الأمم المتحدة

A/76/187

الجمعية العامة

Distr.: General
19 July 2021
Arabic
Original: English/Spanish

الدورة السادسة والسبعون

البند 96 من جدول الأعمال المؤقت*

التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي

الارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي

تقرير الأمين العام

المحتويات

* A/75/150.

160921 080921 21-10045 (A)

أولا - مقدمة

1 - في 7 كانون الأول/ديسمبر 2020، اعتمدت الجمعية العامة القرار 32/75 المعنون "الارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي"، وذلك ضمن بند من جدول الأعمال المعني "بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي".

2 - وفي الفقرة 2 من القرار، دعت الجمعية العامة جميع الدول الأعضاء إلى أن تراعي التقييمات والتوصيات الواردة في تقارير فريق الخبراء الحكوميين فتواصل موافاة الأمين العام بآرائها وتقييماتها بشأن المسائل التالية:

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

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

3 - وعملا بذلك الطلب، أُرسلت مذكرة شفوية في 18 شباط/فبراير 2021 إلى جميع الدول الأعضاء تدعُوها إلى تقديم معلومات بشأن هذا الموضوع. ولتيسير تقديم آراء الدول الأعضاء بشأن المسائل المبينة أعلاه، كان الموعد النهائي لتقديمها هو 31 أيار/مايو 2021.

4 - وترد الردود التي وردت وقت إعداد التقرير في الفرعين الثاني والثالث أدناه. وستُنشر الردود الإضافية الواردة بعد 31 أيار/مايو 2021 في الموقع الشبكي لمكتب شؤون نزع السلاح[1] باللغة الأصلية التي وردت بها. ولن تصدر أي إضافات.

ثانيا - الردود الواردة من الحكومات

أستراليا

[الأصل: بالإنكليزية]
[31 أيار/مايو 2021]

ترحب أستراليا بفرصة الردّ على دعوة الجمعية العامة الواردة في قرارها 32/75 حتى تقدّم وجهات نظرها بشأن الارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي. وتستند هذه المذكرة إلى المعلومات التي قدمتها أستراليا في عام 2020 عملا بالقرار 28/74 وفي عام 2016 عملا بالقرار 237/70، وفي عام 2014 عملا بالقرار 243/68، وفي عام 2011 عملا بالقرار 41/65 بشأن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي.

الاستراتيجية الدولية للتعامل مع تكنولوجيا الفضاء الإلكتروني والتكنولوجيا الحيوية

في 21 نيسان/أبريل 2021، أطلقت وزيرة الخارجية مريس باين استراتيجية أستراليا الدولية للتعامل مع تكنولوجيا الفضاء الإلكتروني والتكنولوجيا الحيوية، التي تحدد مصالح أستراليا وأهدافها في مجال الفضاء الإلكتروني والتكنولوجيا الحيوية. ويتمثل الهدف الرئيسي لأستراليا في جعل البلد آمنا ومزدهرا في منطقة

(1) https://www.un.org/disarmament/ict-security.

المحيطين الهندي والهادئ وفي العالم بفضل تكنولوجيا الفضاء الإلكتروني والتكنولوجيا الحيوية (www.internationalcybertech.gov.au/).

وتحدد الاستراتيجية مصالح أستراليا في السعي لتحقيق هذا الهدف عبر مجموعة من المسائل المتعلقة بتكنولوجيا الفضاء الإلكتروني والتكنولوجيا الحيوية. ويشمل ذلك مبادئنا وقيمنا الأساسية المتعلقة بحقوق الإنسان وسيادة القانون والإنصاف والمنافسة الحرة والأمن والشفافية والاحترام والنزاهة.

وتضبط الاستراتيجية ثلاث ركائز رئيسية هي: القيم والأمن والازدهار، لتوجيه انخراط أستراليا في تكنولوجيا الفضاء الإلكتروني والتكنولوجيا الحيوية على المستوى الدولي:

(أ) *القيم* – ستسعى أستراليا دائما إلى اتباع نهج قائم على القيم في التعامل مع تكنولوجيا الفضاء الإلكتروني والتكنولوجيا الحيوية، وهي تعارض الجهود الرامية إلى استخدام التكنولوجيات في تقويض هذه القيم؛

(ب) *الأمن* – ستدعم أستراليا دائما السلام والاستقرار الدوليين والتكنولوجيا الآمنة والموثوقة والمرنة.

(ج) *الازدهار* – ستنادي أستراليا دائما بجعل الفضاء الإلكتروني والتكنولوجيا يدعمان النمو الاقتصادي والتنمية المستدامين من أجل تعزيز الازدهار.

وفي 6 آب/أغسطس 2020، أصدرت أستراليا أيضا استراتيجيتها للأمن السيبراني لعام 2020 من أجل بلوغ عالم أكثر أمنا على الإنترنت بالنسبة للأستراليين ولأعمالهم وللخدمات الأساسية التي تعتمد عليها أستراليا (www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf).

إطار لسلوك الدول المسؤول في الفضاء الإلكتروني

مع تزايد ممارسة الدول للقوة والنفوذ في الفضاء الإلكتروني، ترى أستراليا أنه من المهم أن تكون هناك قواعد واضحة. وتقارير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي لعام 2010 (A/65/201) وعام 2013 (A/68/98) وعام 2015 (A/70/174) تؤكد مجتمعةً سريان القانون الدولي القائم وأهميته الحيوية في صون السلام والاستقرار داخل الفضاء الإلكتروني. وتعرض التقارير أيضاً 11 من القواعد الطوعية غير الملزمة لسلوك الدول المسؤول، وتسلم في الوقت نفسه بالحاجة إلى تدابير لبناء الثقة وإلى بناء القدرات على نحو منسق. وبصورة مجتمعة، يتيح القانون الدولي والقواعد وتدابير بناء الثقة وبناء القدرات المرتكزَ الذي يكفل انفتاح الفضاء الإلكتروني وأمانه واستقراره وازدهاره، وكثيرا ما يشار إلى هذه القوانين والقواعد والتدابير على أنها إطار لسلوك الدول المسؤول.

وقد شاركت أستراليا بنشاط في عمليتين للأمم المتحدة أُجريتا مؤخرا للنظر في سلوك الدول المسؤول في الفضاء الإلكتروني، واختتمتا في عام 2021؛ وهاتان العمليتان هما: فريق الخبراء الحكوميين السادس (انظر A/76/135) والفريق العامل المفتوح العضوية (انظر A/75/816)، اللذان يؤكدان من جديد هذا الإطار ويستندان إليه.

وتؤكد أســـتراليا من جديد التزامها بالعمل وفقا لتقارير فريق الخبراء الحكوميين للأعوام 2010 و 2013 و 2015 و 2021 مجتمعة (A/65/201 و A/68/98 و A/70/174) ولتقرير الفريق العامل المفتوح العضوية (A/75/816).

القانون الدولي

يرد موقف أستراليا بشأن كيفية تطبيق القانون الدولي على سلوك الدول في الفضاء الإلكتروني ضمن سلسلة من الوثائق هي: استراتيجية أستراليا الدولية لعام 2017 بشأن التعامل مع تكنولوجيا الفضاء الإلكتروني (www.internationalcybertech.gov.au/about/2017-International-Cyber-Engagement-Strategy)، وملحق القانون الدولي لعام 2019 (**Error! Hyperlink reference not valid.**)، ودراسات الحالات الإفرادية عن سريان القانون الدولي على الفضاء الإلكتروني المنشورة في شباط/فبراير 2020 (https://www.dfat.gov.au/sites/default/files/australias-oewg-non-paper-case-studies-on-the-application-of-international-law-in-cyberspace.pdf)، *واستراتيجية أستراليا الدولية لعام 2021 بشأن التعامل مع تكنولوجيا الفضاء الإلكتروني والتكنولوجيا الحيوية*، ومذكرة أستراليا بشأن القانون الدولي التي سترد ضمن مرفق تقرير عام 2021 لفريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي (لم يصدر بعد).

انخراط الجهات المعنية المتعددة

تدرك أستراليا أهمية دوائر الجهات المعنية المتعددة، التي تشمل المجتمع المدني والقطاع الخاص والأوساط الأكاديمية والتقنية، في الإسهام في إنشاء فضاء إلكتروني حر ومفتوح وآمن ومستقر وميسَّر وسلمي.

ولهذا الغاية، تشعر أستراليا بالسرور للمشاركة في رعاية مبادرة LetsTalkCyber (letstalkcyber.org)، التي وفرت منبرا للجهات المعنية المتعددة لكي تقدم وجهات نظرها وتتفاعل مع الفريق العامل المفتوح العضوية، ولكي يتم إجراء مشاورات بين الدول والمجتمع المدني والقطاع الخاص والأوساط الأكاديمية والأوساط التقنية. وأجرت أستراليا أيضا عدة جولات من المشاورات الوطنية بين الجهات المعنية المتعددة، وسعت بنشاط إلى الحصول على آراء هذه الجهات من أجل إثراء مواقفها في عمليات الفريق العامل المفتوح العضوية وفي فريق الخبراء الحكوميين.

وبالإضافة إلى ذلك، أنشأت أستراليا شبكة كواد للتكنولوجيا (Quad Tech Network) لدعم البحوث وتعزيز المشاركة بين الدول والجهات الشريكة من الأكاديميين ومراكز الفكر، من أستراليا والهند واليابان والولايات المتحدة الأمريكية، في تناول مسائل تكنولوجيا الفضاء الإلكتروني والتكنولوجيا الحيوية. وستصدر شبكة كواد للتكنولوجيا بحوثا وتوصيات ذات صلة بالسياسات؛ وستعمّق وتعزز فهم الجمهور لقضايا الفضاء الإلكتروني والتكنولوجيا الحيوية؛ وستشجع الحوار العام المستنير. وقد تم إطلاق هذه الشبكة في 9 شباط/فبراير بسلسلة من الأوراق العامة عن السلام والأمن الدوليين، والاتصال والمرونة الإقليمية، وحقوق الإنسان والأخلاق، والأمن القومي (www.internationalcybertech.gov.au/node/139).

كولومبيا

[الأصل: بالإسبانية]
[31 أيار/مايو 2021]

عملا بقرار الجمعية العامة 32/75 بشأن الارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي، وبمراعاة التقييمات والتوصيات الواردة في التقارير الصادرة عن فريق الخبراء الحكوميين، يسرّ كولومبيا موافاة الأمين العام بآرائها وتقييماتها بشأن المسائل التالية:

- الجهود المبذولة على الصعيد الوطني لتعزيز أمن المعلومات وتشجيع التعاون الدولي بهذا الشأن؛
- مضمون المفاهيم المشار إليها في تقارير فريق الخبراء الحكوميين.

ويستند هذا التقرير إلى التقرير المقدم في عام 2020، ليسلط الضوء على التقدم المحرز في العام الماضي، ولا سيما فيما يتعلق بالتوصيات المعروضة على نظر الدول ضمن تقرير فريق الخبراء الحكوميين لعام 2015، وذلك من أجل تهيئة بيئة مفتوحة وآمنة ومستقرة وميسرة وسلمية في مجال تكنولوجيا المعلومات والاتصالات.

قواعد سلوك الدول المسؤول وضوابطه ومبادئه الطوعية

عملا بمقاصد الأمم المتحدة، بما فيها المقصد المتعلقة بصون السلام والأمن الدوليين، ينبغي للدول أن تتعاون على وضع وتطبيق تدابير لزيادة الاستقرار والأمن في استخدام تكنولوجيات المعلومات والاتصالات، ولمنع ما يتصل بتلك التكنولوجيات من ممارسات تعتبر ضارة أو قد تشكل تهديدات للسلام والأمن الدوليين.

وجرى التشديد على مفهوم الملكية في السياسة الوطنية بشأن الثقة والأمن الرقميين (الوثيقة رقم 2020/3995 الصادرة عن المجلس الوطني للسياسات الاقتصادية والاجتماعية)، الذي يكمن أحد أهدافه الرئيسية المعلنة في بناء قدرات المواطنين في مجال الأمن الرقمي داخل القطاعين العام والخاص.

وقد نفذت حكومة كولومبيا، من خلال وزارة تكنولوجيا المعلومات والاتصالات ودائرة التدريب الوطنية ووزارة التعليم، سلسلة من الأنشطة المحددة القائمة على استراتيجية الملكية، وذلك كالآتي:

- وفي إطار برنامج "دعونا نتحدث عن الحكومة الرقمية"، الذي يغطي الفترة من 2020 إلى 2021، عقدت وزارة تكنولوجيا المعلومات والاتصالات 15 جلسة توعية تتعلق بالأمن الرقمي للمواطنين، وصلت إلى أكثر من 000 4 شخص. وفي عام 2020، عقدت الوزارة ثلاث حلقات عمل تدريبية في مجال الأمن الرقمي لأصحاب المؤسسات المتناهية الصغر والصغيرة والمتوسطة، بمشاركة 483 شخصا، من بينهم 156 امرأة. كما عقدت حلقتي عمل تتعلقان بجوانب محددة من نموذج أمن المعلومات والخصوصية.
- وفي إطار "شهر الأمن الرقمي"، أجريت عدة أنشطة، بما في ذلك أربع حلقات عمل عن مواضيع متخصصة تتعلق بإدارة الحوادث، بدعم من شركة سيسكو ومن فريق مواجهة الطوارئ الحاسوبية في كولومبي؛ وحلقتي عمل عن أهمية التدقيق وإدارة المخاطر في الكيانات العامة؛ وجلستين في إطار برنامج "دعونا نتحدث عن الحكومة الرقمية" عن نتائج العملية التي أجريت مع منظمة الدول

الأمريكية؛ وأول اجتماع لمجلس الابتكار في مجال أمن الفضاء الإلكتروني يُعقد في كولومبيا؛ والمحادثات المعنونة "توصيات لتجنب أن تصبح ضحية لمجرمي الإنترنت" و "التضليل على شبكة الإنترنت من منظور قانوني"، الموجهة إلى عامة الناس. وفي ختام أنشطة هذا الشهر، تم عقد الاجتماع الثاني لمجلس الابتكار في مجال أمن الفضاء الإلكتروني وذلك بالتعاون مع منظمة الدول الأمريكية. وشارك في هذه الأنشطة ما مجموعه 040 1 شخصا، بمن فيهم موظفون حكوميون ومستخدمون نهائيون، وكانت المرأة تشكل نسبة 45 في المائة من هؤلاء المشاركين.

- وخلال فعالية "كولومبيا 4,0"، وفي إطار الأنشطة التي نفذت خلال قمة كبار مسؤولي شؤون المعلومات لعام 2020، التي جمعت قادة التكنولوجيا في الكيانات العامة، عُقد مؤتمر تحت عنوان "كيفية تجاوز كوفيد-19 والتحول الرقمي دون التعرض للاختراق"، ضم 490 شخصا. وعُقدت أيضا حلقة عمل تحت عنوان "أفضل الممارسات للكشف عن التهديدات والتصدي لها استنادا إلى نموذج MITRE ATT&.CK و XDR"، شاركت فيها المرأة بنسبة 40 في المائة حسب التقديرات. ونُظمت أنشطة للتوعية على نموذج أمن المعلومات والخصوصية وذلك لفائدة 196 3 مسؤولا من 834 1 كيانا، بما في ذلك 131 كيانا وطنيا و 224 1 كيانا محليا.

- أطلقت وزارة تكنولوجيا المعلومات والاتصالات، في إطار مبادرتها المعنونة "المواهب الرقمية"، مسابقة "المهارات الرقمية – التدريب على أمن الفضاء الإلكتروني" لاختيار موظفين كولومبيين وتدريبهم وبناء قدراتهم في المسائل المتعلقة بهذا الأمن. وتم تقديم دورتين دراسيتين للحصول على دبلوم في مجال تطوير المهارات المتخصصة: '1' دورة عن أمن الفضاء الإلكتروني للمديرين التنفيذيين والمديرين؛ و '2' دورة عن أمن الفضاء الإلكتروني للموظفين التقنيين.

- تقدم دائرة التدريب الوطنية برامج عن المواضيع التالية: أمن شبكات الحاسوب، وإدارة قواعد البيانات والأمن، ورصد الأمن الرقمي، وبرمجة البرامج الثابتة للأجهزة، واستحداث نظم إدارة أمن المعلومات وفقا للمعيار رقم 27001 للمنظمة الدولية للتوحيد القياسي/اللجنة الكهربائية التقنية الدولية، وتطبيق تقنيات التشخيص في مجال أمن الفضاء الإلكتروني، وإدارة أمن الحواسيب.

- لتشجيع الملكية، نفذت وزارة التعليم أنشطة تتعلق بنشر المحتوى (استخدام الشبكات الاجتماعية، وتنظيم حملات وحلقات عمل مع الكيانات العامة والمؤسسات المتناهية الصغر والصغيرة والمتوسطة). وأقامت الوزارة أيضا شراكات مع القطاع الخاص وشاركت في التعاون الدولي.

- وضعت وزارة التعليم أيضا دراسات دبلوم استفاد منها 216 2 معلما، وقامت بإدراج استراتيجية الأمن الرقمي ضمن مشروع التعلم الرقمي لطلاب المدارس الابتدائية والأساسية والثانوية، ليستفيد منها 093 4 طالبا، بما في ذلك على بوابة "كولومبيا تتعلم" *(Colombia Aprende)*، التي تنطوي على أكثر من 30 بندا من بنود المحتويات.

واستجابة للتوصية التي تدعو الدول إلى عدم السماح عن علم باستخدام أراضيها لارتكاب أفعال غير مشروعة دولياً باستخدام تكنولوجيات المعلومات والاتصالات، نفذت حكومة كولومبيا الأنشطة المبينة أدناه.

- السياسة الوطنية للثقة والأمن الرقميين (الوثيقة رقم 2020/3995 الصادرة عن المجلس الوطني للسياسات الاقتصادية والاجتماعية) نصت على دور المنسق الوطني، بوصفه آلية للتنسيق والحوكمة، حيث يضطلع بهذا الدور مكتب مستشاري الرئيس لشؤون التحول الاقتصادي والرقمي،

ولجنة الأمن الرقمي، التي هي عبارة عن هيئة جماعية تتألف من كيانات معنية بتعزيز الأمن الرقمي هدفها النظر في مسائل محددة تتعلق بالأمن الرقمي على المستويات الاستراتيجية، وذلك ضمن المجالات التي تشملها ولايتها وهي: (1) سياسة الأمن الرقمي وقوانينه؛ (2) وحماية البنى التحتية الإلكترونية الحيوية الوطنية والدفاع عنها؛ (3) وإدارة مخاطر الأمن الرقمي؛ (4) ورصد الأزمات والتهديدات الإلكترونية؛ (5) وحماية البيانات الشخصية؛ (6) وقضايا الأمن الرقمي الدولي؛ (7) والاتصالات الاستراتيجية من أجل الأمن الرقمي.

- أنشأت الحكومة مركز قيادة موحد لأمن الفضاء الإلكتروني وذلك من أجل أمن وسلامة البنى التحتية التكنولوجية والمواقع الإلكترونية التابعة للحكومة خلال الأعياد الوطنية والانتخابات وغيرها من الأحداث البارزة. وتتمثل أهداف المركز فيما يلي: '1' حماية المواطنين والحكومة من التهديدات الإلكترونية؛ '2' ومنع التهديدات الإلكترونية واستباقها وإجراء التحقيقيات القضائية؛ '3' والتصدي لحوادث أمن الفضاء الإلكتروني؛ '4' وضمان استقرار الهيئات الحكومية والمؤسسية؛ '5' وتعزيز البرامجيات. ووضعت الحكومة أيضا بروتوكولات عمل من أجل التصدي للهجمات المحتملة، مثل هجمات حجب الخدمة الموزع على بوابات الإنترنت، ونقاط الضعف الشبكية، والأخبار الزائفة.

- اضطلعت الحكومة بأنشطة منسقة مع مجلس الشيوخ الوطني، بما في ذلك التدريب على وضع أفضل الممارسات لاستخدام المنصات الافتراضية.

وفيما يتعلق بأفضل السبل للتعاون على تبادل المعلومات، وتقديم المساعدة المتبادلة، والملاحقة القضائية على الاستخدام الإرهابي والإجرامي لتكنولوجيات المعلومات والاتصالات، وتنفيذ تدابير تعاونية أخرى لمواجهة هذه التهديدات، انضمّت كولومبيا في 16 آذار/مارس 2020 إلى الاتفاقية المتعلقة بالجريمة الإلكترونية، التي اعتُمدت في بودابست في عام 2001، وبدأ نفاذها في 1 تموز/يوليه 2020. والجهود مبذولة حاليا من أجل تنفيذ هذه الاتفاقية.

واتخذت كولومبيا التدابير المناسبة لحماية الهياكل الأساسية الحيوية من تهديدات تكنولوجيا المعلومات والاتصالات وذلك بتعزيز الفريق الحكومي المعني بالتصدي لحوادث أمن الفضاء الإلكتروني حتى يتمكن من حماية المؤسسات العامة. وتهدف كولومبيا من خلال هذه المبادرة إلى وضع حل شامل يكفل أن يزوّد الفريق الحكومي كيانات الدولة بخدمات أقوى وأكثر كفاءة، ويعزز أثر الفريق في جميع أنحاء البلد من خلال تطوير تكنولوجيا المعلومات والبنى التحتية المادية والمواهب البشرية وضمان الخدمات على مدار الساعة وطوال الأسبوع.

واقترحت كولومبيا أيضا عددا من المبادرات، منها إعداد تقييم حديث وخطة من أجل التحسين المستمر لقدراتها التشغيلية والإدارية والبشرية والعلمية وللبنى التحتية التكنولوجية، وذلك بغية حشد الموارد لتعزيز قدرات تلك الكيانات في مجال الأمن الرقمي. ويجري أيضا تنفيذ مشروع من أجل نقل مقر الفريق الحكومي المعني بالتصدي لحوادث أمن الفضاء الإلكتروني وتحسين أساليب عمله.

واستجابة للتوصية التي تدعو الدول إلى أن تشجع على الإبلاغ المسؤول عن نقاط الضعف المتصلة بتكنولوجيات المعلومات والاتصالات وأن تقدم ما لديها من معلومات ذات صلة عن الوسائل المتاحة لعلاجها من أجل تقليل، وربما استئصال، التهديدات المحتملة التي تتعرض تكنولوجيات المعلومات

والاتصـــالات والبنى التحتية المعتمدة على تلك التكنولوجيات، تعمل كولومبيا، بالاشـــتراك مع منظمة الدول الأمريكية ومع منظمة التعاون والتنمية في الميدان الاقتصـــادي، على تشـــجيع الإبلاغ المســـؤول عن أوجه الضـــعف في تكنولوجيا المعلومات والاتصـــالات، وهي الآن بصـــدد اتخاذ خطوات معقولة لضـــمان ســـلامة سلسلة الإمداد ومنع انتشار أدوات وتقنيات تكنولوجيا المعلومات والاتصـالات الخبيثة والخاصـيات الوظيفية الخفية الضارة.

وتضمّنت وثيقة السياسة العامة الجديدة (وثيقة المجلس الوطني للسياسات الاقتصادية والاجتماعية رقم 2020/3995)، المعنونة "الســـياســـة الوطنية في مجال الثقة والأمن في الفضـــاء الإلكتروني"، تدابير محددة من أجل تطوير نموذج للإبلاغ الدوري عن مواطن الضـــعف في جميع القطاعات بين نقاط اتصـــال مالكي ومشغلي الأصول التي تدعم الأنشطة الحيوية والهيئات الحكومية الوطنية ذات الصلة. وسيشارك في هذه العملية العديدُ من الجهات المعنية، وسيتم أخذ التجارب الدولية في الاعتبار لدى وضع هذا النموذج.

وفي إطار الاستجابة للتوصية الداعية إلى ألاّ تنفّذ الدول أو تدعم عن علم أي نشاط يلحق الضرر بنظم المعلومات الخاصـــة بأفرقة مواجهة حالات الطوارئ المفوضـــة (المعروفة أحياناً بأفرقة مواجهة الطوارئ الحاسوبية أو أفرقة الاستجابة لحوادث أمن الفضاء الإلكتروني) التابعة لدولة أخرى، وإلى ألاّ تستخدم أفرقة مواجهة الطوارئ المفوضـــة في القيام بأنشـــطة دولية خبيثة، اتّخذت كولومبيا خطوات وفقا للقانون الدولي وميثاق الأمم المتحدة، وهي تسلّم بأنّها تتحمل المسؤولية الأساسية عن تهيئة بيئة آمنة وسلمية لتكنولوجيات المعلومات والاتصالات.

