الأمم المتحدة

A/71/172

الجمعية العامة

Distr.: General
19 July 2016
Arabic
Original: Arabic/English/French/
Russian/Spanish

الدورة الحادية والسبعون
البند ٩٤ من جدول الأعمال المؤقت*

التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي

تقرير الأمين العام

المحتويات

الصفحة

أولا – مقدمة ٣
ثانيا – الردود الواردة من الحكومات ٣
ألبانيا ٣
أستراليا ٥
كندا ٦
كولومبيا ٨
كوبا ١٠
السلفادور ١٢

* A/71/150.

150816 110816 16-12486 (A)

فنلندا ١٢
الهند ١٤
اليابان ١٥
الأردن ١٦
لبنان ٢٠
بولندا ٢٢
البرتغال ٢٤
صربيا ٢٥
إسبانيا ٢٧
سويسرا ٢٨
توغو ٣٠
تركمانستان ٣١
المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية ٣٣

أولا - مقدمة

١ - اتخذت الجمعية العامة، في ٢٣ كانون الأول/ديسمبر ٢٠١٥، القرار ٧٠/٢٣٧ المعنون ”التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي“. وفي الفقرة ٤ من القرار، دعت الجمعية العامة 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/70/174)، 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 ٣ من القرار؛

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

٢ - واستجابة لذلك الطلب، تم توجيه مذكرة شفوية في ١٥ شباط/فبراير ٢٠١٥ إلى جميع الدول الأعضاء لدعوتها إلى تقديم معلومات عن الموضوع. ويتضمن الفرع الثاني الردود التي وردت إبّان كتابة هذا التقرير. وستصدر الردود التي تَرِدُ لاحقا في شكل إضافات لهذا التقرير. ويمكن الاطلاع على النص الكامل لجميع العروض في الموقع: www.un.org/disarmament/topics/informationsecurity.

ثانياً - الردود الواردة من الحكومات

ألبانيا

[الأصل: بالإنكليزية]
[١٥ نيسان/أبريل ٢٠١٦]

تتمثل الأولوية الرئيسية بالنسبة إلى ألبانيا في مجال الأمن وحماية المعلومات السرية في توقيع الاتفاق المبرم بين حكومة جمهورية ألبانيا والاتحاد الأوروبي - الاتفاق المتعلق بالإجراءات الأمنية لتبادل وحماية المعلومات السرية. وقد تم توقيع الاتفاق المذكور أعلاه في ٣ آذار/مارس ٢٠١٦ في تيرانا، ومن المتوقع أن يصدِّق عليه برلمان جمهورية ألبانيا في الوقت المحدد.

وفي سياق بدء وتنفيذ التدابير المناسبة في ألبانيا، جرت مراجعة النظم القانونية التالية من أجل تعزيز أمن المعلومات وتشجيع التعاون الدولي في هذا الشأن:

- قرار مجلس الوزراء رقم ١٨٨، المؤرخ ٤ آذار/مارس ٢٠١٥، بشأن ''الموافقة على قواعد تكفل أمن الموظفين''
- قرار مجلس الوزراء رقم ١٨٩، المؤرخ ٤ آذار/مارس ٢٠١٥، بشأن ''كفالة الأمن المادي للمعلومات السرية التي تعتبر من 'أسرار الدولة' ومعلومات منظمة حلف شمال الأطلسي''
- قرار مجلس الوزراء رقم ١٩٠، المؤرخ ٤ آذار/مارس ٢٠١٥، ''الذي ينص على إدخال عدة تعديلات وإضافات على قرار مجلس الوزراء رقم ٨١، بشأن 'تحديد معايير وإجراءات تدمير المعلومات السرية'''
- قرار مجلس الوزراء رقم ٧٠١، المؤرخ ٢٢ تشرين الأول/أكتوبر ٢٠١٤، بشأن ''الموافقة على قواعد تأمين المعلومات السرية في الميدان الصناعي''

ولدى ألبانيا نظام قانوني أشمل يعنى بالأمن المادي للمعلومات السرية. ويعاد تحديد ''مجالات الأمن'' والوقوف عليها، مع مراعاة المستويات المختلفة لسرية المعلومات.

وعلى إثر اتخاذ القرار الجديد المتعلق بأمن الموظفين، فقد ازداد في نهاية المطاف التعاون فيما بين المؤسسات والإشراف على المؤسسات الحكومية ومراقبتها. وبدأت الوكالات الحكومية عملية تنقيح قوائم مهام الموظفين وإصدار شهادات الأمن ذات الصلة وفقا لمجالات المسؤولية.

وفيما يتعلق بالأمن الصناعي، تركز ألبانيا على استعراض سياسة أمن المعلومات، عن طريق استعراض ممارسات مجلس الوزراء بموجب القرار رقم ٧٠١، المؤرخ ٢٢ تشرين الأول/أكتوبر ٢٠١٤.

ومن الخطوات الهامة الأخرى التي ركزنا عليها صياغة قانون جديد للتعامل مع المعلومات السرية – وهي مبادرة تنطوي على قانون حديث يتسم بالكفاءة ويستخدم المعايير الأوروبية الرفيعة. ويتم استعراض التشريعات الوطنية في هذا الميدان في ظل مراعاة تشريعات الاتحاد الأوروبي، ولا سيما قرار المجلس 2013/488/EU بشأن القواعد الأمنية لحماية المعلومات السرية في الاتحاد الأوروبي.

أستراليا

[الأصل: بالإنكليزية]
[٣١ أيار/مايو ٢٠١٦]

ترحب أستراليا بهذه الفرصة لكي تلبي الدعوة الواردة في قرار الجمعية العامة ٧٠/٢٣٧، فتعرض آراءها بشأن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي. ويستند هذا التقرير إلى المعلومات التي قدمتها أستراليا في عام ٢٠١٤ استجابة للقرار ٦٨/٢٤٣، والمعلومات التي قدمتها في عام ٢٠١١ استجابة للقرار ٦٥/٤١.

ويرتبط أمن الفضاء الإلكتروني ارتباطا جوهريا بالابتكار بقدر ما يرتبط بالأمن القومي. فهو الأساس الذي يقوم عليه الابتكار والنمو والازدهار. ويشكل أمن الفضاء الإلكتروني فرصة عالمية تستثمر فيها جميع الحكومات ومكونات القطاع الخاص والمجتمعات المحلية، ويمكن لهذه الجهات كلها أن تجني فوائد منه.

ويتعين على المجتمع العالمي أن يتناول أمن الفضاء الإلكتروني بالطريقة الصحيحة. وينبغي أن تتضافر جهود الجميع – الحكومات والمؤسسات التجارية والأفراد – لتهيئة بيئة جديرة بالثقة على شبكة الإنترنت. ولا يقتصر الغرض من ذلك على حماية المعلومات الحيوية، بل يمتد إلى توفير بيئة يزدهر فيها الابتكار؛ وتمكين قطاع التكنولوجيا من الازدهار؛ والاستفادة من الحاجة المتنامية على الصعيد العالمي إلى التوصل إلى حلول أفضل في مجال أمن الفضاء الإلكتروني وإلى الحصول على المعدات والمهارات اللازمة.

وتدرك أستراليا بأن قوة أمن الفضاء الإلكتروني تشكل عنصرا أساسيا من عناصر النمو والازدهار في ظل الاقتصاد العالمي. ففي عام ٢٠١٥، قامت أستراليا باستعراض نهجها إزاء أمن الفضاء الإلكتروني وشرعت في تنفيذ استراتيجيتها الجديدة في مجال أمن الفضاء الإلكتروني في ٢١ نيسان/أبريل ٢٠١٦.

وترى أستراليا أن من المهام ذات الأولوية التي يتعين على المجتمع الدولي القيام بها توضيح كيفية انطباق القانون الدولي على سلوك الدول في الفضاء الإلكتروني، ولا سيما في غير حالات النزاع. وثمة حاجة إلى مزيد من العمل للتوصل إلى أوجه تفاهم بشأن كيفية انطباق مفاهيم رئيسية من قبيل السيادة والولاية القضائية في الفضاء الإلكتروني، مع مراعاة مصلحتنا المشتركة في الحفاظ على الطابع العالمي للإنترنت. وثمة مجال لمواصلة وضع القواعد الطوعية المبينة في تقرير عام ٢٠١٥ الصادر عن فريق الخبراء الحكوميين في ما يتعلق بحماية

الهياكل الأساسية الحيوية، وأفرقة التصدي للطوارئ الحاسوبية، ومسؤولية الدول عن المساعدة والتعاون فيما يخص جرائم الفضاء الإلكتروني، ومنع انتشار الأدوات والتقنيات الحاسوبية الخبيثة. ومن المهم أن ينتقل العمل بشأن تدابير بناء الثقة إلى المرحلة التالية، ابتداء من تعزيز الشفافية وانتهاء عند تنفيذ التدابير التعاونية.

كندا

[الأصل: بالإنكليزية]
[٢٧ أيار/مايو ٢٠١٦]

فيما يتعلق بمسائل الفضاء الإلكتروني، ترى كندا ما يلي:

- يؤدي إنشاء فضاء إلكتروني آمن وحر ومفتوح دورا حاسما في تحقيق الأمن العالمي والازدهار الاقتصادي وتعزيز حقوق الإنسان والديمقراطية والإدماج.
- يجب أن يقترن أي نهج إزاء التصدي للتهديدات الواقعة في الفضاء الإلكتروني باحترام حقوق الإنسان والحريات الأساسية.
- ينطبق القانون الدولي الحالي على استخدام الدول لتكنولوجيا المعلومات والاتصالات.
- يساعد تعزيز المعايير التي تحكم السلوك في أوقات السلم على الحفاظ على بيئة تسترشد فيها الدول في تصرفاتها بمبادئ السلوك المسؤول، كما يدعم الشراكات ويساعد على استقرار الفضاء الإلكتروني.
- تشكل التدابير العملية لبناء الثقة طريقة من الطرق التي ثبتت فعاليتها في مجال التخفيف من حدة التوترات ومن خطر نشوب النزاعات المسلحة.

وعلى الصعيد الوطني، منذ أن أصدرت الحكومة الكندية استراتيجيتها لأمن الفضاء الإلكتروني في عام ٢٠١٠، واصلت الجهود المبذولة للمساعدة على تأمين النظم الإلكترونية لكندا وحماية الكنديين على شبكة الإنترنت. ومنذ ذلك الحين، أطلقت كندا أيضا حملة لتوعية الجمهور تحت عنوان ”كن في مأمن من مخاطر الفضاء الإلكتروني“. وفي الآونة الأخيرة، التزمت الحكومة بإجراء استعراض للتدابير القائمة لحماية الكنديين والهياكل الأساسية الحيوية في كندا من التهديدات الإلكترونية.

