الأمم المتحدة

A/66/152

الجمعية العامة

Distr.: General
15 July 2011
Arabic
Original: English/Russian

الدورة السادسة والستون

البند ٩٣ 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

المحتويات

* A/66/150.

020811 020811 11-41689 (A)

أولاً – مقدمة

١ – دعت الجمعية العامة جميع الدول الأعضاء، في الفقرة ٣ من قرارها ٦٥/٤١، إلى أن تواصل، آخذة في اعتبارها التقييمات والتوصيات الواردة في تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي[(١)]، 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 – وفي ١٦ آذار/مارس ٢٠١١، عملا بذلك الطلب، أُرسلت مذكرة شفوية إلى الدول الأعضاء تدعوها إلى توفير معلومات عن الموضوع. وترد في الفرع الثاني أدناه الردود التي تم تلقيها. وستصدر أي ردود إضافية يتم تلقيها في شكل إضافات لهذا التقرير.

ثانيا – الردود الواردة من الحكومات

أستراليا

[الأصل: بالإنكليزية]
[٣١ أيار/مايو ٢٠١١]

ترحب أستراليا بفرصة تقديم هذا الرد المتضمن لآرائنا عملا بقرار الجمعية العامة ٦٥/٤١ بشأن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي.

وتتطلع أستراليا لأن تصبح من الدول الرائدة عالميا في أمن الفضاء الإلكتروني. ونحن نسلم بأهمية تطور التكنولوجيا والفوائد التي تعود من ذلك على الاقتصاد الرقمي العالمي وأمن الدول كافة. وتهدف أستراليا إلى تحقيق أكبر قدر من المكاسب الاقتصادية والأمنية لجميع الدول نتيجة لخبرتنا الفنية.

(١) A/65/201.

ومع انتشار التكنولوجيا لتعم جميع أوجه حياتنا، فإن اعتماد الحكومات ودوائر الأعمال والأفراد عليها آخذ في التزايد لطائفة متنوعة من الأغراض والمهام التي تتراوح بين مشتريات السلع والخدمات عبر الإنترنت، والتواصل مع الآخرين، والبحث عن المعلومات، وإدارة الشؤون المالية، والتحكم في المعدات في قطاعي التعدين والصناعة التحويلية. وبغية تحقيق أقصى قدر من الفوائد من الإنترنت والاقتصاد الرقمي، ولتعزيز أمن الفضاء الإلكتروني حول العالم، من الضروري للغاية أن تعمل الدول مجتمعة لكي يصبح الفضاء الإلكتروني مكانا موثوقا به، وآمنا، ومرنا. وتسعى أستراليا جاهدة لكي تصبح طرفا سباقا وفعالا في تعزيز الفضاء الإلكتروني لجميع المستخدمين – من الدول، ودوائر الأعمال، والأفراد.

التقييم العام لمسائل أمن المعلومات

تقر أستراليا بأن أمن الفضاء الإلكتروني يشكل إحدى الأولويات العليا للأمن الوطني. ويظل المجتمع العالمي يشهد زيادة في حجم الجريمة الإلكترونية ومستوى تعقيدها والنجاح في ارتكابها. ومع تزايد كمية وقيمة المعلومات الإلكترونية، تزايدت كذلك جهود المجرمين وغيرهم من فاعلي الشر الذين اتخذوا من الإنترنت سبيلا أكثر خفية وملاءمة وربحية للقيام بأنشطتهم.

ويجب الموازنة بين جهود التصدي لهذه المخاطر والتعامل معها والحريات المدنية الفردية، بما في ذلك الحق في الخصوصية، وضرورة تعزيز الكفاءة والابتكار لكفالة تحقيق أستراليا للإمكانات الكاملة للاقتصاد الرقمي.

ويعتمد أمن أستراليا الوطني وازدهارها الاقتصادي ورفاهها الاجتماعي، وينطبق ذلك على كل دولة بمفردها، اعتمادا حاسما على توافر وسلامة وسرية طائفة من تكنولوجيات المعلومات والاتصالات. واستجابة لذلك، خصصت الحكومة الأسترالية موارد كبيرة للقيام على نحو استباقي بتعزيز صيانة بيئة تشغيل إلكترونية موثوق بها وآمنة ومرنة لمصلحة جميع المستخدمين.

وفي حين أن السياسة الأمنية الإلكترونية للحكومة الأسترالية تعنى بالدرجة الأولى بتوافر تكنولوجيا المعلومات والاتصالات الأسترالية وسلامتها وسريتها، فإن تلك السياسة يتم تنسيقها مع السياسات والبرامج ذات الصلة الأخرى مثل سلامة الفضاء الإلكتروني التي تركز على حماية الأفراد، خاصة الأطفال، من المحتويات الضارة، أو الترهيب، أو الترصد، أو ”الاستمالة“ على الإنترنت لأغراض الاستغلال الجنسي.

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

الجهود المحلية لتعزيز أمن المعلومات

تقر أستراليا بأنه لا بد لها من تقديم المثل على أفضل الممارسات محليا لتتمكن من تعزيز التعاون الدولي في الفضاء الإلكتروني. ولأستراليا نهج متكامل تقوده الحكومة إزاء حماية الفضاء الإلكتروني وتعزيز أمنه. وفي عام ٢٠٠٩، بدأت الحكومة تنفيذ استراتيجيتها الأولية لأمن الفضاء الإلكتروني التي تجسد الهدف الأسمى لسياسة الحكومة الأسترالية لأمن الفضاء الإلكتروني وغاياتها وتحدد الأولويات الاستراتيجية التي ستتبعها الحكومة لتحقيق تلك الغايات. وتتضمن الاستراتيجية أيضا وصفا للإجراءات والتدابير الرئيسية التي ستُتخذ من خلال مجموعة شاملة من الأعمال التي ستنفذ في جميع مكونات الحكومة الأسترالية لبلوغ تلك الأولويات الاستراتيجية.

والهدف من سياسة أستراليا لأمن الفضاء الإلكتروني هو الحفاظ على بيئة تشغيل إلكتروني موثوق بها وآمنة ومرنة تدعم الأمن الوطني لأستراليا وتحقق أقصى قدر من الفوائد للاقتصاد الرقمي. وتشمل المبادرات الرئيسية للاستراتيجية إنشاء منظمتين داعمتين لبعضهما، وهما: فريق جديد للتصدي للطوارئ الحاسوبية ومركز عمليات أمن الفضاء الإلكتروني. ويوفر فريق التصدي للطوارئ الحاسوبية، الذي أنشئ عام ٢٠١٠، نقطة اتصال وحيدة لمعلومات أمن الفضاء الإلكتروني لجميع الأستراليين ولدوائر الأعمال الأسترالية ويكفل حصول مستخدمي الإنترنت في أستراليا على المعلومات عن الأخطار التي تهدد الفضاء الإلكتروني، ونقاط الضعف في أنظمتهم، ومعلومات عن الكيفية المثلى لحماية تكنولوجيا المعلومات والاتصالات لديهم. ويحافظ الفريق على علاقات عمل وثيقة مع مالكي ومشغلي الهياكل الأساسية الحيوية ودوائر الأعمال التي تشغل أنظمة هامة لأمن أستراليا الوطني. ويوفر الفريق لدوائر الأعمال هذه معلومات مستهدفة عن مهددات أمن الفضاء الإلكتروني وأوجه ضعفه للمساعدة في توفير حماية أفضل لهياكلها الأساسية لتكنولوجيا المعلومات والاتصالات. ويوفر مركز العمليات، الذي أنشئ عام ٢٠١٠، وعيا بحالة أمن الفضاء الإلكتروني من جميع المصادر للحكومة الأسترالية وقدرة معززة لتيسير الاستجابات التشغيلية لأحداث الفضاء الإلكتروني ذات الأهمية الوطنية. ويقوم المركز بتحديد الهجمات المعقدة على الفضاء الإلكتروني وتحليلها، ويقدم المساعدة في الاستجابة لأحداث الفضاء الإلكتروني عبر الأنظمة والهياكل الأساسية الحيوية للحكومة والقطاع الخاص.

وتتمثل إحدى أولويات الاستراتيجية في تثقيف جميع الأستراليين وتمكينهم بتزويدهم بالمعلومات والثقة والأدوات العملية لحماية أنفسهم على الإنترنت. والمبدأ الموجه للاستراتيجية هو مبدأ المسؤولية المشتركة حيث ينبغي لجميع المستخدمين، وهم يستمتعون بمزايا تكنولوجيا المعلومات والاتصالات، اتخاذ خطوات مسؤولة لتأمين أنظمتهم الخاصة، وينبغي لهم توخي الحيطة في توصيل وتخزين المعلومات الحيوية، وعليهم التزام باحترام معلومات وأنظمة المستخدمين الآخرين. ولتمكين الأفراد من الاضطلاع بدور نشط في أمن المعلومات، من الضروري أن يكون لدى الأفراد وعي وتفهم لبيئة الفضاء الإلكتروني ومخاطرها. ولبلوغ ذلك، لدى أستراليا برنامج مستمر للتوعية يشمل موقعا لمعلومات أمن الفضاء الإلكتروني يستهدف مستخدمي الإنترنت من المترل ومستخدمي الإنترنت من أصحاب الأعمال التجارية الصغيرة، بما في ذلك أصحاب المعرفة المحدودة بالفضاء الإلكتروني ومهاراته (انظر الموقع www.staysmartonline.gov.au)، وأسبوعا للتوعية بأمن الفضاء الإلكتروني يُنظم بالاشتراك مع دوائر الأعمال، وجماعات المستهلكين، والمنظمات المجتمعية الأساس. ويساعد أسبوع التوعية الأستراليين على فهم مخاطر أمن الفضاء الإلكتروني ويثقف مستخدمي الإنترنت من المترل ومستخدمي الإنترنت من الأعمال التجارية الصغيرة بالخطوات البسيطة التي يمكن لهم اتخاذها لحماية معلوماتهم الشخصية والمالية على الإنترنت. وخلال أسبوع التوعية بأمن الفضاء الإلكتروني الوطني لعام ٢٠١٠، شارك نحو ١٥٠ من الوكالات الحكومية والقطاعات الصناعية والمنظمات المجتمعية ومنظمات المستهلكين في تنظيم مناسبات وأنشطة في المدن والأقاليم والمناطق الريفية في أستراليا. وفي عام ٢٠١١، سينظم أسبوع التوعية في الفترة من ٣٠ أيار/مايو إلى ٤ حزيران/يونيه.