كما أصـــدرت حكومة كولومبيا القرار رقم 500 والتوجيه الرئاســـي رقم 3 لشـــهر آذار/مارس 2021 من أجل وضع مبادئ توجيهية ومعايير لاستراتيجية الأمن الرقمي، واعتماد نموذج للأمن والخصوصية يكون بمثابة عنصر تمكين لسياسة الحكومة في المجال الرقمي.

وتضـــبط المادة 16 من المرســـوم رقم 2106 لســـنة 2019 قواعد تتيح تبســـيط وإلغاء وإصـــلاح الإجراءات والعمليات غير الضـــرورية للإدارة العامة، وهي تنصّ على ضـــرورة أن يكون لدى الســـلطات اســـتراتيجية أمنية رقمية لإدارة الوثائق إلكترونيا وللحفاظ على المعلومات، وذلك وفقا للمبادئ التوجيهية الصادرة عن وزارة تكنولوجيا المعلومات والاتصالات.

وتحدد وزارة تكنولوجيا المعلومات والاتصـــالات، بوصـــفها أحد عوامل التمكين لســـياســـة الحكومة الرقمية، مبادئ توجيهية لتنفيذ نموذج أمن المعلومات وخصـــوصـــيتها وإدارة مخاطر أمن المعلومات، فضـــلا عن إجراءات إدارة حوادث الأمن الرقمي، ومبادئ توجيهية ومعايير بشأن استراتيجية الأمن الرقمي.

واختارت كولومبيا اتخاذ تدابير تشـــمل إنفاذ القانون والاســـتخبارات والأدوات الدبلوماســـية من أجل وقف الهجمات الإلكترونية ومنع تدمير الممتلكات وإحداث الخسائر في الأرواح، وهي تستنفذ جميع الخيارات المتاحة للدفاع عن الشبكة قبل القيام بأي عملية في الفضاء الإلكتروني.

وركزت حكومة كولومبيا، لدى وضـع السياسـة الوطنية للأمن الرقمي، على ثلاثة مجالات أساسـية هي: ’1‘ بناء القدرات على إدارة المخاطر في البيئة الرقمية؛ ’2‘ وإنشـــاء مؤســـســـات تدعم الحوكمة؛ ’3‘ وتقييم أطر الأنشـطة وأفضـل الممارسـات الدولية. ومن أجل تنفيذ هذه السـياسـة، تتمثل اسـتراتيجية الحكومة فيما يلي:

- إعداد تقييم حديث وخطة من أجل التحسين المستمر لقدراتها التشغيلية والإدارية والبشرية والعلمية وللبنى التحتية التكنولوجية.

- صياغة مبادئ توجيهية لإنشاء شبكة مشاركة مدنية رقمية يمكن من خلالها لمختلف الجهات المعنية التفاعل والتعاون في التصدي للتهديدات الإلكترونية، وذلك من أجل تعزيز وتوسيع قدرات الأمن الرقمي في كولومبيا وفقا للقانون الدولي.

- تنسيق عملية وضع مبادئ توجيهية لخطط تحسين الأمن الرقمي من أجل تعزيز قدرات نظام الضمان الاجتماعي الشامل على التعامل مع المعلومات وإدارتها وتبادلها، حيث يشكل هذا النظام بنية تحتية إلكترونية بالغة الأهمية.

- وضع مبادئ توجيهية، في إطار النموذج الوطني لإدارة الحوادث، تُبيّن الظروف الخاصة لإدارة المخاطر والتصدي لحوادث الأمن الرقمي المتصلة بمعالجة معلومات نظام الضمان الاجتماعي الشامل وإدارتها وتبادلها؛ ويتعين إدراج هذه الشروط ضمن الإجراء العام لإدارة الحوادث الذي حددته لجنة الأمن الرقمي.

- تنسيق عملية توحيد الآليات التقنية والقانونية والتنظيمية وغيرها من الآليات المناسبة لجمع الأدلة الرقمية اللازمة في حالة وقوع حادث أمن إلكتروني عند التعامل مع المعلومات وإدارتها وتبادلها من النظام الفرعي الصحي التابع لنظام الضمان الاجتماعي الشامل.

- تصميم وتطوير وتقديم مشروع خطة لنشاء فريق الاستجابة لحوادث أمن الفضاء الإلكتروني، التابع لقطاع الضمان الاجتماعي الشامل.

- تصميم وتطوير وتقديم مشروع خطة إنشاء فريق الاستجابة لحوادث أمن الفضاء الإلكتروني، التابع لقطاع الاستخبارات، وذلك من أجل المساعدة في ضمان الأمن الرقمي الوطني.

- وضع مقترح لإنشاء سجل مركزي وحيد لحوادث الأمن الرقمي على المستوى الوطني، من أجل تحليل أنواع الحوادث والقيام دوريا بتقييم مدى الحاجة إلى تخصيص الاستراتيجيات والموارد على سبيل الأولوية لفائدة إدارة الحوادث. وينبغي أن يتضمن هذا السجل التقارير المنجزة عن الموضوع من مختلف الجهات المعنية، وأن يهدف إلى تبسيط إرسال المعلومات، وإنشاء وسائل آمنة للتسليم، وضمان سرية المعلومات المتبادلة بين الأطراف وحفظها واستخدامها على النحو المناسب.

وتسعى كولومبيا إلى حماية الحقوق والحريات الدستورية للمواطنين فيما يتعلق بالحصول على المعلومات واستخدامها.

واعتمدت كولومبيا التدابير التشريعية اللازمة لتجريم الأفعال التالية: ’1‘ الوصول المتعمد وغير المأذون إلى نظام حاسوبي أو إلى أي جزء منه؛ ’2‘ والإضرار المتعمد وغير المأذون بالبيانات الحاسوبية أو حذفها أو تخريبها أو تغييرها أو حجبها؛ ’3‘ والاعتراض المتعمد وغير المأذون، بالوسائل التقنية، للبيانات الحاسوبية؛ ’4‘ وإنتاج أو نشر أو نقل المواد الإباحية عن الأطفال.

وتعمل كولومبيا على وضع تعاريف واضحة للبنى التحتية الحيوية الوطنية والدولية، وهي بصدد تحديد القطاعات التي تعتبر منتجاتها أو خدماتها بنية تحتية حيوية، وتحتفظ بقائمة بالأصول الحيوية. وهي تقوم باطلاع المجتمع الدولي على تلك التعاريف كتدبير لبناء الثقة.

وتعمل كولومبيا أيضا على إنشاء شبكات لحل الأزمات تجمع بين الجهات المعنية في القطاع العام التي تطلب الدعم. وهي تخطط أيضا للتعاون مع المجتمع الدولي من أجل إنشاء شبكة من نقاط الاتصال "على الصعيدين السياسي والتقني". وفي هذا الصدد، قامت كولومبيا بما يلي:

- تصميم تدريبات وطنية ودولية على أمن الفضاء الإلكتروني من أجل اختبار قدرتها بشكل منتظم على التواصل مع الدول الأخرى والاستجابة لطلبات المساعدة والتخفيف من المخاطر (لا سيما قنوات الاتصال والبروتوكولات والإجراءات) وذلك من خلال تدريبات مشتركة على أمن الفضاء الإلكتروني.
- المشاركة في أنشطة ضمن إطار فعالية CyberEx وفعالية CyberDrills التابعتين للاتحاد الدولي للاتصالات، وفي تدريبات محاكاة الأزمات الوطنية التي يتم تنسيقها مع القيادة الإلكترونية المشتركة.
- استخدام ما هو قائم من الشبكات الوطنية من الأطراف المعنية في مجال حلّ الأزمات، والاعتماد على خبرات التخفيف من المخاطر، التي توفرها الدولة وكذلك الجهات الفاعلة من غير الدول، خلال العمليات الإلكترونية من هذا النوع، وذلك باتباع أفضل الممارسات المتعلقة بالإبلاغ عن الحوادث على الصعيدين الوطني والدولي.
- تنفيذ أنشطة مع الجمعيات – وقد ظلّ الاتحاد الكولومبي لصناعة البرمجيات وتكنولوجيا المعلومات، منذ الهجمات التي شنتها في خضم الاحتجاجات الاجتماعية في الفضاء الإلكتروني جماعات القراصنة ضد الحكومة والشركات الخاصة كليهما، يتعاون مع الحكومة باسم مجموعة من الشركات من أجل وضع حلول أمنية رقمية محددة. وفي إطار هذا التعاون، عقد الاتحاد اجتماعات مع الحكومة للنظر في المجالات التي يستطيع مساعدتها فيها، وأجرى لهذا الغرض دراسة استقصائية لأعضائه من الشركات فيما يتعلق بقدراتها في مجالي الاستخبارات والرصد.

وقد تعاونت حكومة كولومبيا مع الولايات المتحدة في التصدي للعمليات الإلكترونية الخبيثة ضد البنى التحتية الحيوية.

التدابير الطوعية في مجال بناء الثقة

وفيما يتعلق بتعزيز التعاون، بما في ذلك تعيين جهات اتصال لتبادل المعلومات عن الاستخدامات الخبيثة لتكنولوجيا المعلومات والاتصالات والمساعدة في التحقيقات، ما فتئت الشرطة الوطنية تتعاون، من خلال مركز الشرطة المعنية بالجرائم الإلكترونية التابع لمديرية التحقيقات الجنائية والمنظمة الدولية للشرطة الجنائية، مع الكيانات الأعضاء في لجنة الأمن الرقمي التابعة للحكومة الوطنية على معالجة ثلاثة عناصر من أمن الفضاء الإلكتروني هي: الوقاية وإجراء التحقيقات والتحقيق جنائي حاسوبي.

ونتيجة لذلك، تم في عامي 2020 و 2021 تنفيذ 32 عملية لمكافحة الجرائم الإلكترونية، أسفرت عن إلقاء القبض على 219 شخصا ضالعين في هذه الجرائم؛ وتم التصدي لـ 072 14 من حوادث أمن الفضاء إلكتروني من خلال خدمة CAI الافتراضية العاملة على مدار الساعة وطوال الأسبوع؛ وحظر 139 7 من المواقع الإلكترونية التي تحتوي على مواد الاعتداء الجنسي على الأطفال و 648 1 موقعا غير قانوني من مواقع القمار؛ وإصدار 454 نشرة إخبارية.

كما عززت كولومبيا التعاون النشـط من خلال تنفيذ برنامج مراكز القيادة في الفضـاء الإلكتروني، التي يتولى زمامها مركز كولومبيا لقدرات أمن الفضـــاء الإلكتروني، وذلك من أجل تعزيز قدرات هذا الأمن وقدرات الدفاع الإلكتروني في البلد.

وما فتئ مركز قدرات أمن الفضاء الإلكتروني في كولومبيا ينفذ الاستراتيجية الشاملة لأمن الفضاء الإلكتروني من أجل ضمان التنسيق الفعال بين الشرطة القضائية المركزية ووحدات التحقيق الجنائي المحلية البالغ عددها 51 وحدة، وذلك بغية توحيد تقنيات التحقيق، فضلا عن أدوات وآليات التعاون الفعال.

وكما أفاد مكتب النائب العام، فإن الجرائم الإلكترونية آخذة في الارتفاع منذ عام 2009، وهي قد سـجلت زيادة حادة في عام 2019. وشـهدت سـنة 2018 وقوع 238 22 جريمة إلكترونية، فيما شـهدت سـنة 2019 وقوع 197 24 جريمة، أي بزيادة قدرها 9 في المائة. وتعزز هذا الاتجاه في عام 2020 حيث شـــهدت الفترة من 1 كانون الثاني/يناير إلى 31 كانون الأول/ديســـمبر 2020 وقوع 346 35 جريمة إلكترونية، أي بزيادة قدرها 70 في المائة. وبذلك يكون عدد قضـــايا الجرائم الإلكترونية في البلد قد ارتفع خلال الجائحة.

وتوجد لدى مكتب المدعي العام قناة اتصـال دائمة يتبادل من خلالها المعلومات مع مركز الشرطة المعنية بالجرائم الإلكترونية، الذي هو بمثابة جهة الاتصـــال على مدار الســـاعة وطوال الأســـبوع عملا بالمادة 35 من الاتفاقية المتعلقة بالجريمة الإلكترونية.

ومن أجل تحســـين التعاون بين الكيانين، قدم مركز قدرات أمن الفضـــاء الإلكتروني في كولومبيا التابع للشـــرطة الوطنية تدريبا لأفرقة مكتب المدعي العام المســـؤولة عن مكافحة الجرائم الإلكتروني على قدرات مركز الشرطة المعنية بالجرائم الإلكترونية.

وكما لوحظ ســـابقا، تســـعى كولومبيا، من خلال وثيقة المجلس الوطني للســـياســـة الاقتصـــادية والاجتماعية رقم 2020/3995، إلى تعزيز ســـياســـة أمن الفضـــاء الإلكتروني والدفاع الإلكترونية والتعاون الدولي. وهي تأمل أيضـا في تحسين تبادل المعلومات والتعاون والتنسـيق بشـكل قوي وفعال وحسـن التوقيع بين الجهات المعنية بأمن الفضاء الإلكترونية على المستوى الوطني من خلال آليات الاستجابة للأزمات مثل مراكز القيادة الموحدة.

وفيما يتعلق بالتعاون، ســـيعطي مكتب المدعي العام الأولوية للتحقيق في الجرائم الإلكترونية وذلك وفقا للقانون الوطني والدولي، ومن أجل الاستجابة لطلبات المساعدة المقدمة من دول أخرى من أجل التحقيق في الجرائم المتصـــلة بتكنولوجيا المعلومات والاتصـــالات أو اســـتخدام تكنولوجيا المعلومات والاتصـــالات لأغراض إرهابية، أو من أجل التخفيف من أنشـطة تكنولوجيا المعلومات والاتصـالات الخبيثة الصـادرة من كولومبيا، كما هو مبين في التوجيه الاسـتراتيجي لمكتب المدعي العام للفترة 2020–2024، الذي هو بمثابة خريطة طريق يضبط بها المكتب عمله المتوخى للسنوات المقبلة بشكل شامل. وبناء عليه، سيطوّر المكتب استراتيجيةً لتعزيز وتنسيق قدرات التحقيق لدى المحققين والمدعين العامين المعنيين بهذه القضايا.

وضمن القسم المعنون "البيانات المفتوحة لمكتب المدعي العام: البحث والملفات القابلة للتنزيل" في الموقع الشـبكي لمكتب المدعي العام، يمكن الاطلاع على الإحصـاءات الشـهرية للجرائم الإلكترونية خلال الفترة الممتدة من تاريخ إصـــدار القانون رقم 1273 لعام 2009 وحتى الوقت الحاضـــر، وذلك باســـتخدام بارامترات مثل نوع الجريمة بموجب القانون الجنائي لكولومبيا، والســـنة التي تلقى فيها مكتب النائب العام

تقرير الجريمة أو السنة التي وقعت فيها الأحداث، والإقليم الذي وقعت فيها الأحداث، وحالة الإجراءات والمرحلة التي بلغتها، والجنس والفئة العمرية للضحايا أو للمشتبه فيهم. ويحتوي النموذج أيضا على معلومات تشير، بالنسبة للجرائم المبلغ عنها، إلى ما إذا كانت هناك تُهم أو إداناتٌ قد وُجّهت، أو مذكرات توقيف قد صدرت، أو ما إذا كانت القضايا قد أُغلقت لأنّ الأحداث لم تشكل جريمة أو أنّها لم تقع.

وتتولى الأفرقة الوطنية المسؤولة عن مكافحة الجرائم الإلكتروني والتابعة لمكتب المدعي العام، الموجودة في مدن البلد الرئيسية، المسؤولية عن تجهيز وتحليل وحفظ الأدلة الرقمية، والتحقيق في الجرائم الإلكترونية، بما في ذلك السرقة باستخدام الحاسوب والمواد الإباحية المتعلقة بالأطفال، التي تقع ضمن اختصاص هذه الأفرقة بسبب مكان وقوع الأحداث. والمطلوب من هذه الأفرقة، خلال هذه التحقيقات، إجراء المقابلات وعمليات التفتيش، وإصدار أوامر المنع من مغادرة البلد، وعمليات التحقق، وعمليات البحث والمصادرة والاعتقال، ومرافقة الأشخاص المقبوض عليهم إلى جلسات الاستماع بأنواعها. وهي مكلفة أيضا بمساعدة جميع المكاتب الخاضعة لولايتها القضائية في استخراج وحفظ الأدلة الرقمية من الأجهزة أو من مواقع الإنترنت ضمن جميع القضايا الجنائية التي تتطلب مثل هذه الأنشطة، بما في ذلك حالات القتل، والأفعال الجنسية مع القصر دون سن 14 عاما، والمواد الإباحية التي تنطوي على قصّر دون سن 18 عاما، وأحيانا حتى التشهير والقذف.

وتتولى مديرية الشؤون الدولية التابعة لمكتب المدعي العام النظر في جميع طلبات المساعدة القانونية، التي ينطوي معظمها على الاحتجاج بالاتفاقية المتعلقة بالجريمة الإلكترونية، وهي قد طبقت بالفعل المعايير والضوابط الموصى بها في *الدليل العملي لطلب الأدلة الإلكترونية عبر الحدود*، الذي اشترك في إعداده مكتب الأمم المتحدة المعني بالمخدرات والجريمة، والمديرية التنفيذية لمكافحة الإرهاب التابعة للأمم المتحدة، والجمعية الدولية لأعضاء النيابة العامة، وتمت ترجمته إلى الإسبانية بدعم من منظمة الدول الأمريكية.

ومن خلال مركز قدرات أمن الفضاء الإلكتروني في كولومبيا، أصبحت الشرطة الوطنية، بوصفها جهة الاتصال العاملة على مدار الساعة وطوال الأسبوع بموجب الاتفاقية المتعلقة بالجريمة الإلكترونية، واحدة من كيانات التعاون الدولي الرئيسية بما لديها جهات اتصال هامة في مجال مكافحة الجريمة الإلكترونية، من قبيل وكالة الاتحاد الأوروبي للتعاون في مجال إنفاذ القانون والمنظمة الدولية للشرطة الجنائية (الإنتربول)، وبفضل تعزيز المؤسسات المشاركة في تنفيذ الاتفاقية.

ومن خلال جهة الاتصال العاملة على مدار الساعة وطوال الأسبوع، تعتزم كولومبيا التعجيل بتجهيز طلبات تبادل المساعدة القضائية وذلك بالتعاون مع 65 من الدول الأطراف و 13 من الجهات المراقبة في الاتفاقية المتعلقة بالجريمة الإلكترونية.

وتتعلق المعلومات الواردة أدناه بالتوصية التالية: في ضوء وتيرة تطور تكنولوجيا المعلومات والاتصالات وحجم المخاطر التي تحملها، هناك حاجة تستدعي تعزيز التوصل إلى تفاهمات مشتركة وتكثيف التعاون، وفي هذا الصدد ينبغي بذل جهود لإجراء حوار بين المؤسسات على أساس منتظم تشرف عليه الأمم المتحدة ويتسع لعدد كبير من المشاركين، وأيضا لإجراء حوار منتظم من خلال المحافل الثنائية والإقليمية والمتعددة الأطراف، والمنظمات الدولية الأخرى.

إنّ كولومبيا مستمرة في المشاركة بنشاط في الحوارات المتعددة الأطراف تحت رعاية الأمم المتحدة وغيرها من المحافل الدولية، ولا سيما بشأن المسائل المتصلة بسلوك الدول المسؤول في الفضاء الإلكتروني والتطورات في ميدان المعلومات والاتصالات ضمن سياق الأمن الدولي.

وفي ظل البيئة الحالية التي تتسم بترابط عالمي غير مسبوق، تقيم الدول علاقات ترابط معقدة وتشترك في مشاكل مشتركة لا تستطيع حلّها بمفردها. ولذلك، يجب عليها أن تختار التعاون الدولي على أمن الفضاء الإلكتروني، لأن نشر واستخدام تكنولوجيات ووسائط المعلومات يؤثران على مصالح المجتمع الدولي بأسره. لذلك، من مصلحة كل الدول تشجيع استخدام تكنولوجيا المعلومات والاتصالات في الأغراض السلمية ومنع نشوب النزاعات بسبب استخدامها. ومن ثم، لا بُدّ للدول من:

- تقديم المساعدة لبناء القدرات في مجال تكنولوجيا المعلومات والاتصالات، وهو أمر أساسي للأمن الدولي، عن طريق تحسين قدرة الدول على التعاون والعمل الجماعي وتشجيع استخدام تكنولوجيا المعلومات والاتصالات في الأغراض السلمية، مع الاستفادة من التعاون الدولي الذي يقوده فريق الاستجابة لحوادث أمن الفضاء الإلكتروني.
- إنشاء آليات لمشاركة القطاع الخاص والأوساط الأكاديمية ومنظمات المجتمع المدني من أجل الإسهام في مجال المعلومات والاتصالات السلكية واللاسلكية ضمن سياق الأمن الدولي، الذي تشارك فيه كل الدول.

وفيما يتعلق بتنفيذ تدابير التعاون الطوعي في المنظمات الثنائية والمتعددة الأطراف والإقليمية، ومن أجل ضمان التعاون الطوعي الفعال وزيادة الثّقة دعما للجهود المشتركة التي تبذلها الدول من أجل التصدي للتهديدات الوطنية والدولية لتكنولوجيا المعلومات والاتصالات، قامت حكومة كولومبيا، عن طريق وزارة تكنولوجيا المعلومات والاتصالات، بما يلي:

- المشاركة في برامج إقليمية مثل المائدة المستديرة للأمن الفضاء الإلكترونية التي نظمتها شبكة قادة الحكومات الإلكترونية في أمريكا اللاتينية ومنطقة البحر الكاريبي، ومواصلة التعاون مع منظمة الدول الأمريكية.
- العمل منذ عام 2017 على مشروع المسار الوظيفي لأمن الفضاء الإلكتروني، الذي ينسقه برنامج أمن الفضاء الإلكتروني التابع لمنظمة الدول الأمريكية وتموله مؤسسة سيتي، والذي يهدف إلى توفير التدريب وتعزيز التطوير المهني في مجال الأمن أمن الفضاء الإلكتروني لفائدة الشباب الذين تتراوح أعمارهم بين 18 و 25 عاما والمنحدرين من الأسر ذات الدخل المنخفض في البرازيل وبيرو والجمهورية الدومينيكية وكوستاريكا وكولومبيا.
- تطوير مبادرة "الفتيات قراصنة الحواسيب"، التي تهدف إلى تعزيز وخلق مساحات تعليمية وفرص عمل للنساء من خلال تحسين معرفتهن بالمسائل المتعلقة بالأمن الإلكتروني. وقدمت وزارة تكنولوجيا المعلومات والاتصالات من خلال هذه المبادرة التدريب لأكثر من 350 خبيرة في مجال الأمن، سيشكلن جزءا من فريق مؤهل من خبيرات المستوى الأول في مجال الأمن الرقمي في كولومبيا، وسيصبحن في المستقبل أعضاء في مجموعة "الفتيات قراصنة الحواسيب في كولومبيا"، بما يجعل البلد رائدا في مثل هذه المبادرات على المستوى الإقليمي.

- استضافة حوارات برعاية مجالس الابتكار في مجال أمن الفضاء الإلكتروني، تم خلالها عقد مناسبتين بقيادة خبراء إقليميين ومتخصصين في التفكير التصميمي، وبمشاركة مسؤولين تنفيذيين كبار من القطاعين العام والخاص والنقابات والأوساط الأكاديمية، وذلك بغية تعزيز الابتكار وزيادة الوعي بين المشاركين ونشر أفضل الممارسات في مجال أمن الفضاء الإلكتروني داخل المنطقة. وقد أنشئت مجالس الابتكار هذه بموجب اتفاق بين برنامج أمن الفضاء الإلكتروني التابع لمنظمة الدول الأمريكية وشركة سيسكو، وهي تعقد اجتماعاتها بدعم من هذه المنظمة.

وفيما يتعلق بالالتزام بالعمل الجماعي من أجل جعل الإنترنت مكانا أكثر أمانا وتشجيع المساعدة التقنية المقدمة من شركات التكنولوجيا لحماية المدنيين، وبما أن الممتلكات المدنية الخاصة هي الهدف الرئيسي للهجمات، قامت حكومة كولومبيا، من خلال وزارة تكنولوجيا المعلومات والاتصالات، بتنفيذ برنامج "الثقة بتكنولوجيا المعلومات والاتصالات"، الذي يعزز تطوير المهارات الرقمية من أجل التصدي بأمان للمخاطر المرتبطة باستخدام الإنترنت وهذه التكنولوجيا، ويشجّع على استخدام الإنترنت وملكيتها باعتبارهما فرصة لخلق بصمة رقمية إيجابية. ويستهدف هذا البرنامج الإناث والذكور الذين تتراوح أعمارهم بين 6 سنوات و 28 سنة، وهو يقدم استراتيجيات متباينة، ضمن جلسات افتراضية وحضورية، لمساعدة المستفيدين منه على تطوير مهارات تحديد المخاطر وتعزيز التعايش والفاعلية الرقميين واستخدام الأدوات التكنولوجية لنصرة القضايا الإيجابية المشتركة على شبكة الإنترنت.

