الأمم المتحدة

A/64/129

الجمعية العامة

Distr.: General
8 July 2009
Arabic
Original: English/Russian/Spanish

الدورة الرابعة والستون

البند ٩٠ من القائمة الأولية*

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

المحتويات

* A/64/50.

310709 310709 09-39631 (A)

أولا – مقدمة

١ – دعت الجمعية العامة في الفقرة ٣ من قرارها ٣٧/٦٣ جميع الدول الأعضاء إلى مواصلة موافاة الأمين العام بآرائها وتقييماتها بشأن المسائل التالية:

(أ) التقدير العام لمسائل أمن المعلومات؛

(ب) الجهود المبذولة على الصعيد الوطني لتعزيز أمن المعلومات وتشجيع التعاون الدولي في هذا الميدان؛

(ج) محتوى المفاهيم المذكورة في الفقرة ٢ من القرار؛

(د) التدابير المحتملة التي يمكن أن يتخذها المجتمع الدولي لتعزيز أمن المعلومات على الصعيد العالمي.

٢ – وعملا بذلك الطلب، أُرسلت مذكرة شفوية في ٢٧ شباط/فبراير ٢٠٠٩ إلى الدول الأعضاء تدعوهما إلى تقديم معلومات عن هذا الموضوع. ويحتوي الفرع الثاني أدناه على الردود التي وردت. وستصدر أي ردود إضافية يجري تلقيها كإضافات لهذا التقرير.

ثانيا – الردود الواردة من الحكومات

البرازيل

[الأصل: بالإنكليزية]
[١١ حزيران/يونيه ٢٠٠٩]

١ – تُعد المعلومات والاتصالات السلكية واللاسلكية جزءا أساسيا من المجتمعات العصرية التي تعتمد عليها إلى حد كبير. والاعتماد القوي على التوافر المستمر لهذه الخدمات متأصل في أنشطة عالم اليوم، مما يجعلها موارد قيمة للغاية، وحاسمة الأهمية لثروة الأمم وازدهارها.

٢ – كما أن أوجه التقدم التكنولوجي التي جعلت هذا السيناريو حقيقة واقعة أثارت أيضا عددا من القضايا في سياق الأمن الدولي. ونظرا لأن المجتمعات تعتمد بصورة متزايدة على توافر المعلومات وعلى الهياكل الأساسية للاتصالات السلكية واللاسلكية، فقد ظهرت جوانب ضعف جديدة يمكن أن تُستغل لاستخدامها في النزاعات العسكرية وفي الأنشطة الإجرامية والإرهابية.

٣ - وقد تنطوي أوجه الاستغلال هذه على إمكانية عرقلة أنشطة الشركات الخاصة والبنوك وأسواق الأسهم والمنظمات الحكومية. وفي حين لا يوجد شك في أن الترابط المتزايد بين شبكات الاتصالات الأساسية مفيد، فإن ذلك الترابط يؤدي إلى ظهور مجموعة جديدة من الشواغل التي ينبغي للدول أن تعالجها على الصعيدين الوطني والدولي.

٤ - وفي نفس الوقت الذي يمكن فيه للتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية أن تؤدي إلى نواحي ضعف، فإنها تمثل أيضا أحد الأصول التي يمكن أن تستخدم كوسائل لحرب حاسوبية. وتوجد بالفعل قوات مسلحة وطنية بها وحدات عسكرية متخصصة مدربة ومجهزة لإعاقة عمل الهياكل الأساسية الحاسمة الأهمية أو حتى تدميرها عن طريق غزو شبكات المعلومات وتخريبها. وتتراوح تأثيرات هذه الهجمات، حسب الهدف والوسيلة المستخدمة، بين ''تدمير الأنظمة الإلكترونية'' لسلاح العدو أو نظم أجهزة الاستشعار به، والتعطيل المدمر لشبكات الطاقة في جميع أنحاء البلد.

٥ - ومما يعزز هذا النوع من الحرب كونها تحتاج إلى استثمارات قليلة نسبيا لتطوير كثير من تلك القدرات. ونظرا لهذه العوامل، فقد تصبح الحرب الحاسوبية نقطة انطلاق النزاعات العسكرية بين الدول في المستقبل القريب. وقد يستخدم الإرهابيون الأفراد أو المنظمات الإرهابية نفس تلك التكتيكات أيضا.

٦ - ونظرا لوعي البرازيل بأهمية هذا الموضوع لصون السلم والأمن الدوليين، فإنها تقترح أن يجري تناول تلك المسألة بطريقتين مختلفتين. أولا، ينبغي للمجتمع الدولي أن يسعى إلى استحداث أدوات ملائمة للتعامل مع الأنشطة الإجرامية والإرهابية التي تنطوي على استخدام تكنولوجيا المعلومات. وفي سياق نهج منفصل ولكن مكمل لذلك، يجب أن ينظر المجتمع الدولي في أثر نشوء الحرب الحاسوبية، والحاجة المحتملة إلى نظم نزع السلاح ومنع الانتشار والقانون الدولي المتعلقة بالحرب، ليأخذ في اعتباره تأثيراتها المتعددة.

٧ - ويجب مناقشة الأنشطة الإجرامية والإرهابية على نحو صحيح في منتديات ملائمة، كما يجب أن تقوم الأمم المتحدة بدور مهم في مساعدة الدول الأعضاء، حسب الاقتضاء، على بلوغ أهداف منها الأهداف التالية:

- إقامة شبكات للطوارئ وشبكات بديلة لحماية الهياكل الأساسية الحاسمة الأهمية؛
- فحص بنية الشبكات، وتحليل جوانب الترابط بينها، وتحديد السبل الفعالة لحمايتها؛
- التعاون الوثيق بين القطاعين الحكومي والخاص، والذي يرمي إلى الوصول إلى المستوى المرغوب من الأمن للمعلومات التي تتدفق فيما بين المنظمات؛

- إقامة نظم للحماية من أجل تجنب تأثيرات الهجمات الحاسوبية أو تقليل تلك التأثيرات إلى أدنى حد؛
- تطبيق أدوات وتدابير لتمكين السلطات من تعقب مصدر الهجمات الحاسوبية؛
- إجراء نقاش حول استصواب وملاءمة الصكوك الدولية الملزمة بشأن الجرائم الحاسوبية؛
- تأهيل المؤسسات الوطنية لإجراء عمليات اختبار وتقييم المستوى الأمني لنظم المعلومات؛
- استحداث إجراءات للإبلاغ المتبادل عن التهديدات الحاسوبية فيما بين السلطات الوطنية المختصة؛
- تجنب الآليات التمييزية التي قد تحول دون إمكانية وصول البلدان إلى التكنولوجيا العالية في ميدان الاتصالات السلكية واللاسلكية ونظم المعلومات؛
- القيام بأنشطة التثقيف والتوعية فيما يخص أهمية الأمن الحاسوبي.

٨ - وينبغي للأمم المتحدة أن تضطلع بدور قيادي في المناقشات الجارية حول استخدام المعلومات والاتصالات السلكية واللاسلكية كوسائل لحرب حاسوبية في حالات النزاع بين الدول، مع إيلاء اهتمام خاص بالجوانب التالية:

- تحديد حرب المعلومات وخصائصها وتصنيفها؛
- تحديد وتصنيف أسلحة المعلومات، والوسائل التي يمكن استخدامها كأسلحة معلومات؛
- وضع مدونة سلوك لاستخدام أسلحة المعلومات؛
- كفالة أن تتمتع جميع البلدان بحقوق متساوية فيما يخص حماية كيانها الوطني من الهجمات الحاسوبية؛
- إنشاء مسرد للأمم المتحدة يحتوي على تعاريف للمصطلحات الرئيسية المتعلقة بالمعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي.

