الأمم المتحدة

A/79/81

الجمعية العامة

Distr.: General
21 May 2024
Arabic
Original: Chinese/English/French/
Russian/Spanish

الدورة التاسعة والسبعون

البند 93 من القائمة الأولية*

التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي

التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي

تقرير الأمين العام

موجز

يتضمّن هذا التقرير موجزا جامعا للعناصر المقدّمة في الردود الواردة من الدول الأعضاء عملا بقرار الجمعية العامة 237/78، دون المساس بالمواقف الفردية لتلك الدول. والتقرير تجميعٌ لآراء الدول بشأن أمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها، ولا سيما بشأن الجولة المقبلة من الحوار المؤسسي المنتظم بشأن هذه المسائل تحت رعاية الأمم المتحدة. والآراء الواردة من الدول الأعضاء قبل انقضاء المهلة المحددة مُدرجة بالكامل في مرفق هذا التقرير. وينتهي التقرير بملاحظات الأمين العام.

280624 120624 24-08163 (A)

المحتويات

الصفحة

أولا - مقدمة

1 - دعت الجمعية العامة جميع الدول الأعضاء، في الفقرة 8 من القرار 237/78، إلى مواصلة إعلام الأمين العام بآرائها وتقييماتها بشأن أمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها، ولا سيما بشأن الجولة المقبلة للحوار المؤسسي المنتظم حول هذه المسائل المتوخى أن تُعقد برعاية الأمم المتحدة، وطلبت إلى الأمين العام أن يحيل إلى الجمعية العامة في دورتها الثامنة والسبعين تقريرا يعده بناء على تلك الآراء لمواصلة المناقشات بين الدول الأعضاء في هذا الصدد خلال اجتماعات الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025 في دورته الثامنة المقرر عقدها في عام 2024. ويُقدَّم هذا التقرير تلبيةً لذلك الطلب.

2 - ففي 5 كانون الثاني/يناير 2024، عمم مكتب شؤون نزع السلاح مذكرة شفوية على جميع الدول الأعضاء يوجّه انتباهها إلى الفقرة 8 من القرار، ويلتمس آراءها في الأمر. وترد في مرفق هذا التقرير الآراء الواردة بحلول 1 أيار/مايو 2024. وأما الآراء الواردة بعد هذا التاريخ فقد نُشرت على الموقع الشبكي لمكتب شؤون نزع السلاح "Meetings Place"[(1)].

3 - ويرد في الفرع الثاني من هذا التقرير معلومات أساسية تتعلق بمناقشات الدول عن مسألة الحوار المؤسسي المنتظم بشأن أمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها. ويتضمّن الفرع الثالث موجزا جامعا للعناصر الواردة من الدول الأعضاء، دون المساس بالمواقف الفردية لتلك الدول. أما الفرع الرابع، فيعرض ملاحظات الأمين العام واستنتاجاته.

ثانيا - معلومات أساسية

4 - تحت رعاية الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025، تواصل الدول، وفقا لجدول أعمال الفريق المتفق عليه والوارد في الوثيقة A/AC.292/2021/1، مناقشة مسألة إقامة حوار مؤسسي منتظم، تحت رعاية الأمم المتحدة، بشأن المسائل ذات الصلة بمشاركة واسعة من الدول. وعلى مدار سبع دورات موضوعية للفريق العامل، من كانون الأول/ديسمبر 2021 إلى آذار/مارس 2024، انخرطت الدول في مناقشات مركزة للتعمق في مناقشة المقترحات المتعلقة بالحوار المؤسسي المنتظم، بما في ذلك برنامج عمل مقترح.

5 - واتفقت الدول من حيث المبدأ في التقرير المرحلي السنوي الثاني للفريق العامل، المعتمد بتوافق الآراء في تموز/يوليه 2023، والوارد في الوثيقة A/78/265، على أن تستند أي آلية مقبلة للحوار المؤسسي المنتظم إلى العناصر المشتركة التالية، واتفقت على مواصلة المناقشات بشأن عناصر إضافية:

(أ) ستكون آلية دائمة أحادية المسار تقودها الدول تحت رعاية الأمم المتحدة، وتقدم تقاريرها إلى اللجنة الأولى للجمعية العامة للأمم المتحدة؛

(ب) الهدف من الآلية المقبلة هو مواصلة تعزيز بيئة مفتوحة وآمنة ومستقرة ويمكن الوصول إليها وسلمية وقابلة للتشغيل المتبادل لتكنولوجيا المعلومات والاتصالات؛

(1) https://meetings.unoda.org/ga-c1/general-assembly-first-committee-seventy-ninth-session-2024.

