

Distr.
GENERAL

A/54/213
10 August 1999
ARABIC

ORIGINAL: ARABIC/ENGLISH/
RUSSIAN/SPANISH

الجمعية العامة



الدورة الرابعة والخمسون

البند ٧١ من جدول الأعمال المؤقت*

التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي

تقرير الأمين العام

المحتويات

الصفحة

٢	مقدمة	-	أولا -
٢	الردود الواردة من الحكومات	-	ثانيا -
٢	استراليا		
٣	الاتحاد الروسي		
٩	بروني دار السلام		
٩	بييلاروس		
١٠	عمان		
١٢	قطر		
١٤	كوبا		
١٩	المملكة العربية السعودية		
١٩	المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية		
٢١	الولايات المتحدة الأمريكية		

أولا - مقدمة

١ - في الفقرتين ٢ و ٣ من القرار ٧٠/٥٣ المؤرخ ٤ كانون الأول/ ديسمبر ١٩٩٨، والمعنون "التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي"، دعت الجمعية العامة جميع الدول الأعضاء إلى إبلاغ الأمين العام بآرائها وتقييماتها بشأن المسائل التالية: (أ) التفهم العام لقضايا أمن المعلومات؛ (ب) تعريف المفاهيم الأساسية المتصلة بأمن المعلومات، بما فيها التدخل غير المأذون به في نظم المعلومات والاتصالات السلكية واللاسلكية وموارد المعلومات أو إساءة استخدامها؛ (ج) استصواب وضع مبادئ دولية يكون من شأنها أن تعزز أمن النظم العالمية للمعلومات والاتصالات السلكية واللاسلكية، وأن تساعد في مكافحة الإرهاب والإجرام المتصلين بالمعلومات؛ وطلبت إلى الأمين العام أن يقدم إليها تقريرا في هذا الشأن في دورتها الرابعة والخمسين.

٢ - وفي ١٩ آذار/ مارس ١٩٩٩، وجه الأمين العام مذكرة شفوية إلى الدول الأعضاء طلب إليها فيها تقديم آرائها عملا بدعوة الجمعية العامة. وقد استنسخت أدناه الردود التي وردت من الحكومات.

ثانيا - الردود الواردة من الحكومات

استراليا

[الأصل: بالإنكليزية]

[٢ حزيران/يونيه ١٩٩٩]

١ - تولت استراليا رئاسة فريق الخبراء التابع لمنظمة التعاون والتنمية في الميدان الاقتصادي الذي أعد المبادئ التوجيهية لهذه المنظمة بشأن أمن نظم المعلومات. كما تتولى استراليا رئاسة فرقة العمل التابعة للمنظمة المذكورة والمعنية بأمن المعلومات وسريتها، وهي الفرقة التي تقع عليها المسؤولية، في جملة أمور، عن رصد تطور الحاجة إلى أمن المعلومات. وتشارك استراليا في قيام المنظمة الدولية لتوحيد المقاييس بوضع معايير لأمن تكنولوجيا المعلومات. وعلى الصعيد الداخلي، فإن لدى استراليا عمليات تفصيلية لحماية أمن المعلومات الحكومية، وقامت الهيئة الاسترالية للمقاييس، بالاشتراك مع الهيئة النيوزيلندية للمقاييس، بوضع مقياس مشترك لإدارة أمن المعلومات يقوم على المقياس البريطاني. وتتعاون الحكومة والدوائر الصناعية في استراليا حاليا في اتخاذ خطوات لحماية الهياكل الأساسية الوطنية للمعلومات. وقد أصدرت استراليا تشريعا لحماية نظم الاتصالات السلكية واللاسلكية من التنصت والتدخل وبعض أشكال سوء الاستعمال.

٢ - وهدف أمن المعلومات، كما ورد تفصيلا في المبادئ التوجيهية لمنظمة التعاون والتنمية في الميدان الاقتصادي فيما يتعلق بأمن نظم المعلومات، وكما هو معمول به في استراليا، هو: "... حماية مصالح من يعتمدون على نظم المعلومات من الضرر الناجم عن تعذر التوفر والسرية والسلامة".

٣ - وفي ظل تضافر التكنولوجيات، يمكن توسيع هذا الهدف ليشمل نظم الاتصالات السلكية واللاسلكية التي تمثل نوعا محددًا من نظم المعلومات. فكل تدخل في نظم المعلومات أو إساءة لاستخدامها سيكون له وقع إما على توفر المعلومات أو سريتها أو سلامتها. وهناك خطر مائل هو تطوير أنواع محددة من التكنولوجيا في ظل بيئة آخذة في التغيير بسرعة.

٤ - ولا توافق استراليا على أن إدارة شؤون نزع السلاح التابعة للأمانة العامة للأمم المتحدة هي الهيئة المناسبة للقيام بوضع مبادئ دولية لأمن نظم المعلومات والاتصالات السلكية واللاسلكية العالمية. فالهيكل الأساسية للاتصالات السلكية واللاسلكية والمعلومات تمارس تأثيرا على مسائل التجارة والتنمية الاقتصادية ورفاه المجتمع، فضلا عن إنفاذ القوانين والأمن الوطني. وقد سبق أن وضعت مبادئ وخطوط توجيهية بشأن هذه المسائل في محافل أخرى، مثل منظمة التعاون والتنمية في الميدان الاقتصادي والمنظمة الدولية لتوحيد المقاييس والاتحاد الدولي للاتصالات السلكية واللاسلكية من زوايا أوسع من الزوايا المقترحة في قرار الجمعية العامة ٧٠/٥٣. وبالإضافة إلى ذلك، هناك هيئات دولية، مثل معهد الأمم المتحدة لمنع الجريمة ومعاملة المجرمين في آسيا والشرق الأقصى والمركز الدولي لمنع الجريمة، تعكف حاليا على تناول قضايا الجرائم الحاسوبية. ولا ترى استراليا نفعا في قيام أجهزة أخرى للأمم المتحدة بأعمال تشكل ازدواجا لأعمال يجري الاضطلاع بها في جهات أخرى فيما يتصل بأمن الحواسيب أو سوء استعمالها. وستؤيد استراليا أي اقتراح يدعو إلى إنشاء مورد معلومات عن الأعمال الجاري الاضطلاع بها في محافل أخرى.

الاتحاد الروسي

[الأصل: بالروسية]

[٩ حزيران/يونيه ١٩٩٩]

تعليقات عامة

١ - من بين السمات المميزة للمرحلة الراهنة من التقدم العلمي والتكنولوجي في العالم ثورة المعلومات العالمية - أي التطور السريع والتطبيق العالمي لأحدث تكنولوجيات المعلومات ووسائل الاتصال السلكية واللاسلكية العالمية. ولما كانت ثورة المعلومات تؤثر على جميع مجالات الأنشطة الحيوية للدول، فإنها تهيئ فرصا جديدة لإقامة تعاون دولي وتخلق مجالا عالميا للمعلومات تتحول فيه المعلومات إلى جزء قيم للغاية من ثروات البلاد ومواردها الاستراتيجية.

٢ - وفي الوقت نفسه، صار واضحا، أن الجوانب الإيجابية لتلك العملية تقترن أيضا بخطر حقيقي يتمثل في إمكانية استخدام التطورات في مجال المعلومات لأغراض لا تتفق مع أهداف الحفاظ على الاستقرار والأمن الدوليين، والامتثال لمبادئ تساوي الدول في السيادة، والتسوية السلمية للنزاعات والصراعات، وعدم استعمال القوة، وعدم التدخل في الشؤون الداخلية، واحترام حقوق الإنسان وحرياته.

٣ - إن استخدام أحدث تكنولوجيات المعلومات لبناء القدرات العسكرية للبلدان يغير التوازن العالمي والإقليمي بين القوى ويشير التوتر بين مراكز القوة والنموز التقليدية والناشئة.

٤ - إن مجالا جديدا تماما للمواجهة في الساحة الدولية آخذ في التبلور، وهناك خطر مائل هو أن تؤدي التطورات العلمية والتكنولوجية في ميدان المعلومات والاتصالات إلى تصعيد لسباق التسليح. وفي هذه الحالة سيتأثر كل من الأمن القومي لكل دولة على حدة والنظام العام للأمن الجماعي الدولي على الصعيدين الإقليمي والعالمي.

