الأمم المتحدة

A/C.2/57/L.10/Rev.1

الجمعية العامة

Distr.: Limited
10 December 2002
Arabic
Original: English

الدورة السابعة والخمسون
اللجنة الثانية
البند ٨٤ (ج) من جدول الأعمال
المسائل المتعلقة بسياسات الاقتصاد الكلي:
تسخير العلم والتكنولوجيا لأغراض التنمية

الاتحاد الروسي، إثيوبيا، الأرجنتين، استراليا، ألمانيا، إيطاليا، باكستان، بلغاريا، بولندا، تركيا، تونس، الجمهورية التشيكية، جمهورية كوريا، جنوب أفريقيا، الدانمرك، رومانيا، سلوفاكيا، السويد، سويسرا، شيلي، كرواتيا، كندا، المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية، النرويج، نيوزيلندا، الهند، الولايات المتحدة واليابان: مشروع قرار منقح

إنشاء ثقافة أمنية عالمية للفضاء الحاسوبي

إن الجمعية العامة،

إذ تلاحظ تنامي اعتماد الحكومات والأعمال التجارية والمنظمات الأخرى وفرادى المستعملين على تكنولوجيات المعلومات لتوفير السلع والخدمات الأساسية وتسيير الأعمال وتبادل المعلومات،

وإذ تسلم بالحاجة إلى إحداث زيادات في أمن الفضاء الحاسوبي مع زيادة البلدان مشاركتها في مجتمع المعلومات،

وإذ تشير إلى قراريها ٦٣/٥٥ المؤرخ ٤ كانون الأول/ديسمبر ٢٠٠٠ و ١٢١/٥٦ المؤرخ ١٩ كانون الأول/ديسمبر ٢٠٠١ المتعلقين بإيجاد الأساس القانوني لمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية،

101202 101202 02-73137 (A)
0273137

وإذ تشير كذلك إلى قراراتها ٥٣/٧٠ و ٥٤/٤٩ و ٥٥/٢٨ و ٥٦/١٩ و ٥٧/٥٣ المتعلقة بالتطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي،

وإذ تدرك أن الأمن الفعال للفضاء الحاسوبي ليس مجرد مسألة ممارسات حكومية أو إنفاذ للقوانين، وإنما يجب توفيره من خلال الوقاية ودعمه من جانب المجتمع بكامله،

وإذ تدرك أيضا أن التكنولوجيا وحدها لا تستطيع أن تكفل أمن الفضاء الحاسوبي وأنه يتعين إيلاء الأولوية لتخطيط أمن الفضاء الحاسوبي وإدارته من جانب المجتمع بكامله،

وإذ تسلّم بأنه يجب على الحكومات والأعمال التجارية والمنظمات الأخرى وفرادى مالكي ومستخدمي تكنولوجيا المعلومات أن يدركوا، كل حسب دوره، الأخطار التي تتهدد أمن الفضاء الحاسوبي والتدابير الوقائية في هذا الصدد، وأن يتحملوا المسؤولية وأن يتخذوا الخطوات اللازمة لتعزيز أمن تكنولوجيا المعلومات تلك،

وإذ تدرك أن الفجوة الحالية في الحصول على تكنولوجيا المعلومات واستخدامها من جانب الدول يمكن أن تقلل من فعالية التعاون الدولي في مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية وفي إنشاء ثقافة عالمية بشأن أمن الفضاء الحاسوبي وإذ تلاحظ الحاجة إلى تيسير نقل تكنولوجيا المعلومات ولا سيما إلى البلدان النامية،

وإذ تسلّم بأهمية التعاون الدولي لتحقيق أمن الفضاء الحاسوبي من خلال دعم الجهود الوطنية الرامية إلى تعزيز القدرات البشرية وزيادة فرص التعلم والعمل وتحسين الخدمات العامة وتحسين نوعية الحياة من خلال الاستفادة من تكنولوجيا المعلومات المتطورة والمأمونة والآمنة والشبكات وتعزيز الفرص ليحصل عليها الجميع،

وإذ تلاحظ أنه نتيجة لازدياد إمكانية الترابط الإلكتروني، تتعرض نظم وشبكات المعلومات حاليا لعدد مطرد وطائفة متنوعة من مواطن الخطر والضعف ما يطرح مسائل أمنية جديدة لدى الجميع،

وإذ تنوه بالأعمال ذات الصلة التي تضطلع بها المنظمات الدولية والإقليمية بشأن تعزيز أمن الفضاء الحاسوبي وأمن تكنولوجيات المعلومات،

١ - **تحيط علما** بالعناصر المرفقة بهذا القرار بهدف إنشاء ثقافة عالمية لأمن الفضاء الحاسوبي؛

٢ - **تدعو** جميع المنظمات ذات الصلة أن تراعي من جملة أمور، العناصر المرفقة فيما يتعلق بإنشاء ثقافة عالمية لأمن الفضاء الحاسوبي في أية أعمال مقبلة بشأن أمن الفضاء الحاسوبي؛

