الأمم المتحدة

A/72/315

الجمعية العامة

Distr.: General
11 August 2017
Arabic
Original: Arabic/English/French/
Russian/Spanish

الدورة الثانية والسبعون

البند ٩٥ من جدول الأعمال المؤقت*

التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي

تقرير الأمين العام

المحتويات

الصفحة

* A/72/150.

17-13876 (A) 200917 250917

أولا – مقدمة

١ – اتخذت الجمعية العامة، في ٥ كانون الأول/ديسمبر ٢٠١٦، القرار ٧١/٢٨ بشأن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي. وفي الفقرة ٣ من القرار، دعت الجمعية العامة جميع الدول الأعضاء إلى أن تواصل، آخذة في اعتبارها التقييمات والتوصيات الواردة في التقرير الصادر عن 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 ٢ من القرار؛

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

٢ – واستجابة لذلك الطلب، وجهت مذكرة شفوية في ١٦ شباط/فبراير ٢٠١٦ إلى جميع الدول الأعضاء لدعوتها إلى تقديم معلومات عن الموضوع، أعقبتها مذكرة شفوية أخرى مؤرخة ١٢ حزيران/يونيه ٢٠١٧. ويتضمن الفرع الثاني الردود التي وردت حتى إعداد هذا التقرير. وستنشر الردود الإضافية التي وردت بعد ٣١ تموز/يوليه ٢٠١٧ في الموقع الشبكي لمكتب شؤون نزع السلاح (www.un.org/disarmament/) باللغة الأصلية.

ثانياً – الردود الواردة من الحكومات

أفغانستان

[الأصل: بالإنكليزية]
[٢٦ أيار/مايو ٢٠١٧]

فيما يخص الفقرة ٣ من منطوق قرار الجمعية العامة ٧١/٢٨ بشأن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، أفادت وزارة تكنولوجيا المعلومات والاتصالات في جمهورية أفغانستان الإسلامية بما يلي.

الإنجازات

عملا على تعزيز الأمن الدولي لتكنولوجيا المعلومات وسلامة المعاملات الإلكترونية، أنشأت وزارة تكنولوجيا المعلومات والاتصالات جهازا عاما رئيسيا للبنية التحتية. وأنشأت الوزارة أيضا منظومة لمراكز إدارة الشبكات، وتعتزم ربط هذا المنظومة بنظيراتها في الدول الأعضاء من أجل الوقوف على صحة الإحصاءات البيانات المتدفقة عبر الإنترنت والتحقق منها.

وأعدت الوزارة مشاريع قوانين للجرائم السيبرانية وأرسلتها إلى وزارة العدل لدراستها. وفي ضوء هذه القوانين، يمكن إيجاد حلول أساسية تسمح بإجراء المزيد من المعاملات الإلكترونية المأمونة ومنع الجرائم السيبرانية.

ووضعت الوزارة استراتيجية سيبرانية من أجل تبادل المعلومات بشكل مأمون، وإنشاء إطار لأمن تكنولوجيا المعلومات لصالح مشروع الهيئة الوطنية للتبادل عن طريق الإنترنت (نيكسا) الذي ستنفذه الوزارة، والتصدي للجرائم السيبرانية والوقوف عليها.

المقترحات

تطلب وزارة تكنولوجيا المعلومات والاتصالات إلى البلدان المتقدمة التي تتوافر لديها شرطة سيبرانية أن تساعد الوزارة وتتعاون معها في إنشاء الشرطة السيبرانية.

وبغية التصدي للجرائم السيبرانية ومكافحة هذه الظاهرة جديا ينبغي إنشاء نظام متماسك (يوفر المعلومات الجنائية) على الصعيد الدولي.

ومن الحلول الهامة لأمن الإنترنت إنشاء حوكمة للإنترنت. فمن خلال حوكمة الإنترنت، يمكن توفير أساس لتبادل المعلومات والبيانات السرية بين جميع إدارات الحكومة ومكاتبها من أجل تنفيذ الشبكة المذكورة أعلاه. وفي هذا الصدد، تلتمس الوزارة تعاون جميع الدول الأعضاء.

وتطلب الوزارة أيضا إلى الدول الأعضاء أن تدعم موظفي الوزارة في مكافحة الجرائم السيبرانية وتحسين أمن المعلومات، عن طريق تزويدهم ببرامج تدريبية مهنية وتقنية.

أرمينيا

[الأصل: بالإنكليزية]
[٣١ أيار/مايو ٢٠١٧]

التقييم العام لمسائل أمن المعلومات

بالنظر إلى وتيرة تطور مجتمع المعلومات في جمهورية أرمينيا، تتسم مسائل أمن المعلومات بأهمية كبيرة لجميع جوانب الأمن الوطني وتؤثر عليها تأثيرا هائلا.

وتطرح الاتجاهات السائدة في مجال تكنولوجيا المعلومات والاتصالات تهديدات وتحديات جديدة من الناحية النوعية تتطلب تنسيقا منتظما واتباع نُهج جديدة لضمان الاستخدام المأمون لتكنولوجيا المعلومات والاتصالات. وتعلق أرمينيا، مراعاة منها لأن تقنيات ”حرب المعلومات“ باتت تستخدم في بيئات نزاع مختلفة، أهمية كبرى على ضمان أمن المعلومات من أجل الحفاظ على السلام والأمن الدوليين.

الجهود المبذولة على المستوى الوطني لتعزيز أمن المعلومات وتشجيع التعاون الدولي في هذا الميدان

اضطلعت أرمينيا بأنشطة ترمي إلى صون مصالح الدولة وعامة الجمهور في ميدان أمن المعلومات، وإلى تحقيق تناسق بين التشريعات ذات الصلة والمعايير الدولية. وبدأ نفاذ مجموعة من الصكوك المعيارية التي تحكم هذا الميدان، تشمل الاستراتيجية الأمنية الوطنية ومفهوم أمن المعلومات، وكذلك قوانين تتعلق بمكافحة الإرهاب؛ وأسرار الدولة والأسرار الرسمية؛ والوثائق الإلكترونية والتوقيعات الرقمية؛ وحماية البيانات الشخصية؛ وحرية المعلومات؛ ووسائط الإعلام.

وتنفيذا للقرارات ذات الصلة التي اتخذتها الحكومة، تم القيام بما يلي:

(أ) اتخاذ عدد من التدابير لضمان حماية معلومات الهيئات الحكومية التي يمكن لعامة الجمهور الوصول إليها بواسطة الإنترنت، وربط نظم المعلومات الخاصة بها بشبكة الإنترنت عن طريق وصلة مأمونة؛

(ب) اعتماد متطلبات دنيا للمواقع الشبكية الرسمية التي تنشئها الهيئات الحكومية على الإنترنت.

واعتمدت أرمينيا وطبقت مجموعة من معايير المنظمة الدولية لتوحيد المقاييس تتصل بأمن المعلومات. وفي تشرين الأول/أكتوبر ٢٠٠٦، تم التصديق على اتفاقية مجلس أوروبا المتعلقة بالجرائم السيبرانية، وأعقب ذلك إدخال التعديلات اللازمة على التشريعات الوطنية.

وتشارك أرمينيا بنشاط في البرامج والدورات التدريبية والمبادرات التعاونية ذات الصلة المنفذة ضمن أطر دولية مختلفة مثل رابطة الدول المستقلة، ومنظمة معاهدة الأمن الجماعي، والاتحاد الأوروبي، ومنظمة حلف شمال الأطلسي. وبوجه خاص، نفذت الدول الأعضاء في رابطة الدول المستقلة في عام ٢٠١٦ عملية ''مكافحة الإرهاب السيبراني''، وهي عملية مشتركة ذات مرحلتين. وأُقترح إعداد مشروع ''اتفاق بشأن التعاون بين الدول الأعضاء في منظمة معاهدة الأمن الجماعي في مجال ضمان أمن المعلومات'' توطئة للموافقة الداخلية عليه على المستوى المشترك بين الإدارات في مطلع عام ٢٠١٧.

مضمون المفاهيم المذكورة في الفقرة ٢

يُعَرِّفُ مفهوم أمن المعلومات الخاص بجمهورية أرمينيا مصطلح ''أمن المعلومات'' بأنه ''حماية المصالح الوطنية في ميدان المعلومات، وهو أمر يرتبط بمجمل المصالح المتوازنة للأفراد والمجتمع والدولة''.

ومراعاة للتطور السريع لتكنولوجيا المعلومات والاتصالات، أنشئ فريق عامل مشترك بين الوكالات كي يصوغ، بحلول أواخر عام ٢٠١٧، مفهوما محدثا بشأن أمن المعلومات وسياسة المعلومات في جمهورية أرمينيا.

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

تؤكد أرمينيا أهمية تعزيز التعاون الدولي الفعال بشأن المسائل المتعلقة بأمن المعلومات، وتشدد على دور الاتحاد الدولي للاتصالات.

بيلاروس

[الأصل: بالروسية]
[٥ حزيران/يونيه ٢٠١٧]

التقييم العام لمسائل أمن المعلومات

إن الحالة الراهنة لأمن المعلومات على الصعيد الدولي لا تبعث على الارتياح. إذ تبذل محاولات لاستخدام تكنولوجيا المعلومات لأغراض سياسية.

وتواجه بيلاروس عددا من المسائل الخاصة في مجال أمن المعلومات هي:

(أ) عدم توافر حماية كافية للقطاع الوطني تصونه من التعرض لحجب الخدمة الموزع، وذلك على مستوى مقدمي الخدمة الرئيسيين والمحليين، بل وحتى على مستوى منصات الاستضافة؛

(ب) إمكان أن تظهر في منتجات أمن المعلومات قدرات غير معلنة ومواطن ضعف مع الافتقار إلى القدرة على كشفها في الوقت المناسب، مما يقوض في كثير من الأحيان أثر التدابير الرامية إلى حماية المعلومات؛

(ج) التهديد من دخلاء يهاجمون البنية التحتية الحرجة والبنية التحتية لتكنولوجيا المعلومات، مثل نظم الإمداد بالطاقة والنظم المؤتمتة لإدارة الإنتاج والنقل.