(ج) تتخذ الآلية المقبلة أساسا لعملها الاتفاقات التي تم التوصل إليها بتوافق الآراء بشأن إطار سلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات، في التقارير السابقة للفريق العامل المفتوح العضوية وفريق الخبراء الحكوميين؛

(د) ستكون عملية مفتوحة وشاملة للجميع وشفافة ومستدامة ومرنة يمكن أن تتطور وفقا لاحتياجات الدول وكذلك وفقا لما يحصل من تطورات في بيئة تكنولوجيات المعلومات والاتصالات.

6 - وشددت الدول كذلك على أهمية مبدأ توافق الآراء فيما يتعلق بإنشاء الآلية المقبلة نفسها وكذلك فيما يتعلق بعملية صنع القرار ضمن الآلية. وبالإضافة إلى ذلك، فإن الدول القادرة على إنشاء أو دعم برامج الرعاية وغيرها من الآليات لضمان المشاركة الواسعة في عمليات الأمم المتحدة تُشجَّع على مواصل النظر في القيام بذلك.

7 - وطوال المناقشات التي دارت في الفريق العامل المفتوح العضوية بشأن جولة مقبلة من الحوار المؤسسي المنتظم حول المسائل المتصلة بأمن تكنولوجيات المعلومات والاتصالات، تناولت الدول بالبحث النطاق والأهداف والهيكل والطرائق المحتملة، بما في ذلك فيما يتعلق باتخاذ القرارات ومتابعة التنفيذ. ولتيسير المناقشات، قدم رئيس الفريق العامل المفتوح العضوية في شباط/فبراير 2024 ورقة مناقشة بشأن مشروع عناصر آلية دائمة لأمن تكنولوجيات المعلومات والاتصالات، تلتها في أيار/مايو 2024 صيغة منقحة. وطُلب أيضا في التقرير المرحلي السنوي الثاني عقد اجتماعين فيما بين الدورات يكرَّسان لموضوع الحوار المؤسسي المنتظم. وستنخرط الدول أيضا خلال هاتين الدورتين في مناقشات مركّزة تتناول العلاقة بين برنامج العمل والفريق العامل المفتوح العضوية[2].

ثالثا - وجهات النظر في الحوار المؤسسي المنتظم بشأن أمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها

التفاهمات والمبادئ العامة

8 - شددت دول عديدة في ورقات ردودها على خطر النشاط الخبيث في استخدام تكنولوجيات المعلومات والاتصالات، وأشارت إلى تزايد الشواغل على الصعيد الدولي إزاء ما يمكن أن يتعرض له الأمن والاستقرار الدوليان من تهديدات. وكان ثمة من أعرب عن القلق من إفراط عدد من الدول في تطوير قدرات تكنولوجيا المعلومات والاتصالات لأغراض لا تنسجم مع القانون الدولي ومع أهداف صون الاستقرار والأمن الدوليين. ولوحظ أن بعض الجهات الفاعلة قد انتهكت القانون الدولي عن طريق نشاط تدخل فيه تكنولوجيات المعلومات والاتصالات. وورد الإعراب أيضا عن القلق إزاء تأثير النشاط الخبيث على سلامة الأفراد ورفاههم.

9 - ولاحظت بعض الدول أن تكنولوجيات المعلومات والاتصالات يمكن أن تكون حافزا للتقدم والتنمية البشرية، في حين لوحظ أيضا أنه يمكن استخدامها لأغراض لا تنسجم مع أهداف صون الأمن الدولي وبطريقة تؤثر سلبا على التنمية الاقتصادية والاجتماعية.

10 - وشددت دول كثيرة على أنه من الضروري، في ضوء البيئة الأمنية الراهنة، أن يركز أي حوار مؤسسي منتظم يُجرى في المستقبل بشأن أمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها على

(2) انظر A/78/76.

زيادة تعزيز بيئة لتكنولوجيات المعلومات والاتصالات تكون مفتوحة وآمنة ومستقرة وميسَّرة وسلمية. وشددت بعض الدول أيضا على أهمية التعاون الدولي فيما بين الدول للحفاظ على الاستقرار الدولي في هذا المجال.