وعلى الصعيد الدولي، تنشط كندا بطرق عدة فيما يتصل بمسائل الفضاء الإلكتروني:

- سوف تواصل كندا تعزيز عملية تطوير المعايير التي تحكم سلوك الدول في الفضاء الإلكتروني في أوقات السلم، بما في ذلك النتائج التي خلص إليها فريق الخبراء الحكوميين التابع للأمم المتحدة في الفترتين ٢٠١٢-٢٠١٣ و ٢٠١٤-٢٠١٥. وقد وقع الاختيار على كندا للمشاركة في الفريق للفترة ٢٠١٥-٢٠١٦.

- صدَّقت كندا على اتفاقية بودابست في تموز/يوليه ٢٠١٥. وتشجع كندا البلدان على أن تصبح أطرافا في الاتفاقية، أو أن تتخذها نموذجا لتنفيذ قوانينها الخاصة بجرائم الفضاء الإلكتروني.

- منذ عام ٢٠٠٧، تعهدت كندا بمبلغ ٨,٢٥ ملايين دولار لدعم مشاريع بناء القدرات في مجال أمن الفضاء الإلكتروني في الأمريكتين وجنوب شرق آسيا.

- كندا من الشركاء المؤسسين للمنتدى العالمي لخبرات الفضاء الإلكتروني.

- تتعاون كندا مع الولايات المتحدة من أجل مواءمة المبادرات الكندية فيما يتصل بحملة توعية الجمهور بمسائل أمن الفضاء الإلكتروني عن طريق الائتلاف المعنون ”توقف - فكِّر - تواصَل“.

- تتعاون كندا أيضا مع الولايات المتحدة من أجل تنفيذ خطة عمل أمن الفضاء الإلكتروني المشتركة بين كندا والولايات المتحدة، والتي تهدف إلى تعزيز قدرة الهياكل الأساسية للفضاء الإلكتروني الكندي على الصمود.

- دأبت كندا على وضع تدابير لبناء الثقة في مختلف المحافل، بما فيها منظمة الأمن والتعاون في أوروبا والمنتدى الإقليمي لرابطة أمم جنوب شرق آسيا.

- تدعم كندا ما تبذله منظمة حلف شمال الأطلسي (الناتو) من جهود في سبيل تعزيز قدرة التحالف وكذلك فرادى الحلفاء على الدفاع عن الفضاء الإلكتروني. وساهمت كندا بمبلغ مليون دولار في مركز الامتياز المعني بالدفاع عن الفضاء الإلكتروني التعاوني التابع للناتو.

- تؤيد كندا استخدام تكنولوجيا المعلومات والاتصالات كأدوات للتنمية، لأغراض منها مساعدة المنظمات المجتمعية على تقديم الخدمات الأساسية من قبيل المساعدة في حالات الطوارئ عند نشوب النزاعات.

- يساعد مركز بحوث التنمية الدولية التابع لكندا على النهوض بالتنمية في جميع أنحاء العالم بتسخير تكنولوجيا المعلومات والاتصالات لأغراض بحوث التنمية وبناء القدرات.

كولومبيا

[الأصل: بالإسبانية]
[١٣ حزيران/يونيه ٢٠١٦]

حققت كولومبيا بفضل خطتها الرقمية ''Vive Digital'' (٢٠١٠-٢٠١٤) وخطتها الرقمية الجديدة ''Live Digital - for the people'' (٢٠١٤-٢٠١٨) ثورةً رقميةً، حيث قامت بزيادة مجموع حالات الربط بشبكة الإنترنت لديها من ٢,٢ مليون حالة إلى أكثر من ١٢,٢ مليون حالة على مدى خمس سنوات فقط. وستكون كولومبيا أول بلد في أمريكا اللاتينية يتميز بإمكانية الربط بشبكة الإنترنت بسرعة فائقة في جميع البلديات. وخلال الفترة نفسها، تم تزويد المؤسسات التعليمية بأكثر من مليوني محطة طرفية؛ وباتت نسبة ٧٤ في المائة من المشاريع المتناهية الصغر والصغيرة والمتوسطة الحجم موصولة الآن بالإنترنت (بالمقارنة مع ٧ في المائة في عام ٢٠١٠)؛ وقد حققنا نموا بنسبة ٩٠ في المائة في عدد الأسر المعيشية الموصولة بشبكة الإنترنت؛ وقمنا بإيصال شبكة الإنترنت إلى أكثر المناطق الريفية انعزالا عن طريق ٦٢١ ٧ من الأكشاك التي أقيمت في إطار الخطة الرقمية ''Vive Digital'' (الموجودة في المراكز الريفية التي يقيم بها أكثر من ١٠٠ نسمة). ومن بين الإنجازات الأخرى العديدة، لدينا أيضا أكبر جماعة من منظمي المشاريع الرقمية في أمريكا اللاتينية، تضم أكثر من ٠٠٠ ١٠٠ عضو.

وتدرك الحكومة الوطنية أن من غير الممكن تعظيم فوائد تكنولوجيا المعلومات والاتصالات واستخدامها إذا لم يكن المواطنون أو أصحاب الشركات يثقون بها، وبعبارة أخرى، إذا كان هناك نقص متصور في أمن البيئة الرقمية. ولتزايد عدد الحوادث الأمنية الرقمية تأثير متزايد على هذه التصورات.

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

لقد شرعت كولومبيا للتو في تنفيذ سياسة وطنية جديدة في مجال الأمن الرقمي، وهي السياسة الواردة في الوثيقة CONPES 3854 لعام ٢٠١٦، والتي تسعى إلى التأكد من أن الحكومة والمنظمات العامة والخاصة وموظفي إنفاذ القانون والأوساط الأكاديمية والأفراد بشكل عام في كولومبيا بإمكانهم الاعتماد على بيئة رقمية آمنة وموثوقة تؤدي إلى تعظيم المزايا الاقتصادية والاجتماعية وتعزيز القدرة التنافسية والإنتاجية في جميع قطاعات الاقتصاد. وهذه السياسة هي نتاج عملية شارك فيها العديد من أصحاب المصلحة،

وهي إحدى السياسات الوطنية الأولى في العالم – والأولى في المنطقة – التي تضمنت التوصيات المتعلقة بإدارة المخاطر الأمنية الرقمية الصادرة في أيلول/سبتمبر ٢٠١٥ عن منظمة التعاون والتنمية في الميدان الاقتصادي.

وتنص هذه السياسة، أولا وقبل كل شيء، على إنشاء إطار مؤسسي واضح للأمن الرقمي. ولهذه الغاية، سوف تنشأ هيئات للتنسيق وتقديم المشورة في مجال الأمن الرقمي على أرفع المستويات الحكومية، وسوف تقام وحدات للاتصال مشتركة بين القطاعات في جميع الوكالات التابعة للسلطة التنفيذية الوطنية. ثانيا، ستهيأ الظروف المناسبة لتمكين أصحاب المصلحة المتعددين من إدارة المخاطر التي تهدد الأمن الرقمي في أنشطتهم الاجتماعية والاقتصادية، ولبعث الثقة في استخدام البيئة الرقمية، من خلال وضع آليات المشاركة المستمرة الفعالة، وكفالة الإطار القانوني والتنظيمي الملائم، وتوفير التدريب في مجال السلوك المسؤول في البيئة الرقمية. ثالثا، سيتم تعزيز الدفاع والأمن الوطنيين في البيئة الرقمية على الصعيدين الوطني وعبر الوطني، باعتماد نهج لإدارة المخاطر. وأخيرا، وليس آخرا، سيتم إنشاء آليات دائمة، مع التركيز على البعد الاستراتيجي، من أجل تعزيز التعاون والمساعدة في مجال الأمن الرقمي على الصعيدين الوطني والدولي.

(ب) مضمون المفاهيم المذكورة في الفقرة ٣ من القرار ٧٠/٢٣٧:

إن كولومبيا، بصفتها عضوا في أحدث فريق للخبراء الحكوميين (٢٠١٤-٢٠١٥)، توافق تماما على ضرورة مواصلة دراسة المفاهيم المتصلة بأمن المعلومات ونظم الاتصالات السلكية واللاسلكية العالمية والمسائل المتصلة بتطبيق القانون الدولي في الفضاء الإلكتروني.

(ج) التدابير التي يمكن أن يتخذها المجتمع الدولي لتعزيز أمن المعلومات على الصعيد العالمي:

اتساقا مع ما سبق، فإننا نؤيد تماما التوصيات الهامة الصادرة بتوافق الآراء عن الخبراء الذين كانوا أعضاء في فريق الخبراء الحكوميين، بما في ذلك ما يتعلق بالاعتماد الطوعي للتدابير والممارسات الجيدة، فضلا عن بناء القدرات والتعاون الذي تبذله الدول من أجل تعزيز الاستخدام السلمي لتكنولوجيا المعلومات والاتصالات، كي تظل بمثابة أدوات للتنمية الاقتصادية والاجتماعية للبلدان، لا سيما أقل البلدان تقدما من الناحية التكنولوجية.

كوبا

[الأصل: بالإسبانية]
[٦ أيار/مايو ٢٠١٦]

تشاطر كوبا الجمعية العامة قلقها المعرب عنه في القرار ٧٠/٢٣٧ من احتمال استخدام تكنولوجيا المعلومات ووسائلها في أغراض لا تتفق مع أهداف صون الاستقرار والأمن الدوليين وقد تؤثر تأثيرا سلبيا في سلامة الهياكل الأساسية للدول مما يضر بأمنها في الميدانين المدني والعسكري على السواء.

ويشدد القرار ٧٠/٢٣٧ أيضا بصورة ملائمة على ضرورة منع استخدام مصادر أو تكنولوجيات المعلومات في تحقيق أغراض إجرامية أو إرهابية.

وفي هذا الصدد، تكرر كوبا الإعراب عن بالغ قلقها من قيام أفرادٍ ومنظماتٍ ودولٍ باستخدام النظم المعلوماتية الموجودة في بلدانٍ أخرى، على نحو سري وغير مشروع، بغرض مهاجمة بلدان ثالثة لأن ذلك قد يتسبب بنشوب نزاعات دولية.

