الأمم المتحدة

A/75/123

الجمعية العامة

Distr.: General
23 June 2020
Arabic
Original: Arabic/English/French/
Spanish

الدورة الخامسة والسبعون

البند 98 من القائمة الأولية*

التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي

تقرير الأمين العام

المحتويات

الصفحة

أولا – مقدمة 3

ثانيا – الردود الواردة من الحكومات 3

أرمينيا 3

أستراليا 4

البوسنة والهرسك 6

كندا 12

كولومبيا 15

الدانمرك 30

فرنسا 33

جورجيا 44

هندوراس 49

* A/75/50.

180820 100820 20-08285 (A)

هنغاريا 52
إندونيسيا 55
أيرلندا 58
إيطاليا 63
اليابان 68
المكسيك 71
سنغافورة 76
تركيا 78
أوكرانيا 81
الإمارات العربية المتحدة 88
ثالثا – الردود الواردة من المنظمات الحكومية الدولية 91
الاتحاد الأوروبي 91

أولا - مقدمة

1 - في 12 كانون الأول/ديسمبر 2019، اعتمدت الجمعية العامة القرار 28/74 المعنون "الارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي" في إطار البند 93 من جدول الأعمال، وهو البند المتعلق بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي.

2 - وفي الفقرة 2 من القرار 28/74، دعت الجمعية العامة جميع الدول الأعضاء إلى أن تواصل، آخذة في اعتبارها التقييمات والتوصيات الواردة في التقارير الصادرة عن فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، موافاة الأمين العام بآرائها وتقييماتها بشأن المسائل التالية:

(أ) 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 27 كانون الثاني/يناير 2020 إلى جميع الدول الأعضاء تدعُوها إلى تقديم معلومات بشأن هذا الموضوع. وبسبب الأزمة المستمرة جرّاء مرض فيروس كورونا (كوفيد-19)، وبهدف تيسير تقديم الدول الأعضاء آراءها بشأن المسائل المشار إليها أعلاه، مُدّد الموعد النهائي المحدد لذلك بدايةً، وهو 15 أيار/مايو 2020، ليُصبح 31 أيار/مايو 2020.

4 - وترد الردود التي وردت وقت إعداد التقرير في الفرعين الثاني والثالث. وستُنشر الردود الإضافية الواردة بعد 31 أيار/مايو 2020 في الموقع الشبكي لمكتب شؤون نزع السلاح (www.un.org/disarmament/ict-security) باللغة الأصلية التي وردت بها.

ثانيا - الردود الواردة من الحكومات

أرمينيا

[الأصل: بالإنكليزية]
[13 أيار/مايو 2020]

تولي أرمينيا أهمية كبيرة لانفتاح الفضاء الإلكتروني وحريته واستقراره وأمانه وارتكازه على الامتثال التام لمبادئ وقواعد القانون الدولي وميثاق الأمم المتحدة ككل. وبالنظر إلى عالمية الفضاء الإلكتروني، من المهم حماية حقوق الإنسان والحريات على الإنترنت، وخاصة حرية الرأي والتعبير، وهي تشمل الحق في السعي إلى الحصول على المعلومات وتلقيها ونقلها. ومن جهة أخرى، تنجم عن استخدام تكنولوجيات المعلومات والاتصالات وعن البيئة الإلكترونية تحديات متنوعة واسعة المدى. ولذلك، ينبغي للمجتمع الدولي أن يتضافر في ما يتخذ من تدابير من أجل منع إساءة استخدام تكنولوجيا المعلومات والاتصالات، وأن يُسهم في استخدامها على نحو سلمي وتعاوني. وإذ تضع أرمينيا ذلك في اعتبارها، فهي تشارك بنشاط في المنابر التعاونية الدولية من أجل تعزيز الشفافية وإمكانية التنبؤ والاستقرار في الفضاء الإلكتروني، والحد من المخاطر التي ينطوي عليها استخدام تكنولوجيا المعلومات والاتصالات.

وتلتزم أرمينيا التزاما تاما بالتنفيذ التام لاتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية وبروتوكولها الإضافي المتعلق بتجريم الأفعال المتسمة بطابع العنصرية وكراهية الأجانب المرتكبة عبر النظم الحاسوبية. وتشارك أرمينيا بنشاط منذ عام 2019 في تنفيذ مشروع "سايبر إيست" (CyberEast) المشترك بين الاتحاد الأوروبي ومجلس أوروبا، والهدف من هذا المشروع هو تعزيز القدرات في مجال صمود النظم الإلكترونية والعدالة الجنائية والأدلة الإلكترونية. وتنفذ أرمينيا كذلك بأمانة تدابير بناء الثقة التي وضعتها منظمة الأمن والتعاون في أوروبا (قرار المجلس الدائم 1202) للحد من مخاطر استخدام تكنولوجيا المعلومات والاتصالات. وفي تموز/يوليه 2019، استضافت أرمينيا فريق خبراء من إدارة مكافحة التهديدات عبر الوطنية التابعة لمنظمة الأمن والتعاون في أوروبا لإنجاز تقييم لقدراتها الوطنية في مجال التحقيق في الجرائم الإلكترونية وملاحقة مرتكبيها قضائيا. وفي تشرين الثاني/نوفمبر 2019، نظمت إدارة مكافحة التهديدات عبر الوطنية التابعة لمنظمة الأمن والتعاون في أوروبا اجتماع مائدة مستديرة في يريفان بمشاركة الجهات الأرمنية المعنية لمناقشة نتائج ذلك التقييم معها. واستنادا إلى تقرير الخبراء عن التقييم الذي أنجزوه والاستنتاجات التي خُلص إليها في اجتماع المائدة المستديرة، أعدت إدارة مكافحة التهديدات عبر الوطنية التابعة لمنظمة الأمن والتعاون في أوروبا مذكرة مفاهيمية مكرسة لهذا الموضوع، ويمكن أن تتطور هذه المذكرة لتصبح مشروعا في المستقبل.

وتعبّر محتويات واستنتاجات تقارير فريق الخبراء الحكوميين لعامي 2013 و 2015 عن مواقف عدد محدود من الدول الأعضاء في الأمم المتحدة التي تشارك في عملية إعداد تقارير أفرقة الخبراء الحكوميين، وهي لم تسهم من ثمّ في استحداث مجموعة قواعد عالمية وشاملة تحظى بقبول جميع الدول الأعضاء. وفي هذا السياق، نعتقد أن بوسع الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، بوصفه منتدى للمناقشات بين الدول الأعضاء يتميز بالشمولية والشفافية، أن يضع قائمة موحدة وشاملة من الضوابط والقواعد والمبادئ، المقبولة لدى جميع الدول الأعضاء، لما يشكّل سلوك الدول المسؤول في استخدام تكنولوجيا المعلومات والاتصالات.

أستراليا

[الأصل: بالإنكليزية]
[29 أيار/مايو 2020]

ترحب أستراليا بالفرصة المتاحة لها، عملا بطلب الجمعية العامة الوارد في قرارها 28/74، لتقديم آرائها بشأن الارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي. وتبني الآراء المقدمة هنا على المعلومات التي قدمتها أستراليا في 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.

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، وخاصة ميثاق الأمم المتحدة ككل، في هذا السياق وضرورته لصون السلام والاستقرار ودعم انفتاح بيئة تكنولوجيا المعلومات والاتصالات وأمانها واستقرارها وتيسُّرها وسلميّتها. وتعرض التقارير أيضاً قواعد طوعية غير ملزمة لسلوك الدول المسؤول، وتسلم في الوقت

نفســـه بالحاجة إلى تدابير لبناء الثقة وإلى بناء القدرات على نحو منســـق. وتُتيح هذه التدابير مجتمعة (القانون الدولي، والقواعد، وتدابير بناء الثقة، وبناء القدرات) المرتكز الذي يكفل انفتاح الفضـــاء الإلكتروني وأمانه واستقراره وازدهاره، وكثيرا ما يشار إليها على أنها إطار لسلوك الدول المسؤول.

وتؤكد أستراليا من جديد التزامها بالتصرف وفق مضامين تقارير فريق الخبراء الحكوميين للأعوام 2010 و 2013 و 2015 مجتمعةً (A/65/201؛ A/68/98؛ A/70/174). وتشـارك أسـتراليا بنشـــاط في فريق الخبراء الحكوميين الســـادس، وفي الفريق العامل الافتتاحي المفتوح العضـــوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي (أنشئ فريق الخبراء الحكوميين عملا بالقرار 266/73، بينما أُنشئ الفريق العامل عملا بالقرار 27/73).

القانون الدولي

يردُ موقف أستراليا بشأن أوجه سريان القانون الدولي على سلوك الدول في الفضاء الإلكتروني في اســـتراتيجية العمل الدولي بشـــأن الفضـــاء الإلكتروني (2017) المكمّلة بملحق القانون الدولي لعام 2019 (وكلاهما متاح على الموقع الشـــبكي لوزارة الخارجية والتجارة على الرابط التالي: https://www.dfat.gov.au/sites/default/files/application-of-international-law-to-cyberspace.pdf).

وفي شباط/فبراير 2020، نشرت أستراليا ورقة غير رسمية عنوانها "دراسات حالات إفرادية عن ســـريان القانون الدولي في الفضـــاء الإلكتروني" (وهي متاحة على الموقع الشـــبكي للفريق العامل المفتوح العضـــوية على الرابط التالي: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/australian-international-law-case-studies-final-5-february-2020.pdf)؛ وعلى الموقع الشـــبكي لوزارة الخارجية والتجارة على الرابط التالي: www.dfat.gov.au/sites/default/files/australias-oewg-non-paper-case-studies-on-the-application-of-international-law-in-cyberspace.pdf).

التنفيذ

عملا بدعوة الجمعية العامة جميع الدول الأعضاء في عام 2015 إلى "أن تسترشد في استخدامها لتكنولوجيات المعلومات والاتصالات بتقرير عام 2015 الصادر عن فريق الخبراء الحكوميين" (انظر القرار 237/70)، نشرت أستراليا لمحة عامة عن كيفية امتثال أستراليا وتطبيقها للركائز الأربع الأساسية الواردة في تقرير عام 2015 الصادر عن فريق الخبراء الحكوميين وهي: القانون الدولي، قواعد سلوك الدول المسؤول، وتدابير بناء الثقة، وبناء القدرات (واللمحة العامة متاحة على الموقع الشبكي للفريق العامل المفتوح العضوية على الرابط التالي: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/fin-australian-oewg-national-paper-Sept-2019.pdf؛ وعلى الموقع الشـــبكي لوزارة الخارجية والتجارة في أســـتراليا على الرابط التالي: https://www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/international-security-and-cyberspace).

ويعرض تقرير عام 2015 الصـــادر عن فريق الخبراء الحكوميين الأنشـــطة التي تعد من الممارسات الأفضل التي عملت بها بلدان كثيرة أو هي في طور العمل بها. وتشجع أستراليا جميع البلدان

على تقييم الأنشطة الجارية المتسقة مع تقرير عام 2015 الصادر عن فريق الخبراء الحكوميين (من حيث سريان القانون الدولي، وتطبيق قواعد سلوك الدول المسؤول وتدابير بناء الثقة، وبناء القدرات)، وإيجاد الثغرات والتحديد (إن اقتضى الأمر) لما هي القدرات اللازمة لسد هذه الثغرات. وكان من دواعي سرور أستراليا أن تقدم مع المكسيك و 24 دولة أخرى اقتراحا إلى الفريق العامل المفتوح العضوية (المنشأ عملا بالقرار 27/73) لإجراء دراسة استقصائية عن التنفيذ الوطني لقرار الجمعية العامة 237/70 (المقترح متاح على الموقع الشبكي للفريق العامل المفتوح العضوية على الرابط التالي: https://front.un-arm.org/wp-content/uploads/2020/04/final-joint-oewg-proposal-survey-of-national-implementation-16-april-2020.pdf؛ وعلى الموقع الشبكي لوزارة الخارجية والتجارة على الرابط التالي: https://www.dfat.gov.au/sites/default/files/joint-oewg-proposal-survey-of-national-implementation-april-2020.pdf).

الشؤون الجنسانية

كما هو مسلّم به في الخطة المتعلقة بالمرأة والسلام والأمن، تتأثر المرأة على نحو مختلف ومتفرّد بالنزاعات وبالتهديدات للسلام والأمن الدوليين. وتشيد أستراليا في هذا الصدد بالتقرير الأخير الذي أصدره معهد الأمم المتحدة لبحوث نزع السلاح عن التوازن بين الجنسين في دبلوماسية تحديد الأسلحة ونزعها وعدم انتشارها المعنون "استمرار التخلف عن الركب"، ويرد في هذا التقرير أن اللجنة الأولى لديها أدنى نسبة من الدبلوماسيات مقارنة بأي لجنة من اللجان الرئيسية للجمعية العامة. وثمة مبادرة مشتركة بين حكومات أستراليا والمملكة المتحدة وكندا وهولندا ونيوزيلندا وهي برنامج زمالات المرأة في مجالي الأمن الدولي والفضاء الإلكتروني. وتشجع هذه المبادرة على زيادة مشاركة النساء في المناقشات التي تجري في الأمم المتحدة بشأن قضايا الأمن الدولي المتصلة بسلوك الدول المسؤول في الفضاء الإلكتروني. وستواصل أستراليا اتخاذ خطوات محددة لدعم المشاركة الفعلية والمجدية للنساء في المناقشات المتعددة الأطراف المتعلقة بالأمن الدولي ونزع السلاح.

البوسنة والهرسك

[الأصل: بالإنكليزية]
[11 أيار/مايو 2020]

معلومات عن الجهود المبذولة على الصعيد الوطني في البوسنة والهرسك لتعزيز أمن المعلومات وتشجيع التعاون الدولي في هذا الميدان

أُعدّ هذا التقرير باستقاء البيانات من المؤسسات التالية في البوسنة والهرسك: وزارة الأمن في البوسنة والهرسك، ووزارة الدفاع في البوسنة والهرسك، ووزارة النقل والاتصالات في البوسنة والهرسك، وإدارة الشرطة الاتحادية، ووزارة الداخلية في جمهورية صربسكا، ووزارة التنمية العلمية والتكنولوجية والتعليم العالي ومجتمع المعلومات في جمهورية صربسكا. والمؤسسات المعنية التي لم تقدم بيانات إلى وزارة الأمن في البوسنة والهرسك قبل إحالة هذا التقرير هي: شرطة مقاطعة برتشكو، والوزارة الاتحادية للنقل والاتصالات.

وقد وقّعت البوسنة والهرسك على اتفاقات واتفاقيات دولية متعلقة بالمعلومات وأمن الفضاء الإلكتروني. وأبرزُها الاتفاقية المتعلقة بالجريمة الإلكترونية واتفاق الاستقرار والانتساب. وفُتح باب التوقيع

على الاتفاقية في 23 تشرين الثاني/نوفمبر 2001 في بودابست، وتوصلت هيئة رئاسة البوسنة والهرسك إلى اتخاذ قرار التصديق على هذا الصك في جلستها التاسعة والثمانين المعقودة في 25 آذار/مارس 2006. وبذلك، أصبح لزاما على البوسنة والهرسك أن تعتمد تشريعات وتدابير أخرى ضرورية متعلقة بمكافحة الجرائم الإلكترونية حتى تصبح متسقة مع الدول الأخرى الموقعة على الاتفاقية من حيث ما يتعلق بالمعاملة الجنائية وحيازة البيانات ومعالجتها وتخزينها.

والتشريعات التالية لها أهمية في البوسنة والهرسك من حيث المواضيع المشمولة بالاتفاقية:

- القانون الجنائي للبوسنة والهرسك، الجريدة الرسمية للبوسنة والهرسك، 03/3
- قانون الإجراءات الجنائية، الجريدة الرسمية للبوسنة والهرسك، 03/3، 03/32، 03/36، 04/26، 04/63، 05/13، 05/48، 06/46، 06/76، 07/29، 07/32، 07/53، 07/76، 08/15، 08/58، 09/12، 09/16، 09/93، 13/72
- القانون الجنائي لاتحاد البوسنة والهرسك، الجريدة الرسمية لاتحاد البوسنة والهرسك، 03/36، 04/21، 04/69، 05/18، 10/42، 11/42، 14/59، 14/76، 16/46، 17/75
- قانون الإجراءات الجنائية لاتحاد البوسنة والهرسك، الجريدة الرسمية لاتحاد البوسنة والهرسك، 03/35، 03/37، 03/56، 04/78، 05/28، 06/55، 07/27، 07/53، 09/09، 10/12، 13/08، 14/59
- القانون الجنائي لجمهورية صربسكا، الجريدة الرسمية لجمهورية صربسكا، 17/64، 18/104
- قانون الإجراءات الجنائية لجمهورية صربسكا، الجريدة الرسمية لجمهورية صربسكا، 12/53، 17/91، 18/66
- القانون الجنائي لمقاطعة برتشكو، الجريدة الرسمية لمقاطعة برتشكو، 13/33، 16/26، 17/13، 18/50
- قانون الإجراءات الجنائية لمقاطعة برتشكو، الجريدة الرسمية لمقاطعة برتشكو، 13/33، 14/27، 19/3

على صعيد الدولة

قامت وزارة الأمن في البوسنة والهرسك بالأنشطة المبينة أدناه، بدافع ما أُشير إليه أعلاه وإدراكاً منها للمخاطر التي ينطوي عليها الفضاء الإلكتروني.

وبناء على اقتراح وزارة الأمن في البوسنة والهرسك، اعتمد مجلس وزراء البوسنة والهرسك في جلسته الثالثة والتسعين، المعقودة في 8 آذار/مارس 2017، قرار إنشاء فريق لمواجهة الطوارئ الحاسوبية لمؤسسات البوسنة والهرسك، ونُشر هذا القرار في الجريدة الرسمية للبوسنة والهرسك رقم 17/25، وبذلك نُصّ على تأسيس فريق لمواجهة الطوارئ الحاسوبية وإدماجه في إدارة تكنولوجيا المعلومات ونظم الاتصالات السلكية واللاسلكية بوزارة الأمن في البوسنة والهرسك.

ووفقا للمادة 4 من هذا القرار، يتعين على وزارة الأمن في البوسنة والهرسك أن تعدل تنظيمها الداخلي وهيكلها الوظيفي من أجل كفالة أداء فريق مواجهة الطوارئ الحاسوبية مهامه على النحو السليم. ووردت في أواخر عام 2017 جميع الآراء الضروري تلقيها وفق الإجراء الواجب العمل به عند تغيير التنظيم الداخلي لمؤسسة ما ولهيكلها الوظيفي، وكانت جميع هذه الآراء إيجابية، وأُعدت كذلك جميع الوثائق اللازمة.

وقد أدخلت وزارة الأمن في البوسنة والهرسك التغييرات والتعديلات اللازمة على تنظيمها الداخلي وهيكلها الوظيفي من أجل كفالة أداء فريق مواجهة الطوارئ الحاسوبية مهامه على النحو السليم، وأحالتها إلى مجلس وزراء البوسنة والهرسك ليعتمدها. ولائحة القواعد المقترحة هي الآن في انتظار موافقة مجلس وزراء البوسنة والهرسك عليها. وبعد الحصول على الموافقة، ستشرع وزارة الأمن في البوسنة والهرسك في الإرساء التقني والتشغيلي لفريق مواجهة الطوارئ الحاسوبية لمؤسسات البوسنة والهرسك. ومن التغييرات المقترح إدخالها على التنظيم الداخلي إضافة خمس وظائف إلى الشعبة الجديدة في إدارة تكنولوجيا المعلومات ونظم الاتصالات السلكية واللاسلكية.

وتعتزم وزارة الأمن في البوسنة والهرسك تعزيز فريق مواجهة الطوارئ الحاسوبية من النواحي التشغيلية والمؤسسية والتقنية، بهدف تحقيق الأهداف الاستراتيجية لهذه الكيان (التنسيق والتعاون مع الكيانات المعنية في البوسنة والهرسك، وتبديد وخفض الآثار المترتبة على الحوادث الأمنية الناجمة عن الوصول غير المأذون به إلى نظم تكنولوجيا المعلومات والاتصالات في مؤسسات البوسنة والهرسك، وتعزيز موثوقية نظم تكنولوجيا المعلومات والاتصالات في مؤسسات البوسنة والهرسك من خلال تكريس الجهود لذلك باستمرار، والعمل على منع وقوع الحوادث الأمنية والتقليل من احتمالات وقوعها إلى أقصى حد، ومساعدة المسؤولين الإداريين في تنفيذ التدابير المتعلقة بالحوادث الأمنية، وما إلى ذلك)، وتنفيذ الأنشطة وفقا للمادة 6 من القرار المؤسس للفريق، وإنشاء شبكة لأفرقة مواجهة الطوارئ الحاسوبية في البوسنة والهرسك.

وإضافة إلى ذلك، وبناء على اقتراح وزارة الأمن في البوسنة والهرسك، اعتمد مجلس وزراء البوسنة والهرسك، في جلسته 107 المعقودة في 6 تموز/يوليه 2017، التحليل المتعلق بمواءمة التشريعات في مجال أمن الفضاء الإلكتروني في البوسنة والهرسك، وأمرَ وزارة الأمن في البوسنة والهرسك بتكثيف أنشطتها لصياغة الاستراتيجية المتعلقة بأمن الفضاء الإلكتروني في البوسنة والهرسك.

وبناء على ذلك، تجري حاليا أنشطة للتوفيق بين آراء الكيانات والهيئات فيما يتعلق بنموذج الوثيقة الاستراتيجية التي ستُواكب الأمر التوجيهي الصادر عن الاتحاد الأوروبي بشأن أمن الشبكات ونظم المعلومات من جهة، وستفي بمقتضيات التنظيم الدستوري للبوسنة والهرسك من جهة أخرى.

وشُكّل فريق عامل غير رسمي تحت رعاية منظمة الأمن والتعاون في أوروبا. ويتألف هذا الفريق من ممثلين عن المؤسسات المختصة/المهتمة في البوسنة والهرسك، وقد صاغ الفريق "المبادئ التوجيهية لإطار استراتيجي لأمن الفضاء الإلكتروني في البوسنة والهرسك".

وتشارك وزارة الأمن في البوسنة والهرسك كذلك في الأنشطة الجارية لصياغة الاستراتيجية الجديدة لمنع الإرهاب ومكافحته في البوسنة والهرسك والتي يُفترض أن تتناول استخدام البيئة الرقمية في إنجاز الأعمال المندرجة في هذا الإطار.

وتشارك وزارة الأمن في البوسنة والهرسك بنشاط في أعمال لجنة اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية.

وبناء على اقتراح وزارة الأمن في البوسنة والهرسك، اعتمد مجلس وزراء البوسنة والهرسك، في جلسته الثمانين المعقودة في 10 تشرين الثاني/نوفمبر 2016، قرار إنشاء الفريق العامل المشترك بين الوزارات المعني بتنفيذ مشروع بناء القدرات في مجال الجريمة الإلكترونية (iPROCEEDS) (القرار منشور في الجريدة الرسمية للبوسنة والهرسك رقم 17/14).

وكان الاتحاد الأوروبي ومجلس أوروبا قد وقعا، في كانون الثاني/يناير 2016، اتفاقا بشأن مشروع إقليمي يهدف إلى بناء قدرات بلدان جنوب شرق أوروبا في مجال مكافحة الجريمة الإلكترونية، وهو المشروع المسمى iPROCEEDS، مع التركيز على مصادرة العائدات المتأتية من ارتكاب جرائم على الإنترنت أو جرائم إلكترونية. وكانت مدة المشروع 42 شهرا. وموّل الاتحاد الأوروبي ومجلس أوروبا هذا المشروع، بينما تولى تنفيذه المكتب المعني بالجريمة الإلكترونية الذي يتبع لمجلس أوروبا ويوجد مقره في بوخارست. واقتُرح أن يتألف فريق المشروع الذي يمثل البوسنة والهرسك من ممثلين عن وزارة العدل من ذوي الاختصاص بالجريمة المعنية، أي: مكتب الادعاء العام، والشرطة، وإدارة الاستخبارات المالية، وغيرهم. وقد شُكّل الفريق العامل وفق ذلك.

وعلاوة على ما سبق، تنسق وزارة الأمن في البوسنة والهرسك بين أعضاء فريق مشروع iPROCEEDS-2 بشأن استهداف عائدات الجرائم المرتكبة على الإنترنت وتأمين الأدلة الإلكترونية في جنوب شرق أوروبا وتركيا، وقد انطلق هذا المشروع في كانون الثاني/يناير 2020. وسيبني هذا المشروع على النتائج التي تحققت أثناء تنفيذ مشروع iPROCEEDS، وسيركز على تقديم دعم محدد الأهداف في مجالات المشروع التالية: (أ) التشريعات المتعلقة بتأمين الأدلة الإلكترونية والوصول إلى البيانات في إطار الاحترام التام للحقوق والحريات الأساسية، بما في ذلك حماية الخصوصية والبيانات الشخصية؛ (ب) الاتساق مع قواعد الاتحاد الأوروبي ومجلس أوروبا لحماية البيانات الشخصية؛ (ج) تعزيز السياسات والاستراتيجيات المتعلقة بالجرائم الإلكترونية وأمن الفضاء الإلكتروني؛ (د) التعاون بين الوكالات والقطاعين العام والخاص فيما يتعلق بالتحقيق في الجرائم الإلكترونية والعائدات المتأتية من ارتكاب جرائم على الإنترنت؛ (هـ) نظم الإبلاغ العمومي عن الاحتيال عبر الإنترنت وغيره من الجرائم الإلكترونية؛ (و) التدريب القضائي في مجال الجرائم الإلكترونية والأدلة الإلكترونية والتحقيقات المالية وتدابير مكافحة غسل الأموال المتصلة بذلك؛ (ز) التعاون الدولي وتبادل المعلومات فيما يتعلق بالتحقيق في الجرائم الإلكترونية، وبالعائدات المتأتية من الجرائم المرتكبة على الإنترنت. والمدة المحددة لإنجاز هذا المشروع هي 42 شهرا.

وتقوم وزارة الأمن في البوسنة والهرسك بنجاح بدور المنسق لتنفيذ تدابير منظمة الأمن والتعاون في أوروبا لبناء الثقة. ومن الأنشطة المنجزة في هذه الفترة تقديم التقارير والمعلومات بنجاح عن حالة أمن الفضاء الإلكتروني في البوسنة والهرسك، والمشاركة في أعمال الفريق العامل المشترك بين الوزارات الذي شُكّل بناء على قرار المجلس الدائم 1039، والمشاركة في سبع عمليات للتحقق من حالة الاتصالات، واستضافة تدريب دون إقليمي يتعلق بأمن الفضاء الإلكتروني وتكنولوجيا المعلومات والاتصالات في أيار/مايو 2019، وغير ذلك. وقدمنا أيضا الدعم إلى منظمة الأمن والتعاون في أوروبا من خلال إتاحة قدراتنا ومعارفنا في سياق تنظيم عدة مؤتمرات وحلقات عمل محلية.

وأُشركت البوسنة والهرسك كذلك في المشروع الإقليمي المسمى "بناء قدرات مزاولي أعمال العدالة الجنائية الذين يكافحون الجرائم الإلكترونية والجرائم التي ييسرها الفضاء الإلكتروني في جنوب شرق أوروبا". ومولت حكومتا ألمانيا والولايات المتحدة الأمريكية المشروع، وتتولى تنفيذه إدارة مكافحة التهديدات عبر

الوطنية التابعة لمنظمة الأمن والتعاون في أوروبا، بالتعاون مع ممثلي بلدان المنطقة (ألبانيا، والبوسنة والهرسك، والجبل الأسود، وكوسوفو[1]، وصربيا، ومقدونيا الشمالية) والبعثات الميدانية التابعة لهذه المنظمة. والهدف الرئيسي من هذا المشروع هو تثقيف وتدريب الخبراء الذين يعملون على قضايا الجريمة المنظمة الإلكترونية والقضايا المتصلة بها. وأُنجز المشروع في الفترة 2017-2019، وأسهم في وضع إطار استراتيجي عام وشامل لحل مسائل الجريمة الإلكترونية والتهديدات التي تهدد أمن الفضاء الإلكتروني، وتعزيز القدرات المتوفرة لمكافحة الجريمة الإلكترونية والتصدي للتهديدات التي تهدد أمن الفضاء الإلكتروني. وتولت وزارة الأمن في البوسنة والهرسك دور المنسق لهذا المشروع في البوسنة والهرسك.

ووزارة الدفاع في البوسنة والهرسك في طور إنجاز أنشطة من أجل أن يكون لديها نظام فعال ومستدام لأمن الفضاء الإلكتروني في نطاق سلطتها بحلول عام 2023. ومما أُنجز حتى حينه اعتماد هذه الوزارة في 4 تشرين الأول/أكتوبر 2017 استراتيجية لقطاع الدفاع متعلقة بأمن الفضاء الإلكتروني. واعتُمدت خطة تنفيذية مفصلة لهذه الاستراتيجية في 27 كانون الأول/ديسمبر 2017. وتركز الأهداف الأمنية على منع وقع حوادث أمنية والتصدي لها، وتثقيف الموظفين العاملين في مجال أمن الفضاء الإلكتروني في قطاع الدفاع في البوسنة والهرسك ومنحهم شهادات الكفاءة، وزيادة وعي المستعملين النهائيين بأمن نظم الاتصالات والمعلومات. وبهدف وضع المسائل المبينة أعلاه موضع التنفيذ، أعدت وزارة الدفاع في البوسنة والهرسك وثائق تنفيذية معينة أو اعتمدتها.

وشرعت وزارة الدفاع في البوسنة والهرسك أيضا في عملية إنشاء فريق لمواجهة الطوارئ الحاسوبية تابع لوزارة الدفاع في البوسنة والهرسك.

ووزارة الدفاع في البوسنة والهرسك مُلزمة، في إطار شراكة منظمة حلف شمال الأطلسي من أجل السلام، بتنفيذ الهدف G7300 المحدد للشركاء والمتعلق بالدفاع عن الفضاء الإلكتروني، ويقتضي هذا الهدف ما يلي: (أ) اعتماد سياسات وإجراءات ووثائق أخرى لإدماج الدفاع عن الفضاء الإلكتروني بشكل واضح في العمليات وفي تدابير التخطيط للعمليات، وتوفُّر قواعد تنظيمية دولية في مجال الفضاء الإلكتروني، وتدابير أمنية لتبادل الهيئات الوطنية والدولية العاملة في مجال أمن الفضاء الإلكتروني المعلومات عن المخاطر وتقييم التهديدات التي تهدد الفضاء الإلكتروني؛ (ب) وجود فريق لمواجهة الطوارئ الحاسوبية؛ (ج) إرساء قدرات لضمان سرية وتوافر وسلامة المعلومات ونظم المعلومات في وزارة الدفاع في البوسنة والهرسك والقوات المسلحة للبوسنة والهرسك؛ (د) اعتماد برامج لتثقيف وتدريب الخبراء في هذا الميدان والمستخدمين النهائيين؛ (هـ) إقرار برامج تثقيفية من خلال تنظيم تدريبات وحلقات دراسية وطنية بشأن الفضاء الإلكتروني، ومشاركة ممثلين لموظفي وزارة الدفاع في البوسنة والهرسك والقوات المسلحة للبوسنة والهرسك في تدريبات وحلقات دراسية دولية بشأن الفضاء الإلكتروني.

وبناء على اقتراح من وزارة النقل والاتصالات في البوسنة والهرسك، وبالتعاون مع وزارة الأمن في البوسنة والهرسك، اعتمد مجلس وزراء البوسنة والهرسك، في جلسته الخامسة والتسعين المعقودة في 22 آذار/مارس 2017، سياسة إدارة أمن المعلومات لمؤسسات البوسنة والهرسك للفترة 2017-2022.

وتعمل وزارة النقل والاتصالات في البوسنة والهرسك حاليا، مع وزارة الأمن في البوسنة والهرسك، على إعداد ومواءمة قانون بشأن أمن المعلومات والشبكات ونظم المعلومات وفقا للأمر التوجيهي للاتحاد

(1) هذه الإشارة إلى كوسوفو لا تمسّ الموقف إزاء وضعها.

الأوروبي 1148/2016 بشأن أمن الشبكات ونظم المعلومات. وعملت الوزارة أيضا على تقرير عن نضج القدرة على تقييم قدرات أمن الفضاء الإلكتروني في البوسنة والهرسك، وذلك مع المركز العالمي لقدرات أمن الفضاء الإلكتروني التابع لجامعة أكسفورد، والبنك الدولي، والمركز العالمي للارتقاء بأمن الفضاء الإلكتروني، وجهات أخرى.

وفيما يتعلق بالأنشطة المقبلة، تعتزم وزارة النقل والاتصالات في البوسنة والهرسك اقتراح قانون يتعلق بتحديد الهوية الإلكترونية في مجال الخدمات الاستئمانية للمعاملات الإلكترونية، وصياغة استراتيجية لتنمية مجتمع المعلومات في البوسنة والهرسك.

على صعيد الكيان

اتحاد البوسنة والهرسك

أدركت إدارة الشرطة الاتحادية أهمية أمن الفضاء الإلكتروني، وأنشأت من هذا المنطلق وحدة لمكافحة الجرائم الإلكترونية في عام 2015. ولدى هذه الوحدة ومركز التحليل الجنائي ما يكفي من الموظفين والمعارف والمعدات. ويعمل بهذه الوحدة 10 خبراء، ومركز التحليل الجنائي عضو في الشبكة الأوروبية لمعاهد علوم الأدلة الجنائية. وتشارك هذه المؤسسة أيضا بنشاط في إنجاز مشروع يتعلق بمنع الاستغلال والانتهاك الجنسيين للأطفال في البيئة الرقمية في البوسنة والهرسك، وذلك مع منظمة الأمم المتحدة للطفولة، ورابطة إيمايوس الدولية، ومنظمة إنقاذ الطفولة. وقامت هذه المؤسسة كذلك بدور هام في إنجاز المشاريع المشار إليها أعلاه، مثل مشروع iPROCEEDS والمشروع المسمى "بناء قدرات مزاولي أعمال العدالة الجنائية الذين يكافحون الجرائم الإلكترونية والجرائم التي ييسرها الفضاء الإلكتروني في جنوب شرق أوروبا"، وهي تقوم بدور بالغ الأهمية أيضا في إنجاز المشروع الجديد iPROCEEDS-2.

واعتمد اتحاد البوسنة والهرسك في عام 2018 قرار إنشاء الفريق العامل لمواجهة الطوارئ الحاسوبية لمؤسسات اتحاد البوسنة والهرسك، وحُددت له نفس أهداف وغايات الهيئتين المشار إليهما أعلاه.

جمهورية صربسكا

أبلغت وزارة الداخلية في جمهورية صربسكا عن إنجاز عدد من الأنشطة من أجل مواءمة التشريعات داخل هذا الكيان مع تشريعات الاتحاد الأوروبي. واعتمدت في هذا السياق توجيهات للتطوير للفترة 2017–2021 وخطة عمل لتنفيذ هذه التوجيهات للفترة 2017–2019. واعتمدت كذلك برنامجاً يتعلق بتطوير تكنولوجيا المعلومات والاتصالات للفترة 2017–2021 يتضمن هدفاً يُركز على تحسين نظام المعلومات والاتصالات وتكامله. وتمشيا مع ذلك، حُدّث قانون الشرطة والشؤون الداخلية لجمهورية صربسكا، مما أدى إلى إنشاء آليات لتنفيذ لائحة الاتحاد الأوروبي 2014/910 بشأن تحديد الهوية الإلكترونية والخدمات الاستئمانية للمعاملات الإلكترونية في السوق الداخلية، وأمره التوجيهي 1148/2016 بشأن أمن الشبكات ونظم المعلومات.

وبناء على اقتراح من وزارة الداخلية في جمهورية صربسكا، اعتُمد القانون المتعلق بأمن البنى التحتية الحيوية (الجريدة الرسمية لجمهورية صربسكا، 19/58)، مما وفَّر الأساس لتنفيذ الأمر التوجيهي EC/114/2008 والأمر التوجيهي للاتحاد الأوروبي بشأن أمن الشبكات ونظم المعلومات. وبذلك، أُرسيت قدرات تشريعية، وأُرسي كذلك تعريف لما يشكّل بنى تحتية حيوية في هذا الكيان في سياق مواجهة أي حوادث، بما في ذلك الحوادث المتصلة بالفضاء الإلكتروني.

وشاركت هذه المؤسسة كذلك في المشاريع التالية: مشروع عام 2015 لأداة تقديم المساعدة في مرحلة ما قبل الانضمام، ومشروع "تعزيز جودة وسلامة عمليات تبادل المعلومات بين وكالات إنفاذ القانون في البوسنة والهرسك"، ومشروع "بناء قدرات مزاولي أعمال العدالة الجنائية الذين يكافحون الجرائم الإلكترونية والجرائم التي ييسرها الفضاء الإلكتروني"، ومشروع iPROCEEDS، ومشروع iPROCEEDS-2. وتعمل هذه الوزارة أيضا على إعداد البنى التحتية اللازمة لتبادل البيانات على نحو مأمون مع المؤسسات الأخرى والأشخاص الاعتباريين، وتُقدم خدمات على أساس الآليات الأمنية المحددة في لائحة الاتحاد الأوروبي بشأن تحديد الهوية الإلكترونية والخدمات الاستئمانية للمعاملات الإلكترونية في السوق الداخلية. ويجري كذلك إعداد وثائق متعلقة بتفعيل الآليات الحالية في سياق أمن المعلومات.

ولدى وزارة الداخلية في جمهورية صربسكا أيضا وحدة مكرسة لمكافحة الجرائم الفائقة المستوى التكنولوجي، وهي تعمل، مثلها مثل جميع وكالات إنفاذ القانون الأخرى في البوسنة والهرسك، مع المنظمة الدولية للشرطة الجنائية، ووكالة الاتحاد الأوروبي للتعاون في مجال إنفاذ القانون، ووكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية، ومكتب الأمم المتحدة المعني بالمخدرات والجريمة، ومنظمة الأمن والتعاون في أوروبا، وكلية الشرطة الأوروبية، وسفارة الولايات المتحدة الأمريكية، وبرنامج المساعدة التدريبية في مجال التحقيقات الجنائية الدولية، والرابطة الدولية للشرطة، ومنظمة الأمم المتحدة للطفولة، والعديد من السفارات والمنظمات الدولية الأخرى. ويشمل هذا التعاون مجالات منها التعليم والتدريب وتبادل المعارف والبيانات.

وفيما يتعلق بوجود هيئات إضافية لضمان أمن الفضاء الإلكتروني في البوسنة والهرسك، اعتمد كيان جمهورية صربسكا في عام 2011 القانون المتعلق بأمن المعلومات (الجريدة الرسمية لجمهورية صربسكا، 11/70) الذي يحدد القواعد الأساسية لأمن المعلومات. وعملا بهذا القانون، أُنشئت إدارة أمن المعلومات، أي فريق الاستجابة للطوارئ الحاسوبية، في جمهورية صربسكا ضمن ما كان يُسمى سابقا وكالة مجتمع المعلومات في جمهورية صربسكا (أصبحت هذه الوكالة وزارة التنمية العلمية والتكنولوجية والتعليم العالي ومجتمع المعلومات). وتتولى هذه الهيئة مهمة تنسيق التدابير الوقائية، والحماية من حوادث أمن الحواسيب، وحماية البنى التحتية الإلكترونية للهيئات العمومية والأشخاص الاعتباريين والطبيعيين. وفي السنتين الماضيتين، أنشأت هذه الهيئة مركز عمليات الأمن لحكومة جمهورية صربسكا بهدف تأمين الحماية للبنى التحتية المعنية من منطلق أمن المعلومات. وأُنجزت تدريبات للمشغلين، وبدأ تطبيق نظام عمل ثلاثي النوبات. وتكثف هذه الهيئة مساعيها لتحصل على اعتماد من المنظمات الدولية المعنية أو لتصبح عضوا فيها.

كندا

[الأصل: بالإنكليزية والفرنسية]
[7 أيار/مايو 2020]

فيما يتعلق بأمن الفضاء الإلكتروني:

- تلتزم كندا بتعزيز الاستقرار الدولي، وحرية الفضاء الإلكتروني وانفتاحه وأمانه
- تعتقد كندا أن القانون الدولي يسري على استخدامات الدول لتكنولوجيا المعلومات والاتصالات، وأنه يُعزز استقرار الفضاء الإلكتروني

- تشـــجع كندا الدول على احترام القواعد المتفق عليها لســـلوك الدول في الفضـــاء الإلكتروني، بما في ذلك القواعد المبينة في تقرير عام 2015 لفريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصـــالات الســـلكية واللاســـلكية في ســـياق الأمن الدولي الذي أقرته الجمعية العامة

- تعتقد كندا أن التدابير العملية لبناء الثقة هي طريقة لتعزيز اســـتقرار الفضـــاء الإلكتروني ثبتت جدواها

وعلى الصعيد الوطني، تنشط كندا في هذا السياق بعدد من الطرق:

- في حزيران/يونيه 2018، أصـدرت الحكومة، بقيادة مكتب كندا للسـلامة العامة، اسـتراتيجية كندا الوطنية لأمن الفضـــاء الإلكتروني. وتهدف الاســـتراتيجية إلى تعزيز الشـــراكات لتأمين النظم الإلكترونية الحيوية داخل الحكومة الاتحادية وخارجها، وحماية الكنديين والشـــركات الكندية أثناء اتصـالهم بالإنترنت. وتسـعى الاسـتراتيجية كذلك إلى تعزيز سـبل الكشـف عن التهديدات المتغيرة باسـتمرار التي تهدد الفضـاء الإلكتروني، وتدعيم القدرة على مواجهتها. والاسـتراتيجية منظّمة وفقا لثلاثة أهداف رفيعة هي: (أ) أمان النظم الكندية وقدرتها على الصـــمود؛ (ب) تميُّز المنظومة الإلكترونية بالابتكار والقدرة على التكيف؛ (ج) القيادة والإدارة والتعاون. وتنفذ كندا أهداف هذه الاستراتيجية بواسطة خطة العمل الوطنية لأمن الفضاء الإلكتروني لعام 2019 التي تحدد مبادرات بعينها لتُنفذ على مدى خمس سنوات.

- في إطار تنفيذ الاسـتراتيجية الوطنية لأمن الفضـاء الإلكتروني، أنشـأت كندا المركز الكندي لأمن الفضاء الإلكتروني الذي جمّع الوحدات التنفيذية الحكومية لأمن الفضاء الإلكتروني ضمن مؤسسة عمومية منفردة. وهذا المركز، بصفته فريق كندا لمواجهة الطوارئ الحاسوبية، مصدرٌ موحد لتقديم مشـورة الخبراء والتوجيه والخدمات والدعم إلى الحكومة وأصـحاب ومشـغلي البنى التحتية الحيوية والقطاع الخاص والجمهور الكندي.

- رصـدت الاسـتراتيجية الوطنية لأمن الفضـاء الإلكتروني لعام 2018 تمويلاً لوحدة التنسـيق الوطنية الجديدة المعنية بالجرائم الإلكترونية. وتُدار هذه الوحدة من طرف شـــرطة الخيالة الملكية الكندية، لكنها ستقدم خدماتها إلى جميع وكالات الشرطة الكندية وستعمل مع الشركاء من القطاعين العام والخاص. وتتولى هذه الوحدة، التي ستعمل بكامل طاقتها بحلول عام 2023، تنسيق التحقيقات في الجرائم الإلكترونية وفكّ أوجه التضـارب فيها، مسـتهدفةً ولايات قضـائية متعددة على صـعيد كندا وعلى الصعيد الدولي.

