الأمم المتحدة

A/59/116/Add.1*

الجمعية العامة

Distr.: General
28 December 2004
Arabic
Original: English, Spanish

الدورة التاسعة والخمسون

البند ٦١ من القائمة المؤقتة**

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***

إضافة

المحتويات

الصفحة

* أعيد إصدارها لأسباب فنية.

** A/59/150.

*** وردت المعلومات التي يتضمنها هذا التقرير بعد تقديم التقرير الرئيسي.

120105 120105 04-47509 (A)
0447509

الردود الواردة من الدول الأعضاء

فنزويلا

[الأصل: بالإسبانية]

[٢٨ حزيران/يونيه ٢٠٠٤]

١ - ترى حكومة جمهورية فنزويلا البوليفارية أن أي انتهاك لأمن المعلومات يناقض حق الدول في ممارسة سيادتها بصورة كاملة وشرعية. وفي هذا السياق، يأتي استخدام وسائط وتكنولوجيات المعلومات لأغراض زعزعة الاستقرار السياسي والاقتصادي مناقضا للقيم الأساسية للديمقراطية.

٢ - من هنا، يكتسي أمن المعلومات طابعا مزدوجا. فهو، من جهة، يؤمن غطاء وحماية لهذه المعلومات، ويكفل من جهة أخرى، حُسن استخدامها وصحتها. أما الاستخدام غير المشروع وعدم الاستخدام المتعمد لنظم المعلومات والاتصالات السلكية واللاسلكية أو لموارد المعلومات بهدف زعزعة الاستقرار فهو يمثل عامل إخلال في سياق الأمن الدولي.

٣ - إن الجمهورية الفنزويلية البوليفارية تشاطر صياغة المبادئ الدولية التي ترمي إلى تعزيز أمن نظم المعلومات والاتصالات السلكية واللاسلكية العالمية التي تعمل على إتاحة أو تيسير مكافحة الإرهاب والجريمة في مجال المعلومات، دون مساس بسيادة الدول.

المكسيك

[الأصل: بالإسبانية]

[١٨ آب/أغسطس ٢٠٠٤]

١ - لقد أدى التطور المفاجئ في نظم المعلومات والاتصالات السلكية واللاسلكية في الحقبة المعاصرة إلى توعية المجتمع الدولي على واقع آخر يواكب هذا التطور يتمثل في نشوء ترابط متين بين مستخدمي هذه النظم بشكل واسع ومتنوع أدى إلى اختراق الحدود الإقليمية والقانونية للدول.

٢ - وقد أدى هذا المستوى من الترابط إلى إحداث درجة مباشرة متماثلة من الهشاشة في سياق الأمن الوطني والدولي، بما يؤكد أن المعلومات ونظم الاتصالات السلكية واللاسلكية تشكل مادة استراتيجية تؤثر تأثيرا هاما في الظروف السلمية والأمنية الدولية.

٣ - ترى المكسيك أن التدابير التي يتعين اتخاذها من أجل الحد من الأخطار التي تنشأ في هذا السياق، إلى جانب انسجامها مع ضرورة الحفاظ على حرية تداول المعلومات وتعزيز تطور هذه العناصر في الأغراض السلمية، يجب أن تعود بفوائد ملموسة على نزع السلاح وعدم الانتشار، والتقريب بين الأمم، فضلا عن تشجيع مزيد من التعاون الدولي في هذا المجال.

٤ - وينبغي في تقديرنا النظر إلى المعلومات والاتصالات السلكية واللاسلكية من منظور متحرك وفعال. فإيقاع تقدم التطور العلمي والتكنولوجي، إذ ساهم في إيجاد فجوة بين القواعد التي ينبغي التقيد بها والقدرة الحقيقية لهذه النظم، إنما أدى مباشرة أيضا إلى ازدياد الأخطار المحتملة والحقيقية في مجال أمن المعلومات.

