الأمم المتحدة

A/68/156

الجمعية العامة

Distr.: General
16 July 2013
Arabic
Original: English/Russian/Spanish

الدورة الثامنة والستون

البند ٩٤ من القائمة الأولية*

التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي

التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي

تقرير الأمين العام

المحتويات

* A/68/50.

120813 120813 13-39733 (A)

أولا – مقدمة

١ – في ٣ كانون الأول/ديسمبر ٢٠١٢، اعتمدت الجمعية العامة القرار ٢٧/٦٧ المعنون ”التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي“. وفي الفقرة ٣ من القرار، دعت الجمعية العامة جميع الدول الأعضاء إلى أن تواصل موافاة الأمين العام بآرائها وتقييماتها بشأن المسائل التالية، آخذة في اعتبارها التقييمات والتوصيات الواردة في تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي (A/65/201):

(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 هذا القرار؛

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

٢ – استجابة لذلك الطلب، أُرسلت في ٢٢ شباط/فبراير ٢٠١٣ مذكرة شفوية إلى الدول الأعضاء تدعوها إلى تقديم معلومات عن الموضوع. وترد في الفرع الثاني أدناه الردود التي تم تلقيها. وأي ردود أخرى يتم تلقيها ستصدر في شكل إضافات لهذا التقرير.

ثانيا – الردود الواردة من الحكومات

كوبا

[الأصل: بالإسبانية]
[٢٠ أيار/مايو ٢٠١٣]

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

وتشاطر كوبا تماما القلق الذي أعربت عنه الجمعية العامة في القرار ٢٧/٦٧ بخصوص استخدام تكنولوجيات المعلومات ووسائل الاتصالات السلكية واللاسلكية التي قد

تؤثر على الاستقرار والأمن الدوليين والسلامة الإقليمية للدول، مما يقوِّض أمنها في المجالين المدني والعسكري. ويشدد هذا القرار أيضا على النحو الواجب على ضرورة منع استخدام موارد المعلومات وتكنولوجياتها في أغراض إجرامية أو إرهابية.

وفي هذا الصدد، تكرر كوبا إدانتها لما تقوم به الإدارات المتعاقبة للولايات المتحدة الأمريكية من تصعيد عدواني لحربها الإذاعية والتليفزيونية ضد كوبا مما ينتهك المعايير الدولية السارية التي تحكم المجال اللاسلكي. ويُشَن هذا العدوان دون مراعاة الأضرار التي قد تلحق بالسلام والأمن الدوليين من جراء خلق أوضاع خطيرة، من قبيل استخدام طائرة عسكرية لبث إشارات تليفزيونية باتجاه كوبا دون موافقتها.

ويشكل البث من الطائرات انتهاكا للفقرة الفرعية ٤ من المادة ٤٢ من أنظمة الاتصالات اللاسلكية للاتحاد الدولي للاتصالات، التي تحظر تشغيل محطة للبث الإذاعي محمولة على طائرة تعمل في البحر أو فوق البحر.

وفي عام ٢٠١٢، قامت الولايات المتحدة بـ ١٩٢ رحلة جوية أجرت خلالها عمليات بث لاسلكي غير مشروع على موجات التضمين الترددي بالتزامن مع بث غير مشروع لإشارات تلفزيونية من الطائرات إلى الأراضي الكوبية. وأدت هذه الأعمال إلى التشويش على المحطات التلفزيونية في كوبا، وهي مسجلة في السجل الرئيسي الدولي للترددات التابع للاتحاد الدولي للاتصالات.

وتقوم كل أسبوع محطات بث تقع في أراضي الولايات المتحدة ببث ٤٠٠ ٢ ساعة في المتوسط من الإرسال الإذاعي والتلفزيوني غير المشروع على ٣٠ موجة مختلفة من الموجات التليفزيونية وموجات التضمين الترددي اللاسلكية متوسطة المدى وقصيرة المدى. والعديد من محطات البث هذه مملوك لمنظمات ترتبط بعناصر إرهابية معروفة تعيش في كوبا وتعمل ضدها انطلاقا من أراضي الولايات المتحدة، أو تقدِّم خدمات لتلك المنظمات، وهي تبث برامج تحرض فيها على التخريب، والقيام بهجمات سياسية واغتيالات، وغير ذلك من أشكال الإرهاب الإذاعي.

وتهدف عمليات البث الإذاعي والتلفزيوني غير المشروعة ضد كوبا إلى تشجيع الهجرة غير المشروعة والتشجيع والتحريض على العنف، وازدراء النظام الدستوري وارتكاب الأعمال الإرهابية. وتكرر كوبا التأكيد على أن استخدام المعلومات من أجل هدف واضح يتمثل في تقويض النظام الداخلي للدول الأخرى، وانتهاك سيادتها والتدخل في شؤونها الداخلية يشكل عملا غير قانوني.

ويشكل بث هذه البرامج الاستفزازية ضد كوبا انتهاكا للقواعد الدولية التي تنظم استخدام الاتصالات اللاسلكية الإلكترونية، وترد هذه القواعد في الاتفاقية الدولية للاتصالات اللاسلكية، التي وقعت عليها حكومة الولايات المتحدة بوصفها طرفا فيها.

وأيدت كوبا قرار الجمعية العامة ٢٤/٦٦ وستواصل الإسهام في التطوير السلمي لتكنولوجيات المعلومات والاتصالات في العالم واستخدامها لما فيه خير البشرية جمعاء.

إسبانيا

[الأصل: بالإسبانية]
[٢٩ أيار/مايو ٢٠١٣]

١ - مقدمة

أمن المعلومات هو جانب رئيسي من جوانب مجتمع المعلومات. وقد أدّت التطورات التكنولوجية إلى تحقيق زيادة متواصلة ومتسارعة في القدرات المتعلقة بتجهيز المعلومات وتخزينها في أشكال متعددة. ومن جهة أخرى، شهد مجال الاتصالات زيادة كبيرة جدا في عرض النطاق المتاح. ويترتب على ذلك إمكانية إرسال وتلقي كميات ضخمة من المعلومات حاليا بشكل آني تقريبا ودون الحاجة إلى هياكل أساسية غاية في التعقيد.

وبينما تساهم هذه التطورات التكنولوجية في تحسين فرص الوصول إلى المعلومات بمختلف أنواعها، فإنها تسهل أيضا إمكانية استخدام تلك المعلومات والوصول إليها لأغراض غير قانونية، ولا سيما استخدام نظم تكنولوجيا المعلومات والاتصالات السلكية واللاسلكية لأغراض عدائية أو إجرامية، بل ولارتكاب أعمال إرهابية أو عدوانية بين الدول أو الجهات الفاعلة عبر الحدود الوطنية.

وقد تأكد في السنوات الأخيرة تنامي الاتجاه نحو استخدام المنظمات الإجرامية والجماعات الإرهابية بوجه خاص للإنترنت. وتستغل هذه المنظمات والجماعات أساسا اثنتين من خصائص الشبكة وهما طابعها العالمي وما تتيحه من ضمانات كبيرة بشأن سرية الهوية.

ونتيجة لذلك، لا بد من تحقيق توازن بين تطوير مجتمع المعلومات وتكنولوجيا المعلومات من جهة، والعمل من جهة أخرى، وبموازاة مع ذلك، على تطوير نظم قانونية وطنية ودولية مستكملة ومحدثة تواكب البيئة التكنولوجية الجديدة وتستطيع التصدي للتحديات التي تطرحها ضرورة حماية المعلومات من أجل منع استخدامها بصورة غير مشروعة دون المساس بحقوق وحريات الأشخاص.

٢ - إساءة استعمال الإنترنت لأغراض إرهابية

تتمثل حاليا التهديدات الرئيسية الناجمة عن استخدام المنظمات الإرهابية لشبكة الإنترنت فيما يلي:

(أ) استخدام الإنترنت كسلاح، أي استخدامها كوسيلة لشن هجمات ضد نظم المعلومات المتعلقة بالهياكل الأساسية الحيوية أو ضد الهياكل الأساسية للإنترنت نفسها. وتعتبر مثل هذه الهجمات التي يرتكبها أشخاص عاديون متواترة نسبيا، بيد أن الهجوم الذي تعرضت له إستونيا في عام ٢٠٠٧ كشف أن الهياكل الأساسية المعلوماتية لدولة ما يمكن أن تتأثر أيضا بهجوم من هذا النوع. ومن العوامل المرتبطة مباشرة بهذا النوع من التهديد الزيادة الكبيرة في عدد البرامجيات الحاسوبية الجديدة الضارة التي ظهرت في السنوات الأخيرة وشبكات الروبوت (البوتنت) (botnets) أو شبكات الحواسيب الشريرة (zombies) التي تستخدم لشن هجمات ضد نظم المعلومات.

