الأمم المتحدة

A/69/112

الجمعية العامة

Distr.: General
30 June 2014
Arabic
Original: English/Spanish

الدورة التاسعة والستون
البند ٩٢ 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/69/50.

240714 240714 14-56479X (A)

أولا - مقدمة

١ - في ٢٧ كانون الأول/ديسمبر ٢٠١٣، اتخذت الجمعية العامة القرار ٦٨/٢٤٣ المعنون ''التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي''. وفي الفقرة ٣ من القرار، دعت الجمعية جميع الدول الأعضاء إلى أن تواصل، آخذة في اعتبارها التقييمات والتوصيات الواردة في تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي (A/68/98)، موافاة الأمين العام بآرائها وتقييماتها بشأن المسائل التالية:

(أ) التقييم العام لمسائل أمن المعلومات؛

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

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

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

٢ - واستجابة لذلك الطلب، أُرسلت، في ١٩ شباط/فبراير ٢٠١٤، مذكرة شفوية إلى الدول الأعضاء تدعوها إلى تقديم معلومات عن ذلك الموضوع. وترد الردود التي تم تلقيها في الفرع الثاني أدناه. وستصدر أية ردود إضافية يتم تلقيها في شكل إضافات لهذا التقرير.

ثانيا - الردود الواردة من الحكومات

أستراليا

[الأصل: بالإنكليزية]

[٣٠ أيار/مايو ٢٠١٤]

ترى استراليا أن القانون الدولي القائم يوفر إطارا لسلوك الدول في الفضاء الإلكتروني، وللاستجابات التي تتخذها الدول بصورة ملائمة للنشاط غير المشروع على شبكة الإنترنت. ويشمل ذلك، عند الاقتضاء، القانون الدولي الإنساني، والقانون المتعلق باستخدام القوة، والقانون الدولي لحقوق الإنسان، والقانون الدولي المتعلق بمسؤولية الدول. وأية قواعد جديدة أو إضافية لسلوك الدول في الفضاء الإلكتروني لا بد وأن تُوضع بما يتفق مع القانون الدولي.

وقد أسهم التقرير الذي توافقت عليه آراء فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي (A/68/98) إسهاما كبيرا في توجيه الدول من خلال التأكيد على انطباق القانون الدولي، وبخاصة ميثاق الأمم المتحدة، على استخدام الدول للفضاء الإلكتروني، وضرورته للحفاظ على السلام والاستقرار. وترى استراليا أن هذه النتيجة تتسم بأهمية جوهرية. وتعتقد أستراليا أنه ينبغي للدول، فرادى وجماعات، أن تؤكد مجددا وعلنا فهمها لأن القانون الدولي ينطبق على سلوك الدول في الفضاء الإلكتروني، والتزامها بالعمل في الفضاء الإلكتروني وفقا لفهمها للقانون الدولي.

وقد سلم التقرير بضرورة مواصلة النقاش وتوضيح كيفية انطباق القانون الدولي على استخدام الدول للفضاء الإلكتروني، وأوصى بإجراء المزيد من الدراسات في هذا المجال. وأشار إلى إمكان وضع قواعد إضافية بمرور الوقت. وتعتقد استراليا أن تحديد كيفية انطباق القانون الدولي على سلوك الدول في الفضاء الإلكتروني في حالات النزاع وفي غير حالات النزاع على حد سواء، مع الاعتراف بما ينطوي عليه ذلك من تعقيدات، هو مهمة تتسم بالأولوية بالنسبة للمجتمع الدولي.

كما قدم التقرير توصيات مبتكرة بشأن تدابير بناء الثقة في الفضاء الإلكتروني. وتسلم أستراليا بأن توضيح كيفية انطباق القانون الدولي على استخدام الدول للفضاء الإلكتروني هو مهمة طويلة الأجل. أما في المدى القصير، فهناك حاجة لاتخاذ تدابير عملية لمعالجة ومنع نشوء المشاكل بين الدول في الفضاء الإلكتروني مما قد ينجم عن سوء الفهم، ومما يمكن أن يؤدي، من خلال سوء التقدير والتصعيد، إلى نشوب النزاعات. وترى استراليا أن منظمات الأمن الإقليمي مؤهلة بصفة خاصة للنظر في وضع وتطوير وتنفيذ تدابير لبناء الثقة في الفضاء الإلكتروني. وتقود أستراليا الجهود المبذولة في المنتدى الإقليمي التابع لرابطة أمم جنوب شرق آسيا لدفع هذا البرنامج الهام قدما، وهو البرنامج الذي ينبغي أن يشمل أهدافا تتعلق ببناء القدرات، نظرا لتفاوت قدرات الأعضاء.

النمسا

[الأصل: بالإنكليزية]

[١٩ أيار/مايو ٢٠١٤]

توفر الاستراتيجية النمساوية لأمن الفضاء الإلكتروني، التي اعتمدت في آذار/مارس ٢٠١٣، مفهوما شاملا واستباقيا لحماية الفضاء الإلكتروني والأشخاص في المحيط الافتراضي،

مع الحرص على ضمان حقوق الإنسان في الوقت نفسه. وهي تعزز أمن وقدرات البُنى الأساسية والخدمات النمساوية في الفضاء الإلكتروني. والأهم من ذلك، إنها تعمل على بناء الوعي والثقة في المجتمع النمساوي.

ويُعد بناء الشبكات العالمية والتعاون الدولي من الأمور الضرورية للاستراتيجية النمساوية لأمن الفضاء الإلكتروني. ويتحقق الأمن في الفضاء الإلكتروني من خلال مزيج من السياسات المنسقة على الصعيدين الوطني والدولي. وستشارك النمسا في ''سياسة خارجية [نشطة] للفضاء الإلكتروني'' في إطار شراكات تقوم على اتباع نهج منسق وموجه مع الاتحاد الأوروبي، والأمم المتحدة، ومنظمة الأمن والتعاون في أوروبا، ومجلس أوروبا، ومنظمة التعاون والتنمية في الميدان الاقتصادي، ومنظمة حلف شمال الأطلسي (الناتو).

وستسهم النمسا إسهاما كبيرا في تنفيذ استراتيجية الاتحاد الأوروبي لأمن الفضاء الإلكتروني، وستشارك مشاركة كاملة في الجهود الاستراتيجية والتشغيلية التي يضطلع بها الاتحاد الأوروبي. وستتخذ الوزارات المختصة التدابير اللازمة لتنفيذ اتفاقية مجلس أوروبا المتعلقة بالجرائم الإلكترونية والاستفادة منها بشكل كامل. وعلى المستوى الدولي، تدعو النمسا إلى حرية شبكة الإنترنت. فلا بد من ضمان حرية ممارسة جميع حقوق الإنسان في الفضاء الافتراضي؛ وعلى وجه التحديد، يجب ألا يتعرض الحق في حرية التعبير والحصول على المعلومات لأية قيود على نحو غير مبرر في شبكة الإنترنت.

وستواصل النمسا تعاونها الثنائي في إطار شراكة منظمة حلف شمال الأطلسي، وستدعم بصورة نشطة إعداد قائمة من التدابير الملموسة لبناء الثقة والأمن في منظمة الأمن والتعاون في أوروبا. وتشارك النمسا بصورة نشطة في تخطيط وتنفيذ تمارين خاصة بالفضاء الإلكتروني على المستوى عبر الوطني. وسيُستفاد من الخبرة المكتسبة بصورة مباشرة في تخطيط التعاون العملي ومواصلة تطويره. وتتولى وزارة الشؤون الخارجية تنسيق تدابير السياسة الخارجية ذات الصلة بأمن الفضاء الإلكتروني. وسيؤخذ في الاعتبار إبرام اتفاقات ثنائية أو دولية، حيثما كان ذلك مناسبا.

