الأمم المتحدة

A/68/156/Add.1

الجمعية العامة

Distr.: General
9 September 2013
Arabic
Original: Arabic

الدورة الثامنة والستون

البند ٩٤ من جدول الأعمال المؤقت*

التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي

التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي

تقرير الأمين العام

إضافة**

المحتويات

* A/68/150.

** وردت المعلومات المضمنة هذا التقرير بعد صدور التقرير الرئيسي.

091013 091013 13-47543 (A)

ثانيا – الردود الواردة من الحكومات

أرمينيا

[الأصل: بالإنكليزية]
[٥ تموز/يوليه ٢٠١٣]

اعتُمد مفهوم أمن المعلومات بموجب أمر صادر عن رئيس جمهورية أرمينيا برقم NK-97، مؤرخ ٢٥ حزيران/يونيه ٢٠٠٩. وينص هذا الأمر على أن الأمن الوطني لجمهورية أرمينيا يتوقف إلى حد بعيد على أمن المعلومات الذي يشمل عناصر من قبيل نظم المعلومات والاتصالات والاتصالات السلكية واللاسلكية. ويشمل المفهوم أيضا تقييما عاما لمشاكل أمن المعلومات في جمهورية أرمينيا، والتحديات والتهديدات الراهنة وأسبابها الجذرية، وخصائصها المميزة، فضلا عن أساليب التصدي لهذه التحديات في مختلف مجالات الحياة العامة.

وقد أنشئت لجنة حكومية دولية لتتولى تنسيق تنفيذ البرامج المتصلة بمفهوم أمن المعلومات.

وتمت الموافقة على المفهوم المتعلق بإنشاء ''مجتمع للفضاء الحاسوبي'' بموجب قرار اتخذته حكومة جمهورية أرمينيا في ٢٥ شباط/فبراير ٢٠١٠. وأنشئ مجلس الحوكمة الإلكترونية لجمهورية أرمينيا، وحُدد النطاق العام لأمن الفضاء الإلكتروني في إطار مفهوم إنشاء ''مجتمع الفضاء الإلكتروني''. ويحدد المرفق ٤ للمفهوم الأنشطة التي تكفل أمن الفضاء الإلكتروني للدولة. وقد أنشئت لجنة حكومية وفريق من الخبراء ليتوليا العمل من أجل تحقيق الأهداف المذكورة أعلاه.

واتخذت أيضا التدابير التالية على الصعيد الوطني من أجل تعزيز أمن المعلومات.

وعملا بالمرسوم الحكومي رقم N-479، المؤرخ ٣٠ نيسان/أبريل ٢٠٠٩، أُنشئت محطة اتصال خاصة لمعالجة أمن شبكة الإنترنت، وهي تعمل في الوقت الحاضر. وتكفل المحطة أمن المعلومات العامة للهيئات الحكومية، المحملة على شبكة الإنترنت، وتأمين ربط نظم المعلومات لدى الهيئات الحكومية بشبكة الإنترنت.

وفي بداية عام ٢٠١٢، قام فريق الخبراء بإعداد مشروع برنامج وطني يتعلق بإنشاء نظام لأمن الفضاء الإلكتروني في جمهورية أرمينيا. ويخضع مشروع البرنامج هذا في الوقت الحاضر للمناقشة في حكومة أرمينيا.

وفي عام ٢٠٠٦، صدقت جمهورية أرمينيا على اتفاقية الجرائم الإلكترونية، التي فتح باب التوقيع عليها في بودابست في عام ٢٠٠٦، والاتفاقية المتعلقة بحماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية، في عام ٢٠١٢. وتمثل دائرة الأمن الوطني وشرطة جمهورية أرمينيا الوكالتين الحكوميتين المختصتين بتنفيذ أحكام الاتفاقيتين المذكورتين أعلاه. وفي المرحلة الحالية، يضطلع فريق الخبراء الحكومي الدولي بأنشطة تهدف إلى جعل التشريعات الوطنية ذات الصلة متماشية مع الاتفاقية.

وتقيم جمهورية أرمينيا تعاونا فعليا بشأن أمن الفضاء الإلكتروني في إطار منظمة الأمن والتعاون في أوروبا. وفي الوقت الراهن، يشارك الجانب الأرمني في المفاوضات في إطار الفريق العامل غير الرسمي لوضع مجموعة من تدابير بناء الثقة بشأن أمن الفضاء الإلكتروني.

وقد أضاف الجانب الأرمني إجراء ضمن سبعة إجراءات فرعية في مجال الدفاع عن الفضاء الإلكتروني ضمن خطة عمله المتعلقة بالشراكات الفردية للفترة ٢٠١١-٢٠١٣، التي يجري تنفيذها بالتعاون مع منظمة حلف شمال الأطلسي.

كندا

[الأصل: بالإنكليزية]
[٣ أيلول/سبتمبر ٢٠١٣]

تود كندا، إذ تأخذ في اعتبارها التقييمات والتوصيات الواردة في تقرير فريق الخبراء الحكومي المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، أن تبلغ الأمين العام آراءها وتقييماتها بشأن المسائل التالية.

١ - أمن المعلومات

تشعر كندا بالقلق إزاء التهديدات الفعلية والمتصاعدة التي تشكلها أنشطة الجرائم الإلكترونية، وتقرّ بأن التصدي للأنشطة الإلكترونية الخبيثة يتطلب تعاونا على الصعد الوطنية والإقليمية والدولية.

إن لكندا مصلحة استراتيجية في الحفاظ على الفضاء الإلكتروني مفتوحا، بالنظر إلى أهميته بالنسبة إلى ازدهار كندا وأمنها وقيمها المتعلقة بالديمقراطية وبحقوق الإنسان. إن الجهات الفاعلة في كلا القطاعين العام والخاص في كندا، تعتمد على وجود هياكل أساسية معلوماتية آمنة وقوية ومستقرة لتقوم بأعمالها اليومية. وتشكل النظم الحاسوبية، إضافة إلى النظم القائمة على شبكة الإنترنت والشبكات الحاسوبية، العمود الفقري لجزء كبير من

الهياكل الأساسية البالغة الأهمية في كندا، بما في ذلك الطاقة، والشؤون المالية، والاتصالات السلكية واللاسلكية وقطاعات الصناعات التحويلية ونظم المعلومات الحكومية. فمن شأن التشغيل السلس للهياكل الأساسية الحيوية أن يدعم أسلوب الحياة لدينا ودعم رفاه كندا السياسي والاقتصادي والاجتماعي.

على الصعيد الوطني

لقد أقرت الحكومة الكندية، منذ عام ١٩٩٦، بأن النظم ذات الأهمية الحيوية في تشغيل الهياكل الأساسية لكندا يمكن أن تتعرض لهجمات إلكترونية، وأن على الحكومة أن تقوم بدور في حماية هذه النظم من تلك الهجمات. وفي السنوات اللاحقة، اتخذت الحكومة إجراءات في ذلك الصدد. وبعد استعراض قدراتها على تقييم جوانب الضعف في هياكلها الأساسية والحد منها، قامت بوضع وتنفيذ نهج شامل لحماية الهياكل الأساسية الحيوية في كندا من خلال شراكات أقامتها، وقامت برصد الهجمات والتهديدات الإلكترونية الموجهة ضد نظم الحكومة الاتحادية وتحليلها. وفي عام ٢٠١٠، أصدرت الحكومة استراتيجيتها وخطة عملها الوطنيتين للهياكل الأساسية الحيوية، وفي وقت سابق من هذا العام، أصدرت خطة عملها للفترة ٢٠١٠-٢٠١٥، في ما يتعلق باستراتيجية كندا لأمن الفضاء الإلكتروني، وهي استراتيجية تهدف إلى تأمين النظم الحكومية، والدخول في شراكات من أجل تأمين النظم الإلكترونية الحيوية خارج الحكومة الاتحادية، ومساعدة الكنديين على أن يكونوا بأمان على شبكة الإنترنت.

على الصعيد الدولي

ظلت كندا، منذ عام ٢٠٠٧، أحد المساهمين الرئيسيين في برنامج أمن الفضاء الإلكتروني لمنظمة الدول الأمريكية، الذي يساعد الدول في الأمريكتين على منع التهديدات الإلكترونية ورصدها والتصدي لها من خلال تعزيز التنسيق والتخطيط على الصعيد الوطني، فضلا عن التعاون الإقليمي. ومن خلال بناء برنامجها المتعلق ببناء القدرات على مكافحة الإرهاب، قدمت كندا المساعدة لعدد من الدول الأعضاء في منظمة الدول الأمريكية في وضع استراتيجياتها الوطنية الخاصة بها لأمن الفضاء الإلكتروني والانضمام إلى شبكة نصف الكرة الغربي لأفرقة الاستجابة لحوادث أمن الفضاء الإلكتروني التابعة لمنظمة الدول الأمريكية.

وعملت كندا والدول المشاركة الأخرى في منظمة الأمن والتعاون في أوروبا من أجل وضع تدابير لبناء الثقة والأمن، من أجل الحد من مخاطر التصورات الخاطئة، وتصاعد النزاعات التي قد تنشأ جراء استخدام تكنولوجيات المعلومات والاتصالات.

وتشارك كندا أيضا بنشاط في المبادرات الدولية لمكافحة الجرائم الإلكترونية في عدد من المنتديات، بما في ذلك مجموعة الثمانية، والمكتب المعني بالمخدرات والجريمة، ومنظمة الدول الأمريكية. وشاركت كندا أيضا في آخر فريق خبراء حكوميين تابع للأمم المتحدة معني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي (٢٠١٢-٢٠١٣).

٢ - المفاهيم الدولية

تنطبق قوانين المعاهدات والقوانين الدولية العرفية على استخدام تكنولوجيات المعلومات والاتصالات من جانب الدول، وهي أساسية للحفاظ على السلام والاستقرار، وتعزيز بيئة مفتوحة وآمنة وسلمية ويمكن الوصول إليها لتكنولوجيا المعلومات والاتصالات. ومن بين القوانين الدولية القائمة ذات الصلة بالفضاء الإلكتروني ميثاق الأمم المتحدة، والقانون الدولي لحقوق الإنسان، والقانون الإنساني الدولي. وقد كان من دواعي سرور كندا أن ترى، في آخر تقرير لفريق الخبراء الحكوميين للأمم المتحدة، تصميما واضحا من جانب الدول على انطباق القانون الدولي على الفضاء الإلكتروني بوصفه حجر الزاوية في ما يتعلق بالقواعد والمبادئ المتعلقة بالسلوك المسؤول من جانب الدول.

وترى كندا أيضا أن معالجة أمن تكنولوجيا المعلومات والاتصالات يجب أن تمضي جنبا إلى جنب مع احترام حقوق الإنسان والحريات الأساسية. بما في ذلك الحق في اعتناق الآراء بدون أي تدخل، وكذلك الحق في حرية التعبير وتكوين الجمعيات والتجمع، واحترام الخصوصية. وترد الإشارة إلى الحق في حرية التعبير في الإعلان العالمي لحقوق الإنسان والعهد الدولي الخاص بالحقوق المدنية والسياسية. وتنص هذه الصكوك على أن الحقوق التي يحظى بها الأشخاص خارج شبكة الإنترنت ينبغي أن تُشمل بالحماية أيضا داخل الشبكة، ولا سيما حرية التعبير، التي تنطبق بصرف النظر عن الحدود، وعن طريق أي وسائط إعلام يختارها المرء.

٣ - التدابير التي يمكن اتخاذها لتعزيز أمن المعلومات على الصعيد العالمي

تعمل كندا عن كثب مع الشركاء الدوليين، بما في ذلك المنظمات المتعددة الأطراف ورابطات القطاع الخاص الرئيسية، من أجل تعزيز أمن المعلومات للشبكات التي يعتمد عليها

رفاه كندا الاقتصادي وأمنها. وتعمل كندا أيضا من أجل تعزيز التعاون وتبادل المعلومات مع بعض شركائها الرئيسيين وضمن المنظمات المتعددة الأطراف بشأن أمن الفضاء الإلكتروني.