٥ - ونشير هنا إلى استحداث "سلاح المعلومات" الذي يمكن أن يكون لاستخدامه، حسب مستوى تكنولوجيا المعلومات التي يمتلكها أحد المجتمعات ومدى ضعف هياكله الحيوية، آثار وخيمة مماثلة لآثار أسلحة الدمار الشامل. ومن البديهي أن هذا السلاح يمكن أن تستخدمه الجماعات الإرهابية أو المتطرفة أو جماعات المجرمين فضلا عن منتهكي القوانين من الأفراد.

٦ - وهكذا فإن الطابع العالمي أو السري أو المَغفل لسلاح المعلومات وإمكانية استخدامه على نطاق واسع عبر الحدود الوطنية وتكلفته الاقتصادية وفعالته بصفة عامة تجعل من هذا السلاح وسيلة خطيرة للغاية لممارسة النفوذ، ولا يتضمن القانون الدولي المعاصر أية وسيلة تقريبا لتنظيم إنتاج هذا السلاح واستخدامه.

٧ - وثمة حاجة ملحة في هذا الصدد إلى تنظيم قانوني دولي لتطوير تكنولوجيا المعلومات المدنية والعسكرية في جميع أنحاء العالم، وإلى صياغة سياسة دولية منسقة بشأن أمن المعلومات تلبي احتياجات الأمن الدولي.

التدابير المقترحة

٨ - يمكن أن يستند المجتمع الدولي في بذله لمزيد من الجهود في هذا المجال إلى قرار الجمعية العامة ٧٠/٥٣ المعنون "التطورات في ميدان المعلومات والاتصالات السلوكية واللاسلكية في سياق الأمن الدولي"، الذي اتخذته الجمعية العامة بتوافق الآراء في ٤ كانون الأول/ ديسمبر ١٩٩٨؛ وكان الاتحاد الروسي هو الذي قدم مشروع القرار المتعلق بهذا الموضوع.

٩ - ويجب أن تتخذ الجمعية العامة قرارات بشأن مسألة أمن المعلومات بغية الحد من التهديد باستخدام المعلومات في الأغراض الإرهابية أو الإجرامية أو العسكرية.

١٠ - ولا بد من مواصلة النظر المشترك في الحالة في مجال أمن المعلومات بغية تحديد جميع المواقف والآراء الراهنة ووضعها في الاعتبار عند بذل الجهود المشتركة الرامية إلى النهوض بمفهوم أمن المعلومات.

١١ - ومع تحديد النهج والاتجاهات المشتركة، ينبغي بدء العمل في وضع مبادئ دولية (على سبيل المثال نظام أو مدونة لقواعد السلوك تلتزم بها الدول) بغية تعزيز أمن المعلومات الدولي. ويمكن أن تتخذ هذه المبادئ في البداية شكل إعلان متعدد الأطراف؛ ويمكن إدراجها فيما بعد في صك قانوني دولي متعدد الأطراف. وينبغي للعمل في هذا المجال أيضا أن يتم في إطار مؤتمر نزع السلاح في جنيف.

١٢ - وفي الوقت نفسه، ينبغي للمجتمع الدولي أن ينظر في المبادئ المذكورة آنفا وأن يعتمدها بوصفها مجموعة شاملة، أي أن توضع في الاعتبار التهديدات ذات الطابع العسكري أو الإرهابي أو الإجرامي، ومع استهداف تطبيق تلك المبادئ على كل من الميدانين العسكري والمدني.

التهديدات الرئيسية لأمن المعلومات الدولي

١٣ - تتمثل التهديدات الرئيسية لأمن المعلومات الدولي فيما يلي:

(أ) استحداث واستخدام وسائل تؤثر على موارد المعلومات ونظمها في دولة أخرى أو إلحاق الضرر بها؛

(ب) الاستخدام المتعمد للمعلومات من أجل التأثير على الهياكل الحيوية لدولة أخرى؛

(ج) استخدام المعلومات بغرض تقويض نظام سياسي واجتماعي لإحدى الدول؛ والتأثير النفسي على أحد الشعوب بغرض زعزعة استقرار المجتمع؛

(د) اتخاذ دول لإجراءات بقصد السيطرة على مجال المعلومات والتحكم فيه، ومنع الوصول إلى أحدث تكنولوجيات المعلومات وخلق حالة تكون فيها دول أخرى تابعة تكنولوجيا في مجال المعلومات؛

(هـ) التجاء الجمعيات أو المنظمات أو المجموعات الإرهابية أو المتطرفة أو الإجرامية أو منتهكي القوانين من الأفراد باتخاذ إجراءات تهدد موارد الدولة من المعلومات وهياكلها الحيوية؛

- (و) قيام الدول بصياغة واعتماد خطط أو مبادئ تدعو إلى إمكانية شن حروب معلومات ومن شأنها إثارة سباق التسلح والتسبب في توتر العلاقات بين الدول، والتسبب في حد ذاتها في قيام حروب المعلومات؛
- (ز) استخدام تكنولوجيات المعلومات ووسائلها ضد حقوق الإنسان والحريات في مجال المعلومات؛
- (ح) نشر المعلومات عبر الحدود دون مراقبة في انتهاك لمبادئ القانون الدولي ومعاييرها والتشريعات الداخلية لبلدان بعينها؛
- (ط) التلاعب بتدفقات المعلومات، وبت المعلومات المضللة، وإخفاء المعلومات بغرض تقويض البيئة النفسية والروحية لأحد المجتمعات وإذابة القيم الثقافية والمعنوية والأخلاقية والجمالية؛
- (ي) التوسع في نشر المعلومات واكتساب الهيمنة على الهياكل الأساسية للمعلومات والاتصالات السلكية واللاسلكية الوطنية لدولة أخرى، بما في ذلك شروط تشغيلها في مجال المعلومات الدولي.

المهام والأهداف الرئيسية لوضع نظام دولي لأمن المعلومات

١٤ - ثمة حاجة إلى وضع أساس قانوني دولي لما يلي:

- (أ) تحديد السمات المميزة لحروب المعلومات وتصنيفها؛
- (ب) تحديد السمات المميزة لأسلحة المعلومات وتصنيفها، فضلا عن الطرق والوسائل التي يمكن اعتبارها أسلحة معلومات؛
- (ج) تقييد الاتجار في أسلحة المعلومات؛
- (د) حظر إنتاج أو نشر أو استخدام الأنماط البالغة الخطورة من أسلحة المعلومات؛
- (هـ) منع التهديد بحروب المعلومات؛
- (و) حظر استخدام تكنولوجيات المعلومات ووسائلها لأغراض عدائية، ولا سيما ضد فئات متفق عليها من المرافق؛

(ز) الاعتراف بأن استخدام أسلحة المعلومات ضد الهياكل الحيوية له آثار مماثلة لآثار استخدام أسلحة الدمار الشامل؛

(ح) تهيئة الظروف اللازمة للتبادل الدولي العادل والآمن للمعلومات، على أساس التوازن بين مصالح الفرد والمجتمع والدولة؛

(ط) منع التهديد باستخدام تكنولوجيات المعلومات ووسائلها لأغراض إرهابية أو إجرامية أخرى؛

(ي) منع التهديد باستخدام تكنولوجيات المعلومات ووسائلها للتأثير على الوعي الاجتماعي بغرض زعزعة استقرار المجتمع والدولة؛

(ك) وضع إجراء لتبادل الإخطار عن استخدام المعلومات بطريقة غير مأذون بها للتأثير على دول أخرى، ومنع ذلك الاستخدام؛

(ل) إنشاء آلية لتسوية حالات النزاع في مجال أمن المعلومات؛

(م) وضع نظام دولي لتوثيق تكنولوجيات المعلومات ووسائلها (بما في ذلك البرمجيات والمعدات) بغرض ضمان أمن المعلومات المستخدمة فيها؛

(ن) وضع نظام للتعاون الدولي بين وكالات إنفاذ القانون بغرض منع الجريمة في ميدان المعلومات؛

(س) إنشاء آلية لرصد الامتثال لشروط نظام أمن المعلومات الدولي؛

(ع) تنسيق التشريع الوطني من أجل كفالة أمن المعلومات.

