

Distr.: General
2 July 2007
Arabic
Original: Arabic/Chinese/English/
French/Spanish

الجمعية العامة



الدورة الثانية والستون

البند ٩٥ من القائمة الأولية*

التطورات في ميدان المعلومات والاتصالات
السلوكية واللاسلكية في سياق الأمن الدولي

التطورات في ميدان المعلومات والاتصالات السلوكية واللاسلكية في
سياق الأمن الدولي

تقرير الأمين العام

المحتويات

الصفحة

١	أولا - مقدمة
٣	ثانيا - الردود المتلقاة من الحكومات
٣	بروني دار السلام
٨	بروكينا فاسو
١٠	شيلي
١١	الصين
١٣	كوبا
١٦	لبنان
٢١	المكسيك



أولا - مقدمة

١ - في الفقرة ٣ من القرار ٥٤/٦١ المتعلق بالتطورات في ميدان المعلومات والاتصالات السلوكية واللاسلكية في سياق الأمن الدولي، دعت الجمعية العامة جميع الدول الأعضاء إلى مواصلة موافاة الأمين العام بآرائها وتقييماتها بشأن المسائل التالية: (أ) التقييم العام لمسائل أمن المعلومات؛ و (ب) الجهود المبذولة على الصعيد الوطني لتعزيز أمن المعلومات وتشجيع التعاون الدولي في هذا الميدان؛ و (ج) مضمون المفاهيم الدولية ذات الصلة التي تهدف إلى تعزيز أمن النظم العالمية للمعلومات والاتصالات السلوكية واللاسلكية؛ و (د) التدابير التي يمكن أن يتخذها المجتمع الدولي لتعزيز أمن المعلومات على الصعيد العالمي.

٢ - وفي ٢٣ شباط/فبراير ٢٠٠٧، أرسلت مذكرة شفوية إلى الدول الأعضاء لدعوها إلى إحاطة الأمين العام علما بآرائها وتقييماتها بشأن هذا الموضوع. وترد الردود المتلقاة في الفرع الثاني أدناه، وستصدر في إضافات لهذا التقرير أية ردود إضافية تُقدم في هذا الصدد.

ثانيا - الردود المتلقاة من الحكومات

بروني دار السلام

[الأصل: بالانكليزية]

[٢٥ حزيران/يونيه ٢٠٠٧]

قدمت بروني دار السلام التقرير التالي الذي أعدته قوات الشرطة الملكية بروني.

أولا - مقدمة

(تقييم عام لمسائل أمن المعلومات)

١ - أصبحت تكنولوجيا المعلومات، بما فيها جميع التطورات الناشئة في ميدان المعلومات والاتصالات السلكية واللاسلكية، تلعب دورا حيويا في قطاعات المجتمع كافة. فقد أحدثت تكنولوجيا المعلومات تحولا في السبل التي نعتمدها لإيجاد المعلومات وجمعها وتجهيزها وإدارتها وتقاسمها. وأصبحت المعاملات والسجلات الإلكترونية هي الشكل السائد والأساس المحوري في جميع الميادين من التجارة إلى الرعاية الصحية. ويعد الربط الشبكي الحاسوبي القوة المحركة لهذه التغيرات، ويجسد النمو المطرد لشبكة الإنترنت ولعدد مستخدميها كل عام هذا التحول إلى مجتمع يعتمد على الربط الشبكي الحاسوبي.

٢ - وأصبح أمن المعلومات نتيجة لذلك مكونا أساسيا في تكنولوجيا المعلومات، لا سيما في سياق مجتمع المعلومات. بيد أن هذا الموضوع يتسم بالتعقيد إضافة إلى أن التدابير الملائمة تتوقف في كثير من الأحيان إلى حد كبير على نوع معدات تكنولوجيا المعلومات وبنيتها الأساسية، وأماكن وجودها.

٣ - ويعتبر الربط الشبكي الحاسوبي العامل المحفزة للكثير من هذه التغيرات التي تثير بدورها نقاط قلق جديدة تتعلق بأمن المعلومات المتاحة عن طريق الربط الشبكي الحاسوبي والحفاظ على سريتها. وما لم تعالج تلك النقاط على النحو المناسب، فإنها يمكن أن تحد من الاستفادة من كامل إمكانات الربط الشبكي الحاسوبي، سواء من حيث المشاركة في استخدامه أو من حيث فائدته. ومن ثم، فإن الأمر يستلزم وجود ضمانات مؤسسية وتكنولوجية تكفل الحماية لطائفة عريضة من المعلومات الشخصية أو الحساسة أو المعلومات المحفوظة حقوق تأليفها ونشرها أو حقوق ملكيتها.

٤ - وسيتعين إجراء تقييم متأن للتهديدات والمخاطر الأمنية المحتملة وقوعها في كل حالة من الحالات. ومن الضروري للغاية أن تجري توعية جميع من يعينهم الأمر بالتهديدات

والمخاطر التي تمسهم ويمكنهم السيطرة عليها، فحينئذ فقط سيفهمون تماما إجراءات الأمن التي ينبغي اتخاذها ويطبقونها تطبيقا كاملا.

٥ - وسينصب محور التركيز على حماية المعلومات غير السرية المتاحة على الشبكات الحاسوبية، وعلى أمن الشبكات وقابليتها للبقاء، ومدى موثوقية خدمات الشبكة التي تكفل إمكانية الوصول إلى المعلومات.

٦ - وهناك ثلاثة مجالات رئيسية ينبغي النظر فيها هي: (أ) سياسة التشفير، بما في ذلك المعايير والضوابط الحكومية لتجهيز المعلومات؛ و (ب) الإرشادات المقدمة لحماية المعلومات غير السرية في الوكالات الحكومية؛ و (ج) المسائل القانونية وأمن المعلومات، بما في ذلك التجارة الإلكترونية والحفاظ على السرية وحقوق الملكية الفكرية.

