الأمم المتحدة

A/64/129/Add.1

الجمعية العامة

Distr.: General
9 September 2009
Arabic
Original: French/Spanish

الدورة الرابعة والستون

البند ٩١ من جدول الأعمال المؤقت*

التطورات في ميدان المعلومات الاتصالات السلكية واللاسلكية في سياق الأمن الدولي

التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي

تقرير الأمين العام

إضافة**

المحتويات

الصفحة

* A/64/150 و Corr.1.

** وردت المعلومات المضمنة في هذه الوثيقة بعد تقديم التقرير الرئيسي.

250909 240909 09-50573 (A)

ثانيا – الردود الواردة من الحكومات

كوبا

[الأصل: بالإسبانية]
[٢ تموز/يوليه ٢٠٠٩]

الرد المتعلق بالقرار ٣٧/٦٣ المعنون "التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي"

١ – تشاطر كوبا جميع مظاهر القلق المعبر عنه في نص القرار ٣٧/٦٣ بخصوص استخدام تكنولوجيات ووسائل المعلومات في أغراض لا تتسق مع تحقيق الاستقرار والأمن الدوليين، وتؤثر سلبا على السلامة الإقليمية للدول، مما يضر بأمنها في الميدانين المدني والعسكري. إضافة إلى ذلك، يؤكد هذا القرار بالقدر الكافي على ضرورة منع استخدام موارد وتكنولوجيا المعلومات في أغراض إجرامية أو إرهابية.

٢ – وتؤكد كوبا مجددا أن الاستعمال العدائي للاتصالات السلكية واللاسلكية الذي يهدف، سرا أو علنا، إلى تقويض النظام القانوني والسياسي للدول، يمثل انتهاكا للقواعد الدولية المعترف بها في هذا المجال، ويشكل مظهرا سلبيا مجردا من روح المسؤولية في استعمال تلك الوسائل، قد تتمثل آثاره في إحداث توترات وحالات تضر بالسلام والأمن الدوليين، ومن ثم تقويض المبادئ والمقاصد المكرسة في ميثاق الأمم المتحدة.

٣ – وتنوه كوبا، مع القلق، إلى أن نظم المعلومات والاتصالات السلكية واللاسلكية يمكن أن تقوم مقام الأسلحة إذا ما صُممت و/أو استُخدمت بغرض إلحاق أضرار بالمرافق الأساسية لدولة ما، وهي بالتالي يمكن أن تشكل تهديدا للسلم والأمن الدوليين.

٤ – وفي هذا السياق، تكرر جمهورية كوبا إدانتها التي سبق أن أعربت عنها في مختلف المحافل الدولية لما تقوم به الإدارات المتعاقبة في الولايات المتحدة الأمريكية من تصعيد عدواني في حربها الإذاعية والتلفزيونية ضد كوبا، مما يشكل انتهاكا سافرا للمعايير الدولية السارية في مجال تنظيم المجال اللاسلكي.

٥ – ولا تعير حكومات الولايات المتحدة الأمريكية اهتماما للضرر الذي يمكن أن يلحق بالسلم والأمن الدوليين جراء التسبب في حالات خطيرة من قبيل استخدام طائرة عسكرية لبث إشارات تلفزيونية باتجاه كوبا دون موافقتها. وهذا تصرف لا يليق بعضو دائم في مجلس الأمن للأمم المتحدة.

٦ - ويشكل العدوان اللاسلكي الموجه من إقليم الولايات المتحدة الأمريكية ضد كوبا انتهاكا لمبادئ القانون الدولي التي تنظم العلاقات بين الدول ولقواعد الاتحاد الدولي للاتصالات وأنظمته التي تحدد قواعد السلوك للبلدان الأعضاء في هذه الوكالة المتخصصة التابعة لمنظومة الأمم المتحدة.

٧ - وفي أواخر شهر أيار/مايو ٢٠٠٩، تلقت كوبا ما مجموعه **٩٢٤ ١ ساعة من البث الأسبوعي غير القانوني الموجه ضد كوبا انطلاقا من الولايات المتحدة باستخدام ٣٠ من التـرددات اللاسـلكية**. والعديد من مصادر الإرسال اللاسلكي تلك مملوكة أو موالية لمنظمات مرتبطة بعناصر إرهابية معروفة تقيم على أراضي الولايات المتحدة الأمريكية وتعمل ضد كوبا من هناك، حيث تبث برامج تحرض على التخريب والهجمات السياسية والاغتيالات وغير ذلك من المواضيع التي يتناولها الإرهاب الإذاعي.

٨ - وتشكل هذه البرامج الاستفزازية ضد كوبا انتهاكات للمبادئ الدولية التالية:

- المبادئ الأساسية للاتحاد الدولي للاتصالات الواردة في ديباجة دستوره والمتعلقة بالأهمية المتزايدة التي تكتسيها الاتصالات السلكية واللاسلكية من أجل صون السلام وتحقيق التنمية الاقتصادية والاجتماعية لجميع الدول بهدف تيسير العلاقات السلمية والتعاون الدولي بين الشعوب وبلوغ التنمية الاقتصادية والاجتماعية من خلال حسن تشغيل الاتصالات السلكية واللاسلكية. ويتسم محتوى البرامج التلفزيونية التي تبثها حكومة الولايات المتحدة ضد كوبا بطابع تخريبي يهدف إلى زعزعة الاستقرار والتضليل ويتعارض مع المبادئ المذكورة.

- الحكمان CS 197 و CS 198 من دستور الاتحاد الدولي للاتصالات، اللذان ينصان على ضرورة إنشاء وتشغيل جميع المحطات، كيفما كانت أهدافها، على نحو لا يحدث تشويشا يضر بالاتصالات أو الخدمات اللاسلكية التابعة لدول أعضاء أخرى.

