الأمم المتحدة

A/60/95/Add.1

الجمعية العامة

Distr.: General
21 September 2005
Arabic
Original: English

الدورة الستون

البند ٨٦ من جدول الأعمال

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

121005 121005 05-51875 (A)

ثانيا – الردود الواردة من الحكومات

البرازيل

[الأصل: بالانكليزية]
[٢٤ حزيران/يونيه ٢٠٠٥]

في معرض تحليل انعكاسات التطورات الحاصلة في ميدان تكنولوجيات المعلومات والاتصالات السلكية واللاسلكية على الأمن الدولي، يجب على المرء أن يستهل بالتسليم بأن العلاقة بين المجتمعات والتطور التكنولوجي لا يمكن أن تُحصر في التفاعلات البسيطة أحادية الاتجاه؛ ذلك أنها ترتكز على تفاعل معقد بين الضرورات والإبداع ومبادرات تنظيم المشاريع والاستغلال الجماعي للتكنولوجيا. ويشرق القرن الحادي والعشرون عن عهد جديد، يُنتظر في ظله أن يُملي صعود ''مجتمع المعلومات'' تحولات عميقة في جميع مجالات النشاط البشري، بدءا بتفاعلات الأفراد والمجتمعات، وانتهاء بأنماط الإنتاج الاقتصادي وحكم الدول.

لقد أصبحت المعلومات بالفعل عنصرا حاسما بالنسبة لثروة الأمم ورفاهها، ويُنظر إليها اليوم، بحق، على أنها مورد من أنفس موارد الأمم. وتترابط الشركات الخاصة والمصارف وأسواق الأسهم المالية والمؤسسات الحكومية (بما فيها مؤسسات الدفاع) فيما بينها بشبكات معلومات عالمية أضحت على درجة من الحيوية، بالنسبة للتقدم الاقتصادي، تعادل الطاقة الكهربائية وإمدادات المياه. بيد أن هذه الدرجة العالية والمتصاعدة من الترابط أحدثت أيضا، بالنسبة للحكومات والاقتصادات، مجموعة جديدة من مواطن الضعف الممكنة يمكن أن تستغل في الصراعات العسكرية وفي الأنشطة الإجرامية والإرهابية على السواء.

وخلال العقود الأخيرة، هيّأ الاستعمال الواسع للتكنولوجيا والأتمتة في الحروب الظروف التي جعلت الصراعات بين الدول أقدر على التركيز أكثر على الأهداف العسكرية وتحاشي الأضرار الجانبية. وفي الوقت ذاته، يفرض التأثير المتنامي لوسائط الإعلام ودوائر المجتمع المدني المنظمة قيودا عديدة على طريقة تنفيذ العمليات العسكرية. فالحرب المعاصرة يُفترض أن تكون ''نظيفة'' بل حتى ''دقيقة دقة جراحية''.

وينسجم هذا انسجاما كاملا مع الإمكانات التي تُتيحها ''الحرب الإلكترونية''. وقد قامت فعلا بعض القوات المسلحة بنشر وحدات عسكرية متخصصة، مُدربة ومجهزة لشلّ، أو حتى تدمير الهياكل الأساسية الدقيقة عن طريق غزو شبكات المعلومات وتخريبها. وتبعا للهدف المنشود والوسائل المستعملة، يمكن للآثار المترتبة على هذه الهجمات أن تتراوح ما بين ''قتل الأنظمة الإلكترونية'' لأسلحة العدو أو نظمه الحساسة إلى التعطيل الكارثي

لشبكات الكهرباء على مستوى البلاد كلها. ومما يزيد كفاءة هذا الشكل من الحروب كون الكثير من تلك القدرات يُمكن تشكيله بواسطة استثمارات صغيرة نسبيا. وبالنظر إلى هذه العوامل، يمكن فعلا للحرب الإلكترونية أن تمهد للصراعات العسكرية بين الدول في المستقبل القريب. كما يمكن أيضا أن تُستغل نفس مواطن الضعف تلك من جانب منظمات إرهابية، وهو ما يحتمل أن تكون له عواقب أوخم وأكثر فُجائية.

ومع أن نطاق استخدام أدوات تكنولوجيا المعلومات الهجومية هاته من جانب المجرمين أضيق من حيث حجم الآثار المترتبة عنه، إلا أن المجرمين بدؤوا فعلا في استخدامها استخداما واسعا: ففي كل سنة، يجري اختراق نظم تكنولوجيا المعلومات للعديد من المؤسسات المالية والشركات التجارية والوكالات الحكومية وغزوها من جانب أفراد أو مجموعات تبحث على نحو غير مشروع عن الربح و/أو المعلومات السرية.