وعملت الحكومة الأسترالية على نحو استباقي مع رابطة صناعة الإنترنت، وهي تقر بأن أمن الفضاء الإلكتروني هو مسؤولية مشتركة، لوضع مدونة مبتكرة لممارسات أمن الفضاء الإلكتروني لمقدمي خدمات الإنترنت العاملين بصفة طوعية (''المدونة'')، حيث بدأ ذلك في كانون الأول/ديسمبر ٢٠١٠. وتوفر المدونة نهجا متسقا لمقدمي خدمات الإنترنت الأستراليين للمساعدة في إعلام عملائهم وتثقيفهم وحمايتهم فيما يتصل بمسائل أمن الفضاء الإلكتروني. وقدمت أستراليا عرضا عن التنفيذ الناجح للمدونة في منتديات متعددة الأطراف وأشركت غيرها في الدروس المستفادة من وضع المدونة. وقد قُدمت العروض في الفرقة العاملة المعنية بأمن المعلومات والخصوصية والتابعة لمنظمة التعاون والتنمية في الميدان الاقتصادي في كانون الأول/ديسمبر ٢٠١٠، وفي الفريق العامل المعني بالاتصالات السلكية واللاسلكية والمعلومات التابع لرابطة التعاون الاقتصادي لآسيا والمحيط الهادئ، وفي جماعة آسيا والمحيط الهادئ للاتصالات السلكية واللاسلكية. وتتطلع أستراليا إلى تقاسم هذه المدونة

مع الدول الأخرى، عن طريق الأنشطة الثنائية لبناء القدرات والمنتديات المتعددة الأطراف، ومساعدة الدول الأخرى على تحسين التعاون مع مقدمي خدمات الإنترنت هؤلاء وجعلهم يتحلون بقدر أكبر من المسؤولية عن تثقيف المستخدمين وحمايتهم.

تعزيز التعاون الدولي

تولي أستراليا أولوية عليا للتعاون الدولي في مجال أمن الفضاء الإلكتروني. وبالنظر إلى الطابع عبر الوطني للإنترنت الذي يتطلب فيه أمن الفضاء الإلكتروني الفعال اتخاذ إجراءات عالمية منسقة، اعتمدت أستراليا نهجا نشطا ومتعدد المستويات إزاء المشاركة الدولية. ويشمل ذلك، في جملة أمور، التعاون مع الحكومات والمنظمات الأجنبية على الصعيد الثنائي وفي منتديات متعددة الأطراف للمساعدة في تعزيز أفضل الممارسات الدولية، والدروس المستفادة، وبناء القدرات، والتشجيع على اتخاذ نهج عالمي منسق إزاء محاربة مهددات أمن الفضاء الإلكتروني.

وتشمل مشاركة أستراليا في الأمم المتحدة المشاركة في تقديم القرارات بشأن إنشاء ثقافة عالمية لأمن الفضاء الإلكتروني ومراجعة الجهود الوطنية لحماية الهياكل الأساسية للمعلومات الحيوية، وبشأن التطورات في ميدان المعلومات والاتصالات اللاسلكية في سياق الأمن الدولي. واستجابت أستراليا أيضا لقرار الجمعية العامة للأمم المتحدة ٦٤/٢١١ بتقديم مساهمة عن أفضل الممارسات في مجال حماية الهياكل الأساسية للمعلومات الحيوية، بما فيها تكنولوجيا المعلومات والاتصالات، بهدف تعزيز فرص حدوث تحسن عالمي في أمن الفضاء الإلكتروني. وأستراليا عضو في الاتحاد الدولي للاتصالات السلكية واللاسلكية، وهي تسهم في المجموعات الدراسية في إطار قطاعي توحيد مقاييس الاتصالات السلكية واللاسلكية وتطوير الاتصالات السلكية واللاسلكية التابعين للاتحاد. وتوفر أستراليا التمويل لقطاع تطوير الاتصالات السلكية واللاسلكية التابع للاتحاد من أجل أعمال بناء القدرات في منطقة آسيا والمحيط الهادئ، بما في ذلك مبادرات أمن الفضاء الإلكتروني. وأستراليا مساهم نشط في الفرقة العاملة المعنية بأمن المعلومات والخصوصية والتابعة لمنظمة التعاون والتنمية في الميدان الاقتصادي والرئيس السابق لها، وهي تعمل الآن بصفتها بلدا متطوعا في التحليل المقارن الذي تجريه الفرقة لاستراتيجيات أمن الفضاء الإلكتروني. وعملت أستراليا بوصفها دولة قائدة أساسية في وضع وتنفيذ اتفاق مكافحة البريد الإلكتروني التطفلي بين سول وملبورن بشأن التعاون بين دولتي منطقة آسيا والمحيط الهادئ على مكافحة البريد الإلكتروني التطفلي وخطة عمل لندن وهي الشبكة البارزة للإنفاذ والتعاون على الصعيد الدولي في مجال مكافحة البريد الإلكتروني التطفلي.

وتتمتع أستراليا بعلاقة تعاونية مع شركائها الإقليميين وهي ملتزمة بالعمل معهم. ونحن نشارك عن كثب مع البلدان الأخرى في منطقتنا في بناء القدرات من أجل بلوغ فضاء إلكتروني موثوق به ومرن وآمن. وتشارك أستراليا في أنشطة الفريق العامل المعني بالاتصالات السلكية واللاسلكية والمعلومات التابع لرابطة التعاون الاقتصادي لآسيا والمحيط الهادئ وفي عمل المنتدى الإقليمي لرابطة أمم جنوب شرق آسيا في مجال أمن الفضاء الإلكتروني. وأستراليا هي الجهة الداعية النائبة للفريق التوجيهي لأمن وازدهار الاتصالات السلكية واللاسلكية التابع لرابطة التعاون الاقتصادي لآسيا والمحيط الهادئ. وتسعى أستراليا حاليا إلى المشاركة في قيادة المجال الأساسي المعني بالإرهاب الإلكتروني والجريمة عبر الوطنية في إطار خطة عمل المنتدى الإقليمي لرابطة أمم جنوب شرق آسيا.

وعلى الصعيد التنفيذي، يحتفظ فريق التصدي للطوارئ الحاسوبية بعلاقات عمل وثيقة مع المنظمات الوطنية للتصدي للطوارئ الحاسوبية حول العالم. وفي أستراليا، يشارك الفريق بنشاط في تبادل المعلومات على نحو موثوق وسريع وتيسيره على الصعيد العالمي، بما في ذلك المعلومات عن الأخطار وأوجه الضعف، لكفالة الإبقاء على الوعي بالحالة الأمنية والاستجابة العالمية المتسقة والمنسقة للأخطار على شبكة الإنترنت. ويساهم الفريق بنشاط في مبادرات بناء القدرات، خاصة في منطقة آسيا والمحيط الهادئ، بسبل منها عضويته في فريق آسيا ومنطقة المحيط الهادئ لمواجهة الطوارئ الحاسوبية. وإدراكا بأن أمن المعلومات أمر غير محدود جغرافيا، يعمل الفريق أيضا في تعاون وثيق مع الشركاء الآخرين من خلال عضويته في منتدى فرق التصدي للحوادث والأمن والشبكة الدولية للمراقبة والإنذار.

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

ينبغي لجميع الدول، بما فيها أستراليا، أن تواصل السعي لإيجاد تدابير تقليدية وابتكارية على حد سواء من أجل تعزيز أمن المعلومات. ويتطلب التحدي العالمي الذي يفرضه أمن الفضاء الإلكتروني مضاعفة الجهود في المنتديات المتعددة الأطراف بهدف تحسين أمن شبكات العمل البيني. ويشمل ذلك الجهود المبذولة داخل الأمم المتحدة والاتحاد الدولي للاتصالات، والمنتديات الإقليمية مثل رابطة التعاون الاقتصادي لآسيا والمحيط الهادئ ومجموعات دولية معنيَّة أكثر بمواضيع محددة، كمنتدى أفرقة التصدي للحوادث والأمن والشبكة الدولية للرصد والإنذار.

وتؤيد أستراليا وضع مبادئ دولية للسلوك المسؤول في الفضاء الإلكتروني، بما يشمل الاتفاق على مجموعة واسعة من المبادئ المتعلقة بالسلوك المعياري في ذلك الفضاء، مما سيسهِّل تحسين التعاون الدولي وتعزيز الثقة على هذا الصعيد، ويؤدي إلى وضع قواعد

دولية متفق عليها بشأن الفضاء الإلكتروني. وستستمر أستراليا، بوصفها عضواً في المجتمع العالمي، في دعم التقدم بهذا الخصوص عن طريق المنتديات الثنائية والمتعددة الأطراف للمساعدة على إقامة بيئة إلكترونية أكثر أمناً ومرونة وجدارة بالثقة.