- الاتفاق الصادر عن الجلسة العامة التاسعة للمؤتمر العالمي للاتصالات اللاسلكية المعقودة في تشرين الثاني/نوفمبر ٢٠٠٧، والذي ينص في فقرته الفرعية 'ز' من الفقرة ٦-١ على أنه ''لا يمكن اعتبار قيام محطة إذاعية تعمل على متن طائرة وتبث موجاتها باتجاه إقليم إدارة أخرى دون موافقتها عملا يتماشى مع أنظمة الاتصالات اللاسلكية''.

- الفقرة الفرعية ٣ من المادة ٨ من أنظمة الاتصالات اللاسلكية للاتحاد، التي تنص على وجوب قيام الإدارات الأخرى بمراعاة الترددات المخصصة والمسجلة التي تحظى باعتراف دولي لدى قيامها بتخصيص تردداتها من أجل تلافي إلحاق تشويش ضار.

- الفقرة الفرعية ٤ من المادة ٤٢ من أنظمة الاتصالات اللاسلكية للاتحاد، التي تحظر على المحطات المنشأة على متن طائرات تعمل في البحر أو فوق البحر توفير أي خدمات للبث الإذاعي.

- قرار مجلس أنظمة الاتصالات اللاسلكية الذي أقر في اجتماعه الخامس والثلاثين المعقود في كانون الأول/ديسمبر ٢٠٠٤ بوقوع تشويش ضار للخدمات الكوبية من جراء البث عند تردد ٢١٣ ميغاهيرتز، وطالب إدارة الولايات المتحدة الأمريكية باتخاذ التدابير المناسبة لوقفه. علاوة على ذلك، دأب مجلس أنظمة الاتصالات اللاسلكية منذ أيلول/سبتمبر ٢٠٠٦ على مطالبة إدارة الولايات المتحدة الأمريكية باتخاذ تدابير ترمي إلى إزالة التشويش على موجة التردد ٥٠٩ ميغاهيرتز دون أن يتلقى أي رد حتى الآن. وفي ٢٠ آذار/مارس ٢٠٠٩، اختتم المجلس اجتماعه الخمسين وأكد مجددا في موجز قراراته (الوثيقة RRBO9-1/5) عدم مشروعية البث وطالب إدارة الولايات المتحدة الأمريكية باتخاذ التدابير اللازمة من أجل وضع حد لحالات التشويش على الخدمات التلفزيونية لكوبا.

- الفقرة الفرعية ٣ من المادة ٢٣ من أنظمة الاتصالات اللاسلكية للاتحاد، التي تقيّد الإرسال التلفزيوني خارج الحدود الوطنية. ويعترف تقرير لمكتب المراجعة الداخلية لحكومة الولايات المتحدة الأمريكية (وهي هيئة رسمية في الولايات المتحدة) صادر في كانون الثاني/يناير ٢٠٠٩ بأن برنامج الإرسال الإذاعي والتلفزيوني لحكومة الولايات المتحدة الأمريكية الموجه ضد كوبا ينطوي على انتهاكات للأحكام الدولية وللقانون المحلي.

٩ - وتشير كوبا كذلك إلى أن المؤتمر العالمي للاتصالات اللاسلكية الذي انعقد في جنيف، سويسرا، في الفترة من ٢٢ تشرين الأول/أكتوبر إلى ١٦ تشرين الثاني/نوفمبر ٢٠٠٧ قد أقر نص الاستنتاجات الذي يصف عمليات البث الموجهة من طائرات في الولايات المتحدة باتجاه كوبا بأنها مخالفة لأنظمة الاتصالات اللاسلكية. وجاء في نص الاستنتاجات المعتمدة في الجلسة العامة بأنه ''لا يمكن اعتبار قيام محطة إذاعية تعمل على متن طائرة بالبث حصرا باتجاه إقليم إدارة أخرى دون موافقتها عملا متماشيا مع أنظمة الاتصالات اللاسلكية''. وقد تم الاتفاق على هذه الاستنتاجات في الجلسة العامة للمؤتمر

وتكتسي قوة قانونية فيما يتعلق بعمل الاتحاد. وبذلك يكون المؤتمر العالمي للاتصالات اللاسلكية قد أيد الإعلان الصادر في عام ١٩٩٠ عن المجلس الدولي لتسجيل الترددات، الذي كان قائما آنذاك، والذي ينص على أن توجيه البث التلفزيوني من على متن منطاد مبرمج من بعد باتجاه الإقليم الوطني الكوبي يشكل انتهاكا للأنظمة.

١٠ - ويتجلى العداء الذي تناصبه حكومة الولايات المتحدة الأمريكية لكوبا في الحصار الاقتصادي والتجاري والمالي الذي تفرضه عليها منذ قرابة ٥٠ عاما، والذي يؤثر أيضا على مجال المعلومات والاتصالات السلكية واللاسلكية، وهو ما يتضح من الأمثلة التالية التي سيقت من بين حالات أخرى عديدة:

- لا يحق لكوبا الاستفادة من الخدمات التي يعرضها عدد كبير من المواقع على شبكة الإنترنت، بحيث ينطبق المنع بمجرد ما يتبين أن الاتصال يجري من عنوان لبروتوكول إنترنت مخصص لنطاق كوبي (*cu*.).

- ودون إشعار سابق، قام مكتب مراقبة الممتلكات الأجنبية في الآونة الأخيرة بحظر أسماء النطاقات *com*. المرتبطة بكوبا.

- الإعلان العام الصادر في أيار/مايو ٢٠٠٩ عن اتحاد تكنولوجيا مايكروسوفت والقاضي بحجب خدمة المحادثة التي يتيحها برنامج ''ويندوز لايف مسنجر آي إم'' عن كوبا وبلدان أخرى ''امتثالا لالتزامها بالخضوع لقوانين الولايات المتحدة الأمريكية''. ولدى محاولة ربط الاتصال بهذا الموقع، تظهر رسالة محتواها: ''لقد قطعت مايكروسوفت خدمات ويندوز لايف مسنجر على المستخدمين في البلدان المشمولة بحظر من الولايات المتحدة، ولذا فقد توقفت مايكروسوفت عن تقديم خدمات ويندوز لايف لبلدك''.