وعلى الصعيد الوطني، يقوم فريق توجيهي بوضع خطة تنفيذ للاضطلاع بالتدابير الأفقية المنصوص عليها في الاستراتيجية النمساوية لأمن الفضاء الإلكتروني. وتتولى الهيئات المختصة مسؤولية تنفيذ هذه التدابير في إطار ولاية كل منها، مع تولي فريق التوجيه مهمة التنسيق بينها. واستنادا إلى الاستراتيجية النمساوية لأمن الفضاء الإلكتروني، ستقوم تلك الهيئات بوضع استراتيجيات فرعية في مجالات مسؤوليات كل منها. وتم تكليف الوزارات الممثلة في فريق التوجيه بتقديم خطة تنفيذ نصف سنوية إلى الحكومة الاتحادية. وسيتواكب

إعداد الخطة مع استعراض للاستراتيجية النمساوية لأمن الفضاء الإلكتروني، لتنقيحها وتحديثها إذا لزم الأمر.

كولومبيا

[الأصل: بالإسبانية]

[٢٣ أيار/مايو ٢٠١٤]

تقييم عام لمسائل أمن المعلومات

تم في السنوات الأخيرة إحراز تقدم كبير في تطوير وتطبيق تكنولوجيا المعلومات والاتصالات؛ وأحدث ذلك تغيرات وفوائد كبرى أسهمت إسهاما واسعا في تطوير العديد من البلدان، مع تشجيع ازدياد التعاون الدولي لنشر المعلومات في نفس الوقت.

غير أن هذا التقدم التكنولوجي قد أبرز أيضا مخاوف عميقة إزاء إمكان أن تُستخدم تلك التطورات لتقويض الاستقرار والأمن الدوليين، والتأثير سلبا على سلامة البُنى الأساسية للدول، بما يسفر عنه ذلك من تقلص أمنها المدني والعسكري.

وفي هذا السياق، يُعد استخدام التكنولوجيات الجديدة لتوليد التهديدات الحاسوبية، والتهديد القائم للجريمة في الفضاء الإلكتروني، من الأمور التي تثير قلقا بالغا وتتسم بأقصى قدر من الأهمية الوطنية بالنسبة لكولومبيا.

وبالتالي، فلا بد لكولومبيا من وضع سياسات واستراتيجيات للحيلولة دون استخدام تكنولوجيا المعلومات في أغراض إرهابية أو جنائية.

الجهود المبذولة على الصعيد الوطني لتعزيز أمن المعلومات وتشجيع التعاون الدولي

الاستجابات على الصعيدين التشريعي والمؤسسي

في عام ٢٠٠٥ طبقت كولومبيا المعيار ٢٧٠٠١ للمنظمة الدولية لتوحيد المقاييسISO 27001، الذي يعتبر نظاما إداريا يحدد مستويات رفيعة لمعايير أمن المعلومات في الكيانات الوطنية، ويدعو لتأمين سرية وسلامة وتوافر[1] المعلومات.

(١) السرية: منع استخدام المعلومات من قِبل جهات غير مرخص لها من أفراد أو عمليات. السلامة: حماية دقة وكمال أي شيء ذي قيمة بالنسبة لمنظمة معينة. التوافر: كفالة وصول الكيانات المرخص لها إلى المعلومات وإمكانية استخدامها لها.

وبعد أربع سنوات، سن كونغرس جمهورية كولومبيا القانون رقم ١٢٧٣ لسنة ٢٠٠٩، الذي عدَّل القانون الجنائي، بإنشاء مصلحة جديدة تتمتع بالحماية القانونية، هي ''حماية المعلومات والبيانات''. وأتاح هذا التعديل إنشاء إطار قانوني وطني للسلطات المختصة لمقاضاة ومحاكمة الجرائم المتصلة بتكنولوجيا المعلومات.

وفي هذا الإطار، تجرِّم كولومبيا، ضمن جملة أمور، الدخول غير المشروع إلى النظم الحاسوبية؛ وتعطيل النظم الحاسوبية بصورة غير مشروعة؛ والهجمات على سلامة البيانات؛ والهجمات على سلامة النظم الحاسوبية؛ وإساءة استخدام أجهزة الحواسيب؛ والتزييف باستخدام الحاسوب؛ والاحتيال باستخدام الحاسوب؛ واستغلال الأطفال في المواد الإباحية؛ والجرائم المرتكبة ضد الملكية الفكرية وما يتصل بذلك من حقوق.

وفي عام ٢٠١١، أطلقت كولومبيا، من خلال الوثيقة رقم ٣٧٠١ للمجلس الوطني للسياسة الاقتصادية والاجتماعية، سياستها الوطنية للدفاع عن الفضاء الإلكتروني وأمن الفضاء الإلكتروني المبنية على ثلاث ركائز أساسية:

(أ) اعتماد إطار مناسب مشترك بين المؤسسات للوقاية والتنسيق والرصد وصياغة التوصيات للتصدي لما ينشأ من تهديدات ومخاطر؛

(ب) وضع برامج للتدريب المتخصص في أمن المعلومات؛

(ج) تعزيز التشريع الخاص بتلك المسائل والتعاون الدولي، والعمل في ذلك الإطار من أجل تسريع انضمام كولومبيا إلى العديد من الصكوك الدولية، وبخاصة اتفاقية بودابست.

ومن أجل تنفيذ المبادئ الاستراتيجية المذكورة أعلاه بشكل شامل، صممت كولومبيا وأنشأت أربع سلطات:

١ - اللجنة المشتركة بين القطاعات، المسؤولة عن رسم الرؤية الاستراتيجية لإدارة المعلومات ووضع المبادئ التوجيهية لسياسات إدارة الهياكل الأساسية العامة لتكنولوجيا المعلومات وأمن الفضاء الإلكتروني والدفاع عن الفضاء الإلكتروني؛

٢ - الفريق الكولومبي للتصدي للطوارئ الحاسوبية، وهي وكالة التنسيق الوطنية المعنية بمسائل أمن الفضاء الإلكتروني والدفاع عن الفضاء الإلكتروني؛

٣ - القيادة المشتركة للفضاء الإلكتروني التابعة للقوات المسلحة، المكلفة بمنع ومكافحة أي تهديد أو هجوم إلكتروني يؤثر على القيم والمصالح الوطنية؛

٤ - مركز الشرطة المعنية بالجرائم الإلكترونية؛ وهو مسؤول عن أمن الفضاء الإلكتروني في كولومبيا، وتوفير المعلومات والدعم والحماية من الجرائم الإلكترونية.

كما أن لدى كولومبيا إطار قانوني لحماية البيانات الشخصية، أنشئ بموجب القانون رقم ١٥٨١ لعام ٢٠١٢ والمرسوم رقم ١٣٧٧ لعام ٢٠١٣، الذي ينظم جوانب من ذلك القانون. وعلاوة على ذلك، أنشئت إدارة لحماية البيانات الشخصية في هيئة الرقابة على الصناعة والتجارة.

وقامت وزارة تكنولوجيا المعلومات والاتصالات بوضع وتنفيذ استراتيجية حكومية لشبكة الإنترنت، تضمنت إلزام الكيانات باعتماد نظم لإدارة أمن المعلومات. وبالمثل، قامت الوزارة منذ عام ٢٠٠٨ بتدريب نحو ٣٠٠ ٦ من موظفي الخدمة المدنية على العمليات المتعلقة بإدارة تكنولوجيا المعلومات.

كما تجدر الإشارة إلى أنه يجري، في مجال القدرات، إحراز تقدم في تحديد البنية الأساسية الحيوية (أي البنية الأساسية التي يمكن، في حالة تلفها، أن تؤدي إلى خسائر في الأرواح أو أضرار اقتصادية أو تقليص القدرة على حكم البلد)، وذلك بغية ضمان أمن الفضاء الإلكتروني في تلك المواقع.

التعاون الدولي

في عام ٢٠١٣، طلبت كولومبيا رسميا الانضمام إلى عضوية الاتفاقية الأوروبية بشأن الجريمة الإلكترونية، التي تنص على مبادئ الاتفاق الدولي بشأن أمن الفضاء الإلكتروني والعقوبات الموقعة على الجرائم المقابلة، والتي يتمثل الهدف الرئيسي لها في حماية المجتمع من الجريمة الإلكترونية من خلال وضع التشريعات المناسبة والتعاون الدولي.

وبالإضافة إلى ذلك، انضمت كولومبيا في عام ٢٠١٢ إلى اتفاق متعدد الأطراف مع المنتدى الاقتصادي العالمي، يُعرف باسم ''الشراكة من أجل تنمية قدرات التصدي في الفضاء الإلكتروني''، وهي شراكة تهدف إلى تحديد ومعالجة المخاطر المنهجية العالمية الناجمة عن ازدياد الارتباطات بين الأشخاص والعمليات والأشياء بدرجة أكبر من أي وقت مضى.