كازاخستان

[الأصل: بالروسية]
[٢ تموز/يوليه ٢٠٠٩]

١ - تنشأ عن التطور الحثيث في تكنولوجيا المعلومات والاتصالات العالمية تغيرات واسعة النطاق في جميع مجالات الحياة على صعيد العالم بأسره. ويشير ميثاق أوكيناوا بشأن مجتمع المعلومات العالمي إلى أن ''تكنولوجيا المعلومات والاتصالات هي أحد أهم العوامل المؤثرة في بناء مجتمع القرن الحادي والعشرين. فقد أثّرت بصورة جذرية على أسلوب حياة الناس، وتعلمهم وعملهم، وكذلك على التفاعل بين الحكومة والمجتمع المدني''.

٢ - وفي الظروف الحالية التي تشهد ازدياد التقدم العلمي والتقني تتبين بوضوح التوجهات صوب الحوسبة وإنشاء النظم الواسعة النطاق لمعالجة البيانات. وتؤثّر الإنترنت في جميع جوانب الحياة تقريبا سواء على الصعيد العام أم على صعيد المجتمع، ويزداد عدد مستخدمي الإنترنت باستمرار. وفي هذه الحالة، تصبح موارد المعلومات ونظم معالجة البيانات والشبكات الحاسوبية أضعف حلقات الهياكل الرئيسية الوطنية للدولة.

٣ - ونظرا لأن الإنترنت لا يزال، كسابق عهده، مجالا يكاد يكون حرا وغير خاضع لسيطرة أحد، تحاول الجماعات الإجرامية الاستفادة من إمكانيات تكنولوجيا المعلومات والاتصالات الحديثة استفادة كبيرة. وحسب تقديرات خبراء غرفة التجارة الدولية، فإن الزيادة في عدد الجرائم المرتكبة باستخدام شبكة الإنترنت تتناسب طردا مع عدد المستخدمين. ووفقا لبيانات المنظمة الدولية للشرطة الجنائية (إنتربول)، أصبحت الإنترنت مجالا ''تزداد فيه الجريمة بأسرع الوتائر في العالم''.

٤ - ويمكن تقسيم هذه الجرائم بشكل تقريبي إلى ثلاث فئات:

(أ) الجرائم الشاملة على صعيدي الدولة والمجتمع: التي تشكل تهديدا للأمن الوطني والأمن العام (بما في ذلك الدعوة إلى قلب النظام القائم وإلى المساس بالسيادة والاستقلال، وتقويض المصالح الوطنية، والدعاية للإرهاب والمغالاة في الوطنية وكره الأجانب، وجميع أشكال التطرف والتمييز الإثني والعرقي والديني والجنساني، وغيره من أشكال التمييز؛

(ب) الجرائم المدنية الشاملة: التي تشكل تهديدا لحقوق الفرد وحرياته (بما في ذلك انتهاك حقوق الفرد وحرياته، وتشويه السمعة، وممارسة الضغط على الفرد، والتشكيك في

مصداقيته، ونشر المعلومات السرية، والاستفادة من خدمات شبكة الإنترنت على حساب الآخرين، وتزوير الوثائق، وانتهاك حقوق التأليف والنشر)؛

(ج) الجرائم التقليدية: التي تشكل تهديدا للمبادئ الأخلاقية والآداب العامة (بما في ذلك الصور الإباحية، والميل الجنسي إلى الأطفال، وغيره من أنواع الشذوذ الجنسي، وإدمان المخدرات، وإدمان الكحول).

٥ - ويبين ظهور هذا النوع من المعلومات قصور التشريعات الوطنية في مجال تنظيم العلاقات القانونية التي تنشأ عن استخدام الإنترنت ويتطلب اتباع نهج فوق وطني جديد. فعلى الصعيد الدولي، لا يوجد حتى الآن نهج تنظيمي موحد لتحديد التهديدات في مجال أمن المعلومات الدولي وتقييمها، كما لا توجد آليات للتعاون الدولي على درء هذه التهديدات. وفي الوقت نفسه، لا يوجد حتى الآن أي تصور ذي طابع شامل مقدم من فرادى الدول للأمن الدولي في مجال تكنولوجيا المعلومات.

٦ - وتتمثل أسباب ذلك في الفجوة التكنولوجية بين أكثر البلدان نموا وأقلها نموا، والخلافات السياسية الكامنة، وتناقض النهج في تقييم التطورات والحوادث الحاصلة في الفضاء الحاسوبي، وجملة من العوامل الأخرى.

٧ - وتولي الصكوك الدولية قيد النظر على مستوى مؤسسات الأمم المتحدة والمنظمات الأوروبية (مثل منظمة الأمن والتعاون في أوروبا)، أولوية أساسية لبحث تهديدات الجريمة العادية والإرهاب في مجال تكنولوجيا المعلومات في حين تغفل احتمال إساءة استعمال منجزات تكنولوجيا المعلومات واستخدامها كأسلحة معلومات في النزاعات المسلحة لبسط السيطرة على فضاء المعلومات وتهديد السيادة والهوية الوطنية، كما تُغفل هذه الصكوك التهديدات الطبيعية والتهديدات التي هي من صنع الإنسان للهياكل الأساسية الوطنية للمعلومات.

٨ - ولئن كان يمكن للترتيبات المتخذة مع الشركاء العسكريين والسياسيين في مجال أمن المعلومات الدولي أن تشكل عنصرا هاما من عناصر الحماية من هذه التهديدات، فإن الاتفاقات السياسية والقانونية في مجال عدم استعمال أسلحة المعلومات بشكل متبادل، والآليات المشتركة لتخفيف العواقب السلبية للأعمال الضارة إلى أدنى حد وإصلاح الهياكل الأساسية الوطنية للمعلومات وغيرها من التدابير يمكن أن تشكل هي أيضا عنصرا هاما آخر من عناصر الحماية.

٩ - وتجدر الإشارة إلى أن هذا العمل يجري بالفعل بمشاركة ممثلي جمهورية كازاخستان في إطار منظمة معاهدة الأمن الجماعي ومنظمة شانغهاي للتعاون حيث تُدرس على مستوى

الخبراء إمكانية إبرام الاتفاقات الحكومية الدولية المناسبة. وعلى وجه الخصوص، وعملا بخطة عمل الدول الأعضاء في منظمة شانغهاي للتعاون لضمان أمن المعلومات الدولي، المعتمدة بقرار من مجلس رؤساء الدول الأعضاء في المنظمة، المعقود في مدينة بيشكيك في ١٦ آب/أغسطس ٢٠٠٧، وضع فريق خبراء من الدول الأعضاء في المنظمة يُعنى بقضايا أمن المعلومات الدولي مشروع اتفاق حكومي دولي بشأن التعاون في مجال ضمان أمن المعلومات الدولي. ووُقع الاتفاق في ١٥ حزيران/يونيه ٢٠٠٩ في يكاتيرنبورغ خلال اجتماع مجلس رؤساء الدول الأعضاء في المنظمة.

١٠ - ولا بد من لفت الانتباه إلى أنه ليس لهذا الاتفاق مثيل في العالم؛ وسيكون له، في حال توقيعه، أهمية دولية كبرى نظرا لإمكانية انضمام دول أخرى إليه.

١١ - وبالإضافة إلى ذلك، يقوم، في إطار منظمة معاهدة الأمن الجماعي، فريق عامل مؤقت يُعنى بسياسات المعلومات وأمنها بتقديم التقارير إلى لجنة أمناء مجالس الأمن، التابعة للمنظمة. ووضع الفريق برنامج عمل مشترك من أجل إنشاء نظام أمن المعلومات لصالح الدول الأعضاء في المنظمة.

١٢ - واتخذت الدول الأعضاء في المنظمة تدابير تنفيذية ووقائية مشتركة في إطار عملية ''بروكسي'' استنادا إلى تصور موحد لاتجاهات التعاون بين المؤسسات الأمنية والأجهزة التابعة لوزارات الداخلية (الشرطة).

١٣ - ومع مراعاة الطابع الواسع النطاق والعابر للحدود لشبكة الإنترنت، نقترح على الدول الأعضاء في الأمم المتحدة وضع اتفاقية دولية لأمن المعلومات واعتمادها بحيث يكون أحد أركانها الأساسية مكافحة الجرائم المرتكبة باستخدام شبكة الإنترنت.

