كيان واحد جميع الخدمات الأوروبية للاتصالات السلكية واللاسلكية وشبكات التلفزة السلكية وأنظمة السواتل. وتؤيد البلدان الأوروبية استخدام خدمات أساسية عابرة لأوروبا، بما في ذلك خدمات البريد الإلكتروني وبث الملفات وتسجيلات الفيديو.

٢٨ - وتكرس البلدان الأوروبية أيضا اهتماما كبيرا بالجانب الاجتماعي للمرحلة المقبلة من الثورة التكنولوجية العالمية. وأصدر مجلس أوروبا قرارات ووثائق بشأن وضع سياسات وطنية تتعلق ببناء مجتمع المعلومات. ولا ينظر إلى ذلك بوصفه مجاراة للنمط السائد، بل بوصفه شرطا ضروريا للتطور، سيؤدي تجاهله إلى فقدان الزخم والتراجع عن الصدارة في المواقف الاقتصادية والتكنولوجية.

٢٩ - والاتجاهات العالمية في التنظيم القانوني للأنشطة المرتبطة بأحدث تكنولوجيات البث تشهد على الحاجة إلى صياغة نُهُج موحدة إزاء وضع صكوك تشريعية وتوحيدية لجميع المشاركين في التبادل الدولي للمعلومات. وفي رأي رابطة الحقوقيين الأمريكيين، يوجد بالفعل اليوم طلب حقيقي من أجل إنشاء هيئة متعددة الجنسيات معنية بالتشريع المتعلق بالفضاء الحاسوبي. وإنشاء ''محكمة حاسوبية'' يمثل أحد أهم العناصر في قائمة المسائل الموصى بأن تنظرها الهيئة التي ستنشأ في المستقبل. وفي المرحلة الحالية، تتمثل المشكلة الرئيسية للتشريعات المتعلقة بأمن المعلومات في الحاجة إلى تكييف القواعد القانونية الحالية مع أوجه التقدم في تكنولوجيا المعلومات.

٣٠ - ويستحيل اليوم تخيل فضاء معلوماتي بدون شبكات حاسوبية. وهذه التكنولوجيا هي التي تسببت تحديدا في بروز وتطور العديد من أنواع الأنشطة التجارية: بطاقات المحاسبة الإلكترونية، والتسوية التشغيلية بين المصارف، وخدمات سوق الأوراق المالية، وخدمات السمسرة، وما إلى ذلك.

٣١ - ويُتوقع بحول عام ٢٠٠٥ أن يتاح الوصول إلى شبكة إنترنت أمام نصف سكان الاتحاد الأوروبي. ومن ثم فإن بلدان الاتحاد الأوروبي توجه جهودها نحو بناء الثقة في العمليات التجارية والمالية عن طريق شبكة إنترنت وتحث الخطو للتحول إلى التجارة الإلكترونية.

٣٢ - وفي ٧ أيار/مايو ١٩٩٩، توصل البرلمان الأوروبي إلى اتفاق بشأن مشروع لصك ''الشرطة الحاسوبية'' لعام ١٩٩٨، يأذن للوكالات المختصة بالشروع قانونا في الرصد الشبكي. وتعلق الأمر في الواقع بمشروع قرار للمجلس بشأن الاعتراض المشروع للاتصالات

السلكية واللاسلكية فيما يتصل بالتكنولوجيات الجديدة. وتدعو هذه الوثيقة إلى تمكين الوكالات التي تقوم بالرصد من الوصول إلى جميع شبكات الاتصالات السلكية واللاسلكية في الوقت الحقيقي، بما في ذلك شبكة إنترنت وأنظمة الاتصال الهاتفي بالسواتل. وبدأت حكومة المملكة المتحدة في تنفيذ مشروع متعلق بإنشاء مركز معني باعتراض كل الاتصالات الإلكترونية في البلد.

٣٣ - وتسيطر حكومة الصين على الوصول إلى الشبكة بمنح تراخيص لاستخدام أجهزة المودم، وتمر جميع تدفقات معلومات شبكة إنترنت عبر عدد محدود من جهات التشغيل الوطنية.

٣٤ - ويمكن استرعاء الانتباه إلى المشاكل التالية المتعلقة بأمن المعلومات:

- التعدي على حقوق الملكية الفكرية؛
- نشر المعلومات ذات الأثر الضار على صحة الناس الاجتماعية، بما في ذلك المشاكل المرتبطة بوصول الأطفال إلى شبكة إنترنت؛
- إجراء العمليات التجارية غير المشروعة؛
- الوصول غير المأذون إلى المعلومات السرية؛
- التعدي على حقوق الأفراد ومصالحهم المشروعة خلال تبادل المعلومات؛
- نشر الإعلانات المتدنية المستوى.

