الأمم المتحدة

A/77/92

الجمعية العامة

Distr.: General
8 June 2022
Arabic
Original: Arabic/English/Russian/
Spanish

الدورة السابعة والسبعون

البند 94 من القائمة الأولية*

التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي

التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وتعزيز السلوك المسؤول من جانب الدول في استخدام تكنولوجيات المعلومات والاتصالات

تقرير الأمين العام

المحتويات

* A/77/150.

270722 180722 22-08761X (A)

أولا - مقدمة

1 - في 6 كانون الأول/ديسمبر 2021، اتخذت الجمعية العامة القرار 19/76 المعنون "التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وتعزيز السلوك المسؤول من جانب الدول في استخدام تكنولوجيات المعلومات والاتصالات"، في إطار البند 95 من جدول الأعمال، بشأن "التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي".

2 - وفي الفقرة 6 من القرار 19/76، دعت الجمعية العامة جميع الدول الأعضاء إلى أن تواصل، آخذة في اعتبارها التقييمات والتوصيات الواردة في تقرير الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي وتقارير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، 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 تقرير الفريق العامل المفتوح العضوية وتقارير فريق الخبراء الحكوميين.

3 - وعملاً بذلك الطلب، أُرسلت مذكرة شفوية في 24 كانون الثاني/يناير 2022 إلى جميع الدول الأعضاء تدعوها إلى تقديم معلومات بشأن هذا الموضوع.

4- ويتضمن الفرعان الثاني والثالث من هذا التقرير الردود التي وردت حتى وقت إعداده. وستُنشر الردود الإضافية الواردة بعد 31 أيار/مايو 2022 في الموقع الشبكي لمكتب شؤون نزع السلاح (www.un.org/disarmament/ict-security) باللغة الأصلية التي وردت بها.

ثانيا - الردود الواردة من الحكومات

أرمينيا

[الأصل: بالإنكليزية]

[31 أيار/مايو 2022]

الجهود المبذولة على الصعيد الوطني لتعزيز أمن المعلومات وتشجيع التعاون الدولي

أنشأت حكومة أرمينيا مجلساً للرقمنة من أجل تعزيز تنمية المهارات الرقمية ورقمنة نظام الإدارة العامة والاقتصاد. ووفقاً لبيانات عام 2021، تمت مناقشة ما يقرب من 25 برنامجاً ووثيقة استراتيجية، ويجري العمل المستمر في مجالات تحديد الهوية الرقمية، والتحقق من صحة الوثائق الرسمية، ومنح التراخيص الإلكترونية، واستحداث الإشعارات الفردية والعامة، واستحداث نُظم موحدة للعدالة الإلكترونية، وفيما يتعلق بعدد من المسائل الأخرى المدرجة على برنامج العمل الرقمي.

ووافقت جمهورية أرمينيا في 11 شـــباط/فبراير 2021 على اســـتراتيجية للرقمنة. وتتوخى هذه الاســـتراتيجية تحقيق التحول الرقمي للحكومة والاقتصـــاد والمجتمع من خلال إدخال وتطوير التكنولوجيات المبتكرة، وأمن الفضـــاء الإلكتروني، وســـياســـة البيانات، والخدمات الإلكترونية ونظم الحكومة الإلكترونية، وتنســـيق عمليات الرقمنة، وتحديد معايير مشـــتركة وبيئة رقمية، فضـــلاً عن القيام بمبادرات للتشـــجيع على استخدام التكنولوجيات الرقمية في القطاع الخاص للاقتصاد ووضع وتنفيذ برامج تشجع على استخدام عامة الجمهور للأدوات الإلكترونية.

ومن المقرر الاضـــطلاع بالمبادرات التالية في إطار اســـتراتيجية الرقمنة في أرمينيا للفترة 2021–2025:

(أ) إجراء التعديلات التشريعية والقانونية المعيارية في مجال أمن المعلومات؛

(ب) بلورة مفهوم لسياسة عامة للبيانات المفتوحة؛

(ج) تنفيذ التدريب على أمن الفضـــاء الإلكتروني لســـكان القرى الحدودية (يجري حالياً تنظيم دورات في مجال أمن الفضاء الإلكتروني لموظفي الدولة)؛

(د) إنشـــاء مركز وطني لأمن الفضـــاء الإلكتروني. ويجري النظر بوجه خاص في إمكانية وضـع معايير لأمن الفضـاء الإلكتروني، وإنشـاء أفرقة حكومية للاسـتجابة السـريعة، وتنفيذ أنشـطة للتوعية العامة تهدف إلى زيادة الإلمام بالمسائل الإلكترونية.

وتعتزم وزارة الصـناعة الرفيعة التكنولوجيا وضـع سياسـة شـاملة وخطة عمل للتغلب على التحديات في مجال أمن الفضـاء الإلكتروني، ستشـمل عملية إنشـاء المركز وتشـكيل آليات لإدارة المخاطر والاسـتجابة السريعة خلال الكوارث الطبيعية وحالات الطوارئ والأحكام العرفية.

وتشـدد الوزارة على أهمية التعاون الوثيق مع القطاع الخاص، والتعاون فيما بين الوكالات، وتوطين الخبرات الدولية، ومراعاة المعايير الدولية لأمن الفضـاء الإلكتروني، والتعاون فيما بين الدول، والعضـوية في الهياكل الأمنية الدولية.

وتعكف أرمينيا على وضـع السـياسـات وتنمية القدرات في مجال أمن الفضـاء الإلكتروني بالتعاون مع المنظمات الدولية والإقليمية، بسـبل منها مشـاركة المؤسـسـات الأرمينية ذات الصـلة في مختلف الحلقات الدراسية والمؤتمرات والدورات التدريبية المواضيعية.

وجمهوريـة أرمينيـا طرف في اتفـاقيـة مجلس أوروبـا المتعلقـة بـالجريمـة الإلكترونيـة. وفي الآونـة الأخيرة، شـــرعت أرمينيا في إجراء وطني للتوقيع على البروتوكول الإضـــافي الثاني بشـــأن تعزيز التعاون والكشف عن الأدلة الإلكترونية الملحق باتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية.

وتشـــارك أرمينيا مشـــاركة فعالة في الجهود التي يبذلها الفريق العامل المفتوح العضـــوية المعني بالتطورات في ميدان المعلومات والاتصـالات السـلكية واللاسـلكية في سـياق الأمن الدولي. وقد صُـمم الفريق العامل تصميماً فريداً ليشكل الأساس لوضع معايير جديدة في ميدان تكنولوجيا المعلومات والاتصالات.

ويهدف التعاون الجاري في إطار "المشـروع الإلكتروني للمنطقة الشـرقية" التابع لمجلس أوروبا إلى بناء القدرات لدى خبراء المؤسسات الحكومية الأرمينية في مجال مكافحة تهديدات الجريمة الإلكترونية.

وتقدّر أرمينيا أيضـــاً الجهود المتواصـــلة الجاري بذلها في إطار تدابير منظمة الأمن والتعاون في أوروبا لبناء الثقة في مجال تكنولوجيا المعلومات والاتصـالات، التي تسـاعد على بناء الشـفافية والقدرة على التنبؤ والاستقرار في ذلك المجال.

ومن الأمور الجديرة بالملاحظة في الوقت نفســـه، التعاون مع الشـــركات التي تتجاوز الحدود الوطنية. إذ تستضـيف أرمينيا شـركات رائدة في مجال تكنولوجيا المعلومات، مثل سـينوبسـيس Synopsys ومنتور غرافيكس Mentor Graphics وناشـيونال إنسـترومنتس National Instruments وميكروسـوفت Microsoft وفي إم وير VMware ودي-لنك D-Link وأوراكل Oracle وســيســكو Cisco وغيرها. وتبدي ميكروسـوفت Microsoft وسـيسـكو Cisco تعاونهما أو تحضـران المنتديات بانتظام من أجل دعم حكومة أرمينيا بأحدث التطورات في مجال أمن الفضاء الإلكتروني والدفاع الإلكتروني.

أستراليا

[الأصل: بالإنكليزية]

[31 أيار/مايو 2022]

تعرب أســتراليا عن ترحيبها بالفرصـــة التي أتيحت لها، اســتجابة للدعوة الواردة في قرار الجمعية العامة 19/76، لموافاة الأمين العام بآرائها فيما يتعلق بتعزيز السلوك المسؤول من جانب الدول في الفضـاء الإلكتروني. ويســتند هذا التقرير إلى المعلومات التي قدمتها أســتراليا اســتجابةً للقرارات الســابقة للجمعية العامة[(1)]، بما في ذلك مؤخراً في أيار/مايو 2021 (انظر A/76/187). وتشـجع أسـتراليا جميع الدول على المشـاركة بشـكل اسـتباقي في تقديم معلومات مسـتكملة منتظمة إلى الأمين العام، بغية زيادة الشـفافية وبناء الفهم لجهود بعضها البعض الرامية إلى الارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني.

إطار السلوك المسؤول من جانب الدول في الفضاء الإلكتروني

وتؤكد تقارير فريق الخبراء الحكوميين المعني بالتطورات في مجال المعلومات والاتصـالات السلكية واللاســلكية في ســياق الأمن الدولي للأعوام 2010 و 2013 و 2015[(2)] مجتمعة أن القانون الدولي القائم واجب التطبيق وضـروري للحفاظ على السـلام والاسـتقرار في الفضـاء الإلكتروني. وتوضـح التقارير أيضـاً 11 معياراً طوعياً غير ملزم لسلوك الدول المسؤول مع التسليم في الوقت ذاته بالحاجة إلى اتخاذ تدابير لبناء الثقة وإلى بناء القدرات على نحو منسـق. وكثيراً ما يشـار إلى هذه المبادئ الأربعة مجتمعة على أنها إطار السلوك المسؤول للدول في الفضاء الإلكتروني.

وقد أعربت أســتراليا عن ســرورها لأن تقرير آذار/مارس 2021 للفريق العامل المفتوح العضــوية المعني بالتطورات في ميدان المعلومات والاتصـــالات الســـلكية واللاســـلكية في ســـياق الأمن الدولي (A/75/816)، الذي تفاوضت عليه وأيدته جميع الدول الأعضاء في الأمم المتحدة البالغ عددها 193 دولة، ينمُّ عن التزام عالمي بهذا الإطار. ومن دواعي سرور أستراليا كذلك أن يشارك خبير بارز في فريق الخبراء الحكوميين السادس المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي،

(1) القرارات 41/65 و 243/68 و 237/70 و 28/74 و 32/75.

(2) A/65/201 و A/68/98 و A/70/174، على التوالي.

الذي قدم كذلك توجيهات عملية إضـــافية فيما يتعلق بكيفية تنفيذ الإطار (انظر A/76/135)، الأمر الذي رحبت به الجمعية العامة لاحقاً في قرارها 19/76.

وتؤكد أســـتراليا من جديد التزامها بالعمل وفقاً لمجموعة تقارير فريق الخبراء الحكوميين ولتقرير الفريق العامل. ولا تزال أستراليا تشارك بنشاط في الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصـالات وأمن اسـتخدامها للفترة 2021–2025، المنشـأ بموجب القرار 240/75، وهي من المشاركين الملتزمين بتقديم اقتراح فرنسا ومصر بوضع برنامج للعمل. وتؤيد أستراليا وضع برنامج عمل يتيح منتدى دائماً وشـاملاً ومتسـماً بالشـفافية للنقاش الجاري والإجراءات العملية الجاري اتخاذها بشـأن المسـائل المتعلقة بالفضاء الإلكتروني تحت رعاية الأمم المتحدة.

ومن منطلق الشـفافية، سـتنشـر أسـتراليا قريباً معلومات مسـتكملة عن كيفية تنفيذها ومراعاتها للمعايير الطوعية الـ 11 غير الملزمة للسلوك المسؤول من جانب الدول. وفي حين أن المعايير لا تحلُّ محل التزامات الدول أو حقوقها بموجب القانون الدولي (وهي حقوق ملزمة) أو تغيرها، فإن أسـتراليا تؤكد من جديد على هذه المعايير الـــــ 11 بوصفها مكملة للقانون الدولي، توفر إرشادات محددة إضافية بشأن ما يشكل سلوكاً مسؤولا للدول في استخدام تكنولوجيات المعلومات والاتصالات. وستتيح أستراليا أيضاً للجمهور تقييمها الذاتي الأولي لتنفيذنا لالتزامات الأمم المتحدة المتعلقة بالفضـاء الإلكتروني باسـتخدام الدراسـة الاسـتقصـائية الوطنية التي أجراها معهد الأمم المتحدة لبحوث نزع السـلاح عن طريق بوابة المعهد لسـياسـات الفضـاء الإلكتروني في المسـتقبل القريب. وتزكّي أسـتراليا هذه الدراسـة الاسـتقصـائية الوطنية لجميع الدول وتشـجع الدول على النظر أيضـاً في إتاحة تقييماتها الذاتية للجمهور. وتوفر الدراسـة الاسـتقصـائية لتنفيذ توصـيات الأمم المتحدة عدة فوائد. وعلى وجه التحديد، يمكن للدول أن تقف على الكيفية التي نفذت بها الإطار، والمواضع التي قد توجد بها ثغرات في التنفيذ وأي عوائق تعترض التنفيذ. ومن المحتمل أن يساعد هذا بدوره في وضع برامج محددة الأهداف للتعاون وبناء القدرات، قد تكون مناسبة للتغلب على أي ثغرات في القدرات و/أو عوائق تعترض التنفيذ يتم تبيُّنها.

القانون الدولي

وتشجع أستراليا جميع الدول على أن تواصل دراسة مواقفها بشأن كيفية انطباق القانون الدولي على سلوك الدول في الفضاء الإلكتروني وأن تتحلى بالشفافية فيما يتعلق بها. ونكرر التأكيد على أنه حتى عندما تختلف وجهات النظر، فإن تفهُّم مواقف بعضـــنا البعض بشـــأن كيفية تطبيق القانون الدولي في الفضـــاء الإلكتروني يزيد من إمكانية التنبؤ ويقلل من مخاطر ســـوء التقدير، الأمر الذي قد يؤدي إلى تصـــعيد في سلوك الدول. وتؤكد أسـتراليا مجددًا كذلك أن أقصـى قدر من فعالية القانون الدولي يتحقق عندما تنفذ الدول التزاماتها القانونية الدولية وتتقيَّد بها، وحيثما تتعاون، عند الضـرورة، لدعم القانون الدولي وضـمان المسـاءلة عن الانتهاكات.

وقد رحَّبت أســـتراليا بـالاســـتنتاجات الواردة في تقرير فريق الخبراء الحكوميين لعام 2021 (A/76/135) بأن القانون الدولي الإنساني ينطبق على الأنشطة الإلكترونية في حالات النزاع المسلح.

ويرد عرض لموقف أسـتراليا بشـأن كيفية انطباق القانون الدولي على سـلوك الدول في الفضـاء الإلكتروني في مجموعة من الوثائق هي:

- تقرير أستراليا لعام 2021 الوارد في الثُبت الرسمي بالمساهمات الوطنية الطوعية المتعلقة بموضوع كيفية انطباق القانون الدولي على استخدام الدول لتكنولوجيا المعلومات والاتصالات، التي قدمها الخبراء الحكوميون المشاركون في فريق الخبراء الحكوميين (A/76/136)؛
- الاستراتيجية الدولية لعام 2021 للتعامل مع تكنولوجيا الفضاء الإلكتروني والتكنولوجيا الحيوية؛
- دراسات الحالة الإفرادية لعام 2020 عن سريان القانون الدولي على الفضاء الإلكتروني (قُدّمت إلى الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي)؛
- ملحق القانون الدولي لعام 2019؛
- الاستراتيجية الدولية لعام 2017 للتعامل مع الأنشطة الدولية في مجال الفضاء الإلكتروني.

وبالإضافة إلى مشاركة أستراليا في عمليات الأمم المتحدة المتعلقة بانطباق القانون الدولي على الفضاء الإلكتروني، فهي تسعى أيضاً إلى المشاركة في المناقشات التي تجري في هذا الصدد في المحافل الإقليمية. وفي هذا الصدد، أدلت أستراليا في أواخر عام 2021 ببيان في الدورة التاسعة والخمسين للمنظمة الاستشارية القانونية الآسيوية الأفريقية بشأن القانون الدولي في الفضاء الإلكتروني.

الردع والتصدي لسلوك الدول غير المسؤول

ولا تتسامح أستراليا مع الأنشطة في الفضاء الإلكتروني التي تضرُّ بالسلم والاستقرار الدوليين أو التي تتعارض مع الإطار، الذي اتفقت عليه جميع الدول الأعضاء في الأمم المتحدة. وتشجع أستراليا المجتمع العالمي على تسليط الضوء على النشاط الإلكتروني الخبيث ومحاسبة الجهات الفاعلة المسؤولة. وتتبع أستراليا سياسة تقضي بنسبة النشاط الإلكتروني الخبيث إلى صاحبه علناً عندما يكون المصدر معروفاً وعندما يكون من مصلحتنا القيام بذلك. ولا تستهدف هذه السياسة أي بلد بعينه. وقد نسبت أستراليا النشاط الإلكتروني الخبيث علناً، حتى الآن، في 13 مناسبة. وفي الآونة الأخيرة، في 10 أيار/مايو 2022، انضمت أستراليا إلى الولايات المتحدة الأمريكية والاتحاد الأوروبي في نسبة مجموعة من الأنشطة الإلكترونية المدمرة والتخريبية والمزعزعة للاستقرار ضد أوكرانيا إلى الحكومة الروسية.

مشاركة أصحاب المصلحة المتعددين

وتشكر أستراليا برهان غفور، رئيس الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025، على جهوده البنَّاءة للتوصل إلى اتفاق بتوافق الآراء بشأن مجموعة من الطرائق الشفافة والمتوازنة لمشاركة أصحاب المصلحة غير الحكوميين في الفريق العامل في المستقبل. وتتطلع أستراليا إلى اعتماد هذه الطرائق رسمياً في الدورة الموضوعية الثالثة للفريق العامل، المقرر عقدها في تموز/يوليه 2022. وتدعم أستراليا بثبات مشاركة أصحاب المصلحة المتعددين في المناقشات المتعلقة بسلوك الدول المسؤول في الفضاء الإلكتروني. والفضاء الإلكتروني فريد من نوعه: يؤدي القطاع الخاص والأوساط التقنية والمجتمع المدني والدوائر الأكاديمية دوراً حيوياً في إدارته وحوكمته على الصعيد التقني، ويمكن لدوائر أصحاب المصلحة المتعددين تقديم وجهات نظر تساعدنا على فهم التهديدات الإلكترونية الناشئة وآثارها وكيفية معالجتها بشكل أفضل. وقد أصيبت أستراليا بخيبة أمل إزاء

الجهود التي تبذلها بعض الدول لعرقلة مشاركة أصحاب المصلحة في هذه العملية، الأمر الذي نرى أنه تتعارض مع الروح التي أنشئ بها الفريق العامل. وتعتقد أستراليا أن الفريق العامل من شأنه أن يكون له تأثير بعيد المدى على كثير من أصحاب المصلحة، بما في ذلك إحداث آثار مباشرة على المجتمعات المحلية والأفراد، وأن التصدي للتهديدات الناشئة عن الفضاء الإلكتروني يقتضي منا الاستفادة من تجارب جميع أصحاب المصلحة المعنيين وخبراتهم ومواردهم. ولذلك، فهي ترحب بالطرائق المتفق على اتباعها بوصفها خطوة نحو الشفافية واستيعاب الجميع.