٧ - وتتزايد أهمية ضمانات حماية المعلومات، لا سيما تلك المستندة إلى التشفير. فالضمانات الملائمة (التدابير المضادة) لا بد أن تضع في الاعتبار التغيرات التقنية والمؤسسية والاجتماعية التي تلقي بشكل متزايد بمسؤولية حماية المعلومات على عاتق المستخدم النهائي، وأن تتنبأ بهذه التغيرات. ولن تثمر الجهود الأعم المبذولة لحماية المعلومات المتاحة عن طريق الربط الشبكي الحاسوبي إلا إذا عولجت المسائل المتعلقة بسياسات التشفير. وأهم خطوة يمكن أن تتخذ لتطبيق ضمانات ملائمة من أجل حماية المعلومات المتاحة عن طريق الربط الشبكي في الوكالات الحكومية أو غيرها من المنظمات هي أن تقوم الإدارة العليا بتحديد الأهداف العامة للمنظمة، وتصوغ سياسة لأمن المنظمة تعكس تلك الأهداف، وتعمل على تنفيذها. والإدارة العليا وحدها هي القادرة على تعزيز توافق الآراء وحشد الموارد اللازمة لتوفير الحماية الفعالة للمعلومات المتاحة عن طريق الربط الشبكي الحاسوبي.

٨ - ويعد هذا الرأي محاولة لتقييم التهديدات والمخاطر التي تنشأ عن الأنشطة الإجرامية في دوائر تكنولوجيا المعلومات ولتحديد المشورة التي يمكن للشرطة أن تقدمها بشأن الإجراءات الأمنية وسبل منع الجرائم الحاسوبية. وقد تنشأ المخاطر التي تهدد نظم المعلومات عن أفعال تتم بقصد وبغير قصد، وقد تأتي من مصادر داخلية وخارجية على حد سواء.

ثانيا - أوجه القلق

٩ - يساور القلق قوات الشرطة الملكية ببروني بسبب عدم تغطية الترتيبات الأمنية في سياق وضع مبادرات الحكومة الإلكترونية على الصعيد الوطني.

١٠ - حتى الآن، لم تُدع قوات الشرطة الملكية إلى الاشتراك في الترتيبات الوطنية الرامية إلى دخول عصر المعلومات ولم تنخرط فيها. وقد تم في السنوات الثلاث الماضية اعتماد الكثير من

التشريعات استعدادا لدخول البلد عصر المعلومات، وهناك العديد من الهيئات الحكومية والكيانات المنظمة التي أنشئت كي تقود مبادرات الحكومة الإلكترونية أو التي يجري إنشاؤها لذلك الغرض.

١١ - ولم تلق مسائل الأمن في سياق أعمال التحضير لإنفاذ القانون الاهتمام الكافي ولم تحظ بنفس الدرجة من الأولوية التي حظيت بها غيرها من المسائل المدرجة في جدول الأعمال الوطني. وترى قوات الشرطة الملكية أن الأمن يلعب دورا هاما فيما يتصل بالتطلعات الوطنية للانضمام إلى مجتمع المعلومات.

١٢ - والأمن مسألة حيوية عندما يتعلق الأمر بعصر المعلومات. ولا يمكن المغالاة في أهمية إنشاء بنية أساسية آمنة وموثوقة.

ثالثا - مبادرات قوات الشرطة الملكية ببروني دار السلام

(الجهود التي تُبذل على الصعيد الوطني لتعزيز أمن المعلومات وتشجيع التعاون الدولي في هذا الميدان)

١٣ - بما أن قوات الشرطة الملكية هي الوكالة الرئيسية المناط بها إنفاذ القانون في البلد، فإنها تود تقديم المساعدة عن طريق القيام بدور ريادي فيما يتعلق بالجوانب الأمنية التي تتطلبها دخول عصر المعلومات بشكل كامل.

١٤ - ولهذا الغرض، أُوفد عدد كبير من الضباط إلى الخارج لتلقي التدريب عن الجرائم المتعلقة بشبكة الإنترنت، لا سيما الجرائم المرتكبة في الفضاء الإلكتروني والجرائم العابرة للحدود الوطنية. ولم يتحقق في بادئ الأمر أي تقدم إضافي في مجال شراء معدات تكنولوجيا المعلومات وبرامجها اللازمة للتحقيق في محاولات اقتحام النظم الحاسوبية وذلك نظرا لنقص التمويل، لكن قوات الشرطة الملكية لديها الآن القدرة على إجراء التحقيقات في الجرائم المرتكبة في الفضاء الإلكتروني.

١٥ - وقد اتخذت قوات الشرطة الملكية خطوات لتوطيد التعاون الدولي في هذا الميدان عن طريق المشاركة النشطة في منتديات عدة تتناول تعزيز القدرات على إنفاذ القانون. ولقوات الشرطة الملكية صلات بالشبكات الحاسوبية الإقليمية والدولية لإنفاذ القانون مما يعزز من قدرتها على ملاحقة المجرمين الفارين.

رابعاً - اقتراحات قوات الشرطة الملكية ببروني وتوصياتها

(التدابير التي يمكن أن يتخذها المجتمع الدولي لتعزيز مجتمع المعلومات وأمن المعلومات على الصعيد العالمي)

١٦ - تطرح قوات الشرطة الملكية النقاط التالية باعتبارها نقاطاً للانطلاق نحو تيسير توفير الأمن وتحسينه في سياق أمن المعلومات.

ألف - الإبلاغ عن التهديدات ومواطن الضعف ورصدها:

(١) منذ تشكيل فريق بروني دار السلام للاستجابة لحالات الطوارئ الحاسوبية في عام ٢٠٠٤، أصبح هناك نوع من أنواع الرقابة، وإن لم يكن وافياً نظراً لعدم وجود صلات على الإطلاق بين الفريق وقوات الشرطة الملكية والافتقار إلى آلية تكفل الاستجابة السريعة، كرصد التسلل أو اعتراضه في حينه وغير ذلك من أنواع الاستجابة.

باء - آليات التثقيف والأمن لاستخدام الحاسوب بشكل آمن:

(١) توفير الدعم اللازم لوضع مواد وبرامج تثقيفية عن الفضاء الإلكتروني يستفيد منها المستخدمون كافة. وسيوفر ذلك تدريباً مبكراً على ممارسات وسلوكيات الأمن عند استخدام شبكة الإنترنت؛

(٢) الاستثمار في حملات للتوعية يجري فيها التشديد على ضرورة تلقي القائمين على إدارة النظم ومديري الشبكات وكبار موظفي شؤون المعلومات التدريب على مسائل الأمن؛

(٣) تيسير وضع آليات لأمن المعلومات المتاحة في الفضاء الإلكتروني تسمح لكل طرف من أطراف المعاملة بأن يقرر ما يريد اعتماده من احتياطات وقيود، وتعميم استخدام تلك الآليات.

