الأمم المتحدة

A/74/120

الجمعية العامة

Distr.: General
24 June 2019
Arabic
Original: English/French/Spanish

الدورة الرابعة والسبعون

البند ٩٥ من القائمة الأولية*

التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي

تقرير الأمين العام

المحتويات

الصفحة

أولا – مقدمة ٢

ثانيا – الردود الواردة من الحكومات ٣

الأرجنتين ٣

كولومبيا ٧

كوبا ١٢

مصر ١٤

فرنسا ١٨

اليونان ٣٠

اليابان ٣٢

سنغافورة ٣٨

تركيا ٤٠

* A/74/50.

010819 250719 19-10580 (A)

الرجاء إعادة استعمال الورق

أولا – مقدمة

١ – اتخذت الجمعية العامة في دورتها الثالثة والسبعين قرارين في إطار البند ٩٦ من جدول الأعمال بشأن التطورات الحاصلة في مجال المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي.

٢ – وفي ٥ كانون الأول/ديسمبر ٢٠١٨، اتخذت الجمعية العامة القرار ٢٧/٧٣ بشأن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وفي ٢٢ كانون الأول/ديسمبر، اتخذت القرار ٢٦٦/٧٣ بشأن الارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي.

٣ – وفي الفقرة ٤ من القرار ٢٧/٧٣، دعت الجمعية العامة جميع الدول الأعضاء إلى أن تواصل، آخذة في اعتبارها التقييمات والتوصيات الواردة في التقرير الصادر عن فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، موافاة الأمين العام بآرائها وتقييماتها بشأن المسائل التالية:

(أ) التقييم العام لمسائل أمن المعلومات؛

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

(ج) مضمون المفاهيم المذكورة في الفقرة ٣ من القرار؛

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

٤ – وفي الفقرة ٢ من القرار ٢٦٦/٧٣، دعت الجمعية العامة جميع الدول الأعضاء إلى أن تواصل، آخذة في اعتبارها التقييمات والتوصيات الواردة في تقارير فريق الخبراء الحكوميين، موافاة الأمين العام بآرائها وتقييماتها بشأن المسألتين التاليتين:

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

(ب) مضمون المفاهيم المشار إليها في تقارير فريق الخبراء الحكوميين.

٥ – واستجابة لذلك الطلب، أُرسلت في ٦ شباط/فبراير ٢٠١٩ مذكرة شفوية إلى جميع الدول الأعضاء لدعوتها إلى تقديم معلومات عن هذا الموضوع. ويتضمن الفرع الثاني الردود التي وردت حتى إعداد هذا التقرير. وستُنشر الردود الإضافية التي وردت بعد ١٥ أيار/مايو ٢٠١٩ في الموقع الشبكي لمكتب شؤون نزع السلاح (www.un.org/disarmament/ict-security) باللغة الأصلية التي وردت بها.

ثانيا – الردود الواردة من الحكومات

الأرجنتين

[الأصل: بالإسبانية]
[١٥ أيار/مايو ٢٠١٩]

التقييم العام لمسائل أمن المعلومات

تتيح تكنولوجيات المعلومات والاتصالات فرصاً حقيقية للتقدم الاقتصادي والاجتماعي والثقافي والعلمي والسياسي، ويرتبط تقدم هذه التقنيات ارتباطاً وثيقاً بمستويات أعلى من التنمية والرفاهية. وقد أصبح الفضاء الإلكتروني عنصراً أساسياً في حياة الأشخاص والمؤسسات، ويعتمد عدد متزايد من الخدمات الأساسية على الشبكات الحاسوبية.

ومع ذلك، وبما أن الفضاء الإلكتروني أتاح مستويات من التفاعل والتقدم لم يسبقها مثيل، فإنه يخضع أيضاً لعدة أخطار ذات طبيعة مختلفة وللجهات الفاعلة التي تعرض أمن الأفراد والشركات والمؤسسات والدول وكذلك السلم والأمن الدوليين للخطر.

وتعتمد التنمية الاقتصادية وتوفير الخدمات الأساسية ورفاهية المواطنين والأداء السليم لوكالات الدولة اعتماداً شديداً على الأمن السيبراني.

وقد بدأت تظهر مخاطر جديد نتيجة لكثرة استخدام الأجهزة الذكية منخفضة التكلفة نسبياً التي تتيح الوصول إلى شبكة الإنترنت دون أدنى مستوى من الأمن، مما يزيد من حيز الهجمات الإلكترونية المحتملة.

ويتطلب هذا النمو مواكبة سياسات الدولة لاستراتيجيات الشركات المسؤولة التي تسمح بمعالجته.

وبالمثل، فإن الخطط التي تدفع بعض الدول إلى استحداث آليات تسمح لها بفك تشفير المعلومات في الأجهزة/التطبيقات و/أو آليات ''الأبواب الخلفية''، تشكل خطراً إضافياً.

الجهود المبذولة على الصعيد الوطني لتعزيز أمن المعلومات

في عام ٢٠١٧، أنشأت الحكومة الأرجنتينية بموجب المرسوم ٢٠١٧/٥٧٧ لجنة الأمن السيبراني، برئاسة أمانة شؤون التحديث الحكومية التابعة لرئاسة مجلس الوزراء، التي تشارك فيها أمانة الشؤون الاستراتيجية التابعة لرئاسة مجلس الوزراء، ووزارة الدفاع، ووزارة الأمن، ووزارة الخارجية وشؤون العبادة، ووزارة العدل وحقوق الإنسان. ومن بين وظائف اللجنة المذكورة وضع الاستراتيجية الوطنية للأمن السيبراني وإعداد خطة العمل اللازمة لتنفيذها.

وقد ساعد إنشاء لجنة الأمن السيبراني على إيجاد الفرص لتبادل المعلومات عن الحوادث التي سمحت بتحسين سبل التنسيق في مواجهة الحوادث، الأمر الذي كان فعالا خلال مؤتمر قمة مجموعة العشرين الذي انعقد في الأرجنتين في عام ٢٠١٨.

وللأرجنتين برنامج وطني للبنية التحتية للمعلومات الحيوية والأمن السيبراني، أُنشئ بموجب القرار ٢٠١١/٥٨٠ الصادر عن رئاسة مجلس الوزراء، والهدف منه، من بين أهداف أخرى، هو تحديد

وحماية البنية التحتية الاستراتيجية والحيوية للقطاعين العام والخاص والمؤسسات المشتركة بين الأقاليم، وكذلك إدارة جميع المعلومات المتعلقة بتقارير الحوادث الأمنية وتسخير حلولها الممكنة بطريقة منظمة وموحدة.

وفي هذا الإطار، وُضع بروتوكول لظروف التعرض الشديد لمخاطر الأمن الحاسوبي في أوساط الوكالات العامة، ينص على تغطية القطاع الخاص.

ويجري العمل حالياً على وضع معيار يوافق على تعريف البنى التحتية الحيوية للمعلومات، ومعايير لتحديد مدى أهميتها الحيوية وتصنيفها في مختلف القطاعات.

وفي إطار البرنامج الوطني للبنية التحتية للمعلومات الحيوية والأمن السيبراني، أُنشئ بموجب البند رقم ٢٠١٣/٢ فريق التصدي لحوادث الأمن الحاسوبي.

ومن الناحية التشريعية، أُدرجت الجريمة الإلكترونية في قانون العقوبات في عام ٢٠٠٨ بواسطة القانون 26.388. وفي عام ٢٠١٣، أقر الكونغرس الوطني القانون رقم 26.904، الذي يصنِّف أنماط جريمة إغراء الأطفال عبر الإنترنت لأغراض جنسية (الاستمالة) ويشدِّد العقوبات المفروضة على الجرائم المتعلقة باستغلال الأطفال في المواد الإباحية على شبكة الإنترنت. وفي عام ٢٠١٧، وافق الكونغرس على القانون رقم 27.411 الخاص بالانضمام إلى الاتفاقية المتعلقة بالجريمة الإلكترونية. وفي كانون الثاني/يناير ٢٠١٩، سن الكونغرس القانون 27.482 بشأن تعديل قانون الإجراءات الجنائية الاتحادي، الذي يتضمن وسائل للحصول على الأدلة الرقمية (اعتراض الاتصالات الرقمية وتسجيل وحفظ البيانات والأنظمة الحاسوبية).

والعمل جار حالياً على إعداد مشروع قانون لتعديل القانون الجنائي يأخذ بعين الاعتبار تصنيف العديد من الجرائم الحاسوبية، وخاصة ما يتعلق بتضرر البنى التحتية الحيوية.

ومن أجل تحسين القدرات في مكافحة الجريمة السيبرانية، نظمت وزارة العدل وحقوق الإنسان العديد من حلقات العمل التدريبية للمهنيين العاملين في النظام الجنائي بشأن الجرائم السيبرانية ومعالجة الأدلة الرقمية والأشكال الحديثة للبحث والتحري، إلى جانب منظمات دولية مثل منظمة الدول الأمريكية ومجلس أوروبا. وقد نُظمت حلقات العمل تلك في مناطق مختلفة من البلاد وكانت موجهة للقضاة والمدعين العامين وأفراد قوات الأمن على المستوى الاتحادي ومستوى الأقاليم. ومنذ عام ٢٠١٦ حتى اليوم، استفاد من هذه البرامج التدريبية حوالي ٥٠٠ قاضٍ ومدع عام من جميع أنحاء البلاد.

ومن ناحية أخرى، من بين الأهداف المتوخاة من برنامج العمل الرقمي للأرجنتين، الذي أُقر بموجب المرسوم ٢٠١٨/٩٩٦، تنمية المهارات في مجال الأمن السيبراني لبث الثقة في أوساط التكنولوجيا الرقمية. وفي هذا الصدد، ومن أجل تعزيز القدرات للتوعية/للتعريف بالمخاطر في استخدام الشبكات الاجتماعية والإنترنت، مع التركيز بوجه خاص على السكان بشكل عام وعلى المجموعات المعرّضة للمخاطر، استُحدثت برامج لتدريب المدرِّبين بالتنسيق مع برنامج Programa Punto Digital. وتم فيها تناول مواضيع مثل التسلط عبر الإنترنت، والاستمالة، واستراق الهوية الرقمية، والأمن السيبراني، واستراتيجيات لمساعدة و/أو احتواء الضحايا و/أو للوقاية من جرائم الإنترنت وكشفها، مع التركيز على الشباب والمراهقين وكبار السن.

وفي ما يتعلق بحماية البيانات الشخصية، كانت الأرجنتين من أوائل البلدان في المنطقة التي أنشأت إطاراً تنظيمياً لحماية البيانات الشخصية، من خلال سن القانون 25.326. وقد انضمت إلى اتفاقية مجلس أوروبا لحماية الأفراد في ما يتعلق بالمعالجة الآلية للبيانات الشخصية.

واعتباراً من ١ حزيران/يونيه ٢٠١٩، سيبدأ في جمهورية الأرجنتين سريان اتفاقية حماية الأفراد في ما يتعلق بالمعالجة الآلية للبيانات الشخصية والبروتوكول الإضافي الملحق بها.

التدابير المتخذة لتعزيز التعاون الدولي في مجال أمن المعلومات

تعمل الأرجنتين على إبرام اتفاقات على المستوى الثنائي والإقليمي والمتعدد الأطراف، يكون الغرض منها أن تساهم في إنشاء فضاء إلكتروني آمن وسلمي، وتسعى إلى أن المشاركة في جميع أعمال المنظمات الدولية العاملة في مجال الأمن السيبراني، والمشاركة الفعالة في جميع الأوساط الأكاديمية والتقنية الدولية التي تُعنى بهذا الموضوع.

وفي هذا الصدد، تشارك الأرجنتين بنشاط في أنشطة لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية وتساعد الدول التي لم تصبح بعد أطرافاً في هذا الصك وتريد الانضمام إليه. ومن بين المزايا المحددة التي توفرها هذه المعاهدة لأعضائها أن تكون جزءاً من شبكة ٧/٢٤، التي تهيّئ قناة للتعاون وتسهل إجراء التحقيقات الجنائية بين مختلف الدول الأطراف.

ومع ذلك، ومراعاة لطبيعة ظاهرة الجريمة السيبرانية التي تتعدى الحدود الوطنية والحاجة إلى وجود آليات للتصدي لها على الصعيد العالمي، تدعم الأرجنتين كلاً من العمليات في إطار الاتفاقية المتعلقة بالجريمة الإلكترونية وكذلك هيئات النقاش التي تسعى إلى التقدم، في إطار الأمم المتحدة، نحو التفاوض على وضع إطار قانوني عالمي في هذا الصدد (عملية فيينا).

وشاركت الأرجنتين في أعمال فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي في عامي ٢٠١٣ و ٢٠١٤، وتسعى إلى المساهمة في المناقشات الجارية في الجمعية العامة حول هذا الموضوع.

وتدرك الأرجنتين الأهمية المحورية لبناء القدرات، وهي عضو في المنتدى العالمي للخبرات السيبرانية، وتشارك إلى جانب منظمة الدول الأمريكية وشيلي والمكسيك وإستونيا وإسبانيا في مبادرة الأمن السيبراني في الدول الأعضاء في منظمة الدول الأمريكية.

وفي تشرين الثاني/نوفمبر ٢٠١٨، انضمت الأرجنتين إلى نداء باريس من أجل الثقة والأمن في الفضاء الإلكتروني.

وعلى الصعيد الإقليمي، تشارك الأرجنتين في اجتماعات الفريق العامل المعني بتدابير تعزيز التعاون والثقة في الفضاء الإلكتروني للجنة البلدان الأمريكية لمناهضة الإرهاب التابعة لمنظمة الدول الأمريكية، وقد ساهمت في أنشطة مرصد الأمن السيبراني في أمريكا اللاتينية ومنطقة البحر الكاريبي، حيث قدمت معلومات لإعداد الطبعة الثانية من الدراسة المعنونة *¿Estamos Ciberseguridad preparados en América Latina y el Caribe?* (*الأمن السيبراني: هل نحن مستعدون في أمريكا اللاتينية ومنطقة البحر الكاريبي؟*)، التي أجرتها منظمة الدول الأمريكية ومصرف التنمية للبلدان الأمريكية.

واستضافت المنتدى الدولي الثاني للشؤون الجنسانية والأمن السيبراني، الذي نُظم بالاشتراك مع منظمة الدول الأمريكية، يومي ٢٩ و ٣٠ أيار/مايو ٢٠١٨.

وفي إطار السوق المشتركة لبلدان المخروط الجنوبي، شجعت الأرجنتين على وضع جدول الأعمال الرقمي للسوق المشتركة لبلدان المخروط الجنوبي، الذي يشمل أيضاً الأمن السيبراني.

وعلى الصعيد الثنائي، وقّعت الأرجنتين وإسبانيا في عام ٢٠١٧ مذكرة تفاهم بين المؤسسات بشأن الأمن السيبراني. وفي العام ذاته، أنشأت مع الولايات المتحدة فريقاً عاملا ثنائياً حكومياً دولياً مكلفاً بسياسة الفضاء الإلكتروني يُعنى بقضايا الأمن السيبراني، وفي عام ٢٠١٨، وقعت الأرجنتين وشيلي اتفاقاً للتعاون في مجال الأمن السيبراني والجرائم الإلكترونية والدفاع عن الفضاء الإلكتروني. تعتبر الأرجنتين أنه من المهم الحفاظ على قنوات حوار مفتوحة في مجال الأمن السيبراني مع جميع البلدان والمناطق.

التعليقات على محتوى تقارير فريق الخبراء الحكوميين وقرار الجمعية العامة ٢٧/٧٣ والتدابير التي يمكن أن يتخذها المجتمع الدولي لتعزيز أمن المعلومات على الصعيد العالمي

تؤيد الأرجنتين وتدعم مضمون المفاهيم المذكورة في تقارير فريق الخبراء الحكوميين.

ومن مسؤوليات الدول الحرص على وجود فضاء إلكتروني آمن وسلمي، لذلك من الضروري الحفاظ على السلوك المسؤول عن طريق تطبيق القانون الدولي الحالي، وكذلك عن طريق وضع معايير طوعية جديدة والتعاون الدولي وتدابير الثقة المتبادلة، وفقاً لقرارات الجمعية العامة ٢٨/٦٩ و ٢٣٧/٧٠ و ٢٨/٧١ و ١٨٧/٧٣ و ٢٦٦/٧٣، المتعلقة بهذه المسألة.

ويكتسي التعاون الثنائي والإقليمي والمتعدد الأطراف أهمية جوهرية لبناء قدرة الدول التي تحتاج إلى تعزيز أنظمتها الخاصة بالوقاية من التهديدات في الفضاء الإلكتروني والكشف عنها والإنذار بها والتصدي لها.

ومكافحة الجريمة الإلكترونية الفعالة عنصرٌ أساسي لإيجاد فضاء إلكتروني آمن وسلمي، ومن ثم فهي مسألة ذات أولوية قصوى بالنسبة للتعاون بين الدول.

وفي ما يخص قرار الجمعية العامة ٢٧/٧٢، ولا سيما مجموعة القواعد والقواعد والمبادئ الدولية للسلوك المسؤول للدول المذكورة في الفقرة ١ من القرار، فإن الأرجنتين تؤيد أهمية هذه المواد. ومع ذلك، تجدر الإشارة إلى أنه بالنظر إلى طبيعة التهديدات في الفضاء الإلكتروني والوتيرة التي تتطور بها، يُستصوب أن يطلب من الدول بذل أقصى جهد ممكن لمنع استخدام أراضيها من قبل جهات من غير الدول لارتكاب أفعال غير مشروعة دولياً باستخدام تكنولوجيا المعلومات والاتصالات. ومع ذلك، لا يمكن القول إن بإمكانها ضمان ذلك.

وعلاوة على ذلك، وفي ضوء النطاق العالمي والعابر للحدود للتهديدات في الفضاء الإلكتروني، ينبغي تعزيز التركيز الذي يوليه المجتمع الدولي لبناء القدرات حتى تتمكن جميع الدول، وخاصة البلدان النامية، من تعزيز أنظمتها الخاصة بالوقاية من التهديدات في الفضاء الإلكتروني والكشف عنها والإنذار بها والتصدي لها.

وتدرك الأرجنتين أنه من الضروري مواصلة العمل في إطار عمليات الأمم المتحدة، مثل فريق الخبراء الحكوميين والفريق العامل المفتوح العضوية المعني بالتقدم في مجال المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، الذي أنشئ بموجب قرار الجمعية العامة ٢٧/٧٣. ومن الضروري التوصل إلى توافق في الآراء بشأن كيفية تطبيق القانون الدولي على الفضاء الإلكتروني، الذي لا بد له من الحوار والشفافية في ما يتعلق برؤية كل دولة. وبالمثل، من الأهمية بمكان إيجاد آليات وأدوات يمكن أن تتكيف بسرعة مع التغييرات والتحديات الجديدة التي يولدها التقدم السريع للتكنولوجيا بطريقة مستمرة.

كولومبيا

[الأصل: بالإسبانية]
[١٥ أيار/مايو ٢٠١٩]

تقييم عام

تتفق حكومة كولومبيا مع الحاجة إلى تعزيز التنسيق والتعاون بين الدول لدراسة التهديدات وتدابير التعاون الممكنة للتصدي لها، وتطبيق القانون الدولي على استخدام الدول لتكنولوجيات المعلومات والاتصالات، وكذلك معايير وقواعد ومبادئ السلوك المسؤول للدول.

وتعتقد أن من المهم للغاية للاستقرار الدولي أن تستخدم الدول تكنولوجيا المعلومات والاتصالات استخداماً مسؤولا وأن يروَّج لاستخدامها باعتبارها أداة للتنمية الاقتصادية والاجتماعية.

وتؤيد كولومبيا إيجاد شبكة إنترنت حرة ومفتوحة وآمنة، ومن الضروري أن تمتلك البلدان الأدوات التي تتيح لها التعاون الفعال على مكافحة الجريمة السيبرانية وتعزيز قدراتها الوطنية وتوطيد تدابير الثقة بين البلدان.

ومن الضروري إدراك ومواجهة التحديات المتعلقة بالهوية الرقمية، وهي من بين أمور أخرى التعاون مع مقدِّمي خدمات الإنترنت؛ والأدلة الرقمية وأساليب الحصول عليها وتخزينها، وسلسلة العهدة، وإصدار الشهادات والصلاحية؛ وحماية البيانات والخصوصية واحترام حقوق الناس وحرياتهم.

ومع ذلك، يُعتقد أن المناقشات الجارية بشأن الجرائم الإلكترونية ينبغي مواصلة مناقشتها من الناحية التقنية والسياسية في لجنة منع الجريمة والعدالة الجنائية من خلال فريق الخبراء الحكومي الدولي المعني بالجريمة الإلكترونية باعتباره المنتدى الرئيسي، ولا ينبغي إنشاء أفرقة بديلة جديدة تحد من مشاركة البلدان، وكذلك في فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي.

وكولومبيا مهتمة بالمشاركة في المناقشات الدولية التي تجري في الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي وفي فريق الخبراء الحكومي الدولي. وقد قدمت كولومبيا مرشحاً لها في ما يخص هذا الفريق الأخير. وفي حالة عدم إمكانية مشاركتها في هذا السيناريو الأخير، ستوجَّه المساهمات عبر هيئات المشاورات الإقليمية التي أنشأتها منظمة الدول الأمريكية لهذا الغرض.

ملاحظات بشأن قراري الجمعية العامة ٧٣/٢٦٦ المتعلق بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي، و ٧٣/٢٧ المتعلق بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي

تتفق حكومة كولومبيا مع ضرورة تحسين التنسيق والتعاون بين الدول لتعزيز الاستخدام المسؤول لتكنولوجيا المعلومات والاتصالات من جانب الدول، كعنصر أساسي للاستقرار الدولي، وكذلك لتكون تكنولوجيا المعلومات والاتصالات أداة حقيقية للتنمية الاقتصادية والاجتماعية.

وقد كانت كولومبيا مشاركةً نشطة في فريق الخبراء الحكومي الدولي في الفترة ٢٠١٤-٢٠١٥، حيث حصلت على آخر وثيقة تعدُّ في هذا السياق، وهي تتفق تماماً مع المفاهيم والاعتبارات والتفسيرات والتوصيات الواردة فيها.