الجهود المبذولة على المستوى الوطني لتعزيز أمن المعلومات وتشجيع التعاون الدولي في هذا الميدان

تشمل هذه الجهود ما يلي:

(أ) العمل على نطاق النظام بأسره لتحديث المتطلبات المتعلقة بالحماية التقنية والترميزية للمعلومات التي يُقيَّد نشرها و/أو توفيرها؛

(ب) تنظيم وتطبيق قواعد ومعايير تقنية تتصل بالحماية التقنية والترميزية للمعلومات؛

(ج) تنفيذ اتفاقات تبادل المعلومات المبرمة مع الشركات الرائدة في مجال أمن المعلومات؛

(د) التعاون المنتظم مع الهيئات والمنظمات التابعة للدولة من أجل تيسير الاستجابات السريعة لحوادث محددة تتعلق بأمن المعلومات؛

(هـ) قيام البلدان نفسها بتعهد حزم برامجها المتعلقة بالكشف عن البرامجيات الخبيثة؛

(و) التعاون مع بلدان منظمة معاهدة الأمن الجماعي من خلال مركز تنسيق استشاري.

دراسة المفاهيم الدولية الرامية إلى تعزيز أمن نظم المعلومات والاتصالات السلكية واللاسلكية على الصعيد العالمي

يرتبط نهج رئيسي تتبعه بيلاروس بشأن أمن المعلومات على الصعيد الدولي بضرورة درء الاستغلال المحتمل لتكنولوجيا المعلومات والاتصالات بما يقوض الأمن الوطني والاستقرار والأمن الدولي.

وتشارك بيلاروس مشاركة نشطة في المناقشات التي تدور بشأن أمن المعلومات على الصعيد الدولي في محافل منظمات دولية مختلفة، من بينها الأمم المتحدة، ومنظمة معاهدة الأمن الجماعي، ومنظمة الأمن والتعاون في أوروبا.

وتدعم بيلاروس المبادرة الرامية إلى اعتماد صك عالمي بشأن أمن المعلومات في إطار الأمم المتحدة.

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

مما يتسم بأهمية حاسمة، على الصعيد الدولي، التوسع تدريجيا في إعمال مبدأ عدم التدخل في الشؤون الداخلية للدول ذات السيادة والرفض المشترك للأعمال العدوانية في ميدان المعلومات. وينبغي أن تتخذ هذه الخطوات بصورة رئيسية من خلال دعم السيادة المعلوماتية للدول الأعضاء في الأمم المتحدة من أجل:

(أ) دعم حقوق المواطنين في تلقي وتخزين ونشر معلومات كاملة وموثوقة ومناسبة التوقيت؛

(ب) إقامة مجتمع معلومات يتيح للدول الأعضاء في الأمم المتحدة أن تشارك على قدم المساواة في علاقات معلوماتية عالمية؛

(ج) ضمان الإدارة المعلوماتية الفعالة لسياسة حكومية دولية ترمي إلى منع انتشار الأفكار الإرهابية والمتطرفة؛

(د) ضمان مرونة أداء البنية التحتية الحرجة.

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

(أ) إنشاء آليات للتعاون الدولي، على النحو المبين في صكوك القانون الدولي الحالية والمقبلة؛

(ب) إقامة تعاون فعال بين المجتمع الدولي والشركات المتعددة الجنسيات التي تتحكم في الأغلبية الساحقة من تكنولوجيا المعلومات والاتصالات، من أجل تحديد وحجب المصادر التي تهدد أمن المعلومات.

بروني دار السلام

[الأصل: بالإنكليزية]
[٢٩ حزيران/يونيه ٢٠١٧]

تعترف بروني دار السلام بأن الاتجاهات العالمية قد تبدلت بحكم ما يشهده ميدان المعلومات والاتصالات السلكية واللاسلكية من تطورات تتزايد أهميتها. وطرح ذلك أيضا، في الوقت نفسه، تهديدات وتحديات جديدة، في صورة قرصنة وجرائم سيبرانية وإرهاب سيبراني، تعرض للخطر البنى التحتية والشبكات والخدمات الحيوية على الصعيد العالمي. ويتطلب طابعها العابر للبلدان وغير الملموس جهودا تعاونية من جانب المجتمع الدولي لبناء بيئة إلكترونية مأمونة وموثوق بها.

وعلى الصعيد الوطني يقيم البلد، تحت رعاية لجنة الأمن الوطني، روابط تعاونية قوية مع طائفة من الوكالات الأمنية المحلية لمواجهة التهديدات الداخلية المحدقة بالأمن السيبراني. وفي أيار/مايو ٢٠٠٤، أنشئ الفريق الوطني للاستجابة للطوارئ الحاسوبية في بروني وأصبح الوكالة الوطنية المرجعية الجامعة في التعامل مع الحوادث الأمنية الحاسوبية والشبكية. ومن خلال الارتباط مع الفرق الأخرى المعنية بالاستجابة للطوارئ الحاسوبية على الصعيد العالمي، يحصل الفريق الوطني على معلومات قيمة عن التهديدات الأمنية لتكنولوجيا المعلومات والاتصالات، ويتبادل النتائج المتعلقة بالمخاطر الأمنية التي تم الوقوف عليها في إطار البنية التحتية لتكنولوجيا المعلومات والاتصالات في البلد.

وبروني دار السلام ملتزمة بالعمل مع الشركاء الإقليميين والدوليين للحفاظ بصفة متواصلة على حالة الاستعداد في مواجهة التهديدات السيبرانية الدولية الكبرى. وستشارك بروني دار السلام، ضمن الهيكل الإقليمي لرابطة أمم جنوب شرق آسيا (آسيان)، في فريق الخبراء العامل المعني بالأمن السيبراني، المنشأ في إطار اجتماع وزراء دفاع رابطة آسيان وشركائها، وهو فريق يضم ١٨ بلدا ويرمي إلى تعزيز التعاون العملي والفعال وزيادة القدرة على حماية الفضاء السيبراني للمنطقة ومواجهة التحديات التي تواجه الأمن السيبراني.

وتعترف الحكومة بالتهديدات الماثلة في كل البيئات السيبرانية، بما فيها الحوسبة السحابية والنظم الجوالة، وترى أنها تمثل جانبا رئيسيا من أولويات الأمن والدفاع لبروني دار السلام.

كندا

[الأصل: بالإنكليزية]
[١٧ تموز/يوليه ٢٠١٧]

فيما يخص المسائل السيبرانية، ترى كندا:

(أ) أن الفضاء السيبراني الحر والمفتوح والآمن يتسم بأهمية حاسمة لتعزيز الأمن والرخاء وحقوق الإنسان؛

(ب) أن القانون الدولي الحالي ينطبق على استخدام الدول لتكنولوجيا المعلومات والاتصالات؛

(ج) أن تعزيز المعايير التي تحكم السلوك في أوقات السلم يساعد على تهيئة بيئة تسترشد الدول فيها بمبادئ السلوك المسؤول فيما تقوم به من أعمال؛

(د) أن التدابير العملية لبناء الثقة طريقة ثبتت فعاليتها في الحد من خطر نشوب النزاع المسلح.

وعلى الصعيد الوطني، أصدرت الحكومة في عام ٢٠١٠ استراتيجية لأمن السيبراني التي ركزت على تأمين النظم السيبرانية الكندية وحماية الكنديين على شبكة الإنترنت. وانتهت الحكومة مؤخرا من استعراض تدابير الأمن السيبراني القائمة. واستنادا لهذا الاستعراض، سيَصدر في أواخر عام ٢٠١٧ النهج الجديد الذي سيتبعه البلد في مجال الأمن السيبراني.

وتتضمن السياسة الدفاعية لعام ٢٠١٧ استثمارات جديدة وتوجيها جديدا للسياسات من أجل تحسين الاستفادة من القدرات السيبرانية في دعم العمليات العسكرية. وستخضع القدرات السيبرانية الفعالة للقوات الكندية لنفس القواعد الصارمة التي تخضع لها الأدوات العسكرية الأخرى، بما في ذلك القوانين المحلية والدولية وقواعد الاشتباك الواجبة الانطباق.

وعلى الصعيد الدولي، تنشط كندا بعدد من الطرق:

(أ) تواصل كندا التشجيع على تطوير المعايير التي تحكم سلوك الدول في الفضاء السيبراني في أوقات السلم، بما في ذلك النتائج التي خلص إليها فريقا الخبراء الحكوميين الدوليين المعنيان بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، في الفترتين ٢٠١٢-٢٠١٣ و ٢٠١٤-٢٠١٥؛

(ب) صدَّقت كندا على اتفاقية مجلس أوروبا للجرائم السيبرانية (اتفاقية بودابست) في تموز/يوليو ٢٠١٥. وتشجع كندا البلدان على أن تصبح أطرافا في الاتفاقية، أو أن تتخذها نموذجا لتنفيذ قوانينها المتعلقة بالجرائم السيبرانية؛

(ج) خصصت كندا، منذ عام ٢٠٠٧، مبلغ ١١ مليون دولار لدعم مشاريع بناء القدرات في مجال الأمن السيبراني؛

(د) تتعاون كندا أيضا مع الولايات المتحدة من أجل تنفيذ خطة عمل الأمن السيبراني المشتركة بين كندا والولايات المتحدة، والتي تهدف إلى تعزيز قدرة بنيتها التحتية السيبرانية على الصمود؛

(هـ) دأبت كندا على تنفيذ تدابير لبناء الثقة في مختلف المحافل، بما فيها منظمة الأمن والتعاون في أوروبا والمنتدى الإقليمي لرابطة أمم جنوب شرق آسيا؛

(و) تدعم كندا ما تبذله منظمة حلف شمال الأطلسي من جهود من أجل تعزيز قدرات الدفاع السيبراني للمنظمة ولفرادى الحلفاء.

كوبا

[الأصل: بالإسبانية]
[٥ نيسان/أبريل ٢٠١٧]

يمكن للتطورات العلمية والتكنولوجية أن يكون لها، كما جاء في قرار الجمعية العامة ٧١/٢٨، تطبيقات مدنية وعسكرية على حد السواء، ويجب الحيلولة دون أن تؤثر هذه التطورات على الأمن الدولي.