المفاهيم الأساسية المتصلة بأمن المعلومات الدولي

١٥ - تشمل المفاهيم الأساسية المتصلة بأمن المعلومات الدولي ما يلي:

(أ) مجال المعلومات - نطاق النشاط المنطوي على إنتاج المعلومات أو تحويلها أو استخدامها، بما في ذلك الوعي الفردي والاجتماعي، والهياكل الأساسية للمعلومات والاتصالات السلوكية واللاسلكية، والمعلومات نفسها؛

(ب) موارد المعلومات - الهياكل الأساسية للمعلومات (معدات ونظم إنتاج المعلومات وتجهيزها وتخزينها ونقلها)، بما في ذلك ملفات وقواعد البيانات، والمعلومات وتدفقات المعلومات؛

(ج) حرب المعلومات - المواجهة بين الدول في ميدان المعلومات بهدف إلحاق الضرر بنظم المعلومات وعملياتها ومواردها وهيكلها الحيوية، وتقويض النظامين السياسي والاجتماعي لدولة أخرى، فضلا عن التأثير النفسي الشامل على سكان إحدى الدول وزعزعة استقرار المجتمع؛

(د) سلاح المعلومات - الوسائل والطرق المستخدمة بهدف إلحاق الضرر بموارد المعلومات وعملياتها ونظمها في دولة أخرى؛ واستخدام المعلومات ضد نظم إحدى الدول الدفاعية أو الإدارية أو السياسية أو الاجتماعية أو الاقتصادية أو نظمها الحيوية الأخرى، والتأثير الشامل على سكان إحدى الدول بغرض زعزعة استقرار المجتمع والدولة؛

(هـ) أمن المعلومات - حماية المصالح الأساسية للفرد والمجتمع والدولة في مجال المعلومات، بما في ذلك الهياكل الأساسية للمعلومات والاتصالات السلكية واللاسلكية، والمعلومات في حد ذاتها، فيما يتعلق بخصوصيتها، كسلامتها وموضوعيتها وإمكانية الوصول إليها وسريتها؛

(و) تهديد أمن المعلومات - العوامل التي تهدد المصالح الأساسية للفرد والمجتمع والدولة في مجال المعلومات؛

(ز) أمن المعلومات الدولي - حالة العلاقات الدولية التي تمنع انتهاك الاستقرار الدولي وتشكيل تهديد لأمن الدول والمجتمع الدولي في مجال المعلومات؛

(ح) الاستخدام غير المشروع لنظم المعلومات والاتصالات السلكية واللاسلكية وموارد المعلومات - استخدام نظم وموارد الاتصالات السلكية واللاسلكية والمعلومات دون الحصول على التصريح اللازم لذلك أو انتهاكا لقواعد القانون الدولي أو تشريعاته أو معايير المطبقة؛

(ط) التدخل غير المأذون به في نظم المعلومات والاتصالات السلكية واللاسلكية وموارد المعلومات - التدخل في جمع المعلومات أو تجهيزها أو تراكمها أو تخزينها أو البحث عنها أو نشرها أو استخدامها بهدف تعطيل نظم المعلومات عن عملها بصورة طبيعية، أو انتهاك سلامة موارد المعلومات أو سريتها أو إمكانية الوصول إليها؛

(ي) الهياكل الحيوية - مرافق الدولة ونظمها ومؤسساتها، والتأثير المتعمد على موارد المعلومات التي قد يكون لها آثار مباشرة على الأمن القومي (النقل والإمداد بالطاقة، والائتمان والمالية، والاتصالات، والأجهزة الإدارية للدولة، ونظام الدفاع، ووكالات إنفاذ القانون، وموارد المعلومات الاستراتيجية، والمؤسسات

العلمية والتطورات العلمية والتكنولوجية، والمنشآت التي تشكل أخطارا تكنولوجية وبيئية بالغة، وهيئات إزالة آثار الكوارث الطبيعية أو حالات الطوارئ الأخرى)؛

(ك) إرهاب المعلومات الدولي - استخدام نظم وموارد الاتصالات السلكية واللاسلكية أو المعلومات أو التأثير على تلك النظم أو الموارد في مجال المعلومات الدولية لأغراض الإرهاب؛

(ل) جريمة المعلومات الدولية - استخدام نظم وموارد الاتصالات السلكية واللاسلكية أو المعلومات أو التأثير على تلك النظم أو الموارد في مجال المعلومات الدولية لأغراض غير مشروعة.

بروني دار السلام

[الأصل: بالإنكليزية]

[١٧ حزيران/يونيه ١٩٩٩]

فيما يتعلق بقرار الجمعية العامة ٧٠/٥٣ المؤرخ ٤ كانون الأول/ ديسمبر ١٩٩٨، والمعنون "التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي"، تتشرف البعثة الدائمة لبروني دار السلام بأن تحيل آراء وزارة الدفاع في بروني دار السلام الواردة أدناه:

"توافق وزارة الدفاع، بصفتها الوزارة المسؤولة عن الأمن الوطني، على أن أمن المعلومات في عصر تكنولوجيا المعلومات الذي نعيش فيه الآن أمر له أهميته. وترى هذه الوزارة أن كل شكل من أشكال المعلومات يمكن استعماله في تهديد الأمن الوطني لدى بثها يعتبر أمرا هاما، على أن وزارة الدفاع، بسبب ما يربطها من صلات بتكنولوجيا المعلومات ولأن هذه التكنولوجيا تدخل أيضا في اختصاص وزارات أخرى في البلد، ستتعاون مع الهيئات المختصة من أجل الوفاء بمتطلبات القرار. ومن أجل حماية وضمان أمن الاتصالات السلكية واللاسلكية العالمية، ينبغي عدم النظر إلى المسؤولية عن ذلك على أنها تخرج عن اختصاص محكمة العدل الدولية".

بيلاروس

[الأصل: بالإنكليزية]

[٢٥ أيار/ مايو ١٩٩٩]

١ - تؤيد جمهورية بيلاروس تأييدا تاما قرار الجمعية العامة ٧٠/٥٣ المؤرخ ٤ كانون الأول/ ديسمبر ١٩٩٨، المعنون: "التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي". إن التطبيق النشط للجديد من تكنولوجيات المعلومات ووسائل الاتصالات السلكية واللاسلكية يفتح أوسع

الفرص للتطور السريع للحضارة العالمية. وفي الوقت ذاته، فكما جاء في قرار الجمعية العامة ٧٠/٥٣ فإن "هناك احتمالاً في أن] تستخدم هذه التكنولوجيات والوسائل لتحقيق أهداف لا تتفق مع أهداف صون الاستقرار والأمن الدوليين وقد تؤثر تأثيراً سلبياً على أمن الدول".

٢ - لقد جاء اعتماد قرار الجمعية العامة ٧٠/٥٣ في الوقت والحال المناسبين لأنه يلتفت انتباه المجتمع الدولي إلى احتمال استخدام تكنولوجيات المعلومات في شن الحروب وإلى الحاجة إلى منع التكنولوجيات والوسائل الجديدة للمعلومات في سياق عسكري يمكن فيه مقارنتها بأسلحة الدمار الشامل. وعلاوة على ذلك، فبعد اعتماد قرار الجمعية العامة أصبحت هناك إمكانية للنظر تحديداً في مشكلة أمن نظم المعلومات، بما في ذلك التدخل غير المأذون به في نظم المعلومات والاتصالات السلكية واللاسلكية وإساءة استعمالها. وأخيراً، فمن المستصوب وضع واعتماد مفهوم لأمن المعلومات على الصعيد الدولي، ووضع مبادئ قانونية دولية ترمي إلى تعزيز أمن النظم الدولية للمعلومات والاتصالات السلكية واللاسلكية وإلى منع الإرهاب والإجرام في ميدان المعلومات.