(ب) استخدام الإنترنت باعتبارها وسيلة لتنظيم أنشطة أخرى ولا سيما منها ما يلي:

- أنشطة الاتصال - لقد أصبحت المنظمات الإجرامية تلجأ أكثر فأكثر إلى استخدم الشبكة في اتصالاتها بدلا من الوسائل الأخرى من قبيل الهواتف الثابتة أو المحمولة. وأكثر الأدوات استخداما للاتصال عبر الإنترنت بشكل آمن ودون الكشف عن الهوية هي البريد الإلكتروني وبرامج تبادل الرسائل الآنية ومنتديات الإنترنت.
- بث الدعاية والمواد المتعلقة بالأنشطة الإرهابية - توجد في الوقت الراهن آلاف المواقع الشبكية التي تحرض على العنف أو ترتبط بأنشطة إرهابية، وهو اتجاه ما فتئ يتزايد نتيجة ظهور الشبكة العالمية، الجيل ٢,٠ وشبكات التواصل الاجتماعي (المدونات). ويعتبر منع المنظمات الإرهابية من استخدام الشبكة العالمية لهذه الأغراض مسألة على قدر كبير من التعقيد نظرا لسهولة ترحيل هذه المواقع. وهذه الظاهرة تتجاوز حدود الدول، ذلك لأن الخادوم الذي يستضيف الموقع الشبكي قد يكون موجودا في بلد مغاير للبلد الذي يُدار منه بينما قد تكون المنظمة الإرهابية المعنية تعمل في بلد ثالث. وإذا لم تكن هناك اتفاقات ثنائية مبرمة بين هذه البلدان، ينشأ فراغ قانوني.
- التجنيد - تستخدم الإنترنت في بعض الأحيان كوسيلة لتنفيذ أنشطة التجنيد، ولا سيما من خلال المنتديات الإلكترونية وبرامج تبادل الرسائل الآنية.

- التمويل – تتيح الإنترنت أيضا فرصا تضطلع المنظمات الإرهابية من خلالها بأنشطة بهدف الحصول على التمويل. ومن المثير للاهتمام بشكل خاص أنه بإمكان المنظمات الإرهابية أن تشارك في ارتكاب عمليات احتيال وابتزاز وغسل أموال عبر الإنترنت كوسيلة للحصول على التمويل.
- نشر أدلة التدريب – تستخدم المنظمات الإرهابية شبكة الإنترنت لنشر أدلة تتناول تقنيات إرهابية وطرائق صنع المتفجرات و مناولة الأسلحة.
- جمع المعلومات بغرض شن هجمات إرهابية – شكل الإنترنت مصدرا هاما للغاية للمعلومات التي كثيرا ما تستخدمها المنظمات الإرهابية للحصول على بيانات بشأن أهداف أنشطتها، سواء كانت هذه الأهداف أفرادا أو منظمات أوهياكل أساسية.

٣ – التدابير المتخذة على الصعيد الوطني من أجل مكافحة استخدام المنظمات الإرهابية للإنترنت

٣-١ التدابير التشريعية

من جملة التدابير التي تتخذها مختلف الدول، الجهود الكبيرة التي بذلتها إسبانيا في السنوات الأخيرة، وبخاصة في عام ٢٠٠٧. وقد أدرجت في نظامها القانوني سلسلة من القوانين التي تتناول أمن المعلومات وحرية ممارسة الحقوق والحريات المعترف بها في الإعلان العالمي لحقوق الإنسان وفي الدستور الإسباني. ووضعت تشريعات وأنظمة شاملة وضمنتها الجوانب الوطنية البحتة والتوجيهات الواردة من الاتحاد الأوروبي بهدف تحقيق هذين الهدفين. وتطبيق معايير جديدة في مجال أمن المعلومات تنص على أن توفير درجة معقولة من الحماية للمعلومات، فضلا عن الحفاظ على سريتها، أصبح يقتضي في معظم الحالات الحفاظ على سلامتها وتوافرها. وتجدر الإشارة بوجه خاص إلى سن القوانين واللوائح التالية:

- القانون التنظيمي رقم ١٩٩٢/٥ المؤرخ ٢٩ تشرين الأول/أكتوبر ١٩٩٢ بشأن تنظيم التجهيز الآلي للبيانات الشخصية، الرامي إلى وضع آليات للحماية تحول دون انتهاك الخصوصية في سياق تجهيز المعلومات؛ ولوائحه التطبيقية.
- القانون التنظيمي رقم ١٥/١٩٩٩ المؤرخ ١٣ كانون الأول/ديسمبر ١٩٩٩ بشأن حماية البيانات الشخصية، ويهدف إلى ضمان وحماية الحريات العامة والحقوق الأساسية للأفراد، وبخاصة شرفهم وخصوصياتهم الشخصية والأسرية؛ ولوائحه التطبيقية.

- المرسوم الملكي بقانون رقم ١٤/٩١٩٩ المؤرخ ١٧ أيلول/سبتمبر ١٩٩٩ بشأن التوقيع الإلكتروني، الرامي إلى تشجيع الشركات والمواطنين والإدارات العامة على التعجيل بإدماج التكنولوجيا الجديدة في مجال أمن الاتصالات الإلكترونية وإلى نقل التوجيه رقم 1999/93/EC الصادر عن البرلمان الأوروبي والمجلس الأوروبي في ١٣ كانون الأول/ديسمبر ١٩٩٩بشأن وضع إطار للجماعة الأوروبية يتعلق بالتوقيعات الإلكترونية إلى القانون العام الإسباني. ويستكمل القانون رقم ٥٩/٣٢٠٠ المؤرخ ١٩ كانون الأول/ديسمبر ٢٠٠٣ بشأن التوقيع الإلكتروني هذا التوجيه الإطاري من خلال إدخال تعديلات عليه تعتبر مستصوبة في ضوء التجربة المتراكمة منذ دخوله حيز النفاذ.

- القانون رقم ١١/٢٢٠٠ المؤرخ ٦ أيار/مايو ٢٠٠٢ المنظم للمركز الوطني للاستخبارات، والمرسوم الملكي رقم ٤٢١/٤٢٠٠ المؤرخ ١٢ آذار/مارس ٢٠٠٤ المنظم للمركز الوطني للتشفي اللذان يسندان إلى المركز الوطني للاستخبارات مهاما تشمل تنسيق الإجراءات التي تتخذها مختلف الأجهزة الحكومية التي تستخدم أساليب وإجراءات الشفرة، وضمان أمن تكنولوجيا المعلومات في هذا المجال وكفالة الامتثال للأنظمة القانونية المتعلقة بحماية المعلومات السرية.

- القانون رقم ٣٤/٢٢٠٠ المؤرخ ١١ تموز/يوليه ٢٠٠٢ بشأن خدمات مجتمع المعلومات والتجارة الإلكترونية. ويهدف إلى تضمين النظام القانوني الإسباني التوجيه رقم 2000/31/EC المؤرخ ٨ حزيران/يونيه ٢٠٠٠ المتعلق بجوانب قانونية معينة من خدمات مجتمع المعلومات، وبخاصة التجارة الإلكترونية في السوق الداخلية (التوجيه بشأن التجارة الإلكترونية). ويتضمن هذا القانون أيضا جزءا من التوجيه رقم EC98/27/ الصادر عن البرلمان الأوروبي والمجلس الأوروبي في ١٩ أيار/مايو ١٩٩٨ بشأن الأوامر المتعلقة بحماية مصالح المستهلكين نظرا لأنه ينظم، وفقا لأحكام ذلك التوجيه، أوامر مكافحة السلوك المخل بأحكام هذا القانون.

- القانون العام المتعلق بالاتصالات السلكية واللاسلكية رقم ٣٢/٣٢٠٠ المؤرخ ١٣ تشرين الثاني/نوفمبر ٢٠٠٣ المنظم لتشغيل الشبكات وتقديم الخدمات في مجال الاتصالات الإلكترونية.

- القانون رقم ٥٩/٣٢٠٠ المؤرخ ١٩ كانون الأول/ديسمبر ٢٠٠٣ بشأن التوقيع الإلكتروني المشار إليه أعلاه.

- القانون رقم ٧٢٠٠/١١ المؤرخ ٢٢ حزيران/يونيه ٢٠٠٧ بشأن وصول المواطنين إلى الخدمات الإلكترونية العامة، الذي ينظم الاتصال بين المواطنين والإدارات العامة باستخدام التقنيات والأساليب الإلكترونية والمعلوماتية واللاسلكية.

- القانون التنظيمي رقم ٧٢٠٠/١٠ المؤرخ ٨ تشرين الأول/أكتوبر ٢٠٠٧ الذي ينظم قاعدة بيانات الشرطة المتعلقة بمحددات الهوية المستخلصة من الحمض النووي الريبي المترع الأوكسجين، الذي ينشئ قاعدة بيانات تدمج فيها، بشكل منفرد، ملفات الوكالات الحكومية المعنية بأمن الدولة وإنفاذ القانون التي تتضمن بيانات تحديد الهوية المستمدة من تحليلات الحمض النووي الريبي المترع الأوكسجين التي تُجرى في إطار التحقيق الجنائي أو في سياق إجراءات تحديد هوية الجثث أو التحقيق بشأن الأشخاص المختفين.