- تلقت شـــرطة الخيالة الملكية الكندية كذلك تمويلاً إضـــافياً في عام 2018 لزيادة القدرة التنفيذية الاسـتخباراتية في مجال التحقيقات ولتعزيز الخبرات التقنية المتخصـصـة لدعم الإجراءات المتخذة ضد الأنشطة الإجرامية الإلكترونية الوطنية والدولية.

وعلى الصعيد الدولي، تنشط كندا في هذا السياق بعدد من الطرق:

- تتواصـــل كندا مع المجتمع الدولي والدول والحلفاء الذين لديهم نفس نظرتها للأمور في منتديات دولية متعددة لتعزيز المحيط الدولي لأمن الفضـــاء الإلكتروني. فعلى ســـبيل المثال، تواصـــل كندا

الترويج لتطوير القانون الدولي واحترام القواعد المتفق عليها لسلوك الدول في الفضاء الإلكتروني، بما في ذلك القواعد التي أقرتها الجمعية العامة والمبينة في تقرير فريق الخبراء الحكوميين لعام 2015. وتشارك كندا أيضا بنشاط في أنشطة الفريق العامل الحالي المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وتقدم آراءها بشأن المناقشات الجارية لفريق الخبراء الحكوميين، حسب الاقتضاء. وتأمل كندا أن يدعم الفريق العامل المفتوح العضوية تنفيذ القواعد المتفق عليها وأن يتناول الجوانب الجنسانية لأمن الفضاء الإلكتروني، بالإضافة إلى مسائل أخرى.

- في المحافل المتعددة الأطراف للأمم المتحدة، تعمل كندا على النهوض بالقواعد والمعايير، وتحث الدول على احترام التزاماتها في مجال حقوق الإنسان. ويشمل ذلك التصدي للعنف ضد النساء والفتيات الذي تيسره تكنولوجيا المعلومات والاتصالات، وضمان أمانهن وسلامتهن الشخصية في سياق الإنترنت وخارجه. وسعت كندا إلى تحقيق هذه الأهداف بطرق شتى، بما في ذلك قيادة عملية اعتماد قرار في مجلس حقوق الإنسان بشأن القضاء على العنف ضد النساء والفتيات في السياقات الرقمية.

- تعمل كندا، مسترشدة بسياستها الدفاعية لعام 2017 التي تحمل شعار "كندا قوية وآمنة ومنخرطة"، على ردع الأنشطة الإلكترونية الخبيثة والتصدي لها بسبل منها تسخير قدراتها الإلكترونية لدعم العمليات العسكرية. وتخضع القدرات الإلكترونية النشطة للقوات المسلحة الكندية لنفس المقتضيات الصارمة التي تخضع لها القدرات العسكرية الأخرى، بما في ذلك القوانين والالتزامات الوطنية والدولية السارية وقواعد الاشتباك.

- في قمة شارلفوا المعقودة في حزيران/يونيه 2018، أعلن قادة مجموعة الدول السبع عن إنشاء آلية الاستجابة السريعة. والآلية مكلفة بتنسيق الجهود التي تبذلها مجموعة الدول السبع للكشف عن التهديدات المتنوعة والمتغيرة التي تواجهها ديمقراطياتنا والتصدي لها، بما في ذلك المعلومات المضللة، وذلك من خلال تبادل المعلومات وإنجاز التحليلات وإيجاد فرص تتيح تنسيق الاستجابات. والهدف المتوخى من الآلية هو التصدي لمجموعة واسعة من التهديدات التي تهدد النظام الديمقراطي، لما فيه صالح أعضاء مجموعة الدول السبع والمجتمع الدولي ككل.

ومن الجهود الدولية الأخرى الجارية ما يلي:

- التزمت كندا منذ عام 2015 بتقديم أكثر من 4 ملايين دولار لدعم مشاريع بناء القدرات في مجال أمن الفضاء الإلكتروني. وموّلت كندا كذلك مشاركة دبلوماسيات من الأمريكتين في الفريق العامل المفتوح العضوية، في إطار برنامج زمالات المرأة في مجال الفضاء الإلكتروني الذي يهدف إلى تعزيز المشاركة المجدية للمرأة في مناقشات الأمم المتحدة بشأن الفضاء الإلكتروني.

- تدعم كندا مساعي منظمة حلف شمال الأطلسي لتعزيز الدفاع عن الفضاء الإلكتروني للحلف وفرادى الحلفاء.

- عملت كندا على تنفيذ تدابير بناء الثقة في مختلف المحافل، بما في ذلك منظمة الأمن والتعاون في أوروبا، ومنظمة الدول الأمريكية، والمنتدى الإقليمي لرابطة أمم جنوب شرق آسيا.

- كندا عضـــو نشـــط في التحالف من أجل الحرية على شـــبكة الإنترنت، وهو منظمة دولية متعددة الأطراف تدعم إعمال حقوق الإنســـان على الإنترنت، حيث ترأس كندا فرقة عمل متعددة الجهات صاحبة المصلحة تُعنى بالذكاء الاصطناعي وحقوق الإنسان.

وتظل كندا ملتزمة بالنهوض بالجهود العالمية لضـمان الأمن والاسـتقرار في الفضـاء الإلكتروني لما فيه صالح الجميع.

كولومبيا

[الأصل: بالإسبانية]
[29 أيار/مايو 2020]

عملا بقرار الجمعية العامة 28/74 المعنون "الارتقاء بسـلوك الدول المسـؤول في الفضـاء الإلكتروني في سـياق الأمن الدولي"، يسُـرّ كولومبيا، آخذة في اعتبارها التقييمات والتوصـيات الواردة في التقارير الصادرة عن فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات، السلكية واللاسلكية في سياق الأمن الدولي، موافاة الأمين العام بآرائها وتقييماتها بشأن المسائل التالية:

- الجهود المبذولة على الصـعيد الوطني لتعزيز أمن المعلومات وتشـجيع التعاون الدولي في هذا الميدان؛
- مضمون المفاهيم المشار إليها في تقارير فريق الخبراء الحكوميين.

مقدمة

تؤيد كولومبيا من منطلق عام أن تكون البيئة الرقمية حرة منفتحة آمنة مكفولٌ فيها حياد الإنترنت، وتعتقد من هذا المنطلق أن من المهم مواصـلة إعطاء الأولوية لبناء القدرات والتعاون على أسـاس القانون الدولي والقواعد والاتفاقات القائمة، ولتنفيذ تدابير بناء الثقة في الفضاء الإلكتروني.

وبذلت كولومبيا جهوداً كبيرة في مجال الفضـاء الإلكتروني بتعزيزها التنسـيق بين الوكالات على أعلى المستويات لكفالة تعزُّز أمن هذا الفضاء.

وعملاً بالسـياسـة العامة للأمن الرقمي المعتمدة في عام 2016، أنشـأت الحكومة الوطنية لجنة الأمن الرقمي التي تشـارك فيها الكيانات المعنية والتي تنسـق الجهود الهادفة إلى مواجهة ما يُحتمل أن يقع من أزمات في أمن الفضـاء الإلكتروني على الصـعيد الوطني. ويرأس اللجنة منسـق وطني يشـغل حاليا منصب المستشار الرئاسي للشؤون الاقتصادية والتحول الرقمي. وتقوم وزارة تكنولوجيا المعلومات والاتصالات بدور الأمانة الفنية لهذه اللجنة.

وينسـق هذا الهيكل المؤسـسـي الجهود الهادفة إلى تفحّص وتحديث السـياسـات والقوانين المتعلقة بالأمن الرقمي، واسـتعراض برنامج العمل الدولي في هذا الصـدد، وكفالة الدفاع والأمن الوطنيين فيما يتعلق بالبيئة الرقمية، وذلك لتوجيه الأنشـطة الهادفة إلى التخفيف من آثار الهجمات الإلكترونية والتصـدي لها، وحماية البنية التحتية الحيوية للبلد، وتعزيز القدرات البشـرية والتقنية والتكنولوجية والمادية على النحو المبين فيما يلي:

- **فريق مواجهة الطوارئ الحاسوبية في كولومبيا** – هو هيئةٌ ضمن وزارة الدفاع تهدف إلى تنسيق الأنشطة اللازم القيام بها لحماية البنية التحتية الحيوية للدولة من أي طوارئ في أمن الفضاء الإلكتروني من شأنها تهديد أو تقويض الأمن والدفاع الوطنيين. وهي مسؤولة عن مواجهة الحوادث المخلة بأمن الحواسيب.

- **القيادة الإلكترونية المشتركة للقوات العسكرية الوطنية** – هي هيئة إشرافية مسؤولة عن توجيه العمليات الإلكترونية المشتركة وتخطيطها وتنسيقها ودمجها وتنفيذها ومزامنتها. وهي مكلفة بتنفيذ تدابير الدفاع الإلكتروني وإنجاز عمليات إلكترونية عسكرية من المستوى الاستراتيجي من أجل كفالة الأمن والدفاع الوطنيين فيما يتعلق بالفضاء الإلكتروني، بما في ذلك التنسيق بشأن البنية التحتية الحيوية.

- **مركز قدرات أمن الفضاء الإلكتروني في كولومبيا التابع لمركز الشرطة الإلكترونية** – هو شعبةٌ ضمن مديرية التحقيقات الجنائية وشؤون المنظمة الدولية للشرطة الجنائية التابعة لجهاز الشرطة الوطني مسؤولةٌ عن وضع استراتيجيات وبرامج ومشاريع متعلقة بالتحقيقات الجنائية لكفالة أمن البيئة الرقمية والفضاء الإلكتروني وحماية معلومات وبيانات سكان البلد المتداولة في الفضاء الإلكتروني.

- **فريق مواجهة الحوادث الأمنية الحاسوبية** – لدى كولومبيا أفرقة لمواجهة الحوادث من هذا القبيل على الصعيد الحكومي والمالي والقطاعي والقطاع الخاص. وعلى صعيد المنطقة، وفي إطار منظمة الدول الأمريكية، كولومبيا عضو في شبكة نصف الكرة الغربي لأفرقة مواجهة الحوادث الأمنية الحاسوبية في الأمريكتين التي تهدف إلى تحسين نشر الإنذارات في المنطقة.

وتتّفق كولومبيا مع ضرورة تعزيز التنسيق والتعاون بين الدول من أجل النظر في ما يوجد من تهديدات وما يمكن اتخاذه من تدابير تعاونية لمواجهتها. ومن المهم بصفة خاصة تعزيز التعاون الدولي، وذلك ليس فقط بنقل المعارف والتكنولوجيات وأفضل الممارسات، بل أيضا بالعمل المشترك المنسق.

ومن الضروري أيضا أن تبرم البلدان الأقل نمواً من الناحية التكنولوجية اتفاقات تحول دون أن يصبح الفضاء الإلكتروني مسرحاً للنزاعات المتصاعدة حدتها لأن ذلك قد يضر بها، سواء نتيجة استهدافها بعمليات إلكترونية أو استخدامها "كدول واسطة" لأنها لا تمتلك القدرة الكافية لاتقاء ذلك.

وفي هذه البلدان، يمكن أن ينجم أثر بالغ عن أي ضرر يلحق ببنية الفضاء الإلكتروني التحتية الحيوية، وذلك ليس فقط بسبب الاعتماد على تكنولوجيات المعلومات والاتصالات والتحول إلى اعتماد التشغيل الآلي للعمليات الصناعية باستخدام التقنيات الموصولة بالإنترنت، ولكن أيضاً بسبب نقص الوعي بالمخاطر والتهديدات والنقص في الموارد اللازمة لتعزيز الأمن الرقمي للشركات التي تدير هذه البنية التحتية.

ولذلك، ينبغي اعتبار نقص القدرات عاملَ خطرٍ يقتضي إقامة آليات للتعاون الدولي لتقصي المخاطر وبناء القدرات.

هذا بالإضافة إلى أن عدم توفر تصنيفات للمخاطر وتدابير وقائية وحمائية فيما يتصل بالأنشطة البالغة الأهمية يطرحُ مخاطر أمام الدول الأقل تقدما في مجال الأمن الرقمي. والافتقار إلى أطر لإدارة الأمن الرقمي، الذي يعوق بدوره التنسيق بين الوكالات والتنسيق الدولي، يُشكل هو أيضا خطراً.

وبالإضافة إلى مواجهة التهديدات الجديدة أو التهديدات التي قد تنشأ في المستقبل نتيجة الوتيرة المذهلة للتطور التكنولوجي، يجب معالجة مسائل سلوك الدول المسؤول في الفضاء الإلكتروني ومسائل أمن المعلومات والاتصالات باتباع نهج عابر للحدود الوطنية حتى يتسنى مواجهة التهديدات بفعالية. ويلزم بذل جهود مشتركة، سواء على مستوى ضمان نشر المعلومات في الوقت المناسب، بما في ذلك التبادل المسؤول للمعلومات عن مواطن الضعف، أو على مستوى مواجهة التهديدات المحتملة بفعالية.

وتؤكد كولومبيا من جديد استعدادها التام للاستمرار في تعزيز التنسيق والتعاون في النظر في ما هو موجود وما هو محتمل من تهديدات وما يمكن اتخاذه من تدابير لمواجهتها، بما في ذلك التعاون.

قواعد سلوك الدول المسؤول وضوابطه ومبادئه الطوعية

تتفق كولومبيا كليا مع المفاهيم والاعتبارات والتفسيرات والتوصيات الواردة في تقارير أفرقة الخبراء الحكوميين، ولا سيما تقرير عام 2015 الذي بنى على عمل الأفرقة السابقة والذي رحبت الجمعية العامة بتوصياته في العام نفسه معتبرة إياها دليلا للدول الأعضاء في استخدام تكنولوجيا المعلومات والاتصالات.

وينبغي أن تركز الجهود في الأجل القريب على تعميم هذه التوصيات وتنفيذها على نطاق واسع. ولا تعتقد كولومبيا أن هناك حاجة في الوقت الحاضر إلى صك ملزم.

والتعاون الدولي أمر هام كذلك إذا ما أُريد تعزيز القدرة الوطنية على تنفيذ التوصيات.

وتؤكد كولومبيا مجددا استعدادها أن تتعاون، بما يتفق ومقاصد الأمم المتحدة، بما فيها مقصد صون السلام والأمن الدوليين، في وضع وتطبيق تدابير لزيادة استقرار وأمن استخدام تكنولوجيات المعلومات والاتصالات ولمنع ما يتصل بتلك التكنولوجيات من ممارسات معروفة بضررها أو باحتمال أن تشكل تهديدات للسلام والأمن الدوليين.

وفي هذا الصدد، أيدت كولومبيا في 23 أيلول/سبتمبر 2019 البيان الذي أعدته الولايات المتحدة الأمريكية بشأن الارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني، والذي يعكس التزاما مشتركا من عدة بلدان بضمان قدر أكبر من المساءلة والاستقرار في الفضاء الإلكتروني من خلال التعاون على نحوٍ الهدف منه مواجهة وردع الأنشطة الخبيثة والمثيرة للاضطرابات والتخريبية والمزعزعة للاستقرار على نحو أكثر فعالية. ويشدد هذا البيان على أن ما يُشكّل سلوك الدول المسؤول في الفضاء الإلكتروني يجب أن ينبني على الاسترشاد بالقانون الدولي، والتقيد بالقواعد الطوعية لسلوك الدول المسؤول في وقت السلم، وتنفيذ تدابير عملية لبناء الثقة.

وتدعم كولومبيا أيضاً نداء باريس من أجل الثقة والأمن في الفضاء الإلكتروني، وهي مبادرة أطلقتها حكومة فرنسا في 12 تشرين الثاني/نوفمبر 2018، وتشجع هذه المبادرة على وضع مبادئ مشتركة لتعزيز أمن الفضاء الإلكتروني، وقد حظيت بتأييد بلدان وشركات خاصة ومنظمات مجتمع مدني متعددة.

وبالإضافة إلى ذلك، تؤيد كولومبيا نداء كرايستتشيرش للقضاء على المحتوى الإرهابي والذي يتسم بالتطرف العنيف على الإنترنت، وهي مبادرة من حكومتي فرنسا ونيوزيلندا أُطلقت في أيار/مايو 2019.

ولدى كولومبيا سياسات عامة تسري على الصعيد الوطني، وهي ترد في وثائق المجلس الوطني للسياسات الاقتصادية والاجتماعية. وفي عام 2011، أضفت كولومبيا الطابع الرسمي على سعيها لإقرار أن

يصبح أمن الفضاء الإلكتروني والدفاع عنه من أركان الدفاع الوطني. وفي هذا السياق، أصدرت الحكومة الوطنية وثيقة المجلس الوطني للسياسات الاقتصادية والاجتماعية رقم 3701، المعنونة "المبادئ التوجيهية لسياسة أمن الفضاء الإلكتروني والدفاع عنه"، وهدفها العام هو تعزيز قدرة الدولة على مواجهة التهديدات التي تهدد الأمن والدفاع الوطنيين فيما يتعلق بالفضاء الإلكتروني (أمن الفضاء الإلكتروني والدفاع عنه) حتى يتسنى تهيئة بيئة وظروف يكون الفضاء الإلكتروني فيها محمياً. وأُحرز تقدم في ثلاثة مجالات رئيسية هي: (أ) إنشاء هيئات تركز في عملها على مواجهة الحوادث الأمنية الإلكترونية، وإصدار مبادئ توجيهية لتعزيز قدرة الدولة على مواجهة التهديدات في الفضاء الإلكتروني؛ (ب) إنشاء آليات للتدريب في مجال أمن المعلومات وتوسيع نطاق الأبحاث المتصلة بهذا الشأن؛ (ج) تعزيز قوانين أمن الفضاء الإلكتروني.

وفي عام 2016، أصدرت الحكومة وثيقة المجلس الوطني للسياسات الاقتصادية والاجتماعية رقم 3854، المعنونة "السياسة الوطنية للأمن الرقمي"، وتتمحور هذه السياسة حول أربعة أهداف رئيسية هي: (أ) تعزيز الإطار المؤسسي؛ (ب) تعزيز قدرات مختلف الجهات المعنية في مجال تحديد المخاطر التي تهدد السلامة الرقمية في سياق أنشطتهم الاجتماعية والاقتصادية على الإنترنت، وفي مجالات إدارة هذه المخاطر ومواجهتها والتخفيف من آثارها؛ (ج) تعزيز تقاسم المسؤولية؛ (د) الأخذ بنهج لإدارة المخاطر في الأنشطة الإلكترونية لمختلف الجهات المعنية.

وتعمل الحكومة منذ عام 2019 على وضع سياسة عامة بشأن الثقة والأمن الرقميين، ومن الغايات التي تتوخاها هذه السياسة تقييم وتحديث إطار إدارة الأمن الرقمي لكي يتحسّن. وتنص هذه السياسة على إنشاء نظام وطني لإدارة الحوادث الأمنية الإلكترونية يهدف إلى تحقيق الأهداف التالية: (أ) تنسيق الجهود المؤسسية بما يضمن إدارة الحوادث الأمنية الإلكترونية في الوقت المناسب؛ (ب) العمل بوصفه المصدر الرسمي لإحصاءات الحوادث الأمنية الإلكترونية المبلّغ عنها في البلد؛ (ج) إرساء آلية موحّدة للإبلاغ الدوري بالحوادث وبمواطن الضعف حتى يتسنى الوقوف عليها وتقييمها وإبلاغ الجهات المعنية بها؛ (د) توفير معلومات لتسترشد بها الحكومة الوطنية في اتخاذ القرارات. ونخطط حاليا لإرساء التكنولوجيا التي يقوم عليها هذا النظام. وسيُتاح لأجهزة أمن الدولة أن تطلع على المعلومات الموجودة في هذا النظام في الوقت الحقيقي.

وأُدرج التعاون الدولي في المسائل الأمنية وتسخير الابتكار والعلم والتكنولوجيا لتعزيز قدرات قطاع الدفاع ضمن أهداف التحول الاستراتيجي المحددة في المبادئ التوجيهية للسياسات الدفاعية والأمنية.

وتبذل كولومبيا مساع دبلوماسية في مجالي أمن الفضاء الإلكتروني والدفاع عنه في إطار الأمن التعاوني من خلال شراكات دولية استراتيجية. فعلى سبيل المثال، تتبادل كولومبيا المعارف بوصفها شريكا عالميا لمنظمة حلف شمال الأطلسي؛ وتعمل، في إطار البرنامج الفردي للشراكة والتعاون، على تعزيز قدرات القوات العسكرية الوطنية وجهودها المنسقة لمواجهة التهديدات وحماية الفضاء الإلكتروني.

ووضعت كولومبيا مبادئ توجيهية بالاستناد إلى أفضل الممارسات والمعايير الدولية لإنشاء وتشغيل أفرقة مواجهة الحوادث الأمنية الحاسوبية للقطاعين العام والخاص والقطاع المختلط الجامع بينهما، وذلك لإتاحة الإدارة التنفيذية فيما يتعلق بالحوادث الأمنية الإلكترونية التي تمسّ المصالح الوطنية؛ وتعزيز التعاون والتآزر والتعاضد الدولي في مجال الأمن الرقمي وأمن الفضاء الإلكتروني والدفاع عنه مع أعضاء أفرقة مواجهة الحوادث الأمنية الحاسوبية في الأمريكتين وأوروبا؛ وتبادل الخبرات وأفضل الممارسات.

وتشـــارك القيادة الإلكترونية المشـــتركة في المنتدى الأيبيري – الأمريكي للدفاع عن الفضـــاء الإلكتروني من أجل تعزيز التعاون، وتبادل الدروس المستفادة، وتعزيز القدرة على إدارة المخاطر والتهديدات عبر الوطنية في الفضاء الإلكتروني، والمشاركة في التدريبات الوطنية والدولية.

ومن خلال مركز قدرات أمن الفضـــاء الإلكتروني في كولومبيا، يُنجز مركز الشـــرطة الإلكترونية التحليلات، ويُصـــدر إنذارات للوقاية، ويُشـــارك في الأنشـــطة المرتبطة بإدارة الحوادث الأمنية الإلكترونية، ويُجري التحقيقات في الجرائم الإلكترونية.

وتتمثل أهداف لجنة تنظيم الاتصالات في ما يلي: (أ) إقامة آليات لتعزيز التعاون في مجال الأمن الرقمي بين الجهات المقدمة لخدمات الاتصـــالات وفريق مواجهة الطوارئ الحاســـوبية في كولومبيا؛ (ب) تجميع المعلومات القطاعية عن حوادث أمن المعلومات في الكيان المسـؤول عن إدارة هذه المعلومات؛ (ج) تزويد فريق مواجهة الطوارئ بالمعلومات اللازمة لإدارة الحوادث والتوعية بها لفائدة مختلف المعنيين.

ولذلك، أصدرت لجنة تنظيم الاتصالات القرار رقم 5569 لعام 2018 الذي ينص على ضرورة أن تعمل كل شـــبكة اتصـــالات وكل جهة مقدمة لخدمات اتصـــالات بنظامٍ لإدارة أمن المعلومات وأن تعدل عملياتها بما يضمن سلامة البيانات وسريتها وتوفرها.

وتجدر الإشـارة إلى أن سـياسـة الأمن الرقمي أخذت في الاعتبار التوصـيات التي قدمتها منظمة التعاون والتنمية في الميدان الاقتصـــادي في الوثيقة المعنونة "إدارة المخاطر المحدقة بالأمن الرقمي لكفالة الرخاء الاقتصادي والاجتماعي".

وتوصي المنظمة في هذه الوثيقة بأن عملية إدارة مخاطر الأمن الرقمي ينبغي أن تبدأ بتحديد الأهداف الاقتصـــادية والاجتماعية أو بوضـــع أنشـــطة محددة، بحيث يمكن، خلال مرحلة إدارة المخاطر، تقييم مســـتوى الخطر المرتبط بالنشاط والتعرف على الأثر المحتمل لهذا الخطر على الأهداف الاقتصادية والاجتماعية.

وبعـد ذلـك، ينبغي للمعنيين أن يحـددوا، أثنـاء مرحلـة مواجهـة المخـاطر، كيف ينبغي تعـديـل الاســتراتيجيات حتى يزيد احتمال نجاح النشــاط وتُصــان الأهداف المحددة، وذلك بتقرير ما إذا كان ينبغي قبول الخطر أو الحد منه أو تحويله أو تجنبه. وللحد من الخطر، يمكنهم اختيار تدابير أمنية والعمل بها أو النظر في تدابير مبتكرة وتدابير للتأهب.

وبناء على ذلك، وفي حالة وقوع حوادث في ميدان تكنولوجيا المعلومات والاتصـــالات، تنظر كولومبيا في جميع المعلومات ذات الصـــلة، بما في ذلك الســـياق الأوســـع للحادث، وتحديات تحديد الجهة الفاعلة في بيئة تكنولوجيات المعلومات والاتصالات، وطبيعة العواقب ومداها.

وفيما يتعلق بتوصيف الحوادث ولزوم إبلاغ السلطات المختصة بها، راعت لجنة تنظيم الاتصالات أيضـــا في تحديد فئات حوادث أمن المعلومات، الواردة في القرار رقم 5569 لعام 2018، المبادئ التوجيهية وأفضـــل الممارســـات الواردة في مجموعة المقاييس 27000 التي وضـــعتها المنظمة الدولية لتوحيد المقاييس واللجنة الكهربائية التقنية الدولية (ولا ســـيما الفئات المحددة تحت المقياس رقم 1-27035). وبموجب ذلك القرار، عندما تقع حوادث في ميدان أمن المعلومات، يتعين على شـــبكات الاتصـــالات والجهات المقدمة لخدمات الاتصـالات أن ترسـل تقريرا إلكترونيا إلى فريق مواجهة الطوارئ الحاسـوبية في كولومبيا بعد احتواء الخطر والقضاء عليه والتعافي من مفعوله.

وعملا بالتوصية التي تدعو الدول إلى عدم السماح عن علم باستخدام أراضيها لارتكاب أفعال غير مشروعة دولياً باستخدام تكنولوجيات المعلومات والاتصالات، تعمل دولة كولومبيا على منع وقوع حوادث أمنية إلكترونية من جميع التصنيفات والأنواع في جميع أنحاء البلد وتتصدى لها بواسطة لجنة الأمن الرقمي التي تضم في عضويتها كيانات الدولة لأمن الفضاء الإلكتروني مثل فريق مواجهة الطوارئ الحاسوبية في كولومبيا، والقيادة الإلكترونية المشتركة، ومركز الشرطة الإلكترونية، والفريق الحكومي لمواجهة الحوادث الأمنية الحاسوبية.

وتسعى كولومبيا إلى التعاون على الصعيد الدولي عن طريق تبادل المعلومات والمساعدة، والملاحقة القضائية للإرهابيين ولاستخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية، والعمل بتدابير تعاونية أخرى لمواجهة التهديدات.

وفي هذا الصدد، تنص الوثيقة الجديدة للمجلس الوطني للسياسات الاقتصادية والاجتماعية، التي تتعلق بالثقة والأمن الرقميين والجاري إعدادها حاليا، على إنشاء وتطبيق نظام لتبادل المعلومات عن الفضاء الإلكتروني يهدف إلى تيسير نشر مؤشرات التعرض للخطر على الجهات المعنية الناشطة في البيئة الرقمية على الصعيدين الوطني والدولي. وسيُواءم هذا النظام مع السجل المركزي المنفرد لحوادث الأمن الرقمي.

ويستخدم مكتب المدعي العام قنوات التعاون الدولي وفقا للاتفاقات الثنائية والمتعددة الأطراف. غير أنه يلزم إقامة قناة تكنولوجية أو خدمة شبكية مأمونة لتمكينه من أن يقوم مباشرة باستشارة الجهات المقدمة لخدمات الإنترنت، ومعظمها من القطاع الخاص، والحصول على المعلومات منها، بحيث يمكن إرسال طلبات تبادل المساعدة القانونية وتلقيها وتبادلها والنظر فيها والاستجابة لها في الوقت المناسب.

فأوقاتُ الاستجابة في ظل الآليات القائمة حاليا بطيئة، وهو ما يعرقل الدعاوى الجنائية. وعندما يردُ الردّ، يكون التحقيق في كثير من الأحيان قد بلغ مرحلة لا تسمح باستخدام ما وردَ في الدعاوى.

وتنسق مديرية الاستخبارات الوطنية مع أجهزة الاستخبارات في بعض البلدان بشأن تحديد عملية لتبادل المعلومات العملياتية في الوقت المناسب، وبشأن طلب معلومات إضافية متصلة بحوادث محددة تتطلب التحقيق فيها أو تأكيدها.

ويتعلق هذا التنسيق بمعلومات إضافية متصلة بحوادث أو اتجاهات يتم الوقوف عليها في الفضاء الإلكتروني ويلزم ربط الأحداث أو سجل الأنشطة بخصوصها حتى يُمكن مراقبة العناصر العدوانية الناشطة في الفضاء الإلكتروني.

وأصدرت المحكمة الدستورية في كولومبيا عددا من الأحكام المتصلة بالتوصية التي تنص على أنه ينبغي للدول، في سعيها لضمان الاستخدام الآمن لتكنولوجيات المعلومات والاتصالات، أن تحترم قراري مجلس حقوق الإنسان 8/20 و 13/26 بشأن تعزيز وحماية حقوق الإنسان على الإنترنت والتمتع بها، وقراري الجمعية العامة 167/68 و 166/69 بشأن الحق في الخصوصية في العصر الرقمي، لضمان الاحترام التام لحقوق الإنسان، بما في ذلك الحق في حرية التعبير.

وعلى سبيل المثال، رأت المحكمة في الحكم الموحد رقم SU-420 لعام 2019 أن حرية التعبير في كولومبيا تسري على الإنترنت مثل سريانها على وسائل الاتصال الأخرى، وخلُصت إلى أن شبكات التواصل الاجتماعي لا يمكنها كفالة متسع يُتيح التشهير؛ ورغم أنه من غير الممكن إخضاع نشر المحتوى

لإذن أو ترخيص مسبق، فوضعُ الأولوية المخول لحرية التعبير لا يعني أنها بلا حدود؛ وبالتالي فإن أي شخص يمارس هذا الحق يخضع للعواقب التي تنشأ عن أي أثر يلحق بأطراف أخرى.

وأصدرت لجنة تنظيم الاتصالات القرار رقم 5111 لعام 2017 الذي حددت فيه خطة لحماية حقوق مستخدمي خدمات الاتصالات، وعدّلت الفصل الأول من الجزء الثاني من قرارها رقم 5050 لعام 2016، إضافة إلى تحديدها أحكاماً أخرى. وبموجب خطة حماية حقوق مستخدمي خدمات الاتصالات، يتعين على شبكات الاتصالات والجهات المقدمة لخدمات الاتصالات أن يستخدموا الأدوات التكنولوجية المناسبة لمنع التلاعب ضمن شبكاتهم وأن يتحققوا دوريا من فعالية هذه الأدوات. وإذا قدّم مستخدم طلباً أو شكوى أو مطالبة أو التماسا يتعلق بحالة تلاعب مزعوم، فيجب على الجهة المقدمة للخدمات أن تحقق في ذلك.

ومن أجل تحديد ما هي الإصلاحات القانونية والتنظيمية اللازمة لتعزيز الأمن الرقمي وبناء القدرات، تنص السياسة الجديدة المتعلقة بالثقة والأمن الرقميين على إجراء تقييم لتحديد الصكوك التي تتطلب تعديلات في مجالات مثل: (أ) أمن تكنولوجيا المعلومات والاتصالات؛ (ب) حماية الخصوصية والدفاع عنها وحرية التعبير وغير ذلك من حقوق الإنسان على الإنترنت؛ (ج) الإبلاغ المسؤول عن مواطن الضعف؛ (د) حماية البيانات؛ (هـ) حماية المستهلكين؛ (و) إدارة المخاطر والحوادث؛ (ز) مراكز مواجهة الحوادث أو غيرها من الكيانات ذات الصلة بهذا الشأن؛ (ح) إنشاء أفرقة قطاعية لمواجهة الحوادث الأمنية الحاسوبية. وسيأخذ هذا التقييم في الاعتبار مختلف الجهات المعنية، وسيحدد كيفية إجراء التعديلات اللازمة.

وعملا بالتوصية التي تدعو الدول إلى اتخاذ التدابير المناسبة لحماية بنيتها التحتية الحيوية من تهديدات تكنولوجيا المعلومات والاتصالات، تسعى كولومبيا إلى وضع خطة أمنية ودفاعية متعلقة بالبنية التحتية الحيوية من أجل قطاع تكنولوجيا المعلومات والاتصالات، وذلك بالتنسيق مع مختلف الجهات المعنية، وستُحدَّد في هذه الخطة مبادئ توجيهية عامة من أجل مؤسسات هذا القطاع. وستكون هذه الوثيقة خطوة أولية نحو تعزيز وتنسيق الجهود الهادفة إلى حماية هذه البنية التحتية.

وتتعاون كولومبيا دولياً وتستجيب للطلبات التي تتلقاها من دول أخرى من أجل التخفيف من آثار الأنشطة الخبيثة في مجال تكنولوجيا المعلومات والاتصالات. فعلى سبيل المثال، انضمت كولومبيا في 16 آذار/مارس 2020 إلى الاتفاقية المتعلقة بالجريمة الإلكترونية. واتخذت أيضا خطوات لكفالة سلامة سلسلة الإمداد حتى يمكن للمستخدمين النهائيين الوثوق بأمن منتجات تكنولوجيا المعلومات والاتصالات.

وفيما يتعلق بالإبلاغ المسؤول عن مواطن الضعف في تكنولوجيات المعلومات والاتصالات والموافاة بما يرتبط بذلك من معلومات عن سبل التقويم المتاحة لمواطن الضعف هذه حتى يتسنى الحد من احتمالات تعرض تكنولوجيات المعلومات والاتصالات والبنية التحتية المعتمِدة على هذه التكنولوجيات للخطر، وتبديد هذه الاحتمالات إذا أمكن، تنصُّ السياسة الجديدة بشأن الثقة والأمن الرقميين على وضع عملية لتعزيز الإبلاغ المسؤول عن مواطن الضعف في نظم المعلومات والبنية التحتية التكنولوجية لكيانات الدولة حتى يُمكن للكيان المعني أن يقوّمها.

وبالإضافة إلى ذلك، أصدرت الحكومة الوطنية، من خلال وثيقة المجلس الوطني للسياسات الاقتصادية والاجتماعية رقم 3854 لعام 2016، مبادئ توجيهية لإنشاء أفرقة مواجهة الطوارئ الحاسوبية وأفرقة مواجهة الحوادث الأمنية في الفضاء الإلكتروني.

تدابير بناء الثقة الطوعية

كولومبيا ملتزمة التزاماً راسخاً بمواصلة وضع واعتماد تدابير لتعزيز الثقة والأمن في الفضاء الإلكتروني. وأُنجزت أعمال في هذا السياق على الصعيد الإقليمي من خلال منظمة الدول الأمريكية.

ففي نيسان/أبريل 2017، قادت شيلي وكندا وكولومبيا والمكسيك والولايات المتحدة عملية اتخاذ القرار المتعلق بإنشاء فريق عامل معني بالتعاون وتدابير بناء الثقة في الفضاء الإلكتروني ضمن لجنة البلدان الأمريكية لمكافحة الإرهاب التابعة لمنظمة الدول الأمريكية. وفي شباط/فبراير 2018، انتُخبت كولومبيا رئيسة لهذا الفريق العامل. وفي الاجتماع الثاني لهذا الفريق، الذي عقد في شيلي في نيسان/أبريل 2019، خلفت شيلي كولومبيا في منصب رئاسة الفريق.

وفيما يلي تدابير بناء الثقة التي اعتمدتها منظمة الدول الأمريكية في مجال أمن الفضاء الإلكتروني:

1 - تقديم معلومات عن السياسات الوطنية لأمن الفضاء الإلكتروني، مثل الاستراتيجيات الوطنية، والكتب البيضاء، والأطر القانونية، وغيرها من الوثائق التي تعتبرها كل دولة عضو ذات صلة؛

2 - تحديد جهة اتصال وطنية معنية بالسياسات العامة قادرة على مناقشة الآثار المترتبة على التهديدات الإلكترونية في نصف الكرة الغربي؛

3 - تعيين جهات اتصال، في حالة عدم وجودها، داخل وزارات الخارجية، بغرض تيسير العمل على التعاون والحوار الدوليين في مجالي الفضاء الإلكتروني وأمنه؛

4 - تطوير وتعزيز بناء القدرات من خلال أنشطة مثل الحلقات الدراسية والمؤتمرات وحلقات العمل بشأن دبلوماسية الفضاء الإلكتروني لفائدة موظفي القطاعين العام والخاص؛

5 - تشجيع إدراج المواضيع المتعلقة بالفضاء الإلكتروني وأمنه في الدورات التدريبية للدبلوماسيين والمسؤولين في وزارات الخارجية والوكالات الحكومية الأخرى؛

6 - تشجيع التعاون وتبادل أفضل الممارسات المتعلقة بدبلوماسية الفضاء الإلكتروني، والفضاء الإلكتروني وأمنه من خلال إنشاء أفرقة عاملة، وآليات أخرى للحوار، وتوقيع اتفاقات بين الدول.

وتشكّل تدابير بناء الثقة المتصلة بدبلوماسية الفضاء الإلكتروني، على وجه التحديد، إسهاماً هاماً يجري عن طريق منظمة الدول الأمريكية.

ومن خلال دبلوماسية الفضاء الإلكتروني، يُمكن إيجاد سبل لمواجهة تحديات أمن الفضاء الإلكتروني. ولا يتطلب ذلك تعزيز المشاركة النشطة للدول في المناقشات الدولية بشأن أمن الفضاء الإلكتروني فحسب، وهذا هدف يقتضي بدوره توفير التدريب المناسب للمسؤولين الدبلوماسيين، بل يتطلب ذلك أيضاً كفالة المشاركة النشطة للخبراء في المنتديات المتعددة الأطراف.

وينبغي إيلاء الاعتبار لتشجيع الإجراء المنتظم لحوارات مؤسسية والمشاركة الواسعة فيها، وتوسيع ودعم الممارسات المتعلقة بالتعاون بين أفرقة مواجهة الطوارئ الحاسوبية وأفرقة مواجهة الحوادث الأمنية في الفضاء الإلكتروني.

وفيما يتعلق بالاقتراح الداعي إلى إعداد قائمة شاملة لجهات الاتصال، ينبغي تعيين جهات اتصال على مستويات مختلفة، كأن تُعيَّن جهة اتصال واحدة على المستويين السياسي والدبلوماسي وجهات اتصال أخرى على المستوى التقني (مقررو السياسات، ومكاتب المدعين العامين، وأفرقة مواجهة الطوارئ الحاسوبية، وما إلى ذلك).

وسيكون من المهم تحديد من سيتولى إدارة المعلومات وكفالة تحديثها. وينبغي النظر في وضع بروتوكول لإدارة المعلومات إدارة واضحة ومنفتحة، وذلك بما يشمل إدارة قواعد البيانات.

وفيما يتعلق بتحديد جهات اتصال وطنية على المستويين التقني والسياساتي لمواجهة حوادث تكنولوجيا المعلومات والاتصالات الخطيرة، حددت وزارة تكنولوجيا المعلومات والاتصالات بوضوح الأفراد المسؤولين عن معالجة كل بعد من أبعاد الأمن الرقمي. ويمكن تبادل البيانات في هذا الصدد مع أي هيئات تحتاج إليها.

ولدى وزارة تكنولوجيا المعلومات والاتصالات أيضا دليل يتضمن معلومات الاتصال برؤساء موظفي شؤون المعلومات وبرؤساء موظفي شؤون أمن المعلومات في كيانات الدولة، وبمختلف الجهات المعنية التي شاركت في المناقشات بشأن المبادئ التوجيهية للأمن الرقمي، وفي الأنشطة المنسقة في كل مرحلة من مراحل عمليات إدارة الحوادث التي قام بها الفريق الحكومي لمواجهة الحوادث الأمنية الحاسوبية.

وفيما يتعلق بإنشاء ودعم آليات وعمليات المشاورات الثنائية والإقليمية ودون الإقليمية والمتعددة الأطراف بهدف تعزيز بناء الثقة بين الدول والحد من احتمال أن تنشأ عن حوادث تكنولوجيا المعلومات والاتصالات تصورات خاطئة أو تصعيد أو نزاعات، تُشارك كولومبيا بنشاط في منتديات دولية مختلفة.

وشاركت كولومبيا على وجه التحديد في مناقشات جرت في الأمم المتحدة (في نيويورك وفيينا وجنيف)، وفي آليات ومناسبات إقليمية، وذلك في إطار منظمة الدول الأمريكية بالأساس.

وتشارك كولومبيا، في إطار فريق برنامج العمل الرقمي لتحالف المحيط الهادئ، وبدعمٍ من شبكة منظمة الدول الأمريكية لأفرقة مواجهة الحوادث الأمنية في الفضاء الإلكتروني في الأمريكتين، في مشروع تبادل الدول الأعضاء في تحالف المحيط الهادئ المعلومات عن التهديدات التي تهدد الفضاء الإلكتروني. وفي هذا السياق، بدأ تشغيل المنصة التكنولوجية لتبادل المعلومات بين أفرقة البلداء الأعضاء لمواجهة الحوادث الأمنية في الفضاء الإلكتروني منذ 23 كانون الثاني/يناير 2020. ويتولى فريق كولومبيا لمواجهة الحوادث الأمنية الإلكترونية تشغيل الفرع الوطني الكولومبي من هذه المنصة.

وعلى الصعيد الثنائي، أبرمت كولومبيا مذكرة تفاهم مع شيلي بشأن الفضاء الإلكتروني وأمنه والدفاع عنه والجريمة الإلكترونية والاستخبارات الإلكترونية، ووقع عليها وزيرا خارجية البلدين في 21 آذار/مارس 2019. والكيانات المشاركة من كولومبيا هي المكتب الاستشاري الرئاسي للشؤون الاقتصادية والتحول الرقمي، ووزارة تكنولوجيا المعلومات والاتصالات، ووزارة الدفاع، ومركز قدرات أمن الفضاء الإلكتروني في كولومبيا التابع للشرطة الوطنية، ومديرية الاستخبارات الوطنية، ومكتب المدعي العام، ووزارة العدل، ووزارة الخارجية.

وجرى في 15 نيسان/أبريل 2020 تبادل للخبرات في مجال الأمن الرقمي بين خبراء حكوميين من كولومبيا وبيرو عبر الفضاء الإلكتروني. وتم في إطار ذلك تبادل معلومات عن السياسات والاستراتيجيات الوطنية، وإقامة قناة للاتصال بشأن أنشطة الدعم في المستقبل لمواجهة الحوادث الأمنية المتصلة بتكنولوجيا المعلومات والاتصالات.

وتشارك كولومبيا أيضا في مجالس الابتكار في مجال أمن الفضاء الإلكتروني، وهي مبادرة لمنظمة الدول الأمريكية وشركة سيسكو، وهذه المجالس هي منتدى للتعاون بين القادة الرئيسيين في القطاعين العام والخاص والمجتمع المدني والأوساط الأكاديمية لجهود تعزيز الابتكار، والتوعية، ونشر أفضل الممارسات المتعلقة بأمن الفضاء الإلكتروني في المنطقة. وتسهم هذه المنابر إسهاما هاما في تنفيذ تدابير بناء الثقة في الفضاء الإلكتروني، ومن شأنها دعم تنفيذ سياسات أكثر فعالية في مجال الأمن الرقمي على الصعيدين الوطني والدولي.