ومن الضروري اتخاذ تدابير لتعزيز النظر، على الصعد المتعددة الأطراف، في الأخطار القائمة والمحتملة في ميدان أمن المعلومات، وكذلك في الاستراتيجيات الممكنة لدرئها والتصدي لها.

ولا سبيل إلى منع تحويل الفضاء الإلكتروني إلى مسرح للعمليات العسكرية سوى التعاون المشترك بين جميع الدول.

وتدعم كوبا عمل فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، المنشأ بموجب القرار ٣٢/٥٨، والذي يشارك فيه خبير كوبي.

ونرى أن من الضروري إنشاء إطار تنظيمي دولي ملزم قانونا، يكون مكملا للقانون الدولي القائم ولكنه يسري على تكنولوجيات المعلومات والاتصالات.

وإن نظم المعلومات والاتصالات السلكية واللاسلكية يمكن تحويلها إلى أسلحة عندما تُصمَّم أو تُستخدَم من أجل إلحاق ضرر بالبنية التحتية لدولة من الدول. ويجب على جميع الدول أن تحترم المعايير الدولية القائمة في هذا المجال. ويتعين أن تكون إمكانات الوصول إلى نظم المعلومات أو الاتصالات السلكية واللاسلكية لدى دولة أخرى متمشية مع ما أُبرم من اتفاقات التعاون الدولي، وينبغي أن تستند إلى مبدأ موافقة الدولة المعنية. ويجب أن يتقيد طابع ونطاق التبادلات بقوانين الدولة التي تتيح إمكانية الوصول إلى نظامها.

ويشكل الاستخدام العدائي للاتصالات السلكية واللاسلكية، بنية معلنة أو خفية تتوخى تقويض النظام القانوني والسياسي للدول، انتهاكا للمعايير الدولية المتعارف عليها في هذا المجال، ويمثل استخداما غير قانوني وغير مسؤول لهذه الوسائل. ويمكن أن يؤدي هذا الاستخدام إلى نشوء توترات وأوضاع غير مؤاتية لتحقيق السلام والأمن الدوليين، ويمكن أن يؤثر تأثيرا سلبيا في سلامة البنى التحتية للدول مما يضر بأمنها في كل من المجالين المدني والعسكري.

وتكرر كوبا الإعراب عن قلقها من قيام أفرادٍ ومنظماتٍ ودولٍ باستخدام النظم الحاسوبية للدول الأخرى، على نحو سري وغير مشروع، بغرض مهاجمة بلدان ثالثة لأن ذلك قد يتسبب في نشوب نزاعات دولية.

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. وفي عام ٢٠١٦ جرى، انطلاقا من أراضي الولايات المتحدة، بث ما متوسطه ١ ٨٧٥ ساعة من البرامج غير المشروعة أسبوعيا ضد كوبا، باستخدام ٢٥ ترددا. وتتعارض البرامج الإذاعية والتلفزيونية المستمرة التي تبثها الولايات المتحدة ضد كوبا مع مقاصد ميثاق الأمم المتحدة ومبادئه والقانون الدولي ومع الأنظمة الصادرة عن الاتحاد الدولي للاتصالات.

ومرة أخرى، تدعو كوبا إلى الوقف الفوري لهذه السياسات العدوانية التي تنتهك سيادة كوبا والتي تتنافى، علاوة على ذلك، مع إقامة علاقات تستند إلى الاحترام المتبادل والتعاون بين الدول.

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.

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 فيما بينها 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 الخامس للجماعة، الذي عقد في بونتا كانا بالجمهورية الدومينيكية في كانون الثاني/يناير ٢٠١٦، تم مجددا إبراز أهمية تكنولوجيات المعلومات والاتصالات، بما في ذلك شبكة الإنترنت، بوصفها أدوات لتعزيز السلام ورفاه الإنسان والتنمية والمعرفة والإدماج الاجتماعي والنمو الاقتصادي.

وتكرر كوبا – تأكيد أن التعاون الدولي أمرٌ أساسي لمواجهة المخاطر التي تنطوي عليها إساءة استخدام تكنولوجيات المعلومات والاتصالات. وتشدد كوبا أيضا على أنه يتعين على الاتحاد الدولي للاتصالات أن يقوم بدور مهم في المناقشة الحكومية الدولية بشأن مسائل الأمن السيبراني.

إكوادور

[الأصل: بالإسبانية]
[٢٨ تموز/يوليه ٢٠١٧]

ترى إكوادور أن – الأمن في العلاقات الدولية يجب أن يستند إلى الثقة والاحترام بين الدول. والحالات التي يتواصل الكشف عنها لاستخدام نظم التجسس الواسعة النطاق والعشوائية في رصد اتصالات جميع المواطنين في جميع أنحاء العالم، فضلا عن استخدام تكنولوجيات المعلومات والاتصالات على نحو ينتهك القانون الدولي، تنتقص من مبدأي احترام السيادة وعدم التدخل في الشؤون الداخلية للدول. وعلاوة على ذلك، فإن هذه الإجراءات تُدخل عنصراً خطيراً من عدم الاستقرار في العلاقات بين الدول وتؤثر بالتالي على الأمن الدولي. وتنتهك نظمُ التجسس هذه أيضا مختلفَ حقوق الإنسان الأساسية.

ولهذا السبب، تؤيد إكوادور الجهود المبذولة لمواصلة دراسة التهديدات القائمة والمحتملة في ميدان أمن المعلومات والتدابير التعاونية التي يمكن اتخاذها للتصدي لها، فضلا عن الطريقة التي ينبغي بها تطبيق القانون الدولي على استخدام الدول لتكنولوجيات المعلومات والاتصالات، وكذلك معايير وقواعد ومبادئ السلوك المسؤول للدول في هذا المجال.

السلفادور

[الأصل: بالإسبانية]
[٢٤ أيار/مايو ٢٠١٧]

إن السلفادور، امتثالا لالتزاماتها تجاه الأمم المتحدة، يشرفها أن تفيد، فيما يتعلق بقرار الجمعية العامة ٧١/٢٨ بشأن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، بأن القوات المسلحة في السلفادور قد اقتنت في عام ٢٠١٦ نظاما لتشفير وثائقها المؤسسية من أجل تعزيز أمن المعلومات. والنظام في مرحلة التنفيذ.

إستونيا

[الأصل: بالإنكليزية]
[٣١ أيار/مايو ٢٠١٧]

تُسلِّم إستونيا بأن الأمن في العالم السيبراني أصبح مسألة بالغة الأهمية في سياق الأمن الدولي الأوسع نطاقا. ولذلك، فإن دور الأمم المتحدة ومشاركتها يكتسيان أهمية متزايدة.

لقد كان الأمن على شبكة الإنترنت إحدى الأولويات العليا للحكومة الإستونية. والوثيقة التوجيهية الرئيسية بشأن هذه المسألة هي الاستراتيجية الوطنية للأمن السيبراني (٢٠١٤-٢٠١٧). ويدعم مجلس الأمن السيبراني التابع للجنة الأمن الحكومية التعاون فيما بين الوكالات على المستوى الاستراتيجي ويشرف على تنفيذ أهداف استراتيجية الأمن السيبراني. وقد أنشئ في تالين مركز الامتياز التعاوني للدفاع السيبراني، التابع لمنظمة حلف شمال الأطلسي، ووصل عدد الدول الأعضاء المساهمة فيه حتى ٣٠ أيار/مايو ٢٠١٧ إلى ٢٠ دولة.

وإستونيا مقتنعة بأن الاستخدام الواسع للخدمات الرقمية يتطلب درجة عالية من الأمن السيبراني. وبالنسبة لإستونيا، فإن الجانبين الاجتماعي - الاقتصادي والسياسي - العسكري للأمن السيبراني متشابكان. وترى استونيا أنه من الأساسي أن تمتنع البلدان عن مهاجمة البنى التحتية الحيوية الوطنية. وتدعو إستونيا أيضا إلى اتباع سلوك مسؤول تجاه البنى التحتية العالمية للاتصالات لتعزيز الوصول إلى المعلومات والثقة بتكنولوجيا المعلومات والاتصالات. وترى أن من مسؤولية كل بلد صياغة وإنفاذ قوانين وطنية تساعد في ضبط الاستخدامات الضارة لتكنولوجيا المعلومات والاتصالات من جانب جهات من غير الدول، والتماس سبل لتحسين صياغة ونشر وترويج سياسات وأساليب سرد وطرق محاججة مسؤولة وفعالة فيما يخص الفضاء السيبراني.

وإستونيا عضو في فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وذلك للمرة الرابعة على التوالي. وقد عمل الفريق كمنتدى مثمر للغاية. وفي المستقبل، يمكن أن يكون أداة مفيدة لا فيما يتعلق بدراسة التهديدات السيبرانية وسبل الانتصاف الممكنة فحسب، بل لفهم كيفية تنفيذ البلدان المختلفة للقوانين والمعايير والقواعد والمبادئ الدولية القائمة. وترى إستونيا أنه ينبغي للفريق أن يواصل عمله بشأن النهوض بالحوار فيما بين الدول الأعضاء، مما ييسر تبادل المعلومات وأفضل الممارسات. وبالإضافة إلى ذلك، ينبغي له أن يناقش تدابير التعاون العملي وآلياته للنهوض ببناء قدرات الدول الأعضاء، بهدف نهائي يتمثل في تزويدها بالكفاءة والقدرة على مواجهة التحديات المتعلقة بالإنترنت من جميع جوانبها.

ومن المهم المضي قدما بالتقدم الذي أحرز في اجتماعات فريق الخبراء الحكوميين للفترة ٢٠١٤-٢٠١٥ من خلال مواصلة تعزيز معايير سلوك الدول التي تدعم الانفتاح والمساءلة وغير ذلك من القيم الديمقراطية الأخرى في الفضاء السيبراني. وتأمل إستونيا أن يصدر الفريق مرة أخرى تقريرا بتوافق الآراء في حزيران/يونيه ٢٠١٧.

فنلندا

[الأصل: بالإنكليزية]
[٢١ تموز/يوليه ٢٠١٧]

ترحب فنلندا بفرصة تقديم تقرير عن تنفيذ قرار الجمعية العامة ٧١/٢٨.