- القانون رقم ٧٢٠٠/٢٥ المؤرخ ١٨ تشرين الأول/أكتوبر ٢٠٠٧ بشأن حفظ البيانات المتعلقة بالاتصالات الإلكترونية والشبكات العامة للاتصالات، الذي يؤثر تأثيرا إيجابيا في التحقيقات الجارية في هذا المجال.

- المرسوم الملكي رقم ٢٠٠٧/١٧٢٠ المؤرخ ٢١ كانون الأول/ديسمبر ٢٠٠٧ المصدق على اللوائح التطبيقية للقانون التنظيمي رقم ٩١٩٩/١٥ المؤرخ ١٣ كانون الأول/ديسمبر ١٩٩٩ بشأن حماية البيانات الشخصية.

- القانون رقم ٧٢٠٠/٥٦ المؤرخ ٢٨ كانون الأول/ديسمبر ٢٠٠٧ بشأن تدابير تعزيز مجتمع المعلومات.

- تجريم الأعمال الإلكترونية التالية المرتبطة بنشاط المنظمات الإرهابية في شبكة الإنترنت:

  - عمليات التخريب الحاسوبي، المادة ٢٦٤ من القانون الجنائي

  - التهديدات، المادة ١٦٩ وما يليها من القانون الجنائي

  - تبرير الإرهاب وتمجيده، المادة ٥٧٨ من القانون الجنائي

٣-٢ تدابير أخرى

- إنشاء أفرقة للشرطة مختصة في مكافحة استخدام المجموعات الإجرامية للإنترنت.

- المشاركة في مشروع ”مراقبة شبكة الإنترنت“ الذي وضعه مكتب الشرطة الأوروبي (يوروبول).

- يقدم المركز الوطني للتشفير التابع للمركز الوطني للاستخبارات مساهمة يومية كبيرة في الجهود الرامية إلى مكافحة الهجمات الإلكترونية. وعلى وجه الخصوص، يملك فريق التصدي للطوارئ الحاسوبية التابع للمركز الوطني للتشفير القدرة على الاستجابة لحوادث أمن المعلومات. وأنشئ الفريق في أوائل عام ٢٠٠٧ بوصفه هيئة حكومية إسبانية ويشارك في المحافل الدولية الرئيسية، حيث يتبادل الأهداف والأفكار والمعلومات بشأن أمن الفضاء الإلكتروني.

- إنشاء المركز الوطني لحماية الهياكل الأساسية الحيوية تتخذ وزارة الدفاع عدة خطوات في مجال الدفاع عن الفضاء الإلكتروني وتشارك من خلال رؤساء أركان الدفاع في مركز الامتياز المعني بالدفاع الحاسوبي التعاوني التابع لمنظمة حلف شمال الأطلسي، الذي ما فتئت إسبانيا تساعد في تمويله منذ إنشائه، وتزوده باثنين من الخبراء. ويتضح الدور متزايد الأهمية الذي يضطلع به المركز في الجهود الدولية الرامية إلى مكافحة الإرهاب الإلكتروني من خلال الزيارة التي قام بها مؤخرا جلالة الملك، وأكد خلالها على التزام إسبانيا بالمبادرات الدولية المتعلقة بأمن الفضاء الإلكتروني.

- وتقوم منظمة حلف شمال الأطلسي بدور فعال للغاية في أنشطة الدفاع عن الفضاء الإلكتروني؛ وقد وضعت مفهوما واعتمدت سياسة، وعينت هيئة لإدارة الدفاع عن الفضاء الإلكتروني لخدمة التحالف.

- وأنشأت منظمة الأمن والتعاون في أوروبا فريق عامل غير رسمي معني بتدابير بناء الثقة المتصلة بتكنولوجيا المعلومات والاتصالات. ويتمثل هدف الفريق العامل في الحد من احتمال الهجمات الإلكترونية، وتعزيز الأمن المشترك في الوقت نفسه من خلال التعاون الدولي وتعزيز الوضوح والشفافية والحد من مخاطر التصورات الخاطئة التي يمكن أن تؤدي إلى تصعيد النزعات من خلال وضع تدابير بناء الثقة السياسية والعسكرية المتعلقة باستخدام تكنولوجيات المعلومات والاتصالات.

- وتحدد خطة الأمن الوطني سياسة أمنية وطنية لاستخدام وسائط الإعلام الإلكترونية. وتستند الخطة إلى مبادئ أساسية وحد أدنى من المتطلبات التي توفر الحماية الكافية للمعلومات، وتشارك جميع الإدارات الحكومية في أعمالها. ويستند الأساس القانوني لها إلى مرسوم ملكي سيصدر قريبا بموجب المادة ٤٢ من القانون رقم ٧٢٠٠/١١. وتحدد الاستراتيجية الأمنية لإسبانيا التهديدات والمخاطر الأمنية الرئيسية وتضع خطة للتصدي لها، وتنص على أن الفضاء الإلكتروني هو أحد المجالات التي ينبغي اتخاذ

إجراءات بشأنها. ويشكل هذا التحليل أساسا لوضع استراتيجيات التصدي لتلك المخاطر، وبناء القدرات وتنفيذ الإصلاحات الإدارية.

ويتضمن توجيه الدفاع الوطني لعام ٢٠١٢ قائمة بالتهديدات العالمية التي يجب على إسبانيا التصدي لها مشيرا إلى أن الهجمات الإلكترونية هي أحد المخاطر الرئيسية ولا يمكن منعها إلا من خلال تحالف ن للقوات يستند، في حالة إسبانيا، إلى منظمة حلف شمال الأطلسي والاتحاد الأوروبي، ولكنه سيحتاج أيضا إلى دعم البلدان ومجموعات البلدان الأخرى التي لها مصلحة مباشرة أيضا في رصد هذه المسائل.

ويدعو هذا التوجيه أيضا إلى المشاركة في تعزيز الإدارة الشاملة لأمن الفضاء الإلكتروني في إطار المبادئ ذات الصلة للاستراتيجية الوطنية لأمن الفضاء الإلكتروني.

ويشير أيضا التوجيه المتعلق بسياسات الدفاع، الذي اعتمد في عام ٢٠١٢ إلى بروز الفضاء الإلكتروني كمجال جديد في العلاقات الدولية، ويعتبر تعزيز نظم جمع المعلومات والاستخبارات أولوية دفاعية من أجل دعم عمليات، مثل نظم القيادة والتحكم، وذلك بهدف الحد من خطر الهجمات الإلكترونية.

وفي كانون الثاني/يناير ٢٠١١، أصدر رئيس هيئات أركان الدفاع رؤية بشأن الدفاع العسكري عن الفضاء الإلكتروني، تتضمن توجيهات تتعلق بالتخطيط، والتطوير واستخدام القدرات العسكرية اللازمة من أجل كفالة فعالية استخدام الفضاء الإلكتروني أثناء العمليات العسكرية.

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

أدّت زيادة الاعتماد على نظم المعلومات وزيادة الترابط بين الهياكل الأساسية إلى جعل أمن الفضاء الإلكتروني أمرا حيويا لأداء الدولة الحديثة لوظائفها. ولهذا السبب، ينبغي أن يكون أمن الفضاء الإلكتروني جزءا لا يتجزأ من تخطيط الأمن الوطني.

ولا تتوفر في الوقت الحاضر حماية لإطار قانوني دولي لمواجهة العوامل المهددة لأمن الفضاء الإلكتروني. لذلك، ينبغي التوصل، دون المساس بسيادة الدول في المسائل المتصلة بأمن الفضاء الإلكتروني، إلى توقيع اتفاقات تعاون متعددة الأطراف في هذا المجال (مماثلة للاتفاقية الدولية لسلامة الأرواح في البحار، أو مشابهة لها) تتعهد الدول بموجبها بمواءمة تشريعاتها لضمان محاكمة مرتكبي الجرائم المرتبطة بشبكة الإنترنت، والسعي قدر الإمكان إلى

كفالة الحيلولة دون تحويل الشبكة، في ظل ما تتيحه من سرية الهوية وغياب للتشريعات ومن مصالح اقتصادية، إلى أرضية خصبة للجريمة والإرهاب.

ويتعين إشراك القطاع الخاص، ولا سيما مقدمو خدمات الإنترنت، في الجهود الرامية إلى مكافحة الجريمة الإلكترونية. ويكتسي تعاون القطاع الخاص أهمية أساسية بالنظر إلى تحكم شركات القطاع الخاص في معظم الخدمات المعروضة على الإنترنت. وقد تصدى القطاع الخاص لفترة طويلة للتهديدات ذات الصلة بالإنترنت ويمكن أن تكون معارفه وتجاربه ذات قيمة كبيرة في هذا المجال.