وموقف حكومة كولومبيا هو أن القانون الدولي يجب أن ينطبق على العالم ''الافتراضي'' كما ينطبق على العالم ''المادي''. هذا الموقف أو الرؤية لم ينظر فيهما فقط خبراء فريق الخبراء الحكومي الدولي الذين توصلوا إلى توافق في الآراء بشأن الجوانب الأساسية للتطبيق، ولكن هذا يتجلى أيضاً في تدابير بناء الثقة التي وضعتها منظمة الأمن والتعاون في أوروبا ورابطة دول جنوب شرق آسيا وإعلان لوكا لمجموعة الدول السبع بشأن السلوك المسؤول للدول في الفضاء الإلكتروني، وحظي بالإجماع بدعم من فريق الخبراء في الإصدار ٢,٠ لدليل تالين. وفي كل الأحوال، فإن قابلية تطبيق الجوانب المرتبطة بالقانون الدولي الساري على عمليات الإنترنت بشكل فعال يتطلب مزيداً من الدراسة لضمان عدم وجود ''مواضع غامضة'' أو تفسيرات متباينة محتملة في تطبيقه.

وبالنسبة للبلدان الأقل نمواً من الناحية التكنولوجية، من الأهمية بمكان التوصل إلى اتفاقات تمنع الفضاء الإلكتروني من أن يصبح مسرحاً للصراعات المتنامية، بسبب الآثار المحتملة التي قد تترتب على تضررها من ذلك، سواء كأهداف لعمليات إلكترونية موجَّهة ضدها أو لاستخدامها ''كدول واسطة'' بسبب عدم كفاية القدرات لتجنب ذلك.

وفي البلدان الأقل نمواً من الناحية التكنولوجية، يمكن أن يكون لتضرر بعض البنى التحتية الحيوية السيبرانية تأثيرٌ كبير، ليس فقط بسبب الاعتماد على تكنولوجيات المعلومات والانتقال إلى التحكم الآلي في العمليات الصناعية باستخدام التقنيات المرتبطة بالإنترنت، ولكن أيضاً بسبب نقص الوعي بالمخاطر والتهديدات، وكذلك الموارد اللازمة لتعزيز الأمن الرقمي للشركات المسؤولة عن هذه البنى التحتية.

ومن الضروري تشجيع النقاش على أعلى مستوى بشأن ما يقتضيه ميثاق الأمم المتحدة وقابليته للتطبيق على صون السلام والاستقرار، وذلك لتهيئة بيئة مفتوحة وآمنة ومستقرة ويمكن الوصول إليها وسلمية في ميدان تكنولوجيا المعلومات والاتصالات.

التدابير المتخذة على المستوى الوطني لتعزيز أمن المعلومات وتعزيز التعاون الدولي في هذا المجال، والتحديات القائمة على المستوى الوطني

من أجل معالجة بواعث الشك والمخاطر والتهديدات ونقاط الضعف والحوادث الرقمية، أصدرت الحكومة الوطنية في عام ٢٠١١ الوثيقة ٣٧٠١ للمجلس الوطني للسياسة الاقتصادية والاجتماعية، المعنونة ''المبادئ التوجيهية لسياسة الأمن السيبراني والدفاع عن الفضاء الإلكتروني''.

وركزت هذه السياسة جهود البلاد على مواجهة الزيادة الحاصلة في التهديدات الحاسوبية التي أضرت بها بشكل كبير وعلى إعداد إطار تنظيمي ومؤسسي لمواجهة التحديات في جوانب الأمن السيبراني. ويرد أدناه بيان بالتقدم المحرز في تنفيذ هذه المبادئ التوجيهية للسياسة المذكورة وأنشطة استعراضها خلال عامي ٢٠١٤ و ٢٠١٥.

وكان الهدف العام المتوخى من الوثيقة ٣٧٠١ هو تعزيز قدرات الدولة على مواجهة الأخطار التي تهدِّد الدفاع والأمن القوميين في المجال السيبراني (الأمن السيبراني والدفاع عن الفضاء الإلكتروني)، وإيجاد بيئة وظروف تساعد على توفير الحماية في الفضاء السيبراني. ولتحقيق هذا الهدف العام، تمت صياغة ثلاثة أهداف محددة هي: (أ) إنشاء الهيئات المناسبة لمنع الحوادث السيبرانية أو الطوارئ وتنسيقها والتصدي لها ورصدها والسيطرة عليها، ووضع توصيات لمواجهة التهديدات والمخاطر التي تهدد الأمن السيبراني والدفاع عن الفضاء الإلكتروني على الصعيد الوطني؛ (ب) توفير تدريب متخصص في مجال أمن المعلومات وتوسيع أنشطة البحث في مجالي الدفاع عن الفضاء الإلكتروني والأمن السيبراني؛ (ج) وتعزيز التشريعات المتعلقة بالأمن السيبراني والدفاع عن الفضاء الإلكتروني والتعاون الدولي، والمضي قدماً نحو انضمام كولومبيا إلى مختلف الصكوك الدولية المعتمدة في هذا المجال.

ومن بين مستجدات هذه السياسة، وبفضل رؤية جديدة مستمدة من أفضل الممارسات الدولية، ولا سيما بفضل اتباع مبادئ وتوصيات المنظمات متعددة الأطراف مثل منظمة حلف شمال الأطلسي، ومنظمة التعاون والتنمية في الميدان الاقتصادي، والاتحاد الدولي للاتصالات، ومنظمة الدول الأمريكية، وجمعيات عالمية من القطاع الخاص حلَّلت سبل معالجة الأمن الرقمي في ظل الظروف الحالية للبيئة الرقمية، أصدرت الحكومة الوطنية في عام ٢٠١٦ الوثيقة ٣٨٥٤ للمجلس الوطني للسياسة الاقتصادية والاجتماعية، المعنونة ''السياسة الوطنية للأمن الرقمي''، الذي سيستمر العمل بها حتى كانون الأول/ديسمبر ٢٠١٩ والمراد منها تعزيز قدرات أصحاب المصلحة المتعددين على تحديد مخاطر الأمن الرقمي في أنشطتهم الاجتماعية الاقتصادية في البيئة الرقمية ومواجهتها ومعالجتها وتخفيف آثارها، في إطار من التعاون والتآزر والمساعدة. ومن المتوقع أن يُساهم ذلك في نمو الاقتصاد الرقمي الوطني، الذي سيعزِّز بدوره الرخاء الاقتصادي والاجتماعي في البلاد.

ولرسم الهدف العام المتوخى من هذه السياسة العامة، وُضعت الأهداف المحددة التالية:

(أ) إنشاء إطار مؤسسي للأمن الرقمي يتوافق مع نهج إدارة المخاطر؛

(ب) تهيئة الظروف المؤاتية لأصحاب المصلحة المتعددين لإدارة مخاطر الأمن الرقمي في أنشطتهم الاجتماعية الاقتصادية وبث الثقة في استخدام البيئة الرقمية؛

(ج) تعزيز أمن الأفراد والدولة في البيئة الرقمية، على الصعيدين الوطني وعبر الوطني، مع اتباع نهج لإدارة المخاطر؛

(د) تعزيز الدفاع والسيادة الوطنية في البيئة الرقمية من خلال اعتماد نهج لإدارة المخاطر؛

(هـ) إنشاء آليات دائمة واستراتيجية لتعزيز التعاون والتعاون والمساعدة في مجال الأمن الرقمي، على الصعيدين الوطني والدولي.

ومنذ أن وافق المجلس الوطني للسياسة الاقتصادية والاجتماعية على هذه السياسة في نيسان/أبريل ٢٠١٦، أنجزت الكيانات العامة المسؤولة الأنشطة المقرَّرة في خطة العمل وقامت بمتابعة سياسة الأمن الرقمي الوطني، وذلك من أجل تحقيق الهدف العام والأهداف المحددة للسياسة.

وباختصار، ومن بين مجموع الإجراءات المتخذة، يمكن تسليط الضوء على الإنجازات التالية:

- بدأ إنشاء إطار مؤسسي واضح يشمل أصحاب المصلحة المتعددين لتنفيذ سياسة الأمن الرقمي الوطني، ولا سيما إنشاء منصب منسق الأمن الرقمي الوطني في ديوان رئاسة الجمهورية وضمان استمرار عمل الفريق المكلف بالتصدي للطوارئ الحاسوبية في كولومبيا.
- بدأت عملية تصميم وتنفيذ نموذج لإدارة مخاطر الأمن الرقمية في الحكومة الوطنية، مع مراعاة الإطار المفاهيمي لهذه السياسة ومعايير الأمن الدولية والإطار الشامل لإدارة المخاطر على الصعيد الوطني.
- بدأت تهيئة الظروف الملائمة لأصحاب المصلحة المتعددين لإدارة مخاطر الأمن الرقمي في أنشطتهم الاجتماعية الاقتصادية وبث الثقة في ما يتعلق باستخدام البيئة الرقمية، لا سيما عن طريق إجراء دراسة عن تأثير الجنح والجرائم في الأوساط الرقمية في البلاد وتعديل الإطار التنظيمي لقطاع تكنولوجيا المعلومات والاتصالات لتعزيز الأمن الرقمي.
- وُضعت خطط لتعزيز القدرات التشغيلية والإدارية والبشرية والعلمية والمادية والتكنولوجية وقدرات البنى التحتية للكيانات التي هي جزءٌ من الإطار المؤسسي الحالي للحكومة الوطنية.
- وقِّعت اتفاقات تعاون دولية مع بلدان متحالفة ومع ممثِّلي الصناعة المهمين، بهدف تعزيز القدرات وتبادل المعلومات عن التهديدات. وفي عام ٢٠١٧، وافقت منظمة حلف شمال الأطلسي بالإجماع على توقيع برنامج فردي للتآزر والتعاون مع كولومبيا، حيث أصبحت بلادنا أول بلد في أمريكا اللاتينية يكتسب هذا الوضع، لتصبح شريكاً عالمياً. وضمن هذا الصك القانوني، تتمثل إحدى النقاط التي يضمها في تحسين الكفاءات في مجال الفضاء الإلكتروني. وبالنسبة لكولومبيا، من الأمور الأساسية تعزيز المبادرات القائمة والحالية في مختلف الأوساط في إطار الأمم المتحدة.

وفي ما يتعلق بهدف إنشاء إطار مؤسسي للأمن الرقمي يتماشى مع نهج إدارة المخاطر، أُحرز بعض التقدم مثل إنشاء منصب منسِّق الأمن الرقمي الوطني (مع ما يلزمه من الوسائل التقنية والقانونية)، وكذلك إنشاء لجنة الأمن الرقمي كهيئة مشرفة على مجلس إدارة وتدبير الوظيفة العامة ولتكون أعلى هيئة مشتركة بين المؤسسات والقطاعات في الحكومة الوطنية لتوفير التوجيهات الرفيعة المستوى في قضايا الأمن الرقمي. وبالمثل، صُممت أدوات أساسية مثل نموذج إدارة مخاطر الأمن الرقمي، الذي يتعين على الكيانات الوطنية التابعة للفرع التنفيذي اعتماده وتنفيذه، والذي أدمجته الإدارة الإدارية للوظيفة العمومية في *دليل مواجهة المخاطر المرتبطة بالإدارة والفساد والأمن الرقمي وتصميم الضوابط في الكيانات العامة*، في آب/أغسطس ٢٠١٨.

ومن بين التحديات المصادفة ضرورة تنفيذ وتعزيز إدارة مخاطر الأمن الرقمي في الهيئات المسؤولة عن الأمن السيبراني والدفاع عن الفضاء الإلكتروني للمؤسسات المنشأة. وهناك أيضاً ضرورة تعزيز

القدرات القطاعية من خلال اعتماد نهج أكثر كفاءة في الترويج لفرق التصدي لحوادث الأمن السيبراني القطاعية وإنشائها، ووضع خريطة طريق فعالة من أجل التطوير الفعال للجنة الأمن الرقمي، واستحداث مرسوم فعال بين مرافق التعاون القطاعية والإقليمية والمرافق الوطنية للتنسيق في مجال الأمن الرقمي، وكذلك تمكين مختلف أصحاب المصلحة المتعددين من تبيُّن المخاطر وتقييمها وإدارتها بصورة فعالة.

وفي ما يخص الهدف الثاني، المتعلق بتهيئة الظروف الملائمة لأصحاب المصلحة المتعددين لإدارة مخاطر الأمن الرقمي في أنشطتهم الاجتماعية الاقتصادية وبث الثقة في ما يتعلق باستخدام البيئة الرقمية، أُحرز بعض التقدم في ما يتعلق بصياغة مشروع خطة الأمن الرقمي الوطنية. لكن من الضروري مواصلة تعزيز الارتباط بين المناقشات التي يجريها جميع أصحاب المصلحة المتعددين، والحصول على مزيد من المساهمات الأكاديمية (البحث) في هذا الموضوع، ومساعدة الكيانات العامة على اعتماد نموذج إدارة المخاطر الأمنية الرقمية. ونُفذت بعض حملات التوعية، مثل برنامج ''En TIC confío'' (''أثق في تكنولوجيا المعلومات والاتصالات'')، وبالإضافة إلى ذلك، أُعدت بدعم من منظمة الدول الأمريكية في عام ٢٠١٧ *دراسة التأثير الاقتصادي للحوادث والتهديدات والهجمات الإلكترونية في كولومبيا*، ويجري إعداد الدراسة نفسها لعام ٢٠١٨.

ومن بين التحديات المصادفة ضرورة تحديد مسارات البحث التي يجب أن تستمر وتعزَّز حول الأمن الرقمي، وتحديد نموذج واضح وفعال للتنسيق والاتصال يسمح بإنشاء الإطار القانوني اللازم في مجال الأمن الرقمي الذي يشجع التحوُّل الرقمي لأصحاب المصلحة المتعددين، والتعميم الفعلي لنتائج الدراسات الاستراتيجية على المستويات الحكومية العليا لاتخاذ القرارات وإعادة توجيه استراتيجية إعداد محتوى تعليمي لإدراجه في المناهج الأكاديمية على مختلف مستويات المنظومة التربوية.

وفي ما يخص الهدف الثالث، المتعلق بتعزيز أمن الأفراد والدولة في البيئة الرقمية، على الصعيدين الوطني وعبر الوطني، مع اتباع نهج لإدارة المخاطر، أُحرز بعض التقدم في رسم الخطط لبناء قدرات الجهات الفاعلة الأساسية، وإعداد التقارير المتعلقة بإحصاءات الجرائم الإلكترونية وضد تعزيز قدرات المسؤولين عن الأمن السيبراني في البلد في مجال إدارة المخاطر.

والتحدي الماثل هنا هو التنفيذ العاجل للخطط الرامية إلى تعزيز القدرات التنفيذية والإدارية والبشرية والعلمية وقدرات البنية التحتية المادية والتكنولوجية الخاصة بالأجهزة والكيانات المسؤولة عن الأمن السيبراني، وكذلك وضع مبادئ توجيهية لتكييف الإطار القانوني والتنظيمي الحالي ليتواءم مع الاحتياجات في ما يتعلق بما يلي: (أ) تحليل جرائم الفضاء الإلكتروني والجرائم الإلكترونية والظواهر المستجدة في البيئة الرقمية والجُنح والجرائم التي تستخدم البيئة الرقمية كوسيلة، واستباقها والوقاية منها وكشفها والتصدي لها والتحقيق فيها؛ (ب) ومقاضاة وتجريم أنواع جديدة من الجرائم، من بينها جرائم الفضاء الإلكتروني، التي تسهِّل غسل الأموال؛ (ج) تحديث أجهزة الأمن والدفاع التابعة للدولة والاستخبارات في البيئة الرقمية، وفقاً للمبادئ الأساسية لسياسة الأمن الرقمي الوطني.

وفي ما يخص الهدف الرابع، المتعلق بتعزيز الدفاع والسيادة الوطنية في البيئة الرقمية من خلال اعتماد نهج لإدارة المخاطر، أُحرز بعض التقدم في رسم خطط لتعزيز قدرات الجهات الفاعلة الأساسية والتحديث الدوري لقائمة البنية التحتية الحيوية الوطنية للفضاء الإلكتروني، وإعداد بعض محتويات خطط حماية البنية التحتية الحيوية للفضاء الإلكتروني، وإنشاء عدد من أفرقة التصدي لحوادث الأمن السيبراني

القطاعية لتيسير التدبير المناسب للحوادث الرقمية في البنية التحتية الحيوية الوطنية للفضاء الإلكتروني (مثل تلك الخاصة بالحكومة والقطاع المالي وقطاع الكهرباء) ومشاركة بعض الأطراف المهتمة في تمارين المحاكاة والتدريب، على الصعيدين الوطني والدولي، وذلك لتنمية مهارات وقدرات أصحاب المصلحة المتعددين المسؤولين عن البنية التحتية الحيوية الوطنية للفضاء الإلكتروني والدفاع الوطني في البيئة الرقمية.

ومن بين التحديات المصادفة في تحقيق هذا الهدف ضرورة القيام من أعلى مستوى بإعادة صوغ المبادئ التوجيهية المتعلقة بحماية البنية التحتية الحيوية الوطنية للفضاء الإلكتروني والدفاع عنها، مع مراعاة الظروف الجديدة، وضرورة إصدار مرسوم رسمي لإدارة حوادث الأمن الرقمي لهذا النوع من البنية التحتية والتصدي لها. كما أنه من الضروري وضع استراتيجية تقوم فيها الحكومة الوطنية بتوحيد أعمال الوعي والتدريب في مجال الأمن الرقمي في إطار الدفاع الوطني.

وختاماً، وفي ما يخص الهدف الخامس، المتعلق بإنشاء آليات دائمة واستراتيجية لتعزيز التعاون والتعاون والمساعدة في مجال الأمن الرقمي، على الصعيدين الوطني والدولي، أُحرز بعض التقدم في الانضمام إلى آليات لتعزيز التعاون والتآزر والمساعدة على المستوى الدولي في مجال الأمن الرقمي. ومن بين أوجه التقدم المحرز عملية الانضمام إلى الاتفاقية المتعلقة بالجريمة الإلكترونية، والتقدم المحرز في إعداد مشروع خطة استراتيجية للتعاون والتآزر والمساعدة على المستوى الدولي.

أما يتعلق بالتحديات المصادفة، من الضروري تحديد الهيئات التي ينبغي لكولومبيا أن تشارك فيها في مجال الأمن الرقمي وترتيب الهيئات ذات الأولوية منها، وتحديد نموذج واضح وفعال للتنسيق والاتصال بين أصحاب المصلحة يسمح بوضع وتنفيذ وثائق استراتيجية لتعزيز التعاون والتآزر والمساعدة، على الصعيدين الوطني والدولي، في مسائل الأمن الرقمي.

ومراعاة لكل ما تقدم ذكره، وبالنظر إلى أن سياسة الأمن الرقمي الوطنية المحددة في الوثيقة ٣٨٥٤ الصادرة عن المجلس الوطني للسياسة الاقتصادية والاجتماعية عام ٢٠١٦ تتضمن خطة عمل ينتهي العمل بها في عام ٢٠١٩، فإن الحكومة الوطنية عاكفة، بدعم من منظمة الدول الأمريكية، على وضع سياسة جديدة تعالج التحديات المذكورة.

كوبا

[الأصل: بالإسبانية]
[٢٩ نيسان/أبريل ٢٠١٩]

يجب استخدام تكنولوجيا المعلومات والاتصالات الجديدة بطريقة سلمية من أجل الصالح العام للبشرية ولتعزيز التنمية المستدامة لجميع البلدان، أياً كان مستواها من التطور العلمي والتكنولوجي.

وقد يكون لهذا التقدم العلمي والتكنولوجي تطبيقات مدنية وعسكرية، ويجب الحيلولة دون تأثير هذا التقدم على الأمن الدولي للدول.

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

وفي هذا الصـــدد، نؤيد إنشـــاء فريق عامل مفتوح العضـــوية معني بالتقدم في مجال المعلومات والاتصـالات السـلكية واللاسـلكية في سـياق الأمن الدولي، عملا بقرار الجمعية العامة ٢٧/٧٣، وذلك بغية جعل عملية مفاوضـات الأمم المتحدة بشـأن الأمن في اسـتخدام تكنولوجيا المعلومات والاتصـالات أكثر ديمقراطية وشمولية وشفافية.

ونرى أنه من الضـــروري إنشـــاء إطار تنظيمي دولي ملزم قانوناً، يكون مكمِّلا للقانون الدولي الحالي لكنه يسري على تكنولوجيا المعلومات والاتصالات.

ويجب على جميع الدول احترام المعايير الدولية الحالية في هذا المجال. ويجب أن تكون ســـبل الوصـول إلى المعلومات أو أنظمة الاتصـالات السـلكية واللاسـلكية لأي دولة أخرى متوافقة مع اتفاقات التعاون الدولي المبرمة، بناء على مبدأ موافقة الدولة المعنية. ويجب أن تتقيد أشـــكال التبادلات ونطاقها بتشريعات الدولة التي تتيح الدخول إلى نظامها.

ويشـكل الاسـتخدام العدائي للاتصـالات السـلكية واللاسـلكية، بنية مُعلنة أو خفية تتوخى تقويض النظام القانوني والســياســي للدول، انتهاكاً للمعايير الدولية المتعارف عليها في هذا المجال، ويمثل استخداما غير قانوني وغير مسؤول لهذه الوسائل.

ومن خلال بث برامج إذاعية وتلفزيونية غير قانونية، تعرضـت موجات الأثير الكوبية لهجوم دائم من الخارج، وذلك ببث برامج مصـمَّمة خصيصاً للتحريض على الإطاحة بالنظام الدستوري الذي أنشأه الشعب الكوبي.

ففي المتوسط، جرى خلال عام ٢٠١٨ بث برامج غير مشروعة مناوئة لكوبا بمتوسط ١ ٦٥٣ ســاعة في الأســبوع، باســتخدام ٢٠ تردداً انطلاقاً من أراضــي الولايات المتحدة، وهو ما يتعارض مع مقاصد ومبادئ ميثاق الأمم المتحدة والقانون الدولي وأحكام الاتحاد الدولي للاتصالات.