وفي الوقت نفسه، وضعت أمانة لجنة البلدان الأمريكية لمكافحة الإرهاب التابعة لمنظمة الدول الأمريكية نهجا شاملا لبناء القدرات في مجال أمن الفضاء الإلكتروني فيما بين الدول الأعضاء. وكان الإنجاز الرئيسي للأمانة يتمثل في تشكيل أفرقة وطنية ''للتأهب والمراقبة والإنذار''، تُعرف أيضا باسم ''فرق الاستجابة لحوادث الأمن الحاسوبية''، وهي

تمتلك الولاية والقدرة على الاستجابة للأزمات والحوادث والتهديدات التي يتعرض لها أمن الفضاء الإلكتروني.

وفي هذا الإطار، وبالتعاون مع لجنة مكافحة الإرهاب التابعة لمنظمة الدول الأمريكية، شكلت كولومبيا أفرقة ''للتأهب والمراقبة والإنذار'' تسهم في تطوير استراتيجيات وطنية لأمن الفضاء الإلكتروني. كما شاركت في حلقات عمل ودورات ومؤتمرات تتناول التعامل مع الحوادث المتعلقة بأمن الفضاء الإلكتروني وأمن المعلومات والجريمة الإلكترونية.

وتجدر الإشارة أيضا إلى أن كولومبيا قد توصلت إلى اتفاقات مع شركات ومنظمات دولية تعمل في مجال صناعة المعلومات والاتصالات، ومن أبرزها اتفاق مع شركة مايكروسوفت لتمكين مؤسسات مثل ''مركز الجرائم الإلكترونية'' وبرامج أمن الفضاء الإلكتروني الأخرى من الوصول إلى موارد الشركة؛ واتفاق مع ''الفريق العامل المعني بمكافحة التصيد الإلكتروني'' بغرض الانضمام إلى التحالف العالمي للسلطات القانونية والمؤسسات الصناعية والهيئات الحكومية التي تعمل من أجل إنشاء آليات أكثر كفاءة للإنذار في حالات حوادث الفضاء الإلكتروني والاستجابة لها.

التدابير الدولية المتخذة لتعزيز أمن المعلومات

أمن الفضاء الإلكتروني ليس مشكلة الحكومة وحدها، ولا يمكن أن تحلها الحكومة وحدها: فلا بد من توفر دعم الجهات الفاعلة الأخرى، وهي الأوساط الأكاديمية ودوائر الصناعة والمجتمع المدني، للتصدي بشكل فعال للمخاطر الناشئة عن ازدياد استخدام تكنولوجيا المعلومات والاتصالات في جميع القطاعات بدرجة أكثر كثافة من أي وقت مضى.

وترى كولومبيا أنه لتعزيز أمن المعلومات الدولية على الصعيد الدولي، فإن من الأهمية أن يعمد المجتمع الدولي إلى ما يلي:

- السعي لإنشاء آليات لرفع مستوى الوعي في المجتمع، وبين المسؤولين المنتخبين والكيانات في كل دولة، بالحاجة إلى خلق ثقافة أمن المعلومات وبأهمية التعاون الدولي لمكافحة الجريمة الإلكترونية.
- تشجيع الدول على الالتزام بوضع استراتيجيات تهدف إلى تعزيز القدرات الوطنية في مجال أمن الفضاء الإلكتروني والدفاع عن الفضاء الإلكتروني.

- حث الدول على تحديد البنية الأساسية الحيوية وإنشاء برنامج يهدف على وجه التحديد إلى تعزيز أمنها وقدرتها على الصمود.
- توفير الحوافز لتوفيق الأطر القانونية المحلية مع الصكوك الدولية القائمة في مجال أمن الفضاء الإلكتروني. وزيادة المواءمة بين مختلف البلدان ستسهل إنشاء قنوات للتعاون من أجل الوقاية والتحقيق والملاحقة القضائية للجرائم الإلكترونية من جانب الدول.

وينبغي أن تسهم جهود المواءمة هذه في تحديد الجرائم ذات الصلة بالتكنولوجيا ووضع قواعد واضحة بشأن الاختصاص القضائي وصلاحية المحاكمة.

- التشجيع على إنشاء التزامات تلزم الدول والكيانات الوطنية العامة والخاصة بحفظ السجلات الحاسوبية لاستخدامها لاحقا في التحقيقات والمحاكمات.
- تجميع مسرد بالمصطلحات الحاسوبية المتصلة بالجرائم الإلكترونية غير المعروفة بوجه عام لمسؤولي نظام العدالة الجنائية، لضمان سرية وسلامة النظم والشبكات والبيانات الحاسوبية.
- تشجيع تبادل الخبرات والممارسات المثلى في مجال أمن الفضاء الإلكتروني، فضلا عن إنشاء شبكات للتدريب المتخصص.
- حث الدول على الانضمام إلى شبكات الإنذار بحوادث الفضاء الإلكتروني.

كوبا

[الأصل: بالإسبانية]

[٢٧ أيار/مايو ٢٠١٤]

تشاطر كوبا تماما القلق الذي أعرب عنه القرار ٦٨/٢٤٣ إزاء استخدام تكنولوجيات المعلومات ووسائل الاتصالات السلكية واللاسلكية التي قد تؤثر على الاستقرار والأمن الدوليين وسلامة الدول، مما يقوِّض أمنها في المجالين المدني والعسكري. ويشدد القرار أيضا على النحو الواجب على ضرورة منع استخدام موارد المعلومات وتكنولوجياتها في أغراض إجرامية أو إرهابية.

وفي هذا الصدد، تعرب كوبا عن بالغ قلقها إزاء استخدام الأفراد والمنظمات للنظم الحاسوبية للبلدان الأخرى، بصورة سرية وغير مشروعة، بغرض مهاجمة بلدان ثالثة، لما ينطوي عليه ذلك من إمكانية تفجير النزاعات الدولية. بل وتقول بعض الحكومات إن من

الممكن الرد على مثل هذه الهجمات باستخدام الأسلحة التقليدية. والتعاون المشترك بين جميع الدول هو السبيل الوحيد لمنع ومعالجة هذه التهديدات المستجدة، وتجنب تحويل الفضاء الإلكتروني إلى مسرح للعمليات العسكرية.

إن الاستخدام العدائي للاتصالات السلكية واللاسلكية الذي يرمي سرا أو علانية إلى تقويض النظام القانوني والسياسي للدول، يشكل انتهاكا للقواعد الدولية المعترف بها في هذا المجال، ويمكن أن يؤدي إلى نشوء توترات وأوضاع لا تفضي إلى تحقيق السلام والأمن الدوليين.

وفي هذا الصدد، تكرر كوبا إدانتها للحرب الإذاعية والتلفزيونية التي تشنها حكومة الولايات المتحدة الأمريكية ضد كوبا، والتي تنتهك القواعد الدولية السارية في مجال تنظيم المجال اللاسلكي. وهي ترتكب هذا العدوان دون أن تقيم اعتبارا للأضرار التي يمكن أن يسببها للسلم والأمن الدوليين من خلال خلق حالات تنطوي على الخطر.

وتهدف موجات البث الإذاعي والتلفزيوني غير المشروعة ضد كوبا إلى الدعوة للهجرة غير الشرعية، وتشجيع العنف والتحريض عليه، وازدراء النظام الدستوري، وارتكاب الأعمال الإرهابية. ويُعد استخدام المعلومات بغرض تقويض النظام الداخلي للدول الأخرى، وانتهاك سيادتها والتدخل في شؤونها الداخلية، أمرا غير قانوني.

وتشكل هذه الإذاعات ضد كوبا انتهاكا للقواعد الدولية السارية في دستور الاتحاد الدولي للاتصالات السلكية واللاسلكية، الذي تقر ديباجته بالأهمية المتزايدة للاتصالات السلكية واللاسلكية في حفظ السلام والتنمية الاقتصادية والاجتماعية لجميع الدول، بهدف تيسير العلاقات السلمية والتعاون الدولي بين الشعوب وتحقيق التنمية الاقتصادية والاجتماعية من خلال كفاءة خدمات الاتصالات السلكية واللاسلكية.