جيم - البحث والتطوير:

(١) تخصيص الأموال للبحث والتطوير في المجالات المتعلقة بأمن هياكل النظم ذات صلاحيات الاستخدام غير المحددة والرقابة الموزعة على عدة مراكز، وقابلية تلك النظم للبقاء؛

(٢) وضع مجموعات أدوات شاملة تدعم الجهود التي يبذلها القائمون على إدارة الشبكات لتشغيل نظم آمنة؛

(٣) تطوير تقنيات لبرامج الكشف عن المخاطر والتخفيف منها بصورة شاملة ومستمرة.

دال - استخدام المعايير:

(١) وضع معايير لأمن البرمجيات وتشجيع القبول بها كوسيلة قصيرة الأجل تعتبر نقطة انطلاق لعملية تحسين الأمن فيما يتعلق بمنتجات شبكة الإنترنت؛

(٢) صياغة سياسة حكومية تقضي بضرورة أن تفي المعدات والبرمجيات الحاسوبية التي تشتريها الحكومة بمعايير أمن محددة تشمل اشتراط وجود خدمة للتنبيه الأمني بقصد إخطار العميل بمواطن الضعف وسبل إصلاحها.

هاء - القوانين وإنفاذها:

(١) تقديم الدعم لضباط الشرطة المخصصين لجرائم الفضاء الإلكتروني وتخصيص التمويل المناسب لوكالات إنفاذ القانون من أجل دعم التدريب والموارد المادية والموظفين اللازمين للتعامل مع الجرائم التي يُبلغ عن ارتكابها في الفضاء الإلكتروني؛

(٢) كفالة تلبية السياسة الوطنية لاحتياجات القائمين على إنفاذ القانون فيما يتعلق بالتنسيق على الصعيد الدولي لمعالجة جرائم الفضاء الإلكتروني، وتقديم الدعم لوكالات إنفاذ القانون من أجل إبرام اتفاقات دولية للمطاردة الحثيثة؛

(٣) كفالة تيسير السياسة العامة استخدام الترميز على نطاق واسع لحماية المعلومات المتاحة في الفضاء الإلكتروني وحماية مستخدميه.

بور كينا فاسو

[الأصل: بالفرنسية]

[٢٠ حزيران/يونيه ٢٠٠٧]

- ١ - أكدت بور كينا فاسو منذ وقت مبكر للغاية أن لديها الإرادة السياسية اللازمة لتطوير التكنولوجيات الجديدة للمعلومات والاتصالات التي تعتبر أداة استراتيجية لتعزيز الحكم الصالح والتنمية الاقتصادية والاجتماعية.
- ٢ - وقد انخرطت بور كينا فاسو بالفعل ابتداء من عام ١٩٩٦ في عملية شاملة لدراسة تطوير التكنولوجيات الجديدة للمعلومات والاتصالات. وكان الهدف من ذلك هو تسخير تكنولوجيات المعلومات لأغراض تحديث الخدمات العامة وتحسين فعالية العمل الإداري.
- ٣ - وفي عام ١٩٩٩، وضعت بور كينا فاسو خطة للفترة ٢٠٠١-٢٠٠٥ تتناول البنية الأساسية الوطنية في مجال المعلومات والاتصالات وتهدف إلى التقريب بين السياسات الوطنية في ميادين الاتصالات السلكية واللاسلكية وتكنولوجيا المعلومات ووسائل الاتصال.
- ٤ - وفي عام ٢٠٠٤، اعتمدت حكومة بور كينا فاسو الاستراتيجية المتعلقة بتنفيذ خطة تطوير البنية الأساسية الوطنية للمعلومات والاتصالات. وتلتزم الحكومة بموجب هذه الخطة بكفالة نشر تكنولوجيات المعلومات والاتصالات في المجتمع بأسره، وضمان إتاحتها لجميع طبقات المجتمع وتملكها لها، والاستفادة من إمكاناتها لخدمة الاستراتيجيات الإنمائية الوطنية.
- ٥ - بيد أنه، بالنظر إلى المخاطر الناشئة عن استخدام نظم المعلومات، تعكف الحكومة على وضع إطار قانوني يهدف إلى حماية المعلومات، وتوفير الأمن لنظم المعلومات، وحماية الحقوق الأساسية للأفراد، وبث الثقة في نظم المعلومات في أوساط الشركات والإدارات.
- ٦ - وفي هذا السياق، اعتمد القانون رقم 010-2004/AN، المؤرخ ٢٠ نيسان/أبريل ٢٠٠٤، الذي يحمي البيانات ذات الطابع الشخصي. ويكفل هذا القانون حماية الحقوق والحريات الأساسية للأفراد وخصوصياتهم في سياق المعالجة الحاسوبية أو غير الحاسوبية للمعلومات التي تشمل بيانات ذات طابع شخصي. وتطبيقاً لهذا القانون، شُكلت بموجب المرسوم 2007-283/PRES/PM/MPDH المؤرخ ١٨ أيار/مايو ٢٠٠٧ لجنة معنية بتكنولوجيا المعلومات والحريات. وتعد هذه اللجنة هيئة إدارية مستقلة مهمتها كفالة أن تتم المعالجة الآلية للمعلومات الشخصية التي تقوم بها كيانات عامة أو خاصة بما يتفق مع أحكام القانون. ولدى اللجنة، صلاحيات تنظيمية وجزائية تخول لها التدخل في المراحل الأولية والنهائية من

عملية معالجة المعلومات وذلك من خلال ما تصدره من إشعارات وبيانات مسبقة ومن خلال فرض الرقابة والجزاءات.

٧ - وأخيراً، فقد أنشئت أجهزة تنظيمية لتلبية الاحتياجات الأمنية لمجتمع المعلومات، ومنها المجلس الأعلى للمعلومات والإدارة العامة المكلفة بتنسيق برامج تطوير تكنولوجيات المعلومات والاتصالات ومقرها وزارة البريد وتكنولوجيات المعلومات والاتصالات السلوكية واللاسلكية.