وتؤدي أفرقة التصدي للطوارئ الحاسوبية دورا رئيسيا في أمن الفضاء الإلكتروني. ويعتبر إنشاء الأفرقة المتخصصة وتدريب أعضائها باستمرار أول خطوتين ينبغي أن تتخذهما الحكومات لضمان أمن الفضاء الإلكتروني. ومن المهم أيضا إنشاء وحدات لإنفاذ القانون متخصصة في التحقيق في الجرائم المرتكبة عن طريق شبكة الإنترنت.

ونظرا لأن أمن الفضاء الإلكتروني يمثل تحديا عالميا فمن الضروري تعزيز التعاون الدولي من أجل تحسينه على الصعيدين السياساتي والتنفيذي. وينبغي أن تكون هناك اتصالات مستمرة بين أفرقة التصدي للطوارئ الحاسوبية في مختلف البلدان من أجل تيسير تبادل المعلومات عن الهجمات في غضون مدّة استجابة قصيرة. وينبغي أيضا تبادل الدروس المستفادة وأفضل الممارسات الوطنية والدولية.

وتشمل التدابير الأخرى:

- تدريب المواطنين وتوعيتهم، في سن مبكرة، بالحاجة إلى إيلاء الاهتمام لأمن نظم المعلومات التي يستخدمونها. ويستفيد مرتكبو العديد من أنواع جرائم الفضاء الإلكتروني من تقاعس العديد من مستعملي شبكة الإنترنت عن اتخاذ الاحتياطات اللازمة (أو ربما يعولون على ذلك) لجعل حواسيبهم وحساباتهم في مأمن وغير قابلة للاختراق قدر الإمكان. ولذلك، من المهم تثقيف المستعملين. ومن شأن زيادة الوعي بهذه المشكلة أن تقلل من عدد الحواسيب التي يستخدمها مجرمو الفضاء الإلكتروني من أجل القيام بأنشطتهم، لا سيما تلك المتعلقة بشبكات الروبوط (بوت نت).
- التعجيل بوضع إجراءات التعاون الدولي والتعاون في مجال الشرطة لكي تتسنى محاكمة مرتكبي الأعمال الجنائية بسرعة وفعالية، في ضوء الطابع المشتت للإنترنت وتقلب سجلات الربط بالإنترنت، والإطار القانوني لكل بلد.

- تنظيم منتديات وحلقات دراسية ومؤتمرات متعددة الجنسيات من أجل تعزيز معرفة الخبراء وتبادل المعارف بشأن مختلف أنواع الهجمات والاتجاهات الجديدة في مجال هجمات الفضاء الحاسوبي، وتقييم مواطن الضعف وأثر الهجمات المحتملة، وتبادل الدروس المستفادة وأفضل الممارسات وتشجيع عقد دورات تدريبية موحدة للشرطة في مجال التحقيق في جرائم الفضاء الإلكتروني.
- تنسيق جهود المنظمات المتخصصة في مجالات محددة لأمن الفضاء الإلكتروني، مثل مجلس أوروبا ومنظمة حلف شمال الأطلسي، من أجل تجنب ازدواجية في الجهود لا داعي لها.
- إصدار الأدلة وتسجيل الممارسات الجيدة، بالتعاون مع القطاع الخاص والمجتمع المدني، من أجل تحسين أمن الفضاء الإلكتروني.

وختاما، ترى إسبانيا أنه ينبغي أن يتخذ المجتمع الدولي التدابير التي يرتئيها مناسبة لحماية المعلومات انطلاقا من رؤية عالمية موحدة، وأن يعمل إن أمكن على إنشاء هيئة موحدة تحدد قواعد ومعايير مشتركة لجميع البلدان وتضع مجموعة متوازنة وشاملة من التدابير المحددة في مجال الحماية وتسمح بمواءمة السياسات والإجراءات التي تتبعها مختلف المنظمات الوطنية والدولية المعنية.

أوكرانيا

[الأصل: بالروسية]
[٣١ أيار/مايو ٢٠١٣]

١ - تقييم عام لمشاكل أمن المعلومات

تحظى مجالات أمن المعلومات، وأمن الاتصالات والتصدي لجرائم الفضاء الإلكتروني بمكانة مركزية في الأمن الوطني لأوكرانيا. ويعزز الأمن الوطني لأوكرانيا، بدوره، تقوية الأمن الدولي في عالم معولم.

ويسهم كلٌ من العولمة، وإنشاء مجتمع معلومات، واعتماد تكنولوجيات معلومات جديدة، وهي كلها ظواهر تحدث على الصعيد العالمي، في الأهمية المتزايدة لأمن المعلومات كعنصر من عناصر الأمن الوطني. ويُعرَّف أمن المعلومات بأنه درجة حماية المصالح الوطنية في مجال المعلومات من التهديدات الخارجية والداخلية.

ووفقاً لذلك، يندرج ما يلي كله تحت عنوان التهديدات الدولية لأمن المعلومات:

- الاستخدام غير المشروع لموارد المعلومات؛
- الأنشطة غير المأذون بها والمدمرة داخل النظم الآلية، بما في ذلك تلك النظم المستخدمة في إدارة مرافق الهياكل الأساسية الوطنية الحيوية؛
- استخدام الفضاء الإلكتروني، أو ما يتصل به من أنشطة، أو تكنولوجيات المعلومات ومواردها، بطريقة تنتهك حقوق الإنسان والحريات الأساسية أو بغرض القيام بأعمال إرهابية أو متطرفة أو غيرها من الأعمال الإجرامية، بما في ذلك أعمال العدوان؛
- استخدام الهياكل الأساسية للمعلومات في نشر معلومات تحض على العداء والكراهية، بوجه عام أو في بلد بعينه؛
- نشر معلومات تتعارض مع التشريع الوطني القائم والقواعد والمبادئ الأخلاقية؛
- استخدام الفضاء الإلكتروني في زعزعة استقرار المجتمع وتقويض النظام الاقتصادي والسياسي والاجتماعي لدولة أخرى، أو في نشر معلومات مضللة ترمي إلى تشويه القيم الثقافية والأخلاقية والجمالية؛
- منع الوصول إلى التكنولوجيات المتطورة، وترسيخ التبعية في مجال تكنولوجيا المعلومات من أجل تحقيق مكسب والسيطرة على الفضاء الإلكتروني الأجنبي.

وينبغي إبراز المجالات التالية المنطوية على مشاكل المرتبطة بالعولمة: عمليات التحايل المعلوماتي والنفسي التي تستهدف جماعات أو أفراد؛ والقيود على حصول المستهلكين على الخدمات المعتمدة على تكنولوجيات المعلومات والاتصالات؛ وجرائم الفضاء الإلكتروني.

ويرى الخبراء الأوكرانيون أن العوامل التالية، قد تفضي إلى زيادة احتمال تحقق التهديدات المبينة أعلاه:

- انخفاض مستوى الإلمام بالحاسوب لدى معظم مستخدمي موارد المعلومات وخدمات الفضاء الإلكتروني؛
- الافتقار إلى إطار مفاهيمي دولي مشترك لأمن المعلومات؛
- تنوع النهج المتبعة في التشريعات الوطنية إزاء تدابير حماية المعلومات الرامية إلى إنشاء وتحديث (تحديد) الهياكل الأساسية للمعلومات؛
- تفاوت مستويات الحوسبة وأمن المعلومات من بلد إلى آخر؛

- خطر ربط الموارد المدمرة بنظم المعلومات والاتصالات احتمال عدم تحديد مصادر الأنشطة غير المأذون بها في مجال الفضاء الإلكتروني تحديدا واضحا.

٢ - الجهود الوطنية الرامية إلى تعزيز أمن المعلومات ودعم التعاون الدولي في مجال أمن المعلومات

الهيئات الحكومية الرئيسية المسؤولة عن أمن المعلومات وعناصره هي وزارة الداخلية، وجهاز الأمن، والدائرة الحكومية لاتصالات المتخصصة وحماية المعلومات. وتنخرط هذه الوكالات بنشاط في تنظيم المجالات المختلفة لأمن المعلومات. وتركز بوجه خاص على الإطار التنظيمي والقانوني للعنصر المتعلق بالفضاء الإلكتروني (أمن الفضاء الإلكتروني).

وتنفذ أوكرانيا حاليا الأحكام التشريعية التالية بشأن العلاقات الاجتماعية في المسائل المتعلقة بأمن المعلومات.

وتنص المادة ١٧ من الدستور الأوكراني على أن أمن المعلومات وظيفة حيوية للدولة، إلى جانب حماية السيادة وسلامة الأراضي والحفاظ على الأمن الاقتصادي.

وطبقا للمادة ٣ من قانون المعلومات الأوكراني، تشكل كفالة أمن المعلومات في أوكرانيا إحدى المجالات الرئيسية لسياسة الدولة بشأن المعلومات.