والطلبات الدولية المتعلقة بمسائل أمن الفضاء الإلكتروني تُوجَّه عموما عن طريق مكتب تنسيق جهود منع الجرائم التابع لوزارة الخارجية.

وفيما يتعلق بتعزيز التعاون، بما في ذلك تعيين جهات اتصال لتبادل المعلومات عن الاستخدامات الخبيثة لتكنولوجيا المعلومات والاتصالات والمساعدة في التحقيقات، من المهم الإشارة إلى العمل الذي تقوم به مختلف السلطات والكيانات الحكومية بشأن إعداد بروتوكول وطني لإدارة الحوادث يهدف إلى دعم بذل جهود مبكرة ومنسقة لمواجهة الحوادث الأمنية في الفضاء الإلكتروني التي قد تهدد النظام الاقتصادي والاجتماعي أو الأمن الوطني. ومن بالغ الأهمية تنفيذ هذا البروتوكول لأنه يركز على الوقوف على الحادث، ودراسة الحقائق، والنظر في التهديد، وتحديد الطريقة المناسبة لاحتواء الوضع أو تقويمه.

وتوجد ضمن مكتب المدعي العام ثلاثة أفرقة مسؤولة عن معالجة المسائل المتعلقة بالجريمة الإلكترونية، وهي تُتيح تلقي الدعم والمساعدة من الخبراء في التحقيقات التي يُباشر فيها بناء على طلبات ترد في إطار طلبات المساعدة القانونية المتبادلة ويُرصد فيها استخدام خبيث لتكنولوجيا المعلومات والاتصالات.

وهذه الأفرقة هي: (أ) مكتب المدعي العام لمكافحة الجريمة المنظمة؛ (ب) مكتب المدعي العام لأمن المواطنين؛ (ج) مديرية هيئات التحقيقات التقنية. وبالإضافة إلى تقديم المساعدة في التحقيقات، تعمل أفرقة الخبراء هذه، ضمن مكتب المدعي العام، على الترويج للاتجاهات المستجدة وأفضل الممارسات المتعلقة بالجريمة الإلكترونية والأدلة الرقمية.

وتتلقى مديرية الشؤون الدولية التابعة لمكتب المدعي العام الدعمَ في إجراء التحقيقات في الجرائم الإلكترونية من مختلف المدعين العامين المتخصصين ومن أفرقة هذا المكتب المعنية بالجريمة الإلكترونية.

وقدَّمت وزارة العدل في الولايات المتحدة التدريب في المسائل المتعلقة بطلبات المساعدة القانونية المتبادلة. ففي الولايات المتحدة، يتعين على السلطات الملتمسة للمساعدة أن تفي بمقاييس ومعايير استدلالية ليُتاح لها الوصول إلى الاتصالات الإلكترونية المحفوظة. إذ يتعين على السلطات الملتمسة للمساعدة، على وجه التحديد، أن تقدم وقائع متسلسلة زمنيا يُمكن استنباط تأويلات منها تبيّن أن هناك أسبابا معقولة للاعتقاد بأن السجلات الإلكترونية المطلوبة تكتسي أهمية وأن لها قيمة جوهرية في التحقيق الجاري. ويجب عليها أيضاً أن تثبت أنا هناك وقائع سليمة وموثوقة تُشير إلى ارتكاب جريمة، وليس مجرد وقائع مفترضة، وأن حساب البريد الإلكتروني أو حساب شبكة التواصل الاجتماعي المعني يحتوي على معلومات تتعلق بالجريمة الجاري التحقيق فيها.

وتقوم المديرية الوطنية للاستخبارات كذلك، في إطار التعاون الدولي، بإجراء تحقيقات واستقصاءات منسقة مزدوجة الاتجاه استجابة للطلبات الواردة مباشرة من البلدان.

التعاون والمساعدة على الصعيد الدولي في ميدان أمن تكنولوجيا المعلومات والاتصالات وبناء القدرات فيه

ترى كولومبيا أن بناء القدرات مسألةٌ أساسية فيما يتعلق بمسائل التكنولوجيا.

وإدارة مخاطر الأمن الرقمي مجالٌ يمكن أن تعمل فيه سوياً الدول والقطاع الخاص والأوساط الأكاديمية، وينبغي النظر لهذا الغرض في آليات للتعاون والمساعدة على الصعيد الدولي.

ومن المهم إشراك مختلف الجهات المعنية في أعمال تحليل مسألة أمن الفضاء الإلكتروني. فمن شأنها تقديم مساعدة جد قيّمة في تحديد واعتماد التدابير الأمنية الوقائية وتدابير مواجهة الحوادث والطوارئ.

ومن المهم أن تبدأ الدول بتحديد المجالات التي تحتاج إلى تعزيز قدراتها فيها. ويمكن لها أن تستند في هذا الصدد إلى نماذج نضج القدرات المعدّة دولياً.

وينبغي لها أن تضع، مستندة إلى ذلك، خططا تشملُ تنمية القدرات التشغيلية والإدارية والبشرية والعلمية وإقامة البنية التحتية المادية والتكنولوجية، وتكونُ موجّهة للهيئات والكيانات المسؤولة عن أمن الفضاء الإلكتروني وعن القطاعات الرئيسية. ومن المهم كذلك، في إطار تعزيز القدرات، أن يُحدَّث بانتظام دليل البنى التحتية الحيوية الوطنية للفضاء الإلكتروني وخطط حمايتها وآليات التنسيق فيما بينها.

وبما أن هذه مسألة تعنينا جميعا، فمن الضروري العمل على إنشاء محتوى تثقيفي بشأن الأمن الرقمي ليُدرج في المناهج الدراسية لمختلف مستويات التعليم وفي الدورات الدراسية غير النظامية.

وبهدف وضع إجراءات لتبادل المساعدة في مواجهة الحوادث وفي التعامل مع المشاكل الأمنية الشبكية القصيرة الأجل، بما في ذلك إجراءات للتعجيل بتقديم المساعدة، لدى كولومبيا نموذج وطني لمواجهة الحوادث يُحدد بروتوكول إدارة الحوادث التي تقع في جميع أنحاء البلد، وتتصرف كيانات الفضاء الإلكتروني بموجبه وفقاً لصلاحياتها ومهامها.

وعلى وجه التحديد، أنشئ الفريق الحكومي لمواجهة الحوادث الأمنية الحاسوبية بهدف تعزيز المنظومة الرقمية في كيانات الدولة وتزويدها بالخدمات مجانا. ويغطي دليل الخدمات ثلاثة أنواع من الخدمات: الإدارة الاستباقية والتفاعلية والأمنية. ويشمل ذلك رصد توفُّر المواقع الشبكية، وتحليل مكامن الضعف، ورصد الأحداث الأمنية، وتقديم الدعم لإدارة الحوادث ومواجهتها، والتوعية بإدارة الحوادث.

ويُنسق الفريق الحكومي لمواجهة الحوادث الأمنية الحاسوبية مع الكيانات الحكومية الأخرى المعنية بالفضاء الإلكتروني (فريق مواجهة الطوارئ الحاسوبية في كولومبيا، والقيادة الإلكترونية المشتركة، ومركز الشرطة الإلكترونية) في إدارة الحوادث التي تقع في كيانات الدولة؛ ويُشارك، من خلال لجنة الأمن الرقمي، في وضع استراتيجيات لمعالجة المسائل التي تمس الأمن الرقمي للمواطنين العاديين والدولة.

ومن أجل تيسير التعاون عبر الحدود لمعالجة ما يتجاوز الحدود الوطنية من مكامن ضعف في البنية التحتية الحيوية، يُنسِّق مكتب المدعي العام أيضا مع بلدان المنطقة بشأن استراتيجيات لتبادل المعلومات في الوقت المناسب وبصورة مبسطة عند إجراء تحقيقات وطنية يتبيّن فيها وجود احتمال بأن تُشنّ هجمات على البنية التحتية الحيوية أو أن تُخترق.

وتقوم وزارة تكنولوجيا المعلومات والاتصالات، من خلال الفريق الحكومي لمواجهة الحوادث الأمنية الحاسوبية، بالتنسيق مع فريق مواجهة الطوارئ الحاسوبية ومركز الشرطة الإلكترونية للتحقق من صحة المعلومات من خلال مصادر دولية مختلفة تُتيح تسريع أعمال التخفيف من الآثار وأعمال التحقيق إذا اقتضى الأمر ذلك.

وفيما يتعلق بوضع استراتيجيات الاستدامة في إطار مبادرات بناء القدرات المتعلقة بأمن تكنولوجيا المعلومات والاتصالات، أُدرجت المبادئ التوجيهية والتوصيات المتعلقة ببناء القدرات في مختلف صكوك السياسات العامة الواردة في وثيقتي المجلس الوطني للسياسات الاقتصادية والاجتماعية رقم 3711 و 3854 الصادرتين في عام 2016. وإضافة إلى ذلك، تعلن وزارة تكنولوجيا المعلومات والاتصالات، ووزارة الدفاع، وجهات غيرهما، عن تدابير إدارية وقانونية أخرى لتعزيز القدرة على المواجهة.

وفي هذا الصدد، أُبرمت، على سبيل المثال، اتفاقات تعاون بين حكومة كولومبيا ومنظمة الدول الأمريكية تقوم الأطراف من خلالها بمضافرة جهودها في مجال التعاون التقني بما يدعم تحديثَ المبادئ التوجيهية للأمن الرقمي وتعزيزَ القدرات والمهارات التقنية لإدارة المخاطر التي تهدد الفضاء الإلكتروني من خلال مبادرات في مجالين أساسيين هما: (أ) وضع السياسات وتعميمها؛ (ب) بناء القدرات.

وقد اتّبع مكتب المدعي العام، من خلال مديرية الشؤون الدولية، المبادئ التوجيهية والتوصيات الصادرة عن مختلف المنظمات المتعددة الأطراف بشأن تعزيز الأمن في الفضاء الإلكتروني، وذلك لضمان الإدارة السليمة للتحقيقات في الجرائم الإلكترونية، ومن ثم الحد من الإفلات من العقاب قدر الإمكان.

وبقصد المساهمة في القدرات الوطنية في مجال الفضاء الإلكتروني، قرّرت المديرية الوطنية للاستخبارات إنشاء فريق لمواجهة الحوادث الأمنية الحاسوبية خاص بقطاع الاستخبارات ليكون بمثابة آلية تنسيقية في التعامل مع الأحداث والحوادث في هذا القطاع، ولتعزيز تعميم المعلومات التقنية عن الأحداث والحوادث، وإجراء التحقيقات في حوادث الفضاء الإلكتروني.

وأُعطيت الأولوية في كولومبيا أيضا إلى التوعية بشؤون أمن تكنولوجيا المعلومات والاتصالات وإلى بناء القدرات في الخطط والميزانيات الوطنية بهدف إعطاء مسألة الأمن الأهمية الواجبة لها في تخطيط التنمية والمعونة. وفي هذا الصدد، وإضافةً إلى ما سبق ذكره فيما يتعلق بالسياسات العامة المتعلقة بالأمن الرقمي، وُضعت برامج توعوية بهدف تثقيف وإعلام المؤسسات والمواطنين بشأن أمن تكنولوجيا المعلومات والاتصالات.

وعملت وزارة تكنولوجيا المعلومات والاتصالات في هذا السياق على وضع برنامج يُركز على بناء القدرات، وقامت، من خلال اتفاقات التعاون المبرمة، بتنظيم دورات دراسية ومنح دبلومات وشهادات في مجال أمن المعلومات وإدارة تكنولوجيا المعلومات لفائدة 134 1 موظفا عموميا من الوكالات الحكومية على الصعيدين الوطني والمحلي.

ومن أبرز هذه البرامج برنامج "لنتحدث عن الحكومة الرقمية" الذي شارك من خلاله أكثر من 250 موظفا من موظفي شؤون تكنولوجيا المعلومات وشؤون الأمن من الكيانات العمومية في حلقة نقاش حول بناء القدرات في مجال إدارة المخاطر الأمنية والرقمية.

وحضر 40 من القادة في مجال تكنولوجيا المعلومات مسابقةً بشأن الفضاء الإلكتروني للموظفين العموميين عُقدت في مدينة بيريرا. وشاركوا أيضا في مسابقة بشأن أمن الفضاء الإلكتروني تناولوا فيها التحديات والحالات التي قد تنشأ على الإنترنت. ونظمت منظمة الدول الأمريكية هذه المسابقة بدعم من شركة تريند مايكرو، وهي شركة متعددة الجنسيات لأمن الفضاء الإلكتروني.

وفيما يتعلق بالحلقات التدريبية المعنونة "تعزيز الأمن الرقمي من أجل تعزيز المنطقة"، حضر أكثر من 400 1 مسؤول، من بينهم قادة في مجال تكنولوجيا المعلومات وموظفون لشؤون الأمن من الكيانات العمومية، اجتماعات عُقدت في 24 مدينة في كولومبيا وبلغ عددها 25 اجتماعا.

وبدعم منظمة الدول الأمريكية، عُزّز التدريب في المنطقة. فعلى سبيل المثال، عُقدت في مناسبات عديدة الدورة الدراسية المعنونة "عملية لاهاي: العمليات الأمنية الدولية والفضاء الإلكتروني" والممولة من مملكة هولندا. وفي عام 2019، عقدت هذه الدورة الدراسية في كولومبيا؛ وقُدّم التدريب لمسؤولين من كولومبيا، وشارك فيه أيضا مندوبون من أمريكا اللاتينية ومنطقة البحر الكاريبي يتولون مسؤوليات عن مسائل أمن الفضاء الإلكتروني. ويشمل منهج هذه الدورة الدراسية مواضيع مثل السيادة، والولاية القضائية، ومبدأ بذل العناية الواجبة، واستخدام القوة، والقانون الدولي لحقوق الإنسان، وقانون البحار، والاتفاقات السلمية، ومواضيع أخرى في هذا الصدد، وتتناول الدورة جميع هذه المواضيع في سياق أكاديمي يتعلق بعمليات الفضاء الإلكتروني.

وفيما يتعلق ببناء القدرات في مجال تقنيات الأدلة الجنائية وفي مجال تدابير التعاون للتصدي لاستخدام تكنولوجيا المعلومات والاتصالات لأغراض إرهابية أو إجرامية، استضافت حكومة كولومبيا حلقة عمل إقليمية لأمريكا اللاتينية بشأن الحصول على الأدلة الإلكترونية من الجهات المقدمة لخدمات الاتصالات من القطاع الخاص سعياً لمنع الإرهاب والجريمة المنظمة في إطار التحقيقات العابرة للحدود الوطنية، ونُظمت حلقة العمل من طرف منظمة الدول الأمريكية، والمديرية التنفيذية للجنة مكافحة الإرهاب، ومكتب الأمم المتحدة المعني بالمخدرات والجريمة، والرابطة الدولية للمدعين العامين، وآلية التنسيق الوطنية للأمن الرقمي، ووزارة تكنولوجيا المعلومات والاتصالات في كولومبيا. وحضر حلقة العمل مندوبون من 13 بلدا من بلدان أمريكا اللاتينية (مسؤولون من شرطة التحقيقات الجنائية ووكالات حكومية أخرى)، وتلقوا تدريبا بشأن المسائل المتعلقة بالحصول على أدلة رقمية عبر الحدود، والمستجدات التشريعية في الولايات المتحدة وكندا والاتحاد الأوروبي، وطلبات الإفصاح عن المعلومات في حالات الطوارئ، وإعداد طلبات المساعدة القانونية المتبادلة، ومسائل أخرى، بهدف تعزيز التعاون الدولي في مجال منع الإرهاب والجريمة المنظمة.

وخلال السنوات الثلاث الماضية، وافق مكتب المدعي العام على إيفاد محققين جنائيين من أفرقة الجريمة الحاسوبية والأدلة الجنائية الحاسوبية لحضور حلقات دراسية ودورات تدريبية هامة نظمتها منظمةُ الدول الأمريكية وسجلُّ عناوين الإنترنت لأمريكا اللاتينية ومنطقة البحر الكاريبي وجهات غيرهما، وللعمل مع مدعين عامين لهم إلمام بالتحقيقات المتعلقة بالتكنولوجيا ويقودون تحقيقات من هذا القبيل (التكنولوجيا كوسيلة في ارتكاب جريمة أو كغاية من ارتكابها).

وبالإضافة إلى ذلك، عُقدت، بدعم من كيانات من القطاع الخاص وجامعات محلية، دورات تدريبية مختلفة بشأن مكافحة الجريمة الإلكترونية وتحسين التقنيات مثل البروتوكولات والتدريب على الأجهزة والبرامج الحاسوبية لتحليل الأدلة الرقمية من أجل إيجاد الروابط بين الحالات وكشف الأنماط.

وتخطط مديرية الاستخبارات الوطنية، بالتنسيق مع فريق مواجهة الحوادث الأمنية الحاسوبية الخاص بقطاع الاستخبارات، لبناء القدرات في مجالات اختبارات الكشف عن حالات الاختراق وتحليل مكامن الضعف، وتحليل الأدلة الجنائية واستعادة المعلومات الرقمية، وتحليل البرامجيات الخبيثة والأدوات الإلكترونية، وتحليل التطبيقات، والمختبرات المفتوحة المصدر، ودراسة ظواهر الفضاء الإلكتروني.

واستجابة للتوصية الداعية إلى وضع نُهج إقليمية لبناء القدرات، مع مراعاة القضايا المميزة ذات الطابع الثقافي أو الجغرافي أو السياسي أو الاقتصادي أو الاجتماعي، من أجل دعم الأخذ بنهج يتناسب مع كل حالة على حدة، تقوم وزارة تكنولوجيا المعلومات والاتصالات، من خلال فريق الأمن والخصوصية التابع لمديرية الحكومة الرقمية، بتطبيق نموذج لأمن المعلومات والخصوصية يجمع بين الأدوات التي تمكن كيانات الدولة على الصعيدين الوطني والمحلي من التعامل مع التهديدات التي تهدد الفضاء الإلكتروني، بما يُرسي ثقافة أمنية تمكّن من الإلمام بالأوضاع عند التعامل مع التهديدات التي تهدد الفضاء الإلكتروني والتي تؤثر في المؤسسات على مستوى عبر وطني.

وإضافة إلى ذلك، تعمل السلطات المسؤولة عن السياسات المتعلقة بالجريمة على وضع خطة وطنية تغطي المسائل المتعلقة بمختلف أشكال الجريمة.

وتعمل المديرية الوطنية للاستخبارات على بناء قدرات الدوائر الاستخباراتية الوطنية في مجال التبادل الآمن للمعلومات. وفي هذا الصدد، يجري إعداد مشروع لتقديم التدريب وبناء القدرات لفائدة البلدان الكاريبية في مجالي الحماية وإدارة الممارسات الجيدة، بالتنسيق مع الوكالة الرئاسية للتعاون.

وكما أشير إليه سابقا، فمن أجل بناء القدرات في مجال أمن تكنولوجيا المعلومات والاتصالات، شاركت كولومبيا في مبادرات للتعاون الثنائي والمتعدد الأطراف بهدف تحسين الظروف في هذا السياق بما يمكّن من تبادل المساعدة على نحو فعال في مواجهة حوادث تكنولوجيا المعلومات والاتصالات.

ووضعت وزارة تكنولوجيا المعلومات والاتصالات كذلك استراتيجيات للتعاون مع شركات الأمن والكيانات المعنية بالفضاء الإلكتروني على المستوى الدولي، بهدف تبادل المعلومات الاستخباراتية عن التهديدات على كل من المستوى الاستراتيجي والتكتيكي والتنفيذي.

انطباق القانون الدولي على استخدام تكنولوجيات المعلومات والاتصالات

ترى كولومبيا أن القانون الدولي، ولا سيما ميثاق الأمم المتحدة، وبما في ذلك القانون الدولي لحقوق الإنسان والقانون الدولي الإنساني، ينطبق على العالم "الافتراضي" مثل انطباقه على العالم "المادي".

وتتفق كولومبيا مع البيان الذي يرد في تصدير تقرير عام 2015 لفريق الخبراء الحكوميين والذي يعود للأمين العام آنذاك: "لا يمكن تحقيق استقرار وأمن الفضاء الإلكتروني إلا من خلال تعاون دولي يقوم على أساس القانون الدولي ومبادئ ميثاق الأمم المتحدة".

وعليه، ترى كولومبيا أن بالإمكان تطبيق المفاهيم العامة للقانون الدولي على الفضاء الإلكتروني بعد إدخال التعديلات التي تقتضيها طبيعة العمليات الافتراضية.

ومراعاة مختلف التفسيرات الممكنة للمسائل المرتبطة بالقانون الدولي في الفضاء الإلكتروني لا يمنع من وضع أدلة أو مراجع بشأن تطبيق القانون الدولي العام في الفضاء الإلكتروني.

وفي هذا الصـــدد، فإن الممارســـة المتبعة فيما يتعلق بالاتفاقية المتعلقة بالجريمة الإلكترونية التي تتضمن مذكرات توجيهية تقدم إرشادات بشأن تنفيذ أحكامها وجعلها متسقة مع التطورات التكنولوجية قد تكون ممارسة مفيدة جدا. وهذه ممارسة تعتبر جيدة ويمكن محاكاتها.

وبما أن الجمعية العامة أوصت ورحبت بمجموعة الضوابط والقواعد والمبادئ الدولية لسلوك الدول المسؤول المتضمنة في تقارير أفرقة الخبراء الحكوميين، ترى كولومبيا أن المهمة التي يجب القيام بها على الفور هي تعزيز تنفيذ هذه الضوابط والقواعد والمبادئ. ولا تعتقد كولومبيا أن هناك حاجة في الوقت الحاضر إلى صك ملزم.

ويجدر أيضا التأكيد على أن كولومبيا تتقيد بالالتزامات والضمانات المحددة.

المفاهيم

تتواصل، في سياق السيناريوهات المتعددة الأطراف، مناقشةُ التوسع في المفاهيم الذي رُئي أنه ضروري لتعزيز الإلمام بالمفاهيم المتصلة بالسلم والأمن الدوليين في سياق استخدام تكنولوجيات المعلومات والاتصالات من حيث البعد القانوني والتقني والسياسي نظراً لطابعها المميز وحداثة تطبيقها.

وهذه المناقشات ضرورية لتعديل الإطار القانوني الدولي بحيث يصبح متناسبا مع تحديات الفضاء الإلكتروني، وليتسنى التوصل إلى توافق في الآراء بشأن كيفية تطبيق القانون الدولي في هذا الفضاء الافتراضي. وفي هذا الصدد، تتفق كولومبيا مع الاستنتاجات التي خلص إليها فريق الخبراء الحكوميين في تقريره لعام 2015، وهي على استعداد لإجراء مناقشات أكثر استفاضة مع الوفود الأخرى في الأمم المتحدة.

وهذا هو السبيل الوحيد لضمان الاستخدام المناسب لتكنولوجيات المعلومات والاتصالات التي هي أساسية في مواجهة التحديات الماثلة حاليا أمام المجتمع الدولي، وللحيلولة دون استخدامها بطريقة تتعارض مع مقاصد ومبادئ ميثاق الأمم المتحدة، بما في ذلك الصون التام للسلم والأمن الدوليين.

واستخدام التكنولوجيات الجديدة لتقديم الخدمات على نحو فيه قطعٌ مع المعتاد يدفع بنوع جديد من العلاقات في مجتمع المعلومات يقومُ على المعالجة الآمنة للمعلومات والحماية الفارقة للبيانات الشخصية، مما يشجع على دعم فوائد التقدم التكنولوجي وإسهامه في التنمية الاجتماعية والاقتصادية.

ولذلك، من الضروري تعزيز الدور القيادي للحكومات في هذا الصدد لتحديد رؤية جديدة متسقة مع أفضل الممارسات الدولية في التصدي لمخاطر الأمن الرقمي، مع مراعاة المبادئ التي تدعم سلوك الدول المسؤول، وتسهل مشاركتها في منتديات النقاش بشأن الأمن الرقمي الدولي، وتشجعها على التصرف تجاه نظيراتها بطريقة شفافة يمكن التنبؤ بها، والحد بذلك من احتمالات أن ينشأ سوء تفسير أو تصعيد أو نزاع عن مسائل الأمن الرقمي.

وأخيرا، يُسهم تنفيذ الاستراتيجيات والتدابير المتعلقة بالاستخدام المسؤول للبيئة الرقمية في بناء السلام من خلال تهيئة الظروف المواتية للتعايش الرقمي على أساس الاحترام، بما في ذلك دعم حرية التعبير واستعمال الألفاظ اللائقة على شبكة الإنترنت بهدف تعظيم فوائد تكنولوجيا المعلومات والاتصالات ودعم التأقلم مع المستقبل الرقمي.

الدانمرك

[الأصل: بالإنكليزية]
[29 أيار/مايو 2020]

تعمل الدانمرك، مثل بقية دول العالم، على زيادة معدل ربطها مؤسساتها بشبكة الإنترنت. فالحلول الرقمية تشكل جزءا من الحياة اليومية وتساعد على الدفع بالنمو الاقتصادي. ومن الأهمية بمكان بالنسبة للدانمرك، بوصفها أحد أكثر البلدان استخداما للتكنولوجيا الرقمية في العالم، أن تنهض بفضاء إلكتروني عالمي مفتوح ومستقر وسلمي وآمن، تُطبّق فيه حقوق الإنسان والحريات الأساسية، فضلاً عن سيادة القانون، تطبيقاً كاملاً.

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.

ويخصص اتفاق الدفاع للفترة 2018-2023 مبلغا قدره 1,4 مليار كرونة دانمركية لتعزيز أمن الفضاء الإلكتروني والدفاع الإلكتروني، ما يعزز بالتالي قدرتنا على الصمود. وقد اتخذت الاستراتيجية الدانمركية لأمن الفضاء الإلكتروني والمعلومات للفترة 2018-2021 خطوات إضافية لزيادة أمن الفضاء الإلكتروني. فمن خلال 25 مبادرة و 6 استراتيجيات موجهة تتناول ما يعرف حتى الآن بأنه قطاعات حيوية (الطاقة، والتمويل، والنقل، والرعاية الصحية، والاتصالات السلكية واللاسلكية، والملاحة البحرية)، عززت الدانمرك القدرة التكنولوجية على الصمود في بنيتها التحتية الرقمية، وحسنت معارف ومهارات المواطنين والشركات والسلطات، وعززت التنسيق والتعاون فيما يتعلق بأمن الفضاء الإلكتروني. وبالإضافة إلى ذلك، أُدمج التوجيه الأوروبي المتعلق بأمن شبكات ونظم المعلومات بكامله في القانون الدانمركي.

وفي إطار الاستراتيجية الدانمركية لأمن الفضاء الإلكتروني والمعلومات للفترة 2018-2021، أنشئت وحدات مخصصة 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 المعلومات وأمن الفضاء الإلكتروني. وتشارك في المنتدى أيضا وكالة الرقمنة ودائرة الأمن والاستخبارات الدانمركية.

ومن أجل الحصول على العدد الكافي من الموظفين المهرة لكشف الهجمات الإلكترونية ضد الدانمرك والتصدي لها، ولا سيما فيما يتعلق بالهياكل الأساسية الحيوية، قام مركز الأمن الإلكتروني، علاوة على ذلك، بتأسيس وتشغيل أكاديميته الخاصة بالتعلم الإلكتروني المكثف. وبلغ عدد خريجي الأكاديمية 15 شخصًا في عام 2019 يعملون الآن في مركز العمليات التابع لمركز الأمن الإلكتروني. وإلى جانب الأكاديمية، يدعم مركز الأمن الإلكتروني أيضاً التعليم والبحوث في مجال أمن الفضاء الإلكتروني. فعلى سبيل المثال، في عام 2019، تعاون مركز الأمن الفضائي مع كلية كوبنهاغن للتصميم والتكنولوجيا، وجامعة آلبورغ، وجامعة جنوب الدانمرك، وكلية كوبنهاغن للأعمال، والجامعة التقنية الدانمركية على افتتاح أول مدرسة صيفية لأمن الفضاء الإلكتروني.

وفي عام 2019، أنشئ مجلس مشترك بين القطاعين العام والخاص للأمن الإلكتروني (Cybersikikhedsråd) بهدف تأهيل عمل السلطات الوطنية والقطاع الخاص، وتعزيز الديمقراطية الرقمية وتحسين المعرفة بالتهديدات والفرص التي تتيحها الرقمنة والتكنولوجيات الجديدة.

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. والدانمرك أيضا عضو نشط في الفريق التعاوني المعني بأمن المعلومات الشبكية وفي شبكة فريق مواجهة الحوادث الأمنية الحاسوبية، كما أنها عضو في مجلس إدارة وكالة الاتحاد الأوروبي لأمن الفضاء الإلكتروني. وقد دأبت الدانمرك، من خلال مشاركتها في هذه المنتديات، على الترويج لفضاء إلكتروني عالمي ومفتوح ومستقر وسلمي وآمن.

وعلاوة على ذلك، اضطلعت الدانمرك بدور نشط في تطوير مجموعة أدوات الاتحاد الأوروبي للجيل الخامس من شبكات الاتصال اللاسلكية. وتسعى مجموعة الأدوات إلى تحديد نهج أوروبي منسق تجاه الجيل الخامس استناداً إلى مجموعة مشتركة من التدابير، تهدف إلى التخفيف من المخاطر الرئيسية لشبكات الجيل الخامس على أمن الفضاء الإلكتروني.

وتشدد الدانمرك على أن الفضاء الإلكتروني، على نحو ما أوضح المجتمع الدولي، راسخ الجذور في القانون الدولي القائم، كما شهدت بذلك أفرقة الخبراء الحكوميين المعنية بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي في تقاريرها المعدة 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. وتشدد الدانمرك أيضا على أهمية المعايير الطوعية الـ 11 غير الملزمة المتعلقة بسلوك الدول المسؤول، الواردة في تقارير فريق الخبراء الحكوميين لعام 2015، باعتبارها تكملة للقانون الدولي الملزم.

وعلى الرغم من جهودنا المشتركة، فلا تزال قدرة الجهات الفاعلة من الدول وغير الدول على القيام بأنشطة إلكترونية شريرة ورغبتها في ذلك آخذة في الازدياد. وينبغي أن يكون ذلك موضع اهتمام على الصعيد العالمي. وقد تشكل الأنشطة الشريرة في الفضاء الإلكتروني أفعالا غير مشروعة بموجب القانون الدولي، فضلا عن أنها تؤدي إلى زعزعة الاستقرار والمخاطرة بمفاقمته. ولا تزال الدانمرك مصممة على منع الأنشطة الشريرة 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 إنشاء فضاء إلكتروني عالمي ومفتوح ومستقر وسلمي وآمن تطبَّق فيه حقوق الإنسان والحريات الأساسية وسيادة القانون تطبيقا كاملا.

مضمون المفاهيم المشار إليها في تقارير فريق الخبراء الحكوميين

الأخطار القائمة والناشئة

تدرك الدانمرك، كما ذُكر أعلاه، أن الفضـــاء الإلكتروني يتيح فرصـــا هائلة لزيادة رفاه مواطنينا، وتعزيز نموهم الاقتصـادي المسـتدام، وتحسـين نوعية حياتهم. ومع ذلك، فإن اعتمادنا على الحلول الرقمية يطرح أيضاً بعض التحديات.

وتشـعر الدانمرك بالقلق إزاء تزايد الأنشـطة الشـريرة في الفضـاء الإلكتروني التي تقوم بها جهات فاعلة من الدول ومن غير الدول، واسـتخدام الفضـاء الإلكتروني للتعدي على الملكية الفكرية. وهذه الأعمال تهدد استقرار المجتمع الدولي ونموه الاقتصادي.

ولم يحدث من قبل أن كانت الحاجة إلى فضـاء إلكتروني مفتوح وآمن ومسـتقر وميسَّـر وسـلمي أوضـــح ممـا عليـه خلال جـائحـة مرض فيروس كورونـا (كوفيـد-19). وتتيح تكنولوجيـات المعلومـات والاتصالات التواصل والتعاون وتبادل المعارف التي يحتاجها العالم من أجل مكافحة الوباء.

ومع ذلك، شـهدنا خلال الأزمة الحالية من كوفيد-19 أن الجهات الفاعلة الشريرة سوف تستغل أي فرصـة – حتى وإن كانت جائحة عالمية. ويشـمل ذلك التدخل في الهياكل الأسـاسـية الحيوية، بما في ذلك المستشفيات الضرورية لمكافحة الجائحة. 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 الشريرة في مجال تكنولوجيا المعلومات والاتصالات التي تنطلق من أراضيها.

كيفية انطباق القانون الدولي على استخدام تكنولوجيات المعلومات والاتصالات

تؤيد الدانمرك بقوة إقامة نظام متعدد الأطراف يستند إلى النظام الدولي القائم على القواعد للتصدي للتهديدات القائمة والمحتملة الناشئة عن استخدام تكنولوجيا المعلومات والاتصالات لتحقيق أغراض خبيثة.

وأوضـح المجتمع الدولي أن الفضـاء الإلكتروني راسـخ الجذور في القانون الدولي القائم، كما تشـهد بذلك أيضـــاً تقارير فريق الخبراء الحكوميين لعامي 2013 و 2015 التي أُعدت بتوافق الآراء. وتشـــدد 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.

فالسيادة وعدم التدخل وحظر استخدام القوة هي مبادئ أساسية في القانون الدولي، وانتهاك الدول لها يشـكل فعلا غير مشـروع دوليا، يمكن للدول أن تتخذ تدابير مضـادة 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 العضـوية المعني بالتطورات في ميدان المعلومات والاتصـــالات السـلكية واللاسـلكية في سـياق الأمن الدولي – وغيرها من المبادرات الدولية والإقليمية – في السعي إلى تحقيق هذه النتيجة.

ومن المهم ألا تسـتخدم الدول مبدأ السـيادة لتقييد القانون الدولي لحقوق الإنسـان أو انتهاكه داخل حدودها؛ فقانون حقوق الإنســان واجب التطبيق على الإنترنت، وكذلك خارجه، 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، التي يسترشد فيها القادة العسكريون لإدراج اعتبارات الامتثال للقانون الدولي عند القيام بعمليات في الفضاء الإلكتروني. وهكذا، فإن القانون الإنساني الدولي، 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 عاملاً تمكينياً للنزاعات، بل وسيلة لحماية المدنيين والحد من الآثار غير التناسبية.

والقانون الدولي القائم – الذي تكمله المعايير الطوعية الـ 11 غير الملزمة المتعلقة بسلوك الدول المسؤول، الواردة في تقارير 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 إطار قانوني دولي 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 تطبيقه. وتأمل الدانمرك أن يسهم عمل وتوصيات فريق الخبراء الحكوميين الحالي والفريق العامل المفتوح العضوية في تقديم الإيضاحات، وبالتالي تيسير امتثال الدول الذي تمس الحاجة إليه، ما يعزز في نهاية المطاف من إمكانية التنبؤ ويقلل من خطر التصعيد.

معايير سلوك الدول المسؤول وقواعده ومبادئه

تنضم الدانمرك إلى الاتحاد الأوروبي وزملائها 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 تقارير فريق الخبراء الحكوميين المتعاقبة لأعوام 2010 و 2013 و 2015 تشكل استكمالا للقانون الدولي الملزم 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.

فرنسا

[الأصل: بالفرنسية]
[29 أيار/مايو 2020]

ترحب فرنسا بالفرصة المتاحة للاستجابة لقرار الجمعية العامة 28/74 بشأن الارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي، وتود أن تقدم المعلومات التالية.

1 - التقييم العام لمسائل أمن الفضاء الإلكتروني

تود فرنسا أن تكرر مجددًا في بادئ الأمر أنها لا تستخدم مصطلح "أمن المعلومات" وتفضل استخدام مصطلح "أمن نظم المعلومات" أو "أمن الفضاء الإلكتروني". ولا تعتبر فرنسا المعلومات في حد ذاتها مصدرا محتملا للضرر. ومصطلح "أمن الفضاء الإلكتروني" يتسم بدقة أكبر لدلالته على قدرة أي نظام للمعلومات على تحمُّل أحداث يكون مصدرها الفضاء الإلكتروني ويكون من شأنها أن تعرض للخطر إتاحة البيانات المخزَّنة أو المعالَجة أو المنقولة، أو سلامتها أو سريتها، والخدمات ذات الصلة التي تقدمها هذه النظم أو تيسِّر الحصول عليها.

وترى فرنسا أن الفضاء الرقمي يجب أن يظل مجالا للحرية والتبادل والنمو، ما يسهم في تحقيق الازدهار والتقدم في مجتمعاتنا. وهذا الفضاء الإلكتروني المفتوح والآمن والمستقر والميسَّر والسلمي، الذي يتيح فرصا اقتصادية وسياسية واجتماعية، والذي ما فتئت فرنسا تروِّج له خلال العقود الثلاثة الماضية، يتعرض حاليا للخطر من جراء ممارسات مستجدة شريرة تنشأ فيه. والواقع أن خصوصيات الفضاء الإلكتروني (بما يشمل إغفال الهوية النسبي، وانخفاض تكاليف الأدوات الضارة وسهولة الحصول عليها، ووجود ثغرات في بعض الأدوات وانتشارها) مكَّنت عددًا من الجهات الفاعلة من التجسس، والاتجار غير المشروع، وزعزعة الاستقرار، والتخريب. ولا ينضوي بعض التهديدات ذات المستوى المنخفض تحت مسائل الأمن القومي بل يتعلق بشكل من أشكال الجريمة، لكن استخدام هذه الأسلحة ضد النظم الإلكترونية أو الهياكل الأساسية الحيوية أو المؤسسات الخاصة بالدولة يمكن أن يفضي إلى عواقب وخيمة.

وقد أصبحت التحديات التي يواجهها أمن الفضاء الإلكتروني جزءً لا يتجزأ من استراتيجيات القوة وعلاقات القوة التي تحكم العلاقات الدولية؛ والأمر إنما يتعلق هنا بمسألة ذات أولوية وبرِهان سياسي من الدرجة الأولى. وترى فرنسا أنه يجب على الدول أن تُبقي سلطة استخدام العنف المشروع حكرا عليها، في الفضاء الإلكتروني كما في المجالات الأخرى. غير أن انتشار التكنولوجيا الرقمية باعتبارها أداة جديدة ومجالا للمواجهة ينيط بالقطاع الخاص، ولا سيما عدد معين من الجهات الفاعلة المعنية بالنظم، دورا حاسما ومسؤولية غير مسبوقة في صون السلم والأمن الدوليين.

2 - جهود فرنسا في مجال أمن الفضاء الإلكتروني على الصعيدين الوطني والدولي، وآراؤها بشأن جوهر المفاهيم الواردة في تقارير فريق الخبراء الحكوميين

تتبع فرنسا منذ عدة سنوات سياسة عامة وتشارك في دبلوماسية نشطة للحفاظ على الفضاء الإلكتروني المفتوح والآمن والمستقر والميسّر والسلمي، وتطويره وتعزيزه، والتصدي للأخطار التي تهدد الاستقرار والأمن الدوليين.

وقد أتاح عمل الأفرقة الخمسة الأولى من الخبراء الحكوميين المعنيين بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، الذي شاركت فيه فرنسا، إحراز تقدم في تحديد المبادئ المشتركة وفي الفهم الجماعي للفضاء الإلكتروني، ولا سيما في مجالات التعاون الدولي ومعايير القانون الدولي وتطبيقه.

الإجراءات التي اتخذتها فرنسا في سياق التعاون الدولي، وبناء القدرات، وتعزيز تدابير بناء الثقة وتطويرها

تعمل فرنسا على تعزيز التعاون الدولي بشأن أمن الفضاء الإلكتروني على الصعد الثنائي والأوروبي والدولي

ومن أجل تعزيز قدرة النظم الإلكترونية على الصمود في الاتحاد الأوروبي، تساعد فرنسا في وضع إطار تطوعي للتعاون بغرض منع وقوع الحوادث وإيجاد حلول لها. ويستند الإطار، بوجه خاص، إلى وضع معايير وإجراءات تنفيذية موحدة للتعاون فيما بين الشركاء؛ ويتم اختبار هذه المعايير والإجراءات من خلال تدريبات تجري في كافة البلدان الأوروبية. وشاركت فرنسا أيضا في إعداد "مجموعة أدوات إلكترونية" تتيح إطارا أوروبيا للتصدي دبلوماسيًا بشكل مشترك لأي هجوم إلكتروني، وتستند إلى تدابير الوقاية والتعاون وتحقيق الاستقرار والاستجابة، ولا سيما التدابير التقييدية، ذات الصلة بالحوادث الإلكترونية. وتشارك فرنسا أيضا في تطوير شبكة "سايكلون" (CyCLONe) لتنظيم التعاون العملياتي فيما بين الوكالات الأوروبية الوطنية المعنية بأمن الفضاء الإلكتروني في حال حدوث أزمات إلكترونية، وفي تدريبات مشتركة استعدادًا لمواجهة هذه الأزمات باعتبار ذلك استكمالا للتعاون بين أفرقة مواجهة الطوارئ الحاسوبية التابعة لتلك الوكالات.

وفي إطار منظمة حلف شمال الأطلسي، وبمبادرة من فرنسا، اعتمد الحلفاء، في مؤتمر قمة وارسو في حزيران/يونيه 2016، التزاماً بالدفاع الإلكتروني، وهو "تعهد الدفاع الإلكتروني"، الذي أخذت فيه كل دولة عضو على نفسها تخصيص حصة مناسبة من مواردها لتعزيز قدراتها في مجال الدفاع الإلكتروني، ما أدى إلى تحسين أمن الحلف عموماً.

وفرنسا، إذ تشارك بفعالية في الفريق العامل غير الرسمي التابع لمنظمة الأمن والتعاون في أوروبا المعني بأمن الفضاء الإلكتروني، تواصل الترويج لتنفيذ تدابير بناء الثقة الستة عشر التي وضعتها تلك المنظمة في هذا المجال. وعلى وجه الخصوص، تقوم فرنسا، إلى جانب الدول المشاركة الأخرى، بتجربة تنفيذ التدبير 15 من تدابير بناء الثقة، بشأن تأمين الهياكل الأساسية الحيوية.

وتستصوب فرنسا أيضًا تناول العديد من قضايا أمن الفضاء الإلكتروني باتباع نهج قائم على تعدد أصحاب المصلحة لكي يُؤخذ في الاعتبار دور الجهات الفاعلة من غير الدول ومسؤولياتها المحددة. وشددت فرنسا في نداء باريس من أجل الثقة والأمن في الفضاء الإلكتروني، الصادر في 2018، على ضرورة اتباع نهج معزز يقوم على تعدد أصحاب المصلحة. وترى فرنسا أن المجتمع المدني والأوساط الأكاديمية والقطاع الخاص والأوساط التقنية لديها مهارات وموارد مفيدة لتحديد بعض الجوانب ذات الصلة بسياسات أمن الفضاء الإلكتروني. ونداء باريس[2]، الذي عرضه رئيس الجمهورية في منتدى إدارة الإنترنت الذي عقدته منظمة الأمم المتحدة للتربية والعلم والثقافة في 12 تشرين الثاني/نوفمبر 2018، يبرهن على الدور الفعال الذي يضطلع به البلد في الترويج لجعل الفضاء الإلكتروني آمنا ومستقرا ومفتوحا. ويتلقى نداء باريس، وهي أكبر مبادرة عالمية لأصحاب المصلحة المتعددين في مجال أمن الفضاء الإلكتروني، الدعم من 78 دولة وأكثر من 000 1 كيان من غير الدول. ويهدف إلى تعزيز بعض المبادئ الأساسية لتنظيم الفضاء الإلكتروني، ومنها مثلا إعمال القانون الدولي وحقوق الإنسان في الفضاء الإلكتروني، والسلوك

(2) متاح على الرابط التالي: https://pariscall.international/en.