وقامت كندا بوضع عملية جديدة لتنسيق التصدي على الصعيد الوطني للحوادث الإلكترونية الرئيسية وإشراك مالكي ومشغلي هياكلها الحيوية الأساسية من أجل وضع وتنفيذ استراتيجياتهم الخاصة بشأن أمن الفضاء الإلكتروني.

وهناك اهتمام واسع النطاق لدى البلدان الأخرى من أجل تعزيز أمن الفضاء الإلكتروني ومنع الجرائم الإلكترونية. والصك الدولي الرئيسي الذي يتناول الجرائم الإلكترونية على وجه التحديد هو اتفاقية الجرائم الإلكترونية لمجلس أوروبا، التي وقعت كندا عليها في عام ٢٠٠١. وهذه الوثيقة المعروفة أيضا باسم اتفاقية بودابست، وهي بمثابة مبدأ توجيهي لوضع تشريعات وطنية شاملة لمكافحة الجرائم الإلكترونية، وبمثابة إطار للتعاون الدولي بين الدول.

ألمانيا

[الأصل: بالإنكليزية]
[٢٥ حزيران/يونيه ٢٠١٣]

التقييم العام لمسائل أمن المعلومات

استخدام التكنولوجيا الرقمية في المعاملات الاقتصادية والإدارية، ليس أمرا جاريا فحسب، بل إنه يتسارع. ويتيح فرصا لم يسبق لها مثيل لكل من البلدان الصناعية والبلدان النامية. وفي الوقت ذاته، فإن الاعتماد المتزايد على تكنولوجيا المعلومات والاتصالات يولّد أوجه ضعف وعجز في صميم النظم. وهناك أيضا ترابط جديد لدى جميع الجهات الفاعلة، بدءا بالمستخدم الخاص وانتهاء بالمؤسسات التجارية والمنظمات الحكومية. أما التوجه في ما يتعلق بالهجمات الإلكترونية فهو ينحو بوضوح نحو القيام بأنشطة شريرة أكثر تطورا، من قبيل التهديدات المستمرة المتطورة أو البرامجيات المتطورة الخبيثة التي توجه هجومها نحو أهداف عالية القيمة. والدافع وراء هذه الأنشطة هو الرغبة في الربح، أو الحصول على معلومات من أجل السيطرة على أصول ونظم وهياكل أساسية حيوية، على التوالي، مع ما يترتب على ذلك من عواقب وخيمة على الحكومات وعلى العديد من المؤسسات والمنظمات، بما في ذلك مقدمو خدمات الهياكل الأساسية الهامة. ويصعب الكشف عن الأنشطة الشريرة المتطورة للغاية. وعادة ما تكون الابتكارات أسرع من المحاولات الرامية إلى تأمين التكنولوجيات الموجودة. وما يزيد من حدة الأخطار هو أن الأدوات والوسائل

الشريرة متوافرة على نحو يتيح الحصول عليها بسهولة نسبيا، لكونها متاحة تجاريا في السوق السوداء أو غير الخاضعة لأي أنظمة. ولا يمكن تأمين بيئات تكنولوجيا المعلومات الحالية لدينا ضد هذه الأدوات بالاعتماد على نهج أمن تكنولوجيا المعلومات التقليدية وحده.

ويكرس المهاجمون الذين يتمتعون بقدر كبير من الكفاءة الفنية وسائل تقنية ومالية كبيرة للكشف عن مواطن الضعف في نظم تكنولوجيا المعلومات والاتصالات، واستغلال تلك النقاط لتحقيق أغراضهم الخاصة. ثم إن صعوبة إسناد تلك الهجمات على نحو موثوق، وما ينجم عن ذلك من فرص لشن هجمات متخفية، تشكل مخاطر إضافية على الأمن على الصعيدين الوطني والدولي، ولا سيما جراء سوء الفهم وسوء التقدير. وعمليات الاقتحام الرامية إلى جمع معلومات لا تبدو في بادئ الأمر، وفي كثير من الأحيان مختلفة عن تلك التي لديها أهداف تدميرية. وهذا يزيد من مخاطر حدوث تصورات خاطئة بشأن احتمال وقوع هجمات واحتمال انتهاكها الحظر المفروض على استخدام القوة في العلاقات الدولية.

ومما يولد حالة إضافية من عدم القدرة على التنبؤ حدوث غموض سائد بشأن ما ينطبق في هذا الصدد من معايير في الفضاء الإلكتروني. وقد أثبتت نظم مراقبة العمليات المتعلقة بالهياكل الأساسية أنها عرضة بوجه خاص لعمليات خبيثة في مجال تكنولوجيا المعلومات والاتصالات. أما المخاطر المحتملة من حدوث أضرار لا يمكن السيطرة عليها على النطاق العالمي، فهي عالية، وتشمل هذه الأضرار إصابة نظم المراقبة الصناعية، حيث تنجم آثار مادية مدمرة. فوقوع هجوم إلكتروني واحد على الهياكل الأساسية الرئيسية للاتصالات السلكية واللاسلكية يمكن أن يحدث اختلالات على الصعيد العالمي تفوق ما يحدثه هجوم مادي واحد.

وبصرف النظر عن تفاوت درجات ما تحظى به تكنولوجيا المعلومات والاتصالات من قدرات وأمن لدى مختلف الدول، يجري في كثير من الحالات إرجاء ما يتعين اتخاذه من خطوات ملموسة من أجل تعزيز القدرة على التصدي، أو تبقى غائبة تماما عن برنامج التصدي، وذلك جراء حالة عدم اليقين التي تكتنف المخاطر التي يتعرض لها أمن الفضاء الإلكتروني وسبل التصدي لها بفعالية، وما تتسم به الهجمات الرقمية من تعقيد وابتكار، وطابع السرية الذي يضفي تعتيما على طبيعة الحوادث الفردية.

الجهود المبذولة على الصعيد الوطني

في عام ١٩٩١، أُنشئ المكتب الاتحادي لأمن المعلومات (Bundesamt fur Sicherheit in der Informationstechnik, BSI) ليكون أول وأهم مقدم لخدمات أمن تكنولوجيا المعلومات المركزية لدى الحكومة الاتحادية. وفي هذه المهمة، يقوم المكتب بنشر الحد الأدنى

من معايير الأمن الملزمة للإدارة الاتحادية، ويعمل بمثابة مكتب مركزي تابع لها للإبلاغ عن الحوادث. وهو، علاوة على ذلك، يعمل باعتباره طرفا محايدا لتقديم المشورة والدعم في مجال أمن تكنولوجيا المعلومات. ومن الإنجازات الرئيسية لعمل المكتب، هناك، على سبيل المثال، معيار إدارة أمن تكنولوجيا المعلومات (Grundschutz)، وفريق الاستجابة للطوارئ الحاسوبية للوكالات الاتحادية (CERT-Bund) بوصفه منبرا للتعامل مع الحوادث وتبادل المعلومات (ويعود إنشاؤه إلى عام ١٩٩٤)، وفريق التصدي للطوارئ الحاسوبية للمواطنين (CERT-Buerger)، الذي أنشئ في عام ٢٠٠٦، ليكون وسيلة للتعامل مع الشرائح الكبرى في المجتمع، ولزيادة الوعي. علاوة على ذلك، يقوم المكتب الاتحادي لأمن المعلومات بإصدار تحذيرات بشأن البرامجيات الخبيثة والثغرات الأمنية في منتجات وخدمات تكنولوجيا المعلومات، ويتولى إبلاغ الأطراف المعنية (بما في ذلك بائعو منتجات وخدمات تكنولوجيا المعلومات وعموم الجمهور)، ويقدم توصيات بشأن ما ينبغي اتخاذه من تدابير مضادة.

وقد تلا الخطة الوطنية لعام ٢٠٠٥ المتعلقة بحماية الهياكل الأساسية للمعلومات، التي تستهدف خدمة الحكومة والصناعة، استراتيجية أمن الفضاء الإلكتروني التي اعتمدتها الحكومة الاتحادية في شباط/فبراير ٢٠١١. الأساسية. وهدفها الرئيسي هو حماية الهياكل الأساسية الحيوية.

ولا تزال الحكومة الألمانية والجهات القائمة بتشغيل الهياكل الأساسية الحيوية، منذ عام ٢٠٠٨، تتعاون في شراكة قائمة بين القطاعين العام والخاص. وتضم خطة ''التنفيذ الإلكتروني'' هذه (UP KRITIS) أفرقة عاملة معنية بمختلف جوانب أمن الفضاء الإلكتروني، من قبيل عمليات إدارة الأزمات، والتدريبات وتوفير الخدمات ذات الأهمية الحاسمة.

ويتولى المركز الوطني المعني بحالة تكنولوجيا المعلومات (Nationales IT-Lagezentrum)، الذي يديره المكتب الاتحادي لأمن المعلومات، متابعة الحالة الأمنية لتكنولوجيا المعلومات على الصعيدين الوطني والعالمي من أجل كشف الحوادث الأمنية وتحليلها على وجه السرعة، وتقديم توصيات بشأن ما ينبغي اتخاذه من تدابير وقائية. وفي حالة حدوث أزمة تتصل بتكنولوجيا المعلومات، فإنه يقوم بتوسيع نطاق سلطاته ليصبح المركز الوطني للتصدي لأزمات تكنولوجيا المعلومات (Nationales IT-krisenreaktionszentrum)، فيركز قدراته للتعامل مع أزمات تكنولوجيا المعلومات، حيث يغطي جميع الجوانب الوطنية، بما في ذلك الشبكات الحكومية والهياكل الأساسية الحيوية.

وتمشيا مع استراتيجية أمن الفضاء الإلكتروني لعام ٢٠١١، يتعين على جميع السلطات الحكومية التي تتعامل مع مسائل أمن الفضاء الإلكتروني أن تتعاون على نحو وثيق

ومباشر فيما بينها ومع القطاع الخاص في إطار المركز الوطني للاستجابة في مجال الفضاء الإلكتروني (Nationales Cyber-Abwehrzentrum)، الذي يديره ويستضيفه المكتب الاتحادي لأمن المعلومات.

وفي ما يتعلق بالسياسات، فإن المجلس الوطني للأمن الإلكتروني (Nationaler Cyber-Sicherheitsrat)، على مستوى وزارة الخارجية، يتولى معالجة مسائل أمن الفضاء الإلكتروني الرئيسية وموقف ألمانيا بشأنها. ويشمل ذلك تنسيق السياسة الخارجية المتعلقة بالفضاء الإلكتروني، بما في ذلك جوانب السياسات الخارجية والدفاعية، والسياسات الاقتصادية والأمنية.

علاوة على ذلك، أُنشئ منبر في تشرين الأول/أكتوبر ٢٠١٢، للتعاون وتبادل المعلومات على الصعيد الوطني: ويقوم التحالف من أجل أمن الفضاء الإلكتروني (Allianz für Cybersicherheit) بتيسير التعاون الوثيق بين الشركاء في المجالات الاقتصادية والأكاديمية والإدارية، وبوجه خاص مع المؤسسات العاملة في المجالات المتصلة بالمصلحة العامة.

ويجري حاليا استكمال خطة التنفيذ بعد أربع سنوات من تشغيلها. وسوف تتاح لمزيد من مشغلي الهياكل الأساسية الحيوية، وسيتم في إطارها إنشاء عدد من الأفرقة العاملة الجديدة ضمن قطاعات الهياكل الأساسية الحيوية. إضافة إلى ذلك، سيقام التعاون مع التحالف الجديد للأمن الإلكتروني.