وتشمل الجهود المحددة التي يمكن أن يبذلها المجتمع الدولي لتعزيز أمن المعلومات على الصعيد العالمي ما يلي:

(أ) وضع معايير عالمية، بما في ذلك الاتفاق على مجموعة واسعة من المبادئ الدولية للسلوك المعياري في الفضاء الإلكتروني من أجل تسهيل التعاون الدولي على نحو أفضل وتعزيز الثقة؛

(ب) التوسُّع في قدرة النظام القانوني الدولي على مكافحة الجرائم الإلكترونية، بما في ذلك تحقيق الاتساق في الأطر القانونية (توسيع إمكانية الانضمام إلى اتفاقية مجلس أوروبا بشأن الجرائم الإلكترونية مثلاً، التي تتوقع أستراليا أن تلبِّي متطلباتها بحلول نهاية عام ٢٠١١)، وتعزيز التعاون في مجال إنفاذ القانون لتمكين البلدان من إرساء القانون المحلي بفعالية؛

(ج) تطوير وتشجيع أفضل الممارسات في تقدير الحالة والإنذار الاستراتيجي والاستجابة للحوادث، بما في ذلك إنشاء أفرقة وطنية للتصدي للطوارئ الحاسوبية، تتولى إجراء وتنسيق هذه الأنشطة بين جميع الدول؛

(د) اضطلاع الدول ذات الخبرة الطويلة والراسخة في هذا المجال بمبادرات التوعية وأنشطة بناء القدرات لمساعدة الدول النامية على إقامة فضاء إلكتروني موثوق به وآمن وقابل للتكيف لفائدة الجميع؛

(هـ) اتباع نهج أكثر اتساقاً في إقامة الشراكات مع القطاعات ذات الصلة بالإنترنت لوضع مبادئ توجيهية بشأن السلوك في الفضاء الإلكتروني، كمدونة قواعد الممارسات الأسترالية المتعلقة بقطاع الإنترنت مثلاً.

المفاهيم الدولية ذات الصلة

يوفر القانون الدولي الحالي إطاراً للحماية من التهديدات القائمة إزاء أمن المعلومات والناشئة عن مجموعة متنوعة من العناصر الفاعلة. وبالإمكان تطبيق مجموعة من المبادئ القانونية الدولية القائمة حالياً في استخدامات الفضاء الإلكتروني، منها مبادئ المساواة في السيادة بين الدول، وحظر استعمال القوة والأعمال العدوانية، وكذلك القانون الإنساني الدولي. ومن الضروري إجراء مزيد من المناقشات بين الدول، سواء في المحافل الدولية أو الإقليمية، للتوصل إلى تحديد أدق لنطاق هذه المبادئ وقابلية تطبيقها إزاء التهديدات الناشئة عن عالم الإنترنت.

جورجيا

[الأصل: بالإنكليزية]

[١ حزيران/يونيه ٢٠١١]

في سياق جورجيا، أُوليت مسائل أمن المعلومات اهتماماً خاصاً بعد آب/أغسطس ٢٠٠٨، حين شنَّ الاتحاد الروسي هجوماً كبيراً موزعاً لقطع الخدمات عن جورجيا.

ونظراً لتقييم هذه الأحداث وفي ظل التطورات الأخيرة السريعة والواسعة النطاق لمشاريع وخدمات الحوكمة الإلكترونية، أصبح أمن المعلومات يشكل أحد الجوانب الهامة لمفهوم الأمن الوطني. وسعياً إلى تحسين تنظيم أمن المعلومات، بدأت حكومة جورجيا تنفيذ عدد من المبادرات الهامة في الأعوام الأخيرة.

ففي عام ٢٠١٠، أُنشئ كيان قانوني تابع لوزارة العدل في جورجيا، يُدعى وكالة تبادل البيانات، وأُوكلت إليه المسؤولية المباشرة عن وضع وتنفيذ سياسة أمن المعلومات في القطاع الحكومي. وبإنشاء هذه الوكالة، وضعت حكومة جورجيا الآلية المؤسسية لتحقيق الحوكمة الإلكترونية وأمن المعلومات على نحو منسق.

وتتعاون وكالة تبادل البيانات مع وزارة العدل في جورجيا، في إطار المهام المنصوص عليها في القانون والميثاق الخاص بها، في اتباع سياسة أمن المعلومات وتنفيذها على نحو يتوخى فيه الامتثال لمعيار المنظمة الدولية لتوحيد المقاييس ٠٠٠ ٢٧. وتنسِّق الوكالة أيضاً إنفاذ واعتماد الآليات أو المعايير اللازمة لأمن المعلومات في القطاعات الحكومية والتجارية، ولا سيما بتنفيذ الأنشطة على مستويات مختلفة من الأهمية. ويُعد من أهم هذه الأنشطة المؤتمر الجورجي السنوي للابتكارات في مجال تكنولوجيا المعلومات، الذي يتناول جدول أعماله على الدوام أمن المعلومات وأمن الفضاء الإلكتروني؛ كما أناطت الوكالة بالمؤتمر المذكور ولاية وضع وتنفيذ سياسة التوعية العامة بشأن مسائل أمن المعلومات وأمن الفضاء الإلكتروني.

وفي سياق أمن الفضاء الإلكتروني اليومي، عُهد إلى الوكالة بمسؤولية إنشاء وتشغيل فريق التصدي للطوارئ الحاسوبية الذي يعمل حالياً داخل الوكالة بهدف إدارة حوادث أمن المعلومات في الفضاء الإلكتروني الجورجي. وتعمل الوكالة أيضاً على رصد سير عمل الشبكة الحكومية الجورجية بغرض حماية أمنها.

كما تقضي مهام الوكالة، في سياق تكنولوجيا المعلومات والاتصالات، برفع مستويات التعليم المهني (لتدريب أخصائيي أمن المعلومات) وإعداد المقترحات، ورصد الأمن، وإصدار شهادات التوقيعات الرقمية. ونظراً للنطاق الذي يغطيه التعليم المهني، تخطط الوكالة لتنفيذ عدد من المشاريع الخاصة بمساعدة الجهات المانحة الدولية (كالاتحاد الأوروبي والبنك الدولي). وستكفل هذه المشاريع المستوى المناسب للتعليم المهني؛ أما بالنسبة لأمن التوقيعات الرقمية، فسوف تؤدي وكالة تبادل البيانات هذه المهمة عند قيام وكالة السجل المدني بإصدار بطاقات الهوية الإلكترونية للمواطنين (التي تحمل التوقيعات الرقمية).

وإلى جانب نشاط وكالة تبادل البيانات التي تمثل الوكالة الرائدة والمنسِّقة لأمن المعلومات، ينبغي الإشارة إلى المبادرات الأخرى التي تنفذها حكومة جورجيا حالياً وتشارك فيها وكالة تبادل البيانات بنشاط، وهي:

(أ) أُنشئ فريق الخبراء العامل المعني باستراتيجية وخطة عمل أمن الفضاء الإلكتروني (التي حُددت على نحو ملموس في الجزء التالي)، وهو تابع لمجلس الأمن الوطني الجورجي؛

(ب) يجري وضع عدد من المبادرات التشريعية، بما في ذلك القانون الإداري والقانون المنظم لأسرار الدولة اللذان من المقرر أن يصدرا عن برلمان جورجيا في عام ٢٠١١. وتجدر الإشارة بوجه خاص إلى مشروع قانون أمن المعلومات الذي تعمل وكالة تبادل البيانات على وضعه حالياً قبل تقديمه إلى البرلمان للنظر فيه عام ٢٠١١؛

(ج) في عام ٢٠١٠، وضعت وزارة العدل ووزارة المالية في جورجيا، بمساعدة الوكالة، النُظم الداخلية لأمن المعلومات (السياسة والمبادئ التوجيهية) وبدأت باعتمادها. ومن المتوقع أيضاً تنفيذ مبادرات مماثلة في مؤسسات حكومية أخرى.

ألمانيا

[الأصل: بالإنكليزية]

[٦ حزيران/يونيه ٢٠١١]

شهدت الحالة الأمنية في الفضاء الإلكتروني تغيراً جوهرياً على مدى الأعوام الأخيرة. فمن ناحية، بوسعنا أن نشاهد عملية ابتكار جارية تحرّكها التكنولوجيا بالنظر إلى أن عدداً لا يني يتزايد من العمليات التجارية بات يدار اليوم إلكترونياً، وهي عمليات مترابطة، وتكون أحياناً متصلة بشبكة الإنترنت بشكل مباشر أو غير مباشر. وبشكل مستمر، تزداد

نُظم تكنولوجيا المعلومات تعقيداً، فيما تُطوى بسرعة متنامية دورة الابتكار لتحل محلها دائماً دورات ابتكارية جديدة. ومن ناحية أخرى، تهاجم الجريمة المنظمة والجهات الفاعلة الأخرى من غير الدول شبكات تكنولوجيا المعلومات وقواعد بياناتها ومواقعها الشبكية. وفي بعض الحالات، تخلِّف هذه الهجمات آثاراً لم تقيَّم بعد تقييماً واقعياً.

ولهذا السبب، اعتمدت الحكومة الاتحادية في شباط/فبراير ٢٠١١ استراتيجية جديدة لأمن الفضاء الإلكتروني. ويقوم أساس الاستراتيجية على حماية الهياكل الأساسية الحيوية. ويتعين على جميع السلطات الحكومية التي تتعامل مع مسائل أمن الفضاء الإلكتروني أن تعمل، في إطار هذه الاستراتيجية، بشكل وثيق ومباشر مع بعضها البعض ومع القطاع الخاص في إطار مركز جديد للاستجابة الإلكترونية لكشف وتحليل الحوادث الكبرى في مجال تكنولوجيا المعلومات على وجه السرعة، والتوصية باعتماد تدابير وقائية. وفيما يتعلق بالسياسة، يُعنى مجلس الأمن الإلكتروني الجديد، على مستوى وزير الدولة، بالمسائل الرئيسية لأمن الفضاء الإلكتروني وموقف ألمانيا بشأنه.