٥ - ونظرا للطابع الملح لهذا الموضوع وأهمية النظر في المفاهيم التي تتيح لنا تحديد هذه الظاهرة بمزيد من الدقة بغية مواجهتها بصورة ملائمة، تشجع المكسيك العمل الذي استهلته هي في شباط/فبراير من هذا العام بهدف إنشاء فريق خبراء حكوميين يتعاون مع الأمين العام للأمم المتحدة في صياغة دراسة تتصل بالنظر في الأخطار الحقيقية والمحتملة في سياق أمن المعلومات، وفي تدابير التعاون الممكنة لمواجهة هذه الأخطار، فضلا عن المفاهيم الدولية ذات الصلة الرامية إلى تعزيز أمن النظم العالمية للمعلومات والاتصالات السلكية واللاسلكية، على نحو ما هو مشار إليه في الفقرتين ٤ و ٢ من منطوق القرار ٣٢/٥٨. وفي هذا الصدد، نأمل أن يتضمن التقرير المزمع تقديمه إلى الجمعية العامة في دورتها الستين توصيات بهذا الشأن وأن يتم إحراز تقدم في التعريف المفاهيمي والقانوني للموضوع.

٦ - لهذه الغاية، ترى المكسيك أن التطورات والمناقشات التي جرت بشأن هذا الموضوع في إطار اللجان الأخرى التابعة للجمعية العامة، والأحكام ذات الصلة الواردة في الصكوك الدولية النافذة، فضلا عن أوجه التقدم الذي أحرزته المنظمات الدولية الأخرى، من قبيل اليونيسكو، في مجال الأمن الدولي والإرهاب الدولي والمعلومات ومجتمع المعلومات، سيكون لها فائدة كبيرة.

٧ - وفي ما يتعلق بالفقرة ٣ من المنطوق المتعلقة بتحديد المعايير الأساسية لأمن المعلومات، ولا سيما ما يتعلق بالتدخل غير المأذون به في نظم المعلومات والاتصالات السلكية واللاسلكية وموارد المعلومات أو الاستخدام غير المشروع لهذه النظم والموارد، تشدد المكسيك على أن مفهوم التدخل غير المأذون به قد يفضي إلى تشوش غير مرغوب فيه، حيث أنه ينطوي على مغزى مرتبط بأفعال تقوم بها دول معينة تتذرع بأسباب إنسانية وأسباب أخرى قابلة للنقاش تؤدي بها إلى التدخل، سواء بصورة فردية أو بالتنسيق مع دول أخرى، في شؤون دول ثالثة.

٨ - وفي هذا الصدد، قد يكون من الأفضل التخلي عن هذا المفهوم والاستعاضة عنه بمفهوم ''الوصول غير المسموح به''، أو إما ببساطة ''الوصول غير المشروع''، إشارة إلى الأفعال التي يقوم بها بعض الأشخاص أو الكيانات في ما يتعلق بنظم المعلومات.

٩ - وإزاء القلق الواضح بشأن مشاكل الأمن المتأتية من احتمال هشاشة نظم المعلومات التي تحكم برامج الدفاع في بعض البلدان، فضلا عن استخدام المعلومات والاتصالات السلكية واللاسلكية من جانب إرهابيين أو لأغراض الردع، تؤكد المكسيك مجددا أن الحوار والتفاوض والتعاون الدولي والقانون الدولي تشكل وحدها القنوات التي يمكن بواسطتها تجنب أن تؤدي التدابير المتخذة للتصدي لمشاكل أمن المعلومات إلى المساس بأي شكل من الأشكال بحرية المعلومات والاتصالات.

الولايات المتحدة الأمريكية

[الأصل: بالانكليزية]

[١٣ تموز/يوليه ٢٠٠٤]

يتسم أمن شبكات المعلومات وهياكلها الأساسية بالأهمية لكفالة موثوقية شبكات المعلومات الوطنية والعالمية هذه وتوافرها وسلامتها، حيث أن الدول ومواطنيها يعتمدون عليها بشكل متزايد في توفير الخدمات الأساسية والأمن الاقتصادي. والمسألة التي يتعين أن تعالج هي كيفية عمل الدول فرديا وجماعيا لتعزيز أمن شبكات المعلومات وهياكلها الأساسية ومنع الهجمات التي تؤدي إلى إضعافها.