- وثمة صفحات أخرى على الإنترنت يُمنع الدخول إليها من نطاق الأسماء المخصص لكوبا (.cu): نظم سيسكو سيستمز (http://tools.cisco.com/RPF/register.do) لتكنولوجيات الاتصال، وموجهات خوادم الوصول إلى الإنترنت، بما في ذلك معدات الفيديو الرقمي؛ وسوليد وركس (http://www.solidworks.com/sw/termsofuse.html) لنظم التصميم الآلية وسيمانتيك (http://www.symantec.com/about/profile/policies/legal) للبرامجيات الحاسوبية المخصصة للحماية من الفيروسات.

- ومن قبيل السخرية والنفاق التام أن تتهم الولايات المتحدة كوبا بأكذوبة إعاقة وصول مواطنيها إلى الشبكة العالمية في حين أن الحقيقة الواضحة هي أن كوبا

لا تستطيع، بسبب قوانين الحظر التي تفرضها عليها الولايات المتحدة، إقامة الربط بكابلات الألياف الضوئية التي تحيط بشبه الجزيرة الكوبية، مما يضطرها لتكبد التكاليف الباهظة التي تتطلبها الخدمات الساتلية.

- وقد تكبدت الشركة الكوبية ETECSA للاتصالات خسائر تناهز ٧٦٩,٨ ٥٣ من دولارات الولايات المتحدة حتى كانون الأول/ديسمبر ٢٠٠٨. وتعزى هذه الخسائر أساسا إلى تعذر وصولها إلى سوق الولايات المتحدة الأمريكية لشراء المعدات المتخصصة. وبالتالي، فإنها تضطر إلى الاستعانة بوسطاء، مما يرفع إلى أقصى حد تكاليف المنتجات اللازمة لضمان خدماتها.

١١ - إن هذا الموقف الذي تتخذه الولايات المتحدة الأمريكية يقوض الإرادة والنتائج والروح التي سادت بين دول العالم بأسره عندما اجتمعت في سويسرا وتونس أثناء انعقاد مؤتمر القمة العالمي المعني بمجتمع المعلومات. وقد حث هذا المؤتمر الدولَ بقوة، في سعيها إلى بناء مجتمع المعلومات، على اتخاذ خطوات لمنع وتحاشي أية تدابير انفرادية لا تتفق مع القانون الدولي وميثاق الأمم المتحدة ويمكن أن تعرقل التحقيق الكامل للتنمية الاقتصادية والاجتماعية للسكان في البلدان المعنية أو تعوق رفاههم.

١٢ - وشكلت الدورة الثانية عشرة للجنة المعنية بتسخير العلم والتكنولوجيا من أجل التنمية المعقودة في جنيف في الفترة من ٢٥ إلى ٢٩ أيار/مايو ٢٠٠٩، من خلال تحليلها للتقدم المحرز في تنفيذ ومتابعة نتائج مؤتمر القمة العالمي المعني بمجتمع المعلومات، إطارا هاما لتكرار إدانة كوبا لسياسة الحصار التي تفرضها حكومة الولايات المتحدة الأمريكية، ولا سيما تطبيق التدابير القسرية الانفرادية بشأن تطوير تكنولوجيا الاتصالات والوصول إلى المعلومات، فضلا عن تنفيذ سياسة عدائية ضد المجال اللاسلكي لكوبا، مما يتعارض مع الأحكام المعتمدة في مرحلتي مؤتمر القمة المذكور.

١٣ - وتكتسي المناقشة التي تجري في الجمعية العامة للأمم المتحدة بشأن أوجه التقدم في ميدان تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي أهمية بالغة تزداد كل يوم. وتعرّض كوبا لأعمال من قبيل تلك المبينة سابقا والصادرة عن الولايات المتحدة الأمريكية يؤكد ضرورة إجراء هذا النقاش والحاجة الملحة إلى اتخاذ تدابير لوضع حد لمثل هذه التصرفات التي تندرج ضمن مظاهر إرهاب الدولة.

١٤ - وتؤيد كوبا بحزم العملية الجارية في الجمعية العامة للأمم المتحدة. ولذلك، فقد انضمت إلى الدول الأعضاء التي صوتت لصالح القرار ٣٧/٦٣ وعددها ١٧٨ دولة في تعارض مع موقف الولايات المتحدة الأمريكية، البلد الوحيد الذي صوت ضده.

١٥ - وستواصل كوبا بذل قصارى جهودها للإسهام في التطوير السلمي لتكنولوجيا المعلومات والاتصالات في العالم واستخدامها لما فيه خير البشرية جمعاء، وهي على استعداد للتعاون مع باقي البلدان، بما فيها الولايات المتحدة الأمريكية، لإيجاد الحلول الكفيلة بتذليل العقبات التي تحول دون تحقيق هذين الهدفين.

مالي

[الأصل: بالفرنسية]
[٩ تموز/يوليه ٢٠٠٩]

آراء وملاحظات بشأن تنفيذ القرار المتعلق بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي

التقييم العام لمسائل أمن المعلومات

١ - إن حجب الخدمة بهدف وقف عمل نظام حاسوبي ما، واختراق الحواسيب من أجل الاستيلاء على المعلومات هي أبرز أشكال الهجوم على نظم المعلومات.

٢ - والأخطار التي تهدد النظم الحساسة للمؤسسات الحكومية أو الشركات هي أخطار أو حوادث تطال سلامة البنية التحتية الحيوية للمعلومات أو سريتها أو توافرها.