إن أوجه الترابط على الصعيد الدولي في الفضاء الإلكتروني تعني أن تنسيق العمل على الصعيد الدولي أمر أساسي. ولذلك فإن ألمانيا، في إطار الاتحاد الأوربي والمنظمات الدولية، تدعو بقوة إلى تعزيز أمن الفضاء الإلكتروني، مع القيام، في الوقت نفسه، بحماية المنافع الاجتماعية والاقتصادية في الفضاء الإلكتروني.

وتدعو ألمانيا، في إطار استراتيجيتها المتعلق بأمن الفضاء الإلكتروني، وفي ضوء الترابط العالمي في مجال تكنولوجيا المعلومات، إلى وضع قواعد بشأن سلوك الدول في مجال الفضاء الإلكتروني تكون واضحة وغير مثيرة للخلاف وملزمة سياسيا. وينبغي أن تكون مقبولة لدى جزء كبير من المجتمع الدولي، وأن تشمل تدابير لبناء الثقة وزيادة الأمن.

تدابير بناء الثقة والأمن في الفضاء الإلكتروني

الفضاء الإلكتروني منفعة عامة وفضاء عام. ولذلك، علينا البحث في أمن الفضاء الإلكتروني من حيث مرونة هياكله الأساسية، فضلا عن سلامة النظم والبيانات والأمان من فشلها. ولكون الفضاء الإلكتروني فضاء عاما، يتعين على الدول تعزيز الأمن

في هذا الفضاء، وخاصة فيما يتعلق بالأمان من الجريمة والأنشطة الضارة، بحماية الأشخاص الذين يختارون استخدام الأدوات المتعلقة بالتثبت من الهوية، بغرض مكافحة سرقة الهوية، وضمان سلامة البيانات والشبكات وسريتها.

ولما كان الفضاء الإلكتروني عالميا بطبيعته، فإن ضمان أمن الفضاء الإلكتروني وإعمال الحقوق وحماية الهياكل الأساسية الحيوية للمعلومات يتطلب بذل الدولة جهودا كبيرة على الصعيد الوطني وبالتعاون مع الشركاء الدوليين على السواء. أما على الصعيد الوطني، فإن لألمانيا ثقافة متميزة من التعاون بين عدد كبير من أفرقة التصدي للطوارئ الحاسوبية في جميع الهيئات الاقتصادية والأكاديمية والإدارية. وفي هذا السياق، يشكل اتحاد أفرقة التصدي للطوارئ الحاسوبية جهة تنسيق راسخة لدى هذه الأفرقة. أما على الصعيد الأوروبي والدولي، فإن الاتحاد يقيم تعاونا وثيقا مع مجموعة أفرقة التصدي للطوارئ الحاسوبية الحكومية الأخرى، ومع منتدى شبكة أفرقة التصدي للحوادث والأمن، باعتباره المنتدى العالمي الأكثر أهمية للربط بين أفرقة التصدي للطوارئ الحاسوبية في الفضاء الإلكتروني.

وبناء عليه، فإن ألمانيا على استعداد للعمل على وضع جملة من القواعد السلوكية تتناول السلوك بين دولة وأخرى في الفضاء الإلكتروني، ولا سيما تدابير بناء الثقة والشفافية والأمن، ليوقع عليها أكبر عدد ممكن من البلدان. لذلك، شاركت ألمانيا بنشاط في فريق الخبراء الحكوميين للفترة ٢٠١٢/٢٠١٣، المكلف بمواصلة ”دراسة التهديدات القائمة والمحتملة في مجال أمن المعلومات، والتدابير التعاونية الممكن اتخاذها للتصدي لتلك التهديدات، بما فيها المعايير أو القواعد أو المبادئ المتعلقة بسلوك الدول المسؤول، وتدابير بناء الثقة في ما يتعلق بحيز المعلومات المتاح“ (قرار الجمعية العامة ٦٦/٢٤).

وقد حددت ألمانيا مؤخرا العناصر الممكن تضمينها مدونة السلوك هذه المتعلقة بالمعايير الدولية في مؤتمر منظمة الأمن والتعاون في أوروبا المتعلق بأمن الفضاء الإلكتروني، الذي عُقد في ٩ و ١٠ أيار/مايو ٢٠١١ على النحو التالي:

(أ) التأكيد على المبادئ العامة المتعلقة بتوافر البيانات والشبكات وسريتها ونزاهتها وتنافسيتها ونزاهتها، وأصالتها، وخصوصية حقوق الملكية الفكرية وحمايتها؛

(ب) احترام الالتزام بحماية الهياكل الأساسية الحيوية؛

(ج) تعزيز التعاون بهدف اتخاذ تدابير لبناء الثقة، والحد من المخاطر، وتحقيق الشفافية والاستقرار من خلال ما يلي:

- تبادل الاستراتيجيات الوطنية وأفضل الممارسات والمفاهيم الوطنية التي تحيل إلى التشريعات الدولية للفضاء الإلكتروني؛
- تبادل وجهات النظر الوطنية بشأن القواعد القانونية الدولية المتعلقة باستخدام الفضاء الإلكتروني؛
- إنشاء جهات اتصال وإخطارها؛
- إنشاء آليات للإنذار المبكر وتعزيز التعاون في جملة أمور فيما بين أفرقة الاستجابة للطوارئ الحاسوبية؛
- رفع مستوى روابط الاتصال في حالات الأزمات لتشمل حوادث الفضاء الإلكتروني، ودعم وضع توصيات فنية تعزز إقامة هياكل أساسية إلكترونية عالمية تكون قوية وآمنة؛
- تحمُّل المسؤولية عن مكافحة الإرهاب بحيث تشمل تبادل الممارسات وتعزيز التعاون للتعامل مع الجهات الفاعلة من غير الدول؛
- دعم بناء القدرات في مجال أمن الفضاء الإلكتروني في البلدان النامية، ووضع تدابير طوعية ترمي إلى تقديم الدعم لأمن الفضاء الإلكتروني للمناسبات الكبيرة.

ومن هذا المنطلق، قدمت ألمانيا، في تموز/يوليه ٢٠١٢، ورقة موقف إلى فريق الخبراء الحكوميين التابع للأمم المتحدة. ونحن نرحب ترحيبا حارا بتوصيات الخبراء بشأن معايير السلوك المسؤول للدول أو قواعده أو مبادئه، وتدابير بناء الثقة في الفضاء الإلكتروني، بالإضافة إلى ما أكد عليه الخبراء بشأن اعتماد نهج يتعلق بتعدد أصحاب المصلحة في أمن الفضاء الإلكتروني.

وفي عامي ٢٠١١ و ٢٠١٢، قدمت ألمانيا الدعم للمشاريع المتعلقة بأمن الفضاء الإلكتروني وتدابير بناء الثقة والأمن التي يقوم بها على الصعيد الدولي معهد الأمم المتحدة لبحوث نزع السلاح، ومعهد بحوث السلام والسياسات الأمنية في جامعة هامبورغ. وشكّل مؤتمر برلين الأول المتعلق بالفضاء الإلكتروني، والمعقود في كانون الأول/ديسمبر ٢٠١١، منبرا لمناقشات دولية أُجريت بشأن المخاطر والاستراتيجيات وبناء الثقة على الصعيد الدولي في مجال أمن الفضاء الإلكتروني. وركز مؤتمر برلين الثاني للفضاء الإلكتروني المعقود في أيلول/سبتمبر ٢٠١٢، على الإنترنت وحقوق الإنسان. وتمثل أحد الاستنتاجات الرئيسية في أن الأمن والحرية والخصوصية على شبكة الإنترنت هي مفاهيم يكمل أحدها الآخر. وقدمت أيضا الدعم لمؤتمر عام ٢٠١٢ لمعهد الأمم المتحدة لبحوث نزع السلاح، المتعلق

بأمن الفضاء الإلكتروني، والذي عقد في جنيف في ٨ و ٩ تشرين الثاني/نوفمبر ٢٠١٢، حيث ركز على تدابير بناء الثقة في كفالة استقرار الإنترنت.

علاوة على ذلك، فإننا نرى ضرورة بدء نقاش بشأن إقامة تعاون دولي في ما يتعلق بمسألة إسناد الهجمات الإلكترونية، التي عادة ما يكون تتبعها صعبا للغاية، ومسؤولية الدول عن الهجمات الإلكترونية التي تشن من أراضيها عندما لا تفعل تلك الدول شيئا لوقف تلك الهجمات على الرغم من علمها بها، ومسؤولية الدول عن عدم تسهيل وجود مجالات تسودها الفوضى في الفضاء الإلكتروني، من قبيل التغاضي عن علم عن تخزين بيانات شخصية تُجمع بشكل غير قانوني على أراضيها.

وفي ٢٧ و ٢٨ حزيران/يونيه ٢٠١٣، سعى مؤتمر برلين الثالث المتعلق بالفضاء الإلكتروني، المعقود بشأن ”تأمين حرية الفضاء الإلكتروني واستقراره: دور القانون الدولي وأهميته“، والذي نظمته وزارة الخارجية الاتحادية، بالتعاون الوثيق مع جامعة بوتسدام، إلى توفير تقييمات القانوني الدولي لعمليات الفضاء الإلكتروني التي لا تتعدى حدود الهجوم المسلح، ومن ثم فإنها لا تستوجب الاحتكام إلى قانون النزاعات المسلحة. فالدول، وفقا للقواعد والمبادئ الدولية القائمة، هي المسؤولة عن الإجراءات التي تُتخذ ضمن نطاق سيطرتها والتي تؤثر على أمن تكنولوجيا المعلومات والاتصالات واستقرارها. وينبغي أن تنظر كل دولة في الكيفية التي يمكن بها التقليل إلى أدنى حد من الأنشطة الإلكترونية الخبيثة الناشئة داخل نطاق سيطرتها أو التي تنتقل عبر شبكاتها. وتتحمل الدول المسؤولية عن أنشطة الفضاء الإلكتروني غير المشروعة دوليا التي تُعزى إليها، بما في ذلك أنشطة الفضاء الإلكتروني غير المشروعة دوليا التي تقوم بها جهات تعمل بالوكالة لحساب الدولة وبدعم من الدولة أو بناء على توجيهات الدولة أو تحت إشرافها، وفقا للقواعد الحالية المتعلقة بمسؤولية الدول بموجب القانون الدولي العرفي. وينبغي أن تتخذ الدول جميع التدابير اللازمة التي تكفل عدم استخدام أراضيها من جانب دول أخرى أو من جانب جهات فاعلة من غير الدول لأغراض الاستخدام غير المشروع لتكنولوجيا المعلومات والاتصالات ضد دول أخرى ومصالحها. وينبغي أن تشمل هذه التدابير اللازمة الأطر التشريعية والتنظيمية الوطنية الملائمة اللازمة للوفاء بمسؤولياتها الدولية. ويمكن أن تؤثر أنشطة الفضاء الإلكتروني غير المشروعة دوليا على الدول بطرق رئيسية ثلاث، هي: (١) من حيث كونها بلدان المنشأ لأنشطة مرتكبة في مجال الفضاء الإلكترونية بنية الإيذاء، حيث يمكن أن تترتب عليها آثار مدمرة؛ (٢) من حيث كونها بلدان مرور عابر تُستغل هياكلها الأساسية لتكنولوجيا المعلومات والاتصالات أداةً للقيام بأنشطة ذات نوايا خبيثة؛ (٣) من حيث كونها بلدانا مستهدفة، حيث تحدث الآثار المدمر المترتبة على أنشطة الفضاء الإلكتروني الخبيثة. وفي جميع

هذه السيناريوهات، فإن الدول ملزمة ببذل العناية الواجبة، التي يمكن أن تكون ذات طبيعة مادية وإجرائية على حد سواء، ويمكن أن تتراوح بين المنع، أي الفترة التي تسبق حدوث الأضرار المحتملة، والاحتواء، أي بين بدء النشاط الإلكتروني الفعلي الجاري الضار والمتابعة، أي الفترة التي تلي تنفيذ الأنشطة الإلكترونية الخبيثة.