المرأة في مجال الفضاء الإلكتروني

حسبما تسلم به الخطة المتعلقة بالمرأة والسلام والأمن، تتأثر النساء والفتيات على نحو فريد وغير متناسب بالنزاعات والأزمات، كما أنهن ممثلات تمثيلاً ناقصاً في عمليات السلام والأمن الدوليين (ومستبعدات منها). وعلى نحو ما هو محدد في تقرير معهد الأمم المتحدة لبحوث نزع السلاح المعنون "ما زلنا متخلفين عن الركب: التوازن بين الجنسين في دبلوماسية تحديد الأسلحة وعدم الانتشار ونزع السلاح"، فإن عمليات اللجنة الأولى تتخلف بشكل كبير عن الخطوات التي تخطوها لجان الأمم المتحدة الأخرى نحو تحقيق التكافؤ بين الجنسين. ويتبيَّن من بيانات المعهد أن 27 في المائة من المتكلمين في مناقشات اللجنة الأولى هم من النساء. وتنخفض هذه النسبة إلى ما متوسطه 20 في المائة في المنتديات التي تتناول مواضيع أكثر تخصصاً.

ولمعالجة ذلك، أطلقت أستراليا، إلى جانب كندا والمملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية ونيوزيلندا وهولندا والولايات المتحدة، زمالة المرأة في مجال الأمن الدولي والفضاء الإلكتروني في شباط/فبراير 2020. وتوفر هذه الزمالة للدبلوماسيات في الفترة من أوائل إلى منتصف حياتهن المهنية التدريب على المفاوضات المتعددة الأطراف، وسياسات الفضاء الإلكتروني، والقانون الدولي، وتدعم سفرهن إلى نيويورك للانضمام إلى الوفود الوطنية لبلادهن في اجتماعات الأمم المتحدة التي تنظر في السلوك المسؤول من جانب الدول في الفضاء الإلكتروني، بما في ذلك في اجتماعات الفريق العامل.

ومن دواعي سرور أستراليا أن العديد من الزميلات تمكنَّ، عن طريق الزمالة، من الانضمام إلى وفود بلادهن الوطنية في الدورتين الأولى والثانية للفريق العامل وقدَّمن مساهمة كبيرة في الفريق العامل وفي النهوض بالخطة المتعلقة بالمرأة والسلام والأمن. ففي الدورة الأولى للفريق العامل، التي عقدت في كانون الأول/ديسمبر 2021، قدمت المتكلمات ما نسبته 37 في المائة من المداخلات. وفي دورته الثانية، التي عقدت في آذار/مارس 2022، أدلت النساء المتكلمات بما نسبته 43 في المائة من المداخلات، ونصف جميع البيانات المتعلقة بالقانون الدولي.

أذربيجان

[الأصل: بالإنكليزية]

[31 أيار/مايو 2022]

خلال السنوات الأخيرة، أُقِرَّت عدة قوانين جديدة في أذربيجان من أجل ضمان أمن المعلومات. وبالإضافة إلى ذلك، اعتُمد مفهوم التنمية، وخريطة الطريق الاستراتيجية، والاستراتيجية الوطنية، وبرامج الدولة، وأُرسي التعاون مع مختلف البلدان بموجب مراسيم وأوامر صادرة عن رئيس أذربيجان.

ونظراً لضـــرورة اعتبار أمن الهياكل الأســـاســـية الحيوية للمعلومات من الأولويات، اعتُمد قانون معياري لتعزيز الأمن في هذا المجال. ويراعى في القانون الســالف الذكر تصـــنيف المرافق الخاصـــة بهذه الهياكل الأســـاســـية وفقاً لأهميتها وتحديد المتطلبات الأمنية العامة والخاصـــة، ومن المتوخى أن يُضـــطلع بالمراقبة المستمرة من خلال تطبيق الأساليب المناسبة.

وأنشئت لجنة التنسيق المعنية بأمن المعلومات في عام 2018، بناء على أمر من رئيس أذربيجان.

وحفاظاً على أمن الهياكل الأساسية الحيوية للمعلومات، تقرر توزيع السلطات بين المؤسسات وفقاً لمرسوم رئيس أذربيجان المؤرخ 17 نيسان/أبريل 2021.

ولتعزيز رأس المال البشـــري في هذا المجال، نظمت الأكاديمية الإلكترونية التابعة لوزارة التنمية الرقمية والنقل دورات تدريبية مختلفة، تمنح شهادات وطنية ودولية.

وعقد خبراء دوليون حلقات دراسـية افتراضـية بشـأن حماية البيانات الشـخصـية والجرائم الإلكترونية والأدلة الإلكترونية لممثلي الهيئات الحكومية ذات الصـــلة في أذربيجان، في إطار البرنامجين "المشـــروع الإلكتروني للمنطقة الشـرقية" و "مشـروع أمن الفضـاء الإلكتروني للمنطقة الشـرقية" المشـتركين بين الاتحاد الأوروبي ومجلس أوروبا.

وحضـــر ممثلو عدة هيئات حكومية في أذربيجان أول تدريب معتمد لهم بشـــأن أمن الفضـــاء الإلكتروني، في إطار برنامج المنح التابع للوكالة الكورية للتعاون الدولي.

وبالإضـــافة إلى ما ذكر أعلاه، أجريت مشـــاورات وأقيمت مبادرات للتعاون مع أفرقة التصـــدي للطوارئ الحاسوبية التابعة لدول مختلفة.

وتحتل أذربيجان المرتبة الأربعين في العالم والثالثة (بعد الاتحاد الروســي وكازاخســتان) في رابطة الدول المستقلة في المؤشر العالمي للأمن الإلكتروني لعام 2020 الصادر عن الاتحاد الدولي للاتصالات.

ونظراً للزيادة في عدد التهديدات الإلكترونية خلال جائحة مرض فيروس كورونا (كوفيد-19) ، فضلاً عن نقاط الضعف المكتشفة في المعدات البرنامجية والتقنية، فقد جرى نشر الإخطارات والرسائل ذات الصلة المتعلقة بطرق الحماية من التهديدات الإلكترونية على الموقع www.cert.az وعلى شبكات التواصل الاجتماعي.

كوبا

[الأصل: بالإسبانية]

[31 أيار/مايو 2022]

لا تزال إساءة استخدام تكنولوجيات المعلومات والاتصالات السلكية واللاسلكية مثار قلق بالغ لدى المجتمع الدولي، ومن هنا تبرز الحاجة إلى التصدي للتهديدات المتزايدة في ذلك المجال.

وندين إســاءة اســتخدام المنصــات الإعلامية، بما في ذلك وســائط التواصــل الاجتماعي والبث الإذاعي، كأداة للتدخل في شؤون الدول من خلال الترويج لخطاب الكراهية والتحريض على العنف والتخريب

وزعزعة الاستقرار ونشر الأخبار الزائفة وتحريف الواقع لأغراض سياسية وكذريعة لشن الحرب أو للتهديد باستعمال القوة أو استعمالها، في انتهاك لمقاصد ميثاق الأمم المتحدة والقانون الدولي ومبادئهما.

وفي هذا الصدد، نرفض أساليب الحرب غير التقليدية التي تشنها حكومة الولايات المتحدة ضد كوبا، بوسائل منها استخدام تكنولوجيات المعلومات الجديدة وغيرها من المنصات الرقمية لزعزعة استقرار بلدنا وتشويه سمعته.

ونؤكد من جديد أن من حق الدول ومن واجبها التصدي، ضمن صلاحياتها الدستورية، لنشر الأخبار الكاذبة أو المشوهة، التي يمكن أن تفسر على أنها تدخل في الشؤون الداخلية لدول أخرى أو على أنها أخبار ضارة بجهود تعزيز السلام، وأواصر التعاون، والعلاقات الودية بين الدول والأمم.

ولا يمكننا أن نتجاهل أن التطوير المتزايد للقدرات والعمليات الهجومية الإلكترونية يمكن أن يحوّل الفضاء الإلكتروني إلى مسرح جديد للنزاع. ونرفض المحاولات الرامية إلى مساواة الاستخدام الخبيث لتكنولوجيات المعلومات والاتصالات بمفهوم "الهجوم المسلح" بغية تبرير ممارسة حق الدفاع عن النفس المنصوص عليه في المادة 51 من ميثاق الأمم المتحدة.

ونرفض الاستخدام المتعمد لهذه التكنولوجيات لإلحاق الضرر بالهياكل الأساسية الحيوية للدول الأخرى، بما في ذلك نظم المعلومات الخاصة بها، أو لإعاقة استخدام وتشغيل الهياكل الأساسية الحيوية، وهو أمر ضروري للاستقرار الاجتماعي للدول وأمنها.

والأمم المتحدة هي المنتدى المتعدد الأطراف البارز والمنبر الرئيسي لمعالجة شواغل دولها الأعضاء فيما يتعلق بأمن تكنولوجيات المعلومات والاتصالات واستخدامها. وفي هذا الصدد، يمثل الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025، المنشأ عملا بقرار الجمعية العامة 240/75، الآلية الشاملة الوحيدة المتاحة للدول الأعضاء لمناقشة قضايا أمن الفضاء الإلكتروني بطريقة شفافة وعلى قدم المساواة.

ونؤكد مجدَّداً أهمية الفريق العامل السالف الذكر ونأمل أن تسهم هذه العملية الحكومية الدولية في ملء الفراغ القانوني الحالي بمعايير ملزمة تُفضي إلى اعتماد صك قانوني شامل بشأن تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي.

ورغم أن تدابير بناء الثقة أداة مفيدة، فإن هذه التدابير وحدها لا تضمن الاستخدام السلمي المحض لتكنولوجيات المعلومات والاتصالات، نظراً لعدم وجود صك قانوني ملزم قانوناً من هذا القبيل في هذا المجال.

وكوبا، بوصفها عضواً في حركة بلدان عدم الانحياز، تهيب مرة أخرى بالبلدان المتقدمة النمو والكيانات الدولية ذات الصلة أن تقدم إلى البلدان النامية، بناء على طلبها، المساعدة والتعاون، بوسائل منها توفير الموارد المالية وبناء القدرات ونقل التكنولوجيا، مع مراعاة الاحتياجات والخصائص المحددة لكل دولة متلقية.

ونعارض تطبيق التدابير القسرية الانفرادية، كالحصار الاقتصادي والتجاري والمالي الذي تفرضه حكومة الولايات المتحدة على كوبا، التي تمنع أو تحدُّ من وصول الجميع إلى تكنولوجيات المعلومات والاتصالات واستخدامها والتمتع بها في الأغراض السلمية من أجل رفاه سكاننا.

الدانمرك

[الأصل: بالإنكليزية]

[31 أيار/مايو 2022]

تشـــكل الحلول الرقمية في الدنمارك، كما هو الحال في أجزاء كثيرة من العالم، جزءاً لا يتجزأ من الحياة اليومية. وهي في آن واحد منبر للأنشطة المجتمعية الأساسية ومحرك رئيسي للنمو الاقتصادي. ومع ذلك، فمع تزايد ترابط مجتمعاتنا وهياكلنا الأســاســية الرقمية، تزداد أيضــاً قدرة الجهات من الدول ومن غير الدول على القيام بأنشــطة إلكترونية خبيثة واســتعدادها لذلك. وينبغي أن يكون هذا الأمر موضــع اهتمام عالمي، لأن الأنشطة الخبيثة في الفضاء الإلكتروني قد تشكل أفعالاً غير مشروعة بموجب القانون الدولي وتؤدي إلى تصــعيد محتمل، مما يهدد بدوره الأمن والاســتقرار الدوليين. وغزو روســيا غير المبرر وغير القانوني لأوكرانيا، الذي يشمل أيضاً الهجمات الإلكترونية ضد الهياكل الأساسية الحيوية، أمر مثير للقلق بشكل خاص وغير مقبول على الإطلاق، لأنه يشكل انتهاكاً للقانون الدولي ويقوّض إطار السلوك المسؤول للدول في الفضاء الإلكتروني.

وبناء على ذلك، فلا تزال الدانمرك، بوصــفها واحدة من أكثر البلدان اســتخداماً للتكنولوجيا الرقمية في العالم، مصــممة على منع الأنشــطة الخبيثة وردعها والتصــدي لها، وعلى تعزيز التعاون الدولي لهذا الغرض. وتســعى الدانمرك، جنباً إلى جنب مع الاتحاد الأوروبي، إلى تعزيز التعاون الدولي من أجل إنشــاء فضاء إلكتروني عالمي ومنفتح ومستقر وسلمي وآمن تُطبَّق فيه حقوق الإنسان والحريات الأساسية وسيادة القانون تطبيقاً كاملاً. وفي هذا الصدد، تشدد الدانمرك على أهمية تقيد الدول بإطار السلوك المسؤول للدول في الفضـــاء الإلكتروني، الذي يدعم النظام الدولي القائم على القواعد، وتؤكد وجوب تطبيق القانون الدولي، والامتثال للمعايير الطوعية لسلوك الدول المسؤول، ووضــع تدابير عملية لبناء الثقة وتنفيذ تلك التدابير. وقد أكَّد جميع أعضــاء الجمعية العامة هذا الإطار مراراً وتكراراً بوصــفه حجر الزاوية في جهود المجتمع الدولي الرامية إلى ردع ســلوك الدول المتهور وغير المســؤول في الفضـــاء الإلكتروني وتجنب أكثر الهجمات الإلكترونية ضرراً وحالات التصعيد المحتمل. ولذلك، ندعو جميع الدول الأعضاء، بما فيها الاتحاد الروسي، إلى الوفاء بالتزاماتها.

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

لقد اتخذت الدانمرك، حتى الآن، عدَّة خطوات لتعزيز أمنها في مجال المعلومات وفي فضـــائها الإلكتروني وتشــجيع التعاون الدولي في مجال أمن الفضــاء الإلكتروني. ويخصــص اتفاق الدفاع الدانمركي للفترة 2018–2023 مبلغاً قدره 1,4 بليون كرونة دانمركية لتعزيز أمن الفضـــاء الإلكتروني والدفاع الإلكتروني، وبالتالي تعزيز قدرة المجتمع الدانمركي على الصمود وصلابته في مواجهة الهجمات الإلكترونية.

وبصدور الاستراتيجية الدانمركية لأمن الفضاء الإلكتروني وأمن المعلومات للفترة 2018–2021، استحدثت 25 مبادرة، علاوة على ستّ استراتيجيات مخصَّصة، للأهداف التالية:

(أ) زيادة أمن الفضاء الإلكتروني وأمن المعلومات، لا سيما في القطاعات الحيوية؛

(ب) ضمان بذل جهود منهجية ومنسقة؛

(ج) تعزيز القدرة التكنولوجية للهياكل الأساسية الرقمية على الصمود؛

(د) تحسين معرفة المواطنين والشركات والسلطات فيما يتعلق بأمن الفضاء الإلكتروني.

وفي إطار هذه الاستراتيجية، أنشئت وحدات مخصصة لأمن الفضاء الإلكتروني وأمن المعلومات في القطاعات الحيوية الستة (الطاقة، والمالية، والنقل، والرعاية الصحية، والاتصالات السلكية واللاسلكية، والبحرية)، فضلاً عن منتديات لتتبادل الوحدات من خلالها الخبرات.

وكذلك أطلق مركز أمن الفضاء الإلكتروني أكاديمية إلكترونية مكثفة خاصة به وهو يدعم التعليم والبحث على نطاق واسع في مجال أمن الفضاء الإلكتروني. وبالمثل، أعدَّت وكالة الحكومة الرقمية عدة دورات دراسية ومواد تعليمية وفعاليات بشأن أمن الفضاء الإلكتروني وأمن المعلومات موجهة إلى الرؤساء التنفيذيين والأخصائيين في مجال الفضاء الإلكتروني والموظفين العموميين.

وبالإضافة إلى ذلك، أعدَّت وكالة الحكومة الرقمية الموقع الشبكي www.sikkerdigital.dk، الذي يوفر للمواطنين إرشادات عملية بشأن أمن الفضاء الإلكتروني وأمن المعلومات ويدير حملات وطنية بشأن السلوك الرقمي الآمن بالتعاون الوثيق مع البلديات والمناطق.

وقد أنشأت الدانمرك مجلساً للأمن الإلكتروني (Cybersikkerhedsråd) مشتركاً بين القطاعين العام والخاص، يقدّم المشورة للحكومة بشأن كيفية تعزيز أمن الفضاء الإلكتروني وتحسين تبادل المعارف بين السلطات والشركات التجارية والباحثين. وأخيراً، بفضل الاستراتيجية الدانماركية لأمن الفضاء الإلكتروني وأمن المعلومات للفترة 2018-2021، عززت الدنمارك أيضاً مشاركتها في العمل الدولي بشأن الفضاء الإلكتروني، مما أتاح للبلد زيادة مشاركته في المنتديات الإلكترونية المتعددة الجنسيات، من قبيل الأمم المتحدة، والاتحاد الأوروبي، ومنظمة حلف شمال الأطلسي(ناتو)، ومنظمة الأمن والتعاون في أوروبا.

وفي كانون الأول/ديسمبر 2021 ، قدمت الحكومة استراتيجية وطنية جديدة للأمن السيبراني وأمن المعلومات للفترة 2022-2024. وتستند هذه الاستراتيجية إلى الجهود الحالية وتتوسع فيها من خلال زيادة تعزيز أمن الفضاء الإلكتروني وأمن المعلومات عن طريق 34 مبادرة رئيسية تستهدف القطاعين العام والخاص والمواطنين الدانمركيين بوجه عام. وبشكل عام، تتضمن الاستراتيجية أربعة أهداف رئيسية على النحو التالي:

(أ) أولاً، تعمل الاستراتيجية على تعزيز قدرة الهياكل الأساسية الحيوية لتكنولوجيا المعلومات والاتصالات التي تدعم قدرة الوظائف المجتمعية الحيوية على الصمود. ولضمان مستوى كاف من أمن الفضاء الإلكتروني لكل من الوكالات الحكومية والشركات التجارية ، بُدئ في اتخاذ سلسلة من الإجراءات الاستراتيجية، بما في ذلك تشديد المتطلبات الأمنية لإدارة النظم الحكومية لتكنولوجيا المعلومات والاتصالات ذات الأهمية الحيوية للمجتمع وتعزيز استجابة الشرطة للجرائم الإلكترونية. وتزيد الاستراتيجية كذلك عدد القطاعات الحيوية لتشمل مجموعة أوسع من الوكالات الحكومية المسؤولة عن الوظائف المجتمعية الحيوية المدعومة بتكنولوجيا المعلومات. ويتعين على الوكالات الحكومية في هذه القطاعات الحيوية الامتثال لعدد من المتطلبات الأمنية المحددة بالإضافة إلى الحد الأدنى من المتطلبات التي سبق استحداثها في استراتيجية الفترة 2018-2021. والغرض من ذلك هو ضمان أن تكون الوزارات التي تضطلع بمسؤولية خاصة عن الوظائف المجتمعية الحيوية قادرة على التصرف بسرعة وكفاءة في حالة وقوع حادث إلكتروني خطير؛

(ب) ثانياً، تشمل الاستراتيجية عدداً من المبادرات التي تعزز مهارات أمن الفضاء الإلكتروني لدى المواطنين الدانمركيين وتزيد من التزام الإدارة بتعزيز أمن الفضاء الإلكتروني. ومن بين هذه المبادرات برامج تدريبية جديدة مخصصة لموظفي الحكومة، فضلاً عن برامج تعليمية تزود الأطفال والشباب والكبار بالكفاءات اللازمة ليكونوا على إلمام بالتكنولوجيا الرقمية. وعلاوة على ذلك، يواجه كبار المديرين والقادة متطلبات وتوقعات متزايدة بإيلاء أولوية للأمن الإلكتروني وأمن المعلومات؛

(ج) ثالثاً، تعزز الاستراتيجية التعاون في مجال أمن الفضاء الإلكتروني وأمن المعلومات بين القطاعين العام والخاص. وتتسم إمكانية تبادل المعرفة والخبرات بين القطاعات بأهمية بالغة لتحقيق مستوى رفيع من أمن الفضاء الإلكتروني وأمن المعلومات. ولهذا السبب، سيُنشأ خط هاتفي ساخن لشؤون الفضاء الإلكتروني، سييسّر التماس المشورة فيما يتعلق بالجرائم الإلكترونية، كما ستُنشأ وحدة مكرسة للأمن الإلكتروني للمؤسسات الصغيرة والمتوسطة الحجم، من أجل تعزيز قدرة مركز أمن الفضاء الإلكتروني على تقديم التوجيه؛

(د) رابعاً، تعزز الاستراتيجية كذلك الجهود الدولية التي تبذلها الدانمرك في مجال أمن الفضاء الإلكتروني. ويشمل ذلك تخصيص موارد إضافية لخدمتها الدبلوماسية من أجل تعزيز مساهمة البلد في التعاون المتعدد الأطراف فيما يتعلق بأمن الفضاء الإلكتروني داخل الاتحاد الأوروبي ومنظمة حلف شمال الأطلسي والأمم المتحدة وتشجيع التعاون مع صناعة التكنولوجيا الدولية والأوساط الأكاديمية ومراكز الفكر، فضلاً عن فرض ضوابط التصدير على المنتجات الرقمية. وأخيراً، تشمل الاستراتيجية أيضاً مبادرات من شأنها تعزيز الجهود التي يبذلها البلد على الصعيدين الوطني والدولي لإقامة دفاعات إلكترونية نشطة وزيادة الردع في هذا الصدد.