عُمان

[الأصل: بالإنكليزية]

[٢٢ حزيران/يونيه ١٩٩٩]

١ - إن الهيئة العامة للمواصلات السلكية واللاسلكية بالسلطنة ليست مسؤولة عن توفير المعلومات للمشاركين، إلا أنها تقوم بتوفير الشبكات والتقنيات التي تسهل النفاذ والوصول إلى أنظمة المعلومات.

٢ - إن الهيئة العامة للمواصلات السلكية واللاسلكية، بصفتها الجهة التي تقوم بتوفير الشبكات والتقنيات، على علم بالفهم العام لقضايا أمن المعلومات. ويمكن الإشارة هنا إلى أن هناك إمكانية لاستخدام التقنيات التي توفرها الهيئة للوصول إلى الاستخدام من قبل بعض الجهات غير المصرح لها بالحصول على هذه المعلومات مما قد يترتب عليه آثار سلبية.

٣ - إن الهيئة بصفتها الجهة التي توفر خدمات الاتصالات السلكية واللاسلكية لا تقع عادة تحت مسؤوليتها أمن معلومات الأشخاص (المشاركين) الذين عليهم وضع الضمانات اللازمة للتأكد من الاحتياجات الأمنية لمعلوماتهم. إلا أن الهيئة يمكنها تقييد النفاذ إلى المعلومات في بعض الحدود (Public domain) لبعض الخدمات مثل الإنترنت.

٤ - أما عن المفاهيم الأساسية المتصلة بأمن المعلومات، فإن الأنظمة المعمول بها في السلطنة، خاصة تلك المتعلقة بحماية حقوق المؤلف، التي تصنف المعلومة بأن لها قيمة مادية ومعنوية وبالتالي توفر لها الحماية القانونية. ويمكن من خلال هذا المبدأ تعريف المفاهيم الأساسية المتصلة بأمن المعلومات، وأهمها:

- (أ) الالتقاط غير المشروع للمعلومات أو البيانات؛
- (ب) الدخول غير المشروع على أنظمة الحاسوب؛
- (ج) التجسس والتنصت على البيانات والمعلومات؛
- (د) انتهاك خصوصيات الغير أو التعدي على حقهم في الاحتفاظ بأسرارهم؛
- (هـ) تزويد البيانات أو الوثائق المخزنة آلياً أيًا كان شكلها؛
- (و) إتلاف وتغيير ومحو البيانات وإعادة استخدامها؛
- (ز) جمع المعلومات وإعادة استخدامها؛
- (ح) تسريب المعلومات والبيانات؛
- (ط) التعدي على برامج الحاسوب سواء بالتعديل أو الاصطناع؛
- (ي) النسخ غير المشروع للبرامج بما يشكل انتهاكاً لقوانين حقوق الملكية الفكرية؛
- (ك) سرقة واستخدام عناوين الشبكات؛
- (ل) تغيير أو إضافة أو حذف معلومات في الرسالة الأصلية أثناء بثها وقبل وصولها إلى الجهة المرسلة إليها؛
- (م) إدخال الفيروسات والعبث بمحتويات الشبكة؛
- (ن) التخريب الفعلي (الجسماني) على الأجهزة والمباني التابعة لها.
- ٥ - أما عن الحلول التي يمكن بها حماية نظم المعلومات فتتمثل فيما يلي:
- (أ) تثقيف العاملين أمنياً بالمخاطر والوقاية منها؛
- (ب) إصدار التصاريح بمختلف أنواعها للمخولين بالدخول للمعلومات حسب تصنيفها (Access control)؛

- (ج) استخدام الهوية الرقمية (التوقيع الرقمي، الشهادات الرقمية) للتخاطب بين المستخدمين الحقيقيين؛
- (د) تشفير المعدات والبرمجيات؛
- (هـ) استخدام السواتر المنيعة (الجدران النارية) لمنع دخول المعلومات التي تم العبث بها؛
- (و) استخدام مضادات الفيروسات.

كما تأمل السلطنة وضع مبادئ دولية تعزز أمن النظم العالمية للمعلومات خاصة وأن السلطنة قد أدخلت خدمة الشبكة العالمية للمعلومات (الإنترنت) مما يجعلها عرضة للمخاطر فيما يتعلق بأمن المعلومات.

قطر

[الأصل: بالانكليزية]

[١٠ حزيران/يونيه ١٩٩٩]

أرسلت السلطات المعنية في دولة قطر المعلومات التالية فيما يتعلق بآرائها وتقييماتها بشأن الفقرتين ٢ و ٣ من قرار الجمعية العامة ٧٠/٥٣ المؤرخ ٤ كانون الأول/ ديسمبر ١٩٩٨:

(أ) التفهم العام لقضايا أمن المعلومات - يمكن تحقيق التفهم العام لقضايا أمن المعلومات عن طريق تبادل الخبرات وإدراك خطر التدخل غير المأذون به، فضلا عن تأثيره على الجوانب الأمنية والمالية؛

(ب) تعريف المفاهيم الأساسية المتصلة بأمن المعلومات - تتمثل المفاهيم الأساسية لتعزيز الأمن في الخطوات التي يجب اتباعها لتأمين طرق ووسائل تبادل المعلومات، فضلا عن التحديات التي تطرأ بشكل غير متوقع، كما هو مبين في الجدولين ١ و ٢ أدناه اللذين يعرضان الخطوات الواجب اتباعها في جميع المراحل لكفالة أمن المعلومات، بالإضافة إلى التحديات الجديدة في هذا الصدد؛

(ج) المبادئ التي من شأنها تعزيز أمن الاتصالات. يمكن أن يتحقق تعزيز أمن المعلومات عن طريق مواصلة التقدم في وسائل نقل المعلومات، والنقاط التالية هي أهم النقاط التي تتعلق بتعزيز أمن الاتصالات، وهي تضع في اعتبارها التكلفة المالية المرتفعة المنطوية على تنفيذها:

'١' استخدام بروتوكولات غير معتادة للاتصالات يمكن تصميمها خصيصا لتبادل معلومات معينة؛

'٢' استخدام نظام ترميز مصمم لغرض محدد ولا ينبغي استخدامه في برامج تنتج بكميات تجارية؛

'٣' إجراء تغييرات في توقيعات مختلفة وبترميز مختلف.

الجدول ١ - حلول أمن الشبكات

خطوات الأمن

الوظيفة	الحل الأمني	التهديد
يرمز البيانات لمنع التلاعب بها	ترميز البيانات (معايير ترميز البيانات، وخوارزم RSA)	التنصت على البيانات أو قراءتها أو تعديلها بطرق غير مشروعة
يحدد ويدير امتيازات المستخدم	برمجيات للتحكم في الوصول	وصول أحد المستخدمين الشرعيين إلى بيانات غير مسموح له بالوصول إليها
تقنية تشمل برمجيات للترميز وبطاقات مرمزة للتحقق من هوية كل من المرسل والمستقبل	التحقق من الهوية	قيام أحد المستخدمين بالتلاعب في تقديم هويته لارتكاب عملية تدليس
ينقي ويمنع بعض حركات الدخول إلى الشبكة أو الخادم	الساتر المنيع	وصول أحد المستخدمين غير المأذون لهم باستخدام شبكة ما إلى شبكة أخرى
تسد الثغرات المعروفة في نظام التشغيل	أدوات نظام التشغيل	استغلال أحد قرصنة الحاسوب ثغرات في نظام تشغيل الخادم بغرض الوصول إلى المعلومات والتلاعب بها

الجدول ٢ - تحديات الأمن

التحديات	التغيرات
أمنها مهدد للأسباب التالية:	شبكة اليوم:
تسهل سرقة الحواسيب المحمولة يمكن استغلال الوصلات اللاسلكية بسهولة أكبر يصعب حماية المواقع البعيدة ينسى المستخدم كلمة السر أو يسجل كلمات سر متعددة يدخل قرصنة الحاسوب على الشبكات العامة ينطوي نظام التشغيل يونيكس على أوجه ضعف خاصة	تتألف من عدد متزايد من الحواسيب المحمولة بها عدد أكبر من الوصلات اللاسلكية أكثر تفرقا من الناحية الجغرافية تربط بين مجموعة أكثر تنوعا من أنظمة التشغيل يتزايد اتصالها بالشبكات العامة مثل الإنترنت كثيرا ما تستخدم حواسيب تعمل بنظام "يونيكس"

كوبا

[الأصل بالاسبانية]

[٢٨ حزيران/يونيه ١٩٩٩]

تقييم عام لمسائل أمن المعلومات

١ - يشير الاستخدام الواسع الانتشار لتكنولوجيات المعلومات في معظم مجالات النشاط الإنساني، الذي كان يسمى "حوسبة المجتمع" ويطلق عليه كثيرون "عصر المعلومات" بسبب اعتماد العالم المتزايد على نظم المعلومات، يشير مشاكل أمنية جديدة يلزم النظر فيها بقدر كبير من الجدية ليس من جانب كل دولة فحسب بل من جانب المجتمع الدولي بأسره.