٣٥ - وهناك خطر آخر يرتبط بشبكة إنترنت، وهو إمكانية استخدام معلومات الأشخاص السرية بدون إذنهم. ومن الممكن الحصول على هذه المعلومات بتحليل استخدام الأشخاص لشبكة إنترنت.

٣٦ - وشبكة إنترنت وسيلة محددة جدا للاتصال يصعب إخضاعها، بسبب طابعها العابر للحدود، للتنظيم القانوني. وجميع مستخدمي شبكة إنترنت خاضعون لقوانين بلد كل منهم. بيد أن المحتوى غير المشروع يمكن أن يعرض في إقليم بلد غير البلد الموجود فيه حاسوب الخدمة. ووجود اتفاقيات دولية أمر أساسي من أجل تنظيم العلاقات القانونية المتصلة بشبكة إنترنت، بيد أن اعتماد تلك الاتفاقات يتعقد بدوره نتيجة لتعدد النُهُج التي تتبعها التشريعات الوطنية إزاء مختلف أنواع الجرائم. وعلى سبيل المثال، فإن مفهوم ''المواد الخليعة'' يخضع لتفسيرات مختلفة. واليوم نجد أن الاتجاه العام في المبادرات القانونية المتصلة بشبكة إنترنت هو صوب إنشاء مسؤولية موفري خدمات الاستضافة عن محتوى المعلومات الموجودة في

حواسيبهم. ولما كانت هذه مسألة معقدة للغاية من وجهة النظر التقنية، فإن تشريعات بعض البلدان تُخضع إنشاء المسؤولية لموفري الخدمات لشرط وعيهم بمحتوى المعلومات غير المشروعة.

٣٧ - وقد أبلغت المنظمة الدولية للشرطة الجنائية (إنتربول)، التي تشمل عضويتها وكالات إنفاذ القانون من ١٧٨ بلدا، بأنها ستنشر معلومات عن جرائم شبكة إنترنت على موقع شركة ''أتوميك تانجرين'' "Atomic Tangerine" الأمريكية. وتوفر منظمة إنتربول معلومات عن مخترقي الأنظمة الحاسوبية وأنواع الجرائم التي تهدد الشركات المشاركة في الأنشطة الاقتصادية. وشركة أتوميك تانجرين، بدورها، يجب عليها أن تحيل إلى منظمة إنتربول المعلومات التي يتم الحصول عليها عن طريق نظام "NetRadar" للإنذار المبكر المملوك للشركة والمصمم لرصد شبكة إنترنت.

٣٨ - والاتصالات المجهولة المصدر تمثل إحدى أهم المشاكل، حيث إنها تعقد تحديد هوية صاحب المعلومات غير المشروعة ومحاكمته، بل وتجعل ذلك أمرا مستحيلا أحيانا. ومن ثم فإن خبراء من بلدان عديدة يقترحون فرض حظر قانوني على الاتصالات المجهولة المصدر وإن سمح في الوقت نفسه بإجراء الاتصالات بأسماء مستعارة، حيث أنه يتسنى، عند الضرورة، تحديد مصادر تلك الاتصالات.

٣٩ - وفي ٢١ كانون الأول/ديسمبر ١٩٩٨، اعتمد مجلس الاتحاد الأوروبي خطة عمل لزيادة الأمان في شبكة إنترنت اقترحها البرلمان الأوروبي. وطبقت هذه الخطة لفترة أربع سنوات (من ١ كانون الثاني/يناير ١٩٩٩ إلى ٣١ كانون الأول/ديسمبر ٢٠٠٢). وتوفرت لها ميزانية تبلغ ٢٥ مليون يورو. واقترحت الخطة إنشاء مجموعة منوعة من معايير النوعية لشبكة إنترنت يجري وضعها وفقا للنقاط المرجعية للشبكة بشأن المنتجات. وكان من المقرر إدماج هذه الأحكام في التشريعات الوطنية وفي مدونات التنظيم الشخصي لمقدمي خدمات شبكة إنترنت في آن واحد. وفي آذار/مارس ١٩٩٩، اعتمدت اللجنة الأوروبية، عقب مناقشة أحكام التقرير بشأن التقارب بين قطاعات تكنولوجيا الاتصالات السلكية واللاسلكية ووسائط الإعلام والمعلومات، تقريرا يتضمن الخلاصة الأساسية التالية: إن التنظيم القانوني لشبكة إنترنت يجب أن يتسم بالشفافية، والوضوح، والتناسب.