وضمن النظام الأمني لأوكرانيا ككل، يحتل أمن المعلومات مترلة خاصة، إذ تشكل العلاقات والعمليات المتصلة بالمعلومات أجزاء مكوِّنة لجميع العمليات داخل المجتمع والدولة. وفي هذا السياق، يُعرَّف أمن المعلومات بأنه وضع فضاء (بيئة) المعلومات - الشامل لتكنولوجيات المعلومات، وموارد المعلومات، والعلاقات المتصلة بالمعلومات بين الأطراف الفاعلة ذات الصلة - الذي يضمن تطور واستخدام فضاء المعلومات لصالح الفرد والمجتمع والدولة.

وعلى أساس أولويات الأمن الوطني، المقترنة بالمصالح المتعلقة بالتنمية الاجتماعية، تُحدد الأهداف الرئيسية لأمن المعلومات. وهذه الأهداف هي:

- كفالة السيادة المعلوماتية الوطنية لأوكرانيا مع ازدياد عولمة تدفق المعلومات وتتنافس البلدان الأخرى على التفوق في مجال المعلومات؛
- تهيئة بيئة معلوماتية تدعم التنمية الثقافية والأخلاقية والثقافية للفرد والمجتمع ككل؛
- الحفاظ على موارد المعلومات الخاصة بأوكرانيا عند مستويات كافية لكفالة الأداء والتنمية المستدامين للفرد والمجتمع والدولة؛

- حماية معلومات الأشخاص الطبيعيين والقانونيين والدولة من التهديدات المعلوماتية الخارجية والداخلية، ويشمل ذلك مكافحة الجرائم الحاسوبية؛
- كفالة صحّة حقوق الجهات صاحبة المصلحة في مجال المعلومات في أوكرانيا في إنشاء واستخدام موارد المعلومات الوطنية، وتكنولوجيات المعلومات، والهياكل الأساسية للمعلومات، وإعمال تلك الحقوق.

ولتعزيز أمن المعلومات، يجري تنفيذ إطار تنظيمي وقانوني ونظام للتدريب المهني، ويتم تنسيق أنشطة وكالات الدولة المسؤولة عن أمن المعلومات. ويشمل هذا التنسيق التعاون مع الفريق الأوكراني للتصدي للطوارئ الحاسوبية، ومنتدى أفرقة التصدي للحوادث والأمن، وهي منظمة معتمدة دولية.

وبموجب القانون الأوكراني، يعمل الفريق الأوكراني للتصدي للطوارئ الحاسوبية كجزء من الدائرة الحكومية للاتصالات المتخصصة وحماية المعلومات، التي تنسق عمل الشركات والمؤسسات والمنظمات، بغض النظر عن هيكل الملكية، وذلك من أجل منع الأعمال غير المأذون بها التي تستهدف موارد المعلومات الحكومية في نظم المعلومات والاتصالات وتحليل تلك الأعمال والتصدي لآثارها.

وعلاوة على ذلك، يتعاون الفريق الأوكراني للتصدي للطوارئ الحاسوبية مع الهيئات والمنظمات الأجنبية والدولية ذات الصلة، وتشجع التزامات الفريق إزاء مناظريه الأجانب (العضوية الكاملة في منتدى أفرقة التصدي للحوادث والأمن، والعضوية في الشراكة الدولية متعدِّدة الأطراف لمكافحة تهديدات الفضاء الإلكتروني التي أنشأها الاتحاد الدولي للاتصالات) التعاون الدولي في مجال أمن المعلومات.

وبموجب القانون الأوكراني المتعلق بإدخال تعديلات على قانون أوكرانيا بشأن التصديق على الاتفاقية المتعلقة بالجريمة الحاسوبية، فإن وزارة الداخلية هي الهيئة المأذون لها بإنشاء الشبكة الوطنية العاملة على مدار الساعة الشاملة لجهات الاتصال المعنية بمساعدات الطوارئ للنظم الحاسوبية والتحقيق في البيانات المتعلقة بالجرائم؛ وملاحقة الأفراد المتهمين بارتكاب تلك الجرائم؛ والجمع الإلكتروني للأدلة.

تعمل الوحدة ذات الصلة، التي تدير شبكة التصدي لجرائم الفضاء الإلكتروني على مدار الساعة التابعة لشعبة مكافحة جرائم الفضاء الإلكتروني، داخل وزارة الداخلية، وهي مسؤولة عن تنفيذ الأنشطة والعمليات ذات الصلة، بما في ذلك ما يلي:

- مكافحة توزيع هجمات تعطيل تقديم الخدمة؛

- مكافحة الجرائم المرتكبة باستخدام بطاقات الدفع أو بيانات حساباتها؛
- مكافحة التدخل غير المأذون به في عمليات إنجاز الخدمات المصرفية عن بعد عبر التعامل بين ''المصرف والعميل''؛
- مكافحة نشر المحتوى غير القانوني على الإنترنت (في انتهاك لحقوق التأليف والنشر)؛
- مكافحة نشر المواد الإباحية، بما في ذلك استغلال الأطفال في المواد الإباحية، على الإنترنت؛
- مكافحة جرائم الاتصالات؛
- مكافحة الجرائم المتعلقة بالاتصال غير المأذون به بشبكات إرسال البيانات بالساتل؛
- مكافحة جرائم الغش المالي وغيره من أنواع الغش التي ترتكب على الإنترنت؛
- مكافحة الأفعال الإجرامية وسائر جرائم التجارة الإلكترونية؛
- إدارة عمليات التصدي لجرائم الفضاء الإلكتروني التي تقوم بها شبكة جهات الاتصال العاملة على مدار الساعة.

وتُبذل حاليا جهود لتحديث التشريعات الوطنية لأمن المعلومات من أجل إعداد إطار تنظيمي وقانوني متوافق مع القواعد الدولية.

وتعكف حاليا أوكرانيا على إعداد مشروع قانون بشأن أمن الفضاء الإلكتروني، وذلك وفقا للمرسوم الرئاسي رقم ١١١٩ المؤرخ ١٠ كانون الأول/ديسمبر ٢٠١٠ بشأن قرار مجلس الأمن والدفاع الوطني الأوكراني المؤرخ ١٧ تشرين الثاني/نوفمبر ٢٠١٠ المتعلق بالتحديات والتهديدات في مجال الأمن الوطني لأوكرانيا في عام ٢٠١١.

وفيما يلي المجالات السياسات الوطنية التي قد تلقى عناية أكبر بموجب الصكوك التنظيمية والقانونية القائمة:

(١) ترد الأهداف التالية في كلٍ من: المرسوم الرئاسي رقم ١١٩٩ المؤرخ ١٠ كانون الأول/ديسمبر ٢٠١٠ بشأن قرار مجلس الأمن والدفاع الوطني الأوكراني المؤرخ ١٧ تشرين الثاني/نوفمبر ٢٠١٠ المتعلق بالتحديات والتهديدات في مجال الأمن الوطني لأوكرانيا في عام ٢٠١١ (الفقرة ٤)؛ والمرسوم الرئاسي رقم ٣٨٨ المؤرخ ٨ حزيران/يونيه ٢٠١٢ بشأن قرار مجلس الأمن والدفاع الوطني المؤرخ ٢٥ أيار/مايو ٢٠١٢، المتعلق بأنشطة تعزيز مكافحة الإرهاب في أوكرانيا (الفقرة ١)؛ والمرسوم الرئاسي رقم

٣٨٩ المؤرخ ٨ حزيران/يونيه ٢٠١٢ بشأن قرار مجلس الأمن والدفاع الوطني المؤرخ ٨ حزيران/يونيه ٢٠١٢ المتعلق باستراتيجية الأمن الوطني المحدَّثة (الفقرات الفرعية ٣-١-١، و ٣-٣ و ٤-٣)؛ والمرسوم الرئاسي رقم ٣٩٠ المؤرخ ٨ حزيران/يونيه ٢٠١٢ بشأن قرار مجلس الأمن والدفاع الوطني المؤرخ ٨ حزيران/يونيه ٢٠١٢ المتعلق بالمفهوم العسكري الأوكراني المحدَّث (الفقرتان الفرعيتان ٧ و ١٩):

- إنشاء نظام وطني لأمن الفضاء الإلكتروني؛
- إنشاء نظام موحد على الصعيد الوطني لمكافحة جرائم الفضاء الإلكتروني؛
- صياغة وإقرار سجل بالمواقع الحيوية للأمن والدفاع الوطنيين التي لها الأولويات في الحماية من هجمات الفضاء الإلكتروني؛
- صياغة مشروع قانون بشأن أمن الفضاء الإلكتروني الوطني وتقديمه للبرلمان؛
- تعريف أمن الفضاء الإلكتروني كأحد التهديدات المركزية للاستقرار الدولي والأمن الوطني الأوكراني؛
- الموافقة، كهدف استراتيجي وكهدف رئيسي من أهداف سياسة الأمن الوطني، على إعداد معايير ونظم تقنية وطنية لاستخدام تكنولوجيات المعلومات والاتصالات ومواءمتها مع المعايير ذات الصلة للدول الأعضاء في الاتحاد الأوروبي؛
- تعريف مصطلح ''الإرهاب الإلكتروني''؛
- إنشاء آلية فعالة في أوكرانيا للتصدي لأحدث التهديدات للأمن الوطني (الظواهر والاتجاهات التي يمكن، في ظل ظروف معينة، أن تهدد المصالح الوطنية) المتعلقة باستخدام تكنولوجيا المعلومات في عالم معولم، لا سيما ''تهديدات الفضاء الإلكتروني''؛
- تحليل هجمات الفضاء الإلكتروني التي تستهدف مرافق الصناعة النووية والكيميائية، والمرافق العسكرية - الصناعية، وغيرها من المواقع التي تشكل خطرا محتملا، في استعراض للقوة العسكرية ضد أوكرانيا من شأنه أن يفضي إلى نشوب نزاع عسكري؛