المسؤول للدول، واحتكار الدولة لسلطة العنف المشروع، والإقرار بالمسؤوليات المحددة للجهات الفاعلة من القطاع الخاص.

ودعمت فرنسا أيضا المقترحات التي وضعتها اللجنة العالمية المعنية باستقرار الفضاء الإلكتروني بشأن المعايير والسياسات الرامية إلى تعزيز الأمن والاستقرار الدوليين وتوجيه سلوك الدول المسؤول في الفضاء الإلكتروني. وقد عُرض التقرير الذي يتضمن استنتاجات اللجنة في منتدى باريس الثاني للسلام.

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

وبذلت فرنسا أيضا جهودا هامة في إطار منظمة التعاون والتنمية في الميدان الاقتصادي. وهي ترأس حالياً الفرقة العاملة المعنية بالأمن والخصوصية في الاقتصاد الرقمي التابعة لمنظمة التعاون والتنمية في الميدان الاقتصادي، وترغب في العمل على مسائل من قبيل مسؤولية الجهات الفاعلة من القطاع الخاص، وتأمين المنتجات والخدمات، والكشف عن مواطن الضعف بشكل مسؤول.

وفي مجال بناء القدرات، ترى فرنسا أن الترابط الذي تتسم به الشبكات والمجتمعات لن يضمن أمن الفضاء الإلكتروني للجميع إلا عندما تتوافر لكل دولة ما يكفي من القدرات لحماية نظمها المعلوماتية. ولذلك، فهي تعزز قدرات شركائها على ضمان أمن الفضاء الإلكتروني، على الصعيد الثنائي أو المتعدد الأطراف. وهذه الجهود الرامية إلى تعزيز التعاون تفيد الأطراف كافة، وتتيح لنا مواكبة أحدث التطورات من خلال التنافس مع أقراننا والتعلم منهم، وتشجع على الإثراء المتبادل للمعارف والخبرات، كما تتيح بث الثقة بين الجهات المعنية صاحبة المصلحة. ففي السنوات الأخيرة، نشرت فرنسا أيضا ضمن قوات الأمن الداخلي في بلدان شريكة خبراء تقنيين دوليين في مجال أمن الفضاء الإلكتروني. فعلى سبيل المثال، تواصل فرنسا مع السنغال الاضطلاع بأنشطة مدرسة داكار الوطنية لأمن الفضاء الإلكتروني، وهي مؤسسة ذات امتداد إقليمي دُشنت في نهاية عام 2018. ويتمثل الهدف من هذا المشروع في تنظيم دورات تدريبية قصيرة المدة وقابلة للتكييف لفائدة أخصائيي أمن الفضاء الإلكتروني وكبار المسؤولين من غرب أفريقيا على سبيل الأولوية.

تعريف معايير السلوك المسؤول: إنجاز كبير

أنشأت فرنسا مجموعة من الآليات، من خلال عقيدتها الوطنية، وترتيباتها وقوانينها الإدارية، لتطبيق معايير السلوك الموصى بها في تقارير فريق الخبراء الحكوميين، ولا سيما تقريره لعام 2015 (A/70/174). ويتمثل الهدف من المعلومات الواردة أدناه، في جملة أمور، في تبيان السبل التي سعت بها فرنسا إلى تنفيذ القواعد.

القاعدة (أ): ينبغي للدول، بما يتفق ومقاصد الأمم المتحدة، بما فيها مقصد صون السلام والأمن الدوليين، أن تتعاون في وضع وتطبيق تدابير لزيادة استقرار وأمن استخدام تكنولوجيات المعلومات والاتصالات ولمنع ما يتصل بتلك التكنولوجيات من ممارسات معروفة بضررها أو باحتمال أن تشكل تهديدات للسلام والأمن الدوليين.

وقد اتخذت فرنسا مجموعة من التدابير استجابة لهذه القاعدة، بطرق منها تحديدًا تعزيز استراتيجية وطنية لأمن الفضاء الإلكتروني تركز على الدفاع والوقاية والمرونة والتعاون. وفي استعراضنا الاستراتيجي

للدفاع الإلكتروني، الذي صدر في شباط/فبراير 2018[3]، تم وضع عقيدة لإدارة الأزمات وتوضيح أهدافنا. فالنموذج الفرنسي، الذي يميز بين المؤسسات المسؤولة عن القدرات الهجومية والمؤسسات التي تتولى المهام الدفاعية، هو نموذج ثبتت فعاليته، كما أن الهدف الدبلوماسي المتمثل في تطوير الثقة والاستقرار في الفضاء الإلكتروني مؤكد بقوة.

وتقوم فرنسا أيضاً بإقامة حوارات استراتيجية ثنائية مع مختلف الشركاء بشأن قضايا أمن الفضاء الإلكتروني. وتنشط فرنسا أيضا، كما ذُكر أعلاه، في العديد من المحافل المعنية بالتعاون والتنسيق على الصعيدين الإقليمي والدولي.

كما اعترفت فرنسا بأن لديها القدرة على القيام بعمليات عسكرية دفاعية وهجومية في الفضاء الإلكتروني من أجل ضمان سيادتها الوطنية، في امتثال صارم للقانون الوطني والدولي. ومن أجل ضمان الشفافية والاتساق، جعلت عقيدتها في متناول أكبر عدد ممكن من الناس في عام 2019 من خلال نشر العديد من الوثائق بشأن مواضيع منها العقيدة العسكرية المتعلقة بالحرب الإلكترونية الهجومية، وورقة بيضاء بشأن القانون الدولي تنطبق على العمليات العسكرية في الفضاء الإلكتروني. ومن شأن هذه الرغبة في توضيح رؤية البلد ومشاطرتها أن تمكّن من الحد من سوء الفهم وعدم اليقين، ومن ثم المساعدة على توطيد الثقة والشفافية في الفضاء الإلكتروني. وتشجع فرنسا الدول الأخرى على أن تحذو حذوها.

القاعدة (ب): في حالة وقوع حوادث في ميدان تكنولوجيات المعلومات والاتصالات، ينبغي للدول أن تنظر في جميع المعلومات ذات الصلة، بما في ذلك السياق الأوسع لذلك الحادث، والتحديات المتمثلة في تحديد الجهة الفاعلة في بيئة تكنولوجيات المعلومات والاتصالات، وطبيعة العواقب ومداها.

ووضعت فرنسا الإجراءات التالية لإدارة الأزمات والهياكل والسياسات الوطنية في حالة وقوع حادث متعلق بالتكنولوجيا:

- خلية أزمات مشتركة بين الوزارات، يتم نشرها في حالة حدوث أزمة كبرى؛
- مركز تنسيقي للأزمات الإلكترونية يجتمع كل شهر ويضم مستويات تقنية أو تشغيلية ومستوى استراتيجيًا رفيع المستوى مشتركًا بين الوزارات، ويعمل أعضاؤه على تحليل الحوادث الإلكترونية في سياق أوسع، وتقييم عواقبها، ويجوز لهم إسنادها. وترى فرنسا أن الإسناد وقرار الإعلان عن ذلك هو من الصلاحيات السيادية.

وقد وضعت فرنسا وسائل لتقييم الحوادث، بطرق منها مقياس خطورة لمساعدة صانعي القرار على إجراء التحليلات واتخاذ الإجراءات اللازمة. وفي تحديد مدى خطورة الحادث، تأخذ فرنسا في الاعتبار، في جملة أمور، عواقبه على ما يلي:

- مصالح الأمة وسيادتها، والديمقراطية
- الأمن الداخلي والمدني

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

- الناس والبيئة
- الاقتصاد

ويمكن أن تؤخذ في الاعتبار معايير أخرى، مثل النية والخطورة والإسناد والحجم والتكرار.

القاعدة (ج): ينبغي ألا تسمح الدول عن علم باستخدام أراضيها لارتكاب أفعال غير مشروعة دولياً باستخدام تكنولوجيات المعلومات والاتصالات.

ولكفالة عدم استخدام أراضيها في القيام بأعمال شريرة، قامت فرنسا بما يلي:

- طلبت من المشغلين ذوي الأهمية الحيوية، أي مشغلي الهياكل الأساسية الوطنية الحيوية (انظر القانون رقم 2013-1168) ومشغلي الخدمات الأساسية (انظر القانون رقم 2018-133)، تعزيز أمن نظم المعلومات والاتصالات الخاصة بهم؛
- جرَّمت في المادة 323-1 من القانون الجنائي التدخلات غير المرخص بها في نظم أمن المعلومات الخاصة بأطراف ثالثة؛
- عزّزت قدرة الوكالة الوطنية لأمن الفضاء الإلكتروني، من خلال القانون رقم 2018-607، على كشف الحوادث الإلكترونية التي تؤثر على مشغلي الهياكل الأساسية الحيوية؛
- شجّعت الكشف المسؤول عن الثغرات من خلال القانون رقم 2016-1321، الذي يوفر الحماية من الإجراءات القانونية للأفراد الذين يبلغون الوكالة الوطنية لأمن الفضاء الإلكتروني عن ثغرة في منتج رقمي أو خدمة رقمية.

القاعدة (د): ينبغي للدول أن تنظر في أفضل سبل التعاون في تبادل المعلومات، ومساعدة بعضها بعضا، والملاحقة القضائية للاستخدام الإرهابي والإجرامي لتكنولوجيات المعلومات والاتصالات، وتنفيذ تدابير تعاونية أخرى بهدف التصدي لهذه التهديدات. وقد تحتاج الدول إلى النظر فيما إذا كان من الضروري وضع تدابير جديدة في هذا الصدد.

وبالإضافة إلى المعلومات المقدمة أعلاه بشأن التعاون، وضعت فرنسا مجموعة من التدابير لتحسين التعاون مع شركائها لمنع استخدام تكنولوجيات المعلومات لأغراض إجرامية وإرهابية، ولا سيما بالانضمام إلى الاتفاقية المتعلقة بالجريمة الإلكترونية (اتفاقية بودابست) ودعم نداء كرايستتشيرش للقضاء على المحتوى الإرهابي والذي يتسم بالتطرف العنيف على الإنترنت.

وعلى المستوى التقني، تواصل الوكالة الوطنية لأمن الفضاء الإلكتروني إقامة شراكات مع نظرائها في العديد من البلدان للتشجيع على تبادل المعلومات الفائقة الأهمية، من قبيل المعلومات عن الثغرات الأمنية أو العيوب في المنتجات والخدمات. وبالإضافة إلى ذلك، ينشط الفريق الحكومي لمواجهة الطوارئ الحاسوبية، التابع للوكالة الوطنية لأمن الفضاء الإلكتروني، في إطار عدة شبكات متعددة الأطراف (منتدى فرق التصدي للحوادث والأمن، وفرقة العمل الأوروبية المعنية بأفرقة مواجهة الحوادث الأمنية الحاسوبية، والفريق الحكومي الأوروبي المعني بمواجهة الطوارئ الحاسوبية، وشبكة فريق مواجهة الحوادث الأمنية الحاسوبية التابعة للاتحاد الأوروبي) يقيم من خلالها اتصالات مع أفرقة مواجهة الطوارئ الحاسوبية في جميع أنحاء العالم.

القاعدة (هـ): ينبغي للدول، في سعيها لضمان الاستخدام الآمن لتكنولوجيات المعلومات والاتصالات، أن تحترم قراري مجلس حقوق الإنسان 20/8 و 26/13 بشأن تعزيز وحماية حقوق الإنسان على الإنترنت والتمتع بها، فضلاً عن قراري الجمعية العامة 167/68 و 166/69 بشأن الحق في الخصوصية في العصر الرقمي، لضمان الاحترام التام لحقوق الإنسان، بما في ذلك الحق في حرية التعبير.

وتعلق فرنسا أهمية قصوى على المبادئ التي تنص على وجوب احترام حقوق الإنسان وتعزيزها على شبكة الإنترنت، وعلى ضرورة أن يتمتع الأفراد بنفس الحقوق على الإنترنت كما خارجه على حد سواء. ومنذ عام 1978، أصبحت اللجنة الوطنية لتكنولوجيا المعلومات والحريات هي الهيئة المسؤولة عن ضمان احترام حقوق الإنسان والحريات الأساسية، ولا سيما الحق في الخصوصية وحرية التعبير في البلد.

وتشارك فرنسا أيضا في اعتماد نظام أوروبي يأخذ في الاعتبار متطلبات التنافسية والإمكانات التي تتيحها التكنولوجيا الرقمية، مع الاستمرار في حماية المواطنين والشركات في الدول الأعضاء (بما يشمل الحق في الخصوصية وحماية البيانات الشخصية، وحماية الهياكل الأساسية الحيوية، ومكافحة المحتوى الإرهابي على شبكة الإنترنت). وقد كانت تلك الرغبة واضحة في عام 2016 أثناء اعتماد اللائحة (الاتحاد الأوروبي) رقم 2016/679 الصادرة عن البرلمان الأوروبي والمجلس بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وبشأن حرية نقل هذه البيانات، واعتماد التوجيه (الاتحاد الأوروبي) رقم 2016/1148 الصادر عن البرلمان الأوروبي والمجلس بشأن التدابير الرامية إلى تحقيق مستوى مشتركًا عاليًا من الأمن في شبكات ونظم المعلومات في جميع أنحاء الاتحاد، وفي الدعم الذي تقدمه فرنسا لتعزيز اختصاصات وكالة الاتحاد الأوروبي لأمن الفضاء الإلكتروني. وأخيرا، تعمل فرنسا على كفالة أن يوفر الاتحاد الأوروبي، من خلال سياسته الصناعية، الدعم للقدرات في مجال البحث والتطوير المتقدمين من أجل تعزيز نشر تكنولوجيا وخدمات الأمن الرقمي والاتصالات الموثوق فيها والخاضعة لتقييم مستقل. وشاركت فرنسا أيضاً بنشاط في صياغة المبادئ التوجيهية للاتحاد الأوروبي الخاصة بحقوق الإنسان في مجال حرية التعبير على الإنترنت وخارجه، التي اعتمدها المجلس في 12 أيار/مايو 2014.

وفي مجلس أوروبا، تؤيد فرنسا العمل على حماية حقوق الإنسان على الإنترنت. فقد أيدت، مثلاً، اعتماد "دليل حقوق الإنسان لمستخدمي الإنترنت" في نيسان/أبريل 2014، الذي صاغته لجنة الوزراء في المجلس، والذي يركز بشكل خاص على حرية التعبير، والوصول إلى المعلومات، وحرية تكوين الجمعيات، والحق في الخصوصية، وحماية البيانات الشخصية، والحماية من الجرائم الإلكترونية؛ وهذه الحقوق والحريات تنطبق على الإنترنت كما خارجه على حد سواء.

وفي الأمم المتحدة، أيدت فرنسا اعتماد جميع قرارات مجلس حقوق الإنسان بشأن تعزيز حماية حقوق الإنسان والتمتع بها على الإنترنت، وقرار الجمعية العامة 167/68 بشأن الحق في الخصوصية في العصر الرقمي.

وفي منتدى باريس الثاني للسلام، الذي عُقد في تشرين الثاني/نوفمبر 2018، أعلن رئيس فرنسا، إيمانويل ماكرون، و 11 رئيس دولة وحكومة آخرين أيضا إطلاق مبادرة حكومية دولية بشأن المعلومات والديمقراطية، بناء على العمل الذي أنجزته بالفعل منظمة مراسلون بلا حدود غير الحكومية بشأن هذا الموضوع. وهذه المبادرة الآن تحت رعاية التحالف من أجل تعددية الأطراف، الذي أطلقته فرنسا وألمانيا.

القاعدة (و): ينبغي للدولة ألا تقوم بأي نشاط من أنشطة تكنولوجيات المعلومات والاتصالات أو تدعمه عن علم بما يتعارض مع التزاماتها بموجب القانون الدولي ويتقصّد الإضرار بالهياكل الأساسية الحيوية المستخدمة في تقديم الخدمات إلى الجمهور أو يعطل، بأي شكل آخر، استخدام تلك الهياكل الأساسية الحيوية وتشغيلها.

وانطلاقا من روح هذه القاعدة، وكما ذُكر أعلاه، جرّمت فرنسا، في المادة 323-1 من القانون الجنائي، التدخلات غير المرخص بها في النظم الآلية لتجهيز البيانات الخاصة بأطراف ثالثة.

كما أن فرنسا قد أثبتت بوضوح، في العناصر العامة لعقيدتها، بما في ذلك كتابها الأبيض لعام 2019 بشأن القانون الدولي المطبق على العمليات في الفضاء الإلكتروني، أن القانون الدولي الإنساني ينطبق بشكل كامل على العمليات الإلكترونية التي تتم في سياق النزاع المسلح وفيما يتعلق به، على النحو الذي سيتم مناقشته بمزيد من التفصيل أدناه فيما يتعلق بالقانون الدولي.

القاعدة (ز): ينبغي أن تتخذ الدول التدابير المناسبة لحماية هياكلها الأساسية الحيوية من التهديدات المرتبطة بتكنولوجيات المعلومات والاتصالات، آخذة في اعتبارها قرار الجمعية العامة 199/58 بشأن إرساء ثقافة عالمية لأمن الفضاء الإلكتروني وحماية الهياكل الأساسية الحيوية للمعلومات وغيره من القرارات ذات الصلة.

وقد وضعت فرنسا، كما ذُكر أعلاه، إطارا تنظيميا لحماية الهياكل الأساسية الحيوية من خلال مطالبة المشغلين ذوي الأهمية الحيوية بتعزيز أمن نظم المعلومات الحساسة التي يشغّلونها، والمعروفة بنظم المعلومات ذات الأهمية الحيوية (القانون رقم 2013-1168 المؤرخ 18 كانون الأول/ديسمبر 2013)، وعن طريق تعزيز كفاءات الوكالة الوطنية لأمن الفضاء الإلكتروني وقدرتها على كشف الحوادث. ويجب على المشغلين الذين يتسمون بأهمية حيوية أيضا أن يعززوا تدابيرهم الأمنية وأن يستخدموا نظم الكشف التي توافق عليها الوكالة. وتشجع فرنسا على التعاون بين القطاعين العام والخاص لتطوير حماية الهياكل الأساسية الحيوية وتحديد إطار فعال ومناسب لذلك.

القاعدة (ح): ينبغي أن تستجيب الدول لطلبات المساعدة المناسبة التي تأتيها من دول أخرى تتعرض هياكلها الأساسية الحيوية لأعمال شريرة باستخدام تكنولوجيات المعلومات والاتصالات. وينبغي أن تستجيب الدول أيضا للطلبات المناسبة للتخفيف من ضرر نشاط من أنشطة تكنولوجيات المعلومات والاتصالات ينطلق من أراضيها ويستهدف الهياكل الأساسية الحيوية لدولة أخرى، مع مراعاة السيادة على النحو الواجب.

وللتوافق مع هذه القاعدة، أنشأت فرنسا، على سبيل المثال، شبكة للتعاون القائم على الثقة من خلال الشراكات التقنية للوكالة الوطنية لأمن الفضاء الإلكتروني، وهي شبكة تتيح، في جملة أمور، الاتصال بين أفرقة مواجهة الطوارئ الحاسوبية من خلال جهات اتصال دائمة.

ومن أجل تنظيم إدارة الأزمات، أنشأت فرنسا أيضا آلية دائمة مشتركة بين الوزارات لتحليل التهديدات والاستعداد لها والتنسيق بشأنها، في شكل مركز للتنسيق خلال الأزمات الإلكترونية. وبصفة خاصة، يتيح المركز تبادل المعلومات على نحو سلس فيما بين مختلف الدوائر لتحسين التنسيق الوطني وتلبية هذه الاحتياجات.

وأنشأت فرنسا أيضا شبكة تعمل على مدار الساعة مؤلفة من نقاط اتصال بموجب الاتفاقية المتعلقة بالجريمة الإلكترونية للسماح بتجميد البيانات.

وفي منظمة الأمن والتعاون في أوروبا، تشارك فرنسا في وضع قائمة بأسماء نقاط الاتصال المنشأة عملا بالتدبير 8 من تدابير بناء الثقة الواردة في مقرر المجلس الدائم رقم 1106، كما دعمت مختلف الجهود الرامية إلى كفالة قيام كل دولة بإنشاء قنوات مناسبة للتواصل وتبادل المعلومات وفقا للتدبير 13 من تدابير بناء الثقة الواردة في قرار المجلس الدائم رقم 1202.

القاعدة (ط): ينبغي أن تتخذ الدول خطوات معقولة لكفالة سلامة سلسلة التوريد حتى يمكن للمستخدمين النهائيين الوثوق بأمن منتجات تكنولوجيات المعلومات والاتصالات. وينبغي للدول أن تسعى إلى منع انتشار أدوات وتقنيات تكنولوجيات المعلومات والاتصالات الكيدية واستخدام الوظائف الخفية الضارة.

وشجعت فرنسا على وضع قواعد ومعايير لهذه الصناعة، ولا سيما من خلال نداء باريس. كما شجعت على بدء العمل الدولي بشأن هذا الموضوع في منتديات مختلفة، وذلك أساسا من خلال فرقة العمل المعنية بالاقتصاد الرقمي التابعة لمجموعة العشرين وفي منظمة التعاون والتنمية في الميدان الاقتصادي.

وشجعت فرنسا أيضا على استخدام مبادئ التصديق من أطراف ثالثة، تحت سلطة الوكالة الوطنية لأمن الفضاء الإلكتروني، لكفالة أن يقدم السوق أعلى المستويات الأمنية. ويجري حالياً تجريب هذه العملية في الوكالة من قبل المركز الوطني للتصديق. كما شجعت فرنسا على استحداث عمليات التصديق على مستوى الاتحاد الأوروبي.

وبغية تعزيز الجهود المبذولة لمكافحة انتشار التقنيات والأدوات الضارة، أيدت فرنسا أيضا إدراج برمجيات الاختراق على قائمة السلع المزدوجة الاستخدام الواردة في ترتيب فاسنار بشأن ضوابط تصدير الأسلحة التقليدية والسلع والتكنولوجيات المزدوجة الاستخدام.

القاعدة (ي): ينبغي للدول أن تشجع على الإبلاغ المسؤول عن نقاط الضعف المتصلة بتكنولوجيات المعلومات والاتصالات وأن تقدم ما لديها من معلومات ذات صلة حول الوسائل المتاحة لعلاجها من أجل تقليل، وربما استئصال، التهديدات المحتملة التي تتعرض تكنولوجيات المعلومات والاتصالات والهياكل الأساسية المعتمِدة على هذه التكنولوجيات.

وكما ذُكر أعلاه، اتخذت فرنسا مختلف الخطوات للسماح بالكشف عن الثغرات الحاسوبية على نحو مسؤول، كما طورت التعاون على المستوى التقني من خلال الوكالة الوطنية لأمن الفضاء الإلكتروني، التي تتبادل بانتظام المعلومات عن الثغرات والحلول المتاحة مع نظرائها وشركائها.

القاعدة (ك): ينبغي للدول ألا تجري أو تدعم عن علم أي نشاط يلحق الضرر بنظم المعلومات الخاصة بأفرقة الاستجابة لحالات الطوارئ المفوضة (المعروفة أحياناً بأفرقة مواجهة الطوارئ الحاسوبية أو أفرقة الاستجابة لحوادث أمن الفضاء الإلكتروني) التابعة لدولة أخرى. وينبغي ألا تستخدم أي دولة أفرقة الاستجابة لحالات الطوارئ المفوضة في القيام بأنشطة دولية شريرة.

وكان القانون رقم 88-19، الذي صدر في 5 كانون الثاني/يناير 1988 بشأن الاحتيال الحاسوبي، المعروف باسم قانون غودفران، أول قانون فرنسي يعاقب على جرائم الحاسوب والقرصنة. ويجرّم القانون فعل الدخول عن طريق الاحتيال إلى أي من النظم الآلية لتجهيز البيانات، جزئيا أو كليا، أو البقاء فيها.

ويكفل نموذج الإدارة الفرنسي، الذي يستطيع تمييز القدرات الهجومية عن القدرات والمهام الدفاعية، احترام هذا المبدأ. وتشمل مهام الفريق الحكومي لمواجهة الطوارئ الحاسوبية تنسيق الاستجابة للحوادث الإلكترونية والتحقيق فيها، ليس فقط بالنسبة للحكومة ولكن أيضا بالنسبة لمشغلي الهياكل الأساسية الحيوية والخدمات الأساسية على النحو المحدد في القانون، وذلك بمساعدة هؤلاء المشغلين على تحديد المستوى اللازم من الحماية، والكشف عن الثغرات في الشبكات والنظم، وتنظيم الاستجابة للحوادث، بمساعدة من الشركاء إذا لزم الأمر، والمشاركة في شبكة موثوقة من أفرقة مواجهة الحوادث الأمنية الحاسوبية.

تطبيق القانون الدولي، بما في ذلك ميثاق الأمم المتحدة، على الفضاء الإلكتروني: مبدأ آخر حظي باعتراف فريق الخبراء الحكوميين

ترى فرنسا أن وضع إطار إجماعي لأمن الفضاء الإلكتروني لا يمكن أن يقوم إلا على الامتثال لقواعد القانون الدولي. ولذلك، فإنها لا تعتقد أنه ينبغي في هذه المرحلة وضع صك دولي جديد ملزم قانونا مكرس لمواجهة التحديات التي يواجهها أمن الفضاء الإلكتروني. فالقانون الدولي القائم ينطبق على الفضاء الإلكتروني كما ينطبق على مجالات أخرى، ويجب احترامه.

وكما خلص فريق الخبراء الحكوميين في تقريره لعام 2013، فإن مبادئ وقواعد القانون الدولي تنطبق على سلوك الدول في الفضاء الإلكتروني. ورغم أن الفضاء الإلكتروني له خصائصه المميزة، من قبيل سرية الهوية ودور الجهات الفاعلة من القطاع الخاص، لكنه يوفر الوسائل اللازمة لضبط سلوك الدول بطريقة مسؤولة في هذه البيئة.

وينطبق مبدأ السيادة على الفضاء الإلكتروني. ولذا تؤكد فرنسا من جديد أنها تمارس سيادتها على نظم المعلومات وعلى الأشخاص والأنشطة الإلكترونية على أراضيها أو ضمن حدود ولايتها، وفقا لالتزاماتها بموجب القانون الدولي. وما يمكن أن يشكل انتهاكًا للسيادة هو الاختراق غير المأذون به للنظم الفرنسية وإحداث آثار على الأراضي الفرنسية بوسائل إلكترونية هجومية من قبل جهة تابعة للدولة أو غير تابعة لها تعمل بإيعاز من إحدى الدول أو تحت إشرافها.

ويتوقف نطاق التدابير التي يمكن أن تتخذها الدول تصديًا لهجوم إلكتروني محتمل على خطورة آثار هذا الهجوم. ولذا يمكن اعتبار أي عملية إلكترونية استخداما للقوة محظورا بموجب الفقرة 4 من المادة 2 من ميثاق الأمم المتحدة. ولا يتوقف تجاوز تلك العتبة على الوسائل الإلكترونية المستخدمة بل بالأحرى على آثار العمليات الإلكترونية. فإذا ماثلت هذه الآثار نظيرتها الناتجة عن استخدام الأسلحة التقليدية، فيمكن اعتبار العملية الإلكترونية بمثابة استخدام للقوة. وترى فرنسا أنه إذا كان نطاق أو آثار هجوم إلكتروني كبير تشنه جهات فاعلة تابعة للدول أو غير التابعة لها تعمل تحت إشراف دولة ما أو بإيعاز منها، تصل إلى عتبة كافية (من قبيل الخسائر الكبيرة في الأرواح، أو الأضرار المادية الكبيرة، أو إعطاب الهياكل الأساسية الحيوية التي تسفر عن عواقب وخيمة)، فإن ذلك الهجوم يمكن أن يشكل "عدوانا مسلحا" بالمعنى المقصود في المادة 51 من الميثاق، ما يبرر بالتالي الحق بالدفاع عن النفس. ويجوز اللجوء إلى الدفاع عن النفس بالوسائل التقليدية أو الإلكترونية، وفقا لمبدأي الضرورة والتناسب. وتوصيف الهجوم الإلكتروني بأنه

”عدوان مسلح“، بالمعنى المقصود في المادة 51 من الميثاق، هو قرار سياسي يُتَّخذ على أساس كل حالة على حدة وفي ضوء المعايير المحددة في القانون الدولي.

وتعترف فرنسا أيضا بأن القانون الدولي الإنساني ينطبق تمامًا على العمليات الإلكترونية التي تجري في سياق النزاعات المسلحة أو في ما يتعلق بها. وتُنفَّذ العمليات الإلكترونية الهجومية حاليًا بالاقتران مع العمليات العسكرية التقليدية.

وتظل هذه العمليات، بالرغم من طابعها غير المادي، خاضعة للنطاق الجغرافي لتطبيق القانون الدولي الإنساني؛ وبعبارة أخرى، تقتصر آثارها على أراضي الدول الأطراف في نزاع مسلح دولي أو تقتصر، في سياق نزاع مسلح غير دولي، على الأراضي التي تقع فيها الأعمال العدائية. وتخضع عمليات المكافحة الإلكترونية الهجومية التي تنفذها القوات المسلحة الفرنسية لاحترام مبادئ القانون الدولي الإنساني، بما يشمل ما يلي:

- مبدأ التمييز بين الأصول المدنية والأهداف العسكرية. من هذا المنظور، تُحظر الهجمات الإلكترونية غير الموجهة ضد هدف عسكري محدد أو التي تنفَّذ بواسطة أسلحة إلكترونية لا يمكن توجيهها ضد هدف عسكري محدد. وفي هذا الصدد، قد تشكل بعض البيانات، رغم أنها غير ملموسة، أصولا مدنية محمية بموجب القانون الدولي الإنساني. ووفقا لهذا المبدأ، يجب التمييز بين المقاتلين، أو أفراد الجماعات المسلحة المنظمة، والمدنيين. ولا يجوز أيضا أن تستهدف العمليات السكان المدنيين عمومًا أو الأفراد المدنيين، ما لم يشاركوا مباشرة في الأعمال العدائية، على أن يكون الاستهداف، في هذه الحالة، أثناء فترة مشاركتهم تلك. وفي سياق النزاع المسلح، يجوز شن هجوم بالوسائل التقليدية أو الإلكترونية ضد أي مقاتل إلكتروني تابع للقوات المسلحة لأي طرف في النزاع، أو أي عضو في جماعة مسلحة منظمة يرتكب هجمات إلكترونية ضد طرف آخر، وأي مدني يشارك مباشرة في الأعمال العدائية عبر وسائل إلكترونية؛
- مبدأ التناسب والمبدأ الوقائي. يجب أن تُنفذ العمليات مع الحرص الدائم على حماية الأشخاص المدنيين والأصول المدنية من آثار الأعمال العدائية. يجب أن تكون الأضرار التبعية متناسبة مع المكاسب العسكرية الملموسة والمباشرة المتوخاة. ويتطلب مبدأ التناسب في الفضاء الإلكتروني مراعاة جميع الآثار المتوقعة لاستخدام السلاح، بالإضافة إلى كونها مباشرة (من قبيل تضرر النظام المستهدف أو انقطاع الخدمة)، أو غير مباشرة (الآثار المترتبة على الهياكل الأساسية التي يتحكم فيها النظام الذي يتعرض للهجوم، وعلى الأشخاص المتضررين من إعطاب النظم أو تدميرها أو من تغيير البيانات أو إفسادها) بشرط أن يكون بين تلك الآثار والهجوم علاقة سببية كافية. ووفقاً لهذا المبدأ، يُحظر أيضاً استخدام الأسلحة الإلكترونية التي لا يمكن التحكم فيها في الزمان والمكان.

وترد هذه المعلومات في التقرير عن القانون الدولي المطبق على العمليات في الفضاء الإلكتروني، الذي نشرته وزارة القوات المسلحة في 9 أيلول/سبتمبر 2019، وكذلك في العناصر العامة للعقيدة العسكرية الفرنسية بشأن الحرب الإلكترونية الهجومية، الذي نُشر في العام نفسه.

وترى فرنسا أن من الضروري التوصل إلى فهم مشترك على الصعيد الدولي للالتزامات التي تقع على عاتق الدولة التي قد تُستخدم بناها التحتية لأغراض خبيثة، وذلك ضد مصالح دولة أخرى. والغرض

من ذلك هو توضيح كيفية انطباق مبدأ بذل العناية الواجبة على الفضاء الإلكتروني، وهو المبدأ الذي ينص على أن كل دولة ملزَمة "بعدم السماح، عن علم، باستخدام أراضيها لارتكاب أعمال تمس بحقوق دول أخرى"[4]. وبناء على ذلك، ينبغي للدول ألا تسمح عن علم باستخدام أراضيها في أعمال ترتكب بوسائل إلكترونية ويُحظرها القانون الدولي، ويجب عليها أن تتخذ جميع التدابير التي يمكن أن يتوقع منها على نحو معقول أن تكفل عدم استخدام أراضيها من جانب جهات فاعلة من غير الدول لارتكاب تلك الأعمال. وقد اعتبرت فرنسا تنظيم قدرة الجهات الفاعلة من القطاع الخاص على الاستجابة للحوادث مجالا هاما من مجالات العمل، يمكن أن يساعد على ضمان احترام مبدأ بذل العناية الواجبة عن طريق الحد من الإجراءات التي تؤثر سلبا على الأطراف الثالثة[5]. ومن شأن تحسين فهم كيفية انطباق هذا المبدأ على التحديات الماثلة في هذا المجال أن يعزز التعاون بين الدول بهدف حماية بعض الهياكل الأساسية الحيوية، وإحباط الهجمات الإلكترونية الكبرى التي قد تمر عبر بلدان ثالثة.

جورجيا

[الأصل: بالإنكليزية]
[29 أيار/مايو 2020]

فيما تشجع حكومة جورجيا على إيجاد حلول آمنة ومرنة ومُحكمة وموثوقة للحكومة الإلكترونية، وتطوير مجتمع المعلومات ككل، فإنها تدرس بدقة أي فرصة متاحة لتناول توصيات فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي بشأن الارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني. وتطمح جورجيا إلى الإسهام بنشاط في المبادئ العامة والمبادئ التوجيهية التي وضعها الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وفي وضع آليات وطنية مكرسة تحقيقًا لذلك الغرض.

وتلخص هذه الوثيقة التحديثات الهامة بشأن أمن الفضاء الإلكتروني وتطوير أمن المعلومات في جورجيا والجهود المبذولة على الصعيد الوطني لتعزيز أمن المعلومات وتشجيع التعاون الدولي في هذا الميدان.

ولا تزال جورجيا ملتزمة بتطوير وضعها في مجال أمن الفضاء الإلكتروني والتقدم نسبيًا بمركزها في هذا المجال على الساحة الدولية. ومن الواضح أن الظروف الجيوسياسية لجورجيا تزيد من المخاطر التي تتعرض لها جهودها في مجال تطوير أمن الفضاء الإلكتروني. ففي 28 تشرين الأول/أكتوبر 2019، شُنّ هجوم إلكتروني واسع النطاق على المواقع الشبكية والخواديم وغيرها من نظم التشغيل التابعة لإدارة رئيس جورجيا، والمحاكم، ومختلف المجالس البلدية، وهيئات الدولة، ومنظمات القطاع الخاص، ووسائل الإعلام. وقد استهدف الهجوم الإلكتروني الأمن القومي لجورجيا، وكان القصد منه هو إلحاق الضرر بالمواطنين الجورجيين والهياكل الحكومية الجورجية عن طريق تعطيل وشل سير العمل لدى مختلف المنظمات. وأسفر التحقيق الذي أجرته السلطات الجورجية، إلى جانب المعلومات التي جُمعت من خلال التعاون مع شركائنا، عن أن هذا الهجوم الإلكتروني قد خططت له ونفذته الشعبة الرئيسية في هيئة الأركان

(4) *Corfu Channel case, Judgment of 9 April 1949, I.C.J. Reports 1949*, p. 4.

(5) ينبغي أن تستند هذه اللائحة، التي يُفترض أن يُسترشد بمبدئها الأساسي في عمل فريق الخبراء الحكوميين، إلى تحليل للمخاطر يتعلق بالتدابير التي يمكن أن تتخذها الجهات الفاعلة من القطاع الخاص على مسؤوليتها الخاصة استجابة لحادث ما.

العامة للقوات المسلحة في الاتحاد الروسي. ويمثل الحادث المذكور أعلاه تأكيدا لأهمية الجهود التي تبذلها الحكومة الجورجية لتعزيز أمن الفضاء الإلكتروني على الصعيد الوطني، ودليلا آخر على ضرورة تعزيز الشراكة الدولية في مجال أمن الفضاء الإلكتروني.

وتوجه جورجيا جميع مواردها لتصبح بلدا أشد قوة ومنعَة وأمنًا في الفضاء الإلكتروني. وعلى وجه الخصوص، تسعى الحكومة الجورجية إلى تمكين كل مجموعة مستهدفة من مجتمع المعلومات من امتلاك المستوى المطلوب من المعرفة والخبرة لمواجهة التهديدات الإلكترونية. ويوفر نموذج الحوكمة في جورجيا القدرة للمنظمات العامة والخاصة على حد سواء، وبشكل جماعي ومستقل كذلك، على كفالة أمن الفضاء الإلكتروني في البلد والاستدامة ذات الصلة من خلال المشاركة في تقاسم الموارد. وبالإضافة إلى ذلك، تتمتع جورجيا، بوصفها شريكا موثوقا به في مجال أمن الفضاء الإلكتروني، بإشادة شركائها الدوليين ودعمهم على الصعيد الدولي.

وتسعى حكومة جورجيا جاهدة إلى توفير فضاء إلكتروني مفتوح وسالم وآمن. فأمن الفضاء الإلكتروني هو توجه استراتيجي يحظى باهتمام سياسي كبير ويتناول سياسة الأمن الوطني التي تنتهجها حكومة جورجيا ويجعلها أكثر تطورا وقدرة على الصمود. وترى الحكومة أن من حقها تهيئة بيئة تمكينية لمجتمع المعلومات والاقتصاد الرقمي والحكومة الإلكترونية في البلد؛ فالحكومة مسؤولة عن وضع الأطر الاستراتيجية، والمؤسسية – الإدارية، والقانونية – التنظيمية ذات الصلة التي من شأنها أن تدعم سلامة وأمن الأداء الوظيفي للمواطنين، وكذلك القطاعين العام والخاص في بيئة إلكترونية، مع مراعاة استخدامهم الفضاء الإلكتروني بأمان.

ويحتل تعزيز التعاون الثنائي والإقليمي والدولي في مجال أمن الفضاء الإلكتروني مرتبة متقدمة على جدول الأعمال السياسي لحكومة جورجيا. وجورجيا مثال جيد للشراكة على الصعيدين الإقليمي والدولي، وفي صيغ متعددة الأطراف (الاتحاد الأوروبي، ومنظمة حلف شمال الأطلسي، ومنظمة الأمن والتعاون في أوروبا، والأمم المتحدة، والشراكة الشرقية، ومجلس أوروبا، ووكالة الاتحاد الأوروبي للتعاون في مجال إنفاذ القانون، ومنظمة الشرطة الجنائية الدولية، ووكالة الاتحاد الأوروبي للتدريب على إنفاذ القانون، ووكالة الاتحاد الأوروبي لأمن الفضاء الإلكتروني). وتشارك جورجيا بنشاط في المشاريع والاجتماعات الدولية المتعلقة بأمن الفضاء الإلكتروني.

وفي السنوات الماضية، تم تنفيذ مبادرات التعاون والشراكة التالية:

- الخطوات الرامية إلى تعزيز أمن الفضاء الإلكتروني التي اتخذتها جورجيا في العقد الماضي هي خطوات إيجابية، كما تحظى الإصلاحات المكتملة والعمليات الجارية بتقييم إيجابي على الصعيد الدولي. وتحتل جورجيا مركزا متقدما وموقعا رائدا في مجال تطوير أمن الفضاء الإلكتروني في الشراكة الشرقية، ولهذا السبب تشارك بلدانُ المنطقة في أنشطة متعددة لبناء القدرات وتبادل المعلومات وأفضل الممارسات، التي تضطلع فيها جورجيا بدور مركز إقليمي لأمن الفضاء الإلكتروني.
- ولا يزال التعاون بين جورجيا وحلف الناتو في مجال أمن الفضاء الإلكتروني في مرحلة التطوير. جورجيا في مرحلة نشطة من التعاون مع الدول الأعضاء في حلف الناتو وتشارك بشكل فردي وجماعي في مختلف المشاريع التي تدار تحت رعاية الحلف. ويشمل ذلك أيضا مشاركة جورجيا في مبادرات التعلم الاستراتيجية أو التقنية. ويساعد الناتو (المقر ومكتب الاتصال) السلطات

الإلكترونية الجورجية في القيام بأنشطة منتظمة ومستمرة للتوعية والتدريب في جميع أنحاء جورجيا موجهة إلى مختلف الفئات المستهدفة. وتقدم جورجيا بانتظام إنجازاتها ومبادراتها في مجال أمن الفضاء الإلكتروني إلى اللجنة المشتركة بينها وبين الحلف، وتوجه نفسها عن كثب باستخدام تعهد حلف الناتو للدفاع الإلكتروني.

- جورجيا والاتحاد الأوروبي. من خلال البرنامج الخمسي "الأمن والمساءلة ومكافحة الجريمة في جورجيا – الاتحاد الأوروبي 4" تتلقى جورجيا المساعدة من الاتحاد الأوروبي في مجالات الجريمة الإلكترونية، والتصدي للتهديدات الإلكترونية والهجينة، وإدارة الحدود، والحماية المدنية، والإشراف على قطاع الأمن. وعززت جورجيا تعاونها في إطار منبر الاتحاد الأوروبي للسياسة المشتركة للأمن والدفاع، الذي يعكس الأهداف الاستراتيجية المحددة دوليا للمنظمة، ويدعم إجمالاً توطيد الأمن الوطني لجورجيا من خلال تطوير قدراتها الدفاعية.

- جورجيا ومنظمة الأمن والتعاون في أوروبا. ترى جورجيا قيمة كبيرة في بناء شبكة موثوقة بين البلدان الشريكة، يمكن تمكينها من خلال تدابير بناء الثقة في مجال الأمن الإلكتروني. وتشارك جهات الاتصال الجورجية بنشاط في منبر أمن الفضاء الإلكتروني لمنظمة الأمن والتعاون في أوروبا وفي مبادراتها.

- وقّعت حكومتا جورجيا والمملكة المتحدة على مذكرة التفاهم بشأن التعاون في مجال الأمن الإلكتروني التي تهدف إلى تعزيز العمل المتبادل، وتبادل أفضل الممارسات، وتحسين مواءمة النُهج بشأن مختلف مواضيع الأمن الإلكتروني.

- جورجيا وبلدان الشراكة الشرقية. تواصل وكالة تبادل البيانات التعاون مع بلدان الشراكة الشرقية في نطاق برنامج "الاتحاد الأوروبي 4 الرقمي: تحسين القدرة على الصمود في وجه الهجمات الإلكترونية في بلدان الشراكة الشرقية". ويساعد مشروع "سايبر إيست" جورجيا وبلدان الشراكة الشرقية الأخرى على زيادة القدرات في مجال التصدي للهجمات الإلكترونية، والعدالة الجنائية، والأدلة الإلكترونية، لبلدان الشراكة الشرقية، من أجل التصدي بشكل أفضل للجريمة الإلكترونية. وينصب التركيز على تحسين الأطر القانونية والسياساتية؛ وتعزيز قدرات السلطات القضائية وسلطات إنفاذ القانون والتعاون بين الوكالات؛ واستحداث آليات فعالة للتعاون الدولي بغية زيادة الثقة في العدالة الجنائية، والجرائم الإلكترونية، والأدلة الإلكترونية، لدى جهات منها مقدمي الخدمات وسلطات إنفاذ القانون.