٢ - ولهذا السبب تعتبر الأمم المتحدة المحفل المناسب لمناقشة السبل والوسائل المناسبة للتصدي للأخطار المحتمل أن تلحق بالمجتمع الدولي من جراء استعمال التكنولوجيات الجديدة للمعلومات والاتصالات السلكية واللاسلكية في الأغراض غير السلمية.

٣ - وفضلا عن ذلك، يجب اتخاذ التدابير اللازمة لإتاحة تلك التكنولوجيات لتنمية جميع الدول، وبخاصة البلدان المتخلفة النمو التي تفتقر إلى الموارد الكافية لتطوير تلك التكنولوجيات بذاتها.

٤ - ومن ناحية أخرى، فقد أصبحت العولمة بالفعل حقيقة واقعة في مجال المعلومات والاتصالات السلكية واللاسلكية، إذ لم تعد المسافات تشكل عتبة في سبيل تبادل المعلومات؛ وفي الوقت ذاته، تتعرض النظم التي تيسر هذا التبادل للمعلومات لأخطار أمنية متزايدة. ويجب التأكيد على أن العولمة تستتبع مستوى ما من توحيد المقاييس، الأمر الذي يزيد من سهولة التدخل في تلك النظم.

٥ - ويجب ألا ننسى أننا نقصد بحدوثنا التكنولوجيات التي تنشأ في البلدان المتقدمة النمو، التي تحتل بينها الولايات المتحدة الأمريكية، أكبر قوة متسلطة في العالم، وبخاصة في ميدان المعلومات والاتصالات السلكية واللاسلكية، موقعا بارزا يمكنها من فرض معاييرها التكنولوجية وييسر استخدام نظم المعلومات والاتصالات السلكية واللاسلكية كوسيلة للعدوان.

٦ - وعلى النقيض من ذلك، ليس لدى البلدان المتخلفة النمو وسيلة أخرى غير قبول تلك التكنولوجيات لكي يكتب لها البقاء في ظل تلك الظروف الجديدة، ولا تكون تلك البلدان في معظم الأحيان مدركة تماما للأخطار التي ينطوي عليها استعمال تلك التكنولوجيات وكثيرا ما لا تستخدم الترتيبات أو الخدمات أو الآليات الأمنية استخداما كافيا. ويؤدي ذلك إلى انكشاف نظم معلوماتها، الأمر الذي يمكن أن يفضي، بسبب الاستعمال الواسع الانتشار لتكنولوجيات المعلومات والاتصالات السلكية واللاسلكية في جميع ميادين التنمية البشرية، إلى إفراز أوضاع تهدد الأمن الدولي.

٧ - ويسر كوبا جدا أن تتاح لها فرصة النظر في هذا البند في الجمعية العامة عملاً بالمبادرة التي أفضت إلى اعتماد قرار الجمعية العامة ٧٠/٥٣ بتوافق الآراء. وتدرك كوبا أهمية ذلك البند وستشارك بنشاط في عمليات التقييم التي دعا إليها القرار المذكور.

تعريف المفاهيم الأساسية المتصلة بأمن المعلومات،
بما في ذلك التدخل دون إذن في نظم المعلومات والاتصالات
السلكية واللاسلكية وموارد المعلومات أو إساءة استعمالها

٨ - يشهد العالم الذي نعيش فيه زيادة غير مسبوقه في استعمال تكنولوجيا المعلومات والاتصالات السلكية واللاسلكية، وهو ما أدى مع الأسف إلى إمكانية استعمالها في تحقيق أغراض عدائية تنفيذاً لسياسات عدوانية تبنتها بعض الدول تجاه دول أخرى.

٩ - ويجدر بالإشارة في هذا الصدد أن نمو وشعبية الشبكات العالمية، ولا سيما الإنترنت، كانت لهما نتائج مهمة. فنظم المعلومات والاتصالات السلكية واللاسلكية، رغم الاستعمال المتزايد لها، لا يزال يجري تشغيلها على أساس تعاوني بحث. وهذا أمر له أهميته بالنظر إلى أن الطابع الطوعي للإنترنت هو مصدر قوتها وأكبر نقطة ضعف فيها في الوقت ذاته.

١٠ - ومجموعة القواعد الموحدة الموضوعة لضمان فعالية وتعزيز الأمن التشغيلي للشبكات العالمية هي مجموعة قواعد طوعية لأن البلدان لم تعتمد تشريعات موحدة بشأن تشغيل شبكات المعلومات.

١١ - بيد أنه بالنظر إلى أن الارتباط بتلك الشبكات العالمية هو أمر اختياري، فإن من المعقول أن نذهب إلى ضرورة أن تكون أي قاعدة للسلوك تنظم تشغيل تلك الشبكات جزءاً من الاتفاق المتعلق بذلك الارتباط، وأن انتهاك تلك القواعد، بصرف النظر عن الهياكل الأساسية القانونية القائمة، يمكن أن يؤدي إلى توقيع عقوبات.

١٢ - ويتضمن أمن المعلومات حماية سريتها (فينبغي ألا تتاح إمكانية الوصول إلى المعلومات إلا لمن لهم الحق في استعمالها)، وحماية المعلومات من تعديلها دون إذن (سلامتها)، وحماية النظم من حرمانها من الخدمات (التوافر) ومن الوصول إليها دون إذن.

١٣ - وفي هذا السياق، يجب أخذ بعض المعايير الأساسية في الاعتبار:

(أ) يتحمل المستعملون مسؤولية سلوكهم الخاص بهم؛ بمعنى أن الدخول على حاسوب دون إذن أو استعمال شبكة ما بغير إذن يشكلان انتهاكاً صريحاً لقواعد السلوك، مهما كان ضعف السبل المستخدمة في حماية نظم المعلومات؛

(ب) تتحمل المنظمات التي تستعمل تلك التكنولوجيات المسؤولية عن استعمال موظفيها لتلك التكنولوجيات بالصورة الملائمة ولذا ينبغي لها أن تضع سياسات أمنية لهذا الغرض، فضلا عن تدابير وإجراءات تكفل مراقبتهم. كما ينبغي لكل بلد أن يضع الآليات المناسبة لضمان امتثال المنظمات الموجودة في أراضيها لتلك المتطلبات؛

(ج) يتحمل مقدمو الخدمات والشبكات الحاسوبية المسؤولية عن الحفاظ على أمن النظم التي يقومون بتشغيلها. كما يتحملون المسؤولية عن إعلام المستعملين بسياساتهم الأمنية وبأي تغيير يطرأ على تلك السياسات؛

(د) يتحمل بائعو وموردو النظم المسؤولية عن توفير نظم يعول عليها تتضمن ضوابط أمنية مناسبة. ويجب على البائع أو المورد تقييم كل نظام من حيث الضوابط الأمنية قبل طرح النظام في الأسواق. ويجب أن يرد في كل منتج وصف للخصائص الأمنية التي يضمنها. والبائعون والموردون ملزمون بإصلاح أوجه الخلل في الأجزاء ذات الصلة في النظم التي يبيعونها أو يوزعونها، وذلك دون مقابل؛

(هـ) يتحمل المستعملون ومقدمو الخدمات وبائعو البرامجيات والمعدات الحاسوبية المسؤولية عن التعاون في توفير الأمن. ومن المأمول فيه أن يقوم كل موقع بإبلاغ الموقع الآخر إذا اكتشف أن موقعا ما يتعرض للاختراق، وأن يساعد بعضها بعضا في اتخاذ تدابير لمواجهة انتهاكات الأمن. ويمكن أن تتضمن تلك المساعدة تعقب التوصيلات، وكشف الانتهاكات، والمساعدة القانونية.