ويشمل ذلك تنسيق السياسة الخارجية للمجال الإلكتروني، بما يشمل جوانب من السياسة الخارجية والدفاعية والاقتصادية والأمنية. وتشير الصلات الدولية القائمة في مجال الفضاء الإلكتروني إلى أن العمل المنسق على الصعيد الدولي أمر جوهري. ولذا، فإن ألمانيا ستدعو بإلحاح إلى تعزيز أمن الفضاء الإلكتروني داخل الاتحاد الأوروبي وفي المنظمات الدولية.

وتدعو ألمانيا في إطار استراتيجيتها لأمن الفضاء الإلكتروني، وبالنظر إلى الترابط العالمي لتكنولوجيا المعلومات، إلى وضع معايير عامة، غير خلافية، وملزِمة سياسياً لسلوك الدول في الفضاء الإلكتروني. وينبغي أن تكون هذه المعايير مقبولة لجزء كبير من المجتمع الدولي وأن تتضمن تدابير لبناء الثقة وتعزيز الأمن.

اليونان

[الأصل: بالإنكليزية]

[٦ حزيران/يونيه ٢٠١١]

بات يجري اليوم تناول مسائل أمن المعلومات على نطاق أوسع مما كان في الماضي. ويُنظر حالياً في اتخاذ تدابير للتصدي للتهديدات الملازمة لعولمة الشبكات والنظم. ويتم دراسة وتطبيق تدابير للحفاظ على حرية تدفق المعلومات في السياقين الوطني والدولي معاً.

ويجري اتباع المفاهيم الدولية والمتعددة الجنسيات الحالية وإجراء دراسات بشأنها. وهناك حاجة إلى إصدار توجيه دولي بشأن تقييم المخاطر. وينبغي أيضا تناول موضوع حماية الفضاء الإلكتروني. وينبغي الاحتفاظ بالحقوق السيادية الوطنية فيما يتصل بأمن المعلومات في أي عملية تبادل لهذه المعلومات على الصعيد العالمي.

وغني عن القول إنه ينبغي أن تواصل جميع الدول الأعضاء إبلاغ الأمين العام بآرائها وتقييماتها بشأن المسائل ذات الصلة. وفي هذا الصدد، يجدر ذكر النقاط التالية:

(أ) تولَى جميع المسائل المتصلة بأمن المعلومات أولوية عليا؛

(ب) يجري دراسة وتطبيق سبل الحفاظ على التدفق الحر للمعلومات والعمل على تحقيق المستويات المطلوبة لسريتها وسلامتها وتوافرها، عبر الحدود الوطنية والدولية؛

(ج) ينبغي صياغة مفاهيم الربط بين الشبكات التي توفر القدرات المستحدثة والمشتركة على الصعيدين الوطني والدولي والاتفاق بشأنها. ويجب أن يتوفر تقييم لمخاطر الربط بين الشبكات والتوجيه الدولي في هذا الصدد. وبالإضافة إلى ذلك، وبما أن حماية الفضاء الإلكتروني تشكل أحد مصادر القلق البالغ بالنسبة لكل دولة، فإن هناك حاجة لاتخاذ تدابير لحماية هذا الفضاء واعتماد توجيه دولي منسق للتعاون وإعمال روح الكفاءة والاقتصاد. وأخيرا وليس آخرا، لا يمكن تجاهل حاجة البلد للحفاظ على سيادته وعلى قاعدة معلومات خاصة به، ويجب مراعاة هذا الأمر في صياغة أي من المفاهيم التي تتم صياغتها؛

(د) في ما يلي التدابير التي يمكن أن يتخذها المجتمع الدولي لتعزيز أمن المعلومات على الصعيد العالمي:

'١' ينبغي أن تكون المفاهيم الدولية ذات الصلة مفصلة ومتفقا عليها؛

'٢' يمكن اقتراح خطة توجيهية بشأن وضع هياكل أساسية عامة منسقة تغطي مسائل التشريع الأساسية، وذلك لكفالة أمن المعلومات المطلوب في مناولة جميع المراسلات والرسائل إلكترونيا، وإتاحة سبل الاتصال المتعددة؛

'٣' ينبغي مواءمة وتوسيع نطاق المفاهيم التي تتبعها التحالفات المتعددة الجنسيات وتجمعات الدول الصغيرة على نحو يجعلها قابلة للتطبيق على الصعيد العالمي. ويمكن أن يكون الاتفاق بشأن تحديد التهديد وأثره السلبي على البشرية أهم من وضع تدابير متطورة يتم استحداثها، حيث إن هذه التدابير قد يستخدمها الخصوم أيضا؛

'٤' بالتوازي مع كل ما سبق، ينبغي أن تُفهم سيادة الدولة على أنها المرجعية الأساسية لكل محاولة للعولمة. وينبغي وضع مفهوم دولي لتحديد مداخل تبادل المعلومات الوطنية في ظل سيناريوهات تعكس مستوى التكامل المطلوب، واستخدامه كدليل في جميع الجهود المبذولة على الصعيد الوطني والمتعدد الجنسيات والدولي.

تدابير بناء الثقة والأمن في الفضاء الإلكتروني

الفضاء الإلكتروني منفعة عامة وفضاء عام. ولذلك، فعلينا 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 يستخدمون أدوات التثبت من الهوية لمكافحة سرقة الهوية، وضمان سلامة البيانات والشبكات وسريتها.

ولما كان الفضاء الإلكتروني فضاء عالميا بطبيعته، فإن ضمان أمن الفضاء الإلكتروني وإعمال الحقوق وحماية الهياكل الأساسية الحيوية للمعلومات يتطلب بذل الدولة لجهود كبيرة على الصعيد الوطني وبالتعاون مع الشركاء الدوليين على السواء.

وبناء عليه، فإن ألمانيا على استعداد للعمل على وضع جملة من القواعد السلوكية تنظم سلوك الدول فيما بينها في الفضاء الإلكتروني، ولا سيما تدابير بناء الثقة والشفافية والأمن، ليقوم أكبر عدد ممكن من البلدان بالتوقيع عليها.

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

(أ) التأكيد على المبادئ العامة كمبدأ توافر البيانات والشبكات وسريتها وسلامتها وتنافسيتها وأصالتها، والخصوصية، وحماية حقوق الملكية الفكرية؛

(ب) احترام الالتزام بحماية الهياكل الأساسية الحيوية؛

(ج) تعزيز التعاون بهدف اتخاذ تدابير بناء الثقة والحد من المخاطر والشفافية والاستقرار من خلال:

- تبادل الاستراتيجيات الوطنية وأفضل الممارسات والمفاهيم الوطنية التي تحيل إلى التشريعات الدولية للفضاء الإلكتروني؛
- تبادل وجهات النظر الوطنية عن القواعد القانونية الدولية المتعلقة باستخدام الفضاء الإلكتروني؛
- إعداد جهات الاتصال وإخطارها؛
- إعداد آليات للإنذار المبكر وتعزيز التعاون فيما بين أفرقة الاستجابة للطوارئ الحاسوبية؛
- ترقية روابط الاتصال في حالات الأزمات لتشمل حوادث الفضاء الإلكتروني، ودعم وضع توصيات فنية تعزز إقامة هياكل أساسية إلكترونية عالمية تكون قوية وآمنة؛
- المسؤولية عن مكافحة الإرهاب التي تضم 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 الضخمة، كالألعاب الأولمبية.

وعلاوة على ذلك فإننا نرى ضرورة بدء نقاش حول إقامة تعاون دولي في إطار إسناد الهجمات الإلكترونية، التي عادة ما يكون تتبعها صعبا للغاية، ومسؤولية الدولة عن الهجمات الإلكترونية التي تشن من أراضيها عندما لا تفعل تلك الدول شيئا لوقف مثل هذه الهجمات على الرغم من علمها بها، ومسؤولية الدول عن عدم تسهيل وجود مجالات يسودها الفلتان الأمني في الفضاء الإلكتروني، من قبيل التغاضي عن علم عن تخزين البيانات الشخصية التي تُجمع بشكل غير قانوني على أراضيها.

الجوانب العسكرية لأمن الفضاء الإلكتروني

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

بيد أن أمن المعلومات، في الفكر العسكري، يواجه، في أي فهم عملياتي، لا بتحديات من خصم محتمل باستخدام أسلحة التدمير المادي للهياكل الأساسية للمعلومات

فحسب، ولكن أيضا من مستخدمين لا يتحلّون بحس المسؤولية، أو من تكنولوجيا معطوبة، أو مجرمين، أو ببساطة نتيجة للحوادث.

وبالتالي، فإن الجهود التي يتعين بذلها تتراوح بين توعية كل مستخدم من المستخدمين وضمان موثوقية سلسلة التوريد لتكنولوجيا المعلومات وبين الدفاعات المرنة من أجل درء هجمات قراصنة الفضاء الإلكتروني وبين تكنولوجيا معلومات تكون ذات هياكل أساسية مرنة عموما.

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

وفي مرحلة سابقة أنشأت القوات المسلحة الألمانية هياكل أساسية مرنة للقيادة والتحكم، واستحدثت تقنيات وإجراءات أمنية فضلا عن إنشاء منظمة لأمن تكنولوجيا المعلومات تضم جميع فروع القوات المسلحة وتشمل إنشاء فريق مستقل للاستجابة للطوارئ الإلكترونية قادر على التدخل في حالات الأعطال الحرجة في عمل تكنولوجيا المعلومات. ويمثل تكييف قدراتنا الشخصية والفنية لمواجهة استمرار زيادة مستوى التهديد مهمة دائمة.