وبالإضافة إلى ذلك، تقدم حكومة كولومبيا، من خلال وزارة تكنولوجيا المعلومات والاتصالات، تدريبا متخصصا في مجال أمن المعلومات للكيانات العامة التي تطلب مساعدة فريق الاستجابة لحوادث أمن الفضاء الإلكتروني، وهي تقوم بتوسيع نطاق بحوث أمن الفضاء الإلكتروني وبتعزيز القدرات التشغيلية والإدارية والبشرية والعلمية وتعزيز البنى التحتية المادية والتكنولوجية. وقامت كولومبيا بما يلي على سبيل المثال:

- وضع دليل يتضمن المشورة والمساعدة على تنفيذ النظام الشامل لأمن المعلومات والخصوصية للكيانات، وهو دليل يرتكز على سياسة الحكومة الرقمية، ويستند إلى ما يلي: '1' نموذج أمن المعلومات والخصوصية؛ و '2' نموذج المخاطر الأمنية الرقمية – دليل إدارة المخاطر وتصميم الضوابط للكيانات العامة التابعة إدارة الشؤون الإدارية بالخدمة المدنية.

- وضع استراتيجية لتولي زمام سياسة الأمن الرقمي، تم تحديدها من خلال حلقات العمل ومناقشات التوعية وتطوير الأدوات التفاعلية والدورات التدريبية.

- تقديم الفريق الحكومي المعني بالتصدي لحوادث أمن الفضاء الإلكتروني خدمات أساسية استباقية وتفاعلية في مجال إدارة الأمن لفائدة جميع كيانات الدولة عن طريق إصدار تنبيهات وتحذيرات بشأن التهديدات ومواطن الضعف، وإجراء فحص للحوادث وتحليلها ومواجهتها وتنسيقها، وتحسين الوعي الأمني، وتعزيز ثقافة الأمن الرقمي لدى كل العاملين والمسؤولين في مجال الأمن الرقمي.

- تقديم الفريق الحكومي المعني بالتصدي لحوادث أمن الفضاء الإلكتروني، من خلال حافظة خدماته، المساعدة والدعم إلى كيانات الدولة حتى يتم تحسين العمليات الأمنية للبنية التحتية التكنولوجية، وإدارة حوادث أمن الفضاء الإلكتروني، والتوعية بالأمن الرقمي. ويتألف الفريق الحكومي من مجموعة من الفنيين المتخصصين الذين ينفذون ويطورون أنشطة لمنع حوادث أمن الفضاء الإلكتروني وإدارتها.

التعاون والمساعدة على الصعيد الدولي في مجالي أمن تكنولوجيا المعلومات والاتصالات وبناء القدرات على توفير هذا الأمن

فيما يتعلق بتيسير التعاون عبر الحدود على تلافي مواطن ضعف البنية التحتية الحيوية، التي تتجاوز الحدود الوطنية، لاحظ مكتب المدعي العام أيضا أن من المهم تطوير القدرات في المنطقة لمكافحة الجريمة الإلكترونية. ولذلك، سعت كولومبيا إلى إقامة شراكات استراتيجية وشاركت في مختلف المحافل؛ وأصبحت على سبيل المثال دولة طرفا في الاتفاقية المتعلقة بالجريمة الإلكترونية، وشاركت في أفرقة عاملة مختلفة تابعة للأمم المتحدة، ووقعت مذكرات تفاهم مع مختلف الدول الأخرى لمكافحة الجريمة الإلكترونية.

وبالإضافة إلى ذلك، وفي إطار جهودها للتعاون والتنسيق، تعمل كولومبيا جنبا إلى جنب مع شبكة أفرقة الاستجابة لحوادث أمن الفضاء الإلكتروني في الأمريكتين، التي هي بمثابة منبر لتبادل المعلومات المتصلة بالتهديدات وللتعاون بين أفرقة الاستجابة للحوادث في المنطقة.

وتشارك كولومبيا أيضا في مشاريع دولية لتبادل المعلومات، منها النشرات والإنذارات المبكرة الموجهة للكيانات الحكومية والإشرافية ذات الصلة بالقطاع المالي داخل بلدان أخرى في المنطقة (مثل مجلس أمريكا الوسطى للمراقبين الماليين للمصارف وشركات التأمين والمؤسسات المالية الأخرى وتحالف المحيط الهادئ).

وقد شجع مكتب المدعي العام على توقيع عدد من مذكرات التفاهم مع دول أخرى لمكافحة الجرائم الإلكترونية والجرائم ذات الصلة.

وفيما يتعلق بمواصلة العمل ضمن مجال بناء القدرات، كالقدرات في مجال علم الأدلة الجنائية أو القدرات على اتخاذ تدابير تعاونية للحيلولة دون استخدام المجرمين أو الارهابيين لتكنولوجيات المعلومات والاتصالات، سار نسق التقدم في الجهود الرامية إلى الارتقاء بالتكنولوجيا والقدرات بوتيرة أقل سرعة نظرا لارتفاع تكلفة الترخيص والمعدات والتدريب.

وفيما يتعلق بالتوصية الداعية إلى أن تعمد الدول، من أجل بناء القدرات الأمنية في مجال تكنولوجيا المعلومات والاتصالات، إلى النظر في بلورة مبادرات للتعاون الثنائي والمتعدد الأطراف تستند إلى علاقات الشراكة القائمة من أجل بناء القدرات الأمنية لتكنولوجيا المعلومات والاتصالات، ومن أجل المساعدة على تحسين بيئة تقديم المساعدة المتبادلة الفعالة في التصدي لحوادث تكنولوجيا المعلومات والاتصالات بين الدول والمنظمات الدولية المختصة، بما فيها الأمم المتحدة ووكالاتها، فضلا عن القطاع الخاص، والأوساط الأكاديمية، ومنظمات المجتمع المدني، تولت حكومة كولومبيا، من خلال وزارة تكنولوجيا المعلومات والاتصالات، رئاسة اللجنة التنفيذية لشبكة قادة الحكومات الإلكترونية في أمريكا اللاتينية ومنطقة البحر الكاريبي، التي تجمع بين السلطات الحكومية الرقمية من 34 بلدا في المنطقة لأجل معالجة مسائل أمن الفضاء الإلكتروني.

وتم اقتراح الأنشطة التالية لأجل تعزيز فهم حالة أمن الفضاء الإلكتروني، وعُرضت على موافقة الشبكة جملة من التدابير الهادفة إلى تحسين مستوى هذا الأمن داخل البلدان الأعضاء في الشبكة وفي المنطقة:

- دراسة لمصرف التنمية للبلدان الأمريكية ومنظمة الدول الأمريكية بشأن مستوى نضج أمن الفضاء الإلكتروني.
- مستوى نضج أفرقة مواجهة الطوارئ الحاسوبية وأفرقة الاستجابة لحوادث أمن الفضاء الإلكتروني SIM3.
- أرشفة أدلة أمن الفضاء الإلكتروني والإجراءات والممارسات الجيدة بشأنه.
- تنظيم فعالية بشأن أمن الفضاء الإلكتروني لفائدة صناع القرارات.
- وضع استراتيجيات إقليمية لأمن الفضاء الإلكتروني.
- تطوير ممارسات جيدة طوعية إقليمية في التعامل مع البيانات الحساسة (تحسين استخدام التوقيع الرقمي عبر الحدود وقابلية التشغيل البيني).
- دراسة حالة أفرقة الاستجابة لحوادث أمن الفضاء الإلكتروني التابعة لأعضاء الشبكة.
- تطوير أفرقة قطاعية في مجال الاستجابة لحوادث أمن الفضاء الإلكتروني والتعاون بين هذه الأفرقة في المنطقة.
- بناء القدرات في مجال أمن الفضاء الإلكتروني.
- بناء قدرات أفرقة الاستجابة لحوادث أمن الفضاء الإلكتروني.
- إنشاء منصة لتبادل المعلومات عن البرامجيات الخبيثة (أفرقة الاستجابة لحوادث أمن الفضاء الإلكتروني داخل الأمريكتين).
- تحليل الأطر الإقليمية لحماية البيانات.

وبالإضافة إلى ذلك، وبالاتفاق مع منظمة الدول الأمريكية ووزارة تكنولوجيا المعلومات والاتصالات، اتخذت حكومة كولومبيا خطوات لوضع سلسلة من المقترحات بشأن وضع نموذج لإدارة الأمن الرقمي ودليل منهجي على تحديد وإدارة المخاطر الأمنية الرقمية وذلك في إطار اعتماد كولومبيا للتكنولوجيات الناشئة لكولومبيا من خلال:

- تجميع المصادر والمراجع لكلا المنتَجيْن المقترحين.
- تحليل أفضل الممارسات لكلا المنتجين من خلال القياس والتعلم، وذلك باستخدام نماذج الحوكمة المطبقة على الأمن الرقمي.
- تحليل السياق المحلي (المؤسسات والجهات المعنية، وما إلى ذلك).
- وضع المبادئ والأهداف المقترحة لنموذج الحوكمة.
- الموافقة على الأهداف المقترحة والحصول على اقتراحات من جهات معنية عديدة بشأن نموذج الحوكمة.
- تحديد توقعات الجهات المعنية فيما يتعلق بنموذج الحوكمة.

ومن أجل الموافقة على المبادئ والأهداف المقترحة وإقرار مصـــالح الجهات المعنية فيما يتعلق بنموذج الإدارة، عقدت كولومبيا في 30 تشـــرين الأول/أكتوبر 2020 أول دورة لفريق عامل خلال الدورة الرسمية للجنة الأمن الرقمي، حضرها أكثر من 80 مشاركا يمثلون العديد من الجهات المعنية داخل منظومة أمن الفضاء الإلكتروني.

وبغية وضـــع منبر للتعاون التنفيذي ليس فقط مع الدول الأخرى بل أيضـــا مع القطاع الخاص الوطني من أجل التصـدي للحوادث والأزمات الواسـعة النطاق المتعلقة بأمن الفضـاء الإلكتروني ومعالجتها، تعمل حكومة كولومبيا، بقيادة وزارة الدفاع، على تنفيذ الأهداف التالية المبينة في خطة عمل المجلس الوطني للسياسات الاقتصادية والاجتماعية رقم 2020/3995:

(أ) تطوير الثقة الرقمية من خلال إدخال تحســـينات على الأمن الرقمي، وذلك بغية جعل كولومبيا مجتمعا شـــاملا وتنافســـيا في المســـتقبل الرقمي من خلال بناء القدرات وتحديث إطار حوكمة الأمن الرقمي.

(ب) اعتماد نماذج تؤكد التكنولوجيات الجديدة وتجعل من الضروري تنفيذ التكنولوجيا المؤسسة للنظام الوطني لإدارة حوادث أمن الفضـاء الإلكتروني، وذلك من أجل تنسـيق الجهود المؤسـسـية لإدارة هذه الحوادث في الوقت المناسب وتحديد المصدر الرسمي للإحصاءات بشأن الحوادث المبلغ عنها في البلد.

(ج) إرســاء آلية موحّدة للإبلاغ الدوري بحوادث أمن الفضــاء الإلكتروني وبمواطن الضــعف حتى يتسـنى الوقوف عليها وتقييمها وإبلاغها إلى الجهات المعنية، وجعل الحكومة الوطنية تسـترشـد بها في اتخاذ القرارات.

انطباق القانون الدولي على استخدام تكنولوجيات المعلومات والاتصالات

ترى كولومبيا أن القانون الدولي، ولا ســـيما ميثاق الأمم المتحدة والقانون الدولي لحقوق الإنســـان والقانون الدولي الإنســـاني، ينطبق على المجال "الافتراضـــي" مثل انطباقه على العالم "المادي"، على أن يكون من المفهوم أنّ القانون الدولي الإنسـاني ينطبق في حالات النزاع المسـلح إما على المجال الافتراضـي أو على العالم المادي.

والقانون الدولي، وبخاصـة ميثاق الأمم المتحدة، ينطبق على صـون السـلام والاسـتقرار وتهيئة بيئة مفتوحة وآمنة ومسـتقرة وميسـرة وسـلمية لتكنولوجيا المعلومات والاتصـالات، وهو أسـاسـي لتحقيق ذلك. ومن ثم، فإنّ مبدأ المســاواة في الســيادة، يشــكل من بين مبادئ أخرى من مبادئ القانون الدولي كســيادة الدول وتســوية المنازعات بالطرق الســلمية وعدم التدخل في الشــؤون الداخلية للدول الأخرى، الأســاس للمزيد من الأمن في استخدام الدول لتكنولوجيات المعلومات والاتصالات.

المفاهيم

من أجل اكتســاب فهم أعمق للمفاهيم المتصــلة بالســلام والأمن الدوليين في اســتخدام تكنولوجيا المعلومات والاتصـالات على المسـتويات القانونية والتقنية والسـياسـية، ونظرا للطابع المحدد والحديث لتطبيقات هذه التكنولوجيا، تعتقد كولومبيا أنه ينبغي مواصـــلة مناقشـــة هذه المفاهيم في المحافل المتعددة الأطراف،

وفقا لاستنتاجات الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، الواردة في تقريره النهائي المعتمد بتوافق الآراء في شهر آذار/مارس 2021.

ومن أجل اكتساب فهم أعمق لمسألة تطبيق القانون الدولي في الفضاء الإلكتروني، ينبغي استحداث أدوات لبناء القدرات من أجل مساعدة الدول على تطوير مفردات مشتركة ومعرفة أشمل حتى تتمكن من تعديل الإطار القانوني الدولي ليصبح متناسبا مع تحديات الفضاء الإلكتروني، وتتوصل إلى توافق في الآراء بشأن كيفية تطبيق القانون الدولي في المجال الافتراضي.

ومن المهمّ مواصلة تنفيذ توصيات فريق الخبراء الحكوميين والفريق العامل المفتوح العضوية.

ومن المهم أيضا إنشاء آلية عالمية للحوار المؤسسي المنتظم تحت رعاية الأمم المتحدة من أجل إحراز تقدم بهذا الشأن، ومواصلة العمل الجاري على الصعيد الإقليمي وتعزيزه.

ولذلك، تدعم كولومبيا وتشترك في استضافة المبادرة الرامية إلى وضع برنامج عمل بشأن الاستخدام المسؤول لوسائل تكنولوجيا المعلومات والاتصالات ضمن سياق الأمن الدولي، يكون بمثابة آلية دولية دائمة وشاملة وتوافقية وعملية المنحى هدفها تعزيز السلوك المسؤول في استخدام تكنولوجيا المعلومات والاتصالات ضمن سياق الأمن الدولي.

الدانمرك

[الأصل: بالإنكليزية]
[28 أيار/مايو 2021]

في الدانمارك، كما هو الحال في أنحاء كثيرة من العالم، الحلول الرقمية هي جزء من الحياة اليومية وتساعد على دفع النمو الاقتصادي. ومن الأهمية بمكان بالنسبة للدانمرك، بوصفها أحد أكثر البلدان استخداما للتكنولوجيا الرقمية في العالم، أن تنهض بفضاء إلكتروني عالمي مفتوح وحر ومستقر وسلمي وآمن، تُطبّق فيه حقوق الإنسان والحريات الأساسية، فضلا عن سيادة القانون، تطبيقا كاملا.

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

اتخذت الدانمرك خطوات عديدة لتعزيز أمن المعلومات وتشجيع التعاون الدولي في مجال الفضاء الإلكتروني.

ويُخصِّص اتفاق الدفاع للفترة 2018-2023 مبلغا قدره 1,4 بليون كرونة دانمركية لتعزيز أمن الفضاء الإلكتروني والدفاع الإلكتروني، ما يعزز بالتالي قدرة الدانمرك على الصمود. وتتخذ الاستراتيجية الدنماركية الوطنية لأمن الفضاء الإلكتروني والمعلومات للفترة 2018-2021 خطوات إضافية لتعزيز أمن الفضاء الإلكتروني والمعلومات وضمان بذل جهود منهجية ومنسقة. ومن خلال 25 مبادرة و 6 استراتيجيات موجهة تتناول ما يعرف حتى الآن بأنه قطاعات حيوية (الطاقة، والمالية، والنقل، والرعاية الصحية، والاتصالات السلكية واللاسلكية، والملاحة البحرية)، عززت الدانمرك القدرة التكنولوجية على الصمود لبنيتها التحتية الرقمية، وحسنَّت معارف ومهارات المواطنين والشركات والسلطات، وعززت التنسيق والتعاون فيما يتعلق بأمن الفضاء الإلكتروني.

وفي إطار الاستراتيجية الوطنية لأمن الفضاء الإلكتروني والمعلومات للفترة 2018–2021، أنشئت وحدات مخصَّصة لأمن الفضاء الإلكتروني وأمن المعلومات في القطاعات الستة الحيوية المذكورة أعلاه. وعلاوة على ذلك، أنشأت الاستراتيجية الوطنية منتدى للوحدات القطاعية المخصصة ومركز الأمن الإلكتروني، مع التركيز على تبادل خبراتها في العمل في مجال أمن الفضاء الإلكتروني والمعلومات. وتشارك في المنتدى أيضا وكالة الرقمنة وجهاز الأمن والمخابرات الدانمركي.

وسعيا للحصول على العدد الكافي من الموظفين المهرة لكشف الهجمات الإلكترونية ضد الدانمرك والتصدي لها، ولا سيما فيما يتعلق بالبنى التحتية الحيوية، قام مركز الأمن الإلكتروني، علاوة على ذلك، بتأسيس وتشغيل أكاديميته الخاصة بالتعلم الإلكتروني المكثف. وإلى جانب الأكاديمية، يدعم مركز الأمن الإلكتروني أيضاً التعليم والبحوث في مجال أمن الفضاء الإلكتروني.

وبالإضافة إلى هذه الجهود، قامت وكالة الرقمنة بتطوير وتنفيذ العديد من الدورات والمواد التعليمية والأنشطة المتعلقة بأمن الفضاء الإلكتروني والمعلومات التي تستهدف مستوى الرؤساء التنفيذيين والأوساط المتخصصة في الفضاء الإلكتروني وكذلك الموظفين الحكوميين.

وفي إطار الاستراتيجية الوطنية لأمن الفضاء الإلكتروني والمعلومات للفترة 2018–2021، طورت وكالة الرقمنة الموقع الإلكتروني sikkerdigital.dk، الذي يقدم إرشادات ومقالات وأدوات تعليمية للمواطنين حول أمن الفضاء الإلكتروني والمعلومات والمعارف بشأن التهديدات المختلفة. وبالإضافة إلى هذا الموقع الإلكتروني، تدير وكالة الرقمنة حملات وطنية بشأن السلوك الرقمي الآمن بالتعاون مع البلديات والمناطق.

ولدى الدانمرك أيضا مجلس مشترك بين القطاعين العام والخاص للأمن الإلكتروني أنشئ لتقديم المشورة للحكومة بشأن كيفية تعزيز أمن الفضاء الإلكتروني وتحسين تبادل المعارف بين السلطات والشركات والباحثين. ومن خلال الاستراتيجية الدانمركية لأمن الفضاء الإلكتروني والمعلومات للفترة 2018–2021، عززت الدانمرك أيضاً أنشطتها الدولية في مجال الفضاء الإلكتروني من خلال إيفاد ملحقين معنيين بهذا المجال إلى بروكسل؛ وتعيين منسق دولي معني بالفضاء الإلكتروني في وزارة الخارجية؛ وتعيين مستشار لأمن الفضاء الإلكتروني لدى مكتب سفير الدانمرك للتكنولوجيا في وادي السيليكون (سيليكون فالي)؛ والانضمام إلى مركز الامتياز التعاوني للدفاع الإلكتروني في تالين التابع لمنظمة حلف شمال الأطلسي. وهذا ما أتاح للدانمرك زيادة مشاركتها في المنتديات الإلكترونية المتعددة الجنسيات، من قبيل الأمم المتحدة، والاتحاد الأوروبي، ومنظمة حلف شمال الأطلسي، ومنظمة الأمن والتعاون في أوروبا.

وتعمل حكومة الدانمرك حاليا على إعداد استراتيجية وطنية جديدة لأمن الفضاء الإلكتروني والمعلومات للفترة 2022–2024. وستعتمد الاستراتيجية على الجهود الحالية وتوسعها من خلال زيادة تعزيز أمن الفضاء الإلكتروني والمعلومات عن طريق مبادرات تستهدف القطاعين العام والخاص والمواطنين الدانمركيين.

وفي الوقت نفسه، تواصل الدنمارك مشاركتها في مواجهة التهديدات الهجينة مثل الهجمات الإلكترونية والتأثير على العمليات من خلال التعاون مع شركائها وحلفائها في حلف شمال الأطلسي والاتحاد الأوروبي. ولقد أدت الزيادة في الهجمات والعمليات خلال جائحة مرض فيروس كورونا (كوفيد–19) إلى بذل جهود دبلوماسية متواصلة داخل الأمم المتحدة والاتحاد الأوروبي وحلف شمال الأطلسي ومنظمة الأمن والتعاون في أوروبا، من أجل تعزيز فضاء إلكتروني حر ومفتوح ومستقر وسلمي وآمن باستمرار. وعلاوة على

ذلك، الدانمرك عضـــو نشـــط في الفريق التعاوني المعني بأمن المعلومات الشـــبكية وفي شـــبكة أفرقة مواجهة الحوادث الأمنية الحاسوبية، كما أنها عضو في مجلس إدارة وكالة الاتحاد الأوروبي لأمن الفضاء الإلكتروني.

وتشدد الدانمرك على أن الفضاء الإلكتروني، كما أوضح المجتمع الدولي، راسخ الجذور في القانون الدولي القائم، كما يشـــهد على ذلك التقريران اللذان أعدتهما أفرقة الخبراء الحكوميين بتوافق الآراء لعامي 2013 و 2015. وينطبق القانون الدولي القائم، بما في ذلك ميثاق الأمم المتحدة في مجمله، والقانون الدولي الإنساني والقانون الدولي لحقوق الإنسان، على سلوك الدول في الفضاء الإلكتروني، ويعتبر أساسيا في صـون السـلام والاسـتقرار والنهوض ببيئة لتكنولوجيا المعلومات والاتصـالات منفتحة ومأمونة ومسـتقرة وسـلمية ويمكن الوصـول إليها. وتشـدد الدانمرك كذلك على أهمية المعايير الطوعية الـــ 11 غير الملزمة المتعلقة بســـلوك الدول المســـؤول، الواردة في تقارير فريق الخبراء الحكوميين لعام 2015، باعتبارها مكملة للقانون الدولي القائم ومنبثقة عنه.

وعلى الرغم من الجهود الوطنية والدولية، لا تزال قدرة الجهات الفاعلة من الدول وغير الدول على القيام بأنشـطة إلكترونية خبيثة ورغبتها في ذلك آخذة في الازدياد. وينبغي أن يكون ذلك موضـع اهتمام على الصـعيد العالمي. وقد تشـكل الأنشـطة الخبيثة في الفضـاء الإلكتروني أفعالا غير مشـروعة بموجب القانون الدولي، فضـلا عن أنها تؤدي إلى زعزعة الاستقرار والمخاطرة بمفاقمته. ولا تزال الدانمرك مصممة على منع الأنشطة الخبيثة وردعها والتصدي لها، والسعي إلى تعزيز التعاون الدولي في هذا الصدد. وتنضم الدانمرك إلى الاتحاد الأوروبي في دعوة المجتمع الدولي إلى تعزيز التعاون الدولي من أجل إنشـــاء فضـــاء إلكتروني عالمي ومفتوح ومستقر وسلمي وآمن تُطبَّق فيه حقوق الإنسان والحريات الأساسية وسيادة القانون تطبيقا كاملا.

مضمون المفاهيم المشار إليها في تقارير فريق الخبراء الحكوميين

التهديدات القائمة والناشئة

تدرك الدانمرك أن الفضـــاء الإلكتروني يتيح فرصـــا هائلة لزيادة رفاه مواطنينا، وتعزيز نموهم الاقتصادي المستدام، وتحسين نوعية حياتهم. ومع ذلك، فإن اعتمادنا على الحلول الرقمية يطرح أيضاً بعض التحديات ويتسبب بمواطن ضعف.

ويساور الدانمرك القلق إزاء تزايد الأنشطة الخبيثة في الفضاء الإلكتروني التي تقوم بها جهات من الدول ومن غير الدول، وزيادة الســـرقة الممكَّنة بالفضـــاء الإلكتروني للملكية الفكرية. وتهدد هذه الأعمال استقرار المجتمع الدولي ونموه الاقتصادي.