11 - ولاحظت دول عديدة أن هناك طلبا متزايدا على إنشاء آلية دائمة لاتخاذ القرارات بشأن المسائل ذات الصلة تحت رعاية الأمم المتحدة. وعلاوة على ذلك، شدد كثير من الدول أيضا على الأهمية المحورية للاستفادة من الاتفاقات التي تم التوصل إليها في العمليات السابقة تحت رعاية الأمم المتحدة، بما في ذلك ضمن أفرقة الخبراء الحكوميين والفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي[3]. وشددت بعض الدول على ضرورة الاستفادة من هذه "المكتسبات الجماعية"، مشيرة إلى أنها تتألف من المعايير القائمة لسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات، وانطباق القانون الدولي على استخدام الدول لهذه التكنولوجيات، وتدابير بناء الثقة، وبناء القدرات. وكان ثمة أيضا من رأى أن أي آلية توضع في المستقبل ينبغي أن تفسح المجال للتعمق أكثر في مناقشة مسألة التنفيذ العملي للاتفاقات التي سبق التوصل إليها. وذهب بعض الرأي أيضا في هذا الصدد إلى أن دليل جهات الاتصال الحكومية الدولية ينبغي أن يكون جزءا لا يتجزأ من أي آلية مقبلة.

12 - وشددت عدة دول على أهمية الاستمرارية من حيث النتائج التي تم التوصل إليها بتوافق الآراء في العمليات السابقة. وعلى نفس المنوال، أشارت عدة دول إلى أنه ينبغي إنشاء الآلية المؤسسية الجديدة أو المنبر المؤسسي الجديد بعد انتهاء ولاية الفريق العامل المفتوح العضوية الحالي المعني بأمن تكنولوجيا المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025. وشددت بعض الدول على ضرورة القيام بذلك في موعد أقصاه عام 2026 لضمان الاستمرارية.

13 - وشددت عدة دول على أهمية تجنب ازدواجية الجهود الدولية في هذا المجال وحذرت من إقامة عمليات موازية، مشيرة إلى التحديات التي تواجهها الوفود في القدرات ذات الصلة. وشددت دول عديدة على أهمية إقامة حوار مؤسسي منتظم أحادي المسار ودائم وشامل تحت رعاية الأمم المتحدة. وأشارت بعض الدول أيضا إلى أن إنشاء آلية وحيدة وشاملة ودائمة من شأنه أن يسهم أيضا في وضوح الرؤية والاستقرار المؤسسي، مع تجنب الحاجة إلى التفاوض بشأن ولايات جديدة على فترات منتظمة. ووردت الإشارة أيضا إلى أن الدول الصغيرة والنامية ذات الموارد المحدودة لن تكون قادرة على المشاركة على نحو مستدام في العمليات المتوازية المزدوجة المسارات. وعلاوة على ذلك، كان ثمة من يرى أن أي آلية مقبلة ينبغي أن تكون بمثابة مركز جامع شامل لمعالجة أمن تكنولوجيات المعلومات والاتصالات.

14 - وأكدت بعض الدول أن القانون الدولي، ولا سيما ميثاق الأمم المتحدة، ينطبق وضروري لصون السلام والأمن والاستقرار في بيئة تكنولوجيات المعلومات والاتصالات. وثمة من رأى في هذا الصدد أنه يمكن التعمق في مناقشة آلية مقبلة بشأن كيفية تطبيق القانون الدولي. واقتُرِحَ إنشاءُ آلية في المستقبل لاستكشاف مسار عمل مكرس لهذا الموضوع. وذهب رأي إلى أن إنشاء آلية في المستقبل يمكن أن يكون بمثابة إطار شامل للمناقشات بشأن القانون الدولي، بما في ذلك لتبادل وجهات النظر الوطنية، وعقد جلسات إحاطة للخبراء، واستكشاف أنشطة بناء القدرات في هذا المجال.

15 - وذكرت الدول عدة مبادئ أساسية ينبغي أن يقوم عليها حوار مؤسسي منتظم في المستقبل بشأن أمن تكنولوجيات المعلومات والاتصالات وأمكن استخدامها، بما في ذلك الانفتاح والشمولية والشفافية،

(3) انظر A/65/201 و A/68/98 و A/70/174 و A/75/816 و A/76/135.

كما قالت إن الحوار ينبغي أن يكون عملي المنحى وأحادي المسار وديمقراطيا. وثمة من ذهب إلى أن الآلية المقبلة ينبغي أن تتولى الدول قيادتها وأن ترتكز على الامتثال لمبادئ ميثاق الأمم المتحدة، مثل المساواة بين الدول في السيادة، وعدم استخدام القوة أو التهديد باستخدامها، والتسوية السلمية للمنازعات. ومن الاقتراحات المعبّر عنها أيضا أن تكون الآلية على قدر كاف من المرونة والقدرة على التطور لمسايرة الاحتياجات المتغيرة للدول وظهور مهام جديدة في ميدان ضمان الأمن في استخدام تكنولوجيات المعلومات والاتصالات.