أمن الفضاء الإلكتروني في منظمة الأمن والتعاون في أوروبا

دأبت منظمة الأمن والتعاون في أوروبا طوال عدة سنوات على مناقشة مسائل أمن الفضاء الإلكتروني. وفي مؤتمر قمة منظمة الأمن والتعاون الذي عُقد في أستانا في عام ٢٠١٠، أكد رؤساء دول وحكومات ٥٦ دولة مشاركة من دول منظمة الأمن والتعاون على وجوب تحقيق ''قدر أعلى من حيث وحدة الهدف والعمل في مواجهة ما ينشأ من تهديدات عابرة للحدود الوطنية''. وأشار إعلان أستانا التذكاري إلى التهديدات في الفضاء الإلكتروني من حيث كونها أحد هذه التهديدات الناشئة العابرة للحدود الوطنية.

وشاركت ألمانيا بنشاط في مؤتمر منظمة الأمن والتعاون في أوروبا، المعقود في فيينا، في عام ٢٠١١، بشأن ''استكشاف دور منظمة الأمن والتعاون في أوروبا في المستقبل'' في ما يتعلق باعتماد نهج شامل إزاء أمن الفضاء الإلكتروني ٩ وفي سياق المؤتمر، نوقشت توصيات ملموسة في ما يتعلق بأنشطة المتابعة التي ستضطلع بها المنظمة. وفي أيار/مايو ٢٠١٢، أُنشئ فريق عامل غير رسمي بموجب قرار المجلس الدائم ١٠٣٩ (PC.DEC/1039) وكُلِّف بوضع مجموعة من مشاريع تدابير لبناء الثقة من أجل تعزيز التعاون والشفافية، والقدرة على التنبؤ، والاستقرار بين الدول، ومن أجل الحد من مخاطر التصورات الخاطئة، وتصعيد النزاعات التي قد تنشأ جراء استخدام تكنولوجيات المعلومات والاتصالات. وقدمت ألمانيا ورقة غفلا إلى الفريق في حزيران/يونيه ٢٠١٢ تتضمن مقترحات ألمانيا بشأن وضع مجموعة أولى من تدابير لبناء الثقة ضمن إطار منظمة الأمن والتعاون في أوروبا. وتعرب ألمانيا عن أسفها لعدم التمكن من الوصول، في مجلس دبلن الوزاري المعقود في كانون الأول/ديسمبر ٢٠١٢، إلى توافق في الآراء من أجل اعتماد تلك المجموعة الأولى من تدابير بناء الثقة، ولكنها ترحب باستئناف فريق العمل عمله في عام ٢٠١٣.

وستواصل ألمانيا تقديم دعمها الفعلي لمناقشات منظمة الأمن والتعاون في أوروبا التي تتناول استكشاف دور المنظمة في المستقبل في مجال أمن الفضاء الإلكتروني.

الجوانب العسكرية لأمن الفضاء الإلكتروني

لما كانت القوات العسكرية أيضا تعتمد اعتمادا متزايد على تكنولوجيا المعلومات لإتقان تصورات أكثر تعقيدا مما كانت عليه في أي وقت مضى على جميع مستويات القيادة، فقد أصبحت حماية المعلومات والوسائل اللازمة لمعالجتها مهمة من الدرجة الأولى.

بيد أن أمن المعلومات، في الفكر العسكري، يواجه، في أي فهم للعمليات، لا بتحديات من خصم محتمل يستخدم أسلحة لإحداث دمار التدمير مادي في الهياكل الأساسية للمعلومات فحسب، بل ومن مستخدمين لا يتحلّون بحس المسؤولية، أو من تكنولوجيا معطوبة، أو مجرمين، أو ببساطة نتيجة حوادث ما.

ومن هنا، فإن الجهود التي يتعين بذلها تتراوح بين توعية كل مستخدم من المستخدمين وضمان موثوقية سلسلة الإمداد في ما يتعلق بتكنولوجيا المعلومات وبناء دفاعات المضادة لصد هجمات قراصنة الفضاء الإلكتروني، وبين تكنولوجيا معلومات تكون ذات هياكل أساسية قادرة على المقاومة عموما.

وباختصار، يلزم تحقيق إدارة شاملة للمخاطر مع اتخاذ تدابير لتعزيز أمن المعلومات على النطاقين الوطني والعالمي.

وفي مرحلة سابقة، أنشأت القوات الألمانية المسلحة (Bundeswehr) هياكل أساسية وتقنيات وإجراءات أمنية مرنة، فضلا عن إنشاء منظمة لأمن تكنولوجيا المعلومات تضم جميع فروع القوات المسلحة وتشمل فريقا مستقلا للاستجابة للطوارئ الإلكترونية ولديه القدرة على التدخل في حالات أعطال حرجة في عمليات تكنولوجيا المعلومات. ويمثل تكييف القدرات الشخصية والفنية لمواجهة استمرار تزايد مستوى التهديدات مهمة دائمة.

وتقوم القوات المسلحة الألمانية بالتعاون الوثيق مع وزارة الداخلية لألمانيا الاتحادية في ما تبذله من جهود، وتدعم بقوة تعزيز أمن المعلومات في منظمة حلف شمال الأطلسي والاتحاد الأوروبي، وفي صوغ السياسات وتحسين تنسيق القدرات لهذه الغاية. علاوة على ذلك، تجري القوات المسلحة عمليات تبادل منتظمة مع عدد من البلدان في سياق أمن المعلومات على صعيد السياسات وصعيد العمل على حد سواء.

وترحب القوات المسلحة الألمانية بأي مبادرات، وتعمل إلى جانب الوزارات الأخرى في حكومة ألمانيا الاتحادية من أجل تلبية الطلبات الدولية بمواصلة توفير الحماية لعمل شبكات المعلومات على نطاق العالم، على سبيل المثال، وضع مدونة دولية طوعية لقواعد السلوك في الفضاء الإلكتروني.

الدفاع عن الفضاء الإلكتروني في منظمة حلف شمال الأطلسي (الناتو)

حددت منظمة حلف شمال الأطلسي (الناتو) أمن الفضاء الإلكتروني بوصفه أحد التحديات الأمنية الناشئة الرئيسية. وينص المفهوم الاستراتيجي الذي اعتمده رؤساء الدول والحكومات في قمة منظمة حلف شمال الأطلسي، المعقودة في لشبونة في تشرين الثاني/نوفمبر ٢٠١٠، على أن ''الهجمات الإلكترونية يمكن أن تبلغ حدا يهدد الازدهار والأمن والاستقرار على الصعيدين الوطني والأوروبي الأطلسي''.

وعلى نحو ما كلف به في إعلان القمة وزراء الدفاع في منظمة حلف شمال الأطلسي اعتمد الوزراء سياسة بشأن الدفاع عن الفضاء الإلكتروني وخطة عمل للدفاع عن الفضاء الإلكتروني في حزيران/يونيه ٢٠١١. ولا تزال المنظمة، منذ ذلك الحين، تنفذ خطة العمل باستمرار.

وتركز السياسة على حماية شبكات منظمة حلف الناتو والشبكات الوطنية للدول الأعضاء المرتبطة بشبكات المنظمة أو التي تعالج معلومات المنظمة (بما في ذلك وضع مبادئ ومعايير مشتركة لضمان حد أدنى من الدفاع عن الفضاء الإلكتروني في جميع الدول الأعضاء). وللحد من المخاطر العالمية الناشئة عن الفضاء الإلكتروني تعتزم المنظمة التعاون مع الدول الشريكة والهيئات الدولية ذات الصلة، كالأمم المتحدة والاتحاد الأوروبي والقطاع الخاص والأوساط الأكاديمية.

وترحب ألمانيا بالتزام المنظمة في ما يتعلق بأمن الفضاء الإلكتروني، وهي تقدم الدعم الفعلي للمناقشات.

جمهورية إيران الإسلامية

[الأصل: بالإنكليزية]
[٧ حزيران/يونيه ٢٠١٣]

ترى جمهورية إيران الإسلامية أن استخدام تكنولوجيات ووسائل المعلومات والاتصالات يتيح العديد من الفرص لجميع الدول وللإنسانية جمعاء. وتشكل المعلومات والاتصالات اليوم أجزاء أساسية من المجتمعات الحديثة. فهي من الموارد البالغة الأهمية لثروة الأمم وازدهارها. وتعتقد إيران أنه ينبغي بذل كل جهد ممكن، على الصعيدين الوطني والدولي، لتوفير الأساس لكي تستخدم جميع الأمم تكنولوجيات ووسائل المعلومات والاتصالات على أوسع نطاق ممكن، ولكفالة أن تظل تلك التكنولوجيات والوسائل من بين القوى المحركة الرئيسية للتنمية في جميع المجتمعات.

وما من شك في أن تحقيق هذا الهدف النبيل يتوقف، إلى حد كبير، على ضمان الاحترام الكامل للحق السيادي لكل دولة في ميدان المعلومات والاتصالات، بما في ذلك تطوير تكنولوجيات ووسائل المعلومات والاتصالات وما يتصل بها من خدمات، وحيازتها واستخدامها واستيرادها وتصديرها وإمكانية الحصول عليها دونما قيد أو تمييز. وفي الواقع، فإن كفالة توافر المعلومات وموثوقيتها وسلامتها وأمنها باستمرار، وتهيئة بيئة آمنة ومأمونة للمعلومات والاتصالات تخدم مصلحة جميع الأمم، وعليه، فهي تعد ضرورة قصوى. ومما لا سبيل إلى إنكاره أن اعتماد أي تدبير بهدف منع أو تقييد نقل الدراية والتكنولوجيات والوسائل المتقدمة في مجال المعلومات إلى البلدان النامية، ومنع أو تقييد توفير المعلومات والاتصالات لهذه البلدان من شأنه أن يجر آثارا سلبية على تنميتها الشاملة، ومن ثم وجب تجنب ذلك.

وفي نفس الوقت، فإن تكنولوجيات ووسائل المعلومات والاتصالات تنطوي على إمكانية أن تستخدم لأغراض غير مشروعة، من بينها الإضرار بالهياكل الأساسية للدول ومصالحها في المجالات الاجتماعية والثقافية والاقتصادية والسياسية والأمنية. ويدل اعتماد المجتمعات المتزايد باستمرار على توافر المعلومات والهياكل الأساسية للاتصالات من جهة، واستغلال تكنولوجيات ووسائل المعلومات والاتصالات لأغراض غير مشروعة من جهة أخرى، لا سيما من قبل المجرمين والإرهابيين، بما في ذلك إرهاب الدولة، على مواطن الضعف القائمة والآثار الواسعة النطاق التي قد تنجم عن أي تهديد محتمل يكون مصدره المعلومات والاتصالات. وبناء على ذلك، فإن من الأهمية بمكان اتخاذ جميع التدابير القانونية والتقنية والمتعلقة بالهياكل الأساسية المناسبة على الصعيد الوطني لتعزيز أمن تكنولوجيات ووسائل المعلومات والاتصالات ولمنع استخدامها لأغراض غير مشروعة.

ومع ذلك، ونظرا للطبيعة المعقدة والخصائص الفريدة لتكنولوجيات ووسائل المعلومات والاتصالات، بما في ذلك مجالها غير المحدود وديناميتها وسريتها وسرعتها وما تتسم به من تقدم تكنولوجي سريع، فضلا عن زيادة الترابط بين ما ترتكز عليه من شبكات المعلومات والاتصالات، يبدو أن ضمان أمن المعلومات والاتصالات بمجرد اعتماد تدابير وطنية أمر مستحيل. ولهذا السبب، ومع الأخذ في الاعتبار الحالات المتزايدة لاستخدام هذه التكنولوجيات والوسائل في العديد من البلدان لأغراض غير مشروعة، ينبغي أن تعمل الدول جميعها على الصعيد الوطني، وأن تتعاون في نفس الوقت فيما بينها.