١٤ - وينبغي أن يكون الهدف من هذا الصك التعاون الدولي. بما فيه مصلحة الجميع في مجال أمن المعلومات ومنع ظهور عواقب جيوسياسية سلبية ناجمة عن إشاعة المعلوماتية على المستوى العالمي.

١٥ - وبالإضافة إلى ذلك، ينبغي في إطار الاتفاقية، توخي إنشاء آليات تنظيمية وتقنية وبرنامجية واجتماعية في مجال تلقي المعلومات واستعمالها من أجل حماية النظام الدستوري، وسيادة جميع الدول الأعضاء في الأمم المتحدة وسلامتها الإقليمية، وضمان الاستقرار السياسي والاقتصادي والاجتماعي، وسيادة القانون والنظام، فضلا عن الآليات اللازمة لإعمال الحقوق والحريات الدستورية للإنسان والمواطن.

١٦ - وعلى الصعيد الوطني، وُضع في كازاخستان مشروع قانون ''عن إدخال تعديلات وتذييلات على بعض القوانين التشريعية لجمهورية كازاخستان بشأن شبكات المعلومات والاتصالات''، وهو قيد نظر مجلس الشيوخ.

١٧ - ويقترح مشروع القانون تعزيز القواعد الناظمة لنشر المعلومات في إقليم جمهورية كازاخستان من خلال شبكات المعلومات والاتصالات.

١٨ - وبغية تعزيز أمن المعلومات وتيسير التعاون الدولي في هذا المجال، تقوم أجهزة الأمن الوطني بالجهود الأساسية على الصعيد الوطني. وتُتخذ بشكل دائم التدابير اللازمة للكشف عن الجرائم الحاسوبية ومنع ارتكابها على الصعيد الدولي.

١٩ - ففي عام ٢٠٠٨، دأبت مثلا لجنة الأمن الوطني ودائرة الأمن الاتحادي في الاتحاد الروسي على وضع حد لنشاط مجموعة إجرامية منظمة عابرة للحدود الوطنية من قراصنة الحاسوب الذين كانوا يبتزون مبالغ مالية طائلة مقابل وقف الهجمات الموزعة من قبيل ''رفض تقديم الخدمة'' على المواقع الشبكية للشركات التي تقوم بأنشطة تجارية بوساطة شبكة الإنترنت.

٢٠ - وتشير نتائج التدابير التنفيذية والتحريات في هذا المجال إلى ظهور أساليب جديدة لتنفيذ الجرائم باستخدام شبكة الإنترنت من قبيل الابتزاز بالإكراه، والابتزاز بالتهديد، والاتجار بالبشر، والقِوادة، ونشر المواد الإباحية، والمواد التي تشيد بالقسوة والعنف، والإرهاب والتطرف.

٢١ - وعلى سبيل المثال، في عام ٢٠٠٨، اكتشفت ٤٥ حالة نشر مواد إباحية. كما تجدر الإشارة إلى زيادة إمكانية الوصول على الإنترنت إلى المواد الإباحية التي يُستغل فيها الأطفال. وهكذا، ففي حين اكتشفت حالة واحدة من حالات نشر المواد الإباحية التي يستغل فيها الأطفال في ٢٠٠٥-٢٠٠٦، و ٧ حالات في عام ٢٠٠٧، فقد اكتشفت ١٤ حالة في عام ٢٠٠٨، منها حالتان مصدرهما شبكة الإنترنت في كازاخستان.

٢٢ - وتجدر الإشارة أيضا إلى أن جهود مكافحة الجرائم في مجال أمن المعلومات والتكنولوجيا المتقدمة غير كافية نظرا لعدم وجود إطار قانوني لتنظيم مسائل أمن المعلومات بصورة دقيقة.

٢٣ - وتحتاج الصكوك القانونية المعيارية في هذا المجال إلى المزيد من التطوير مراعاة لواقع العصر الحالي.

٢٤ - ونرى أنه من المستصوب، استنادا إلى تجربة الدول المتقدمة، تحديث التشريعات الجنائية السارية لجهة تشديد الإجراءات العقابية في حال ارتكاب جرائم من هذه الفئة.

٢٥ - وبالإضافة إلى ذلك، ومع مراعاة الطابع العابر للحدود للجرائم الحاسوبية، ينبغي لأجهزة إنفاذ القانون توسيع مجالات تعاونها العمليات بشكل دائم من أجل التصدي لهجمات الإنترنت بسرعة. وتشير نتائج تعاون أجهزة إنفاذ القانون في كازاخستان مع أجهزة الأمن وهيئات إنفاذ القانون في الدول الأخرى إلى ازدياد الهجمات الحاسوبية التي مصدرها شبكة الإنترنت في كازاخستان. ولهذا السبب تواجه الجهات المتضررة دائما مشكلةَ الفعالية لدى تبلّغ معلومات عن شن هجوم ما نظرا لعدم وجود هيئة رسمية في جمهورية كازاخستان تتولى تلقي المعلومات عن الحوادث الحاسوبية وتبليغها إلى الأجهزة الحكومية المختصة على غرار مراكز أمن الإنترنت العاملة في دول أخرى (المعروفة عامة تحت اسم أفرقة الاستجابة للطوارئ الحاسوبية).

٢٦ - وفي هذا الصدد، نرى ضرورة إنشاء وحدات متخصصة مستقلة في أجهزة إنفاذ القانون تُعنى باكتشاف الجرائم في مجال أمن المعلومات ومنع ارتكابها وكشفها، وتزويد هذه الوحدات بأحدث الوسائل اللازمة لمكافحة هذا النوع من الجرائم.

٢٧ - وكذلك تقدمت كازاخستان بترشحها لعضوية فريق الخبراء الحكوميين الذي سينشأ وفقا للفقرة ٤ من قرار الجمعية العامة ٣٧/٦٣ المعنون ''التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي''.

لبنان

[الأصل: بالإنكليزية]
[٢٢ أيار/مايو ٢٠٠٩]

١ - نحن بصدد إصدار قانون جديد يغطي قطاع تكنولوجيا المعلومات والاتصالات في لبنان، وهو في المرحلة النهائية لاعتماده من جانب مجلس النواب؛ وسيغطي هذا القانون جميع المسائل ذات الصلة بهذا القطاع بما في ذلك الأمن وجميع الأمور المتعلقة بجرائم المعلومات.

٢ - وبمجرد أن يبدأ سريان القانون المذكور أعلاه، ستضع وزارة الاتصالات ترتيبات فيما يتعلق بالأمور المتعلقة بالنقاط (ب) و (ج) و (د) (من الفقرة ٣ من القرار ٣٧/٦٣) مع الوزارات الأخرى وجميع الإدارات العامة المعنية.

ليتوانيا

[الأصل: بالإنكليزية]
[٢٦ أيار/مايو ٢٠٠٩]

١ - تولي ليتوانيا أهمية كبرى لمسألة أمن المعلومات في جدول أعمالها الوطني والدولي على حد سواء. وتشكل مسألة الأمن الحاسوبي عنصراً هاماً من عناصر الأمن الوطني.

٢ - ويتسم التعاون على الصعيد الدولي بأهمية كبرى من أجل تعزيز حماية نظم الاتصالات والمعلومات، وكذلك رفع مستوى الوعي. وترحب ليتوانيا باكتساب مسألة أمن المعلومات المزيد من الاهتمام على جدول أعمال المنظمات الدولية مثل الأمم المتحدة والاتحاد الأوروبي ومنظمة حلف شمال الأطلسي ومنظمة الأمن والتعاون في أوروبا، كما تشارك بنشاط في عمل هذه المنظمات الرامي إلى معالجة هذه المسألة. وتتعاون المؤسسات الليتوانية بشكل وثيق مع شركائها. وليتوانيا طرف في اتفاقية مجلس أوروبا المتعلقة بالجرائم الحاسوبية منذ ١ تموز/يوليه ٢٠٠٤.