وتشمل الجهود المبذولة على الصعيد الوطني ما يلي:

(أ) تحدد الاستراتيجية الوطنية للأمن السيبراني (٢٠١٣) وبرنامج تنفيذها المُحَدَّث (٢٠١٧) المبادئ التوجيهية والإجراءات الرئيسية في مجال تعزيز الأمن السيبراني وقدرته على الصمود؛

(ب) أنشأت فنلندا مركزا وطنيا للأمن السيبراني ومركزا لمنع الجرائم السيبرانية، وعينت سفيرا للشؤون السيبرانية في وزارة الخارجية. واعتُمدت الاستراتيجية الوطنية لأمن المعلومات في عام ٢٠١٦.

(ج) تسهم فنلندا بنشاط في التعاون في مجال الفضاء السيبراني داخل الاتحاد الأوروبي؛

(د) تؤيد فنلندا الاستفادة من الأشكال المختلفة لتكنولوجيا المعلومات والاتصالات في مجال التنمية، ومشاريع بناء القدرات ذات الصلة بالفضاء السيبراني. وهي من الشركاء المؤسسين للمنتدى العالمي لخبرات الفضاء السيبراني. وفي عام ٢٠١٦، انضمت إلى الصندوق الاستئماني للشراكة من أجل التنمية الرقمية التي أقامها البنك الدولي. وتؤيد فنلندا إدارة شبكة الإنترنت استنادا إلى نموذج يقوم على تعدد أصحاب المصلحة. وقد شاركت بنشاط في القمة العالمية لمجتمع المعلومات وعملية متابعته، بما في ذلك المشاركة في أعمال منتدى إدارة الإنترنت وتوفير التمويل له. وعُقد المنتدى الفنلندي الثامن لشبكة الإنترنت في هلسنكي في نيسان/أبريل ٢٠١٧؛

(هـ) تشارك فنلندا بنشاط في الحوار بشأن مسائل الفضاء السيبراني في المحافل المتعددة الأطراف والإقليمية، وعلى المستوى الثنائي. وفي إطار منظمة الأمن والتعاون في أوروبا، تعمل على تعزيز الثقة والأمن والاستقرار في الفضاء السيبراني، وتقوم بتنفيذ التدابير المتفق عليها في مجال بناء الثقة في الفضاء السيبراني.

(و) صدقت فنلندا على تقرير عام ٢٠١٥ الصادر عن فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وتشارك بنشاط في عمل الفريق الحالي. وشاركت بنشاط في المناقشات الدائرة بشأن القانون الدولي في الفضاء السيبراني، ومثال ذلك المشاورات المتعلقة بالإصدار ٢,٠ لدليل تالين، كما شاركت في حلقات عمل نظمها معهد الأمم المتحدة لبحوث نزع السلاح؛

(ز) انضمت فنلندا إلى تحالف الحرية على شبكة الإنترنت في عام ٢٠١٢، وهي تساهم في شراكة المدافعين عن الحرية الرقمية. ونظمت مؤتمر اليوم العالمي لحرية الصحافة لعام ٢٠١٦، الذي عقد في هلسنكي؛

(ح) تعد فنلندا طرفا في اتفاقية مجلس أوروبا المتعلقة بالجرائم السيبرانية. وتستهدف خطةٌ استراتيجية جديدة للشرطة (٢٠١٥) تخصيص الموارد لمنع الجريمة الإلكترونية وتطوير الدراية في مجال الأمن السيبراني. وهناك أيضا خطة شاملة لمنع الجرائم السيبرانية.

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

(أ) عمل فريق الخبراء الحكوميين الحالي الذي توليه فنلندا أهمية كبيرة وهي مستعدة للإسهام في نجاحه، بما في ذلك مواصلة تحديد قواعد السلوك المسؤول للدول في الفضاء السيبراني، مع التركيز بصفة خاصة على الأنشطة المضطلع بها في وقت السلم؛

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

(ج) مواصلة دعم بناء القدرات السيبرانية لتعزيز القدرة على الصمود وتوطيد الأمن في الفضاء السيبراني؛

(د) الحوار بين أصحاب المصلحة المتعددين، الذي ستواصل فنلندا دعمه وتشجيعه، وتعزيز الشراكات بين القطاعين العام والخاص على الصعيدين الوطني والدولي.

ألمانيا

[الأصل: بالإنكليزية]
[٣٠ أيار/مايو ٢٠١٧]

يتيح تطور تكنولوجيا المعلومات والاتصالات العديد من الفرص الاقتصادية والاجتماعية والعلمية. وقد أضحت كفالة الوصول إلى الفضاء السيبراني، والحفاظ على سلامة البيانات وصحتها وسريتها في الفضاء السيبراني مسألتين حيويتين في القرن الحادي والعشرين.

وفي عالم يزداد ترابطا بصورة مطردة، تعتمد الدول والبنى التحتية الحيوية ومؤسسات الأعمال التجارية والأفراد على الأداء الموثوق به لتكنولوجيا المعلومات والاتصالات. وقد لا تبقى عواقب سوء استخدام تكنولوجيا المعلومات والاتصالات مقتصرة على الفضاء الإلكتروني، إذ بإمكانها أن تسبب أضرارا اجتماعية واقتصادية وسياسية وأضرار أخرى. فعلى سبيل المثال، يمكن أن تؤثر الهجمات التي تستهدف مؤسسات الدولة أو العمليات الديمقراطية والسياسية على النظام العام والسلامة العامة.

وتتعامل ألمانيا مع هذه التحديات عن طريق تعزيز الالتزام بالقانون الدولي والتقيد بالقواعد وبناء الثقة في سياق استخدام الدولة لتكنولوجيا المعلومات والاتصالات على ثلاثة مستويات:

(أ) على المستوى العالمي، تدعم ألمانيا الجهود الرامية إلى الاتفاق على كيفية تطبيق القانون الدولي على استخدام الدولة لتكنولوجيا المعلومات والاتصالات ووضع معايير أو قواعد أو مبادئ طوعية غير ملزمة للسلوك المسؤول للدول الذي يهدف إلى إيجاد بيئة مفتوحة وآمنة ومستقرة ومتاحة وسلمية لتكنولوجيا المعلومات والاتصالات. ومما له أهمية خاصة في هذا السياق عمل الأفرقة المتعاقبة من الخبراء الحكوميين المعنيين بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي. وقد شارك الخبراء الألمان بنشاط في تلك الأفرقة، وتلتزم ألمانيا بتعزيز توصياتهم. وقد حان الوقت الآن لتوسيع نطاق المناقشة وإشراك أعضاء الأمم المتحدة على نطاق أوسع، بغية إضفاء طابع عالمي على العمل المتعلق بتكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي. وتؤيد ألمانيا قيام الأمم المتحدة بدور قيادي وتعزيز قدراتها في هذا المجال. وتشمل المسائل التي يتعين المضي في استكشافها تبادل

المعلومات والتعاون على الصعيد الدولي بشأن تحديد مصادر الهجمات السيبرانية. وينبغي أن تكون هناك قواعد واضحة ومحترمة عالميا تتناول الاستخدام الخبيث للقدرات السيبرانية، فضلا عن التجسس عبر الإنترنت لأغراض اقتصادية؛

(ب) وعلى المستوى الإقليمي، تساعد تدابير بناء الثقة على التصدي لخطر تصاعد حوادث تكنولوجيا المعلومات والاتصالات إلى أزمات سياسية أو حتى عسكرية. وفي إطار منظمة الأمن والتعاون في أوروبا، ظلت ألمانيا نشطة منذ سنوات في تحديد وتنفيذ تدابير بناء الثقة الرامية إلى تحقيق الأمن في مجال تكنولوجيا المعلومات والاتصالات وفي استخدام الدولة لها. وخلال تولي ألمانيا رئاسة منظمة الأمن والتعاون في أوروبا في عام ٢٠١٦، وافقت الدول المشاركة على تدابير إضافية من هذا القبيل. ووافق المجلس الوزاري لمنظمة الأمن والتعاون في أوروبا لعام ٢٠١٦، الذي عقد في هامبورغ، على هذه التوصيات، وأصدر توجيهات تهدف لا إلى تنفيذها فحسب، بل تهدف أيضا إلى الاضطلاع بمزيد من العمل. وهذا يحتاج إلى عدم الاقتصار على الجوانب السياسية – العسكرية ومراعاة الأبعاد المتعددة للأمن. وخارج منظمة الأمن والتعاون في أوروبا، تدعم ألمانيا أيضا جهودا مماثلة في منظمات إقليمية في قارات أخرى.

(ج) وعلى المستوى الثنائي، تواصل ألمانيا عقد حوارات سيبرانية وتجري مشاورات سيبرانية منتظمة مع شركاء متعددين. واستنادا إلى علاقات الشراكة القائمة، تدعم ألمانيا أيضا الجهود المبذولة لبناء قدرات الأمم الأخرى في مجال الأمن السيبراني. وقررت الحكومة الألمانية، لدى تحديث استراتيجيتها المتعلقة بالأمن السيبراني في تشرين الثاني/نوفمبر ٢٠١٦، العمل على إنشاء معهد ألماني للأمن السيبراني الدولي بغية تنظيم تلك الجهود في إطار ممنهج وزيادتها.

وتعد الجهود التي تبذلها ألمانيا بشأن المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي جزءاً من العمل المكثف للنهوض بأمن تكنولوجيا المعلومات والاتصالات بوجه عام. وتهدف التدابير التنظيمية الوطنية الأخيرة، مثل قانون أمن تكنولوجيا المعلومات لعام ٢٠١٥، وتحديث الاستراتيجية الوطنية للأمن السيبراني لعام ٢٠١٦، إلى تحسين أمن تكنولوجيا المعلومات والاتصالات من جميع جوانبه في ألمانيا.

اليونان

[الأصل: بالإنكليزية]
[٢٦ أيار/مايو ٢٠١٧]

في إطار مجلس أوروبا، صدقت اليونان بموجب القانون ٢٠١٦/٤٤١١ (الجريدة الحكومية A 142، ٣ آب/أغسطس ٢٠١٦) على اتفاقية مجلس أوروبا المتعلقة بالجرائم السيبرانية (بودابست، ٢٠٠١/١١/٢٣) وعلى البروتوكول الإضافي للاتفاقية المتعلق بتجريم الأعمال ذات الطابع العنصري والمنطوية على كراهية الأجانب التي ترتكب عن طريق النظم الحاسوبية (ستراسبورغ، ٢٨ كانون الثاني/يناير ٢٠٠٣).