١٤ - وتمثل الأهداف الرئيسية للشخص الذي يعتدي على شبكات المعلومات فيما يلي:

(أ) الحصول على المعلومات أو تغييرها أو إتلافها. ولا شك في أن ذلك هو الهدف الرئيسي لمعظم المعتدين؛

(ب) اقتحام حواسيب الغير واستعمالها كما لو كان من المستعملين المأذون لهم باستعمالها؛

(ج) التمهيد لمزيد من الاعتداءات. فيمكن اقتحام بعض النظم لغرض واحد هو استخدام تلك النظم في القيام باعتداءات جديدة؛

(د) الحرمان من الخدمة، بمعنى جعل المعلومات غير متاحة لشخص ما يكون في حاجة إليها ومن حقه الحصول عليها؛

(هـ) اكتساب شهرة، وذلك مفيد جدا في حالة حواسيب خدمة الشبكة.

١٥ - وتشكل إساءة استعمال نظم المعلومات والاتصالات السلكية واللاسلكية وموارد المعلومات، وخاصة عندما تستعمل بعض الدول تلك النظم والموارد لتنفيذ سياساتها الخاصة بالتدخل في شؤون الدول الأخرى، عدوانا على سيادة الدول المتأثرة واستقلالها وتوجد مراكز توتر يمكن أن تشكل تهديدا خطيرا للأمن الدولي.

١٦ - وتستتبع الجهود المتواصلة التي تبذلها الدول لتحقيق غايات سياسية تخدم مصالحها الوطنية الاستعمال غير الصحيح، أي الذي لا يتماشى مع المعايير الدولية المقررة، لوسائل منها محطات الإذاعة والتلفزيون لزعزعة النظام الدستوري للدول الأخرى التي تعتبرها تلك الدول أعداء لها.

١٧ - وكوبا هي مثال على الدول المتأثرة بالسياسات المشار إليها في الفقرة المتقدمة. وإعطاء فكرة عن خطورة المسألة، نذكر أن كوبا تتعرض منذ عدة عقود للعدوان عبر إذاعة وتلفزيون الولايات المتحدة، كجزء من سياسة عدوانية متواصلة تنتهجها أكبر قوة عسكرية واقتصادية وسياسية في العالم هدفها المعلن هو قلب نظام الحكم في كوبا.

١٨ - وتحقيقا لهذه الغاية، كانت في إقليم الولايات المتحدة الأمريكية حتى ١٧ نيسان/أبريل ١٩٩٩، على سبيل المثال، ما مجموعه ١٧ محطة تبث معلومات تخريبية إلى كوبا.

١٩ - وكان يبث كل يوم ما يتراوح بين ٢٨٨,٥ ساعة من المواد الإذاعية عبر الموجات المتوسطة والقصيرة وموجات التشكيل الترددي؛ أي ٢٠٨٤,٥ ساعة كل أسبوع، وإذا أضفنا إلى ذلك المواد التلفزيونية التي كانت تبث كل أسبوع، فإن مجموعها يصل إلى ٢٠٨٩ ساعة.

٢٠ - وفي معظم الحالات، كانت تلك المحطات تحرض المواطنين الكوبيين على ارتكاب أعمال عصيان مدني والقيام بأفعال تخريبية وإرهابية.

٢١ - ولقد كانت كوبا تؤيد دوما حل الخلافات بين الدول على أساس المساواة واحترام السيادة الوطنية لتلك الدول واستقلالها وأعربت عن ذلك علنا في مناسبات مختلفة. ولا يزال هذا الموقف قائما دون تغيير.

استصواب وضع مبادئ دولية تعزز أمن النظم العالمية
للمعلومات والاتصالات السلكية واللاسلكية وتساعد في
مكافحة الإرهاب والإجرام في مجال المعلومات

٢٢ - لا شك في أن تطوير تكنولوجيات المعلومات الجديدة يقتضي بذل جهود متوازية لضمان التطوير التدريجي للقانون الدولي في ذلك المجال، بما في ذلك وضع الإطار القانوني المناسب الذي من شأنه أن يعزز أمن نظم المعلومات.

٢٣ - ولن يكون ذلك مهمة يسيرة، إذا أخذنا في اعتبارنا أنه لا تزال هناك مسائل تقتضي وضع تعاريف تحظى بقبول عام لتيسير التدوين اللاحق لمبادئ جديدة تساعد في تحقيق الأهداف المرجوة في مجال الأمن.

٢٤ - ويتجاوز طابع الشبكات العالمية ذاته حدود الولاية القضائية لكل بلد؛ ويؤدي ذلك في كثير من الحالات إلى استحالة الاعتماد على الحدود الجغرافية. وفضلا عن ذلك، يؤدي تفاوت الدول في النمو، بين عوامل أخرى، إلى صعوبة وضع قواعد تنظيمية دولية موحدة يمكن تطبيقها على جميع البلدان التي تستعمل تلك التكنولوجيات.

٢٥ - بيد أن البداية لن تكون من الصفر، لأنه توجد فعلا مبادئ تحظى بقبول عام وصكوك قانونية دولية اتفقت عليها الدول وأقرتها في محافل شتى متعددة الأطراف في سياق مواكبة التطورات التكنولوجية الأخيرة. ومن شأن تلك المبادئ والصكوك أن تكون مفيدة جدا في ترسيخ المبادئ الدولية القائمة لتعزيز أمن النظم العالمية للمعلومات والاتصالات السلكية واللاسلكية والمساعدة في مكافحة الإرهاب والإجرام في مجال المعلومات، أو في وضع مبادئ دولية جديدة لتحقيق هذين الهدفين.

٢٦ - ولإيراد بضعة أمثلة ذات صلة على تلك الصكوك، فإن كوبا ترى أنه ينبغي أخذ ما يلي في الاعتبار:

(أ) قرار الجمعية العامة ١١٠ (د - ٢) المؤرخ ٣ تشرين الثاني/نوفمبر ١٩٤٧، الذي يدين الدعاية التي تستهدف التحريض أو التشجيع على أي تهديد للسلام، أو على خرق السلام، أو على عمل من أعمال العدوان؛

(ب) الاتفاقية الدولية للاتصالات السلكية واللاسلكية، المعتمدة في نيروبي في عام ١٩٨٢، والصكوك القانونية الدولية ذات الصلة التي اعتمدها منظمة الأمم المتحدة للتربية والعلم والثقافة والاتحاد الدولي للاتصالات السلكية واللاسلكية؛

(ج) المبادئ المنظمة لاستخدام الدول للسواتل الأرضية في الإرسال التلفزيوني الدولي المباشر، التي اعتمدها الجمعية العامة والتي تنص على أنه ينبغي الاضطلاع بتلك الأنشطة على النحو الذي يتفق والقانون الدولي ويتمشى مع تنمية التفاهم المتبادل وتعزيز العلاقات الودية والتعاون فيما بين الدول والشعوب لصالح صون السلام والأمن الدوليين؛

(د) اتفاقية حظر استحداث وإنتاج وتخزين واستعمال الأسلحة الكيميائية وتدمير تلك الأسلحة، التي يتضمن مرفقها أحكاما بشأن حماية المعلومات السرية التي يمكن أن تستخدم كمرجع مفيد في وضع المبادئ السالفة الذكر.

٢٧ - وأخيراً، وكجزء من الدور الريادي الذي ينبغي للأمم المتحدة أن تضطلع به في الدراسات التحليلية التي قد يتم إجراؤها بشأن هذا الموضوع، ترى كوبا أنه ينبغي للمنظمة أن تقوم بأمور منها التسليم بأن لكل بلد الحق في حماية نظم معلوماته واتصالاته السلكية واللاسلكية باستخدام نظم مؤمنة للحماية، والتوصية بأن تعتمد الدول الأعضاء قوانين تعاقب على إنشاء ونشر الفيروسات الحاسوبية والبرامج الضارة الأخرى. وفضلاً عن ذلك، يمكن في إطار الأمم المتحدة إبرام اتفاقات متعددة الأطراف ملزمة قانوناً تحظر الاعتداء على نظم المعلومات والاتصالات السلكية واللاسلكية. ويمكن أيضاً النظر في إبرام اتفاقات تضمن استعمال التكنولوجيات الجديدة الجاري تطويرها في الأغراض السلمية، وتكفل توافرها لجميع الدول.