٣ - **تدعو** الدول الأعضاء إلى أن تراعي هذه العناصر في جهودها المبذولة لتنمية ثقافة أمن الفضاء الحاسوبي في تطبيق واستخدام تكنولوجيات المعلومات، على صعيد المجتمع بكامله؛

٤ - **تطلب** من الدول الأعضاء وجميع المنظمات الدولية ذات الصلة أن تضع في اعتبارها هذه العناصر وضرورة إيجاد ثقافة عالمية لأمن الفضاء الحاسوبي، في أعمالها التحضيرية لمؤتمر القمة العالمي لمجتمع المعلومات المزمع عقده في جنيف في كانون الأول/ديسمبر ٢٠٠٣ وفي تونس في عام ٢٠٠٥؛

٥ - **تشدد** على ضرورة تيسير نقل تكنولوجيا المعلومات وبناء القدرات في البلدان النامية لمساعدتها في اتخاذ التدابير المتعلقة بأمن الفضاء الحاسوبي.

المرفق

عناصر إنشاء ثقافة عالمية لأمن الفضاء الحاسوبي

إن التطورات السريعة في تكنولوجيا المعلومات قد غيرت الطريقة التي تقوم بها الحكومات والأعمال التجارية والمنظمات الأخرى وفرادى المستخدمين الذين يطورون ويمتلكون ويوفرون ويديرون ويخدمون ويستخدمون نظم وشبكات المعلومات (''المشتركون'')، بتناول مسألة أمن الفضاء الحاسوبي. وستتطلب الثقافة العالمية لأمن الفضاء الحاسوبي من جميع المشتركين تبني المبادئ التكميلية التسعة التالية:

(أ) **الوعي**: ينبغي أن يعي المشتركون ضرورة توافر الأمن لنظم وشبكات المعلومات وما يمكنهم عمله لتعزيز هذا الأمن؛

(ب) **المسؤولية**: المشتركون مسؤولون عن أمن نظم وشبكات المعلومات بما يتناسب وأدوارهم. وينبغي لهم أن يستعرضوا بانتظام سياساتهم وممارساتهم وتدابيرهم وإجراءاتهم، وينبغي لهم أن يقدروا ما يتلاءم منها مع بيئاتهم؛

(ج) **الاستجابة**: ينبغي للمشتركين أن يعملوا متعاونين على منع الحوادث الأمنية وكشفها والرد عليها في حينها. وينبغي أن يتبادلوا المعلومات عن مكامن الخطر والضعف، حسب الاقتضاء، وأن ينفذوا إجراءات من أجل التعاون بسرعة وفعالية على منع الحوادث الأمنية وكشفها والاستجابة لها. وقد يشمل ذلك التعاون وتبادل المعلومات عبر الحدود؛

(د) **قواعد السلوك**: نظرا لانتشار نظم وشبكات المعلومات وشيوعها في المجتمعات المعاصرة، يتعين على المشتركين احترام المصالح المشروعة للآخرين وإدراك أن قيامهم بأعمال أو إحجامهم عنها قد يضر بالآخرين؛

(هـ) **الديمقراطية:** ينبغي أن يطبق الأمن بطريقة تتماشى مع القيم التي تعترف بها المجتمعات الديمقراطية، بما في ذلك حرية تبادل الأفكار والآراء، والتدفق الحر للمعلومات، وسرية المعلومات والاتصالات، والحماية الكافية للمعلومات الشخصية، والانفتاح، والشفافية؛

(و) **تقييم الأخطار:** ينبغي لجميع المشتركين أن يقوموا بتقييمات دورية للأخطار تحدد مواطن الخطر والضعف؛ وأن تكون مبنية على قاعدة عريضة بدرجة كافية للإحاطة بالعوامل الرئيسية، الداخلية والخارجية، مثل التكنولوجيا، والعوامل المادية والبشرية، والسياسات، والخدمات التي تقدمها أطراف ثالثة وتنطوي على آثار أمنية؛ وأن يسمحوا بتحديد مستوى المجازفة المقبول؛ وأن يساعدوا في اختيار الضوابط المناسبة لإدارة الأخطار التي تنطوي على ضرر بنظم وشبكات المعلومات في ضوء طبيعة وأهمية المعلومات الواجب حمايتها؛

(ز) **تصميم الأمن وتنفيذه:** ينبغي للمشتركين أن يدرجوا الأمن عنصرا أساسيا في تخطيط نظم وشبكات المعلومات وتصميمها واستخدامها؛

(ح) **إدارة الأمن:** ينبغي للمشتركين أن يعتمدوا نهجا شاملا لإدارة الأمن يستند إلى تقييم الأخطار ويكون ديناميا وشاملا لأنشطة المشتركين بشتى مستوياتها ولعملياتهم من جميع جوانبها؛

(ط) **إعادة التقييم:** ينبغي للمشتركين أن يستعرضوا أمن نظم وشبكات المعلومات وأن يعيدوا تقييمه، وينبغي لهم أن يدخلوا التعديلات اللازمة على السياسات والممارسات والتدابير والإجراءات الأمنية بما يشمل تناول مواطن الخطر والضعف المستجدة والمتغيرة.