وتواصل حكومة الولايات المتحدة الأمريكية بث الإذاعات الصوتية كل يوم على موجة متوسطة تجارية على مدار ٢٤ ساعة يوميا. ولا يُخصص هذا النطاق الترددي للخدمات الموجهة إلى بلدان أخرى. وتقدم محطات الإذاعة التجارية الأخرى الخدمات لمنظمات معادية لكوبا لبث إذاعاتها التي تهدف إلى تخريب النظام الداخلي وتضليل الشعب الكوبي.

وتقوم منظمات عديدة من هذه المنظمات ببث هذه الإذاعات على الموجة القصيرة، بعلم كامل من حكومة الولايات المتحدة.

وفي الفترة ما بين نيسان/أبريل ٢٠١٣ ونيسان/أبريل ٢٠١٤، كان متوسط عدد ساعات البث للإذاعات ذات المحتوى التخريبي إلى كوبا يتراوح بين ١٩٠٩ ساعات و ٢٠٧٠

ساعة أسبوعيا، وذلك باستخدام ٢٧ ترددا. وفي شهري أيلول/سبتمبر وتشرين الأول/أكتوبر ٢٠١٣، بدأت محطتان من أمريكا الشمالية البث من جنوب ولاية فلوريدا لإذاعات تم التقاطها في الأجزاء الغربية والوسطى من كوبا تتضمن برامج ذات طبيعة معادية للثورة.

كما الإذاعات المعادية لكوبا من محطة إذاعة وتلفزيون مارتي عبر أنظمة سواتل دولية ومحلية في الولايات المتحدة.

وعلاوة على ذلك، تم خلال العام الحالي فضح عملية ZunZuneo، وهي عبارة عن مخطط معقد مدعوم بملايين الدولارات من حكومة الولايات المتحدة بهدف تشجيع التخريب في كوبا باستخدام خدمة الرسائل على الشبكات الاجتماعية.

وهذا البرنامج غير المشروع، الذي ظل يعمل حتى عام ٢٠١٢، كان يُستخدم لجمع البيانات الخاصة للمستخدمين الكوبيين، دون موافقتهم، ومعالجة ملفاتهم الشخصية حسب الجنس والعمر والأذواق ومختلف أنواع الانتماءات لاستخدامها لأغراض سياسية.

وعملية ZunZuneo، كغيرها من العمليات ذات الأغراض التخريبية، تخالف القوانين الكوبية وقوانين الولايات المتحدة، ومنها مثلا قانون مكافحة المواد الإباحية والتسويقية غير المرغوب فيها لعام ٢٠٠٣ (القانون رقم ١٠٨-١٨٧) الذي أقره الكونغرس الأمريكي في كانون الأول/ديسمبر ٢٠٠٣، والذي يحظر توجيه رسائل تسويقية أو من أي نوع آخر للغير دون موافقة صريحة منهم.

وكان ذلك انتهاكا آخر لدستور الاتحاد الدولي للاتصالات السلكية واللاسلكية، حيث من الواضح أن هذه الاستخدامات للتكنولوجيات الجديدة، وللشبكات الاجتماعية على وجه الخصوص، ليست مواتية لقيام علاقات سلمية وتعاون دولي من خلال خدمات الاتصالات السلكية واللاسلكية الفعالة.

وكانت تلك العادة الضارة لإرسال البريد غير المرغوب فيه (البريد المتطفل) محلا لأكثر من ١٠ توصيات من مكتب توحيد مقاييس الاتصالات السلكية واللاسلكية، وهي تشكل انتهاكا للبند رقم ٣٧ من إعلان مبادئ القمة العالمية لمجتمع المعلومات التي عقدت في جنيف عام ٢٠٠٣.

ويجب على حكومة الولايات المتحدة احترام القانون الدولي ومقاصد ومبادئ ميثاق الأمم المتحدة؛ ولذلك، يجب أن تتوقف الإجراءات غير القانونية والسرية ضد كوبا، التي ندد بها الشعب الكوبي والرأي العام الدولي.

وفي هذا الصدد، اعتمدت جماعة دول أمريكا اللاتينية ومنطقة البحر الكاريبي في ٢٩ نيسان/أبريل بيانا، شددت فيه على أن الاستخدام غير القانوني لتكنولوجيا المعلومات والاتصالات الجديدة يترك أثرا سلبيا على الدول ومواطنيها.

وأعربت الجماعة، في هذا البيان، بقوة عن رفضها لاستخدام تكنولوجيا المعلومات والاتصالات على نحو يخالف القانون الدولي، ولجميع الإجراءات من هذا القبيل. وشددت على أهمية ضمان استخدام هذه التقنيات بما يتوافق تماما مع مقاصد ومبادئ ميثاق الأمم المتحدة والقانون الدولي، وخاصة مبادئ السيادة، وعدم التدخل في الشؤون الداخلية للآخرين، والمعايير المعترف بها دوليا للتعايش بين الدول. كما كررت التزامها بتكثيف الجهود الدولية لتأمين الفضاء الإلكتروني وتشجيع استخدامه للأغراض السلمية حصرا، وباعتباره وسيطا يسهم في التنمية الاقتصادية والاجتماعية.

وتؤيد كوبا القرار ٦٨/٢٤٣، وسوف تستمر في المساهمة في التطوير السلمي لتكنولوجيا المعلومات والاتصالات واستخدامها على الصعيد العالمي من أجل خير الإنسانية جمعاء.

السلفادور

[الأصل: بالإسبانية]

[٢٦ أيار/مايو ٢٠١٤]

أنشأت القوات المسلحة السلفادورية، في إطار أمن المعلومات والاتصالات السلكية واللاسلكية، شبكة للاتصالات السلكية واللاسلكية بالصوت والصورة والبيانات بصورة منفصلة عن الشبكة العامة، وتعتزم حماية كافة المعلومات من أي طرف خارجي قد يحاول التسلل إليها، وكذلك تأمينها من هجمات الفضاء الإلكتروني.

جورجيا

[الأصل: بالإنكليزية]

[٣٠ حزيران/يونيه ٢٠١٤]

موجز تنفيذي

أدت الحرب الإلكترونية، التي تعرضت لها جورجيا في عام ٢٠٠٨، إلى وضع حماية البنية الأساسية الحيوية في صدارة جدول أعمال حكومة جورجيا. فاعتماد البنية

الأساسية الحيوية والخدمات الحكومية الذي يزداد بوتيرة سريعة على تكنولوجيا المعلومات يزيد من التعرض للحوادث المتصلة بالجريمة الإلكترونية. وبناء على ذلك، فإن توفير الحماية الكافية للبنية الأساسية الحيوية من تهديدات الفضاء الإلكتروني هو من بين أولويات حكومة جورجيا.

وكانت المواقع الحكومية ومواقع وسائط الإعلام أول الأهداف التي استهدفتها الهجمات الإلكترونية عام ٢٠٠٨. ثم اتسع نطاق الهجمات بعد ذلك ليشمل المزيد من المواقع الحكومية، والمؤسسات المالية الجورجية، وجمعيات رجال الأعمال، والمؤسسات التعليمية، والمزيد من المواقع الإخبارية الإعلامية، ومنتدىً جورجياً للقرصنة الإلكترونية. وكانت هذه الهجمات الإلكترونية تهدف إلى تعطيل سير العمليات الطبيعية لتلك المؤسسات. وإلى جانب اثنين من المصارف الكبرى، كانت الأهداف المتصلة بالأعمال التجارية تتمثل في المقام الأول في المنظمات التي تُستخدم في الاتصال وتنسيق الاستجابات بين مختلف الأعمال التجارية.

وتوضح التجربة المذكورة أعلاه أن الهجمات الإلكترونية على البنية الأساسية الحيوية في جورجيا من جانب دول وجهات خاصة يمكن أن تسبب أضرارا مادية بالغة، فضلا عن أضرار مالية فادحة للقطاعين العام والخاص. لذلك، تعتبر حكومة جورجيا أمن الفضاء الإلكتروني جزءا من السياسة الأمنية العامة للبلد، وخاصة في ضوء اعتمادها بصورة متزايدة على تكنولوجيا المعلومات كوسيلة لتوفير الخدمات الحكومية.