٨ - غير أن بوركينا فاسو، في مواجهة مجتمع المعلومات الذي لا يعترف بالحدود، ترى أن التعاون الدولي أمر أساسي بالنسبة لمسألة توفير الأمن لنظم المعلومات. فبلدان الجنوب، بغض النظر عن الفجوة الرقمية، معرضة لمخاطر ذات صلة بالأمن شأنها في ذلك شأن بلدان الشمال. وبناء على ذلك، فإن التعاون بين البلدان أمر لا بد منه إذا أُريد ضمان أمن الدول والمؤسسات والشركات والأفراد علاوة على أمن شبكات المعلومات ونظمها. ولا يمكن لمكافحة الجرائم المرتكبة في الفضاء الإلكتروني أن تكون فعالة إلا بتعزيز التعاون الدولي.

٩ - وترحب بوركينا فاسو بالاهتمام الذي توليه الأمم المتحدة لمسألة أمن المعلومات وترى أن الفرصة مهيأة الآن للعمل على وضع صك دولي يتناول أمن تكنولوجيا المعلومات من ناحية وحماية البيانات ذات الطابع الشخصي من ناحية أخرى. وعلى أية حال، فإن التطورات في ميدان تكنولوجيا المعلومات والاتصالات، ومسائل الأمن الدولي ينبغي النظر فيها في ضوء حقوق الإنسان تفادياً للوقوع تحت نير مجتمع عالمي قائم على المراقبة التي يغلب عليها الطابع الأمني إلى حد يجرّد الإنسان من آدميته.

شيلي

[الأصل: بالإسبانية]

[١٣ حزيران/يونيه ٢٠٠٧]

- ١ - تولي شيلي أهمية كبيرة لأمن المعلومات في إطار الأمن الدولي. ونحن نشاطر المجتمع الدولي انزعاجه إزاء احتمال استخدام تكنولوجيات المعلومات لأغراض تنافي الهدف المتمثل في الحفاظ على الاستقرار والأمن على الصعيد الدولي وتضرر بالبنية الأساسية في مختلف الدول. ونرى أنه من اللازم منع استغلال تكنولوجيات المعلومات لأغراض إجرامية.
- ٢ - وعلى صعيد التشريعات، أُحرز تقدم فيما يتعلق باعتماد قوانين وقواعد مختلفة بشأن أمن الوثائق الإلكترونية والحفاظ على سريتها وفعالية الاتصالات فيما بين الأجهزة الإدارية للدولة والاتصالات بينها وبين المواطنين.
- ٣ - ونظرا لأهمية هذا الموضوع، فقد شارك بلدنا مشاركة نشطة في مرحلتي مؤتمر القمة العالمي المعني بمجتمع المعلومات اللتين عُقدتا في جنيف في كانون الأول/ديسمبر ٢٠٠٣، وتونس في تشرين الثاني/نوفمبر ٢٠٠٥.

الصين

[الأصل: بالصينية]

[١٥ أيار/مايو ٢٠٠٧]

١ - يؤدي في الوقت الحاضر التطور السريع لتكنولوجيا المعلومات وتطبيقها الواسع النطاق دورا إيجابيا في تعزيز التنمية الاقتصادية والاجتماعية وفي النهوض بحياة السكان في جميع بلدان العالم. وقد أصبح أمن المعلومات في الوقت ذاته عاملا هاما في أمنفرادى البلدان عامة، بل وأمن واستقرار العالم برمته. وتعد المعالجة السليمة لهذه المسألة بما يحقق المصالح المشتركة لجميع البلدان مسؤولية مشتركة تقع على عاتق المجتمع الدولي.

٢ - وترى الصين أن مسألة أمن المعلومات لا تتعلق فقط بالمخاطر التي يشكلها ضعف الهياكل الأساسية للمعلومات والترابط فيما بينها، بل تتعلق أيضا بالمشاكل السياسية والاقتصادية والعسكرية والاجتماعية والثقافية والعديد من المشاكل الأخرى الناجمة عن إساءة استعمال تكنولوجيا المعلومات. وينبغي التصدي لكلا العاملين المذكورين آنفا لدى النظر في مسألة أمن المعلومات.

٣ - وترى الصين أن تكنولوجيا المعلومات ينبغي تطبيقها وفقا لميثاق الأمم المتحدة والقواعد الأساسية التي تنظم العلاقات الدولية، وينبغي أن تُكفل حرية تدفق المعلومات شريطة صون سيادة كل بلد وأمنه، واحترام الاختلافات التاريخية والثقافية والسياسية القائمة فيما بين البلدان، وينبغي أن يتمتع كل بلد بالحق في تنظيم فضائه الإلكتروني وفقا لتشريعاته الداخلية؛ ونظرا لتفاوت التنمية في ميدان الاتصالات السلكية واللاسلكية بين البلدان، ينبغي أيضا للمجتمع الدولي أن يعزز التعاون في مجال البحوث والاستفادة بتكنولوجيا المعلومات وأن يكفل بتراهة سبل الحصول على تلك التكنولوجيا أمام جميع البلدان.

٤ - وما فتئت الحكومة الصينية تعلق دائما أهمية كبيرة على تكنولوجيا المعلومات. وقد وضعت استراتيجية وطنية لأمن المعلومات وتقوم تدريجيا بتنفيذها، كما أعدت مجموعة من القوانين واللوائح والمعايير لتنظيم أمن المعلومات. وهي تبذل جهودا كبيرة للنهوض بمراقبة أمن الشبكات، وتحسين آليات التنسيق والإدارة، والاضطلاع بالبحوث المتعلقة بتكنولوجيا أمن الشبكات، وبناء نظام لمواجهة حالات الطوارئ في ذلك المجال. وما زال النمو مستمرا في مجال القدرة على حماية أمن شبكات المعلومات الأساسية ونظم المعلومات الهامة.

٥ - وتشارك الصين بهمة في جهود التعاون الدولي في مجال أمن المعلومات. وفي ١١ حزيران/يونيه ٢٠٠٦، وقع رؤساء الدول الأعضاء في منظمة شنغهاي "البيان الصادر

عن رؤساء الدول الأعضاء في منظمة شنغهاي بشأن أمن المعلومات على الصعيد الدولي“، الذي تقرر فيه إنشاء فريق من الخبراء الحكوميين معني بأمن المعلومات. وتشارك الصين على نحو بناء في أعمال ذلك الفريق.