وإدراكا من البرازيل لأهمية هذا الموضوع في صون السلام والأمن الدوليين، فإنها تقترح اتباع طريقتين مختلفتين في معالجة هذه المسألة. أولا، ينبغي للمجتمع الدولي أن يسعى جاهدا من أجل استحداث الأدوات المناسبة للتصدي للأنشطة الإجرامية والإرهابية التي تنطوي على استخدام تكنولوجيا المعلومات. وينبغي للمجتمع الدولي أن يتبع نهجا منفصلا، لكنه مكمل للطريقة الأولى، يكمُن في دراسة الآثار المترتبة على نشوء الحرب الإلكترونية والحاجة المحتملة إلى وضع أنظمة لنزع السلاح وعدم الانتشار وقانون بشأن الحرب يأخذ في الحسبان آثارها المتعددة.

وبالنظر إلى إمكانية وقوع أعمال إرهابية وإجرامية، فإننا نقترح أن تقود الأمم المتحدة الدول الأعضاء في مسعى للتعاون من أجل وضع التدابير التالية:

- استحداث شبكات للطوارئ وشبكات بديلة لحماية الهياكل الأساسية الحيوية،
- فحص بنية شبكاتها، وتحليل أوجه الترابط بينها، وتحديد أساليب فعالة للحماية،
- تعزيز التفاعلات بين الحكومات والقطاعات الخاصة الرامية إلى تحقيق المستوى المطلوب لأمن تدفق المعلومات بين المنظمات،
- وضع نظم للحماية لتحاشي آثار الهجمات الإلكترونية، أو التقليل منها إلى أدنى حد،
- تطبيق أدوات وتدابير لتمكين السلطات من تعقب مصدر الهجمات الإلكترونية،
- تأهيل المؤسسات الوطنية لإجراء اختبارات للمستوى الأمني لنظم المعلومات وتقييمه،

- التفاوض بشأن اتفاقية دولية لمكافحة الجرائم الإلكترونية واعتمادها،
- تعزيز وتطوير التكنولوجيا المتعلقة بوسائل أمن المعلومات وأساليبها،
- ضمان إمكانية وصول الجمهور كافة إلى المعلومات المتاحة وتكنولوجيا المعلومات،
- تفادي وضع آليات من شأنها أن تحول دون وصول البلدان إلى التكنولوجيا العالية في مجال الاتصالات السلكية واللاسلكية ونظم المعلومات،
- وضع إجراءات للإخطار المتبادل فيما بين السلطات الوطنية المختصة بشأن التهديدات الإلكترونية،
- تثقيف السكان بأهمية الأمن الإلكتروني.

وفيما يتعلق باستخدام أسلحة المعلومات في الصراعات بين الدول، فإننا نعتقد أنه ينبغي للأمم المتحدة أن تُجري تقييما لإمكانية الترويج لاتفاقيات بشأن المواضيع التالية:

- تعريف حرب المعلومات وتحديد خواصها وتصنيفها،
- تحديد أسلحة المعلومات والوسائل التي يمكن أن تُستخدم كأسلحة معلومات، وتصنيفها،
- منع استخدام الأسلحة أو المعارف العسكرية الحاسوبية من جانب الجماعات الإرهابية،
- وضع مدونة قواعد سلوك لاستخدام أسلحة المعلومات،
- ضمان تمتع جميع البلدان بحقوق متكافئة فيما يتعلق بحماية أوطانها من الهجمات الإلكترونية،
- استحداث آليات دولية من أجل توجيه تسوية الصراعات المتعلقة بالاعتداءات الإلكترونية،
- وضع مسرد للأمم المتحدة يتضمن تعريف المصطلحات الرئيسية المتعلقة بأمن المعلومات.

كندا

[الأصل: بالانكليزية]

[٤ آب/أغسطس ٢٠٠٥]

تعد الهياكل الأساسية للمعلومات مكونا رئيسيا للهياكل الأساسية الحيوية لكندا، التي تشمل القطاعات التالية: الطاقة والمرافق، والاتصالات وتكنولوجيا المعلومات، والمالية، والرعاية الصحية، والغذاء، والمياه، والنقل، والحكومة والتصنيع. وتبقى التحديات التي تكتنف تأمين الهياكل الأساسية للمعلومات هي نفس التحديات التي تواجهها جميع القطاعات، التي يُقدّر أن ٩٠ في المائة منها مملوك للقطاع الخاص الذي يتولى تشغيله. وقد دفعت الأهمية التي تكتسيها في نظر جميع الكنديين الهياكل الأساسية للمعلومات في كندا، بالحكومة إلى العمل من أجل الحفاظ على أمن نظمها وتوفرها ونزاهتها، وإلى اتخاذ خطوات لمنع الحوادث الإلكترونية والاستجابة السريعة لأية أعطال يُبلّغ عنها.