بوليفيا

[الأصل: بالإسبانية]
[١٧ حزيران/يونيه ٢٠٠٣]

التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي

١ - تعرب بوليفيا عن قلقها من أن يُستخدم تطور التكنولوجيا لأغراض تتعارض مع الاستقرار والأمن الدوليين فتؤثر سلبيا في سلامة الدول وتضر بأمنها العسكري والمدني.

٢ - وتؤكد بوليفيا ضرورة منع استخدام الموارد التي تتيحها تكنولوجيا المعلومات في أغراض إجرامية أو إرهابية.

٣ - وفي هذا الصدد، تعرض بعض المعايير الأساسية المتصلة بأمن المعلومات والتدخل غير المأذون به في النظم ذات الصلة:

أهمية المعلومات

٤ - عند الحديث عن المعلومات بشكل مباشر أو غير مباشر نقصد النظم الحاسوبية والاتصالات السلكية واللاسلكية (التكنولوجيات الجديدة وتطبيقات البرمجيات الجديدة والمعدات الحاسوبية الجديدة والأشكال الجديدة لتجهيز المعلومات بمزيد من الاتساق والموثوقية والسرعة)، مع إيلاء الاعتبار أساسا لأمن النظم والأخطار التي يمكن أن تتعرض لها.

٥ - ومن الضروري ألا يغيب عن الأذهان أن المكان الذي تتمركز فيه المعلومات غالبا يمكن أن يكون ذا أهمية قصوى، وفي نفس الوقت، معرضا جدا للخطر.

٦ - والاتصالات السلكية واللاسلكية معرضة بشدة للخطر، وبخاصة شبكة الإنترنت والاتصالات الهاتفية. فشبكة الإنترنت مرتبطة مباشرة بالنظم الحاسوبية؛ أما الاتصالات الهاتفية فتشمل الهاتف الخلوي والهاتف الثابت. والاتصال عن طريق الهاتف الخلوي يعني الاستخدام المباشر لفضاء إرسال مشترك (عن طريق الموجات اللاسلكية)، حيث يجد المستعمل نفسه وسط حركة الاتصالات ومكالمته معرضة ليلتقطها غيره.

الخلفية التاريخية للجرائم الحاسوبية

٧ - لقد شهدت الجرائم العارضة التي يُستخدم في ارتكابها الحاسوب أو أجهزة الاستقبال زيادة من حيث عددها وأشكالها وتنوعها. والواقع أن نسبة مئوية كبيرة من هذه الجرائم تُكتشف عن طريق الصدفة (عمليات الغش والتزوير وبيع المعلومات).

٨ - وفيما يتصل بإدارة النظم الحاسوبية، نذكر الفيروس الحاسوبي بوصفه برنامجا وُضع خطأ أو عمدا ويتطلب اهتماما خاصا ويجب التصدي له عن طريق أساليب تشغيلية دقيقة.

٩ - وفيما يتصل بالجرائم، من المهم التشديد على أنه عند وجود المشاكل يجب التصدي للسبب والبحث فورا عن حلول. ومن بين أخطر الأسباب نذكر: المنفعة الشخصية، والتشبه بروبن هود، وكراهية المؤسسة، واختلال المدارك العقلية، والغش، أما الأسباب الأقل خطرا فمنها فائدة المؤسسة، والألعاب.

المفاهيم التنظيمية المتصلة بالأمن

١٠ - تؤدي المفاهيم دورا هاما في فلسفة العلم الحالية، إذ تتوقف عليها القواعد التي تنظم الأبحاث.

١١ - ومن المفاهيم الرئيسية الكثيرة يمكن أن نذكر ما يلي: مسؤولية مراجعة نظام ما يتحملها المستعمل وإدارة المراجعة الداخلية، ونظم الأمن لا تأخذ في الاعتبار إمكانية الغش الداخلي، والحوادث العارضة ليس من المحتمل أن تقع للمؤسسة، وهناك دائما مواطن قصور بحيث لا يوجد نظام خال من العيوب.

إثبات وجود الأخطار

١٢ - من المهم توعية المستعملين في المؤسسة بالخطر الذي قد تتعرض له المعلومات وبأن الأمن جزء من عملهم. ولهذا الغرض، ينبغي تحديد تكلفة نظام الأمن ونوعيته، وتصنيف تركيبه من حيث الأخطار، وتحديد التطبيقات المحفوفة بخطر كبير، والقيام بتحديد كمي لأثر وقف التشغيل، واتخاذ التدابير الأمنية اللازمة.