16 - وأشارت عدة دول إلى الاقتراح الداعي إلى وضع برنامج عمل للارتقاء بسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي. ولوحظ أن هذا الاقتراح روعي في التقارير السابقة لهيئات الأمم المتحدة ذات الصلة، بما في ذلك في التقارير السنوية الصادرة بتوافق الآراء عن الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025. ولوحظ أيضا أن الاقتراح حظي بتأييد مجموعة من الدول من أقاليم مختلفة ويمكن أن يكون بمثابة هيكل دائم للمناقشات بشأن تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي يتم إنشاؤه عقب اختتام أعمال الفريق العامل المفتوح العضوية الحالي.

17 - وأشارت عدة دول إلى أنه ينبغي إنشاء فريق عامل دائم مفتوح العضوية فور اختتام الفريق العامل الحالي عند متم عام 2025. ولاحظت هذه الدول أن الفريق العامل المفتوح العضوية الحالي قد أثبت كفاءته وأهميته باعتباره أنسب شكل لآلية من هذا القبيل، وبوصفه فريقا عاملا دائما مفتوح العضوية لصنع القرار مكلفا بالتركيز على مواصلة تعزيز بيئة مفتوحة وآمنة ومستقرة وميسّرة وسلمية لتكنولوجيات المعلومات والاتصالات، وذلك عن طريق جملة أمور من بينها وضعُ قواعد ومعايير ومبادئ ملزمة قانونا تتعلق بسلوك الدول المسؤول، وإنشاءُ آلية فعالة لتنفيذ تلك القواعد والمعايير والمبادئ، باعتبارها عناصر لمعاهدة عالمية مقبلة تهدف إلى ضمان أمن المعلومات على الصعيد الدولي.

النطاق والأهداف

18 - شددت دول كثيرة على أن الهدف الأسمى لإجراء حوار مؤسسي منتظم في المستقبل بشأن أمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها هو الإسهام في تحقيق السلام والأمن الدوليين في هذا المجال. وقد أشارت عدة دول إلى أن أي آلية مقبلة ينبغي أن تعزز بيئة مفتوحة وآمنة ومستقرة وميسَّرة وسلمية في مجال تكنولوجيات المعلومات والاتصالات. وأشارت بعض الدول أيضا إلى أن الآلية المقبلة ينبغي أن تيسر الحوار والتعاون فيما بين الدول وأن تسهم في منع نشوب النزاعات وحالات سوء الفهم.

19 - وشددت عدة دول على أن التوصيات التي صدرت بتوافق الآراء في عمليات الأمم المتحدة السابقة، والتي أسفرت عن إطار موحد لسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات، ينبغي أن تظل محط تركيز محوري لأي آلية مؤسسية مقبلة. وشددت عدة دول على أهمية تقديم الدعم في تنفيذ النتائج المتفق عليها سابقا، بينما أشارت دول أخرى إلى أن أي آلية مقبلة ينبغي أن تنظر في التنفيذ العملي للاتفاقات التي توصل إليها الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025. واقتُرح أن تضع أي آلية مقبلة توجيهات ملموسة لدعم الدول في تنفيذ الإطار المعياري المتفق عليه فضلا عن تعزيز فهم الإطار نفسه.

20 - وتناولت الدول في مذكرات ردودها الحاجة إلى مواصلة تطوير الإطار القائم. فقد أشارت بعض الدول إلى خيارات لتحديد أي ثغرات، أو وضع معايير إضافية، أو وضع قواعد جديدة والتزامات ملزمة

قانونا. وأيدت عدة دول السعي إلى وضع صك ملزم قانونا، في حين أكدت دول أخرى أنه يمكن إخضاع الإطار للمزيد من التطوير والتحديث، إذا لزم الأمر، استجابة للتهديدات الجديدة في إطار مسايرة تطورها مع مرور الوقت. وأشارت عدة دول إلى أن الآلية ينبغي أن تقيم توازنا بين جانبين متساويين في الأهمية من جوانب العمل – وهما تنفيذ الإطار القائم ومواصلة تطويره.

21 – وذهب رأي إلى أنه ينبغي لأي آلية مقبلة أن تنظر إلى الأمام وإلى الخلف ليشمل تركيزها مراقبة وتنفيذ الإطار الحالي المتفق عليه لسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات، وليشمل على وجه الخصوص إثراء بناء القدرات، وصياغة معايير جديدة استجابة لآخر التطورات، من قبيل ما يتعلق منها بأمن البيانات، ووضع خطط عمل جديدة بشأن بناء القدرات وصك ملزم قانونا.