٣ - ونذكر من هذه الأخطار ما يلي:

- التهديدات التي تدبرها حكومة أجنبية أو جماعة إرهابية أو جهات متطرفة تعمل بدافع سياسي
- التهديدات المنفذة لأغراض التجسس أو التخريب أو التدخل الأجنبي أو العنف السياسي (الإرهاب)

٤ - وبات استخدام تكنولوجيا المعلومات بديلا عن اللجوء إلى أساليب تقليدية، مثل التدمير أو التشويش بالإشعاع الكهرمغنطيسي أو التسلل الفعلي أو التحكم في مصادر داخلية للمعلومات.

٥ - ويمكن للهجمات الإلكترونية أن تستهدف الأفراد، كما يمكنها أن تستهدف الشركات أو المؤسسات العامة. وفيما يتعلق بالهجمات التي تهدد الدفاع أو الأمن الوطني، فإن دوائر الدولة والجهات الفاعلة الحيوية والشركات العاملة في مجالات استراتيجية أو حساسة تُستهدف بشكل خاص. إلا أن هذه الهجمات لا تترتب عليها نفس العواقب،

وذلك حسبما إذا كانت تستهدف مواقع أو خدمات متاحة للعموم، أو نظما تشغيلية، أو بشكل مباشر أكثر أشخاصا لديهم معلومات حساسة.

٦ - وتنطوي مهمة التعرف على مصدر هجمة إلكترونية ما على صعوبة خاصة. فالأساليب المتبعة تتضمن في معظم الأحيان استخدام مجموعة من الحواسيب التي قد توجد طائفة من البلدان. ويتطلب تعقب سلسلة الأجهزة المستخدمة في مثل هذه العمليات إجراء تحقيقات طويلة للغاية، تتوقف على احتمالات التعاون القضائي الدولي. وطرائق التضليل متعددة، ومنها الاستيلاء على حواسيب دون علم أصحابها واللجوء إلى استخدام حواسيب عامة أو مجهولة، مثل تلك الموجودة في مقاهي الإنترنت.

٧ - ومع ذلك، ترى معظم الدوائر الحكومية والمراقبين أن وراء هذه الهجمات جماعات القرصنة الإلكترونية التي تستخدم على ما يبدو أساليب أكثر فأكثر تطورا.

الجهود المبذولة على الصعيد الوطني لتعزيز أمن المعلومات وأنشطة التعاون الدولي في هذا الميدان

(أ) على الصعيد الوطني

٨ - ليس لدى مالي، في الوقت الراهن، قوانين سارية في مجال أمن المعلومات.

٩ - ويشكّل وضع إطار قانوني وتنظيمي أحد المحاور ذات الأولوية في الخطة الاستراتيجية الوطنية لتكنولوجيا المعلومات والاتصالات التي اعتمدتها الحكومة في حزيران/يونيه ٢٠٠٥.

١٠ - وحصلت مالي على قرض (رقم 4033 MLI) من المؤسسة الإنمائية الدولية لتمويل مشروع دعم النمو، وتعتزم استخدام جزء من هذا القرض لإجراء دراسة استشارية بشأن المساعدة التقنية اللازمة لإعداد إطار قانوني وتنظيمي يتعلق بتكنولوجيا المعلومات والاتصالات في مالي.

١١ - أفضت عملية اختيار الاستشاريين، من جانب الجهات المقترضة من البنك الدولي إلى إصدار طلب الإعراب عن الاهتمام رقم 001/2009/SPM/UCP-PAC وفقا للإطار المرجعي الذي أعدته وكالة تكنولوجيا المعلومات والاتصالات في أيار/مايو ٢٠٠٨.

١٢ - وفي هذا الإطار القانوني والتنظيمي، من المقرر وضع نصوص تشريعية بشأن الحريات، والأعمال، والتجارة الإلكترونية، والملكية الفكرية، وأمن البيانات وسريتها، والجرائم والجنح المرتكبة في الفضاء الإلكتروني، وحرية الاطلاع على المعلومات العامة وتلك التي تشكل تراثا إنسانيا.

(ب) أنشطة التعاون الدولي الرامية إلى تعزيز أمن المعلومات

١٣ - تتعدى الهجمات الإلكترونية الحدود الجغرافية، ويمكن أن تُوجه بطريقة متزامنة ضد العديد من الدول. وتستدعي مراقبة الشبكات ووضع إجراءات التصدي لهذه الهجمات في حال حدوثها وجود علاقات التعاون والمساعدة على الصعيد الدولي. وبصفة أعم، فإن حماية نظم المعلومات من الأنشطة غير القانونية تشكّل اليوم أحد الشواغل المشتركة بين العديد من الدول.

١٤ - وقد اختارت مالي، من جهة أخرى، نهجا إقليميا فيما يتصل بتطوير الأنظمة المتعلقة بقطاع الاتصالات السلكية واللاسلكية، وهو ما أفضى إلى التصديق على التوجيهات الصادرة عن الاتحاد الاقتصادي والنقدي لغرب أفريقيا عام ٢٠٠٦ والصكوك الإضافية الصادرة عن الجماعة الاقتصادية لدول غرب أفريقيا عام ٢٠٠٧.

١٥ - ويعمل الاتحاد الدولي للاتصالات على وضع إطار دولي لتعزيز الأمن الحاسوبي (برنامج الأمن الحاسوبي العالمي)، وهو محط اهتمام خاص لدولة مالي. وأفضى تعزيز الأمن الحاسوبي إلى إنشاء فريق خبراء رفيع المستوى مكلف باقتراح استراتيجية بعيدة المدى تشمل التدابير القانونية، والتدابير التقنية اللازمة لتجاوز أوجه القصور في البرامجيات، بالإضافة إلى منع الهجمات الإلكترونية وكشفها، وإدارة الأزمات.

