الأمم المتحدة

A/RES/57/239

Distr.: General
31 January 2003

الجمعية العامة

الدورة السابعة والخمسون
البند ٨٤ (ج) من جدول الأعمال

قرار اتخذته الجمعية العامة

[بناء على تقرير اللجنة الثانية (*A/57/529/Add.3*)]

٥٧/٢٣٩ - إنشاء ثقافة أمنية عالمية للفضاء الحاسوبي

إن الجمعية العامة،

إذ تلاحظ تنامي اعتماد الحكومات والأعمال التجارية والمنظمات الأخرى وفرادى المستعملين على تكنولوجيا 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 ٥٥/٦٣ المؤرخ ٤ كانون الأول/ديسمبر ٢٠٠٠ و ٥٦/١٢١ المؤرخ ١٩ كانون الأول/ديسمبر ٢٠٠١ المتعلقين بإيجاد الأساس القانوني لمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية،

وإذ تشير أيضا إلى قراراتها 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 المتعلقة بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية 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، بطريقة ملائمة لأدوارهم، الأخطار التي تتهدد أمن الفضاء الحاسوبي والتدابير الوقائية في هذا الصدد، وأن يتحملوا المسؤولية عن أمن تكنولوجيا المعلومات تلك وأن يتخذوا الخطوات اللازمة لتعزيزه،

وإذ تدرك أيضا 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 تدرك كذلك أهمية 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 وشبكات المعلومات والاتصالات المتطورة والمأمونة والآمنة وتعزيز الفرص ليحصل عليها الجميع،

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

وإذ تلاحظ أيضا الأعمال التي تضطلع بها المنظمات الدولية والإقليمية ذات الصلة بشأن تعزيز أمن الفضاء الحاسوبي وأمن تكنولوجيا المعلومات،

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

٢ - **تدعو** جميع المنظمات الدولية ذات الصلة أن تراعي من جملة أمور، هذه العناصر المتعلقة بإنشاء مثل هذه الثقافة في أية أعمال مقبلة بشأن أمن الفضاء الحاسوبي؛

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

٤ - **تدعو** الدول الأعضاء وجميع المنظمات الدولية ذات الصلة إلى 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 الفترة من ١٠ إلى ١٢ كانون الأول/ ديسمبر ٢٠٠٣ وفي تونس في عام ٢٠٠٥؛

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

الجلسة العامة ٧٨

٢٠ كانون الأول/ديسمبر ٢٠٠٢

المرفق

عناصر إنشاء ثقافة عالمية لأمن الفضاء الحاسوبي

إن التطورات السريعة في تكنولوجيا المعلومات قد غيرت الطريقة التي يتعين بها على الحكومات والأعمال التجارية والمنظمات الأخرى وفرادى المستخدمين الذين يطورون ويمتلكون ويوفرون ويديرون ويخدمون ويستخدمون نظم وشبكات المعلومات

(''المشتركون'')، تناول مسألة أمن الفضاء الحاسوبي. وستتطلب الثقافة العالمية لأمن الفضاء الحاسوبي من جميع المشتركين تبني العناصر 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؛ وتكون 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؛ وتسمح بتحديد مستوى المجازفة المقبول؛ وتساعد في اختيار الضوابط المناسبة لإدارة الأخطار التي تنطوي على ضرر محتمل بنظم وشبكات المعلومات في ضوء طبيعة وأهمية المعلومات الواجب حمايتها؛

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

(ح) **إدارة الأمن**: ينبغي للمشتركين أن يعتمدوا نهجا شاملا لإدارة الأمن يستند إلى تقييم للأخطار يكون 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.