وقد أعلن رئيس الوزراء، في كانون الأول/ديسمبر ٢٠٠٣ إنشاء إدارة جديدة للسلامة العامة والتأهب لحالات الطوارئ. وقد أدمجت هذه الإدارة الحكومية الجديدة في وزارة واحدة ما كان يعرف سابقا بمكتب حماية الهياكل الأساسية الحيوية والتأهب لحالات الطوارئ، وشرطة الخيالة الملكية الكندية، ودائرة الاستخبارات الأمنية الكندية – وهي ثلاث وكالات اتحادية رئيسية مكلفة بولايات في مجال الأمن الإلكتروني. وتتولى إدارة السلامة العامة والتأهب لحالات الطوارئ مسؤولية رصد وتحليل التهديدات الإلكترونية التي تواجه النظم الحكومية، عن طريق توفير نقطة مركزية للإبلاغ عن الحوادث الإلكترونية، وإنذار الإدارات الحكومية بالتهديدات الجديدة ومواطن الضعف. وتتولى دائرة الاستخبارات الأمنية الكندية مسؤولية التحقيق في الحوادث التي تشكل تهديدا للأمن القومي. وتتولى شرطة الخيالة الملكية الكندية مسؤولية التحقيق في أية حوادث إلكترونية إجرامية، أو حوادث إلكترونية إجرامية يحتمل وقوعها. وإضافة إلى هذا، فإن مؤسسة أمن الاتصالات، وهي السلطة التقنية المختصة بأمن تكنولوجيا المعلومات، تتولى مسؤولية وضع المعايير التشغيلية للترخيص للنظم واعتمادها وتحليل المخاطر ومواطن الضعف وتقييم المنتجات وتحليل أمن النظم والشبكات.

وفي نيسان/أبريل ٢٠٠٤، أعلنت كندا لأول مرة عن سياسات الأمن القومي التي تُحدد استراتيجية متكاملة وخطة عمل مُصممة للتصدي للتهديدات الراهنة والمستقبلية. وأكدت هذه الخطة على وجه التحديد أن الأمن الإلكتروني يشكل تحديا بالنسبة للسلامة العامة، واقترحت إنشاء فرقة عمل وطنية رفيعة المستوى معنية بالأمن الإلكتروني يمثل فيها

القطاعان العام والخاص من أجل وضع استراتيجية وطنية للأمن الإلكتروني للتصدي لهذه المسألة. ويجري حاليا تشكيل فرقة العمل المذكورة.

وفي شباط/فبراير ٢٠٠٥، أنشأت إدارة السلامة العامة والتأهب لحالات الطوارئ المركز الكندي للاستجابة للحوادث الإلكترونية، ليكون بمثابة جهة الاختصاص الوطنية في مجال تنسيق الاستجابة لحوادث الأمن الإلكتروني ورصد بيئة التهديدات الإلكترونية. ويعمل هذا المركز انطلاقا من مركز عمليات الحكومة، وهو مُنشأة تعمل على مدار الساعة وطيلة أيام الأسبوع كجزء من النظام الوطني الكندي للاستجابة لحالات الطوارئ.

وتُركز المحافظات والأقاليم الكندية على حماية هياكلها الأساسية الحيوية، بما فيها النظم الإلكترونية والشبكات التي تعتمد عليها. ويجري حاليا العمل من أجل شن مبادرات مشتركة بين المحافظات، مثل القدرة التعاونية للرصد الإلكتروني.

ويشترك القطاع الخاص على نحو فعال في مبادرات الأمن الإلكتروني. فشركات القطاع الخاص تقوم بحماية هياكلها الأساسية الهامة لتكنولوجيا المعلومات، وتعمل عن طريق رابطات الصناعة على تبادل المعلومات بشأن مواطن الضعف الإلكترونية والحوادث والحلول المتوفرة في إطار قطاعاتها. وتعمل رابطات الصناعة مع إدارة السلامة العامة والتأهب لحالات الطوارئ في منتدى يسمح بتبادل أوسع للمعلومات على نطاق القطاعات الصناعية.

واشتركت كندا أيضا في المبادرات المتعددة الأطراف بشأن الأمن الإلكتروني. وشملت تلك المبادرات المجموعة الفرعية لمجموعة بلدان الثمانية المعنية بجرائم التكنولوجيا العالية، التي أنشئت سنة ١٩٩٧، والتي اعتمدت ١٠ مبادئ لمحاربة الجرائم الحاسوبية؛ واتفاقية مجلس أوروبا المعنية بالجرائم الإلكترونية، التي تهدف إلى تنسيق القوانين الوطنية من أجل تحديد الجرائم ووضع إجراءات التحقيق والمقاضاة لمجاراة الشبكات العالمية وإنشاء نظام سريع وفعال للتعاون الدولي؛ ومنظمة الدول الأمريكية، التي اتفقت الدول الأعضاء بها على ”النظر في إعداد صكوك قانونية جوهرية للبلدان الأمريكية، وسنّ تشريع نموذجي لغرض تعزيز التعاون في ما بين بلدان النصف الغربي من الكرة الأرضية في مكافحة الجريمة الإلكترونية، والنظر في وضع معايير تتعلق بالسرية وحماية المعلومات والجوانب الإجرائية ومنع الجريمة“.