ومرة أخرى، تحث كوبا على وضع حد فوري لهذه السياسات العدوانية التي تنتهك سيادة كوبا والتي تتنافى، علاوة على ذلك، مع إقامة علاقات قوامها الاحترام المتبادل والتعاون بين الدول.

لقد تسـبَّب الحصـار الاقتصـادي والتجاري والمالي الذي تفرضـه حكومة الولايات المتحدة على كوبا منذ حوالي ٦٠ عاماً في إلحاق أضـرار جسـيمة بالشـعب الكوبي، بما في ذلك اسـتخدام تكنولوجيا المعلومات والاتصالات والتمتع بها.

وأعلن رؤسـاء ورئيسـات دول وحكومات أمريكا اللاتينية ومنطقة البحر الكاريبي، في مؤتمر القمة الثاني لرؤسـاء دول وحكومات جماعة دول أمريكا اللاتينية ومنطقة البحر الكاريبي، منطقة أمريكا اللاتينية ومنطقة البحر الكاريبي منطقة سلام، وذلك بغية تحقيق أهداف من بينها تعزيز علاقات الصداقة والتعاون فيما بينها ومع الدول الأخرى، بصـرف النظر عن اختلاف نُظمها السـياسـية والاقتصـادية والاجتماعية أو تباين مستويات تنميتها، وانتهاج التسامح والتعايش في جو من السلام وحُسن الجوار.

وخلال مؤتمر القمة الخامس لرؤســاء دول وحكومات جماعة دول أمريكا اللاتينية ومنطقة البحر الكاريبي، الذي عقد في بونتا كانا (الجمهورية الدومينيكية) في كانون الثاني/يناير ٢٠١٧، أُبرزت مجدداً أهمية تكنولوجيا المعلومات والاتصـالات، بما في ذلك شبكة الإنترنت، بوصـفها أدوات لتعزيز السـلام رفاه الإنسان والتنمية والمعرفة والوئام الاجتماعي والنمو الاقتصادي.

مصر

[الأصل: بالإنكليزية]
[٩ أيار/مايو ٢٠١٩]

مقدمة

شهد العالم في العقود الثلاثة الماضية طفرة هائلة في استخدام شبكة الإنترنت والهواتف الذكية والأدوات الحديثة لتكنولوجيا المعلومات والاتصالات، إلى جانب كم هائل من استخدامات تكنولوجيا المعلومات والاتصالات في مجالات الأعمال والتجارة والخدمات الحكومية والتعليم والمعرفة والترفيه والسياحة والرعاية الصحية وغيرها من الأنشطة الاقتصادية والاجتماعية والثقافية. وإلى جانب الفرص الناجمة عن النمو المستمر في مجال الاتصالات السلكية واللاسلكية واستخدام الإنترنت وتكاثر المعاملات الإلكترونية والخدمات الإلكترونية، من المهم إدراك التهديدات والتحديات التي تستهدف البنية التحتية لتكنولوجيا المعلومات والاتصالات والمعاملات الإلكترونية بشكل عام وتواجهها، لأنها تقوض الثقة في الخدمات الإلكترونية والأعمال التجارية الإلكترونية والاطمئنان إليها على وجه الخصوص.

لذلك فإن مصر تولي أهمية كبرى للدور الكبير المتمثل في استحداث وتطبيق أحدث تقنيات المعلومات ووسائل الاتصالات من أجل تحقيق التقدم الاقتصادي والاجتماعي على الصعيدين الوطني والدولي. كما تدعم مصر بهمة ونشاط استخدام تكنولوجيا المعلومات والاتصالات من أجل الصالح العام للبشرية وتعزيز التنمية المستدامة لجميع البلدان، بغض النظر عن مستويات تطورها العلمي والتكنولوجي. وعلاوة على ذلك، تعتقد مصر أنه ينبغي للأمم المتحدة أن تقوم بدور رئيسي في قيادة الجهود الدولية المبذولة في هذا الصدد وتشجع الحوار بين الدول الأعضاء للتوصل إلى فهم دولي مشترك لتطبيق القوانين والمعايير الدولية ومبادئ وقواعد سلوك الدولة المسؤول في مجال المعلومات، بما في ذلك تنفيذ الصكوك الملزمة قانوناً.

أهم التحديات والتهديدات الإلكترونية

١ - خطر اختراق البنية التحتية لتكنولوجيا المعلومات والاتصالات وتخريبها

ظهرت مؤخراً أنواع جديدة من الهجمات الإلكترونية الخطيرة للغاية، التي تهدف إلى تعطيل الخدمات الحيوية ونشر البرامجيات الخبيثة والفيروسات لتدمير أو تعطيل البنية التحتية لتكنولوجيا المعلومات والاتصالات وأنظمة التحكم الصناعية الهامة، لا سيما في المنشآت الرئيسية، بما فيها مؤسسات الطاقة النووية والنفط والغاز الطبيعي والكهرباء والطيران، ومختلف أشكال النقل، وقواعد البيانات الوطنية الرئيسية، والدوائر الحكومية، والرعاية الصحية، ودوائر تقديم المساعدة في الحالات الطارئة. وتنشُر هذه الهجمات الإلكترونية العديد من القنوات، بما في ذلك الشبكات اللاسلكية والذاكرة المحمولة، وقنوات شائعة أخرى مثل رسائل البريد الإلكتروني والمواقع الشبكية ووسائط التواصل الاجتماعي وشبكات الاتصالات السلكية واللاسلكية، التي قد يكون لها تأثير كبير على استخدام البنية التحتية الحيوية والخدمات المرتبطة بها والشركات. ومن حيث الممارسة العملية، قد تكون المنشآت الحساسة عرضة لهجمات إلكترونية متطورة، حتى لو لم تكن مرتبطة مباشرة بشبكة الإنترنت.

٢ - خطر الإرهاب الإلكتروني والحرب الإلكترونية

انتشرت في الآونة الأخيرة أنواع خطيرة للغاية من الهجمات والجرائم الإلكترونية، تُستخدم فيها تقنيات متقدمة مثل الحوسبة السحابية والتنصت على المكالمات الهاتفية وأجهزة اقتحام الشبكات والتشفير المتقدم وأدوات القرصنة الآلية التي تستهدف الأنظمة الحاسوبية وقواعد البيانات. وبالإضافة إلى ذلك، قد يتم نشر برامجيات خبيثة متقدّمة لتقويض أنظمة أمان الشبكات والمس بالأنظمة الحاسوبية لتشكيل شبكة حواسيب مصابة، يمكن استخدامها لاحقاً في مجموعة متنوعة من الأنشطة الإجرامية وغير القانونية. وقد تتكون شبكة الحواسيب المصابة الآلية من عشرات أو مئات الآلاف أو ملايين أجهزة الحاسوب المعرضة للخطر والتي يمكن استخدامها لشن هجمات إلكترونية خطيرة، مثل شن هجمات حجب الخدمة الموزع على الشبكات والمواقع المستهدفة لأغراض تدميرية و/أو إرهابية و/أو لغرض الابتزاز.

وغالباً ما يتطلب استحداث فيروسات الحاسوب المعقدة والمتطورة مستويات متقدمة من المعرفة والخبرة غير التقليدية، وهي متوفرة فقط في البلدان المتقدمة من الناحية التكنولوجية، لاستخدامها في الأغراض التكتيكية والاستراتيجية والحربية، بالإضافة إلى هجمات الجيوش التقليدية، أو أحيانًا بدلاً منها، في ما يُعرف باسم الحرب الإلكترونية. ومع ذلك، تنقُل المنظمات الإرهابية هذه التقنيات الخبيثة أو تستنسخها أو تعيد إنتاجها لاستخدامها في العمليات الإرهابية والجريمة المنظمة، وكذلك في تهديد وتعطيل البنية التحتية لتكنولوجيا المعلومات والاتصالات لأغراض الابتزاز و/أو التجسس الصناعي. وتؤكد مصر من جديد المواقف التي ذكرها كبار خبراء الأمن السيبراني الذين يتوقعون زيادة انتشار الهجمات الإلكترونية الشرسة والمتطورة في الفترة المقبلة.

٣ - خطر الهوية الرقمية وسرقة البيانات الخاصة

سرقة الهوية الرقمية واحدة من أخطر الجرائم التي تهدِّد مستخدمي شبكة الإنترنت ومستقبل الخدمات الإلكترونية. فبيانات الهوية والبيانات الشخصية المسروقة يمكن أن تسهل انتحال شخصية الأفراد في الفضاء الإلكتروني وقد تؤدي إلى خسائر في الأموال والممتلكات أو قد تورِّط أسماء الضحايا في أنشطة مشبوهة أو غير قانونية. ويستخدم سارقو الهوية عادة المعلومات المتاحة بالفعل على شبكة الإنترنت، وخاصة على وسائط التواصل الاجتماعي والشبكات المهنية المفتوحة؛ وقواعد البيانات الوطنية؛ وشبكات الخدمات الحكومية وخدمات الضمان الاجتماعي والرعاية الصحية؛ ومواقع التجارة الإلكترونية؛ والأسواق الافتراضية؛ وشبكات الدفع الإلكتروني؛ وآلات الصراف الآلي؛ والبورصات. وبالإضافة إلى ذلك، قد تتعرض الأدوات والأنظمة المستخدمة في إجراء المعاملات الإلكترونية للخطر أو السرقة أو التلف، مما يشكل تهديداً خطيراً لمصالح المستخدمين ومستقبل الخدمات الإلكترونية. وقد تمس الهجمات الشاملة والواسعة النطاق بالقطاع المالي الوطني. وقد تُسرق أيضاً بيانات المؤسسات العامة والشركات، مما يؤدي إلى خسائر كبيرة من الناحية المادية ومن حيث المصداقية وإلحاق الضرر بسمعة الشركة وتناقص العملاء واضمحلال قيمة الأصول غير الملموسة، مما قد يضر بالاقتصاد الوطني ككل.

الجوانب الرئيسية لخطورة التهديدات الإلكترونية المستجدة

قد تكون التهديدات الإلكترونية المستجدة خطيرة للغاية بسبب ثلاثة جوانب رئيسية:

١ - غالباً ما تنشُر تقنيات متقدِّمة ومتطورة؛ وتحتكر البلدان المتقدمة للغاية والشركات الكبرى في كثير من الأحيان هذه التقنيات. والعديد من هذه التقنيات سرية للغاية وغير متاحة للتصدير. وعلاوة على ذلك، قد تحتوي نسخُ بعض التقنيات القابلة للتصدير على أبواب خلفية أو نقاط ضعف تجعلها مصدر تهديدات إضافية.

٢ - يمكن أن تنتشر بسهولة، مما يساعد على نشر الفيروسات الخبيثة بسرعة وشن هجمات حجب الخدمة الموزع والهجمات الإلكترونية المتقدمة الأخرى بسرعة وسهولة، وذلك بسبب الاستخدام الواسع النطاق لتكنولوجيا المعلومات والاتصالات وبسبب سهولة شن هذه الهجمات عن بُعد ونقل الفيروسات عبر الحدود من أي مكان وبتكلفة منخفضة. كما أنه من الصعب بل وغالباً ما يتعذر تتبع المصدر الرئيسي لتلك التهديدات والمخاطر في حينها بغرض التصدي لها والتغلب عليها.

٣ - يمكن أن يكون لها تأثير واسع النطاق؛ فقد يكون للهجمات الإلكترونية تأثير مباشر وغير مباشر واسع النطاق على البنية التحتية، مما يتسبب في أضرار وخسائر كبيرة. بالإضافة إلى ذلك، قد تُنفذ عن بُعد ويتوسع نطاقها فجأة بطريقة لا يمكن التنبؤ بها، ويُحتمل أن تؤثر على المؤسسات الحيوية وعلى أعداد كبيرة من المواطنين (يعدّون بالآلاف أو الملايين).

الطريق إلى الأمام: نحو مواجهة التحديات الإلكترونية

قد تتجاوز الهجمات والجرائم الإلكترونية الحدود الجغرافية للبلدان ويُعتمد فيها عادة على شبكات الجريمة المنظمة التقليدية والتقنية. لذلك يجب أن تشمل الإجراءات المتخذة لمواجهة هذه الهجمات والجرائم آليات التعاون الدولي التقليدية لمكافحة الجرائم ومواجهة التهديدات الإلكترونية، وكذلك الأطر التشريعية والتنظيمية المزودة بآليات خاصة للتعامل مع التطورات التقنية المستجدة. ويستلزم التصدي الفعال للهجمات والجرائم الإلكترونية التعاون والتنسيق على المستوى الوطني، بين الشركاء الذين يوفرون ويديرون شؤون البنية التحتية في القطاعات الحيوية والشركاء الذين يقدمون الخدمات، بما في ذلك الوكالات الحكومية والمؤسسات والشركات. وبالإضافة إلى ذلك، فإن التعاون والتنسيق على الصعيدين الدولي والإقليمي من الأمور الأساسية للغاية ويجب أن يشمل المنظمات الدولية الرئيسية والتجمعات الإقليمية والمنتديات الدولية المهنية والمتخصصة.

مساهمات مصر

تدرك مصر أهمية التعاون الدولي في مواجهة تحديات أمن الفضاء الإلكتروني. وقد ساهم الخبراء المصريون في عدد من مجموعات الخبراء الحكومية ذات الصلة التي كلفتها الجمعية العامة بالتوصل إلى توصيات متفق عليها بشأن أمن الفضاء الإلكتروني من منظور الأمن الدولي. وعلاوة على ذلك، كانت مصر، بصفتها عضواً في الاتحاد الدولي للاتصالات، ضمن فريق الخبراء الرفيع المستوى المعني بالأمن السيبراني التابع للاتحاد، وشاركت في أنشطة جدول أعمال الأمن السيبراني العالمية. بالإضافة إلى ذلك، اقترحت مصر إنشاء الفريق العامل التابع لمجلس الاتحاد الدولي للاتصالات والمعني بحماية الطفل على شبكة الإنترنت وترأست الفريق من عام ٢٠١٠ حتى عام ٢٠١٧. وتشارك مصر في مؤتمرات وحلقات عمل إقليمية عن الأمن السيبراني وحلقات العمل التي تنظمها منظمات دولية مثل الاتحاد الدولي للاتصالات ومنظمة التعاون الإسلامي ومنظمة الأمن والتعاون في أوروبا ومنظمة التعاون الاقتصادي

والتنمية ومنتدى فرق التصدي للحوادث والأمن، وتستضيف تلك المؤتمرات وحلقات العمل أيضاً. كما تشارك مصر في دراسات الأمن السيبراني الدولية والإقليمية مع المنظمات المهنية مثل رابطة النظام العالمي للاتصالات المتنقّلة. وعلاوة على ذلك، تشارك مصر بنشاط في الجهود الإقليمية في الأوساط الأفريقية والعربية لتعزيز تدابير بناء الثقة وبناء القدرات ونشر أفضل الممارسات. وشاركت مصر أيضاً في مشاورات ومفاوضات ثنائية مع عدد من الدول والمنظمات الدولية والشركاء لإبرام اتفاقات بشأن التعاون الثنائي في هذا المجال الاستراتيجي.

أما على المستوى الوطني، وفي ضوء المادة (٣١) من الدستور المصري، أُنشئ المجلس الأعلى لحماية البنى التحتية للاتصالات والمعلومات الحرجة والأمن السيبراني (أي المجلس الأعلى المصري للأمن السيبراني) على مستوى مجلس الوزراء في وقت متأخر من عام ٢٠١٤. ويرأس هذا المجلس وزير الاتصالات وتكنولوجيا المعلومات ويضم أعضاء من القطاعات الحيوية وكذلك من وكالات الأمن الرئيسية. وعلى المستوى التنفيذي، أصبح الفريق الوطني للاستعداد لحالات الطوارئ الحاسوبية بمثابة الذراع التقني للمجلس. وقد وضع المجلس أول استراتيجية وطنية للأمن السيبراني في مصر في عام ٢٠١٧. ويتوافق نطاق الاستراتيجية وبنيتها وأهدافها مع المتطلبات الوطنية وتتقيد بالمعايير والقواعد والمبادئ الدولية. وبالمثل، فإن تنفيذ الاستراتيجية يسير على نفس المنوال.

الخلاصة

تكرِّر مصر تأكيد الحاجة الملحة إلى تكثيف بناء قدرات البلدان النامية في مجال أمن تكنولوجيا المعلومات والاتصالات وتقديم المساعدة التقنية لها، خاصة مع مراعاة أنه في كثير من الحالات، فإن قوة أمن الفضاء السيبراني لا تُقاس إلا بقوة أضعف حلقاته.

وعلاوة على ذلك، فإن العمل الفعال لفريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي وتقارير النتائج ذات الصلة التي أحالها الأمين العام إلى الجمعية العامة تمثل خطوات هامة في الاتجاه الصحيح. ومن أبرزها إظهار الأهمية المركزية لالتزامات الدول بمبادئ ميثاق الأمم المتحدة وغيرها من مبادئ القانون الدولي، بما في ذلك المساواة في السيادة؛ وتسوية النزاعات الدولية بالوسائل السلمية؛ والامتناع في علاقاتها الدولية عن التهديد باستعمال القوة أو استعمالها ضد السلامة الإقليمية أو الاستقلال السياسي لأية دولة، أو بأي طريقة أخرى تتعارض مع مقاصد الأمم المتحدة؛ واحترام حقوق الإنسان والحريات الأساسية؛ وعدم التدخل في الشؤون الداخلية للدول الأخرى. والهدف الأسمى هو إيجاد بيئة موثوقة وآمنة لتكنولوجيا المعلومات والاتصالات بما يتوافق مع الحاجة إلى الحفاظ على التدفق الحر للمعلومات.

وفي ضوء شدة التهديدات السيبرانية المستجدة، تقدِّر مصر وتؤيد بشدة التوصية الواردة في القرار ٢٧/٧٣ الذي أُنشئ بموجبه فريقٌ عامل مفتوح العضوية، يستند في عمله إلى توافق الآراء، ليواصل، على سبيل الأولوية، صقل قواعد ومعايير ومبادئ السلوك المسؤول للدول بهدف جعل عملية الأمم المتحدة التفاوضية بشأن الأمن في استخدام تكنولوجيات المعلومات والاتصالات أكثر ديمقراطية وشمولية وشفافية. وعلاوة على ذلك، تتطلع مصر إلى الانضمام إلى جهود الفريق العامل المفتوح العضوية ودعمها لابتداع السبل الكفيلة بتنفيذ هذه القواعد والمعايير وتدابير بناء الثقة.

وتتطلع مصر أيضاً إلى المشاركة في أنشطة فريق الخبراء الحكوميين المنشأ عملا بالقرار ٧٣/٢٦٦، بما في ذلك أنشطة التعاون مع المنظمات الإقليمية ذات الصلة بالموضوع من خلال سلسلة من المشاورات.

فرنسا

[الأصل: بالفرنسية]
[١٤ أيار/مايو ٢٠١٩]

١ - التقييم العام لمسائل أمن الفضاء الإلكتروني

تود فرنسا أن تذكّر أولا بأنها لا تستخدم مصطلح ”أمن المعلومات“ وتفضل استخدام مصطلح ”أمن نظم المعلومات“ أو ”أمن الفضاء الإلكتروني“. والواقع أن فرنسا، التي تعمل بهمة في مجال تعزيز حرية التعبير على شبكة الإنترنت (كما يتبين من مشاركتها في تقديم قرار مجلس حقوق الإنسان ٣٨/٧ في عام ٢٠١٨)، لا تعتبر المعلومات في حد ذاتها عاملَ ضعفٍ يتعين الحماية منه، بقطع النظر عن التدابير التي يمكن اتخاذها بطريقة متناسبة وشفافة وفي ظل الشروط التي يحددها القانون بدقة طبقا للمادة ١٩ من العهد الدولي الخاص بالحقوق المدنية والسياسية.

ومن ثم، فإن مصطلح ”أمن الفضاء الإلكتروني“ يتسم بدقة أكبر لدلالته على قدرة أي نظام للمعلومات على تحمل أحداث يكون مصدرها الفضاء الإلكتروني ويكون من شأنها أن تعرض للخطر إتاحة البيانات المخزَّنة، المعالج منها أو المنقول، أو سلامتها أو سريتها والخدمات التبعية التي تقدمها هذه النظم أو تيسِّر الحصول عليها. ويُستعان في أمن الفضاء الإلكتروني بتقنيات أمن نظم المعلومات، كما أنه يقوم على مكافحة جرائم الفضاء الإلكتروني وعلى إقامة نظام للدفاع عن الفضاء الإلكتروني.

وترى فرنسا أن الفضاء الرقمي يجب أن يظل مجالا للحرية والتبادل والنمو، وأن تحقيق الازدهار والتقدم في مجتمعاتنا مشروط بذلك. وتذهب فرنسا، على نحو ما أكدته من قبلُ في استراتيجيتها الوطنية للأمن الرقمي[(١)] في عام ٢٠١٥، إلى أن ”تكنولوجيا المعلومات والاتصالات عامل من عوامل الابتكار لأنها تجلب الجديد من الاستخدامات والخدمات. وهي تُنشئ طفرة في معظم المهن، وتحدث تحولا في قطاعات الأنشطة والشركات بحيث تجعلها أكثر مرونة وتنافسية“. وتتيح تلك التكنولوجيا لأفراد أي مجتمع فرصا لكي يحسنوا عيشهم اليومي بفضل خدمات الاتصال والتجارة والمعلومات عبر الإنترنت، كما تتيح فرصا اقتصادية بفضل زيادة المنافسة أو الاقتصاد التعاوني.

وهذا الفضاء الإلكتروني المفتوح والآمن والمستقر والميسَّر والسلمي، الذي يتيح فرصا اقتصادية وسياسية واجتماعية، والذي ما فتئت فرنسا تروّج له خلال العقود الثلاثة الماضية، يتعرض حاليا للخطر من جراء ممارسات مستجدة مدمِّرة تنشأ فيه. والواقع أن خصائص الفضاء الإلكتروني (سرية الهوية النسبية، وانخفاض التكاليف وسهولة الوصول إلى الأدوات الضارة، وسهولة التنفيذ، وتكاثر النقائص الأمنية، وما إلى ذلك من الخصائص) تمكِّن العديد من الجهات الفاعلة من تطوير ترسانة رقمية تُستخدم لأغراض التجسس والاتجار غير المشروع وزعزعة الاستقرار والتخريب. وبعض التهديدات ذات المستوى المنخفض لا يدخل ضمن مسائل الأمن القومي بل يتعلق بشكل من أشكال الجريمة، لكن استخدام

(١) متاح على الرابط التالي: www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf.