وتجدر الإشارة إلى أنه يجري حالياً دمج الأمر التوجيهي للاتحاد الأوروبي بشأن أمن نظم الشبكات والمعلومات في القوانين الوطنية. ويكتسي هذا الأمر التوجيهي أهمية قصوى من أجل تعزيز

القدرة على الصمود في مواجهة الهجمات السيبرانية على الصعيد الوطني، ويحدد عددا من الالتزامات ذات الصلة بهذه الغاية لجميع الدول الأعضاء في الاتحاد الأوروبي، ويشمل أيضا اعتماد استراتيجية وطنية بشأن أمن الشبكات ونظم المعلومات.

ووفقا للمعلومات المقدمة من وزارة الدفاع اليونانية، تقوم رؤية اليونان للأمن السيبراني على تطوير مجموعة كاملة من القدرات للدفاع عن بناها التحتية وشبكاتها الوطنية ضد أحدث التهديدات السيبرانية ومرتكبي الجرائم السيبرانية. ويشمل ذلك معالجة قضايا الدفاع السيبراني على أعلى مستوى استراتيجي داخل المنظمات المعنية بالدفاع في البلد، وزيادة إدماج الدفاع السيبراني في العمليات، وتوسيع نطاق التغطية لتشمل الشبكات القابلة للنشر. وتم الاضطلاع بالجهود التالية على الصعيد الوطني لتعزيز أمن المعلومات وتشجيع التعاون الدولي

(أ) يجري حاليا وضع إطار الاستراتيجية الوطنية للدفاع السيبراني، أما الاستراتيجية الوطنية للأمن السيبراني فتمضي في سبيلها كي تتحول إلى قانون، وهي استراتيجية تنظم الإطار العام للأمن السيبراني وتحدد الإجراءات اللازمة للحفاظ على الحد الأدنى من متطلبات الأمن السيبراني؛

(ب) أصبح الدفاع السيبراني بالفعل جزءاً من خطط عمليات الدفاع الوطني، بينما أُدرج النظام الوطني للإنذار بحالات الطوارئ في معظم وثائق السياسات التي تشير إلى نظم المعلومات، وأُدمج في جميع العمليات الوطنية الرئيسية. وأدرج الأمن السيبراني في خطط العمليات المتعلقة بفترات الأزمات في جميع المؤسسات العامة؛

(ج) وقد طورت اليونان قدرات الاستجابة للطوارئ وهي تحسنها باستمرار في إطار المركز العسكري للتصدي للحوادث الحاسوبية. ويمكن أن تنتشر أفرقة الرد السريع في غضون مهلة قصيرة للمساعدة على التصدي للحوادث السيبرانية واستعادة القدرة على العمل بعد وقوعها، وذلك فيما يخص الشبكات التابعة للمؤسسات العسكرية أو الشبكات العامة. وقد تم دمج التعليمات المتعلقة باستعادة القدرة على العمل بعد الأعطال أو الهجمات السيبرانية في الوثائق المتعلقة بسياسة أمن المعلومات الحاسوبية؛

(د) ويجري حاليا إنشاء مركز لعمليات الأمن السيبراني لجميع نظم شبكات الدفاع العسكري الوطنية، بينما توجد على الصعيد الوطني أربعة أفرقة مسؤولة عن التصدي للطوارئ الحاسوبية في القطاعين العام والخاص.

وفيما يلي التدابير التي يمكن أن يتخذها المجتمع الدولي من أجل تحقيق مستوى أعلى من أمن المعلومات:

(أ) زيادة قدرات الاستجابة للحوادث، وقدرات رصد الشبكات، والدفاع العملي ضد التهديدات السيبرانية من خلال مراكز عمليات وطنية للأمن السيبراني تتوافر لها مقومات التشغيل الكامل؛

(ب) إدماج الدفاع عن الفضاء السيبراني في العمليات إدماجا تاما؛

(ج) وضع استراتيجيات وطنية للأمن السيبراني والدفاع السيبراني؛

(د) تعزيز الوعي السيبراني لدى الموظفين العاملين في مجال الدفاع السيبراني وتحسين القدرات التقنية القائمة؛

(هـ) توفير التدريب المستمر للموظفين العاملين في منظمات الدفاع السيبراني؛

(و) تحقيق التناسق بين القوانين الوطنية والقوانين والتوجيهات العالمية المتعلقة بالأمن السيبراني.

ووفقا للمعلومات المقدمة من الشرطة اليونانية، تتضمن مهمة شعبة الجرائم السيبرانية التابعة للشرطة اليونانية، وفقا للمادة ٣٠ من المرسوم الرئاسي ٢٠١٤/١٧٨، منع الجرائم المرتكبة عبر الإنترنت أو غيرها من وسائط الاتصال الإلكترونية والتحقيق فيها والمقاضاة عليها. وشعبة الجرائم السيبرانية هي دائرة مركزية مستقلة يسند الإشراف عليها مباشرة إلى رئيس مقر قيادة الشرطة اليونانية.

وتتولى إحدى وحدات الشعبة المسؤولية عن أمن الاتصالات الإلكترونية والهاتفية وحماية البرامجيات وحماية حقوق التأليف والنشر. وبصورة أكثر تحديدا، تقوم الوحدة بالتحقيق في حالات الاختراق غير المشروع للأنظمة الحاسوبية، وسرقة البرامجيات والبيانات الرقمية والمصنفات السمعية البصرية في جميع أنحاء البلد أو تدميرها أو الاتجار بها.

وتعمل شعبة الشرطة السيبرانية التابعة للشرطة اليونانية بالتعاون الوثيق مع الهيئة الوطنية لمكافحة الهجمات الإلكترونية، التي هي جزء من دائرة الاستخبارات الوطنية. وتتمثل مهمة الهيئة الوطنية في العمل على منع الهجمات الإلكترونية ضد شبكات الاتصالات ومرافق تخزين البيانات ونظم تكنولوجيا المعلومات والاتصالات والتصدي لها بالسلب والإيجاب. وإضافة إلى ذلك، فإن السلطة مسؤولة عن تجهيز البيانات وإبلاغ السلطات المختصة.

اليابان

[الأصل: بالإنكليزية]
[٢٧ تموز/يوليه ٢٠١٧]

ترى اليابان أن الفضاء السيبراني ينبغي أن يكون فضاء تُكفل فيه الحرية دون فرض قيود غير لازمة، ولا يمنع كل من يرغب في الدخول إليه من ذلك، ولا يُستبعد منه دون سبب مشروع. وتتقيد جهود اليابان في هذا الصدد بالمبادئ الخمسة التالية: التدفق الحر للمعلومات، وسيادة القانون، والانفتاح، والحوكمة الذاتية، واتباع نهج يقوم على تعدد أصحاب المصلحة.

واستنادا إلى استراتيجية الأمن السيبراني التي وُضعت في أيلول/سبتمبر ٢٠١٥، تبذل اليابان جهودا لتعزيز أمن المعلومات.

وتقوم الجهود التي تبذلها اليابان على الركائز الثلاث التالية: تعزيز سيادة القانون في الفضاء السيبراني، وتدابير بناء الثقة، وبناء القدرات.

وفيما يتعلق بتعزيز سيادة القانون، تسهم اليابان على نحو فعال في النقاش الدولي الرامي إلى ترويج فهم مشترك مفاده أن القانون الدولي الحالي ينطبق في الفضاء السيبراني، وكذلك في وضع قواعد طوعية غير ملزمة. وتشكل هذه القواعد أساساً لكفالة استقرار المجتمع الدولي وإمكانية التنبؤ بمسلكه.

وبالنظر إلى الخصائص الفريدة لتكنولوجيا المعلومات والاتصالات، فإن الأمر يقتضي مزيدا من الإيضاح لكيفية تطبيق كل واحد من القواعد والمبادئ المختلفة.

ولدى النهوض بتدابير بناء الثقة، من الضروري ضمان الشفافية وتقاسم المعلومات؛ بيد أن مستوى التدابير المتخذة يختلف من دولة إلى أخرى، حيث أن لكل دولة سلطة تحديد المستوى الذي تتوخى أن تتصرف في حدوده. وتشارك اليابان في تعزيز بناء الثقة من خلال الحوار الثنائي والأطر المتعددة الأطراف مثل المنتدى الإقليمي لرابطة أمم جنوب شرق آسيا. ولا بد من إجراء دراسة عن سبل إقامة تعاون حقيقي.

وفيما يتعلق ببناء القدرات، ما برحت اليابان تشجع على استحداث قوانين ونظم أساسية وأطر سياساتية للأمن السيبراني، وما فتئت تشارك في ضمان الأمن السيبراني للهيئات الحكومية ومشغلي البنية التحتية الأساسية للمعلومات؛ ووضع تدابير لمكافحة الجريمة السيبرانية؛ وتنمية الموارد البشرية من أجل التشجيع على الاستعانة بخبراء الأمن السيبراني؛ والبحث والتطوير في مجال تكنولوجيات الأمن السيبراني. واستنادا إلى هذه الخبرات والمعارف المتراكمة، ستواصل اليابان التعاون الاستباقي على صعيد بناء القدرات.

الأردن

[الأصل: بالعربية]
[٢٣ آذار/مارس ٢٠١٧]

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، بما ينعكس على مستوى الفرد داخل المجتمع وانفتاحه على المجتمع الدولي بشتى النواحي.