22 – وشددت دول كثيرة على أن موضوع بناء القدرات ينبغي أن يحتل مكانة مركزية في أي آلية مقبلة. وشددت بعض الدول على أهمية تضافر الجهود القائمة، بما في ذلك المبادرات ذات الصلة التي يقوم بها الاتحاد الدولي للاتصالات والبنك الدولي. ووردت الإشارة إلى المبادئ المتفق عليها لبناء القدرات المرفقة بالتقرير المرحلي السنوي الثاني للفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021–2025[4]. وأشارت عدة دول إلى أن أي آلية مقبلة ينبغي أن تيسر جهود بناء القدرات، بما في ذلك من خلال تبادل المعلومات بشأن أفضل الممارسات. وشددت عدة دول على أهمية الجهود القائمة على الاحتياجات والمحددة الأهداف. وكان ثمة من رأى أن وظيفة أي آلية في بناء القدرات يجب أن ترتبط بصورة مباشرة بالجهود التي تبذلها الدول على الصعيد الوطني لتنفيذ الإطار المعياري لسلوك الدول المسؤول.

23 – وأثيرت أيضا إمكانية إنشاء آلية تمويل مكرسة تستفيد من خبرات المرافق القائمة في محافل الأمم المتحدة الأخرى من أجل دعم جهود بناء القدرات ذات الصلة. واقتُرِحَ إنشاء "نظام شراكة" طوعي عابر للحدود الإقليمية، يمكن من خلاله الجمع بين دول تختلف من حيث قدراتها بهدف تعزيز التعاون وتبادل الممارسات في مجال الغذاء. وكان هناك اقتراح بإنشاء آلية متعددة العناصر لبناء القدرات، بما في ذلك تبادل الآراء بشأن واقع التهديدات، والتحديد الذاتي للاحتياجات من القدرات، ومطابقة الاحتياجات مع الموارد، فضلا عن "حلقة لإبداء التعليقات" لتبادل الخبرات ذات الصلة.

24 – وأشارت عدة دول إلى أن أي آلية مقبلة يمكن أن تكون بمثابة إطار مؤسسي شامل للمبادرات والجهود ذات الصلة في مجال أمن تكنولوجيات المعلومات والاتصالات، بما في ذلك دليل جهات الاتصال الحكومية الدولية.

25 – واقترحت الدول مجالات أخرى يمكن التركيز عليها، بما في ذلك إقرار فهم مشترك لكيفية انطباق القانون الدولي على استخدام تكنولوجيات المعلومات والاتصالات والكيفية التي يمكن من خلالها تكييف المعايير القائمة مع الخصائص المحددة لهذا المجال. وذهب رأي إلى أن وضع آلية في المستقبل يمكن أن يدفع قُدما بالمناقشات بشأن التهديدات القائمة والناشئة وكيفية تطبيق القانون الدولي، بما في ذلك القانون الدولي الإنساني والقانون الدولي لحقوق الإنسان، على استخدام الدول لتكنولوجيات المعلومات والاتصالات. وحُددت أيضا مسألة وضع وتنفيذ تدابير لبناء الثقة وآليات للتعاون العملي بين الدول باعتبارها بنودا ينبغي معالجتها.

(4) A/78/265، المرفق جيم.

الإنشاء والطرائق واتخاذ القرارات

26 - عرضت الدول آراء متنوعة بشأن طرائق إنشاء آلية في المستقبل، فضلا عن الجهود التحضيرية السابقة عن إنشائها. فمن الآراء المعرب عنها أن المساهمات المقدّمة من الدول الأعضاء في إطار الفريق العامل المفتوح العضوية الحالي، بما في ذلك المساهمات المتعلقة ببرنامج العمل المقترح، وتقرير الأمين العام المعد عملا بقرار الجمعية العامة 37/77[5]، فضلا عن هذا التقرير والتوصيات ذات الصلة الواردة في تقارير الفريق العامل المفتوح العضوية الحالي، ينبغي أن تمثل الأساس الذي يُستند إليه في إنشاء الآلية في المستقبل من حيث النطاق والهيكل والطرائق.

27 - وشددت دول كثيرة على أهمية التوصل إلى توافق في الآراء بشأن نطاق الآلية المقبلة وهيكلها وطرائق عملها. وأعربت دول كثيرة عن تأييدها لمواصلة صياغة وتطوير الآلية في إطار الفريق العامل المفتوح العضوية الحالي. وأيدت عدة دول إجراء مناقشات مكرسة أكثر تركيزا في إطار الفريق العامل المفتوح العضوية الحالي لوضع الآلية والسعي إلى التوصل إلى توافق في الآراء بشأن شكلها وهيكلها. وفيما يتعلق ببرنامج العمل، أيدت عدة دول عقد اجتماعات مكرسة فيما بين الدورات بشأن هذا الاقتراح في عامي 2024 و 2025 لصياغة المزيد من جوانب الآلية. واقتُرِح أيضا إجراء مزيد من المناقشات بشأن الآثار المترتبة في الميزانية.