الأسلحة الإلكترونية ضد النظم الإلكترونية الخاصة بالدولة أو البنى التحتية الحيوية أو المؤسسات الكبرى قد يفضي إلى عواقب وخيمة.

وقد أصبحت تحديات أمن الفضاء الإلكتروني جزءً لا يتجزأ من استراتيجيات فرض القوة وعلاقات تجاذب القوى التي تحكم العلاقات الدولية؛ والأمر إنما يتعلق هنا بمسألة ذات أولوية وبرهان سياسي من الدرجة الأولى. وعلى نحو ما يُشدَّد عليه في الاستعراض الاستراتيجي للدفاع والأمن القومي لعام ٢٠١٧[٢]، فإن ''الرقمنة الواسعة النطاق التي تشهدها مجتمعاتنا منذ عقد من الزمان والترابط العالمي لنظم المعلومات والاتصالات يُنشئان تهديدات جديدة وفرصا جديدة على السواء. فهُما يتيحان للجميع أدوات قوية للتعبير والتأثير والدعاية والاستخبارات، وحجما هائلا من البيانات، ولكنهما يتيحان أيضا وسائل هجوم مهولة. وهما يمكِّنان لبروز جهات فاعلة جديدة في القطاع الخاص، تفرض نفسها على الساحة الدولية كتحدٍّ لسيادة الدول، ولكن أيضا كشركاء أساسيين في بعض الأحيان. ويحدثان بحكم الواقع تحولا في علاقات القوة بين الجهات الفاعلة الحكومية والجهات الفاعلة غير الحكومية والقطاع الخاص''.

ونحن نتحمل جميعا قسطا من المسؤولية عن الحفاظ على الفضاء الإلكتروني مفتوحا وآمنا ومستقرا وميسَّرا وسلميا، وعن تطويره وتعزيزه. وفي مواجهة التهديدات المشتركة التي تؤثر على الاستقرار والأمن الدوليين، ظلت فرنسا منذ سنين عديدة تنتهج سياسة ودبلوماسية نشطتين ابتغاء تعزيز أمن الفضاء الإلكتروني واستقراره والثقة فيه.

٢ - الجهود المبذولة لتعزيز أمن الفضاء الإلكتروني القومي وتشجيع التعاون الدولي في هذا الميدان

(أ) تعزيز الإجراءات الفرنسية في مجال أمن الفضاء الإلكتروني

ظلت التوجهات الاستراتيجية التي اتُّبعت في السنوات الأخيرة على أعلى مستوى في الدولة الفرنسية تعتبر أمن الفضاء الإلكتروني من أولويات العمل الحكومي.

وتواصل فرنسا تعزيز إجراءاتها الوطنية وتعميق نضجها. واستمراريةً للتدابير التي اتُّخذت منذ عقد من الزمان (إنشاء وتعزيز الوكالة الوطنية لأمن نظم المعلومات منذ عام ٢٠٠٩، ووضع أول استراتيجية فرنسية للدفاع وأمن نظم المعلومات في شباط/فبراير ٢٠١١، وتعزيز الأدوات القانونية والزيادة الكبيرة في الموارد المخصصة لأمن الفضاء الإلكتروني بموجب أحدث القوانين المتعلقة بالبرمجة العسكرية، ونشر وزارة شؤون الجيش ''ميثاق الدفاع عن الفضاء الإلكتروني'' في شباط/فبراير ٢٠١٤، وإنشاء ''مركز التميّز في مجال الفضاء الإلكتروني'' للمضي في تحفيز تطوير التدريب والبحث الأكاديمي والقاعدة الصناعية والتكنولوجية لأمن الفضاء الإلكتروني)، تتبع فرنسا أيضا سياسة لتحقيق الشفافية بشأن استراتيجيتها الوطنية والدولية على السواء.

وبالفعل، اعتمدت فرنسا في عام ٢٠١٥ استراتيجية وطنية للأمن الرقمي تروم مواكبة التحول الرقمي للمجتمع الفرنسي. وفي مجال الأمن، تبرز الاستراتيجية مساهمة التصدي القوي لأعمال المراقبة الإلكترونية وتتوخى جعل الأمن الرقمي ميزة تنافسية للشركات الفرنسية.

(٢) متاح على الرابط التالي: www.defense.gouv.fr/dgris/presentation/evenements-archives/revue-strategique-de-defense-et-de-securite-nationale-2017.

وفي كانون الأول/ديسمبر ٢٠١٧، جاءت استراتيجية فرنسا الدولية المعنية بتكنولوجيا المعلومات والاتصالات[٣] لتكملة تلك الوثيقة مع تحديد المبادئ والأهداف التي تتوخاها فرنسا في المجال الرقمي على الصعيد الدولي. وبناءً على ثلاثة محاور كبرى (الحوكمة والاقتصاد والأمن)، تروم هذه الاستراتيجية ما يلي:

- تعزيز عالم رقمي مفتوح ومتنوع وموثوق به عالميا؛
- تدعيم نموذج أوروبي للتوازن بين النمو الاقتصادي والحقوق والحريات الأساسية والأمن؛
- تعزيز تأثير فرنسا وجهاتها الفاعلة في العالم الرقمي وجاذبيتها وأمنها ومواقعها التجارية.

ويحدد الاستعراض الاستراتيجي للدفاع عن الفضاء الإلكتروني[٤] الذي قُدم في شباط/فبراير ٢٠١٨ عقيدةً لإدارة الأزمات الإلكترونية، ويوضح الأهداف الاستراتيجية الوطنية في مجال الدفاع عن الفضاء الإلكتروني. ويؤكد الاستعراض أهمية النموذج الفرنسي والمسؤولية الرئيسية التي تقع على عاتق الدولة في مجال أمن الفضاء الإلكتروني، ويتمحور حول سبعة مبادئ رئيسية هي:

- تحسين حماية نظم المعلومات في بلدنا؛
- إحباط الهجمات بفضل مجموعة من التدابير الدفاعية والمتعلقة بتعزيز القدرة على الصمود وبقدرات الصدّ والرد؛
- تأكيد السيادة الرقمية لفرنسا وممارستها؛
- زيادة فعالية التصدي الجنائي لجرائم الفضاء الإلكتروني؛
- تعزيز ثقافة تشاركية لأمن المعلومات؛
- المشاركة في تطوير تكنولوجيا المعلومات والاتصالات في أوروبا، بما يجعلها مأمونة وموثوقة؛
- اتخاذ إجراءات دولية لتحقيق الحوكمة الجماعية والمتحكم فيها للفضاء الإلكتروني.

وينص قانون البرمجة العسكرية للفترة ٢٠١٩-٢٠٢٥[٥]، استمراريةً لما سبقه من قوانين، على زيادة كبيرة في الموارد المخصصة للدفاع عن الفضاء الإلكتروني، ولا سيما من حيث مستوى الملاك الوظيفي، مع تحديد هدف يتمثل في تجنيد ١ ٥٠٠ فرد إضافيين، بغية الوصول إلى عدد للأفراد المكرَّسين لمواجهة مثل هذه التحديات في وزارة شؤون الجيش بحلول عام ٢٠٢٥، وهو ٤ ٠٠٠ فرد.

وتساهم الجهات الفاعلة التالية في تحقيق فعالية الإجراءات التقنية والعملياتية الفرنسية:

- الوكالة الوطنية لأمن نظم المعلومات التي تتولى المسؤولية عن الوقاية (بما يشمل وضع المعايير) من الحوادث المعلوماتية التي تستهدف الدولة ومقدمي خدمات الاتصالات ذوي الأهمية الحيوية وعن الرد على تلك الحوادث. ويعمل في الوكالة حاليا ٦٠٠ موظف، وهي آخذة في النمو. وقد

(٣) متاح على الرابط التالي: www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf.

(٤) متاح على الرابط التالي: www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf.

(٥) متاح على الرابط التالي: www.legifrance.gouv.fr/eli/loi/2018/7/13/ARMX1800503L/jo/texte.

فرضت نفسها كجهة مرجعية في مجال تحديد المعايير ذات الصلة الوثقى بأمن الفضاء الإلكتروني.

- وزارة شؤون الجيش التي تتولى المهمة المزدوجة المتمثلة في ضمان حماية الشبكات التي تتيح لها إنجاز عملها ودمج عمليات الفضاء الإلكتروني في صميم العمل العسكري. وتوطيدا لعمل الوزارة في هذا الميدان، عُيِّن في أيلول/سبتمبر ٢٠١٧ لواءٌ قائدٌ لشؤون الدفاع عن الفضاء الإلكتروني، تحت إمرة رئيس أركان الدفاع. وفي هذا الصدد، أصدرت وزارة شؤون الجيش في أوائل عام ٢٠١٩ سياسة المكافحة الإلكترونية الدفاعية؛ وقدم رئيس أركان الدفاع بالتزامن مع ذلك أول إفصاح عن عقيدة العمليات العسكرية في ما يتعلق بالمكافحة الإلكترونية الهجومية.
- وزارة الداخلية ووزارة العدل اللتان تتوليان مهمة مكافحة جميع أشكال جرائم الفضاء الإلكتروني التي تستهدف المؤسسات والمصالح الوطنية والجهات الفاعلة الاقتصادية وسلطات الجماعات المحلية والأفراد.

(ب) تعزيز التعاون الدولي تحقيقا لاستقرار وأمن الفضاء الإلكتروني

إن تعزيز الاستقرار الاستراتيجي والأمن الدولي في ما يتعلق بالفضاء الإلكتروني من الأهداف ذات الأولوية بالنسبة لفرنسا. وعلى نحو ما جاء في الاستعراض الاستراتيجي للدفاع عن الفضاء الإلكتروني، فإن ''التعاون الدولي في مجال الفضاء الإلكتروني وسيلة فعالة لتعزيز الاستقرار من خلال معرفة الجهات الفاعلة بعضها بعضا، بل وبث مزيد من الثقة في ما بينها، ومن خلال إنشاء آليات تُعنى بالإدارة المشتركة للأزمات وبالاتصالات وتخفيف التوتر''. والإجراءات التي تتخذها فرنسا في مجال تعزيز التعاون الدولي بشأن تحديات أمن الفضاء الإلكتروني تتم في إطار أوروبي ودولي.

منع الأزمات بتعزيز جهود التعاون وتنمية القدرات

ترى فرنسا أن الهدف الأول الذي يُتوخى من إجراءاتها المتخذة في ما يتعلق بالفضاء الإلكتروني هو منع الأزمات. ولذلك، فعلى نحو ما أُبرز في الاستعراض الاستراتيجي للدفاع عن الفضاء الإلكتروني، ''يسهم تعزيز الحماية والقدرة على الصمود وتعاون جميع الجهات الفاعلة في الفضاء الإلكتروني إسهاما مباشرا في تعزيز أمننا القومي''. وتحقيق هذا المبتغى يمر عبر تقوية التعاون التقني والعملياتي والهيكلي مع الشركاء الحكوميين والمنظمات الدولية ابتغاء تطوير قدرات كل من هذه الجهات الفاعلة المختلفة وتحقيق قدرة الفضاء الإلكتروني على الصمود عالميا.

وفي الواقع، ترى فرنسا أنه، بسبب الترابط الذي تتسم به الشبكات والمجتمعات، لن يتم ضمان أمن الفضاء الإلكتروني للجميع إلا عندما تتوافر كل دولة على ما يكفي من القدرات لحماية نظم معلوماتها. ولذلك تبذل فرنسا قصارى جهدها من أجل تعزيز قدرات شركائها في مجال أمن الفضاء الإلكتروني، في إطار مبادرات ثنائية أو متعددة الأطراف. وعلاوة على ذلك، فمثل هذا الاستثمار في التعاون يفيد الأطراف كافة، فهو يتيح لنا مواكبة أحدث التطورات من خلال التنافس مع أقراننا والتعلم منهم، وهذا إثراء متبادل للمعارف والدراية التقنية، كما يتيح بث الثقة بين الجهات الفاعلة المعنية.

وعلى المستوى التقني، تواصل الوكالة الوطنية لأمن نظم المعلومات إقامة شراكات مع نظرائها في العديد من البلدان للنهوض بتبادل المعلومات الأساسية، مثل المعلومات عن النقائص الأمنية أو الثغرات

في المنتجات والخدمات. وبالإضافة إلى ذلك، يعمل المركز الحكومي للمراقبة والإنذار والرد على الهجمات الإلكترونية التابع للوكالة بفعالية في إطار عدة شبكات متعددة الأطراف (منتدى فرق التصدي للحوادث والأمن، وفرقة العمل الأوروبية لمراكز التصدي لحوادث أمن المعلومات، ومجموعة المراكز الحكومية الأوروبية للتصدي لحوادث أمن المعلومات، وشبكة مراكز التصدي لحوادث أمن المعلومات التابعة للاتحاد الأوروبي) يقيم بفضلها علاقات مع مراكز التصدي للطوارئ المعلوماتية في جميع أنحاء العالم.

وفي ما يتعلق بالتعاون العملياتي والهيكلي، تتبع فرنسا سياسة استباقية. ففي السنوات الأخيرة، نشرت فرنسا ضمن قوات الأمن الداخلي في بلدان شريكة خبراء تقنيين دوليين في مجال أمن الفضاء الإلكتروني. وتواصل فرنسا أيضا العمل مع السنغال لبدء الأنشطة الإقليمية لمدرسة داكار الوطنية لأمن الفضاء الإلكتروني التي دُشنت في نهاية عام ٢٠١٨. ويروم هذا المشروع تنظيم دورات تدريبية قصيرة المدة وقابلة للتكييف لفائدة أخصائيي أمن الفضاء الإلكتروني وكبار المسؤولين من غرب أفريقيا، على سبيل الأولوية.

وعلى مستوى الاتحاد الأوروبي، فتوخيا لتعزيز قدرة النظم الإلكترونية على الصمود في المنطقة الأوروبية، تساهم فرنسا في وضع إطار تطوعي للتعاون بغرض منع وقوع الحوادث وإيجاد حلول لها. ويقوم هذا الإطار على وجه الخصوص على وضع المعايير العملياتية والإجراءات المشتركة للتعاون بين الشركاء، التي تخضع للاختبار في عمليات البلدان الأوروبية. وشاركت فرنسا أيضا في إعداد ''مجموعة أدوات إلكترونية'' تتيح إطارا أوروبيا للتصدي الدبلوماسي المشترك لأي هجوم إلكتروني، وتستند إلى استخدام تدابير الوقاية والتعاون وتحقيق الاستقرار.

وبذلت فرنسا أيضا قصارى جهدها لاعتماد تقنين أوروبي يأخذ في الاعتبار متطلبات التنافسية والإمكانات التي تتيحها تكنولوجيا المعلومات والاتصالات، مع الاستمرار في حماية المواطنين والشركات والدول الأعضاء (الحق في الخصوصية وحماية البيانات الشخصية، وحماية البنية التحتية الحيوية، ومكافحة المحتوى الإرهابي على شبكة الإنترنت). ويتضح ذلك من اعتماد لائحة البرلمان الأوروبي والمجلس الأوروبي رقم 2016/679 (UE) المؤرخة ٢٧ نيسان/أبريل ٢٠١٦ والمتعلقة بحماية الأشخاص الطبيعيين في ما يتصل بمعالجة البيانات الشخصية وبحرية تداول هذه البيانات، والأمر التوجيهي من البرلمان الأوروبي والمجلس الأوروبي رقم 2016/1148 (UE) المؤرخ ٦ تموز/يوليه ٢٠١٦ والمتعلق بإجراءات ضمان مستوى عال مشترك من أمن الشبكات ونظم المعلومات في الاتحاد الأوروبي، كما يتضح من بدء النفاذ الوشيك للائحة البرلمان الأوروبي والمجلس الأوروبي رقم 2019/881 (UE) المؤرخة ١٧ نيسان/أبريل ٢٠١٩ والمتعلقة بوكالة الاتحاد الأوروبي لأمن الفضاء الإلكتروني وبإصدار شهادات سلامة تكنولوجيات المعلومات والاتصالات من حيث أمن الفضاء الإلكتروني، التي تلغي اللائحة رقم No°526/2013 (UE) (اللائحة المتعلقة بأمن الفضاء الإلكتروني). وتدعم فرنسا أيضا بشكل فعال اعتماد لائحة أوروبية تتوخى منع نشر المحتوى الإرهابي على شبكة الإنترنت وفرض التزامات موحَّدة على مقدمي خدمات الإنترنت.

وأخيرا، تعمل فرنسا على جعل السياسة الصناعية في الاتحاد الأوروبي داعمة للقدرات في مجال البحث والتطوير المتقدمين دعما لنشر تكنولوجيا وخدمات المعلومات والاتصالات الموثوق في أمنها والخاضعة للتقييم.

وفي إطار منظمة حلف شمال الأطلسي، اعتمد الحلفاء بمبادرة من فرنسا تعهدا بالدفاع عن الفضاء الإلكتروني، وذلك في مؤتمر قمة وارسو في حزيران/يونيه ٢٠١٦. ويكفل هذا التعهد التأكد من تكريس كل دولة عضو في منظمة حلف شمال الأطلسي حصة مناسبة من مواردها لتعزيز قدراتها المتعلقة بالدفاع عن الفضاء الإلكتروني، ومن ثم رفع المستوى العام لأمن الدول الأعضاء كافة. وفي أيار/مايو ٢٠١٨، استضافت فرنسا المؤتمر الأول من نوعه المكرَّس لهذا التعهد. وعلاوة على ذلك، فقد أقر الحلفاء بأن الفضاء الإلكتروني ميدان للعمليات، مما يلزم منظمة حلف شمال الأطلسي بالدفاع عن نفسها فيه، تماما كما تفعل برا وجوا وبحرا.

منع الأزمات من خلال وضع معايير تنظم سلوك الجهات الفاعلة في مجال الفضاء الإلكتروني

ترى فرنسا أن وضع إطار لأمن الفضاء الإلكتروني الجماعي لا يمكن أن ينبني إلا على التوازنات التي يحددها القانون الدولي. وعلاوة على ذلك، فكما هو مشدد عليه في الاستراتيجية الفرنسية الدولية لتكنولوجيا المعلومات والاتصالات، تولي فرنسا أهمية للمضي في إجراء ”حوار تعاوني مع جميع من يعنيهم الأمر من أصحاب المصلحة من القطاعين العام والخاص، ومع كافة الشركاء الدوليين الذين يبدون استعدادهم لذلك، على المستويين الثنائي والمتعدد الأطراف معا“.

وقد اضطلعت فرنسا بدور فعال في المفاوضات التي جرت داخل منظمة الأمم المتحدة في إطار الاجتماعات الخمسة الأخيرة لفريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي. وستواصل مشاركتها في المناقشات المستأنفة سواء في فريق الخبراء الحكوميين أو في الفريق العامل المفتوح باب العضوية لكي تمدهما برؤيتها التي تتعلق بفضاء إلكتروني تسوده الحرية والتبادل ويتوخى تحقيق النمو، بما يسهم في رخاء مجتمعاتنا وتقدمها. وهي تشارك أيضا في المحافل الدولية الأخرى التي تعالج فيها هذه المسائل المتصلة بأمن الفضاء الإلكتروني.

وقد صدَّقت فرنسا على الاتفاقية المتعلقة بالجريمة الإلكترونية في عام ٢٠٠٦، التي تتيح الأساس القانوني لتحديد شتى المخالفات المتصلة بمكافحة جرائم الفضاء الإلكتروني، وتنص على وسائل حديثة ومرنة للتعاون الدولي في هذا الميدان (مثلا إنشاء شبكة تعمل على مدار الساعة من أجل تسريع إجراءات المساعدة المتبادلة بين الدول الأطراف). وتدافع فرنسا حاليا على تحقيق عالمية الاتفاقية التي يبلغ عدد الدول الأطراف فيها حتى الآن ٦٣ دولة طرفا من جميع القارات. وهي تشارك بفعالية في التفاوض على البروتوكول الإضافي الثاني الملحق بالاتفاقية، الذي يسعى إلى زيادة تعزيز التعاون الدولي في هذا الميدان بتطوير التعاون بين أجهزة الشرطة وتبادل المساعدة في المسائل الجنائية، وخاصة في ما يتعلق بتحصيل الأدلة الإلكترونية. وتدعم فرنسا كذلك أعمال فريق الخبراء الحكومي المعني بإجراء دراسة شاملة عن مشكلة الجريمة السيبرانية، وهي الأعمال التي تؤكد الدور المحوري الذي يضطلع به مكتب الأمم المتحدة المعني بالمخدرات والجريمة في هذا المجال.

ونداء باريس من أجل بث الثقة في الفضاء الإلكتروني وجعله آمنا[٦]، الذي عرضه رئيس الجمهورية في منتدى حوكمة الإنترنت الذي عقدته منظمة الأمم المتحدة للتربية والعلم والثقافة في ١٢ تشرين الثاني/نوفمبر ٢٠١٨، يبرهن على الدور الفعال الذي تضطلع به فرنسا في الترويج لجعل

(٦) متاح على الرابط التالي: www.diplomatie.gouv.fr/IMG/pdf/texte_appel_de_paris_-_fr_cle0d3c69.pdf.

الفضاء الإلكتروني آمنا ومستقرا ومفتوحا. وهذا النص، الذي يحظى حتى الآن بدعم ٦٦ بلدا وما يناهز ٥٠٠ كيان غير حكومي، يبتغي تعزيز بعض المبادئ الأساسية لتنظيم الفضاء الإلكتروني، ومنها مثلا إعمال القانون الدولي وحقوق الإنسان في الفضاء الإلكتروني، والسلوك المسؤول للدول، واحتكار الدولة لسلطة العنف المشروع، والإقرار بالمسؤوليات المحددة للجهات الفاعلة الخاصة.

وبذلت فرنسا أيضا جهودا هامة في إطار منظمة التعاون والتنمية في الميدان الاقتصادي. فقد عملت على تنظيم أول اجتماع للمنتدى العالمي لمنظمة التعاون والتنمية في الميدان الاقتصادي المعني بتسخير الأمن الرقمي لتحقيق الازدهار في كانون الأول/ديسمبر ٢٠١٨ بشأن موضوع مسؤولية الجهات الفاعلة في القطاع الخاص في مجال أمن الفضاء الإلكتروني.