- تواصل جورجيا تعزيز التعاون الإقليمي مع البلدان المجاورة تحت مظلة منظمة الديمقراطية والتنمية الاقتصادية. ففي عام 2019، شارك ممثلون جورجيون في اجتماعات عقدت في مقر المنظمة في كييف.

- وقّع فريق مواجهة الطوارئ الحاسوبية، وهو وحدة فرعية من وكالة تبادل البيانات التابعة لوزارة العدل في جورجيا، عددا كبيرا من مذكرات التعاون لتبادل المعارف والخبرات مع المنظمات المعنية في بلدان الشراكة الأوروبية والشرقية (أي ليتوانيا ورومانيا ومولدوفا وأوكرانيا وبيلاروس). وتشارك جورجيا بنشاط في البرامج الدولية للتدريبات الإلكترونية والبرامج الدراسية، التي يحتل فيها البلد باستمرار مركزا متقدما من حيث النتائج الملحوظة.

ومن الناحية العملية، تَعتبر جورجيا، بما لديها من معارف وطنية ضخمة في هذا المجال، أفضلَ الخبرات الدولية وأكثرها أهمية بمثابة توجيهات وفرص قيّمة للتعاون في وضع ركائزها الاستراتيجية والقانونية والمؤسسية وركائز بناء القدرات، وكذلك لعملية التحول في مجال الثقافة الإلكترونية.

والتعاون النشط بين الوكالات القطاعية[6] في مجال الأمن الإلكتروني، تم وضع المشروع الثالث للاستراتيجية الوطنية للأمن الإلكتروني وخطة العمل المتصلة بها في جورجيا في عام 2019[7]. واضطلع مكتب مجلس الأمن القومي بدور تنسيقي في هذه العملية. وفي الوقت نفسه، شارك أيضا أصحاب المصلحة المعنيون من القطاع الخاص والأوساط الأكاديمية والمجتمع المدني في كل من هذه المساعي. وفي الوقت الذي تسعى فيه جورجيا جاهدة إلى جعل إطارها الوطني متوافقا مع الآليات الأوروبية الأطلسية المعنية، فإن الخبراء الأجانب والخبراء الاستشاريين الوطنيين ذوي التفكير المماثل ينصحون بشدة بتنفيذ عملية التنمية الاستراتيجية. وتكتسي المساعدة التي قدمتها المملكة المتحدة إلى الجهات الفاعلة ذات الصلة في مجال أمن الفضاء الإلكتروني في جورجيا أهمية خاصة في سياق صياغة الاستراتيجية الوطنية لأمن الفضاء الإلكتروني وخطة العمل ذات الصلة اللتين ستعتمدهما حكومة جورجيا خلال عام 2020. وستخضع الوثائق المعنية للتدقيق من جانب اللجنة الدائمة المشتركة بين الوكالات التي أنشئت في كانون الثاني/يناير 2020 في مجلس الأمن الوطني، وعهد إليها بمهمة التنسيق في إعداد الوثائق المفاهيمية على الصعيد الوطني في ميدان الأمن. ومن ثم سيقدم مجلس الأمن القومي مشاريع الوثائق إلى حكومة جورجيا للموافقة عليها.

وتواصل جورجيا تعزيز إنفاذ الأطر القانونية والتنظيمية المتعلقة بالمجالات الإلكترونية. ونُفذت في جورجيا أطر تشريعية وتنظيمية شاملة في مجال تكنولوجيا المعلومات والاتصالات تتناول الأمن الإلكتروني، واعتُمدت فيها تشريعات لحماية حقوق الأفراد والمنظمات في البيئة الرقمية. وتتناول القوانين حماية الهياكل الأساسية الحيوية للمعلومات، ومسؤولية مقدمي خدمات الإنترنت، والتزامات الإبلاغ عن الحوادث، وأمن العمليات الإلكترونية. ولدى جورجيا، كخطوة تالية، خطط طموحة لجعل إطارها القانوني للأمن الإلكتروني متوافقا مع الأمر التوجيهي الصادر عن الاتحاد الأوروبي بشأن أمن الشبكات ونظم المعلومات. وبالتحديد، بدأت الوكالات المسؤولة، خلال عام 2019، عملية التعاون مع الاتحاد الأوروبي، وبحلول نهاية هذا العام، سيتم إعداد "بطاقة التوأمة"، بهدف مساعدة جورجيا في عملية المواءمة. ونتيجة لمشروع التوأمة، ستقوم جورجيا بتحديث قانون أمن المعلومات الخاص بها، الذي سيحدد بوضوح، من بين جوانب أخرى هامة، إطار حوكمة الأمن الإلكتروني، وصلاحيات الأمر التوجيه، والأدوار والمسؤوليات في مجال أمن الفضاء الإلكتروني على المستويات الاستراتيجية والتشغيلية والتكتيكية.

وبدأت جورجيا أيضا عملية طموحة أخرى لتصميم واعتماد نموذج متوافق مع الاتحاد الأوروبي لحماية الهياكل الأساسية الحيوية للمعلومات. وخلال عام 2019، نُظِّمت عدة حلقات عمل لمناقشة وضع نظام مناسب لتحديد الهياكل الأساسية الحيوية في مجال الإنترنت والتعاون معها. وقد وضعت جورجيا منهجية ذات صلة واستبيانات تتعلق بالهياكل الأساسية الحيوية للمعلومات. وشملت العملية إجراء مناقشات مع ممثلي القطاع الحيوي المملوك للقطاع الخاص من مختلف القطاعات ومجالات الأعمال.

(6) وكالة تبادل البيانات (وزارة العدل)، ومكتب أمن الفضاء الإلكتروني(وزارة الدفاع)، والوكالة التشغيلية والتقنية (دائرة أمن الدولة).

(7) مُتوقعة لفترة السنوات الثلاث 2020–2023.

ويجري حاليا تنفيذ سياسة أمن المعلومات والاحتياجات المتعلقة بأمن الفضاء الإلكتروني في جميع المنظمات المعتبرة هياكل أساسية حيوية للمعلومات. وتساعد الوكالات الحكومية المسؤولة هذه الكيانات في تنفيذ سياسات أمن المعلومات والتدابير الأساسية لأمن الفضاء الإلكتروني، وتقدم التوصيات والخبرات والتدريبات، وكذلك من خلال الاضطلاع بأنشطة أكثر شمولا، من قبيل عمليات مراجعة أمن المعلومات، واختبار الاختراق، وغير ذلك من خدمات المعلومات والأمن الإلكتروني. وقد بدأت مشاريع مختلفة لتنفيذ نظام لإدارة أمن المعلومات في الوكالات التي تشكل جزءا من النظم الحيوية للمعلومات. وتتلقى هذه الكيانات الدعم في اعتماد سياسات أمن المعلومات، ومهام إدارة الأصول، واستعراضات السياسات. وفي الوقت نفسه، تضع الحكومة معايير وإجراءات لأمن المعلومات من خلال سن التشريعات والقوانين المحلية (استناداً إلى المجموعة 27000 من معايير ISO) وتنظّم دورات تدريبية بشأن أمن المعلومات لممثلي الحكومات والقطاع الخاص. والهدف التالي هو وضع واعتماد أحكام قانونية بشأن حماية الهياكل الأساسية الحيوية للمعلومات في اتساق مع التوجيه الصادر عن الاتحاد الأوروبي بشأن أمن الشبكات ونظم المعلومات، بما يضمن قابلية تطبيق الأحكام القانونية الموسعة المتعلقة بأمن الشبكات ونظم المعلومات على التدابير المتخذة لحماية الهياكل الأساسية الحيوية للمعلومات.

وقد نجحت حكومة جورجيا في استخدام منصات أصحاب المصلحة المتعددين المشتركة بين القطاعين العام والخاص كأداة لبناء الثقة بين جميع أصحاب المصلحة وتبادل المعلومات والمعارف، وإطلاق مبادرات جديدة، وتمكين القطاع الخاص من المشاركة في عملية وضع السياسات والاستراتيجيات. وقد قامت وكالة تبادل البيانات، التي تقود عملية التعاون بين القطاعين العام والخاص، بتنظيم العديد من حلقات العمل والاجتماعات خلال عام 2019 مع قطاعات المالية والطاقة والاتصالات السلكية واللاسلكية من أجل الانضمام إلى المشاورات التحضيرية لعملية تحديد الهياكل الأساسية الحيوية. وأصحاب المصلحة من القطاع الخاص هم جزء من جميع عمليات التشاور الرئيسية بشأن المشاريع الأفقية في إطار المبادرات المتعلقة بالاستراتيجيات والسياسات والقوانين والتنظيمات وبناء القدرات.

وتضطلع جورجيا بأنشطة منهجية ومستمرة للتوعية والتدريب من أجل بناء القدرة المهنية والكفاءة في مجال الفضاء الإلكتروني، وتلك الأنشطة موجهة إلى مختلف الفئات المستهدفة. ومن خلال إشراك المنظمات الحكومية في جورجيا، نُفذت حملات واسعة النطاق للتوعية تَمثّل الهدف منها في زيادة مستوى معرفة السكان بنظافة الفضاء الإلكتروني؛ كما يجري حالياً تنفيذ برامج التعلم وإعادة التدريب الموجهة لمختلف الفئات المستهدفة في مجال الأمن الإلكتروني. وسنة بعد سنة، يتحسّن مستوى نضج قدرات أمن الفضاء الإلكتروني الجورجية نتيجة لمختلف المبادرات والبرامج التعليمية، وكانت حكومة جورجيا ولا تزال نشطة جدا في محاولاتها لرفع مؤهلات المهنيين العاملين في مجال أمن الفضاء الإلكتروني في القطاع العام. وقد اكتسبوا، نتيجة لذلك، كفاءات مهنية عالية، كما أن الكثير منهم حائز على شهادات معترف بها دوليا وذات سمعة عالية (معهد SANS، ورابطة مراجعة ومراقبة نظم المعلومات، والمنظمة الدولية لتوحيد المقاييس).

وأخيرا، ستواصل جورجيا مشاركتها النشطة في الحوار الدولي بشأن حوكمة الإنترنت وغيرها من المبادرات الدولية المتعلقة بأمن الفضاء الإلكتروني الجماعي.

هندوراس

[الأصل: بالإسبانية]
[17 نيسان/أبريل 2020]

تقرير عن التدابير المتخذة فيما يتعلق بأمن الفضاء الإلكتروني في سياق الأمن الدولي

تتخذ الشـــرطـة الوطنيـة في هندوراس مختلف الخطوات على الصـــعيد الداخلي في ســـياق المعيار 27001 (المعيار الدولي لأمن المعلومات) من معايير المنظمة الدولية لتوحيد المقاييس بهدف إيجاد ثقافة عمل تتســـق مع مبادرة الحكومة الرقمية التي يروج لها مكتب رئيس الجمهورية. وتركز هذه الخطوات على الاستخدام المسؤول لموارد الإنترنت وفقا لدليل أمن المعلومات، الذي يتضـمن بيانا واضـحا بالسـياسـة العامة الموضـوعة لحماية مختلف الأنشـطة التنفيذية التي يضـطلع بها عناصـرنا وتقليص الثغرة القائمة التي يمكن أن تتسبّب في وقوع أنظمتنا ضحية لهجوم أو لعمل شرير.

ويرد فيما يلي بعض التدابير التي اعتمدتها الشرطة الوطنية فيما يتعلق بالفضاء الإلكتروني.

1 - تطوير سياسة أمن المعلومات

تضـــع ســـياســـة أمن المعلومات معايير ومبادئ توجيهية لكفالة الاســـتخدام المناســـب للأدوات التكنولوجية المصممة لحماية تكنولوجيا المعلومات والموارد المادية للشرطة، باعتبارها مُدخلا أساسيا في أداء مهمتها الدستورية، وضمان مواصلة تحسين هذه المهمة وإدارتها وحمايتها من خلال التطبيق الفعال لأفضل الممارسات والضوابط وضمان السرية، وإتاحة المعلومات وسلامتها بشكل عام.

2 - الدورات التدريبية

تعقد الشـــرطة الوطنية في هندوراس بانتظام، من خلال مديرية الاتصـــالات المعلوماتية البُعدية التابعة للشـرطة، دورات توعية بشـأن الفضـاء الحاسـوبي للموظفين التنفيذيين والإداريين. وتشـارك أيضـا في أنشـطة خاصـة، حيث تقدم التدريب على قضـايا من قبيل التنمر عبر الإنترنت، والهندسـة الاجتماعية، والأخبار المزيفة، والجرائم الإلكترونية، والأمن الإلكتروني.

3 - تنفيذ شبكة محلية

تُسـتخدم صـفحة الإنترانت الخاصـة بنا "Poliweb" لإبقاء موظفينا على علم بأحدث الاتجاهات في مجال الجريمة الإلكترونية، ونشـر رسـائل إخبارية هامة عن تطورات أمن الفضـاء الإلكتروني في بيئتنا، ونشر السياسات المستمدة من دليل أمن المعلومات من أجل المحافظة على أمن الحواسيب.

وتتيح هذه القدرة الداخلية على الاتصـال الإلكتروني تنفيذ جميع العمليات الداخلية للشـرطة الوطنية من خلال شبكتنا المحلية أو الإنترانت، ما يقلل من خطر وصول مستخدمينا إلى مواقع غير معروفة والحفاظ على موارد الإنترنت وعرض النطاق الترددي.

4 - إدارة الحوادث والتحقيق فيها

يقوم فريق أمن المعلومات برصد شبكة البيانات المؤسسية بشكل مستمر، وتحديد نقاط الضعف في المعدات والتهديدات التي قد يسببها مستخدمونا، إما من خلال تصفح الإنترنت غير الملائم أو من خلال محاولات التحايل على القيود التي نفرضها. وفي الوقت نفسه، يجري اتخاذ خطوات للتحقيق في الحوادث الحاسوبية التي تتعرض لها الشبكة المؤسسية ولإدارتها. ويقوم قسم إدارة المعلومات وقسم إدارة الحوادث التابعين لإدارة أمن المعلومات بتحليل مواطن الضعف المعروفة التي يمكن أن تعرض النظم والمعلومات المؤسسية للخطر. وتجري مواجهة أوجه الضعف هذه ومعالجتها على النحو المناسب من خلال الإجراء الرسمي التالي:

- تزويد عمليات جرد أصول المعلومات بالبيانات المتعلقة بمزود البرامجيات، ورقم النسخة، وحالة النشر الحالية، والمسؤول عن البرامجيات.
- إجراء تحليل كل سنتين لقابلية التضرر.
- الحصول على أحدث المعلومات عن مواطن الضعف الجديدة.
- وضع جدول زمني لإصلاح وعلاج نقاط الضعف المعروفة.
- اختبار عمليات الإصلاح أو التصحيح المتعلقة من خلال معالجة أوجه الضعف قبل النشر في بيئات الإنتاج.

5 - عمليات المراجعة

يتم التحقق من الامتثال للسياسات الصادرة ذات الصلة باستخدام وصلات المعدات الحاسوبية والشبكية للشرطة على الوجه الصحيح من خلال الخطة السنوية للمراجعة.

ويرد فيما يلي بعض القيود:

- حظر تركيب الشبكات الخصوصية الافتراضية (VPN) على أجهزة الحاسوب.
- حظر استخدام مختلف متصفحات الإنترنت المتخفية، من قبيل Tor، و i2P، DuckDuckGo و Whonix.
- حظر استخدام شبكات التواصل الاجتماعي (باستثناء الإدارات الخاصة).
- حظر استخدام مواقع البث ذات الاستهلاك العالي المستوى من قبيل مواقع التلفزيون الرقمي ومشاهدة الفيديوهات.
- حظر تخزين الوثائق الشخصية وتركيب برامجيات غير متعلقة بالعمل.

تحتفظ نظم المعلومات، وكذلك الخواديم وأجهزة الشبكة وغيرها من الخدمات التكنولوجية بسجلات المراجعة (دفاتر المراجعة) التي تشمل، حينما يمكن ذلك:

- تحديد المستخدم.
- تاريخ المعاملة ووقتها.

- عنوان بروتوكول الإنترنت واسم الجهاز المستخدم في إجراء المعاملة.
- نوع المعاملة.
- تحديد المعاملة.
- البيانات التي تم الاطلاع عليها أو تعديلها أو حذفها.
- محاولات الاتصال الفاشلة.
- التغييرات في تهيئة النظام.
- تغيير الامتيازات أو إلغاؤها.
- الملفات المستخدمة.
- إشارات الإنذار التي أطلقتها نظم المراقبة.
- تعطيل آليات الحماية.

6 - برامجيات مكافحة الفيروسات

تظل برامجيات مكافحة الفيروسات موضع التشغيل باعتبارها خطًا آخر للحماية من البرامجيات الخبيثة؛ فهي توفر لنا قدرات مكافحة التصيد الإلكتروني، والحماية من هجمات فيروسات اليوم صفر، وقدرات مكافحة فيروسات الفدية، كما توفر تحديثات لملفات الترقيعات الأمنية.

7 - إدارة الجدار الناري

يتم تقسيم الشبكات والإذن بدخولها باستخدام أحد برامجيات الطوق الأمني ويدعى "الجدار الناري"، الذي يمنع محاولات اختراق شبكتنا ويحسب عدد عمليات تسجيل الدخول من جانب مستخدمينا، ويحدد عدد مرات زيارة الموقع وعمليات تسجيل الدخول إلى مختلف الأنظمة المؤسسية.

8 - الاتصالات المشفّرة

فيما يتعلق بالاستجابة لحالات الطوارئ الأمنية الوطنية والتنسيق الداخلي للشرطة الوطنية، لدينا نظام اتصالات لاسلكية متطور ذو تشفير أمني بهدف ضمان سلامة الاتصالات التي نجريها.

وتعمل جميع التدابير المعتمدة على تحسين حماية المعلومات المؤسسية وتسهم في الجهود الرامية إلى منع وقوع الهجمات الإلكترونية، مع الأخذ في الاعتبار عدم وجود أية تدابير لحماية النظم الخاصة بنا. وفي الوقت الحاضر لا يوجد نظام آمن تماما، ولكن إذا ما قمنا بتنفيذ بعض هذه التدابير، فإننا نحد من الثغرة الأمنية ونكفل حوكمة الفضاء الإلكتروني فيما يتعلق بتحديد الهجمات الإلكترونية وصدّها.

هنغاريا

[الأصل: بالإنكليزية]
[15 أيار/مايو 2020]

تقييم عام للقضايا المتصلة بالفضاء الإلكتروني في سياق الأمن الدولي

في كانون الأول/ديسمبر 2019، اتخذت الجمعية العامة قرارًا بشأن الارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي. وفي القرار، تدعو الجمعية العامة الدول الأعضاء إلى أن تواصل موافاة الأمين العام بآرائها وتقييماتها بشأن الجهود المبذولة على الصعيد الوطني لتعزيز أمن المعلومات وتشجيع التعاون الدولي في هذا الميدان، مضمون المفاهيم المشار إليها في تقارير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي.

وترحب هنغاريا بالاستمرار في عملية مناقشة المعايير والقواعد والمبادئ الطوعية المتعلقة بالسلوك المسؤول للدول، وتدابير بناء الثقة والقانون الدولي في إطار اللجنة الأولى للأمم المتحدة، وإنشاء أفرقة جديدة من الخبراء الحكوميين.

وفي عام 2018، أيدت هنغاريا قراري الجمعية العامة 266/73 و 27/73 على التوالي، اللذين أنشآ فريقا آخر من الخبراء الحكوميين المعنيين بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي، وفريقا عاملا مفتوح العضوية معنيًا بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، بوصفهما خطوتين هامين مقبلتين في التصدي للتهديدات التي يشكلها استخدام تكنولوجيات المعلومات والاتصالات.

ولأول مرة، تشارك هنغاريا أيضا في هذه المفاوضات، على الرغم من أننا تابعنا أعمال أفرقة الخبراء الحكوميين السابقة باهتمام كبير، بما في ذلك خلال اعتماد أولى استراتيجياتنا الوطنية للأمن الإلكتروني في عام 2013. ومنذ إنشاء الفريق العامل المفتوح العضوية، كانت هنغاريا ممثلة في اجتماعيه الرسميين الأول والثاني من جانب ممثلها الدائم لدى منظمة الأمن والتعاون في أوروبا (وهو أيضا رئيس الفريق العامل غير الرسمي المعني بأمن الفضاء الإلكتروني التابع للمنظمة نفسها) ومنسق شؤون الفضاء الإلكتروني في وزارة الخارجية والتجارة، على التوالي. وتشارك هنغاريا أيضا بنشاط في المشاورات المتعلقة بصياغة مشروع تقرير رئيس الفريق العامل المفتوح العضوية. وبصفة عامة، تؤيد هنغاريا موقف الاتحاد الأوروبي.

وتدعم هنغاريا بقوة إقامة نظام فعال متعدد الأطراف، يستند إلى نظام دولي قائم على القواعد، يحقق نتائج في التصدي للتحديات العالمية في الفضاء الإلكتروني. ومن الأمثلة الجيدة على ذلك مشاركتنا في مختلف المبادرات الحكومية الدولية والمبادرات المتعددة أصحاب المصلحة ودعمنا لها. وتكرر هنغاريا تأكيد إمكانية انطباق القانون الدولي القائم على سلوك الدول في الفضاء الإلكتروني، بالشكل المعترف به في تقارير فريق الخبراء الحكوميين التي أُعدت بتوافق الآراء في 2010 و 2013 و 2015. غير أن عدم امتثال الجهات الفاعلة من الدول ومن غير الدول للالتزامات في إطار القانون الدولي لا يزال يشكل تهديدا رئيسيا للسلم والأمن الدوليين ولسيادتنا الوطنية، في العالم المادي وفي الفضاء الإلكتروني على حد سواء. لذلك، نحن بحاجة إلى أن نكون قادرين على ردع الهجمات التقليدية وغير التقليدية والحيلولة دون وقوعها على حد سواء.

دعم خطة نزع السلاح

تشاطر هنغاريا الأمين العام الشواغل التي أعرب عنها بشأن تزايد استخدام تكنولوجيات المعلومات والاتصالات تحقيقًا لأغراض خبيثة، وبالتالي فهي تدعم الترويج لإقامة بيئة سلمية لتكنولوجيا المعلومات والاتصالات كأولوية رئيسية منصوص عليها في خطة نزع السلاح التي أعلنها الأمين العام في أيار/مايو 2018. واعترافا بالمستوى الرفيع لمشاركتنا، حدد مكتب الأمم المتحدة لشؤون نزع السلاح هنغاريا بوصفها أحد مؤيدي الإجراء 31 من خطة نزع السلاح، الذي يهدف إلى تعزيز المساءلة والتقيد بالمعايير الناشئة في مجال الفضاء الإلكتروني.

وتدعم هنغاريا المساعي الحميدة التي يبذلها الأمين العام لمنع تصاعد حوادث الفضاء الإلكتروني وتفعيل المعايير الإلكترونية الطوعية، فضلا عن زيادة التعاون بهدف سد الفجوة القائمة في المعرفة الإلكترونية بين الدول الأعضاء.

أمن الفضاء الإلكتروني باعتباره أحد قضايا الأمن القومي

في نيسان/أبريل 2020، اعتمدت الحكومة استراتيجية هنغاريا الجديدة للأمن الوطني (مرفقة بالمقرر الحكومي (.IV .21) 1163/2020)، التي يجب بالاستناد إليها إجراء استعراض لاستراتيجيتنا الوطنية للأمن الإلكتروني. وتقدم الاستراتيجية الجديدة للأمن الوطني لمحة عامة عن التغيرات التي طرأت على مشهد التهديدات الأمنية في الفترة منذ عام 2012. ويتمثل أحد أهدافها الرئيسية في تحديد التحديات الأمنية التي يطرحها التطور السريع لتكنولوجيات المعلومات والاتصالات ومواجهتها والتصدي لها.

ومن المتوقع على نطاق واسع أن يستمر عدد الهجمات الإلكترونية وتعقّدها في الازدياد. ولذلك، ستبذل حكومة هنغاريا، بالتعاون مع أصحاب المصلحة الآخرين، كل ما في وسعها لتعزيز قدراتها من أجل الوقاية من الهجمات الإلكترونية الخبيثة التي تستهدف هياكلنا الأساسية الحيوية للمعلومات، وزيادة الوعي العام بنظافة الفضاء الإلكتروني.

ويمثل التصدي للتحديات الناجمة عن انتشار المعلومات المضللة والكاذبة على الإنترنت وخارجه على حد سواء إحدى أولوياتنا الرئيسية، لا سيما اليوم، ونحن نواصل معركتنا ضد جائحة كوفيد-19. فيمكن أن تتسبب المعلومات المزيفة، في حالة الطوارئ الوطنية، في إلحاق أضرار بالغة.

ويجب أن يكون تطوير القدرات الإلكترونية الهجومية والدفاعية متسقاً مع التزامات الدولة بموجب القانون الدولي. وإلا فإن استخدام القدرات الهجومية لتكنولوجيا المعلومات والاتصالات يمكن أن يسهم في عسكرة الفضاء الرقمي.

ونعتبر أن القدرات الإلكترونية التي يمكنها تهديد الأمن والاستقرار على الصعيد الوطني أسلحة يمكن أن يكون استخدامها بمثابة هجوم مسلح يمكن للدول أيضا أن تتصدى بشكل هجومي كوسيلة للدفاع عن النفس. وبالنظر إلى التحديات التي تواجهها مسألة الإسناد في بيئة تكنولوجيا المعلومات والاتصالات، ينبغي للسلطات العامة، في حالة وقوع حادث من حوادث تكنولوجيا المعلومات والاتصالات، أن تتصرف مع مراعاة العناية الواجبة وأن تنظر في جميع المعلومات ذات الصلة، بما في ذلك السياق الأوسع للحدث وطبيعة العواقب ونطاقها.

التعاون الدولي والمبادرات الأخرى لأصحاب المصلحة المتعددين

تشارك هنغاريا بنشاط، بوصفها عضوا في الاتحاد الأوروبي، في تطوير صندوق أدوات الدبلوماسية الإلكترونية التابع للاتحاد الأوروبي لكي يتمكن الاتحاد الأوروبي من تنسيق استجابته للأنشطة الإلكترونية الضارة التي تنشأ من خارج الاتحاد الأوروبي ضد مؤسساته ودوله الأعضاء. وإذ نؤكد على أهمية التعاون الدولي، فإننا نؤيد تعزيز الحوار مع شركائنا الاستراتيجيين وحلفائنا وسائر المنظمات الدولية.

ولا يمكن لأي بلد أو منظمة أن ينجحا بمفردهما في التصدي للتهديدات الأمنية المعاصرة. وهذا ما يجعل الشراكات، ولا سيما التعاون بين الاتحاد الأوروبي ومنظمة حلف شمال الأطلسي (الناتو) أكثر أهمية اليوم من أي وقت مضى. ولا بديل عن ذلك سوى مواصلة هذا التعاون وتعميق أواصره في السنوات القادمة. ومن المؤكد أن مواجهة التهديدات الهجينة (بما في ذلك التهديدات ضد الأمن الإلكتروني) هي أحد المجالات الرئيسية التي ينبغي للمنظمتين أن تركزا جهودهما فيها.

ومن المتوقع أن يزداد النزاع في الفضاء الإلكتروني احتدامًا في السنوات المقبلة، وأن تتسع الفجوة في القدرات بين البلدان المتقدمة تكنولوجيا والبلدان النامية. ففي تموز/يوليه 2016، أكد الحلفاء مجددًا ولاية حلف الناتو الدفاعية واعترفوا بالفضاء الإلكتروني باعتباره ساحة عمليات يجب على الحلف أن يدافع عنها. وفي تموز/يوليه 2018، أعلن الحلفاء مرة أخرى استعداد حلف الناتو لمواصلة التكيف مع مشهد التهديدات الإلكترونية الآخذ في التطور، والذي يتأثر بالجهات الفاعلة من الدول ومن غير الدول على حد سواء، بما في ذلك الجهات الفاعلة التي ترعاها الدول. ووافقت الدول الأعضاء في حلف الناتو على دمج الآثار الإلكترونية السيادية، التي يقدمها الحلفاء طواعية، في إطار الرقابة السياسية القوية. وفي معرض إعادة الحلف تأكيده على ولايته الدفاعية، فقد أعلن أنه يعتزم توظيف مجموعة كاملة من القدرات، بما في ذلك القدرات الإلكترونية، لردع التهديدات الإلكترونية والحماية منها والتصدي لها. ويلتزم الحلف بمواصلة تطوير شراكته مع الأوساط الصناعية والأكاديمية من جميع الحلفاء لمواكبة أوجه التقدم التكنولوجي من خلال الابتكار.

والتزام هنغاريا بأمن الفضاء الإلكتروني ليس بالأمر الجديد. فقد تم الاتفاق في بودابست في عام 2001 على الاتفاق الدولي الأول الذي لا يزال الوحيد من نوعه بشأن مكافحة الجريمة الإلكترونية، الذي يُسمى اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية، والمعروف أيضا باسم اتفاقية بودابست، وهو يُعد، منذ ذلك الحين، بمثابة مبدأ توجيهي لوضع تشريعات وطنية شاملة لمكافحة الجريمة الإلكترونية وإطار للتعاون الدولي. وجرى التصديق على المعاهدة بموجب القانون LXXIX لعام 2004. وبالإضافة إلى أن هنغاريا طرف في اتفاقية بودابست، فإنها تعمل بنشاط على تشجيع بلدان ثالثة على الانضمام إليها.

وكمساهمة وطنية، يواصل الممثل الدائم لهنغاريا عمله منذ عام 2017 رئيسًا للفريق العامل غير الرسمي التابع لمنظمة الأمن والتعاون في أوروبا، الذي أنشئ بموجب مقرر المجلس الدائم 1039 بشأن وضع تدابير لبناء الثقة بهد الحد من مخاطر النزاع الناجم عن استخدام تكنولوجيا المعلومات والاتصالات. وتدعم هنغاريا الجهود الرامية إلى توثيق التعاون بين عمليات الأمم المتحدة وسائر المنظمات الإقليمية ذات الصلة، من قبيل منظمة الأمن والتعاون في أوروبا. وعلى الصعيد الإقليمي، نؤكد أهمية تنفيذ مجموعة تدابير بناء الثقة التي اعتمدتها منظمة الأمن والتعاون في أوروبا. كما أننا نؤيد التوسع في عولمة تدابير بناء الثقة الإقليمية في سياق الفريق العامل المفتوح العضوية. ومع ذلك، ينبغي أن ينصب تركيزنا على تفعيل كل تدبير إقليمي لبناء الثقة بالمستوى ذاته من الفعالية.

وهنغاريا هي أحد البلدان القليلة التي لديها موظفون في مجال الدبلوماسية الإلكترونية. ويتولى منسق شؤون الفضاء الإلكتروني في وزارة الخارجية والتجارة المسؤولية عن أنشطة التوعية الدولية بشؤون الفضاء الإلكتروني في العلاقات الثنائية والمتعددة الأطراف على حد سواء، بما في ذلك الأمم المتحدة، والاتحاد الأوروبي، ومنظمة الأمن والتعاون في أوروبا وغيرها من المبادرات ذات الصلة التي تضم أصحاب المصلحة المتعددين، من قبيل المنتدى العالمي للخبرات الإلكترونية. والدبلوماسية الإلكترونية مجال جديد نسبيا من مجالات تعاوننا الدولي التي يمكن لحكومتنا أن تستفيد منها وهي تتصدى للأنشطة الإلكترونية الضارة.

وتسهم هنغاريا في جهود بناء القدرات في بلدان ثالثة. وفي إطار هذه الجهود، يؤدي أمن الفضاء الإلكتروني دوراً أساسياً في سياسة هنغاريا للتعاون الإنمائي الدولي، لا سيما إزاء البلدان الأفريقية الشريكة. وتحقيقا لهذه الغاية، ما فتئت هنغاريا تقدم المساعدة الإنمائية إلى أوغندا في مجال أمن تكنولوجيا المعلومات بهدف مساعدتها على مواجهة تحديات القرن الحادي والعشرين. ويشكل مجال أمن الفضاء الإلكتروني عنصرا أساسيا من عناصر التعاون المنصوص عليها في إستراتيجية إفريقيا التي تبنتها هنغاريا مؤخرًا واستراتيجيتها للتعاون الإنمائي الدولي للفترة 2020-2025.

وبالإضافة إلى كونها جزءا من مختلف المفاوضات الحكومية الدولية، فإن الحكومة الهنغارية تؤيد مبادرات أصحاب المصلحة المتعددين، من قبيل نداء باريس من أجل الثقة والأمن في الفضاء الإلكتروني، استجابةً للدعوة إلى مزيد من التعاون الوطيد بشأن وضع معايير سلوك الدول وقواعده ومبادئه في الفضاء الإلكتروني. وانضمت إلى حكومتنا في هذه الجهود عشرات من منظمات القطاع الخاص الهنغارية. كما أن هنغاريا من مؤيدي نداء كرايستتشيرش للقضاء على المحتوى الإرهابي والذي يتسم بالتطرف العنيف على الإنترنت، الذي يعود بآثار سلبية على حقوق الإنسان وعلى أمننا الجماعي.

وتشاطر هنغاريا الرأي القائل بأن المنظمات غير الحكومية (المجتمع المدني، والأوساط الأكاديمية، والقطاع الخاص، ومجتمع تكنولوجيا المعلومات والاتصالات) لديها مجموعة من الخبرات التقنية و/أو الموارد اللازمة للمساهمة في إنشاء فضاء إلكتروني آمن ومستدام في إطار أدوار كل منها ومسؤولياته. وتضطلع الدول بدور قيادي في تعزيز هذا التنسيق والتعاون.

إندونيسيا

[الأصل: بالإنكليزية]
[31 أيار/مايو 2020]

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

يبلغ عدد مستخدمي الإنترنت في إندونيسيا أكثر من 170 مليون مستخدم، أي ما يمثل 65 في المائة من مجموع سكانها. وأتاحت تكنولوجيات المعلومات والاتصالات لإندونيسيا فرصاً حيوية لبلوغ أهداف التنمية المستدامة. ومن ناحية أخرى، فإن التحديات في الفضاء الإلكتروني آخذة في الازدياد أيضا. وفي عام 2019، تعرضت إندونيسيا لأكثر من 220 مليون هجوم إلكتروني، ما أعاق استخدام الفضاء الإلكتروني بشكل مفيد.

وتواصل إندونيسيا بنشاط تنفيذ تدابير متعددة لتعظيم الإمكانات الرقمية والتصدي للتهديدات الإلكترونية من خلال تعزيز الجوانب القانونية والسياسية للهياكل الأساسية المؤسسية وبناء القدرات والتعاون الدولي.

الجهود المبذولة على الصعيد الوطني

في عام 2017، تأسست الوكالة الوطنية للإنترنت والتشفير لتكون الهيئة المركزية لإندونيسيا المعنية بالأمن الإلكتروني. وقد أنشئ الفريق الوطني لمواجهة الطوارئ الحاسوبية في إطار الوكالة من أجل الاستجابة على وجه السرعة لحوادث الفضاء الإلكتروني، الموجهة إلى الهياكل الأساسية الحكومية أو الخاصة. كما أنشئ فريق للاستجابة لحوادث أمن الفضاء الإلكتروني في كل وكالة حكومية مركزية ومناطقية في 34 مقاطعة في إندونيسيا، لمواجهة تلك الحوادث والتعافي منها.

وفي إطار تعزيز الإطار القانوني والسياساتي الوطني، أصدرت إندونيسيا قانون المعلومات والمعاملات الإلكترونية، وكذلك خارطة الطريق الوطنية للتجارة الإلكترونية للفترة 2017–2019، والتي تتضمن الجهود الرامية إلى تأمين المعاملات الإلكترونية والرقمية. وقد اعتُمدت المبادئ التوجيهية للدفاع الإلكتروني في إندونيسيا من خلال لائحة وزارة الدفاع رقم 82 لعام 2014. واعتَمد أيضا النظام الوطني لتوحيد المقاييس في إندونيسيا معيارين دوليين لأمن تكنولوجيا المعلومات والاتصالات، هما ISO/IEC27001 و ISO 15408.

وقد أُدرج قانون أمن الفضاء الإلكتروني في إندونيسيا في قائمة مشاريع القوانين ذات الأولوية لعام 2020، وتجري حاليًا العملية التشريعية ذات الصلة. كما تقوم إندونيسيا حالياً بصياغة الاستراتيجية الوطنية للأمن الإلكتروني للفترة 2020–2024، التي تشمل خمس ركائز هي: القدرة على الصمود في وجه الهجمات الإلكترونية، وتعزيز الإطار القانوني، وقدرات التكنولوجيا الإلكترونية، ودعم النمو الاقتصادي الرقمي، والتعاون الوطني والدولي.

وإندونيسيا ملتزمة أيضا بمواصلة تعزيز التعاون المحلي، ولا سيما مع المؤسسات المملوكة للدولة والقطاع الخاص والصناعة لدعم إيجاد ثقافة شاملة تتناول أمن الفضاء الإلكتروني. ومنذ عام 2018، بدأت حكومة إندونيسيا حملة محو الأمية في مجال أمن الفضاء الإلكتروني لتعزيز الوصول الآمن إلى الإنترنت، وحملة ضد الاحتيال والتنمر عبر الإنترنت، وأخلاقيات وسائل التواصل الاجتماعي، والاستخدام المسؤول، وتوجيه الآباء بشأن سلامة الأطفال على الإنترنت.

الجهود المبذولة على الصعيد الدولي

تواصل إندونيسيا، من خلال تعهداتها المتعددة، تعزيز التعاون المتبادل، وأفضل الممارسات، والقدرات للمساعدة في التمكين من إنشاء صرح فعال للأمن الإلكتروني يمكن اعتماده في نهاية المطاف على الصعيد العالمي.

وفيما يتعلق بالمشاركة العالمية المتعددة الأطراف، تشارك إندونيسيا بنشاط في الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، بما في ذلك بصفتها منسق الفريق العامل المعني بنزع السلاح التابع لحركة بلدان عدم الانحياز. كما تشغل إندونيسيا حاليا، من ضمن 25 بلدا آخر، عضوية فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي.

وعلى الصعيد الإقليمي، تشارك إندونيسيا في تدابير بناء الثقة في إطار رابطة أمم جنوب شرق آسيا، من خلال جملة أمور منها دعم إنشاء نقاط اتصال في الهيئات القطاعية للرابطة التي تتعامل مع القضايا الإلكترونية في إطار ركائزها المجتمعية السياسية والأمنية والاجتماعية، ومن خلال تبادل

المعلومات، والتعاون المنتظم في مجال الأمن الإلكتروني، والحوارات بين الدول الأعضاء. وتعزز الرابطة أيضا تعاونها بشأن قضايا أمن الفضاء الإلكتروني من خلال إنشاء لجنة تنسيق مشتركة بين الركائز. ومن خلال المنتدى الإقليمي للرابطة، اتسع نطاق المناقشة المتعلقة بتدابير بناء الثقة في سياق أمن الفضاء الإلكتروني إلى ما هو أبعد من الرابطة ليشمل بلداناً أخرى وشركاء آخرين.

وعلاوة على ذلك، تواصل إندونيسيا الحوارات الثنائية والتعاون مع مختلف الدول والشركاء. وستواصل تعزيز الجهود الهادفة إلى تعزيز سلوك الدولة المسؤول، فضلا عن تعزيز بيئة مفتوحة وآمنة ومستقرة وميسَّرة وسلمية لتكنولوجيا المعلومات والاتصالات.

مضمون المفاهيم المشار إليها في تقارير فريق الخبراء الحكوميين

إن إساءة استخدام الفضاء الإلكتروني من جانب الجهات الفاعلة من الدول وغير الدول على حد سواء، بما في ذلك الجهات التي تعمل بالوكالة عنها، تشكل مخاطر على السلام والأمن الدوليين، وكذلك على استقرار المجالات السياسية والاقتصادية والاجتماعية على الصعيد الوطني. وثمة تحول كبير نحو تكنولوجيا المعلومات والاتصالات يجري حاليا على الصعيد الدولي في التصدي للآثار المتعددة الأبعاد المترتبة على جائحة كوفيد-19. وقد تحاول الجهات الفاعلة الخبيثة في الفضاء الإلكتروني أن تستغل، على وجه الخصوص، نظم تكنولوجيا المعلومات والاتصالات وانتشار المعلومات في الفضاء الإلكتروني.

ويمثل التفاهم والتعاون والتآزر وتدابير بناء الثقة والمساعدة وبناء القدرات أمورا أساسية لتعزيز الأمن والاستقرار في الفضاء الإلكتروني. ويجب في هذا الصدد دعم الجهود الثنائية والإقليمية والعالمية، والنظر إليها باعتبارها تكمل بعضها البعض لا على أنها تتنافس فيما بينها.

وتؤيد إندونيسيا مواصلة مناقشة وتنفيذ القواعد غير الملزمة وفقا لتقرير فريق الخبراء الحكوميين لعام 2015. وتؤكد إندونيسيا من جديد الدور الحيوي الذي تؤديه الأمم المتحدة والمنظمات الإقليمية في تعزيز مناقشة وتنفيذ 11 من المعايير وتدابير بناء الثقة والقدرات المتعلقة بالأمن الإلكتروني، لا سيما في تضييق الفجوة الرقمية بين البلدان وسدِّها.

وترى إندونيسيا أن المعايير الطوعية وغير الملزمة تشكل إطارا هاما لسلوك الدول المتسم بالمسؤولية. ورغم أن الفجوة في الإلكتروني غير الخاضعة للتنظيم تحتاج إلى معالجة، فإن إندونيسيا تشجع على إيجاد ممارسات أخرى للدول فضلا عن ممارسات عرفية.

وإندونيسيا مستعدة لمناقشة تطبيق القانون الدولي القائم على الفضاء الإلكتروني، بما في ذلك إمكانية وضع *قانون خاص*. وهي تشدد على أن استخدام الفضاء الإلكتروني ينبغي أن يتم وفقا للمبادئ القانونية الدولية، ولا سيما المتعلقة منها بالاحترام الكامل للسيادة، وعدم التدخل، وتسوية المنازعات بالوسائل السلمية، وحقوق الإنسان، وميثاق الأمم المتحدة.

وتؤيد إندونيسيا إعلانًا من جميع الدول في الجمعية العامة للامتناع عن عسكرة الفضاء الإلكتروني، الذي يقوض السلام والأمن الدوليين ويتعارض مع حقوق الدول والتزاماتها بموجب القانون الدولي.

وتشدد إندونيسيا على توسيع نطاق التفاهم وترسيخ المشاركة، ولا سيما بالنسبة للبلدان والمناطق التي لم تشارك بالقدر الكافي في الخطاب والتدابير المتعلقة بالأمن الإلكتروني.

أيرلندا

[الأصل: بالإنكليزية]
[30 أيار/مايو 2020]

ترحب أيرلندا بهذه الفرصة للاستجابة لطلب الأمين العام عملا بالفقرة 2 من القرار 28/74 بشأن الارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي. وتؤيد أيرلندا أيضاً الرسالة المقدمة من الاتحاد الأوروبي في هذا الصدد.