المملكة العربية السعودية

[الأصل: بالعربية]

[٢٧ أيار/ مايو ١٩٩٩]

إن التقدم في مجال تقنية المعلومات جعل الكثير من المؤسسات الحكومية والخاصة في كل دولة تعتمد اعتماداً متزايداً على أنظمة المعلومات الآلية، إلا أنه يواكب هذا التطور تطوراً في عمليات الاختراق والتهديد والعبث بهذه الأنظمة من خلال جهات دولية هدفها التخريب والإرهاب، مما يسبب ضرراً في مختلف المجالات الاقتصادية والاجتماعية والأمنية، ولا بد من وضع مبادئ وقوانين دولية لمكافحة التهديد والعبث بأمن المعلومات ومحاربة وتجريم هذه الأعمال دولياً وبالتالي محاكمة ومعاينة مرتكبيها عبر المنظمات الدولية المعنية.

المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية

[الأصل: بالإنكليزية]

[٣٠ أيار/ مايو ١٩٩٩]

نظرة عامة

١ - لقد بلغ الوصل العالمي للنظم القائمة على المعلومات اليوم حداً يجعل العديد من الدول، إن لم نقل جميعها، يواجه إمكانية التعرض لخطر يهدد عناصر هامة من هيكلها الأساسية الحيوية من جراء هجمات إلكترونية يقوم بها مجرمون وإرهابيون. ورغم أن التعرض لخطر الهجوم الإلكتروني قد يكون طفيفاً في الوقت الراهن، إلا أنه سيزداد مع مرور الوقت حيث أن اعتماد القطاعين العام والخاص على السواء على نظم الحاسوب التي يتزايد اتصال بعضها ببعض في ارتفاع مستمر. وفضلاً عن ذلك، وبما أن النظم أصبحت موصولة بعضها ببعض دولياً، أخذ الخطر يعبر الحدود الوطنية. وبالتالي فإن المحاولات الإجرامية والإرهابية لاختراق نظمنا لأغراض خبيثة تمثل تحدياً يواجه جميع الدول الأعضاء في الأمم المتحدة. ولذا

ترحب المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية ببدء الأعمال الهادفة إلى البحث عن وسائل، انفرادية أو متعددة الأطراف، يمكننا بواسطتها السعي إلى المحافظة على سلامة هياكلنا الأساسية الحيوية القائمة على المعلومات من مثل هذه الهجمات.

الإجراءات المحلية

٢ - ومن أجل تحقيق ذلك، أعلنت حكومة جلالة الملكة، في كانون الثاني/يناير ١٩٩٩، اتخاذ خطوات تهدف إلى التقليل إلى أدنى حد ممكن من إمكانية تعرض الهياكل الأساسية الوطنية الحيوية للمملكة المتحدة لهجوم إلكتروني. وهذه التدابير المحلية تشمل ما يلي:

(أ) ضمان أن يجري، داخل الحكومة، تعيين جميع النظم الحيوية، وأن تجري إدارة عملية حماية تلك النظم وإخضاعها للرقابة على نحو فعال؛

(ب) العمل مع القطاع الخاص لوضع تدابير تجاري تفاقم مستوى الخطر ولكفالة مستويات وافية من حماية النظم الرئيسية المندرجة ضمن الهياكل الأساسية القومية الحيوية؛

(ج) زيادة الوعي ومستويات أمن المعلومات على نحو أعم في القطاع الخاص بمواصلة المبادرات القائمة لتعزيز أفضل الممارسات.

الإجراءات الدولية

٣ - في الوقت نفسه، فإن الوصل العابر للحدود يترتب عليه امتداد آثار الهجمات الموجهة ضد النظم في الدول الأخرى إلى الهياكل الأساسية الوطنية الحيوية للمملكة المتحدة، واحتمال أن يسعى إرهابيون ومجرمون، يعملون انطلاقاً من بلد ثالث، إلى مهاجمة نظم المملكة المتحدة ذاتها. ولهذا فإن المملكة المتحدة تسلّم بأن التعاون الدولي أمر أساسي لمكافحة التهديد بالهجمات الخبيثة، وهي تسعى إلى تعزيز الحوار الجاري بشأن هذه المسائل مع شركائها الدوليين. وينضوي تحت ذلك، العمل ضمن فريق جرائم التكنولوجيا العالية المعني بالمساعدة القانونية المتبادلة التابع لمجموعة الثماني، وفي مجلس أوروبا بشأن وضع اتفاقية عن الجرائم الإلكترونية.

٤ - وترى المملكة المتحدة أنه ينبغي للأمم المتحدة رصد العمل الجاري في هذين المحظنين وفي المحافل الأخرى حتى تقيّم، حين يؤون الأوان، نوع الإجراءات الموضوعية التي يمكن أن تساهم بها في هذا الميدان على نحو مفيد. ويمكن لهذه الإجراءات أن تشمل وضع مبادئ دولية لزيادة أمن النظم العالمية والمساعدة على مكافحة الإرهاب والإجرام في مجال المعلومات.

الولايات المتحدة الأمريكية

[الأصل: بالانكليزية]

[٢٠ أيار/ مايو ١٩٩٩]

التفهم العام لقضايا أمن المعلومات وتعريف المفاهيم الأساسية

١ - ترى الولايات المتحدة الأمريكية أن أمن المعلومات هو موضوع واسع ومعقد. وهو يشمل عوامل عديدة ويؤثر في العديد من الأنشطة المتنوعة للأفراد والجماعات والحكومات. ورغم أن الموضوع العام يشمل جوانب تتصل بالسلام والأمن الدوليين (نطاق عمل اللجنة الأولى)، إلا أنه يتضمن أيضا جوانب تقنية تتصل بالاتصالات العالمية، وكذلك مسائل غير تقنية تتصل بالتعاون الاقتصادي والتجارة، وحقوق الملكية الفكرية، وإعمال القوانين، والتعاون في مجال مكافحة الإرهاب، ومسائل أخرى ينظر فيها في إطار اللجنتين الثانية والسادسة. ولا تعتبر الإجراءات والبرامج الحكومية المجال الوحيد المناسب لتركيز الاهتمام لأن أمن المعلومات ينطوي أيضا على مسائل هامة تشغل الأفراد والمشاريع والمؤسسات التجارية والمنظمات الأخرى النشطة في القطاع الخاص.

الجوانب المتعلقة بالأمن الدولي

٢ - خلال الصراعات المسلحة، استخدمت الأمم تقنيات شتى تتصل بأمن المعلومات. وليس التشويش باستخدام الترددات اللاسلكية والتدابير الكهرطيسية المضادة سوى مثالين جليين على ذلك؛ فهذه التقنيات قديمة جدا. وفي المستقبل، سيكون من المهم بالنسبة للقوات العسكرية أن تحمي ما تمتلكه من وصلات البيانات والنظم الأخرى المتصلة بالحاسوب. وبالإضافة إلى ذلك، فإن الدول الأعضاء بحاجة إلى امتلاك القدرة على إصلاح نظم المعلومات الرئيسية إن أدت كوارث طبيعية أو نكبات طارئة إلى تعطيل مرافق الاتصالات الرئيسية أو غيرها من شبكات البيانات في القطاعين العام والخاص. ويمتد إطار أمن المعلومات ليشمل أيضا حماية المعلومات المتصلة بالقدرة العسكرية وغير ذلك من أوجه الأمن الوطني.

العوامل الاقتصادية والتجارية والتقنية

٣ - يشمل أمن المعلومات ضرورة حماية البحوث العلمية ذات الطابع التجاري وكذلك تكنولوجيات الإنتاج وغير ذلك من أنماط البيانات المتعلقة بحقوق الملكية (مثل خطط التسويق والمعلومات المتصلة بخدمة الزبائن).