مضمون المبادئ الدولية الكفيلة بتعزيز أمن نظم المعلومات والاتصالات السلكية واللاسلكية

١٦ - ينبغي أن يستند أمن المعلومات على الصعيد الدولي إلى القانون الدولي الساري (قانون مسوغات الحرب)، الذي يحدد كيفية التصدي للأخطار التي تهدد السلام والأمن الدوليين، وإلى القانون الدولي الإنساني (قانون الحرب) المتعلق بأساليب ووسائل الحرب، وحماية الدول التي ليست أطرافا في النزاع، وكذلك فئات الأشخاص والممتلكات التي تضررت أو قد تتضرر من النزاع.

١٧ - ويمثل ميثاق الأمم المتحدة حجر الزاوية في القانون الدولي المتعلق بحفظ السلام والأمن الدوليين.

١٨ - ويُجمع أخصائيو القانون الدولي على أن هذه القواعد تنشئ آلية أمنية عالمية للحفاظ على السلام والأمن الدوليين. وفي حين أصبحت تكنولوجيا المعلومات والاتصالات تُصمّم أو تُستخدم كوسائل للتدمير (أو ما يعرف بـ ''أسلحة المعلومات'') ولم يتفق المجتمع الدولي بعد على مكانة أمن المعلومات في القانون الدولي الساري، فإن ميثاق الأمم المتحدة يمكن أن

يفسر بطريقة تتيح للفاعلين الدوليين هامشا كبيرا من الحرية لاستخدام تكنولوجيا المعلومات والاتصالات للقيام بأعمال عدوانية وتسوية النزاعات والخلافات الدولية.

١٩ - ونشأت هذه الحالة الغريبة لأن القانون الدولي لا يتناول بعد صراحة الأعمال العدائية في مجال المعلومات بنفس مستوى تناوله للأعمال العدائية التي تُستخدم فيها الأسلحة التقليدية، مع أن ترابط عالم اليوم واعتماده على تكنولوجيا المعلومات والاتصالات يعني أن هجمة من هذا النوع قد تكون لها آثار مدمرة ترقى إلى مستوى آثار الهجمة التقليدية، بل وربما تتعداها. ومما يزيد من حدة الصعوبات عدم وجود تفسيرات مقبولة على نطاق واسع بشأن مفاهيم من قبيل ''العمل العدواني'' (المادة ١)، و''القوة'' (المادة ٢، الفقرة ٤)، و''الاعتداء المسلح'' (المادة ٥١) فيما يتعلق بأمن المعلومات.

٢٠ - ويحدد قرار الجمعية العامة ٣٣١٤ (د-٢٩)، المؤرخ ١٤ كانون الأول / ديسمبر ١٩٧٤، مفهوم العمل العدواني.

٢١ - ورغم أن هذا القرار لم يُتخذ بتوافق الآراء، فإن أحكامه الإرشادية تتيح لمجلس الأمن ولجميع أعضاء المجتمع الدولي معايير لتحديد ما إذا كان العمل عدوانيا أم لا.

٢٢ - ويمكن تفسير استخدام سلاح من أسلحة المعلومات على أنه عمل عدواني إذا كان هناك ما يجعل الدولة الضحية تعتقد أن الهجوم قد تم على يد القوات المسلحة لدولة أخرى وكان الهدف منه تعطيل عمل المنشآت العسكرية، أو تدمير القدرات الدفاعية أو الاقتصادية، أو انتهاك سيادة الدولة على إقليم معين.

التدابير التي يمكن أن يتخذها المجتمع الدولي لتعزيز أمن المعلومات على الصعيد العالمي

٢٣ - سعيا إلى تعزيز أمن المعلومات على الصعيد العالمي والتصدي لخطر استخدام تكنولوجيا المعلومات والاتصالات لأغراض عدائية، ينبغي للمجتمع الدولي أن يعزز إجراءاته في مجالات محددة، منها ما يلي:

(أ) مؤازرة الدول في توعية مختلف الجهات الفاعلة (الإدارات والشركات والمستخدِمون) وتحسيسها بالمسؤولية بشأن أمن نظم المعلومات؛

وفي هذا السياق، ينبغي إيلاء اهتمام كبير لتنسيق السياسات بين الدول في مجال الدعم المقدم للقاعدة الصناعية والتكنولوجية فيما يتعلق بالمنتجات المؤمنة. وينبغي أيضا إعطاء مكان الصدارة للتعاون بين الدول والقطاع الخاص.

(ب) تعزيز قدرات الدول بأن توضع رهن إشارتها الموارد البشرية والخبرات التقنية اللازمة لمراقبة التدفقات غير العادية التي تتم عبرها الهجمات الإلكترونية، ومن ثم كشفها؛

(ج) إعادة تنظيم سياسات مختلف المؤسسات الدولية العاملة في مجال أمن نظم المعلومات بإسناد اختصاصات لكل منها؛

(د) وضع مؤشرات في مجال أمن المعلومات لمساعدة البلدان على تحسين إدارة البنى التحتية لتكنولوجيا المعلومات والاتصالات. ومن الجوانب التي يمكن أن تشملها هذه المؤشرات ما يلي:

- استرجاع البيانات في حال وقوع كارثة
- استخدام المعايير (القواعد)
- مراقبة الأداء (تحديد نقاط مرجعية)
- التحويل الإلكتروني
- التعاون مع الإنتربول
- منصة الدخول.

خاتمة

٢٤ — في ختام ملاحظاتنا، يبدو أن المسائل المتصلة بأمن المعلومات واستخدام تكنولوجيا المعلومات والاتصالات لأغراض عدوانية أصبحت تدعو للقلق بشكل متزايد. ومن المؤكد أن هذه التكنولوجيا لها مزايا لا تعد ولا تحصى، لكن يمكنها أن تسبب كوارث من الصعب التنبؤ بعواقبها، وذلك بالنظر إلى تطورها المتسارع.

٢٥ - وتظل الأسئلة القانونية التي يثيرها تطور هذه التكنولوجيا دون أجوبة شافية بسبب وجود قواعد تنظيمية مختلفة وغير ملائمة في كثير من الأحيان.