٦ - وترى الصين أن الأمم المتحدة هي المنتدى الملائم لاستكشاف مسألة أمن المعلومات. وخلال الفترة ما بين عامي ٢٠٠٤ و ٢٠٠٥، قام فريق للخبراء الحكوميين بمناقشة هذه المسألة بجميع جوانبها وطرح عدة مقترحات مفيدة بشأن طائفة من المواضيع في ميدان أمن المعلومات، وضعت أساسا سليما يواصل المجتمع الدولي بناء عليه بحث المسائل المتعلقة بأمن المعلومات. وتؤيد الصين إعادة إنشاء فريق للخبراء الحكوميين من جانب الأمم المتحدة في عام ٢٠٠٩، يجري دراسة متعمقة وشاملة للتهديدات والتحديات القائمة في ميدان أمن المعلومات، إلى جانب وضع برامج وسياسات فعالة لمواجهتها. وستستمر الصين، كما دأبت في الماضي، في دعم الجهود الدولية المبذولة لمعالجة مشكلة أمن المعلومات، وفي المشاركة في تلك الجهود.

كوبا

[الأصل: بالإسبانية]

[١٦ أيار/مايو ٢٠٠٧]

- ١ - يتسم الأساس الذي تقوم عليه منجزات كوبا الحالية في مجال تكنولوجيا المعلومات بطابع اجتماعي عميق يخلو من مظاهر السلوك الاستهلاكي، وقد أفرز ذلك متخصصين من طراز جديد يتسمون بالتفاني التام ويتحلون بقيم أخلاقية تختلف عن الأنماط التي يشجعها العالم المتجه إلى العولمة والليبرالية الجديدة.
- ٢ - وتعد التحسينات الكبيرة التي أجريت على الهياكل الأساسية التكنولوجية والعمليات الواسعة والدقيقة التي تجري لإعداد الموارد البشرية في مراحل العمر المبكرة من الأمثلة التي تشهد بالجهود الهائلة التي تبذلها الدولة الكوبية للانتقال بالمجتمع على وجه السرعة إلى عالم المعلوماتية، باعتبار ذلك وسيلة للنهوض بنوعية الحياة في البلد وبكفاءة البلد وقدرته على المنافسة.
- ٣ - وعلى أساس تلك السياسة، قامت كوبا في إجراء اجتماعي واسع النطاق بتنظيم الاستخدام الرشيد والكفؤ للموارد الحاسوبية، سواء من حيث المعدات أو من حيث إمكانية الاتصال بشبكة الإنترنت. ومن ثم، فقد أدرجت على سلم الأولويات قطاعات رئيسية، من قبيل الصحة والتعليم والمراكز العلمية والمؤسسات الثقافية والأعمال التجارية، تكفل التنمية الاقتصادية والاجتماعية للبلد.
- ٤ - بيد أن تلك التنمية قد اصطدمت بالحظر الاقتصادي والتجاري والمالي القاسي الذي تفرضه الولايات المتحدة الأمريكية، والذي ازداد حدة مع تولي الإدارة الحالية لمقاليد السلطة.
- ٥ - ويعود تاريخ اتصال كوبا بشبكة الإنترنت إلى عام ١٩٩٦، عندما منحت حكومة الولايات المتحدة كوبا ترخيصا بالوصول إلى الشبكة. ولكن على الرغم من أن كابات الألياف الضوئية الدولية تمر حاليا على مقربة شديدة من السواحل الكوبية، فإن قوانين الحظر قد أعاققت إمكانية ربط كوبا بتلك الكابات، مما اضطر البلد إلى الاستعانة بقناة ساتلية لا يزيد نطاق ترددها عن مجرد ٦٥ ميغابايت في الثانية للتحميل و ١٢٤ ميغابايت في الثانية للإنزال. والواقع أن الاتصال عن طريق الألياف الضوئية لا يتيح فقط مزيدا من السرعة في الاتصال بشبكة الإنترنت، وإنما أيضا يتيح ذلك بتكاليف أقل بكثير. وتقتضي القوانين

المذكورة الحصول على ترخيص من وزارة المالية بالولايات المتحدة كلما أجريت أي إضافات أو تعديلات جديدة على تلك القناة.

٦ - وفيما يتصل بالهياكل الأساسية التكنولوجية، لا يقتصر تأثير الحصار الذي تفرضه الولايات المتحدة على كوبا على إعاقة عمليات شراء المعدات والبرامجيات من شركات تلك الدولة؛ وإنما يؤثر أيضا، بسبب طابعه الذي يتجاوز حدود الدولة، في العمليات التجارية التي تقوم بها مع شركات من جنسيات أخرى، كما يحظر إنزال البرامجيات وتكنولوجيا المعلومات، بما في ذلك المتاحة مجانا، إذا كانت تحمل رقم بروتوكول الإنترنت الخاص بكوبا.

٧ - والإنترنت، بصفقتها مجالا عالميا مشتركا، تنطوي على تحديات معينة لا بد من مواجهتها، ولا يقتصر ذلك على التحديات المتصلة باشتراك البشرية جمعاء في تنظيمها، وبالتالي إشراك جميع البلدان في إدارتها، ولكن يمتد الأمر أيضا إلى القضاء على الآفات التي يدينها الجميع، من قبيل انتشار المواد الإباحية، والتحرير على الإرهاب، والعنصرية، والغش، ونشر العقائد الفاشية، والجرائم الإلكترونية بأنواعها.

٨ - ولكن ثمة تحد آخر تقف البلدان الغنية أمامه مكتوفة الأيدي، وهو إزالة الطابع الانتقائي النخبوي لشبكة الإنترنت، الذي ينقل اليوم التفاوتات والعوائق القائمة في العالم الحقيقي إلى الفضاء الإلكتروني، مما يوجد ما يسمى بـ "الفجوة الرقمية".