ولا سبيل إلى درء هذه التهديدات ومواجهتها وتفادي تحويل الفضاء الإلكتروني إلى مسرح للعمليات العسكرية سوى التعاون المشترك بين جميع الدول.

ويشكل استخدام الاتصالات السلكية واللاسلكية لتحقيق مآرب معلنة أو خفيّة تتمثل في تقويض النظام القانوني والسياسي للدول انتهاكا للقواعد الدولية المعترف بها في هذا المجال، وقد يؤدي إلى نشوء توترات وأوضاع يحتمل أن تضر بالسلام والأمن الدوليين.

وخلال مؤتمر القمة الثاني لجماعة دول أمريكا اللاتينية ومنطقة البحر الكاريبي المعقود في هافانا في كانون الثاني/يناير ٢٠١٤، قام رؤساء دول وحكومات أمريكا اللاتينية ومنطقة البحر الكاريبي بإعلان منطقة أمريكا اللاتينية والبحر الكاريبي منطقةَ سلام، تحقيقاً لأهداف منها دعم التعاون والعلاقات الودية مع بعضها بعضا ومع الدول الأخرى، بصرف النظر عن اختلاف نُظمها السياسية والاقتصادية والاجتماعية أو تباين مستويات تنميتها، وانتهاج التسامح والتعايش في جو من السلام وحُسن الجوار.

وفي مؤتمر القمة الرابع للجماعة، الذي عقد في كيتو في كانون الثاني/يناير ٢٠١٦، تم مجددا إبراز أهمية تكنولوجيا المعلومات والاتصالات، بما في ذلك شبكة الإنترنت، بوصفها أدوات لتعزيز السلام ورفاه الإنسان والتنمية والمعرفة والإدماج الاجتماعي والنمو الاقتصادي. وجرى التأكيد أيضا على الاستخدام السلمي لتكنولوجيا المعلومات

والاتصالات على نحو يتماشى مع مقاصد ميثاق الأمم المتحدة ومبادئه ومع القانون الدولي، وتم التشديد على أن هذه التكنولوجيا ينبغي ألا تُستخدم أبدا بهدف تقويض المجتمعات أو خلق أوضاع قد تؤدي إلى تأجيج النزاعات بين الدول.

غير أن البرامج الإذاعية والتلفزيونية التي دأبت حكومة الولايات المتحدة على بثّها تجاه كوبا لا تزال تهدد هذه المساعي، إذ تتعارض مع مقاصد ميثاق الأمم المتحدة ومبادئه وتتنافى مع شتى الأنظمة الصادرة عن الاتحاد الدولي للاتصالات، كما أنها تشكل انتهاكا لسيادة كوبا.

ودأبت الولايات المتحدة، من خلال برامج إذاعية وتلفزيونية غير مشروعة، على مهاجمة موجات الأثير الكوبية، وذلك ببث برامج مصممة خصيصا للتحريض على الإطاحة بالنظام الدستوري الذي أنشأه الشعب الكوبي. وكمثال على ذلك، فقد تم بث برامج غير مشروعة مناوئة لكوبا بمتوسط ٨٨٠ ١ ساعة في الأسبوع، باستخدام ٢٣ ترددا في الربع الأول من عام ٢٠١٦ فقط.

وتأمل كوبا أن تتوقف هذه السياسات العدوانية فوراً، على أن هذه السياسات تتنافى أيضا مع إقامة علاقات على أساس الاحترام المتبادل والتعاون بين كوبا والولايات المتحدة، على نحو ما اتفقت عليه الحكومتان عند قيامهما باستئناف العلاقات الدبلوماسية بينهما.

وتعرب عن أملها أيضا في أن يُرفع الحصار الاقتصادي والتجاري والمالي، الذي تسبب في أضرار بالغة للشعب الكوبي. وقد كان للحصار أثر ضار في مجال المعلومات والاتصالات، من جملة جوانب أخرى من جوانب الحياة اليومية للشعب الكوبي.

والتعاون الدولي أمر أساسي لمواجهة المخاطر المرتبطة بسوء استخدام تكنولوجيا المعلومات والاتصالات. ويتعين على الاتحاد الدولي للاتصالات أن يقوم بدور هام في المناقشة الحكومية الدولية لمسائل أمن الفضاء الإلكتروني.

وقد أيدت كوبا القرار ٢٣٧/٧٠، وسوف تواصل إسهامها في التطوير السلمي لتكنولوجيا المعلومات والاتصالات على الصعيد العالمي واستخدامها بما يعود بالنفع على الإنسانية جمعاء.

السلفادور

[الأصل: بالإسبانية]
[٢٦ نيسان/أبريل ٢٠١٦]

لقد قامت القوات المسلحة للسلفادور بتطوير المعدات الحاسوبية لأمن المنطقة المحيطة بها، وبتنفيذ السياسات الأمنية التي تنظم إمكانية الوصول إلى موارد الشبكات الحاسوبية (تغيير كلمات سر المستعملين بانتظام، وتقييد إمكانية الوصول إلى منافذ USB وأجهزة قراءة أقراص الفيديو الرقمية والأقراص المضغوطة، ومنع الوصول إلى وحدة المعدات جيم.

فنلندا

[الأصل: بالإنكليزية]
[٣١ أيار/مايو ٢٠١٦]

ترحب فنلندا بفرصة تقديم معلومات فيما يتعلق بقرار الجمعية العامة ٧٠/٢٣٧. وقد بُذلت الجهود التالية على الصعيد الوطني:

(أ) تحدد الاستراتيجية الوطنية لأمن الفضاء الإلكتروني في فنلندا (٢٠١٣) وبرنامج تنفيذها (٢٠١٤) المبادئ التوجيهية والإجراءات الرئيسية في مجال تعزيز أمن الفضاء الإلكتروني وقدرته على الصمود. ويجري تحديث برنامج التنفيذ من خلال عملية تشاورية مع أصحاب المصلحة المتعددين بهدف وضعه في صيغته النهائية في عام ٢٠١٦.

(ب) منذ اعتماد الاستراتيجية الوطنية لأمن الفضاء الإلكتروني، أنشأت فنلندا المركز الوطني لأمن الفضاء الإلكتروني ومركز منع جرائم الفضاء الإلكتروني، كما جرى تعيين سفير لشؤون الفضاء الإلكتروني. واعتُمدت الاستراتيجية الوطنية لأمن المعلومات في شباط/فبراير ٢٠١٦.

(ج) في إطار التعاون الإنمائي في فنلندا، تدعم فنلندا تسخير مختلف تكنولوجيات المعلومات والاتصالات لأغراض مشاريع التنمية وبناء القدرات فيما يتعلق بالفضاء الإلكتروني. وفنلندا من الشركاء المؤسسين للمنتدى العالمي لخبرات الفضاء الإلكتروني. وقد انضمت فنلندا إلى مبادرة الربط العالمية التي تقودها الولايات المتحدة، والتي تسعى إلى ربط ١,٥ بليون شخص بشبكة الإنترنت بحلول عام ٢٠٢٠. وتسعى فنلندا إلى الانضمام

إلى الصندوق الاستئماني الجديد للشراكة من أجل التنمية الرقمية التي أقامها البنك الدولي. وتؤيد فنلندا إدارة شبكة الإنترنت استنادا إلى نموذج يقوم على تعدد أصحاب المصلحة.

(د) تشارك فنلندا بنشاط في الحوار الدولي بشأن مسائل الفضاء الإلكتروني في المحافل المتعددة الأطراف والإقليمية، وفي سياق الاتصالات الثنائية. وفي إطار منظمة الأمن والتعاون في أوروبا، تعمل فنلندا على تعزيز الثقة والأمن والاستقرار في الفضاء الإلكتروني، وتقوم بتنفيذ التدابير المتفق عليها في مجال بناء الثقة والأمن في الفضاء الإلكتروني.

(هـ) تؤيد فنلندا تقرير عام ٢٠١٥ الصادر عن فريق الأمم المتحدة للخبراء الحكوميين في مجال تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي. وقد شاركت فنلندا بنشاط في المناقشات الدائرة بشأن القانون الدولي في الفضاء الإلكتروني، ومثال ذلك المشاورات المتعلقة بالإصدار ٢,٠ لدليل تالين، كما شاركت في حلقات عمل نظمها معهد الأمم المتحدة لبحوث نزع السلاح. وانضمت فنلندا إلى تحالف الحرية على شبكة الإنترنت في عام ٢٠١٢، وهي تساهم في شراكة المدافعين عن الحرية الرقمية.

(و) فنلندا طرف في اتفاقية بودابست منذ عام ٢٠٠٧. وقد شُرع في عام ٢٠١٥ في تنفيذ الخطة الاستراتيجية الجديدة للشرطة، التي تستهدف تخصيص الموارد لمنع الجريمة الإلكترونية وتطوير الدراية في مجال أمن الفضاء الإلكتروني. وهناك أيضا خطة شاملة لمنع جرائم الفضاء الإلكتروني.

المجالات ذات الأولوية التي تستلزم مزيدا من العمل من جانب المجتمع الدولي:

(أ) تعلق فنلندا قدرا كبيرا من الأهمية على عمل فريق الخبراء الحكوميين الجديد، وهي مستعدة للمساهمة في نجاحه، لأغراض منها مواصلة تحديد قواعد السلوك المسؤول للدول في الفضاء الإلكتروني مع التركيز بصفة خاصة على الأنشطة المضطلع بها في وقت السلم؛

(ب) مواصلة وضع وتنفيذ تدابير بناء الثقة على الصعيد الإقليمي في إطار منظمة الأمن والتعاون في أوروبا؛

(ج) مواصلة دعم بناء القدرات الإلكترونية بهدف تعزيز القدرة على الصمود والأمن في الفضاء الإلكتروني؛

(د) ستواصل فنلندا دعم وتشجيع الحوار بين أصحاب المصلحة المتعددين. ويشكل تعزيز الشراكات بين القطاعين العام والخاص على الصعيدين الوطني والدولي مسألة ذات أولوية.