28 - ووردت الإشارة إلى إمكانية إقامة حوار مؤسسي منتظم في المستقبل من خلال قرار تتخذه الجمعية العامة بتوافق الآراء. وفي هذا الصدد، ذهب بعض الرأي إلى أن قرارا للجمعية العامة ينبغي أن ينشئ فريقا عاملا دائما مفتوح العضوية. وثمة أيضا من رأى أن الفريق العامل المفتوح العضوية الحالي يمكن أن ينشئ الآلية المقبلة عن طريق إعلان سياسي تعتمده الجمعية العامة في وقت لاحق. وذُكر أن تأكيد التزام الدول بأن تسترشد بإطار سلوك الدول المسؤول يمكن أن يكون عنصرا رئيسيا من عناصر هذا الإعلان السياسي.

29 - وفيما يتعلق بالاقتراح المحدد المتعلق بوضع برنامج عمل، أعربت عدة دول عن تأييدها لوضع برنامج العمل عن طريق إعلان سياسي. واقتُرح استكمال الإعلان بقرار من اللجنة الأولى للجمعية العامة يصف وظائف برنامج العمل وهيكله وطرائق عمله. ومن الاقتراحات المقدمة أيضا أن يُعقد مؤتمر دولي في موعد أقصاه عام 2026 لصياغة هذا الإعلان واعتماده. وكان ثمة من رأى أنه في حال فشل الفريق العامل المفتوح العضوية الحالي في التوصل إلى توافق في الآراء بشأن تقرير نهائي، بما في ذلك الاتفاق على آلية، ستكون هناك حاجة إلى عقد مؤتمر دولي أكثر شمولا أو إلى عملية تحضيرية أخرى تُنشأ من خلال الجمعية العامة لضمان استمرارية هذه المناقشات الهامة المتعددة الأطراف.

آلية المتابعة والتنفيذ

30 - قدمت الدول اقتراحات مختلفة بشأن آلية المتابعة، منها عقد اجتماعات منتظمة، مثل الجلسات العامة ومؤتمرات الاستعراض، فضلا عن الاجتماعات التي تعقد فيما بين الدورات، بما في ذلك اجتماعات الأفرقة العاملة التقنية. واقتُرِحَ أيضا عقد اجتماعات رسمية سنوية للآلية. واختلفت المقترحات المتعلقة بوتيرة الجلسات العامة بين من رأى أن تُعقد كل سنتين ومن رأى أن تُعقد كل ثلاث سنوات. وكان ثمة أيضا من رأى أن الآلية المقبلة ينبغي أن تعقد اجتماعات مرة كل سنتين لتنفيذ برنامج عملها المتفق عليه. وورد

(5) A/78/76.

أيضا رأي يقول إنه سيكون من المفيد إجراء استعراض دوري لعمليات الآلية الدائمة للتأكد من أن النهُج التي تتّبعها ذات صلة بالمشهد الدينامي للتهديدات التشغيلية.

31 - وأيدت بعض الدول إنشاء أفرقة عاملة تقنية تُعنى بمسائل محددة ذات أولوية، مثل انطباق القانون الدولي، ووضع معايير وقواعد ومبادئ جديدة، فضلا عن الالتزامات الملزمة قانونا، حسب الاقتضاء. وثمة من رأى أن الأفرقة العاملة التقنية ستكون هي جوهر أي آلية عملية المنحى. واقتُرِحَ أن تنظر أفرقة فرعية في جوانب محددة من ولاية الآلية. وذهب بعض الرأي إلى أن اجتماعات الأفرقة العاملة التقنية بشأن مسائل محددة خلال فترات ما بين الدورات ينبغي أن تعقد في شكل هجين لتيسير مشاركة الدول على نطاق واسع. ولوحظ أن اجتماعات الأفرقة الفرعية ينبغي ألا تُعقد بالتوازي لضمان المشاركة الكاملة للوفود. ولتيسير مشاركة الدول على نطاق واسع، اقتُرح إعداد برنامج للزمالات.