ولم يحدث من قبل أن كانت الحاجة إلى فضـــاء إلكتروني عالمي وحر ومفتوح وآمن ومســـتقر وســـلمي أوضـــح مما عليه خلال جائحة مرض فيروس كورونا (كوفيد-19). وتتيح تكنولوجيات المعلومات والاتصالات التواصل والتعاون وتبادل المعارف التي يحتاجها العالم من أجل مكافحة الجائحة.

ومع ذلك، شـهدنا خلال أزمة كوفيد-19 الحالية أن جهات فاعلة خبيثة سـتسـتغل أي فرصـة، حتى وإن كانت جائحة عالمية. ويشمل ذلك التدخل في البنى التحتية الحيوية، بما في ذلك المستشفيات الضرورية لمكافحة الجائحة والسرقة الممكَّنة بالفضاء الإلكتروني للملكية الفكرية. وأي محاولة لإعاقة قدرة البنى التحتية الحيوية غير مقبولة ويمكن أن تعرض حياة الناس للخطر. ومما يثير قلق الدانمرك بوجه خاص الزيادة التي سُجِّلت مؤخرا في الأنشطة التي تؤثر على أمن وسلامة منتجات وخدمات تكنولوجيا المعلومات والاتصالات،

التي قد تكون لها آثار عامة. وهذا أمر مرفوض ويجب على جميع الدول أن تدينه بشدة. وعلاوة على ذلك، يجب على الدول أن تبذل العناية الواجبة وأن تتخذ إجراءات سريعة وحازمة ضد الأنشطة الخبيثة باستخدام تكنولوجيا المعلومات والاتصالات التي تنطلق من أراضيها.

وبالإضافة إلى ذلك، وكما أُقِرَّ في التقارير السابقة لفريق الخبراء الحكوميين والفريق العامل المفتوح العضوية، ونظرا 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 محايدا من الناحية التكنولوجية. وهذا يتسق مع مفهوم الأمم المتحدة واعترافها 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 إقامة نظام متعدد الأطراف يستند إلى النظام الدولي القائم على القواعد للتعامل مع التهديدات القائمة والمحتملة الناشئة عن استخدام تكنولوجيات المعلومات والاتصالات لأغراض خبيثة.

ولقد أوضح المجتمع الدولي أن الفضاء الإلكتروني راسخ الجذور في القانون الدولي القائم، كما يشهد على ذلك التقريران اللذان أعدتهما أفرقة الخبراء الحكوميين بتوافق الآراء لعامي 2013 و 2015. وتشدد الدانمرك على أن القانون الدولي القائم، بما في ذلك ميثاق الأمم المتحدة في مجمله، والقانون الدولي الإنساني والقانون الدولي لحقوق الإنسان، ينطبق على سلوك الدول في الفضاء الإلكتروني. وتعرب الدانمرك عن ارتياحها لأن الجمعية العامة اختتمت ذلك بتوافق الآراء في وقت سابق من هذا العام وذلك بتأييد التقرير النهائي للفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي. ويتعين الآن على جميع الدول الأعضاء أن تفي بهذا الالتزام.

فالسيادة وعدم التدخل وحظر استخدام القوة هي مبادئ أساسية في القانون الدولي، وانتهاك الدول لها يشكل فعلا غير مشروع دوليا، يمكن للدول أن تتخذ تدابير مضادة له وأن تلتمس التعويض بموجب قواعد مسؤولية الدول. ولا يزال هناك مجال لتعزيز الفهم المشترك والتفسير الموحَّد لهذه المبادئ الأساسية، وتدعم الدانمرك عمل فريق الخبراء الحكوميين والفريق العامل المفتوح العضوية، وغيرها من المبادرات الدولية والإقليمية، مثل برنامج عمل جديد للارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني، في السعي إلى تحقيق هذه النتيجة.

ومن المهم ألا تستخدم الدول مبدأ السيادة لتقييد 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 على السواء بأن تمتنع، على التوالي، عن القيام بأعمال تنتهك حقوق الإنسان، وبأنه يتوجب عليها كفالة 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. وتنعكس هذه المسألة أيضاً في *العقيدة الوطنية المشتركة المتعلقة بالعمليات العسكرية في الفضاء الإلكتروني لعام 2019*، حيث يقع على عاتق القادة العسكريين إدراج اعتبارات 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، من خلال وضع حدود واضحة لشرعيته في أوقات النزاع المسلح. وتود الدانمرك أن تنضم إلى الاتحاد الأوروبي في التأكيد على أن القانون الدولي ليس عاملا مساعدا 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 إطارا للسلوك المسؤول في الفضاء الإلكتروني. وتدعو الدانمرك جميع الدول إلى التقيد بهذا الإطار وتنفيذ التوصيات المنبثقة عنه.

وبما أن هناك بالفعل إطارا قانونيا دوليا يتناول مسائل الفضاء الإلكتروني، فإن الدانمرك لا تدعو إلى وضع صكوك قانونية دولية جديدة لمسائل الفضاء الإلكتروني ولا ترى ضرورة لذلك. ومع ذلك، هناك مجال لتعزيز الفهم المشترك لكيفية انطباق القانون الدولي القائم على مسائل الفضاء الإلكتروني. ومن المأمول أن يسهم عمل وتوصيات فريق الخبراء الحكوميين الحالي والفريق العامل المفتوح العضوية الجديد في تقديم الإيضاحات، وبالتالي تيسير امتثال الدول وكذلك تعزيز إمكانية التنبؤ والتقليل من خطر التصعيد.

معايير سلوك الدول المسؤول وقواعده ومبادئه

تنضم الدانمرك إلى الاتحاد الأوروبي وزميلاتها من الدول الأعضاء في تشجيع جميع الدول على البناء على العمل الذي أقرته الجمعية العامة مرارا، ولا سيما في القرار 237/70، والنهوض به، وعلى مواصلة تنفيذ هذه المعايير وتدابير بناء الثقة المتفق عليها، التي تؤدي دورا أساسيا في منع نشوب النزاعات.

ونظرا لأن المعايير والقواعد والمبادئ المتعلقة بسلوك الدول المسؤول التي وردت في التقارير المتعاقبة لفريق الخبراء الحكوميين للأعوام 2010 و 2013 و 2015 تشكل استكمالا للقانون الدولي القائم وتنبثق عنه فإنها تتسم بقيمة فائقة. وستواصل الدانمرك الاسترشاد بالقانون الدولي، وكذلك من خلال التقيد بهذه المعايير والقواعد والمبادئ الطوعية. وينبغي مواصلة تنفيذ هذه المعايير من خلال زيادة التعاون والشفافية بشأن أفضل الممارسات.

جمهورية مولدوفا

[الأصل: بالإنكليزية]
[24 أيار/مايو 2021]

أصبحت تكنولوجيات المعلومات والموارد الإعلامية ونظم الاتصالات الإلكترونية جزءا لا غنى عنه من جميع مجالات نشاط الفرد والمجتمع والدولة. وتسهم تكنولوجيات المعلومات في التحولات الأساسية للنظام الاجتماعي، وهي بمثابة مولد لمجتمع معلوماتي موحد على المستويات الوطنية والإقليمية والدولية. ولذلك، تجاوزت تكنولوجيات المعلومات الإطار القانوني لحدود الدول أو جماعات الدول.

وإلى جانب الفوائد التي لا جدال فيها للتكنولوجيات الحديثة، فإن حيز المعلومات عرضة لعدة تهديدات أمنية. وبالتالي، فإنه يسهل المنافسة غير الشريفة، والتجسس، وتضليل الجماهير، والدعاية، والإرهاب والجريمة المنظمة، ونشر أشكال الكراهية والتحريض على العنف، ولا سيما على أساس معايير نوع

الجنس والعرق والقومية والأصل الإثني واللغة والدين والانتماء السياسي وغيرها من المعايير، التي لا يزال يُقلَّل من شأنها ونادرا ما يتم علاجها أو مكافحتها.

إن زيادة مستوى أمن المعلومات وتهيئة الظروف المواتية لبعض الأنشطة التي تقوم بها جهات فاعلة في القطاعين العام والخاص، بما في ذلك بالنسبة للمستعملين العاديين لنظم المعلومات، هما الأولويتان الأساسيتان للسياسة الوطنية لضمان أمن المعلومات في دولة القانون. ويعني إنجاز هذه الإجراءات وجود إطار تنظيمي مستكمل وشامل يغطي المسائل الرئيسية في مجال أمن المعلومات. وفي هذا الصدد، اعتمدت في جمهورية مولدوفا استراتيجية أمن المعلومات وخطة الأنشطة لتنفيذها. ولذلك، فإن الغرض من الاستراتيجية هو ضمان حماية الحقوق والحريات الأساسية والديمقراطية وسيادة القانون في الحيز المعلوماتي.

ويسهم تصنيف المخاطر والتهديدات ومواطن الضعف، فضلا عن تنظيم الأنشطة التي تكفل أمن المعلومات، في زيادة مستوى الثقة في الفضاء الإلكتروني، وهو ما يتجلى في استراتيجية أمن المعلومات في جمهورية مولدوفا.

وتهدف الاستراتيجية إلى ربط الميادين ذات الأولوية قانونا ودمجها منهجيا بالمسؤوليات والاختصاصات لضمان أمن المعلومات على الصعيد الوطني استنادا إلى صمود النظم الإلكترونية والتعددية المتعددة الوسائط والتقارب المؤسسي في المجال الأمني بهدف حماية سيادة جمهورية مولدوفا واستقلالها وسلامتها الإقليمية.

ومن ثم، فإن هذه الاستراتيجية توفر آليات عملية وواضحة لتحديد المخاطر التي تهدد أمن المعلومات ومكافحتها والتصدي لها، فضلا عن المواعيد النهائية لتحقيق أهداف تنفيذها.

وتتوجه الآليات والأهداف المدرجة في الاستراتيجية نحو وضع الإطار المعياري وتحديثه وتنفيذ عناصر الأداء التقني والبرامج التي ستجابه التحديات من داخل البلد وخارجه، وتدريب الموظفين وتكثيف التعاون مع الهيئات المختصة الوطنية والدولية.

وفي هذا الصدد، تنص الاستراتيجية على إنشاء نظام متكامل للاتصال والتقييم فيما يتعلق بالمخاطر التي تهدد أمن المعلومات ووضع تدابير استجابة فعالة. وينطوي ذلك على إنشاء/تعيين كيان باعتباره المركز الوطني للاستجابة لحوادث أمن الفضاء الإلكتروني يكون النقطة الوحيدة للإبلاغ عن الحوادث المتعلقة بأمن الفضاء الإلكتروني للسلطات العامة المختصة والأفراد والكيانات القانونية. ومن شأن إنشاء فريق وطني لمواجهة الطوارئ الحاسوبية أن يعزز شبكة الأفرقة في إقليم جمهورية مولدوفا ويكفل التصدي السريع للحوادث.

وبالإضافة إلى ذلك، وبالنظر إلى ضرورة الرصد المستمر وكفالة مستوى عال من أمن الفضاء الإلكتروني، تنص الاستراتيجية على تنفيذ مراجعة للبنى التحتية لتكنولوجيا المعلومات ذات الأهمية الوطنية وتنفيذ المعايير الدولية لأمن المعلومات.

وعلاوة على ذلك، توفر الاستراتيجية آليات حماية لشبكات الاتصالات الخاصة في جمهورية مولدوفا، وللاطلاع على المعلومات المقيَّد الوصول إليها. ولقد صُممت نظم الاتصال ونظم المعلومات وشبكات نقل البيانات لتخزين البيانات الهامة للدولة ومعالجتها وزيادة نقلها، مما يتطلب اتباع نهج محدد فيما يتعلق بحمايتها وتطويرها.

إن العدد المتزايد من وسائل حماية التشفير وتعقيد خوارزميات التشفير يجعلان من الضروري ضمان السيطرة على استيراد وسائل حماية المعلومات والتصديق عليها واستخدامها. ولذلك، تتطلب الاستراتيجية التصديق على وسائل حماية المعلومات التقنية والتشفيرية، وتطوير نظم رصد الاستيراد لوسائل حماية المعلومات، ومواءمة الإطار القانوني الوطني في مجال حماية المعلومات المشفرة مع الإطار القانوني الأوروبي، وإنشاء قاعدة بيانات عن الوسائل التقنية ووسائل حماية المعلومات المشفرة.

وعلاوة على ذلك، فإن حرية الوصول إلى الشبكة العالمية للإنترنت، ووجود بيانات ذات طابع إباحي ومتطرف، إلى جانب صعوبة تحديد مصدر البيانات المحمَّلة وصحتها، تجعل من الضروري وضع آليات حماية للمستخدمين، ولا سيما الأطفال، من أي شكل من أشكال إساءة المعاملة في الفضاء الإلكتروني.

وكان من الضروري إجراء تقييم لفضاء الإنترنت بهدف تحديد الكيانات و/أو الأفراد المشاركين في إنتاج ونشر محتوى إعلامي على الإنترنت له تأثير على أمن المعلومات في جمهورية مولدوفا من أجل تحديد التهديدات المرتبطة بأمن المعلومات في الفضاء الإعلامي ومواجهتها والتصدي لها.

كذلك، وبغية تطوير آليات الاتصال الاستراتيجية، وتعزيز المصالح القومية لجمهورية مولدوفا، وضمان أمن الحيز الإعلامي، تنص الاستراتيجية على إجراء دراسة شاملة تهدف إلى الكشف عن العناصر الضعيفة لعنصر وسائط الإعلام داخل نظام أمن المعلومات وتقييمها، فضلا عن إنشاء مورد إعلامي للاتصال الاستراتيجي يتضمن معلومات عن الحوادث الأمنية وعن محاولات التضليل و/أو التلاعب المكتشفة.

وعلاوة على ذلك، تجدر الإشارة إلى أن الاستراتيجية تتضمن أهدافا ضرورية للتعاون الدولي في مجال أمن المعلومات ومكافحة جرائم الفضاء الإلكتروني.

ولقد اعتمدت استراتيجية أمن المعلومات للفترة من 2019 إلى 2024، وهي تحدد عددا من الأهداف والتدابير التي يتعين تحقيقها تدريجيا، بما في ذلك بمساعدة الشركاء على الصعيد الدولي.

وعلى الرغم من أن جمهورية مولدوفا تحاول على الصعيد الوطني تنفيذ عدة تدابير لتعزيز قدراتها في مجال أمن المعلومات، فإننا نرى أن الحالة في الفضاء الإلكتروني أصبحت أكثر تعقيدا على الصعيد الدولي، حيث تقوم جهات فاعلة خبيثة من الدول بشنّ هجمات إلكترونية متطورة للتدخل في العمليات الانتخابية لبلدان أخرى، وتلحق الضرر بالبنية التحتية الحيوية وتنفذ هجمات التجسس الإلكتروني من نوع "سلسلة الإمداد"، وكلها تتعارض مع قرارات الأمم المتحدة.

وفي الوقت نفسه، تستغل الجهات الفاعلة من غير الدول في الفضاء الإلكتروني تماما الثغرات الأمنية في نظام المعلومات لأغراض إجرامية من أجل الحصول على مكاسب مالية، باستخدام أدوات "البرامجيات الخبيثة المتوفرة كخدمة".

وتتسبَّب المسائل المذكورة أعلاه في إحجام السكان عن التكنولوجيات الجديدة، وتمثل عقبة أمام التطوير الجيد لتكنولوجيات المعلومات.

سنغافورة

[الأصل: بالإنكليزية]
[24 أيار/مايو 2021]

تلتزم سنغافورة التزاما قويا بإرساء 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 جيدا لسلوك الدولة المسؤول، وتدابير قوية لبناء الثقة، وبناء منسق للقدرات. ومن المهم أن يستمرَّ إجراء المناقشات بشأن هذه القوانين والقواعد والمعايير في الأمم المتحدة، التي هي المنتدى المتعدد الأطراف العالمي الشامل الوحيد الذي تتمتع فيه جميع الدول بصوت متساوٍ.

ولقد شاركت 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 الذي أنهى أعماله مؤخرا، وأنشئ عملا بقرار الجمعية العامة 27/73. وما زلنا نلتزم بالمساهمة بصورة بناءة في عمل الأمم المتحدة لوضع وتنفيذ المعايير والقواعد المتعلقة بأمن الفضاء الإلكتروني وسنواصل المشاركة بنشاط في عمليات الأمم المتحدة المقبلة. ومن المهم، في رأينا، أن تراعي المناقشات المتعلقة بأمن الفضاء الإلكتروني في الأمم المتحدة طائفة واسعة من الآراء، لا سيما من الدول الصغيرة والبلدان النامية المعرضة بشكل خاص للآثار المترتبة على نزاعات الفضاء الإلكتروني. وتحقيقا لهذه الغاية، ينبغي أن تكون أي عملية مستقبلية للأمم المتحدة بشأن أمن الفضاء الإلكتروني مفتوحة وشاملة وتعاونية لزيادة تعزيز التعاون الدولي وإحراز تقدم في النهوض بسلوك الدول المسؤول في الفضاء الإلكتروني. وستواصل سنغافورة، بوصفها الرئيسة المشاركة لمجموعة الأصدقاء المعنية بالحوكمة الإلكترونية وأمن الفضاء الإلكتروني مع إستونيا، استخدام هذا المنبر للتوعية بتحديات الفضاء الإلكتروني، وتبادل أفضل الممارسات، وتعزيز بناء القدرات في الأمم المتحدة.

وتعتقد سنغافورة أنه يتوجب على الدول تعزيز الوعي بالمعايير الطوعية وغير الملزمة القائمة لسلوك الدول المسؤول ودعم تنفيذها. وتؤيد سنغافورة زيادة تفصيل هذه المعايير عند الحاجة. فعلى سبيل المثال، يمكن اعتبار البنى التحتية الحيوية العابرة للحدود للمعلومات، التي تعد حمايتها مسؤولية مشتركة لجميع الدول الأعضاء، فئة خاصة من هذه البنى التحتية الحيوية وينبغي إدراجها في مجموعة المعايير القائمة، لأن تهديدات تكنولوجيا المعلومات والاتصالات لهذه البنى التحتية يمكن أن تكون لها آثار مزعزعة للاستقرار إقليميا وعالميا[2].

ويمكن للمنظمات الإقليمية أن تؤدي دورا هاما. فقد أكدت رابطة أمم جنوب شرق آسيا من جديد على الحاجة إلى نظام دولي قائم على القواعد في الفضاء الإلكتروني في أول بيان لقادة الرابطة بشأن التعاون في مجال أمن الفضاء الإلكتروني صدر في نيسان/أبريل 2018. وفي أيلول/سبتمبر 2018، قرر المشاركون في المؤتمر الوزاري الثالث لرابطة أمم جنوب شرق آسيا بشأن أمن الفضاء الإلكتروني الالتزام من

(2) البنى التحتية الحيوية العابرة للحدود للمعلومات هي تلك البنى التحتية الحيوية للمعلومات التي تملكها شركات خاصة وتعمل عبر الحدود الوطنية، ولكنها لا تخضع لولاية أي دولة بمفردها.

حيث المبدأ بالمعايير الـ 11 الواردة في تقرير فريق الخبراء الحكوميين لعام 2015، إضافة إلى التركيز على بناء القدرات على الصعيد الإقليمي في إطار تنفيذ هذه المعايير. وفي تشرين الأول/أكتوبر 2019، قرر المشاركون في المؤتمر الوزاري الرابع لرابطة أمم جنوب شرق آسيا بشأن أمن الفضاء الإلكتروني إنشاء لجنة عاملة للنظر في وضع خطة عمل إقليمية طويلة الأجل من أجل ضمان التنفيذ الفعال والعملي للمعايير بما في ذلك في مجالات التعاون بين أفرقة مواجهة الطوارئ الحاسوبية، وحماية البنية التحتية الحيوية للمعلومات والمساعدة المتبادلة في مجال أمن الفضاء الإلكتروني. وكرر المشاركون في المؤتمر الوزاري الخامس لرابطة أمم جنوب شرق آسيا بشأن أمن الفضاء الإلكتروني، الذي عقد في عام 2020، التزام الرابطة بوضع خطة عمل لرسم خريطة طريق تنفيذ المعايير بوتيرة مناسبة لجميع الدول الأعضاء في الرابطة. واتفق المشاركون أيضا على الحاجة الملحة لحماية البنى التحية الحيوية للمعلومات على المستوى الوطني وعبر الحدود.

ويكتسب بناء القدرات أهمية بالغة لضمان أن تطور فرادى الدول القدرة على التنفيذ الناجح لمعايير سلوك الدول المسؤول والتزاماتها في إطار القانون الدولي. وفي إطار هذا الجهد، أنشأت سنغافورة برنامجا للرابطة معنيا بالقدرات المتعلقة بالفضاء الإلكتروني في عام 2016 لدعم بناء القدرات في بلدان الرابطة بشأن السياسات العامة الإلكترونية، فضلا عن المسائل التشغيلية والتقنية. وحتى الآن، درب البرنامج المعني بالقدرات المتعلقة بالفضاء الإلكتروني للرابطة أكثر من 600 مسؤول من الدول الأعضاء في الرابطة. وكامتداد للبرنامج، دشن مركز الامتياز المشترك بين الرابطة وسنغافورة المعني بأمن الفضاء الإلكتروني في عام 2019 بالتزام بمبلغ 30 مليون دولار لتقديم برامج سياساتية وتقنية لكبار مسؤولي الرابطة. ويعمل مركز الامتياز منذ نيسان/أبريل 2020. وعلى الرغم من القيود المفروضة على السفر بسبب جائحة كوفيد-19، واصل مركز الامتياز برامجه التدريبية على الإنترنت ونظَّم سبعة برامج افتراضية في مجال بناء القدرات في عام 2020.

واشتركت سنغافورة أيضاً في تنظيم حلقة دراسية في إطار البرنامج المشترك بينها والأمم المتحدة في مجال الفضاء الإلكتروني للتوعية بمعايير الفضاء الإلكتروني في الدول الأعضاء في الرابطة. وبالإضافة إلى ذلك، أقامت سنغافورة شراكة مع مكتب شؤون نزع السلاح لإعداد دورة تدريبية رئيسية على الإنترنت مفتوحة لجميع الدول الأعضاء في الأمم المتحدة. وتهدف الدورة إلى تشجيع فهم أكبر لاستخدام تكنولوجيات المعلومات والاتصالات والآثار المترتبة عليها بالنسبة للأمن الدولي. وما زلنا نلتزم بتقاسم تجربتنا وخبرتنا مع الدول الأعضاء في الأمم المتحدة، ولا سيما البلدان الصغيرة النامية.

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

(أ) *إقامة بنية تحتية قادرة على الصمود* – بدأت وكالة أمن الفضاء الإلكتروني في سنغافورة العمل بالخطة الرئيسية للأمن الإلكتروني للتكنولوجيا التشغيلية في عام 2019 في إطار جهودنا المستمرة لتعزيز أمن ومرونة قطاعات البنية التحتية الحيوية للمعلومات في سنغافورة في تقديم الخدمات الأساسية. وترمي الخطة الرئيسية إلى تحسين الاستجابة الشاملة لعدة قطاعات للتخفيف من التهديدات الإلكترونية في بيئة التكنولوجيا التشغيلية وتعزيز الشراكات مع القطاع الصناعي والجهات صاحبة المصلحة من خلال تحديد مبادرات رئيسية تشمل كلا من الأشخاص والعمليات والتكنولوجيا لتعزيز قدرات مالكي بنيتنا التحتية

الحيوية للمعلومات والمنظمات التي تستخدم نظم التكنولوجيا التشغيلية. وفي عام 2021، ستضع وكالة أمن الفضاء الإلكتروني برنامجا لسلسلة إمداد البنى التحتية الحيوية للمعلومات وتبدأ العمل به، تشارك فيه الجهات صاحبة المصلحة بما في ذلك الوكالات الحكومية ومالكي البنى التحتية الحيوية للمعلومات وبائعيهم. وسيوفر البرنامج العمليات الموصى بها والممارسات السليمة لجميع الجهات صاحبة المصلحة لإدارة مخاطر أمن الفضاء الإلكتروني في سلسلة الإمداد؛

(ب) *إيجاد فضاء إلكتروني أكثر أمانا* – في إطار الجهود التي نبذلها للارتقاء بأمن الفضاء الإلكتروني على الصعيد الوطني في سنغافورة، أطلقت وكالة أمن الفضاء الإلكتروني الخطة الرئيسية لفضاء إلكتروني أكثر أمانا في عام 2020 من أجل القيام بما يلي: '1' تأمين بنيتنا التحتية الرقمية الأساسية؛ '2' حماية أنشطتنا في الفضاء الإلكتروني؛ و '3' تمكين سكاننا البارعين في مجال الفضاء الإلكتروني. وتحدد الخطة الرئيسية 11 مبادرة تهدف إلى زيادة اعتماد الأمان حسب التصميم لدى المؤسسات والمنظمات، فضلا عن تعزيز الوعي بأمن الفضاء الإلكتروني والممارسات الجيدة في مجال النظافة الإلكترونية لدى المستخدمين النهائيين. ومن بين هذه المبادرات خطة وضع العلامات المتعلقة بأمن الفضاء الإلكتروني للأجهزة الذكية المتصلة بالشبكة. ولقد بدأ العمل بخطة العلامات المتعلقة بأمن الفضاء الإلكتروني في عام 2020 باعتبارها خطة طوعية لإتاحة الوقت للسوق والمطورين لفهم كيف تفيدهم هذه الخطة. وستوفر علامات أمن الفضاء الإلكتروني مؤشرا على مستوى الأمان الموجود في المنتجات. ويمكن للمستهلكين اختيار المنتجات ذات التصنيفات الأمنية الأفضل باستخدام المعلومات المتاحة على علامة أمن الفضاء الإلكتروني. وتهدف الخطة إلى تحفيز المصنعين على تطوير وتوفير المنتجات التي لها خصائص محسنة ومعترف بها فيما يتعلق بأمن الفضاء الإلكتروني.