الهند

[الأصل: بالإنكليزية]
[٩ حزيران/يونيه ٢٠١٦]

تؤدي تكنولوجيا المعلومات إلى تيسير النمو الاقتصادي وفرص الترابط الاجتماعي، إلا أن هناك تحديات خطيرة يتعين التصدي لها. فالنمو الذي يشهده قطاع تكنولوجيا المعلومات والاتصالات يرافقه أيضا تنامي التهديدات الإلكترونية التي تتراوح بين الهجمات الإلكترونية والجرائم الإلكترونية والإرهاب الإلكتروني والتجسس وغسل الأموال. وتبين الأدلة أن الجماعات الإرهابية (مثل تنظيم الدولة الإسلامية) تستخدم شبكة الإنترنت ومنابر وسائل التواصل الاجتماعي للاضطلاع بأنشطتها الشائنة، بما في ذلك التجنيد وجمع الأموال والدعاية وتغذية نزعة التطرف. وتعد إساءة استخدام وسائل التواصل الاجتماعي من بين الشواغل الرئيسية. وفي حين تتيح تلك الوسائل قدرة هائلة على الاتصال الإلكتروني، يمكن أن يساء استخدامها أيضا بحيث تؤدي إلى تفاقم عوامل الانقسام الإثني والاجتماعي.

ومن المهم أن يتوصل المجتمع الدولي إلى فهم مشترك فيما يتعلق بسلوك الدول في الفضاء الإلكتروني وأن يعتمد تدابير لبناء الثقة وبناء القدرات على نحو ما أوصى به فريق الخبراء الحكوميين التابع للأمم المتحدة في تقريره لعام ٢٠١٥. ولا ينبغي أن يُسمح بعرقلة مسألة إدارة شبكة الإنترنت بسبب خلافات تتعلق بدلالات الألفاظ. وبينما يتعين على مختلف أصحاب المصلحة أن يضطلعوا بأدوارهم كل في مجاله، يتعين على الحكومات أن تقوم بدور رئيسي في قضايا أمن الفضاء الإلكتروني المتعلقة بالأمن القومي. وثمة حاجة إلى وضع آليات مناسبة لتبادل المعلومات فيما يتعلق بالتهديدات الإلكترونية وجرائم الفضاء الإلكتروني والإرهاب الإلكتروني. وثمة حاجة أيضا إلى التعاون الآني بين الوكالات الحكومية لمعالجة الجريمة الإلكترونية. وينبغي كذلك أن تناقَش في جميع المحافل الدولية مسألة الحرب الإلكترونية والنظريات المتعلقة بالفضاء الإلكتروني وآثارها على الأمن الدولي. وعلى الرغم من أنه لا يزال يتعين الاتفاق على قواعد السلوك المسؤول للدول في الفضاء الإلكتروني، يمكن اللجوء إلى تفاهم مشترك بشأن تدابير بناء الثقة على النحو الوارد في تقرير عام ٢٠١٥ الصادر عن فريق الأمم المتحدة للخبراء الحكوميين من أجل اتخاذ التدابير المناسبة لبناء القدرات في مجال أمن الفضاء الإلكتروني. وفي هذا الصدد، يوفر الإطار الذي وضعه المنتدى العالمي لخبرات الفضاء الإلكتروني توجيها مفيدا.

والهند من أهم الجهات المعنية باستخدام تكنولوجيا المعلومات والاتصالات. وهي تدعم تعدد أصحاب المصلحة في إدارة شبكة الإنترنت، كما أنها سبّاقة إلى المشاركة

في مختلف المحافل الدولية، بما في ذلك فريق الخبراء الحكوميين، وعملية التشاور المفتوح بشأن الاستعراض الشامل لتنفيذ نتائج القمة العالمية لمجتمع المعلومات، وهيئة الإنترنت للأسماء والأرقام المخصصة. وقد اعتمدت الهند، بالتشاور مع جميع أصحاب المصلحة، نهجا متكاملا إزاء سلسلة من التدابير السياساتية والقانونية والتقنية والإدارية المتخذة لمعالجة الشواغل المتعلقة بأمن الفضاء الإلكتروني ولتعزيز التعاون الدولي بشأن هذا الموضوع. ويتسق إطارها القانوني مع سائر الأطر القانونية في العالم. وقد وُضعت السياسة الوطنية لأمن الفضاء الإلكتروني (٢٠١٣) في ظل رؤية تهدف إلى بناء فضاء إلكتروني آمن وقادر على الصمود من أجل المواطنين ومؤسسات الأعمال والحكومة. وتشدد الهند على بناء القدرات وتطوير المهارات وإقامة الشراكات بين القطاعين العام والخاص بشأن أمن الفضاء الإلكتروني.

اليابان

[الأصل: بالإنكليزية]
[٢٧ أيار/مايو ٢٠١٦]

تقييم عام لمسائل أمن المعلومات

ترى اليابان أن الفضاء الإلكتروني ينبغي أن يكون فضاء تُكفل فيه الحرية دون فرض قيود غير لازمة، وحيث لا يمنع كل من يرغب في الدخول إليه من ذلك ولا يُستبعدون من دون أي سبب مشروع. وتتقيد جهودنا بالمبادئ الخمسة التالية: التدفق الحر للمعلومات، وسيادة القانون، والانفتاح، والإدارة الذاتية، والنهج القائم على تعدد أصحاب المصلحة.

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

١ - الجهود المبذولة على الصعيد الوطني لتعزيز أمن المعلومات

استنادا إلى استراتيجية أمن الفضاء الإلكتروني التي وُضعت في أيلول/سبتمبر ٢٠١٥، تبذل اليابان جهودا لتعزيز أمن المعلومات.

٢ - الجهود المبذولة على الصعيد الوطني لتشجيع التعاون الدولي

تقوم الجهود التي تبذلها اليابان على الركائز الثلاث التالية: (١) تعزيز سيادة القانون في الفضاء الإلكتروني؛ (٢) وتدابير بناء الثقة؛ (٣) وبناء القدرات. وفيما يتعلق بتعزيز سيادة القانون، تسهم اليابان على نحو فعال في النقاش الدولي من أجل تعزيز فهم مشترك مفاده

أن القانون الدولي الحالي ينطبق في الفضاء الإلكتروني، ومن أجل تطوير قواعد طوعية غير ملزمة للسلوك المسؤول للدول. وفيما يتعلق بتدابير بناء الثقة، فإن اليابان تشارك في تعزيز بناء الثقة من خلال الحوار الثنائي والأطر المتعددة الأطراف مثل المنتدى الإقليمي لرابطة أمم جنوب شرق آسيا (آسيان). وفيما يتعلق ببناء القدرات، فإن اليابان تشارك بنشاط في المساعدة على تنمية الموارد البشرية والتعاون التقني الذي يركز على منطقة رابطة أمم جنوب شرق آسيا.

مضمون المفاهيم المذكورة في الفقرة ٣ من القرار

يشكل تأكيد انطباق القانون الدولي وتطوير قواعد طوعية غير ملزمة للسلوك المسؤول للدول في الفضاء الإلكتروني أساس كفالة استقراره وإمكانية التنبؤ به في المجتمع الدولي.

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

فيما يتعلق بتعزيز سيادة القانون، تحث اليابان على زيادة بلورة النقاش بشأن قواعد القانون الدولي في وقت السلم، والقانون المتعلق بحق الدفاع عن النفس، والقانون الدولي الإنساني، كما تحث على وضع قواعد طوعية على مستوى فريق الخبراء الحكوميين المقبل. وفيما يتعلق بتدابير بناء الثقة وبناء القدرات، من الأهمية بمكان تشجيع قيام كل دولة وكل منطقة على حدة بتنفيذ التوصيات الواردة في تقارير الفريق. ولا بد من إجراء دراسة عن سبل التعاون الملموس.

الأردن

[الأصل: بالعربية]
[٢ أيار/مايو ٢٠١٦]

تعتبر تكنولوجيا المعلومات والاتصالات من الأمور التي أصبحت أساسية في حياتنا اليومية، والتي تعزز نمو المجتمعات المحلية وتطورها من جميع النواحي، وخصوصاً الاجتماعية والثقافية والاقتصادية منها، وذلك بما ينعكس على مستوى الفرد داخل المجتمع وانفتاحه على المجتمع الدولي بشتى النواحي.

إن التقدم الهائل والسريع في تكنولوجيا المعلومات والاتصالات يجعلها عرضة للمخاطر والتحديات، مما يظهر الحاجة للتصدي لهذه المخاطر ومواجهتها بالوسائل

التكنولوجية والقانونية وإيجاد الحلول العملية القابلة للتطبيق للحد من أخطارها وتفادي الخسائر الفادحة التي تسببها.

تلعب القوات المسلحة الأردنية دوراً فعالاً ومؤثراً في تعزيز الأمن والسلم على المستوى الوطني والإقليمي والعالمي من خلال تطوير واستخدام التكنولوجيا وتوظيفها في مجال أمن المعلومات والاتصالات السلكية واللاسلكية. ويتمثل هذا التطور في المجالات التالية:

(أ) تحديث كافة أنظمة الاتصالات ونقل المعلومات من خلال شبكات محمية ومشفرة تعتمد تقنية (IP) المشفرة في كافة أنحاء المملكة، بما فيها الحدود، لتعزيز الأمن الوطني والإقليمي؛

(ب) التعاون مع المجتمع الدولي في حفظ الأمن الدولي من خلال أنظمة اتصالات متوافقة مع أنظمة الاتصالات المستخدمة في منظمة حلف شمال الأطلسي والجيش الأمريكي وضمن المعايير الدولية ذات التشفير العالي المستوى (type 1)؛

(ج) تعزيز القدرات الفنية من خلال امتلاك أنظمة اتصالات لا تعتمد على البنية التحتية لتأمين مناطق النزاع ومخيمات اللاجئين والمناطق النائية لتعزيز الأمن الوطني وخدمة القوات المسلحة الأردنية – الجيش العربي في دعم عمليات حفظ السلام في مناطق الصراع حول العالم؛

(د) تدريب وتأهيل كافة المستخدمين والمعنيين على إدامة وصيانة كافة أنظمة الاتصالات دون الاعتماد على الشركات الموردة لزيادة الاعتمادية والموثوقية لاستخدامها في كافة الأوقات؛

(هـ) تطبيق أعلى المعايير لأنظمة القيادة والسيطرة على الأنظمة المستخدمة في الجيوش لرفع مستوى التنسيق والتعاون لدعم الأمن الوطني والإقليمي والدولي؛

(و) المشاركة الفاعلة في المؤتمرات الدولية والتماشي مع قراراتها لزيادة التكاملية بين الجيوش الصديقة لتأمين بيئة خالية من التشويش أو التداخل بين أنظمة الاتصالات المستخدمة في الدول المجاورة وضمن الإقليم والتنسيق في ما بينها للسيطرة والمراقبة على الحدود الدولية.