وتعبيرا عن هذه المخاوف، وضع مجلس الأمن القومي وفريق عامل خاص مؤلف من مختلف الوكالات الحكومية استراتيجية لأمن الفضاء الإلكتروني الوطني جورجيا خلال عام ٢٠١١، كجزء من استعراض للأمن القومي. وقُدمت استراتيجية أمن الفضاء الإلكتروني وخطة العمل الموضوعة لتنفيذها إلى الجمهور لمناقشتهما في آذار/مارس ٢٠١٢، وتم اعتمادهما أخيرا في كانون الثاني/يناير ٢٠١٣.

واتخذت في ٢٠١٠ خطوة أخرى تمثلت في إنشاء وكالة لتبادل البيانات في وزارة العدل الجورجية لتكون الكيان الحكومي المركزي المسؤول عن وضع وتنفيذ سياسات وحلول الحكومة الإلكترونية. ويتمثل جزء هام من ولاية الوكالة في أمن المعلومات للقطاع العام والكيانات الخاصة على النحو التالي:

- اعتماد وتنفيذ سياسات ومعايير أمن المعلومات في القطاع العام والبنية الأساسية الحيوية

- تقديم الخدمات الاستشارية في مجال أمن المعلومات والقيام بعمليات تدقيق أمن المعلومات
- أنشطة التوعية بالمسائل المتعلقة بأمن المعلومات في القطاع العام، فضلا عن القطاع المدني
- الاضطلاع بولاية أمن الفضاء الإلكتروني من خلال الفريق الوطني للتصدي للطوارئ الحاسوبية.

ويمكن الاطلاع على النص الكامل للعرض المقدم من جورجيا من خلال الموقع الشبكي: http://www.un.org/disarmament/topics/informationsecurity/.

ألمانيا

[الأصل: بالإنكليزية]

[٣٠ أيار/مايو ٢٠١٤]

موجز تنفيذي

تتيح تكنولوجيات المعلومات والاتصالات فرصا غير مسبوقة للبلدان الصناعية والنامية على حد سواء. غير أن النظم الحاسوبية لا تخلو، في الوقت نفسه، من جوانب الانكشاف ونقاط الضعف.

وهناك اتجاه نحو الأنشطة المتطورة والخبيثة التي يصعب تعقبها، والتي تستهدف أهدافا ذات قيمة عالية، وهو ما قد يتسبب في عواقب وخيمة. فالهجوم الإلكتروني على البُنى الأساسية الرئيسية يمكن أن يحدث تعطيلا أكبر من الهجمات المادية المعزولة، بما يؤدي في بعض الأحيان إلى عواقب لا يمكن التنبؤ بها بالنسبة للكيانات الأخرى المتصلة بشبكة الإنترنت.

ولكن على الرغم من هذه المخاطر، لا يبدو من الواقعي في الوقت الراهن احتمال نشوب ''حرب إلكترونية'' شاملة. فالسيناريو الأكثر احتمالا قد يتمثل في الاستخدام المحدود للقدرات الإلكترونية كجزء من مجهود حربي أوسع نطاقا. وأخيرا، فإن ثمة خطرا من أن حوادث الفضاء الإلكتروني قد تتصاعد إلى درجة نشوب نزاع ''واقعي حقيقي''.

وفي هذه الحالة، فإن زيادة القدرات الإلكترونية، والاتفاق على القوانين والقواعد التي تنطبق على استخدام تكنولوجيا المعلومات والاتصالات، والمشاركة في تدابير بناء الثقة، تصبح أكثر أهمية من أي وقت مضى.

وقد تحقق تقدم جدير بالترحيب في عام ٢٠١٣: فقد أوضح التقرير الأخير لفريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي أن القانون الدولي ينطبق على الفضاء الإلكتروني. كما رأى الفريق أن سيادة الدولة والقواعد والمبادئ التي تنبع من السيادة تنطبق على إدارة الدولة للأنشطة المتصلة بتكنولوجيا المعلومات والاتصالات والبنية الأساسية وبولايتها القضائية على تكنولوجيا المعلومات والاتصالات داخل أراضيها. وتتطلع ألمانيا إلى رؤية المدى الذي سيصل إليه فريق الخبراء بهذه المسألة.

وفيما يتعلق بتدابير بناء الثقة، أحرزت منظمة الأمن والتعاون في أوروبا تقدما هاما باعتماد أول مجموعة من الخطوات لزيادة التعاون والشفافية والقدرة على التنبؤ والاستقرار فيما بين الدول، وذلك بغية الحد من مخاطر سوء الفهم وتصعيد النزاعات مما قد ينجم عن استخدام تكنولوجيا المعلومات والاتصالات. وقد يكون اتفاق المنظمة هذا مفيدا كنموذج للمنظمات الإقليمية الأخرى.

وتنطلق استراتيجية أمن الفضاء الإلكتروني الألمانية (٢٠١١) من التأكيد على أن توافر الفضاء الإلكتروني وسلامة وصحة وسرية البيانات في الفضاء الإلكتروني أصبحت تتسم بأهمية حيوية. فقد تحول ضمان أمن الفضاء الإلكتروني إلى واحد من التحديات المحورية التي تواجه الدولة ودوائر الأعمال والمجتمع. فهي جميعا بحاجة إلى العمل معا، على الصعيد الوطني وبالتعاون مع الشركاء الدوليين على حد سواء. وتحدد استراتيجية أمن الفضاء الإلكتروني في ألمانيا الأهداف والتدابير التالية:

- حماية البنية الأساسية الحيوية للمعلومات
- تأمين نظم تكنولوجيا المعلومات
- تعزيز أمن تكنولوجيا المعلومات في الإدارة العامة
- تشغيل مركز وطني للاستجابة في مجال الفضاء الإلكتروني
- إنشاء مجلس وطني لأمن الفضاء الإلكتروني
- فعالية مكافحة الجريمة في الفضاء الإلكتروني
- فعالية جهود التنسيق لضمان أمن الفضاء الإلكتروني في أوروبا وفي أنحاء العالم
- استخدام تكنولوجيا معلومات موثوقة وجديرة بالثقة
- تنمية قدرات الموظفين فيما بين السلطات الاتحادية

- تطوير أدوات للرد على الهجمات الإلكترونية.

وفي أعقاب الانتخابات العامة الألمانية في أيلول/سبتمبر ٢٠١٣، ووفقا لاتفاق الائتلاف، احتل أمن الفضاء الإلكتروني موقعا متقدما على جدول أعمال الحكومة. ومن المقرر أن ترتفع معايير خصوصية البيانات. وتشمل المواضيع الرئيسية للسنوات الأربع القادمة تحسين حماية المستهلك؛ وإدخال تعديلات على القوانين الجنائية لتوفير حماية أفضل للأفراد؛ وإصدار قانون لأمن تكنولوجيا المعلومات مع وضع معايير أمن إلزامية دنيا لتكنولوجيا المعلومات للبنية الأساسية الحيوية؛ وإلزام جميع السلطات الاتحادية باستثمار ١٠ في المائة من ميزانية تكنولوجيا المعلومات فيها من أجل تحسين أمن نظمها.

ونتيجة للمخاوف المتعلقة بمراقبة الاتصالات و/أو اعتراضها بصورة تعسفية أو غير قانونية، فضلا عن قيام أطراف ثالثة بجمع البيانات الشخصية بصورة تعسفية أو غير قانونية، فإن حكومة ألمانيا تشجع بقوة مقدمي خدمات تكنولوجيا المعلومات على تشفير الاتصالات السلكية واللاسلكية وعدم تزويد أجهزة المخابرات الأجنبية ببيانات تلك الاتصالات.

ويمكن الاطلاع على النص الكامل للعرض المقدم من ألمانيا من خلال الموقع الشبكي: http://www.un.org/disarmament/topics/informationsecurity/.