وبالإضافة إلى المبادرات التي جرى إطلاقها في إطار الاستراتيجيات الوطنية للأمن الإلكتروني وأمن المعلومات، تواصل الدانمرك مشاركتها الواسعة في مكافحة التهديدات الهجينة من قبيل الهجمات الإلكترونية وعمليات التأثير من خلال التعاون مع شركائها وحلفائها في حلف شمال الأطلسي والاتحاد الأوروبي. وتساهم الدانمرك أيضاً في الجهود الدبلوماسية التي تُبذل داخل الأمم المتحدة والاتحاد الأوروبي وحلف شمال الأطلسي ومنظمة الأمن والتعاون في أوروبا، من أجل تعزيز فضاء إلكتروني حر ومفتوح ومستقر وسلمي وآمن باستمرار.

ومن الجدير بالذكر أن الدانمرك تؤيد فكرة وضع برنامج عمل للأمم المتحدة يمكن أن يوفر منبراً للدول والجهات الفاعلة من غير الدول لمزيد من التعاون، على سبيل المثال، فيما يتعلق بالاضطلاع بأنشطة لبناء القدرات متلائمة مع احتياجاتها أو النهوض بجهودها الوطنية للتنفيذ في إطار الأمم المتحدة، مما يؤدي إلى زيادة القدرة الجماعية على الصمود وزيادة الاستقرار في مجال تكنولوجيا المعلومات والاتصالات.

وعلاوة على ذلك، الدانمرك أيضاً عضو نشط في الفريق التعاوني لنظم الشبكات والمعلومات وفي شبكة أفرقة الاستجابة لحوادث أمن الفضاء الإلكتروني، كما أنها عضو في مجلس إدارة وكالة الاتحاد الأوروبي لأمن الفضاء الإلكتروني.

محتوى المفاهيم الواردة في تقرير الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي وتقارير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي؛

التهديدات القائمة والناشئة

تدرك الدانمرك أن الفضاء الإلكتروني يتيح فرصاً هائلة لزيادة رفاه مواطنينا، وتعزيز نموهم الاقتصادي المستدام، وتحسين نوعية حياتهم. ومع ذلك، فإن اعتمادنا على الحلول الرقمية يطرح أيضاً بعض التحديات ويتسبب في وجود مواطن ضعف.

ويساور الدانمرك القلق إزاء تزايد الأنشطة الخبيثة في الفضاء الإلكتروني التي تقوم بها جهات من الدول ومن غير الدول، وزيادة سرقة الملكية الفكرية باستخدام الفضاء الإلكتروني. وتهدد هذه الأعمال النمو الاقتصادي واستقرار المجتمع الدولي.

وقد أظهرت جهات من الدول ومن غير الدول استعدادها لاغتنام أي فرصة للقيام بأنشطة إلكترونية خبيثة. ويشمل ذلك التدخل في الهياكل الأساسية الحيوية واستخدام الفضاء الإلكتروني لسرقة الملكية الفكرية. وأي محاولة لإعاقة قدرة البنى التحتية الحيوية هي أمر غير مقبول ويمكن أن يعرّض حياة الناس للخطر. ومما يثير قلق الدانمرك بوجه خاص الزيادة التي طرأت مؤخراً على الأنشطة التي تؤثر على أمن وسلامة منتجات وخدمات تكنولوجيا المعلومات والاتصالات، مما قد تكون له آثار عامة. وعلى وجه التحديد، فإن استخدام روسيا للهجمات الإلكترونية ضد الهياكل الأساسية الحيوية كجزء من الغزو غير المبرر وغير القانوني لأوكرانيا أمر غير مقبول على الإطلاق، ومن ثم يجب إدانته بشدة من قِبَل المجتمع الدولي بأسره. ويجب على الدول الامتناع عن استخدام الهجمات الإلكترونية، وممارسة العناية الواجبة، واتخاذ إجراءات سريعة وحازمة لمكافحة أنشطة تكنولوجيا المعلومات والاتصالات الخبيثة الناشئة من أراضيها، بما يتفق مع القانون الدولي وتقارير أفرقة الخبراء الحكوميين الصادرة بتوافق الآراء في الأعوام 2010 و 2013 و 2015 و 2021 وتقرير الفريق العامل الصادر في عام 2021.

وكما أقِر بذلك في التقارير السابقة لفريق الخبراء الحكوميين، وفي تقرير الفريق العامل، ونظراً للطابع الفريد لتكنولوجيات المعلومات والاتصالات، فإن نهج الأمم المتحدة والدول الأعضاء فيها في معالجة المسائل المتعلقة بالفضاء الإلكتروني في سياق الأمن الدولي يجب أن يظل محايداً من الناحية التكنولوجية. وهذا يتسق مع المفهوم ومع اعتراف الأمم المتحدة بأن القانون الدولي القائم ينطبق على المجالات الجديدة، بما في ذلك استخدام التكنولوجيات الناشئة.

كيفية انطباق القانون الدولي على استخدام تكنولوجيات المعلومات والاتصالات

تؤيد الدانمرك بقوة وجود نظام متعدد الأطراف يستند إلى النظام الدولي القائم على القواعد للتصدي للتهديدات القائمة والمحتملة الناشئة عن الاستخدام الخبيث لتكنولوجيات المعلومات والاتصالات.

وعلى نحو ما هو معترف به في تقارير أفرقة الخبراء الحكوميين الصادرة بتوافق الآراء للأعوام 2010 و 2013 و 2015 و 2021، فضلاً عن المبادئ المنصوص عليها في الفقرات الفرعية 71 (ب) إلى (ز) من تقرير عام 2021 والتي نص عليها الفريق العامل، فقد أوضح المجتمع الدولي بجلاء أن الفضاء الإلكتروني راسخ الجذور في القانون الدولي القائم. وتشدد الدانمرك على أن القانون الدولي القائم،

بما في ذلك ميثاق الأمم المتحدة في مجمله، والقانون الدولي الإنساني والقانون الدولي لحقوق الإنسان، تنطبق على سلوك الدول في الفضاء الإلكتروني. ولذلك ندعو جميع الدول الأعضاء إلى الوفاء بهذا الالتزام.

فالسيادة وعدم التدخل وحظر استخدام القوة هي مبادئ أساسية للقانون الدولي، وقد يشكل انتهاك الدول لها عملاً غير مشروع دولياً، يجوز للدول أن تتخذ تدابير مضادة إزاءه وأن تلتمس جبر الضرر بموجب قواعد مسؤولية الدول. ولا يزال ثمة مجال لتعزيز الفهم المشترك والتفسير الموحَّد لهذه المبادئ الأساسية. وتدعم الدانمرك عمل فريق الخبراء الحكوميين والفريق العامل، فضلاً عن المبادرات الدولية والإقليمية الأخرى، بما في ذلك برنامج العمل للنهوض بسلوك الدول المسؤول في الفضاء الإلكتروني، في السعي إلى تحقيق هذه النتيجة.

والأهم من ذلك، ينبغي ألا تستخدم الدول مبدأ السيادة للحدّ من القانون الدولي لحقوق الإنسان أو انتهاكه داخل حدودها. فقانون حقوق الإنسان واجب التطبيق على شبكة الإنترنت وكذلك خارجها، ويترتب على الدول في كلتا الحالتين التزام سلبي وإيجابي معاً، على التوالي، بأن تمتنع عن القيام بأعمال تنتهك حقوق الإنسان، وبوجوب أن تكفل قدرة الناس على ممارسة حقوقهم وحرياتهم.

وكما هو موضح في الدليل العسكري الدانمركي، لا تختلف عمليات الفضاء الإلكتروني عن استخدام القدرات العسكرية التقليدية فيما يتعلق بالقانون الدولي المنطبق. وتتجلى هذه المسألة أيضاً في العقيدة الوطنية المشتركة المتعلقة بالعمليات العسكرية في الفضاء الإلكتروني لعام 2019، والتي بموجبها يلتزم القادة العسكريون بإدراج اعتبارات بشأن الامتثال للقانون الدولي عند القيام بعمليات في الفضاء الإلكتروني. وهكذا، فإن القانون الدولي الإنساني، بما في ذلك مبادئ الحيطة والإنسانية والضرورة العسكرية والتناسب والتمييز، ينطبق على سلوك الدول في الفضاء الإلكتروني وهو قانون يوفر الحماية الكاملة أيضاً، من خلال وضع حدود واضحة لشرعيته، في أوقات النزاع المسلح. وتود الدانمرك أن تنضم إلى الاتحاد الأوروبي في التأكيد على أن القانون الدولي ليس عاملاً مساعداً لنشوب النزاعات، بل وسيلة لحماية المدنيين والحد من الآثار غير التناسبية.

والقانون الدولي القائم – الذي تُكمِّله المعايير الطوعية الـ 11 غير الملزمة المتعلقة بسلوك الدول المسؤول، الواردة في تقرير فريق الخبراء الحكوميين لعام 2015 – يوفر للدول إطاراً للسلوك المسؤول في الفضاء الإلكتروني. وتدعو الدانمرك جميع الدول إلى التقيُّد بهذا الإطار وتنفيذ التوصيات المنبثقة عنه.

وبما أن القانون الدولي القائم ينطبق على الفضاء الإلكتروني، فإن الدانمرك لا تدعو إلى وضع صكوك قانونية دولية جديدة لمسائل الفضاء الإلكتروني ولا ترى ضرورة لذلك. بيد أن هناك مجالاً لتعزيز الفهم المشترك لكيفية انطباق القانون الدولي القائم على هذه المسائل. وتأمل الدانمرك أن يسهم عمل الفريق العامل وتوصياته في مزيد من الإيضاحات، ومن ثم في تيسير امتثال الدول، وأن يعمل كذلك على زيادة إمكانية التنبؤ وأن يقلل من خطر التصعيد. وتحقيقاً لهذه الغاية، تعكف الدانمرك حالياً على اتخاذ موقف وطني بشأن كيفية انطباق القانون الدولي على إجراءات الدول في الفضاء الإلكتروني.

معايير سلوك الدول المسؤول وقواعده ومبادئه

تنضم الدانمرك إلى الاتحاد الأوروبي ودوله الأعضاء في تشجيع جميع الدول على البناء على العمل الذي أقرَّته الجمعية العامة مراراً، ولا سيما في القرار 19/76، والنهوض به، وعلى تنفيذ المعايير

المتفق عليها للسلوك المسؤول من جانب الدول في الفضاء الإلكتروني، وتدابير بناء الثقة، التي تؤدي دوراً أساسياً في منع نشوب النزاعات. ونرحب بإجراء حوار شامل وبنَّاء في إطار الفريق العامل، وبإمكانية التعاون العملي ربما من خلال برنامج عمل للأمم المتحدة.

ونظراً لأن المعايير والقواعد والمبادئ المتعلقة بسلوك الدول المسؤول التي وردت في التقارير المتعاقبة لفريق الخبراء الحكوميين في الأعوام 2010 و 2013 و 2015 و 2021، وفي تقرير الفريق العامل، تشكل استكمالاً للقانون الدولي القائم وتنبثق عنه فإنها تتسم بقيمة فائقة. وستواصل الدانمرك الاسترشاد بالقانون الدولي، كما ستواصل التقيد بهذه المعايير والقواعد والمبادئ الطوعية. وينبغي مواصلة تنفيذ هذه المعايير من خلال زيادة التعاون والشفافية بشأن أفضل الممارسات.

تدابير بناء الثقة

يشكل بناء آليات فعالة للتعاون بشأن مسائل الفضاء الإلكتروني بين الدول أمراً بالغ الأهمية من أجل تبادل المعلومات وبناء الثقة ومنع نشوب النزاعات. وقد أنشأت المنتديات الإقليمية من قبيل منظمة الأمن والتعاون في أوروبا بالفعل منابر مهمة لتدابير بناء الثقة والتعاون بين الجهات الفاعلة ذات الشواغل المشتركة والمصالح المشتركة من أجل التصدي بفعالية للتحديات من منظور إقليمي. وعلاوة على ذلك، ينبغي أيضاً النظر إلى الفريق العامل نفسه باعتباره من تدابير بناء الثقة، لأنه يوفر منتدى دولياً لجميع الدول الأعضاء لكي تتبادل فيه المعلومات وتتشاطر الآراء فيما يتعلق بمسائل الفضاء الإلكتروني.

وتنضم الدانمرك إلى الاتحاد الأوروبي ودوله الأعضاء في تشجيع المجتمع الدولي على مواصلة تطوير وتنفيذ تدابير بناء الثقة في الفضاء الإلكتروني التي تزيد من إمكانية التنبؤ بسلوك الدول وتقلل من خطر إساءة التفسير والتصعيد والنزاع، وتسهم بالتالي في الاستقرار الطويل الأجل في الفضاء الإلكتروني.

التعاون والمساعدة الدوليان فيما يتعلق بأمن تكنولوجيات المعلومات والاتصالات وبناء القدرات المتعلقة بها

إن تعزيز صمود النظم الإلكترونية لمجتمعاتنا أمر بالغ الأهمية من أجل الحد من المخاطر الناجمة عن الاستخدام الخبيث لتكنولوجيات المعلومات والاتصالات، والحد من التوترات ومنع نشوب النزاعات. ولذلك، وكما هو مبين أعلاه، قدمت حكومة الدانمرك عدداً كبيراً من المبادرات لتعزيز المنعة السيبرانية الوطنية. وبالمثل، يتعاون الاتحاد الأوروبي ودوله الأعضاء، بما فيها الدانمرك، أيضاً من أجل تعزيز القدرة على الصمود على نطاق الاتحاد الأوروبي، ولا سيما من خلال التوجيهات المتعلقة بأمن نظم الشبكات والمعلومات.

وبالإضافة إلى هذه الجهود، تساهم الدانمرك أيضاً – إلى جانب الاتحاد الأوروبي ودوله الأعضاء – في زيادة قدرة النظم الإلكترونية للبلدان النامية على الصمود من خلال عدد من البرامج والمبادرات المصممة خصيصاً، التي تهدف إلى تنمية المهارات والقدرات من حيث التصدي للحوادث الإلكترونية وإلى تيسير تبادل أفضل الممارسات.

وتنضم الدانمرك إلى الاتحاد الأوروبي ودوله الأعضاء في التسليم بأن تعزيز بنية تحتية رقمية أكثر قدرة على الصمود سيسهم في إيجاد فضاء إلكتروني أكثر أمناً واستقراراً، وتشجع جميع الجهات الفاعلة

ذات الصلة على المشاركة في بناء القدرات في هذا الصدد، وتدعو كذلك إلى تعزيز التعاون مع الشركاء الرئيسيين والمنظمات الدولية الرئيسية على الصعيد الدولي لدعم بناء القدرات في بلدان ثالثة.

وعلاوة على ذلك، تؤيد الدانمرك أيضاً إنشاء آلية للأمم المتحدة لتعزيز برامج بناء القدرات المصممة خصيصاً لتلبية الاحتياجات التي تحددها الدول المستفيدة، مثل برنامج العمل، والوقوف على الآليات التي تيسّر مشاركة جميع الجهات صاحبة المصلحة في تنفيذ إطار السلوك المسؤول.

مصر

[الأصل: بالعربية]

[31 أيار/مايو 2022]

الآراء والمقترحات المصرية بشأن تعزيز أمن المعلومات وتشجيع التعاون الدولي

أولا - الجهود الوطنية

- قامت مصر خلال الفترة الماضية بتعزيز جهودها في بناء القدرات وإعداد الأطر التنظيمية اللازمة في مجال أمن الاتصالات والمعلومات، بما يتماشى مع توصيات التقارير الختامية لمجموعة العمل المفتوحة العضوية السابقة، وتقارير فريق الخبراء الحكوميين.

- اضطلاع الدولة المصرية باتخاذ سياسات متوازنة في مجال مكافحة الجرائم الإلكترونية والمستحدثة، والتصدي للأنشطة غير المشروعة عبر شبكة الإنترنت ووسائل التواصل الاجتماعي طبقاً لغطاء تشريعي يرتكز على عدد من القوانين التي تم استحداثها في هذا الشأن (قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، وقانون تنظيم الصحافة والإعلام رقم 180 لسنة 2018، وقانون حماية البيانات الشخصية رقم 151 لسنة 2020).

- تم إنشاء المجلس الأعلى للأمن السيبراني ليكون الجهة المختصة والمرجع الوطني في شؤون الأمن السيبراني، وإطلاق الاستراتيجية الوطنية للأمن السيبراني وفق رؤية جمهورية مصر العربية 2030، لتؤسس منظومة وطنية متكاملة ومتسقة مع أبرز الممارسات الدولية المتميزة في هذا المجال ومن شأنها تعزيز الشراكة الوطنية بين الجهات الحكومية والقطاع الخاص لتحقيق الأمن السيبراني، ووضع برامج لبناء دفاعات سيبرانية قوية من خلال إنشاء ورفع كفاءة فرق الاستجابة لطوارئ الحاسبات والشبكات المشكلة بقطاعات الدولة المختلفة، ووضع وتطوير برامج للتوعية بالأمن السيبراني تستهدف عدة شرائح من المجتمع "طلاب المدارس، والجهات الحكومية، وكبار السن"، وتشجيع البحث العلمي والابتكار في مجال الأمن السيبراني.

- تم اعتماد عدد من السياسات الوطنية وآليات الحوكمة والأطر والمعايير التنظيمية، منها الضوابط الأساسية للأمن السيبراني، وضوابط الأمن السيبراني للأنظمة، وكذلك المراقبة المستمرة لحالة الأمن السيبراني على المستوى الوطني.

- تعمل مصر على تعزيز التعاون الدولي الثنائي والمتعدد الأطراف فيما يخص أمن المعلومات وبناء القدرات.