وتقوم القوات المسلحة الألمانية بالتعاون تعاونا وثيقا مع وزارة الداخلية الألمانية الاتحادية في جهودها ويدعم بقوة تعزيز أمن المعلومات في حلف شمال الأطلسي والاتحاد الأوروبي، وصوغ السياسات والقدرات اللازمة لهذه الغاية. علاوة على ذلك، تجري القوات المسلحة تبادلات منتظمة مع عدد من البلدان في سياق أمن المعلومات على صعيد السياسات والصعيد العملي على حد سواء.

وترحب القوات المسلحة الألمانية بالمبادرات وتعمل إلى جانب الوزارات الأخرى للحكومة الألمانية الاتحادية على تلبية الطلبات الدولية بتأمين مزيد من الحماية لعمل شبكات المعلومات على نطاق العالم، من مثل وضع مدونة دولية طوعية لقواعد السلوك في الفضاء الإلكتروني.

الدفاع عن الفضاء الإلكتروني في حلف شمال الأطلسي (الناتو)

يعتبر حلف شمال الأطلسي (الناتو) أمن الفضاء الإلكتروني أحد التحديات الأمنية الناشئة الرئيسية. وينص المفهوم الاستراتيجي الذي اعتمده رؤساء الدول والحكومات في قمة حلف شمال الأطلسي المعقودة في لشبونة في تشرين الثاني/نوفمبر ٢٠١٠ على أن ”الهجمات الإلكترونية يمكن أن تبلغ حدا تهدد معه الازدهار والأمن والاستقرار على الصعيدين الوطني والأوروبي - الأطلسي“.

وكلف رؤساء الدول والحكومات مجلس حلف شمال الأطلسي، في إعلان القمة، ”بأن يقوم، مستندا إلى حد كبير إلى الهياكل الدولية القائمة وعلى أساس مراجعة لسياستنا الحالية، برسم سياسة متعمقة للحلف في مجال الدفاع عن الفضاء الإلكتروني بحلول حزيران/يونيه عام ٢٠١١، وأن يعد خطة للعمل من أجل تنفيذها“.

وفي خطوة أولى صوب السياسة الجديدة، اعتمد وزراء دفاع الحلف مفهوما للدفاع عن الفضاء الإلكتروني في آذار/مارس ٢٠١١.

ويركز المفهوم على حماية شبكات حلف الناتو والشبكات الوطنية للدول الأعضاء المرتبطة بشبكات الحلف أو التي تعالج معلومات الحلف (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 يعتزم الناتو التعاون مع الدول الشريكة والهيئات الدولية المعنية كالأمم المتحدة والاتحاد الأوروبي والقطاع الخاص والأوساط الأكاديمية.

وترحب ألمانيا بالتزام الناتو المتعلق بأمن الفضاء الإلكتروني، وتنشط في دعمها للمناقشات.

أمن الفضاء الإلكتروني في منظمة الأمن والتعاون في أوروبا

دأبت منظمة الأمن والتعاون في أوروبا طوال عدة سنوات على مناقشة قضايا 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 أنه لا بد من تحقيق ”وحدة أكبر للهدف والفعل في مواجهة ما ينشأ من تهديدات عابرة للحدود الوطنية“. وذكر إعلان أستانا التذكاري التهديدات في الفضاء الإلكتروني مثالا على هذه التهديدات الناشئة العابرة للحدود الوطنية.

وشاركت ألمانيا مشاركة نشطة في مؤتمر منظمة الأمن والتعاون المتعلق باتّباع نهج شامل الأمن الفضاء الإلكتروني: ”بحث الدور المستقبلي لمنظمة الأمن والتعاون في أوروبا“، الذي عقد في فيينا يومي ٩ و ١٠ أيار/مايو ٢٠١١. وفي سياق المؤتمر، نوقشت توصيات ملموسة لأنشطة المتابعة التي ستضطلع بها منظمة الأمن والتعاون في أوروبا.

وستواصل ألمانيا دعمها الفعلي لمناقشات منظمة الأمن والتعاون في أوروبا التي تدور حول بحث الدور المستقبلي للمنظمة في مجال أمن الفضاء الإلكتروني.

كازاخستان

[الأصل: بالروسية]

[٧ تموز/يوليه ٢٠١١]

في عام ٢٠١٠ أنشأت جمهورية كازاخستان فريقا للاستجابة للطوارئ الإلكترونية من أجل ضمان أمن الفضاء الإلكتروني لتكنولوجيا المعلومات والاتصالات.

وفي هذا الصدد، فإن المعلومات الواردة من مستخدمي شبكة كازنت عن وجود أي فيروسات أو رموز أمنية أو برامج لنظام البناء – التشغيل – نقل الملكية أو انتهاكات للشروط القانونية (المواد الإباحية والعنف والتعدي على حقوق النشر والتأليف، إلخ) المكتشفة في نطاق KZ أو في المواقع التي تستضيفها كازاخستان، ترسَل إلى فريق الاستجابة للطوارئ الإلكترونية لتحليلها.

هولندا

[الأصل: بالإنكليزية]

[٦ حزيران/يونيه ٢٠١١]

التقييم العام لمسائل أمن المعلومات

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

وتوفر تكنولوجيا المعلومات والاتصالات فرصا، ولكنها أيضا تزيد من الهشاشة التي يعاني منها مجتمعنا. وتجعل الطبيعة العابرة للحدود للتهديدات من التعاون الدولي أمرا حاسما. ولن يكون العديد من التدابير فعالا إلا إذا نفذت تلك التدابير، أو نُسقت، على المستوى الدولي. وفي هذا الصدد، تولي هولندا أهمية كبيرة للشراكات بين القطاعين العام والخاص وللمسؤولية الفردية من جانب جميع مستخدمي تكنولوجيا المعلومات والاتصالات.

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

تعمل هولندا على الصعيدين الوطني والدولي على تأمين بيئة رقمية آمنة. فعلى الصعيد الوطني، قدمت الحكومة الهولندية، في شباط/فبراير ٢٠١١، استراتيجية وطنية للأمن في الفضاء الإلكتروني بعنوان ''القوة عبر التعاون''. وفي إطار الاستراتيجية، ستقوم الحكومة في تموز/يوليه من هذا العام بإنشاء مجلس وطني لأمن الفضاء الإلكتروني لضمان انتهاج نهج تعاوني بين القطاع العام، والقطاع الخاص، والمؤسسات الأكاديمية والبحثية. وستنشئ الحكومة أيضا مركزا وطنيا للأمن في الفضاء الإلكتروني من أجل تحديد الاتجاهات والتهديدات والمساعدة في إدارة الحوادث والأزمات. ومن المهام الرئيسية للمركز إجراء تحليلات للتهديدات الناشئة في الفضاء الإلكتروني استنادا إلى معلومات واردة من الجهات العامة والخاصة. وسيضم المركز الفريق الحالي للاستجابة للطوارئ الإلكترونية.

وعلى الصعيد الدولي، تساهم هولندا بنشاط في الجهود التي يبذلها الاتحاد الأوروبي وحلف شمال الأطلسي، ومنتدى إدارة شبكة الإنترنت، والاتحاد الدولي للاتصالات السلكية واللاسلكية، والشراكات الأخرى. وتشجع هولندا التعاون العملي بين مراكز أمن الفضاء الإلكتروني (بما في ذلك منظمات أفرقة الاستجابة للطوارئ الإلكترونية)، وتعزيز الشبكة الدولية للمراقبة والإنذار. ويتطلب النمو السريع في جرائم الفضاء الإلكتروني الإنفاذ الفعال للحفاظ على الثقة في المجتمع الرقمي. وبالنسبة للإنفاذ، تهدف هولندا إلى تشجيع 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.

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

تدرك هولندا أهمية مواصلة الحوار بشأن وضع معايير لسلوك الدول تهدف إلى الاستخدام الآمن للفضاء الإلكتروني. وهي تحرص على المساهمة الفعالة في هذا الحوار. ومنطلق هولندا في ذلك هو توفير شبكة إنترنت مفتوحة تشجع الابتكار وتحفز النمو الاقتصادي وتضمن الحريات الأساسية.

وتولي هولندا أهمية كبيرة لإشراك القطاع الخاص ومؤسسات المعرفة في هذا الحوار وتحرص على تبادل الخبرات وأفضل الممارسات مع الآخرين. ويمثل التبادل الدولي المكثف للمعارف والمعلومات بين جميع الجهات المعنية والمنظمات أمرا بالغ الأهمية لزيادة أمان الفضاء الإلكتروني وموثوقيته. كما يمثل الاتساق في تطبيق الأطر القانونية الدولية القائمة قضية هامة أخرى تستحق الاهتمام الدولي.

الولايات المتحدة الأمريكية

[الأصل: بالإنكليزية]
[٧ حزيران/يونيه ٢٠١١]

أولا – مقدمة

تشكل تكنولوجيا المعلومات والاتصالات أمرا هاما بالنسبة لتطور جميع الدول الأعضاء. فمن شأن هذه التكنولوجيات، المتصلة ببعضها لإنشاء الفضاء الإلكتروني، المساعدة في إيجاد رؤية مشتركة لمجتمع المعلومات على النحو المتوخى في مؤتمر القمة العالمي المعني بمجتمع المعلومات الذي عُقد في عامي ٢٠٠٣ و ٢٠٠٥. وتُسهم تكنولوجيا المعلومات والاتصالات في الأعمال الأساسية للحياة اليومية، وفي التجارة وتوفير السلع والخدمات، والأبحاث، والابتكار، ومبادرات رجال الأعمال، وتدفق المعلومات بحرية بين الأفراد والمنظمات والحكومات. فهي تشكل وسيلة جديدة قوية، تمكن من إنشاء الحكومة الإلكترونية، وتعزيز التنمية الاقتصادية، وتيسير تقديم المساعدات الإنسانية، والتمكين من تحقيق السلامة المدنية العامة الهامة، وبناء الهياكل الأساسية الأمنية الوطنية. علاوة على ذلك، ليس هناك مغالاة في الإمكانيات التي توفرها الاتصالات الشبكية للحد من الحواجز التي تقف في طريق الفهم والتعاون الدوليين.