٢٦ - وبالتالي، فإن الدول هي المسؤولة عن وضع هذه الأدوات بصورة متسقة لضمان الارتقاء بصورة أفضل نحو مجتمع معلومات أكثر أمانا.

إسبانيا

[الأصل: بالإسبانية]
[٨ تموز/يوليه ٢٠٠٩]

موقف إسبانيا بشأن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي

مقدمة

١ - يشكل أمن المعلومات جانبا رئيسيا من جوانب مجتمع المعلومات. وقد أتاحت التطورات التكنولوجية تحقيق زيادة متواصلة ومتسارعة في القدرات المتعلقة بتجهيز وتخزين المعلومات في أشكال متعددة؛ ومن جهة أخرى، شهد مجال الاتصالات زيادة كبيرة جدا في عرض النطاق المتاح، مما يعني إمكانية إرسال وتلقي كميات ضخمة من المعلومات بشكل آني تقريبا ودون الحاجة إلى بنى تحتية على درجة خاصة من التعقيد.

٢ - وفي حين تساهم هذه التطورات التكنولوجية في تحسين فرص الوصول إلى المعلومات بمختلف أنواعها، فإنها تسهل أيضا إمكانية استخدام تلك المعلومات أو الوصول إليها لأغراض غير قانونية، ولا سيما استخدام نظم المعلومات والاتصالات السلكية واللاسلكية لأغراض عدائية أو إجرامية، بل ولارتكاب أعمال إرهابية أو عدوانية بين الدول أو الجهات الفاعلة عبر الحدود الوطنية.

٣ - وقد تأكد في السنة الماضية تنامي الاتجاه نحو استخدام الإنترنت من جانب المنظمات الإجرامية، وبوجه خاص الجماعات الإرهابية التي تستغل أساسا اثنين من خصائص الشبكة وهما طابعها العالمي وما تتيحه من ضمانات كبيرة بشأن سرية الهوية.

٤ - ونتيجة لذلك، لا بد من تحقيق توازن بين تطور المجتمع وتكنولوجيا المعلومات من جهة، والعمل من جهة أخرى، وبموازاة مع ذلك، على تطوير قوانين وطنية ودولية مستكملة ومحدثة تواكب البيئة التكنولوجية الجديدة وتكفل التصدي للتحديات التي تطرحها ضرورة حماية المعلومات من أجل منع استخدامها بصورة غير مشروعة دون المساس بحقوق وحريات الأشخاص.

إساءة استعمال الإنترنت لأغراض إرهابية

٥ - تتمثل التهديدات الرئيسية الناجمة عن استخدام المنظمات الإرهابية لشبكة الإنترنت فيما يلي:

(أ) استخدام الإنترنت كسلاح، بمعنى استخدام الإنترنت بوصفه وسيلة لشن هجمات ضد نظم المعلومات المتعلقة بالبنى التحتية الحيوية أو ضد البنى التحتية للإنترنت نفسها. وتعتبر مثل هذه الهجمات متواترة نسبيا في مجال جرائم القانون العام، بيد أن الهجوم الذي تعرضت له إستونيا في عام ٢٠٠٧ كشف أن البنية التحتية المعلوماتية لدولة ما يمكن أن تتأثر أيضا بهجوم من هذا النوع. ومن العوامل المرتبطة مباشرة بهذا النوع من التهديد هناك الزيادة الكبيرة في عدد البرامجيات الحاسوبية الجديدة الضارة التي ظهرت في السنتين الأخيرتين وشبكات البناء والتشغيل والنقل (botnets) أو شبكات الحواسيب الشريرة (zombies) التي تستخدم لشن هجمات ضد نظم المعلومات.

(ب) استخدام الإنترنت باعتباره وسيلة لتنظيم أنشطة أخرى ولا سيما منها ما يلي:

- أنشطة الاتصال. لقد أصبح استخدام الشبكة يحل محل الاتصالات التي كانت تجريها المنظمات الإجرامية عبر وسائل أخرى من قبيل الهواتف الثابتة أو المحمولة. وتتمثل أكثر الأدوات استخداما لإجراء الاتصالات عن طريق الإنترنت في البريد الإلكتروني وبرامج تبادل الرسائل الآنية ومحافل الدردشة.
- بث الدعاية ومواد تتعلق بأنشطة إرهابية. توجد في الوقت الراهن آلاف المواقع الشبكية التي ترتبط بأنشطة إرهابية أو تحرض على العنف، وهو اتجاه ما فتئ يتزايد جراء نشوء ظاهرة المدونات. أما طريقة منع المنظمات الإرهابية من استخدام الشبكة العالمية لهذه الأغراض، فهي مسألة على قدر كبير من التعقيد نظرا لسهولة ترحيل هذه المواقع. ويتعلق الأمر بظاهرة تتجاوز حدود الدول، ذلك أن البلدان التي توجد فيها الخوادم التي تستضيف الصفحة وتتم منها إدارتها قد تكون متعددة ومغايرة للبلد الذي تعمل فيه المنظمة الإرهابية المعنية.
- أنشطة التجنيد. يستخدم الإنترنت في بعض الأحيان كوسيلة لتنظيم أنشطة التعبئة، ولا سيما من خلال المحافل وبرامج تبادل الرسائل الآنية.
- التمويل. يتيح الإنترنت أيضا فرصا تضطلع المنظمات الإرهابية من خلالها بأنشطة ترمي إلى الحصول على التمويل. ومن المثير للاهتمام بشكل خاص قدرة المنظمات الإرهابية على المشاركة في ارتكاب عمليات احتيال عبر الإنترنت كوسيلة للحصول على التمويل.
- نشر أدلة التدريب. تستخدم المنظمات الإرهابية شبكة الإنترنت لنشر أدلة تتناول تقنيات إرهابية وطرائق صنع المتفجرات أو مناولة الأسلحة.