(ج) *تهيئة بيئة حيوية لأمن الفضاء الإلكتروني* – تُسلِّم سنغافورة بأن تعزيز أمن الفضاء الإلكتروني يشمل بناء البيئة الإلكترونية وتشجيع الابتكار ضمن القطاع الصناعي ذي الصلة. وهناك أيضا حاجة متزايدة إلى تكوين مجموعة من الأفراد الموهوبين الذين يمكنهم تولي أدوار قيادية في مجال أمن الفضاء الإلكتروني في المنظمات. ولقد عملت وكالة أمن الفضاء الإلكتروني مع الوكالات الحكومية والرابطات والشركاء الصناعيين والأوساط الأكاديمية في سنغافورة على توسيع وتطوير القوة العاملة في مجال أمن الفضاء الإلكتروني. وتهدف مبادرة تشجيع المواهب في مجال أمن الفضاء الإلكتروني في سنغافورة إلى اجتذاب المواهب المتحمسة ورعايتها في مجال أمن الفضاء الإلكتروني منذ سن مبكرة ومساعدة الأوساط المتخصصة في أمن الفضاء الإلكتروني على صقل مهاراتها في هذا المجال. وتهدف المبادة إلى التواصل مع ما لا يقلُّ عن 000 20 شخص على مدى ثلاث سنوات لتعزيز قائمة المواهب في مجال أمن الفضاء الإلكتروني في سنغافورة.

سويسرا

[الأصل: بالإنكليزية]
[28 أيار/مايو 2021]

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

اعتمدت سويسرا مجموعة من التدابير على الصعد الوطني والإقليمي والعالمي ترمي إلى النهوض بفضاء إلكتروني أكثر استقرارا وانفتاحا وحرية.

وتحدد استراتيجية السياسة الخارجية السويسرية للفترة 2020-2023[3] الخطوط العريضة والأولويات، بما في ذلك مشاركة سويسرا المستمرة في مساحة رقمية مفتوحة وآمنة تستند إلى القانون الدولي وتدور حول الناس واحتياجاتهم. وتلتزم سويسرا أيضا بتعزيز مكانة جنيف كمركز رقمي عالمي رائد. وتستند الاستراتيجية الأولى للسياسة الخارجية الرقمية في سويسرا للفترة 2021-2024[4] إلى استراتيجية السياسة الخارجية وتحدد المبادئ الرئيسية الرامية إلى ضمان مساحة رقمية مفتوحة وحرة وآمنة.

وتعتمد الاستراتيجية الوطنية الثانية لحماية سويسرا من مخاطر الفضاء الإلكتروني للفترة 2018-2022 على الأهداف الاستراتيجية المبينة في الاستراتيجية الوطنية الأولى لحماية سويسرا من مخاطر الفضاء الإلكتروني لعام 2012[5]. وتعترف كلتا الاستراتيجيتين بأهمية تكنولوجيات المعلومات والاتصالات بوصفها محركات لا غنى عنها للأنشطة الاجتماعية والاقتصادية والسياسية، وتضعان الأساس لنهج شامل ومتكامل وكلي للتصدي للتهديدات القائمة على تكنولوجيا المعلومات والاتصالات. وتسعى سويسرا إلى تحسين اكتشافها المبكر للأخطار الإلكترونية والتهديدات الناشئة، وزيادة صمود بنيتها التحتية الحيوية، والحد بشكل عام من مخاطر الفضاء الإلكتروني. والأساس المنطقي الكامن وراء هذه الاستراتيجيات هو الحاجة إلى إرساء ثقافة أمن الفضاء الإلكتروني، وتقاسم المسؤولية بين مختلف مستويات الحكومة وبين القطاعين العام والخاص، فضلا عن الحاجة إلى اتباع نهج قائم على المخاطر. وتدعو هاتان الاستراتيجيتان إلى تنسيق أقوى على المستوى الحكومي، وتشجع الشراكات بين القطاعين العام والخاص وتعزيز التعاون على الساحة الدولية. وحُدِّد التعاون، سواء على الصعيد الوطني أو الدولي، بأنه أحد الأركان الأساسية للنهج السويسري في معالجة التهديدات الإلكترونية. ولقد تأسس المركز الوطني لأمن الفضاء الإلكتروني في عام 2019، وهو بمثابة نقطة اتصال للشركات والأوساط الأكاديمية وعموم الجمهور والوكالات الحكومية. كما يساعد مركز أمن الفضاء الإلكتروني، الذي يقوده المندوب الاتحادي المعني بأمن الفضاء الإلكتروني، على زيادة الوعي بأمن الفضاء الإلكتروني.

وفي أيلول/سبتمبر 2020، اعتمد المجلس الاتحادي الاستراتيجية الرقمية الجديدة لسويسرا[6]. وتحدد هذه الاستراتيجية عددا من مجالات العمل للتعاون بين الحكومة والأوساط الأكاديمية والقطاع الخاص والمجتمع المدني من أجل تشكيل التحول الرقمي لمجتمعنا بما يعود بالنفع على الجميع في سويسرا وضمان إتاحة الفرص التي يوفرها للجميع.

وفي آذار/مارس 2021، اعتمدت وزارة الدفاع الاتحادية استراتيجيتها للدفاع الإلكتروني للفترة 2021-2024[7]. وتهدف هذه الاستراتيجية إلى توقع التهديدات الإلكترونية والنشاط الخبيث والكشف المبكر

(3) متاح على الرابط التالي: https://www.eda.admin.ch/eda/en/fdfa/foreign-policy/implementing-foreign-policy/aussenpolitischestrategie.html.

(4) متاح على الرابط التالي: www.eda.admin.ch/eda/en/fdfa/fdfa/aktuell/newsuebersicht/2020/11/ digitalaussenpolitik-strategie.html.

(5) متاح على الرابط التالي: www.ncsc.admin.ch/ncsc/en/home/strategie/strategie-ncss-2018-2022.html.

(6) متاح على الموقع الشبكي التالي: www.digitaldialog.swiss/en/.

(7) متاح على الرابط التالي: www.newsd.admin.ch/newsd/message/attachments/66203.pdf.

عنها، ومنع وإسناد حوادث الفضاء الإلكتروني التي تستهدف المصالح السويسرية، وتثقيف وتدريب الموظفين المدنيين والعسكريين، فضلا عن صمود النظم الإلكترونية للبنى التحتية الحيوية.

وفيما يتعلق بحماية البنى التحتية الحيوية، تتبع سويسرا نهجا لامركزيا. وتسند الولاية المتعلقة بحماية البنى التحتية الحيوية إلى مختلف الوزارات والمكاتب الاتحادية مثل المكتب الاتحادي للحماية المدنية، والمكتب الاتحادي للإمدادات الاقتصادية الوطنية، وجهاز المخابرات الاتحادي، وبالتالي فهي لا تقتصر على وكالة واحدة.

ومنذ اعتماد الاستراتيجيات الوطنية لحماية سويسرا من مخاطر الفضاء الإلكتروني، تواصل تطوير القدرات المصممة لإسناد الأنشطة الإلكترونية الخبيثة إلى الجناة. وتحديد هوية الجناة نهج شامل يشمل تحليل الخصائص التقنية للحادث الإلكتروني، ويأخذ في الاعتبار السياق الجغرافي السياسي ويستخدم الطيف الاستخباراتي بأكمله للحصول على المعلومات ذات الصلة. وقد حدَّدت سويسرا عملية موحدة مشتركة بين الوكالات للإسناد العلني (الإسناد السياسي) لحادث إلكتروني يشكل تهديدا للأمن القومي لسويسرا. وتشكل معايير الإسناد القانوني لحادث إلكتروني وفقا للقانون الدولي جزءا من هذا التقييم.

وفي كانون الثاني/يناير 2019، أنشأت سويسرا "حرم الدفاع الإلكتروني"[8] الذي يقوم بأبحاث لتوقع ورصد التهديدات المحتملة الناجمة عن التطورات التي تحركها التكنولوجيا، ويقترح حلولا ويُدرِّب خبراء الفضاء الإلكتروني. ويجمع الحرم الجامعي خبراء من المكتب الاتحادي للمشتريات الدفاعية والصناعة ومؤسسات البحوث.

وفيما يتعلق بالتواصل والعمل مع القطاع الخاص والأوساط الأكاديمية، تشجع سويسرا مبادرات مختلفة. فعلى سبيل المثال، يستخدم جهاز المخابرات الاتحادي، منذ عام 2004، برنامجه في إطار حملة الوقاية والتوعية "Prophylax" ("الوقاية") من أجل إسداء المشورة للشركات والجامعات ومعاهد البحوث بشأن التدابير الوقائية الممكنة لتحديد أنشطة التجسس والانتشار غير المشروعة والتصدي لها.

مضمون المفاهيم المشار إليها في تقارير فريق الخبراء الحكوميين

فيما يتعلق بتقييم التهديدات، يمكن أن تتسبب الأنشطة الإلكترونية الخبيثة التي تستهدف مباشرة البنى التحتية الحيوية في أضرار جسيمة وأن يكون لها أثر سلبي على أداء الخدمات الأساسية، مثل الرعاية الصحية. وفي السنوات الأخيرة، وقعت عدة وكالات اتحادية وشركات خاصة سويسرية ضحية لعمليات إلكترونية خبيثة برعاية الدول (التجسس الإلكتروني). والهدف النهائي لهذه الأنشطة الإلكترونية الخبيثة هو عموما الحصول على مزايا اقتصادية وسياسية وعسكرية. وأثناء عام 2020، تأثرت البنى التحتية الحيوية السويسرية أساسا بالهجمات ذات الدوافع المالية. وفي المستقبل، تتوقع سويسرا زيادة في هجمات برامج الفدية التي تشنُّها عصابات إجرامية، فضلا عن العمليات الإلكترونية التي تقوم بها الدول أو ترعاها أو تتغاضى عنها. وعلاوة على ذلك، يمكن أن يكون للأنشطة الإلكترونية الخبيثة آثار غير مقصودة على سويسرا وتؤدي إلى أضرار تبعية. ومع استمرار الجهات الفاعلة المهدّدة في تطوير تقنيات وأدوات لتقويض البرامجيات المشروعة والتلاعب بها، تثير الهجمات على سلسلة الإمداد القلق بشكل خاص.

(8) انظر www.ar.admin.ch/en/armasuisse-wissenschaft-und-technologie-w-t/cyber-defence_campus.html.

وشاركت سويسرا مشاركة فاعلة وساهمت في الفريق السادس للخبراء الحكوميين (2019 إلى 2021) والفريق العامل المفتوح العضوية (2019 إلى 2021) فيما يتعلق باستقرار الفضاء الإلكتروني الدولي وبهدف تعزيز تنفيذ إطار الأمم المتحدة للسلوك المسؤول للدول في الفضاء الإلكتروني. وسويسرا مقتنعة بأن تطبيق القانون الدولي، بما في ذلك القانون الدولي لحقوق الإنسان والقانون الدولي الإنساني، والقواعد الطوعية غير الملزمة، وتدابير بناء الثقة وبناء القدرات، هي عناصر أساسية لضمان أمن الفضاء الإلكتروني وصونه على الصعيد الدولي. وترأس الممثل الدائم لسويسرا لدى الأمم المتحدة في نيويورك الفريق العامل المفتوح العضوية. ووافق الفريق برئاسته على تقرير ختامي صادر بتوافق الآراء في آذار/مارس 2021 (A/75/816).

وتشارك سويسرا مع الاتحاد الدولي للاتصالات، ولا سيما في مشاوراته بشأن المبادئ التوجيهية لاستخدام البرنامج العالمي للأمن السيبراني، بهدف بناء الاتساق مع عمليات أخرى على مستوى الأمم المتحدة.

وسويسرا ملتزمة بالنهوض بدور منظمة الأمن والتعاون في أوروبا في تعزيز استقرار الفضاء الإلكتروني، وتشارك بنشاط في فريقها العامل غير الرسمي المعني بأمن الفضاء الإلكتروني. ومنذ إنشاء ولاية منظمة الأمن والتعاون في أوروبا لوضع تدابير بناء الثقة وتنفيذها، زادت سويسرا من الشفافية بشأن سياستها الإلكترونية عن طريق تبادل المعلومات عن الهياكل والمنظمات والسياسات الوطنية في الاجتماعات المنتظمة للأفرقة العاملة غير الرسمية، من خلال منصات تتعهدها منظمة الأمن والتعاون في أوروبا وشبكة الاتصالات التابعة للمنظمة. وإلى جانب ألمانيا، واصلت سويسرا أيضا مشاركتها في تفعيل آلية المعلومات والتشاور المكرسة في التدبير رقم 3 لبناء الثقة.

وسويسرا دولة طرف في اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية وتعتبر تنفيذها وتطبيقها العملي أمرا حاسما في مكافحة الجريمة الإلكترونية. وتشارك سويسرا في المفاوضات بشأن بروتوكول إضافي ثان للاتفاقية، يهدف إلى تعزيز التعاون الدولي.

وعلى الصعيد الثنائي، تجري سويسرا مشاورات سياسية منتظمة مع البلدان بشأن المسائل المتصلة بالفضاء الإلكتروني.

وانضمت سويسرا إلى التحالف من أجل الحرية على شبكة الإنترنت في عام 2019 كعضوه الحادي والثلاثين. وتعتقد سويسرا اعتقادا راسخا أن الحقوق نفسها التي يتمتع بها الأشخاص خارج الإنترنت يجب أن تحظى بالحماية أيضا على الإنترنت. والتحالف من أجل الحرية على شبكة الإنترنت هو مبادرة رئيسية لتعزيز المشاركة بين جميع الجهات صاحبة المصلحة من أجل حماية حقوق الإنسان والحريات الأساسية في عصر الإنترنت. وتدعم سويسرا أيضا جهود التحالف من أجل الحرية على شبكة الإنترنت ماليا.

وفي عام 2019، أطلقت سويسرا حوار خبراء القانون حول كيفية تطبيق القانون الدولي في الفضاء الإلكتروني. وفي عام 2021، ستواصل سويسرا هذا الجهد لتعزيز الفهم المشترك لكيفية تطبيق القانون الدولي، مع التركيز على تطبيق القانون الدولي الإنساني في الفضاء الإلكتروني.

وفي عام 2018، أطلقت سويسرا حوار جنيف حول السلوك المسؤول في الفضاء الإلكتروني، الذي يوفر منتدى أصحاب المصلحة المتعددين لإجراء مناقشات حول الأدوار والمسؤوليات المتعلقة بالاستقرار الإلكتروني الدولي. ويركز حوار جنيف منذ عام 2020 على دور الشركات في تنفيذ المعايير المتفق عليها على المستوى الدولي.

وقد بدأ المركز الوطني لأمن الفضاء الإلكتروني مؤخرا عملية مشتركة بين الوكالات لصياغة نهج شامل للحكومة بأكملها من أجل الكشف عن مكامن الضعف في الفضاء الإلكتروني التي تم تحديدها حديثا بطريقة منسقة ومسؤولة. وتمكن هذه العملية الباحثين الذين يكشفون عن ثغرة أمنية في الأجهزة والبرامج والخدمات الرقمية من إبلاغ المركز عنها. ويهدف الكشف عن هذه المعلومات إلى التخفيف من حدة الثغرة الأمنية (مثل الترقيعات البرمجية) قبل أن يمكن استغلال الثغرة الأمنية لأغراض ضارة.

وتشارك سويسرا في مجموعة من التدريبات الوطنية والدولية، مثل الدروع المقفلة، لاختبار القدرات والإجراءات وعمليات صنع القرار على الصعيد الوطني.

وسويسرا عضو مؤسس في المنتدى العالمي المعني بالخبرة في الفضاء الإلكتروني وتدعم مختلف مشاريع بناء القدرات في الفضاء الإلكتروني. وتدعم سويسرا ماليا أيضا إلى المبادرات الرامية إلى تعزيز قدرة الدبلوماسيين وكذلك الممثلين غير الحكوميين على المشاركة والمساهمة في عمليات الأمم المتحدة ذات الصلة بشأن استقرار الفضاء الإلكتروني الدولي.

تركيا

[الأصل: بالإنكليزية]
[31 أيار/مايو 2021]

أصبحت تكنولوجيات المعلومات والاتصالات جزءاً أساسياً من المجتمع والاقتصاد. فهذه التكنولوجيات تُستخدم في شبكة واسعة تشمل القطاعين العام والخاص والبنية التحتية الحيوية والأفراد، وأصبحت تنتشر على نطاق واسع في تركيا وكذلك في العالم. ونتيجة لذلك، تؤدي تكنولوجيات المعلومات والاتصالات دورا هاما في تحقيق النمو والتنمية المستدامين. ولكن كلما ازداد استخدامنا للتكنولوجيا، أصبحنا أكثر اتكالا عليها وعرضة للمخاطر التي تجلبها. ويواجه الأفراد والشركات والبنية التحتية الحيوية والدول مشاكل خطيرة بسبب التهديدات الإلكترونية.

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

ونشرت الاستراتيجية وخطة العمل الوطنية لأمن الفضاء الإلكتروني للفترة 2020-2023 في الجريدة الرسمية في 29 كانون الأول/ديسمبر 2020، وهي تتضمن الأهداف الاستراتيجية الرئيسية التالية:

- حماية البنية التحتية الحيوية وزيادة القدرة على الصمود
- بناء القدرات الوطنية
- الشبكة العضوية لأمن الفضاء الإلكتروني

- أمن التكنولوجيات الجديدة (إنترنت الأشياء، والجيل الخامس من شبكات الاتصال اللاسلكية، والحوسبة السحابية، إلخ)
- مكافحة الجريمة الإلكترونية
- تطوير التكنولوجيات المحلية والوطنية وتشجيعها
- دمج أمن الفضاء الإلكتروني في الأمن القومي
- تحسين التعاون الدولي

وعلاوة على ذلك، قام الفريق الوطني للتصدي للطوارئ الحاسوبية في تركيا، وهو جزء من هيئة تكنولوجيات المعلومات والاتصالات، بتنسيق مواجهة الحوادث الإلكترونية في تركيا منذ عام 2013. وبالإضافة إلى الكشف عن التهديدات الإلكترونية ومواجهة الحوادث الإلكترونية، بما في ذلك قبل الحوادث وأثناءها وبعدها، يكفل الفريق تنفيذ التدابير الوقائية ضد التهديدات الإلكترونية والردع الإلكتروني.

ومجالات التركيز الرئيسية المتصلة بأمن الفضاء الإلكتروني للفريق الوطني للتصدي للطوارئ الحاسوبية هي التالية:

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

وفي سياق تحسين أمن الفضاء الإلكتروني على الصعيد الوطني، تم أيضاً منذ عام 2013 إنشاء 14 فريقاً قطاعياً لمواجهة الطوارئ الحاسوبية للقطاعات أو البنى التحتية الحيوية (مثل الطاقة، والصحة، والمصارف والمالية، وإدارة المياه، والاتصالات الإلكترونية، والخدمات العامة الحيوية)، و 803 1 أفرقة لمواجهة الطوارئ الحاسوبية المؤسسية. وتعمل جميع أفرقة مواجهة الطوارئ الحاسوبية على مدار الساعة، سبعة أيام في الأسبوع، بتنسيق من الفريق الوطني من أجل التخفيف من المخاطر الإلكترونية ومكافحة التهديدات الإلكترونية. ويستخدم الفريق الوطني لمواجهة الطوارئ الحاسوبية أدوات للكشف والوقاية لأغراض الرصد، وأدوات الإبلاغ لتبادل المعلومات مع الأطراف المعنية. وقام الفريق الوطني لمواجهة الطوارئ الحاسوبية بتطوير منصة لتبادل المعلومات لجميع أفرقة مواجهة الطوارئ الحاسوبية داخل تركيا من أجل توزيع الإنذارات والتحذيرات والإشعارات الأمنية، مما يوفر قناة اتصالات تتسم بالكفاءة والأمان.

وينظم الفريق الوطني لمواجهة الطوارئ الحاسوبية دورات تدريبية ومخيمات صيفية ومسابقات مفتوحة لعدة مجتمعات محلية بشأن أمن الفضاء الإلكتروني، ويقدم لها الدعم. وبالإضافة إلى ذلك، يقدم الفريق دورات تدريبية لأفرقة مواجهة الطوارئ الحاسوبية في مجالات مثل تحليل البرامجيات الخبيثة وتحليل السجلات وغيرها. وقد تم تدريب أكثر من 000 5 شخص في مجالات مختلفة من أمن الفضاء الإلكتروني على يد الفريق الوطني في السنوات الأربع الماضية.

وبالإضافة إلى ذلك، توفر الأكاديمية المنشأة ضمن هيئة تكنولوجيات المعلومات والاتصالات تدريبا إلكترونيا مفتوحا للجمهور في مجال أمن الفضاء الإلكتروني والمجالات الأخرى ذات الصلة من أجل

المســـاهمة في زيادة الخبرة في الموارد البشـــرية في تركيا. ويتوفر محتوى التدريب في البوابة الإلكترونية الرسمية للأكاديمية (www.btkakademi.gov.tr/portal).

وتنظم عدة منظمات ومؤســـسـات وجامعات ومنظمات غير حكومية وكيانات القطاع الخاص في تركيا أيضـا حلقات دراسـية ومؤتمرات ودورات تدريبية على الصـعيد الوطني بشـأن أمن الفضـاء الإلكتروني، وحماية البنى التحتية الحيوية وغير ذلك من المواضيع ذات الصلة.

ويُعدُّ اليوم السـنوي للإنترنت الآمن من بين أنشـطة التوعية، وهدفه الرئيسـي هو الاسـتخدام الواعي والآمن للإنترنت. وأتيح للعموم على البوابة الإلكترونية الرســمية الآمنة خط اتصـــال مجاني للمســاعدة في مجال الإنترنت وموقع شبكي يسمى الشبكة الآمنة، حيث يمكن للأسر أن تجد المشورة فيما يتعلق بالاستخدام الكفؤ للإنترنت (www.guvenlinet.org.tr/).

وتتخذ تركيا أيضـــا خطوات لمواجهة المخاطر الأمنية الرقمية المتزايدة لضـــمان أمن الفضـــاء الإلكتروني وتتخذ تدابير ضمن نطاق جائحة مرض فيروس كورونا (كوفيد-19).