ومع ازدياد الاعتماد على تكنولوجيا المعلومات والاتصالات، تزداد أيضا المخاطر المرافقة لهذا الاعتماد. فمجموعة الأحداث والأنشطة المتباينة، الطبيعية منها والتي من صنع الإنسان، إنما تهدد سير العمل بشكل يمكن الاعتماد عليه في الهياكل الأساسية الوطنية الهامة والشبكات العالمية وسلامة المعلومات التي تنتقل عبرها أو تخزن فيها. فالتهديدات التي من صنع الإنسان آخذة في الازدياد، عددا وتعقيدا وخطورة. وبعض هذه التهديدات مصدره الدول، لكن كثيرا منها مصدره جهات فاعلة من غير الدول، وتنطوي على أنشطة إجرامية أو إرهابية. وتختلف الدوافع، من سرقة الأموال أو المعلومات أو تعطيل المنافسين، إلى النزعة الوطنية وتوسيع الصيغ التقليدية للمنازعات الدولية كي تشمل الفضاء الحاسوبي. والجهات الفاعلة هذه مصدر التهديد تستهدف الأفراد والشركات والهياكل الأساسية الوطنية الحساسة والحكومات، على حد سواء، وأثرها ينطوي على عواقب هامة بالنسبة لرفاه وأمن فرادى الدول والمجتمع الدولي المتصل عالميا ككل.

وأيا كانت الخطوات الوطنية التي قد تتخذها الحكومات محليا لحماية شبكات معلوماتها، فإن التعاون الدولي بشأن وضع استراتيجيات للحد من الأخطار التي تتعرض لها تكنولوجيا المعلومات والاتصالات أمر جوهري لضمان الأمن للجميع. ولا بد للحكومات

من أن تكون على ثقة من أن شبكاتها التي تدعم أمنها الوطني وازدهارها الاقتصادي هي شبكات سليمة وقادرة على التحمل. وإيجاد هياكل أساسية موثوقة من أجل تكنولوجيا المعلومات والاتصالات سوف يضمن أن يحقق الجميع الإمكانيات التي تنطوي عليها ثورة المعلومات.

وهذا الأمر ليس بالمهمة السهلة. فالمجتمع الدولي يواجه تحديا يتمثل في الحفاظ على بيئة تعزز الكفاءة والابتكار والازدهار الاقتصادي وحرية التجارة في ذات الوقت الذي تعزز فيه أيضا السلامة والأمن والحريات المدنية والحقوق المتعلقة بالحياة الخاصة. ومما يزيد من صعوبة هذه المهمة حدة السمات الفريدة التي تتصف بها تكنولوجيا المعلومات والاتصالات. فالشبكات، المتاحة للجميع، يملكها ويديرها غالبا القطاع الخاص وليس الحكومات. ووسائل تكنولوجيا المعلومات المعطِّلة هي، بخلاف الأسلحة التقليدية، سرية ولا يمكن رؤيتها. واستخدامها يمكن أن يمر خلال دول كثيرة، بحيث يكون من الصعب تحديد منشأ الفاعل أو هويته أو دعمه. كما تقوم الجهات الفاعلة من غير الدول بشكل مطرد بتطوير قدرات تزيد من إمكانية استخدام الجهات الفاعلة من الدول ومن غير الدول وكلاء عنهم لارتكاب أنشطة معطِّلة في الفضاء الإلكتروني. وهذه السمات تجعل الاستراتيجيات التقليدية، كوضع تدابير شبيهة بتلك التدابير المستخدمة للحد من الأسلحة، غير فعالة في مراقبة أو تقييد الجهات الفاعلة هذه مصدر التهديد، ولذلك كان من الضروري إيجاد نُهج جديدة خلاقة للتخفيف من هذه المخاطر. ورغم صعوبة هذه المهمة، لا بد للدول الأعضاء من أن تتحد لتحقيق الهدف المشترك المتمثل في الاستمرار في المساهمة التي تقدمها تكنولوجيا المعلومات وتحسينها وذلك عن طريق ضمان أمنها وسلامتها.

ومهام الدول الأعضاء مهام مضاعفة: فهي مهام محلية ودولية معا. فضمان أمن الهياكل الأساسية الوطنية للمعلومات مسؤولية على الحكومات أن تتحملها على الصعيد المحلي، بالتنسيق مع أصحاب المصلحة ذوي الصلة في المجتمع المدني. وفي الوقت ذاته، ينبغي دعم الجهود المحلية عن طريق التعاون الدولي بشأن الاستراتيجيات التي تعالج الطابع عبر الوطني الذي تتصف به مختلف التهديدات التي تتعرض لها نظم شبكات المعلومات. وينبغي أن تتضمن هذه الجهود التعاون بشأن إدارة الأحداث والتخفيف من آثارها والاستجابة لها؛ والتحقيق والمقاضاة الجنائية عبر الوطني؛ والتوصيات الفنية لتحسين متانة الهياكل الأساسية الإلكترونية؛ والتأكيد على مدونات قواعد السلوك المشتركة دوليا التي تدعمها تدابير بناء الثقة المصممة لتعزيز الاستقرار والحد من مخاطر التصورات الخاطئة.

ثانيا – التهديدات والمخاطر ونقاط الضعف

التهديدات التي تتعرض لها شبكة النظم التي تشكل سوية الفضاء الإلكتروني، والمعلومات التي تنتقل عبرها، هي إحدى التحديات العالمية الخطيرة في القرن الحادي والعشرين. فمن خلال تكنولوجيا المعلومات والاتصالات تستطيع الجهات الفاعلة من الدول وغير الدول أن تستهدف المواطنين العاديين، والتجارة، والهياكل الأساسية الصناعية الحيوية، والحكومات. والتلاقي الحاصل بين تكنولوجيا المعلومات والاتصالات والإنترنت والهياكل الأساسية الأخرى إنما يشكل فرصا لم يسبق لها مثيل بالنسبة لشل الاتصالات السلكية واللاسلكية، والطاقة الكهربائية، وأنابيب النقل ومصافي النفط، والشبكات المالية، والهياكل الأساسية الحساسة الأخرى.

فالخصائص الفريدة لتكنولوجيا المعلومات تسهل استخدامها من أجل الأنشطة المعطِّلة وتشكل تحديات شديدة بالنسبة للحكومات التي تسعى إلى الحد من هذه المخاطر. وبخلاف التكنولوجيات العسكرية التقليدية، فإن الشبكات التي تشكل الفضاء الإلكتروني هي ليست حكرا على الحكومات، بل، في كثير من الحالات، تعود ملكيتها وإدارتها للقطاع الخاص. وتكنولوجيا المعلومات بحد ذاتها هي تكنولوجيا متاحة على نطاق واسع وهي بطبيعتها ليست مدنية ولا عسكرية، حيث يعتمد استخدامها حصرا على دوافع المستعمل.

ووسائل البرمجة الحاسوبية المستخدمة من أجل التعطيل، متاحة بحرية للجميع، على الأقل في أشكالها الأساسية. وفي استطاعة أي شخص يتمتع بالمهارات اللازمة أن يوجد نهجا أكثر تعقيدا. وفضلا عن ذلك، فإن هذه الوسائل تتطور بسرعة مستغلة نقاط الضعف المكتشفة حديثا. وهذه الوسائل ليست مرئية بالمعنى التقليدي، فهي سرية تماما وقد تكمن فيها ''تواقيع'' يمكن تقليدها بسهولة. وبسبب طبيعة الإنترنت، بالإمكان تمرير الرمز الضار من خلال الكثير من الأقاليم الوطنية قبل وصوله إلى الهدف، مما يجعل تحديد مصدره شاقا ومضيعا للوقت وغالبا ما يحتاج إلى تعاون كبير على الصعيد عبر الوطني. وحتى لو تم اكتشاف منشئه، يمكن أن تبقى هوية الفاعلين أو الداعمين بعيدة المنال. وبناءاً على ذلك، فإن الجهات الفاعلة ذات النوايا الخبيثة يمكن أن تعمل بكل سرية، متمتعة إلى حد كبير بميزة الإفلات من العقاب، من أي مكان في العالم تقريباً.

ومما يزيد من طمس الهوية طمس الدافع الكامن وراء التسلل في الفضاء الإلكتروني. فقد يعمل المجرمون المنظمون وغيرهم من الأفراد أو المجموعات لتعزيز مصالحهم لكنهم قد يُجندون أيضا للعمل كوكلاء من قِبل الجهات الفاعلة من الدول وغير الدول على حد سواء. وقد يخلق عدم توفر الإسناد الموثوق في الوقت المناسب وإمكانية ''الغش'' عدم اليقين

والبلبلة بالنسبة للحكومات، مما يزيد من احتمال عدم الاستقرار في الأزمات، والردود المغلوطة الوجهة، وفقدان السيطرة على التصعيد خلال الحوادث الحاسوبية الكبيرة.

ومن الجهات الفاعلة الرئيسية التي تشكّل معا تهديدات لعمل الفضاء الإلكتروني بشكل موثوق ما يلي:

(أ) **المجرمون** – منشأ الكثير من الوسائل الشريرة هو الجهود التي يبذلها المجرمون وقراصنة الحاسوب المنظمون. وازدياد تعقيد ونطاق الأنشطة الإجرامية إنما يُبرز احتمال أن تؤثر الأنشطة الشريرة المرتكبة في الفضاء الإلكتروني في القدرة الوطنية على المنافسة، وأن تسبب انحسارا في الثقة بوجه عام في استخدام الإنترنت من أجل التجارة والتبادل التجاري، بل وحتى شل الهياكل الأساسية المدنية عن الحركة. وحجم ونطاق هذه الأنشطة آخذان في التزايد.