- تم إطلاق العديد من البرامج والمبادرات الوطنية لرفع مستوى الوعي المجتمعي وتجنب المخاطر السيبرانية وتقليل آثارها من خلال إصدار التنبيهات بآخر وأخطر الثغرات السيبرانية.
- يتم التعاون مع هيئات وأكاديميات وطنية لبناء القدرات وتأهيل الكوادر الوطنية في مجال الأمن السيبراني وأمن المعلومات.

ثانيا - مقترحات

- أهمية تعزيز التعاون الدولي في مجال أمن الفضاء السيبراني للحد من الأنشطة الإلكترونية الإجرامية العابرة للحدود، للحيلولة دون وقوع أية جرائم سيبرانية، فضلاً عن ضرورة تبادل الخبرات والتقنيات الحديثة المستخدمة في مجال متابعة كافة الاستخدامات غير المشروعة على شبكة الإنترنت مما يتيح للدول مجابهتها، وعقد الدورات التدريبية لتطوير قدرات الأجهزة الأمنية المنوط بها مكافحة الجرائم السيبرانية.
- ضرورة اتخاذ إجراءات لحوكمة تداول العملات الرقمية المشفرة حتى لا يتم استخدامها في تمويل الأنشطة غير المشروعة، إلى جانب بحث إنشاء وحدة متخصصة لمكافحة الجرائم السيبرانية في المنظمة الدولية للشرطة الجنائية (الإنتربول) لتسهيل تبادل المعلومات بين الأجهزة الأمنية المعنية بمكافحتها.

الاتحاد الروسي

[الأصل: بالروسية]

[31 أيار/مايو 2022]

يمثل القرن الحادي والعشرون عصر إنجازات في ميدان تكنولوجيا المعلومات، التي غزت عملياً كل جانب من جوانب حياتنا. وتشهد القطاعات الحكومية والعامة والتجارية التقليدية الآن تحولاً كاملاً. وقد ظهرت فرص جديدة لتنمية الاقتصاد وخلق فرص العمل وتحسين نوعية الحياة للجميع. ومع ذلك، فإن التكنولوجيات الجديدة تأتي مصحوبة بتحديات جديدة.

وقد أصبح الفضاء الرقمي العالمي موقعاً متكرراً لحروب المعلومات التي لا هوادة فيها، والهجمات الحاسوبية، بما في ذلك ضد الهياكل الأساسية الحيوية للمعلومات، والمنافسة غير العادلة وإساءة الاستخدام من قِبَل الشركات الخاصة. وتشمل التهديدات الرئيسية استخدام تكنولوجيا المعلومات والاتصالات في المجالات العسكرية والسياسية وغيرها من المجالات لتقويض السيادة وانتهاك السلامة الإقليمية والتدخل في الشؤون الداخلية للدول؛ ونشر البرامجيات الخبيثة من خلال المصادر المفتوحة؛ واستخدام تكنولوجيا المعلومات والاتصالات للأغراض الإرهابية أو المتطرفة أو الإجرامية. وتغيّر هذه التهديدات العالم تغييراً جذرياً وتعرّض الأمن الدولي لخطر متزايد.

وكانت روسيا من أوائل الدول التي دعت المجتمع الدولي إلى توحيد الجهود في هذا المجال الجديد. وفي عام 1998، اتخذت الجمعية العامة، بمبادرة منا، قراراً بشأن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي. وكان القرار دعوة إلى التعاون على أوسع نطاق ممكن في مكافحة التهديدات المشتركة في مجال المعلومات، وفي مقدمتها محاولات استخدام أحدث

تكنولوجيات المعلومات لتقويض السلم والاستقرار الدوليين. وقد أدت جهودنا إلى إدراج موضوع أمن المعلومات في جدول أعمال الجمعية العامة وكفلت أن يصدر القرار المتعلق بأمن المعلومات على الصعيد الدولي كل عام.

وكانت روسيا أيضاً وراء المبادرة، في عام 2004، لإنشاء فريق الخبراء الحكوميين، وهو أول منتدى من نوعه لخبراء الأمم المتحدة لمناقشة الجوانب الأمنية لتكنولوجيا المعلومات والاتصالات. ومنذ ذلك الحين، كان هناك ستة أفرقة من الخبراء الحكوميين. وقد مكنت التطورات السريعة في مجال المعلومات من الارتقاء بالمناقشات إلى مستوى جديد تماماً.

وفي عام 2018، صوَّتت غالبية الدول الأعضاء في الأمم المتحدة لاعتماد القرار الذي قدمته روسيا فيما يتعلق بأمن المعلومات على الصعيد الدولي. وحدَّد القرار مجموعة أولية من القواعد والمعايير والمبادئ الخاصة بسلوك الدول المسؤول فيما يتعلق باستخدام تكنولوجيا المعلومات والاتصالات. وقررت الجمعية العامة أيضاً عقد اجتماع لفريق عامل مفتوح العضوية، من أجل مواصلة تطوير تلك القائمة، وبصفة عامة، إجراء مناقشة لأمن المعلومات الدولي بطريقة أكثر ديمقراطية. وأكمل الفريق عمله، واعتمدت الدول الأعضاء تقريره النهائي بتوافق الآراء في 12 آذار/مارس 2021 في نيويورك.

وعملت روسيا مع الوفود ذات التفكير المماثل لضمان استمرارية عملية التفاوض برعاية الأمم المتحدة من خلال إنشاء فريق عامل جديد مفتوح العضوية معني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021–2025. وتتمثل ولاية الفريق في مواصلة تطوير قواعد ومعايير ومبادئ السلوك المسؤول للدول وسبل تنفيذها. وسيقوم الفريق العامل بذلك في المقام الأول عن طريق التوصل إلى فهم مشترك لتهديدات أمن المعلومات، وإمكانية تطبيق القانون الدولي على استخدام الدول لتكنولوجيا المعلومات والاتصالات، وتدابير بناء الثقة وبناء القدرات، وعن طريق تعزيز الروابط فيما بين الوكالات ذات الصلة. ويكفل الفريق قيام الدول بدور قيادي في المناقشة ويتيح للمنظمات غير الحكومية فرصة المشاركة.

ويتبع الاتحاد الروسي نهجاً متسماً بالشفافية والاتساق لضمان أمن المعلومات على الصعيد الدولي. وتقرَّر أن يكون أمن المعلومات على الصعيد الدولي أولوية وطنية استراتيجية في استراتيجية الأمن القومي للاتحاد الروسي، التي تمت الموافقة عليها بموجب المرسوم الرئاسي رقم 400 المؤرخ 2 تموز/يوليه 2021. ووفقاً لإطار سياسة الدولة للاتحاد الروسي في مجال أمن المعلومات على الصعيد الدولي، المعتمد بموجب المرسوم الرئاسي رقم 213 المؤرخ 12 نيسان/أبريل 2021 ، يتمثل الغرض من سياسة الدولة في تشجيع إنشاء نظام قانوني دولي لتنظيم فضاء المعلومات العالمي.

ونعتقد أن الاتفاقات العالمية الملزمة قانوناً ضرورية لمنع نشوب النزاعات وتعزيز التعاون المتبادل المنفعة في مجال المعلومات. ويمكن لمشروع الاتفاقية المتعلقة بمكافحة استخدام تكنولوجيا المعلومات والاتصالات في الأغراض الإجرامية، الذي قدمته روسيا في اللجنة الخاصة المنشأة بمبادرة منا، أن يُتَّخذ أساساً لهذه الاتفاقات، شأنه شأن الاقتراح الروسي بإبرام اتفاقية للأمم المتحدة بشأن أمن المعلومات على الصعيد الدولي.

وينبغي أن تخدم تكنولوجيا المعلومات والاتصالات أهداف التنمية المستدامة وأن تهيّء الظروف المواتية للبحث العلمي والتنفيذ السريع للحلول التقنية. وبغية ضمان إدماج هذه المبادئ في التزامات قانونية متفق عليها عالمياً ومنصفة في المستقبل، بادرت روسيا والولايات المتحدة الأمريكية في عام 2021 إلى

اعتماد قرار الجمعية العامة 19/76، بتوافق الآراء، وانضمت 108 دول أعضاء إلى قائمة مقدمي مشروع القرار.

وتؤمن روسيا بحرمة السيادة الرقمية للدول. ويمكن لكل بلد، بل وينبغي له، أن يضع معاييره الخاصة لتنظيم فضائه المعلوماتي وهياكله الأساسية ذات الصلة. وتصرُّ روسيا على تدويل حوكمة الإنترنت وعلى المساواة في الحقوق بين الدول فيها. وأي محاولات للحدّ من الحق السيادي للدول في تنظيم القطاعات الوطنية من الشبكة العالمية وتأمين تلك القطاعات غير مقبولة.

ومن المهم اتخاذ تدابير قانونية على الصعيدين الوطني أو الدولي لمنع بعض الدول من الهيمنة على المجال الرقمي. ومن المهم اتخاذ خطوات لضمان حصول جميع المستعملين في فضاء المعلومات على حماية موثوقة ومتساوية. ولا يجوز لأي دولة بمفردها أو لمجموعة من البلدان أن تضع من جانب واحد مبادئ وقواعد ومعايير لتشغيل الإنترنت. وتحقيقاً لهذه الغاية، تصرُّ روسيا على أن توضع إدارة الإنترنت ضمن اختصاص الاتحاد الدولي للاتصالات السلكية واللاسلكية، وهو وكالة متخصصة تابعة للأمم المتحدة تتمتع بالخبرة اللازمة في ميدان الاتصالات السلكية واللاسلكية وتكنولوجيا المعلومات والاتصالات.

وروسيا، كما كان الحال من قبل، منفتحة على الحوار والتعاون البنَّاء مع جميع شركائها، سواء على الصعيد الثنائي أو من خلال الهيئات والمنتديات الدولية، وفي المقام الأول، في الأمم المتحدة.

سنغافورة

[الأصل: بالإنكليزية]

[31 أيار/مايو 2022]

تلتزم سنغافورة التزاماً قوياً بتعزيز نظام دولي قائم على القواعد في الفضاء الإلكتروني يكون بمثابة أساس للثقة والاطمئنان بين الدول الأعضاء، وييسر إحراز التقدم الاقتصادي والاجتماعي. ولجني الثمار الكاملة للتكنولوجيات الرقمية، يجب على المجتمع الدولي تهيئة فضاء إلكتروني آمن وموثوق ومفتوح وقابل للتشغيل البيني يستند إلى القانون الدولي المنطبق، ومعايير محددة جيداً لسلوك الدول المسؤول، وتدابير قوية لبناء الثقة، وبناء منسق للقدرات. وترى سنغافورة من الأهمية بمكان أن يستمرَّ إجراء المناقشات بشأن هذه المسائل، بما في ذلك القوانين والقواعد والمعايير المتعلقة بالسلوك المسؤول للدول، في نطاق الأمم المتحدة، فهي المنتدى المتعدد الأطراف العالمي الشامل الوحيد الذي تتمتع فيه جميع الدول بصوت متساوٍ.

وشاركت سنغافورة في فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي للفترة من 2019 إلى 2021 والفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، المنشأ عملاً بقرار الجمعية العامة 27/73. ونحن نشارك بنشاط في جهود الرئيس الرامية إلى إنشاء فريق عامل مفتوح العضوية عملي المنحى معني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025 وندعمها للمضي قدماً في المناقشات بشأن معايير الفضاء الإلكتروني الدولية والإطار المتفق عليه لسلوك الدول المسؤول في الفضاء الإلكتروني. وما زلنا على التزامنا بالإسهام على نحو بنَّاء في عملية الفريق العامل لزيادة تعزيز التعاون الدولي وإحراز تقدم في الارتقاء بالسلوك المسؤول في الفضاء الإلكتروني من جانب الدول. وستواصل سنغافورة، بوصفها الرئيسة المشاركة لمجموعة الأصدقاء المعنية بالحوكمة

الإلكترونية والأمن الإلكتروني مع إستونيا، استخدام هذا المنبر لزيادة الوعي بتحديات الفضاء الإلكتروني، وتبادل أفضل الممارسات، وتعزيز بناء القدرات في الأمم المتحدة.

قواعد سلوك الدول المسؤول ومعاييره ومبادئه

وتعتقد سنغافورة أن من الضروري بذل جهود إضافية لتعزيز الوعي بالمعايير الطوعية وغير الملزمة القائمة لسلوك الدولة المسؤول ودعم تنفيذها. وتؤيد سنغافورة أيضاً مواصلة تفصيل هذه المعايير عند الاقتضاء. فعلى سبيل المثال، يمكن اعتبار الهياكل الأساسية الحيوية للمعلومات العابرة للحدود التي توفر الخدمات عبر عدة دول، والتي تقع المسؤولية المشتركة في حمايتها على عاتق جميع الدول الأعضاء، فئة خاصة من هذه الهياكل الأساسية الحيوية، وينبغي إدراجها في مجموعة المعايير القائمة، لأن التهديدات التي تشكلها تكنولوجيا المعلومات والاتصالات لهذه الهياكل الأساسية يمكن أن يكون لها آثار مزعزعة للاستقرار على الصعيدين الإقليمي والعالمي[3].

ويمكن للمنظمات الإقليمية أن تؤدي دوراً هاماً في دعم تنفيذ الإطار المعياري القائم. وقد انضمت رابطة أمم جنوب شرق آسيا من حيث المبدأ إلى المعايير الـ 11 الطوعية غير الملزمة بشأن سلوك الدول المسؤول في استخدام تكنولوجيا المعلومات والاتصالات، ولا تزال حتى الآن المنظمة الإقليمية الوحيدة التي اعتمدت هذه المعايير. وفي المؤتمر الوزاري السادس لرابطة أمم جنوب شرق آسيا المعني بأمن الفضاء الإلكتروني، الذي عقد في عام 2021، ناقش المشاركون التقدم المحرز في خطة العمل الإقليمية الطويلة الأجل للرابطة بشأن تنفيذ معايير السلوك المسؤول للدول في الفضاء الإلكتروني، التي تسعى إلى ضمان التنفيذ الفعال والعملي لهذه المعايير، في مجالات منها التعاون بين أفرقة التصدي للطوارئ الحاسوبية، وحماية الهياكل الأساسية الحيوية للمعلومات، والمساعدة المتبادلة في مجال أمن الفضاء الإلكتروني. وقد أُقِرت خطة العمل الإقليمية في لجنة تنسيق أمن الفضاء الإلكتروني الثانية التابعة لرابطة أمم جنوب شرق آسيا في تشرين الثاني/نوفمبر 2021 ولا تزال وثيقة قابلة للتعديل ستخضع لمزيد من الاستعراض. وتمثل استراتيجية التعاون في مجال أمن الفضاء الإلكتروني لرابطة أمم جنوب شرق آسيا للفترة 2021-2025 تحديثاً لاستراتيجية رابطة أمم جنوب شرق آسيا للتعاون في مجال أمن الفضاء الإلكتروني من أجل إنشاء فضاء إلكتروني أكثر سلامة وأكثر أمناً في منطقة الرابطة. وقد وافقت رابطة أمم جنوب شرق آسيا على إنشاء فريق إقليمي للتصدي للطوارئ الحاسوبية، سيضم آلية تبادل المعلومات لفريق التصدي للطوارئ الحاسوبية التابع للرابطة، بغية تعزيز استجابة الرابطة لحوادث أمن الفضاء الإلكتروني. ومن خلال دليل جهات الاتصال التابعة للمنتدى الإقليمي لرابطة أمم جنوب شرق آسيا المعني بأمن تكنولوجيا المعلومات والاتصالات واستخدامها، يمكن لأعضاء المنتدى الاتصال بنظرائهم في حالة وقوع حادث من حوادث أمن الفضاء الإلكتروني.

بناء القدرات

وتعتقد سنغافورة أن بناء القدرات ركيزة أساسية للإطار المعياري المتفق عليه، بالنظر إلى أهمية ضمان أن تكون لدى جميع الدول القدرة على تنفيذ الإطار المعياري والوفاء بالتزاماتها بموجب القانون

(3) الهياكل الأساسية الحيوية للمعلومات العابرة للحدود هي الهياكل الأساسية الحيوية للمعلومات التي تملكها شركات خاصة وتعمل عبر الحدود الوطنية، ولكنها لا تخضع لولاية أي دولة بمفردها.

الدولي. وتمشـياً مع ذلك، تلتزم سـنغافورة بتشـاطر تجربتنا وخبراتنا مع الدول الزميلة الأعضـاء في الأمم المتحدة، ولا سيما البلدان النامية الصغيرة، على الصعيدين الإقليمي والعالمي.

ولدعم بناء القدرات على المسـتوى الإقليمي، أنشـأت سـنغافورة برنامجاً للرابطة معنياً بالقدرات المتعلقة بالفضـاء الإلكتروني في عام 2016 لدعم بناء القدرات في بلدان الرابطة بشـأن السـياسـات العامة الإلكترونية، فضـلاً عن المسـائل التشـغيلية والتقنية. وبعد ردود الفعل الإيجابية من الشـركاء والمشـاركين الدوليين في البرنامج، أعلنت سـنغافورة عن إنشـاء مركز التميُّز في مجال أمن الفضـاء الإلكتروني المشـترك بين رابطة أمم جنوب شـرق آسـيا وسـنغافورة في تشـرين الأول/أكتوبر 2019، مع الالتزام بتقديم مبلغ قدره 30 مليون دولار على مدى خمس سـنوات حتى عام 2023، للاضـطلاع ببرامج تدريبية في مجال أمن الفضـاء الإلكتروني لكبار مسؤولي السياسات والمسؤولين التقنيين في رابطة أمم جنوب شرق آسيا. وافتُتح مقرُّ المركز رسمياً في تشرين الأول/أكتوبر 2021 خلال أسبوع سنغافورة الدولي للفضاء الإلكتروني. وحتى الآن، نفذ المركز أكثر من 30 برنامجاً حضـرها أكثر من 250 1 من كبار المسؤولين من رابطة أمم جنوب شـرق آسـيا وخارجها، وتعاون مع أكثر من 40 جهة شـريكة تشـمل الحكومات والقطاع الخاص والأوسـاط الأكاديمية والمنظمات غير الحكومية. وعلى الرغم من القيود المفروضـة على السـفر الناجمة عن جائحة مرض فيروس كورونا (كوفيد-19)، واصـل المركز تنفيذ برامج تدريبية عبر الإنترنت ونظم 21 برنامجاً افتراضياً في مجال بناء القدرات منذ أيار/مايو 2020.

وعلى الصـعيد العالمي، تعمل سـنغافورة في شـراكة مع مكتب شـؤون نزع السـلاح بشـأن المبادرات التالية:

(أ) في إطار البرنامج المشـترك بين الأمم المتحدة وسـنغافورة في مجال الفضـاء الإلكتروني، تعكف سـنغافورة على وضـع قائمة مرجعية لتنفيذ المعايير من خلال مجموعة من حلقات العمل في مختلف المناطق، بالشـراكة مع مكتب شـؤون نزع السـلاح. وسـتتخذ القائمة المرجعية شـكل دليل يحدد مجموعة من الإجراءات التي يمكن للبلدان النامية اتخاذها لتنفيذ المعايير الطوعية الـ 11 غير الملزمة بشأن سلوك الدول المسـؤول. وعقدت سـنغافورة حلقة العمل الأولى بشـأن تنفيذ المعايير لوضـع القائمة المرجعية مع الدول الأعضـاء في رابطة أمم جنوب شـرق آسـيا في آذار/مارس 2022، التي ركزت على تنفيذ المعايير المتعلقة بحماية البنى التحتية الحيوية، والإبلاغ عن مواطن الضـعف، وحماية أفرقة التصـدي للطوارئ الحاسـوبية وأفرقة الاستجابة لحوادث أمن الفضاء الإلكتروني؛

(ب) وفي أواخر عام 2022، سيشترك مكتب شؤون نزع السلاح وسنغافورة في تنظيم الزمالة المشـتركة بين الأمم المتحدة وسـنغافورة في مجال الفضـاء الإلكتروني، وهي برنامج مصـمم لتزويد كبار المسؤولين الحكوميين من الدول الأعضاء في الأمم المتحدة بالخبرة المتعددة التخصصات اللازمة للإشراف بفعالية على السياسات والاستراتيجيات والعمليات الوطنية للأمن السيبراني والأمن الرقمي.