ولقد استفادت مجتمعاتنا ودولنا من تكنولوجيات المعلومات والاتصالات، ما سهل التواصل، والتعليم، والابتكار، والنشاط الاقتصادي، وتعزيز الازدهار. ولكن في عالم يزداد ترابطا، يمكن أن يكون لإساءة استخدام هذه التكنولوجيات القوية أيضا أثر سلبي للغاية، كما أن ازدياد الأنشطة الإلكترونية الضارة، وتحديدًا خلال الجائحة الحالية، يشكل مصدر قلق كبير لأيرلندا. وتؤثر هذه الأنشطة على المواطنين وعلى ثقتهم في المؤسسات. كما أن آثارها محسوسة على مستوى المجتمعات والدول، حيث يمكن أن تتسبب في نشوب النزاعات أو في تصعيدها.

ولا تزال الأمم المتحدة المنتدى البارز للتصدي للتحديات المتعلقة بإساءة استخدام تكنولوجيا المعلومات والاتصالات والأنشطة الإلكتروني الضارة، التي تؤثر على جميع الركائز الثلاث لجدول أعمال الأمم المتحدة المتمثلة في السلام والأمن، وحقوق الإنسان، والتنمية المستدامة. وأيرلندا، بوصفها بلداً له قطاع مهم في مجال تكنولوجيا المعلومات والاتصالات، وبلداً لديه التزام راسخ تجاه الأمم المتحدة، ستواصل دعمها للأمم المتحدة في تشجيع وتعزيز سلوك الدول المسؤول في الفضاء الإلكتروني. وستواصل أيرلندا أيضا المشاركة بصورة فعالة وقائمة على التعاون مع الشركاء في الأمم المتحدة وعلى الصعيد الدولي لدعم فضاء إلكتروني مفتوح وحر ومنيع وآمن، وتعزيز حرية التعبير وتكوين الجمعيات والتجمع على الإنترنت، والحد من خطر نشوب النزاعات وتعزيز السلام، وكفالة أن تكون الفوائد الاجتماعية والاقتصادية للفضاء الإلكتروني في متناول الجميع، دعمًا لتحقيق أهداف منها أهداف التنمية المستدامة. ونعتقد أن التقدم في التصدي للتحديات التي تواجهنا لا يمكن أن يستمر إلا من خلال المشاركة المتعددة الأطراف وأصحاب المصلحة، التي نلتزم بها على الصعيد الوطني من خلال مبادرات منها مجموعة أيرلندا الإلكترونية التي أُنشئت في عام 2019 بتمويل حكومي وتجمع بين العديد من أصحاب المصلحة من الصناعة والأوساط الأكاديمية والحكومة لمناقشة التعاون والتوعية وتعزيزهما بشأن التعليم والفرص الوظيفية المرتبط بالفضاء الإلكتروني، وتعزيز الابتكار في قطاع أمن الفضاء الإلكتروني في أيرلندا. كما نعرب عن التزامنا بنهجنا الدولي، ونرحب في هذا الصدد بالمبادرات التي تتخذها الأمم المتحدة وفي محافل أخرى لتعزيز التعاون والحوار على نطاق أوسع، بسبل منها الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي. وتدعم إيرلندا أيضا اجتماعات فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي.

ولا يزال نهج أيرلندا في التعامل مع القضايا الإلكترونية قائماً على التزامنا بانطباق القانون الدولي وبمركزيته، بما في ذلك ميثاق الأمم المتحدة، والقانون الدولي الإنساني، والقانون الدولي لحقوق الإنسان. وترحب أيرلندا أيضا بتوافق الآراء الذي توصلت إليه الجمعية العامة في عام 2015 على أن تسترشد جميع الدول في استخدامها تكنولوجيا المعلومات والاتصالات بتقرير فريق الخبراء الحكوميين لعام 2015، الذي حدد 11 من المعايير الطوعية وغير الملزمة لسلوك الدول المسؤول. ونرى أن هذه المعايير، مقترنة بالقانون

الدولي، والمستكمَلة بتدابير بناء القدرات المتخذة من أجل بناء القدرات الإلكترونية وتيسير زيادة فرص الحصول على تكنولوجيا المعلومات والاتصالات، وتدابير بناء الثقة الرامية إلى الحد من خطر نشوب نزاعات مسلحة، توفر إطارا قويا للارتقاء بسلوك الدول على نحو إيجابي في الفضاء الإلكتروني. ويمكن لمبادرات بناء القدرات في مجال تكنولوجيا المعلومات والاتصالات أن تساعد أيضا في معالجة الفجوة الرقمية العالمية المستمرة، وتحويل حياة الناس والمجتمعات المحلية، وتعزيز الازدهار، والإسهام في تنفيذ أهداف التنمية المستدامة وتيسيرها، بما يشمل المجالات الجنسانية.

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

استراتيجية إيرلندا الوطنية لأمن الفضاء الإلكتروني للفترة 2019-2024

يجب على جميع الدول، في فضاء إلكتروني مترابط، أن تكفل بناء القدرة على الصمود في وجه المخاطر المتصلة به، على الصعيدين المحلي والعالمي. وتحدد استراتيجية إيرلندا الوطنية لأمن الفضاء الإلكتروني 2019-2024[8] الإجراءات والأهداف الرئيسية في هذا الصدد. وتدعم هذه الاستراتيجية هدف الأمم المتحدة المتمثل في تعزيز سلوك الدول المسؤول في الفضاء الإلكتروني والحفاظ على السلام والأمن الدوليين من خلال حماية أيرلندا وشعبها وهياكلها الأساسية الوطنية الحيوية من التهديدات التي يتعرض لها الأمن الإلكتروني. كما أنها تدعم مشاركة أيرلندا على الصعيد الدولي في دعم فضاء إلكتروني حر ومفتوح وسلمي وآمن. وينفذ المركز الوطني لأمن الفضاء الإلكتروني سياسة أيرلندا المتعلقة بهذا المجال، وهذا ما يسهم في جدول أعمال الأمم المتحدة المتصل بالفضاء الإلكتروني عن طريق تعزيز الحوار بشأن الفضاء الإلكتروني والتعاون مع الوكالات الشريكة وسائر أصحاب المصلحة على الصعيد الدولي، وتعزيز الثقة والأمن في الفضاء الإلكتروني.

وتشمل الأهداف الرئيسية لاستراتيجية أيرلندا في مجال أمن الفضاء الإلكتروني ما يلي:

- مواصلة تحسين قدرة أيرلندا على كشف الحوادث التي تهدد أمن الفضاء الإلكتروني والتصدي لها ومكافحتها
- تحديد وحماية الهياكل الأساسية الوطنية الحيوية من خلال زيادة القدرة على الصمود أمام الهجمات الإلكترونية
- تحسين أمن وقدرة نظم تكنولوجيا المعلومات في القطاع العام على الصمود في وجه الهجمات الإلكترونية من أجل حماية الخدمات التي يعتمد عليها المواطنون وبياناتهم بشكل أفضل
- الاستثمار في المبادرات التعليمية من أجل إعداد القوى العاملة للوظائف الهامة في مجال تكنولوجيا المعلومات وأمن الفضاء الإلكتروني
- زيادة الوعي بمسؤوليات الشركات عن تأمين شبكاتها وأجهزتها ومعلوماتها والدفع بالبحث والتطوير في مجال أمن الفضاء الإلكتروني في أيرلندا، بسبل منها تيسير الاستثمار في التكنولوجيا الجديدة

(8) متاحة على الرابط التالي: www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf.

- مواصلة العمل مع الشركاء الدوليين والمنظمات الدولية لضمان أن يظل الفضاء الإلكتروني مفتوحا وآمنا وموحدا وحرا وقادرا على تيسير التنمية الاقتصادية والاجتماعية ودعم بناء القدرات المستدامة
- رفع المستوى العام للمهارات والوعي لدى الأفراد بشأن الممارسات الأساسية للتوعية بممارسات النظافة الإلكترونية ودعمهم في هذا الصدد من خلال المعلومات والتدريب

الكتاب الأبيض بشأن الدفاع

يشير *الكتاب الأبيض لأيرلندا بشأن الدفاع* (نُشر في عام 2015[9] وحُدِّث في عام 2019[10]) إلى المخاطر التي يشكلها النشاط الإلكتروني الضار محليًا ودوليًا، وتحديدًا على الهياكل الأساسية الحيوية والخدمات الرئيسية، ويعترف أيضًا بكيفية إساءة استخدام القضايا الإلكترونية لتقويض القيم الأساسية، بما في ذلك الكرامة الإنسانية والحرية والديمقراطية. ولا تزال أيرلندا تسترشد *بالكتاب الأبيض بشأن الدفاع* والاستراتيجية الوطنية لأمن الفضاء الإلكتروني خلال مشاركتها في تكنولوجيا المعلومات والاتصالات والقضايا الإلكترونية.

النهج الثنائية والإقليمية والمتعددة الأطراف

تواصل أيرلندا تعزيز الحوار بشأن تكنولوجيا المعلومات والاتصالات والقضايا الإلكترونية في مشاركتها مع الدول الأخرى على الصعيد الثنائي وفي المحافل الإقليمية والمتعددة الأطراف.

وترحب أيرلندا بعمل منظمة الأمن والتعاون في أوروبا وغيرها من المنظمات الإقليمية في جميع أنحاء العالم في تعزيز تدابير بناء الثقة والاطمئنان.

وتدعم أيرلندا المبادرات التي تتخذها الجهات الحكومية وغير الحكومية التي تعزز الثقة والأمن والسلام في الفضاء الإلكتروني، بما في ذلك نداء باريس من أجل الثقة والأمن في الفضاء الإلكتروني. وتدعم أيرلندا أيضا نداء كرايستتشيرش للقضاء على المحتوى الإرهابي والذي يتسم بالتطرف العنيف على الإنترنت. وأيرلندا عضو في التحالف من أجل الحرية على شبكة الإنترنت الذي يضم 31 دولة تعمل معاً من أجل النهوض بالحرية على شبكة الإنترنت.

كما قدمت أيرلندا مذكرة إعلان نوايا تلتمس فيها الانضمام إلى مركز الامتياز للدفاع التعاوني الإلكتروني في تالين، للمساهمة في التصدي بشكل تعاوني للتحديات التي تواجه أمن الفضاء الإلكتروني مع الشركاء ذوي التفكير المماثل. وستنضم أيرلندا إلى المركز باعتبارها مشاركًا مساهمًا (كونها ليست من أعضاء الناتو).

تعزيز التعاون الدولي في الاتحاد الأوروبي

تواصل أيرلندا الاضطلاع بدور كامل وفعّال في الاتحاد الأوروبي بشأن قضايا الفضاء الإلكتروني، وتعمل بشكل وثيق مع شركائها في الاتحاد الأوروبي على الترويج لفضاء إلكتروني حر ومستقر وآمن عالميًا، ما يسهم في منع نشوب النزاعات، بسبل مبادرات الدبلوماسية الإلكترونية ومجموعة أدوات

(9) متاح على الرابط التالي: https://assets.gov.ie/21963/f1e7723dd1764a4281692f3f7cb96966.pdf.

(10) متاح على الرابط التالي: www.gov.ie/en/publication/a519cf-white-paper-on-defence-update-2019/.

الدبلوماسية الإلكترونية للاتحاد الأوروبي. وتشارك أيرلندا أيضا، في تطوير قدراتها على الصمود في وجه الهجمات الإلكترونية، في عدد من المبادرات التي أطلقتها وكالة الدفاع الأوروبية.

تعزيز التعاون الدولي في الأمم المتحدة

تدعم أيرلندا، على مستوى الأمم المتحدة، عمل فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي (انظر أدناه أيضا)، وقد أسهمت بنشاط في الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي. كما تحدث سفير أيرلندا لدى الأمم المتحدة في الاجتماع الذي عقده مجلس الأمن في 22 أيار/مايو 2020 وفقًا لصيغة آريا بشأن استقرار الفضاء الإلكتروني ومنع نشوب النزاعات وبناء القدرات، فأكّد التزام أيرلندا بالعمل مع الأمم المتحدة بشأن طائفة واسعة من الأنشطة في هذا المجال، بما في ذلك استخدام تكنولوجيا المعلومات والاتصالات والفضاء الإلكتروني لتحقيق أهداف التنمية المستدامة، مع الإشارة بشكل خاص إلى الهدف المتعلق بالمساواة بين الجنسين.

مضمون المفاهيم المشار إليها في تقارير أفرقة الخبراء الحكوميين

مبادئ عامة

تؤيد أيرلندا اتباع نهج متعدد الأطراف ومحايد تكنولوجيًا لتعزيز أمن الفضاء الإلكتروني العالمي، يستند إلى نظام دولي قائم على القواعد. وترى أيرلندا أن المناقشات التي دارت في أحدث الاجتماعات التي عقدها الفريق العامل المفتوح العضوية قد أُثريت بفضل مشاركة أصحاب المصلحة وإسهاماتهم (بما في ذلك ممثلي المجتمع المدني، والأوساط الأكاديمية، والتقنية، والصناعية). وسوف يؤدي أصحاب المصلحة هؤلاء دوراً تزداد أهمية باطراد في تقديم المشورة للدول بشأن التطورات المقبلة في مجال تكنولوجيا المعلومات والاتصالات وفي الحفاظ بشكل مباشر على فضاء إلكتروني آمن ومستقر. وتعتقد أيرلندا أن تعزيز مشاركة أصحاب المصلحة في الاجتماعات المقبلة وغيرها من المناقشات بشأن قضايا الفضاء الإلكتروني أمر قيّم وضروري وينبغي وضعه في سياق رسمي.

الأخطار القائمة والناشئة

تقدّر استراتيجية إيرلندا الوطنية لأمن الفضاء الإلكتروني الأثر المتزايد والإيجابي لتكنولوجيا المعلومات والاتصالات على التنمية الاقتصادية والاجتماعية، لكنها تسلط الضوء أيضاً على ارتفاع معدلات الجريمة الإلكترونية وسرقة الملكية الفكرية وانتشار المعلومات المضللة، فضلاً عن استخدام الدول لإمكانيات إلكترونية هجومية. وقد أظهرت جائحة كوفيد-19 اعتمادنا على تكنولوجيا المعلومات والاتصالات من أجل العمل والتواصل بمرونة وأمان فضلا عن مواصلة النشاط الاقتصادي. بيد أن الجائحة أبرزت أيضا أنشطة الجهات الفاعلة الخبيثة التي تستغل مواطن الضعف، التقنية منها والبشرية على السواء، لارتكاب الجرائم في الفضاء الإلكتروني، أو لنشر معلومات مضللة، وبث البلبلة، وعدم الثقة، والانقسام. وتلاحظ أيرلندا بقلق بالغ الهجمات الإلكترونية الأخيرة التي شُنّت ضد الخدمات الصحية والطبية والخدمات ذات الصلة. وهذه الهجمات على خدمات الرعاية الصحية وغيرها من الخدمات الأساسية تعرض حياة الناس للخطر. وقد أدانت أيرلندا، إلى جانب شركائها في الاتحاد الأوروبي، هذه الهجمات ودعت كل دولة إلى بذل العناية الواجبة واتخاذ

الإجراءات المناسبة ضد الجهات الفاعلة التي تقوم بهذه الأنشطة من أراضيها، بما يتفق مع القانون الدولي والتقارير الصادرة عن أفرقة الخبراء الحكوميين بتوافق الآراء لأعوام 2010 و 2013 و 2015.

القانون الدولي

تؤمن أيرلندا إيمانا راسخا بإمكانية انطباق القانون الدولي وبمركزيته، بما في ذلك ميثاق الأمم المتحدة، والقانون الدولي الإنساني، والقانون الدولي لحقوق الإنسان. ويجب احترام حقوق الإنسان والحريات الأساسية على الإنترنت كما خارجه. وبالنظر إلى الإطار القانوني الدولي القائم، فقد عرضت أيرلندا تحفظاتها بإيجاز، في محافل منها الاجتماعات الأخيرة التي عقدها الفريق العامل المفتوح العضوية، بشأن الدعوات إلى صياغة صك قانوني جديد. غير أنها أيرلندا ترحب بالحوار الجاري من أجل تعزيز فهم مشترك أكبر بشأن تطبيق القانون الدولي القائم على استخدام الدول لتكنولوجيا المعلومات والاتصالات.

معايير سلوك الدول المسؤول وقواعده ومبادئه

تؤيد أيرلندا معايير سلوك الدول المسؤول وقواعده ومبادئه الواردة في تقرير فريق الخبراء الحكوميين لعام 2015 وترحب بالاتفاق الذي توصلت إليه الجمعية العامة بتوافق الآراء على ضرورة أن تسترشد بالتقرير جميع الدول أثناء استخدامها تكنولوجيا المعلومات والاتصالات. وتعزز هذه المعايير الاستقرار والأمن في البيئة العالمية لتكنولوجيا المعلومات والاتصالات كما يمكن أن تسهم في صون السلام الدولي. وتعكس استراتيجية أيرلندا الوطنية لأمن الفضاء الإلكتروني والسياسة الأيرلندية هذه المعايير والقواعد والمبادئ، وتحديدًا فيما يتعلق منها ببناء القدرات المستدامة. وقد دعت أيرلندا، في الأمم المتحدة، إلى مواصلة وضع توجيهات بشأن كيفية تنفيذ هذه المعايير القائمة، التي أقرتها جميع الدول الأعضاء بتوافق الآراء، ووضعها موضع التطبيق.

تدابير بناء الثقة

تساهم أيرلندا مساهمة فعالة في المناقشات المتعلقة بتكنولوجيات المعلومات والاتصالات وقضايا أمن الفضاء الإلكتروني وتروج لها في الاجتماعات والمنتديات الثنائية والإقليمية والمتعددة الأطراف، في سياقات منها السلام والأمن العالميان، والتنمية المستدامة، وحقوق الإنسان. وتعرب أيرلندا عن تقديرها للعمل الواسع النطاق الذي تضطلع به المنظمات الإقليمية ومبادرات أصحاب المصلحة من الدول ومن غير الدول، بما في ذلك نداء باريس، في تعزيز الثقة والاطمئنان، وتؤيد عمومًا المقترحات الرامية إلى إنشاء آليات لتبادل أفضل الممارسات بشأن تدابير بناء الثقة دعمًا للمبادرات المقبلة.

تدابير بناء القدرات

تشمل الاستراتيجية الوطنية لأمن الفضاء الإلكتروني في أيرلندا التزاماً بتعزيز تدابير بناء القدرات المستدامة. وتقدر أيرلندا أيضاً وضع نهج متعدد أطراف وأصحاب المصلحة لبناء قدرة جميع الدول على الصمود ضد النشاط الإلكتروني الضار والحد من مواطن الضعف وحماية الهياكل الأساسية الحيوية وتوسيع نطاق المنافع الكاملة الناجمة عن استخدام تكنولوجيا المعلومات والاتصالات ليشمل جميع الدول. وتعتقد أيرلندا أيضا أن من الأهمية بمكان أن تكون لدى جميع الدول وأصحاب المصلحة الرئيسيين القدرة على المشاركة في المناقشات العالمية بشأن قضايا الفضاء الإلكتروني. وفي هذا الصدد، أعربت أيرلندا

عن سـرورها برعاية الاجتماع غير الرسـمي الذي عقده الفريق العامل المفتوح العضـوية فيما بين الدورات في الفترة من 2 إلى 4 كانون الأول/ديسـمبر 2019، والذي جمع الدول إلى جانب أصـحاب المصـلحة، وشـمل ممثلي المنظمات غير الحكومية والمجتمع المدني، والخبراء الفنيين، والباحثين والأكاديميين، والقطاع الخاص. كما تؤيد أيرلندا بقوة الجهود الرامية إلى معالجة الفجوة الرقمية بين الجنسـين. وترحب أيرلندا بتقوية الروابط القائمة بين مناقشـات الأمم المتحدة ومبادراتها المقبلة في مجال بناء القدرات وأهداف التنمية المستدامة والخطة المتعلقة بالمرأة والسلام والأمن.

إيطاليا

[الأصل: بالإنكليزية]
[29 أيار/مايو 2020]

مقدمة

تؤيد إيطاليا المواقف التي أعرب عنها الاتحاد الأوروبي في مسـاهمته في التقرير، وتود أن تزود الأمين العام بالمعلومات الوطنية التالية.

ولأغراض هذا التقرير، لن تنظر إيطاليا في عبارة "أمن المعلومات"، التي لا تُسـتخدم في النظام القانوني الإيطالي. وتُسـتخدم عبارات أخرى، مثل "أمن الفضـاء الإلكتروني" أو "أمن الشـبكات ونظم المعلومات"، ومن ثم فهي مفضـلة. ويعترف بحرية التعبير – سـواء على شـبكة الإنترنت أو خارجها – في القانون الأساسي الإيطالي والمادة 19 من العهد الدولي الخاص بالحقوق المدنية والسياسية، الذي صدقت عليه إيطاليا في عام 1978.

ووفقاً لمرسـوم رئيس الوزراء الإيطالي المؤرخ 17 شـباط/فبراير 2017، الذي يتضـمن مبادئ توجيهية لحماية الفضـاء الإلكتروني وأمن تكنولوجيا المعلومات والاتصـالات على الصـعيد الوطني، يشـير مصـطلح "أمن الفضـاء الإلكتروني" إلى حماية الفضـاء الإلكتروني التي تُكفل من خلال التدابير الأمنية المادية والمنطقية والإجرائية المناسبة بهدف منع وقوع الحوادث ومواجهتها، سواء كانت مقصودة أو عرضية، بما في ذلك الحصـول على البيانات ونقلها دون مبرر، أو تعديل البيانات أو تدميرها بصـورة غير مشـروعة أو السـيطرة غير المبررة على الشـبكات ونظم المعلومات أو مكوناتها أو إلحاق الضـرر بها أو تدميرها أو وقف سير عملها العادي.

وبالمثل، تشـير عبارة "أمن الشـبكات ونظم المعلومات" إلى قدرة شـبكة أو نظام معلومات على القيام، على مسـتوى معين من السـرية، بمقاومة أي عمل يسـتهدف توافر البيانات المخزنة أو المنقولة أو المعالجة أو صـحتها أو سـلامتها أو سـريتها والخدمات ذات الصـلة المتاحة أو التي يمكن الوصـول إليها من خلال هذه الشـبكة أو نظام المعلومات هذا، على النحو المحدد في المرسـوم التشـريعي 2018/65 الذي ينقل توجيه الاتحاد الأوروبي بشأن أمن الشبكات ونظم المعلومات.

الجهود المبذولة على الصعيد الوطني لتعزيز أمن الفضاء الإلكتروني: الإطار المؤسسي والمعياري

في كانون الأول/ديسـمبر 2013، اعتمدت إيطاليا الإطار الاسـتراتيجي الوطني لأمن الفضـاء الإلكتروني، الذي يحاط فيه علماً بالتهديدات المتزايدة والمتطورة الناجمة عن اسـتخدام تكنولوجيا المعلومات

والاتصـــالات، ويهدف إلى تعزيز قدرات إيطاليا في المجال الإلكتروني وقدرتها على الصـــمود فيه. وتحدد خطط العمل الوطنية التالية، التي صـــدرت آخر خطة منها في آذار/مارس 2017 واعتُمدت وفقاً لمرســـوم رئيس الوزراء المذكور أعلاه المؤرخ 17 شـباط/فبراير 2017، عدداً من الإجراءات والبنود والأولويات الرامية إلى تنفيذ الإطار الاستراتيجي.

ويحدد مرســوم رئيس الوزراء الهيكل الوطني لأمن الفضــاء الإلكتروني وإدارة هذا الهيكل، وينشــئ داخل إدارة الاستخبارات الأمنية مجلسا لإدارة أمن الفضاء الإلكتروني، يتولى المسؤولية عن منع وقوع أزمة متعلقة بأمن الفضـاء الإلكتروني على الصـعيد الوطني والتحضـير لها، فضـلا عن تنسـيق أنشـطة الاسـتجابة والتعافي التي يتعين على القطاعين العام والخاص القيام بها امتثالا لقرارات رئيس الوزراء.

ويتكون مجلس إدارة أمن الفضــاء الإلكتروني من أمانة ومجلس مشــترك يرأســه نائب المدير العام لشــؤون الفضــاء الإلكتروني التابع لإدارة الاســتخبارات الأمنية ويتألف من ممثلين عن دوائر الاســتخبارات (إدارة الاســتخبارات الأمنية، ووكالة الاســتخبارات، والأمن الخارجي، ووكالة الاســتخبارات والأمن الداخلي)، والمســـتشـــار العســـكري لرئيس الوزراء، ووزارات الخارجية والتعاون الدولي، والداخلية، والعدل، والدفاع، والاقتصــاد والمالية، والتنمية الاقتصــادية، وإدارة الحماية المدنية، ووكالة إيطاليا الرقمية. وينضــم ممثل عن المكتب المركزي للسرية التابع لإدارة الاستخبارات الأمنية إلى المجلس كلما كان حادث يمس نظم المعلومات السرية قيد المناقشة.

وفي حالة حدوث أزمة تتعلق بالفضــاء الإلكتروني الوطني، يمكن أن يضــم المجلس أيضــا ممثلين عن وزارة الصـحة، ووزارة البنية التحتية والنقل، وإدارة المطافئ. ويمكن لرئيس الوزراء، استنادا إلى المعلومات التي يقدمها مجلس الأمن القومي، أن يعلن حالة أزمة متعلقة بالفضـــاء الإلكتروني كلما تعذر على المكتب الوحيد المعني التعامل مع حادث في الفضــاء الإلكتروني بســبب حجمه أو شــدته أو طبيعته، ويتطلب نهجا مشتركا ومنسقا، يكفله مجلس إدارة أمن الفضاء الإلكتروني.

وتلت مرسوم رئيس الوزراء نصوص تشريعية إضافية، هي:

- المرســـوم التشـــريعي رقم 2018/65، الذي ينقل توجيه الاتحاد الأوروبي بشـــأن أمن الشـــبكات ونظم المعلومـات، ويعين إدارة الاســـتخبـارات الأمنيـة جهـةَ اتصـــــال وحيـدة فيمـا يخص نظم الشبكات والمعلومات
- ينطبق القانون المتعلق بمحيط أمن الفضــاء الإلكتروني الوطني (القانون 2019/133)، الذي دخل حيز النفاذ في تشـــرين الثاني/نوفمبر 2019، على الكيانات العامة والخاصـــة الوطنية التي تؤدي وظائف أســاســية أو تقدم خدمات أســاســية لتنفيذ أنشــطة تعتبر حيوية للمصــالح الوطنية الإيطالية. وأدرِجت كيانات عامة وخاصة في "المحيط" وفقا لمبدأ "الأولوية التدريجية للأمن الوطني". ويغطي القانون تلك الشبكات ونظم تكنولوجيا المعلومات والخدمات التي تملكها أو تديرها الكيانات المذكورة أعلاه، والتي يمكن أن تؤثر على الأمن القومي. ويترتب على القانون ما يلي:
  - الإخطار بالحوادث، من أجل ضـــمان تدفق فوري للمعلومات نحو الهياكل ذات الصـــلة المســؤولة عن منع وقوع حوادث الفضــاء الإلكتروني والإعداد لها وإدارتها، وهي مجلس إدارة أمن الفضــاء الإلكتروني وفريق مواجهة الحوادث الأمنية الحاســوبية، وهما يشــكلان جزءا من إدارة الاستخبارات الأمنية

- تدابير أمنية تشمل المسائل والعمليات والإجراءات المؤسسية، بما في ذلك شراء تكنولوجيا المعلومات والاتصالات

- الفحص التكنولوجي لمنتجات وخدمات تكنولوجيا المعلومات والاتصالات التي تندرج في فئات محددة وتتعلق بالأصول/الكيانات المدرجة في المحيط. ووفقا للقانون، يجب على أي مشغل يرغب في شراء هذه الأصناف أن يبلغ المركز الوطني للتقييم والتصديق الذي يجوز له، بدوره، إجراء تقييمات أولية، وفرض شروط، واشتراط اختبار الأجهزة أو البرامجيات. وفي الحالة الأخيرة، تشمل الدعوات ذات الصلة لتقديم العروض والعقود بنداً يعلق سياسات الإلغاء، فيما يتصل بالمتطلبات الواجب الوفاء بها أو بالنتائج الإيجابية للاختبارات التي يفرضها المركز الوطني للتقييم والتصديق

- أنشطة التفتيش وفرض العقوبات بالنسبة للجهات الفاعلة في القطاعين العام والخاص التي يقوم بها على التوالي رئاسة مجلس الوزراء ووزير التنمية الاقتصادية.

وفي حالة حدوث خطر شديد ووشيك على الأمن القومي فيما يتعلق بالشبكات، ونظم تكنولوجيا المعلومات والخدمات، يجوز لرئيس الوزراء أن يأمر بإغلاق/تعليق كلي أو جزئي لواحد أو أكثر من الأجهزة أو المنتجات المركبة على الشبكات أو النظم أو المتصلة بتقديم الخدمات. ويخضع القرار لمداولة مسبقة للجنة المشتركة بين الوزارات المعنية بأمن الجمهورية، ويكون صالحا للوقت اللازم فقط للقضاء على التهديد أو التخفيف منه، وفقا لمبدأ التناسب.

- ويشمل المرسوم بقانون رقم 2019/22 المحوَّل إلى القانون 2019/41 (المادة 1)، الذي يكمل المرسوم بقانون المتعلق "بالصلاحيات الذهبية" رقم 2012/21 المُحوَّل إلى القانون رقم 2012/56 "بشأن الصلاحيات الخاصة المتعلقة بامتلاك الأسهم في قطاعي الدفاع والأمن الوطني، وكذلك بالأنشطة ذات الأهمية الاستراتيجية في قطاعات الطاقة والنقل والاتصالات"، خدمات الاتصالات الإلكترونية ذات النطاق العريض القائمة على تكنولوجيات الجيل الخامس ضمن الأنشطة ذات الأهمية الاستراتيجية بالنسبة للدفاع والأمن الوطنيين. ووفقاً لأحدث الأحكام، تخضع العقود أو الاتفاقات المتعلقة باقتناء السلع أو الخدمات اللازمة لتخطيط وتنفيذ وصيانة وإدارة الشبكات المتعلقة بخدمات الاتصالات الإلكترونية ذات النطاق العريض القائمة على تكنولوجيات الجيل الخامس، أو اقتناء "مكونات التكنولوجيا العالية القدرة" المفيدة للتنفيذ أو الإدارة المذكورين أعلاه، لإخطار المجلس ذي "الصلاحيات الذهبية" المنشأ داخل رئاسة مجلس الوزراء كلما شملت العقود والاتفاقات كيانات غير تابعة للاتحاد الأوروبي. والأساس المنطقي لذلك هو السماح بممارسة حق النقض أو فرض أوامر وشروط محددة، يمكن تعديلها أو مزجها بتدابير إضافية، بما في ذلك استبدال المنتجات والمعدات، إذا كشف المركز الوطني للتقييم والتصديق عن وجود مواطن ضعف يمكن أن تمس سلامة وأمن الشبكات وبياناتها.

الدفاع عن الفضاء الإلكتروني

يعترف في الكتاب الأبيض للأمن والدفاع الدوليين لعام 2015 بالحاجة إلى حماية المجال الإلكتروني والدفاع عنه، بطرق منها إنشاء "قدرات تشغيلية دفاعية محددة ... من أجل الحفاظ على صلابة الهياكل السياسية والاقتصادية والاجتماعية". ووفقاً لما جاء في وثيقة التخطيط المتعدد السنوات لوزارة الدفاع

للسنوات 2019-2021، يجب حماية الفضاء الإلكتروني والدفاع عنه عند وقوع الهجمات على الخدمات الشبكية أو الحاسوبية والبنية التحتية الحيوية. وفي السنوات الأخيرة، خضعت وزارة الدفاع لعدد من الإصلاحات لتعزيز حمايتها، وكذلك قدرتها على الصمود ووضعها العام.

وفي جملة أمور، أنشأت وزارة الدفاع الإيطالية في عام 2017 القيادة المشتركة للعمليات في الفضاء الإلكتروني، وهي قيادة عسكرية مسؤولة عن تخطيط العمليات في الفضاء الإلكتروني والإعداد لها وتنفيذها، بهدف الكشف عن التهديدات والهجمات على شبكات ونظم وخدمات وزارة الدفاع داخل البلد وكذلك في مسارح العمليات خارج الحدود الإيطالية والقضاء عليها.

وتم مؤخرا دمج القيادة المشتركة للعمليات في الفضاء الإلكتروني في قيادة مكونات الفضاء الإلكتروني المنشأة حديثاً، بهدف وضع تسلسل قيادة مباشر بدرجة أكبر وضمان المزيد من الكفاءة والتنسيق بين جميع الإدارات المعنية بأمن الفضاء الإلكتروني ذات الصلة الموجودة داخل قطاعات الدفاع (القوات الجوية والجيش والبحرية). وتدعم قيادة مكونات الفضاء الإلكتروني مقر العمليات المشتركة الإيطالية، وهي مكلفة بإجراء عمليات دفاعية لحماية وزارة الدفاع الإيطالية وجهازها العسكري من الحوادث والهجمات الإلكترونية.

وبالإضافة إلى ذلك، فإن القيادة:

- مسؤولة عن أمن الفضاء الإلكتروني والدفاع الإلكتروني لشبكات وزارة الدفاع، اللذين تكفلهما من خلال فريق مواجهة الطوارئ الحاسوبية، المكلف برصد النشاط في الفضاء الإلكتروني ومنع وإدارة الحوادث وحالات الطوارئ التي تؤثر على قطاع الدفاع؛
- تقوم حاليا بدراسة لتحديد الإطار القانوني في مسارح العمليات، مع الامتثال الكامل للقانون الدولي والقانون الدولي الإنساني. وسوف تهدف هذه الدراسة إلى تحديد المعايير الدنيا وقواعد الاشتباك لدعم العمليات من خلال الأنشطة التي تنفذ في الفضاء الإلكتروني. وتتبع الحاجة إلى إطار قانوني من جملة أمور منها الأنشطة والعمليات الوطنية والدولية العديدة التي نفذت في السنوات الأخيرة، بما في ذلك في إطار منظمة حلف شمال الأطلسي.

وتم إنشاء مختبر إلكتروني داخل القيادة المشتركة للفضاء الإلكتروني بهدف وضع أدوات للتحقيق في نقاط الضعف الإلكترونية وتنظيم أنشطة تدريبية.

وتشمل الأنشطة الأخرى إجراء اختبار أولي لإنشاء نطاق إلكتروني للتدريب الإلكتروني التقني في مدارس الاتصالات السلكية واللاسلكية التابعة للقوات المسلحة الإيطالية والتعاون مع العديد من الجامعات الإيطالية في مجال أمن الفضاء الإلكتروني.

الجهود المبذولة لتعزيز التعاون الدولي في مجال أمن الفضاء الإلكتروني، بما في ذلك ما يتعلق بتقارير فريق الخبراء الحكوميين

وفقا للمادة 10 من الدستور الإيطالي: "يمتثل النظام القانوني الإيطالي لقواعد القانون الدولي المعترف بها عموما".

ولذلك، فإن إيطاليا ملتزمة بتعزيز تطبيق القانون الدولي القائم في الفضاء الإلكتروني، بما في ذلك ميثاق الأمم المتحدة برمته، وفقا أيضا لموقف الاتحاد الأوروبي حسب ما جاء في المساهمة المذكورة أعلاه؛ وبالتقيد بقواعد ومعايير ومبادئ السلوك المسؤول للدول التي وضعها فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي لعام 2015، والأفرقة التي سبقته؛ ووضع تدابير لبناء الثقة وبرامج لبناء القدرات؛ وإدارة شبكة الإنترنت استنادا إلى نهج متعدد أصحاب المصلحة.

وتؤيد إيطاليا نداء باريس من أجل الثقة والأمن في الفضاء الإلكتروني فيما يتعلق بتنفيذ تدابير تعاونية للحد من المخاطر التي تهدد استقرار الفضاء الإلكتروني وبناء الثقة والقدرات. وإيطاليا هي أيضا من بين الموقعين على نداء كرايستتشيرش للقضاء على المحتوى الإرهابي والذي يتسم بالتطرف العنيف على الإنترنت.

ويشكل تعزيز أنشطة بناء القدرات مع بلدان ثالثة جزءا من استراتيجيتنا الوطنية لأمن الفضاء الإلكتروني ويجري تنفيذه وفقاً "لاستنتاجات المجلس بشأن المبادئ التوجيهية للاتحاد الأوروبي المتعلقة ببناء القدرات الخارجية"، التي اعتمدها مجلس الشؤون العامة للاتحاد الأوروبي في اجتماعه 3629 الذي عقد في 26 حزيران/يونيه 2018. وتركز أنشطة بناء القدرات مع بلدان ثالثة أساسا على تبادل المعلومات وأفضل الممارسات، ولا سيما فيما يتعلق بمواجهة الحوادث الأمنية الحاسوبية، والتعليم، والتدريب.

كما أن المشاركة في المحافل الدولية ودعم الالتزام بمعايير السلوك المسؤول للدول في الفضاء الإلكتروني هما أيضا جزء أساسي من الاستراتيجية الوطنية الإيطالية لأمن الفضاء الإلكتروني. ويناقَش أيضا التعاون الدولي في مجال أمن الفضاء الإلكتروني، بما في ذلك ما يتعلق بتقارير فريق الخبراء الحكوميين، حيثما يكون ذلك مناسبا، في حواراتنا و/أو مشاوراتنا الثنائية والمتعددة الأطراف. والمحافل المتعددة الأطراف الرئيسية التي تسهم فيها إيطاليا بنشاط في تعزيز التعاون في مجال الفضاء الإلكتروني هي الأمم المتحدة، والاتحاد الأوروبي، ومنظمة حلف شمال الأطلسي، ومنظمة الأمن والتعاون في أوروبا، ومجلس أوروبا، ومجموعة الدول السبع.

وفيما يتعلق بهذه الأخيرة، استضافت إيطاليا يومي 10 و 11 نيسان/أبريل 2017 الاجتماع الوزاري لمجموعة الدول السبع عن الشؤون الخارجية، الذي اعتمد "إعلان مجموعة الدول السبع بشأن سلوك الدول المسؤول في الفضاء الإلكتروني". ويدعو الإعلان جميع الدول إلى الاسترشاد في استخدامها لتكنولوجيا المعلومات والاتصالات بالتقارير التراكمية لأفرقة الخبراء الحكوميين التابعة للأمم المتحدة في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي.

وخلال الرئاسة الإيطالية لمنظمة الأمن والتعاون في أوروبا في عام 2018، دعمت إيطاليا بنشاط التنفيذ الفعلي لتدابير بناء الثقة التي اتخذتها المنظمة في مجال أمن المعلومات والاتصالات من قبل الدول المشاركة، وذلك من خلال جملة أمور منها تنظيم مناقشة تستند إلى سيناريوهات حول استخدامها في حالة وقوع حادث إلكتروني دولي، على هامش مؤتمر أمن الفضاء الإلكتروني/تكنولوجيا المعلومات والاتصالات، الذي عُقد في روما يومي 27 و 28 أيلول/سبتمبر 2018 وشمل المنظمة برمتها. وفي عام 2019، نظمت إيطاليا، خلال رئاستها لفريق الاتصال الآسيوي التابع لمنظمة الأمن والتعاون في أوروبا، المؤتمر الآسيوي العشرين للمنظمة، بشأن "كيفية تحقيق الأمن الشامل في العصر الرقمي: وجهات نظر منظمة الأمن

والتعاون في أوروبا وشركائها الآسيويين"، الذي عقد في طوكيو يومي 2 و 3 أيلول/سبتمبر 2019. ودعمت إيطاليا أيضاً عدداً من مشاريع منظمة الأمن والتعاون في أوروبا بشأن بناء القدرات في مجال الفضاء الإلكتروني/تكنولوجيا المعلومات والاتصالات، مثل "التدريب دون الإقليمي بشأن دور تكنولوجيات المعلومات والاتصالات في سياق الأمن الإقليمي والدولي" الذي نُظم في أثينا يومي 7 و 8 شباط/فبراير 2019.

وتشارك إيطاليا بنشاط في أنشطة الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وتدعم العمل الذي يضطلع به حاليا فريق الخبراء الحكوميين والذي اضطلعت به الأفرقة السابقة. وتشير إيطاليا أيضا إلى أن قرار الجمعية العامة 237/70 يرحب بالاستنتاجات التي توصل إليها فريقا الخبراء الحكومِيين السابقَين في تقريريهما لعامي 2013 و 2015، وتهيب بالدول الأعضاء أن تسترشد بتقرير عام 2015 في استخدامها لتكنولوجيات المعلومات والاتصالات.

والهدف من إنشاء إدارة مؤخراً تعنى بأمن الفضاء الإلكتروني والسياسات المتعلقة بالفضاء الإلكتروني داخل وزارة الخارجية والتعاون الدولي في إيطاليا هو زيادة تعزيز وتشجيع عملنا الدبلوماسي وتعاوننا الدولي في هذا المجال.

اليابان

[الأصل: بالإنكليزية]
[31 أيار/مايو 2020]

ترحب اليابان بفرصة الاستجابة لقرار الجمعية العامة 28/74 بشأن الارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي.

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

الجهود المبذولة على الصعيد الوطني لتعزيز أمن المعلومات

في اليابان، أعِد الأساس القانوني لاستخدام البيانات، بما في ذلك القانون الأساسي المتعلق بالنهوض باستخدام البيانات في القطاعين العام والخاص والقانون المعدَّل المتعلق بحماية المعلومات الشخصية. واعتمدت الحكومة أيضا سياسة للوصول إلى مجتمع محوره الإنسان ينجز كلا من التنمية الاقتصادية وتسوية المسائل الاجتماعية من خلال ارتفاع مستوى إدماج الفضاء الإلكتروني مع الفضاء الحقيقي. وفي ظل هذه الظروف، تُراكم حاليا كميات هائلة من البيانات المتأتية من أجهزة الاستشعار وسائر أنواع الأجهزة في الفضاء الحقيقي وتُحلل في الفضاء الإلكتروني. وعلاوة على ذلك، يمكن النظر بعين التشاؤم إلى نشوء وتطور الإمداد في الفضاء الحقيقي بمنتجات وخدمات جديدة تضيف قيمة من خلال استخدام البيانات في العديد من الميادين. فالفضاء الإلكتروني والفضاء الحقيقي لم يعودا يوجدان باعتبارهما كيانين مستقلين، ولكن باعتبارهما كيانين يتفاعلان فيما بينهما، بحيث لا يمكن اعتبارهما منفصلين بعد الآن. ولذلك، ينبغي اعتبار الفضاءين كياناً عضوياً واحداً يتطور باستمرار.

ويزيد توحيد الفضاء الإلكتروني والفضاء الحقيقي بدرجة كبيرة من إمكانية إتاحة الوفرة للمجتمع. وهو يزيد في الوقت نفسه أيضا من الفرص المتاحة للجهات الفاعلة الشريرة لإساءة استعمال الفضاء الإلكتروني. ومن المتوقع أن يتسع نطاق خطر الخسائر أو الأضرار الاقتصادية والاجتماعية في الفضاء

الحقيقي وأن يتسارع بصورة هائلة. وبشكل خاص، يبدو أن تفشي مرض فيروس كورونا (كوفيد-19) يعجل بالاتجاه نحو زيادة اعتماد البشرية على تكنولوجيا المعلومات والاتصالات، كما يزيد في الوقت نفسه من المخاطر والمشاكل الناجمة عن الاستخدام الخبيث لهذه التكنولوجيا. وهناك قلق متزايد بشأن التقارير عن الهجمات والأنشطة الخبيثة في الفضاء الإلكتروني التي تستفيد من الأزمة، بما في ذلك برامج الفدية التي تضرب المؤسسات والسلطات الطبية، فضلا عن الهجمات الرامية إلى تعطيل تقديم الخدمة التي تُشن من خلال نظم متعددة ضد مرافق البحوث الطبية. وفي ظل هذه الظروف، يجب ضمان أمن الفضاء الإلكتروني، الذي يشكل أساس المجتمع الاقتصادي، ويتعين في الوقت نفسه ضمان تطوره وتنميته على نحو مطرد ومستقل من أجل تحقيق التقدم المستدام والثروة للمجتمع.