ويقوم الفريق الوطني لمواجهة الطوارئ الحاسوبية الذي يعمل على مدار 24 ساعة في اليوم، سبعة أيام في الأسـبوع، بتحليل البرامجيات الخبيثة وهجمات التصـيد الإلكتروني وغيرها من التهديدات الإلكترونية التي تستغل اتجاهات جائحة كوفيد-19. ومن خلال مراكز القيادة والسيطرة، يتم تحديد ومنع الروابط الخبيثة لهذه التهديدات الإلكترونية من أجل حماية البنى التحتية الحيوية والمواطنين. وضـــمن هذا النطاق، يجري إعداد تقارير عن الاسـتخبارات الإلكترونية وتقاسـمها مع الأطراف المعنية. ولقد أُعدَّت أيضـا مبادئ توجيهية ونشرت، تتناول مواضيع منها:

- مبادئ الأمان لوسائل الاتصال عن بعد
- حماية المستخدمين من هجمات التصيد الإلكتروني
- تطبيقات وهمية تتعلق بكوفيد-19
- مبادئ الأمان لإعداد واستخدام برامج المؤتمرات والاجتماعات عبر الفيديو

وما فتئت تركيا تؤدي أدواراً مهمة في العديد من المنظمات، إما باعتبارها عضـواً مؤسِّـسـاً أو من خلال المســاهمة في جهود التعاون في المســائل المتعلقة بأمن الفضـــاء الإلكتروني والمعلومات. وفي هذا الســـياق، تعلق تركيا أهمية على تبادل المعلومات مع مختلف البلدان والمنظمات في طائفة واســـعة من المجالات. والفريق الوطني لمواجهة الطوارئ الإلكترونية في تركيا عضـو في منتدى فرق التصـدي للحوادث والأمن، ومؤسسة Trusted Introducers، والاتحاد الدولي للاتصالات، والمنتدى المتعدد الجنسيات لتبادل المعلومات عن البرامجيات الخبيثة التابع لمنظمة حلف شـــمال الأطلســـي (الناتو)، وتحالف أمن الفضـــاء الإلكتروني من أجل التقدم المشـترك، وفريق مواجهة الطوارئ الحاسـوبية التابع لمنظمة المؤتمر الإسـلامي. وتشـــارك تركيا أيضـــا في مركز الامتياز للدفاع التعاوني الإلكتروني التابع للناتو كدولة راعية منذ تشـرين الثاني/نوفمبر 2015. وبالإضـــافة إلى ذلك، هناك تعاون ثنائي ومتعدد الأطراف جار بشـــأن أمن الفضـــاء الإلكتروني مثل مذكرات التفاهم الموقعة مع العديد من البلدان. وتقوم تركيا بالمشـاركة والمسـاهمة بنشـاط في دراسـات منظمات دولية مثل الناتو، والأمم المتحدة، ومنظمة الأمن والتعاون في أوروبا، ومنظمة

التعاون والتنمية في الميدان الاقتصـــادي، ومجموعة العشـــرين، ومجلس التعاون للدول الناطقة بالتركية، والمركز الإقليمي للمساعدة على التحقق من تحديد الأسلحة وتنفيذه – مركز التعاون الأمني.

وتمارين أمن الفضـاء الإلكتروني هي نشـاط مهم آخر بالنسـبة للتعاون والتأهب. ويسـهم هذا النوع من التمارين الذي يجرى على الصـعيدين الوطني والدولي في تعزيز أمن الفضـاء الإلكتروني واختبار التدابير التي ســـتتخذ لمواجهة التهديدات الإلكترونية المحتملة. ومنذ عام 2011، نظمت وزارة النقل والبنية التحتية أربعة تمارين وطنية وتمرينين دوليين على أمن الفضـاء الإلكتروني. وفي الآونة الأخيرة، اشـتركت وزارة النقل والبنية التحتية وهيئة تكنولوجيات المعلومات والاتصـــالات في تنظيم "الدرع الإلكتروني" لعام 2019، وهو تمرين دولي في مجال أمن الفضاء الإلكتروني، في 19 كانون الأول/ديسمبر 2019 في أنقرة. وحظي تمرين "الدرع الإلكتروني" لعام 2019 بدعم من الاتحاد الدولي للاتصـــالات وتحالف أمن الفضـــاء الإلكتروني من أجل التقدم المشـــترك. وعلاوة على ذلك، تشـــارك تركيا في التمارين الدولية لأمن الفضـــاء الإلكتروني مثل "الدروع المقفلة" للناتو، والائتلاف المعني بالفضـــاء الإلكتروني التابع للناتو، وتمرين إدارة الأزمات للحلف نفســه، كما تســاهم في هذه التمارين. وفضــلا عن الدراســات الأخرى المتعلقة ببناء القدرات والتوجيه، تظل التمارين الدولية في مجال أمن الفضـاء الإلكتروني بالغة الأهمية لزيادة مسـتويات التأهب وبناء القدرات على مواجهة الحوادث الإلكترونية في جميع أنحاء العالم.

ويتطلب السـلام والأمن الدوليان في الفضـاء الإلكتروني مزيداً من الدراسـات اسـتناداً إلى التعاون الدولي المعزز. ويمكن أن يتبين بوضـــوح أن القانون الدولي والمعايير والقواعد المذكورة في تقارير فريق الخبراء الحكوميين والأفرقة العاملة المفتوحة العضـوية وفي الدراسـات ذات الصـلة تسـهم في إيجاد فضـاء إلكتروني أكثر أمانا.

وبالإضـافة إلى ذلك، يكتسـب تحسـين التعاون ودعم آليات تبادل المعلومات أهمية بالغة لمكافحة التهديدات في الفضاء الإلكتروني، وينبغي إعطاؤهما الأهمية الواجبة.

وعلاوة على ذلك، تدرك تركيا أهمية تنفيذ القانون الدولي ومعايير الســـلوك المســـؤول للدول في الفضـاء الإلكتروني والحاجة إلى تعاون دولي فعال. وتتخذ تركيا الخطوات اللازمة بعزم لضـمان تحقيق هذه الأهداف، وسيظلّ تعزيز أمن الفضاء الإلكتروني على الصعيدين الوطني والدولي إحدى أولوياتها الرئيسية.

أوكرانيا

[الأصل: بالإنكليزية]
[31 أيار/مايو 2021]

يبين تحليل للمعلومات المتاحة أن أحد التهديدات الرئيســـية للأمن القومي، في ظروف الحرب "المختلطة" ضد دولتنا، هو المعلومات المدمرة والعمليات الخاصـة ذات الطابع النفسـي التي يقوم بها الاتحاد الروسي بهدف تقويض النظام الدستوري، وانتهاك سيادة أوكرانيا وسلامتها الإقليمية، والتسبب في تفاقم الحالة الاجتماعية – السـياسـية والاجتماعية – الاقتصـادية في بلدنا. وأصـبح النشـر المتعمد للمعلومات المضـللة والمعلومات الزائفة، إلى جانب العدوان المسلح، خطرا محدقا ليس بأوكرانيا فحسب، بل بالعالم بأسره أيضا، لأنه يؤثر على وعي مواطني بلدان أخرى، وينتج صورة مشوهة عن أوكرانيا، ويشكل رأيا عاما مفيدا لروسيا وحدها.

وتتخذ الدولة المعتدية على نحو متزايد تدابير ترمي إلى التقليل من مستوى أمن المعلومات في دولتنا، واستحداث وسائل تأثير على مؤسسات الدولة وفضاء المعلومات بغية تعزيز موقفها، وتشكيل رأي أجنبي موات، وممارسة الضغط على مؤسسات الدولة الأوكرانية لاتخاذ قرارات في صالحها. وتحقيقا لهذه الغاية، تجري عملية الترويج في فضاء المعلومات والإعلام الأوكراني، بشكل ممنهج، وعلى شبكة الإنترنت، بما في ذلك من خلال شبكات التواصل الاجتماعي، والمتراسلين، والموارد الإلكترونية، ومنتجات المعلومات المعدة خصيصا، ولا سيما ذات الطابع المضلل.

ومن أجل إحداث هذا التأثير السلبي من خلال المعلومات على بلدنا، أنشأ الاتحاد الروسي نظاما قويا للترويج للمحتوى الدعائي، يشمل شبكة من منصات المعلومات (مدونات ومواقع) ووسائط الإعلام وموارد الإنترنت المتحكم فيها، ومجمعي المعلومات ومُوردي الأخبار بشكل مكثف، والمدونين وقادة الرأي لنشر المحتوى، ووكالات الأنباء وشركات العلاقات العامة لعرض رسائل دعائية ضمن أبرز عناوين الأخبار. وهناك أيضا استخدام واسع النطاق من قبل روسيا لشبكات روبوتات على الإنترنت للنشر السريع لمعلومات مضللة ورسائل معادية لأوكرانيا تهدف إلى التلاعب بالوعي الجماهيري. والجهات الرئيسية في فضاء المعلومات التي يستخدمها الجانب الروسي لنشر المعلومات المضللة هي الشبكات الرائدة في العالم في مجال التواصل الاجتماعي (Facebook، و Instagram، و Twitter)، التي تزايد جمهورها كثيرا بسبب الحظر المفروض في أوكرانيا على شبكتي التواصل الاجتماعي الروسيتين VKontakte و Odnoklassniki. وهناك ميل إلى إعادة توجيه مستخدمي الجزء الأوكراني من شبكة الإنترنت نحو الاستخدام الواسع النطاق لخدمات المراسلة (Telegram، و WhatsApp، و Viber، وما إلى ذلك)، وذلك بسبب إمكانية الحفاظ على سرية الهوية، وكفاءة وضع المحتوى وزيادة توزيعه على نطاق واسع، وارتفاع مستويات التفاعل وإبداء التعليقات.

وتُستعمل الخدمات المستضيفة لشرائط الفيديو (YouTube، و Yandex.Video، و RuTube، و Video@Mail.Ru) أيضا لنشر المعلومات المضللة، حيث تعمل الشركات التي تمتلك خدمات استضافة الصور وشرائط الفيديو وفق قوانين البلدان التي توجد في إقليمها. ويستخدم ذلك من قبل القائمين بالدعاية الروس لوضع ونشر محتوى على هذه المنصات على شبكة الإنترنت يشكل تهديدا لأمن المعلومات في أوكرانيا. ونظرا لأن مصدر هذه الرسائل هو المواقع المستضيفة في الولايات المتحدة وأوروبا، فإن المحتوى يوزع بحرية على شبكة الإنترنت.

وبالإضافة إلى ذلك، يبذل البلد المعتدي جهودا للتطوير المستمر لشبكة من مصادر المعلومات المتحكم فيها. وعلى وجه الخصوص، تتخذ إدارات الاحتلال في الأراضي المحتلة مؤقتا في دولتنا تدابير ممنهجة تهدف إلى إنشاء منصات إعلامية جديدة، وزيادة عدد القنوات التلفزيونية وتوسيع نطاق تغطية البث التلفزيوني والإذاعي، بما في ذلك في الأراضي التي تسيطر عليها السلطات الأوكرانية. وبالإضافة إلى توزيع المحتوى المعادي لأوكرانيا، تُستخدم معدات إعادة إرسال قوية نصبتها سلطات الاحتلال الروسية للقضاء على إشارة البث التلفزيوني والإذاعي المحلي عن طريق نشر ما يسمى بـ ”الضجيج الأبيض“ على الترددات التي يستخدمها الجانب الأوكراني لنقل معلومات موضوعية إلى سكان الأراضي المحتلة مؤقتا. ويكتسي هذا الأمر أهمية خاصة من حيث ترميز أكبر المجموعات الإعلامية في البلد مجموعة إنتر ميديا (Inter Media Group)، ومجموعة ستار لايت ميديا (StarLightMedia)، والمجموعة الإعلامية في أوكرانيا (Ukraine Group Media)، ومجموعة (1+1) للإشارة الساتلية لقنواتها التلفزيونية وحالة التغطية

غير المرضـــية لإقليم أوكرانيا من خلال البث التلفزيوني والإذاعي الوطني بالمعيار الرقمي. ونتيجة لذلك، يتعرض ســـكان المناطق الحدودية في أوكرانيا لتأثير مســـتمر للمحتوى المدمر المقدم من القنوات الدعائية الرئيسية للاتحاد الروسي. وثمة عامل آخر للتأثير السلبي، يعقد إيصال المحتوى المحلي إلى سكان الأراضي الأوكرانية المحتلة مؤقتا، وهو عمل المشغلين ومقدمي الخدمات للأراضي المحتلة مؤقتا، مما يحد من وصول الســـكان المحليين إلى الجزء الأوكراني من شـــبكة الإنترنت. وهكذا، وفي انتهاك للقانون الأوروبي، تقوم المنظمة غير الربحية مركز تنسيق الشبكة الأوروبية لبروتوكول الإنترنت (هولندا) بتسجيل عناوين بروتوكول الإنترنت من أجل عمل ما يســـمى بمقدمي خدمات الإنترنت في جزيرة القرم وفي المناطق المحتلة من دونباس. وبغية جعل أنشطة هذه المنظمة متوافقة مع التشريعات الحالية لأوكرانيا، تتخذ وزارة خارجية أوكرانيا وسفارة أوكرانيا في مملكة هولندا التدابير المناسبة على الصعيد الثنائي مع دولة هولندا.

وهناك أيضـا حالات لاسـتعمال الاتحاد الروسـي لخدمات شـركتي آبل وغوغل لنشـر المعلومات المضـللة من أجل التلاعب بعقول مسـتخدمي الجزء الأوكراني من شـبكة الإنترنت. وعلى وجه الخصـوص، في متجر آبل للتطبيقات (App Store) وســوق اللعب لغوغل (Market Play)، هناك تطبيقات للأجهزة المحمولة وضـعتها كيانات قانونية وأشـخاص طبقت بشـأنهم تدابير (جزاءات) خاصـة واقتصـادية وغيرها من التدابير التقييدية وفقا لقرار المجلس الوطني للأمن والدفاع المؤرخ 14 أيار/مايو 2020 بشـأن تطبيق وإلغاء وتعديل التدابير الشـخصـية والخاصـة والاقتصـادية وغيرها من التدابير التقييدية (الجزاءات)، التي اتخذت بموجب المرسوم رقم 2020/184 الصـادر عن رئيس أوكرانيا بتاريخ 14 أيار/مايو 2020. ولهذه المنتجات البرامجية من حيث خصـائصـها الوظيفية القدرةُ التقنية لتيسـير الوصـول إلى موارد شـبكة الإنترنت المحظورة في أوكرانيا.

وعلى الرغم من كل الجهود التي تبذلها دولتنا لتعزيز أمن المعلومات ووقف انتشـــار المعلومات المضـــللة، باعتبارها أحد أكبر التهديدات في مجال المعلومات، هناك حاجة ملحة إلى مســـاعدة المجتمع الدولي والمؤسـسـات الدولية على التصـدي على نحو ملائم للعدوان الإعلامي من جانب الاتحاد الروسـي، ليس ضـد أوكرانيا فحسـب، بل أيضـا فيما يتعلق ببلدان أخرى تقوم روسـيا انطلاقا منها بأعمال ذات تأثير مدمر في فضاء المعلومات.

وحتى وقت قريب، كان التأثير المدمر للاتحاد الروســـي في مجال المعلومات، ومحاولاته التدخل في الشـؤون الداخلية لدولتنا، ومحاولاته فرض شـروطه في تنفيذ التعاون الدولي والعمليات الداخلية، تُنفَّذ من خلال الأحزاب والحركات السياسية الأوكرانية المنتسبة، والتمويل السري المباشر لمؤسسات مدنية وكيانات اقتصـادية تعمل على أراضـي دولتنا، والضـغط القوي من خلال العدوان العسكري في شرق أوكرانيا أو عرقلة الدعم الدولي وانضمام أوكرانيا إلى الاتحاد الأوروبي ومنظمة حلف شمال الأطلسي (الناتو)، والقيام بحملات وعمليات وإجراءات إعلامية من خلال موارد للمعلومات متحكم فيها.

ومع ذلك، هناك ميل ثابت نحو إعادة توجيه الاتحاد الروســـي لاســـتراتيجية أخرى لما يســـمى "حرب المعلومات" ضـد أوكرانيا في اتجاه إخفاء مشـاركته في وضـع وتنفيذ التدابير التدميرية ضـد دولتنا من خلال تنفيذها من موقع ما يسمى بالبلدان "الثالثة". فمن ناحية، يحدث هذا نتيجة للجزاءات الاقتصـادية التي فرضـها الاتحاد الأوروبي والولايات المتحدة على الاتحاد الروسي بسبب تدخله في الشؤون الداخلية لأوكرانيا وضم جمهورية القرم المتمتعة بالحكم الذاتي والنزاع المسلح في الأراضـي المحتلة مؤقتا في منطقتي دونيتسك ولوهانســك. ومن ناحية أخرى، يعود ذلك أيضــا إلى التدابير التي اتخذها الجانب الأوكراني لمكافحة التأثير

المدمر للبلد المعتدي على الفضـــاء الإعلامي الأوكراني ووعي المواطنين، والتخفيف من الآثار الســـلبية للرسائل المنشورة، وزيادة مستوى وطنية سكان دولتنا ووعيهم الذاتي.

وعلى وجه الخصـوص، هناك زيادة في أعمال التأثير على المعلومات ووقائع التدخل في الشـؤون الداخلية لأوكرانيا. إذ يقوم الاتحاد الروسي بأنشطة استخباراتية وتخريبية من منظور دول أعضاء في منظمة حلف شمال الأطلسي والاتحاد الأوروبي، تشمل إنشاء وتمويل جماعات ضغط للدفاع عن المصالح الروسية لدى السلطات والإدارة الحكومية والمحلية، والأحزاب والحركات السياسية، وأوساط الخبراء والمدونين، ومراكز الفكر، وشـركات الإعلان والاسـتشـارات، والجهات المانحة، والمنظمات غير الحكومية، وقادة الرأي العام، وكذلك من خلال إنشاء وسائل إعلام وموارد إنترنت وشركات للعلاقات العامة متحكم فيها.

وبمسـاعدة سـياسـيين أوروبيين موالين لروسـيا في ما يسـمى بخلايا "العالم الروسـي" في الاتحاد الأوروبي، يحاول الاتحاد الروسي إضفاء الطابع القانوني على فكرة شرعية استفتاء جزيرة القرم وفرضها على المجتمع الدولي، وتبرير عدوانه المسلح على أوكرانيا، وبالتالي تحقيق رفع الجزاءات المفروضـة على روسـيا وعودتها إلى المؤسسات السياسية العالمية. وفي الوقت الراهن، تنشط الفروع الموالية لروسيا في بعض الدول الأوروبية. ويقوم معظم ممثلي هذه القوى السـياسـية، باعتبارهم ممارسـين للضـغط من أجل مصـالح البلد المعتدي داخل بلدهم وخارجه على حد سواء، بنشـر آراء موالية لروسـيا، وتعميم خطابات روسـية، ويتخذون تدابير إعلامية تهدد المصالح الوطنية لأوكرانيا.

وتتجلى إعادة توجيه الاتحاد الروسـي نحو تنظيم وتنفيذ عمليات إعلامية خاصـة وأعمال ذات تأثير إعلامي مدمر من منظور بلدان "ثالثة" في إثارة تناقضـــات تاريخية ومطالبات إقليمية لدول أخرى تجاه أوكرانيا، والتحريض على مظاهرات مطالبة بالانفصـــال والاســتقلال بين الأقليات القومية في أوكرانيا. ومن ناحية، يعقد هذا الأمر العلاقات بين دولتنا والبلدان المجاورة، التي يقوم الاتحاد الروســي انطلاقا من موقعها بمثل هذه الأنشطة التدميرية؛ ومن ناحية أخرى، يصبح سببا لهذه البلدان لإعلان مطالباتها الإقليمية ببعض الأراضـي الأوكرانية. وفي الوقت نفسـه، فإن روسـيا، بابتعادها رسـميا عن هذه العملية، تتجنب تلقي اتهامات مباشرة من أوكرانيا والمجتمع الدولي بالتدخل في الشؤون الداخلية لدولتنا، وتهدد مباشرة علاقات حسن الجوار لأوكرانيا مع دول أخرى، من أجل تشكيل مواقع لممارسة التأثير على الحالة السياسية الداخلية في أوكرانيا.

وفي ضـوء ما تقدم، سـتواصـل أوكرانيا اتخاذ تدابير شـاملة لضـمان السـلوك المسـؤول في الفضـاء الإلكتروني في سياق الأمن الدولي، مع الدعوة في الوقت نفسه إلى دعم المجتمع الدولي وبذل جهود مشتركة لمواجهة الحرب "المختلطة" للاتحاد الروسي على النحو المناسب.

ومن أجل ضـمان تنفيذ إصـلاح تشـريعات التوقيع الرقمي الإلكتروني من خلال التنسـيق مع أحكام اللائحـة التنظيميـة (للاتحـاد الأوروبي) رقم 2014/910 الصـــادرة عن البرلمـان الأوروبي والمجلس بتاريخ 23 تموز/يوليه 2014 بشـأن تحديد الهوية الإلكترونية والخدمات الاسـتئمانية للمعاملات الإلكترونية في السـوق الداخلية، التي تلغي التوجيه 1999/93/EU للبرلمان الأوروبي والمجلس، اعتمد برلمان أوكرانيا (فرخوفنا رادا) القانون رقم 2155–ثامنا بشـأن الخدمات الاسـتئمانية الإلكترونية في 5 تشـرين الأول/ أكتوبر 2017، الذي دخل حيز النفاذ في 7 تشرين الثاني/نوفمبر 2018.

والغرض الرئيسـي هو بدء تطبيق نماذج ومبادئ تقديم الخدمات الاسـتئمانية الإلكترونية المسـتعملة في الاتحـاد الأوروبي في أوكرانيـا، دون تـدمير نظـام التفـاعـل بين الأطراف في مجـال التوقيع الرقمي

الإلكتروني الذي تطور في البلد. ويحدد القانون المبادئ القانونية والتنظيمية لتوفير الخدمات الاستئمانية الإلكترونية، بما في ذلك الخدمات العابرة للحدود، وحقوق والتزامات الأشخاص الذين توجد بينهم علاقات في مجال الخدمات الاستئمانية الإلكترونية، وإجراءات إشراف (مراقبة) الدولة على الامتثال (للامتثال) للتشريعات في مجال الخدمات الاستئمانية الإلكترونية، والمبادئ القانونية والتنظيمية لتحديد الهوية الإلكترونية. واتخذ مجلس وزراء أوكرانيا، لدى وضع أحكام القانون رقم 2155–ثامنا، عددا من القرارات:

- القرار رقم 749 بشأن الموافقة على إجراءات استعمال الخدمات الاستئمانية الإلكترونية في الهيئات العامة والحكومات المحلية والشركات والمؤسسات والمنظمات التي تملكها الدولة، الذي اتخذه مجلس وزراء أوكرانيا في 19 أيلول/سبتمبر 2018.
- القرار رقم 775 بشأن الموافقة على المتطلبات الإلزامية فيما يتعلق بالقائمة المرجعية، الذي اتخذه مجلس وزراء أوكرانيا في 26 أيلول/سبتمبر 2018.
- القرار رقم 821 بشأن الموافقة على إجراءات تخزين المعلومات الوثائقية ونقلها إلى هيئة الإدارة المركزية في حالة إنهاء أنشطة مقدم مؤهل للخدمات الاستئمانية الإلكترونية، الذي اتخذه مجلس وزراء أوكرانيا في 10 تشرين الأول/أكتوبر 2018.
- القرار رقم 992 بشأن الموافقة على المتطلبات في مجال الخدمات الاستئمانية الإلكترونية وإجراءات عمليات التفتيش للتحقق من الامتثال لمتطلبات التشريعات في مجال الخدمات الاستئمانية الإلكترونية، الذي اتخذه مجلس وزراء أوكرانيا في 7 تشرين الثاني/نوفمبر 2018.
- القرار رقم 1215 بشأن الموافقة على إجراءات تقييم المطابقة في مجال الخدمات الاستئمانية الإلكترونية، الذي اتخذه مجلس وزراء أوكرانيا في 18 كانون الأول/ديسمبر 2018.
- القرار رقم 60 بشأن الموافقة على إجراءات الاعتراف المتبادل بالشهادات العامة الرئيسية الأوكرانية والأجنبية والتوقيعات الإلكترونية واستخدام نظام المعلومات والاتصالات في الهيئة المركزية المسؤولة عن ضمان الاعتراف في أوكرانيا بالخدمات الاستئمانية الإلكترونية والشهادات العامة الرئيسية الأجنبية المستخدمة أثناء تقديم خدمات إلكترونية ذات أهمية قانونية في عملية التفاعل بين رعايا دول مختلفة، الذي اتخذه مجلس وزراء أوكرانيا في 23 كانون الثاني/يناير 2019.

ووافقت إدارة الاتصالات الخاصة وحماية المعلومات في أوكرانيا، امتثالا لمتطلبات المادة 8 من القانون، وبموجب الأمر المؤرخ 14 أيار/مايو 2020 على متطلبات أمن وحماية المعلومات المتعلقة بمقدمي الخدمات المرجعية الإلكترونية المؤهلين ونقاط تسجيلهم المنفصلة (المسجلة لدى وزارة العدل الأوكرانية في 16 تموز/يوليه 2020)، التي تفصل وتحدد تنفيذ القانون والمتطلبات في مجال الخدمات الاستئمانية الإلكترونية، التي وافق عليها مجلس وزراء أوكرانيا في 7 تشرين الثاني/نوفمبر 2018 عن طريق القرار رقم 992، لضمان أمن وحماية المعلومات عن مقدمي الخدمات الاستئمانية الإلكترونية ونقاط التسجيل المنفصلة.