32 - واقترحت الدول تحديد فترات دورية مختلفة لمؤتمرات الاستعراض المحتمل عقدها، بما في ذلك كل ثلاث أو أربع أو ست سنوات. وأشارت بعض الدول إلى أن مؤتمرات الاستعراض هذه ينبغي لها أن تستعرض إطار سلوك الدول المسؤول بغرض تحديثه، حسب الاقتضاء، كما ينبغي لها أن تقدم التوجيه الاستراتيجي لعمل الآلية. وثمة من رأى أنه ينبغي لمؤتمرات الاستعراض أن تنظر فيما إذا كان ينبغي وضع معايير أو قواعد أو مبادئ إضافية أو التزامات ملزمة على أساس توافق الآراء.

33 - وتناولت دول عديدة أهمية اتخاذ القرارات بتوافق الآراء في أي آلية مقبلة. فقد شددت بعض الدول على أن القرارات المتعلقة بالمسائل الموضوعية يجب أن تتخذ بتوافق الآراء. وذهبت عدة دول إلى أن مبدأ اتخاذ القرارات بتوافق الآراء من جانب الدول حصريا ينبغي أن يرد بكل وضوح في الوثيقة المنشئة للآلية المقبلة. واقترحت الدول أشكالا مختلفة لتجميع القرارات التي تتخذها الدول في أي آلية مقبلة، كأن يكون ذلك في التقارير المرحلية التي تُقدم إلى الجمعية العامة كل سنتين والتقارير الإجرائية السنوية المشفوعة بالقرارات ذات الصلة التي تُتخذ بتوافق الآراء.

34 - وأشارت بعض الدول إلى إمكانية تقديم تقارير وطنية طوعية في إطار آلية مقبلة. واقتُرح الإبلاغ عن التنفيذ الوطني للإطار المعياري وكذلك عن الممارسات الوطنية. واقتُرح استخدام الأدوات القائمة، مثل الدراسة الاستقصائية الوطنية لتنفيذ توصيات الأمم المتحدة بشأن استخدام الدول المسؤول لتكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي والأمم المتحدة[6].

35 - وأشارت عدة دول إلى أنه في حين أن اتخاذ القرارات سيظل حكرا على الدول، فإن التفاعل مع المنظمات الإقليمية ودون الإقليمية يمكن أن يكون مفيدا، بما في ذلك لتعزيز أوجه التآزر والاستفادة من الهياكل والمنصات القائمة في مجال بناء القدرات. واقتُرِح عقد اجتماعات فيما بين الدورات مع ممثلي هذه المنظمات على أساس سنوي استنادا إلى مشاورات تُجرى مع مجموعات البلدان ورئيس الآلية المقبلة. واقتُرِح أيضا تبادل أفضل الممارسات على المستويات الدولي والأقاليمي والإقليمي.

36 - وأعربت الدول عن آراء مختلفة بشأن التعامل مع الكيانات غير الحكومية في أي آلية مقبلة، موردة أمثلة من طرائق المشاركة في محافل الأمم المتحدة الأخرى، مثل اللجنة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية والفريق العامل

(6) https://nationalcybersurvey.cyberpolicyportal.org/.

المفتوح العضوية المعني بالشيخوخة. وأشارت دول كثيرة إلى أن مشاركة جهات شتى من الجهات صاحبة المصلحة أمر مهم لعمل الآلية في المستقبل. ولوحظ أن إشراك الجهات صاحبة المصلحة على نحو شامل في الجولة المقبلة من الحوار المؤسسي المنتظم سيكون أمرا مفيدا لتحقيق الهدف المشترك المتمثل في صون السلام والأمن في مجال تكنولوجيات المعلومات والاتصالات، ويمكن أن يجلب خبرة قيمة في مسائل من قبيل تقييم التهديدات وتنفيذ المعايير. وأيدت بعض الدول مشاركة الكيانات غير الحكومية تمشيا مع الطرائق المتفق عليها ضمن الفريق العامل المفتوح العضوية الحالي. وأيدت عدة دول المشاركة الرسمية من جانب الجهات صاحبة المصلحة وإجراء مشاورات منتظمة مع هذه الجهات، بينما ذكرت دول أخرى أن التعامل مع الجهات الفاعلة من غير الدول ينبغي أن ينحصر في الطابع التشاوري وغير الرسمي، كأن يكون ذلك من خلال اجتماعات سنوية تُعقد فيما بين الدورات.

37 - وحددت بعض الدول مكتب شؤون نزع السلاح بوصفه الكيان المناسب للقيام بدور الأمانة لأي آلية مقبلة.

رابعا - ملاحظات واستنتاجات الأمين العام

38 - لا يزال صون السلام والأمن في مجال تكنولوجيات المعلومات والاتصالات مهمة ملحة. فبينما يتزايد القلق بشأن استخدام هذه التكنولوجيات من قبل مجموعة من الجهات الفاعلة لأغراض خبيثة، يواجه المجتمع الدولي فجوة رقمية آخذة في الاتساع وموعدا نهائيا يقترب بسرعة لتحقيق أهداف التنمية المستدامة. ولا بد من اتخاذ تدابير ملموسة لمنع توسع رقعة النزاع وزيادة تصعيده ليطال هذا المجال، بما في ذلك لحماية الأرواح البشرية من النشاطات الخبيثة.