تدابير بناء الثقة

وترى سنغافورة أيضاً أنه ينبغي للمجتمع الدولي أن يبذل مزيداً من الجهود لوضع تدابير لبناء الثقة دعماً للإطار المعياري المتفق عليه، بالنظر إلى أن هذه التدابير تنطوي على إمكانية الحد من خطر حدوث حالات سوء الفهم، فضلاً عن منع نشوب النزاعات في الفضاء الإلكتروني وتخفيف حدتها. وتمشياً مع ذلك، تؤيد سنغافورة إنشاء دليل عالمي لجهات الاتصال الوطنية على المستوى التشغيلي أو التقني، على نحو ما

أوصى به الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي. وفي النصف الثاني من عام 2022، ستجري سنغافورة أيضاً أول عملية في مجموعة من عمليات المحاكاة لجهات الاتصال الإلكترونية الوطنية بالشراكة مع معهد الأمم المتحدة لبحوث نزع السلاح. ومن شأن هذه العمليات (أ) إتاحة فرصة لجميع الدول الأعضاء في الأمم المتحدة للمشاركة في عملية إلكترونية موضوعية بصرف النظر عن القدرة التقنية الحالية و/أو حالة الانتساب إلى منظمة إقليمية؛ (ب) تحسين قدرات جهات الاتصال الإلكترونية الوطنية على الاستجابة للحوادث ولأزمات الفضاء الإلكتروني في العالم الحقيقي؛ و (ج) إظهار فعالية الدليل العالمي المقترح وقيمته لجهات الاتصال. وقد سبق أن نظمت هذه العمليات على الصعيد الإقليمي بين أفرقة التصدي للطوارئ الحاسوبية، ولكنها لم تكن مفتوحة لجميع الدول الأعضاء المهتمة بالأمر في الأمم المتحدة، ولا سيما الدول الواقعة خارج شبكات الأفرقة الإقليمية للتصدي للطوارئ الحاسوبية. ولمعالجة ذلك، سيكون برنامج سنغافورة لعمليات المحاكاة أول عملية مفتوحة لمشاركة جميع الدول الأعضاء.

الجهود على المستوى الوطني

وعلى الصعيد الوطني، واصلت سنغافورة تعزيز أمن الفضاء الإلكتروني لنظمها وشبكاتها على الجبهات الثلاث التالية: إقامة هياكل أساسية قادرة على الصمود، وإيجاد فضاء إلكتروني أكثر أماناً، وتهيئة بيئة حيوية لأمن الفضاء الإلكتروني.

إقامة هياكل أساسية قادرة على الصمود

يتعين على الكيانات التي تمتلك هياكلنا الأساسية المحورية وتشغلها أن تلتزم بمدونة لممارسات أمن الفضاء الإلكتروني، توضح بالتفصيل تدابير النظافة الإلكترونية التي ينبغي أن تمارسها هذه الكيانات، من قبيل مواصلة تحديث الأنظمة والبرامجيات، والحفاظ على نسخ احتياطية محدَّثة من البيانات الرئيسية واكتشاف حالات التسلل الإلكتروني بسرعة. وتَصدر أيضاً تنبيهات وإنذارات عند الحاجة لإكمال مدونة الممارسات من أجل التصدي للتهديدات الناشئة (مثل برمجيات انتزاع الفدية). وبالإضافة إلى ذلك، بدأت وكالة أمن الفضاء الإلكتروني في سنغافورة العمل بالخطة الرئيسية لأمن الفضاء الإلكتروني للتكنولوجيا التشغيلية في عام 2019 في إطار جهودنا المبذولة لتعزيز أمن قطاعات الهياكل الأساسية للمعلومات الحيوية في سنغافورة وقدرتها على الصمود في تقديم الخدمات الأساسية. وترمي الخطة الرئيسية إلى تحسين الاستجابة الشاملة عبر القطاعات للتخفيف من التهديدات الإلكترونية في بيئة التكنولوجيا التشغيلية وتعزيز الشراكات مع القطاع الصناعي والجهات صاحبة المصلحة من خلال تحديد مبادرات رئيسية تشمل مجالات الأشخاص والعمليات والتكنولوجيا لتعزيز قدرات مالكي هياكلنا الأساسية الحيوية للمعلومات والمنظمات التي تقوم على إدارة نظم التكنولوجيا التشغيلية. وأطلقت الوكالة أيضا إطار الكفاءات الأساسية للتكنولوجيا التشغيلية، الذي يمكن للمؤسسات الاستفادة منه لإنشاء عمليات أو هياكل أو وظائف لإدارة أمن الفضاء الإلكتروني للتكنولوجيا التشغيلية داخل منظماتها. وفي عام 2022، ستطلق الوكالة برنامجاً لسلسلة توريد الهياكل الأساسية الحيوية للمعلومات، يشمل أصحاب المصلحة من قبيل الوكالات الحكومية والجهات المالكة للهياكل الأساسية للمعلومات الحيوية والبائعين التابعين لهم. وسيوفر البرنامج لجميع أصحاب المصلحة العمليات والممارسات السليمة الموصى بها لإدارة مخاطر أمن الفضاء الإلكتروني في سلسلة التوريد.

إيجاد فضاء إلكتروني أكثر أماناً

وفي إطار الجهود التي نبذلها للارتقاء بأمن الفضاء الإلكتروني على الصعيد الوطني في سنغافورة، أطلقت وكالة أمن الفضاء الإلكتروني الخطة الرئيسية لفضاء إلكتروني أكثر أماناً في عام 2020 من أجل القيام بما يلي: '1' تأمين الهياكل الأساسية الرقمية الأساسية لسنغافورة؛ '2' حماية الأنشطة في الفضاء الإلكتروني؛ '3' تمكين سكاننا البارعين في مجال الفضاء الإلكتروني. وتحدد الخطة الرئيسية 11 مبادرة تهدف إلى زيادة أخذ المؤسسات والمنظمات بإجراءات أمنية مخطط لها، فضلاً عن تعزيز الوعي بأمن الفضاء الإلكتروني والممارسات الجيدة في مجال النظافة الإلكترونية لدى المستخدمين النهائيين. ولجميع المؤسسات والمنظمات دور تؤديه في حماية أنشطتنا الأوسع نطاقاً في مجال الفضاء الإلكتروني. ولتيسير ذلك، أطلقت الوكالة عدداً من الخطط لزيادة وعي أصحاب المصلحة بأمن الفضاء الإلكتروني، مثل مجموعات أدوات أمن الفضاء الإلكتروني التي تستهدف مختلف أصحاب المصلحة في المؤسسات. وتكمل ذلك شهادة أمن الفضاء الإلكتروني للمؤسسات في شكل علامتي "الثقة الإلكترونية" و "الأساسيات الإلكترونية" التي تُمنح تقديراً للمؤسسات التي لديها تدابير وممارسات شاملة لأمن الفضاء الإلكتروني.

وقد أصدرت وكالة أمن الفضاء الإلكتروني إنذارات عامة لتوجيه المؤسسات وعامة الناس بشأن إدارة نقاط الضعف والتهديدات المتعلقة بالفضاء الإلكتروني والتنقل فيه عند ظهورها. فعلى سبيل المثال، أصدرت الوكالة إنذاراً عاماً بشأن قابلية التعرض للضرر في الآونة الأخيرة من جراء البرنامج Log4Shell وعملت مع الرابطات والغرف التجارية على إطلاع المؤسسات السنغافورية على كيفية معالجة هذا الضعف وتأمين نظمها. وبالإضافة إلى ذلك، لدى الوكالة إنذارات دائمة تتناول الجرائم الإلكترونية، كالإنذار العام لإثناء الضحايا عن دفع الفدية للجهات الفاعلة في برمجيات انتزاع الفدية.

وثمة مخاطر متزايدة لأمن الفضاء الإلكتروني مرتبطة بانتشار إنترنت الأشياء، نظراً لاتساع نطاق شبكات اتصالها وعدم توفيرها أمن الفضاء الإلكتروني. وقد استفادت وكالة أمن الفضاء الإلكتروني من المعايير التقنية لرفع مستوى النظافة الإلكترونية وتوفير الضمان بشأن المنتجات والخدمات. وفي عام 2020 ، أطلقت الوكالة مخطط وضع علامات أمن الفضاء الإلكتروني لأجهزة إنترنت الأشياء الاستهلاكية. ويُعرض الآن في الأسواق أكثر من 150 منتجاً يحمل تلك العلامات. وكذلك تؤيد سنغافورة بقوة المعايير الدولية القائمة على القواعد، وهي دولة مانحة للشهادات بموجب ترتيب الاعتراف بالمعايير المشتركة[4]. وستساعد المعايير الدولية على رفع مستوى النظافة الإلكترونية، وتأمين الفضاء الإلكتروني بشكل تعاوني، وخفض الحواجز أمام التجارة عبر الحدود. وتأمل سنغافورة في العمل مع الشركاء ذوي التفكير المماثل لإعداد إطار عالمي لوضع العلامات لأمن إنترنت الأشياء الاستهلاكية من أجل المواءمة بين المعايير الدولية المعمول بها ومتطلبات وضع العلامات، فضلاً عن تيسير الاعتراف المتبادل بهذه المعايير. ومن شأن ذلك أن يساعد على التقليل إلى أدنى حد من تجزئة المعايير، والقضاء على الاختبارات المكررة عبر البلدان، وخفض تكلفة الامتثال للوائح الوطنية، وتيسير نفاذ المطورين إلى الأسواق.

(4) انظر www.commoncriteriaportal.org.

تهيئة بيئة حيوية لأمن الفضاء الإلكتروني

تُسلِّم سنغافورة بأن تعزيز أمن الفضاء الإلكتروني يشمل بناء البيئة الإلكترونية وتشجيع الابتكار ضمن القطاع الصناعي ذي الصلة. وبالنظر إلى مشهد التهديدات السيبرانية سريع التطور، تحتاج شركات أمن الفضاء الإلكتروني إلى الابتكار المستمر والاستثمار في حلول جديدة للبقاء في الطليعة في هذا المجال. وتدعم وكالة أمن الفضاء الإلكتروني الابتكار الذي تقوده الصناعة في مجال أمن الفضاء الإلكتروني من خلال "دعوة صناعة أمن الفضاء الإلكتروني إلى الابتكار". وهذا يشجع شركات أمن الفضاء الإلكتروني على وضع حلول مبتكرة لتلبية احتياجات أمن الفضاء الإلكتروني للمستخدمين النهائيين المحليين الرئيسيين (مثل الكيانات التي تمتلك وتدير الهياكل الأساسية الرقمية الأساسية، والقطاع التجاري)، فضلاً عن تحفيز الطلب في صناعة أمن الفضاء الإلكتروني في البلد. وهناك أيضاً حاجة متزايدة إلى تكوين مجموعة من الأفراد الموهوبين الذين يمكنهم تولي أدوار قيادية في مجال أمن الفضاء الإلكتروني في المنظمات. وقد عملت الوكالة مع الوكالات الحكومية والجمعيات والشركاء الصناعيين والأوساط الأكاديمية في سنغافورة على توسيع القوى العاملة في مجال أمن الفضاء الإلكتروني وتطويرها. وتهدف مبادرة الأمين العام لتشجيع المواهب في مجال أمن الفضاء الإلكتروني إلى اجتذاب المواهب المتحمسة في مجال الأمن الإلكتروني منذ سن مبكرة ومساعدة الأوساط المتخصصة في أمن الفضاء الإلكتروني على صقل مهاراتها في هذا المجال. وتهدف المبادرة إلى التواصل مع ما لا يقلُّ عن 000 20 شخص على مدى ثلاث سنوات لتعزيز قائمة المواهب في مجال أمن الفضاء الإلكتروني في سنغافورة.

تركيا

[الأصل: بالإنكليزية]

[31 أيار/مايو 2022]

وفقاً للتقييمات والتوصيات الواردة في تقرير الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي وتقارير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، ترد أدناه آراء تركيا وتقييماتها بشأن الجهود المبذولة على الصعيد الوطني لتعزيز أمن المعلومات وتعزيز التعاون الدولي في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، فضلاً عن مضمون المفاهيم المذكورة في التقارير ذات الصلة.

وكما أبرزت التقارير السالفة الذكر، فإن الضرورة الحتمية لبناء وصون السلم والأمن والتعاون والثقة على الصعيد الدولي في بيئة تكنولوجيات المعلومات والاتصالات لم تكن قط بهذا الوضوح من قبل. وبصفة خاصة، نظراً لانتشار التكنولوجيات الرقمية وطابعها العابر للحدود، أصبح أمن تكنولوجيا المعلومات والاتصالات أحد العناصر الرئيسية للدفاع الوطني والأمن الدولي إزاء تنوع التهديدات والجرائم الإلكترونية واتساع نطاقها. ولذلك، تبذل الدول الأعضاء جهوداً مكثفة لإنشاء ما يلزم من الهياكل الأساسية التقنية والقدرات المؤسسية ورأس المال البشري في ميدان الأمن الوطني. ولاستباق المخاطر المحتملة على الأمن القومي لتركيا ومنعها، يجري التخطيط واتخاذ الإجراءات اللازمة مثل تطوير التكنولوجيات المتعلقة بأمن الفضاء الإلكتروني وخصوصية البيانات، ومعالجة الثغرات المتعلقة بتوافر الموارد البشرية المؤهلة، واستكمال إعادة الهيكلة المؤسسية، وتحديث الهياكل الأساسية القانونية، وضمان تطبيق التكنولوجيات المتطورة. وعلاوة

على ذلك، هناك حاجة إلى التعاون، ولا سيما على الصعيد الدولي، لمكافحة جرائم الفضاء الإلكتروني. وفي هذا الصدد، يتمثل الهدف في مواصلة تطوير تبادل المعارف والمعلومات والتعاون الدولي من أجل الكشف عن مصدر الجريمة الإلكترونية والمجرمين المتورطين فيها بأكثر الطرق كفاءة.

وتركز تركيا على اتخاذ التدابير اللازمة لتحسين أمن الفضاء الإلكتروني الوطني. ووزارة النقل والبنية التحية هي الهيئة المسؤولة عن رسم السياسات ووضع الاستراتيجيات وخطط العمل فيما يتعلق بأمن الفضاء الإلكتروني الوطني في تركيا. وضمن هذا السياق، جرى نشر وتنفيذ الاستراتيجية الوطنية لأمن الفضاء الإلكتروني، وخطة العمل للفترة 2013–2014، واستراتيجية وخطة العمل الوطنية لأمن الفضاء الإلكتروني للفترة 2016–2019. ومن ثم وضعت تركيا استراتيجيتها وخطة عملها الوطنية لأمن الفضاء الإلكتروني للفترة 2020–2023 بمشاركة جميع الجهات صاحبة المصلحة المعنية ضمن أفرقة دراسة بتنسيق من الوزارة.

ونُشرت الاستراتيجية وخطة العمل الوطنية لأمن الفضاء الإلكتروني للفترة 2020–2023 في *الجريدة الرسمية* في 29 كانون الأول/ديسمبر 2020، وهي تشمل الأهداف الاستراتيجية الرئيسية التالية:

- حماية الهياكل الأساسية الحيوية وزيادة القدرة على الصمود
- بناء القدرات الوطنية
- الشبكة العضوية لأمن الفضاء الإلكتروني
- أمن تكنولوجيات الجيل الجديد
- مكافحة الجريمة الإلكترونية
- تطوير التكنولوجيات المحلية والوطنية وتشجيعها
- دمج أمن الفضاء الإلكتروني في الأمن القومي
- تحسين التعاون الدولي.

وتضطلع وزارة النقل والهياكل الأساسية بالرصد والقياس المتعلقين بخطة العمل على أساس خطوات التنفيذ المحددة، والأنشطة التي تنفذها المؤسسات والمنظمات المسؤولة، ومعايير القياس.

وفي الوقت ذاته، يقوم الفريق الوطني للتصدي للطوارئ الحاسوبية في تركيا، وهو يتبع هيئة تكنولوجيات المعلومات والاتصالات، بتنسيق مواجهة الحوادث الإلكترونية في البلد منذ عام 2013. وبالإضافة إلى الكشف عن التهديدات الإلكترونية والتصدي للحوادث الإلكترونية، بما في ذلك قبل وقوع الحوادث وفي أثنائها وبعدها، يكفل الفريق تنفيذ التدابير الوقائية لمكافحة التهديدات الإلكترونية والاضطلاع بالردع الإلكتروني.

وتتمثل مجالات التركيز الرئيسية للفريق الوطني للتصدي للطوارئ الحاسوبية فيما يتعلق بأمن الفضاء الإلكتروني فيما يلي:

- بناء القدرات في الفضاء الإلكتروني
- التدابير التكنولوجية

- جمع المعلومات المتعلقة بالتهديدات ونشرها
- حماية الهياكل الأساسية الحيوية

وفي سياق تحسين أمن الفضاء الإلكتروني الوطني، تم أيضاً منذ عام 2013 إنشاء 14 فريقاً قطاعياً للتصدي للطوارئ الحاسوبية في القطاعات أو البنى التحتية الحيوية (مثل الطاقة، والصحة، والمصارف والمالية، وإدارة المياه، والاتصالات الإلكترونية، والخدمات العامة الحيوية)، وما يزيد عن 000 2 فريق مؤسسي للتصدي للطوارئ الحاسوبية. وتعمل جميع الأفرقة على مدار الساعة، سبعة أيام في الأسبوع، بتنسيق من الفريق الوطني من أجل التخفيف من المخاطر الإلكترونية ومكافحة التهديدات الإلكترونية. ويستخدم الفريق الوطني أدوات الكشف والوقاية لأغراض الرصد، وأدوات الإبلاغ لتبادل المعلومات مع الأطراف المعنية. وقد طوَّر منصة الاتصال لجميع أفرقة التصدي للطوارئ الحاسوبية داخل تركيا من أجل توزيع الإنذارات والتحذيرات والإشعارات الأمنية، مما يوفر قناة للاتصالات تتسم بالكفاءة والأمن.

وينظم الفريق الوطني الدورات التدريبية والمخيمات الصيفية والمسابقات بشأن أمن الفضاء الإلكتروني ويدعمها، وهي مفتوحة لعدة مجتمعات محلية. وبالإضافة إلى ذلك، يقدم الفريق دورات تدريبية لأفرقة التصدي للطوارئ الحاسوبية في مواضيع من قبيل تحليل البرامجيات الخبيثة وتحليل السجلات وغيرها. وفي نيسان/أبريل 2022 كان الفريق الوطني قد أتمّ تدريب أكثر من 000 5 شخص في مجالات مختلفة للأمن السيبراني.