وبينما تلاحظ جمهورية إيران الإسلامية الجهود المبذولة حاليا في إطار الأمم المتحدة وغيرها من المنظمات الدولية بشأن المسائل المتصلة بالمعلومات والاتصالات، فإنها ترى أن

الآلية الدولية الأنسب للنظر في التطورات الجارية في ميدان المعلومات والاتصالات في سياق الأمن الدولي تتمثل في بدء عمليةٍ في إطار الأمم المتحدة بمشاركة جميع الدول على قدم المساواة. وتؤمن إيران إيمانا راسخا بأن الغرض الرئيسي من هذه العملية ينبغي أن يتمثل في التوصل إلى تفاهم مشترك بين الدول بشأن أهمية تعزيز أمن المعلومات والاتصالات، وطبيعة التهديدات التي تتعرض لها وسائل وتكنولوجيات المعلومات والاتصالات ونطاق تلك التهديدات ومدى خطورتها، وإيجاد السبل والوسائل الكفيلة بمنع تلك التهديدات. ويمكن أن تؤدي هذه العملية إلى اعتماد برنامج عمل يحدد التدابير اللازم اتخاذها من جانب الدول الأعضاء، وأن تتم في شكل مؤتمرات دولية تعقد كل خمس سنوات كي تفضي إلى نتائج سياسية تتراوح بين إصدار الإعلانات ووضع مدونات لقواعد السلوك. ومع ذلك، فإن الهدف النهائي من تلك العملية ينبغي أن يتمثل في التطوير التدريجي لأسس قانونية دولية متينة من أجل تعزيز وضمان أمن المعلومات والاتصالات على الصعيد العالمي، ومنع استخدام تكنولوجيات ووسائل المعلومات والاتصالات لأغراض غير مشروعة.

وترى جمهورية إيران الإسلامية أن النظر في المسائل المتعلقة بالتطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي يجب أن يتم على أساس المبادئ والعناصر التالية:

(أ) كمبدأ عام، ينطبق القانون الدولي على استخدام الدول تكنولوجيات ووسائل المعلومات والاتصالات، ومن ثم ينبغي تطبيقه في هذا المجال. لذلك يجب على الدول أن تتقيد، أثناء استخدامها هذه التكنولوجيات والوسائل، بمقاصد الأمم المتحدة ومبادئها وبما يقع عليها من التزامات بموجب ميثاق المنظمة، ولا سيما الفقرة ٣ من المادة ٢ التي تنص على فض المنازعات الدولية بالوسائل السلمية، وبما ورد في الفقرة ٤ من المادة ٢ من حظر للتهديد باستعمال القوة أو استعمالها على أي وجه لا يتفق ومقاصد الأمم المتحدة، وما ورد في الفقرة ٧ من المادة ٢ من منع للتدخل في الشؤون الداخلية للدول؛

(ب) لا شيء يمس الحق السيادي للدول في ميدان المعلومات والاتصالات، بما في ذلك تطوير الدراية والتكنولوجيات والوسائل المتعلقة بالمعلومات والاتصالات وجميع الخدمات ذات الصلة وحيازتها واستخدامها واستيرادها وتصديرها وإمكانية الاستفادة منها، دونما قيد أو تمييز. وبناء على ذلك، ينبغي للدول أن تمتنع جديا عن اعتماد أي تدابير تهدف إلى منع أو تقييد نقل الدراية والتكنولوجيات والوسائل المتقدمة في مجال المعلومات والاتصالات إلى البلدان النامية، فضلا عن توفير الخدمات المتصلة بالمعلومات والاتصالات لهذه البلدان؛

(ج) تقع المسؤولية عن كفالة أمن المعلومات والاتصالات على الصعيد الوطني على عاتق فرادى الدول دون غيرها من الجهات. بيد أنه نظرا للطابع العالمي للمعلومات والاتصالات، ينبغي تشجيع الدول على أن تتعاون في مجال منع التهديدات الناجمة عن استخدام تكنولوجيات ووسائل المعلومات والاتصالات لأغراض سيئة؛

(د) ينبغي أن يحترم الحق في حرية التعبير بشكل كامل. وفي نفس الوقت، لا ينبغي أن يمارَس هذا الحق بأي حال من الأحوال على نحو يتنافى ومقاصد الأمم المتحدة ومبادئها، أو القوانين الوطنية ومبادئ حماية الأمن القومي، أو النظام العام أو الصحة العامة أو الأخلاق والآداب؛

(هـ) الدول مسؤولة عما تقوم به من أنشطة غير مشروعة دوليا تستخدم فيها تكنولوجيات ووسائل معلومات واتصالات من الواضح أنها تعود إليها؛

(و) ينبغي أن تكون تهيئة بيئة آمنة ومأمونة للمعلومات والاتصالات بما يعود بالنفع على جميع الدول هي المبدأ التوجيهي الرئيسي، وبالتالي، ينبغي أن تمتنع الدول، في جميع الأحوال، عن استخدام تكنولوجيات المعلومات والاتصالات ووسائلها لأغراض عدائية أو تقييدية أو لأغراض أخرى غير مشروعة، بما فيها تطوير أسلحة المعلومات واستخدامها؛ وتقويض أو زعزعة استقرار النظم السياسية أو الاقتصادية أو الاجتماعية لدول أخرى، أو المساس بقيمها الثقافية أو المعنوية أو الأخلاقية أو الدينية؛ ونشر المعلومات عبر الحدود على نحو يخالف القانون الدولي، بما في ذلك دستور ولوائح الاتحاد الدولي للاتصالات، أو يخالف التشريعات الوطنية للبلدان المستهدفة؛

(ز) ينبغي أن تعمل الدول على التوعية، على الصعيدين الوطني والدولي، بضرورة صون وتحسين أمن المعلومات والاتصالات من خلال الاستخدام المسؤول للتكنولوجيات والوسائل ذات الصلة، بهدف تطوير ثقافة مشتركة على الصعيد الدولي لأمن المعلومات والاتصالات.

اليابان

[الأصل: بالإنكليزية]
[١٢ آب/أغسطس ٢٠١٣]

تقييم عام لمسائل أمن المعلومات

ترى اليابان أن الفضاء الإلكتروني هو بمثابة هيكل أساسي للأنشطة الاجتماعية والاقتصادية للقطاعين العام والخاص. فالفضاء الإلكتروني ييسر النمو الاقتصادي والعمالة والتنمية، فضلا عن الديمقراطية وحماية حقوق الإنسان من خلال تأمين التدفق الحر للمعلومات وحرية التعبير عنها. واستخدام الفضاء الإلكتروني لا غنى عنه في حياة الناس، وقد شاع استعماله على الصعيد العالمي.

وفي نفس الوقت، ثمة حاجة متزايدة إلى حماية الخصوصيات وحقوق الملكية الفكرية وضمان أمن الفضاء الإلكتروني من أجل التمتع الكامل بمزايا ''الجانب الإيجابي'' لذلك الفضاء. وبالإضافة إلى ذلك، ما فتئت الهجمات الإلكترونية تُشن في جميع أنحاء العالم، وقد أضحت تشكل تهديدات عابرة للحدود الوطنية. ويمكن أن يضطلع بهذه الهجمات مختلف الكيانات بمختلف الطرق من جميع أنحاء العالم. ولا يمكن أن يتصدى أي بلد بمفرده لتزايد عدد الهجمات والجرائم الإلكترونية؛ فتعاون المجتمع الدولي، بما في ذلك الدول والأطراف المعنية، أمر لا غنى عنه لمواجهة هذه التحديات.

وانطلاقا من هذا المنظور، تسعى اليابان جاهدة إلى بناء فضاء إلكتروني آمن وموثوق به، بالتركيز في المقام الأول على كفالة التدفق الحر للمعلومات وحرية التعبير، مع إيلاء الاهتمام الواجب للتوازن بين حماية الخصوصية وضمان الأمن.

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

الجهود المبذولة على الصعيد الوطني لتعزيز أمن المعلومات

لقد أضحت التهديدات المحدقة بالفضاء الإلكتروني أكثر خطورة في الآونة الأخيرة، وصار الحفاظ على أمن الفضاء الإلكتروني يشكل برنامجا هاما لأمننا القومي ولإدارة الأزمات وتحقيق الرخاء الاقتصادي والاجتماعي، فضلا عن السلامة والسلم للشعب الياباني.

وفي هذا السياق، وضعت اليابان استراتيجية لأمن الفضاء الإلكتروني في حزيران/يونيه ٢٠١٣، تغطي الفترة ٢٠١٣-٢٠١٥. وبفضل هذه الاستراتيجية، ستتخذ

اليابان إجراءات لتحسين أمن المعلومات في الوكالات الحكومية والهياكل الأساسية البالغة الأهمية، ولتعزيز القدرة على اتخاذ تدابير مضادة للهجمات الإلكترونية.

وقد قامت اليابان، على وجه التحديد، بإدراج التدابير التالية في الاستراتيجية: تعزيز تبادل المعلومات بشأن الهجمات الإلكترونية بفضل الشراكة القائمة بين القطاعين العام والخاص؛ وتحسين مدى الإلمام بمسألة أمن المعلومات لا بالنسبة للحكومة والقطاعات المعنية فحسب، ولكن أيضا بالنسبة للشعب الياباني؛ وزيادة الوعي بأمن الفضاء الإلكتروني؛ وتعزيز القدرة على اتخاذ تدابير مضادة للهجمات الإلكترونية بفضل التعاون الدولي؛ وزيادة مساهمتنا في وضع القواعد الدولية ذات الصلة بأمن الفضاء الإلكتروني.

الجهود المبذولة على الصعيد الوطني لتشجيع التعاون الدولي

فيما يتعلق بوضع معايير دولية بشأن استخدام الفضاء الإلكتروني، علينا أن نبادر على وجه الاستعجال إلى وضع قواعد سلوك واقعية وعملية لمعالجة القضايا الراهنة في شكل غير ملزم قانونا للتعامل مع تكنولوجيات الفضاء الإلكتروني التي تشهد تقدما سريعا. وستواصل اليابان المشاركة في هذه الجهود بنشاط في المحافل الدولية.

وفيما يتعلق بتدابير بناء الثقة، فإن اليابان تشارك بنشاط في مشاورات ثنائية مع الدول المهتمة بالأمر، وفي الحوارات الإقليمية، بما في ذلك المنتدى الإقليمي لرابطة أمم جنوب شرق آسيا، وذلك بهدف ”تحسين الشفافية“ و ”تشجيع تبادل المعلومات“. وبالإضافة إلى ذلك، وسعيا إلى تفادي إحداث ثغرات أمنية في الفضاء الإلكتروني، تقدم اليابان المساعدة في مجال بناء القدرات إلى البلدان النامية في آسيا وأوقيانوسيا وأفريقيا، مثل تطوير أفرقة التصدي للطوارئ الحاسوبية وتعزيزها. وتعمل اليابان أيضا على تشجيع تبادل المعلومات على الصعيد الدولي عن طريق تعزيز التنسيق مع الأفرقة الوطنية للتصدي للطوارئ الحاسوبية التابعة لدول أخرى. وتعتقد اليابان أن هذه الجهود تسهم في بناء الثقة مع الدول المهتمة بالأمر.

مضمون المفاهيم المذكورة في الفقرة ٢ من القرار ٦٧/٢٧

تعتقد اليابان أن القانون الدولي القائم، بما في ذلك ميثاق الأمم المتحدة والقانون الدولي الإنساني، ينطبق على استخدام الفضاء الإلكتروني. ومع ذلك، بالنظر إلى الخصائص الفريدة التي تتسم بها تكنولوجيات شبكة المعلومات والاتصالات، تدعو الحاجة إلى مزيد من النظر في كيفية تطبيق فرادى القواعد والمبادئ.