يجب التركيز دائماً على وعي المواطن في فهم التهديدات الإلكترونية المحيطة وتأثير أمن المعلومات عليها من ناحية التقليل من حدوثها وكذلك إمكانية التعامل مع الأنظمة الإلكترونية، مما يؤدي إلى المساعدة في مجابهتها ورفع الحس الأمني بالتعامل مع أي نوع من المعلومات وبشكل لا يتعارض مع استخدام التكنولوجيا والاستفادة منها.

الإجراءات المتخذة للحماية بالنسبة لشبكة المعلومات العالية الأهمية على المستوى الوطني:

(أ) استخدام وسائل التشفير لجميع الشبكات وأنظمة الاتصالات الصوتية والبيانية والفيديو؛

(ب) العمل ضمن شبكة مغلقة (شبكة إنترانت خاصة)؛

(ج) الربط مع الجهات الأمنية الأخرى من خلال أجهزة طرفية منفصلة،؛

(د) تطبيق إجراءات أمن المعلومات والاتصالات ومبدأ الحاجة للمعرفة وتحديدات صلاحيات الدخول إلى المواقع والتدقيق المستمر للمستخدمين؛

(هـ) استخدام شبكات افتراضية (virtualization) حيث يتعامل المستخدم مع شاشة مربوطة على النظام حسب صلاحية الدخول والوصول للمعلومات ولا يستطيع استخدام أي وسيلة إدخال أو ربط مثل الفلاشات؛

(و) قام الأردن بإصدار وتشريع عدد من القوانين المتعلقة بأمن المعلومات:

(١) قانون الجرائم الإلكترونية؛

(٢) قانون المعاملات الإلكترونية؛

(٣) عمل مسودة استراتيجية وطنية لأمن وحماية المعلومات؛

(٤) عمل مسودة سياسات وطنية لأمن وحماية المعلومات؛

(٥) إقرار الاستراتيجية الوطنية لأمن وحماية المعلومات عام ٢٠١٢ من رئاسة مجلس الوزراء.

الإجراءات المقترحة على الصعيد العالمي:

(أ) تصنيف شبكات الاتصال والمعلومات المتداولة حسب الأهمية؛

(ب) تطبيق إجراءات الحماية وأمن المعلومات؛

(ج) تطبيق مبدأ الحاجة للمعرفة؛

(د) استخدام الإجراءات الفنية من تشفير وقفز ترددي؛

(هـ) تدقيق وتصنيف المستخدمين وصلاحيات الدخول على المواقع والشبكات؛

(و) الربط بين الشبكات المختلفة بواسطة أجهزة طرفية مفصولة عن هذه الشبكات (stand alone)؛

(ز) استخدام شبكة إنترانت خاصة ضمن شبكات معينة وتجنب استخدام الشبكة العنكبوتية العالمية ما أمكن؛

(ح) على مستوى الأمم المتحدة، تعزيز شبكة الإنترانت الخاصة بالأمم المتحدة وفصلها عن الشبكات العامة واستخدام الإجراءات الأمنية والفنية اللازمة لحماية هذه الشبكة باستخدام أجهزة التشفير والحماية وصلاحيات الدخول والتدقيق؛

(ط) تعزيز التعاون في عمل طرق متابعة الاختراقات (أفرقة التصدي للطوارئ الحاسوبية) وإجراءات الحماية ومعالجة الثغرات؛

(ي) تعميم الإجراءات الأمنية وأسلوب معالجة الاختراقات.

التركيز على استخدام تكنولوجيا المعلومات والاتصالات في توفير التنمية المستدامة وخاصة للمناطق الفقيرة والنائية من خلال:

(أ) تسريع إنهاء الفقر بوسائل منها الصيرفة المتنقلة التي جلبت بالفعل فوائد مباشرة للملايين من الناس في جميع أنحاء العالم ممن ليس لديهم الخبرة في المصارف؛

(ب) التقليل من آثار المجاعات من خلال استخدام التكنولوجيات الحديثة والوسائل العصرية الجديدة التي توفر أهم المعلومات للمزارعين فتمكنهم من اتخاذ قرارات صحيحة بشأن منتجاتهم.

. التوصيات:

(أ) إنشاء فرق دولية للاستجابة لحوادث أمن المعلومات والتعافي منها ومجابهة الكوارث والأزمات المعلوماتية؛

(ب) إشراك مندوب من الأردن في فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي المقرر إنشاؤه في عام ٢٠١٦؛

(ج) تعزيز التعاون العلمي والبحثي وتبادل الفرص التدريبية بين الدول الأعضاء في مجلس الأمن.

لبنان

[الأصل: بالعربية]
[٢٤ أيار/مايو ٢٠١٦]

تشير وزارة الدفاع الوطني اللبناني إلى ما يلي:

يطال أمن المعلوماتية جميع المسائل الاقتصادية، والاجتماعية، والسياسية، والعسكرية والإنسانية في عصرنا الحالي، ويعتبر الإرهاب الإلكتروني أهم التهديدات المستقبلية على الدول العظمى والنامية.

وتتركز أعمال الحرب المعلوماتية حول المحاور التالية: إنشاء المواقع الإلكترونية للتعبئة وحشد المناصرين، وخدمة الحرب النفسية، وتبادل المعلومات ونشرها من خلال الشبكة المعلوماتية، وتدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية، والتهديد والترويع الإلكتروني.

وتزداد خطورة الإرهاب الإلكتروني في كافة الدول، وقد تعرض لبنان لعدد من الهجمات السيبرانية استهدفت بشكل أساسي القطاع المصرفي أبرزها (Gauss) وقطاع الاتصالات، كما تتعرض معظم الخدمات الإلكترونية لهجمات بشكل مستمر.

إن الجهود المبذولة على الصعيد الوطني لتعزيز أمن المعلوماتية وتشجيع التعاون الدولي هي:

- في العام ١٩٩٩، تم إقرار قانون صون الحق بسرية المخابرات رقم ١٤٠، وقانون الملكية الفكرية رقم ٧٥، اللذين يعالجان جزئياً موضوع قرصنة برامج المعلوماتية.
- في العام ٢٠٠٦، تم إنشاء مكتب مكافحة جرائم المعلوماتية وحماية الملكية الفكرية التابع لقسم المباحث الجنائية الخاصة في المديرية العامة لقوى الأمن الداخلي.
- في العام ٢٠٠٧، تم إنشاء الهيئة الناظمة للاتصالات التي أصبحت عضواً فاعلاً في الشراكة الدولية المتعددة الأطراف لمكافحة التهديدات والهجمات السيبرانية (IMPACT).
- في العام ٢٠٠٩، أنشأت قيادة الجيش قسماً في مديرية المخابرات للأدلة الجنائية الإلكترونية.

- تبذل وزارة الدفاع الوطني جهوداً لإنشاء فريق لبناني للاستجابة لحوادث الحاسب الآلي بالتعاون مع الهيئات الوطنية والعالمية، وذلك عبر المشاركة في كافة المبادرات وتنظيم مؤتمرات ودورات تدريبية.
- في العام ٢٠١٢، أصدر مجلس الوزراء قراراً بتشكيل لجنة وطنية أمنية لاستضافة المواقع الحكومية على شبكة الإنترنت تضم ممثلاً عن وزارة الدفاع الوطني.
- في العام ٢٠١٣، شكل مجلس الوزراء لجنة لدراسة أخطار أبراج اتصالات العدو الإسرائيلي المقابلة للأراضي اللبنانية، تترأسها وزارة الدفاع الوطني وتشارك فيها الوزارات المعنية.
- في العام ٢٠١٥، تم إنشاء قسم متخصص بأمن المعلوماتية في الجيش اللبناني.
- يتم حالياً في مجلس النواب درس مشروع قانون المعاملات الإلكترونية.

إن الخطوات التي يمكن أن يتخذها المجتمع الدولي لتعزيز أمن المعلوماتية على الصعيد الدولي هي:

- التزام القرارات الصادرة عن الأمم المتحدة وعن القمة العالمية لمجتمع المعلومات، والداعية إلى نشر ثقافة المعلوماتية، ووضع إطار تعاون مع الهيئات الدولية المختصة، يضمن تبادل المعلومات ونقل الممارسات الفضلى.
- تأمين انسجام الأنظمة والقوانين الوطنية المتعلقة بمكافحة جرائم المعلوماتية، والقوانين العالمية، لمنع نشوء جنّات رقمية.
- التوصل إلى تحقيق منظومة عالمية قادرة على إدارة الأزمات في مجال أمن المعلوماتية العالمي، والدفع نحو إقرار تشريعات دولية فاعلة وقوية بما يكفي لتحصين القوانين الداخلية للدول وجعلها أكثر قدرة على التعامل مع الصبغة العالمية والدولية لجرائم المعلوماتية.

بولندا

[الأصل: بالإنكليزية]
[١٨ تموز/يوليه ٢٠١٦]

١ - رأي عام

إن أمن الفضاء الإلكتروني أمر حيوي للحفاظ على النمو الاقتصادي وعلى أداء المجتمع المدني. ولا يقتصر تأثير الهجمات الإلكترونية على القطاع الخاص والإدارة العامة، بل إنه يطال نظم التشغيل الآلي الصناعية في مرافق الهياكل الأساسية الحيوية.

ولا بد من كفالة نظام متسق لأمن المعلومات والاتصالات السلكية واللاسلكية بالنظر إلى طبيعة التهديدات القائمة واعتماد المؤسسات التجارية والإدارة والمجتمع بشكل متزايد على تكنولوجيا المعلومات. ويجب على جميع أصحاب المصلحة، بما في ذلك الدولة والمؤسسات التجارية والمنظمات غير الحكومية، أن يشاركوا ويسهموا في أمن الفضاء الإلكتروني.

ويعد احترام القانون الدولي والقواعد الدولية شرطا ضروريا لصون السلام والأمن بين الدول في الفضاء الإلكتروني.

ويشكل تعزيز القدرات الوطنية العنصر الرئيسي في تعزيز الأمن الدولي في الفضاء الإلكتروني.

وسيكون لتعزيز الثقة في الفضاء الإلكتروني أثر إيجابي على العلاقات بين الدول في المجالات الأخرى.

وينبغي حماية حقوق الإنسان والحريات الأساسية سواء في الفضاء الإلكتروني أو في العالم الحقيقي. ويؤدي احترام الحريات الأساسية على الإنترنت دورا رئيسيا في إيجاد مجتمع ديمقراطي وفي تحقيق النمو والازدهار على نحو مستدام.