وفي إطار مجموعة الدول السبع، مهدت مجموعة إيسي – شيما المعنية بمسائل الفضاء الإلكتروني، والمنشأة في عام ٢٠١٦، السبيل لكي يُعتمد في عام ٢٠١٧ إعلان طموح أطلق عليه اسم ”إعلان لوكا“، يتعلق بقواعد السلوك المسؤول للدول في الفضاء الإلكتروني. وفي آذار/مارس ٢٠١٩، اقترحت فرنسا، إبان فترة رئاستها، إنشاء آلية لمتابعة تنفيذ المعايير والتوصيات المعتمدة في منظمة الأمم المتحدة، وهو ما وُثِّق رسميا في إعلان دينار بشأن مبادرة معايير الفضاء الإلكتروني[٧].

وفي إطار مجموعة العشرين، تسعى فرنسا إلى ضمان أن تتناول الأعمال القضايا الأساسية المتعلقة بالمنافسة في الاقتصاد الرقمي، والأنماط الجديدة للتنظيم والحوكمة، والأمن الرقمي، بما يتمشى ونداء باريس.

وفرنسا، إذ تشارك بفعالية في الفريق العامل غير الرسمي التابع لمنظمة الأمن والتعاون في أوروبا المعني بأمن الفضاء الإلكتروني، تواصل الترويج لتنفيذ تدابير بناء الثقة الستة عشر التي وضعتها تلك المنظمة بشأن تحديات الفضاء الإلكتروني. وتقود فرنسا على وجه الخصوص مشروعا تجريبيا لتنفيذ تدبير لبناء الثقة يتعلق بجعل البنية التحتية الحيوية آمنة.

وبغية تعزيز مكافحة انتشار التقنيات والأدوات الضارة، أيدت فرنسا إدراج برمجيات الاختراق على قائمة السلع المزدوجة الاستخدام الواردة في ترتيب فاسنار بشأن ضوابط تصدير الأسلحة التقليدية والسلع والتكنولوجيات المزدوجة الاستخدام. وتعتقد فرنسا أنه يجب المضي في بذل الجهود التنظيمية في هذا الاتجاه، وذلك بإدراج بعض الأدوات المعلوماتية، التي تصنف حسب خطورة أضرارها، على قائمة المعدات الحربية.

وتستصوب فرنسا تناول العديد من قضايا أمن الفضاء الإلكتروني باتباع نهج قائم على تعدد أصحاب المصلحة لكي يُؤخذ في الاعتبار ما يحدَّد للجهات الفاعلة غير الحكومية من دور ومسؤوليات. ومن هذا المنطلق، قدمت فرنسا الدعم لأنشطة اللجنة العالمية المعنية باستقرار الفضاء الإلكتروني. وتروم هذه اللجنة وضع مقترحات لمعايير وسياسات مخصصة لتعزيز الأمن والاستقرار الدوليين وتوجيه سلوك الدول المسؤول في الفضاء الإلكتروني.

(٧) متاح على الرابط التالي: www.diplomatie.gouv.fr/IMG/pdf/g7_-_declaration_de_dinard_sur_l_initative_pour_des_normes_dans_le_cyberespace_cle8a8313.pdf.

٣ - المفاهيم الدولية ذات الصلة الرامية إلى تعزيز أمن الفضاء الإلكتروني عالميا

(أ) المفاهيم التي تمكّن من صون السلم والأمن الدوليين

لكفالة جعل الفضاء الإلكتروني مفتوحا وآمنا ومستقر وميسَّرا وسلميا، تؤكد فرنسا من جديد تمسكها بانطباق القانون الدولي، بما في ذلك ميثاق الأمم المتحدة كاملا والقانون الدولي الإنساني والقانون الدولي لحقوق الإنسان، على استخدام الدول لتكنولوجيا المعلومات والاتصالات.

القانون الدولي العام

على نحو ما استنتجه فريق الخبراء الحكوميين التابع للأمم المتحدة المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، في تقريره الذي نُشر عام ٢٠١٣، تنطبق مبادئ وقواعد القانون الدولي على سلوك الدول في الفضاء الإلكتروني. فالفضاء الإلكتروني له خصائصه المميزة (سرية الهوية ودور الجهات الفاعلة الخاصة)، لكن القانون الدولي يتيح الوسائل اللازمة لتنظيم سلوك الدول بطريقة مسؤولة في هذه البيئة. وفي هذا الصدد، لا يمكن أن يشكل هذا النقص في تأصيل الانطباق عقبة لا تُتجاوز أمام تطبيق القانون الدولي القائم.

وينطبق مبدأ السيادة على الفضاء الإلكتروني. وفي هذا الصدد، تؤكد فرنسا من جديد أنها تمارس سيادتها على نظم المعلومات وعلى الأشخاص والأنشطة الإلكترونية على أراضيها، في حدود التزاماتها بموجب القانون الدولي. ومن شأن الاختراق غير المأذون به للنظم الفرنسية أو إحداث آثار على الأراضي الفرنسية بوسائل إلكترونية من قبل كيان حكومي أو جهات فاعلة غير حكومية تعمل بتعليمات من إحدى الدول أو تخضع لسيطرتها أن يشكلا انتهاكا للسيادة.

ونطاق التدابير التي يمكن أن تتخذها الدول للرد على أي هجوم إلكتروني قد تتعرض له مشروط بدرجة خطورة هذا الهجوم. فكلما كان الهجوم الإلكتروني خطيرا اتسع نطاق التدابير. ويمكن اعتبار أي عملية إلكترونية استخداما للقوة محظورا بموجب الفقرة ٤ من المادة ٢ من ميثاق الأمم المتحدة. وإنّ تجاوز حد استخدام القوة ليس مشروطا بالوسيلة الإلكترونية المستخدمة، وإنما يتوقف على آثار العملية الإلكترونية. فإذا ماثلت هذه الآثار تلك الناتجة عن استخدام الأسلحة التقليدية، فقد تُعتبر العملية الإلكترونية بمثابة استخدام للقوة. وترى فرنسا أن الهجوم الإلكتروني الكبير الذي تشنه دولة أو جهات فاعلة غير حكومية تتصرف وهي خاضعة لسيطرة دولة ما أو بتعليمات منها، والذي يبلغ نطاقه أو آثاره درجة كافية من الخطورة (مثلا الخسائر الكبيرة في الأرواح، والأضرار المادية الكبيرة، والإضرار بالبنية التحتية الحيوية ذي العواقب الوخيمة)، والذي قد يُعزى إلى دولة ما، يمكن أن يشكل ''عدوانا مسلحا'' بالمعنى المقصود في المادة ٥١ من الميثاق، ومن ثم يمكنه أن يبرر الاعتداد بالدفاع عن النفس. ويجوز تنفيذ هذا الدفاع عن النفس بالوسائل التقليدية أو الإلكترونية شريطة احترام مبدأي الضرورة والتناسب. وتوصيف الهجوم الإلكتروني بأنه ''عدوان مسلح''، بالمعنى المقصود في المادة ٥١ من الميثاق، يرتبط بقرار سياسي يُتَّخذ على أساس كل حالة على حدة وفي ضوء المعايير المحددة في القانون الدولي.

وترى فرنسا أن وضع صك دولي جديد ملزم قانونا ومكرَّس لتحديات الفضاء الإلكتروني ليس ضروريا، في هذه المرحلة. فالقانون الدولي القائم ينطبق على الفضاء الإلكتروني كما ينطبق على مجالات أخرى، واحترامه واجب.

القانون الدولي الإنساني

تؤيد فرنسا انطباق القانون الدولي الإنساني على العمليات الإلكترونية التي تتم في سياق النزاعات المسلحة أو في ما يتعلق بها.

وفي الوقت الراهن، هناك تلازم بين عمليات المكافحة الإلكترونية الهجومية والعمليات العسكرية التقليدية. ولا يمكن، من حيث المبدأ، استبعاد فرضية نشوب نزاع مسلح ينطوي حصريا على أنشطة رقمية، ولكن هذه الفرضية تستند إلى قدرة العمليات الإلكترونية على بلوغ مستوى العنف المطلوب لكي تُعطاها صفة النزاع المسلح الدولي أو غير الدولي.

وهذه العمليات، رغم اتسامها بطابع غير مادي، تظل خاضعة للنطاق الجغرافي الذي ينطبق فيه القانون الدولي الإنساني، أي أن آثارها تقتصر على أراضي الدول الأطراف في النزاع المسلح الدولي أو في الأراضي التي تحدث فيها الأعمال العدائية في إطار نزاع مسلح غير دولي.

وتخضع عمليات المكافحة الإلكترونية الهجومية التي تنفذها القوات المسلحة الفرنسية لاحترام مبادئ القانون الدولي الإنساني، بما يشمل ما يلي:

- **مبدأ التمييز بين الأعيان المدنية والأهداف العسكرية**. من هذا المنظور، تُحظر الهجمات الإلكترونية غير الموجهة ضد هدف عسكري محدد أو تلك التي تنفَّذ بواسطة أسلحة إلكترونية لا يمكن توجيهها ضد هدف عسكري محدد. وفي هذا الصدد، قد تشكل بعض بيانات المحتوى، رغم أنها غير ملموسة من حيث طابعها، أعيانا مدنية محمية بموجب القانون الدولي الإنساني.
- **مبادئ الإنسانية**. لا يجوز كذلك أن تستهدف العمليات السكان المدنيين في حد ذاتهم أو الأشخاص المدنيين، ما لم يشاركوا مباشرة في الأعمال العدائية، على أن يكون الاستهداف، في هذه الحالة، أثناء فترة مشاركتهم تلك. وفي سياق النزاع المسلح، يجوز أن يتعرض لهجوم بالوسائل التقليدية أو الإلكترونية أي مقاتل إلكتروني تابع للقوات المسلحة، أو أي عضو في جماعة مسلحة منظمة يرتكب هجمات إلكترونية ضد طرف معاد، أو أي مدني يشارك مباشرة في الأعمال العدائية عبر وسائل إلكترونية.
- **مبدأ التناسب**. يجب أن تُنفذ العمليات مع الحرص الدائم على حماية الأشخاص المدنيين والأعيان المدنية من آثار الأعمال العدائية. ولا يجوز أن تتعدى الأضرار التبعية الميزة العسكرية الملموسة والمباشرة المتوخاة منها. ويتطلب احترام مبدأ التناسب في الفضاء الإلكتروني مراعاة جميع الآثار المتوقعة لاستخدام السلاح، سواء كانت مباشرة (مثل تضرر النظام المستهدف أو انقطاع الخدمة أو ما إلى ذلك)، أو غير مباشرة (الآثار المترتبة على البنية التحتية التي يتحكم فيها النظام المغار عليه، ولكن أيضا على الأشخاص المتضررين من الإضرار بالنظم أو تدميرها أو من تغيير بيانات المحتوى أو إتلافها) بشرط أن يكون بين تلك الآثار والهجوم علاقة سببية كافية. وهذا المبدأ يحظر أيضا استخدام الأسلحة الإلكترونية التي لا يمكن التحكم فيها (خاصة في الزمان والمكان)، أي تلك التي من شأنها أن تلحق ضررا لا يمكن إصلاحه بالبنى التحتية أو النظم أو البيانات ذات المحتوى المدني.

ويشار إلى هذه العناصر بشكل خاص في العناصر العامة للعقيدة العسكرية الفرنسية المتعلقة بالمكافحة الإلكترونية الهجومية المعروضة في أوائل عام ٢٠١٩.

حقوق الإنسان

ترى فرنسا أن الحقوق التي يتمتع بها الناس خارج شبكة الإنترنت يجب أن تحظى بالحماية نفسها على تلك الشبكة، وأن القانون الدولي لحقوق الإنسان ينطبق على الفضاء الإلكتروني. وانتشار المحتوى غير القانوني عبر الإنترنت (محتوى الإرهاب والكراهية ومعاداة السامية) يمس بهذه القيم مساسا خاصا. وتعتبر فرنسا أن من الضروري بشكل خاص إشراك الجهات الفاعلة الخاصة في مجال تكنولوجيا المعلومات والاتصالات في مكافحة المحتوى غير القانوني وتوضيح دورها ومسؤولياتها على المستوى الدولي، حتى تتسنى مكافحة هذا المحتوى وضمان حماية حقوق الإنسان والحريات الأساسية على شبكة الإنترنت.

مبدأ بذل العناية الواجبة

ترى فرنسا أن من الضروري التوصل إلى فهم مشترك على الصعيد الدولي للالتزامات التي تقع على عاتق الدولة التي قد تُستخدم بناها التحتية لأغراض ضارة، وذلك ضد مصالح دولة أخرى. والغرض من ذلك هو توضيح كيفية انطباق مبدأ بذل العناية الواجبة على الفضاء الإلكتروني، وهو المبدأ الذي ينص على أن كل دولة ملزَمة ”بعدم السماح، عن علم، باستخدام أراضيها لارتكاب أعمال تمس بحقوق دول أخرى“[(٨)]. وبناء على ذلك، يتوجب على الدول ألا تسمح، عن علم، باستخدام أراضيها لارتكاب أفعال غير مشروعة دوليا باستخدام وسائل إلكترونية، وألا تستخدم الوسطاء غير الحكوميين (الوكلاء) في ارتكاب انتهاكات للقانون الدولي. ومن شأن تحسين فهم كيفية انطباق هذا المبدأ على التحديات الإلكترونية أن يعزز التعاون بين الدول لحماية بعض البنى التحتية الحيوية، وأن يوقف كذلك الهجمات الإلكترونية الكبرى التي قد تمر عبر بلد ثالث.

(ب) المفهوم الذي يتيح تعزيز التعاون والثقة بين الدول

قواعد السلوك

مكنت شتى جولات المفاوضات التي أجريت في إطار فريق الخبراء الحكوميين المعني بأمن الفضاء الإلكتروني تقدما ملموسا في مجال التنظيم الدولي للفضاء الإلكتروني. ويحدد تقرير عام ٢٠١٥ ما عدده ١١ قاعدة من قواعد سلوك الدولة المسؤول في الفضاء الإلكتروني. وترى فرنسا أنه يجب على كل دولة احترام هذه القواعد ووضع آليات لتنفيذها. ويمكن أيضا أن تحدَّد مستقبلا قواعد أخرى تنطبق على سلوك الدول أو سلوك سائر الجهات الفاعلة الأخرى في الفضاء الإلكتروني.

تدابير بناء الثقة

يجب تعميق العمل في شتى المحافل والمنظمات الإقليمية بغية تطوير تدابير بناء الثقة الخاصة بقضايا أمن الفضاء الإلكتروني. وستمضي فرنسا في تشجيع شركائها على وضع إجراءات مشتركة بين

(٨) [*قضية قناة كورفو*، القرار المؤرخ ٩ نيسان/أبريل ١٩٤٩، محكمة العدل الدولية] *Affaire du Détroit de Corfou*, Arrêt du 9 avril 1949 : C.I.J., Recueil 1949, p. 4.

الوزارات يمكن استخدامها لضمان التواصل الجيد بين الدول في أوقات الأزمات. ووضع هذه الإجراءات والآليات، على أساس الشفافية والتواصل، أمر ضروري لمنع نشوب النزاعات في الفضاء الإلكتروني.

تنمية القدرات

تؤيد فرنسا الهدف المتمثل في بناء القدرات الدولية في مجال أمن الفضاء الإلكتروني. فهذه الجهود تساهم مساهمة مباشرة جدا في تعزيز أمن الجميع واستقرار الفضاء الإلكتروني. وتعتزم فرنسا الاضطلاع بدورها كاملا في هذه الجهود من خلال مبادرات بناء القدرات التي تُتَّخذ على الصُّعد الثنائي والإقليمي والمتعدد الأطراف.

(ج) دور ومسؤوليات الجهات الفاعلة غير الحكومية

النهج القائم على تعدد أصحاب المصلحة

شددت فرنسا في نداء باريس على ''ضرورة اتباع نهج معزز يقوم على تعدد أصحاب المصلحة''. وبالفعل، ترى فرنسا أن المجتمع المدني والأوساط الأكاديمية والقطاع الخاص والأوساط التقنية لديهم مهارات وموارد مفيدة لتحديد بعض الجوانب ذات الصلة بسياسات أمن الفضاء الإلكتروني.

المسؤولية الأمنية التي تقع على عاتق الجهات الفاعلة الخاصة في تصميم المنتجات الرقمية وتعهدها

إن ظهور التكنولوجيا الرقمية كأداة جديدة ومجال للمواجهة ينيط بالقطاع الخاص، ولا سيما عدد معين من الجهات الفاعلة المعنية بالنظم، دورا حاسما ومسؤولية غير مسبوقة في صون السلم والأمن الدوليين. ومن ثم ففرنسا تعترف في نداء باريس ''بمسؤوليات الجهات الفاعلة الرئيسية في القطاع الخاص في ما يتعلق ببناء الثقة في الفضاء الإلكتروني وتحقيق أمنه واستقراره'' وتشجع ''المبادرات الرامية إلى زيادة أمن العمليات والمنتجات والخدمات الرقمية''.

وترى فرنسا أن من المهم أن يُقرَّ، على المستوى الدولي، مبدأ المسؤولية الأمنية التي تقع على عاتق الجهات الفاعلة الخاصة المعنية بالنظم في تصميم منتجاتها وعملياتها وخدماتها الرقمية وتكاملها ونشرها وتعهدها على مدى دورة استخدامها وفي سلسلة توريدها، من البداية حتى النهاية.

مسؤولية المنصات الرقمية في مجال مكافحة الإرهاب

تعمل فرنسا أيضا على إخضاع الجهات الفاعلة الرقمية الخاصة للمساءلة في ما يتعلق بمكافحة إساءة استخدام خدماتها لأغراض إرهابية. وعلى وجه الخصوص، تطرح فرنسا هذا الموضوع لكي يُتناوَل في إطار مجموعة السبع والاتحاد الأوروبي، حيث تؤيد تأييدا فعالا اعتماد مشروع لائحة أوروبية تمكّن من تنظيم عمل مقدمي خدمات الإنترنت في مجال مكافحة المحتوى الإرهابي على شبكة الإنترنت. ويقضي هذا النص بسحب أي محتوى إرهابي في غضون ساعة واحدة بناءً على طلب دولة عضو، وباعتماد تدابير فعالة من قبل المنصات التي تكون عرضة لإقحام محتوى إرهابي فيها، وبالالتزام بتعيين جهة اتصال متاحة على مدار الساعة لمعالجة التنبيهات وطلبات سحب المحتوى، كما يفرض عقوبات على عدم التعاون المنهجي.

منع الأنشطة الهجومية التي تقوم بها الجهات الفاعلة الخاصة

ترى فرنسا أنه يجب على الدول أن تُبقي سلطة استخدام العنف المادي المشروع حكرا عليها، في الفضاء الإلكتروني كما في المجالات الأخرى. وتؤيد في هذا الصدد منع الجهات الفاعلة غير الحكومية، بما في ذلك في القطاع الخاص، من القيام بأنشطة هجومية في الفضاء الإلكتروني خدمة لمصالحها أو لمصالح جهات فاعلة غير حكومية أخرى. وهذه الممارسات، التي تقوم على مبدأ الدفاع الخاص عن النفس (''الاختراق المضاد'')، قد تؤدي إلى زعزعة الاستقرار بسبب ما قد يقع على طرف ثالث من آثار ضارة، كما قد تفضي إلى تصعيد محتمل بين الدول. ومن ثم، ترى فرنسا أن من الضروري أن يوضَّح هامش المناورة المتاحة للجهات الفاعلة الخاصة من حيث الرد على حادث من الحوادث.

٤ - التدابير المحتملة التي يمكن للمجتمع الدولي اتخاذها لتعزيز أمن المعلومات على الصعيد العالمي

في مواجهة التهديدات الجديدة الناشئة عن الثورة الرقمية، ترى فرنسا أن التعاون والقانون ضروريان حتى لا يصبح الفضاء الإلكتروني مجالا للنزاع المستمر. وكما هو الحال في ميادين أخرى، فإن الدول ملزمة باحترام القانون الدولي في العالم الرقمي. وبالإضافة إلى ذلك، فإن الإطار المعياري للسلوك المسؤول للدول في الفضاء الإلكتروني قد نشأ في السنوات الأخيرة، ومن ثم ينبغي أن يُعزَّز. وتعتقد فرنسا أنه، لتعزيز أمن الفضاء الإلكتروني على المستوى الدولي، يمكن اتخاذ التدابير التالية:

- **تعميق العمل المنجز خلال الاجتماعات السابقة لفريق الخبراء الحكوميين**. دون المساس بالمعايير والتوصيات التي كانت موضع توافق في الآراء في جولات التفاوض السابقة، قد يكون من المفيد توضيح السبل التي تمكّن من تنفيذ هذه المعايير والتوصيات وتحسين فهم الممارسات الجيدة، على المستوى الدولي.
- **الاستناد إلى نداء باريس من أجل بث الثقة في الفضاء الإلكتروني وجعله آمنا في المناقشات المقبلة بشأن قضايا أمن الفضاء الإلكتروني في منظمة الأمم المتحدة**. يحظى هذا الإعلان حتى الآن بتأييد أكثر من ثلث الدول الأعضاء في الأمم المتحدة وتأييد عدة مئات من الجهات الفاعلة غير الحكومية الرئيسية لرؤية مشتركة للمبادئ التي يجب أن تحكم سلوك شتى الجهات الفاعلة في الفضاء الإلكتروني.
- **تحقيق عالمية الاتفاقية المتعلقة بالجريمة الإلكترونية**. هذا الصك، الذي اعتُمد في تشرين الثاني/نوفمبر ٢٠٠١ لتعزيز التعاون الدولي في هذا الميدان، قد صدقت عليه حتى الآن ٦٣ دولة، كما أن له أثر على التشريعات الوطنية لأكثر من ثلثي الدول الأعضاء في الأمم المتحدة.
- **تشجيع الدول على البرهنة على شفافيتها**. يتصل هذا الأمر على وجه الخصوص باستراتيجيات الدول المتعلقة بأمن الفضاء الإلكتروني وبعقائدها في إدارة الأزمات السيبرانية والرد على أي هجوم إلكتروني وتفسيرها لانطباق القانون الدولي على الفضاء الإلكتروني.
- **تفعيل ما يكون قد وُضع من تدابير بناء الثقة الخاصة بقضايا الفضاء الإلكتروني في الأطر الإقليمية أو الدولية ذات الصلة.**

- **تعزيز المبادرات والآليات الرامية إلى تقاسم الممارسات الجيدة وبناء القدرات**. ينبغي أن تتوخى هذه الآليات تمكين جميع الدول من نظام فعال لأمن الفضاء الإلكتروني، بما يشمل على الخصوص الوسائل التالية:
  - وضع استراتيجية تتعلق بأمن الفضاء الإلكتروني؛
  - تحديد إطار تشريعي لتعزيز أمن الفضاء الإلكتروني ومكافحة جرائم الفضاء الإلكتروني؛
  - إنشاء مركز للتصدي للطوارئ المعلوماتية؛
  - وضع إجراءات للتعاون مع القطاع الخاص، وخاصة الشركات الكبرى العاملة في مجال التكنولوجيا الرقمية؛
  - تحديد إطار لحماية البنى التحتية الحيوية في الفضاء الإلكتروني.
- **إقرار مبدأ المسؤولية الأمنية التي تقع على عاتق الجهات الفاعلة الخاصة المعنية بالنظم، على المستوى الدولي**. تشمل هذه المسؤولية تصميم المنتجات والعمليات والخدمات الرقمية وتكاملها ونشرها وتعهدها على مدى دورة استخدامها وفي سلسلة توريدها، من البداية حتى النهاية.