وتتخذ أوكرانيا حاليا تدابير ترمي إلى الاعتراف المتبادل بالخدمات الاستئمانية الإلكترونية في إطار اتفاق الشراكة بين أوكرانيا والاتحاد الأوروبي، ونتيجة للاتفاقات التي تم التوصل إليها بين أوكرانيا والاتحاد الأوروبي خلال مؤتمر القمة الثاني والعشرين للاتحاد الأوروبي وأوكرانيا.

وفي الوقت نفسه، من الضروري تنقيح بعض أحكام القانون من أجل مواءمتها قدر الإمكان مع أحكام اللائحة التنظيمية (للاتحاد الأوروبي) رقم 2014/910، ولا سيما من حيث وضع لوائح الدولة التنظيمية في مجال تحديد الهوية الإلكترونية، ومتطلبات تحسين التوقيعات والأختام الإلكترونية، وتوضيح متطلبات التوقيعات أو الأختام الإلكترونية المؤهلة. وينظر مجلس وزراء أوكرانيا حاليا في مشروع قانون أعدته وزارة التحول الرقمي وإدارةِ الاتصالات الخاصة وحماية المعلومات في أوكرانيا.

وبالإضافة إلى ذلك، قام مجلس وزراء أوكرانيا، بموجب القرار رقم 24 المؤرخ 13 كانون الثاني/يناير 2021، بتعديل الفقرة 4 من اللوائح التنظيمية بشأن إدارة الدائرة الحكومية للاتصالات الخاصة وحماية المعلومات في أوكرانيا، التي تدير إدارة الاتصالات الخاصة الحكومية، وحدد وظائف هيئة الاعتماد الآمن المنشأة وفقا للمادة 7 بشأن الترتيبات الإدارية لحماية المعلومات المقيد الوصول إليها بين حكومة أوكرانيا ومنظمة حلف شمال الأطلسي، التي صُدق عليها بموجب القانون رقم 2068 المؤرخ 24 أيار/مايو 2017.

وتتخذ إدارة الاتصالات الخاصة وحماية المعلومات في أوكرانيا، من خلال وضع إجراءات اعتماد وطنية من أجل أمن نظام الاتصالات والمعلومات المخصص لتبادل معلومات الناتو المقيد الوصول إليها، تدابير لتنفيذ لوائح الناتو التنظيمية بشأن هذه المسائل.

وفي إطار تعزيز التعاون الدولي وتوعية المهنيين في مجال أمن المعلومات، تشارك إدارة الاتصالات الخاصة وحماية المعلومات في أوكرانيا في المؤتمرات الدولية لأداة المفوضية الأوروبية للمساعدة التقنية وتبادل المعلومات والحلقات الدراسية "فاير آي" (FireEye).

وبهدف تعزيز أمن المعلومات، يجري باستمرار اعتماد نظام لمراجعة جوانب أمن المعلومات في مرافق البنية التحتية الحيوية، على النحو التالي:

- وضع المتطلبات بالنسبة للمراجعين المستقلين لجوانب أمن المعلومات في مرافق البنية التحتية الحيوية.
- وضع إجراءات منح الشهادات/إعادة منحها لمراجعي جوانب أمن المعلومات، وكذلك نظام تقييم محدد الغرض للتدريب المهني لمراجعي جوانب أمن المعلومات وتحليل نتائج المراجعة المستقلة لأمن المعلومات فيما يتعلق بالمكونات البالغة الأهمية للبنية التحتية في عملية "مراجعة" أمن تكنولوجيا المعلومات.

وفي الوقت نفسه، ومن أجل تنفيذ سياسة الدولة في مجال حماية المعلومات، يقوم موظفو إدارة الاتصالات الخاصة وحماية المعلومات في أوكرانيا بتنفيذ تدابير الرقابة الوطنية على حالة الحماية التقنية في الفضاء الإلكتروني لموارد المعلومات والمعلومات الحكومية على النحو الذي يتطلبه القانون.

وعلاوة على ذلك، اتخذت إدارة الاتصالات الخاصة وحماية المعلومات في أوكرانيا عددا من الإجراءات للتحضير لاعتماد الوثائق التالية وضمان اعتمادها:

- أعدت مقترحات شاملة لمشروع استراتيجية أوكرانيا لأمن الفضاء الإلكتروني (2021-2025) وفقا للمادة 107 من دستور أوكرانيا، والجزء الثاني من المادة 2 من قانون أساسيات الأمن القومي والمرسوم رقم 2020/391 لرئيس أوكرانيا بشأن قرار المجلس الوطني للأمن والدفاع المؤرخ 14 أيلول/سبتمبر 2020.

- قدمت الدعم لاعتماد مجلس وزراء أوكرانيا للقرار رقم 518 بتاريخ 19 حزيران/يونيه 2019 بشأن الموافقة على المتطلبات العامة للحماية الإلكترونية للبنية التحتية الحيوية، الذي بدأ في إطار تشكيل وتنفيذ سياسة الدولة بشأن الحماية الإلكترونية للبنية التحتية الحيوية للمعلومات، ويهدف إلى تحقيق التوافق مع معايير الاتحاد الأوروبي وحلف شمال الأطلسي ذات الصلة، وكذلك إنشاء إطار تنظيمي ومصطلحي بشأن أمن الفضاء الإلكتروني ومواءمة اللوائح التنظيمية في مجال أمن المعلومات وأمن الفضاء الإلكتروني وفقا للمعايير الدولية.

- اعتمد مجلس وزراء أوكرانيا القرار رقم 1109 بشأن بعض المسائل المتعلقة بمرافق البنية التحتية الحيوية والقرار رقم 943 بشأن بعض المسائل المتعلقة بمرافق البنية التحتية الحيوية للمعلومات، اللذين وُضعا مع مراعاة متطلبات تشريعات الاتحاد الأوروبي، ولا سيما توجيه الاتحاد الأوروبي 1148/2016 الصادر عن البرلمان الأوروبي والمجلس في 6 تموز/يوليه 2016 بشأن التدابير الرامية إلى تحقيق مستوى مشترك عال من أمن نظم الشبكات والمعلومات في الاتحاد، وتوجيه المجلس 2008/114/EC المؤرخ 8 كانون الأول/ديسمبر 2008 بشأن تحديد البنية التحتية الحيوية الأوروبية وتعيينها وتقييم الحاجة إلى تحسين حمايتها.

- في 11 تشرين الثاني/نوفمبر 2020، اعتمد مجلس وزراء أوكرانيا القرار رقم 1176 بشأن الموافقة على إجراءات استعراض حالة الحماية الإلكترونية للبنية التحتية الحيوية للمعلومات، وموارد المعلومات والمعلومات الحكومية على نحو ما يقتضيه القانون، الذي يسمح بتنظيم البنية التحتية للمعلومات وموارد المعلومات والمعلومات الحكومية التي يقتضي القانون حمايتها.

ويتخذ فريق مواجهة الطوارئ الحاسوبية في أوكرانيا باستمرار تدابير للتعاون مع الأفرقة الأجنبية لمعالجة القضايا المتعلقة بالتغلب على آثار الهجمات الإلكترونية على البنية التحتية الحيوية للمعلومات، ويحلل البيانات المتعلقة بالحوادث في الفضاء الإلكتروني، ويوفر لأصحاب مرافق أمن الفضاء الإلكتروني مساعدة عملية في منع وقوع الحوادث في الفضاء الإلكتروني والكشف عنها والقضاء على آثارها، ويعد وينشر توصيات لمكافحة الأنواع الحديثة للهجمات الإلكترونية والتهديدات الإلكترونية على موقعه الشبكي الرسمي ويقدم معلومات عن التهديدات الإلكترونية والأساليب المناسبة للحماية منها.

المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية

[الأصل: بالإنكليزية]
[31 أيار/مايو 2021]

ترحب المملكة المتحدة بالدعوة إلى إبلاغ الأمين العام بآرائها وتقييماتها بشأن المسائل المتصلة بتعزيز سلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي، على النحو المبين بالتفصيل في قرار الجمعية العامة 32/75. ونشجع جميع الدول المشاركة في المناقشات المتعلقة بالتطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي على الاستفادة من هذه الفرصة والفرص اللاحقة.

ولا يحترم الفضاء الإلكتروني الحدود الوطنية. وستعمل المملكة المتحدة، بوصفها قوة مسؤولة في الفضاء الإلكتروني، على تشكيل الأطر التي ستنظم هذا الفضاء في المستقبل، مع التقيد بالقواعد القائمة، وبناء توافق في الآراء بشأن معايير السلوك الإيجابية في عالم تشكله التكنولوجيا بالأساس.

وتدرك المملكة المتحدة أن التغير التكنولوجي السريع في مجالات مثل الذكاء الاصطناعي والفضاء الإلكتروني والبيانات سيعيد تشكيل مجتمعاتنا خلال العقد القادم. ويجب على البلدان أن تعمل معا للتصدي لأكبر التحديات العالمية، بما في ذلك لتشجيع تهيئة فضاء إلكتروني حر ومفتوح وسلمي وآمن، والعمل كقوة من أجل الخير في العالم، تدافع عن الديمقراطية وحقوق الإنسان في مجتمعاتنا الرقمية.

وسنشجع اعتماد تلك القواعد والمعايير والالتزام بها، وسنعمل بالتنسيق مع مجموعة كاملة من الشركاء وأصحاب المصلحة لتأكيد المبررات المقنعة لبناء فضاء إلكتروني يحمي المجتمعات المنفتحة ويمكن من الابتكار والتنمية والنمو. وسندعم أيضا تلك البلدان التي تواجه تحديات الرقمنة – من خلال عمليات بناء القدرات الدولية – من أجل بناء الثقة للمشاركة في النقاش الدولي وتنمية قدراتها في مجال أمن الفضاء الإلكتروني.

وترحب المملكة المتحدة بالاختتام الناجح لعمليتي الأمم المتحدة المتزامنتين، الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي، وفريق الخبراء الحكوميين المعني بتعزيز سلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي. ووفر الفريق العامل المفتوح العضوية عملية شاملة تمثل الآراء المتنوعة لجميع الدول الأعضاء وأصحاب المصلحة الآخرين، فيما نعتقد أن تقرير فريق الخبراء الحكوميين سيقدم الدليل التفصيلي للإطار الأولي لسلوك الدول المسؤول في الفضاء الإلكتروني الذي طلبته دول عديدة.

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

في 16 آذار/مارس 2021، نشرت المملكة المتحدة *بريطانيا العالمية في عصر تنافسي. الاستعراض المتكامل للأمن والدفاع والتنمية والسياسة الخارجية*[9]، وهو ورقة تصف رؤية الحكومة لدور المملكة المتحدة في العالم على مدى العقد المقبل والإجراءات التي سنتخذها في الفترة حتى عام 2025. ويحدد الاستعراض الحاجة إلى تشكيل النظام الدولي وهو يتطور في آفاقه المستقبلية – في مجالي الفضاء الإلكتروني والفضاء، حيث تتوسع إمكانيات النشاط الاقتصادي والاجتماعي والعسكري بسرعة. وسنعمل بنشاط على ضمان المساءلة والرقابة الفعالتين اللتين تحميان القيم الديمقراطية، بينما سنعارض التجاوزات في سيطرة الدولة.

وستعتمد المملكة المتحدة أيضا استراتيجية جديدة وشاملة للفضاء الإلكتروني في عام 2021، لتحل محل الاستراتيجية الوطنية السابقة لأمن الفضاء الإلكتروني للفترة 2016–2021. وستدعم الاستراتيجيةَ الحاجةُ إلى نهج "الحكومة بأكملها" إزاء المسائل المتعلقة بالفضاء الإلكتروني، كما هو مشار إلى ذلك مسبقا في الاستعراض المتكامل. وفي إطار هذه الاستراتيجية، ستكون إجراءاتنا ذات الأولوية هي:

- تعزيز البيئة الإلكترونية في المملكة المتحدة، وتمكين اتباع نهج الأمة بأكملها في التعامل مع أمور الفضاء الإلكتروني وتعميق الشراكة بين الحكومة والأوساط الأكاديمية والقطاع المعني.
- بناء مملكة متحدة رقمية مزدهرة وقادرة على الصمود، يشعر المواطنون فيها بالأمان على شبكة الإنترنت والثقة من أن بياناتهم محمية.

(9) www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy.

- الاضطلاع بالريادة في التكنولوجيات الحيوية اللازمة للقوة في الفضاء الإلكتروني، مثل معالِجات البيانات الدقيقة، وتصميم النظم الآمنة، وتقنيات الكم، والأشكال الجديدة لنقل البيانات.
- تشجيع تهيئة فضاء إلكتروني حر ومفتوح وسلمي وآمن، والعمل مع الحكومات الأخرى والقطاع المعني والاستفادة من قيادة المملكة المتحدة الفكرية في مجال أمن الفضاء الإلكتروني.
- كشف خصومنا وتعطيل أعمالهم وردعهم.

ومن خلال هذه الاستراتيجيات، سنعمل مع الحكومات الأخرى وفي إطار شراكة مع القطاع المعني لضمان أن تنظم الفضاء الإلكتروني قواعد ومعايير تحسن الأمن الجماعي، وتعزز القيم الديمقراطية، وتدعم النمو الاقتصادي العالمي، وتتصدى لانتشار الاستبداد الرقمي. وستدعم المملكة المتحدة سيادة القانون في الفضاء الإلكتروني: من خلال تجسيد سلوك الدولة المسؤول، وتشكيل أفضل الممارسات الدولية، وتحفيز الامتثال، وردع الهجمات، ومحاسبة الآخرين على سلوك الدولة غير المسؤول. وعند الحاجة، سنشكل القواعد بحيث توضع أدوات إلكترونية هجومية وتُستخدم بمسؤولية ووفقا للقانون الدولي.

وبالإضافة إلى ذلك، سنقوم بما يلي:

- حماية شبكة إنترنت عالمية يمكن الوصول إليها وقابلة للتشغيل المتبادل من أجل الأجيال القادمة.
- ضمان حماية حقوق الإنسان على شبكة الإنترنت كما هي محمية خارجها.
- كفالة تضمين الشفافية والمساءلة منذ البداية في تصميم التكنولوجيات الجديدة ونشرها.
- الدفاع عن التدفق الدولي للبيانات، وتمكين التبادل الآمن والموثوق به والقابل للتشغيل المتبادل عبر الحدود، مع الحفاظ على معايير حماية البيانات.

وتعتبر المملكة المتحدة أن دبلوماسية الفضاء الإلكتروني عنصر بالغ الأهمية من عناصر ريادتها في هذا الفضاء، حيث توجد شبكة من الموظفين تمتد عبر ست قارات. وبالإضافة إلى برامجنا لبناء القدرات في مجال أمن الفضاء الإلكتروني، بدأنا حوارات بين الحكومات مع 20 بلدا. ومن خلال هذه الحوارات، سنواصل تنمية الشراكة لتعزيز مبررات إنشاء فضاء إلكتروني حر ومفتوح وسلمي وآمن، والتصدي للنشاط الإلكتروني الخبيث الموجه من الدول وردعه.

ونواصل المشاركة في مجموعة واسعة من المنتديات العالمية والإقليمية المخصصة لمناقشات أمن الفضاء الإلكتروني، بما في ذلك كل من الفريق العامل المفتوح العضوية التابع للأمم المتحدة وفريق الخبراء الحكوميين التابع للأمم المتحدة، ومنظمة الأمن والتعاون في أوروبا، والاتحاد الدولي للاتصالات، والمنتدى العالمي المعني بالخبرة في شؤون الفضاء الإلكتروني.

ويمكن للمملكة المتحدة أن تنسب، بل وتنسب فعلا الهجمات الإلكترونية الخبيثة إلى الدول حين تعتقد أن القيام بذلك يخدم مصالحها الفضلى، وللوفاء بالتزامها بالوضوح والاستقرار في الفضاء الإلكتروني. وما زلنا نعتبر أن قرار نسب النشاط الإلكتروني الخبيث إلى دولة ما، وبشكل أساسي إعلان هذا النسب، هو في نهاية المطاف قرار سياسي للدول. وتتاح البيانات والمعلومات الأخرى ذات الصلة على شبكة الإنترنت على الموقعين www.gov.uk و www.ncsc.gov.uk.

وفي عام 2020، أنشأت المملكة المتحدة القوة الوطنية المعنية بالفضاء الإلكتروني. ونحن واحد من عدد من البلدان التي أكدت علنا أنها تطور هذه القدرات. وتقوم القوة الوطنية المعنية بالفضاء الإلكتروني بعمليات هجومية مسؤولة ومحددة الأهداف في الفضاء الإلكتروني لدعم أولويات الأمن القومي للمملكة المتحدة، وتجمع فيها بين القدرات الدفاعية والاستخباراتية. ويمكن أن تشمل أمثلة العمليات في الفضاء الإلكتروني، التي تُستخدم مع القدرات الدبلوماسية والاقتصادية والسياسية والعسكرية، ما يلي:

- التدخل في هاتف محمول لمنع إرهابي من إمكانية التواصل مع معارفه.
- المساعدة على منع استخدام الفضاء الإلكتروني كمنصة عالمية لارتكاب الجرائم الخطيرة، بما في ذلك الاحتيال والاعتداء الجنسي على الأطفال.
- الحفاظ على سلامة الطائرات العسكرية للمملكة المتحدة من الاستهداف بنظم الأسلحة.

والمملكة المتحدة ملتزمة باستخدام قدراتها في مجال الفضاء الإلكتروني بطريقة مسؤولة، بما يتماشى مع قانون المملكة المتحدة والقانون الدولي. ونُفذت العمليات في الفضاء الإلكتروني في الماضي وستظل تنفذ في المستقبل في إطار القوانين القائمة، بما في ذلك قانون أجهزة الاستخبارات لعام 1994 والقانون المنظم لسلطات التحقيق لعام 2016. وهذا يضمن أن تكون عمليات المملكة المتحدة في الفضاء الإلكتروني مسؤولة ومتناسبة ومحددة الأهداف.

واتفقت جميع الدول الأعضاء على أن من مصلحة الدول كلها تشجيع استخدام تكنولوجيات المعلومات والاتصالات للأغراض السلمية. وتؤكد المملكة المتحدة من جديد أن تكنولوجيا المعلومات والاتصالات ليست في حد ذاتها "تهديدا". بل إن التهديد أو الخطر ينشأ عندما تختار دول (أو غيرها من الجهات الفاعلة) أو ينظر إليها على أنها تستخدمها "لأغراض لا تتفق مع السلم والأمن الدوليين". وفي هذا السياق، فإن تعزيز الحوار بشأن كيفية فهم الدول لانطباق القانون الدولي عند التصرف في الفضاء الإلكتروني هو خطوة عملية لزيادة الشفافية والاستقرار والقدرة على التنبؤ.

ويمكن الاطلاع على أحدث المعلومات عن النُهُج التي تتبعها المملكة المتحدة في مجال أمن الفضاء الإلكتروني، بما في ذلك ما يتعلق بالتعاون الدولي، على شبكة الإنترنت على الرابط www.gov.uk/government/cyber-security والموقع www.ncsc.gov.uk.

مضمون المفاهيم المذكورة في تقارير فريق الخبراء الحكوميين

ترحب المملكة المتحدة بأن كلتا العمليتين شهدتا قيام الدول الأعضاء بإعادة تأكيد التقارير الثلاثة السابقة التي صدرت عن فريق الخبراء الحكوميين بتوافق الآراء للأعوام 2010 و 2013 و 2015، والتي أكدت أن القانون الدولي ينطبق على الفضاء الإلكتروني ووضعت إطارا لسلوك الدول المسؤول يتألف من مجموعة من القواعد الطوعية وغير الملزمة وتدابير بناء الثقة، التي يدعمها بناء القدرات. وستكون التقارير الجديدة في عام 2021 مساهمة هامة في هذه المكتسبات.

وترى المملكة المتحدة أن التنفيذ السليم لجميع الدول لكامل الإطار المبين في التقارير الموجودة يوفر نقطة انطلاق عملية لجهودنا الرامية إلى زيادة الاستقرار في الفضاء الإلكتروني. ومن شأن تفعيل عمليات التقييم والتوصيات التراكمية وتعميمها على الصعيد العالمي أن يشكلا خطوة عملية إلى الأمام. ولذلك، يلزم اتباع نُهج عملية وموجهة نحو اتخاذ الإجراءات الملموسة.

التهديدات القائمة والناشئة

فيما يتعلق بالاتجاهات الناشئة، استغل المهاجمون الأزمة خلال جائحة مرض فيروس كورونا (كوفيد-19) في اختيارهم للأهداف، التي شملت المستشفيات وغيرها من البنية التحتية الحيوية المتعلقة بالصحة. واستهدفت الجهات الفاعلة الخبيثة بنشاط المنظمات المشاركة في عمليات التصدي لجائحة كوفيد-19 على الصعيدين الوطني والدولي على حد سواء. وتشمل هذه المنظمات هيئات الرعاية الصحية، وشركات الأدوية، والمؤسسات الأكاديمية، ومنظمات البحوث الطبية، والحكومات المحلية. وكثيرا ما تستهدف هذه الجهات المنظمات من أجل جمع المعلومات الشخصية الضخمة ومعلومات الملكية الفكرية والمعلومات الاستخباراتية التي تتماشى مع الأولويات الوطنية.

وأصبحت البرامجيات الخبيثة أحد أكثر أنواع الحوادث تكرارا التي يتعامل معها المركز الوطني لأمن الفضاء الإلكتروني في المملكة المتحدة وأكثرها إحداثا للاضطرابات. ففي الاستعراض السنوي لعام 2020[10]، لاحظنا أن المركز تصدى لأكثر من ثلاثة أضعاف عدد الحوادث التي وقعت في العام السابق. وشهدت المملكة المتحدة أيضا ارتفاعا حادا في هجمات البرامجيات الخبيثة التي تؤثر على قطاع التعليم في وقت كانت فيه المؤسسات تعمل جاهدة لإدارة التعلم وطلبات التسجيل وإجراءات الاختبار على شبكة الإنترنت. ويرفع المهاجمون بشكل متزايد من حجم الرهانات من خلال التهديد بالتسريب العلني للبيانات المسروقة حين يتردد الضحايا في دفع الفدية. ورأينا أيضا أساليب المهاجمين تزداد تطورا، حيث يظلون في شبكة لمدة طويلة ويبحثون عن البيانات الأكثر قيمة لتشفيرها، وأي معلومات مخزنة بشكل احتياطي على الإنترنت من أجل عرقلة استعادتها.

كيفية انطباق القانون الدولي على استخدام تكنولوجيات المعلومات والاتصالات

تؤكد المملكة المتحدة أن القانون الدولي القائم برمته، بما في ذلك احترام حقوق الإنسان والحريات الأساسية وتطبيق القانون الدولي الإنساني على العمليات المتعلقة بالفضاء الإلكتروني في النزاعات المسلحة، يشكل جزءا من التزامنا المتبادل بالتصرف بمسؤولية في الفضاء الإلكتروني. وينطبق القانون الدولي برمته بنفس الطريقة التي ينطبق بها على أنشطة الدول خارج شبكة الإنترنت.

وفي هذا الصدد، نرحب بدعوة لجنة الصليب الأحمر الدولية إلى أن تؤكد جميع الدول من جديد أن القانون الدولي الإنساني ينطبق على القيام بعمليات في الفضاء الإلكتروني أثناء النزاعات المسلحة. وعندما تقوم الدول بعمليات في الفضاء الإلكتروني، فإن عملياتها ينظمها القانون الدولي تماما مثل الأنشطة في أي مجال آخر. ويوفر تطبيق القانون الدولي الإنساني على العمليات في الفضاء الإلكتروني في النزاعات المسلحة الحماية والوضوح معا. وهو لا يشجع هذه النزاعات ويكفل تطبيق مجموعة المبادئ والقواعد القائمة التي ترمي إلى التقليل إلى أدنى حد من الآثار الإنسانية للنزاعات.

ومع ذلك، نعتقد أننا جميعا بحاجة إلى أن نذهب إلى أبعد من ذلك كدول منفردة وأن نبلور فهمنا الخاص لكيفية انطباق القانون الدولي على الفضاء الإلكتروني. وقد قامت المملكة المتحدة بذلك في عام 2018 عندما حدد النائب العام السابق جيريمي رايت، عضو مجلس الملكة وعضو البرلمان، موقف

(10) www.ncsc.gov.uk/news/annual-review-2020.

المملكة المتحدة بشـــأن تطبيق القانون الدولي على الفضـــاء الإلكتروني. وكانت هذه هي المرة الأولى التي سجل فيها وزير حكومي وجهة نظر المملكة المتحدة في وثيقة.