٣ - وليتوانيا واحدة من ٧ أعضاء في منظمة حلف شمال الأطلسي رعت إنشاء مركز الامتياز المعني بالدفاع الحاسوبي التعاوني التابع لمنظمة حلف شمال الأطلسي في تالين، بإستونيا، الذي أصبح واحدا من مراكز الامتياز التابعة لمنظمة حلف شمال الأطلسي في ١٤ أيار/مايو ٢٠٠٨.

٤ - واعتُمد برنامج ''من أجل شبكة إنترنت أكثر أمناً'' (Safer Internet plus)، وهو برنامج مجتمعي متعدد السنوات يهدف إلى تعزيز استخدام أكثر أمناً لشبكة الإنترنت وتكنولوجيات الإنترنت الجديدة، بموجب قرار صادر عن البرلمان والمجلس الأوروبيين في ١١ آذار/مارس ٢٠٠٥. وتتمثل المهام الرئيسية للبرنامج في توعية المجتمع بالمسائل المتصلة بجعل الإنترنت أكثر أمناً وإنشاء الخطوط الساخنة.

٥ - وأثناء الجمعية العامة للرابطة الدولية للخطوط الساخنة للإنترنت، المعقودة يومي ٢٨ و ٢٩ أيار/مايو ٢٠٠٨ في دبلن، أصبح الخط الساخن الليتواني عضواً في الرابطة.

٦ - وعلى الصعيد الوطني، جرى في عام ٢٠٠٠ أول تقييم لحالة الهياكل الأساسية للمعلومات، مما شكّل بداية المشاركة المعقدة لمعالجة هذه المسألة. وتمثلت إحدى المجالات الرئيسية للتقييم في مستوى فهم مسألة أمن المعلومات والسياسات القائمة ومستوى الحماية الحاسوبية في مؤسسات الدولة.

٧ - وعُهد إلى وزارة الداخلية في جمهورية ليتوانيا الاضطلاع بدور المنسق لتكنولوجيات أمن المعلومات في مؤسسات الدولة بموجب قرار حكومة جمهورية ليتوانيا (رقم ٢٩١، المؤرخ ١٤ آذار/مارس ٢٠٠١).

٨ - وجرى وضع عدد من التدابير وتنفيذها بهدف الحفاظ على أمن المعلومات، وذلك على النحو المحدد في استراتيجية الدولة المتعلقة بأمن تكنولوجيا المعلومات (حتى عام ٢٠٠٤)، واستراتيجية الدولة المتعلقة بأمن المعلومات الإلكترونية في مؤسسات الدولة حتى عام ٢٠٠٨.

٩ - وأُنشئ الفريق العامل المشترك بين المؤسسات المعني بمسائل الأمن الحاسوبي بموجب مرسوم صادر عن رئيس وزراء ليتوانيا في ١٧ حزيران/يونيه ٢٠٠٨. وفي ٢١ تشرين الثاني/نوفمبر ٢٠٠٨، قدم الفريق العامل تقريرا إلى الحكومة يتضمن مقترحات وتوصيات لتحسين الأمن الحاسوبي في ليتوانيا.

١٠ - وتخطط حكومة ليتوانيا لإعداد مشروع القانون المتعلق بشبكات الاتصالات الإلكترونية وأمن المعلومات والاستراتيجية الجديدة المتعلقة بأمن المعلومات الإلكترونية في المستقبل القريب بهدف تحسين قدرات الدولة في مجال أمن المعلومات والدفاع الحاسوبي على وجه الخصوص. ومن بين أهداف الاستراتيجية المذكورة آنفاً كفاءة الهياكل المؤسسية بوصفها إطار الدفاع ضد الهجمات الحاسوبية، وكفالة أمن ومرونة الهياكل الأساسية لنقل البيانات، ووقاية الهياكل الأساسية الحيوية للمعلومات على نحو فعّال من الهجمات الحاسوبية، وتحقيق مستوى عالٍ من الامتثال للسياسات والمتطلبات عن طريق اعتماد سياسة مراجعة تضعها أطراف ثانية وثالثة.

١١ - ومنذ عام ٢٠٠٥، أجرت هيئة تنظيم الاتصالات في ليتوانيا دراسات استقصائية بشأن شبكات الاتصالات الإلكترونية وأمن المعلومات بهدف البتّ في المسائل المعلقة. وتضطلع هيئة تنظيم الاتصالات بمهام فريق وطني للاستجابة للطوارئ الحاسوبية.

١٢ - وتتمثل مهام الفريق الوطني للاستجابة للطوارئ الحاسوبية في ليتوانيا في تعزيز الأمن في مجتمع المعلومات عن طريق منع ومراقبة ومعالجة الحوادث المتصلة بأمن المعلومات ونشر المعلومات المتعلقة بالتهديدات التي تواجه قطاع أمن المعلومات. وافتُتح الموقع الشبكي الجديد www.cert.lt في ٣٠ أيلول/سبتمبر ٢٠٠٨. وفي ١٦ كانون الثاني/يناير ٢٠٠٩، أصبح الفريق عضواً معتمداً لدى شبكة Trusted Introducer، وهي الشبكة موضع الثقة بالنسبة لأفرقة الاستجابة لحوادث الأمن الحاسوبي والأفرقة الوطنية للاستجابة للطوارئ الحاسوبية في أوروبا.

١٣ - وتسعى ليتوانيا لكفالة أن يبقى الاهتمام الدولي المولى لمسألة أمن المعلومات كبيراً وأن تزداد الجهود المبذولة لمعالجة هذه المسألة. كما تسعى ليتوانيا للمشاركة الفعلية في العمل الذي سيضطلع به المجتمع الدولي في المستقبل لتعزيز أمن المعلومات والمساهمة في هذا العمل.

المكسيك

[الأصل: بالإسبانية]
[٨ حزيران/يونيه ٢٠٠٩]

١ - تنبع المشاكل الأمنية، بحسب التصورات الرئيسية السائدة، من مواطن الضعف التي يمكن أن تعاني منها نظم المعلومات التي تحكم برامج الدفاع المعتمدة في البلدان، ومن احتمال استخدام الإرهابيين للمعلومات والاتصالات لأغراض العنف أو الردع.

٢ - وفي هذا السياق، واهتماما منها بتطوير أمن الاتصالات في العالم، شاركت المكسيك في ''الجمعية العالمية لتوحيد مقاييس الاتصالات'' التي عقدت في جنوب أفريقيا في تشرين الأول/أكتوبر ٢٠٠٨، وقدمت فيها مع أعضاء آخرين في لجنة البلدان الأمريكية للاتصالات السلكية واللاسلكية (أوروغواي وباراغواي وكندا) قرارا لدعوة الجامعات إلى المشاركة فعليا في دورات الاتحاد الدولي للاتصالات اللاسلكية لتعزيز عمله.

٣ - وعلى المنوال نفسه، قامت المكسيك على الصعيد الإقليمي مقام نائب رئيس الاجتماع العشرين للجنة التوجيهية الدائمة للجنة البلدان الأمريكية للاتصالات السلكية واللاسلكية، الذي قدمت أثناءه إلى دول المنطقة دورة عن ''حالات التدخل المضرة بالنظم الساتلية'' عن طريق اللجنة الاتحادية للاتصالات السلكية واللاسلكية. واتفقت الدول في هذا الاجتماع على عقد الجمعية العادية الخامسة للجنة البلدان الأمريكية للاتصالات السلكية واللاسلكية في الفصل الأول من عام ٢٠١٠ في المكسيك.

٤ - ومن الأنشطة التي تضطلع بها المكسيك لتعزيز الأمن الدولي في مجال المعلومات والاتصالات، يمكن الإشارة إلى أن المكسيك تعوّل على ''وحدة شرطة الوسائل الحاسوبية'' التي تشمل مهامها، إلى جانب اتخاذ إجراءات وقائية للحيلولة دون ارتكاب جرائم عبر الإنترنت والوسائل الحاسوبية الأخرى، مجالا محددا يتمثل في منع الجرائم ضد القاصرين ومعالجة الشكاوى المقدمة بشأنها.