١٣ - ومتى تحددت درجة الخطر، يجب وضع قائمة بالتدابير الوقائية التي ينبغي اتخاذها وبالتدابير التصحيحية في حالة حدوث عطل كبير، مع الإشارة إلى أولوية كل واحد من هذه التدابير.

١٤ - ويجب دراسة الأخطار وتحديدها كميا على صعيد المؤسسة والدولة وعلى الصعيد الإقليمي، مع الإشارة إلى برامج الدعم من حيث توافرها وإمكانية استرداد البيانات.

ما يجب أن يراعى في نظام أمن شامل

١٥ - إن استحداث نظام أمن يعني ''تخطيط وتنظيم وتنسيق وإدارة ومراقبة الأنشطة المتصلة بتوفير الموارد المستخدمة في التطبيقات الحاسوبية وكفالة سلامتها، وكذلك المحافظة على أصول المؤسسة والدولة والمنطقة''.

١٦ - ولهذا الغرض، علينا تحديد العناصر الإدارية وسياسات الأمن وتنظيم المسؤوليات وتوزيعها ووضع الإجراءات المتصلة بالطوارئ وتحديد الأهداف الأمنية وإجراء تشخيص لحالة الخطر وأمن المعلومات، وختاما وضع برنامج أمن.

جورجيا

[الأصل: بالانكليزية]
[٢٤ حزيران/يونيه ٢٠٠٣]

١ - شرعت حكومة جورجيا في إعداد استراتيجية إعلامية وطنية تهدف إلى تطوير قطاع الاتصالات السلكية واللاسلكية وتطوير التكنولوجيات الجديدة، مع القيام في الوقت نفسه بإبراز أهمية السياسات الحكومية في إتاحة فرص استخدام تكنولوجيات الإعلام.

٢ - وعلاوة على ذلك، تنتهج حكومة جورجيا، إدراكا منها كذلك لجميع المخاطر والتحديات القائمة في مجال أمن المعلومات، سياسات رامية إلى إدماج جورجيا في مجتمع المعلومات العالمي.

٣ - وترى حكومة جورجيا أن المشاركة في البرامج والمشاريع التعاونية الدولية الرامية إلى إنشاء مجتمع معلومات دولي أكثر أمانا تكتسي أهمية قصوى، وذلك إدراكا منها أنه من المستحيل معالجة المسائل المتعلقة بأمن المعلومات بصورة انفرادية، بالنظر إلى الواقع الحالي لتكنولوجيات ونظم المعلومات، فضلا عن خصائص المنطقة التي تقع فيها جورجيا.

السلفادور

[الأصل: بالإسبانية]
[٣٠ حزيران/يونيه ٢٠٠٣]

رد حكومة السلفادور بشأن القرار ٥٣/٥٧

"التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي"، الفقرة ٣ من المنطوق

١ - يُحظر التشويش واعتراض المكالمات الهاتفية بموجب المادة ٢٤ من دستور الجمهورية، وهو الإطار الدستوري السائد حاليا في السلفادور فيما يتعلق بأمن المعلومات والاتصالات السلكية واللاسلكية.

٢ - وبهذا الشأن تُجرِّم المواد ١٨٤ و ١٨٥ و ١٨٦ و ٣٠٢ من القانون الجنائي الاستيلاء على مراسلات خطية أو برمجيات أو غيرها من الوثائق أو الأمتعة الشخصية غير الموجهة للجهة التي استولت عليها أو وضع اليد على بيانات خاصة ذات طابع شخصي أو أسري؛ والأفعال التي يلجأ فيها إلى التقاط المراسلات، مثل اعتراض أو قطع المراسلات البرقية أو الهاتفية والتشويش عليها والتدخل فيها، باستخدام وسائل تقنية للتنصت على تلك المراسلات أو تسجيلها.

٣ - ولا تُجرَّم الحالات المذكورة عند صدور تهديدات، بما يتطلب إنقاذ شخص محتجز أو مختطف أو عندما يتعلق الأمر بالجريمة المنظمة، لدى توجيه المجني عليه أو ممثله، عند الاقتضاء، طلبا خطيا إلى المدعي العام للجمهورية أو إصداره إذنا خطيا له بالتنصت على المحادثات أو الأفعال التي تتضمن تهديدات أو مطالبات.