(٢) اللوائح والقوانين التنظيمية لمجلس الوزراء: الأمر رقم 720-r المؤرخ ٢٢ آب/أغسطس ٢٠١٢ بالموافقة على البرنامج الوطني السنوي للتعاون بين أوكرانيا ومنظمة حلف شمال الأطلسي لعام ٢٠١٢، وكذلك التوجيه رقم ١٢-١/١/٢٤٠٦٦

المؤرخ ١٥ حزيران/يونيه ٢٠١٢ الصادر بموجب القرار سالف الذكر لمجلس الأمن والدفاع الوطني المنفذ بموجب والمرسوم الرئاسي رقم ٣٨٨ المؤرخ ٨ حزيران/يونيه ٢٠١٢ الذي نص أيضا على إعداد قانون تشريعي بشأن أمن الفضاء الإلكتروني؛

(٣) ينظر برلمان أوكرانيا في مشاريع قوانين لتعديل بعض الصكوك المتعلقة بأمن الفضاء الإلكتروني الوطني. وتنص مشاريع القوانين هذه، في جملة أمور، على استخدام التشريع الوطني لمفاهيم مثل ''أمن الفضاء الإلكتروني للدولة''، و ''مواقع الهياكل الأساسية الحيوية''، و ''مواقع الهياكل الأساسية الحيوية للمعلومات''، و ''الفضاء الإلكتروني''، كما تنص على تعريف تهديدات الأمن الوطني الرئيسية المتعلقة بالفضاء الإلكتروني، والمجالات الرئيسية لسياسة الدولة، ومهام الكيانات المسؤولة عن الأمن الوطني في هذا المجال.

٣ - اعتماد أطر دولية لتعزيز أمن نظم المعلومات والاتصالات العالمية

تمتلك أوكرانيا إطارا تنظيميا وقانونيا لحماية المعلومات في نظم المعلومات والاتصالات تتواءم مبادؤه ونهجه المتعلقة بالحماية مع المعايير المشتركة لتقييم أمن تكنولوجيا المعلومات التي أعدتها المنظمة الدولية لتوحيد المقاييس (١٥٤٠٨).

وبالنظر إلى أن الجرائم الحاسوبية قد تجاوزت الحدود الوطنية وأصبحت ظاهرة دولية، فإن أوكرانيا تتعاون مع الوكالات الأجنبية لإنفاذ القانون بشكل مستمر.

وإضافة إلى ذلك، تعمل أوكرانيا على كفالة أمن المعلومات على الصعيد الدولي في إطار مشاريع وبرامج مع منظمة الأمن والتعاون في أوروبا، والجمعية البرلمانية لمجلس أوروبا، ومجلس أوروبا، وبرنامج الشراكة من أجل السلام الذي تنفذه منظمة حلف شمال الأطلسي، وفي سياق الاتفاقات الثنائية.

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

نظرا للطابع عبر الوطني للجرائم الحاسوبية، قد يكون آن الأوان لصياغة مجموعة من المبادئ الدولية الرامية إلى تقوية أمن شبكات المعلومات والاتصالات والسياسة الأمنية الدولية عموما، وتعزيز سبل ووسائل وموارد الكشف عن تهديدات أمن المعلومات وتقييمها والتنبؤ بها.

ويتعلق أحد المجالات الرئيسية لأمن المعلومات على الصعيد العالمي بصياغة واعتماد صكوك قانونية دولية لحذف المصطلحات غير الدقيقة في مجال أمن المعلومات. وقد يتمثل

جانب هام من ذلك في تحديد المركز القانوني الدولي للفضاء الإلكتروني، وتكريس الولايات القضائية للدول فيما يتعلق بالعناصر الوطنية لهذا الفضاء (على نحو تمكن مقارنته بالمجال الجوي للدول ومياهها الإقليمية) في صكوك تنظيمية وقانونية، وبزيادةتنظيم المسائل المتعلقة بالحرب الإلكترونية والعدوان الإلكتروني.

ويتمثل جانب أساسي آخر لعملية وضع المعايير في هذا المجال في اعتماد مفهوم موحد لجرائم الفضاء الإلكتروني، فضلا عن تصنيف واضح للجرائم ذات الصلة.

وقد تتضمن التدابير الأخرى التي يمكن أن يتخذها المجتمع الدولي من أجل تقوية أمن المعلومات العالمي مواءمة الإطار التنظيمي والقانوني لحماية المعلومات؛ وإعداد معايير وأساليب متفق عليها لتقييم فعالية نظم وموارد أمن المعلومات؛ والاعتراف المتبادل بشهادات أمن المعلومات؛ وتوسيع نطاق التعاون من أجل معالجة المسائل البحثية والتقنية والقانونية المتعلقة بأمن المعلومات. وفي الوقت نفسه، فمن الأهمية بمكان، من أجل كفالة التعاون الناجح، تعزيز التعاون بين وكالات إنفاذ القانون الوطنية بغرض منع الجرائم الحاسوبية وقمعها ومحاكمة مرتكبيها.

المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية

[الأصل: بالإنكليزية]
[١٦ أيار/مايو ٢٠١٣]

ترحب المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية بالفرصة المتاحة للاستجابة لقرار الجمعية العامة ٦٧/٢٧ المعنون ”التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي“.

التقييم العام لمسائل أمن المعلومات

تستخدم المملكة المتحدة في هذه المذكرة مصطلحها المفضل ”أمن الفضاء الإلكتروني“ والمفاهيم ذات الصلة، مع الإشارة إلى الجهود الرامية إلى الحفاظ على سرية المعلومات وتوافرها ونزاهتها في الفضاء الإلكتروني. وكثيراً ما تستخدم المؤسسات التجارية ومنظمات توحيد المقاييس عبارة ”أمن المعلومات“ لتقصد بها الأمر ذاته، كما أن المملكة المتحدة تقبل العبارة بهذا المعنى المحدد. وهناك مجال لاحتمال حدوث خلط في استخدام عبارة ”أمن المعلومات“، حيث تستخدمها بعض البلدان والمنظمات في إطار مفهوم يعتبر المعلومات في حد ذاتها تهديداً ينبغي توفير المزيد من الحماية منه. ولا تعترف المملكة المتحدة

بصحة عبارة ''أمن المعلومات'' عندما تستخدم في هذا السياق، ذلك لأنه يمكن استخدامها في محاولات لإضفاء المزيد من الشرعية على الضوابط المفروضة على حرية التعبير بخلاف تلك المتفق عليها في الإعلان العالمي لحقوق الإنسان والعهد الدولي الخاص بالحقوق المدنية والسياسية.

وليس الفضاء الإلكتروني مجال الفرص الكبيرة فحسب، بل يشكل أيضاً مصدر تهديدات فعلية ومحتملة. فقد بات هناك ما يزيد عن مليوني شخص يرتبطون الآن بالفضاء الإلكتروني عن طريق الإنترنت، ومن المتوقع أن يتواصل ارتفاع هذا العدد مع استفادة البلدان النامية من الفوائد الجمة التي تتيحها تكنولوجيا الأجهزة المحمولة الأقل تكلفة. وتوفر شبكة الإنترنت محركاً للنمو الاقتصادي وتتيح إمكانية الحصول على التعليم؛ وتعزز التفاعل والتفاهم بين البشر وتزيل الحواجز الثقافية والجغرافية وتسمح بتقديم الخدمات إلكترونياً وتعزز الديمقراطية من خلال مساءلة الحكومات أمام مواطنيها بطرق حديثة وديناميية. فعلى سبيل المثال:

- تسهم الإنترنت بنسبة ثمانية في المائة في الناتج المحلي الإجمالي للمملكة المتحدة. ومن العوامل الحيوية لضمان النمو الاقتصادي أن يشعر أصحاب مؤسسات الأعمال التجارية والزبائن بالأمان عند القيام بنشاطهم في الفضاء الإلكتروني.
- بدأت المملكة المتحدة العمل بخدمة العريضة الإلكترونية في عام ٢٠١١، فسمحت بذلك لكل فرد بأن يفتتح أو يوقع على عريضة بشأن أي مسألة تقع مسؤوليتها على عاتق الحكومة. و يُنظر في جميع العرائض التي يوقع عليها ١٠٠ ٠٠٠ شخص أو أكثر لتناقش في البرلمان. وفي العام الأول، افتتح ما يزيد عن ٦٠٠ ١٥ عريضة تجاوزت ١٠ منها عتبة المائة ألف توقيع. وجميع هذه العرائض إما ناقشها البرلمان أو قرر موعدا لمناقشتها.