وبالنظر إلى الدور الهام الذي يؤديه القانون الدولي في تأمين استقرار البيئة القانونية وإمكانية التنبؤ بها في المجتمع الدولي، فإننا نعتقد أن القيام بتحديد وتوضيح الكيفية التي يمكن أن ينطبق بها القانون الدولي الساري على الفضاء الإلكتروني من شأنه أن يكمل عملية وضع معايير دولية محددة فيما يتعلق بالفضاء الإلكتروني وأن يسهم أيضا في بناء فضاء إلكتروني مستقر.

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

القواعد الدولية لاستخدام الفضاء الإلكتروني

ليس هناك أي قواعد دولية تنظم مسألة الهجمات الإلكترونية أو التجسس الإلكتروني في الميادين الأمنية والاقتصادية والاجتماعية. وبالإضافة إلى ذلك، تظل صلاحية القواعد الملزمة قانونا في الفضاء الإلكتروني غير واضحة في هذه المرحلة. فمن الصعب التحقق من النظرة المستقبلية للفضاء الإلكتروني في الوقت الراهن، حيث تتطور تكنولوجيا الفضاء الإلكتروني بسرعة فائقة. وعلاوة على ذلك، سيستغرق تشكيل توافق في الآراء بشأن القواعد الملزمة قانونا وقتا طويلا جدا. وبالتالي، وفيما يتعلق بالطبيعة القانونية لتلك القواعد، ترى اليابان أن من المهم البدء بمناقشة مسألة إنشاء قواعد سلوك عامة غير ملزمة.

تدابير بناء الثقة

بما أن تراكم الجهود الرامية إلى بناء الثقة بين الدول يمكن أن يؤثر بشكل إيجابي على وضع قواعد دولية، يتعين على المجتمع الدولي مواصلة تشجيع تلك الجهود. ولدى تعزيز تدابير بناء الثقة، من الضروري ضمان الشفافية وتبادل المعلومات؛ غير أن مستوى التدابير المتخذة يختلف من دولة إلى أخرى، إذ أن كل دولة على حدة لها سلطة تحديد المستوى الذي يمكن أن تتصرف فيه. لذا ينبغي تشجيع تبادل المعلومات من خلال الأطر العالمية من قبيل الأطر التي ترعاها الأمم المتحدة، ومن خلال الأطر الإقليمية.

هولندا

[الأصل: بالإنكليزية]
[٧ آب/أغسطس ٢٠١٣]

ترحب هولندا ترحيبا حارا بالفرصة التي أتيحت لها لتقديم ردها على القرار ٢٧/٦٧.

تقييم عام لمسائل أمن المعلومات

تدعم هولندا وجود تكنولوجيا معلومات واتصالات آمنة وموثوق بها، وتأمين الحماية لشبكة إنترنت مفتوحة وحرة وتحترم حقوق الإنسان. فذلك أمر ضروري لتحقيق الرخاء والرفاه، وهو يؤدي دورا محفزا للنمو الاقتصادي المستدام.

ويتيح الفضاء الإلكتروني فرصا سانحة، ولكنه يجعل أيضا مجتمعاتنا أكثر عرضة للأخطار. ومن شأن الطابع العابر للحدود لهذه التهديدات أن يجعل التعاون الدولي أمرا بالغ الأهمية. والعديد من التدابير لن تكون فعالة إلا إذا نُفذت أو نُسِّقت على الصعيد الدولي. وفي هذا الصدد، تولي هولندا أهمية كبيرة للشراكات القائمة بين القطاعين العام والخاص، ولبناء الجسور من خلال تدابير بناء الثقة، والتوعية بالمسؤولية الفردية التي تقع على جميع مستخدمي تكنولوجيا المعلومات والاتصالات.

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

تعمل هولندا على الصعيدين الوطني والدولي على تأمين بيئة رقمية آمنة. فعلى الصعيد الوطني، تنفذ هولندا الاستراتيجية الوطنية لأمن الفضاء الإلكتروني المسماة ”القوة عبر التعاون“. وستقوم بتحديث هذه الاستراتيجية في عام ٢٠١٣، ومن المتوقع أن يتم نشرها في النصف الثاني من عام ٢٠١٣. وستعالج الاستراتيجية المنقحة النظرة الشاملة عن الفضاء الإلكتروني، مع الأخذ في الاعتبار الفرص الاقتصادية والانفتاح والحريات، والأمن.

ولهولندا مجلس وطني لأمن الفضاء الإلكتروني يهدف إلى ضمان اتباع نهج تعاوني بين القطاع العام، والقطاع الخاص، والمؤسسات الأكاديمية والبحثية، وإلى إسداء المشورة لصانعي القرارات الرفيعي المستوى في مجال أمن الفضاء الإلكتروني. ولها أيضا مركز وطني لأمن الفضاء الإلكتروني يهدف إلى تحديد الاتجاهات والتهديدات وتقديم المساعدة في إدارة الحوادث والأزمات. ولمهمة المركز ثلاث جوانب هي: إجراء تحليلات للتهديدات الناشئة في

الفضاء الإلكتروني استنادا إلى المعلومات الواردة من الجهات العامة والخاصة؛ والتصدي للتهديدات والحوادث في الفضاء الإلكتروني؛ وتنسيق الأعمال التنفيذية المتعلقة بمعالجة حالات الأزمات في مجال تكنولوجيا المعلومات والاتصالات. ويضم المركز فريق التصدي للطوارئ الحاسوبية القائم التابع للحكومة. وخلال العام الماضي، وسع المركز قدراته وأقام علاقات قوية مع مراكز رئيسية لتبادل المعلومات وتحليلها. ويجمع المؤتمر السنوي الدولي الذي ينظمه المركز الوطني للأمن في الفضاء الإلكتروني خبراء من الحكومات والشركات الخاصة، وخبراء إنفاذ القانون وخبراء تقنيين لتبادل أفضل الممارسات. ونفذت هولندا مجموعة كبيرة من التدابير لتحسين أمن الفضاء الإلكتروني وتحدوها رغبة قوية في إفادة بلدان ثالثة بالنماذج التي استخدمتها.

ومن الأمثلة على الشراكة بين القطاعين العام والخاص التي تستخدَم في قطاع الأمن النووي هناك الاجتماعات التقنية التي نظمتها الحكومة والتي يمكن للصناعة النووية فيها تحديد احتياجاتها في مجال أمن المعلومات. واستخدمت الحكومة المعلومات من أجل تحسين فهم ''التهديد المتخذ مرجعا''. وتعتبر ''الواقعية'' و ''التناسب'' كلمتين رئيسيتين في هذا الصدد.

وعلى الصعيد الدولي، تساهم هولندا بنشاط في الجهود التي يبذلها الاتحاد الأوروبي، وحلف شمال الأطلسي، ومنظمة الأمن والتعاون في أوروبا؛ ومنتدى إدارة شبكة الإنترنت، والشراكات الأخرى. وتنظر هولندا بعين الرضا إلى الرسالة المشتركة للمفوضية الأوروبية، وممثلة الاتحاد الأوروبي السامية للشؤون الخارجية والسياسة الأمنية التي تدعو إلى إنشاء فضاء إلكتروني مفتوح وحر وآمن للاتحاد الأوروبي والتي أيدها المجلس الأوروبي. ويتصدى الاتحاد الأوروبي لهذا التحدي مع شركائه الدوليين والمنظمات الدولية والقطاع الخاص والمجتمع المدني. وتؤيد هولندا تأييدا تاما أهداف الاتحاد الأوروبي الرامية إلى ضمان وجود شبكة إنترنت آمنة، والقيام في الوقت ذاته بتعزيز الانفتاح والحرية على شبكة الإنترنت، وإلى تشجيع وضع تدابير لبناء الثقة وقواعد للسلوك، وإلى تطبيق القانون الدولي القائم في الفضاء الإلكتروني. ونحن نؤمن إيمانا قويا بأن الأمن وحق الدخول عنصران أساسيان في الحفاظ على التطور المتواصل للإنترنت. ولتحقيق هذه الغاية، اعتمد الاتحاد الأوروبي قيما أساسية، هي كرامة الإنسان، والحرية، والديمقراطية، والمساواة، وسيادة القانون واحترام الحقوق الأساسية مبدأً توجيهياً له. وتؤيد هولندا تلك القيم الأساسية وتراها أساسا لأية استراتيجية لأمن الفضاء الإلكتروني. وتوافق هولندا على أن تشجيع وجود فضاء إلكتروني قوي وقادر على الصمود في وجه الأزمات يستوجب من القطاعين العام والخاص معا تطوير قدراتهما والعمل معا بكفاءة.

وعلى المستوى التنفيذي، تشجع هولندا التعاون العملي بين مراكز أمن الفضاء الإلكتروني (بما في ذلك منظمات أفرقة التصدي للطوارئ الحاسوبية)، وتعزيز الشبكة الدولية للمراقبة والإنذار. ويتطلب النمو السريع في جرائم الفضاء الإلكتروني الإنفاذ الفعال للحفاظ على الثقة في المجتمع الرقمي. وبالنسبة للإنفاذ، تشجع هولندا زيادة التحقيق العابر للحدود مع وكالات الإنفاذ في البلدان الأوروبية الأخرى وخارجها. وهولندا طرف في اتفاقية مجلس أوروبا المتعلقة بالجرائم الإلكترونية، وهي تشجع الدول الأخرى على الانضمام إلى تلك الاتفاقية.

وفي ما يتعلق بأمن المعلومات النووية، تتبادل هولندا في إطار الرابطة الأوروبية لمنظمي الأمن النووي المعلومات بشأن النُهج السياساتية وأفضل الممارسات بشأن الأمن النووي، في جملة مجالات منها الفضاء الإلكتروني. وتشارك هولندا بنشاط في الاجتماعات التقنية للوكالة الدولية للطاقة الذرية التي تهدف إلى تبادل المعلومات عن أمن الفضاء الإلكتروني وأمن المعلومات.

وتؤمن هولندا بأن الحرية والشفافية والأمن تسير جنبا إلى جنب ويعزز بعضها البعض. وهذا هو السبب في بدء هولندا ”تحالف الحرية على شبكة الإنترنت“ الذي يضم ٢١ حكومة عضوا. ويلتزم التحالف بتعزيز الحرية على شبكة الإنترنت والتشديد على أهمية الحقوق الرقمية. ولتحقيق هذه الغاية، يتولى تحالف الحكومات المتقاربة التفكير تنسيق جهودها، ويعمل مع المجتمع المدني والقطاع الخاص في عملية تضم أصحاب مصلحة متعددين لدعم قدرة الأفراد على ممارسة حقوق الإنسان والحريات الأساسية على الإنترنت. ولتعزيز هدف الحفاظ على شبكة الإنترنت مفتوحة وحرة للجميع، أنشأ أعضاء التحالف شراكة المدافعين الرقمية، وهو صندوق لدعم الحلول الابتكارية لحماية المدوِّنين ونشطاء شبكة الإنترنت الذين هم في خطر ولنشر خدمات الإنترنت في حالات الطوارئ في البلدان حيث شبكة الإنترنت ليست حرة أو لا يكون الوصول إليها متيسرا. وتصل مساهمة هولندا في هذا الصندوق إلى ١ ٠٠٠ ٠٠٠ يورو للفترة من ١ تشرين الأول/أكتوبر ٢٠١٢ إلى ٣١ كانون الأول/ديسمبر ٢٠١٤.