٩ - وهناك الملايين من الأشخاص في العالم أبعد ما يكون عن الانضمام لصفوف مستعملي الإنترنت، فهم لا يعرفون القراءة أو الكتابة وشاغلهم اليومي الأساسي هو التغلب على الجوع والعطش والمرض. ومع توافر الإرادة السياسية لدى الحكومات ومع التعاون على الصعيد الدولي وتخصيص الحد الأدنى من الموارد التي يهدرها الآن ما يسمى بالعالم المتقدم في الدعاية أو الاستهلاك المفرط أو سباق التسلح، يمكن أن تصبح الإنترنت أداة لإحداث ثورة ثقافية وتعليمية تشجع على المعرفة وتعزز التعليم والثقافة والتعاون والتضامن، إلى جانب القيم المعنوية والأخلاقية اللازمة لهذا القرن الجديد، بما ينشر المشاعر الإنسانية النبيلة ويؤدي إلى التخلص من السلوكيات غير الإنسانية الأنانية التي لا تركز إلا على الفرد.

١٠ - ومن ناحية أخرى، يحظى هذا الموضوع باهتمام خاص من جانب أجهزة الأمن التي تستخدم أغلبيتها تلك التكنولوجيات لمساعدة الحكومات. وتضع تلك الأجهزة التي تخصص لها مبالغ طائلة تدابير وبرامج مختلفة لتعزيز التكنولوجيات القائمة أو إيجاد إمكانيات جديدة للتجسس على الاتصالات، والوصول إلى نظم وقواعد البيانات، ونظم تحديد هوية المركبات والأشخاص ورصدهم. وتشمل هذه الشبكات المعقدة نظم الهوائيات ومحطات التنصت

وأجهزة الرادار والسواتل، التي تعاونها الغواصات وطائرات التجسس، وتربط بينها جميعا حواسيب عملاقة وبرامجيات متخصصة.

١١ - ومن السداجة بمكان أن نعتقد أن الشركات التي تقدم الخدمات والتكنولوجيات لن تقوم في سياق تعاونها مع الوكالات المذكورة بتسهيل توفير المعلومات التي تمكن تلك الوكالات من الاضطلاع بأعمال الاستخبارات والتجسس. ومن الجدير بالإشارة أن أحكام ما يسمى بـ "قانون الولاء للوطن" في الولايات المتحدة الأمريكية تخول الحكومة سلطة طلب المعلومات من أي هيئة، سواء كانت المعلومات سرية أو غير ذلك، إذا رئي أن لها أهمية للأمن القومي.

١٢ - وانطلاقا من اعتبار المعرفة تراثا للإنسانية جمعاء، ينبغي أن يجري الأخذ بالديمقراطية فيما يتعلق بتوفير وتوزيع رأس المال الخاص بالمعلومات الذي ينبغي أن يوضع في خدمة السلام والتنمية، اللذين لا غنى عنهما من أجل إحراز التقدم في هذه الألفية الجديدة.

لبنان

وردت الرسالتان التاليتان من بعثة لبنان الدائمة لدى الأمم المتحدة. وتمثل هاتان الرسالتان خلاصة المخاطبات التي جرت بين البعثة ووزارات الاتصالات والداخلية والدفاع اللبنانية.

وزارة الاتصالات

[الأصل: بالانكليزية]

[٤ حزيران/يونيه ٢٠٠٧]

١ - نحن بصدد إصدار قانون جديد يغطي قطاع تكنولوجيا المعلومات والاتصالات في لبنان، وهو في المرحلة النهائية لاعتماده من قبل مجلس النواب. وسيغطي هذا القانون الأمن وجميع المسائل المتعلقة بمجرائم المعلومات.

٢ - وبمجرد أن يبدأ سريان القانون المذكور أعلاه، سترتب وزارة الاتصالات الأمور المتعلقة بالنقاط ب و ج و د مع الوزارات الأخرى وجميع الهيئات المعنية.

وزارة الداخلية

[الأصل: بالعربية]

[٢٣ أيار/مايو ٢٠٠٧]

أولا - على الصعيد الوطني:

١ - فيما خص تبادل المعلومات بين مختلف قطاعات قوى الأمن الداخلي يتم ذلك عبر وسائل الاتصالات السلكية (هاتف/فاكس) واللاسلكية (كغرف العمليات في مختلف المناطق) إلا أن هذه الطريقة في تبادل المعلومات تبقى معرضة للانتهاك والخرق وذلك عبر التنصت على عمليات التبادل المذكورة مع الإشارة إلى أن جانب المديرية العامة باشرت منذ مدة بتطوير شبكة الاتصالات *TETRA* المعتمدة في قوى الأمن الداخلي عبر المباشرة باستعمالها في بعض المناطق اللبنانية تمهيدا لتعميمها على كافة المناطق. هذا بالإضافة إلى تزويد قوى الأمن مؤخرا بشبكة خطوط خليوية مقفلة تنفيذا لقرار مجلس الوزراء رقم ٤٧ تاريخ ١٥ أيلول/سبتمبر ٢٠٠٦.

ثانيا - على الصعيد الدولي:

٢ - يتم تبادل المعلومات لا سيما الأمنية منها بين مؤسسة قوى الأمن الداخلي وسائر المنظمات الدولية من قبل شعبة الاتصال الدولي في المديرية العامة لقوى الأمن الداخلي والتي يتبع لها خطة لبث وتلقي المعلومات الأمنية بواسطة مكتب إنتربول بيروت التابع للشعبة المذكورة حيث يستخدم حاليا منظومة اتصالات دورية تستند في عملها إلى تكنولوجيا الإنترنت وتمتاز بسرعة تبادل المعلومات والحفاظ على سرّيتها عبر شبكات متخصصة يعد إليها أمر صيانتها بالاتفاق مع المنظمة الدولية للشرطة الجنائية (إنتربول) التي تشرف على إدارة وتحديث تلك الشبكة.

ثالثا:

٣ - بالنسبة للفقرة A/ المتعلقة بالتقييم العام لمواضيع أمن المعلومات، أن قوى الأمن الداخلي تجهد في استخدام الوسائل التقنية الفعالة في مجال أمن المعلومات والاتصالات السلوكية واللاسلكية، وهي في هذا المجال تواجه تحديات جمة أبرزها توحيد مقاييس البنية الأمنية المعلوماتية وبيئة حمايتها ضمن معايير مناسبة ومقبولة توخيا لإنشاء وتطبيق وتوثيق إدارة أنظمة المعلومات الأمنية وإجراءات التحكم بهذه الأنظمة.