٤ - ويدخل تحديد نطاق سريان الإطار التنظيمي للاتصالات السلكية واللاسلكية وفرض جزاءات إدارية ضمن صلاحيات الهيئة العليا العامة للكهرباء والاتصالات السلكية واللاسلكية، وفقا للمادة ٤ من قانونها التأسيسي والفقرة (ب) من المادة ٢٩ من قانون الاتصالات السلكية واللاسلكية، التي تنص على حماية سرية المراسلات.

٥ - وخلال عامي ٢٠٠١ و ٢٠٠٢، عرض على الجمعية التشريعية مقترح لإصلاح دستور الجمهورية، بغرض السماح بالتشويش و/أو التدخل الهاتفيين، بوصفهما آلية تساعد على مكافحة الجريمة المنظمة والاتجار بالمخدرات، وهو مقترح لم يوافق عليه حتى الآن.

السنغال

[الأصل: بالفرنسية]
[٩ حزيران/يونيه ٢٠٠٣]

١ - التدابير المتعلقة بالأمن المعلوماتي تدخل ضمن مجال تبادل المعلومات، وعلى الخصوص المتعلقة منها بتداول الأسلحة. وهي معلومات ينبغي أن يضفى عليها طابع سري.

٢ - وتبعا لذلك، ينبغي ضمان أمن تلك المعلومات باتخاذ عدد من التدابير منها ما يلي:

- ضمان أمن المعدات والبرمجيات ووسائل التجهيز المعلوماتية عن طريق وضع آليات تقنية ملائمة.
- ضمان أمن الإجراءات المتعلق بتبادل المعلومات عن طريق وضع أنظمة دقيقة وفريدة.

كوبا

[الأصل: بالاسبانية]
[٢٨ أيار/مايو ٢٠٠٣]

١ - أيدت كوبا دواما القرارات المتخذة بشأن ''التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي'' منذ أن بدأ نظر هذا البند في دورة الجمعية العامة عام ١٩٩٨.

٢ - إن إدراج البند على جدول أعمال الجمعية العامة ليبين أن المجتمع الدولي قد أدرك الأخطار التي قد يتعرض لها السلم والأمن الدوليين حال استعمال التكنولوجيات والمعلومات في أغراض غير سلمية.

٣ - وقد أدت العملية التحضيرية لمؤتمر القمة العالمي المعني بمجتمع المعلومات وتقرير عقد هذا المؤتمر على مرحلتين، في جنيف عام ٢٠٠٣ وتونس عام ٢٠٠٥، إلى إدراج البند الذي يتناوله القرار محل النظر، وغيره من القرارات الوثيقة الصلة بالموضوع، على قائمة الأولويات التي يوليها المجتمع الدولي اهتمامه.

٤ - فاستعمال الاتصالات السلكية واللاسلكية في أغراض عدوانية، من قبيل الهدف المعلن أو الخفي بتقويض النظام القانوني والسياسي للدول، هو مظهر من المظاهر السلبية في استعمال هذه الوسائل مما قد يترتب عليه آثار من شأنها خلق التوترات والأوضاع غير الملائمة للسلم والأمن الدوليين، وهو ما يتناقض تناقضا صارخا مع المبادئ والمقاصد المكرسة في ميثاق الأمم المتحدة.

٥ - إن القرار ٥٣/٥٧ يبين بجلاء أن نشر واستعمال التكنولوجيات ووسائل المعلومات سيكون في صالح المجتمع الدولي قاطبة وأن توسيع نطاق التعاون الدولي سيسهم في تحقيق الفعالية المثلى.

٦ - وفي الفقرة الثامنة من ديباجة القرار، أعربت الجمعية العامة عن ''قلقها لاحتمال أن تستخدم هذه التكنولوجيات والوسائل في أغراض لا تتفق والهدفين المتمثلين في صون الاستقرار والأمن الدوليين وقد تؤثران تأثيرا سلبيا في سلامة الهياكل الأساسية للدول مما يضر بأمنها في الميدانين المدني والعسكري على السواء''.

٧ - أما في الفقرة ٣ (ب) من المنطوق، فقد طلبت الجمعية آراء وملاحظات الدول عن تعريف المفاهيم الأساسية المتصلة بأمن المعلومات، ''بما فيها التدخل دون إذن في نظم المعلومات والاتصالات السلكية واللاسلكية وموارد المعلومات أو إساءة استخدامها''.