- جمع المعلومات بغرض شن هجمات إرهابية. يشكل الإنترنت مصدرا لمعلومات بالغة الأهمية كثيرا ما تستخدمها المنظمات الإرهابية للحصول على بيانات بشأن أهداف أنشطتها.

التدابير المتخذة على الصعيد الوطني من أجل مكافحة استخدام المنظمات الإرهابية للإنترنت

التدابير التشريعية

٦ - من جملة التدابير التي تتخذها مختلف الدول، بذلت إسبانيا جهدا كبيرا في السنوات الأخيرة، وبخاصة في عام ٢٠٠٧، لكي تدرج في نظامها القانوني مجموعة من القوانين التي تتناول أمن المعلومات وحرية ممارسة الحقوق والحريات المعترف بها في الإعلان العالمي لحقوق الإنسان وفي الدستور الإسباني. وجرى وضع مجموعة واسعة من التشريعات والأنظمة مع تضمينها الجوانب الوطنية البحتة والتوجيهات الواردة من الاتحاد الأوروبي بهدف تحقيق هذين الهدفين، وتطبيق معايير جديدة لأمن المعلومات تنص على أن توفير درجة معقولة من الحماية للمعلومات، فضلا عن الحفاظ على سريتها، أصبح يقتضي في معظم الحالات الحفاظ على سلامتها وتوافرها. وتجدر الإشارة بوجه خاص إلى القوانين التالية (الواردة حسب الترتيب الزمني):

- القانون الأساسي ١٩٩٢/٥ المؤرخ ٢٩ تشرين الأول/أكتوبر بشأن تنظيم التجهيز الآلي للبيانات الشخصية، الرامي إلى وضع آليات للحماية تحول دون انتهاك الخصوصية في سياق تجهيز المعلومات، وأنظمته التنفيذية.
- القانون الأساسي ١٩٩٩/١٥ المؤرخ ١٣ كانون الأول/ديسمبر بشأن حماية البيانات الشخصية، الذي يهدف إلى ضمان وحماية الحريات العامة والحقوق الأساسية للأشخاص الطبيعيين، فيما يتعلق بتجهيز بياناتهم الشخصية، وبخاصة شرفهم وخصوصياتهم الشخصية والأسرية، وأنظمته التنفيذية.
- المرسوم الملكي بقانون ١٩٩٩/١٤ المؤرخ ١٧ أيلول/سبتمبر بشأن التوقيع الإلكتروني، والصادر بهدف تشجيع الإدماج السريع للتكنولوجيا الجديدة في مجال أمن الاتصالات الإلكترونية في نشاط الشركات والمواطنين والإدارات العامة حيث أدمج في النظام العام الإسباني التوجيه الإطاري المتعلق بالتوقيع الإلكتروني رقم 1999/93/CE الصادر عن البرلمان الأوروبي والمجلس الأوروبي في ١٣ كانون الأول/ديسمبر ١٩٩٩. ويستكمل القانون ٢٠٠٣/٥٩ المؤرخ ١٩ كانون

الأول/ديسمبر بشأن التوقيع الإلكتروني هذا التوجيه الإطاري من خلال إدخال تعديلات تستند إلى التجربة المتراكمة منذ دخوله حيز النفاذ.

- القانون ٢٠٠٢/١١ المؤرخ ٦ أيار/مايو الذي ينظم المركز الوطني للاستخبارات، ثم المرسوم الملكي ٢٠٠٤/٤٢١ المؤرخ ١٢ آذار/مارس الذي ينظم المركز الوطني للتشفير، حيث ينيطان بالمركز الوطني للاستخبارات مهاما من بينها تنسيق الإجراءات التي تتخذها مختلف الهيئات الإدارية التي تستخدم وسائل وإجراءات الشفرة، وضمان أمن تكنولوجيا المعلومات في هذا المجال وكفالة الامتثال للقوانين المتعلقة بحماية المعلومات السرية.

- القانون ٢٠٠٢/٣٤ المؤرخ ١١ تموز/يوليه بشأن خدمات مجتمع المعلومات والتجارة الإلكترونية. ويهدف إلى تضمين النظام القانوني الإسباني التوجيه رقم 2000/31/CE المؤرخ ٨ حزيران/يونيه المتعلق بجوانب معينة من خدمات مجتمع المعلومات، وبخاصة التجارة الإلكترونية في السوق الداخلية (توجيه بشأن التجارة الإلكترونية). ويتضمن هذا القانون أيضا جزءا من التوجيه رقم 98/27/CE الصادر عن البرلمان الأوروبي والمجلس الأوروبي في ١٩ أيار/مايو بشأن دعاوى الإيقاف في مجال حماية مصالح المستهلكين حيث تنظم أحكامه إجراءات دعوى الإيقاف ضد الأعمال التي تنتهك أحكام هذا القانون.

- القانون ٢٠٠٣/٣٢ المؤرخ ١٣ تشرين الأول/نوفمبر بشأن الأحكام العامة للاتصالات السلكية واللاسلكية، الذي ينظم سبل استخدام الشبكات وتقديم خدمات الاتصالات الإلكترونية.

- القانون ٢٠٠٣/٥٩ المؤرخ ١٩ كانون الأول/ديسمبر بشأن التوقيع الإلكتروني المشار إليه أعلاه.

- القانون ٢٠٠٧/١١ المؤرخ ٢٢ حزيران/يونيه بشأن وصول المواطنين إلى الخدمات الإلكترونية العامة، الذي ينظم الاتصال من خلال استخدام وتطبيق التقنيات والوسائل الإلكترونية والمعلوماتية واللاسلكية المتوافرة بين المواطنين والإدارات العامة.