٤ - وبالنسبة للفقرتين B/ و C/ المتعلقة بالجهود المبذولة لتحسين وتمتين الأمن المعلوماتي على الصعيد الوطني والمساهمة الدولية في هذا المجال، إننا قد مررنا بتجارب عملية وواقعية حول إجراء تقييم لمخاطر الاختراق حسب حالة الشبكة المعلوماتية المتوفرة لدينا، ونحن في هذا المجال قد قطعنا شوطا لتحسين شروط الأمان لشبكة المعلومات لدينا مستندينا إلى التقنيات الحديثة والحلول وإجراءات التطبيق المعتمدة حول حماية وإنقاذ الأنظمة واختبارات مناعتها أمام الاختراقات والتطفل والفيروسات وخطط عدم تقطع العمل عند حصول أي من الهجمات على الأنظمة، إضافة إلى تدريب وتأهيل الموارد البشرية توخيا للحصول على الكفاءة الأمثل للتعامل مع كل طارئ.

٥ - وبالنسبة للفقرة D/ المتعلقة بالمقاييس الممكن اعتمادها من المجتمع الدولي بتقوية الأمن المعلوماتي على المستوى العالمي، إننا نقترح بداية اعتماد سياسة وقائية لوقف أعمال التطفل والاختراقات على صعيد الأفراد والتعاون فيما بين أفراد المجتمع الدولي في هذا المجال والعمل على نص قانون يختص بمكافحة أعمال التخريب والتطفل ضد شبكات المعلومات واعتبار هذه الأفعال جرم يعاقب عليه القانون، إضافة إلى تبادل الخبرات فيما بين الدول الأعضاء للاستفادة من التجارب المختلفة مما قد يؤمن قفزة نوعية في هذا المجال.

٦ - وجدير بالذكر أن الخطوات التي قامت بها هذه المديرية العامة على هذا الصعيد هي:

(أ) استحداث مكتب خاص لمكافحة جرائم المعلوماتية في قوى الأمن الداخلي ومن أبرز مهامه الإنذار عن جرائم المعلوماتية والأخطار التي تهدد أمن المعلومات الرقمية بالإضافة إلى التحقيق وملاحقة مرتكبي جرائم المعلوماتية؛

(ب) شاركت قوى الأمن وبواسطة عدد من ضباطها الاختصاصيين في أعمال إعداد مشروع قانون لمكافحة جرائم المعلوماتية والذي تعده لجنة التكنولوجيا النيابية وقد أصبح هذا المشروع جاهزا للتصديق من قبل مجلس النواب؛

(ج) تشارك قوى الأمن بفعالية بنشاطات الإنتربول الدولي وتساهم بأعمال اللجنة الإقليمية للشرق الأوسط وشمال أفريقيا لمكافحة جرائم المعلوماتية في الإنتربول إذ أن نائب رئيس هذه اللجنة وأحد الأعضاء هم من ضباط قوى الأمن الداخلي المتخصصين في حقل المعلوماتية. كما أن رئيس مكتبة مكافحة جرائم المعلوماتية يعتبر ضابط الارتباط مع الإنتربول في قضايا أمن المعلومات ومكافحة جرائم المعلوماتية خاصة تلك التي تطل أمن المعلومات.

٧ - وبما أن التهديدات التي يواجهها الأمن بمفهومه العام، على الصعيدين الوطني والدولي، وبشكل خاص من نظم المعلومات والاتصالات، يستوجب وضع استراتيجية تراعي التطور التقني وتستشرف المستقبل لضمان حماية وإيجاد الوسائل الكفيلة بالتصدي لأية خروقات، وفي هذا المجال نشير إلى التالي:

١ - ديناميكية المعلومات والمعايير الأمنية:

٨ - ديناميكية هائلة في وسائل نقل وحفظ المعلومات نتيجة التطور التقني، إلا أن صعوبة السيطرة "النظم/الوسائل/المضمون"، فرض تدابير حماية على صعيد مختلف الوسائل، وتم وضع معايير دولية لإدارة أمن المعلومات (ISO17799).

٢ - لبنان وأمن المعلومات:

٩ - يفتقد لبنان للعديد من الإجراءات على المستويين التشريعي والتنفيذي لتأمين محيط أمن للمعلومات. إذ لا يوجد أي تشريع أو تدبير إداري يُلزم الإدارات الرسمية والمؤسسات بتطبيق معايير إدارة أمن المعلومات (ISO17799)، علماً أن ما هو مطبق حالياً كناية عن توجيهات مشابهة للمعايير الدولية تبناها مصرف لبنان وبعض المصارف الخاصة، كما أنه لا يوجد تشريعات لأصول التشفير لشبكات الاتصالات الخاصة.

١٠ - على صعيد التطبيق: عدم التقيد بتعميم وزارة الاتصالات رقم ٢/٤ تاريخ ١٩ كانون الأول/ديسمبر ٢٠٠٥، حول الاحتفاظ بملفات حركة سير المعلومات، وعدم وجود تشريع ينظم عمل مقاهي الإنترنت وانعدام فاعلية مراقبة الاتصالات الهوائية في الفضاء اللبناني.

مع الإشارة إلى أن الولايات المتحدة الأمريكية وإثر هجمات ٩ أيلول/سبتمبر الإرهابية، أنشأت وزارة الأمن الداخلي واعتمدت نظام مراقبة لكافة نظم الاتصالات الوطنية وعبر الولايات المتحدة الأمريكية، يؤمن التحليل والمراقبة، كما تم وضع تشريعات صارمة في مجال تشفير المعلومات والولوج من وإلى الشبكة.

٣ - سبل المكافحة والحماية:

١١ - الفضاء الإلكتروني *CYBER SPACE* بدأ كشبكة إنترنت وفقاً لنظام *TCP/IP-PROTOCOL* بيئة هشة وغير آمنة، سمحت لمجموعات الإجرام باقتحامه وتدميره أحياناً، نتيجة إعطاء الأولوية للأهداف التجارية والتسويقية كما تميز الجرم المعلوماتي بالسرعة وانعدام الضوابط أو الحدود، يقابله بطء في المكافحة، وانعدام التنسيق، وضعف التشريعات المعتمدة.