٨ - وتفهم كوبا أن ''التدخل دون إذن'' يعني استعمال تلك الأنظمة خارج نطاق الإجراءات والقواعد المتفق عليها دوليا، لا سيما داخل إطار الاتحاد الدولي للاتصالات السلكية واللاسلكية، وبما يتنافى والأنظمة الوطنية ذات الصلة.

٩ - ويتعين على الدول اعتماد جميع التدابير الضرورية لتعزيز الأنظمة الوطنية المذكورة، إن لم تكن قد فعلت ذلك بعد.

١٠ - ومما لا غنى عنه أيضا، القيام بصفة دورية بتعديل الأنظمة الدولية بشأن الموضوع، مع مراعاة السرعة التي تتطور بها التكنولوجيات ذات الصلة، بحيث تتماشى في فعاليتها وكفاءتها مع ذلك التطور.

١١ - إن نظم المعلومات والاتصالات السلكية واللاسلكية يمكن أن تصبح بمثابة أسلحة عند تصميمها أو استعمالها أو كلا الأمرين، بغرض إحداث أضرار بالبنية الأساسية لدولة من الدول. فمن هذا القبيل، الاعتداء الصادر عن الشبكات الوطنية التي تستخدم برمجيات أجنبية أو عن المصادر الداخلية بالدولة ذاتها، ولكن تكون هذه المصادر موجهة ومصممة في الخارج؛ وعمليات البث الإذاعي أو التلفزيوني الموجهة بغرض تقويض النظام الاجتماعي أو الدستوري لدولة أخرى يوجه إليها هذا البث؛ والأعمال الرامية إلى التشويش على البث الإذاعي والتليفزيوني لدول أخرى، أو الإضرار أو إحداث الشلل به، وما إلى ذلك.

١٢ - وتكرر كوبا تأكيد أنه يجب على جميع الدول احترام القواعد الدولية القائمة في ذلك المجال. ويتعين أن يكون الوصول إلى أنظمة المعلومات أو الاتصالات السلكية واللاسلكية لدولة أخرى متفقا مع ما تم إبرامه من اتفاقات للتعاون الدولي، مع مراعاة أن يكون مبدأ موافقة الدولة المعنية هو حجر الزاوية في هذا الأمر. كما يتعين أن يجري تطبيق أشكال ونطاق عمليات التبادل في احترام لتشريع الدولة التي سيتم الوصول إلى نظام المعلومات لديها.

١٣ - إن السلم والأمن الدوليين قد يتعرضا للأضرار من جراء الاعتداء الذي قد تشنه دولة ضد أنظمة المعلومات أو الاتصالات السلكية واللاسلكية لدى دول أخرى. وللأسف، تستخدم تلك الإجراءات في شكل أدوات ترمي إلى تطبيق سياسات عدوانية.

١٤ - وتعاني كوبا من هذا النوع من الاعتداءات الموجهة والمعتمدة والمنفذة من حكومة الولايات المتحدة منذ زهاء ٢٠ عاما. ففي عامي ١٩٨٥ و ١٩٩٠ أقامت حكومة الولايات المتحدة بصفة غير شرعية محطة إذاعة ومحطة تلفزيون، على التوالي، بغرض التأثير في البث الإذاعي والتليفزيوني الكوبي والتشويش عليهما. ففي كل أسبوع، تبث هاتان المحطتان

وغيرهما نحو بلدنا، ما يزيد على ٢ ٢٢٠ ساعة من البرامج الرامية إلى تخريب نظامنا الدستوري. وهناك ٢٤ ترددا مخصصا للبرامج المعدة خصيصا لتحقيق تلك الأغراض.

١٥ - وأنفقت حكومة الولايات المتحدة على هذا العدوان الإذاعي والتليفزيوني ما يزيد على ٢٠ مليون دولار سنويا منذ عام ١٩٩٠.

١٦ - وحسبما تم تبيانه في إعلان وزارة خارجية جمهورية كوبا، المؤرخ ٢٢ أيار/مايو ٢٠٠٣، شرعت حكومة الولايات المتحدة في اتخاذ إجراءات جديدة تشكل تصعيدا في العدوان الإذاعي الإلكتروني والتليفزيوني الذي تنفذه منذ عقود ضد كوبا.

١٧ - إن محطة الإذاعة التي أنشأتها وتشغلها الولايات المتحدة بغرض إلحاق التخريب بكوبا، قامت بالبث في ٢٠ أيار/مايو ٢٠٠٣، مستخدمة أربعة ترددات جديدة، مما أحدث تداخلا وتأثيرا في عمليات البث الإذاعية الكوبية.