البرتغال

[الأصل: بالإنكليزية]

[٢٠ أيار/مايو ٢٠١٤]

يشير قرار الجمعية العامة ٦٨/٢٤٣ المتعلق بالموضوع المذكور أعلاه إلى أهمية دور العلم والتكنولوجيا في سياق الأمن الدولي، مع التسليم بأن التطورات في هذين المجالين يمكن أن تكون لها تطبيقات مدنية وعسكرية، والتسليم أيضا بوجوب إحراز تقدم فيهما وتشجيع ذلك. والتقدم في مجال المعلومات والاتصالات السلكية واللاسلكية يعني مواصلة تطوير الحضارة وتوسيع فرص التعاون فيما بين الدول وتعزيز الإمكانات الخلاقة لدى البشرية وإدخال تحسينات إضافية على تداول المعلومات في المجتمع ككل.

غير أن تلك التكنولوجيات والوسائل يمكن أن تُستخدم لأغراض لا تتفق مع الاستقرار والأمن الدوليين، ويمكن أن تؤثر سلبا على السلامة الوطنية للدول، في المجالات المدنية والعسكرية.

ويشير قرار الجمعية العامة ٦٨/٢٤٣ إلى تقرير فريق الخبراء الحكوميين A/68/98، ويطلب مساهمة الدول الأعضاء في أربعة مجالات، هي:

١ - التقييم العام لمسائل أمن المعلومات؛

٢ - الجهود المبذولة على الصعيد الوطني لتعزيز أمن المعلومات وتشجيع التعاون الدولي في هذا الميدان؛

٣ - مضمون المفاهيم الرامية لتعزيز أمن نظم المعلومات والاتصالات السلكية واللاسلكية على الصعيد العالمي؛

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

وعرض التقرير بعض التوصيات المتعلقة بالمجالات التالية: معايير وقواعد ومبادئ السلوك المسؤول من جانب الدول؛ وتدابير بناء الثقة وتبادل المعلومات؛ وتدابير بناء القدرات.

واتباعا لتلك التوصيات التالية، يمكن أن نصف سياقنا الوطني على النحو التالي:

(أولا) المعايير والقواعد والمبادئ التي تميز السلوك المسؤول للدول

١ - تعتبر البرتغال أن الأمن في شبكة المعلومات يتسم بالأهمية ويأخذ في الازدياد؛

٢ - لا بد وأن نسلط الضوء على بذل الجهود لتنفيذ التشريعات المتعلقة بأمن الشبكات وسلامتها من خلال اعتماد أساليب تتعلق بالتصدي للمخاطر، وتتطلب اتخاذ تدابير أمنية كافية، على المستويين الفني والتنظيمي، والإلزام بالإبلاغ عن الانتهاكات الأمنية أو الخلل في سلامة النظم مما يترك أثرا كبير على توفر الخدمات. ومن المهم أيضا وجود إجراءات للتدقيق في مجال الأمن، يضطلع بتنفيذها المركز الوطني لإخطارات الإبلاغ عن الانتهاكات الأمنية أو الخلل في سلامة النظم؛

٣ - فيما يتعلق بحماية البيانات الشخصية والخصوصية، من المهم تسليط الضوء على التغييرات التي طرأت، على سبيل المثال في الإبلاغ الإلزامي عن انتهاكات البيانات الشخصية؛

٤ - على مستوى المفاهيم، من المهم تعزيز الفكرة القائلة بضرورة انبثاق اللوائح التنظيمية من القواعد الدولية؛

٥ - على الصعيد الدولي، من المهم تعزيز تبادل المعلومات والقيام بتمارين التدريب الميداني في مناطق الحدود.

(ثانيا) تدابير تعزيز الثقة وتقاسم المعلومات

١ - من الأهمية بمكان تعزيز تقاسم المعلومات، مع مراعاة العولمة الأوسع نطاقا؛

٢ - على الصعيد الوطني، تركزت جهودنا على إنجاز تدريبات مشتركة تشارك فيها كيانات عامة وخاصة، وتشجيع التوحيد التقني، وتنظيم المؤتمرات والحلقات الدراسية، التي يشارك في بعضها متحدثون دوليون.

(ثالثا) تدابير بناء القدرات

١ - من المهم وضع تدابير لبناء القدرات. غير أن هناك، مع ذلك، صعوبات تتعلق بالتدريب والحفاظ على الموارد البشرية المرتبطة بهذه الأنشطة؛

٢ - هناك حاجة لتسهيل الوصول إلى المعرفة؛

٣ - المستويات العليا ليست على دراية كافية بمسؤوليتها في هذه المسائل.

صربيا

[الأصل: بالإنكليزية]

[٢٨ أيار/مايو ٢٠١٤]

نظرا للأهمية الكبيرة التي يتسم بها أمن المعلومات على الصعيدين العالمي والوطني، تضطلع جمهورية صربيا بعدد من الأنشطة من أجل وضع سياسات وطنية كفؤة وإقامة آليات أمن فعالة. وفي استراتيجية تطوير مجتمع المعلومات في جمهورية صربيا حتى عام ٢٠٢٠، التي اعتمدتها حكومة جمهورية صربيا في ٢٠١٠، أُعلن أمن المعلومات واحدا من ستة مجالات تتسم بالأولوية. وليس لدى صربيا استراتيجية وطنية مخصصة لأمن المعلومات دون سواه، ولكن يجري تناول هذا الموضوع في عدد من الوثائق الأخرى. وفي تشرين الأول/أكتوبر ٢٠١٣، تم تشكيل فريق عمل خاص وتكليفه بصياغة مشروع قانون بشأن أمن المعلومات. ويتفق القانون مع الأطر القانونية الدولية والأطر القانونية المعتمدة في الاتحاد الأوروبي، وهو يحدد ما يلي: الإطار المؤسسي لأمن المعلومات؛ والتدابير اللازمة لتوفير الأمن المعزز لنظم تكنولوجيا المعلومات والاتصالات في جمهورية صربيا، بما في ذلك نظم تكنولوجيا المعلومات والاتصالات لدى الهيئات والمؤسسات العامة؛ وقواعد تنسيق الوقاية

من المخاطر الأمنية على نظم تكنولوجيا المعلومات والاتصالات؛ وإنشاء فريق وطني للتصدي للطوارئ الحاسوبية؛ ووضع تدابير أمنية محددة وشروط مسبقة لتطبيقها في نظم المعلومات في أجهزة الدولة؛ وأمن البيانات السرية في أنظمة تكنولوجيا المعلومات والاتصالات؛ والأمن المشفر والحماية من الانبعاثات الكهرومغناطيسية الضارة.

وتضطلع هيئة تكنولوجيا الاتصالات والمعلومات بإدارة الخدمات المشتركة لهيئات الجمهورية بتنفيذ الأنشطة المتصلة بحماية أمن المعلومات، وحماية البيانات، وتنفيذ المعايير الأمنية المقررة لنظم المعلومات في الهيئات الحكومية. وفي التقرير السنوي للإدارة، ذُكر أنه في إطار الولاية المسندة لها بحماية أنظمة تكنولوجيا المعلومات والاتصالات للدولة، توفر الإدارة الحماية من الهجمات الإلكترونية بصورة يومية، حيث تُهاجم الشبكة كل يوم.

وتقوم الشبكة الأكاديمية لجمهورية صربيا بأنشطة التصدي للحوادث الأمنية الحاسوبية في مؤسسات البحوث التربوية والعلمية في جمهورية صربيا. وفي التقرير السنوي للشبكة الأكاديمية لعام ٢٠١٣، أعلن أنه كان هناك عدد متزايد من الحوادث مقارنة بعام ٢٠١٢. وحدد التقرير قِدم المعدات كواحد من الأسباب التي أدت إلى ازدياد عدد الهجمات.

وثقافة أمن المعلومات الوطنية الراسخة في كل مستوى من مستويات المجتمع هي وحدها التي يمكن أن تكون فعالة في تعزيز أمن نظم المعلومات والاتصالات السلكية واللاسلكية الوطنية على الصعيد المحلي. وبالمثل، فإن أنظمة أمن المعلومات الوطنية الراسخة هي وحدها التي يمكن أن تكون جزءا من تطبيق المفاهيم الدولية لأمن المعلومات من أجل تعزيز أمن نظم المعلومات والاتصالات السلكية واللاسلكية العالمية.