وفي الآونة الأخيرة، كان هناك اتجاه عام لدى بعض الدول للتصدي للتهديدات الإلكترونية من خلال التركيز على قيام الدولة بالإدارة والمراقبة من موقع مهيمن. غير أن تعزيز إدارة الدولة للفضاء الإلكتروني ومراقبتها له يؤدي إلى عرقلة إمكانية تنميته بطريقة مستقلة ومستدامة. ويجب من ثم احترام الفضاء الإلكتروني القائم حالياً الذي أنشئ من خلال مبادرات مستقلة قامت بها جميع الجهات صاحبة المصلحة، ويجب حماية أمن الفضاء الإلكتروني من خلال مبادرات تعاونية وتآزرية مع تلك الجهات صاحبة المصلحة. واستنادا إلى هذا الفهم، ومراعاة للحالة المرغوب فيها في عام 2020 وما بعده، لن تدخر اليابان جهداً بشأن تدابير أمن الفضاء الإلكتروني عن طريق توضيح رؤيتها الأساسية لأمن الفضاء الإلكتروني، وتحديد المسائل الجديدة التي يتعين التصدي لها؛ وتنفيذ تلك التدابير على وجه السرعة.

الجهود المبذولة على الصعيد الوطني من أجل تعزيز التعاون الدولي

نظرا لأن آثار الحوادث التي تقع في الفضاء الإلكتروني يمكن أن تتجاوز الحدود الوطنية بسهولة، يمكن للحوادث الإلكترونية التي تقع خارج اليابان أن تضر دائما باليابان. وستمد اليابان يد التعاون والتآزر للحكومات والقطاع الخاص في جميع أنحاء العالم من أجل ضمان أمن الفضاء الإلكتروني والعمل من أجل سلام المجتمع الدولي واستقراره والأمن الوطني لليابان. وتحقيقا لهذه الغاية، ستبادر الحكومة إلى المساهمة في المناقشات الدولية المختلفة والعمل من أجل تبادل المعلومات والتوصل إلى فهم مشترك بشأن المسائل ذات الصلة بالفضاء الإلكتروني. وستقوم الحكومة أيضا بتبادل الخبرات مع البلدان الأجنبية، وتعزيز أشكال محددة من التعاون والتآزر، واتخاذ الإجراءات اللازمة عند الاقتضاء. وعلاوة على ذلك، ستشارك الحكومة بنشاط في المناقشات الدولية لمعالجة المسائل المتصلة بأمن الفضاء الإلكتروني التي ظهرت في ظل تفشي كوفيد-19.

وفي ما يتعلق بسياسة تبادل الخبرات والتنسيق، ستقوم الحكومة بالعمل من خلال الحوارات الثنائية والمؤتمرات الدولية المعنية بأمن الفضاء الإلكتروني لتبادل المعلومات بشأن السياسات والاستراتيجيات والنظم ذات الصلة بأمن الفضاء الإلكتروني للاستجابة، واستخدام تلك المعارف في التخطيط لسياسة اليابان في مجال أمن الفضاء الإلكتروني. وسنسعى أيضا إلى تعزيز تعاوننا وتآزرنا في مجال السياسات المتعلقة بأمن الفضاء الإلكتروني مع الشركاء الاستراتيجيين الذين يتقاسمون معنا نفس المبادئ الأساسية بشأن أمن الفضاء الإلكتروني.

وفي ما يتعلق بالتعاون الدولي في مجال التصدي للحوادث، ستقوم الحكومة بتقاسم المعلومات عن الهجمات والتهديدات الإلكترونية وتعزيز التعاون بين أفرقة مواجهة الطوارئ الحاسوبية لإتاحة الاستجابة

المنسَّقة عند وقوع الحوادث. وستسعى الحكومة أيضاً إلى تحسين القدرات على القيام باستجابات منسقة من خلال التدريب المشترك والمشاركة في التمارين الدولية في مجال الفضاء الإلكتروني. وعلاوة على ذلك، ستستجيب الحكومة على النحو الملائم في حالة وقوع حوادث من خلال التعاون الدولي الملائم.

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

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

وستعمل اليابان على بناء الثقة بين الدول لمنع حدوث الهجمات الإلكترونية. وبسبب سرية الهجمات الإلكترونية وعدم معرفة هوية مرتكبيها، توجد مخاطر تتمثل في إمكانية أن تزيد الهجمات الإلكترونية من حدة التوتر بين الدول عن غير قصد. ولمنع هذه المواجهات العرضية وغير الضرورية، من المهم بناء قنوات اتصال دولية خلال أوقات السلام استعدادا لوقوع الحوادث التي تتجاوز الحدود الوطنية. ومن الضروري أيضا زيادة الشفافية وبناء الثقة بين الدول من خلال تبادل المعلومات بصورة استباقية وإقامة حوارات بشأن السياسات في سياق مشاورات ثنائية ومتعددة الأطراف. وستتعاون الحكومة أيضاً مع الدول الأخرى للنظر في آلية لتنسيق المسائل المتعلقة بالفضاء الإلكتروني. وفي هذا السياق، تشجع اليابان بحماس تدابير بناء الثقة، بسبل منها الشروع في عقد اجتماع ما بين الدورات للمنتدى الإقليمي لرابطة أمم جنوب شرق آسيا في مجال أمن الفضاء الإلكتروني والمشاركة في ترأسه، مع التنفيذ المطرد لأنشطة المساعدة في مجال بناء القدرات، ولا سيما في منطقة آسيا والمحيط الهادئ.

وفي ما يتعلق ببناء القدرات، ولأن الترابط عبر الحدود يتعمق، من غير الممكن أن تتمكن اليابان من تحقيق السلام والاستقرار وحدها. فالتنسيق العالمي للحد من مواطن الضعف في مجال أمن الفضاء الإلكتروني وإزالتها ضروري جدا لضمان الأمن القومي لليابان. ومن هذا المنطلق، تضمن المساعدة المقدمة لبناء القدرات في الدول الأخرى استقرار حياة المقيمين اليابانيين وأنشطة الشركات اليابانية في البلدان الأخرى التي تعتمد على البنى التحتية الحيوية في تلك الدول وكذلك على التطور السليم لاستخدام الفضاء الإلكتروني فيها. ويرتبط بناء القدرات في الوقت نفسه ارتباطا مباشرا بضمان أمن الفضاء الإلكتروني كله ويسهم في تحسين البيئة الأمنية للعالم بأسره بما في ذلك اليابان. وأيضا في مجال جرائم الفضاء الإلكتروني، اليابان أول دولة آسيوية تصادق على الاتفاقية المتعلقة بالجريمة الإلكترونية وهي تضطلع بدور إيجابي في تعزيز الاتفاقية، التي تمثل إطارا قانونيا هاما للتصدي لجرائم الفضاء الإلكتروني، من خلال تقديم المساعدة في مجال بناء القدرات في المنطقة الآسيوية.

2 - مضمون المفاهيم المشار إليها في تقارير فريق الخبراء الحكوميين

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

تأثير الأعمال الإلكترونية الشريرة على المجتمع الدولي

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

تنفيذ المعايير الطوعية وغير الملزمة لسلوك الدول المسؤول

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

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

بغية مواصلة تعزيز الجهود التي تبذلها كل دولة من الدول لإقامة فضاء إلكتروني حر ومنصف وآمن والحفاظ عليه في سياق الأمن الدولي، ينبغي أن نؤكد من جديد أن جميع الدول تبدي إرادة قوية لإزالة الثغرات الأمنية في الفضاء الإلكتروني ومنع جني الأرباح من جرائم الفضاء الإلكتروني. وفي هذا السياق، ينبغي أن يشجع أعضاء الفريق على الدوام جميع الدول على تنفيذ المعايير الطوعية وغير الملزمة لسلوك الدول المسؤول بصورة مطردة، بما في ذلك تدابير بناء الثقة والتعاون في دعم الجهود الوطنية لبناء القدرات من أجل تنفيذ المعايير والتوصيات المذكورة أعلاه، بما في ذلك من خلال عملية فريق الخبراء الحكوميين المقبل والفريق العامل المفتوح العضوية.

المكسيك

[الأصل: بالإسبانية]
[29 أيار/مايو 2020]

أدت تكنولوجيات المعلومات والتطورات الجديدة في مجال الاتصالات السلكية واللاسلكية إلى توسيع إمكانيات التنمية المستدامة وتحقيق عالم قائم على الحقوق والإنصاف والإدماج. ويقع على عاتق المجتمع الدولي بأسره التزام بضمان الاستخدام السلمي لهذه التكنولوجيات من أجل الصالح العام.

وترسي المناقشات التي جرت في الأمم المتحدة بشأن الاستقرار في الفضاء الإلكتروني والأمن فيه وإدارة الفضاء الإلكتروني، ولا سيما تقارير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي بشأن النهوض بالسلوك المسؤول للدول في الفضاء الإلكتروني، الأساس لإحراز التقدم نحو إيجاد فضاء إلكتروني مفتوح وحر ومستقر وآمن.

وتمشيا مع تلك السوابق، تقدم حكومة المكسيك هذا التقرير على أساس أن القرارات التي اتخذتها الجمعية العامة ذات قيمة وأن النهج المتعدد الأطراف هو وحده الذي يمكن أن يكفل، في الأجل الطويل، الاستخدامات المشروعة والسلمية للفضاء الإلكتروني، والقدرة على الصمود في البيئة الرقمية، وإمكانات تكنولوجيات المعلومات بوصفها عوامل تمكينية للتنمية المستدامة، وحماية حقوق الإنسان في الفضاء الإلكتروني.

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

أنشأت حكومة المكسيك آليات التنسيق وهيئات الاستجابة الوطنية التالية التي تركز على أمن المعلومات:

(أ) اللجنة المتخصصة المعنية بأمن المعلومات

هي هيئة جماعية مشتركة بين الوكالات مسؤولة عن وضع سياسات أمن المعلومات التي تنطبق على المؤسسات الأمنية الوطنية وضمان تنفيذها على النحو السليم. وتُمثَّل الهيئات الاتحادية في المكسيك التي تركز على الأمن الوطني والأمن العام والاتصالات السلكية واللاسلكية والقطاع المالي والسياسة الخارجية في هذه اللجنة. وتشمل الأمثلة على المبادرات التي اتخذتها اللجنة تصميم وتحديث الاستراتيجية الوطنية لأمن الفضاء الإلكتروني، والتدريبات على مواجهة الحوادث الأمنية الحاسوبية، وأنشطة التوعية المتعلقة بأمن المعلومات.

(ب) المركز الوطني لمواجهة حوادث أمن الفضاء الإلكتروني

هذه الهيئة، التي تقع تحت مسؤولية الحرس الوطني المكسيكي المنشأ حديثا، مسؤولة عن رصد سلامة البنية التحتية التكنولوجية الاستراتيجية للبلد. وللمركز وحدات تتخصص في منع السلوك غير المشروع عن طريق استخدام الحواسيب والتحقيق فيه، وهو يرصد الشبكات لتحديد السلوك الإجرامي، ويضطلع بأنشطة تهدف إلى الحد من مخاطر التهديدات والهجمات الإلكترونية والتخفيف منها. كما أنه ينفذ برامج التطوير العلمي والتكنولوجي المتعلقة بأمن الفضاء الإلكتروني.

(ج) الفريق المعني بمواجهة الحوادث المتعلقة بأمن المعلومات الحساسة

هو آلية تنسيق تهدف إلى التعامل بفعالية مع الحوادث المتعلقة بأمن المعلومات في القطاع المالي. ويشارك في هذه الآلية مكتب المدعي العام والسلطات المالية الوطنية ونقابات عمال القطاع المالي في المكسيك، وتهدف الآلية إلى التعامل بفعالية مع الحوادث التي تؤثر تأثيرا مباشرا على القطاع المالي.

وعلى الصعيد الوطني، اتخذت المكسيك المبادرات التالية لتعزيز أمن المعلومات في السنوات الأخيرة:

تستضيف حكومة المكسيك، من خلال وزارة الأمن والحماية المدنية، سنويا أنشطة الأسبوع الوطني لأمن الفضاء الإلكتروني. والغرض من هذه المناسبة هو تشجيع الحوار بشأن تعزيز أمن الفضاء الإلكتروني، وتشجيع الشراكة بين القطاعات ذات الصلة من أجل ضمان بيئة رقمية آمنة وقادرة على الصمود. وتهدف هذه المناسبة أيضا إلى التوعية بشأن تكنولوجيات المعلومات والأمن الرقمي من خلال تنظيم مؤتمرات، وحلقات نقاش، وتدريب، وحلقات عمل، وحلقات دراسية شبكية، وأنشطة ترفيهية.

ومنذ عام 2018، استضافت حكومة المكسيك، بالتعاون مع منظمة الدول الأمريكية وشركة تريند مايكرو، مناسبة سنوية تعرف باسم تحدي النساء في مجال أمن الفضاء الإلكتروني (Cyberwomen Challenge). وتهدف هذه المناسبة إلى تعزيز المساواة بين الجنسين في الأنشطة المتعلقة بالحماية من تهديدات أمن الفضاء الإلكتروني والتصدي لها، وإلى زيادة قدرات المؤسسات ذات الصلة.

وفي عام 2019، عقدت وزارة الاتصالات والنقل حلقات عمل بشأن أمن الفضاء الإلكتروني، بمشاركة أكثر من 000 5 شخص من مراكز الشمول الرقمي التابعة للوزارة، التي تقع في جميع أنحاء البلد. وركزت حلقات العمل هذه على تحديد السلوك المحفوف بالمخاطر في استعمال خدمات الاتصالات السلكية واللاسلكية والبث. وكانت المعلومات التي تم جمعها من هذا النشاط بمثابة إسهام في تقرير عن عادات المستخدمين في مجال أمن الفضاء الإلكتروني في المكسيك أعِد في عام 2009.

واستنادا إلى النتائج الواردة في ذلك التقرير، تم تطوير أداة محاكاة بدعم من منظمة الدول الأمريكية وحكومة المملكة المتحدة. وهي أداة تمكن المستخدمين من تجربة تهديدات محاكاة لأمن الفضاء الإلكتروني في بيئة تفاعلية، من أجل تقييم قدرتهم على التصدي لمثل هذه التهديدات وتقديم المشورة بشأن أفضل طرق الحماية.

ومن أجل المساعدة على النهوض بالتعاون الدولي والسلوك المسؤول للدول في الفضاء الإلكتروني، تشارك المكسيك في المنتديات والآليات والمبادرات المتعددة الأطراف والإقليمية التالية:

(أ) اللجنة الأولى التابعة للجمعية العامة للأمم المتحدة

تشارك المكسيك في الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، الذي أنشئ عملا بقرار الجمعية العامة 27/73.

وبالإضافة إلى ذلك، يشارك خبير حكومي من المكسيك في فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي، الذي أنشئ عملا بقرار الجمعية العامة 266/73.

وسعت المكسيك إلى ضمان عمل الهيئتين بطريقة تكاملية، وتقر بأن كلا الهيئتين تواصلان الاستناد إلى عمل أفرقة الخبراء الحكوميين السابقة وإلى تقاريرها التي اعتمدتها الجمعية العامة بتوافق الآراء.

(ب) مجموعة الأصدقاء المعنية بالتكنولوجيات الرقمية

تعلق المكسيك أهمية كبيرة على تصميمِ الأنشطة المتعلقة بالتكنولوجيات الرقمية، ولا سيما تلك التي تدعم تنفيذ أهداف وغايات التنمية المستدامة من خلال تعزيز الاستخدام الإيجابي لتكنولوجيات المعلومات والاتصالات، وعلى التعاونِ في هذا الصدد. وبناء على ذلك، عملت المكسيك، منذ تشرين الثاني/نوفمبر 2019، بالاشتراك مع فنلندا وسنغافورة، كرئيسة مشاركة لمجموعة الأصدقاء المعنية بالتكنولوجيات الرقمية، التي تهدف إلى تشجيع الحوار الشامل مع جميع أصحاب المصلحة من أجل النظر في الروابط بين التكنولوجيات الرقمية والتنمية المستدامة، ومناقشة أشكال التعاون الدولي الشاملة ذات الصلة.

(ج) الفريق الرفيع المستوى المعني بالتعاون الرقمي الذي أنشأه الأمين العام للأمم المتحدة

عملا بتوصيات الفريق الرفيع المستوى المعني بالتعاون الرقمي، قادت المكسيك، بالاشتراك مع هيئة الأمم المتحدة للمساواة بين الجنسين وتمكين المرأة (هيئة الأمم المتحدة للمرأة)، مناقشة للفريق تهدف إلى تحديد خطوات محددة لتنفيذ التوصيتين 1 (ج) و 1 (د)، بشأن الشمول الرقمي والمقاييس ذات الصلة.

(د) الاتحاد الدولي للاتصالات

تشارك المكسيك في المبادرات المتعلقة بأمن المعلومات وأمن الفضاء الإلكتروني التي ينسقها الاتحاد الدولي للاتصالات، مثل البرنامج العالمي لأمن الفضاء الإلكتروني والمؤشر العالمي لأمن الفضاء الإلكتروني.

وتعتبر المكسيك أن البرنامج العالمي لأمن الفضاء الإلكتروني مبادرة هامة تسهم في تهيئة بيئة رقمية أكثر أماناً ومرونة، وهي ذات قيمة جوهرية من حيث أنها تتيح مشاركة جميع أصحاب المصلحة، بما في ذلك الدول والقطاع الخاص والمجتمع المدني والأوساط الأكاديمية.

(هـ) منظمة الدول الأمريكية

تشارك المكسيك بنشاط في برنامج أمن الفضاء الإلكتروني للجنة البلدان الأمريكية لمكافحة الإرهاب التابعة لمنظمة الدول الأمريكية، الذي يعزز وضع السياسات، وتنمية القدرات، والبحث، والتوعية في المنطقة.

ويشارك المركز الوطني لمواجهة حوادث أمن الفضاء الإلكتروني في شبكة أفرقة مواجهة الحوادث الأمنية الحاسوبية في الأمريكتين في إطار برنامج أمن الفضاء الإلكتروني للجنة البلدان الأمريكية لمكافحة الإرهاب التابعة لمنظمة الدول الأمريكية.

وتشارك المكسيك أيضا في الفريق العامل المعني بالتعاون وتدابير بناء الثقة في الفضاء الإلكتروني التابع للجنة البلدان الأمريكية لمكافحة الإرهاب (منظمة الدول الأمريكية). ونتيجة لعمل هذا الفريق الذي أنشئ في عام 2018، تم اعتماد تدابير بناء الثقة التالية:

- تقديم معلومات عن السياسات الوطنية المتعلقة بأمن الفضاء الإلكتروني، مثل الاستراتيجيات الوطنية، والكتب البيضاء، والأطر القانونية، وغيرها من الوثائق التي تعتبرها كل دولة عضو ذات صلة بالموضوع.
- تحديد جهة اتصال وطنية معنية بالسياسات العامة قادرة على مناقشة الآثار المترتبة على التهديدات الإلكترونية في نصف الكرة الأرضية الغربي.
- تعيين جهات اتصال، في حالة عدم وجودها، داخل وزارات الخارجية، بغرض تيسير العمل على التعاون والحوار الدوليين في مجالي الفضاء الإلكتروني وأمنه.
- تطوير وتعزيز بناء القدرات من خلال أنشطة مثل الحلقات الدراسية والمؤتمرات وحلقات العمل بشأن دبلوماسية الفضاء الإلكتروني لفائدة موظفي القطاعين العام والخاص.
- تشجيع إدراج المواضيع المتعلقة بالفضاء الإلكتروني وأمنه في الدورات التدريبية للدبلوماسيين والمسؤولين في وزارات الخارجية والوكالات الحكومية الأخرى.
- تشجيع التعاون وتبادل أفضل الممارسات المتعلقة بدبلوماسية الفضاء الإلكتروني، والفضاء الإلكتروني، وأمنه من خلال إنشاء أفرقة عاملة، وآليات أخرى للحوار، وتوقيع اتفاقات بين الدول.

(و) المنتدى العالمي لخبرات الفضاء الإلكتروني

منذ عام 2015، شاركت المكسيك في هذا المنتدى، الذي يكرس جهوده لبناء القدرات في مجال أمن الفضاء الإلكتروني. والمجالات التي تهم المكسيك هي منع الهجمات الإلكترونية، وحماية البيانات، ومنع الجريمة الإلكترونية (بما في ذلك استغلال الأطفال في المواد الإباحية وما شابهها من جرائم)، ومبادرات الحكومة الإلكترونية والاستراتيجيات الرقمية، وحماية البنية التحتية الحيوية، والاستخدامات السلمية لتكنولوجيات المعلومات والاتصالات والإنترنت، وسريان القانون الدولي على الفضاء الإلكتروني.

(ز) منتدى الأفرقة المعنية بمواجهة الحوادث وبالأمن

المركز الوطني لمواجهة حوادث أمن الفضاء الإلكتروني هو عضو في منتدى الأفرقة المعنية بمواجهة الحوادث وبالأمن، وهو منتدى عالمي يجمع بين أفرقة مواجهة حوادث أمن الفضاء الإلكتروني من جميع أنحاء العالم ويشجع التعاون بينها. وهذا يجعل من الممكن تطوير وتقوية البحوث التي يمكن استخدامها، إلى جانب سياسات أمن الفضاء الإلكتروني للدول الأخرى، لتحديد هوية المرتكبين المحتملين للهجمات الإلكترونية وتحديد أماكنهم.

2 - محتوى المفاهيم المذكورة في تقارير فريق الخبراء الحكوميين

وفقاً للبيانات الواردة في التقارير السابقة لفريق الخبراء الحكوميين، تعتقد المكسيك أن القانون الدولي ينطبق على الفضاء الإلكتروني. ولدعم هذا المبدأ، اتخذت حكومة المكسيك مبادرات على المستوى الوطني لدعم موقفها بأن القانون الدولي المنطبق يشير إلى ميثاق الأمم المتحدة، والقانون الدولي لحقوق الإنسان، والقانون الدولي الإنساني، وقواعد القانون الدولي العرفي المنطبقة، والاجتهاد القضائي ذي الصلة.

وتمشيا مع التقارير السابقة لفريق الخبراء الحكوميين، تعترف المكسيك بالدور والمساهمات المحتملة للهيئات الإقليمية، ولا سيما في تنفيذ تدابير بناء الثقة. ولذلك شجعت حكومة المكسيك هيئاتها الوطنية على النظر في تنفيذ تدابير بناء الثقة المنصوص عليها في تقارير فريق الخبراء الحكوميين والتي تم تطويرها في عمل منظمة الدول الأمريكية.

وتولي المكسيك أهمية كبيرة لمفهوم بناء القدرات الذي تم التأكيد عليه في تقارير فريق الخبراء الحكوميين، لأن هذا المفهوم لا يشير فقط إلى تنمية القدرات الوطنية في مجال أمن المعلومات، ولكن أيضا إلى الحاجة إلى الاستفادة من جميع أشكال التعاون الدولي التي ثبت أنها تسهم في السلام والأمن الدوليين. ويضمن بناء القدرات أن يكون كل من الدول وجميع أصحاب المصلحة الآخرين مجهزين بشكل أفضل لمواجهة تهديدات أمن الفضاء الإلكتروني، ويعزز الفهم المشترك للمسائل المتعلقة بأمن الفضاء الإلكتروني.

وخلال الفترة المشمولة بالتقرير، سعت حكومة المكسيك أيضا إلى تعزيز أوجه التآزر بين مجموعات ومنتديات وهيئات منظومة الأمم المتحدة وكذلك مبادراتها التي تركز على المسائل المتصلة بتكنولوجيا المعلومات، والاتصالات السلكية واللاسلكية، وأمن الفضاء الإلكتروني، وإدارة الفضاء الإلكتروني، والتعاون الرقمي، والتغير التكنولوجي، من أجل تحسين التماسك، وتجنب ازدواجية الجهود، واستخدام الموارد بشكل أفضل من أجل التعاون.

سنغافورة

[الأصل: بالإنكليزية]
[27 نيسان/أبريل 2020]

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 يستند إلى القانون الدولي المنطبق، ومعايير محددة جدًا لسلوك الدولة المسؤول، وتدابير قوية لبناء الثقة، وبناء منسق للقدرات. ومن المهم أن يستمر 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.

وتشارك سنغافورة في كل من فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي وفي الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي. وتؤكد سنغافورة من جديد أنها ترى أن هذين المنتديين يكمل الواحد منهما الآخر، وستواصل الإسهام بصورة بناءة في العمليتين. ولكي تنجح العمليتان، يجب أن تتم أعمالهما بروح من التعاون البناء، وتوافق الآراء، والاحترام المتبادل، والثقة المتبادلة. وسنغافورة، بوصفها رئيسة مشاركة لمجموعة الأصدقاء المعنية بالحوكمة الإلكترونية وأمن الفضاء الإلكتروني مع إستونيا، ملتزمة بإشراك جميع البلدان في دعم سير العمليتين. وتعتقد سنغافورة أن الاجتماع التشاوري غير الرسمي الذي عقده بين الدورات الفريق العامل المفتوح العضوية، برئاسة الرئيس التنفيذي لوكالة أمن الفضاء الإلكتروني في سنغافورة، ديفيد كوه، كان مفيدا في تيسير تبادل تفاعلي للآراء بين الدول الأعضاء، والقطاع الخاص، والمجتمع المدني، والأوساط الأكاديمية، والأوساط التقنية بشأن مجموعة من المسائل الموضوعية.

وتعتقد سنغافورة أنه يتوجب على الدول تعزيز الوعي بالمعايير الطوعية وغير الملزمة القائمة للسلوك المسؤول للدول ودعم تنفيذها. وتؤيد سنغافورة زيادة تفصيل هذه المعايير عند الحاجة. فعلى سبيل المثال، يمكن اعتبار البنية التحتية الحيوية للمعلومات التي تتجاوز حدود الولاية الوطنية فئة خاصة من هذه البنية التحتية الحيوية، التي تُعتبر حمايتها مسؤولية مشتركة بين جميع الدول الأعضاء، ويمكن إدراجها في مجموعة المعايير القائمة[(11)].

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. وقرر المشاركون في المؤتمر الوزاري الثالث لرابطة أمم جنوب شرق آسيا بشأن أمن الفضاء الإلكتروني، الذي عقد في أيلول/سبتمبر 2018، الالتزام من 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

(11) البنى التحتية الحيوية للمعلومات التي تتجاوز حدود الولاية الوطنية هي تلك البنى التي تملكها شركات خاصة وتعمل عبر الحدود الوطنية، ولكنها لا تخضع لولاية أي دولة بمفردها.

تشرين الأول/أكتوبر 2019، قرر المؤتمر الوزاري الرابع للرابطة المعني بأمن الفضاء الإلكتروني إنشاء لجنة عاملة للنظر في وضع خطة عمل إقليمية طويلة الأجل لضمان 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.

وبناء القدرات بالغ الأهمية لضمان أن تطور الدول القدرة على التنفيذ الناجح لقواعد ومعايير سلوك الدول المسؤول. وفي إطار هذا الجهد، أنشأت سنغافورة برنامجا للرابطة معنيا بالقدرات المتعلقة بالفضاء الإلكتروني بقيمة عشرة ملايين دولار سنغافوري في عام 2016 لدعم بناء القدرات في الرابطة بشأن السياسة العامة الإلكترونية والاستراتيجية والمسائل التقنية. وقد تم حتى الآن تدريب 170 مسؤولا من الدول الأعضاء في الرابطة في إطار البرنامج. وكامتداد لبرنامج الرابطة لبناء القدرات في مجال الفضاء الإلكتروني، افتتحت سنغافورة مركز الامتياز المشترك بين سنغافورة والرابطة والمعني بأمن الفضاء الإلكتروني البالغة تكلفته 30 مليون دولار سنغافوري في تشرين الأول/أكتوبر 2019 لمواصلة دعم رسم السياسات في مجال أمن الفضاء الإلكتروني، ووضع الاستراتيجيات، وكذلك بناء القدرات التقنية والتشغيلية في بلدان رابطة أمم جنوب شرق آسيا، فضلاً عن التعاون بشكل أوثق مع الشركاء الدوليين.

وشاركت سنغافورة أيضاً في تنظيم حلقة دراسية في إطار البرنامج المشترك بينها والأمم المتحدة في مجال الفضاء الإلكتروني للتوعية بمعايير الفضاء الإلكتروني وتخطيط السياسات للتعامل مع سيناريوهات 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. كما قامت سنغافورة بتنفيذ عدة دورات تدريبية في مجال أمن الفضاء الإلكتروني في إطار برنامج سنغافورة للتعاون. وما زلنا ملتزمين بتقاسم تجربتنا وخبرتنا مع الدول الأعضاء في الأمم المتحدة، ولا سيما البلدان الصغيرة والنامية.

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* – وضعت وكالة أمن الفضاء الإلكتروني في سنغافورة الخطة الرئيسية للأمن الإلكتروني للتكنولوجيا التشغيلية كجزء من جهود سنغافورة المستمرة لتعزيز أمن ومرونة قطاعات البنية التحتية الحيوية للمعلومات 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 المعني وأصحاب المصلحة. وتحدد الخطة الرئيسية مبادرات رئيسية تشمل كلا من الأشخاص والعمليات والتكنولوجيا لتعزيز قدرات مالكي بنيتنا التحتية الحيوية للمعلومات والمنظمات التي تستخدم نظم التكنولوجيا التشغيلية.

(ب) *إيجاد فضاء إلكتروني أكثر أمانا* – في إطار الجهود الرامية إلى تحسين تأمين الفضاء الإلكتروني ورفع مستويات النظافة الإلكترونية، ستبدأ سنغافورة في تنفيذ خطة وضع العلامات المتعلقة بأمن الفضاء الإلكتروني في عام 2020 للأجهزة الذكية المتصلة بالشبكة. وسيتم إطلاق الخطة الرئيسية باعتبارها

طوعية لإتاحة الوقت للسوق والمطورين لفهم كيف تفيدهم. 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. ويهدف نظام وضع علامات أمن الفضاء الإلكتروني 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* – تسلم سنغافورة بأن تعزيز أمن الفضاء الإلكتروني يشمل بناء البيئة الإلكترونية وتشجيع الابتكار ضمن الصناعة ذات الصلة. وهناك أيضا حاجة متزايدة إلى تكوين مجموعة من الأفراد الموهوبين الذين يمكنهم تولي أدوار قيادية في مجال أمن الفضاء الإلكتروني في المنظمات. ومنذ تأسيس وكالة أمن الفضاء الإلكتروني في عام 2015، عملت مع الوكالات الحكومية والرابطات والشركاء الصناعيين ومؤسسات التعليم العالي في سنغافورة على توسيع وتطوير القوة العاملة في مجال أمن الفضاء الإلكتروني. وتقود وكالة أمن الفضاء الإلكتروني مبادرة وطنية جديدة للمواهب في مجال أمن الفضاء الإلكتروني لجذب ورعاية المتحمسين الموهوبين في مجال أمن الفضاء الإلكتروني منذ سن مبكرة ومساعدة المتخصصين في أمن الفضاء الإلكتروني على صقل مهاراتهم. وتهدف المبادرة إلى التواصل مع ما لا يقل عن 000 20 شخص على مدى ثلاث سنوات.

تركيا

[الأصل: بالإنكليزية]
[22 أيار/مايو 2020]

الجهود المبذولة على الصعيد الوطني لتعزيز أمن المعلومات وتشجيع التعاون الدولي

أصبحت تكنولوجيات المعلومات والاتصالات جزءاً أساسياً من المجتمع والاقتصاد. فهي تُستخدم في شبكة واسعة تشمل القطاعين العام والخاص والبنى 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 الوطني. ووزارة النقل والبنية التحية هي الهيئة المسؤولة عن رسم السياسات ووضع الاستراتيجيات وخطط العمل في ما يتعلق بأمن الفضاء الإلكتروني الوطني في تركيا. وفي هذا السياق، وُضعت الاستراتيجية وخطة العمل الوطنيتان لأمن الفضاء الإلكتروني بمشاركة جميع أصحاب المصلحة المعنيين ضمن أفرقة دراسة بتنسيق من وزارة النقل والبنية التحية. وتم نشر وتنفيذ الاستراتيجية الوطنية لأمن الفضاء الإلكتروني، وخطة العمل للفترة 2013–2014، والاستراتيجية وخطة العمل الوطنيتين لأمن الفضاء الإلكتروني للفترة 2016–2019. وتضع تركيا استراتيجيتها وخطة عملها الوطنيتين المقبلتين لأمن الفضاء الإلكتروني، اللتين من المقرر أن تغطيا السنوات 2020–2023، وسيجري نشرهما قريبا.

والأهداف الاستراتيجية الرئيسية للاستراتيجية وخطة العمل الوطنيتين المقبلتين لتركيا في مجال أمن الفضاء الإلكتروني هي:

- حماية البنى التحتية الحيوية وزيادة القدرة على الصمود
- تنمية القدرات
- أمن التكنولوجيات الجديدة (إنترنت الأشياء، والجيل الخامس من شبكات الاتصال اللاسلكية، والحوسبة السحابية، إلخ)
- مكافحة الجريمة الإلكترونية
- تطوير وتشجيع التكنولوجيات الوطنية
- الشبكة العضوية لأمن الفضاء الإلكتروني
- تحسين التعاون الدولي.

وعلاوة على ذلك، قام الفريق الوطني لمواجهة الطوارئ الإلكترونية 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، فإن الفريق الوطني لمواجهة الطوارئ الإلكترونية مسؤول عن تنفيذ التدابير الوقائية ضد التهديدات الإلكترونية ويكفل الردع الإلكتروني. ومجالات تركيزه الرئيسية في أمن الفضاء الإلكتروني هي: بناء القدرات الإلكترونية، واتخاذ التدابير التكنولوجية، وجمع المعلومات الاستخباراتية عن التهديدات والإبلاغ بها، وحماية البنية التحتية الحيوية.

وفي سياق تحسين أمن الفضاء الإلكتروني الوطني، تم أيضاً منذ عام 2013 إنشاء 14 فريقاً قطاعياً لمواجهة الطوارئ الإلكترونية للقطاعات أو البنى التحتية الحيوية (مثل الطاقة، والصحة، والمصارف والمالية، وإدارة المياه، والاتصالات الإلكترونية، والخدمات العامة الحيوية)، و 299 1 فريقاً مؤسسياً لمواجهة الطوارئ الإلكترونية. وتعمل جميعها على مدار الساعة، سبعة أيام في الأسبوع، بتنسيق من الفريق الوطني من أجل التخفيف من المخاطر الإلكترونية ومكافحة التهديدات الإلكترونية.

وينظم الفريق الوطني لمواجهة الطوارئ الإلكترونية ويدعم الدورات التدريبية، والمخيمات الصيفية، والمسابقات بشأن أمن الفضاء الإلكتروني التي هي مفتوحة لعدة مجتمعات محلية. وبالإضافة إلى ذلك، يقدم الفريق دورات تدريبية لأفرقة مواجهة الطوارئ الإلكترونية في مجالات مثل تحليل البرامجيات الخبيثة وتحليل السجلات وغيرها. وقد تم تدريب أكثر من 500 4 شخص في مجالات مختلفة من أمن الفضاء الإلكتروني على يد الفريق الوطني لمواجهة الطوارئ الإلكترونية في السنوات الثلاث الماضية.

وتشمل الدراسات المتعلقة بالتدابير التكنولوجية الكشف المبكر وأنشطة الإنذارات والتحذيرات. ووضعت تركيا لهذا الغرض نظما للكشف والوقاية. وتلعب هذه النظم دوراً كبيراً في زيادة مستوى أمن الفضاء الإلكتروني الوطني في تركيا.

وتنظم عدة منظمات ومؤسسات وجامعات ومنظمات غير حكومية تركية والقطاع الخاص أيضا حلقات دراسية ومؤتمرات ودورات تدريبية على الصعيد الوطني بشأن أمن الفضاء الإلكتروني، وحماية البنى التحتية الحيوية وغير ذلك من المواضيع ذات الصلة.

وعلاوة على ذلك، يُنظَّم سنويا يوم خاص بالاستخدام الآمن للإنترنت لأنشطة التوعية بشأن الاستخدام الواعي والآمن للإنترنت. وبدأ العمل بخط اتصال مجاني للمساعدة في مجال الإنترنت وبموقع شبكي يسمى الشبكة الآمنة، حيث يمكن للأسر أن تجد المشورة في ما يتعلق بالاستخدام الكفؤ للإنترنت. (https://www.guvenlinet.org.tr/).

وتمشياً مع انتشار استخدام تكنولوجيا المعلومات والاتصالات بين الأفراد، أصبحت المعلومات أو البيانات الشخصية هدفاً جذاباً للمهاجمين في الفضاء الإلكتروني. وخصوصية البيانات الشخصية وحمايتها هما أيضا من بين الشواغل الأمنية الرئيسية. وفي هذا الصدد، دخل القانون رقم 6698 بشأن حماية البيانات الشخصية حيز النفاذ في عام 2016 لحماية الخصوصية.

وما فتئت تركيا تؤدي أدواراً هامة في العديد من المنظمات، إما باعتبارها عضواً مؤسِّساً، أو من خلال المساهمة في جهود التعاون في المسائل المتعلقة بأمن الفضاء الإلكتروني وأمن المعلومات. وفي هذا السياق، تعلق تركيا أهمية على تبادل المعلومات مع مختلف البلدان والمنظمات في مجموعة كبيرة من المجالات. والفريق الوطني لمواجهة الطوارئ الإلكترونية في تركيا عضو في منتدى فرق التصدي للحوادث والأمن، ومؤسسة Trusted Introducers، والاتحاد الدولي للاتصالات، والمنتدى المتعدد الجنسيات لتبادل المعلومات عن البرامجيات الخبيثة التابع لمنظمة معاهدة شمال الأطلسي (الناتو) وتحالف أمن الفضاء الإلكتروني من أجل التقدم المشترك. وما فتئت تركيا تشارك أيضا في مركز الامتياز للدفاع التعاوني الإلكتروني التابع لمنظمة حلف شمال الأطلسي كدولة راعية منذ تشرين الثاني/نوفمبر 2015. وبالإضافة إلى ذلك، هناك تعاون ثنائي ومتعدد الأطراف جار بشأن أمن الفضاء الإلكتروني مثل مذكرات التفاهم مع العديد من البلدان. وعلاوة على ذلك، تقوم تركيا بالمشاركة والمساهمة بنشاط في دراسات منظمات دولية مثل الناتو، والأمم المتحدة، ومنظمة الأمن والتعاون في أوروبا، ومنظمة التعاون والتنمية في الميدان الاقتصادي ومجموعة العشرين، ومجلس التعاون للدول الناطقة بالتركية ومركز التعاون الأمني التابع للمركز الإقليمي للمساعدة على التحقق من تحديد الأسلحة وتنفيذه.

وتمارين أمن الفضاء الإلكتروني هي نشاط هام آخر بالنسبة للتعاون والتأهب. ويسهم هذا النوع من التمارين الذي يجرى على الصعيدين الوطني والدولي في تعزيز أمن الفضاء الإلكتروني واختبار التدابير التي ستتخذ لمواجهة التهديدات الإلكترونية المحتملة. ومنذ عام 2011، نظمت وزارة النقل والبنية التحتية أربعة تمارين وطنية وتمرينين دوليين على أمن الفضاء الإلكتروني. وفي الآونة الأخيرة، شاركت وزارة النقل والبنية التحتية وهيئة تكنولوجيات المعلومات والاتصالات في تنظيم "الدرع الإلكتروني" لعام 2019، وهو تمرين دولي في مجال أمن الفضاء الإلكتروني، في 19 كانون الأول/ديسمبر 2019 في أنقرة، تركيا. وحظي تمرين "الدرع الإلكتروني" لعام 2019 بدعم من الاتحاد الدولي للاتصالات وتحالف أمن الفضاء الإلكتروني من أجل التقدم المشترك. وعلاوة على ذلك، تشارك تركيا في التمارين الدولية لأمن الفضاء الإلكتروني مثل "الدروع المقفلة" للناتو، والائتلاف المعني بالفضاء الإلكتروني التابع للناتو، وتمرين إدارة الأزمات للحلف نفسه، كما تساهم في هذه التمارين.

وصـــدقت تركيا أيضـــا على الاتفاقية المتعلقة بالجريمة الإلكترونية، التي تغطي جرائم مختلفة من قبيل الجرائم التي ترتكب عن طريق الإنترنت وغيرها من الشبكات الحاسوبية، والاحتيال المتصل بالحاسوب، واستغلال الأطفال في المواد الإباحية وانتهاكات أمن الشبكات، وجميع هذه الجرائم مدرجة الآن في التشريعات الوطنية في تركيا.

ويتطلب الســلام والأمن الدوليان في الفضــاء الإلكتروني مزيداً من الدراســات اســتناداً إلى التعاون الدولي المعزز. ويمكن أن يُرى بوضــوح أن القانون الدولي والمعايير والقواعد المبينة في تقارير فريق الخبراء الحكوميين وفي الدراسات ذات الصلة تسهم في إيجاد فضاء إلكتروني أكثر أمنا.

وعلاوة على ذلك، فإن تحســـين التعاون ودعم آليات تبادل المعلومات بالغا الأهمية لمكافحة التهديدات في الفضاء الإلكتروني، وينبغي إعطاؤهما الأولوية الواجبة.

وإضـافة إلى ذلك، فإن الحاجة إلى التوجيه بشـأن أمن تكنولوجيات الجيل الجديد (إنترنت الأشـياء، والجيل الخامس من شبكات الاتصـال اللاسلكية، والحوسبة السحابية، وما إلى ذلك) هي نقطة أخرى ينبغي أخذها في الاعتبار. وســـتســـاعد الأدلة أو التوصـــيات الأمنية الأســـاســـية المتعلقة بالجيل الجديد من التكنولوجيات، التي يجري إعدادها بالتعاون فيما بين الدول الأعضاء، على زيادة مستويات التأهب للتهديدات الإلكترونية الجديدة المصـاحبة لها. وعلاوة على ذلك، وفضـلا عن الدراسـات الأخرى المتعلقة ببناء القدرات والتوجيه، تظل التمارين الدولية في مجال أمن الفضـــاء الإلكتروني بالغة الأهمية لزيادة مســـتويات التأهب وبناء القدرات على مواجهة الحوادث الإلكترونية في جميع أنحاء العالم.

أوكرانيا

[الأصل: بالإنكليزية]
[29 أيار/مايو 2020]

منذ بداية العدوان المختلط للاتحاد الروســـي على أوكرانيا، ظهرت تهديدات وتحديات جديدة، أخذ فيها استخدام آليات التأثير الإلكتروني على حساب أمن الدولة في أوكرانيا مكانا هاما.