٤ - ويتصل أمن المعلومات أيضا بالحاجة إلى أعمال الاتفاقات الدولية بشأن الملكية الفكرية (من قبيل المواد المرثية والسمعية، وكذلك برامجيات الحاسوب) من أجل حمايتها من النسخ والبيع غير المجازين. كما أن حماية الخصوصية تمثل جانبا آخر من جوانب أمن المعلومات، أي كفالة أمن المعلومات الشخصية والتجارية المنقولة عبر الشبكة الدولية العامة أو عبر وصلات البيانات الخاصة.

٥ - وعلى المستوى التقني، تكفل قواعد الاتحاد الدولي للاتصالات السلكية واللاسلكية والأنشطة التي يضطلع بها النظراء الوطنيون تلاؤم الإشارات الإلكترونية، والاستخدام المناسب للطيف الكهرومغناطيسي، وإمكانية الاعتماد الواسع على الشبكة الدولية. وتنطبق هذه الوظائف بالمثل على السواتل التي توفر نطاقا واسعا من الخدمات، مثل ترحيل الصوت والبيانات، وكذلك تحديد المواقع وغير ذلك من المعلومات المستخدمة في الملاحة الجوية والبحرية وفي خدمات البحث والإنقاذ. وبالإضافة إلى ذلك، فإن التصميم ومعايير السلامة تمنح قدرا كبيرا من الطمأنينة لمصنعي ومستخدمي الأجهزة الإلكترونية، بما فيها الحاسوب. وجميع هذه الوظائف التنظيمية والإدارية يمكن أن تنضوي في إطار المفهوم الواسع لأمن المعلومات.

إعمال القوانين والتعاون في مناهضة الإرهاب

٦ - لقد أدى الاعتماد الواسع على التكنولوجيات القائمة على المعلومات إلى درجة غير مسبوقة من الاتصال والترابط على الصعيد العالمي، ويترتب على ذلك أن جوانب عديدة من النشاط الوطني والدولي، في القطاعين العام والخاص على السواء، يمكن أن تكون مهددة نظريا بإساءة الاستعمال الإجرامية أو الإرهابية.

٧ - وفي حين تتفاوت درجة الاعتماد على تكنولوجيا المعلومات من دولة لأخرى، فإن اتساع مجال الأنشطة التي تعتمد على هذه الاتصالات - الاقتصادية والتجارية والصناعية والتعليمية والقانونية - يعني أن من المحتمل أن تصبح جميع الدول عرضة لنتائج الاستغلال الإجرامي. وعلاوة على ذلك، يتوقع أن يزيد هذا الاعتماد حيث أن هذه التكنولوجيات ستصبح تدريجيا جوهرية لتسيير أعمال الحكومات بشكل مستقر وكذلك لصيانة النظم العالمية الرئيسية في المجال التجاري ومجال الاتصالات التي تؤمن استمرار الاتصالات بين الدول.

٨ - ولذا فإن الولايات المتحدة تعتبر أن إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية يمثل تحديا يواجه مصالح جميع الدول، وهي تشاطر الدول الأخرى اهتمامها بالسعي إلى تعزيز الوسائل الملائمة، على الصعيدين الانفرادي والمتعدد الأطراف، من أجل ضمان سلامة مواردنا التي تعتمد على تكنولوجيا المعلومات.

٩ - وبالمثل، تعتبر الولايات المتحدة أن أي اقتحام غير مشروع أو أي محاولة لتعطيل أو تغيير أي جانب من جوانب النظم الوطنية للمعلومات فيها، يمثل خطرا محتملا يهدد هيكلها الأساسية الوطنية

الحيوية، وبالتالي فهو يمثل تهديدا لمصالحها الوطنية. إن الولايات المتحدة، إدراكا منها للخطورة المحتملة لهذا التهديد، قد شرعت على الصعيد الوطني ببرامج طويلة الأجل، على المستويين العام والخاص، مصممة بحيث تحمي هياكلها الأساسية الوطنية الحيوية. ولكن الولايات المتحدة تدرك أيضا أن نجاح جهودها الوطنية في حماية نظمها القائمة على المعلومات سيتوقف في النهاية، جزئيا، على مستوى الأمن الذي تتمتع به تلك النظم الموصولة بها والواقعة خارج حدودها، وذلك نتيجة الترابط العالمي المتزايد للعديد من الهياكل الأساسية الحيوية.

١٠ - ولذلك فإن الولايات المتحدة تعتقد أنه ينبغي لجميع الدول أن تتخذ خطوات على الصعيد الوطني لتضمن سلامة نظم المعلومات الوطنية فيها وإمكانية محاكمة المجرمين والإرهابيين الدوليين العاملين ضمن حدودها الوطنية الذين يحاولون تعطيل تلك النظم بأقصى ما يسمح القانون بفرضه من عقوبات. ويقع على كل دولة أن تتخذ الإجراءات لضمان أن تكون نظم المعلومات فيها موثوقة وبمناى عن إساءة الاستعمال أو الحرمان من تقديم الخدمات لأغراض إجرامية، وأن يكون من الممكن إصلاح نظم المعلومات بسرعة إن حدث أي خلل في سير عملها.

١١ - ويحظر القانون الجنائي للولايات المتحدة العبث بالهياكل الأساسية للمعلومات في الولايات المتحدة. وتحث الولايات المتحدة جميع الدول على إعادة النظر في نظمها القانونية الوطنية لضمان أن تنص هذه القوانين على إمكانية فرض العقوبات المناسبة فيما يتعلق بالأعمال ذات الصلة بإساءة استعمال نظم المعلومات لأغراض إجرامية أو إرهابية. ولقد وجدت الولايات المتحدة مرارا أن من الضروري تعديل قوانينها المتصلة بالحاسوب بغية تحسينها وبغية التصدي للمشاكل الجديدة.

استصواب وضع مبادئ دولية

١٢ - كما أشرنا في السابق، فإن أمن المعلومات موضوع واسع ومعقد، وله أبعاد عديدة تتصل بعضها ببعض بطرق شديدة التعقيد. ونظرا للحاجة الواضحة إلى تحليل جميع جوانب أمن المعلومات والتوصل إلى فهم لكيفية تفاعلها، فمن السابق لأوانه صياغة مبادئ شاملة تتصل بأمن المعلومات من جميع جوانبه. وعوضا عن ذلك، يحتاج المجتمع الدولي إلى إمعان التفكير بصورة منهجية قبل اتخاذ أي خطوات إضافية. ولتيسير ذلك، ينبغي للدول الأعضاء أن تستعين، كل في بلدها ومجتمعها، بأفكار ومعلومات يقدمها عدد كبير ومتنوع من الخبراء.

١٣ - وقد أصبح من الجلي الآن أن التعاون الدولي أمر أساسي للمكافحة الفعالة للمسائل المستجدة والمعقدة التي يسببها الإرهاب والإجرام في مجال المعلومات. وفي الوقت الراهن، ثمة جهود متعددة الأطراف عديدة تتناول موضوع التعاون الدولي. فمجلس أوروبا يدرس مشروع اتفاقية عن الجرائم الإلكترونية؛ وفريق جرائم التكنولوجيا العالية التابع لمجموعة الثماني ينظر في اتخاذ تدابير فيما يتعلق

بالمساعدة القانونية المتبادلة وما يتصل بها من مسائل جرائم التكنولوجيا العالية. كما أن منظمة الدول الأمريكية أنشأت فريقاً لدراسة هذه المسائل؛ ويقوم معهد الأمم المتحدة لمنع الجريمة ومعاملة المجرمين في آسيا والشرق الأقصى بدراسة المسائل المتصلة بالموضوع ضمن إطار الأمم المتحدة.

١٤ - وجميع هذه الجهود المبذولة قيّمة وينبغي بالتأكيد تطويرها كي تؤتي ثمارها. وليس من الحكمة أبداً أن تقوم الأمم المتحدة بوضع استراتيجيات أو القيام بأنشطة قد تؤدي إلى إبطال أو عرقلة العمل الذي بدأه المجتمع الدولي بالفعل.