ويرى بعض الدول إمكانية بلوغ ذلك الهدف عن طريق إبرام اتفاقية دولية تقيد تطوير أو استخدام طائفة واسعة من تكنولوجيات المعلومات. وتنطوي هذه المقترحات ضمنا على تخويل الحكومات الحق في الموافقة على المعلومات التي تنقل إلى إقليمها الوطني من خارج حدودها أو رفضها إذا ما اعتُبرت مسببة للاضطرابات سياسيا أو اجتماعيا أو ثقافيا.

ولا ترى الولايات المتحدة أن هذا النهج يسهم في تحقيق أهداف تعزيز أمن شبكات المعلومات والاتصالات العالمية، وإنما هو يخالف مبدأ حرية تدفق المعلومات الحيوية الأهمية لنماء وتطور الدول كافة. وتنفيذ ''أمن المعلومات'' يجب ألا يمس بحرية أي فرد في استقاء المعلومات والأفكار وتلقيها وإشراك الغير فيها عن طريق أي وسيط من وسائط الإعلام، بما في ذلك الوسائط الإلكترونية، ودون تقيد بالحدود الجغرافية، على النحو المنصوص عليه في المادة ١٩ من الإعلان العالمي لحقوق الإنسان.

وعلى العكس من ذلك، ترى الولايات المتحدة بأن الخطر الرئيسي على الأمن الحاسوبي منشأه الهجمات المتصلة التي يشنها المجرمون الضالعون في الجريمة المنظمة، وفرادى قراصنة الحاسوب، والأطراف من غير الدول، بمن فيهم الإرهابيون. ومن هذا المنظور، فإن أفضل السبل لحماية الفضاء الحاسوبي يمكن أن تتمثل في التركيز في آن واحد على تجريم الدول إساءة استخدام تكنولوجيا المعلومات وعلى التنفيذ الوطني المنهجي للتدابير المصممة لمنع الإضرار بالهياكل الأساسية للمعلومات الحيوية أيا كان مصدر الخطر، وهو ما تسميه الولايات المتحدة إنشاء ثقافة عالمية للأمن الحاسوبي. وحسب هذا التصور، تدرك جميع الأطراف (الحكومة، ودوائر النشاط التجاري، والمجتمع المدني) مسؤولياتها وتعمل وفقا لأدوارها لكفالة الأمن الحاسوبي.

وفيما يتعلق بالتطبيقات العسكرية لتكنولوجيا المعلومات، فإن إبرام اتفاقية دولية أمر لا ضرورة له البتة. وقانون الصراعات المسلحة ومبادؤه القائمة على الضرورة والتناسب والحد من الأضرار التبعية، يحكم بالفعل استخدام هذه التكنولوجيات.

تحقيق الأمن الحاسوبي عن طريق الوقاية

يمكن للدول تحقيق هدف الأمن الحاسوبي على أفضل وجه إذا ما عملت على الصعيد الوطني وتعاونت دوليا لتعزيز أمن هياكلها الأساسية للمعلومات الحيوية. وينبغي لكل دولة أن تضع برنامجا وطنيا يحقق ما يلي:

- التثقيف بأفضل الممارسات في مجال أمن شبكات المعلومات وهياكلها الأساسية وتعزيز الوعي بها،
- التجريم الفعال لإساءة استخدام تكنولوجيا المعلومات،
- التشجيع على قيام شراكة بين الحكومة ودوائر الصناعة لتوفير حوافز لكفالة أمن شبكاتها الوطنية،
- إنشاء قدرة وطنية للإنذار بالحوادث والاستجابة لها وإجراءات لتقاسم المعلومات وطنيا ودوليا على السواء.

وينبغي لكل دولة التركيز على إنشاء ''ثقافة أمن حاسوبي'' لدى جميع أصحاب المصلحة، بما في ذلك الحكومات، ودوائر النشاط التجاري، والمواطنين، وعلى التعاون فيما بين الدول سعيا إلى إنشاء ثقافة عالمية للأمن الحاسوبي.