اليونان

[الأصل: بالإنكليزية]
[١٥ أيار/مايو ٢٠١٩]

في كانون الأول/ديسمبر ٢٠١٨، اتخذت الجمعية العامة قراراً بشأن الارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي. ويطلب القرار إلى الأمين العام أن يلتمس آراء الدول الأعضاء وتقييماتها بشأن: (أ) الجهود المبذولة على الصعيد الوطني لتعزيز أمن المعلومات وتشجيع التعاون الدولي في هذا الميدان؛ و (ب) مضمون المفاهيم المشار إليها في تقارير فريق الخبراء الحكوميين.

وتؤيد اليونان الرأي الذي توصل إليه بتوافق الآراء فريق الخبراء الحكوميين وهو أن القانون الدولي، وبخاصة ميثاق الأمم المتحدة، ينطبق أيضاً في الفضاء الإلكتروني وأنه أساسي لصون السلام والاستقرار والتشجيع على إقامة تهيئة بيئة مفتوحة وآمنة وسلمية وميسَّرة لتكنولوجيا المعلومات والاتصالات. وتؤيد اليونان أيضاً الاستمرار في عملية مناقشة معايير السلوك المسؤول للدول، وتدابير بناء الثقة والقانون الدولي في إطار اللجنة الأولى للأمم المتحدة، وإنشاء فريق جديد للخبراء الحكوميين.

ونسلم بأن الطبيعة المترابطة والمعقدة للفضاء الإلكتروني تتطلب جهودا مشتركة من جانب الحكومات، والقطاع الخاص، والمجتمع المدني، والأوساط التقنية، والمستعملين والأوساط الأكاديمية من أجل التصدي للتحديات المواجهة وندعو جميع الجهات صاحبة المصلحة إلى التسليم بذلك وتحمُّل مسؤولياتها المحددة عن الحفاظ على فضاء إلكتروني مفتوح، وحر، وآمن ومستقر.

ونسلم أيضاً بدور الأمم المتحدة في مواصلة وضع معايير السلوك المسؤول للدول في الفضاء الإلكتروني ونذكّر بأن نتائج مناقشات فريق الخبراء الحكوميين حدّدت مجموعة من المعايير والتوصيات التي

جرى التوصل إليها بتوافق الآراء، والتي تقرها الجمعية العامة بصورة متكررة، والتي ينبغي للدول أن تتخذها أساساً لسلوك الدول المسؤول في الفضاء الإلكتروني.

ومن خلال مشاركتنا في المنظمات الدولية مثل الأمم المتحدة، والاتحاد الأوروبي، ومنظمة حلف شمال الأطلسي، ومنظمة الأمن والتعاون في أوروبا، نسعى إلى وضع قواعد ومبادئ عالمية للسلوك المسؤول للدول في استخدام الفضاء الإلكتروني، والتعاون، وتبادل الخبرات وأفضل الممارسات، والاشتراك في وضع الوسائل الملائمة للتصدي للتهديدات والتحديات المتصلة بأمن الفضاء الإلكتروني. ويسهم بلدنا إلى أقصى حد ممكن في صياغة وتنفيذ القرارات ذات الصلة المتخذة في إطار المنظمات الدولية بهدف زيادة التعاون والشفافية والحد من خطر نشوب النزاعات.

وقامت اليونان، إدراكاً منها لأن جرائم الفضاء الإلكتروني تمثل مشكلة عالمية، بتوقيع المعاهدة المتعلقة بالجريمة الإلكترونية لمجلس أوروبا، المعروفة أيضاً باسم معاهدة بودابست، والتصديق عليها. وتوفر هذه المعاهدة إطاراً مهماً لاعتماد تشريعاتنا الوطنية وللتعاون الدولي في مجال مكافحة الجريمة الإلكترونية على السواء. وجرى التصديق على المعاهدة بموجب القانون ٢٠١٦/٤٤١١. وأيضاً في إطار مشاركتنا في منظمة الأمن والتعاون في أوروبا، وقع بلدنا اتفاق تدابير بناء الثقة، الرامي إلى تعاون الدول الأعضاء بشأن مسائل أمن الفضاء الإلكتروني والشفافية والاستقرار والحد من خطر المواجهة في الفضاء الإلكتروني.

وفي إطار التزامات الاتحاد الأوروبي، أدمجت اليونان في تشريعاتها الوطنية التوجيه ١١٤٨ بشأن أمن الشبكات ونظم المعلومات، المعروف أيضا باسم ''NIS Directive''، الذي يشمل تدابير تهدف إلى تحقيق مستوى مشترك مرتفع من الأمن في جميع أنحاء الاتحاد، من خلال تنفيذ تدابير أمن الفضاء الإلكتروني، وإعداد استراتيجية وطنية وتعزيز التعاون بين الدول الأعضاء. ونتيجة لذلك، تتعزز حماية جميع البنى التحتية الحيوية في بلدنا، في حين تصان مبادئ المجتمع المفتوح، والحريات الدستورية والحقوق الفردية. وتتحمل الهيئة الوطنية لأمن الفضاء الإلكتروني، التي تعمل تحت إشراف وزارة السياسة الرقمية، المسؤولية العامة عن تنفيذ الاستراتيجية الوطنية لأمن الفضاء الإلكتروني.

والأهداف الرئيسية لاستراتيجيتنا الوطنية لأمن الفضاء الإلكتروني هي:

- إقامة وتعزيز فضاء إلكتروني آمن ومرن على أساس المعايير والممارسات الوطنية والأوروبية والدولية
- التحسين المستمر لقدراتنا على الحماية من الهجمات الإلكترونية، مع التركيز على البنى التحتية الحيوية
- تنمية ثقافة قوية في مجال الأمن في القطاعين العام والخاص، يستفاد من خلالها من إمكانات كل من الأوساط الأكاديمية والجهات الفاعلة العامة والخاصة
- تحسين مستوى تقييم وتحليل ومنع التهديدات، من أجل تحقيق أمن نظم المعلومات والبنى التحتية
- وإنشاء إطار فعال للتنسيق والتعاون بين الجهات صاحبة المصلحة من القطاعين العام والخاص
- المشاركة النشطة للبلد في المبادرات الدولية والإجراءات التي تتخذها المنظمات الدولية في مجال أمن الفضاء الإلكتروني

- توعية جميع الجهات الاجتماعية صاحبة المصلحة وإبلاغ المستخدمين بشأن الاستخدام الآمن للفضاء الإلكتروني
- التكييف المستمر للإطار المؤسسي الوطني مع الاحتياجات التكنولوجية الجديدة، وكذلك مع المبادئ التوجيهية الأوروبية
- تعزيز الابتكار وأنشطة البحث والتطوير في مجال المسائل الأمنية.

اليابان

[الأصل: بالإنكليزية]
[١٤ أيار/مايو ٢٠١٩]

١ - التقييم العام لمسائل أمن المعلومات

إن معارف وتكنولوجيات وخدمات الفضاء الإلكتروني، من قبيل الذكاء الاصطناعي وإنترنت الأشياء والتكنولوجيا المالية والبيانات الضخمة والجيل الخامس من شبكات الاتصال اللاسلكية، آخذة في الترسُّخ في المجتمع وهي تؤدي إلى ابتكارات تحوّل الهياكل القائمة في أنشطتنا الاجتماعية الاقتصادية والحياة اليومية للناس، وتُحدث هذه التحولات تقدماً في توحيد الفضاء الإلكتروني والفضاء الحقيقي. ومن أجل التمتع بفوائد معارف وتكنولوجيات وخدمات الفضاء الإلكتروني، من الضروري السيطرة على أوجه عدم اليقين الكامنة فيها بصورة دائمة. وعندما لا تكون تلك السيطرة ممكنة، توجد إمكانية لتزايد التهديدات المتعلقة بأمن الفضاء الإلكتروني بسرعة.

فوائد الفضاء الإلكتروني

عدد مستخدمي الإنترنت في العالم آخذ في الازدياد، شأنه في ذلك شأن انتشار شبكة الإنترنت نفسها. وعلاوة على ذلك، وفي ما يتعلق بالأجهزة، يزداد معدل ملكية الهواتف الذكية الشخصية تزايداً كبيراً، كما أن معدل استخدام الإنترنت آخذ في الارتفاع. ومعدل مستخدمي وسائل التواصل الاجتماعي آخذ في الارتفاع أيضاً، حيث توجد الآن نتيجة لذلك بيئة للتواصل بسهولة في الفضاء الإلكتروني. ولا يعزز تزايد اعتماد المجتمع للخدمات في الفضاء الإلكتروني التدفق الحر للمعلومات فحسب، ولكنه يعزز أيضا تشكيل مختلف المجموعات وتبادل المعلومات. ويُحرز تقدم في مجال الأنشطة المالية أيضا، بما في ذلك التسوق عن طريق الإنترنت، وتجارة الأوراق المالية، والأعمال المصرفية الإلكترونية، في حين تأخذ خدمات جديدة في مجالات التكنولوجيا المالية والاقتصاد التشاركي بالظهور بصورة منتظمة وتقود الابتكار. ويحرز تقدم أيضاً في مجال استخدام تكنولوجيا المعلومات والاتصالات في الطب والتمريض، والرعاية، والتعليم والمجالات الأخرى المتصلة بالمسائل الاجتماعية مثل تراجع عدد السكان في سن العمل وشيخوخة المجتمعات المحلية.

التهديدات المتزايدة في الفضاء الإلكتروني

على الرغم من أن إمكانية أن يؤدي الذكاء الاصطناعي وإنترنت الأشياء، وغيرهما من التكنولوجيات والخدمات، إلى جلب العديد من الفوائد للناس، هناك دائماً خطر كامن يتمثل في أن تفقِد

الجهات الموفرة لهذه التكنولوجيات والخدمات القدرة على السيطرة عليها، ويمكنها أن تتسبب في هذه الحالة في خسائر أو أضرار اقتصادية واجتماعية غير قابلة للقياس. ومع التقدم في توحيد الفضاء الإلكتروني والفضاء الحقيقي، يتزايد احتمال حدوث ذلك تزايداً هائلا. وعلاوة على ذلك، يتسم الفضاء الإلكتروني بأنه مكان غير مقيد بفضاء أو زمان محددين، حيث يستطيع أي شخص، بما في ذلك الجهات الفاعلة الشريرة، إساءة استعمال تكنولوجيات المعلومات والاتصالات الجديدة وحرفها عن وجهتها بسهولة. وتتيح طبيعة التكنولوجيا الرقمية ذاتها للجهات الفاعلة الشريرة نسخ وتوزيع البيانات والمعلومات الحساسة بسهولة، وإطلاق برامج الهجمات، والمرونة في إدماج التكنولوجيات الناشئة واستخدامها مجانا، مثل الذكاء الاصطناعي وتقنية سلسلة السجلات المغلقة. ولهذا السبب، يتفوق المهاجمون بميزة غير متناظرة على المدافعين، ومن المتوقع أن تكبر تلك الميزة بصورة خاصة عندما تتوقف بنية المدافع على السياسات والنظم التكنولوجية القائمة. وفي ظل هذه الظروف، تقع هجمات تستهدف إنترنت الأشياء، والتكنولوجيا المالية، بما في ذلك العملات الرقمية المشفرة، والبنى التحتية الحيوية وسلاسل الإمداد، مما يتسبب في حدوث خسائر مالية مباشرة وتعطل الأعمال التجارية والخدمات، بالإضافة إلى الخرق المعتاد للبيانات، ويؤدي إلى تهديد سلامة وأمن التنمية المستدامة للأنشطة الاجتماعية الاقتصادية ومعيشة الناس. وتقع أيضاً حوادث ضخمة يشتبه في أن دولا تقوم برعايتها. وهناك أيضاً قلق من أن مصداقية البنى التحتية للمعلومات قد تتزعزع إذا كان الفضاء الإلكتروني يخضع لسيطرة وإدارة الحكومة في بعض البلدان من موقع عال. ويُعتقد أن استمرار الفضاء الإلكتروني في اتحاده مع الفضاء الحقيقي سيترافق مع تزايد المخاوف بشأن المحاولات الممكنة لاستهداف مواطن الضعف في إنترنت الأشياء، وسلاسل الإمداد، والابتكار المفتوح، وأن السلوك غير المقصود سيحدُث في هذه النظم. ويمكن أن يؤثر ذلك تأثيراً شديداً ليس على الهيئات الحكومية والجهات المشغلة للبنى التحتية الحيوية فحسب، ولكن أيضاً على الأعمال التجارية الأخرى وحتى على الأفراد.

الالتزام بالموقف الأساسي المتعلق بالفضاء الإلكتروني

بغية الاستمرار في ردع أنشطة الجهات الفاعلة الشريرة وضمان سلامة الناس وحقوقهم، تحتفظ اليابان بخيارات اللجوء إلى الوسائل السياسية، والاقتصادية، والتكنولوجية، والقانونية، والدبلوماسية وسائر الوسائل الناجعة والفعالة باعتبارها خيارات متاحة لها. وتلتزم اليابان بالمبادئ الخمسة لوضع وتنفيذ تدابير أمن الفضاء الإلكتروني، وهي: '١' ضمان التدفق الحر للمعلومات؛ '٢' وسيادة القانون؛ '٣' والانفتاح؛ '٤' والاستقلالية؛ '٥' والتعاون في ما بين أصحاب المصلحة المتعددين.

'١' ضمان التدفق الحر للمعلومات

من أجل التنمية المستدامة للفضاء الإلكتروني بوصفه مكانا للإبداع والابتكار، من الضروري بناء وصون عالم تبلغ فيه المعلومات المرسلة الجهة المتلقية المقصودة دون أن تخضع للرقابة بطريقة جائرة أو تعدل بطريقة غير قانونية وهي في الطريق. ويجب أيضا ضمان الأخذ باعتبارات الخصوصية. ومن الشروط الأساسية للتدفق الحر للمعلومات في الفضاء الإلكتروني، يطلب ألا تتعدى نظم الأخلاق والحس السليم على حقوق الآخرين ومصالحهم.

’٢‘ سيادة القانون

مع التقدم المحرز في توحيد الفضاء الإلكتروني والفضاء الحقيقي، ينبغي الحفاظ أيضا على سيادة القانون في الفضاء الإلكتروني بنفس طريقة القيام بذلك في الفضاء الحقيقي. وتطبق شتى القواعد والمعايير المحلية، بما في ذلك القوانين والأنظمة المحلية، في الفضاء الإلكتروني. وبالمثل، يطبق أيضا القانون الدولي القائم في الفضاء الإلكتروني. ولا يزال تطبيق القانون الدولي القائم ووضع المعايير ضروريا للتنمية المستدامة للفضاء الإلكتروني باعتباره فضاء مأمونا وموثوقا.

’٣‘ الانفتاح

بغية تحقيق التنمية المستدامة للفضاء الإلكتروني بوصفه فضاء لتوليد القيم الجديدة، يجب أن يكون الفضاء الإلكتروني مفتوحا لجميع الجهات الفاعلة دون تقييد إمكانيات الربط بين مختلف الأفكار والمعارف. وتتمسك اليابان بالموقف القائل بأن السيطرة على الفضاء الإلكتروني يجب ألا تكون محصورة في أيدي مجموعة صغيرة من الجهات الفاعلة فيه.

’٤‘ الاستقلالية

يتطور الفضاء الإلكتروني من خلال المبادرات المستقلة لأصحاب المصلحة المتعددين. ومن غير المناسب ومن المستحيل أن تتولى إحدى الدول كامل دور الحفاظ على النظام كي يتطور الفضاء الإلكتروني على نحو مستدام كفضاء يوجد فيه النظام والإبداع جنبا إلى جنب. ويتمثل النهج الوحيد للحفاظ على النظام وردع سلوك الجهات الفاعلة الشريرة والتصدي له في أن تعمل مختلف النظم الاجتماعية بشكل مستقل. وستعزز اليابان هذا النهج.

’٥‘ التعاون فيما بين أصحاب المصلحة المتعددين

الفضاء الإلكتروني عالم متعدد الأبعاد أنشئ من خلال أنشطة أصحاب المصلحة المتعددين، بما في ذلك الدولة، والحكومات المحلية، والجهات المشغلة للبنى التحتية الحيوية، والأعمال التجارية العاملة في مجال الفضاء الإلكتروني وسائر الأعمال التجارية، ومؤسسات التعليم والبحث والأفراد. ومن أجل التنمية المستدامة للفضاء الإلكتروني، يتعين على جميع الجهات الفاعلة الوفاء بصورة واعية بالأدوار والمسؤوليات المنوطة بكل منها. وسيتطلب ذلك التنسيق والتعاون بالإضافة إلى الجهود الفردية. وتتولى الدولة الدور الريادي في تعزيز هذا التنسيق والتعاون، وهي ستعزز التدابير التي تساعد على الاضطلاع بتلك الأدوار.

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

الجهود المبذولة على المستوى الوطني لتعزيز أمن المعلومات

في اليابان، وضع الأساس القانوني لاستخدام البيانات، بما في ذلك القانون الأساسي المتعلق بالنهوض باستخدام البيانات في القطاعين العام والخاص والقانون المعدَّل المتعلق بحماية المعلومات الشخصية، وما إلى ذلك. واعتمدت الحكومة أيضا سياسة للوصول إلى مجتمع محوره الإنسان ينجز كلا من التنمية الاقتصادية وتسوية المسائل الاجتماعية من خلال ارتفاع مستوى إدماج الفضاء الإلكتروني مع

الفضاء الحقيقي. وفي ظل هذه الظروف، تُراكم الكميات الهائلة من البيانات المتأتية من أجهزة الاستشعار وسائر أنواع الأجهزة في الفضاء الحقيقي وتُحلل في الفضاء الإلكتروني. وعلاوة على ذلك، يمكن النظر بعين التشاؤم إلى نشوء وتطور الإمداد في الفضاء الحقيقي بمنتجات وخدمات جديدة تضيف قيمة من خلال استخدام البيانات في العديد من الميادين. فالفضاء الإلكتروني والفضاء الحقيقي لم يعودا يوجدان باعتبارهما كيانين مستقلين، ولكن باعتبارهما كيانين يعزز أحدهما الآخر، بحيث لا يمكن اعتبارهما منفصلين بعد الآن. ولذلك، ينبغي اعتبار الفضاءين كياناً عضوياً واحداً يتطور باستمرار.

ويزيد توحيد الفضاء الإلكتروني والفضاء الحقيقي بدرجة كبيرة من إمكانية إتاحة الوفرة للمجتمع. وهو يزيد في الوقت نفسه أيضا من الفرص المتاحة للجهات الفاعلة الشريرة لإساءة استعمال الفضاء الإلكتروني. ومن المتوقع أن يتسع نطاق خطر الخسائر أو الأضرار الاقتصادية والاجتماعية في الفضاء الحقيقي وأن يتسارع بصورة هائلة. وفي ظل هذه الظروف، يجب ضمان أمن الفضاء الإلكتروني، الذي يشكل أساس المجتمع الاقتصادي، ويتعين في الوقت نفسه ضمان تطوره وتنميته على نحو مطرد ومستقل من أجل تحقيق التقدم المستدام والثروة للمجتمع.

وفي الآونة الأخيرة، كان هناك اتجاه عام لدى بعض الدول للتصدي للتهديدات الإلكترونية من خلال التركيز على قيام الدولة بالإدارة والمراقبة من موقع مهيمن. غير أن تعزيز إدارة الدولة للفضاء الإلكتروني ومراقبتها له يؤدي إلى عرقلة إمكانية تنميته بطريقة مستقلة ومستدامة. ويجب من ثم احترام الفضاء الإلكتروني القائم حالياً الذي أنشئ من خلال مبادرات مستقلة قام بها جميع الجهات صاحبة المصلحة، ويجب حماية الفضاء الإلكتروني من خلال مبادرات تعاونية وتآزرية مع تلك الجهات صاحبة المصلحة. واستنادا إلى هذا الفهم، ومراعاة للحالة الراهنة التي ينبغي الاستمرار بها لعام ٢٠٢٠ وما بعده، ومع أخذ استضافة مناسبات دولية من قبيل الدورة الثانية والثلاثين للألعاب الأولمبية ودورة طوكيو للألعاب الأولمبية للمعوقين لعام ٢٠٢٠ (يشار إليها في ما يلي باسم ”ألعاب طوكيو لعام ٢٠٢٠“) في الاعتبار، لن تدخر اليابان جهداً بشأن تدابير أمن الفضاء الإلكتروني عن طريق توضيح الرؤية الأساسية لأمن الفضاء الإلكتروني، وتحديد المسائل الجديدة التي يتعين التصدي لها؛ وتنفيذ تلك التدابير على وجه السرعة.