(ب) **الدول** – هناك إبلاغ عام متزايد مصدره الروايات المتناقلة من أن الدول تقوم باستخدام واستخدام قدرات توسّع الأشكال التقليدية للمنازعات بين الدول وتدخلها في الفضاء الإلكتروني أو أنها تستخدمه لهذا الغرض أو تعمل من خلاله. بيد أن البينات القاطعة المتعلقة بالمصدر أو النوايا وراء الأحداث التي يُزعم بوجه عام بأنها من فعل دول ما برحت بعيدة المنال. وكما هو الحال في معظم الأحيان، فإن هوية ودافع الفاعل (الفاعلين) يمكن استنتاجهما فقط من الهدف والآثار وغيرها من البيّنات الظرفية المحيطة بالحادث.

(ج) **الإرهابيون** – قدرة الإرهابيين على الإضرار بشبكات المعلومات أو القيام بعمليات ذات آثار مادية من خلال استخدام تكنولوجيا المعلومات والاتصالات منعدمة حاليا، ولو أنه لا يمكن استبعاد إمكانية ظهور مثل هذه القدرات في المستقبل. فمعظم الخبراء متفقون حاليا على أن الإرهابيين يعتمدون على تكنولوجيا المعلومات والاتصالات للتجنيد والتنظيم والتماس التمويل. وقد يكون من التهديدات المحددة الناجمة عن استخدام الإرهابيين للإنترنت استخدامها من أجل تنظيم هجمات إرهابية حركية محددة أو تنفيذها.

(د) **الوكلاء** – ومما يثير قلقا متزايدا الأفراد أو المجموعات الذين ينخرطون في أنشطة ضارة على الشبكة بالإنابة عن آخرين، سواء أكانوا من الجهات الفاعلة من الدول أو من غير الدول، من أجل مكاسب مالية أو بدوافع وطنية أو غيرها من الدوافع السياسية. وتقول التقارير أن ما يُسمى بـ ”Bot-masters“، يقدمون مختلف الخدمات الشريرة لمن يدفع أعلى ثمن. وتقدم الخصائص الفريدة التي تتصف بها تكنولوجيا المعلومات درجة عالية من طمس الهوية لهذه الجهات الفاعلة كما أنها تطمس بشكل فعال أي علاقة بالنسبة إلى الراعي، مما يزوّد الراعي بقدرة حسنة على الإنكار.

والتحديات التي تواجه الدول في التصدي لهذه التهديدات هائلة. فالخصائص التي تتصف بها تكنولوجيا المعلومات والاتصالات تعني أن أفعال كل من هذه الجهات الفاعلة المهددة ليس من المحتمل ظهورها للعيان إلا من حيث آثارها. ولذا فإنه لا يمكن تحقيق إسناد الهوية بشكل موثوق للفاعلين في الوقت المناسب، إن كان هذا ممكنا على الإطلاق، وغالبا ما يتوقف النجاح في ذلك على درجة عالية من التعاون عبر الوطني. كما أن في دور الوكلاء المتزايد ما يزيد من تعقيد عملية الإسناد، بالنظر إلى أنه يجب على الطرف المتأثر بهذه الأعمال ألا يحدد هوية الفاعل فحسب بل أيضا هوية الراعي، مما يجعل هذا التحدي أكثر إشكالا في المستقبل.

وهذه التحديات تتطلب من الحكومات الوطنية أن تنظم وتقود الجهود المحلية في سبيل إيجاد ونشر نظم دفاعية قادرة على التحمل من أجل الهياكل الأساسية للمعلومات والاتصالات بغض النظر عن مصدر هذه التهديدات. وفي الوقت ذاته، فإنه طبيعة هذه التهديدات المعقدة عبر الوطنية، تتطلب تعاونا دوليا بشأن وضع استراتيجيات للتصدي لهذه الأخطار على نطاق عالمي.

ثالثا – المبادئ والقواعد ومعايير السلوك

ألف – مسؤوليات الدول في ضمان أمن الفضاء الإلكتروني

أدركت الدول الأعضاء خلال العقد الماضي مسؤوليتها الوطنية عن اتخاذ خطوات محلية منظمة للدفاع عن نفسها إزاء تهديدات أمن الفضاء الإلكتروني كما أكدت الحاجة إلى التعاون الدولي. وقد لفتت الجمعية العامة النظر في خمسة من قراراتها إلى التدابير الدفاعية الأساسية التي يمكن للحكومات أن تتخذها للحد من الأخطار التي تهدد أمنها. ومع أن القصد من هذه القرارات هو التوعية، فهي تقدم مع ذلك بعض المعايير المفيدة بالنسبة لسلوك الأفراد والدول لمصلحة أمن الفضاء الإلكتروني، وهي:

(أ) القرار ٥٥/٦٣ المتعلق بمكافحة الاستعمال الإجرامي لتكنولوجيات المعلومات، الذي تؤكد فيه الجمعية العامة الحاجة إلى قوانين وطنية حديثة فعالة من أجل مقاضاة الجرائم الحاسوبية بشكل كاف وتيسير التنسيق عبر الوطني للتحقيقات في الوقت المناسب؛

(ب) القرار ٥٦/١٢١ الذي تشير فيه الجمعية العامة على وجه التحديد إلى أعمال المنظمات الدولية والإقليمية في مكافحة الجرائم المتعلقة بالتكنولوجيا المتقدمة، بما في ذلك أعمال مجلس أوروبا في صياغة اتفاقية بشأن الجريمة الحاسوبية:

وهناك أنشطة مكثفة تضطلع بها الأمم المتحدة وغيرها من المنظمات في هذا المجال. ومن مؤسسات الأمم المتحدة التي تركز بشكل رئيسي على استعمال الإنترنت لأغراض إجرامية ما يلي: مكتب الأمم المتحدة المعني بالمخدرات والجريمة، واللجنة المعنية بمنع الجريمة والعدالة الجنائية، ومؤتمر الأمم المتحدة المعني بمنع الجريمة والعدالة الجنائية، والاتحاد الدولي للاتصالات السلكية واللاسلكية، وغيرها؛

(ج) القرار ٢٣٩/٥٧، الذي تؤكد فيه الجمعية العامة الحاجة إلى إيجاد ثقافة عالمية لأمن الفضاء الإلكتروني، يعترف بمسؤولية الحكومات عن قيادة جميع عناصر المجتمع لفهم أدوارها ومسؤولياتها فيما يتعلق بأمن الفضاء الإلكتروني، كما يُبرز العناصر التكميلية التي يتوجب على جميع المشاركين في مجتمع المعلومات معالجتها؛

(د) القرار ١٩٩/٥٨، الذي تركّز فيه الجمعية العامة بوجه خاص على الإجراءات التي ينبغي للدول الأعضاء النظر فيها خلال ما تبذله من جهود لإنشاء ثقافة عالمية لأمن الفضاء الإلكتروني وحماية الهياكل الأساسية للمعلومات الحيوية. ويمكن اعتبار هذه أيضا مجموعة من القواعد التي ينبغي للحكومات أن تُنسب إليها، والتي تقدم أساسا جوهريا أو سابقة أساسية لتيسير التعاون الدولي في مجال الحد من الأخطار؛

(هـ) القرار ٢١١/٦٤، الذي تدعو فيه الجمعية العامة جميع الدول إلى النظر بالتفصيل في جهودها المبذولة من أجل أمن الفضاء الإلكتروني الوطني حتى الآن، في المجالات المذكورة أعلاه وأيضا في مجالات أخرى، وذلك باستخدام وسيلة مرفقة للتقييم الذاتي، ومشاطرة التدابير الناجحة وأفضل الممارسات التي يمكن أن تساعد دولا أعضاء أخرى في جهودها المبذولة لهذا الغرض.

باء – المعايير المنطبقة في سياق الأعمال العدائية

على الرغم من الخصائص التي تنفرد بها تكنولوجيا المعلومات والاتصالات، تستخدم مبادئ القانون الدولي القائمة كإطار مناسب يتم فيه تحديد وتحليل قواعد ومعايير السلوك التي ينبغي أن تحكم استخدام الفضاء الإلكتروني فيما يتصل بالأعمال العدائية. وهناك جزءان مستقلان ولكنهما مترابطان من القانون ينبغي النظر فيهما في هذا الصدد: قانون مسوغات الحرب وقانون وقت الحرب. فالأول يتيح إطارا للنظر فيما إذا كان حادث ما في الفضاء الإلكتروني يرقى إلى مستوى استعمال القوة ويثير حق بلد ما في الدفاع عن النفس. أما الثاني فيتيح إطارا لتحديد القواعد التي تحكم استعمال الفضاء الحاسوبي في سياق النزاع المسلح.

قانون مسوغات الحرب: يستمد معظم الإطار القانوني الذي يحكم استعمال القوة والدفاع عن النفس من ثلاثة أحكام واردة في الميثاق:

(أ) تنص المادة ٢ (٤) من الميثاق على أن ''يمتنع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة ...''؛

(ب) تنص المادة ٣٩ من الميثاق على أن مجلس الأمن هو الذي يقرر ما إذا كان قد وقع تهديد للسلم أو إخلال به أو كان ما وقع عملاً من أعمال العدوان، وتكلفه بتقديم توصيات بشأن ما يجب اتخاذه من التدابير طبقاً لأحكام المادتين ٤١ و٤٢ من الميثاق استجابة لذلك؛

(ج) تقر المادة ٥١ من الميثاق وتعزز المبدأ الذي مفاده أنه ''ليس في هذا الميثاق ما يضعف أو ينتقص الحق الطبيعي للدول، فرادى أو جماعات، في الدفاع عن نفسها إذا اعتدت قوة مسلحة على أحد أعضاء الأمم المتحدة، وذلك إلى أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدوليين''.