١٢ - أجريت العديد من التحسينات على عمل بروتوكولات الإنترنت، سواء للجهة المستخدمين أو التشفير، منها بروتوكول *IPV6*، كما أن الأبحاث لا تزال جارية حول إنتاج تقنيات أمنية مرتبطة بشبكات المعلوماتية تؤمن الردع الإلكتروني لجرائم الخرق والتدمير.

الاتفاقات الدولية لمكافحة جرائم المعلوماتية لا سيما منها اتفاقية بودابست فرضت التعاون السريع بين الدول، حيث تم:

- إنشاء شبكة اتصالات ٢٤/٧ متوازية مع شبكة الإنترنت ومتخصصة بجرائم المعلوماتية.

- إنشاء لجنة عامة (*STEERING COMMITTEE*) ولجان فرعية مناطقية *PARTY REGIONAL WORKING* لتفعيل التعاون التقني وتحديث وتطوير الخبرات بين مكاتب مكافحة جرائم المعلوماتية.

إلا أن هذه الاتفاقية بدت عاجزة عن تأمين سرعة المكافحة الآنية لأية فيروسات يمكن إطلاقها عبر الشبكة.

٤ - في المقترحات:

- تفعيل وتطوير التشريعات في مجال أمن المعلومات وبالتالي تطبيق معايير الحماية الأمنية المعلوماتية.
- تفعيل الجهد الأمني وتطويره على صعيد كافة الأجهزة الأمنية في سبيل حماية وسائل ونظم المعلومات.
- تفعيل وتطوير الأجهزة المتخصصة في وزارة الاتصالات، وتأمين تفاعلها مع الأجهزة الأمنية والمؤسسات العامة والخاصة في سبيل إيجاد بيئة آمنة لنظم المعلومات.
- مواكبة المستجدات الدولية لا سيما منها، في تطبيق بروتوكولات الإنترنت مثل *IPv6* واعتماد الوسائل التقنية اللازمة لمعرفة هوية الشخص الذي يدخل شبكة الإنترنت واعتماد رموز هوية إلكترونية (*DIGITALID (DIGITAL CERTIFICATE)*).
- تفعيل التنسيق بين أجهزة حماية القانون في مجال أمن المعلومات، ووضع معايير دولية واحدة على الصعيد التقني بما يؤمن سهولة المتابعة والمراقبة والتنسيق، وتوحيد نظم التشريع بالحد الأدنى، حفاظاً على الأمن القومي وبتواءم مع متطلبات الأمن الدولي.
- وتفيد المديرية العامة للأمن العام أن اتصالاتها الأمنية هي داخل الأراضي اللبنانية ولا توجد اتصالات خارجية، وأنه بالنسبة للاتصالات الداخلية يتم العمل على تطوير نظم حمايتها عبر الاستعانة بخبرات ودعم بعض الأجهزة الأمنية الصديقة، وإنما ما زالت التجهيزات الضرورية غير مؤمنة لعدم توفر الإمكانيات المادية والتقنية لها.

وزارة الدفاع الوطني

- تشير وزارة الدفاع الوطني إلى أن لبنان يؤكد على ما يلي:
- حرصه على عدم استخدام تكنولوجيا المعلومات ووسائل الاتصال السلكية واللاسلكية في أغراض لا تتفق مع مفاهيم الاستقرار والأمن الدوليين.
- اتخاذ الإجراءات الضرورية على الصعيد الوطني (تطويره وتحديثه للأنظمة والقوانين ذات الصلة) لتعزيز أمن المعلومات، وتشجيعه تبادل المعلومات المتوفرة لدى الأطراف المعنية بذلك.
- تجاوبه وتعاونه مع قرارات الأمم المتحدة الآيلة إلى حماية أمن المعلومات وسريتها وعدم إساءة استخدامها بشتى الطرق، وضرورة منع استخدام مصادر أو تكنولوجيا المعلومات في تحقيق أغراض إجرامية أو إرهابية.

المكسيك

[الأصل: بالإسبانية]

[٢٢ أيار/مايو ٢٠٠٧]

١ - منحت المكسيك تأييدها للقرار الصادر بشأن "التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي"، الذي قدمه الاتحاد الروسي في الجمعية العامة للأمم المتحدة، وهي تولي أهمية كبيرة للعمل على زيادة تبادل وجهات النظر بشأن هذا الموضوع والمفاهيم المتصلة به. وترى المكسيك أنه من الممكن تنظيم عروض يقدمها الخبراء أو عقد مناقشات بشأن هذا الموضوع في إطار أعمال اللجنة الأولى أو غيرها من منتديات نزع السلاح.

٢ - وتعتمد أغلبية آليات التحقق الدولية المنبثقة من الصكوك القانونية الدولية أو الاتفاقات السياسية المتعلقة بمراقبة الصادرات في إعمالها فعليا على وسائل إيصال المعلومات والاتصالات السلكية واللاسلكية، ومن الأهمية بمكان أن تجري دراسة التطورات الناشئة في هذه الميادين. ومن ناحية أخرى، فإن تطوير نظم القذائف الباليستية وتحديث الترسانات النووية يستلزم بالضرورة تطورا في ميدان المعلومات والاتصالات. وفضلا عن ذلك، فلا شك في أن التطورات التي تنشأ فيما يتصل بتكنولوجيات الفضاء الخارجي والسواتل ترتبط بقضايا الأمن الدولي.

٣ - وما فتئت المكسيك توجه الانتباه في إطار مؤتمر نزع السلاح إلى الأهمية العاجلة لاعتماد برنامج عمل تدرج ضمن بنوده الأساسية مسألة "منع سباق التسلح في الفضاء الخارجي"، وهو ما يعتبر أمرا مرتبطا بمواطن الضعف في تكنولوجيات المعلومات والاتصالات الفضائية.

٤ - وترى المكسيك أن من المهم أن يواصل فريق الخبراء الحكوميين المعني بهذه المسألة الذي أنشئ عملا بالقرار ٣٢/٥٨ عمله وأن يعاد تشكيله في عام ٢٠٠٩. ولذا فهي ترى من الضروري أن يجري العمل في غضون ذلك على مناقشة الأمر بصورة مستفيضة.