صربيا

[الأصل: بالإنكليزية]
[٩ حزيران/يونيه ٢٠٠٩]

١ - يلزم على الدول توحيد المعايير القانونية التي تعتمدها في مجال الفضاء الحاسوبي لأنه لم يعد محصورا بأرض بلد واحد ولأن الجماعات و/أو الأفراد المنخرطين في أعمال تخريبية و/أو في الاستخدام غير المأذون به لنظم المعلومات والاتصالات قد لا يكونون غالبا في البلد الذي يقع فيه الحادث. ويتمثل الحل في اتخاذ خطوة أولى وإقامة أساس متين لاعتماد نهج متوازن قائم على توصيات تدعو إلى ترسيخ التشريعات على الصعيد الدولي، والغرض من ذلك هو تعزيز الأمن الدولي من جهة، وكفالة تدفق المعلومات بحرّية من جهة أخرى.

٢ - ويتعين، على مستوى الدولة في المقام الأول، سن قوانين أشد صرامة لا بد أن تكون متماشية مع المهارات التقنية للمستعملين ومستواهم التعليمي، ودعمها بتثقيف المستعملين المستمر وإنشاء وكالات متخصصة تتولى تخطيط الجانب التقني لهذا المجال وتنظيمه ورصده.

٣ - وفي معرض تقييم التقيد بمبدأ أمن المعلومات في مجال نظم المعلومات والاتصالات، جرى تبيان العناصر التالية:

المشاكل:

- إصدار يومي لأنواع جديدة من البرامج الضارة التي تهدد أمن نظم المعلومات والاتصالات؛
- إجراء محاولات عديدة لاختراق المواقع الإلكترونية الرسمية الخاصة بوزارة الدفاع والقوات المسلحة لجمهورية صربيا؛
- ترويج أفكار إرهابية على الإنترنت.

الإجراءات الأمنية والتعاون:

- استخدام البرمجيات الملائمة المضادة للفيروسات على جميع مستويات استخدام نظم المعلومات والاتصالات في وزارة الدفاع والقوات المسلحة لجمهورية صربيا
- مواصلة توفير الحماية من عمليات القرصنة التي تتعرض لها المواقع الإلكترونية الخاصة بوزارة الدفاع والقوات المسلحة لجمهورية صربيا

- المشاركة في المؤتمرات والحلقات الدراسية الهادفة إلى التوعية بمخاطر الجريمة الحاسوبية والإرهاب الحاسوبي

التوصيات:

إنشاء وكالة دولية تُكلَّف بما يلي:

- تقييم المشاكل التي تواجهها حماية قنوات البيانات والاتصالات
- رصد عوامل ''التهديد'' في مجال الجريمة الحاسوبية والإرهاب الحاسوبي الدوليين
- تقييم مشاكل الأمن الدولي في ميدان نظم المعلومات والاتصالات والتوصية بحلول لها
- وضع برامج تثقيفية بغرض التوعية بمخاطر الجريمة الحاسوبية والإرهاب الحاسوبي
- تنظيم عمليات تبادل المعارف والخبرات على الصعد الحكومية الدولية

طاجيكستان

[الأصل: بالإنكليزية]
[٢٠ أيار/مايو ٢٠٠٩]

١ - تُعتبر الاتصالات في يومنا هذا عاملا هاما جدا من عوامل التنمية الاقتصادية والاستقرار والأمن في أي دولة من الدول.

٢ - وقد وفرت طاجيكستان جميع الشروط اللازمة لتطوير حقل الاتصالات عن طريق السماح بالتنافس الحر ومنح الرخص لبدلاء من الجهات التي تدير الاتصالات والتي تقدم خدماتها، وعبر عرض خدمات جديدة.

٣ - ولا بد من إيلاء الاهتمام لكفالة أمن اشتغال الهياكل الأساسية للمعلومات والاتصالات، وتعزيز مستوى الحماية الموفر لنظم المعلومات لدى الشركات، والاستناد إلى ذلك لمواجهة انتشار إيديولوجية الإرهاب والتطرف والعنف.

٤ - وطاجيكستان مستعدة لدعم المبادرة المذكورة أعلاه وللتعاون في مجال تطوير سلامة المعلومات على الصعيد الدولي.

تايلند

[الأصل: بالإنكليزية]
[٣ حزيران/يونيه ٢٠٠٩]

تقييم عام لمسائل أمن المعلومات

١ - دخل العالم اليوم عصر مجتمع المعلومات الذي تستخدم فيه تكنولوجيا المعلومات لجعل الحياة أكثر يسرا في مجالات منها، على سبيل المثال، المعاملات المالية وتبادل الأنباء والمعلومات. غير أن تكنولوجيا المعلومات لا تنطوي فقط على فوائد، بل هي تتيح أيضا لبعض الجماعات فرص استخدامها بشكل غير قانوني وغير أخلاقي، مما يولّد مشاكل من قبيل سرقة المعلومات عبر نظام المعلومات، والاعتداءات الحاسوبية، وتزوير الوثائق الإلكترونية، والتسلل إلى قواعد البيانات الحكومية لسرقة البيانات الشخصية، وانتهاك حرمة الحياة الخاصة. ورغم ذلك، تشكل تكنولوجيا المعلومات والاتصالات عاملا ضروريا للنمو الاقتصادي في جميع البلدان. ويمكن لتزايد تعقيد التكنولوجيا ونقص الموظفين المتمرسين في مجال أمن المعلومات وانعدام الموارد الكافية أن تؤدي إلى انخفاض مستوى أمن المعلومات في النظم والشبكات الحاسوبية، الأمر الذي يمكن أن يؤدي بدوره إلى فقدان ثقة الجمهور، ولا سيما في مجالات العمل المصرفي والتجارة الإلكترونية والإدارة. لذا، يلزم تبيان المشاكل ذات الصلة واستشرافها لوضع ضمانات واتخاذ تدابير أمنية لدرء هذه المخاطر. ولتحقيق هذا الهدف، ينبغي أن تتعاون البلدان لاتخاذ تدابير تكفل أمن المعلومات بهدف تحديد معيار دولي تتقيد به جميع البلدان.

الجهود المبذولة على الصعيد الوطني لتعزيز أمن المعلومات وتشجيع التعاون الدولي في هذا المجال

٢ - اعتبرت الحكومة الملكية التايلندية السياسة الأمنية الوطنية أحد مجالات السياسة العامة ذات الأولوية المشمولة بالخطة الاستراتيجية الحكومية للفترة ٢٠٠٩-٢٠١١ (B.E. 2552-2554). وتتخذ الحكومة حاليا تدابير قانونية لتعزيز أمن المعلومات بحيث لا تُستخدم شبكات المعلومات بشكل لا أخلاقي ولا تضر بالأمن القومي. وتشمل هذه التدابير سن قوانين بشأن الجريمة الحاسوبية، والمعاملات الإلكترونية، والتواقيع الإلكترونية، والتحويلات المالية الإلكترونية.

٣ - وما فتئت وزارة تكنولوجيا المعلومات والاتصالات تولي أهمية كبرى لكفالة أمن المعلومات على شبكة الإنترنت وحل مشكلة المواقع الإلكترونية غير الأخلاقية وغير

القانونية، وأنشأت مركز عمليات لأمن الإنترنت بهدف رصد التهديدات التي تتعرض لها تكنولوجيا المعلومات والتنسيق مع الوكالات الأخرى لوضع حد لاستخدام شبكات المعلومات بشكل يهدد الأمن القومي. ويهدف المركز أيضا إلى إنهاء استخدام شبكات المعلومات بشكل غير قانوني وإقامة نظام لرصد الفيروسات والبريد الإلكتروني غير المرغوب.

٤ - وفيما يتعلق بالتعاون الدولي، ينبغي إقامة هيئة تنسيق تقوم مقام الجهة المرجعية. وينبغي أن تحدد هذه الهيئة السياسات الكفيلة بمنع تدفق المعلومات اللاأخلاقية ومكافحته، والتدابير اللازمة لمواجهة التهديدات التي يتعرض لها أمن المعلومات، والتدابير الوقائية التي يُسترشد بها عند الاضطلاع بأنشطة مشتركة.