وقد تم قبول الفريق الوطني في برنامج الثغرات الأمنية ومواطن التعرض الشائعة التابع لشركة ميتر كوربوريشن MITRE Corporation، وفي هذا السياق، يعطي الفريق أرقاماً خاصة بالثغرات الأمنية ومواطن التعرض لمكامن الضعف في برامج أو أجهزة أو منتجات الأطراف الثالثة ويوفر تنسيق العمليات في معالجتها.

وبالإضافة إلى ذلك، تتيح أكاديمية BTK، وهي مركز التدريب التابع لهيئة تكنولوجيا المعلومات والاتصالات، التي تأسست في عام 2017، تدريباً عبر الإنترنت مفتوحاً للجمهور في مجال أمن الفضاء الإلكتروني والمجالات الأخرى ذات الصلة من أجل المساهمة في زيادة الخبرة داخل الموارد البشرية في تركيا. ومحتويات التدريب متاحة على البوابة الإلكترونية الرسمية للأكاديمية (www.btkakademi.gov.tr/portal).

وكذلك تنظم عدة منظمات ومؤسسات وجامعات ومنظمات غير حكومية وكيانات من القطاع الخاص التركية حلقات دراسية ومؤتمرات ودورات تدريبية على الصعيد الوطني بشأن مواضيع ذات صلة مثل أمن الفضاء الإلكتروني وحماية الهياكل الأساسية الحيوية.

ويوم الإنترنت الآمن الذي ينظم سنوياً هو من بين أنشطة التوعية التي تضطلع بها هيئة تكنولوجيات المعلومات والاتصالات، ويتمثل هدفها الرئيسي في الاستخدام الواعي والآمن للإنترنت. وأتيح للعموم على البوابة الإلكترونية الرسمية الآمنة خط اتصال مجاني للمساعدة في مجال الإنترنت وموقع شبكي يسمى الشبكة الآمنة، حيث يمكن للأسر أن تجد المشورة فيما يتعلق بالاستخدام الكفء للإنترنت (www.guvenlinet.org.tr).

وبالإضافة إلى ذلك ، يجري عقد التدريب والندوات عبر الإنترنت وعن طريق الحضور الشخصي للطلاب والمعلمين وأولياء الأمور بشأن الاستخدام الواعي والمأمون للإنترنت. وعلاوة على ذلك، تم الوصول إلى العديد من الطلاب من خلال القيام بزيارات مدرسية باستخدام شاحنة الإنترنت الأكثر أماناً، التي تعمل على ضمان تفاعل الأطفال والشباب في جميع أنحاء البلاد مباشرة مع التكنولوجيات الجديدة، واستخدامهم التكنولوجيا والإنترنت بشكل صحيح، كما تعمل على زيادة الوعي بخصوص هذه المسألة.

وتتخذ تركيا أيضاً خطوات لمواجهة مخاطر الأمن الرقمي المتزايدة لضمان أمن الفضاء الإلكتروني وقد اتخذت التدابير اللازمة خلال جائحة مرض فيروس كورونا (كوفيد-19).

ويتولى الفريق الوطني للتصدي للطوارئ الحاسوبية، الذي يعمل على مدار 24 ساعة في اليوم، سبعة أيام في الأسبوع، تحليل البرامجيات الخبيثة وهجمات استراق الهوية الرقمية وغيرها من التهديدات السيبرانية التي تستغل اتجاهات جائحة كوفيد-19. ومن خلال مراكز القيادة والسيطرة، يجري تحديد الروابط الخبيثة لهذه التهديدات الإلكترونية ومنعها من أجل حماية الهياكل الأساسية الحيوية والمواطنين. وضمن هذا النطاق، يجري إعداد تقارير الاستخبارات الإلكترونية وإطلاع الأطراف المعنية عليها. وجرى كذلك إعداد عدة مبادئ توجيهية ونشرها، ومنها ما يتعلق بما يلي:

- مبادئ الأمان لوسائل الاتصال عن بعد
- حماية المستخدمين من هجمات استراق الهوية الرقمية
- التطبيقات الوهمية المتعلقة بكوفيد-19
- مبادئ الأمان لإعداد برامج المؤتمرات والاجتماعات عبر الفيديو واستخدامها

وعلاوة على ذلك، دخلت المعايير المهنية الوطنية لموظفي أمن الفضاء الإلكتروني (المستوى 5) حيز النفاذ لدى نشرها في *الجريدة الرسمية*.

وما فتئت تركيا تؤدي أدواراً هامة في كثير من المنظمات، إما باعتبارها عضواً مؤسِّساً، أو من خلال المساهمة في جهود التعاون في المسائل المتعلقة بأمن الفضاء الإلكتروني وأمن المعلومات. وفي هذا السياق، تولي تركيا أهمية قصوى لتبادل المعلومات مع مختلف البلدان والمنظمات. وتركيا عضو في الاتحاد الدولي للاتصالات، والفريق الوطني للتصدي للطوارئ الحاسوبية عضو في منتدى أفرقة الأمن والتصدي للحوادث، ومؤسسة ترستد إنتروديوسرز Trusted Introducers، والمنتدى المتعدد الجنسيات لتبادل المعلومات عن البرامجيات الخبيثة التابع لمنظمة حلف شمال الأطلسي (الناتو)، وتحالف أمن الفضاء الإلكتروني من أجل التقدم المشترك، وفريق التصدي للطوارئ الحاسوبية التابع لمنظمة المؤتمر الإسلامي. وتشارك تركيا أيضاً في مركز الامتياز للدفاع التعاوني الإلكتروني التابع لمنظمة حلف شمال الأطلسي كدولة راعية منذ تشرين الثاني/نوفمبر 2015. وبالإضافة إلى ذلك، هناك جهود مستمرة تتعلق بالتعاون الثنائي والمتعدد الأطراف في مجال أمن الفضاء الإلكتروني، مثل مذكرات التفاهم الموقعة مع كثير من البلدان. وبالإضافة إلى ذلك، تؤيد تركيا المشاركة النشطة والمساهمة في دراسات المنظمات الدولية مثل الأمم المتحدة، ومنظمة حلف شمال الأطلسي، ومنظمة الأمن والتعاون في أوروبا، ومنظمة التعاون والتنمية في الميدان الاقتصادي، ومجموعة العشرين، ومجلس التعاون للدول الناطقة بالتركية، ومنظمة التعاون

الاقتصادي، ومنظمة البلدان النامية الثمانية للتعاون الاقتصادي، والمركز الإقليمي للمساعدة على التحقق من تحديد الأسلحة وتنفيذه – مركز التعاون الأمني.

وتمثل التمارين الخاصة بأمن الفضاء الإلكتروني أحد الأنشطة الأخرى المهمة بالنسبة للتعاون 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. ومنذ عام 2011، أُجريت في تركيا خمسة تمارين وطنية وتمرينان دوليان على أمن الفضاء الإلكتروني. وفي الآونة الأخيرة، أجري تمرين الدرع الإلكتروني الوطني لعام 2021 يومي 12 و13 تشرين الأول/أكتوبر 2021 بالتعاون مع وزارة النقل والهياكل الأساسية وهيئة تكنولوجيات المعلومات والاتصالات، بمشاركة من المؤسسات والمنظمات العامة. وعلاوة على ذلك، اشتركت الوزارة والهيئة في تنظيم تمرين الدرع الإلكتروني الدولي لعام 2019 في 19 كانون الأول/ديسمبر 2019 في أنقرة. وحظي التمرين بدعم من الاتحاد الدولي للاتصالات وتحالف أمن الفضاء الإلكتروني من أجل التقدم المشترك. وعلاوة على ذلك، تواصل تركيا المشاركة في مختلف التمارين الدولية لأمن الفضاء الإلكتروني مثل "الدروع المقفلة" للناتو، والائتلاف المعني بالفضاء الإلكتروني التابع للناتو، وتمرين إدارة الأزمات للحلف نفسه، كما تساهم في هذه التمارين. وفضلاً عن الدراسات الأخرى المتعلقة ببناء القدرات والتوجيه، تظل التمارين الدولية في مجال أمن الفضاء الإلكتروني بالغة الأهمية لزيادة مستويات التأهب وبناء القدرات على التصدي للحوادث الإلكترونية في جميع أنحاء العالم.

ومن المؤسسات الهامة الأخرى في مجال السياسات الوطنية لتكنولوجيا المعلومات والاتصالات مكتب التحول الرقمي التابع لرئاسة تركيا.

ومن أهم الدراسات التي أجراها مكتب التحول الرقمي وأبرزها نشر دليل أمن المعلومات والاتصالات في 24 تموز/يوليه 2020. والدليل هو الوثيقة المرجعية الوطنية الرئيسية المنشورة في هذا الميدان. وهو يؤدي دوراً هاماً في تعزيز قدرات الدفاع الإلكتروني للمؤسسات العامة ومقدمي خدمات الهياكل الأساسية الحيوية.

ويُتوقع من المؤسسات العامة ومقدمي خدمات الهياكل الأساسية الحيوية أن يكملوا أنشطتهم المتعلقة بالامتثال في غضون الفترة المحددة في الدليل، ويتعين عليهم أن يجروا عمليات مراجعة الحسابات مرة واحدة في السنة على الأقل. وسياسات مراجعة الحسابات وإجراءاتها التي يجب أن تقوم بها المؤسسات في هذا الصدد موثقة في دليل مراجعة أمن المعلومات والاتصالات الذي نشره مكتب التحول الرقمي.

وعلاوة على ذلك، تم افتتاح المركز الوطني لمنصات اختبار الهياكل الأساسية الحيوية، الذي يستضيف دراسات لضمان أمن الهياكل الأساسية لتوزيع الكهرباء وإدارة المياه، بالتعاون مع الأطراف ذات الصلة في تركيا. وقد صُمّم المركز، الذي تصاغ فيه نماذج نظم إدارة الطاقة والمياه، لتهيئة بيئة عمل للبحث عن حلول للحماية والوقاية فيما يتعلق بأمن الهياكل الأساسية الحيوية ووضع تلك الحلول والمساهمة في النظام الإيكولوجي للأمن الإلكتروني.

ويمثل إعداد مشاريع تحسين أمن المعلومات وأمن الفضاء الإلكتروني إحدى المسؤوليات الرئيسية لمكتب التحول الرقمي على النحو المحدد في المواد المدمجة بموجب المرسوم الرئاسي رقم 48 المنشور في عدد *الجريدة الرسمية* رقم 30928، بتاريخ 24 تشرين الأول/أكتوبر 2019، في المرسوم الرئاسي بشأن التنظيم الرئاسي رقم 1، المنشور في *الجريدة الرسمية* رقم 30474، بتاريخ 10 تموز/يوليه 2018.

وفي هذا السياق، نفذت مشاريع مختلفة تتعلق بالمعلومات وأمن الفضاء الإلكتروني، ومنها مسابقة الذكاء الإلكتروني ومسابقة HackZeugma Capture the Flag:

- ومسابقة الذكاء الإلكتروني هي جزء من أنشطة التدريب والتوعية التي تهدف إلى زيادة عدد الأفراد الذين لديهم وعي بأمن الفضاء الإلكتروني. وقد أثبتت فعاليتها الكبيرة في هذا الصدد. ونظم مكتب التحول الرقمي المسابقة الثانية للذكاء السيبراني ضمن فعاليات شهر التوعية الإلكترونية في عام 2021.
- ونظّم مكتب التحول الرقمي مسابقة HackZeugma Capture the Flag في إطار مهرجان "تكنوفست" للفضاء الجوي والتكنولوجيا لعام 2020. ومسابقة HackZeugma هي مسابقة تفتح أبوابها لآلاف قراصنة الحواسيب حول العالم للسماح لهم بعرض مواهبهم. ويجري الإعداد لهذه المسابقة مع التركيز بشكل خاص على أمن نظم التكنولوجيا التشغيلية.

وعلاوة على ذلك، جرى إطلاق مشروع المليون وظيفة لإيجاد قوة عاملة مؤهلة في مجال تكنولوجيات المعلومات ولزيادة العمالة من خلال الجمع بين القوى العاملة المدربة وأصحاب العمل. وتتوفر للمشروع سمات جديدة، تتيح لأرباب العمل مسح السير الذاتية عن طريق التسجيل مجاناً ودون شروط. ويهدف هذا المشروع، الذي يتبع وزارة الخزانة والمالية، إلى جعل مليون شخص جاهزين للعمل في مجال تكنولوجيات المعلومات بحلول عام 2023، ويجري تنفيذه في نطاق أهداف "الحركة الوطنية للتكنولوجيا" من أجل تحقيق التحول الرقمي في بلدنا.

ومجموعة أمن الفضاء الإلكتروني التركية هي منصة يتابعها مكتب التحول الرقمي ويدعمها عن كثب، وتهدف بشكل أساسي إلى أن تصبح تركيا منتجة للتكنولوجيا في مجال أمن الفضاء الإلكتروني وقادرة على التنافس مع العالم، بما يتفق مع المهام المنوطة بها المتمثلة في بناء نظام إيكولوجي وطني لأمن الفضاء الإلكتروني، وتطوير منتجات أمن الفضاء الإلكتروني المحلية والوطنية ونشر استخدامها. ومن الأنشطة التي تضطلع بها المجموعة ما يلي:

- إنشاء مختبر لإجراء الاختبارات والتحليلات يوفر الهياكل الأساسية لاختبار القطاع وتطويره
- إنشاء مختبر لإصدار الشهادات
- إنشاء أكاديمية أمن الفضاء الإلكتروني
- تنظيم الأنشطة الوطنية والدولية من قبيل إقامة المؤتمرات والدورات التدريبية والحلقات الدراسية وحلقات النقاش والمعارض، وتنسيق الطلبات والإمدادات لأنشطة التدريب الداخلي
- دعم افتتاح البرامج التعليمية للحصول على مؤهل متوسط أو شهادة جامعية أو شهادة دراسات عليا.

وبالإضافة إلى الجهود المذكورة أعلاه، وضع معهد المعايير التركية ومكتب التحول الرقمي معايير الصناعة كنهج لتحسين أمن الفضاء الإلكتروني في صفوف مالكي الهياكل الأساسية الحيوية والقائمين عليها. وقد استُكملت الدراسات المتعلقة بالمعايير 27701 و 27011 و 27017 و 27018 و 27019 و 27031 و 27799 و 31000 و 62443 للمنظمة الدولية لتوحيد المقاييس/اللجنة الكهربائية التقنية الدولية، ونشرت مؤسسة المعايير التركية المعايير المتعلقة بالهياكل الأساسية الحيوية.

ويكتسي تطوير التعاون الدولي، إلى جانب الأنشطة الوطنية، أهمية كبيرة بالنظر إلى طبيعة أمن الفضاء الإلكتروني. ومع انتشار استخدام تكنولوجيا المعلومات والاتصالات على نطاق واسع، فإن العلاقة التي أقامتها هذه التكنولوجيات مع مواضيع مثل السلام والاستقرار والأمن على الصعيد الدولي والحقوق والحريات الأساسية تتطور باستمرار. وتتطلب هذه الحالة بذل جهود لاستخدام تكنولوجيات المعلومات والاتصالات للأغراض السلمية ولضمان أن تعالج الدول باستمرار مسألة الاستقرار والأمن الدوليين. ومن الواضح أن القانون الدولي والمعايير والقواعد الدولية المعرب عنها في تقارير فريق الخبراء الحكوميين والفريق العامل والدراسات ذات الصلة تسهم في إيجاد إطار مشترك لسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات في سياق السلم والأمن الدوليين. وكما ورد في التقارير المذكورة، فإن المفاهيم من قبيل تطوير التعاون الدولي، واحترام الحقوق والحريات الأساسية، وحماية الهياكل الأساسية الحيوية، ومنع الاستخدام الخبيث لتكنولوجيات المعلومات والاتصالات، ستحتفظ بأهميتها في الجهود الرامية إلى تحقيق الاستقرار والأمن الدوليين في الفترة المقبلة.

وفي الوقت ذاته، ينبغي أيضاً مراعاة أهمية حماية سيادة الدول في الفضاء الإلكتروني وضرورة وضع معايير جديدة بالإضافة إلى المعايير القائمة. وبالإضافة إلى ذلك، يكتسي تحسين التعاون ودعم آليات تبادل المعلومات والخبرات أهمية بالغة لمكافحة التهديدات السيبرانية، ويتعيَّن إيلاؤهما الاهتمام الواجب.

وتدرك تركيا أهمية تنفيذ القانون الدولي، ومعايير السلوك المسؤول للدول في الفضاء الإلكتروني وتدابير بناء الثقة، والحاجة إلى التعاون الدولي الفعال، وتتخذ بحزم الخطوات اللازمة لتحقيق هذه الأهداف.

أوكرانيا

[الأصل: بالإنكليزية]

[31 أيار/مايو 2022]

لطالما كانت أوكرانيا ضحية للعدوان المسلح الروسي المستمر وهدفاً للهجمات الإلكترونية في إطاره، بما في ذلك الهجمات ضد الهياكل الأساسية الحيوية لأوكرانيا. وبناء على ذلك، تشارك أوكرانيا كل المشاركة في القلق المبرر الذي أُعرِب عنه في الفقرة الخامسة من ديباجة قرار الجمعية العامة 19/76، على أن يكون مفهوماً أن الأمر ليس مقصوراً على احتمال استخدام تكنولوجيات المعلومات ووسائلها فحسب، وإنما هي بالفعل أداة تطبقها الدولة المعتدية تطبيقاً نشطاً في الممارسة العملية، وليس ضد أوكرانيا فحسب.

ويثير عجز روسيا الذي تأكد مراراً عن احترام التزاماتها الدولية الشك في استعدادها للامتثال أيضاً لأحكام الفقرتين 3 و 6 من منطوق القرار 19/76.

وينطبق الشيء نفسه على الاتفاقية الدولية الشاملة المتوخاة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية التي اقترحت موسكو وضعها. ويرجع ذلك إلى أنه إذا لم تدخل في النسخة النهائية للاتفاقية الأحكام التي صممتها روسيا لمشروع الاتفاقية، والتي تنذر بخطر التقييد الشديد لحقوق المواطنين وحرياتهم، فلن تكون الاتفاقية محل اهتمام موسكو.

وهذا التقييد، المقترح في مشروع الاتفاقية الروسية، غير مقبول بالنسبة لأوكرانيا وغيرها من الدول الديمقراطية الأطراف في اتفاقية مجلس أوروبا لعام 2001 المتعلقة بالجريمة الإلكترونية، ولكنه يناسب النُظم الاستبدادية، بما فيها النظامان الموجودان في روسيا وبيلاروس، اللتين لم تصبحا طرفاً في الاتفاقية.

وعلى الرغم من العدوان العسكري والسيبراني الروسي، تواصل أوكرانيا تعزيز نظامها الخاص بأمن الفضاء الإلكتروني، بمساعدة مادية واستشارية من الشركاء الغربيين.

ويستند النظام الوطني للأمن الإلكتروني الذي وضعته استراتيجية أمن الفضاء الإلكتروني في أوكرانيا إلى وزارة الدفاع، والدائرة الحكومية للاتصالات الخاصة وحماية المعلومات، ودائرة الأمن، والشرطة الوطنية، والبنك الوطني. وهو يكفل التعاون بين جميع الوكالات الحكومية والسلطات المحلية والوحدات العسكرية ووكالات إنفاذ القانون والمؤسسات البحثية والتعليمية والجماعات المدنية والشركات والمنظمات التي تتعامل مع أمن الاتصالات الإلكترونية وأمن المعلومات أو التي تمتلك الهياكل الأساسية الحيوية للمعلومات، بغضّ النظر عن شكل ملكيتها.

والأشخاص القائمون على ضمان النظام الوطني للأمن الإلكتروني على إلمام بالتقييمات والتوصيات الواردة في تقارير الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي وفريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي.