الجهود المبذولة على الصعيد الوطني من أجل تعزيز التعاون الدولي

نظرا لأن آثار الحوادث التي تقع في الفضاء الإلكتروني يمكن أن تتجاوز الحدود الوطنية بسهولة، يمكن للحوادث الإلكترونية التي تقع خارج اليابان أن تضر دائما باليابان. وستمد اليابان يد التعاون والتآزر للحكومات والقطاع الخاص في جميع أنحاء العالم من أجل ضمان أمن الفضاء الإلكتروني والعمل من أجل سلام المجتمع الدولي واستقراره والأمن الوطني لليابان. وتحقيقا لهذه الغاية، ستبادر الحكومة إلى المساهمة في المناقشات الدولية المختلفة والعمل من أجل تبادل المعلومات والتوصل إلى فهم مشترك بشأن المسائل ذات الصلة بالفضاء الإلكتروني. وستقوم الحكومة أيضا بتبادل الخبرات مع البلدان الأجنبية، وتعزيز أشكال محددة من التعاون والتآزر، واتخاذ إجراءات.

وفي ما يتعلق بسياسة تبادل الخبرات والتنسيق، ستقوم الحكومة بالعمل من خلال الحوارات الثنائية والمؤتمرات الدولية المعنية بأمن الفضاء الإلكتروني لتبادل المعلومات بشأن السياسات والاستراتيجيات والنظم ذات الصلة بأمن الفضاء الإلكتروني للاستجابة، واستخدام تلك المعارف في

التخطيط لسياسة اليابان في مجال أمن الفضاء الإلكتروني. وسنسعى أيضا إلى تعزيز تعاوننا وتآزرنا في مجال السياسات المتعلقة بأمن الفضاء الإلكتروني مع الشركاء الاستراتيجيين الذين يتقاسمون معنا المبادئ الأساسية بشأن أمن الفضاء الإلكتروني.

وفي ما يتعلق بالتعاون الدولي في مجال التصدي للحوادث، ستقوم الحكومة بتقاسم المعلومات عن الهجمات الإلكترونية والتهديدات وتعزيز التعاون بين أفرقة مواجهة الطوارئ الحاسوبية لإتاحة الاستجابة المنسَّقة عند وقوع الحوادث. وستسعى الحكومة أيضاً إلى تحسين القدرات على القيام باستجابات منسقة من خلال التدريب المشترك والمشاركة في التمارين والتدريبات المشتركة الدولية في مجال الفضاء الإلكتروني. وعلاوة على ذلك، ستستجيب الحكومة على النحو الملائم في حالة وقوع حوادث من خلال التعاون الدولي الملائم.

وفي ضوء الجوانب الدبلوماسية للتعاون الدولي المتعلق بالفضاء الإلكتروني، تتألف التزاماتنا من ثلاث ركائز هي: سيادة القانون، وتدابير بناء الثقة، وبناء القدرات في الفضاء الإلكتروني.

- يتسم تعزيز سيادة القانون بأهميته لتحقيق السلام والاستقرار الدوليين والأمن الوطني لليابان. ويتمثل موقف اليابان في أن القانون الدولي القائم، بما في ذلك ميثاق الأمم المتحدة، ينطبق على الفضاء الإلكتروني أيضا، وستبادر اليابان إلى المساهمة في المناقشات بشأن حالات التطبيق الفردية والمحددة للقانون الدولي القائم ووضع المعايير وإضفاء الطابع العالمي عليها. وفيما يتعلق بالتدابير المتخذة لمكافحة الجرائم الإلكترونية، ستتعاون وكالة الشرطة الوطنية وغيرها من الوزارات والوكالات المعنية من أجل المضي في تعزيز الشراكات الدولية من خلال التعاون الدولي في التحقيقات وتبادل المعلومات مع المنظمات الدولية، ووكالات إنفاذ القانون ووكالات المعلومات الأمنية في البلدان الأجنبية للاستفادة من أطر من قبيل الاتفاقية المتعلقة بالجريمة الإلكترونية، ومعاهدات المساعدة القانونية المتبادلة والمنظمة الدولية للشرطة الجنائية.

- ستسعى اليابان إلى بناء الثقة بين الدول بغية منع حدوث ظروف غير متوقعة وتدهور الحالة بسبب الهجمات الإلكترونية. وبسبب إغفال الهوية وسرية الهجمات الإلكترونية، توجد مخاطر تتمثل في إمكانية أن تزيد الهجمات الإلكترونية من حدة التوتر بين الدول وتفاقم الحالة عن غير قصد. ولمنع هذه المواجهات العرضية وغير الضرورية، من المهم بناء قنوات اتصال دولية خلال أوقات السلام استعدادا لوقوع الحوادث التي تتجاوز الحدود الوطنية. ومن الضروري أيضا زيادة الشفافية وبناء الثقة بين الدول من خلال تبادل المعلومات بصورة استباقية وإقامة حوارات بشأن السياسات في سياق مشاورات ثنائية ومتعددة الأطراف. وستتعاون الحكومة أيضاً مع الدول الأخرى للنظر في آلية لتنسيق المسائل المتعلقة بالفضاء الإلكتروني. وفي هذا السياق، تشجع اليابان بحماس تدابير بناء الثقة، بسبل منها الشروع في إنشاء اجتماع ما بين الدورات للمنتدى الإقليمي لرابطة أمم جنوب شرق آسيا في مجال الأمن الإلكتروني والمشاركة في ترأسه، مع التنفيذ المطرد لأنشطة المساعدة في مجال بناء القدرات، ولا سيما في منطقة آسيا والمحيط الهادئ.

- في ما يتعلق ببناء القدرات، ولأن الترابط عبر الحدود يتعمق، من غير الممكن أن تتمكن اليابان من تحقيق السلام والاستقرار وحدها. فالتنسيق العالمي للحد من مواطن الضعف في مجال أمن الفضاء الإلكتروني وإزالتها ضروري لضمان الأمن القومي لليابان. ومن هذا المنطلق، تضمن

المساعدة المقدمة لبناء القدرات في الدول الأخرى استقرار حياة المقيمين اليابانيين وأنشطة الشركات اليابانية في البلدان الأخرى التي تعتمد على البنى التحتية الحيوية في تلك الدول وكذلك على التطور السليم لاستخدام الفضاء الإلكتروني فيها. وترتبط تلك المساعدة في الوقت نفسه ارتباطا مباشرا بضمان أمن الفضاء الإلكتروني كله وتسهم في تحسين البيئة الأمنية للعالم بأسره بما في ذلك اليابان. وأيضا في ميدان جرائم الفضاء الحاسوبي، تشكل اليابان أحد الأطراف غير الأوروبية القليلة في الاتفاقية المتعلقة بالجريمة الإلكترونية وهي تضطلع بدور إيجابي في تعزيز الاتفاقية، التي تمثل إطارا قانونيا هاما للتصدي لجرائم الفضاء الإلكتروني، من خلال تقديم المساعدة في مجال بناء القدرات في المنطقة الآسيوية.

٣ - المفاهيم الدولية ذات الصلة الرامية إلى تعزيز أمن نظم المعلومات والاتصالات السلكية واللاسلكية على الصعيد العالمي

تؤيد اليابان الاتفاقات التي توصلت إليها أفرقة الخبراء الحكوميين السابقة بتوافق الآراء على انطباق القانون الدولي القائم في مجال الفضاء الإلكتروني. ونحن نشهد المناقشة المتعلقة بتحديد السلوك المعياري، وتفعيل تدابير بناء الثقة، وبناء القدرات باعتبارها النهج الرئيسية في تشكيل السلوك المسؤول للدول في الفضاء الإلكتروني. وعلى وجه الخصوص، تسلم اليابان بأن تنفيذ المعايير الطوعية وغير الملزمة لسلوك الدول المسؤول في الفضاء الإلكتروني، على النحو المشار إليه في تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان بيئة تكنولوجيا المعلومات والاتصالات لعام ٢٠١٥، يجب أن يشكل الأساس لكفالة الاستقرار وقابلية التنبؤ على الصعيد الدولي، وللمناقشات المقبلة بشأن هذه المسألة. وفي هذا الصدد، نعتقد أن أي محاولات لإبرام معاهدات شاملة أو صكوك مماثلة بطريقة أخرى لن تعزز بصورة إيجابية أمن الفضاء الإلكتروني في الوقت الراهن.

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

لئن كانت اليابان تعزز التنسيق مع الأطر الإقليمية ذات الصلة التي وضعها المجتمع الدولي استنادا إلى القانون الدولي القائم وجميع المفاهيم المحددة من خلال فريق الخبراء الحكوميين، فهي تعتقد، بوصفها دولة مسؤولة، أن إيجاد فهم مشترك للمعايير الطوعية وغير الملزمة لسلوك الدول المسؤول، وتنفيذ هذه المعايير، سيسهمان في تعزيز الأمن الدولي.

٥ - مضمون المفاهيم المشار إليها في تقارير فريق الخبراء الحكوميين

تعتقد اليابان أن مراعاة جميع الدول للمفاهيم التالية التي حددها فريق الخبراء الحكوميين ذات جدوى وفعالية.

التأثير على المجتمع الدولي عن طريق الأعمال الإلكترونية الشريرة

بغية إدماج التطور السريع لتكنولوجيات المعلومات والاتصالات بمرونة في حياتنا ومنع الأضرار الناجمة عن الأعمال الإلكترونية الشريرة، ينبغي لنا أن نسلم بأهمية توقع التهديدات القائمة والمحتملة في الفضاء الإلكتروني والكيفية التي يمكن أن يتأثر المجتمع الدولي بها.

تنفيذ المعايير الطوعية وغير الملزمة لسلوك الدول المسؤول

بغية التقليل إلى أدنى حد من آثار الأعمال الشريرة في الفضاء الإلكتروني وردع من تسول لهم أنفسهم ارتكابها، ينبغي أن نتذكر أهمية تقرير فريق الخبراء الحكوميين الذي وضع بتوافق الآراء، بما في ذلك المعايير الطوعية وغير الملزمة لسلوك الدول المسؤول المشار إليها فيه. وينبغي لنا تعميق مناقشاتنا، بالتعاون مع المنظمات الإقليمية ذات الصلة، للاستعانة بهذه الجهود الجديرة بالاهتمام بطريقة عملية وفعالة.

تعزيز تنفيذ المعايير الطوعية وغير الملزمة لسلوك الدول المسؤول والتعاون من أجل تدابير بناء الثقة ذات الصلة وبناء القدرات

بغية مواصلة تعزيز الجهود التي تبذلها كل دولة من الدول لإقامة فضاء إلكتروني حر ومنصف وآمن والحفاظ عليه في سياق الأمن الدولي، ينبغي أن نؤكد من جديد أن جميع الدول تبدي الإرادة القوية لإزالة الثغرات الأمنية في الفضاء الإلكتروني ومنع جرائم الفضاء الإلكتروني وغيرها من الأعمال الشريرة. وفي هذا السياق، ينبغي أن يكرِّس أعضاء الفريق أنفسهم على الدوام لتشجيع جميع الدول على تنفيذ لمعايير سلوك الدول المسؤول الطوعية وغير الملزمة بصورة مطردة، بما في ذلك تدابير بناء الثقة والتعاون من أجل المساعدة على بناء القدرات الوطنية على تنفيذ المعايير والتوصيات الطوعية وغير الملزمة المذكورة أعلاه، بما في ذلك من خلال عملية فريق الخبراء الحكوميين المقبل والفريق العامل المفتوح العضوية.

سنغافورة

[الأصل: بالإنكليزية]
[١٣ أيار/مايو ٢٠١٩]

تسلم سنغافورة بأن الأخطار التي تتهدد إقامة فضاء إلكتروني مفتوح وآمن وسلمي تتسم بتعقدها المتزايد وبأنها عابرة للحدود وغير متناظرة بطبيعتها. وتلتزم سنغافورة، بوصفها دولة صغيرة وكثيفة الاتصال بالإنترنت تعرضت لعدد من الهجمات الإلكترونية، التزاماً قوياً بإنشاء نظام دولي قائم على القواعد في الفضاء الإلكتروني. وسيشكل ذلك أساساً للثقة والاطمئنان بين الدول الأعضاء، وسيتيح التقدم الاقتصادي والاجتماعي. ومن أجل جني الفوائد الكاملة للتكنولوجيات الرقمية، يجب على المجتمع الدولي أن يقيم فضاء إلكترونيا آمناً وموثوقاً ومفتوحاً يستند إلى القانون الدولي المنطبق على الفضاء الإلكتروني، والمعايير المحددة جيدا لسلوك الدول المسؤول، وتدابير بناء الثقة القوية وتنسيق بناء القدرات. وتشكل هذه المسارات الثلاثة معا عملية متكررة ذات أجزاء ثلاثة يعزز بعضها بعضا ستتيح إقامة فضاء إلكتروني مأمون ومرن. ومن المهم أن تتواصل الجهود الرامية إلى مناقشة هذه القوانين والقواعد والمعايير في الأمم المتحدة، التي تمثل المنتدى العالمي الوحيد الشامل للجميع والمتعدد الأطراف، حيث تتمكن جميع الدول، الكبيرة منها والصغيرة، من الإدلاء برأيها. وسنغافورة ملتزمة بهذه العملية.

وترحب سنغافورة بإنشاء فريق الخبراء الحكوميين المعني بالتطورات في ميدان بيئة تكنولوجيا المعلومات والاتصالات وبقرار توجيه الدعوة إلى فريق عامل مفتوح العضوية إلى الاجتماع. وترى سنغافورة أن عمل فريق الخبراء الحكوميين وعمل الفريق العامل يمكن، بل ينبغي، أن يكمِّل أحدهما الآخر. ومن

المهم بالنسبة للجهات الفاعلة الرئيسية أن تعمل معاً، بروح من توافق الآراء، والاحترام المتبادل والثقة المتبادلة. وتشعر سنغافورة بالتفاؤل من إمكانية أن تكمل كلتا المنصتين إحداهما الأخرى على نحو إيجابي، وهي ملتزمة بالإسهام البناء في كلتا العمليتين بطريقة بناءة.

وعلى الصعيد الإقليمي، عملت سنغافورة مع الدول الأعضاء الزميلة في رابطة أمم جنوب شرق آسيا لإصدار أول بيان لقيادات الرابطة بشأن التعاون في مجال أمن الفضاء الإلكتروني خلال مؤتمر القمة الثاني والثلاثين للرابطة في نيسان/أبريل ٢٠١٨. وفي البيان، أكدت قيادات الرابطة من جديد على الحاجة إلى نظام دولي قائم على القواعد في الفضاء الإلكتروني. وكلفت أيضاً الوزراء المعنيين بتحديد آلية أو منصة مناسبة لتنسيق السياسات، والجهود الدبلوماسية، وأنشطة التعاون، والجهود التقنية وجهود بناء القدرات المتعلقة بأمن الفضاء الإلكتروني في بلدان الرابطة، وبوضع قائمة محددة بمعايير عملية طوعية لسلوك الدول في الفضاء الإلكتروني يمكن أن تعمل الرابطة من أجل اعتمادها. وعملا ببيان القادة، اتفق المشاركون في المؤتمر الوزاري الثالث لرابطة أمم جنوب شرق آسيا بشأن أمن الفضاء الإلكتروني، الذي عقد في سنغافورة في أيلول/سبتمبر ٢٠١٨، على الالتزام من حيث المبدأ بالمعايير الـ ١١ الواردة في تقرير فريق الخبراء الحكوميين لعام ٢٠١٥ (A/70/174)، إضافة إلى التركيز على بناء القدرات على الصعيد الإقليمي في مجال تنفيذ هذه المعايير.

ويتسم بناء القدرات بأهميته الأساسية لضمان أن تطور الدول القدرة على التنفيذ الناجح لقواعد ومعايير السلوك. ولدى سنغافورة برنامج لبناء قدرات رابطة أمم جنوب شرق آسيا في مجال الفضاء الإلكتروني تكلفته ١٠ ملايين دولار سنغافوري، وهو برنامج مؤلف من وحدات ومتعدد التخصصات ومتعدد أصحاب المصلحة يركّز على بناء القدرات في بلدان رابطة أمم جنوب شرق آسيا في مجال سياسات واستراتيجيات الفضاء الإلكتروني وكذلك في مجال المسائل التقنية. ومنذ إنشاء البرنامج في عام ٢٠١٦، تلقى ١٦٠ مسؤولا من الرابطة التدريب في إطار البرنامج. وتقيم سنغافورة أيضاً شراكة مع مكتب شؤون نزع السلاح لإعداد دورة تدريبية رئيسية على الإنترنت لتعزيز فهم وتنفيذ الاتفاقات التي توصل إليها فريق الخبراء الحكوميين. وستعمل أيضاً مع مكتب شؤون نزع السلاح بشأن برنامج مشترك بين سنغافورة والأمم المتحدة في مجال الفضاء الإلكتروني لبناء وعي بمعايير الفضاء الإلكتروني وتخطيط السياسات للتعامل مع سيناريوهات الفضاء الإلكتروني في الدول الأعضاء في الرابطة. وكامتداد لبرنامج بناء قدرات الرابطة في مجال الفضاء الإلكتروني، ستفتتح سنغافورة مركز الامتياز المشترك بين سنغافورة والرابطة بتكلفة قدرها ٣٠ مليون دولار سنغافوري في عام ٢٠١٩ لمواصلة بناء صنع السياسات في مجال أمن الفضاء الإلكتروني، ووضع الاستراتيجيات، وكذلك بناء القدرات التقنية والتشغيلية في بلدان رابطة أمم جنوب شرق آسيا. وسيكون المركز مفتوحاً وشاملا للجميع، ويمكن للدول الأعضاء في الرابطة الاستفادة منه للتواصل بشكل أوثق مع الشركاء الدوليين.

وعلى الصعيد الوطني، خطت سنغافورة خطوات كبيرة في تعزيز أمن الفضاء الإلكتروني لنظمها وشبكاتها على الجبهات الثلاث التالية: بناء بنية تحتية قادرة على الصمود، وإيجاد فضاء إلكتروني أكثر أماناً، وتهيئة بيئة حيوية لأمن الفضاء الإلكتروني.

(أ) *بناء بنية تحتية قادرة على الصمود* – تعرض التهديدات الإلكترونية العابرة للحدود البنى التحتية الحيوية للبلدان للخطر على نحو متزايد. وينطبق ذلك بصفة خاصة على البنية التحتية للمعلومات التي تتجاوز حدود الولاية الوطنية، على غرار ما هو موجود في قطاعات المالية والبحرية

والاتصالات السلكية واللاسلكية والطيران، حيث يمكن أن تنتشر آثار هجوم إلكتروني ناجح خارج الحدود الوطنية لتضر بالمراكز المترابطة في جميع أنحاء العالم. ومن التطورات الرئيسية في عام ٢٠١٨ إقرار وتنفيذ قانون أمن الفضاء الإلكتروني، الذي أنشأ إطاراً قانونياً للإشراف على أمن الفضاء الإلكتروني الوطني في سنغافورة والمحافظة عليه. ويشدد القانون على الحماية الاستباقية للبنى التحتية الحيوية للمعلومات من الهجمات الإلكترونية، وهي حواسيب أو نظم حاسوبية تدعم توفير الخدمات الأساسية. وتتحقق تلك الحماية عن طريق فرض التزامات قانونية على أصحاب هذه البنى التحتية من أجل أهداف من بينها ما يلي: '١' إنشاء آليات للكشف عن التهديدات التي يتعرض لها أمن الفضاء الإلكتروني والحوادث التي تقع فيه، والإبلاغ عن تلك الحوادث؛ '٢' وإجراء تقييمات منتظمة للمخاطر وعمليات تدقيق بشأن البنى التحتية الحيوية للمعلومات؛ '٣' والمشاركة في تمارين أمن الفضاء الإلكتروني التي تجريها الهيئة الوطنية لأمن الفضاء الإلكتروني. وإلى جانب تعزيز حماية هذه البنى التحتية، فإن الهيئة الوطنية لأمن الفضاء الإلكتروني يخول لها هذا القانون أيضاً منع التهديدات التي يتعرض لها أمن الفضاء الإلكتروني والحوادث المتصلة به التي تقع فيه والتصدي لها والتحقيق فيها؛

(ب) *إيجاد فضاء إلكتروني أكثر أماناً* – في كانون الثاني/يناير ٢٠١٩، حصلت سنغافورة على مركز الدولة المخولة بمنح شهادات بموجب ترتيب الاعتراف بالمعايير المشتركة، وهو ترتيب دولي للاعتراف المتبادل بشهادات المعايير المشتركة في ٣٠ دولة. والمعايير المشتركة هي نموذج تقني يطبق على تقييم منتجات أمن تكنولوجيا المعلومات ومنحها الشهادات، وهي معتمدة على نطاق واسع من قبل الحكومات وأوساط الصناعة على السواء. وسنغافورة هي حالياً واحدة من ١٨ من ٣٠ دولة مخولة بمنح الشهادات في إطار هذا الترتيب. وعلى هذا النحو، فإن سنغافورة مسموح لها بمنح الشهادات لمنتجات أمن تكنولوجيا المعلومات محلياً، مما يساعد على تحسين نوعية منتجات أمن الفضاء الإلكتروني التي تنتجها المؤسسات الصغيرة والمتوسطة في سنغافورة من خلال تقييمها قياساً إلى المعايير الأمنية الدولية؛

(ج) *تهيئة بيئة حيوية لأمن الفضاء الإلكتروني* – تسلم سنغافورة بأن تعزيز أمن الفضاء الإلكتروني ينطوي على بناء البيئة الإلكترونية وتشجيع الابتكار ضمن الصناعة. وتحقيقاً لهذه الغاية، أطلقت سنغافورة أول مركز متكامل فيها لرواد الأعمال في مجال أمن الفضاء الإلكتروني في آذار/مارس ٢٠١٨، تحت اسم ''بيئة الابتكار في مجال أمن الفضاء الإلكتروني في البناء ٧١''، والهدف من هذا المركز المتكامل هو تعزيز بيئة أمن الفضاء الإلكتروني المتنامية في سنغافورة، عن طريق اجتذاب وتطوير الكفاءات والتكنولوجيات العميقة للمساعدة في التخفيف من المخاطر المتزايدة بسرعة التي تتهدد أمن الفضاء الإلكتروني. وهو يساعد أيضاً على إقامة المؤسسات الناشئة في مجال أمن الفضاء الإلكتروني في جميع أنحاء العالم، من خلال مجموعة من البرامج الرامية إلى دعم رواد الأعمال بدءاً من فكرة الإنشاء إلى تسريع إقامة المؤسسات الناشئة في مجال أمن الفضاء الإلكتروني وتوسيع أعمالها لتشمل السوق العالمية.