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

منطلق هولندا هو توفير شبكة إنترنت مفتوحة تشجع الابتكار وتحفز النمو الاقتصادي وتضمن الحريات الأساسية. وتشدد هولندا على أهمية مواصلة الحوار بشأن وضع معايير لسلوك الدول تهدف إلى الاستخدام الآمن للفضاء الإلكتروني. وهي تحرص على المساهمة الفعالة في هذا الحوار. وتلاحظ هولندا مع التقدير العمل الهام الذي قام به أصحاب

مصلحة وجهات فاعلة دوليون وإقليميون، مثل مجلس أوروبا والاتحاد الأوروبي، ومنظمة الأمن والتعاون في أوروبا وفريق الخبراء الحكوميين التابع للأمم المتحدة في ما يتعلق بتدابير بناء الثقة في مجال أمن الفضاء الإلكتروني.

ويؤدي أمن المعلومات دورا مركزيا في إطار عملية مؤتمر قمة الأمن النووي. وينص كل من خطة عمل مؤتمر قمة واشنطن للأمن النووي وبيان سول على أن الدول المشاركة في مؤتمر قمة الأمن النووي تهدف إلى ”منع الجهات الفاعلة من غير الدول من الحصول على المعلومات أو التكنولوجيا اللازمة لاستخدام تلك المواد لأغراض مؤذية؛ ومنع تعطيل نظم التحكم في المنشآت النووية القائمة على تكنولوجيا المعلومات“. وتدعم هولندا، باعتبارها رئيسة مؤتمر قمة الأمن النووي، جميع الجهود المبذولة للإسهام في تحقيق هذا الهدف.

وفي إطار عملية مؤتمر قمة الأمن النووي، تدعم هولندا قيادة المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية في تنفيذ وتبادل أفضل الممارسات المتعلقة بأمن المعلومات في القطاع النووي. ويتم ذلك من خلال تطوير وتعزيز التدابير والترتيبات والقدرات الوطنية من أجل توفير خدمات إدارة و أمن فعالين لهذه المعلومات؛ وتعزيز ثقافة الأمن القومي ذات الصلة؛ والعمل مع الأوساط العلمية والصناعية والأكاديمية الوطنية لتعزيز التوعية وتطوير ونشر أفضل الممارسات وزيادة المعايير المهنية؛ والقيام، بالاعتماد على الوكالة الدولية للطاقة الذرية و بالتعاون معها، بدعم المنظمات الدولية الرئيسية الأخرى والبلدان الشريكة لتيسير الإنجاز المشترك لهذه الأهداف. وتعلق هولندا أهمية كبيرة على وجود نموذج شامل لإدارة الإنترنت، يشرك القطاع الخاص ومؤسسات المعرفة في هذا الحوار وتحرص على تبادل الخبرات وأفضل الممارسات مع الآخرين.

ويمثل التبادل الدولي المكثف للمعارف والمعلومات في ما بين جميع الجهات المعنية والمنظمات أمرا بالغ الأهمية لزيادة أمان الفضاء الإلكتروني وموثوقيته، وتمكينه من اكتساب كامل إمكاناته، سواء من حيث تحقيق التنمية وتحقيق تقارب أكبر بين المجتمعات في جميع أنحاء العالم. ولذلك، ترحب هولندا بالمؤتمرين المتعلقين بالفضاء الإلكتروني اللذين عقدا في لندن وبودابست والمؤتمر القادم الذي سيعقد في سول.

وأخيرا، فإن هولندا ترى أن وضع قواعد لسلوك الدول لا يتطلب إعادة وضع للقانون الدولي، لكنه يحتاج بدلا من ذلك إلى ضمان الاتساق في تطبيق الأطر القانونية الدولية القائمة. ونحن نشجع استمرار الحوار والتفكير لتحقيق توافق في الآراء بشأن الأثر العملي لتطبيق القواعد القائمة والقانون الدولي على الفضاء الإلكتروني.

عمان

[الأصل: بالعربية]
[٢٦ حزيران/يونيه ٢٠١٣]

تود وزارة النقل والاتصالات الإبلاغ بما يلي حول قرار الجمعية العامة رقم ٦٧/٢٧ بشأن التطورات في مجال المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي.

١ - التقييم العام لمسائل أمن المعلومات

- لا شك أن التطور المتسارع لتقنية المعلومات والاتصالات صاحبه في الوقت نفسه تطور واتساع في حجم المخاطر والتهديدات، إضافة إلى التطور في الوسائل والطرق التي يستخدمها قراصنة الإنترنت والمعلومات على المستوى الدولي، وتكمن أهم التحديات والصعوبات التي تواجه الدول والمؤسسات في هذا الخصوص في غياب أو نقص الوعي والثقافة الأمنية المعلوماتية لدى مختلف مستخدمي تقنية المعلومات والاتصالات، إضافة إلى نقص الكوادر المؤهلة العاملة في هذا المجال واختلاف القوانين والتشريعات التي تنظم التعاملات الإلكترونية على الصعيد الدولي، الأمر الذي يتطلب تضافر الجهود والتعاون بين الدول في التصدي للمخاطر والتهديدات الأمنية المعلوماتية ولتحسين مستوى وجاهزية الدول للتعامل معها، إضافة إلى تعزيز الوعي الأمني المعلوماتي على الصعيد الدولي وضرورة تبادل المعلومات والخبرات في هذا المجال.

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

- إنشاء هيئة تنظيم الاتصالات عام ٢٠٠٢ وهيئة تقنية المعلومات عام ٢٠٠٦م وذلك لإدارة وتنظيم قطاعي الاتصالات وتقنيات المعلومات.
- إصدار القوانين والتشريعات المنظمة لهما وذلك بإصدار قانون المعاملات الإلكترونية بموجب المرسوم السلطاني رقم (٨٢٠٠/٦٩) وإصدار قانون تنظيم الاتصالات بموجب المرسوم السلطاني رقم (٢٢٠٠/٣٠).
- استضافة السلطنة مؤخراً المركز الإقليمي للأمن المعلوماتي في الوطن العربي التابع للاتحاد الدولي للاتصالات ومنظمة (IMPACT).
- التعامل مع المخاطر والتهديدات الفنية تم تدشين المركز الوطني للسلامة المعلوماتية بهيئة تقنية المعلومات في نيسان/أبريل ٢٠١٠.
- حصول السلطنة بمثله في هيئة تقنية المعلومات على العديد من العضويات لدى المنظمات العاملة ضمن هذا الإطار سواء على المستوى الإقليمي أو الدولي ومنها مركز أمن المعلومات التابع لمنظمة التعاون الإسلامي (CERT-OIC)، وأيضاً عضوا في المراكز الوطنية للسلامة المعلوماتية لدول الخليج العربي (CERT-GCC)، والمنظمة الدولية لأمن المعلومات (FIRST)، وكذلك حصولها على الكثير من مؤسساتها على شهادات (ISO).

- وجود خطط مستمرة من قبل المؤسسات المعنية بتطوير قطاع الاتصالات والمعلومات.
- توفير عدد من التقنيات والبرامج في مجال أمن المعلومات للمؤسسات الحكومية.
- إنشاء مركز لحماية الشبكة الحكومية.
- توفير خدمات استضافات الخدمات والمواقع الإلكترونية الحكومية مع توفير الحماية لها.
- تقديم الدعم الفني في مجالات أمن المعلومات.
- إصدار مجموعة من السياسات والمعايير في مجال أمن المعلومات.
- عقد مجموعة من التدريبية التخصصية في مجال أمن المعلومات.
- عقد عدد من البرامج والحملات التوعوية في مجال أمن المعلومات.
- إجراء برامج تقييم الجاهزية في مجال الاستجابة للطوارئ المعلوماتية.
- استضافة عدد من حلقات العمل والمؤتمرات الإقليمية والدولية في مجال أمن المعلومات.
- التواجد في الفعاليات والمهرجانات المحلية للتوعية بأمن المعلومات.
- اشتراك جميع أفراد المجتمع في مجال أمن المعلومات.
- تدشين المنتدى الخاص ببرنامج سفراء السلامة المعلوماتية في كانون الثاني/يناير ٢٠١٢.
- إنشاء موقع إلكتروني خاص بحماية الأطفال على الإنترنت (cop.cert.gov.om).
- القيام بعدد من الزيارات التوعوية الميدانية للمدارس والكليات ومقاهي الإنترنت وغيرها من أماكن تجمع النشء.
- تنظيم حلقات العمل حول أمن المعلومات التي تهدف إلى تعزيز الوعي بين الطلبة وأعضاء الهيئة التدريسية.
- تفعيل مشاركة المركز في الفعاليات العامة وذلك لجذب أكبر عدد ممكن من النشء وتعريفهم على المخاطر الأمنية والممارسات المتبعة لتجنبها.
- استحداث برنامج تدريب المدرب الذي يسعى المركز من خلاله إلى تأهيل الكوادر الوطنية من النشء في مجال أمن المعلومات.
- تدشين أول مركز عمليات لأمن المعلومات على مستوى الشرق الأوسط.

٣ - مضمون المفاهيم	• تقوم السلطنة بالمتابعة المستمرة والعمل على دراسة مضمون هذه المفاهيم الدولية وذلك لمواكبة التطورات التي تهدف لتعزيز أمن النظم العالمية للمعلومات والاتصالات السلكية واللاسلكية.
	• ضرورة مراعاة خصوصيات الدول والقوانين والتشريعات التي تنظم التعاملات الإلكترونية فيها.
	• ضرورة التقيد بالقيم والمبادئ التي تحرص كل دولة على المحافظة عليها بما يتناسب مع كل دولة على حدة.
٤ - التدابير التي يمكن أن يتخذها المجتمع الدولي لتعزيز أمن المعلومات على الصعيد العالمي	• تنظيم التعاملات الإلكترونية والأمن السيبراني في مجال المعلومات والاتصالات بين الدول من خلال فكرة إنشاء منظمة دولية تندرج تحت منظمة الأمم المتحدة في مؤتمر الأمن السيبراني المنعقد في السلطنة في شهر آذار/مارس ٢٠١٣.
	• التعاون فيما بين الدول من أجل تأمين قطاع الاتصالات وتقنية المعلومات، والذي أصبح عصبا رئيسيا في معظم الدول والذي يُعتمد عليه بشكل كبير في التنمية، ومن الضروري أن يكون هذا التعاون تحت مظلة دولية.
	• مواصلة التنسيق بين الدول لتعزيز أمن المعلومات والإطلاع على التجارب الرائدة في ذلك المجال.
	• التعاون في مجال الحوادث الأمنية المعلوماتية وتحديد نقاط اتصال لكل بلد يمكن الرجوع إليها في هذا الخصوص.
	• المشاركة في السياسات والضوابط وأفضل الممارسات الأمنية المعلوماتية.
	• المشاركة في الخبرات والتدريب التخصصي في مجال أمن المعلومات وتبادل الزيارات.
	• عقد الندوات وحلقات العمل للعاملين في مجال أمن المعلومات.
	• التعاون لنشر الوعي والثقافة الأمنية على الصعيد الدولي من خلال برامج دولية مشتركة.
	• التعاون على الصعيد الأكاديمي وإيجاد برامج ومناهج في مجالات أمن المعلومات المختلفة.
	• تشجيع وتعزيز البرامج المشتركة في مجالات البحث والتطوير في هذا المجال.

تركيا

[الأصل: بالإنكليزية]
[١٠ حزيران/يونيه ٢٠١٣]

تقييم عام لمسائل أمن المعلومات

أصبح أمن المعلومات ضرورة في عالم معولم مع ازدياد استخدام تكنولوجيات المعلومات. وأمن المعلومات وأمن الفضاء الإلكتروني مسألتان يجب أن تُدارا بالتعاون مع جميع الأطراف ذات الصلة. وفي تركيا، أنشئ مجلس أمن الفضاء الإلكتروني، وهو آلية مركزية للتنسيق بين الأطراف ذات الصلة ومتابعة الدراسات المرتبطة بهذا الموضوع، وذلك بموجب قرار مجلس الوزراء بشأن إنفاذ الدراسات المتعلقة بأمن الفضاء الإلكتروني وإدارتها والتنسيق بينها الذي نُشر في الجريدة الرسمية التركية، العدد رقم ٢٨٤٤٧، المؤرخ ٢٠ تشرين الأول/أكتوبر ٢٠١٢.