ويتولى المجلس الوطني للأمن والدفاع في أوكرانيا تنسيق ومراقبة أنشطة الكيانات في قطاع الأمن والدفاع، ويكفل أمن الفضاء الإلكتروني لأوكرانيا من خلال هيئته العاملة، المركز الوطني لتنسيق أمن الفضاء الإلكتروني.

ويضطلع المركز بوظيفة إشرافية ويقوم بمهام تتعلق بتحليل حالة أمن الفضاء الإلكتروني الوطني والتأهب لمكافحة التهديدات الإلكترونية، فضلاً عن التنبؤ بالتهديدات المحتملة والفعلية ذات الصلة واكتشافها.

وبعد تنفيذ استراتيجية أمن الفضاء الإلكتروني السابقة لأوكرانيا للفترة 2016-2020، تمكنت الدولة من تشكيل جوهر نظام أمن الفضاء الإلكتروني الوطني. وقد زادت أوكرانيا من الإمكانات التي تتيح مزيداً من تطوير هذا النظام على أساس الردع وقدرة النظم الإلكترونية على الصمود والتفاعل.

ويتمثل الغرض من استراتيجية أمن الفضاء الإلكتروني الحالية لأوكرانيا، التي وضعت للفترة 2021-2025، في تهيئة الظروف لعمل الفضاء الإلكتروني بشكل مأمون واستخدامه لصالح الفرد والمجتمع والدولة. وتستند الوثيقة إلى مبادئ الردع وقدرة النظم الإلكترونية على الصمود والتفاعل.

وأتاحت الجهود السالفة الذكر لأوكرانيا الوقوف على التحضيرات الروسية للهجمات السيبرانية الخبيثة ضد الهياكل الأساسية الأوكرانية التي تزامنت مع العدوان المادي. واعتباراً من خريف عام 2021، شهدنا العدد المتزايد من هجمات مجموعات قراصنة الحواسيب التابعين لروسيا ضد الموردين الأوكرانيين المهمين للخدمات الرقمية وخدمات الاتصالات السلكية واللاسلكية. وزادت كذلك جودة هذه الهجمات، فأصبحت أكثر تحديداً للهدف واستخدمت أدوات أكثر تطوراً.

غير أن من الجدير بالإشارة أن معظم تلك الهجمات الإلكترونية لم تكن ناجحة. فقد اكتشفتها الجهات المعنية لدينا، بدعم من شركائنا الدوليين، وخفَّفت من حدتها.

وتعمل أوكرانيا بنشاط على تطوير التعاون في الفضاء الإلكتروني، ولا سيما مع الولايات المتحدة والمملكة المتحدة وإستونيا وغيرها من البلدان الغربية الشريكة، والاتحاد الأوروبي ومنظمة حلف شمال

الأطلسي. وهي تتلقى المساعدة المالية، فضلاً عن المشورة، من خلال الدورات التدريبية الثنائية والمتعددة الجنسيات والحلقات الدراسية والمؤتمرات في الخارج وفي أوكرانيا، إلى جانب المساعدة والأجهزة والبرامجيات الحديثة لتلبية احتياجات أمن الفضاء الإلكتروني وإجراء التحاليل الجنائية الحاسوبية الاحترافية والتحقيق في الجرائم الإلكترونية.

وتعرب أوكرانيا عن امتنانها للبيان الذي أصدرته مؤخراً الولايات المتحدة والمملكة المتحدة والاتحاد الأوروبي وبلدان ومؤسسات أخرى وتدين فيه الأعمال العدوانية الروسية في الفضاء الإلكتروني ضد أوكرانيا وبلدان أخرى.

ومنذ عام 2016، نظمت وزارة الخارجية الأوكرانية 22 جولة من المشاورات السيبرانية الثنائية مع 13 بلداً (اليابان وسنغافورة وماليزيا وفنلندا والولايات المتحدة وألمانيا والمملكة المتحدة وإستونيا وهولندا وسلوفينيا وإسبانيا والبرازيل وإسرائيل). وكان من المقرر إجراء مشاورات من هذا القبيل مع عدد من الدول في عام 2022، ولكنها أرجئت بسبب الغزو العسكري الروسي.

وفي مجال الدفاع الإلكتروني، تتعاون أوكرانيا تعاوناً وثيقا مع الصندوق الاستئماني للدفاع الإلكتروني التابع لمنظمة حلف شمال الأطلسي من أجل تعزيز القدرات التقنية للبلد في مواجهة التهديدات الإلكترونية، وتتطلع إلى التعاون الفعال مع الحلف بوصفها من البلدان المساهمة في مركز الامتياز التعاوني للدفاع الإلكتروني التابع لمنظمة حلف شمال الأطلسي.

وستكون أوكرانيا ممتنة لجميع الدول الأعضاء في الأمم المتحدة التي قد تساعد في تنفيذ المشاريع التالية الجاري تنفيذها وفقاً لاستراتيجية البلد الحالية لأمن الفضاء الإلكتروني من أجل تعزيز القدرات في ميدان أمن الفضاء الإلكتروني والدفاع الإلكتروني، وتطوير الهياكل الأساسية وخدمات تكنولوجيا المعلومات لشبكة من مراكز العمليات الحكومية:

- بناء النطاق الإلكتروني وإجراء التدريبات الإلكترونية على الصعيد الوطني
- أدوات الاستخبارات الخاصة بالتهديدات الإلكترونية للمنصات التكنولوجية
- مركز النسخ الاحتياطي الوطني لموارد الدولة من المعلومات الحيوية
- النظام الوطني لرصد التهديدات الإلكترونية
- منصة خدمة أمن الفضاء الإلكتروني السحابية الحكومية.

ووزارة الخارجية مستعدة لتقديم معلومات تفصيلية عن هذه المشاريع والمساعدة في إقامة اتصال مع منفذيها.

وتبين تجربة أوكرانيا أنه في سبيل التصدي للتهديدات الإلكترونية والهجمات الإلكترونية الخطيرة والمستمرة، يلزم تعزيز التعاون على مستويات متعددة: فيما بين السلطات الوطنية، ومع القطاع الخاص، ومع الشركاء الدوليين، من أجل بناء القدرات الضرورية والتصدي الفعال لهذه التهديدات.

ثالثا - الردود الواردة من المنظمات الحكومية الدولية

الاتحاد الأوروبي

[الأصل: بالإنكليزية]

[31 أيار/مايو 2022]

أصبح الفضاء الإلكتروني، ولا سيما شبكة الإنترنت العالمية المفتوحة، إحدى الدعامات الأساسية لمجتمعاتنا. وهو يوفر منصة تدفع الاتصال الإلكتروني والنمو الاقتصادي. ويؤيد الاتحاد الأوروبي والدول الأعضاء فيه إيجاد فضاء إلكتروني عالمي مفتوح وحر وعالمي ومستقر وآمن يقوم على سيادة القانون وحقوق الإنسان والحريات الأساسية والقيم الديمقراطية التي تحقق التنمية الاجتماعية والاقتصادية والسياسية على الصعيد العالمي.

ومع ترسخ الإنترنت وتكنولوجيات المعلومات والاتصالات بشكل أكثر في حياتنا يجعلنا اعتمادنا على هذه التكنولوجيات أكثر عرضة لسوء استخدامها. ويتزايد استغلال الفضاء الإلكتروني من أجل تحقيق أغراض خبيثة، وتعوق زيادة الاستقطاب على الصعيد الدولي تعددية الأطراف الفعالة. ويشكل سلوك روسيا غير المسؤول في الفضاء الإلكتروني جزءاً لا يتجزأ من غزوها غير القانوني وغير المبرر لأوكرانيا، ويتعارض مع التوقعات التي حددتها جميع الدول الأعضاء في الأمم المتحدة، بما فيها الاتحاد الروسي، بشأن معايير الأمم المتحدة المتفق عليها للسلوك المسؤول من جانب الدول. وبالمثل، يشكل الاستهداف الخبيث للبنية التحتية الحيوية خطراً عالمياً كبيراً. وتهدد القيود المفروضة على إتاحة شبكة الإنترنت وعلى استخدامها، والزيادة في الأنشطة الخبيثة في الفضاء الإلكتروني، بما في ذلك زيادة في الأنشطة التي تؤثر على أمن وسلامة منتجات وخدمات تكنولوجيا المعلومات والاتصالات، الفضاءَ الإلكتروني المفتوح والحر والعالمي والمستقر والآمن، فضلاً عن الديمقراطية وسيادة القانون وحقوق الإنسان والحريات الأساسية.

وقد أعرب الاتحاد الأوروبي والدول الأعضاء فيه بانتظام عن القلق إزاء هذه الأنشطة الخبيثة التي تقوض النظام الدولي القائم على القواعد وتزيد من خطر نشوب النزاعات. وينال الاستخدام الخبيث لتكنولوجيات المعلومات والاتصالات من الفوائد التي توفرها شبكة الإنترنت وتكنولوجيا المعلومات والاتصالات للمجتمع ككل، ويُظهر استعداد بعض الجهات الفاعلة لتهديد السلم والأمن والاستقرار على الصعيد الدولي. وينبغي لجميع الجهات الفاعلة أن تمتنع عن القيام بأنشطة غير مسؤولة ومزعزعة للاستقرار في الفضاء الإلكتروني.

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

إن تعزيز صمود النظم الإلكترونية على الصعيد العالمي عنصر حاسم في الحفاظ على السلام والاستقرار الدوليين، من خلال الحدّ من خطر نشوب النزاعات وكوسيلة للتصدي للتحديات المرتبطة برقمنة اقتصاداتنا ومجتمعاتنا. ويحدُّ صمود النظم الإلكترونية على الصعيد العالمي من قدرة الجناة المحتملين على إساءة استعمال تكنولوجيات المعلومات والاتصالات لأغراض خبيثة وتعزز قدرة الدول على التصدي بفعالية للحوادث الإلكترونية والتعافي منها. ويؤيد الاتحاد الأوروبي والدول الأعضاء فيه بقوة الرؤية السالفة الذكر المتمثلة في إيجاد فضاء إلكتروني مفتوح وحر وعالمي ومستقر وآمن، من خلال تعزيز إطار استراتيجي شامل ومتعدد الأوجه وتطبيقه لمنع نشوب النزاعات وضمان الاستقرار في الفضاء الإلكتروني، بطرق منها

المشاركة الثنائية والإقليمية ومشاركة أصحاب المصلحة المتعددين. وضمن هذا الإطار الاستراتيجي، يعمل الاتحاد الأوروبي على تعزيز القدرة على الصمود على الصعيد العالمي، وتشجيع وتعزيز فهم مشترك للنظام الدولي القائم على القواعد في الفضاء الإلكتروني، ووضع وتنفيذ تدابير تعاونية عملية، بما في ذلك تدابير لبناء الثقة الإقليمية.

وتمثل استراتيجية أمن الفضاء الإلكتروني لعام 2013 المعنونة "فضاء إلكتروني مفتوح وسالم وآمن"[5]، فضلاً عن وثائق السياسات والأدوات والاستراتيجيات اللاحقة المذكورة أدناه، رؤية الاتحاد الأوروبي الشاملة بشأن أفضل السبل لمنع الاضطرابات والهجمات الإلكترونية والتصدي لها. وهي تهدف إلى تعزيز قيم الاتحاد الأوروبي وضمان تهيئة الظروف اللازمة لنمو الاقتصاد الرقمي. وتهدف بعض إجراءات محددة إلى تعزيز قدرة نظم المعلومات على الصمود في الفضاء الإلكتروني، والحد من الجريمة الإلكترونية، وتعزيز سياسة الاتحاد الأوروبي الدولية لأمن الفضاء الإلكتروني ولدفاعه الإلكتروني.

وفي شباط/فبراير 2015، شدد مجلس الاتحاد الأوروبي في استنتاجاته بشأن الدبلوماسية في الفضاء الإلكتروني[6] على أهمية مواصلة تطوير وتنفيذ نهج مشترك وشامل للاتحاد الأوروبي في مجال الدبلوماسية في الفضاء الإلكتروني يعزز حقوق الإنسان والقيم الأساسية للاتحاد الأوروبي، ويضمن حرية التعبير، ويعزز المساواة بين الجنسين، وينهض بالنمو الاقتصادي، ويكافح الجريمة الإلكترونية، ويخفف من التهديدات للأمن الإلكتروني، ويمنع نشوب النزاعات، ويوفر الاستقرار في العلاقات الدولية. ويدعو الاتحاد الأوروبي أيضاً إلى تعزيز نموذج إدارة الإنترنت المتعدد أصحاب المصلحة وإلى تحسين جهود بناء القدرات في بلدان ثالثة. وبالإضافة إلى ذلك، يسلم الاتحاد الأوروبي بأهمية التعاون مع الشركاء الرئيسيين والمنظمات الدولية. ويشدد الاتحاد الأوروبي أيضاً على تطبيق القانون الدولي القائم في الفضاء الإلكتروني وفي مجال الأمن الدولي وعلى أهمية قواعد السلوك، فضلاً عن أهمية إدارة الإنترنت باعتبارها جزءاً لا يتجزأ من النهج المشترك والشامل للاتحاد الأوروبي في مجال الدبلوماسية في الفضاء الإلكتروني.

واستناداً إلى استعراض لاستراتيجية أمن الفضاء الإلكتروني لعام 2013، زاد الاتحاد الأوروبي من تعزيز هياكله وقدراته في مجال أمن الفضاء الإلكتروني بطريقة منسقة، وبالتعاون الكامل للدول الأعضاء ومختلف هياكل الاتحاد الأوروبي المعنية، مع احترام اختصاصاتها ومسؤولياتها. وفي عام 2017، حدَّدت الرسالة المشتركة المعنونة "القدرة على الصمود والردعُ والدفاع: بناء أمن قوي للفضاء الإلكتروني للاتحاد الأوروبي"[7] حجم التحدي ومجموعة التدابير المتوخاة على صعيد الاتحاد الأوروبي، لضمان أن يكون الاتحاد مستعداً بشكل أفضل لمواجهة تحديات أمن الفضاء الإلكتروني المتزايدة باستمرار.

وأعطت الشواغل بشأن تلك التحديات المتزايدة باستمرار زخماً لوضع إطار للتصدي الدبلوماسي المشترك للاتحاد الأوروبي للأنشطة الإلكترونية الخبيثة، يتمثل في مجموعة أدوات الدبلوماسية في الفضاء

(5) انظر الرسالة المشتركة الموجهة إلى البرلمان الأوروبي، والمجلس، واللجنة الأوروبية الاقتصادية والاجتماعية ولجنة المناطق بعنوان "استراتيجية الاتحاد الأوروبي لأمن الفضاء الإلكتروني: فضاء إلكتروني مفتوح وسالم وآمن".

(6) 15/6122 استنتاجات المجلس بشأن الدبلوماسية في الفضاء الإلكتروني.

(7) انظر الرسالة المشتركة الموجهة إلى البرلمان الأوروبي والمجلس المعنونة "القدرة على الصمود والردعُ والدفاع: بناء أمن قوي للفضاء الإلكتروني للاتحاد الأوروبي".

الإلكتروني[8]. وينبغي أن يكون تزايد قدرة جهات حكومية وغير حكومية على تحقيق أهدافها من خلال أنشطة إلكترونية خبيثة، وتعاظم رغبتها في ذلك، مصدر قلق عالمي. وقد تشكل هذه الأنشطة أفعالاً غير مشروعة بموجب القانون الدولي ويمكن أن تؤدي إلى آثار مزعزعة للاستقرار ومتعاقبة مع زيادة مخاطر نشوب النزاعات. والاتحاد الأوروبي والدول الأعضاء فيه ملتزمة بتسوية المنازعات الدولية في الفضاء الإلكتروني بالوسائل السلمية. وتحقيقاً لهذه الغاية، فإن إطار الاستجابة الدبلوماسية المشتركة للاتحاد الأوروبي هو جزء من نهج الاتحاد الأوروبي إزاء الدبلوماسية في الفضاء الإلكتروني، التي تسهم في منع نشوب النزاعات، والتخفيف من تهديدات أمن الفضاء الإلكتروني، وتحقيق استقرار أكبر في العلاقات الدولية. ويشجع الإطار التعاون، وييسر التخفيف من حدة التهديدات المباشرة والطويلة الأجل، ويؤثر على سلوك الجهات الفاعلة الخبيثة على المدى الطويل. وهو كذلك يوفر التنسيق الواجب مع آليات إدارة الأزمات في الاتحاد الأوروبي، بما في ذلك مخطط التصدي المنسق لحوادث أمن وأزمات الفضاء الإلكتروني الواسعة النطاق. ويدعو الاتحاد الأوروبي والدول الأعضاء فيه المجتمع الدولي إلى تعزيز التعاون الدولي من أجل إنشاء فضاء إلكتروني مفتوح وحر وعالمي ومستقر وآمن تُطبَّق فيه حقوق الإنسان والحريات الأساسية وسيادة القانون تطبيقاً كاملاً. وهي مصممة على مواصلة جهودها لمنع الأنشطة الخبيثة والثني عنها وردعها والتصدي لها، وتسعى إلى تعزيز التعاون الدولي في هذا الصدد.

وفي كانون الأول/ديسمبر 2020، حدَّد الاتحاد الأوروبي كذلك استراتيجيته[9] لإحداث تحول رقمي يكفل أمن الفضاء الإلكتروني في بيئة معقدة من التهديدات. وتهدف استراتيجية الاتحاد الأوروبي لأمن الفضاء الإلكتروني في العقد الرقمي إلى تعزيز وحماية فضاء إلكتروني مفتوح وحر وعالمي ومستقر وآمن يستند إلى حقوق الإنسان والحريات الأساسية والديمقراطية وسيادة القانون. وتتضمن الاستراتيجية اقتراحات ملموسة لمعالجة مسألة القدرة على الصمود ومنع التهديدات الإلكترونية وردعها والتصدي لها والتشجيع على تهيئة فضاء إلكتروني عالمي ومفتوح. ويمكِّن منع إساءة استخدام التكنولوجيات، وحماية الهياكل الأساسية الحيوية، وضمان سلامة سلاسل التوريد، الاتحاد الأوروبي أيضاً من التقيد بمعايير الأمم المتحدة وقواعدها ومبادئها المتعلقة بسلوك الدول المسؤول.

وتعزز سياسة الاتحاد الأوروبي الدولية بشأن الفضاء الإلكتروني احترام القيم الأساسية للاتحاد الأوروبي، وتحدد معايير للسلوك المسؤول، وتدعو إلى تطبيق القوانين الدولية القائمة في الفضاء الإلكتروني، مع مساعدة البلدان خارج الاتحاد الأوروبي في بناء القدرات في مجال أمن الفضاء الإلكتروني، وتعزيز التعاون الدولي بشأن القضايا المتعلقة بالفضاء الإلكتروني. ويواصل الاتحاد الأوروبي العمل مع الشركاء الدوليين من أجل تطوير وتعزيز فضاء إلكتروني مفتوح وحر وعالمي ومستقر وآمن، يُحترم فيه القانون الدولي، ولا سيما ميثاق الأمم المتحدة، ويُتقيد فيه بالمعايير والقواعد والمبادئ الطوعية غير الملزمة لسلوك الدول المسؤول. وللنهوض بالسلام والأمن في الفضاء الإلكتروني، هناك حاجة واضحة إلى تنفيذ إطار الأمم المتحدة للسلوك المسؤول للدول في الفضاء الإلكتروني على النحو الذي اتفق عليه فريق الخبراء الحكوميين

(8) 9916/17، مشروع استنتاجات المجلس بشأن إطار للتصدي الدبلوماسي المشترك للاتحاد الأوروبي للأنشطة الإلكترونية الخبيثة ("مجموعة أدوات الدبلوماسية في الفضاء الإلكتروني").