وينبغي لتقرير فريق الخبراء الحكوميين أن يشدد على النُّهُج الواردة في قراري الجمعية العامة للأمم المتحدة ٥٥/٦٣ و ٥٦/١٢١، اللذين يحملان كليهما العنوان ''مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية''، والقرار ٥٧/٢٣٩ المعنون ''إنشاء ثقافة أمنية عالمية للفضاء الحاسوبي''. ويمكن أن يستفيد التقرير من هذه النُّهُج بإدراج عبارات تعزز مبادئ الأمن الحاسوبي يكون الأعضاء قد أقروها بالفعل. ويمكن لهذه الجهود أن تستفيد من الجهود المتعددة الأطراف التي بذلت مؤخرا لتعزيز الأمن الحاسوبي الإقليمي، مثل الجهود التي بذلت في منتدى الاتصالات السلكية واللاسلكية لرابطة التعاون الاقتصادي لآسيا والمحيط الهادئ، ومنظمة الدول الأمريكية، ومؤتمر القمة العالمي المعني بمجتمع المعلومات، ومجموعة البلدان الصناعية الثمانية.

والأخطار المكلفة على سلامة وتوافر الهياكل الأساسية لشبكات المعلومات الوطنية والعالمية تنبع في الغالب الأعم من إساءة الاستخدام الإجرامية. ومن منظور الولايات المتحدة،

من الأمور التي تتسم بأهمية أكبر كثيرا اتخاذ الحكومات خطوات لكفالة إمكانية التحقيق في أعمال هؤلاء الأفراد الذين يقومون بهذا النشاط وتقديمهم إلى المحاكمة. ولهذا السبب، وقعت الولايات المتحدة و٣٤ دولة أخرى اتفاقية مجلس أوروبا للجريمة الحاسوبية التي توفر مبادئ توجيهية من أجل التشريعات الوطنية والتعاون عبر الحدود على إنفاذ القانون. ويتوقع مجلس أوروبا فتح الاتفاقية أمام البلدان من خارج المجلس، وفقا لممارسة مجلس أوروبا (انظر المادة ٣٧). وبالفعل، يمكن لجميع البلدان، سواء كانت طرفا في الاتفاقية أم لا، أن تستخدمها فورا بوصفها نموذجا من أجل صياغة قوانين محلية فعالة لمكافحة الجريمة الحاسوبية.

علاوة على ذلك، وبغض النظر عن منشأ الهجمات أو دوافعها، هناك تشابه بينها من حيث طابع الأدوات المستخدمة والضرر الواقع على شبكات المعلومات. وبالتالي، من المهم أكثر أن تتخذ جميع الدول خطوات منهجية للحد من ضعف شبكاتها وغرس ''ثقافة أمن حاسوبي'' لدى مواطنيها، أي مجموعة من الممارسات والعادات الأمنية المصممة لصيانة الهياكل الأساسية للمعلومات بها.

وتشمل الحماية الفعالة للهياكل الأساسية للمعلومات والشبكات الحيوية الحد من ضعف هذه الهياكل إزاء جميع أشكال الهجمات بغية تخفيض الضرر ووقت الانتعاش إلى الحد الأدنى في حالة حدوث ضرر.

وتتطلب الحماية الفعالة أيضا اتصالات وتنسيقا وتعاونا على الصعيدين الوطني والدولي فيما بين جميع أصحاب المصلحة، مثل دوائر الصناعة، والأوساط الأكاديمية، والقطاع الخاص، والكيانات الحكومية، بما في ذلك وكالات حماية الهياكل الأساسية وإنفاذ القانون. وينبغي بذل هذه الجهود مع المراعاة الواجبة لأمن المعلومات والقوانين المنطبقة فيما يتعلق بالمساعدة القانونية المتبادلة وحماية الخصوصية. وسعيا إلى بلوغ هذه الأهداف، ينبغي تشجيع الدول على تنفيذ المبادئ الأحد عشر التي صاغها خبراء حماية الهياكل الأساسية للمعلومات الحيوية من بلدان مجموعة البلدان الصناعية الثمانية واعتمدها بعد ذلك وزراء العدل والداخلية في بلدان المجموعة في أيار/مايو ٢٠٠٣ وهم يضعون استراتيجية لتخفيض الأخطار التي تهدد الهياكل الأساسية للمعلومات الحيوية، والمبادئ هي:

١ - ينبغي للبلدان إنشاء شبكات للإنذار بالطوارئ فيما يتصل بأوجه الضعف والتهديدات والحوادث الحاسوبية.