و تعتمد المملكة المتحدة، شأنها شأن بلدان عديدة، على الفضاء الإلكتروني في مجالات عديدة من الخدمات الوطنية البالغة الأهمية. ومن المحتمل أن يؤدي تعطل تقديم هذه الخدمات على نطاق واسع، سواء كان ذلك بصورة عرضية أم ناشئ عن اختراق متعمد، إلى ارتباك شديد وأضرار اقتصادية وخسائر في الأرواح.

ويتخذ هذا التهديد مظاهر معقدة وديناميية. إذ تتعرض يومياً نظم حكومة المملكة المتحدة إلى جانب نظم مؤسسات الأعمال التجارية والأفراد لمحاولات اختراق. وتختلف الدوافع بين التجسس السياسي والصناعي والجريمة الإلكترونية وتعطيل الشبكات أو التحكم فيها، أو منع تقديم الخدمة. وتشمل الجهات الفاعلة مصدر التهديد الدول القومية والجهات

العاملة بالوكالة عن الدول والجهات الفاعلة من غير الدول والعصابات الإجرامية المنظمة والأفراد الانتهازيين. ونظرا لترابط الفضاء الإلكتروني فإن الأنشطة التخريبية التي تنفذ ضد أحد الأنظمة يمكن أن تحدث آثاراً غير مقصودة وغير متوقعة في النظم الأخرى. وتواجه محاولات التصدي لهذه التهديدات صعوبة في تحديد مصدر أي حادث إلكتروني بصورة موثوقة، واحتمال أن يتنكر مرتكبو ذلك الفعل كغيرهم، والفهم غير الناضج لسلوك الدولة المقبول في الفضاء الإلكتروني، وعدم قدرة الفضاء الإلكتروني في بعض البلدان على مواجهة العمل التخريبي، والافتقار إلى نهج دولية متسقة للتعرف على مجرمي الفضاء الإلكتروني وملاحقتهم ومحاكمتهم.

وينبغي لجميع مكونات المجتمع، بل ومن واجبها، أن تضطلع بدورها في مواجهة هذه التهديدات. وعلى الحكومات أن تقود الجهود الدولية الرامية إلى تحسين التفاهمات بشأن التصرف المقبول للدول وفي التصدي للجريمة الإلكترونية، ولكنه نظرا لأن غالبية الهياكل الأساسية للفضاء الإلكتروني تملكها وتديرها شركات خاصة، فإن مشاركتها في هذه المناقشة تكتسي أهمية حاسمة. وتعتقد المملكة المتحدة أن تحسين الأمن الإلكتروني يجب ألا يكون على حساب المنافع الاقتصادية والاجتماعية التي يأتي بها الفضاء الإلكتروني. ومن المهم تحديداً ضمان عدم إساءة توظيف الجهود المبذولة لتحسين الأمن الإلكتروني لفرض قيود إضافية على حرية التعبير تتجاوز تلك التي تجيزها الاتفاقات الدولية. وفي هذا الصدد، يكتسي دور منظمات المجتمع المدني أهمية خاصة.

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

النهج الوطنية

عرّفت استراتيجية المملكة المتحدة للأمن القومي التي صدرت في عام ٢٠١٠ الهجمات الإلكترونية بأنها واحدة من أربعة تهديدات من ”المستوى ١“، إلى جانب الأزمات العسكرية الدولية والحوادث الكبرى أو الأخطار الطبيعية، والهجمات الإرهابية. وفي تشرين الثاني/نوفمبر ٢٠١١، أصدرت المملكة المتحدة استراتيجية مستكملة للأمن الإلكتروني تحدد رؤية هدفها ”تحقيق قيمة اقتصادية واجتماعية كبيرة من فضاء إلكتروني مرن وآمن ومفعم بالحياة، تعزز فيه أعمالنا التي نسترشد فيها بقيمنا الأساسية، قيم الحرية والإنصاف والشفافية وسيادة القانون، الرخاء والأمن القومي وبناء مجتمع قوي“. ويدعم تحقيق هذه الاستراتيجية أربعة أهداف هي:

- التصدي للجريمة الإلكترونية وجعل الفضاء الإلكتروني أحد أكثر أماكن العالم أمناً لمزاولة الأعمال التجارية في الفضاء الإلكتروني؛
- زيادة القدرة على التصدي للهجمات الإلكترونية وحماية مصالحنا في الفضاء الإلكتروني بشكل أفضل؛
- المساعدة في بناء فضاء إلكتروني مفتوح ومستقر ومفعم بالنشاط يستطيع الجمهور في المملكة المتحدة أن يستخدمه بأمان، ويدعم المجتمعات المفتوحة؛
- توفير المعرفة والمهارات والقدرات الشاملة التي يحتاجها لتعزيز جميع أهدافنا المتعلقة بالأمن الإلكتروني.

ولدعم تحقيق هذه الأهداف، خصصت حكومة المملكة المتحدة مبلغاً قدره ٦٥٠ مليون جنيه إسترليني من النفقات الإضافية لاستخدامه في برنامج مدته أربع سنوات يهدف إلى تغيير أساليب التصدي للتهديدات الإلكترونية.

واستثمرت المملكة المتحدة في قدرات جديدة وفريدة لحماية شبكاتها وخدماتها الأساسية وتعميق فهمها للتهديد الذي تواجهه. وقد عزز ذلك بدوره المعارف التي تمكنها بشكل أفضل من توجيه الجهود الدفاعية وإعطاءها الأولوية. وأنشأت تحت إشراف وزارة الدفاع وحدة مشتركة بين القوات البرية والبحرية والجوية لوضع أساليب وتقنيات وخطط جديدة لاستخدام القدرات العسكرية في التصدي للتهديدات المعقدة. وتعمل الحكومة على نحو وثيق مع ضحايا الأنشطة الإلكترونية التخريبية وتقدم، استنادا إلى نتائج هذا العمل بإسداء المشورة إلى هذا القطاع ليحسن التدابير التي يتخذها في مجال الأمن الإلكتروني. وفيما يتعلق بشبكاتها الخاصة، فهي تعكف على صياغة نموذج أمني جديد لتبادل الخدمات يشمل التثبت بمزيد من الدقة من صحة البيانات المتعلقة بالموظفين وتحسين ضبط الامتثال وتعزيز قدرة الشبكة على التصدي للأنشطة التخريبية.

واستثمرت حكومة المملكة المتحدة في تعزيز عملية إنفاذ القوانين وقدرات المدعين العامين لمنع الجرائم الإلكترونية والتحقيق فيها والحيلولة دون تنفيذها وتقديم المسؤولين عنها إلى العدالة. وقد تضاعف حجم وحدة الجرائم الإلكترونية المركزية التابعة للشرطة ثلاث مرات، وأنشئت ثلاثة أفرقة شرطة إقليمية لمراقبة الجريمة الإلكترونية، وصُمّمت برامج لتدريب ضباط الشرطة الرئيسيين على مكافحة الجريمة الإلكترونية. وستدمج الوكالة المعنية بالجرائم المنظمة الخطيرة مع وحدة الجرائم الإلكترونية المركزية التابعة للشرطة في مرحلة لاحقة من عام ٢٠١٣ لتشكل وحدة الجريمة الإلكترونية الوطنية التابعة لوكالة الجريمة

الوطنية، التي تعد خطة أخرى تهدف إلى تحسين قدرات المملكة المتحدة على إنفاذ قوانين مكافحة الجريمة الإلكترونية.

والصناعة في المملكة المتحدة هي أولى ضحايا الجريمة الإلكترونية، بما في ذلك انتشار سرقة الملكية الفكرية. وتعمل الحكومة مع القطاع الصناعي والأوساط الأكاديمية على تعزيز الوعي بضرورة التصدي للتهديدات الإلكترونية، وقد وضعت في عام ٢٠١٢ وثيقة إرشادية للرؤساء التنفيذيين في قطاع الصناعة تحدد الطريقة التي ينبغي أن يتبعها كبار المسؤولين التنفيذيين لاعتماد استراتيجيات لحماية أثمن ما بحوزتهم من معلومات. كما أنجزت الحكومة بنجاح مبادرة رائدة توفر بيئة موثوقة للمؤسسات لكي تتبادل المعلومات عن التهديدات الراهنة وإدارة الحوادث. وقد شمل ذلك نحو ١٦٠ شركة في قطاعات الدفاع والمالية والأدوية والطاقة والاتصالات السلكية واللاسلكية.