١٨ - إن تلك الأعمال تشكل انتهاكا صارخا وجسيما للقانون الدولي وللأعراف والأنظمة التي أرساها الاتحاد الدولي للاتصالات السلكية واللاسلكية، وهو منظمة دولية أنشئت بغرض تحسين تشغيل الاتصالات السلكية واللاسلكية في العالم قاطبة، ولا سيما أنظمته المتعلقة بالاتصالات اللاسلكية.

١٩ - ومساء يوم ٢٠ أيار/مايو ذاته، جرى إرسال بث تلفزيوني تحقيقا لأغراض مماثلة صوب كوبا، عن طريق الدوائر الإعلامية الرسمية التابعة للولايات المتحدة، باستخدام طائرة من طراز EC-130 تعمل لدى القوات المسلحة الأمريكية للولايات المتحدة واستمر البث، من الساعة السادسة حتى العاشرة من مساء ذلك اليوم، باستخدام قنوات مخصصة بشكل قانوني لمحطات الإذاعة الكوبية والمسجلة على النحو الواجب لدى المنظمة الدولية المذكورة.

٢٠ - ويشكل ذلك العمل أيضا انتهاكا للقانون الدولي وللأعراف التي اتفقت عليها الدول داخل إطار الاتحاد الدولي للاتصالات السلكية واللاسلكية، لا سيما الفقرة ٢٣-٣ من أنظمته المتعلقة بالاتصالات اللاسلكية، التي تحظر البث التلفزيوني خارج نطاق الحدود الوطنية.

٢١ - إن عمليات البث التليفزيوني المذكورة، تشكل أيضا انتهاكا لديباجة دستور الاتحاد الدولي للاتصالات السلكية واللاسلكية، بسبب القيام بأنشطة لا تيسر العلاقات السلمية، والتعاون الدولي بين الشعوب، والتنمية الاقتصادية والاجتماعية، عن طريق التشغيل السليم للاتصالات السلكية واللاسلكية.

٢٢ - ولذلك ترفض كوبا وتدين موقف سلطات الولايات المتحدة المتواطئ مع أنشطة الإرهابي خوسيه باسولتو ومحاولاته بث إرسال تلفزيوني باتجاه الأراضي الكوبية. ورغم الإبلاغ في الوقت المناسب عبر القنوات الديبلوماسية عن إشعار السيد باسولتو بأن أي إرسال تلفزيوني باتجاه كوبا سيعتبر انتهاكا لقوانين الولايات المتحدة وسيعرضه لإجراءات تتخذ ضده، فإن هذا الإرهابي المعروف حلّق جوا بكل حرية يوم ٢٠ أيار/مايو الماضي، وإن لم يتحقق الإرسال التلفزيوني، فذلك لمشاكل في جهاز الإرسال الذي كان سيستخدمه وليس بسبب اتخاذ إجراءات من قبل السلطات الأمريكية، التي لم تخف تواطؤها معه.

٢٣ - وبموجب الفقرة ١٥-٣٤ من أنظمة الاتحاد الدولي للاتصالات السلكية واللاسلكية المتعلقة بالاتصالات اللاسلكية، يشكل اعتداء الولايات المتحدة عبر الإرسال التلفزيوني تشويشا ضارا، تقف وراءه محطة تلفزيونية تبث من القناة ١٣ ذات التردد العالي جدا (من ٢١٠ إلى ٢١٦ ميغاهرتز)، مما أثر تأثيرا شديدا في الخدمات التلفزيونية الكوبية التي سجلت قانونيا استخدامها القناة المذكورة.

٢٤ - وقد أبلغت السلطات الكوبية المعنية بالاتصالات اللاسلكية لجنة الاتصالات الاتحادية التابعة لحكومة الولايات المتحدة بهذا الأمر، مبينة جميع المعايير التقنية والقانونية التي انتهِكت انتهاكا صارخا.

٢٥ - وتعمد كوبا أيضا إلى إبلاغ الأمين العام للاتحاد الدولي للاتصالات السلكية واللاسلكية بالوقائع المذكورة وإلى طلب اتخاذ التدابير التي يقتضيها الحال.

٢٦ - وترى كوبا أن من اللازم تعزيز الإطار القانوني الدولي في مجال الإعلام والاتصالات السلكية واللاسلكية. كما تعتقد أنه لا غنى عن احترام النظام الدولي القائم في هذا المجال، في إطار الامتثال غير المشروط للقانون الدولي ولميثاق الأمم المتحدة الذي ينبغي أن تكون له الأولوية في العلاقات بين الدول. وبهذا الشأن، هناك بالفعل مبادئ وأنظمة وإجراءات دولية ذات صلة ينبغي احترامها.