٢ - المبادرات الوطنية الرامية إلى تعزيز أمن الفضاء الإلكتروني والتعاون الدولي

يقوم نظام أمن الفضاء الإلكتروني في بولندا على شبكة من المؤسسات. وهو يستند إلى ما تبذله الكيانات من تعاون، في المجالين المدني والعسكري، وفي الميدان المتصل بجرائم الفضاء الإلكتروني.

وتنهض الحكومة البولندية بجهودها الرامية إلى وضع استراتيجية وطنية لأمن الفضاء الإلكتروني وسن القانون الوطني لأمن الفضاء الإلكتروني. وسيكون من بين العناصر الرئيسية لنظام أمن الفضاء الإلكتروني في بولندا الإجراءات والناس والتكنولوجيا.

وفي العام الماضي، استضافت بولندا العديد من المناسبات الدولية الرئيسية التي أسهمت في تعزيز التعاون الدولي، من بينها: مؤتمر أمن الفضاء الإلكتروني لعام ٢٠١٥ (SECURE 2015 Conference)، والمنتدى الأوروبي لأمن الفضاء الإلكتروني (cybersecforum.eu)، والمؤتمر الدولي لأمن الفضاء الإلكتروني المعني بالسلامة والأمن خارج الحدود.

٣ - التدابير التي يمكن اتخاذها لتعزيز أمن الفضاء الإلكتروني على الصعيد العالمي

من الضروري مواصلة تطوير تدابير بناء الثقة في مجال الفضاء الإلكتروني المنفذة على الصعد العالمي والإقليمي والوطني.

وينبغي للمجتمع الدولي أن يشجع بناء القدرات الوطنية في مجال أمن الفضاء الإلكتروني.

ومن المهم تعزيز التعاون الثنائي والإقليمي. ومن الأمثلة الجيدة على الجهود المبذولة على الصعيد الإقليمي منتدى أوروبا الوسطى لأمن الفضاء الإلكتروني، الذي يضم كلا من بولندا والجمهورية التشيكية وسلوفاكيا وهنغاريا والنمسا.

وتتيح التمرينات الدولية في مجال أمن الفضاء الإلكتروني التوصل إلى فهم أفضل لطبيعة التهديدات القائمة ووسائل التصدي لها. ومن الأمثلة على ذلك التمرينات على أمن الفضاء الإلكتروني في أوروبا (Cyber Europe) وتمرينات منظمة حلف شمال الأطلسي على الأدرع المؤمَّنة (Locked Shields).

وينبغي ألا نقلل من قيمة المشاركة في الحوار الدولي الذي يجريه أصحاب المصلحة الذين يمثلون المنظمات غير الحكومية والمؤسسات التجارية والأوساط الأكاديمية.

البرتغال

[الأصل: بالإنكليزية]
[٣١ أيار/مايو ٢٠١٦]

أشارت الجمعية العامة في قرارها ٧٠/٢٣٧ بشأن ”التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي“ إلى أهمية العلم والتكنولوجيا في هذا السياق، مع التسليم بأن التطورات في هذين المجالين يمكن أن تكون لها تطبيقات مدنية وعسكرية. وإذا كان التقدم المحرز في ميادين المعلومات والاتصالات السلكية واللاسلكية يعني تزايد فرص تنمية المعارف والتعاون فيما بين الدول وتعزيز الإبداع الإنساني وتداول المعلومات في المجتمع ككل، فإننا نجد من ناحية أخرى أن هذه التكنولوجيات والوسائل يمكن أن تستخدم بطرق تتنافى مع الاستقرار والأمن الدوليين، وقد تؤثر سلبا على السلامة الإقليمية للدول.

ويطلب القرار ٧٠/٢٣٧ إسهام الدول الأعضاء فيما يتعلق بأربعة مجالات، إذ يشير إلى تقرير فريق الخبراء الحكوميين لعام ٢٠١٥:

(أ) التقييم العام لمسائل أمن المعلومات؛

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

(ج) مضمون المفاهيم التي تهدف إلى تعزيز أمن النظم العالمية للمعلومات والاتصالات السلكية واللاسلكية؛

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

ويعرض التقرير الوارد في الوثيقة A/68/98 بعض التوصيات بشأن المجالات التالية: التوصيات بشأن المعايير والقواعد والمبادئ التي تنظم السلوك المسؤول من جانب الدول؛ والتوصيات المتعلقة بتدابير بناء الثقة وتبادل المعلومات؛ والتوصيات المتعلقة بتدابير بناء القدرات.

وبناء على تلك التوصيات، تقدم البرتغال التعليقات التالية.

أولا - المعايير والقواعد والمبادئ التي تميز السلوك المسؤول للدول

١ - ترى البرتغال أن الأمن في شبكات المعلومات يتسم بالأهمية وأنه آخذ في الازدياد.

٢ - لا بد من تسليط الضوء على التقدم المحرز في الجهود الرامية إلى تنفيذ التشريعات المتعلقة بأمن الشبكات وسلامتها، باعتماد أساليب تقييم المخاطر التي تتطلب اتخاذ تدابير أمنية تعاونية كافية، على المستويين الفني والتنظيمي، وشرط الإبلاغ عن الانتهاكات الأمنية أو اختلال سلامة النظم، التي لها أثر كبير على أداء الخدمات.

٣ - أما على مستوى المفاهيم، من المهم ترسيخ الفكرة القائلة بضرورة انبثاق اللوائح التنظيمية من القواعد الدولية في المقام الأول.

٤ - وعلى الصعيد الدولي، من المهم تعزيز تبادل المعلومات والقيام بتمارين التدريب الميداني في المناطق الحدودية.

ثانياً - تدابير تعزيز الثقة وتبادل المعلومات

١ - من الأهمية بمكان تعزيز تبادل المعلومات فيما بين أصحاب المصلحة كافةً (سواء من القطاع العام أو الخاص)، وذلك مع مراعاة سياق العولمة ككل.

٢ - وعلى الصعيد الوطني، انصبّت جهودنا على إنجاز تدريبات مشتركة شاركت فيها كيانات عامة وخاصة، وعلى تشجيع التوحيد الفني وتنظيم المؤتمرات والحلقات الدراسية، وقد شارك في بعضها متحدثون دوليون.

ثالثا - تدابير بناء القدرات

١ - من المهم وضع تدابير لبناء القدرات. غير أن هناك صعوبات تتصل بتدريب واستبقاء الموارد البشرية المرتبطة بهذه الأنشطة.

٢ - وثمة حاجة إلى تيسير الحصول على المعارف وتشجيع التدريب الجماعي فيما يخص عدة جوانب، بما فيها الأمن، لدى جميع أصحاب المصلحة الرئيسيين.

صربيا

[الأصل: بالإنكليزية]
[٣١ أيار/مايو ٢٠١٦]

إدراكا للأهمية البالغة لضمان أمن المعلومات وتطويره، يُعترف بهذا المجال في جمهورية صربيا بوصفه من إحدى الأولويات الاستراتيجية فيما يتعلق بمجتمع المعلومات.

وقد اعتمدت الجمعية الوطنية لجمهورية صربيا القانون المتعلق بأمن المعلومات في كانون الثاني/يناير ٢٠١٦. وأنشئت بموجب القانون الهيئة المختصة بأمن المعلومات، وأُسندت لها مهام إعداد لوائح تنظيمية وفقا للمعايير الوطنية والدولية، والتعاون مع السلطات المختصة في بلدان أخرى، ومراقبة مدى إنفاذ القوانين. وحدد القانون نظم تكنولوجيا المعلومات والاتصالات التي تكتسي أهمية خاصة في صربيا، والتي سيتعين على متعهدي تشغيلها اتخاذ التدابير التقنية والتنظيمية الملائمة بشأنها من أجل ضمان أمن المعلومات. وهذه النظم هي: (أ) نظم تكنولوجيا المعلومات والاتصالات لدى الهيئات العامة؛ (ب) ونظم تكنولوجيا المعلومات والاتصالات التي تعالج فيها البيانات الشخصية الحساسة؛ (ج) ونظم تكنولوجيا المعلومات والاتصالات في المجالات ذات المصلحة العامة (الطاقة والنقل والغاز والأعمال المصرفية والرعاية الصحية وما إلى ذلك).

وتبذل الهيئة المختصة تعاونها على الصعيد الدولي، وتقدم على وجه الخصوص إنذارات بشأن المخاطر والحوادث التي تتسم بإحدى هذه الخصائص: (أ) تتزايد بسرعة أو تميل إلى أن تصبح مخاطر كبيرة؛ (ب) تتجاوز القدرات الوطنية؛ (ج) قد تؤثر على أكثر من بلد واحد.

وقد أنشئ بموجب القانون فريق وطني للتصدي للحوادث الحاسوبية داخل الوكالة التنظيمية للاتصالات الإلكترونية والخدمات البريدية، على أن يتولى جملة مهام منها التعاون مع المنظمات المماثلة في بلدان أخرى.

وينظم القانون أيضا عملية تأمين الاتصالات عن طريق الترميز والحماية من الانبعاثات الكهرومغناطيسية الضارة.

وبغية تعزيز أمن نظم المعلومات والاتصالات السلكية واللاسلكية العالمية، ينبغي أن تتعاون الدول، لا سيما عن طريق المحافظة على آليات فعالة وطيِّعة لتبادل المعلومات، ومن خلال الإنذارات والإعلانات المتعلقة بحوادث أمن الفضاء الإلكتروني. ولهذا الغرض، ينبغي للدول أن تعين منسقين أو أن تيسر الحصول على بيانات الاتصال بهم. وينبغي التركيز بشكل خاص على حماية الهياكل الأساسية الحيوية، لا سيما إذا كانت تلك الحوادث تمس إقليم أكثر من دولة واحدة. وينبغي للدول أيضا أن تتعاون على تبادل المعارف وعلى التثقيف في هذا المجال.

وإذ يأخذ المجتمع الدولي في الاعتبار المخاطر المتزايدة الناجمة عن الهجمات الإلكترونية وخصائصها في ظل ترابط أجزاء العالم، ينبغي له أن يشجع الدول على التعاون والتحاور، وتعزيز بناء القدرات في مجال أمن الفضاء الإلكتروني بصورة متبادلة، وتقديم

الدعم إلى المنظمات الدولية التي تهدف إلى التعاون في ميدان أمن المعلومات. وسيسهم تضافر الجهود والتعاون الفعال في تأمين البيئة العالمية لتكنولوجيا المعلومات والاتصالات وحمايتها، حيث تجري حماية الدول والمواطنين من مختلف المخاطر التي تهدد الفضاء الإلكتروني.