بحث المفاهيم الدولية ذات الصلة الرامية إلى تعزيز أمن النظم العالمية للمعلومات والاتصالات

٥ - لا بد من اعتماد مفاهيم ومبادئ دولية مشتركة لتعزيز أمن المعلومات الشامل لأن العالم الحاسوبي اليوم أصبح متداخلا وبات بلا حدود. لذا، يمكن لمشكلة أمن المعلومات التي تنشأ في بلد أن تنتقل وتؤثر في بلد آخر.

التدابير المحتملة التي يمكن للمجتمع الدولي اتخاذها لتعزيز أمن المعلومات على الصعيد العالمي

٦ - من التدابير المحتملة التي يمكن للمجتمع الدولي اتخاذها تبادل المعلومات والتدابير الوقائية وتدابير مكافحة التهديدات التي يتعرض لها أمن المعلومات. وينبغي أيضا تعزيز التعاون في تطوير قدرات مختلف البلدان في مجال تكنولوجيا المعلومات لجعلها متساوية، ولا سيما نقل تكنولوجيا البلدان المتقدمة وخبراتها إلى بلدان أقل تقدما للمساعدة في بناء قدرات هذه البلدان الأخيرة. وينبغي أيضا وضع برامج تدريبية تشمل مسائل التوعية بالمخاطر والتهديدات التي يتعرض لها أمن المعلومات ومنعها وكشفها وإدارتها ومواجهتها للتقليل إلى الحد الأدنى من أخطارها.

٧ - وبالإضافة إلى ذلك، من الضروري إنشاء آلية تنسيق لربط أعمال مختلف الوكالات المعنية فيما بينها من أجل تحديد الوجهة والسياسة العامة اللتين ينبغي تبنيهما لضمان أمن المعلومات الوطني لكي يكون بمستوى معين، وسلوك الاتجاه نفسه.

٨ - وينبغي تشجيع الجهود التي يبذلها بعض الوكالات الدولية للحث على تشجيع التعاون الدولي في مجال تعزيز أمن المعلومات، وتحديدا الاتحاد الدولي للاتصالات. وقد نظم هذا الاتحاد مؤتمرا دوليا لتبادل الخبرات وبحث التدابير الكفيلة بحل المشاكل الناجمة عن إساءة

استعمال تكنولوجيا المعلومات. كما أنشئت أفرقة دراسة لتبيان التدابير الكفيلة بتعزيز أمن المعلومات، بحيث يتسنى للحكومات والوكالات المعنية تطبيق واستخدام النتائج التي تخلص إليها تلك الأفرقة.

٩ - وينبغي أيضا إنشاء أفرقة للاستجابة للطوارئ الحاسوبية في كل بلد بمساعدة البلدان التي حققت نجاحا بفعل إنشاء مثل هذه الأفرقة.

١٠ - وينبغي الاهتمام بمسألة حماية الهياكل الأساسية الحيوية في كل بلد من الاعتداءات الحاسوبية وقيام أوساط المجتمع الدولي بتبادل المساعدة وبالتعاون بسرعة، والبحث بصورة مشتركة في التدابير الكفيلة بالتصدي لهذه المخاطر أو التخفيف منها إلى الحد الأدنى.

١١ - وينبغي التشجيع على زيادة التوعية في الأمم المتحدة بمسألة أمن المعلومات وربما مناقشة القواعد والأنظمة التي يمكن تبنيها بشأن حرب المعلومات وإصدار تقارير سنوية عن التهديدات التي يتعرض لها أمن المعلومات ومواطن الضعف التي يعاني منها.

أوكرانيا

[الأصل: بالروسية]

[٢٠ أيار/مايو ٢٠٠٩]

١ - نشأت عن الدور المتعاظم الذي تؤديه المعلومات في مختلف مجالات الحياة اليومية للمجتمع شواغل تتصل بأمن المعلومات. ويؤدي إدخال تكنولوجيا المعلومات المتطورة في مجالي الأنشطة الحكومية وحياة المجتمع إلى زيادة الاعتداءات الحاسوبية المحتملة من جانب العناصر الإجرامية والأفراد الذين يسعون إلى ارتكاب أفعال منافية للقانون، على نظم المعلومات والاتصالات السلكية واللاسلكية وموارد المعلومات لدى الهيئات الحكومية والمؤسسات التجارية.

٢ - ويتصل نصف الجرائم الحاسوبية المكتشفة في العالم بحصول أشخاص غير مأذون لهم على المعلومات الحاسوبية. وتتزايد معدلات الجريمة الحاسوبية ذات الدوافع المغرضة وتتزايد معها الأضرار المادية التي تسببها. ويشهد الوقت الراهن ارتفاعا في معدلات الجريمة المرتكبة على يد الجماعات عبر الوطنية من قراصنة الحاسوب.

٣ - وتتسم الجريمة الحاسوبية بدرجة عالية من السرية، وليس في الإمكان رسم صورة متكاملة لما ينتج عنها من انتهاكات قانونية، نظرا إلى أن كلا من الهيئات الحكومية والمؤسسات التجارية التي تتعرض لجرائم حاسوبية تفعل كل ما في وسعها للتستر عليها وتميل

إلى عدم البوح بالأضرار التي تلحق بها والكشف عن ضعف نظم حماية المعلومات لديها، تخوفا من إشانة السمعة. ونتيجة لما ذكر، لا تصل مثل هذه الأعمال الإجرامية إلى علم الجمهور إلا لماما، مما يؤكد أهمية وضع تدابير مشتركة للوقاية والإنذار المبكر تشكل أساس إنشاء نظام لحماية المعلومات.

٤ - ولا تشكل الجريمة الحاسوبية عادة سوى الخطوة الأولى في سلسلة أعمال إجرامية تقود إلى أشكال أخرى من الأعمال الإجرامية التقليدية - مثل الاحتيال والابتزاز والغش وما إلى ذلك. ويشهد كل يوم استنباط طرائق أحدث لتنفيذ هذه الأعمال الإجرامية، التي يزداد تطورها وتتعاظم سريتها وتترتب عليها أضرار اقتصادية وسياسية جسيمة في جميع بلدان العالم تقريبا. وعلاوة على ذلك، يرى معظم الخبراء أن هناك صلة مباشرة بين السيادة المعلوماتية للدولة ومسائل الأمن الوطني.

٥ - وتثار أثناء مكافحة الجريمة في مجال تكنولوجيا المعلومات مسائل عديدة ذات طابع قانوني، نظرا إلى أن الأدلة الحاسوبية تكون غير مادية وسريعة الزوال في كثير من الأحيان. وتؤكد صعوبة حل المشاكل التي تتميز بها الجريمة الحاسوبية ضرورة التعاون على الصعيد الدولي، مما يحتم على جميع البلدان في نهاية المطاف أن تتشارك ما لديها من مواد قانونية وإجرائية ومعيارية ذات صلة وسمات مشتركة.

٦ - وتدل ممارسات التحقيق في الجرائم الحاسوبية على ضرورة تنسيق التعاون وسط هيئات إنفاذ القانون التابعة لمختلف الدول.

٧ - وهناك ممارسة عالمية تتمثل في تنفيذ تدابير مشتركة عند إجراء التحقيقات في الجرائم الحاسوبية. ويُشارك جهاز الأمن الأوكراني مشاركة فعالة في العمليات المشتركة لهيئات إنفاذ القانون وأجهزة الأمن العالمية، التي تنفذ في إطار مكافحة استغلال الأطفال في المواد الإباحية، وأعمال الغش التي تُنفّذ عن طريق شبكة الإنترنت، والإرهاب الدولي.

٨ - وعلاوة على ذلك يتعين توحيد الجهود من أجل مواصلة تعزيز التعاون في مجال كفالة أمن المعلومات وخدمة المصالح المشتركة وتنفيذ تدابير لحمايتها، ويُفضّل أن يكون ذلك على أساس الاتفاقات الثنائية والمتعددة الأطراف. ولن يتحقق النجاح في حل مشاكل أمن المعلومات، في رأينا، إلا إذا تعاونت الهيئات الحكومية التابعة لمختلف الدول تعاونا فعالا، لا سيما وأن القاعدة القانونية اللازمة لذلك التعاون قد أرسيت بالفعل.