ومكتب مجلس الأمن القومي وحماية المعلومات السرية (ويُشار إليه فيما يلي باسم مكتب مجلس الأمن القومي) هو الخدمة الحكومية الصربية المسؤولة عن تنسيق تنفيذ السياسات الأمنية الوطنية وسياسات الاتحاد الأوروبي على المستوى الوطني (هيئة الأمن القومي). وينعكس جانب معين من أنشطته في اعتماد تدابير تأمين المعلومات وتنسيق تنفيذ تلك التدابير في الهيئات الحكومية وغيرها من المؤسسات بغرض حماية المعلومات السرية. وفي هذا السياق، صدر في عام ٢٠١١ مرسوم التدابير الخاصة لحماية المعلومات السرية في نظم معلومات الاتصالات السلكية واللاسلكية (الجريدة الرسمية، رقم ٥٣/٢٠١١). وعلى الصعيد الدولي، يشارك مكتب مجلس الأمن القومي بنشاط، منذ عام ٢٠١١، في منتدى مديري هيئات الأمن القومي في جنوب شرق أوروبا. ويتمثل أحد الأهداف الرئيسية للمنتدى في تعزيز تأمين المعلومات وحماية المعلومات السرية في بلدان المنطقة، بما يتماشى مع المعايير الدولية. ويعمل مكتب مجلس الأمن القومي باعتباره المنسق الرئيسي

لتطوير مفهوم الدفاع عن الفضاء الإلكتروني للمنطقة في إطار هيئات الأمن القومي في جنوب شرق أوروبا.

وقام مكتب مجلس الأمن القومي بإعداد عدد من المقترحات ذات الصلة وإرسالها إلى الأعضاء الآخرين في الأفرقة العاملة المواضيعية لدراستها وتنسيقها وإقرارها. وهذه المقترحات مصنفة عن طريق وثيقتي العمل التاليتين: (١) أهداف برنامج الدفاع عن الفضاء الإلكتروني؛ (٢) استبيان الدفاع عن الفضاء الإلكتروني الموجه إلى هيئات الأمن القومي في جنوب شرق أوروبا.

وتشارك وزارة الدفاع في جمهورية صربيا في تنفيذ قرار الجمعية العامة ٢٤٣/٦٨. وتنشط إدارات وزارة الدفاع في الفريق العامل المكلف بصياغة قانون أمن المعلومات.

كما أن وزارة الدفاع تعكف على تشكيل إدارات مختلفة سوف تعمل في مجال أمن المعلومات والدفاع عن الفضاء الإلكتروني.

سويسرا

[الأصل: بالإنكليزية]

[٢٩ أيار/مايو ٢٠١٤]

ألف - التقييم العام لمسائل أمن المعلومات

أصبحت تكنولوجيات المعلومات والاتصالات قوة محركة لا غنى عنها للأنشطة الاجتماعية والاقتصادية والسياسية. وتلتزم سويسرا باغتنام الفرص التي يولدها استخدام تكنولوجيات المعلومات والاتصالات. وتأخذ سويسرا في الاعتبار التطورات والتحديات الجديدة فيما يتصل بتكنولوجيات المعلومات والاتصالات، وتشارك بنشاط في تشكيل مجتمع المعلومات عن طريق استراتيجية المجلس الاتحادي لمجتمع المعلومات في سويسرا.

غير أن استخدام تكنولوجيات المعلومات والاتصالات قد عرَّض البنية الأساسية للمعلومات والاتصالات لإساءة استغلالها لأغراض إجرامية أو استخباراتية أو سياسية - عسكرية أو إرهابية، فضلا عن الأعطال التي تعوق عملها. والاضطرابات والتلاعب والهجمات المحددة التي تتم عبر الشبكات الإلكترونية هي المخاطر التي ينطوي عليها مجتمع المعلومات. وفي ضوء هذه الخلفية، أصبحت الدول تشارك على نحو متزايد في سلسلة من مناقشات ومناظرات السياسات الإقليمية والدولية بشأن أمن الفضاء الإلكتروني.

وتتولد هذه المشاركة من شعور متزايد بعدم الأمن نظرا لنقاط الضعف في النظم الحاسوبية والتكنولوجيات المتصلة بها، وكيف يمكن استغلالها لأغراض خبيثة.

ورغم تسجيل وجود نقاط ضعف وتهديدات في هذه البيئة منذ الثمانينات من القرن الماضي، فإن التهديدات ونقاط الضعف الناجمة عن استخدام تكنولوجيات المعلومات والاتصالات لم تُدرج في جدول أعمال الأمن القومي إلا في السنوات السبع الماضية. ونتيجة لذلك، شكلت الحكومة الاتحادية السويسرية فريقا من الخبراء في عام ٢٠١٠ للتدقيق في المخاطر وزيادة القدرة الوطنية على التصدي لهذه التهديدات ونقاط الضعف.

ويتوقف عمل سويسرا كنظام كلي على عدد متزايد من مرافق المعلومات والاتصالات المترابطة بصورة متبادلة (الحواسيب والشبكات). وتعاني هذه البنية الأساسية من الضعف. إذ يمكن للأعطال أو الهجمات التي تشمل كامل نطاق البلد أو تمتد لفترات طويلة أن تحدث آثارا سلبية بالغة على الأداء التقني والاقتصادي والإداري لسويسرا. ويمكن إطلاق مثل هذه الهجمات من قبل مجموعة متنوعة من الفاعلين ولمجموعة متنوعة من الدوافع: فرادى الجناة، والناشطون السياسيون، والمنظمات الإجرامية الضالعة في أعمال الاحتيال أو الابتزاز، والإرهابيون أو جواسيس الدول، ممن يريدون تعطيل وزعزعة استقرار الدولة والمجتمع. وتكنولوجيات المعلومات والاتصالات مغرية بصفة خاصة كأهداف، ليس فقط لأنها تتيح الكثير من إمكانيات سوء الاستخدام والتلاعب والإضرار، ولكن أيضا لأنها يمكن أن تُستغل دون معرفة هوية الفاعلين، ودون كثير من المجهود. وتتمثل المصلحة الوطنية لسويسرا في حماية البنية الأساسية للمعلومات والاتصالات من هذه الاضطرابات والهجمات. وبهذا المعنى، فإننا نرحب بما خلص إليه فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي من أن القانون الدولي ينطبق على تكنولوجيات المعلومات والاتصالات.

باء - الجهود المبذولة على الصعيد الوطني لتعزيز أمن المعلومات وتشجيع التعاون الدولي في هذا الميدان

في ٢٧ حزيران/يونيه ٢٠١٢، اعتمدت الحكومة الاتحادية السويسرية الاستراتيجية الوطنية لحماية سويسرا من المخاطر الإلكترونية، بما وضع أساسا لنهج شامل ومتكامل وكلي لمعالجة المخاطر الإلكترونية. وتسعى الاستراتيجية إلى تحسين الرصد المبكر للمخاطر الإلكترونية والتهديدات الناشئة، وجعل البنية الأساسية السويسرية أكثر قدرة على التصدي للهجمات الإلكترونية، والحد من المخاطر الإلكترونية بوجه عام. وكان التركيز الرئيسي ينصب على الجريمة الإلكترونية وأعمال التجسس والتخريب. وكان المنطق الأساسي

للاستراتيجية ينبثق من الحاجة إلى ثقافة أمن الفضاء الإلكتروني، وتشاطر المسؤولية، وضرورة اتباع نهج قائم على الوقاية من المخاطر. وهي تدعو إلى تعزيز التنسيق على المستوى الحكومي، وتشجيع الشراكة بين القطاعين العام الخاص، وتعزيز التعاون على الساحة الدولية.

وتتألف الاستراتيجية من مجموعة تضم ١٦ تدبيرا ينبغي تنفيذها بحلول عام ٢٠١٧. ومن أجل ضمان تنفيذ هذه التدابير بصورة فعالة في الوقت المناسب، اعتمدت حكومة سويسرا في ١٥ أيار/مايو ٢٠١٣ خطة مفصلة لتنفيذ الاستراتيجية. كما أنشأت لجنة توجيهية، تُمثل فيها الوكالة الرائدة في تنفيذ كل تدابير بعينه. وكُلفت اللجنة التوجيهية بكفالة تنسيق تنفيذ هذه الاستراتيجية بشكل هادف. وتتراوح أدوارها ومسؤولياتها بين ضمان التنسيق بين الإدارات الاتحادية السويسرية[٢] ذات الصلة والوكالات ذات الصلة على المستوى المحلي. وعلى مستوى العمليات، أنشأت الحكومة وحدة تنسيق يُفترض أن تدعم عمل اللجنة التوجيهية.