ولا تزال أوكرانيا ثابتة في التزامها بالقانون الدولي فيما يتعلق باســـتخدام تكنولوجيا المعلومات والاتصـالات، فضـلا عن دعمها الكامل للاستنتاجات والتوصيات الواردة في تقارير فريق الخبراء الحكوميين. فهو يشـير أولا إلى الحفاظ على المسـاواة في السـيادة بين الدول، وعدم اسـتخدام القوة أو التهديد باسـتخدامها ضـــد الســـلامة الإقليمية للدول، وعدم التدخل في الشـــؤون الداخلية للدول الأخرى، واحترام حقوق الإنســـان والحريات الأساسية.

ومن أجل تنظيم إجراءات فعالة لمواجهة التهديدات في الفضاء الإلكتروني والتنظيم القانوني للسلوك في هذا الفضـــاء، والقيام في الوقت ذاته بتحديد عملية وضـــع نظام للعمل على مواجهة هذه التهديدات على مستوى الدولة، اعتُمد عدد من الأنظمة، أهمها استراتيجية أوكرانيا لأمن الفضاء الإلكتروني التي أقرها مجلس الأمن والدفاع الوطني؛ والقرار المتعلق باســتراتيجية أوكرانيا لأمن الفضــاء الإلكتروني (الذي صــدر بموجب المرسوم رقم 96 الصادر عن رئاسة أوكرانيا في 15 آذار/مارس 2016) والقانون المتعلق بالمبادئ الأساسية للحفاظ على أمن الفضاء الإلكتروني في أوكرانيا المؤرخ 5 أيار/مايو 2017.

وتمثلت آلية مستقلة لمواجهة التهديدات الإلكترونية في استخدام أحكام قانون أوكرانيا بشأن الجزاءات المؤرخ 14 آب/أغسطس 2014، الذي أتاح تنظيم تصد سريع للتهديدات المحددة عن طريق تطبيق تدابير تقييدية ضد عدد من الكيانات القانونية والأفراد الضالعين في تدابير تهدف إلى المس بالأمن القومي لأوكرانيا.

واليوم، يجري توفير الحماية الإلكترونية لموارد المعلومات الإلكترونية الحكومية والبنية التحتية الحيوية ذات الصلة في أوكرانيا وفقا لقانون المبادئ الأساسية للحفاظ على أمن الفضاء الإلكتروني في أوكرانيا. وتُستخدم تعاريف السلطة والمهام والوظائف الخاصة بالقائمين على أمن الفضاء الإلكتروني المنصوص عليها في هذا القانون في إنشاء نظام كلي لأمن الفضاء الإلكتروني.

وفي هذا الصدد، فالمبدأ الأساسي في وضع السياسة العامة في مجال أمن الفضاء الإلكتروني والدفاع عنه هو وضع إطار تنظيمي يتسق مع النُهج والمعايير الدولية. ولتنفيذ هذه المهمة، على وجه التحديد، اتُخذت التدابير التالية:

- اعتُمد قرار حكومة أوكرانيا بشأن الموافقة على المتطلبات العامة المتعلقة بالحماية الإلكترونية للبنية التحتية الحيوية؛ وتراعي نُهج أمن الفضاء الإلكتروني التي يحددها هذا القرار متطلبات المعايير الدولية في مجال أمن المعلومات وتنفذ توجيهات الاتحاد الأوروبي، مما يجعل الدولة مشاركة على قدم المساواة في مجال الأمن العالمي
- وُضعت مشاريع قرارات لحكومة أوكرانيا:

– بشأن الموافقة على الإجراء الخاص باستعراض حالة الحماية الإلكترونية للبنية التحتية الحيوية للمعلومات، وموارد معلومات الدولة ومعلوماتها، التي ينص القانون على ضرورة حمايتها

– بشأن الموافقة على إجراء تعيين مرافق البنية التحتية الحيوية

– بشأن الموافقة على إجراء تجميع قائمة بمرافق البنية التحتية الحيوية للمعلومات، وإدراج مرافق البنية التحتية الحيوية للمعلومات في سجل الدولة لمرافق البنية التحتية الحيوية للمعلومات، وتشكيله وتشغيله، مع مراعاة متطلبات توجيه الاتحاد الأوروبي 1148/2016 الصادر عن البرلمان الأوروبي ومتطلبات مجلس أوروبا بشأن التدابير الرامية إلى تحقيق مستوى مشترك عال من الأمن في شبكات ونظم المعلومات في جميع أنحاء الاتحاد

– بشأن الموافقة على البروتوكول المتعلق بالإجراءات المشتركة للكيانات المعنية بأمن الفضاء الإلكتروني ومالكي (مديري) مرافق البنية التحتية الحيوية للمعلومات أثناء الكشف عن الهجمات والحوادث الإلكترونية ومنعها ووقفها، وكذلك في إزالة آثارها.

ومن أجل تعزيز نظام الحماية التقنية والترميزية للمعلومات، تم اعتماد خريطة الطريق لإصلاح مجال حماية المعلومات من خلال تكييف تشريعات أوكرانيا مع متطلبات تشريعات الاتحاد الأوروبي؛ ووُضع مشروع قانون لأوكرانيا بشأن أمن المعلومات ونظم الاتصالات والمعلومات لتنفيذ خريطة الطريق هذه.

ومن العناصر الرئيسية للتطوير الفعال للنظام الوطني لأمن الفضاء الإلكتروني، هناك استعراضُ حالة أمن الفضاء الإلكتروني. وستكون نتائج الاستعراض الأساس لوضع استراتيجية وطنية جديدة لأمن الفضاء الإلكتروني أو تعديل الاستراتيجية القائمة، لتحسين الإطار التنظيمي لكيانات أمن الفضاء

الإلكتروني، وتمويل تدابير الحماية الإلكترونية لموارد المعلومات الحكومية والبنية التحتية الحيوية ذات الصلة، وتحسين نظام تدريب الموارد البشرية في مجال أمن الفضاء الإلكتروني، ووضع نُهج جديدة لبلورة التعاون بين القطاعين العام والخاص في هذا المجال، وتعزيز تبادل المعلومات بين القائمين على أمن الفضاء الإلكتروني وتفاعلهم في معالجة المسائل الأمنية.

وعلاوة على ذلك، ومن أجل تقوية أمن المعلومات وتعزيز التعاون الدولي في هذا المجال، عملت دائرة الاتصالات الخاصة الحكومية على ما يلي:

- اشتغال فريق مواجهة الطوارئ الحاسوبية في أوكرانيا، الذي اعتمده منتدى أفرقة مواجهة الحوادث الأمنية الإلكترونية، والذي يتفاعل مع أفرقة أخرى من 96 دولة
- سيطرة الدولة على حالة الحماية في الفضاء الإلكتروني والحماية التقنية لموارد معلومات الدولة ومعلوماتها، التي ينص القانون على ضرورة حمايتها
- المشاركة في اجتماعات جهات الاتصال الوطنية باستخدام شبكة الاتصالات التابعة لمنظمة الأمن والتعاون في أوروبا
- التوعية العامة وعقد حلقات دراسية عملية بشأن أمن الفضاء الإلكتروني لفائدة القائمين على تسيير النظام الوطني لأمن الفضاء الإلكتروني
- التفاعل مع وكالات إنفاذ القانون وإتاحة المعلومات في الوقت المناسب عن الهجمات الإلكترونية
- القيام بتنسيق وتنظيم وتنفيذ مراجعة لنظم الاتصالات والنظم التكنولوجية في مرافق البنية التحتية الحيوية، مع مراجعة أمن المعلومات وفقا لمعيار دولة أوكرانيا ISO/IEC 27001: 2015.

ونظرا للتحديات والتهديدات الحالية، يجري إنشاء آليات قانونية في مجال الدفاع الإلكتروني في أوكرانيا بهدف:

- تعزيز أمن الشبكات ونظم المعلومات، الذي ينبغي أن يكون الغرض الرئيسي منه هو الحماية الفعالة للمعلومات والبيانات، وضمان استقرار الشبكات والنظم واستمرارية وظائفها، فضلا عن فعالية الكشف عن الحوادث الإلكترونية ومواجهتها والتقليل إلى أدنى حد من أثرها بعد وقوعها
- تطبيق نظام لإدارة المخاطر
- تهيئة الظروف اللازمة لتوفير الموارد، بما في ذلك الموارد البشرية في مجال أمن الفضاء الإلكتروني
- تعزيز قدرة مرافق البنية التحتية الحيوية على الصمود من الناحيتين التشغيلية والإلكترونية
- إنشاء نظام لحفظ موارد المعلومات الحكومية وضمان حماية المعلومات التكنولوجية، وهو أمر بالغ الأهمية بالنسبة لأداء مرافق البنية التحتية الحيوية لوظائفها
- المشاركة في لجنة المعايير الموحدة من خلال الانضمام إلى الاتفاق ذي الصلة (الاتفاق المتعلق بالاعتراف بشهادات المعايير الموحدة في مجال أمن تكنولوجيا المعلومات)، وهو ما سيضمن إدراج المنتجات المعتمدة في أوكرانيا في السجل الذي تعترف به بلدان الاتحاد الأوروبي والبلدان الرائدة الأخرى في هذا المجال

- ضـــمان الامتثال الصـــارم لرؤســـاء الهيئات التي تدير مرافق البنية التحتية الحيوية للمعلومات لمتطلبات التشـــريعات في مجال حماية موارد المعلومات الحكومية، والحماية الترميزية والتقنية للمعلومات، بما في ذلك حماية البيانات الشخصية
- استغلال الفرص المتاحة للشراكات بين القطاعين العام والخاص وتفاعل أصحاب المصلحة لحل مسائل الدفاع الإلكتروني وأمن الفضاء الإلكتروني
- تعزيز ثقافة السلوك على شبكة الإنترنت
- المشاركة النشطة في المبادرات ذات الصلة للمجتمع الدولي والانضمام إلى الهياكل ذات الصلة للمنظمات الدولية الرائدة.

وفي الفترة بين عامي 2015 و 2020، اتخذ المجلس الوطني للأمن والدفاع في أوكرانيا قرارات سنوية بشأن تطبيق التدابير الشخصية والخاصة و الاقتصادية وغيرها من التدابير التقييدية (الجزاءات)، التي تم تنفيذها بموجب المراسيم ذات الصلة الصادرة عن رئاسة أوكرانيا.

وبالإضافة إلى ما سبق، فإن جهاز الأمن في أوكرانيا، باعتباره أحد الكيانات الرئيسية المسؤولة عن أمن الفضاء الإلكتروني، وفقا لاختصاصه كما هو محدد في القانون، يتخذ تدابير لتحسين الإطار التنظيمي الداخلي بشأن الفضاء الإلكتروني. وعلى وجه الخصوص، يجري العمل بانتظام على تحديد الأنظمة اللازمة لتنفيذ القانون المتعلق بالمبادئ الأساسية للحفاظ على أمن الفضاء الإلكتروني في أوكرانيا.

ويجري اتخاذ تدابير لتطبيق أحكام القانون المتعلق بالمبادئ الأساسية للحفاظ على أمن الفضاء الإلكتروني في أوكرانيا على الإطار التنظيمي الذي يسري على أنشطة جهاز الأمن في أوكرانيا.

غير أنه على الرغم من هذه التدابير، لا تزال مسألة تحسين الإطار التنظيمي في مجال المعلومات وأمن الفضاء الإلكتروني ذات أهمية حتى اليوم.

وعلى وجه الخصوص، لم ينظر البرلمانيون الأوكرانيون بعد في عدد من المبادرات التشريعية المتعلقة بجهاز الأمن، التي كانت قيد نظر لجان البرلمان الأوكراني في الدورة التشريعية السابقة (تعزيز المسؤولية الجنائية عن الجريمة الإلكترونية، وتقسيم صلاحيات التحقيق بين جهاز الأمن والشرطة الوطنية، وتحديد المسؤولية عن عدم الامتثال).

ولم تنفذ أحكام الاتفاقية المتعلقة بالجريمة الإلكترونية تنفيذا كاملا.

وصدق البرلمان الأوكراني في أيلول/سبتمبر 2005 على اتفاقية مجلس أوروبا بشأن الجريمة الإلكترونية المؤرخة 23 تشرين الثاني/نوفمبر 2001. وتشمل أحكام الاتفاقية المسؤولية الجنائية عن الجرائم التي تمس سرية البيانات والنظم الحاسوبية وسلامتها وتوافرها، وهي: الوصول غير المشروع إليها؛ والاعتراض غير القانوني؛ والتدخل في البيانات؛ والتدخل في النظم؛ وإساءة استخدام الأجهزة. أي أن تلك الأحكام من الاتفاقية تشمل الجرائم المرتكبة ضد التشغيل المستدام للبنية التحتية الحيوية.

غير أن عددا من أحكام الاتفاقية المتعلقة بالجريمة الإلكترونية لا يجري حاليا تنفيذها في التشريعات الوطنية، التي تحصر أنشطة أجهزة إنفاذ القانون في الكشف عن الجريمة الإلكترونية ومنعها. وعلى وجه الخصوص، تتعلق أحكام الاتفاقية المتعلقة بالجريمة الإلكترونية التي يلزم تنفيذها بالحفظ المعجل

للبيانات الحاسوبية المخزنة، والحفظ المعجل للبيانات المتعلقة بحركة الاتصالات والكشف عنها جزئيا، وإجراءات أمر تقديم بيانات حاسوبية مخزنة، والبحث عنها ومصادرتها، وجمع البيانات المتعلقة بحركة الاتصالات في الوقت الحقيقي (المواد 16-20). ومن الضروري أيضا إدخال تعديلات على قانون الإجراءات الجنائية في أوكرانيا لإدخال فئة مستقلة من الأدلة، هي الأدلة الرقمية، في الإجراءات الجنائية.

وفي الوقت الراهن، يعمل ممثلو جهاز الأمن في أوكرانيا في الفريق العامل التابع للجنة إنفاذ القانون في البرلمان الأوكراني على إعداد مشروع قانون أوكرانيا بشأن إدخال تعديلات على بعض القوانين التشريعية المتصلة بتنفيذ الاتفاقية المتعلقة بالجريمة الإلكترونية من أجل توحيد أحكام الاتفاقية في التشريعات الأوكرانية، وتحسين أحكام قانون الإجراءات الجنائية في أوكرانيا، وإنشاء آلية قانونية فعالة لمكافحة الجريمة الإلكترونية، بما في ذلك:

- منح رؤساء وحدة العمليات والمحقق والمدعي العام سلطة إعطاء تعليمات إلزامية لمالكي البيانات الحاسوبية (مشغلو الاتصالات السلكية واللاسلكية ومقدمو خدماتها والكيانات القانونية الأخرى والأفراد) من أجل التعجيل بحفظ البيانات الحاسوبية المطلوبة لاكتشاف مرتكبي الجريمة، لمدة تصل إلى 90 يوماً
- تحديد شروط كشف مشغلي ومقدمي الاتصالات السلكية واللاسكية، بناء على طلب وكالات إنفاذ القانون، عن المعلومات الضرورية لتحديد هوية مقدمي الخدمات والطريقة التي تم من خلالها إرسال المعلومات
- استحداث آلية فعالة لاستخدام الأدلة في شكل إلكتروني (رقمي) في الإجراءات الجنائية
- إدخال تعديلات على قانون الإجراءات الجنائية في أوكرانيا وقانون الاتصالات السلكية واللاسلكية ومشروع القانون المتعلق بالاتصالات الإلكترونية من أجل ضمان إنشاء آلية قانونية للتقييد المؤقت للوصول إلى المعلومات أو البيانات الحاسوبية المنشورة على مورد (خدمة) معين (محدد) للمعلومات وتحديد إجراءات تنفيذها.

وفي 4 شباط/فبراير 2020، سحب برلمان أوكرانيا مشروع القانون المتعلق بالاتصالات الإلكترونية (النظام رقم 2264)، الذي قدم جهاز الأمن في أوكرانيا بشأنه تعليقات ومقترحات من خلال لجنة برلمان أوكرانيا المعنية بالتحول الرقمي في نهاية عام 2019.

وفي 5 شباط/فبراير 2020، سُجل مشروع قانون يحمل نفس العنوان (بشأن الاتصالات الإلكترونية) وفريق صياغة مماثل تقريباً في برلمان أوكرانيا تحت الرقم 3014. ووفقا لتحليل أولي، لا يتضمن مشروع القانون الجديد أيضا أحكاما من شأنها أن تيسر التنفيذ الكامل لأحكام الاتفاقية المتعلقة بالجريمة الإلكترونية.

ولمعالجة المسائل الراهنة في مجال أمن الفضاء الإلكتروني في عام 2020، أيد جهاز الأمن في أوكرانيا اتخاذ مبادرة تشريعية للنظر في عدد من مشاريع القوانين من قبل برلمان أوكرانيا في الدورة التاسعة. ومن شأن اعتماد مشاريع القوانين أن يؤدي إلى إنشاء أساس قانوني لجهاز الأمن وفقا للقانون المتعلق بالمبادئ الأساسية للحفاظ على أمن الفضاء الإلكتروني في أوكرانيا.

وهناك، على وجه الخصوص، تمييز تشريعي بين محققي الشرطة الوطنية والسلطات الأمنية فيما يتعلق بالتحقيق في الجرائم المرتكبة باستخدام الحواسيب والنظم وشبكات الحواسيب وشبكات الاتصالات السلكية واللاسلكية، وموارد المعلومات الحكومية، والبنية التحتية الحيوية للمعلومات، فضلا عن تشديد العقوبات على ارتكاب هذه الجرائم.

ويتطلب تنفيذ المهام المتعلقة بمنع الجرائم المخلة بالسلم وأمن البشرية التي ترتكب في الفضاء الإلكتروني، والكشف عنها، ووقفها وإماطة اللثام عنها، وتنفيذ تدابير مكافحة التجسس والتحقيق الرامية إلى مكافحة الإرهاب الإلكتروني والتجسس الإلكتروني، إدخال تعديلات على قانون مكافحة التجسس لاستكمال مهام وصلاحيات الهيئات والتقسيمات الفرعية والموظفين التابعين لجهاز الأمن في أوكرانيا.

وبالإضافة إلى ذلك، لم تُوضع المبادئ والمبادئ التوجيهية لبناء نظام الدولة لحماية البنية التحتية الحيوية على المستوى التشريعي، ولم يتم بعد تحديد البنية التحتية الحيوية للدولة على مستوى اللوائح (لم يتم بعد وضع قائمة بمكونات البنية التحتية الحيوية وقائمة بمكونات البنية التحتية الحيوية للمعلومات).

وفي عام 2019، وافقت الحكومة على المتطلبات العامة للحماية الإلكترونية لمرافق البنية التحتية الحيوية (القرار رقم 518 لمجلس وزراء أوكرانيا الصادر في 19 حزيران/يونيه 2019). وهذا القانون غير صالح في غياب قائمة الدولة للبنية التحتية الحيوية وقائمة البنية التحتية الحيوية للمعلومات، التي ينص على وجودهما القانون المتعلق بالمبادئ الأساسية للحفاظ على أمن الفضاء الإلكتروني في أوكرانيا.

ويعقد عدم اليقين بشأن البنية التحتية الحيوية للدولة تنفيذ مهام أمن الفضاء الإلكتروني الموكلة إلى جهاز الأمن في أوكرانيا وغيره من الجهات الفاعلة في مجال أمن الفضاء الإلكتروني.

وأكدت لجنة البرلمان الأوكراني المعنية بالتحول الرقمي على ضرورة ضمان وضع واعتماد القانون المتعلق بالبنية التحتية الحيوية وحمايتها، فضلا عن التعجيل باعتماد قوانين مجلس الوزراء الأوكراني الرامية إلى تنفيذ أحكام القانون المتعلق بالمبادئ الأساسية للحفاظ على أمن الفضاء الإلكتروني في أوكرانيا، وذلك في اجتماع عُقد بشأن أمن الفضاء الإلكتروني والدفاع الإلكتروني على الصعيد الوطني الأوكراني، بما في ذلك في مجال البنية التحتية الحيوية، في 23 كانون الأول/ديسمبر 2019.

وقد تم النظر في مسألة التطبيق العملي للقانون المتعلق بالمبادئ الأساسية للحفاظ على أمن الفضاء الإلكتروني في أوكرانيا واعتماد الأنظمة اللازمة لتنفيذه بشكل منفصل في اجتماع للجنة البرلمان الأوكراني المعنية بالتحول الرقمي عُقد في 19 شباط/فبراير 2020.

وتظل مشكلة غياب أنظمة للحد من الاعتماد الشديد للمؤسسات والمنظمات والشركات المحلية على البرامجيات ذات المنشأ الأجنبي، التي قد تتضمن مكامن ضعف مُضمَّنة عن قصد ووظائف غير موثقة، قائمة.

ووفقاً لما ذكره خبراء جهاز الأمن في أوكرانيا، يتطلب ذلك وضع برنامج وطني لإحلال الواردات في مجال المعلوماتية، ومجموعة من التدابير لدعم منتجي البرامجيات المحليين، وإنشاء:

- سجل لموردي البرامجيات الذين تم التحقق منهم من أجل مرافق البنية التحتية الحيوية للمعلومات، وإعداد إجراء إدراجهم في السجل المحدد أو استبعادهم منه

- سجل للبرامجيات المشمولة بحقوق الملكية الموصى باستخدامها في مرافق البنية التحتية الحيوية للمعلومات
- مستودع وطني للبرامجيات المفتوحة المصدر وتعزيز تنفيذ برامج الدولة من أجل النقل إلى السلطات العامة وإدارة استخدامه.

وعلاوة على ذلك، ومن أجل وضع إجراء تشريعي للتصدي الفوري والفعال للتهديدات القائمة والمحتملة للمصالح الوطنية لأوكرانيا وأمنها في ميدان تكنولوجيا المعلومات والاتصالات، يلزم إدخال تعديلات مناسبة على قانون الجزاءات: فرض قيود على استخدام البنية التحتية الحيوية لجميع أشكال ملكية البرامجيات (بما في ذلك برامج مكافحة الفيروسات) ومعدات الاتصالات السلكية واللاسلكية التي طورتها أو صنعتها كيانات اقتصادية في البلد المعتدي.

وثمة عامل إضافي له أثر سلبي هو الفجوة في التشريعات الداخلية من حيث عدم وجود آلية محددة قانوناً لمنع وصول مستخدم معين إلى موارد الإنترنت وإزالة الرسائل التي تحتوي على معلومات تم الحصول عليها بصورة غير قانونية.

وتجدر الإشارة أيضا إلى أن جهاز الأمن في أوكرانيا ينفذ تدابير التعاون الدولي في مجال تعزيز المعلومات وأمن الفضاء الإلكتروني. والأولويات والمجالات الرئيسية، وفقا لاستراتيجية أوكرانيا لأمن الفضاء الإلكتروني، هي:

- تطوير التعاون الدولي في مجال أمن الفضاء الإلكتروني
- دعم المبادرات الدولية في مجال أمن الفضاء الإلكتروني التي تحقق المصالح الوطنية لأوكرانيا
- تعميق تعاون أوكرانيا مع الاتحاد الأوروبي ومنظمة حلف شمال الأطلسي (الناتو) لتعزيز قدرات أوكرانيا في مجال أمن الفضاء الإلكتروني
- المشاركة في تدابير بناء الثقة في الفضاء الإلكتروني تحت رعاية منظمة الأمن والتعاون في أوروبا.

وعلى وجه الخصوص، يشارك جهاز الأمن في أوكرانيا، في نطاق مجالات اختصاصه، في أنشطة شبكة "سايبر إيست"، وهي مشروع مشترك بين الاتحاد الأوروبي ومجلس أوروبا من أجل بلدان برنامج الشراكة الشرقية، يهدف إلى تنفيذ القرارات التشريعية والسياساتية لتطبيق أحكام اتفاقية بودابست المتعلقة بالجريمة الإلكترونية. وتنفذ مشروع "سايبر إيست" المديرية العامة للاتحاد الأوروبي لمفاوضات الجوار والتوسع بالتعاون مع مكتب البرنامج المتعلق بالجريمة الإلكترونية التابع لمجلس أوروبا.

وإذ يشدد ممثلو جهاز الأمن في أوكرانيا على أهمية إطلاع الشركاء الدوليين على آخر إنجازات أوكرانيا في مجال أمن الفضاء الإلكتروني، فضلا عن تنفيذ بعض تدابير بناء الثقة وفقا لقرارات المجلس الدائم لمنظمة الأمن والتعاون في أوروبا رقم 1039 و 1106 و 1202 في مجال تكنولوجيا المعلومات والاتصالات واستخدامها، فهم يشاركون عادة في اجتماعات الفريق العامل غير الرسمي المعني بتكنولوجيا المعلومات والاتصالات التابع لمنظمة الأمن والتعاون في أوروبا. وبالإضافة إلى ذلك، حدد جهاز الأمن في أوكرانيا جهة اتصال في إطار تدبير بناء الثقة رقم 8 الوارد في القرار 1202، تقوم على المستوى المهني بأنشطة كجزء من عمليات التحقق من الاتصالات المقررة وغير المجدولة.

ويشـــارك جهاز الأمن في أوكرانيا أيضـــا في مشـــروع لمنظمة الأمن والتعاون في أوروبا، الغرض الرئيسي منه هو إجراء تحليل مفصل لهيكل الحوكمة الوطنية في مجال أمن الفضاء الإلكتروني، فضلا عن تنفيذ تدابير أوكرانيا لبناء الثقة في مجال تكنولوجيا المعلومات والاتصـــالات وأمن الفضـــاء الإلكتروني، على النحو المنصوص عليه في القرار 1202.

وعلاوة على ذلك، ووفقا للمهام الموكلة إلى جهاز الأمن في أوكرانيا، وبدعم من الصـــــندوق الاستئماني المشترك بين أوكرانيا والناتو من أجل أمن الفضاء الإلكتروني، تم الحصول على المعدات اللازمة وتم إنشاء مركز العمليات المتعلقة بأمن الفضاء الإلكتروني التابع لجهاز الأمن في أوكرانيا، بهدف:

منع الجرائم المخلة بسلم البشرية وأمنها المرتكبة في الفضاء الإلكتروني وكشفها وقمعها

- اتخاذ تدابير مكافحة التجسس والتحقيق الرامية إلى مكافحة الإرهاب الإلكتروني والتجسس الإلكتروني
- التحقق من مدى جاهزية مرافق البنية التحتية الحيوية لمواجهة الهجمات والحوادث الإلكترونية المحتملة الوقوع
- مكافحة الجريمة الإلكترونية، التي قد تهدد عواقبها المصالح الحيوية للدولة
- التحقيق في الحوادث والهجمات الإلكترونية على موارد المعلومات الإلكترونية الحكومية والبنية التحتية الحيوية للمعلومات
- ضمان مواجهة الحوادث الإلكترونية في مجال أمن الدولة.

وبدأ جهاز الأمن في أوكرانيا أيضـــا التعاون بشـــأن تبادل المعلومات عن التهديدات والهجمات والحوادث الإلكترونية باســـتخدام منصـــة تبادل المعلومات عن البرامجيات الخبيثة وتبادل المعلومات عن التهديدات – الميزة الأوكرانية، وهي منصـــة عامة للتعاون بين جهاز الأمن في أوكرانيا ومرافق البنية التحتية الحيوية، وغيرها من الشركات والمؤسسات والمنظمات، بغض النظر عن الملكية، وكذلك الأفراد في مسائل تحسين أمن مستخدمي المعلومات، والاتصالات السلكية واللاسلكية ونظم المعلومات والاتصالات السلكية واللاسلكية التي يخول لهم توفير الحماية لها بموجب الاتفاقات ذات الصلة أو غيرها من الأسباب القانونية.

الإمارات العربية المتحدة

[الأصل: بالعربية]
[31 أيار/مايو 2020]

التقرير الوطني حول الجهود التي تبذلها دولة الإمارات العربية المتحدة لتعزيز أمن المعلومات وتعزيز التعاون الدولي في ميدان الأمن السيبراني

المقدمة: تولي دولة الإمارات العربية المتحدة اهتماماً كبيراً بالأمن الســـيبراني، كونه إحدى الركائز الأساسية لحفظ الأمن الوطني للدولة من الهجمات التي تستغل تكنولوجيا الاتصالات والمعلومات في تشكيل تهديد حقيقي للبُنى التحتية والخدمات الحكومية والأفراد. ومن أجل ذلك، ســـعت دولة الإمارات إلى خلق منظومة متكاملة تضمن تأمين القطاعات الحيوية وتعزز الثقة لدى المستخدمين وتحفز الابتكار.

الجهود المبذولة على الصعيد الوطني لتعزيز الأمن السيبراني

أطلقت الدولة الاستراتيجية الوطنية للأمن السيبراني، والتي تهدف إلى خلق بيئة سيبرانية آمنة ومرنة تمكّن الأفراد من تحقيق طموحاتهم وتمكّن الشركات من التطور. وتعتمد الاستراتيجية في تحقيق أهدافها على خمسة محاور رئيسية تتمثل فيما يلي:

1 - تنفيذ إطار قانوني وتنظيمي شامل لمعالجة الجرائم السيبرانية، وحماية التقنيات الحالية والناشئة، وتمكين الشركات الصغيرة والمتوسطة وحمايتها من التهديدات السيبرانية؛

2 - تطوير برنامج متكامل لنشر الوعي وبناء القدرات في الأمن السيبراني، لتشجيع اتباع الممارسات الآمنة في استخدام التكنولوجيا، وتطوير مهارات العاملين في مجال الأمن السيبراني للتصدي للهجمات بفاعلية وتأمين الأنظمة والخدمات؛

3 - وضع خطة وطنية فعالة للاستجابة للحوادث السيبرانية لتمكين الاستجابة السريعة والمنسقة في الدولة؛

4 - حماية البنى التحتية الرقمية للقطاعات الحيوية؛

5 - تعزيز الشراكات المحلية والعالمية في مجال الأمن السيبراني.

كما أطلقت دولة الإمارات قانون مكافحة جرائم تقنية المعلومات في عام 2006، الذي يحتوي على العديد من المواد التي من شأنها توفير الحماية القانونية لخصوصية ما يتم نشره وتداوله على وسائل تكنولوجيا الاتصالات والمعلومات، ومعاقبة من يقوم بإساءة استغلالها.

وبالإضافة إلى ذلك، فقد أطلقت دولة الإمارات العديد من البرامج والمبادرات على مدى السنوات لتعزيز الأمن السيبراني، ومن ذلك إنشاء الفريق الوطني للاستجابة لطوارئ الحاسب الآلي aeCERT الذي يقدم مجموعة من الخدمات للجهات الحكومية، تتضمن مراقبة البنية التحتية وفحصها المستمر للتعرف على أي عمليات غير طبيعية أو هجمات والتصدي لها مباشرة، والاستجابة للحوادث السيبرانية بشكل فعال، إضافة إلى فحص المواقع الإلكترونية وتطبيقات الهاتف وتقييمها من حيث الأمان لإغلاق أي ثغرة قد تؤدي إلى اختراقها أو تسريب المعلومات منها، كما ينشر تحذيرات وتقارير أمنية بشكل مستمر للجهات الحكومية والأفراد حول أبرز الهجمات السيبرانية، وذلك عبر عدة منصات منها الموقع الإلكتروني ووسائل التواصل الاجتماعي والقائمة البريدية.

ولضمان تطبيق أفضل ممارسات الأمن السيبراني في القطاعات الحيوية بالدولة، تم إطلاق نظام ضمان أمن المعلومات في دولة الإمارات، ليكون مرجعية لمتطلبات رفع الحد الأدنى من مستوى حماية أصول أمن المعلومات، وأنظمة الدعم.

وإلى جانب السياسات والنُظُم التقنية، كان لا بد من تكثيف الجهود في تطوير الكادر البشري، ليكون واعياً بسبل الاستخدام الآمن والإيجابي لتكنولوجيا الاتصالات والمعلومات ويصبح خط الدفاع الأول لدولته وأسرته ضد المخاطر والهجمات السيبرانية. ولأجل ذلك، أطلقت دولة الإمارات البرنامج الوطني للتوعية وبناء القدرات في الأمن السيبراني، بهدف خلق ثقافة آمنة في المجتمع، وتطوير كفاءات وطنية متميزة في الأمن السيبراني، فتم إطلاق مبادرة "سايبر برو" التي تعمل على تدريب المتخصصين في مجال الأمن السيبراني عبر دورات شهرية، كما تم إنشاء أكاديمية افتراضية تتضمن دورات في الأمن السيبراني. وبالإضافة إلى ذلك، يتم إطلاق حملات وفعاليات توعوية لمختلف شرائح المجتمع بشكل دوري.

أما فيما يتعلق بحماية الأطفال أثناء استخدامهم للتكنولوجيا، فقد تم إطلاق الشخصية الكرتونية "سالم"، والتي كان لها أثر كبير في إيصال مبادئ الاستخدام الآمن للأطفال بسهولة ويسر، وذلك عبر إنشاء منهج السلامة الرقمية بالتعاون مع وزارة التربية والتعليم، وإطلاق موقع سالم الإلكتروني، إضافة إلى آلاف الورش التفاعلية للأطفال لإيصال المعلومات لهم عبر قصص هم أبطالها. كما تم تتويج هذه المبادرات بإشراك الأطفال في التوعية عبر مبادرة سفراء الأمن الإلكتروني، التي تعمل على تهيئة الأطفال ليقوموا بتوعية أقرانهم ويروجوا للأساليب الآمنة والصحيحة.

الجهود المبذولة لتعزيز التعاون الدولي في مجال الأمن السيبراني

تدرك دولة الإمارات العربية المتحدة أن التطبيق الأمثل للأمن السيبراني والتصدي للهجمات والمخاطر يتطلب تعاوناً دولياً ووقفة جادة. وإيماناً بذلك، تسعى دولة الإمارات للمشاركة بشكل فاعل في كافة المحافل الدولية التي تعمل على تطوير الأمن السيبراني على المستوى الدولي، والتي نستعرض بعضها أدناه.

تشارك دولة الإمارات في الاتحاد الدولي للاتصالات، وتعمل بالتعاون مع الدول الأعضاء على وضع الحلول وتحديد الممارسات المثلى في الأمن السيبراني عبر اللجان الدراسية ومجموعات العمل المعنية. كما تسعد الدولة بتولّي بعض المتخصصين من مواطنيها مناصب مهمة في الاتحاد كرئيس الفريق العامل المعني بحماية الطفل على شبكة الإنترنت، والتي تبيّن التزام الدولة في دعم الجهود العالمية في هذه المواضيع الهامة.

كما أن دولة الإمارات، ممثَّلةً بفريق الاستجابة لطوارئ الحاسب الآلي aeCERT، هي عضو في مجلس إدارة الجمعية العمومية لفرق الاستجابة للطوارئ الحاسوبية بمنظمة التعاون الإسلامي OIC-CERT، حيث تتولى إدارة محور التوعية السيبرانية عبر وضع البرامج والأدلة الإرشادية والمواد اللازمة لنشر الوعي حول المخاطر الأمنية التي تمس المؤسسات والأفراد. إضافة إلى أن فريق aeCERT يشارك بفاعلية في المركز العربي الإقليمي للأمن السيبراني ARCC، ولجنة المراكز الوطنية للاستجابة لطوارئ الحاسبات بدول مجلس التعاون لدول الخليج العربية GCC-CERT.

وبالإضافة إلى المحافل والمنظمات الدولية، تحرص دولة الإمارات على تعزيز التعاون الثنائي مع الدول الصديقة في مجال الأمن السيبراني، وذلك عبر توقيع مذكرات تفاهم واتفاقيات بهدف تنظيم تبادل المعلومات والخبرات بين الدول والتعاون في التصدي للهجمات السيبرانية.

آراء حول مضمون المفاهيم المشار إليها في تقارير فريق الخبراء الحكوميين

تعرب دولة الإمارات العربية المتحدة عن شكرها لفريق الخبراء الحكوميين على الجهود التي بُذِلت في إعداد التقارير المعنية بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي. كما تؤيد دولة الإمارات ما خلص إليه الفريق في تقريره من أهمية بذل الدول للجهود اللازمة لمنع الممارسات الضارة في مجال تكنولوجيا المعلومات والاتصالات والتعاون في التصدي للهجمات السيبرانية، ودعم الحوار المبني على الشفافية والعمل المشترك، وتوفير الدعم لتطوير البنى التحتية الرقمية عالمياً وبذل المشورة لتطوير التشريعات والاستراتيجيات والنظم في الأمن السيبراني.

ثالثا - الردود الواردة من المنظمات الحكومية الدولية

الاتحاد الأوروبي

[الأصل: بالإنكليزية]
[20 أيار/مايو 2020]

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 وجود فضاء إلكتروني عالمي مفتوح ومستقر وسلمي وآمن تنطبق فيه حقوق الإنسان والحريات الأساسية وسيادة القانون بشكل كامل، بهدف تحقيق الرفاه الاجتماعي، والنمو الاقتصادي، والازدهار، وسلامة المجتمعات الحرة والديمقراطية.

ومع تزايد ترسخ استخدام الإنترنت في حياتنا، ينشأ في الفضاء الإلكتروني عدد من المسائل نفسها التي نواجهها في العالم المادي. وفي السياق الدولي، يبدو أن بعض الدول قد اعتمدت رؤية للفضاء الإلكتروني تنطوي على درجة عالية من الرقابة الحكومية، مما يثير شواغل بشأن انتهاكات حقوق الإنسان والحريات الأساسية. كما حدثت زيادة مثيرة للقلق في الأنشطة الإلكترونية الخبيثة التي تقوم بها جهات فاعلة حكومية وغير حكومية. 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.

(أ) 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 القدرة على الصمود في الفضاء الإلكتروني 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. وتحد القدرة على الصمود في الفضاء الإلكتروني على الصعيد العالمي من قدرة المخالفين المحتملين على إساءة استخدام تكنولوجيا المعلومات والاتصالات لأغراض خبيثة، وتعزز قدرة الدول على التصدي بفعالية للحوادث الإلكترونية والتعافي من آثارها.

وتمثل استراتيجية أمن الفضاء الإلكتروني "فضاء إلكتروني مفتوح وسالم وآمن"[(12)]، فضلا عن وثائق السياسات اللاحقة الأخرى 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

(12) 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".

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[13] 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 مجال 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"[14] 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 تحديات أمن الفضاء الإلكتروني المتزايدة باستمرار زخماً لوضع إطار لتصد دبلوماسي مشترك للاتحاد الأوروبي للأنشطة الإلكترونية الخبيثة، وهو مجموعة أدوات الدبلوماسية في الفضاء الإلكتروني[15]. 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 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.

(13) 15/6122 استنتاجات المجلس بشأن الدبلوماسية في الفضاء الإلكتروني.

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

(15) 17/10474. استنتاجات المجلس بشأن إطار لتصد دبلوماسي مشترك للاتحاد الأوروبي للأنشطة الإلكترونية الخبيثة ("مجموعة أدوات الدبلوماسية في الفضاء الإلكتروني").

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.

وتعزز سياسة الاتحاد الأوروبي الدولية بشأن الفضاء الإلكتروني احترام القيم الأساسية للاتحاد الأوروبي، وتحدد معايير للسلوك المسؤول، وتدعو إلى تطبيق القوانين الدولية القائمة في الفضاء الإلكتروني، مع مساعدة البلدان خارج الاتحاد الأوروبي في بناء القدرات في مجال أمن الفضاء الإلكتروني، وتعزيز التعاون الدولي بشأن القضايا المتعلقة بالفضاء الإلكتروني.

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

الأخطار 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 تكنولوجيا 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.

وفي الآونة الأخيرة، 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. ويدين الاتحاد الأوروبي والدول الأعضاء فيه هذا السلوك الخبيث في الفضاء الإلكتروني وتشدد على دعمها المستمر لزيادة القدرة العالمية على الصمود في هذا الفضاء.

وأي محاولة لإعاقة قدرة البنى التحتية الحيوية غير مقبولة ويمكن أن تعرض حياة الناس للخطر. 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، 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 والمبادئ وحقوق الإنسان المستمدة منه.

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. وبالإضافة إلى ذلك، يكرر 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.

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 أوقات النزاع. ويؤكد الاتحاد الأوروبي اقتناعه بأن القانون الدولي ليس من العوامل التي تمكن من القيام بسلوك معين؛ 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[16] 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.

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

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 أنه سيسهم في صون السلام ومنع نشوب النزاعات وضمان الاستقرار العالمي.

ونواصل دعم الجهود الجارية الرامية إلى تعزيز تطبيق القانون الدولي القائم على الفضاء الإلكتروني، بما في ذلك تبادل المعلومات وأفضل الممارسات بشأن تطبيق القانون الدولي القائم في الفضاء الإلكتروني. ونحن ملتزمون بمواصلة الإبلاغ عن المواقف الوطنية بشأن كيفية انطباق القانون الدولي على استخدام الدول لتكنولوجيا المعلومات والاتصالات، حيث أنه يعزز الشفافية ويقوي التفاهم العالمي بشأن النهج 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 بانطباق القانون الدولي القائم كوسيلة لتعزيز الاستقرار ومنع نشوب النزاعات في الفضاء الإلكتروني.

معايير سلوك الدول المسؤول وقواعده ومبادؤه

يشجع الاتحاد الأوروبي والدول الأعضاء فيه جميع الدول على الاستفادة من العمل الذي أقرته الجمعية العامة مرارا، ولا سيما في القرار 273/70، والنهوض به، وعلى مواصلة تنفيذ هذه المعايير وتدابير بناء الثقة المتفق عليها، التي تؤدي دورا أساسيا في منع نشوب النزاعات.

وسيسترشد الاتحاد الأوروبي والدول الأعضاء فيه في استخدامها لتكنولوجيا 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 في أعوام 2010 و 2013 و 2015. ونعتقد أن الطريق العملي للمضي قدما ينبغي أن يشجع على زيادة التعاون والشفافية لتبادل 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 بناء آليات فعالة للتعاون والتفاعل بين الدول في الفضاء الإلكتروني عنصر حاسم 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، و المنتدى 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 نشـــوب النزاعات والحد من التوترات الناجمة عن إســـاءة اســـتخدام تكنولوجيات المعلومات والاتصـالات، يهدف الاتحاد الأوروبي والدول الأعضـاء فيه إلى تعزيز القدرة على الصـمود على الصـعيد العالمي، مع التركيز بوجه خاص على البلدان النامية، كوسـيلة للتصـدي للتحديات المرتبطة برقمنة الاقتصـــادات والمجتمعات، وكذلك الحد من قدرة المخالفين المحتملين على إســـاءة اســـتخدام تكنولوجيات المعلومات والاتصـــالات لأغراض خبيثة. وتعزز القدرة على الصـــمود قدرة الدول على التصـــدي بفعالية للتهديدات الإلكترونية والتعافي من آثارها.

ويدعم الاتحاد الأوروبي والدول الأعضـاء فيه مجموعة من البرامج والمبادرات المصـممة خصـيصـا لمســـاعدة البلدان في تطوير مهاراتها وقدراتها لمواجهة الحوادث الإلكترونية، فضـــلا عن المبادرات الرامية إلى تيسير تبادل أفضل الممارسات، سواء من خلال المشاركة المباشرة أو الاتصالات الثنائية أو المشاركة من خلال المؤسسات الإقليمية والمتعددة الأطراف.

ويقر الاتحاد الأوروبي والدول الأعضـــاء فيه بأن تعزيز قدرات الحماية المناســـبة وزيادة مأمونية المنتجات والعمليات والخدمات الرقمية سـيسـهمان في زيادة أمن الفضـاء الإلكتروني وجدارته بالثقة. ونسـلم بمسـؤولية جميع الجهات الفاعلة ذات الصـلة عن المشـاركة في تنمية القدرات في هذا الصـدد، وندعو كذلك إلى تعزيز التعاون مع الشركاء والمنظمات الدوليين الرئيسيين لدعم بناء القدرات في بلدان ثالثة.