إن التقدم الهائل السريع 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) مشفرة 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 وجيش الولايات المتحدة الأمريكية وضمن المعايير الدولية ذات التشفير عالي 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 عالية الأهمية على المستوى الوطني:

(أ) استخدام وسائل التشفير لجميع الشبكات وأنظمة الاتصال الصوتي والبياني وبالفيديو؛

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

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

(د) تطبيق إجراءات أمن المعلومات والاتصالات ومبدأ الحاجة للمعرفة وتحديد 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 وهي:

'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 لضمان أمن المعلومات والأمن السيبراني، ٢٠١٢ من مجلس رئاسة 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 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 (فريق 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 ما يلي:

(أ) تسريع إنهاء الفقر مثل 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 مجموعة فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي المنشأ في عام ٢٠٠٣؛

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

مدغشقر

[الأصل: بالفرنسية]
[٢٠ حزيران/يونيه ٢٠١٧]

تستند توصيات منظمة الأمم المتحدة إلى الأمن الدولي وتتوخى ما يلي:

- مواصلة الدراسات الرامية إلى تعزيز أمن النظم المعلوماتية العالمية والنظم العالمية للاتصالات السلكية واللاسلكية؛
- تقييم جميع التهديدات الموجودة أو التي قد توجد في مجال أمن المعلومات واعتماد استراتيجيات ملائمة للتعامل مع هذه الآفة؛
- التزام المسؤولين الحكوميين بتعزيز أمن المعلومات، بهدف وضع رؤية مشتركة للأمن على الصعيد العالمي؛

ويتناول القرار ٢٨/٧١ تحديدا مجال المعلومات والاتصالات السلكية واللاسلكية، وهو ميدان يشهد نموا هائلا في مدغشقر. وتتطلب الاستجابة لهذا القرار مشورة الخبراء في هذا المجال.

هولندا

[الأصل: بالإنكليزية]
[٣١ أيار/مايو ٢٠١٧]

ترحب هولندا ترحيبا حارا بالفرصة التي أتيحت لها لعرض استجابتها لقرار الجمعية العامة ٢٨/٧١.

ويشكل الفضاء السيبراني، ولا سيما شبكة الإنترنت، موردا بالغ الأهمية للنمو الاقتصادي والمجتمعي. ووَضعت الأهمية المتزايدة لهذا الفضاء المجتمع الدولي أمام تحديات جديدة. وتُعد المجتمعات شديدة الترابط والاعتماد على شبكة الإنترنت وتكنولوجيا المعلومات والاتصالات وأصبحت أكثر عرضة لسوء استخدام هذه التكنولوجيات. وتتجلى التوترات الجيوسياسية في الفضاء السيبراني وتستخدم الدول والجهات الفاعلة الأخرى العمليات السيبرانية على نحو متزايد لتحقيق مصالحها الاستراتيجية. ومع ذلك، قد تتسبب تلك العمليات السيبرانية في عدم استقرار العلاقات الدولية ويمكن أن تشكل مخاطر على السلم والأمن الدوليين.

ومن الواضح أن الحد من هذه المخاطر يستلزم تعاونا دوليا. وفي ضوء ما سبق، فإن هولندا تكثف مشاركتها في مجال الدبلوماسية السيبرانية من أجل صون السلام والاستقرار في الفضاء السيبراني، وتعزيز النظام القانوني الدولي، وتعزيز ثقافة الأمن التعاوني، المبينة في استراتيجيتها السيبرانية الدولية ”بناء الجسور الرقمية“.

ويتخذ المجتمع الدولي خطوات للتصدي لتلك المخاطر. وتتسم تقارير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي بأهمية كبيرة في هذا الصدد. وهولندا ممتنة أيضا لأنه سيتسنى لها أن تساهم في فريق الخبراء الحكوميين لعام ٢٠١٧.

وتواصل هولندا التشجيع على إجراء حوار شامل بشأن سلوك المسؤول للدول في الفضاء السيبراني، وتدافع عن حقوق الإنسان على شبكة الإنترنت، وتعزز بناء القدرات من خلال أنشطة مختلفة. وبذلت هولندا جهودا شتى، منها على وجه الخصوص ما يلي:

(أ) اهتداءً بأفضل نهج لدعم تطوير النظام القانوني الدولي، نَظمت هولندا مشاورات بين المستشارين القانونيين للدول بشأن الإصدار ٢,٠ من دليل تالين المتعلق بالقانون الدولي المنطبق على العمليات السيبرانية؛

(ب) دعمت هولندا معهد الأمم المتحدة لبحوث نزع السلاح في تنظيم سلسلة من ثلاث حلقات عمل بشأن المعايير السيبرانية، والقانون الدولي، والتصدي لانتشار الأدوات والتقنيات الخبيثة، ونجحت في أن تحشد للمشاركة فيها الدبلوماسيين والأوساط التقنية؛

(ج) وأخيرا، أطلقت هولندا العديد من المبادرات الرامية إلى تعزيز القواعد التوجيهية، بما في ذلك اللجنة العالمية المعنية باستقرار الفضاء السيبراني، التي ستعمل على وضع مقترحات القواعد والسياسات الرامية إلى توطيد الأمن والاستقرار الدوليين.

وتهدف كل هذه الجهود إلى تحقيق مزيد من الاستقرار والأمن للعلاقات الدولية في المجال الرقمي وللفضاء السيبراني نفسه. وتعتقد هولندا أن هذا الأمر ضروري للحد من خطر نشوب نزاع وللحفاظ على فضاء سيبراني مفتوح وحر وآمن.

النرويج

[الأصل: بالإنكليزية]
[٢٧ تموز/يوليه ٢٠١٧]

تعد النرويج من بلدان العالم الأشد استخداما للتكنولوجيا الرقمية وتعتمد بشكل متزايد على فضاء السيبراني الجيد الأداء والآمن. وتلتزم بكل صرامة بأن يكون الفضاء السيبراني حرا ومفتوحا وسلميا وآمنا كي يتسنى حماية منافعه الاقتصادية والاجتماعية وإتاحتها للجميع. ولا يعرف الفضاء السيبراني أي حدود وطنية ولا يمكن كفالة الأمن فيه إلا على الصعيد الدولي بالتعاون الوثيق بين الدول والقطاع الخاص.

الجهود المبذولة لتعزيز أمن المعلومات

النهُج الوطنية

أصدرت الحكومة كتابا أبيض بعنوان ”أمن تكنولوجيا المعلومات والاتصالات: مسؤولية مشتركة“ (٢٠١٦-٢٠١٧) يشمل خططا للإطار الوطني الكفيل بتحسين التنسيق بين الجهات الفاعلة ذات الصلة على الصعيد الوطني وإنشاء قاعدة تقنية من أجل تحسين تبادل المعلومات بين كيانات القطاعين العام والخاص.

وفي ٣١ آذار/مارس ٢٠١٧، أُنشئ المركز الموحد للتنسيق السيبراني من أجل خدمات الأمن والاستخبارات.

النهُج الدولية

أصدرت الحكومة كتابا أبيض عن التحديات الأمنية العالمية في سياستها الخارجية (٢٠١٤-٢٠١٥)، وهي تحديات تؤدي التهديدات السيبرانية دورا كبيرا فيها.

والنرويج بصدد إطلاق استراتيجية دولية للفضاء السيبراني خاصة بالبلد.

وتشارك النرويج في عدة مبادرات للتعاون الإقليمي ذات صلة بمسائل الفضاء السيبراني، من قبيل ما يلي:

(أ) العمل في إطار منظمة الأمن والتعاون في أوروبا فيما يتعلق بصياغة مجموعة من المعايير وتدابير بناء الثقة الرامية إلى الحد من مخاطر النزاعات الناشئة عن استخدام تكنولوجيا المعلومات والاتصالات؛

(ب) التعاون الوثيق مع مركز الامتياز المعني بالدفاع السيبراني التعاوني التابع لمنظمة حلف شمال الأطلسي في تالين، بما في ذلك تطبيق القانون الدولي في المجال السيبراني وفي وضع المبادئ المرعية في هذا الصدد؛

(ج) اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية.

وتؤيد النرويج عمل فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي.

وتشارك النرويج في الحوارات الثنائية والإقليمية بشأن المسائل السيبرانية، وخصوصا في إطار دول الشمال الأوروبي.

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

ترى النرويج أن القانون الدولي ينطبق على الفضاء السيبراني، وأن تقيُّد الدول بالقانون الدولي، ولا سيما الالتزامات المنصوص عليها في ميثاق الأمم المتحدة، يشكل إطارا أساسيا لما تتخذه من إجراءات في مجال استخدام تكنولوجيا المعلومات والاتصالات. ويتعين على المجتمع الدولي أن يستكشف بقدر أكبر تطبيق القانون الدولي في المجال السيبراني، وكذلك وضع معايير للسلوك المسؤول في الفضاء السيبراني.

وتعتمد استدامة شبكة الإنترنت العالمية على التوازن الصحيح بين الانفتاح والأمن والمنعة والحرية. ولا يمكن كفالة هذا الشرط إلا من خلال التعاون والحوار الدوليين، على الصعيدين العالمي والإقليمي. وينبغي أن يستمر العمل الجاري بهذا الشأن في محافل مثل الأمم المتحدة والاتحاد الأوروبي، ومنظمة التعاون والتنمية في الميدان الاقتصادي، ومنظمة الأمن والتعاون في أوروبا.

وتنطبق أيضا حقوق الإنسان العالمية على المجال السيبراني. ويجب كذلك أن تحظى نفس الحقوق التي يتمتع بها الأفراد خارج شبكة الإنترنت بالحماية داخل الشبكة، لا سيما حرية التعبير، بما في ذلك حرية التماس المعلومات وتلقيها ونقلها، والحق في الخصوصية.

باراغواي

[الأصل: بالإسبانية]
[٣١ تموز/يوليه ٢٠١٧]

تُقر باراغواي بأن أمن المعلومات مجال تتنامى أهميته على الصعيد العالمي مع اعتماد الحكومات بشكل متزايد على تكنولوجيات المعلومات والاتصالات والفضاء السيبراني. ويتعين أن تكون الاستجابة لارتفاع الهجمات الإلكترونية متضافرة وفعالة ومتناسبة. فبغير استجابة استراتيجية على الصعيد العالمي، ستفتقر الجهود التي يبذلها كل بلد بمفرده في مجال الأمن السيبراني إلى الاستدامة، وستتسم بالتناثر والازدواجية وعدم الكفاءة.