وتتراوح مجموعة التدابير بين تحليل المخاطر ونقاط الضعف، وتحليل ساحة التهديد، والاستمرارية وإدارة الأزمات، وتدابير بناء الكفاءة إلى التعاون والمبادرات على الصعيد الدولي.

ويمكن تقسيم التدابير الـ ١٦ إلى أربعة مجالات رئيسية هي:

- الوقاية (أي تحليل المخاطر ونقاط الضعف وساحات التهديد)؛
- رد الفعل (أي التعامل مع الحادث، واتخاذ تدابير نشطة، وإنفاذ القانون)؛
- الاستمرارية (أي الاستمرارية وإدارة الأزمات)؛
- دعم العمليات (أي التعاون الدولي، والتعليم والبحوث، والمؤسسات القانونية، وما إلى ذلك).

جيم - مضمون المفاهيم المذكورة في الفقرة ٢ من قرار الجمعية العامة ٦٨/٢٤٣

التعاون الدولي هو واحد من مجالات العمل التي تحتاج إلى التعزيز عن طريق الاستراتيجية الوطنية السويسرية للفضاء الإلكتروني. وبالتالي، فقد عقدت سويسرا العزم على التعاون على مستوى السياسات الأمنية الدولية، وذلك لمواجهة التهديدات في الفضاء الإلكتروني جنبا إلى جنب مع الدول الأخرى والمنظمات الدولية. وتلتزم سويسرا بمراقبة

(٢) تعادل الوزارات.

التطورات وتشكيلها على الصعيد الدبلوماسي، وتشجيع أشكال التبادل السياسي في إطار المؤتمرات الدولية والمبادرات الدبلوماسية الأخرى.

وفي ضوء هذه الخلفية، تشارك سويسرا في مختلف العمليات الدولية الرامية إلى تطوير آليات عالمية. وقد اعتمدت منظمة الأمن والتعاون في أوروبا تدابير لبناء الثقة في مجال أمن الفضاء الإلكتروني. وترى سويسرا أن هذه العملية تتسم بأهمية قصوى. وبالتالي، ستركز سويسرا، من خلال انتهاج ''مسار مزدوج''، على تنفيذ أول مجموعة من تدابير بناء الثقة، فضلا عن تطوير المزيد من التدابير. وبالإضافة إلى ذلك، تشكل ''خطة لندن'' عملية هامة أخرى تشارك فيها سويسرا. وأخيرا، فإن سويسرا، بوصفها من غير الأعضاء في فريق الخبراء الحكوميين، تهتم بالتقارير الصادرة عن هذا الفريق. وإننا نؤيد، في هذا الصدد، بصفة خاصة طلب مواصلة دراسة عدة أمور، من بينها الطريقة التي ينطبق بها القانون الدولي، بما في ذلك ميثاق الأمم المتحدة وقانون حقوق الإنسان والقانون الإنساني الدولي، على استخدام تكنولوجيات المعلومات والاتصالات.

وعلى الصعيد الثنائي، تجري سويسرا مشاورات سياسية منتظمة مع البلدان بشأن المسائل المتصلة بالفضاء الإلكتروني.

وسويسرا من البلدان الموقعة على اتفاقية مجلس أوروبا بشأن الجريمة الإلكترونية، التي دخلت حيز النفاذ في ١ كانون الثاني/يناير ٢٠١٢.

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

من المقرر أن يجري التركيز المبادرات والتدابير الرامية إلى زيادة الثقة وتحسين التفاهم وبناء الثقة بين الدول. وعلى المستوى الثنائي، أثبتت حوارات المسارات رقم ١ و ١,٥ و ٢ بين الدول وغيرها من أصحاب المصلحة المعنيين حول قضايا أمن الفضاء الإلكتروني أنها حوارات مثمرة. أما الحوارات في مجال أمن الفضاء الإلكتروني، فتحتاج إلى مزيد من التطوير والتعزيز.

ويمكن تعزيز أمن المعلومات على المستوى العالمي عن طريق إنشاء آليات مشتركة لتجنب التصعيد الذي يصل إلى حد النزاع المسلح. وبالتالي، يمكن إنشاء خطوط اتصال مباشر على المستويين التقني والسياسي على حد سواء. فمن خلال الحفاظ على اتصالات منتظمة على أعلى مستوى، سيكون من الممكن تحسين الأمن في الفضاء الإلكتروني.

المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية

[الأصل: بالإنكليزية]

[٢٩ حزيران/يونيه ٢٠١٤]

موجز تنفيذي

ترحب المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية بهذه الفرصة للرد على قرار الجمعية العامة ٢٤٣/٦٨ المعنون ''التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي''، وهو الرد الذي يستفيد من ردها على القرار ٢٧/٦٧ في عام ٢٠١٣. وتستخدم المملكة المتحدة مصطلح ''أمن الفضاء الإلكتروني'' المفضل لديها، وكذلك المفاهيم ذات الصلة، في جميع أجزاء ردها لتجنب الارتباك، نظرا لاختلاف تفسيرات مصطلح ''أمن المعلومات'' في هذا السياق.

وتسلم المملكة المتحدة بأن الفضاء الإلكتروني عنصر أساسي من عناصر البنية الأساسية الحيوية على الصعيدين الوطني والدولي وركيزة أساسية من ركائز النشاط الاقتصادي والاجتماعي من خلال شبكة الإنترنت. وتُعد التهديدات الفعلية والمحتملة التي تشكلها الأنشطة في الفضاء الإلكتروني مصدر قلق بالغ. ويعرض ردنا تفاصيل النُهج الوطنية والدولية التي اتخذت، وستُتخذ، من أجل تعزيز الأمن وتشجيع التعاون في هذا الميدان. وقد تعززت هذه النُهج بفضل الاستراتيجية الوطنية لأمن الفضاء الإلكتروني في المملكة المتحدة، التي نُشرت في تشرين الثاني/نوفمبر ٢٠١١.

وقد شاركت المملكة المتحدة بنشاط وبروح بناءة في الحوار الدولي حول أمن الفضاء الإلكتروني. ونشارك بخبراء في جميع أفرقة الخبراء الحكوميين الثلاثة، ونرحب بالتقرير الذي توافقت عليه آراء الفريق الأخير، والذي يحرز تقدما قيِّما في التوصل إلى تفاهمات مشتركة بشأن قواعد سلوك الدول في الفضاء الإلكتروني، ويؤكد انطباق القانون الدولي على الفضاء الإلكتروني. وترحب المملكة المتحدة أيضا باعتماد أول مجموعة من تدابير بناء الثقة على الصعيد الإقليمي بشأن الفضاء الإلكتروني التي تم التفاوض بشأنها بنجاح في منظمة الأمن والتعاون في أوروبا. ويعرض الرد جهود المملكة المتحدة في تقاسم أفضل الممارسات في أنحاء العالم، سواء من خلال العمل مع الشركاء الدوليين لمعالجة الجرائم الإلكترونية والحوادث الكبرى، ومن خلال التزامها ببناء قدرات وطاقات الفضاء الإلكتروني.

وتتطلع المملكة المتحدة إلى رؤية المزيد من التقدم في جميع هذه المجالات. ويشمل ذلك فريق الخبراء الحكوميين المقبل، وتنفيذ تدابير بناء الثقة في منظمة الأمن والتعاون في

أوروبا، وتطوير المزيد من تدابير بناء الثقة فيها وفي المجموعات الإقليمية الأخرى، وإنشاء فرق الاستجابة للطوارئ الحاسوبية وزيادة التعاون فيما بينها، وتعزيز التعاون لإنفاذ القانون في مجال الجرائم الإلكترونية، وتشجيع نهج أصحاب المصلحة المتعددين.

ويسر المملكة المتحدة أن تشارك بنشاط في هذه المسائل الهامة، وهي تتطلع إلى مواصلة مشاركتها في تعزيز القدرات والتعاون الدولي في مجال أمن الفضاء الإلكتروني.

ويمكن الاطلاع على النص الكامل للعرض الذي قدمته المملكة المتحدة من خلال الموقع الشبكي: http://www.un.org/disarmament/topics/informationsecurity/.