٢ - ينبغي للبلدان القيام بالتوعية لتيسير فهم أصحاب المصلحة لطبيعة ونطاق الهياكل الأساسية للمعلومات المتاحة لهم، والدور الذي يجب أن يضطلع به كل منهم في حماية تلك الهياكل.

٣ - ينبغي للبلدان أن تدرس هياكلها الأساسية وتحدد أوجه الترابط فيما بينها، مما يعزز حماية هذه الهياكل.

٤ - ينبغي للبلدان تعزيز الشراكات فيما بين أصحاب المصلحة، في القطاعين العام والخاص على السواء، لتقاسم المعلومات عن الهياكل الأساسية الحيوية وتحليلها بغية منع حدوث أضرار لتلك الهياكل أو وقوع هجمات عليها والتحقيق في تلك الأضرار والهجمات والاستجابة لها.

٥ - ينبغي للبلدان إنشاء شبكات للاتصالات في حالات الأزمات واختبار تلك الشبكات للتأكد من أنها ستظل مأمونة ومستقرة في حالات الطوارئ.

٦ - ينبغي للبلدان كفالة أن تراعي سياسات توافر البيانات ضرورة حماية الهياكل الأساسية للمعلومات الحيوية.

٧ - ينبغي للبلدان تيسير تعقب الهجمات على الهياكل الأساسية للمعلومات الحيوية والإفصاح عن المعلومات المتعلقة بالتعقب للبلدان الأخرى، حسب الاقتضاء.

٨ - ينبغي للبلدان أن تنظم تدريبا وتمارين لتعزيز قدرات استجابتها ولاختبار الاستمرارية وخطط الطوارئ في حالة حدوث هجوم على الهياكل الأساسية للمعلومات كما ينبغي لها أن تشجع أصحاب المصلحة على المشاركة في أنشطة مماثلة.

٩ - ينبغي أن تكفل البلدان وجود ما يكفي من القوانين الموضوعية والإجرائية، مثل القوانين المبينة في اتفاقية الجريمة الحاسوبية لمجلس أوروبا المؤرخة ٢٣ تشرين الثاني/نوفمبر ٢٠٠١، والأفراد المدربين لتمكينها من التحقيق في الهجمات على الهياكل الأساسية للمعلومات الحيوية ومحاكمة مرتكبيها، والتنسيق في تلك التحقيقات مع البلدان الأخرى حسب الاقتضاء.

١٠ - ينبغي للبلدان إقامة تعاون دولي، حسب الاقتضاء، لتأمين الهياكل الأساسية للمعلومات الحيوية، بما في ذلك تأمينها عن طريق تطوير وتنسيق شبكات إنذار في حالات الطوارئ، وتقاسم المعلومات وتحليلها فيما يتصل بأوجه الضعف، والتهديدات، والحوادث، وتنسيق التحقيقات في الهجمات على تلك الهياكل وفقا للقوانين المحلية.

١١ - ينبغي للبلدان تعزيز البحث والتطوير على الصعيدين الوطني والدولي وتشجيع تطبيق التكنولوجيات الأمنية المصدقة وفقا للمعايير الدولية.

ويمكن تعزيز الحماية الفعالة وأمن الهياكل الأساسية للمعلومات بالتثقيف والتدريب، والسياسات والقوانين، والتعاون الدولي، ويجوز دعمها بالتكنولوجيا.

وينبغي تقديم الدعم للأمم المتحدة وغيرها من المنظمات المتعددة الأطراف في جهودها الرامية إلى تشجيع الدول الأعضاء على القيام بما يلي:

- تقييم أمن شبكاتها الوطنية الحيوية والهياكل الأساسية للمعلومات، بما في ذلك فهم أوجه ضعفها وترابطها،
- التثقيف وتعزيز الوعي الوطني بأفضل الممارسات في مجال أمن شبكات المعلومات وهياكلها الأساسية،
- التجريم الفعال لإساءة استخدام تكنولوجيا المعلومات وتيسير التحقيق في الجريمة الحاسوبية عبر الحدود،
- التشجيع على إقامة شراكة بين الحكومة ودوائر الصناعة لتوفير حوافز لكفالة أمن شبكاتها الوطنية،
- إنشاء قدرة وطنية للإنذار بالحوادث والاستجابة لها وإجراءات لتقاسم المعلومات وطنيا ودوليا على السواء.