ومن أجل تعزيز أمن المعلومات على الصعيد الوطني، اعتمدت حكومة باراغواي في نيسان/أبريل ٢٠١٧ الخطة الوطنية للأمن السيبراني، التي تم إعدادها بمشاركة مباشرة من ممثلين لجميع القطاعات التي لها دور ومصالح في الفضاء السيبراني. وتُمثل هذه الخطة الأساس الذي تستند إليه الحكومة والسياسات الوطنية في هذا المجال، وتحدد الإجراءات التي ستتخذها باراغواي من أجل تعزيز أمن أصولها البالغة الأهمية ولإيجاد فضاء سيبراني آمن وموثوق ومرن. ويتضمن التشريع الجنائي في باراغواي تعريفا للجرائم السيبرانية. وخلال السنوات الخمس الماضية، استضافت باراغواي مؤتمر ومعرض البلدان الأيبيرية الأمريكية لأمن المعلومات، ويعد هذا المؤتمر منتدى لتبادل الخبرات والتعرف على التطورات وتقييم الحلول للتحديات الناجمة عن نمو استخدام تكنولوجيات المعلومات والاتصالات.

وعلى الصعيد دون الإقليمي، تملك السوق الجنوبية المشتركة (ميركوسور) هيئة دائمة هي اجتماع الهيئات المعنية بأمن المعلومات والخصوصية والبنى التحتية التكنولوجية في بلدان ميركوسور، الذي يقترح السياسات والمبادرات المشتركة المتعلقة بالأمن السيبراني. وعلاوة على ذلك، تملك منطقة الأمريكتين استراتيجية أمريكية شاملة للأمن السيبراني تقر بضرورة أن يدرك جميع المشاركين في نظم وشبكات المعلومات أدوارهم ومسؤولياتهم فيما يتعلق بالأمن، وذلك من أجل إيجاد ثقافة للأمن السيبراني.

ويعتمد إنشاء إطار فعال لحماية شبكات ونظم المعلومات على الصعيد العالمي، بما في ذلك شبكة الإنترنت، والتصدي للحوادث والتعافي منها، على اتخاذ المجتمع الدولي التدابير التالية:

- تقديم المعلومات إلى المستخدمين لتمكينهم من حماية نظم المعلومات الخاصة بهم من التهديدات ومواطن الضعف
- تشجيع الشراكات بين القطاعين العام والخاص لتعزيز التثقيف والتوعية
- تحديد وتقييم المعايير التقنية والممارسات الفضلى لكفالة أمن المعلومات المنقولة عن طريق شبكات الاتصالات، والتشجيع على اعتمادها
- التشجيع على اعتماد سياسات وتشريعات بشأن الجريمة السيبرانية لحماية المستخدمين ومنع وكبح الاستخدام غير الملائم وغير المشروع للمعدات الحاسوبية، إلى جانب احترام ما للمستعملين من حقوق في الخصوصية.

البرتغال

[الأصل: بالإنكليزية]
[٢٧ تموز/يوليه ٢٠١٧]

أشارت الجمعية العامة في قرارها ٧١/٢٨ 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. ويعني التقدم في مجال المعلومات والاتصالات السلكية واللاسلكية زيادة فرص تطوير المعارف، والتعاون فيما بين الدول، وتشجيع الإبداع البشري، وتداول المعلومات في المجتمع ككل؛ ومن ناحية أخرى، ترى البرتغال أن هذه التكنولوجيات والوسائل يحتمل أن تُستخدم بطرق منافية للاستقرار والأمن الدوليين، وقد تؤثر تأثيرا سلبيا على السلامة الوطنية للدول.

وفي القرار ٧١/٢٨ طُلب إلى الدول الأعضاء تقديم معلومات في أربعة مجالات هي:

(أ) التقييم العام لمسائل أمن المعلومات؛

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

(ج) مضمون المفاهيم الرامية إلى تعزيز أمن نظم المعلومات والاتصالات السلكية واللاسلكية على الصعيد العالمي؛

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

وقد عرض فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، في تقريره لعام ٢٠١٣ (A/68/98)، بعض التوصيات فيما يتعلق بالمجالات التالية: المعايير، والقواعد، ومبادئ السلوك المسؤول للدول؛ وتدابير بناء الثقة وتبادل المعلومات؛ وتدابير بناء القدرات.

وبناء على تلك التوصيات، تقدم البرتغال التعليقات التالية.

المعايير والقواعد ومبادئ السلوك المسؤول للدول

تعتبر البرتغال أن الأمن فيما يخص المعلومات المنقولة عبر الشبكات يتسم بالأهمية وأنه ما فتئ يتعزز.

ومن المهم تسليط الضوء على تقدم الجهود الرامية إلى تنفيذ التشريعات المتعلقة بأمن الشبكات وسلامتها، باعتماد أساليب تقييم المخاطر التي تتطلب اتخاذ تدابير أمنية تعاونية كافية، على المستويين التقني والتنظيمي، وتشمل شرط الإبلاغ عن الانتهاكات الأمنية أو اختلالات في سلامة النظم، التي لها أثر كبير على أداء الخدمات.

وعلى مستوى المفاهيم، من المهم ترسيخ الفكرة القائلة بأن اللوائح التنظيمية ينبغي أن تنبثق من القواعد الدولية في المقام الأول.

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

تدابير تعزيز الثقة وتبادل المعلومات

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

وعلى الصعيد الوطني، تركزت الجهود التي تبذلها البرتغال على إنجاز تدريبات مشتركة شاركت فيها الكيانات العامة والخاصة؛ وعلى تعزيز توحيد المقاييس التقنية؛ وعلى تنظيم المؤتمرات والحلقات الدراسية، التي شارك في بعض منها متحدثون دوليون.

تدابير بناء القدرات

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

وثمة حاجة إلى تيسير حصول جميع أصحاب المصلحة الرئيسيين على المعارف وتشجيع التدريب الجماعي في صفوفهم بشأن عدة جوانب، بما فيها الأمن.

قطر

[الأصل: بالإنكليزية]
[٤ أيار/مايو ٢٠١٧]

أدركت دولة قطر منذ فترة من الزمن أن أمن المعلومات أو الأمن الفضاء السيبراني ليس مجرد مسألة تتعلق بالتكنولوجيا فحسب بل أنه أيضا مسألة سياسة وطنية. وتحقيقا لهذه الغاية، تم تشكيل فريق مواجهة الطوارئ الحاسوبية (انظر www.Qcert.org) عام ٢٠٠٥ من أجل حفز التغيير، وبشكل أكثر تحديدا للتعجيل باعتماد ممارسات وسياسات فعالة للأمن السيبراني على نطاق واسع، وتناط بالفريق الآن ولاية وطنية تتمثل في الحفاظ على الأصول الرقمية لدولة قطر.

وفي عام ٢٠١٣، شكل رئيس الوزراء لجنة وطنية للأمن السيبراني. ووضعت اللجنة استراتيجية وطنية للأمن السيبراني من أجل تحسين الحالة الأمنية لقطر وكفالة استمرار نجاح الأمة ونموها من خلال خمس ركائز تحدد المجالات التي ستتخذ إجراءات فيها، وهي:

- صون البنية التحتية الوطنية الحيوية للمعلومات
- التصدي للحوادث والهجمات السيبرانية وحلها والتعافي منها عن طريق تقاسم المعلومات والتعاون واتخاذ الإجراءات في الوقت المناسب
- وضع إطار قانوني وتنظيمي لإيجاد فضاء سيبراني آمن ونابض بالحياة
- تعزيز ثقافة أمن سيبراني تعزز الاستخدام المأمون والمناسب للفضاء السيبراني
- تنمية وصقل القدرات الوطنية في مجال الأمن السيبراني.

وقد نجح فريق مواجهة الطوارئ الحاسوبية في تقديم مختلف خدمات أمن المعلومات لتلبية احتياجات مؤسسات البلد المالية وشركاته التجارية ومنظماته، ولا سيما في مجالات مواجهة الحوادث، والاستخبارات، والقدرة على الصمود، والتدريب والتوعية، وإدارة الأزمات، وإصدار التراخيص وهويات المستخدم فيما يتعلق بالبنى التحتية الرئيسية العامة، وإنشاء الإطار الوطني للامتثال لأمن المعلومات.

وتعتقد قطر أن هناك حاليا فجوة في قدرة الدول على اكتساب وتقاسم المعارف الكافية بالأوضاع السائدة في الفضاء السيبراني على الصعيدين الإقليمي والدولي بما يمكنها من اتخاذ قرارات فعالة. ويلزم القيام بمزيد من العمل بشأن الوقاية القائمة على التعاون من أجل كفالة أمن سيبراني أكثر إحكاما لجميع البنى التحتية والخدمات السيبرانية بما يضمن قدرتها على الصمود، ولا سيما فيما يتعلق بتسيير الحياة اليومية بصورة عادية للحكومات والدوائر والمؤسسات التجارية والمستهلكين والمواطنين.

ولم ولا يتوافر للأمن السيبراني أكبر قدر من الفعالية إلا عندما يستند إلى تبادل المعلومات. ومن شأن العمل على إبرام اتفاقات لتقاسم المعلومات، من خلال أطر تعاونية تصف منهجيات التحقق والامتثال، أن يكون مكسبا كبيرا للدول.

فالهجمات ستقع، ويجب على الدول والحكومات والمنظمات والصناعة المعنية أن تستعد معا لمواجهتها.

سنغافورة

[الأصل: بالإنكليزية]
[٣١ تموز/يوليه ٢٠١٧]

تدعم سنغافورة، بوصفها دولة صغيرة وكثيفة الاتصال بالإنترنت، إيجاد فضاء سيبراني آمن وقادر على الصمود يستند إلى القانون الدولي، وقواعد محددة جيدا للسلوك المسؤول للدول، وجهود منسقة لبناء القدرات من أجل التقيد بهذه القواعد. ويعد التعاون الدولي المتين ضروريا لمواجهة التحديات المستجدة التي تطرحها التهديدات السيبرانية وستضطلع سنغافورة بدورها في هذا الصدد.