وفي إطار الصناعة، ما فتئت حكومة المملكة المتحدة تقوم بالتوعية بالخطر الذي تتوجسه الصناعة والجمهور، ليتخذوا خطوات غالبا ما تكون بسيطة لحماية أنفسهم ويطالبوا بتوفير مستوى أفضل من الأمن في مجال المنتجات والخدمات الإلكترونية. وقد شملت هذه المبادرات ”أسبوع كن في أمان من المخاطر الإلكترونية“ (بمشاركة الاتحاد الأوروبي وكندا)؛ وحملات موجهة بشأن الاحتيال الإلكتروني نظمها كل من الهيئة الوطنية لمكافحة الاحتيال؛ وحملة ”Devils in Your Details“ في عام ٢٠١٢.

وتستثمر المملكة المتحدة في المهارات والبحوث لكي تتوفر لدينا القدرة على مواكبة هذه المشكلة في المستقبل. وقد منحت أول ثماني جامعات في المملكة المتحدة تعد بحوثا في مجال الأمن الإلكتروني لقب ”المركز الأكاديمي للتفوق في بحوث الأمن الإلكتروني“. ويجري وضع مواد تعليمية تفاعلية للطلاب الشباب، وقد أطلقت خطة للتلمذة التقنية هدفها تحديد وتطوير المواهب لدى طلاب المدارس والجامعات. ولضمان حصول العاملين في مجال الأمن الإلكتروني على الحق في التعليم والتدريب، ستساعد المصادقة على خطة تأمين المعلومات للمهنيين الحكومة وقطاع الصناعة على استقدام مهنيين مختصين في الأمن الإلكتروني ممن لديهم المهارات اللازمة والمستوى المطلوب لشغل الوظائف المناسبة.

النهج الدولية

تتبوأ المملكة المتحدة مركز الصدارة في الجهود الدولية المبذولة لتحسين شفافية الفضاء الإلكتروني واستقراره وإمكانية التنبؤ به. وفي تشرين الثاني/نوفمبر ٢٠١١، استضافت المملكة المتحدة المؤتمر الدولي الأول بشأن الفضاء الإلكتروني، الذي جمع معاً شارك فيه ممثلون مما يزيد عن ٦٠ بلداً آتين من ينتمون لمؤسسات تجارية ومنظمات من

المجتمع المدني لمناقشة السبل الكفيلة بتوسيع نطاق المنافع الاقتصادية والاجتماعية للفضاء الإلكتروني؛ والتعاون بشأن التصدي للجريمة الإلكترونية والاستخدام الآمن والموثوق للإنترنت؛ والأمن الدولي. وقد انتقل الزخم الذي تولد عن هذا المؤتمر إلى مؤتمر بودابست الذي عقد في عام ٢٠١٢، ويجري بالفعل التخطيط لمؤتمر عام ٢٠١٣ الذي سيعقد في سول.

والمملكة المتحدة هي عضو نشط في فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وكذلك في الفريق العامل غير الرسمي التابع لمنظمة الأمن والتعاون في أوروبا المعني بوضع تدابير بناء الثقة في مجال الفضاء الإلكتروني.

وفي تشرين الأول/أكتوبر ٢٠١٢، أعلنت المملكة المتحدة مبادرة ترمي إلى إنشاء مركز لبناء القدرات في مجال الأمن الإلكتروني العالمي بتمويل قدره مليوني جنيه إسترليني في السنة، تشمل مبادرات مختلف ثنائية ومتعددة الأطراف. وسيقدم هذا المركز خدمات المشورة والخبرة المستقلة للبلدان الأخرى بشأن طريقة بناء هياكل أساسية وطنية أكثر أمناً ومقاومة، وسيصبح مركزا لتنسيق البحوث العالمية والتعاون الدولي بشأن هذه المسالة الحيوية.

ولمواصلة تعزيز الجهود الدولية الرامية إلى التصدي للجريمة الإلكترونية الدولية، ما فتئت المملكة المتحدة تروج لاتفاقية بودابست بشأن الجرائم الإلكترونية و مبادئها، وذلك باعتبارها أكثر الصكوك فعالية في هذا المجال. وما زالت وكالة المملكة المتحدة لمكافحة الجرائم المنظمة الخطيرة تضطلع بدور رائد مع الشركاء الدوليين في تقديم صورة شاملة عن قضايا إنفاذ القانون إلى شركة الإنترنت للأسماء والأرقام المخصصة.

المفاهيم الدولية ذات الصلة التي تهدف إلى تعزيز أمن النظم العالمية للمعلومات والاتصالات السلكية واللاسلكية

يتعلق المفهوم الأول بتطبيق أحكام القانون الدولي ومعايير السلوك الحالية الناظمة للعلاقات بين الدول وفيما بينها. وتعتقد المملكة المتحدة اعتقاداً راسخاً بأن هذه المبادئ تطبق بنفس القدر من الصرامة على الفضاء الإلكتروني، وأن أي تأكيد صريح من الدول بأن هذه القوانين والقواعد هي التي ستنظم أنشطتها في الفضاء الإلكتروني من شأنه أن يضع الأسس اللازمة لإنشاء فضاء إلكتروني أكثر سلاماً وأمناً وقابلية للتنبؤ.

وفي هذا الصدد، يطرح الفضاء الإلكتروني تحديات خاصة مثل الصعوبات في التوزيع الموثوق للأنشطة وتقييم النوايا ودور الجهات الفاعلة من غير الدول. وسترحب المملكة المتحدة بالمناقشات الدولية بشأن طريقة تطبيق القوانين والقواعد الدولية التي تحكم تصرف الدولة في هذا السياق.

ولا تعتقد المملكة المتحدة بأن المساعي الرامية إلى إبرام معاهدات شاملة متعددة الأطراف أو وضع مدونة للسلوك أو أية صكوك مشابهة من شأنها أن تقدم مساهمة إيجابية لتعزيز الأمن الإلكتروني في المستقبل المنظور. ونظرا للطابع المعقد والشامل لأي اتفاق ملزم يغطي كامل الفضاء الإلكتروني الذي يتطور بسرعة فائقة فأنه لا يمكن أن يكون فعالاً أو يحظى بدعم واسع النطاق إلا بعد سنوات عديدة، إن لم تكن عقوداً، من العمل الدؤوب بشأن وضع قواعد للسلوك وتدابير بناء الثقة من أجل تحقيق التفاهم والثقة الضروريين بين الجهات الموقعة، وضمان إمكانية مساءلتها بطريقة موثوقة عن مدى تقيدها بالتزاماتها. وتدل التجربة في إبرام هذه الاتفاقات المتعلقة بشأن المواضيع الأخرى على أنها لا يمكن أن تكون هادفة وفعالة إلا إذا كانت ثمرة مساع دبلوماسية ترمي إلى وضع تفاهمات ونهج مشتركة، ليس بوصفها نقطة انطلاق لها. وتعتقد المملكة المتحدة أنه ينبغي تركيز جهود المجتمع الدولي على وضع تفاهمات مشتركة بشأن القانون الدولي والمعايير الدولية، عوضاً عن التفاوض بشأن صكوك ملزمة لن تؤدي إلا إلى فرض جزئي وسابق لأوانه لنهج إزاء ميدان لم يبلغ حالياً مرحلة النضج الكافي لدعمه.

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

يفرض طابع الفضاء الإلكتروني الذي لا حدود له واجباً محدداً على الدول بأن تعزز التعاون الثنائي والإقليمي والمتعدد الأطراف لإيجاد سبل مشتركة للتصدي للتهديدات

المشتركة. وترى المملكة المتحدة، أن التدابير التي يمكن أن تقدم أكبر مساهمة في هذه المرحلة هي:

(أ) عقد مناقشات مستمرة فيما بين الدول لوضع إطار معياري لتصرف الدولة المقبول، يقوم على مبادئ القانون الدولي وقواعد القانون العرفي المعمول بها؛

(ب) وضع تدابير لبناء الثقة خاصة بالفضاء الإلكتروني ترمي إلى زيادة شفافية تصرف الدولة وقابلية التنبؤ به، ومن ثم الحد من احتمال وضع تصور خاطئ للأحداث أو تصعيدها بطريقة غير مقصودة؛

(ج) إنشاء الدول لأفرقة تتصدى للطوارئ الحاسوبية تركز على التعامل مع الحوادث وتبادل المعلومات، يزود بإخطارات مراكز الاتصال الرئيسية وآليات الاتصالات الموثوقة في وقت الأزمات؛

(د) وضع تمارين مشتركة لاختبار الإجراءات المشتركة في مجال التعامل مع الحوادث والاتصالات؛

(هـ) وضع نهج قانونية متسقة للتصدي للجريمة الإلكترونية؛

(و) تعزيز الحوار مع ممثلي مؤسسات الأعمال التجارية والمجتمع المدني لضمان تطبيق نهج منسقة ومرتبة حسب الأولوية في ميدان يمتلكه القطاع الخاص ويتولى إدارته إلى حد كبير.

(ز) تعهد الدول التي لديها قدرات أكثر تطوراً من غيرها في مجال الأمن الإلكتروني بدعم بناء قدرات دول أخرى.