٢٧ - ويجب العمل على وضع توجيهات غير ملزمة، وعلى تبني معايير يمكن صياغتها في شكل بروتوكولات أو اتفاقيات دولية أو متعددة الأطراف تكون ملزمة قانونيا.

٢٨ - وينبغي أن تضع المنهجيتان في الاعتبار معايير أساسية، مثل التدخل غير المأذون به أو الاستخدام غير المشروع لنظم المعلومات والاتصالات السلكية واللاسلكية والموارد الإعلامية؛ والجوانب المتعلقة بالسيادة في تلك المواضيع؛ والاستخدام السلمي لوسائط الإعلام والاتصالات السلكية واللاسلكية بجميع جوانبه؛ وتكثيف التعاون الدولي بهدف زيادة تطوير نظم المعلومات والاتصالات السلكية واللاسلكية في البلدان النامية، نظرا لما

لتكنولوجيات الإعلام والاتصال من أثر حاسم في التنمية الاجتماعية والاقتصادية؛ ومنع استخدام هذه النظم لأغراض عدائية ومكافحته والقضاء عليه وتنفيذ تدابير وطنية تعزز تحكم الدول في نظم المعلومات والاتصالات السلكية واللاسلكية وتتصدى للأعمال غير القانونية المرتكبة في هذا الصدد.

٢٩ - وإضافة إلى العناصر المشار إليها آنفا، ترى كوبا أن من الضروري توجيه الانتباه إلى الجوانب التالية، التي تتصل اتصالا وثيقا بالاستفادة إلى أقصى حد من قطاع الاتصالات السلكية واللاسلكية باعتباره أداة لتوطيد السلم والأمن الدوليين:

- ينبغي لجميع الدول الامتناع عن تنفيذ تدابير قسرية انفرادية، تتنافى والقانون الدولي وتفرض قيودا على قدرة الدولة المعنية على استخدام التكنولوجيات والشبكات الدولية لتبادل المعلومات والاتصالات السلكية واللاسلكية.

- ينبغي لنظم المصادقة وفرض الجزاءات في نهاية المطاف على دولة ما فيما يتعلق بإمكانية استخدامها تكنولوجيات الاتصالات السلكية واللاسلكية أو غيرها من التكنولوجيات الوثيقة الصلة، لأسباب تتعلق بتهديد السلم والأمن الدوليين، أن تكون متعددة الأطراف وأن تنفذ استنادا إلى معايير يتفق عليها المجتمع الدولي.

- يجب تكثيف التعاون الدولي في هذا المجال، وحشد الموارد اللازمة لمساعدة البلدان النامية على تعزيز نظم الاتصالات السلكية واللاسلكية لديها وتطويرها.

- ينبغي اتخاذ تدابير تشريعية وغيرها، سواء على الصعيد الوطني أو الدولي، بهدف حظر التركيز غير القانوني للملكية وسائط الاتصالات السلكية واللاسلكية، وغيرها من وسائط الإعلام والاتصال، والتحكم فيها في يد الخواص، نظرا لما يحدثه ذلك من أثر سلبي في تحقيق ما يلزم من تنوع في مصادر الإعلام ولإمكانية استخدامها كأداة للدعاية ضد السلام والتحريض على الحرب.

- ينبغي إنشاء نظام حكومي دولي متعدد الأطراف يكون ديمقراطيا وشفافا لإدارة ومراقبة شبكة إنترنت وغيرها من شبكات الإعلام والاتصال الدولية. ويمثل الطابع الحكومي الدولي لنظام المراقبة هذا شرطا لا غنى عنه.

- ينبغي أن تكون نظم مراقبة ورصد الاتصالات السلكية واللاسلكية وغيرها من أشكال الاتصالات الدولية، شفافة ومتعددة الأطراف، وأن توضع لها مسؤوليات وإجراءات واضحة تحقيقا للرقابة العامة، مع وضع حد لانتهاكات الخصوصية

وسيادة الكثير من الدول وأمنها، بواسطة نظم التجسس العالمية التي تبتكرها بعض الدول الصناعية، وعلى الأخص الولايات المتحدة.

- يجب وضع ضمانات راسخة لاحترام التنوع الثقافي، من شأنها إزالة جميع أشكال التمييز أو التحريض على الكراهية داخل المعلومات التي تُبث في نظم الاتصالات السلكية واللاسلكية على الصعيد الدولي.