إسبانيا

[الأصل: بالإسبانية]
[٢٦ أيار/مايو ٢٠١٦]

ترى إسبانيا أن تكنولوجيا المعلومات والاتصالات تتيح فرصا هائلة للمجتمع الدولي، وما فتئت أهميتها تتزايد. ومع ذلك، فإن ثمة اتجاهات تبعث على القلق حيث تشكل أخطارا على السلام والأمن الدوليين. لذلك ينبغي للدول أن تتعاون بفعالية من أجل منع الممارسات الضارة في الفضاء الإلكتروني، وألا تسمح عن علم باستخدام أراضيها في ارتكاب أفعال غير مشروعة دوليا باستخدام هذه التكنولوجيات.

وفي تموز/يوليه ٢٠١٥، أقر المجلس الوطني لأمن الفضاء الإلكتروني تسع خطط منبثقة عن الخطة الوطنية لأمن الفضاء الإلكتروني من أجل تنفيذ التدابير المنصوص عليها في الاستراتيجية الوطنية لأمن الفضاء الإلكتروني لعام ٢٠١٣.

وتشارك إسبانيا بنشاط في جميع المبادرات الاستراتيجية المتصلة بأمن الفضاء الإلكتروني في الاتحاد الأوروبي، ومنظمة الأمن والتعاون في أوروبا، ومنظمة حلف شمال الأطلسي، ومجلس أوروبا، ومنظمة التعاون والتنمية في الميدان الاقتصادي.

وفي عام ٢٠١٥، انضمت إسبانيا إلى تحالف الحرية على شبكة الإنترنت، والمنتدى العالمي لخبرات الفضاء الإلكتروني.

وتؤيد إسبانيا الوثيقة الختامية للاجتماع الرفيع المستوى للجمعية العامة بشأن الاستعراض العام لتنفيذ نتائج القمة العالمية لمجتمع المعلومات، التي اعتمدت في كانون الأول/ديسمبر ٢٠١٥.

وما فتئ تحسين إمكانية الاتصال الإلكتروني والابتكار وفرص الاستفادة من تكنولوجيا المعلومات والاتصالات يكتسي أهمية بالغة في تيسير إحراز تقدم فيما يخص الأهداف الإنمائية للألفية. وترى إسبانيا أن عملية القمة العالمية لمجتمع المعلومات ينبغي أن تتماشى على نحو وثيق مع خطة التنمية المستدامة لعام ٢٠٣٠، حيث أضحت فرص الاستفادة من تكنولوجيا المعلومات والاتصالات أيضا مؤشرا من مؤشرات التنمية ومطمحا في حد ذاته.

وتؤيد إسبانيا العملية التي تهدف إلى تحقيق توافق آراء دولي بشأن أمن الفضاء الإلكتروني، وترى أن الدول ينبغي لها أن تواصل التفكير في كيفية تفسير مبادئ وقواعد القانون الدولي، ولا سيما تلك المتعلقة باستخدام القوة أو التهديد باستخدامها، والقانون الإنساني وحماية الحقوق والحريات الأساسية للأفراد، وفي كيفية تطبيق تلك المبادئ والقواعد في الفضاء الإلكتروني.

وتؤيد إسبانيا تطلعات المجتمع الدولي فيما يتعلق بالاستخدام السلمي لتكنولوجيا المعلومات والاتصالات خدمة للصالح العام للبشرية؛ وهي ترى أن الميثاق ينطبق في مجمله، وأن للدول حقا طبيعيا في اعتماد تدابير تتسق مع القانون الدولي لكي يتسنى لها التصدي في الوقت المناسب وبصورة مشروعة ومتناسبة للتهديدات أو الهجمات التي قد تمس بأمنها القومي.

سويسرا

[الأصل: بالإنكليزية]
[٧ حزيران/يونيه ٢٠١٦]

١ - تقييم عام لمسائل أمن المعلومات

لقد أضحت تكنولوجيا المعلومات والاتصالات قوة محركة لا غنى عنها للأنشطة الاجتماعية والاقتصادية والسياسية. وتتعهد سويسرا باغتنام الفرص التي يتيحها استخدام تكنولوجيا المعلومات والاتصالات. غير أن استخدام هذه التكنولوجيا قد جعل الهياكل الأساسية للمعلومات والاتصالات عُرضة لإساءة الاستغلال لأغراض إجرامية أو استخباراتية أو سياسية - عسكرية أو إرهابية، فضلا عن تعطيل أدائها. ومن الأخطار التي ينطوي عليها مجتمع المعلومات الاضطرابات وحالات التلاعب والهجمات المحددة التي تتم عن طريق الشبكات الإلكترونية.

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

في عام ٢٠١٢، اعتمدت الحكومة الاتحادية السويسرية الاستراتيجية الوطنية لحماية سويسرا من المخاطر الإلكترونية، فأرست بذلك الأساس لوضع نهج شامل. وتسعى هذه الاستراتيجية إلى تحسين الرصد المبكر للمخاطر الإلكترونية والتهديدات الناشئة، وجعل الهياكل الأساسية السويسرية ككل أكثر قدرة على التصدي للهجمات الإلكترونية، والحد من المخاطر الإلكترونية بوجه عام. وتعكس الاستراتيجية أيضا الحاجة إلى ثقافة الأمن

(أمن الفضاء الإلكتروني)، والمسؤولية المشتركة لجميع المشاركين، والحاجة إلى نهج قائم على تقييم المخاطر. وهي تدعو أيضا إلى التنسيق على المستوى الحكومي، وإلى التعاون على الصعيدين الوطني (أي الشراكة بين القطاعين العام والخاص) والدولي. وتتألف الاستراتيجية من ١٦ تدبيرا. وقد اعتمدت الحكومة الاتحادية السويسرية خطة تفصيلية لتنفيذ الاستراتيجية في عام ٢٠١٣.

٣ - مضمون المفاهيم المذكورة في الفقرة ٣ (من القرار)

يتعين مواجهة المخاطر الإلكترونية عن طريق تعزيز التعاون الدولي (بمجال العمل ٥ المحدد في الاستراتيجية). وتركز السياسة الخارجية السويسرية في مجال أمن الفضاء الإلكتروني على وضع قواعد السلوك المسؤول للدول وتدابير بناء الثقة وبناء القدرات. ومع أخذ ذلك في الاعتبار، تشارك سويسرا في مختلف العمليات الدولية. وقد اعتمدت منظمة الأمن والتعاون في أوروبا تدابير لبناء الثقة في مجال الفضاء الإلكتروني. وترى سويسرا أن هذه العملية تتسم بأهمية قصوى. وبالإضافة إلى ذلك، تشكل عملية لندن عملية أخرى من العمليات الهامة التي تشارك فيها سويسرا. وتدعم سويسرا طائفة من المشاريع التي تهدف إلى تطوير بناء القدرات.

٤ - التدابير التي يمكن أن يتخذها المجتمع الدولي لتعزيز الأمن على الصعيد العالمي

يتعين على جميع التدابير التي يتخذها المجتمع الدولي أن توازن بين الاعتبارات الأمنية واعتبارات حقوق الإنسان. فنفس الحقوق التي يتمتع بها الأشخاص خارج الإنترنت يجب أن تُكفل على شبكة الإنترنت كذلك. ويلزم مواصلة تطوير التدابير الرامية إلى بناء الثقة وبعث الاطمئنان. وتكتسي مجموعة تدابير بناء الثقة التي اعتمدتها منظمة الأمن والتعاون في أوروبا أهمية قصوى لتعزيز الأمن. وسيسهم بناء الشفافية، عن طريق تبادل المعلومات وتعزيز التعاون من خلال أنشطة عملية مشتركة، في الاستقرار العام للفضاء الإلكتروني.

توغو

[الأصل: بالفرنسية]
[٢ حزيران/يونيه ٢٠١٦]

يعد تقدم الاتصالات السلكية واللاسلكية ميزة كبيرة بالنسبة لتقدم البلدان، إلا أنه يشكل في نفس الوقت تهديدا للأمن على الصعيدين الوطني والدولي. فهذه الاتصالات تشكل فضاء افتراضيا يستخدم في كثير من الأحيان لغايات إجرامية أو إرهابية.

وتوغو ليست في مأمن من هذا الخطر، وهي تشهد بالفعل جرائم ترتبط بتكنولوجيا المعلومات والاتصالات، وتتراوح بين النصب والاحتيال وغير ذلك من أشكال الغش، واستغلال الأطفال في المواد الإباحية، وانتهاك حرية الأشخاص وسلامتهم.

وفي زمن الإرهاب، تظل شبكة الإنترنت ووسائل التواصل الاجتماعي مجالا من المجالات التي تستغلها المنظمات الإرهابية للدعاية والتجنيد. ويضاف إلى ذلك أن معظم البلدان بصدد الانتقال إلى الإدارة الإلكترونية، وهو ما يشكل تحديا كبيرا لحكوماتنا، حيث تخشى الهجمات الإلكترونية التي من شأنها أن تضر بأداء الإدارات وأن تمس بالأمن في المجالين المدني والعسكري.

وفي ظل هذا الوضع، من الأهمية بمكان اتخاذ تدابير على الصعيدين الدولي والوطني بهدف التحكم في قطاع المعلومات والاتصالات السلكية واللاسلكية من خلال فرض الرقابة بما يتيح مكافحة استخدامه في أغراض إجرامية.

وقد أُتخذت في توغو العديد من التدابير في هذا الصدد، منها على وجه الخصوص:

- اعتماد المرسوم رقم 2011-120/PR المؤرخ ٦ تموز/يوليه ٢٠١١ الذي ينص على إلزامية تحديد هوية المشتركين في خدمات الاتصالات السلكية واللاسلكية بصورة منهجية؛
- اعتماد القانون رقم 2012-018 بشأن الاتصالات الإلكترونية، والقانون رقم 2013-003 المعدِّل له؛
- إعداد مشاريع أولية لقوانين تتعلق بجرائم الفضاء الإلكتروني وعلم الترميز وأمن الفضاء الإلكتروني وحماية البيانات الشخصية والمعاملات الإلكترونية.

والغرض من هذه القوانين هو كفالة إمكانية تتبع كل الأنشطة الإلكترونية والاتصالات السلكية واللاسلكية ووضع تدابير أمنية تتيح حماية الشبكات المعلوماتية وشبكات الاتصالات ضد أي عملية اختراق احتيالية.