تركيا

[الأصل: بالإنكليزية]
[١٠ أيار/مايو ٢٠١٩]

أصبحت تكنولوجيات المعلومات والاتصالات جزءاً أساسياً من المجتمع والاقتصاد. فهي تُستخدم في شبكة واسعة تشمل القطاع العام والقطاع الخاص والبنى التحتية الحيوية والأفراد، وأصبحت

تنتشـــر على نطاق واســـع في بلدنا وكذلك في العالم. ونتيجة لذلك، تؤدي تكنولوجيات المعلومات والاتصـــالات دورا هاما في تحقيق النمو المســـتدام والتنمية المســـتدامة. ولكن كلما ازداد اســـتخدامنا للتكنولوجيا، أصبحنا أكثر اتكالا عليها وعرضة للمخاطر التي تجلبها. ويواجه الأفراد، والشركات، والبنية التحتية الحيوية والدول مشاكل خطيرة بسبب التهديدات الإلكترونية.

ويأخذنا انتشـــار التكنولوجيا في جميع مناحي حياتنا إلى مرحلة جديدة في ما يتعلق بالمخاطر المرتبطة بها في سياق أمن الفضاء الإلكتروني. وليس ضمان أمن الفضاء الإلكتروني مجرد ضرورة لمواجهة التهديدات في المجالات التي تستخدم فيها التكنولوجيا بكثافة فحسب، بل أيضاً عاملا بارزاً يؤثر على رخاء الدول وأمنها القومي بسبب المخاطر التي يطرحها على مسار الحياة الاجتماعية والاقتصادية.

ويمكن أن تتسبب مواطن الضعف الأمنية في تكنولوجيا المعلومات والاتصالات في تعطيل تلك النظم أو اســتغلالها، أو قد تؤدي في نهاية المطاف إلى خســائر في الأرواح، وخســائر اقتصــادية واســعة النطاق، وإخلال بالنظام العام أو تعريض الأمن الوطني للخطر.

وتركز تركيا على اتخاذ التدابير اللازمة لتحسين أمن الفضاء الإلكتروني على الصعيد الوطني وهي تنفذ الاســتراتيجية وخطة العمل الوطنيتين لأمن الفضــاء الإلكتروني اللتين تغطيان الفترة من عام ٢٠١٦ إلى عام ٢٠١٩ في إطار مهمة توطيد أمن الفضـــاء الإلكتروني على الصـــعيد الوطني، وتحديد وتنســـيق السياسات الناجعة والمستدامة وكفالة ممارسة هذه السياسات. ووزارة النقل والبنى التحية هي الهيئة المسؤولة عن رسم السياسات ووضع الاستراتيجيات وخطط العمل في ما يتعلق بأمن الفضاء الإلكتروني الوطني في تركيا. وفي هذا السياق، وضعت الاستراتيجية وخطة العمل الوطنيتين لأمن الفضاء الإلكتروني بمشاركة جميع الجهات المعنية صاحبة المصلحة ضمن أفرقة دراسة بتنسيق من وزارة النقل والبنى التحية.

وللاستراتيجية وخطة العمل هدفان رئيسيان، أولهما إقرار جميع الجهات المعنية صاحبة المصلحة بأنها تفهم أن أمن الفضاء الإلكتروني يشكل جزءاً لا يتجزأ من الأمن الوطني؛ وثانياً، اكتساب الكفاءات التي تســـمح باتخاذ التدابير الاحتياطية الإدارية والتكنولوجية للحفاظ على الأمن المطلق لجميع النظم والجهات صاحبة المصلحة في الفضاء الإلكتروني الوطني.

وتقوم وزارة النقل والبنى التحية والهيئات ذات الصـــلة بتنفيذ كل إجراء من الإجراءات الواردة في الاستراتيجية وخطة العمل، في حين تقوم الوزارة برصد جميع أوجه التقدم المتعلقة بكل إجراء.

وعلاوة على ذلك، تمثل هيئة تكنولوجيات المعلومات والاتصـــالات فريق تركيا الوطني لمواجهة الطوارئ الحاســـوبية منذ عام ٢٠١٣. وهي مســـؤولة عن جميع المهام التنظيمية المتعلقة بالاتصـــالات الإلكترونية والخدمات البريدية في تركيا. وبالإضافة إلى ذلك، مُنحت الهيئة صلاحية اتخاذ التدابير اللازمة لمكافحة الهجمات الإلكترونية من أجل ضمان أمن الفضاء الإلكتروني الوطني. ويعمل الفريق بوصفه مركز التنســيق على الصــعيد الوطني، من أجل تبيُّن الأخطار التي تهدِّد أمن الفضــاء الإلكتروني لبلدنا، واتخاذ تدابير للحد من تأثير الهجمات الإلكترونية المحتملة وإزالته وتبادل المعلومات مع جهات فاعلة محددة. ويؤدي الفريق دور التنسيق مع جميع الجهات صاحبة المصلحة من قبيل مؤسسات القطاعين العام والخاص والأفراد من أجل كشــف التهديدات الإلكترونية وإزالتها. ومجالات تركيزه الرئيســية في مجال أمن الفضــاء الإلكتروني هي التالية:

- بناء القدرات في مجال الفضاء الإلكتروني
- التدابير التكنولوجية
- جمع ونشر المعلومات المتعلقة بالتهديدات
- حماية البنية التحتية الحيوية

وتشمل أنشطتنا في مجال بناء القدرات الموارد البشرية وأنشطة التدريب والأعمال التحضيرية. وفي إطار هذه الأنشطة، نقوم بتنظيم مسابقات أمن الفضاء الإلكتروني ''الفوز بالعَلم''. ونعتقد أن الموارد البشرية هي أحد أهم العوامل في أمن الفضاء الإلكتروني. وفي سياق الفريق الوطني لمواجهة الطوارئ الحاسوبية، نقوم بتنفيذ مشاريع رئيسية في مجال بناء القدرات. وفي هذا الصدد، نقوم بتنظيم دورات تدريبية في مجال أمن الفضاء الإلكتروني لأفرقة مواجهة الطوارئ الحاسوبية المؤسسية في مختلف القطاعات الحيوية مثل الطاقة، والصحة والمؤسسات العامة. وننفذ أيضا أنشطة تدريبية عملية ومسابقات للطلاب والخريجين. وفي السنتين الأخيرتين، حضر أكثر من ٢ ٥٠٠ متدرِّب برامجنا التدريبية في مجال أمن الفضاء الإلكتروني.

وأنشأنا أيضاً مختبر حقل الرمي الإلكتروني من أجل تحسين برامجنا التدريبية وتوفير المزيد من فرص النشاط العملي. والمختبر مفيد أيضاً لقياس مستوى الخبرة وتوفير برنامج يمنح شهادات للمشاركين.

وتشمل الدراسات المتعلقة بالتدابير التكنولوجية الكشف المبكر وأنشطة الإنذارات والتحذيرات. ووضعنا لهذا الغرض بعض نظم الكشف والوقاية. وتؤدي هذه النظم دوراً كبيراً في زيادة مستوى أمن الفضاء الإلكتروني الوطني في البلاد من خلال فضح واكتشاف مراكز القيادة والسيطرة لشبكات الحواسيب المصابة والبرامجيات الضارة.

وفي نطاق نهج تركيا في تعزيز أمن الفضاء الإلكتروني، تشكل المعلومات الاستخبارية المتعلقة بتهديدات الفضاء الإلكتروني مجال تركيز رئيسي آخر ينبغي إيلاؤه الأهمية. ونعمل في هذا السياق بالتنسيق مع عدد من الجهات من قبيل الجهات الفاعلة في مجال الإنترنت، والمنظمات الدولية، والسلطات القضائية، ومراكز البحوث والشركات الخاصة. وبالإضافة إلى ذلك، أنشئت أفرقة قطاعية لمواجهة الطوارئ الحاسوبية وأكثر من ١ ٠٠٠ فريق مؤسسي لمواجهة الطوارئ الحاسوبية في إطار المؤسسات العامة والخاصة.

وعلاوة على ذلك، ولأن الفضاء الإلكتروني يشكل ميداناً لا حدود له، من الصعب لجهة ما أن تكفل أمن الفضاء الإلكتروني الخاص به بمفردها. فالمسألة متعددة التخصصات ومتعددة الجهات صاحبة المصلحة. ونحن نعمل مع المستعملين والقطاع الخاص والمنظمات غير الحكومية والأوساط الأكاديمية والجهات النظيرة الدولية من أجل مكافحة التهديدات الإلكترونية. فعلى سبيل المثال، يتلقى فريق تركيا الوطني لمواجهة الطوارئ الحاسوبية إخطارات بشأن الفضاء الإلكتروني من مختلف أفرقة مواجهة الطوارئ الحاسوبية الوطنية ويبلغ الجهات المعنية بها لاتخاذ التدابير اللازمة. وهو يرسل أيضاً معلومات عن التهديدات الإلكترونية ويتقاسم المعلومات مع الأفرقة الوطنية الأخرى لمواجهة الطوارئ الحاسوبية والمنظمات الدولية.

وانطلاقاً من منظور شبكة الإنترنت الآمنة، أنشئ مركز الإنترنت الآمنة ضمن هيئة تكنولوجيات المعلومات والاتصالات في عام ٢٠١٧، من أجل زيادة الوعي فيما يتعلق بالاستخدام المناسب والآمن للإنترنت.

وبدأ العمل بخط الاتصال المجاني للمساعدة في مجال الإنترنت وبموقع شبكي يسمى الشبكة الآمنة، حيث يمكن للأسر أن تجد المشورة في ما يتعلق بالاستخدام الكفؤ للإنترنت. وإلى جانب ذلك، أصبحت ”شاحنات الإنترنت الأكثر أماناً“، المجهزة بأدوات تكنولوجيا المعلومات والاتصالات، متاحة للأطفال والشباب الذين لا تتوافر لهم سوى إمكانية محدودة للوصول إلى تكنولوجيات المعلومات والاتصالات. وتوفر هذه الشاحنات منبراً للناس حيث يمكنهم التعامل عن قرب مع التكنولوجيا وتساعد على التوعية بشأن الاستخدام المأمون والواعي للإنترنت للأطفال الذين يتعاملون أكثر من غيرهم مع الإنترنت والتكنولوجيا.

وتنظّم هيئة تكنولوجيات المعلومات والاتصالات مناسبة في إطار يوم الإنترنت الأكثر أماناً كل سنة. وكان الموضوع الرئيسي لعام ٢٠١٨ هو ”ابتدع وتواصل وتبادل الاحترام: شبكة الإنترنت الأفضل تبدأ بكم“. وأطلقت الهيئة وجامعة بهتشه شهير مسابقة ألعاب لوحية لتشجيع الشباب الذين تتراوح أعمارهم بين ١٢ و ١٨ سنة على تصميم لعبة في إطار الموضوع الدولي. وورد العديد من تصاميم الألعاب خلال المسابقة وحصل الفائزون في المسابقة على جوائزهم. وخلال هذه المناسبة، نظم موقعا فيسبوك وغوغل حلقات عمل للطلاب بشأن الألعاب الرقمية وزيادة أمان الإنترنت.

وبالإضافة إلى ذلك، وقعت الهيئة اتفاقات مع وزارة الأسرة والسياسات الاجتماعية، ورابطة مقدّمي خدمات الإنترنت، ووزارة التعليم بشأن أنشطة التوعية ودورات التدريب للمدربين بشأن الاستخدام المأمون والواعي لتكنولوجيا المعلومات والاتصالات والإنترنت. وأُدرجت محتويات مواد التدريب ضمن وحدات للتعلُّم عن بُعد وأُتيحت لجميع المدرسين العاملين في منظومة وزارة التعليم. وحصل المدرسون وآلاف الطلبة على التدريب حتى الآن من خلال هذه الخدمة للتعلُّم عن بُعد.

وعلاوة على ذلك، وفي سياق توفير أمن الفضاء الإلكتروني والحفاظ عليه، يؤدي التنسيق على الصعيد الوطني، وكذلك التعاون وتبادل المعلومات وبناء الثقة على الصعيد الدولي، دوراً بالغ الأهمية.

ويرد أدناه بيانٌ بالمؤلفات والدراسات ذات الصلة في تركيا بشأن نطاق تدابير بناء الثقة المذكورة في تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي لعام ٢٠١٥ (A/70/174) ومفهوم السلوك المسؤول للدول الذي عُرّف في التقرير.

تمشياً مع انتشار استخدام تكنولوجيا المعلومات والاتصالات بين الأفراد، أصبحت المعلومات أو البيانات الشخصية هدفاً جذاباً للمهاجمين في الفضاء الإلكتروني. وفي سياق الحقوق والحريات الشخصية الأساسية، أصبحت حماية المعلومات أو البيانات أيضاً من الشواغل الرئيسية.

وإلى جانب الشفافية والمساءلة والقيم الأخلاقية في بيئة الفضاء الإلكتروني، تراقب جميع الجهات صاحبة المصلحة في تركيا مبدأ سيادة القانون وحقوق الإنسان والحريات الأساسية وحماية الخصوصية، وتسعى في الوقت نفسه إلى ضمان أمن الفضاء الإلكتروني.

وفي هذا الصدد، نُشر القانون رقم ٦٦٩٨ بشأن حماية البيانات الشخصية في العدد رقم ٢٩٦٨١ من الجريدة الرسمية في ٧ نيسان/أبريل ٢٠١٦ ودخل حيز النفاذ. ويتمثل الغرض من هذا القانون في حماية الحقوق والحريات الأساسية للناس، ولا سيما الحق في الخصوصية، في ما يتعلق بمعالجة البيانات الشخصية وتحديد الالتزامات والمبادئ والإجراءات التي تكون ملزمة للأشخاص الطبيعيين أو الاعتباريين الذين يجهزون البيانات الشخصية.

وتؤدي تركيا أدواراً هامة في العديد من المنظمات، إما باعتبارها عضواً مؤسِّساً، أو من خلال المساهمة في جهود التعاون في المسائل المتعلقة بأمن الفضاء الإلكتروني وأمن المعلومات. وتسعى تركيا من ثم إلى ضمان أمن الفضاء الإلكتروني من خلال تبادل المعلومات والأفكار في طائفة واسعة من المجالات مع مختلف البلدان والمؤسسات بشأن ورسم السياسات وبناء القدرات وتبادل المعلومات.

وبما أن الفضاء الإلكتروني ميدانٌ لا حدود له، فلا مناص من التعاون الدولي لمكافحة التهديدات الإلكترونية. ولهذا السبب، تُتابع تركيا الدراسات الدولية المتعلقة بأمن الفضاء الإلكتروني ضمن الأمم المتحدة ومنظمة حلف شمال الأطلسي والاتحاد الأوروبي ومنظمة الأمن والتعاون في أوروبا وغيرها من المنظمات والمؤسسات الدولية، وتشارك فيها بانتظام.

وبالإضافة إلى ذلك، يتمثل الهدف من إقامة اتفاقات ثنائية مع مختلف الدول في ضمان أمن الفضاء الإلكتروني. فقد وقعت وزارة النقل والبنى التحتية وهيئة تكنولوجيات المعلومات والاتصالات وفريق تركيا الوطني لمواجهة الطوارئ الحاسوبية مذكرات تفاهم بشأن أمن الفضاء الإلكتروني مع بعض الدول كجورجيا وروسيا وقيرغيزستان وصربيا والبوسنة والهرسك وكرواتيا واليونان.

وأقرت لجنة الدفاع المعنية بالفضاء الإلكتروني لمنظمة حلف شمال الأطلسي مذكرة التفاهم التي توضِّح سبل التعاون بين المنظمة وحلفائها وتأخذ في الاعتبار آراء دولتنا، ووُقعت المذكرة بين المنظمة ووزارة الدفاع في جمهورية تركيا. وأنشئت مراكز اتصال وتجري حالياً أعمال ذات صلة ضمن نطاق مذكرة التفاهم.

وتتابَع أعمال لجنة التخطيط لحالات الطوارئ المدنية التابعة لمنظمة حلف شمال الأطلسي وفريق الموارد الصناعية وخدمات الاتصالات. وعلاوة على ذلك، فإن تركيا عضو في مركز المعرفة ومجمّع الفكر ومرفق التدريب المعتمد لدى منظمة حلف شمال الأطلسي، مركز الامتياز للدفاع التعاوني في الفضاء الإلكتروني لمنظمة حلف شمال الأطلسي، باعتبارها دولة مزكية منذ عام ٢٠١٥.

وتشارك تركيا في اجتماعات منظمة التعاون والتنمية في الميدان الاقتصادي بشأن الأمن والخصوصية وفريق العمل غير الرسمي لمنظمة الأمن والتعاون في أوروبا المعني بأمن الفضاء الإلكتروني، وتساهم في تلك الاجتماعات.

وتتابَع اجتماعات المركز الإقليمي للمساعدة على التحقق من تحديد الأسلحة وتنفيذه، وتتطور سبل التعاون بشأن مختلف المسائل. والهدف الاستراتيجي للمركز الإقليمي هو تعزيز وضع الاستراتيجيات الأمنية الوطنية عن طريق التشجيع على التعاون الأمني الإقليمي والتفاعل الفعال لمواجهة التحديات الأمنية المستجدة على نحو مستدام، مثل أمن الفضاء الإلكتروني والأشكال الأخرى من التهديدات العابرة للحدود الوطنية، بما في ذلك الإرهاب، وانتشار أسلحة الدمار الشامل، والاتجار غير المشروع، والجريمة

المنظمة، وأمن الحدود وإدارتها، وتغير المناخ، في حين يولى اهتمام خاص لجميع التهديدات الأمنية المستجدة الناشئة عنها.

وتشارك تركيا في الجهود المبذولة بشأن تطوير التعاون الدولي. ففريق تركيا الوطني لمواجهة الطوارئ الحاسوبية عضو في كل من منتدى أفرقة الأمن والاستجابة للحوادث، وخدمة المعرّفين الموثوقين، والشراكة الدولية المتعددة الأطراف لمكافحة التهديدات في الفضاء الإلكتروني التابعة للاتحاد الدولي للاتصالات، والبرنامج المتعدد الجنسيات لتبادل المعلومات عن البرامجيات الضارة التابع لمنظمة حلف شمال الأطلسي، وتحالف الفضاء الإلكتروني لإحراز تقدم مشترك، وهي تسعى إلى التعاون قدر الإمكان من أجل تعزيز أمن المعلومات في الفضاء الإلكتروني وتبادل الخبرات والمعلومات المتعلقة بالتهديدات على المستوى الدولي.

وتمرين أمن الفضاء الإلكتروني هو نشاط هام آخر في ما يتعلق بالتعاون والتأهب. ويسهم هذا النوع من التمارين الذي يجرى على الصعيدين الوطني والدولي في تعزيز أمن الفضاء الإلكتروني واختبار التدابير التي ستتخذ لمواجهة التهديدات الإلكترونية المحتملة. وفي هذا السياق، أجريت تمارين أمن الفضاء الإلكتروني الوطنية في الأعوام ٢٠١١ و ٢٠١٢ و ٢٠١٣ و ٢٠١٧ بتنسيق من وزارة النقل والبنى التحتية. وبمشاركة ١٩ بلداً، أُنجز بنجاح التمرين الدولي لدرع الفضاء الإلكتروني في اسطنبول بالتعاون مع الاتحاد الدولي للاتصالات وشراكته الدولية المتعددة الأطراف لمكافحة التهديدات الإلكترونية في ١٥ و ١٦ أيار/مايو ٢٠١٤.

وتشارك تركيا في تمارين دولية متعلقة بأمن الفضاء الإلكتروني وتساهم فيها على نحو منتظم، وهي ائتلاف الفضاء الإلكتروني لمنظمة حلف شمال الأطلسي، والدروع المقفلة لمنظمة حلف شمال الأطلسي، وتمرين إدارة الأزمات لمنظمة حلف شمال الأطلسي.

وبما أن الفضاء الإلكتروني ميدان لا حدود له، قد تختلف مصادر وأهداف الهجمات الإلكترونية باختلاف البلدان، بما في ذلك المتحالفة منها. فقد يكون مركز قيادة وسيطرة في بلد ما في حين أن هدفه يمكن أن يكون في بلد آخر. ولهذا السبب، يؤدي تبادل المعلومات عن الهجمات الإلكترونية ومجرمي الفضاء الإلكتروني دوراً حاسماً في سياق مكافحة التهديدات الإلكترونية على الصعيد العالمي.

وفُتح في بودابست في عام ٢٠٠١ باب توقيع الاتفاقية المتعلقة بالجريمة الإلكترونية، التي وضعها مجلس أوروبا ودخلت حيز النفاذ في عام ٢٠٠٤، وهي الاتفاقية الوحيدة الملزمة. ووقعتها تركيا في ستراسبورغ في عام ٢٠١٠. وتغطي الاتفاقية جرائم مختلفة من قبيل الجرائم التي ترتكب عن طريق الإنترنت وغيرها من الشبكات الحاسوبية، والاحتيال المتصل بالحاسوب، واستغلال الأطفال في المواد الإباحية وانتهاكات أمن الشبكات، وجميع هذه الجرائم مدرجة الآن في التشريعات الوطنية في تركيا. وبالإضافة إلى ذلك، يغطي القانون الجنائي التركي الدخول غير المأذون به إلى نظم تكنولوجيا المعلومات، مع عمليات التشويش أو الاعتراض أو التعديل أو التدمير غير المأذون بها فيما يتعلق بتلك النظم. ويُعاقب الأشخاص الذين يدانون بارتكاب تلك الجرائم بالسجن لمدة تصل إلى ٣ سنوات أو بدفع غرامات. وبعد ذلك، أُقرت الاتفاقية عن طريق القانون المتعلق بالموافقة على التصديق على الاتفاقية المتعلقة بالجريمة الإلكترونية وأُنجز العمل المتعلق بتكيفها مع التشريعات المحلية في عام ٢٠١٦.