٩ - وإذ يدرك جهاز الأمن الوطني الأوكراني ضرورة مجابهة مخاطر الجريمة الحاسوبية والإرهاب الحاسوبي، فقد أقام علاقات مع هيئات إنفاذ القانون وأجهزة الأمن للدول الأجنبية.

١٠ - وتجدر الإشارة إلى أن الجرائم الحاسوبية تستهدف في أحيان كثيرة شبكات الحاسوب التابعة للهيئات الحكومية، ويكون النجاح في تتبع ومعاقبة مرتكبي هذه الجرائم مرهونا بنوعية العلاقات القائمة على الصعيد الدولي، وكذلك بمدى استكمال القوانين الوطنية وفقا للمعطيات الحديثة.

١١ - ونُفذت في أواخر عام ٢٠٠٨، بالتعاون مع قوة الشرطة الوطنية للمملكة الهولندية ودائرة الأمن الاتحادي بالاتحاد الروسي، عملية منسقة لإحباط أنشطة مخالفة للقانون لمجموعة إجرامية من قراصنة الحاسوب الدوليين، تخصصت في الاستيلاء عن طريق الاحتيال على الموارد المالية لعملاء المؤسسات المالية - الائتمانية، من خلال التدخل بصورة غير مشروعة في عمل النظم الآلية لهذه المؤسسات.

١٢ - ويتواصل توسيع آفاق التعاون الدولي في مجال مكافحة الجريمة الحاسوبية، نظرا إلى استمرار ارتفاع معدلات هذه الجريمة على صعيد العالم، ووجود علاقات تربط الجماعات الإجرامية من قراصنة الحاسوب في البلدان المختلفة، وعدم تأثر مخاطر هذا النوع من الجرائم بالحدود الدولية للبلدان.

١٣ - ومن هذا المنطق ووفقا لأحكام الاتفاقية الدولية المتعلقة بالجريمة الحاسوبية، أنشئت آلية تتسم بالحيوية وسهولة الاستخدام - وهي شبكة وطنية لمراكز اتصال تعمل على مدار الساعة طيلة أيام الأسبوع، تربط بين بلدان مجموعة الثمانية والدول الأخرى الأطراف في الاتفاقية.

١٤ - واستنادا إلى الأمر الصادر عن رئيس أوكرانيا بشأن إنشاء مركز وطني للاتصال على مدار الساعة طيلة أيام الأسبوع باستخدام عناصر من جهاز الأمن الوطني لأوكرانيا، يعكف فريق عامل مكون من موظفين تابعين لجهاز الأمن ووزارة الشؤون الداخلية ومكتب المدعي العام ووزارة العدل في أوكرانيا، على إعداد مشروع قانون أوكراني ''يتعلق بإدخال تعديلات على قانون أوكرانيا 'بشأن التصديق على الاتفاقية المتعلقة بالجريمة الحاسوبية'''' و ''إدخال تعديلات على قانون أوكرانيا 'بشأن الاتصالات السلكية واللاسلكية'، وقانون أوكرانيا 'بشأن هيكل وقوام جهاز الأمن الأوكراني''''، وفضلا عن مرسوم رئاسي بشأن تنظيم أعمال مركز الاتصال المشار إليه.

١٥ - ويعمل جهاز الأمن الأوكراني في الوقت الراهن، في سياق تنفيذ هذا القرار الرئاسي، على اتخاذ خطوات تجاه تسجيل مركز الاتصال الوطني ضمن الشبكة الدولية لمراكز الاتصال.

١٦ - ويُنتظر أن يؤدي تشغيل مركز الاتصال المشار إليه في أوكرانيا إلى تعزيز فعالية ونوعية الحلول المتعلقة بمهام تبادل المعلومات والتعاون في مجال مكافحة الجريمة الحاسوبية على الصعيد الدولي.

١٧ - ولأغراض تنفيذ القرارات الصادرة عن مؤتمر القمة العالمي لمجتمع المعلومات (المرحلة الأولى - جنيف، ١٠-١٢ كانون الأول/ديسمبر ٢٠٠٣؛ والمرحلة الثانية، تونس، ١٦-١٨ تشرين الثاني/نوفمبر ٢٠٠٥)، اعتمد في أوكرانيا قانون بشأن ''المبادئ الأساسية لتنمية مجتمع المعلومات في أوكرانيا للفترة ٢٠٠٧-٢٠١٥''، تتمثل أولوياته الأساسية في الاندماج في الفضاء الحاسوبي العالمي وتنمية مجتمع المعلومات في أوكرانيا. وينص هذا القانون على تعزيز أمن المعلومات في ظروف استخدام أحدث تكنولوجيات المعلومات والاتصالات.

١٨ - بالإضافة إلى ذلك، جرى إعداد واعتماد خطة لتطوير الاتصالات السلكية واللاسلكية في أوكرانيا، وهي خطة ترمي إلى تعزيز الإجراءات التنظيمية - التقنية، التي تهدف إلى كفالة الأمن التشغيلي لجميع عناصر البنية التحتية للاتصالات السلكية واللاسلكية في أوكرانيا، بطرق منها:

- تأسيس قاعدة قوانين معيارية من أجل معالجة المسائل التقنية والمتعلقة بالتشفير في مجال حماية المعلومات، وترسيخ جذورها بشكل تدريجي وتحقيق اتساقها مع المعايير الأوروبية والدولية؛
- إيجاد طرائق حديثة لحماية المعلومات على أساس الوسائل التقنية الخاصة بحل المشاكل المعقدة المتعلقة بتوفير الحماية للمعلومات في شبكات الاتصالات السلكية واللاسلكية؛
- إقامة نظام شرعي لاعتراض المعلومات في شبكات الاتصالات السلكية واللاسلكية، في الحالات المنصوص عليها في القوانين؛
- تأسيس مركز تنسيق حكومي معني بالمسائل الأمنية في شبكات المعلومات والاتصالات السلكية واللاسلكية ذات الاستخدامات العامة، والمساعدة على تأسيس مراكز حكومية وغير حكومية قادرة على التصدي للحوادث التي تشهدها شبكات الاتصالات السلكية واللاسلكية.

١٩ - وتشكل القوانين الأوكرانية التالية أيضا قاعدة قانونية معيارية لحماية المعلومات في أوكرانيا: ''قانون المبادئ الأساسية للأمن الوطني لأوكرانيا''، و ''قانون المعلومات''، و ''قانون الحماية للمعلومات ونظم المعلومات والاتصالات السلكية واللاسلكية''، وأمر

رئيس أوكرانيا بشأن ''حالة المعلومات في أوكرانيا وتوفير الحماية التقنية لها''، وأمر مجلس وزراء أوكرانيا بشأن ''قواعد توفير الحماية لنظم المعلومات والاتصالات السلكية واللاسلكية''، وكذلك ''نظام الارتباط بالشبكات العالمية لبث البيانات''، ومجموعة مسائل أخرى مشابهة، بالإضافة إلى مجموعة كبيرة من القوانين المعيارية المسجلة لدى وزارة العدل، والتي تحكم مسائل ربط نظم المعلومات بالشبكات العالمية، وإصدار التراخيص لفرادى المؤسسات الخاصة، وتحديد نظام التقييم في مجال حماية المعلومات، وما إلى ذلك.

٢٠ - وتنص القوانين المعيارية على أنه يجب ألا تستخدم لأغراض توفير الحماية اللازمة للمعلومات سوى النظم المحمية لتكنولوجيا المعلومات والاتصالات السلكية واللاسلكية، أي تلك التي تشتمل على نظم متعددة العناصر لتوفير الحماية للمعلومات، مثل مجموعة واحدة من الإجراءات القانونية والتنظيمية، وكذلك البرامجيات ومعدات الحاسوب القادرة على مجابهة المخاطر. ويشترط هنا أن تشتمل النظم المتعددة العناصر لحماية المعلومات، وكذلك مجموعة وسائل الحماية المستخدمة فيها، على خصائص تكفل امتثالها للشروط المعيارية الواردة في الصكوك المعتمدة في مجال حماية المعلومات.