وتمت الموافقة على الاستراتيجية الوطنية لأمن الفضاء الإلكتروني وخطة العمل للفترة ٢٠١٣-٢٠١٤ في ٢٠ كانون الأول/ديسمبر ٢٠١٢، وذلك في الاجتماع الأول للمجلس الوطني لأمن الفضاء الإلكتروني.

وأهداف الاستراتيجية وخطة العمل هي كما يلي:

- إنشاء هياكل أساسية تمكن من توافر الخدمات والعمليات والبيانات التي تقدمها المنظمات الحكومية من خلال تكنولوجيات المعلومات
- ضمان أمن نظم المعلومات المستخدمة في الهياكل الأساسية الحيوية التي يقوم بتشغيلها إما الحكومة أو القطاع الخاص
- تحديد الإجراءات الاستراتيجية المتعلقة بأمن الفضاء الإلكتروني للتخفيف إلى أدنى حد من آثار الهجمات في هذا الفضاء وتقصير الفترة الزمنية المستغرقة للعودة إلى الحالة الطبيعية بعد الهجمات
- إنشاء هياكل أساسية تيسر قيام السلطات القضائية وهيئات إنفاذ القانون بالتحقيق في الجرائم الإلكترونية.

والمجالات الرئيسية لخطة العمل هي كما يلي:

١ - الأنظمة

٢ - الدراسات الهادفة إلى تيسير العمليات القضائية

٣ - إنشاء فريق وطني للتصدي للطوارئ الحاسوبية

٤ - تعزيز الهياكل أساسية الوطنية لأمن الفضاء الإلكتروني

٥ - تدريب وتوعية الموارد البشرية بشأن أمن الفضاء الإلكتروني

٦ - تطوير التكنولوجيات الوطنية من أجل أمن الفضاء الإلكتروني

٧ - توسيع نطاقات الآليات الوطنية المتعلقة بأمن الفضاء الإلكتروني.

وتتكون خطة العمل من ٢٩ مجال عمل يتعين تنفيذها في إطار المجالات الرئيسية المذكورة أعلاه.

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

تقوم الهيئة التنظيمية الوطنية التركية، وهي سلطة تكنولوجيات المعلومات والاتصالات (BTK)، التي كُلفت بموجب قانون الاتصالات الإلكترونية (رقم ٥٨٠٩)، بمجموعة من الأنشطة للمساهمة في الجهود المبذولة لتلبية الاحتياجات الوطنية والدولية في مجال أمن المعلومات.

وفي هذا السياق، يرد ذكر أنشطة السلطة في مجال أمن الفضاء الإلكتروني أدناه.

١ - التنظيم وعمليات التفتيش

يرد تحديد لعدة متطلبات للمشغِّلين المأذون لهم في اللائحة الداخلية المتعلقة بأمن الاتصالات الإلكترونية والبلاغ ذي الصلة الذي يتخذ هذه اللائحة أساسا له. وتهدف الدراسات ذات الصلة إلى تعزيز مستوى أمن الفضاء الإلكتروني الوطني مباشرة في أنشطة المشغلين والمساهمة ضمنيا في أمن الفضاء الإلكتروني الدولي.

ومن ناحية أخرى، هناك أيضا أنظمة السلطة المتعلقة بالتوقيع الإلكتروني والبريد الإلكتروني المسجَّل في سياق قانون التوقيع الإلكتروني (رقم ٥٠٧٠) وقانون التجارة التركي (رقم ٦١١٢). وتسهم هذه الأنظمة في الجهود المبذولة من أجل تعزيز أمن وموثوقية عمليات تبادل الوثائق والرسائل الإلكترونية.

٢ - تمارين أمن الفضاء الإلكتروني

تنظم سلطة تكنولوجيات المعلومات والاتصالات تمارين في أمن الفضاء الإلكتروني لزيادة تطوير القدرات التقنية والإدارية، والتوعية وإيجاد فرص للتعاون الدولي.

٢-١ التمرين الوطني المتعلق بأمن الفضاء الإلكتروني لعام ٢٠١١

نظِم التمرين الوطني المتعلق بأمن الفضاء الإلكتروني لعام ٢٠١١ في الفترة من ٢٥ إلى ٢٨ كانون الثاني/يناير ٢٠١١، بمشاركة ٤١ منظمة من المنظمات العامة والخاصة وغير الحكومية التي تشمل ممثلين من قطاعات المالية، وتكنولوجيا المعلومات والاتصالات، والتعليم، والدفاع، والصحة، وكذلك الوحدات القضائية ووحدات إنفاذ القانون وعدة وزارات. وشاركت ست من المنظمات المذكورة في التمرين بصفة مراقب.

٢-٢ تمرين درع الفضاء الإلكتروني لعام ٢٠١٢

نظِم هذا التمرين في أيار/مايو ٢٠١٢ بتنسيق من سلطة تكنولوجيات المعلومات والاتصالات وبمشاركة ١٢ مقدما لخدمات الإنترنت يعملون في قطاع الاتصالات الإلكترونية. وكان المشاركون هم المالكون لأكبر حصة سوقية في القطاع، إلى جانب مقدمي خدمات الإنترنت على الهواتف المحمولة من الجيل الثالث. وفي هذا التمرين، جرى بالأساس تطبيق هجمات حجب الخدمة الموزَّع على المشاركين و تم تقييم مدى كفاية التدابير الأمنية المتخذة ضد الهجمات.

٢-٣ التمرين الوطني المتعلق بأمن الفضاء الإلكتروني لعام ٢٠١٣

عقِد التمرين الوطني الخاص بأمن الفضاء الإلكتروني لعام ٢٠١٣، الذي شاركت في تنظيمه سلطة تكنولوجيات المعلومات والاتصالات ومجلس الأبحاث العلمية والتكنولوجية في تركيا ، تحت رعاية وزارة النقل والشؤون البحرية والاتصالات، في الفترة من ٢٤ كانون الأول/ديسمبر ٢٠١٢ إلى ١١ كانون الثاني/يناير ٢٠١٣، بمشاركة ٦١ منظمة من المنظمات العامة والخاصة والمنظمات غير الحكومية. وعلى الرغم من أن معظم من شارك كانت منظمات عامة، فقد شاركت أيضا منظمات خاصة ومنظمات غير حكومية في هذا التمرين. وبالإضافة إلى ذلك، حضر المناسبة الختامية للتمرين بصفة متحدثَين كل من رئيس تحالف الاتحاد الدولي للاتصالات - الشراكة الدولية المتعدِّدة الأطراف لمكافحة تهديدات الفضاء الإلكتروني وعضو من أعضاء مجلس إدارة منتدى أفرقة التصدي للحوادث والأمن، اللذين هما منبران للتعاون الدولي في مجال أمن الفضاء الإلكتروني.

٣ - مشروع منع تهديدات الفضاء الإلكتروني

يشمل مشروع منع تهديدات الفضاء الإلكتروني (Siber Tehditleri Önleme Projesi-STOP) وضع الآليات اللازمة لإنشاء نظام مصيدة لقراصنة الإنترنت للكشف عن تهديدات الفضاء الإلكتروني، وإقامة وتحسين نظام تقارير عن الهجمات الإلكترونية وإنتاج البيانات الوصفية بشأن تهديدات الفضاء الإلكتروني. وتنفذ الأنشطة التي يتطلبها المشروع وفقا للمواعيد النهائية المتوقعة في خطة العمل المتعلقة بأمن الفضاء الإلكتروني على المدى القصير. وفي سياق بُعد التعاون الدولي للمشروع، أصبحت سلطة تكنولوجيات المعلومات والاتصالات عضوا في التحالف القائم بين الشراكة الدولية المتعدِّدة الأطراف لمكافحة تهديدات الفضاء الإلكتروني والاتحاد الدولي للاتصالات، الذي يعمل تحت إشراف الاتحاد المذكور.

٤ - مشروع منع البريد الإلكتروني الطفيلي

نُفذ هذا المشروع في عام ٢٠٠٩، بتنسيق من سلطة تكنولوجيات المعلومات والاتصالات وبفضل جهود مقدمي خدمات الإنترنت ومقدمي خدمات الاستضافة. وكان الغرض من المشروع هو منع البريد الإلكتروني الطفيلي الذي يشكل تهديدا لأمن شبكة الإنترنت ويقي موارد الشبكة مشغولة. وعند نهاية المشروع، تم تخفيض عدد مقدمي خدمات الإنترنت الذين ينشرون البريد الإلكتروني الطفيلي بنسبة ٩٩ في المائة؛ وقد انعكس هذا التحسن في التقارير التي أعدتها شركات عالمية لأمن الفضاء الإلكتروني.

٥ - إنشاء نقطة محلية للتبادل على الإنترنت

تتسبب ممارسة التوجيه التي يقوم بها مقدمو خدمات الإنترنت، والمتمثلة في القيام بدون داع بنشر حركة استخدام الإنترنت بين نقطتي نهاية انطلاقا من نقطة بعيدة في حدوث انخفاض في جودة الخدمة بسبب التأخر غير الضروري في الإرسال وفي زيادة في المخاوف الأمنية.

وفي هذا السياق، ومن خلال إنشاء نقطة فعالة للتبادل على الإنترنت وقدرة المشغلين على تبادل حركة الاستخدام في ظل ظروف أكثر جاذبية، يمكن تحقيق انخفاض كبير في ممارسات التوجيه غير المرغوب فيها المذكورة والمخاوف الأمنية التي تنجم عنها. ولذلك، تقوم السلطة بأنشطة مختلفة مع الأطراف ذات الصلة (مقدمو خدمات الإنترنت المحليون ومقدمو المحتوى الدوليون) تركز على تشكيل نقطة تبادل على الإنترنت محلية وفعالة.

تدابير لتعزيز أمن المعلومات على الصعيد العالمي

إنشاء فريق وطني للتصدي للطوارئ الحاسوبية

من الضروري اليوم تشكيل منظمة للاستجابة للحوادث في الفضاء الإلكتروني تعمل بشكل فعال على المستوى الوطني للكشف عن تهديدات الفضاء الإلكتروني الناشئة حديثا، واتخاذ التدابير اللازمة للحد من آثار الحوادث المحتملة في الفضاء الإلكتروني وتبادل المعلومات أو القضاء عليها. وتحقيقا لهذه الغاية، فوضت وزارة النقل والشؤون البحرية والاتصالات، في شباط/فبراير ٢٠١٣، مهمة إنشاء وتشغيل الفريق الوطني للتصدي للطوارئ الحاسوبية لتركيا إلى رئاسة الاتصالات، وشرع في تنفيذ أنشطة متنوعة لإنشاء الفريق الوطني للتصدي للطوارئ الحاسوبية الذي سيعمل على مدار الساعة وطيلة أيام الأسبوع لمواجهة تهديدات أمن الفضاء الإلكتروني. وسيعمل فريق التصدي للطوارئ الحاسوبية (USOM)، الذي بدأ في العمل في أيار/مايو ٢٠١٣، بتعاون وثيق مع أفرقة التصدي للطوارئ الحاسوبية في الدول الأخرى والمنظمات الدولية.

ونتيجة للتطور والانتشار السريعين لتكنولوجيات المعلومات والاتصالات، فإن التهديدات التي يتعرض لها أمن المعلومات تتجاوز الحدود الوطنية. ومن ثم، من الأهمية بمكان بالنسبة للمنظمات الدولية والحكومات تعزيز التعاون بشأن المسائل المتصلة بأمن المعلومات وتنفيذ هذا التعاون في أقرب وقت ممكن.