(9) انظر الرسالة المشتركة إلى البرلمان الأوروبي والمجلس بشأن استراتيجية الاتحاد الأوروبي لأمن الفضاء الإلكتروني للعقد الرقمي والوثيقة 21/7290 المؤرخة 22 آذار/مارس 2021، استنتاجات المجلس بشأن استراتيجية الاتحاد الأوروبي لأمن الفضاء الإلكتروني للعقد الرقمي.

السابق والفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي وأقرته الجمعية العامة. ويقترح الاتحاد الأوروبي، إلى جانب 60 من الدول الأعضاء في الأمم المتحدة، وضع برنامج عمل للنهوض بسلوك الدول المسؤول في الفضاء الإلكتروني.

واستناداً إلى التشريعات القائمة التي أقرتها الجمعية العامة بالإجماع، يوفر برنامج العمل آلية دائمة وشاملة وعملية المنحى في الأمم المتحدة للمضي قدماً في تنفيذ التقارير التي تم التوصل إليها بتوافق الآراء ودعم الدول في سياساتها الوطنية لأمن الفضاء الإلكتروني، ولا سيما من خلال برامج بناء القدرات المصمَّمة خصيصاً لتلبية الاحتياجات التي تحدّدها الدول المستفيدة. وكذلك يوفر البرنامج آلية مؤسسية داخل الأمم المتحدة لتحسين التعاون مع أصحاب المصلحة الآخرين مثل القطاع الخاص والأوساط الأكاديمية والمجتمع المدني بشأن مسؤوليات كل منهم عن الحفاظ على بيئة مفتوحة وحرة وآمنة ومستقرة ومتاحة وسلمية لتكنولوجيا المعلومات والاتصالات. وسيعمل برنامج العمل بطريقة تكاملية ومنسقة مع العمليات الأخرى ذات الصلة، مثل الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025.

وقد وافق الاتحاد الأوروبي رسمياً في 21 آذار/مارس 2022 على البوصلة الاستراتيجية[10] من أجل تعزيز قدرته على توقع التهديدات والتحديات الحالية والناشئة بسرعة وردعها والتصدي لها، وحماية المصالح الأمنية للاتحاد. وتتيح البوصلة للاتحاد الأوروبي خطة عمل طموحة لتعزيز سياسته الأمنية والدفاعية بحلول عام 2030، بما في ذلك تعزيز مجموعة أدوات الدبلوماسية الإلكترونية للاتحاد الأوروبي ومواصلة تطوير سياسة الاتحاد الأوروبي للدفاع الإلكتروني ليكون أفضل استعداداً للهجمات الإلكترونية والتصدي لها.

ويشير الاتحاد الأوروبي والدول الأعضاء فيه إلى اعتماد مجلس الاتحاد الأوروبي في 23 أيار/مايو 2022 استنتاجات بشأن تطوير موقف الاتحاد بشأن الفضاء الإلكتروني. ويهدف هذا الموقف إلى إظهار تصميم الاتحاد الأوروبي على القيام بإجراءات فورية وطويلة الأجل للتصدي للجهات الفاعلة التي تشكل تهديداً وتسعى إلى حرمان الاتحاد الأوروبي من الوصول الآمن والمفتوح إلى الفضاء الإلكتروني.

مضمون المفاهيم المشار إليها في تقرير الفريق العامل وتقارير فريق الخبراء الحكوميين

التهديدات القائمة والناشئة

يقرُّ الاتحاد الأوروبي والدول الأعضاء فيه بأن الفضاء الإلكتروني يتيح فرصاً كبيرة للنمو الاقتصادي، فضلاً عن التنمية المستدامة والشاملة. ومع ذلك، فإن التهديدات الجسيمة المتصلة بتكنولوجيا المعلومات والاتصالات المشار إليها في التقارير السابقة لفريق الخبراء الحكوميين وفي تقرير الفريق العامل[11] لا تزال قائمة وتطرح تحديات تتطور باستمرار.

ويساور الاتحاد الأوروبي والدول الأعضاء فيه القلق إزاء تزايد السلوك الخبيث في الفضاء الإلكتروني، بما في ذلك إساءة استخدام تكنولوجيات المعلومات والاتصالات لأغراض خبيثة، من قِبَل جهات

(10) 22/7371، "بوصلة استراتيجية للأمن والدفاع – من أجل اتحاد أوروبي يحمي مواطنيه وقيمه ومصالحه ويسهم في السلم والأمن الدوليين".

(11) A/75/816.

فاعلة حكومية وغير حكومية على السواء، فضلاً عن زيادة سرقة الملكية الفكرية بوسائل يتيحها الفضاء الإلكتروني. وهذا السلوك يقوّض النمو الاقتصادي ويهدّده، كما يهدد سلامة المجتمع العالمي وأمنه واستقراره، ويمكن أن يؤدي إلى آثار مزعزعة للاستقرار ومتعاقبة مع زيادة مخاطر نشوب النزاعات.

وقد أظهرت جائحة مرض فيروس كورونا (كوفيد-19) مخاطر وعواقب الأنشطة الخبيثة لتكنولوجيات المعلومات والاتصالات. ويلاحظ الاتحاد الأوروبي والدول الأعضاء فيه التهديدات الإلكترونية والأنشطة الإلكترونية الخبيثة التي تستهدف المشغلين الأساسيين، وتقرُّ بضعف الهياكل الأساسية الحيوية للمعلومات، والهياكل الأساسية التي توفر الخدمات الأساسية للجمهور، والهياكل الأساسية التقنية الضرورية لتوافر الإنترنت أو سلامتها بوجه عام، وكيانات القطاع الصحي وغيرها من كيانات القطاعات الحيوية في الدول الأعضاء وشركائها. ومما يثير قلق الاتحاد الأوروبي والدول الأعضاء فيه بشكل خاص الزيادة في الأنشطة التي تؤثر على أمن وسلامة منتجات وخدمات تكنولوجيا المعلومات والاتصالات، التي قد تكون لها آثار عامة. وكذلك، في سياق سلوك روسيا غير المتسم بالمسؤولية في الفضاء الإلكتروني بوصفه جزءاً لا يتجزأ من غزوها غير المشروع وغير المبرَّر لأوكرانيا، شهد الاتحاد الأوروبي ودوله الأعضاء استخدام الهجمات الإلكترونية التي تنطوي على أدوات مدمرة، مثل البرامجيات الماسحة للبيانات للتسبب في تعطل النُظم، بل وانقطاع الخدمة أيضاً، ومحاولات التسلل، وعمليات التشويه، وهجمات حجب الخدمة الموزع التي تستهدف أوكرانيا، مع احتمال امتداد آثارها الثانوية إلى بلدان أخرى، ولا سيما الدول المجاورة لأوكرانيا.

ويدين الاتحاد الأوروبي والدول الأعضاء فيه هذا السلوك الخبيث في الفضاء الإلكتروني، بما في ذلك النشاط الخبيث في مجال تكنولوجيا المعلومات والاتصالات الذي يهدف إلى استغلال مواطن الضعف، وتؤكد دعمها المستمر لزيادة قدرة النظم الإلكترونية العالمية على الصمود. فأي محاولة لإعاقة قدرة الهياكل الأساسية الحيوية هي أمر غير مقبول ويمكن أن يعرّض حياة الناس للخطر.

ويدعو الاتحاد الأوروبي والدول الأعضاء فيه جميع البلدان إلى عدم السماح عن علم باستخدام أراضيها لارتكاب أفعال غير مشروعة دولياً في الفضاء الإلكتروني باستخدام تكنولوجيات المعلومات والاتصالات وإلى اتخاذ الإجراءات المناسبة ضد الجهات الفاعلة التي تقوم بهذه الأنشطة من أراضيها، بما يتسق مع القانون الدولي وتقارير الأعوام 2010 و 2013 و 2015 و 2021 الصادرة بتوافق الآراء عن أفرقة الخبراء الحكوميين وعن الفريق العامل في عام 2021. ويؤكد الاتحاد الأوروبي والدول الأعضاء فيه مرة أخرى على أنه ينبغي للدول أن تتخذ جميع التدابير المناسبة والخطوات المتاحة والممكنة على نحو معقول لاكتشاف الحالة والتحقيق فيها ومعالجتها.

وبالإضافة إلى ذلك، وكما أقِرَّ بذلك في التقارير السابقة لفريق الخبراء الحكوميين والفريق العامل، وبالنظر إلى الطابع الفريد لتكنولوجيات المعلومات والاتصالات، فإن نهج الاتحاد الأوروبي في معالجة المسائل المتعلقة بالفضاء الإلكتروني في سياق الأمن الدولي ما زال يتكيف مع التطورات التكنولوجية الجديدة، علماً بأن معايير سلوك الدول المسؤول في الفضاء الإلكتروني محايدة من الناحية التكنولوجية. وهذا يتسق مع مفهوم الأمم المتحدة واعترافها بأن القانون الدولي القائم ينطبق على المجالات الجديدة.

ولا يمكن للاتحاد الأوروبي والدول الأعضاء فيه إلا أن تدعم تطوير واستخدام التكنولوجيات أو النظم أو الخدمات التي تتيحها تكنولوجيات المعلومات والاتصالات والتي تحترم احتراماً كاملاً القانون الدولي

والقواعد الدولية المنطبقة، ولا سيما ميثاق الأمم المتحدة، فضلاً عن القانون الدولي الإنساني وقانون حقوق الإنسان.

كيفية انطباق القانون الدولي على استخدام تكنولوجيات المعلومات والاتصالات

يدعم الاتحاد الأوروبي والدول الأعضاء فيه بقوة إقامة نظام فعال متعدد الأطراف، يستند إلى نظام دولي قائم على القواعد، يحقق نتائج في التصدي للتحديات العالمية الحالية والمقبلة في الفضاء الإلكتروني.

ولا يمكن لإطار عالمي حقيقي لأمن الفضاء الإلكتروني إلا أن يستند إلى القانون الدولي القائم، بما في ذلك ميثاق الأمم المتحدة برمته، والقانون الإنساني الدولي، والقانون الدولي لحقوق الإنسان. ويكرر الاتحاد الأوروبي والدول الأعضاء فيه تأكيد انطباق القانون الدولي القائم على سلوك الدول في الفضاء الإلكتروني، على النحو الذي أقِرَّ به في تقارير فريق الخبراء الحكوميين في الأعوام 2010 و 2013 و 2015 و2021، وكذلك المبادئ المنصوص عليها في الفقرات الفرعية 71(ب) إلى (ز) من تقرير عام 2021 والتي نص عليها الفريق العامل.

وينطبق القانون الدولي، بما في ذلك القانون الدولي الإنساني، الذي يشمل مبادئ الإنسانية والتمييز والحيطة والضرورة العسكرية والتناسب، على سلوك الدول في الفضاء الإلكتروني وهو قانون يركز على الحماية في مجمله، من خلال وضع حدود واضحة لشرعيته، بما في ذلك في سياق النزاع. ويؤكد الاتحاد الأوروبي أن القانون الدولي الإنساني ليس من العوامل التمكينية للنزاعات؛ وإنما هو يحدد القواعد التي تحكم العمليات العسكرية للحد من آثارها، ولا سيما لحماية السكان المدنيين.

وعلاوة على ذلك، يجب احترام حقوق الإنسان والحريات الأساسية المنصوص عليها في الصكوك الدولية ذات الصلة والتمسك بها بطريقة متساوية داخل شبكة الإنترنت وخارجها. ويرحب الاتحاد الأوروبي ودوله الأعضاء بأن مجلس حقوق الإنسان[12] والجمعية العامة قد أكَّدا أيضاً هذه المبادئ، وكذلك فريق الخبراء الحكوميين والفريق العامل.

ولهذه الأسباب، لا يدعو الاتحاد الأوروبي والدول الأعضاء فيه إلى وضع صكوك قانونية دولية جديدة للمسائل المتعلقة بالفضاء الإلكتروني في هذه المرحلة، وتشدّد على ضرورة الاضطلاع بمزيد من العمل لتوضيح كيفية انطباق القانون الدولي على الفضاء الإلكتروني.

ويؤكد الاتحاد الأوروبي والدول الأعضاء فيه من جديد دعمها لمواصلة الحوار والتعاون من أجل تعزيز التفاهم المشترك بشأن تطبيق القانون الدولي القائم على استخدام الدول لتكنولوجيا المعلومات والاتصالات، فضلاً عن دعمها للجهود الرامية إلى إضفاء الوضوح القانوني على كيفية انطباق القانون الدولي القائم، حيث أن ذلك سيسهم في صون السلام ومنع نشوب النزاعات وضمان الاستقرار العالمي.

ونواصل دعم الجهود الجارية الرامية إلى تعزيز تطبيق القانون الدولي القائم على الفضاء الإلكتروني، بما في ذلك تبادل المعلومات وأفضل الممارسات بشأن تطبيق القانون الدولي القائم في الفضاء الإلكتروني. ونحن ملتزمون بمواصلة الإبلاغ عن المواقف الوطنية بشأن كيفية انطباق القانون الدولي على استخدام الدول لتكنولوجيا المعلومات والاتصالات، حيث أنه يعزز الشفافية ويقوّي الفهم العالمي للنُهُج

(12) انظر قرار مجلس حقوق الإنسان 8/20.

الوطنية، وهو أمر أساسي للحفاظ على السلام والاستقرار على المدى الطويل ويقلل من خطر نشوب النزاعات من خلال أعمال في الفضاء الإلكتروني. وينبغي زيادة التركيز على التوعية وبناء القدرات فيما يتعلق بانطباق القانون الدولي القائم كوسيلة لتعزيز الاستقرار ومنع نشوب النزاعات في الفضاء الإلكتروني.

معايير سلوك الدول المسؤول وقواعده ومبادئه

يشجع الاتحاد الأوروبي والدول الأعضاء فيه جميع الدول على الاستفادة من العمل الذي أقرَّته الجمعية العامة مراراً، ولا سيما في القرار 19/76، والنهوض به، وعلى المضي قدماً في تنفيذ هذه المعايير وتدابير بناء الثقة المتفق عليها، التي تؤدي دوراً أساسياً في منع نشوب النزاعات.

ويسترشد الاتحاد الأوروبي والدول الأعضاء فيه في استخدام تكنولوجيا المعلومات والاتصالات بالقانون الدولي القائم وستستمر في ذلك مستقبلاً، وستتقيَّد أيضاً بالمعايير والقواعد والمبادئ الطوعية، غير الملزمة، للسلوك المسؤول للدول وتنفيذها في الفضاء الإلكتروني، على النحو المبين في التقارير المتعاقبة لفريق الخبراء الحكوميين في الأعوام 2010 و 2013 و 2015 و 2021. ونرحب باستمرار الحوار الشامل والبناء داخل الفريق العامل لزيادة تعميق المناقشات بشأن هذا الإطار وبشأن التحديات الأمنية المتصلة باستخدام تكنولوجيات المعلومات والاتصالات. ونعتقد أن الطريق العملي للمضي قدماً ينبغي أن يشجع على زيادة التعاون والشفافية لتبادل أفضل الممارسات، بما في ذلك فيما يتعلق بكيفية تطبيق المعايير الحالية لفريق الخبراء الحكوميين، من خلال المبادرات والأطر ذات الصلة، مثل المنظمات والمؤسسات الإقليمية، لتيسير التوعية والتنفيذ الفعال للمعايير المتفق عليها للسلوك المسؤول للدول.

تدابير بناء الثقة

يمثل بناء آليات فعالة للتعاون بين الدول والتفاعل فيما بينها في الفضاء الإلكتروني عنصرين حاسمين في منع نشوب النزاعات. وأثبتت المنتديات الإقليمية أنها منبر مهم لتهيئة حيّز للحوار والتعاون بين الجهات الفاعلة ذات الشواغل المشتركة والمصالح المشتركة من أجل التصدي بفعالية للتحديات من منظور إقليمي.

وسيزيد وضع وتنفيذ تدابير لبناء الثقة في الفضاء الإلكتروني، بما في ذلك تدابير التعاون والشفافية، في إطار منظمة الأمن والتعاون في أوروبا، والمنتدى الإقليمي لرابطة أمم جنوب شرق آسيا، ومنظمة الدول الأمريكية، وغيرها من الأوساط الإقليمية، من إمكانية التنبؤ بسلوك الدول وسيقللان من خطر سوء التفسير والتصعيد والنزاع الذي قد ينشأ عن حوادث تكنولوجيا المعلومات والاتصالات، وبالتالي سيسهمان في تحقيق الاستقرار في الفضاء الإلكتروني على المدى الطويل.

التعاون والمساعدة الدوليان فيما يتعلق بأمن تكنولوجيات المعلومات والاتصالات وبناء القدرات المتعلقة بها

من أجل منع نشوب النزاعات والحد من التوترات الناجمة عن إساءة استخدام تكنولوجيات المعلومات والاتصالات، يهدف الاتحاد الأوروبي والدول الأعضاء فيه إلى تعزيز القدرة على الصمود على الصعيد العالمي، مع التركيز بوجه خاص على البلدان النامية، كوسيلة للتصدي للتحديات المرتبطة برقمنة الاقتصادات والمجتمعات، وكذلك الحد من قدرة مرتكبي الجرائم المحتملين على إساءة استخدام تكنولوجيات

المعلومات والاتصـــالات لأغراض خبيثة. وتعزز القدرة على الصـــمود قدرة الدول على التصـــدي بفعالية للتهديدات الإلكترونية والتعافي من آثارها.

ويدعم الاتحاد الأوروبي والدول الأعضاء فيه مجموعة من البرامج والمبادرات المصممة خصيصاً لمساعدة البلدان على تطوير مهاراتها وقدراتها للتصدي للحوادث الإلكترونية، فضلاً عن المبادرات الرامية إلى تيسير تبادل أفضل الممارسات، سواء من خلال المشاركة المباشرة أو الاتصالات الثنائية أو المشاركة من خلال المؤسسات الإقليمية والمتعددة الأطراف.

ويقر الاتحاد الأوروبي والدول الأعضـــاء فيه بأن تعزيز قدرات الحماية المناســـبة وزيادة أمن المنتجات والعمليات والخدمات الرقمية سيسهمان في زيادة أمن الفضاء الإلكتروني وجدارته بالثقة. ونسلم بمسؤولية جميع الجهات الفاعلة ذات الصلة عن المشاركة في تنمية القدرات في هذا الصدد، وندعو كذلك إلى تعزيز التعاون مع الشركاء الدوليين الرئيسيين والمنظمات الدولية الرئيسية لدعم بناء القدرات في بلدان ثالثة. ويولي الاتحاد الأوروبي والدول الأعضـــاء فيه أهمية خاصـــة لتعزيز الأمن والاســـتقرار الدوليين في الفضاء الإلكتروني من خلال تشجيع وتيسير اتخاذ إجراءات ملموسة بشأن سلوك الدول المسؤول في الفضاء الإلكتروني، ومن خلال تعزيز التعاون في مجال بناء القدرات المتعلقة بالفضـــاء الإلكتروني، بما في ذلك بدعم من آلية تيسير في الأمم المتحدة بغية تعزيز برامج بناء القدرات المصممة خصيصاً لتلبية الاحتياجات التي تحددها الدول المستفيدة، مثل برنامج العمل، والوقوف على الآليات التي تيسّر مشاركة جميع الجهات صاحبة المصلحة في تنفيذ إطار السلوك المسؤول.