- القانون الأساسي ٢٠٠٧/١٠ المؤرخ ٨ تشرين الأول/أكتوبر الذي ينظم قاعدة بيانات الشرطة المتعلقة بمحددات الهوية المستخلصة من الحمض النووي الريبي المتزوع الأوكسجين، الذي ينشئ قاعدة بيانات تدمج فيها، بشكل منفرد، ملفات الوكالات الحكومية لإنفاذ القانون التي تتضمن بيانات تحديد الهوية المستمدة من

تحليلات الحمض النووي الريبي المتروع الأوكسجين التي أجريت في إطار تحقيق جنائي أو في سياق إجراءات تحديد هوية الجثث أو التحقق من الأشخاص المختفين.

- القانون ٢٠٠٧/٢٥ المؤرخ ١٨ تشرين الأول/أكتوبر بشأن حفظ البيانات المتعلقة بالاتصالات الإلكترونية والشبكات العامة للاتصالات، الذي يؤثر تأثيرا إيجابيا في التحقيقات الجارية في هذا المجال.
- المرسوم الملكي ٢٠٠٧/١٧٢٠ المؤرخ ٢١ كانون الأول/ديسمبر الذي يصدق على نظام تعديل القانون الأساسي ١٩٩٩/١٥ المؤرخ ١٣ كانون الأول/ديسمبر بشأن حماية البيانات الشخصية.
- القانون ٢٠٠٧/٥٦ المؤرخ ٢٨ كانون الأول/ديسمبر بشأن تدابير حفز مجتمع المعلومات.
- تجريم الأعمال الإلكترونية التالية المرتبطة بنشاط المنظمات الإرهابية في شبكة الإنترنت:
  - عمليات التخريب الحاسوبي، المادة ٢٦٤ من قانون العقوبات.
  - التهديدات، المادة ١٦٩ وما يليها من قانون العقوبات.
  - الدعوة إلى الإرهاب وتمجيده، المادة ٥٧٨ من قانون العقوبات.

تدابير أخرى

- إنشاء أفرقة للشرطة مخصصة لمكافحة استخدام الإنترنت من جانب المجموعات الإجرامية.
- المشاركة في مشروع ”راقب الشبكة“ الذي وضعته يوروبول.
- إنشاء مركز للاستجابة السريعة (فريق الاستجابة للطوارئ الحاسوبية) من أجل تحسين أمن نظم المعلومات الخاصة بالإدارات العامة.
- إنشاء مركز وطني لحماية البنى التحتية الحيوية.

التدابير التي يمكن أن يتخذها المجتمع الدولي لتعزيز أمن المعلومات على الصعيد العالمي.

- يشكل استخدام الإنترنت من جانب المنظمات الإرهابية ظاهرة تتجاوز الحدود الوطنية وتتطلب في العديد من الحالات إجراء تحقيقات مشتركة في بلدان مختلفة. وبالتالي، فإن كشف الأنشطة الإرهابية المرتكبة عن طريق الإنترنت ومنعها يتوقفان

بدرجة كبيرة على وجود اتفاقات دولية وصكوك أخرى للتعاون الدولي. ومن المهم في هذا الصدد العمل على مواءمة القوانين بما يكفل مزيدا من الفعالية في مكافحة وجود هذه الجماعات الإجرامية على الشبكة. ويمثل التعاون الدولي في مجال الشرطة أيضا جانبا رئيسيا لأن السرعة تكون حاسمة في هذا النوع من التحقيقات بالنظر إلى تقلب الأدلة الإلكترونية.

- إشراك القطاع الخاص في مكافحة الجريمة الإلكترونية. إذ يكتسي تعاون القطاع الخاص أهمية أساسية بالنظر إلى تحكمه في معظم الخدمات المعروضة على الإنترنت. ويتمتع القطاع الخاص بخبرة طويلة في مواجهة التهديدات القائمة في الإنترنت ويمكن أن تكتسي معارفه وتجاربه قيمة بالغة في هذا المجال.

- توعية المستعمل النهائي لكي يهتم بأمن حواسيبه. ذلك أن زيادة الوعي بهذه المشكلة يمكن أن يساهم في تخفيض عدد الحواسيب التي يستخدمها مجرمو الفضاء الإلكتروني لتنظيم أنشطتهم، وبخاصة تلك المتعلقة بشبكات البناء والتشغيل والنقل (botnets).

- وفيما يتعلق بالتدابير التي يمكن للمجتمع الدولي أن يتخذها من أجل تعزيز أمن المعلومات على الصعيد العالمي، ينبغي التوصل إلى توقيع اتفاقية بين الدول (مماثلة للاتفاقية الدولية لحماية الأرواح في البحر، أو مشابهة لها) تتعهد الدول بموجبها بتوحيد التشريعات لضمان ملاحقة الجرائم المرتبطة بشبكة الإنترنت، والسعي قدر الإمكان إلى الحيلولة دون تحويل الشبكة، في ظل ما تتيحه من سرية الهوية وغياب التشريعات والمصالح الاقتصادية، إلى أرضية خصبة ومثلى للجريمة والإرهاب. وينبغي تحقيق ذلك كله مع الحرص على حماية حرية المعلومات وإمكانية الوصول إليها.

- تبسيط إجراءات التعاون في مجالي القضاء والشرطة على الساحة الدولية لكي تتسنى ملاحقة الأعمال الجنائية بسرعة وفعالية، في ضوء الطابع المشتت للإنترنت وتقلب سجلات ضبط الروابط، وفقا لقوانين كل بلد.

٧ - وختاما، ينبغي للمجتمع الدولي أن يتخذ التدابير التي يرتئيها مناسبة لحماية المعلومات انطلاقا من رؤية استراتيجية موحدة، وأن يعمل إذا أمكن على رسم اتجاه موحد يحدد قواعد ومعايير مشتركة لجميع البلدان ويضع مجموعة متوازنة وكاملة من التدابير المحددة للحماية ويسمح بمواءمة السياسات والإجراءات التي تتبعها مختلف المنظمات الوطنية والدولية المعنية.