ولعل من الصعب التوصل إلى استنتاج قانوني بشأن ما إذا كان نشاط من الأنشطة المسببة للخلل في الفضاء الإلكتروني يشكل هجوما مسلحا يثير الحق في الدفاع عن النفس. فعلى سبيل المثال، عندما يكون عامل التهديد ودافعه مجهولين و لم تؤد نتيجة الآثار مباشرة إلى موت واقعي أو دمار مادي، فقد يكون من الممكن التوصل إلى استنتاجات متباينة بشأن ما إذا كان قد وقع هجوم مسلح. غير أن هذا الغموض وهذا المجال للخلاف لا يدلان على الحاجة إلى إطار قانوني محدد للفضاء الإلكتروني، بل إنما يعكسان التحديات القائمة في العديد من السياقات في تطبيق إطار الميثاق. إلا أن من الممكن، في ظل بعض الظروف، أن يشكل النشاط المسبب للخلل في الفضاء الحاسوبي هجوما مسلحا. وفي هذا السياق، تنطبق المبادئ التالية المعمول بها :

(أ) ينطبق الحق في الدفاع عن النفس ضد هجوم مسلح وشيك أو فعلي سواء كان المهاجم جهة تابعة لدولة أو جهة من غير الدول؛

(ب) يجب أن يقتصر استعمال القوة في الدفاع عن النفس على ما هو ضروري للتصدي لهجوم مسلح وشيك أو فعلي ويجب أن يكون متناسبا مع التهديد الذي تواجهه الدولة؛

(ج) يتعين على الدول أن تتخذ جميع ما يلزم من تدابير لكيلا تستخدم دول أخرى أو جهات أخرى من غير الدول أراضيها لأغراض الاضطلاع بأنشطة مسلحة، بما فيها التخطيط للهجمات المسلحة أو التهديد بها أو التحضير لها أو توفير دعم مادي لها، ضد الدول الأخرى أو ضد مصالحها.

قانون وقت الحرب: يحدد قانون النزاعات المسلحة القواعد، المعروفة بقانون وقت الحرب التي تنطبق على إدارة النزاع المسلح، بما في ذلك استخدام أدوات تكنولوجيا المعلومات في سياق النزاع المسلح. وعلى وجه الخصوص، ستؤدي المبادئ الرئيسية التالية لقانون النزاعات المسلحة دورا مهما في البت في شرعية هجمات الفضاء الإلكتروني أثناء النزاع المسلح:

(أ) يقتضي مبدأ التمييز أن تقتصر الهجمات على الأهداف العسكرية الشرعية وألا تستهدف الأهداف المدنية؛

(ب) يشمل حظر الهجمات العشوائية حظر الهجمات التي تستخدم وسائل أو أساليب حرب ليس من المعقول أن توجه إلى هدف عسكري محدد؛

(ج) يحظر مبدأ التناسب الهجمات التي يتوقع أن تسبب خسائر عرضية في أرواح المدنيين أو إصابة المدنيين أو إلحاق ضرر بالأهداف المدنية قد يكون مفرطا مقارنة بالمكاسب العسكرية الفعلية أو المباشرة المتوقعة.

وتحظر هذه المبادئ شن الهجمات على الهياكل الأساسية المدنية البحتة التي قد لا يعود تعطيلها أو تدميرها بأي مكاسب عسكرية تذكر. إضافة إلى ذلك، يجب تقييم الأضرار الجانبية المحتملة قبل شن هجمات على الأهداف العسكرية. وبعبارة أخرى، يجب إجراء تحليل للأهداف بالنسبة لهجمات تكنولوجيا المعلومات على النحو الذي أجري فيه بالنسبة للهجمات التي تستخدم فيها أسلحة حركية (تقليدية أو استراتيجية).

ولئن كانت المبادئ الواردة أعلاه راسخة ومطبقة في سياق الفضاء الإلكتروني، فمن الصحيح أيضا أن تفسير هاتين الكتلتين من القانون في سياق أنشطة الفضاء الإلكتروني يمكن أن يشكل تحديات جديدة وفريدة تتطلب التشاور والتعاون بين البلدان. وليس ذلك أمرا غير عادي. فعندما يتم استحداث تكنولوجيات جديدة، فغالبا ما تشكل تحديات أمام تطبيق مجموعات القوانين السارية.

جيم – استخدام الوسائل غير المباشرة

يشكل استخدام الوسائل غير المباشرة لإجراء عمليات مسببة للخلل مثالا لمجال تشكل فيه الخصائص الفريدة لتكنولوجيا المعلومات تحديات جديدة للدول. والتصرف عن طريق الوسائل غير المباشرة يزيد بشكل كبير قدرة الدول على الشروع في الهجمات التي تشن مع إنكار مقبول. ومع أن القانون الدولي الساري يتضمن أحكاما تحكم استخدام المرتزقة، فإن استخدام الوسائل غير المباشرة يثير قضايا جديدة وهامة ذات تداعيات واسعة النطاق. وسيتعين على الدول أن تعمل معا لإيجاد حلول لهذه المشكلة.

دال – المسؤولية عن السماح بحرية تدفق المعلومات

لقد تكرس الحق في حرية التعبير والحق في حرية تدفق المعلومات في الإعلان العالمي لحقوق الإنسان وفي العهد الدولي للحقوق المدنية والسياسية اللذين ينصان عموما، مع مراعاة بعض القيود، على أن لكل شخص الحق في التمتع بحرية التعبير، ويشمل هذا الحق حريته في اعتناق الآراء دون مضايقة وفي التماس الأنباء وتلقيها ونقلها إلى الآخرين، بأية وسيلة ودون اعتبار للحدود. وجرى تأكيد هذه المبادئ في العديد من المحافل الدولية، بما فيها الجمعية العامة والاتحاد الدولي للاتصالات ومؤتمر القمة العالمية لمجتمع المعلومات، من بين محافل أخرى.

هاء – المسؤولية عن مكافحة الإرهاب

يدعو ١٦ قرارا على الأقل من قرارات مجلس الأمن الدول إلى مكافحة الإرهاب. وتنطبق هذه الالتزامات تماما عندما يستخدم الإرهابيون أو منظمو العمليات الإرهابية الفضاء الحاسوبي للتجنيد أو جمع الأموال أو نقلها أو حيازة الأسلحة أو تخطيط الهجمات. ويلزم على جميع الدول أن تتبادل المعلومات عن الأنشطة الجارية على الإنترنت لتمويل الإرهاب والتجنيد له وتخطيطه وتيسيره، وتتخذ تدابير لمكافحة هذه الأنشطة، مع احترام سيادة الدول الأخرى ومسؤولياتها الخاصة للسماح بحرية تدفق المعلومات.

خامسا – الشفافية والاستقرار والحد من المخاطر والتدابير التعاونية

على النحو المبين أعلاه، تواجه الدول الأعضاء التحدي المتمثل في إدارة بيئة أخطار مختلفة ومعقدة بدرجة كبيرة. فقد بذلت جهود مكثفة على الصعيد الدولي، خلال العقد الماضي، لمكافحة خطر جرائم الفضاء الإلكتروني. وبذلت جهود للتدريب في مجال التحقيق في جرائم الفضاء الإلكتروني ومقاضاتها في منظمة الدول الأمريكية ومنتدى التعاون الاقتصادي لآسيا والمحيط الهادئ والجماعة الاقتصادية لدول غرب أفريقيا والاتحاد الأفريقي

ومجلس أوروبا، من بين كيانات أخرى. وتم تحقيق تعاون دولي واسع النطاق في مجال التحقيق في جرائم الفضاء الإلكتروني ومقاضاتها عن طريق اتفاقية الجرائم الإلكترونية ومن خلال الجهود الثنائية بين البلدان المتأثرة بهذه الجرائم، وما زال هذا التعاون يشكل أنجع وسيلة للتعامل مع الخطر الذي يتهدد تكنولوجيا المعلومات من جراء الأنشطة الإجرامية.

ولم تحظ بعد مجالات أخرى مثيرة للقلق عبر الحدود بعناية مماثلة. ومن هذه المجالات خطر التصورات الخاطئة الناجمة عن عدم التفاهم فيما يتعلق بالمعايير الدولية المتصلة بسلوك الدول في الفضاء الإلكتروني التي يمكن أن تؤثر على إدارة الأزمات في حالة وقوع حوادث هامة في الفضاء الإلكتروني. ويؤيد ذلك فكرة اتخاذ تدابير رامية إلى تعزيز التعاون أو بناء الثقة أو الحد من المخاطر أو تعزيز الشفافية والاستقرار:

تدابير تحقيق الشفافية

- تبادل الاستراتيجيات وأفضل الممارسات الوطنية المتعلقة بأمن الفضاء الإلكتروني (الدروس المستفادة)
- تبادل الآراء الوطنية بشأن المعايير الدولية التي تحكم استخدام الفضاء الإلكتروني
- تبادل الهياكل التنظيمية الوطنية المخصصة لأمن الفضاء الإلكتروني ونقاط الاتصال

تدابير تحقيق الاستقرار والحد من المخاطر

- وضع أو ترقية خطوط الاتصالات وما يرتبط بها من بروتوكولات لتشمل حوادث الفضاء الإلكتروني
- تعزيز التعاون من أجل التصدي للجهات المنظمة من غير الدول (المجرمون والإرهابيون والوسائل غير المباشرة)
- وضع إجراءات لتمكين تبادل المعلومات بشكل روتيني بين أفرقة الاستجابة لحوادث الأمن الإلكتروني.

التدابير التعاونية

- دعم بناء القدرات في مجال أمن الفضاء الإلكتروني في الدول الأقل نمواً.