وأنشأت سنغافورة وكالة الأمن السيبراني الخاصة بها في عام ٢٠١٥ لتوفير رقابة مركزية على مهام الأمن السيبراني الوطنية. وأُطلقت استراتيجية الأمن السيبراني في سنغافورة في تشرين الأول/أكتوبر ٢٠١٦، وهي تبين النهج الكلي الذي تتبعه لحماية الخدمات الأساسية من التهديدات السيبرانية ولإيجاد فضاء سيبراني آمن. وتقوم هذه الاستراتيجية على ركائز أربع هي: بناء بنية تحتية قادرة على الصمود؛ وإيجاد فضاء سيبراني أكثر أمانا؛ وتهيئة بيئة حيوية للأمن السيبراني؛ وتعزيز الشراكات الدولية.

وعلى الصعيد الإقليمي، تعمل سنغافورة على بناء وتمتين القدرات في البلدان المجاورة لها. وبدأت، بالاشتراك مع رابطة أمم جنوب شرق آسيا، برنامجا لبناء القدرات السيبرانية قيمته ١٠ ملايين دولار سنغافوري من أجل تكملة الجهود الإقليمية فيما يتعلق ببناء القدرات. وفي إطار هذا البرنامج، عقدت سنغافورة حلقة عمل للرابطة بشأن القواعد السيبرانية في أيار/مايو ٢٠١٧، وستعقد حلقة عمل للرابطة بشأن بناء القدرات في المجال السيبراني في آب/أغسطس ٢٠١٧. وتستضيف أيضا أسبوع سنغافورة السيبراني الدولي السنوي، الذي سيعقد في إطاره 'المؤتمر الوزاري لرابطة أمم جنوب شرق آسيا بشأن الأمن السيبراني' و 'الندوة الدولية للقادة في المجال السيبراني' التي سيشارك فيها قادة عالميون من

الحكومة والصناعة المعنية والأوساط الأكاديمية من أجل إذكاء اهتمام المنطقة ومناقشة القضايا المستجدة والجامعة.

وفيما يتعلق بالتعاون المتعدد الأطراف، تؤيد سنغافورة عمل فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، بما في ذلك القواعد الإحدى عشرة الواردة في تقريره لعام ٢٠١٥. ومن المهم تحديد وتنفيذ القواعد التي تحظى بموافقة واسعة النطاق، ولا سيما القواعد التشغيلية. وهي تشمل عدم دعم الأنشطة الإلكترونية التي تلحق الضرر عن قصد بالبنية التحتية الحيوية؛ وعدم دعم الأنشطة التي تمنع أفرقة التصدي لحوادث الأمن الحاسوبي من مواجهة الحوادث السيبرانية؛ وعدم استخدام أفرقة التصدي تلك للاضطلاع بأنشطة دولية ضارة.

تركيا

[الأصل: بالإنكليزية]
[٣١ تموز/يوليه ٢٠١٧]

أصبحت تكنولوجيات المعلومات والاتصالات جزءا أساسيا من مجتمع اليوم ومن الحياة الاقتصادية. وهي تسهم في الثروة والتنمية الاجتماعيتين فضلا عن الحياة اليومية للأفراد. وتستخدم هذه التكنولوجيات مجموعة واسعة من الجهات تشمل القطاعين العام والخاص وقطاعات البنية التحتية الحيوية والأفراد، وأصبحت منتشرة على نطاق واسع في البلد وفي العالم على الرغم من مخاطر الأمن السيبراني.

وفي هذا السياق، شاركت تركيا في العديد من المبادرات عن طريق الإسهام في جهود تعاونية بشأن مسائل الأمن السيبراني. والهدف من ذلك هو ضمان الأمن السيبراني. ونُظمت في هذا السياق تدريبات وطنية في مجال الأمن السيبراني، قامت بتنسيقها وزارة النقل والشؤون البحرية والاتصالات؛ وأنجز في اسطنبول التدريب الدولي الأول للدرع السيبراني، في حين شاركت تركيا وساهمت أيضا بشكل منتظم وسنوي في تدريبات دولية تتصل بالأمن السيبراني، هي الائتلاف السيبراني لمنظمة حلف شمال الأطلسي (الناتو)، وتدريب 'الدروع المقفلة' للناتو، وتدريب الناتو لإدارة الأزمات.

وتم تعزيز الحوار والتعاون مع الأمم المتحدة، والناتو، والاتحاد الأوروبي، ومنظمة الأمن والتعاون في أوروبا، وغيرها من المنظمات الدولية والمنظمات غير الحكومية، والأوساط الأكاديمية، وقادة الرأي. ويجري توطيد هذا النهج عن طريق المؤتمرات والدورات والحلقات الدراسية والاجتماعات والتعليم على مستوى الدراسات العليا وغير ذلك من البرامج الداعمة. وتقود تركيا جهودا إقليمية في مجال الأمن السيبراني عن طريق إبرام اتفاقات ثنائية مع دول مختلفة.

وأقرت لجنة الدفاع السيبراني التابعة للناتو مذكرة التفاهم التي تصف التعاون بين الناتو وحلفائه، ويجري الاضطلاع بالأعمال ذات الصلة من أجل توقيعها. وتعد تركيا بلدا راعيا لمركز الامتياز التعاوني للدفاع السيبراني التابع للناتو. وتتم متابعة عمل لجنة التخطيط في حالات الطوارئ المدنية التابعة للناتو واجتماعات مركز المساعدة الإقليمي للتحقق من تحديد الأسلحة وتنفيذه – مركز التعاون الأمني، ويشهد التعاون تطورا في مختلف المسائل. وتعد تركيا من مؤسسي المنتدى العالمي للخبرات السيبرانية، وأصبحت طرفا في الوثيقة الإطارية وإعلان لاهاي بشأن المنتدى العالمي.

واتُخذ في مؤتمر قمة مجموعة العشرين المعقود في تركيا في ١٥ و ١٦ تشرين الثاني/نوفمبر ٢٠١٥ قرار بشأن الأمن السيبراني نَوَّه بالعمل الذي يضطلع به فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي.

ووقعت تركيا اتفاقية مجلس أوروبا المتعلقة بالجرائم السيبرانية في ستراسبورغ في عام ٢٠١٠ وأقرّتها من خلال القانون رقم ٦٥٣٣ في عام ٢٠١٤، وتم لاحقا الانتهاء من تحقيق التناسق بينها وبين التشريعات الوطنية.

ونتيجة لجمع واستعراض وتقييم المعلومات التي نتجت في نطاق الاجتماعات ومنصات الحلول العملية، أعدت استراتيجية وطنية وخطة عمل للأمن السيبراني للفترة ٢٠١٦-٢٠١٩.

ويعد تعزيز أمن المعلومات على الصعيد العالمي، ومن ثم إيجاد ثقافة أمنية داخل المجتمع الدولي، مسألة حاسمة بالنسبة للجميع. وفي الوقت نفسه، يحق لكل دولة أن تتخذ تدابير لحماية نفسها من الاستخدام الضار لتكنولوجيات المعلومات والاتصالات من جانب الإرهابيين والمتطرفين والجماعات الإجرامية المنظمة وقراصنة الإنترنت المستقلين، من أجل الحفاظ على الأمن القومي. وفي هذا السياق، يتسم تدعيم التشريعات الدولية وتعزيز الاتفاقات الثنائية الدولية بأهمية كبيرة أيضا.

المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية

[الأصل: بالإنكليزية]
[٣١ تموز/يوليه ٢٠١٧]

ترحب المملكة المتحدة بفرصة عرض ردها على قرار الجمعية العامة ٧١/٢٨ بشأن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، ويستند ردها هذا إلى ردها على القرار ٧٠/٢٣٧ في عام ٢٠١٦. وتستخدم المملكة المتحدة في مجمل ردها مصطلح ”الأمن السيبراني“ (cybersecurity) الذي تفضله هو وما يتصل به من مفاهيم تفادياً للبس، نظرا لوجود تفسيرات مختلفة لمصطلح ”أمن المعلومات“ في هذا السياق.

وتدرك المملكة المتحدة أن الفضاء السيبراني عنصر أساسي لتأمين البنى التحتية الحيوية على الصعيدين الوطني والدولي، وركيزة أساسية من ركائز النشاط الاقتصادي والاجتماعي من خلال شبكة الإنترنت. ولا تزال التهديدات الفعلية والمحتملة النابعة من الأنشطة التي تمارس في الفضاء السيبراني تشكّل مصدر قلق بالغ. وستصوغ الاستراتيجية الوطنية الجديدة المتعلقة بالأمن السيبراني، التي نشرت في تشرين الأول/أكتوبر ٢٠١٦، جهود البلد خلال السنوات الخمس المقبلة من أجل الدفاع عن أصوله وردع خصومه وتطوير قطاع الأمن السيبراني فيه.

وتواصل المملكة المتحدة الاضطلاع بدور قيادي في النقاش الدولي بشأن الأمن السيبراني. وقد وفرت خبراء لجميع أفرقة الخبراء الحكوميين الخمسة المعنية بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي. وعلى الرغم من عدم التوصل إلى توافق في الآراء في فريق عام ٢٠١٧، فإن البلد ملتزم بالتشجيع على إيجاد إطار دولي يكفل الاستقرار في مجال الفضاء السيبراني استنادا إلى تطبيق القانون الدولي القائم، والمعايير الطوعية المتفق عليها للسلوك المسؤول للدول، وتدابير بناء الثقة، وذلك بدعم من برامج منسقة لبناء القدرات. وترحب المملكة المتحدة أيضا بالجهود التي

تبذلها منظمة الأمن والتعاون في أوروبا وغيرها من المنتديات الإقليمية لتقديم مقترحات من أجل تنفيذ تدابير بناء الثقة، وستسعى إلى مواصلة توفير مثال يُحتذى به فيما يخص اعتماد هذه التدابير.

ويعرض هذا الرد أعمال المملكة المتحدة بشأن توطيد الأمن السيبراني وتحسينه وتبادل أفضل الممارسات، على الصعيدين المحلي والعالمي، بما في ذلك مع الشركاء الدوليين من أجل التصدي للجرائم السيبرانية والحوادث الكبرى، وبناء القدرات. وتتطلع المملكة المتحدة إلى رؤية المزيد من التقدم، ويسرها المشاركة بفعالية في هذه المسائل. وستواصل المشاركة بشكل كامل في تعزيز القدرات والتعاون الدولي بشأن الأمن السيبراني.