٢١ - ولأغراض تحديد مواصفات النظم المتعدد العناصر لحماية المعلومات وفرادى وسائل الحماية، جرى في أوكرانيا وضع زهاء ٥٠ معيارا تقنيا وبدأ العمل بها، من أجل تحديد شروط تقييم القدرة على حماية المعلومات وتصنيف النظم المحمية للمعلومات والاتصالات السلكية واللاسلكية، وتحديد نظام استخدام أنشطة الحماية المطلوبة لكل واحدة من الوسائل المستخدمة للحماية في النظام المتعدد العناصر، استنادا إلى تصنيفات النظم المحمية والغرض من المعلومات المعنية ومجال استخدامها وطريقة إعدادها.

٢٢ - وأنشئ في أوكرانيا كذلك نظام وطني غير حكومي لمعايير تقييم درجة حماية تكنولوجيا المعلومات. ويستند هذا النظام إلى مجموعة الصكوك المعيارية المتسقة مع الصكوك المماثلة في بلدان الاتحاد الأوروبي ومع المعايير الدولية، وبخاصة المعيار ١٥ ٤٠٨ الخاص بالإعلام والتثقيف والاتصالات للمنظمة الدولية لتوحيد مقاييس اللجنة الكهربائية التقنية الدولية المتعلق بحماية المعلومات في نظم المعلومات والاتصالات السلكية واللاسلكية ضد إمكانيات الحصول عليها بصورة غير مأذون بها.

٢٣ - وبالإضافة إلى ذلك، يجري العمل على المستوى الوطني في أوكرانيا من أجل إنشاء نظام تدابير تنظيمية - تقنية تهدف إلى مكافحة الأنشطة غير المأذون بها فيما يتصل بنظم المعلومات والاتصالات السلكية واللاسلكية التابعة للسلطات التنفيذية الحكومية، وهيئات

إنفاذ القانون والجمارك والضرائب، والمؤسسات الائتمانية – المالية وغيرها، ولا سيما محاولات التدخل في عملها باستخدام إمكانيات شبكة الإنترنت.

٢٤ – وتمثلت استجابة المجتمع الدولي لمثل هذه الأعمال في إنشاء نظام متطور لهياكل محددة المهام من أجل الاستجابة السريعة للحالات التي تهدد أمن موارد المعلومات، وتشكيل أفرقة للاستجابة للطوارئ الحاسوبية. ويجري تنسيق أنشطة هذه الهياكل على الصعيد الدولي من خلال منتدى الأفرقة المعنية بالأمن والتصدي للحوادث – منتدى التصدي للحوادث التي تهدد الأمن.

٢٥ – ولأغراض تهيئة إمكانية إطلاع الدائرة الحكومية لتوفير حماية خاصة لنظم المعلومات والاتصالات بمثل هذه الأعمال، صدر الأمر الرئاسي رقم ٩٤ المؤرخ ١٠ حزيران/يونيه ٢٠٠٨ بشأن اعتماد نظام للهيئات التنسيقية المعنية بالوقاية من آثار الأنشطة غير المأذون بها والكشف عنها والقضاء عليها، فيما يتصل بموارد المعلومات الحكومية في نظم المعلومات والاتصالات السلكية واللاسلكية لدى السلطات الحكومية، والأجهزة المحلية للإدارة الذاتية، والتشكيلات العسكرية، والمؤسسات التجارية، والمؤسسات الحكومية، والمنظمات بغض النظر عن الجهات التي تتبع لها.

٢٦ – وأنشئ، في إطار تنفيذ هذا الأمر، موقع شبكي وصندوق بريد إلكتروني على شبكة الإنترنت (www.cert.gov.ua).

٢٧ – ويجري العمل في أوكرانيا على وضع تدابير لإنشاء مركز تنسيق وطني تابع للدائرة الحكومية لتوفير حماية خاصة لنظم المعلومات والاتصالات، يعنى بالتصدي للهجمات التي تهدد أمن المعلومات في نظم المعلومات والاتصالات السلكية واللاسلكية، واعتماد هذا المركز لدى منتدى الأفرقة المعنية بالأمن والتصدي للحوادث، مع الاستفادة في ذلك من الخبرة الدولية المتعلقة بضمان أمن موارد المعلومات. ولتحقيق هذا الغرض، انعقد في ١٧ آذار/مارس ٢٠٠٩، لقاء ضم ممثلين للإدارة الحكومية ومستشارا أقدم معنيا بمسائل أمن المعلومات من الهيئة الفنلندية للرقابة على الاتصالات.

٢٨ – وعلى الرغم من أن فريق الاستجابة للطوارئ الحاسوبية في أوكرانيا لم يكن معتمدا بعد لدى منتدى الأفرقة المعنية بالأمن والتصدي للحوادث، فقد تلقت أوكرانيا خلال الفترة ٢٠٠٦-٢٠٠٨، أكثر من ٢٠٠ إشعار من أفرقة الاستجابة للطوارئ الحاسوبية في فنلندا وأستراليا والنمسا وسلوفينيا ودول أخرى بشأن أنشطة غير مأذون بها على شبكة الإنترنت، قام بها مستخدمون أوكرانيون للشبكة. وتمخضت الإجراءات المتخذة في هذا الصدد عن توجيه أكثر من ٢٥٠ رسالة إلكترونية إلى عناوين الجهات المقدمة لخدمات الإنترنت بغرض

اتخاذ تدابير لتحديد مصادر البرامجيات والفيروسات المسببة للضرر. وعلاوة على ذلك، اتخذت في أيار/مايو ٢٠٠٧ تدابير لمنع وقوع هجمات موزعة من مصادر في أوكرانيا على خوادم في إستونيا، بغرض رفض تقديم الخدمة وفي تشرين الأول/أكتوبر ٢٠٠٧، تم صد هجوم من هذا النوع على الموقع الشبكي لرئيس أوكرانيا.

٢٩ - يضاف إلى ذلك أن أوكرانيا وضعت إطارا قانونيا وتنظيميا من أجل تيسير العمل المشترك للدائرة الحكومية لتوفير الحماية الخاصة لنظم المعلومات والاتصالات وهيئات إنفاذ القانون، بهدف تنفيذ تدابير تتعلق بضمان أمن موارد المعلومات الحكومية في نظم المعلومات والاتصالات السلكية واللاسلكية، وتعزيز فعالية نظام التصدي للأنشطة غير المأذون بها فيما يتصل بموارد المعلومات المذكورة.

٣٠ - وهكذا، فإن أوكرانيا قادرة اليوم على تنفيذ أنشطة لحماية المعلومات في جميع مراحل إنشاء نظم المعلومات والاتصالات السلكية واللاسلكية ووضع النظم الأمنية المتعددة العناصر التي تشتمل عليها نظم المعلومات والاتصالات السلكية واللاسلكية، بغض النظر عن نوع ودرجة حرجية المعلومات التي يجري تجهيزها وعن نوع نظام المعلومات والاتصالات السلكية واللاسلكية ودرجة تعقيده. ومن ثم، فإن جميع النهج الأساسية لتهيئة متطلبات الحماية لموارد المعلومات في نظم المعلومات والاتصالات السلكية واللاسلكية والتخطيط لهذه الحماية والإعداد لها وتقييمها، تتفق في عمومها مع النهج التي تتبعها الهيئات الحكومية المسؤولة عن الأمن في الدول الأعضاء في الأمم المتحدة والبلدان الأعضاء في الاتحاد الأوروبي.

٣١ - ولأغراض توفير الأنشطة التثقيفية المتعلقة بتأهيل الخبراء في مجال أمن المعلومات وهندسة الحاسوب، أسس معهد لحماية المعلومات تابع للجامعة الحكومية لتكنولوجيا المعلومات والاتصالات، ليعمل كمؤسسة تعليمية وعلمية متفرعة عن الجامعة.