ونســـلم أيضـــا بالحاجة إلى بناء القدرات فيما يتعلق بالقانون الدولي، بطرق منها التمارين الممكنة المتعلقة بفهمنا لتطبيق القانون الدولي. ويمكن أن يحدث بناء القدرات في هذا المجال أثرا ملموســـا في قدرة الدول على بلورة مواقفها والدفاع عن مصـــالحها الوطنية في المفاوضـــات المقبلة، فضـــلا عن ضـــمان عدم توسيعنا للفجوة الرقمية بهذه الطريقة عن غير قصد.

معايير وقواعد ومبادئ السلوك المسؤول للدول

في أيلول/سبتمبر 2019، قدمت المملكة المتحدة للفريق العامل المفتوح العضوية "ورقة غير رسمية عن الجهود المبذولة لتنفيذ معايير سـلوك الدول المسـؤول في الفضـاء الإلكتروني، على النحو المتفق عليه في تقارير فريق الخبراء الحكوميين التابع للأمم المتحدة للأعوام 2010 و 2013 و 2015"[11]. وتظل هذه الورقة دليلا فعالا للجهود التي تبذلها المملكة المتحدة لتنفيذ معايير الســلوك المســؤول للدول. ورحبنا بتقديم الفريق الاستشاري المتعدد أصحاب المصلحة المعني بقضايا الفضاء الإلكتروني في المملكة المتحدة لورقة تكميلية[12]، تقدم اقتراحات بشـأن الكيفية التي يمكن بها لأصـحاب المصـلحة أن يسـهموا في تنفيذ المعايير دعما للدول.

وتعتقد المملكة المتحدة أنه يجب تنفيذ المعايير لكي تكون فعالة. والعوامل الرئيســية في التنفيذ هي كما يلي:

- الوعي داخل الحكومات وأوساط أصحاب المصلحة للمساعدة على بلورة فهم مشترك لقيمة المعايير وتشجيع اعتمادها.
- الموارد اللازمة لدعم التنفيذ. ويمكن أن يكون تنفيذ المعايير عنصـــرا من عناصـــر أي اســـتراتيجية وطنية لأمن الفضـــاء الإلكتروني وينبغي أن يكون كذلك. وفي عام 2019، لم يكن لدى ســـوى 40 في المائة من الدول مثل هذه الاستراتيجية. وتواصل المملكة المتحدة دعم مجموعة من الدول في بناء قدراتها الوطنية في مجال الفضاء الإلكتروني.
- توافر إرشادات بشأن أفضل الممارسات في التنفيذ. وتعتقد المملكة المتحدة أن تقرير فريق الخبراء الحكوميين سيقدم دليلا مفصلا للإطار الأولي لسلوك الدول المسؤول في الفضاء الإلكتروني الذي طلبته دول عديدة. وتساهم الورقة غير الرسمية والورقة التكميلية المشار إليهما أعلاه أيضا في بناء أفضل الممارسات في هذا المجال.

(11) https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/uk-un-norms-non-paper-oewg-submission-final.pdf.

(12) www.un.org/disarmament/wp-content/uploads/2019/12/efforts-implement-norms-uk-stakeholders-12419.pdf.

تدابير بناء الثقة

ترى المملكة المتحدة أنه ينبغي للدول أن تركز على تنفيذ التدابير القائمة لبناء الثقة بدلا من وضع تدابير جديدة. والمنظمات الإقليمية هي وسائل هامة في تعميم وتنفيذ توصيات أفرقة الخبراء الحكوميين السابقة، إلى جانب القطاع الخاص والأوساط الأكاديمية ومنظمات المجتمع المدني. ومع ذلك، لا يزال تنفيذ تدابير بناء الثقة محدودا، مما يترك ثغرة كبيرة في الفعالية المحتملة لإطارنا.

وتشارك المملكة المتحدة بنشاط في الفريق العامل غير الرسمي المعني بتدابير بناء الثقة في الفضاء الإلكتروني التابع لمنظمة الأمن والتعاون في أوروبا. وقد اعتمدنا التدبير 5 من تدابير هذه المنظمة لبناء الثقة المتعلق ببناء القدرات، وتعهدنا بدعم تفعيله فيما بين دول المنظمة. وفي عام 2019، استضفنا مناقشة بشأن قضايا الفضاء الإلكتروني قائمة على السيناريوهات لممارسة تنفيذ وفهم تدابير بناء الثقة بين 40 دولة عضوا. وفي عامي 2020 و 2021، ترأست المملكة المتحدة لجنة الأمن التابعة لمنظمة الأمن والتعاون في أوروبا، واستخدمت دورها لاستضافة مناسبتين ركزتا على الفضاء الإلكتروني.

بناء القدرات

المملكة المتحدة جهة مانحة رئيسية على الصعيد الثنائي في مجال بناء القدرات المتعلقة بالفضاء الإلكتروني. ونرى أن الأمم المتحدة يمكن أن تستخدم قدرتها على عقد الاجتماعات من أجل إبراز بناء القدرات في مجال أمن الفضاء الإلكتروني وتشجيع الممارسات الجيدة المنسقة. وبغية تحقيق أقصى قدر من الكفاءة والفعالية، سيكون من المهم إشراك جميع أصحاب المصلحة وتجنب ازدواجية العمل الجاري. والمنتدى العالمي المعني بالخبرة في شؤون الفضاء الإلكتروني هو بالفعل آلية تنسيق فعالة لبناء القدرات. والأدوات المستقلة لاستعراض القدرات وأدلة أفضل الممارسات والمنظمات، مثل منتدى الأفرقة المعنية بمواجهة الحوادث وبالأمن في أوساط أفرقة مواجهة حوادث أمن الفضاء الإلكتروني، هي أيضا من المساهمين المهمين في تحقيق هذا الهدف.

وخلال الفترة 2019-2021، كانت المملكة المتحدة راعية لبرنامج زمالات المرأة في مجالي الأمن الدولي والفضاء الإلكتروني. ونحن فخورون بشكل خاص بمساهمتنا في زيادة مشاركة المرأة في الفريق العامل المفتوح العضوية من خلال هذا البرنامج.

الحوار المؤسسي المنتظم

المملكة المتحدة هي إحدى الجهات الراعية لاقتراح وضع برنامج عمل لتيسير إجراء حوار مؤسسي منتظم وشامل بشأن سلوك الدول المسؤول في الفضاء الإلكتروني في الأمم المتحدة. ونؤيد القيام بالمزيد من العمل لصياغة هذا الاقتراح ووضعه.

ثالثا - الردود الواردة من المنظمات الحكومية الدولية

الاتحاد الأوروبي

[الأصل: بالإنكليزية]
[31 أيار/مايو 2021]

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 إنشاء فضاء إلكتروني عالمي مفتوح ومستقر وآمن يقوم على سيادة القانون وحقوق الإنسان والحريات الأساسية والقيم الديمقراطية التي تحقق التنمية الاجتماعية والاقتصادية والسياسية على الصعيد العالمي.

ومع تزايد ترسخ استخدام الإنترنت في حياتنا، ينشأ في الفضاء الإلكتروني عدد من المسائل نفسها التي نواجهها في العالم المادي. ويتزايد استغلال الفضاء الإلكتروني من أجل تحقيق أغراض سياسية وأيديولوجية، وتعوق زيادة الاستقطاب على الصعيد الدولي تعددية الأطراف الفعالة. ويتفاقم مشهد التهديدات بسبب التوترات الجغرافية السياسية بشأن شبكة الإنترنت العالمية والمفتوحة وبشأن السيطرة على التكنولوجيات عبر سلسلة الإمداد بأكملها. ويشكل الاستهداف الخبيث للبنية التحتية الحيوية خطرا عالميا كبيرا. وتهدد قيود شبكة الإنترنت والقيود المفروضة عليها، 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 العالمي والمفتوح، وسيادة القانون والحقوق الأساسية والحرية والديمقراطية. وأعرب الاتحاد الأوروبي والدول الأعضاء فيه بانتظام عن القلق إزاء هذه الأنشطة الخبيثة التي تقوض النظام الدولي القائم على القواعد وتزيد من مخاطر نشوب النزاعات.

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

يؤيد الاتحاد الأوروبي والدول الأعضاء فيه بقوة الرؤية المذكورة آنفاً المتمثلة في فضاء إلكتروني مفتوح وحر ومستقر وآمن، من خلال تعزيز وتطبيق إطار استراتيجي شامل ومتعدد الأوجه لمنع نشوب النزاعات وضمان الاستقرار في الفضاء الإلكتروني، بما في ذلك من خلال 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 بناء الثقة الإقليمية بين الدول. وتعزيز صمود النظم الإلكترونية على الصعيد العالمي عنصر حاسم في الحفاظ على السلام والاستقرار الدوليين، من خلال الحد من خطر نشوب النزاعات وكوسيلة للتصدي للتحديات المرتبطة برقمنة اقتصاداتنا ومجتمعاتنا. ويحد صمود النظم الإلكترونية على الصعيد العالمي من قدرة المخالفين المحتملين على إساءة استخدام تكنولوجيا المعلومات والاتصالات لأغراض خبيثة، ويعزز قدرة الدول على التصدي بفعالية للحوادث الإلكترونية والتعافي من آثارها.

وتمثل استراتيجية أمن الفضاء الإلكتروني المعنونة "فضاء إلكتروني مفتوح وسالم وآمن"[13]، الصادرة في عام 2013، فضلا عن وثائق السياسات اللاحقة والصكوك والاستراتيجيات المذكورة أدناه، الرؤية الشاملة للاتحاد الأوروبي 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 الإجراءات المحددة إلى تعزيز قدرة نظم المعلومات على الصمود في الفضاء الإلكتروني، والحد من الجريمة الإلكترونية، وتعزيز سياسة الاتحاد الأوروبي الدولية لأمن الفضاء الإلكتروني ودفاعه الإلكتروني.

وفي شباط/فبراير 2015، شدد مجلس الاتحاد الأوروبي في استنتاجاته بشأن الدبلوماسية في الفضاء الإلكتروني[14] 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 الإلكترونية، ويمنع نشوب النزاعات، ويوفر الاستقرار في العلاقات الدولية. ويدعو الاتحاد الأوروبي أيضا 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 أيضا على تطبيق القانون الدولي القائم في الفضاء الإلكتروني ومجال الأمن الدولي وأهمية قواعد السلوك، فضلا عن أهمية إدارة الإنترنت باعتبارها جزءا لا يتجزأ من النهج المشترك والشامل للاتحاد الأوروبي في مجال الدبلوماسية في الفضاء الإلكتروني.

واستنادا 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، حددت الرسالة المشتركة المعنونة "القدرة على الصمود والردعُ والدفاع: بناء أمن قوي للفضاء الإلكتروني للاتحاد الأوروبي"[15] حجم التحدي ومجموعة التدابير المتوخاة على صعيد الاتحاد الأوروبي، لضمان أن يكون الاتحاد مستعدا بشكل أفضل لمواجهة تحديات أمن الفضاء الإلكتروني المتزايدة باستمرار.

وأعطت الشواغل بشأن تلك التحديات الزخم لوضع إطار لتصد دبلوماسي مشترك للاتحاد الأوروبي للأنشطة الإلكترونية الخبيثة، وهو مجموعة أدوات الدبلوماسية في الفضاء الإلكتروني[16]. وينبغي أن يكون تزايد قدرة جهات فاعلة حكومية وغير حكومية على تحقيق أهدافها من خلال أنشطة إلكترونية خبيثة، وتعاظم رغبتها في ذلك، مصدر قلق عالمي. وقد تشكل هذه الأنشطة أعمالا غير مشروعة بموجب القانون الدولي وقد 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. وتحقيقا لهذه

(13) 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".

(14) 15/6122 استنتاجات المجلس بشأن الدبلوماسية في الفضاء الإلكتروني.

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

(16) 17/10474. استنتاجات المجلس بشأن إطار لتصد دبلوماسي مشترك للاتحاد الأوروبي للأنشطة الإلكترونية الخبيثة ("مجموعة أدوات الدبلوماسية في الفضاء الإلكتروني").

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 الشريرة على المدى الطويل. كما يوفر التنسيق الواجب مع آليات إدارة الأزمات في الاتحاد الأوروبي، بما في ذلك مخطط التصدي المنسق لحوادث وأزمات أمن الفضاء الإلكتروني الواسعة النطاق. ويدعو الاتحاد الأوروبي والدول الأعضاء فيه المجتمع الدولي إلى تعزيز التعاون الدولي من أجل إنشاء فضاء إلكتروني عالمي مفتوح ومستقر وسلمي وآمن تطبَّق فيه حقوق الإنسان والحريات الأساسية وسيادة القانون تطبيقا كاملا. 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، حدد الاتحاد الأوروبي كذلك استراتيجيته لإحداث تحول رقمي يتسم بأمن الفضاء الإلكتروني في بيئة معقدة من التهديدات[17]. وتهدف استراتيجية الاتحاد الأوروبي لأمن الفضاء الإلكتروني للعقد الرقمي إلى تعزيز وحماية فضاء إلكتروني عالمي مفتوح وحر 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 وتشجيع تهيئة فضاء إلكتروني عالمي مفتوح. ويمكِّن أيضا منع إساءة استخدام التكنولوجيات، وحماية البنية التحتية الحيوية، وضمان سلامة سلاسل الإمداد، الاتحادَ الأوروبي من التقيد بمعايير الأمم المتحدة وقواعدها ومبادئها المتعلقة بسلوك الدولة المسؤول.

وتعزز سياسة الاتحاد الأوروبي الدولية بشأن الفضاء الإلكتروني احترام القيم الأساسية للاتحاد الأوروبي، وتحدد معايير للسلوك المسؤول، وتدعو إلى تطبيق القوانين الدولية القائمة على 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 النهوض بفضاء إلكتروني عالمي مفتوح ومستقر وآمن وتعزيزه، يحترم فيه القانون الدولي، ولا سيما ميثاق الأمم المتحدة، ويُتقيد فيه بالمعايير والقواعد والمبادئ الطوعية غير الملزمة لسلوك الدول المسؤول. ولتشجيع إجراء مناقشة فعالة متعددة الأطراف لتعزيز السلام والأمن في الفضاء الإلكتروني، هناك حاجة واضحة إلى المضي قدما في وضع إطار الأمم المتحدة لسلوك الدول المسؤول في الفضاء الإلكتروني. ويقترح الاتحاد الأوروبي، إلى جانب 53 دولة عضوا في الأمم المتحدة، وضع برنامج عمل للنهوض بسلوك الدول المسؤول في الفضاء الإلكتروني. واستنادا إلى التشريعات القائمة التي أقرتها الجمعية العامة، يوفر برنامج العمل منبرا دائما للتعاون وتبادل أفضل الممارسات داخل الأمم المتحدة. ويتيح هذا البرنامج الفرصة لتعزيز برامج بناء القدرات المصممة خصيصا لتلبية الاحتياجات التي تحددها الدول المستفيدة. ويوفر أيضا آلية مؤسسية داخل الأمم المتحدة لتحسين التعاون مع أصحاب المصلحة الآخرين مثل القطاع الخاص والأوساط الأكاديمية والمجتمع المدني بشأن مسؤوليات كل منها في الحفاظ على بيئة مفتوحة وحرة وآمنة ومستقرة ومتاحة وسلمية لتكنولوجيا المعلومات والاتصالات.

(17) انظر الرسالة المشتركة الموجهة إلى البرلمان الأوروبي والمجلس، بعنوان "استراتيجية الاتحاد الأوروبي لأمن الفضاء الإلكتروني للعقد الرقمي"، و 21/7290 (22 آذار/مارس 2021)، استنتاجات المجلس بشأن استراتيجية الاتحاد الأوروبي لأمن الفضاء الإلكتروني للعقد الرقمي.

مضمون المفاهيم المذكورة في تقارير فريق الخبراء الحكوميين

التهديدات القائمة والناشئة

يقر الاتحاد الأوروبي والدول الأعضاء فيه بأن الفضاء الإلكتروني يتيح فرصا كبيرة للنمو الاقتصادي، فضلا عن التنمية المستدامة والشاملة. ومع ذلك، فإن التطورات الأخيرة في الفضاء الإلكتروني تطرح 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 قبل جهات فاعلة حكومية وغير حكومية على السواء، فضلاً عن زيادة سرقة الملكية الفكرية بوسائل يتيحها الفضاء الإلكتروني. وهذا السلوك يقوض ويهدد النمو الاقتصادي، فضلا عن سلامة المجتمع العالمي وأمنه واستقراره، ويمكن أن يؤدي إلى آثار مزعزعة للاستقرار ومتعاقبة مع زيادة مخاطر نشوب النزاعات.

ومع استمرار جائحة مرض فيروس كورونا (كوفيد-19)، لاحظ الاتحاد الأوروبي والدول الأعضاء فيه تهديدات إلكترونية وأنشطة إلكترونية خبيثة تستهدف المشغلين الأساسيين في الدول الأعضاء وشركاءهم الدوليين، بما في ذلك في قطاع الرعاية الصحية. ومما يثير قلق الاتحاد الأوروبي والدول الأعضاء فيه بشكل خاص الزيادة الأخيرة في الأنشطة التي تؤثر على أمن وسلامة منتجات وخدمات تكنولوجيا المعلومات والاتصالات، التي قد تكون لها آثار عامة.

ويدين الاتحاد الأوروبي والدول الأعضاء فيه هذا السلوك الخبيث في الفضاء الإلكتروني وتشدد على دعمها المستمر لزيادة قدرة النظم الإلكترونية على الصمود على الصعيد العالمي. وأي محاولة لإعاقة قدرة البنى التحتية الحيوية غير مقبولة ويمكن أن تعرض حياة الناس للخطر. ويقوض الاستخدام الخبيث لتكنولوجيات المعلومات والاتصالات الفوائد التي توفرها شبكة الإنترنت واستخدام تكنولوجيا المعلومات والاتصالات للمجتمع ككل، ويظهر استعداد بعض الجهات الفاعلة للمخاطرة بالفعل بالأمن والاستقرار الدوليين. وينبغي لجميع الجهات الفاعلة أن تمتنع عن القيام بأنشطة غير مسؤولة ومزعزعة للاستقرار في الفضاء الإلكتروني.

ويدعو الاتحاد الأوروبي والدول الأعضاء فيه كل بلد إلى بذل العناية الواجبة واتخاذ الإجراءات المناسبة ضد الجهات الفاعلة التي تقوم بهذه الأنشطة انطلاقا من أراضيه، بما يتسق مع القانون الدولي وتقارير أفرقة الخبراء الحكوميين التابعة للأمم المتحدة المعتمدة بتوافق الآراء في أعوام 2010 و 2013 و 2015. ويؤكد الاتحاد الأوروبي والدول الأعضاء فيه مرة أخرى على أنه ينبغي للدول ألا تسمح عن علم باستخدام أراضيها لارتكاب أعمال غير مشروعة دولياً باستخدام تكنولوجيات المعلومات والاتصالات، كما ينبغي لها أن تستجيب للطلبات المناسبة من دولة أخرى للتخفيف من الأنشطة الإلكترونية الخبيثة التي تنطلق من أراضيها.

وبالإضافة إلى ذلك، وكما أقِر بذلك في التقارير السابقة لفريق الخبراء الحكوميين والفريق العامل المفتوح العضوية، ونظرا للطابع الفريد لتكنولوجيات المعلومات والاتصالات، فإن نهج الاتحاد الأوروبي في معالجة المسائل المتعلقة بالفضاء الإلكتروني في سياق الأمن الدولي يجب أن يظل محايدا من الناحية التكنولوجية. وهذا يتسق مع فهم الأمم المتحدة واعترافها بأن القانون الدولي القائم ينطبق على المجالات الجديدة، بما في ذلك استخدام التكنولوجيات الناشئة.

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 وحقوق 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 أن يستند إطار عالمي حقا لأمن الفضاء الإلكتروني إلا إلى القانون الدولي القائم، بما في ذلك ميثاق الأمم المتحدة كله، والقانون الدولي الإنساني، والقانون الدولي لحقوق الإنسان. ويكرر الاتحاد الأوروبي والدول الأعضاء فيه تأكيد انطباق القانون الدولي القائم على سلوك الدول في الفضاء الإلكتروني، على النحو الذي أقر به في تقارير فريق الخبراء الحكوميين في أعوام 2010 و 2013 و 2015، وكذلك المبادئ المنصوص عليها في الفقرات الفرعية 28 (أ) إلى 28 (و) من تقرير عام 2015 والفريق العامل المفتوح العضوية.

وينطبق القانون الدولي، بما في ذلك القانون الدولي الإنساني، الذي يشمل مبادئ الحيطة، والإنسانية، والضرورة العسكرية، والتناسب، والتمييز، على سلوك الدول في الفضاء الإلكتروني وهو قانون يركز على الحماية في مجمله، من خلال وضع حدود واضحة لشرعيته، أيضا في سياق النزاع. ويؤكد الاتحاد الأوروبي اقتناعه بأن القانون الدولي ليس عاملا تمكينيا للنزاعات؛ بل إن القانون الدولي يحدد القواعد التي تنظم 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 والدول الأعضاء فيه بأن مجلس حقوق الإنسان[18] والجمعية العامة قد أكدا أيضا هذه المبادئ.

ولهذه الأسباب، لا يدعو الاتحاد الأوروبي والدول الأعضاء فيه إلى وضع صكوك قانونية دولية جديدة للمسائل المتعلقة بالفضاء الإلكتروني ولا ترى ضرورة لذلك في هذه المرحلة، نظرا للوجود الفعلي لإطار قانوني دولي.

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، فضلا 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

(18) A/HRC/RES/20/8.

استخدام الدول لتكنولوجيات المعلومات والاتصالات، حيث أن ذلك يعزز الشفافية ويقوي الفهم العالمي للنُهُج 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 وقواعد ومبادئ السلوك المسؤول للدول

يشجع الاتحاد الأوروبي والدول الأعضاء فيه جميع الدول على الاستفادة من العمل الذي أقرته الجمعية العامة مرارا، ولا سيما في القرار 237/70، والنهوض به، وعلى مواصلة الاستفادة من الفريق العامل المفتوح باب العضوية، ومن تنفيذ هذه المعايير وتدابير بناء الثقة المتفق عليها، التي تؤدي دورا أساسيا في منع نشوب النزاعات.

وسيسترشد الاتحاد الأوروبي والدول الأعضاء فيه في استخدامها لتكنولوجيات المعلومات والاتصالات بالقانون الدولي القائم، وستلتزم أيضا بالمعايير والقواعد والمبادئ الطوعية للسلوك المسؤول للدول وتنفيذها في الفضاء الإلكتروني، على النحو المبين في التقارير المتعاقبة لفريق الخبراء الحكوميين للأعوام 2010 و 2013 و 2015. ونعتقد أن الطريق العملي للمضي قدما ينبغي أن يشجع على زيادة التعاون والشفافية فيما يتعلق بتبادل أفضل الممارسات، بما في ذلك بشأن كيفية 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

إن الآليات الفعالة للتعاون والتفاعل بين الدول في الفضاء الإلكتروني عناصر حاسمة في منع نشوب النزاعات. وأثبتت المنتديات الإقليمية أنها منبر مهم لتهيئة فضاء للحوار والتعاون بين الجهات الفاعلة التي لها شواغل متقاسمة ومصالح مشتركة من أجل التصدي بفعالية للتحديات من منظور إقليمي.

وسيزيد وضع وتنفيذ تدابير لبناء الثقة في الفضاء الإلكتروني، بما في ذلك تدابير التعاون والشفافية، في 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 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 المخالفين المحتملين على إساءة استخدام تكنولوجيات المعلومات والاتصالات لأغراض خبيثة. وتعزز القدرة على الصمود قدرة الدول على التصدي بفعالية للتهديدات الإلكترونية والتعافي من آثارها.

ويدعم الاتحاد الأوروبي والدول الأعضاء فيه مجموعة من البرامج والمبادرات المصممة خصيصا لمساعدة البلدان في تطوير مهاراتها وقدراتها لمواجهة الحوادث الإلكترونية، فضلا 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 الأعضاء فيه بأن تعزيز قدرات الحماية المناسبة وزيادة مأمونية 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 والمنظمات الدوليين الرئيسيين لدعم بناء القدرات في بلدان ثالثة. ويولي الاتحاد الأوروبي والدول الأعضاء فيه أهمية خاصة لتعزيز الأمن والاستقرار الدوليين في الفضاء الإلكتروني من خلال تشجيع وتيسير اتخاذ إجراءات ملموسة بشأن سلوك الدول المسؤول في الفضاء الإلكتروني، وبتعزيز التعاون في مجال بناء القدرات المتعلقة بالفضاء الإلكتروني، بما في ذلك بدعم من آلية تيسير في الأمم المتحدة بغية تعزيز برامج بناء القدرات المصممة خصيصا لتلبية الاحتياجات التي تحددها الدول المستفيدة، مثل برنامج العمل.