وترى توغو أيضا أن من الضروري وضع إطار مؤسسي يكفل الرقابة. لذلك تم إنشاء فريق وطني للتصدي للحوادث الحاسوبية ليكون بمثابة مرصد، على الصعيد الوطني، لأمن الفضاء الإلكتروني. ويأتي هذا الفريق تكملة لإجراءات هيئة تنظيم قطاعي البريد والاتصالات السلكية واللاسلكية.

وبالإضافة إلى ذلك، تجدر الإشارة إلى تعزيز قدرات الموارد البشرية لكي يتسنى لسلطات إنفاذ القانون والهيئات العامة والخاصة المعنية بأمن الفضاء الإلكتروني اتخاذ إجراءات فعالة للتصدي للتهديدات بجميع أنواعها.

ومن جهة أخرى، سوف يتيح التعاون الدولي، لا سيما في إطار الاتحاد الدولي للاتصالات ومنظمة الأمم المتحدة، تعزيز الأمن في ميدان المعلومات والاتصالات السلكية واللاسلكية.

تركمانستان

[الأصل: بالروسية]
[٢٨ آذار/مارس ٢٠١٦]

يشكل الحياد أساس سياسة تركمانستان الداخلية والخارجية القائمة على العلاقة الوثيقة بين المصالح الوطنية والأمن العالمي والتقدم المشترك. ويتمثل أحد العوامل الأساسية بالنسبة لتركمانستان، الذي ينشأ عن وضعها المحايد والتزاماتها الدولية، في الطبيعة المحبة للسلام التي تتسم بها سياستها الخارجية. وبناء على ذلك، تعالج جميع المسائل حصرا من خلال القنوات السياسية والدبلوماسية، ولا سيّما الأمم المتحدة وسائر المنظمات الدولية. وتدعم تركمانستان بالكامل الجهود الدولية الرامية إلى مكافحة انتشار أسلحة الدمار الشامل ووسائل إيصالها وما يتصل بها من تكنولوجيات، وتدعو إلى نزع السلاح بوصف ذلك شرطا مسبقا لتحقيق الأمن على الصعيد العالمي. وتعلن تركمانستان، في تشريعاتها، رفضها امتلاك أو تصنيع أو تخزين أو نقل الأسلحة النووية والكيميائية والبكتريولوجية وسائر أنواع أسلحة الدمار الشامل، بما في ذلك الأنواع الجديدة من هذه الأسلحة أو التكنولوجيات اللازمة لإنتاجها.

وقد انضمت تركمانستان إلى عدد من الصكوك الدولية لنزع السلاح التي يتمثل الغرض الرئيسي منها في تشجيع الدول الأطراف على حفظ السلام والوئام والأمن في العالم.

وإذ تعلق تركمانستان أهمية خاصة على تعزيز السلام والأمن الدوليين، فإنها تدعو إلى الحد من عدد الأسلحة اقتناعا منها بأنه كلما قلّت الأسلحة في العالم، كان تطور العالم أكثر اطرادا وثباتا، وكانت الثقة والتفاهم أكبر بين البلدان والشعوب. وتشدد الوثيقة

الإطارية لسياسة تركمانستان الخارجية للفترة من عام ٢٠١٣ إلى عام ٢٠١٧ على أن تركمانستان ستواصل بنشاط تشجيع عمليات نزع السلاح والحد من ترسانات الأسلحة، وفي المقام الأول أسلحة الدمار الشامل.

وفي الكلمة التي ألقاها رئيس تركمانستان في اجتماع مجلس الوزراء المعقود في ٥ حزيران/يونيه ٢٠١٥، وجه الانتباه بوجه خاص إلى التزامات بلده الدولية إزاء المجتمع الدولي. وشدد على أن الحياد يعني عدم التقيد بالاتحادات والكتل السياسية أو الاقتصادية أو العسكرية؛ وأن لدى تركمانستان جيشا خاصا بها يضم قوامه ما يكفي من القوات لحماية سلام الأمة وحريتها؛ وأن تركمانستان ترفض أسلحة الدمار الشامل وتحظر دخول هذه الأسلحة إقليمها الوطني ومجالها الجوي؛ وأنها ملتزمة بالقيم الإنسانية العالمية والمبادئ الديمقراطية؛ وتحافظ على جو من الوئام المدني والسلام الأهلي في البلد؛ وتنفذ السياسات الداخلية والخارجية بالتعاون الوثيق مع الأمم المتحدة والمنظمات الإنسانية الدولية.

وخلال دورة الجمعية العامة التاسعة والستين المعقودة في ٣ حزيران/يونيه ٢٠١٥، اعتمدت ١٩٣ دولة بالإجماع القرار ٢٨٥/٦٩ المتعلق بحياد تركمانستان الدائم. ويدل ذلك بوضوح على الاعتراف العالمي بسياسة بلدنا الفعالة فيما يتعلق بحماية السلام والأمن والتنمية المستدامة على الصعيدين الإقليمي والدولي. ويشدد القرار على ما يتيحه حياد تركمانستان الدائم من مساهمة هامة في تعزيز السلام والأمن في المنطقة وفي تطوير علاقات ودية تخدم المصالح المتبادلة بين بلدان العالم.

وبوصفها البلد الذي يستضيف مركز الأمم المتحدة الإقليمي للدبلوماسية الوقائية لمنطقة آسيا الوسطى، فإن تركمانستان تدعو تلك الهيئة إلى تعزيز دورها في مختلف جوانب المسائل الإقليمية بدعم من الدول الأعضاء في الأمم المتحدة والمنظمات الأخرى (بما في ذلك منظمة الأمن والتعاون في أوروبا، والاتحاد الأوروبي، ورابطة الدول المستقلة).

وفي عام ٢٠١٥، انعقد بنجاح في عشق أباد منتدى دولي بشأن صون السلام والاستقرار والأمن في منطقة وسط آسيا. وتعتزم تركمانستان، بوصفها طرفا في المعاهدات الدولية واتفاقيات الأمم المتحدة والصكوك المتعددة الأطراف في مجال نزع السلاح، مواصلة بذل قصارى جهدها لتيسير هذه العمليات، على الصعيد الإقليمي في المقام الأول، وتسعى إلى عقد اجتماعات إقليمية منتظمة بشأن مسائل نزع السلاح في وسط آسيا.

المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية

[الأصل: بالإنكليزية]
[٣١ أيار/مايو ٢٠١٦]

ترحب المملكة المتحدة بهذه الفرصة للرد على قرار الجمعية العامة ٧٠/٢٣٧ المعنون ”التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي“، وهو الرد الذي يستند إلى ردها على القرار ٦٩/٢٨ في عام ٢٠١٥. وتستخدم المملكة المتحدة في مجمل ردها مصطلح ”أمن الفضاء الإلكتروني“ (cybersecurity) المفضل لديها، وكذلك المفاهيم ذات الصلة لتفادي الإرباك، نظرا لاختلاف تفسيرات مصطلح ”أمن المعلومات“ في هذا السياق.

وتدرك المملكة المتحدة بأن الفضاء الإلكتروني عنصر أساسي من عناصر الهياكل الأساسية الحيوية على الصعيدين الوطني والدولي، وركيزة أساسية من ركائز النشاط الاقتصادي والاجتماعي من خلال شبكة الإنترنت. وتشير المملكة المتحدة إلى تقييم المخاطر الأمنية على الصعيد الوطني لعام ٢٠١٥ الذي أكد أن المخاطر الإلكترونية لا تزال تشكل تهديدا من المستوى الأول للأمن القومي. وسيجري تعزيز التمويل المخصص من المملكة المتحدة بمقدار ٨٦٠ مليون جنيه إسترليني خلال مدة تنفيذ الاستراتيجية الوطنية السابقة لأمن الفضاء الإلكتروني (٢٠١١-٢٠١٦) باعتماد إضافي قدره ١,٩ بليون جنيه إسترليني على مدى السنوات الخمس المقبلة. وسيتم نشر استراتيجية وطنية جديدة لأمن الفضاء الإلكتروني في عام ٢٠١٦، كما سيتم إنشاء مركز وطني جديد لأمن الفضاء الإلكتروني.

وتدرك المملكة المتحدة أن التعاون الدولي أمر أساسي لتحقيق أمن الفضاء الإلكتروني بنجاح. ونحن نواصل تشجيع إقامة فضاء إلكتروني حر ومفتوح وسلمي وآمن كي يتسنى حماية منافعه الاقتصادية والاجتماعية وإتاحتها للجميع. وتقوم المملكة المتحدة بدور ريادي في مواجهة تحديات أمن الفضاء الإلكتروني العابرة للحدود من خلال مبادرات من قبيل التحالف العالمي لإنهاء الاستغلال الجنسي للأطفال عبر الإنترنت (WePROTECT Global Alliance to End Online Child Sexual Exploitation). ونحن ملتزمون أيضا بتبادل أفضل الممارسات على الصعيد الدولي، وبضمان أن يحصل المجتمع العالمي على المساعدة في تطوير قدراته في مجال أمن الفضاء الإلكتروني.

ولا تزال المملكة المتحدة تشارك بنشاط وعلى نحو بناء في النقاش الدولي حول أمن الفضاء الإلكتروني. وقد قدَّمنا خبراء لأفرقة الأمم المتحدة الأربعة للخبراء الحكوميين،

ونحن نرى أن التقرير الذي أعده الفريق الأخير بتوافق في الآراء أحرز تقدما قيِّما في إعادة التأكيد على أن القانون الدولي ينطبق في الفضاء الإلكتروني، وأن تقيد الدول بالقانون الدولي، ولا سيما التزاماتها بموجب ميثاق الأمم المتحدة، يشكل إطارا أساسيا لأعمالها عند استخدامها تكنولوجيا المعلومات والاتصالات.

وترحب المملكة المتحدة أيضا باستمرار المناقشات بشأن بلورة تدابير محتملة في المستقبل لبناء الثقة في مجال الفضاء الإلكتروني على مستوى منظمة الأمن والتعاون في أوروبا، وبالأعمال المماثلة المضطلع بها في منظمات إقليمية أخرى.

ومن دواعي سرور المملكة المتحدة أن تسهم بنشاط في هذه القضايا المهمة، وهي تتطلع إلى زيادة مشاركتها في تعزيز القدرات والتعاون الدولي في مجال أمن الفضاء الإلكتروني.