39 - ولئن كانت هناك تحديات هائلة تواجه المجتمع الدولي في صون السلام والاستقرار في مجال تكنولوجيات المعلومات والاتصالات، فإن هناك أيضا أساسا متينا يمكن الاعتماد عليه. فعلى مدى أكثر من عقدين من الزمن، ومن خلال إجراءات تتم تحت رعاية الجمعية العامة، أحرزت الدول تقدما حاسما في تحديد التهديدات القائمة والناشئة، حيث أبرزت انطباق القانون الدولي على استخدام الدول لتكنولوجيات المعلومات والاتصالات، ووضعت إطارا لسلوك الدول المسؤول في استخدام هذه التكنولوجيات، ونظرت في اتخاذ تدابير لمد جسور الثقة وفي تنفيذ مبادرات لبناء القدرات. وكان هذا التقدم تراكميا ومتسقا وأُحرِز بالاعتماد على اتفاقات تم التوصل إليها بتوافق الآراء. وبهذا يكون قد تهيأ أساس متين لإحراز مزيد من التقدم.

40 - والجهود التي تبذلها الدول في إطار الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025 دليل على إمكانية اتخاذ مزيد من الإجراءات الملموسة نحو تحقيق الأهداف المشتركة المتمثلة في تهيئة بيئة سلمية وآمنة لتكنولوجيات المعلومات والاتصالات. ويدل التقدم المحرز باستمرار في هذا المحفل على أنه متى وُجدت الإرادة السياسية الكافية، لا يمكن التوصل إلى اتفاقات مشتركة فحسب، بل يمكن أيضا اتخاذ إجراءات عملية. وأنا أرحب في هذا الصدد بالاتفاق الذي توصلت إليه الدول بتوافق الآراء لوضع دليل عالمي لجهات الاتصال الحكومية الدولية من أجل تعزيز التفاعل والتعاون فيما بينها. فهذه خطوة هادفة تعزز السلام والأمن الدوليين وتزيد من الشفافية ووضوح الرؤية.

41 - وفي هذا السياق، اعترفت الدول بالأهمية الحاسمة للاحتفاظ بحوار مؤسسي منتظم بشأن هذه المسائل بغية إتاحة حيز كاف لإحراز تقدم مستمر. ولا يُتوقع سوى أن تزداد هذه القضايا أهميةً مع تزايد تغلغل هذه التقنيات واحتلالها حيزا متعاظما من حياتنا اليومية.

42 - وهناك اتفاق عام بين الدول على أن حوارا مؤسسيا منتظما من هذا القبيل هو الأنسب لأن يجرى تحت رعاية الأمم المتحدة، حيث توفر المنظمة منبرا شاملا لإجراء نقاش من هذا القبيل. وهناك أيضا فهم مشترك بأن هذا الحوار يدعم الأهداف المتمثلة في تعزيز السلام والاستقرار الدوليين ومنع نشوب النزاعات في بيئة تكنولوجيات المعلومات والاتصالات. وتؤكد الدول أيضا على عدة مبادئ حاسمة لدعم هذا الحوار، مثل الشمولية والشفافية والنهج العملي المنحى. وعلاوة على ذلك، هناك فهم مشترك للحاجة إلى آلية أحادية المسار تيسّر مشاركة الدول على أوسع نطاق.

43 - واستناداً إلى هذه الاتفاقات الواسعة والآراء السائدة على نطاق واسع، يبدو التوصل إلى اتفاق بتوافق الآراء بشأن حوار مؤسسي منتظم في المستقبل بشأن تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي مهمة قابلة للتحقيق. فبفضل ما أُحرز من نجاحات بالفعل، توجد لدى الدول فرصة هائلة في إطار الفريق العامل المفتوح العضوية الحالي للتوصل إلى أرضية مشتركة بشأن آلية دائمة أحادية المسار تحت رعاية الأمم المتحدة تعمل بطريقة متفتحة وشاملة وشفافة. والعناصر المشتركة للحوار المؤسسي المنتظم في المستقبل حسبما اتُّفق عليه بالإجماع في التقرير المرحلي السنوي لعام 2023 للفريق العامل المفتوح العضوية تشكل منطلقا معقولا ومفيدا. وهذه المسائل هي من الأهمية بحيث لا يمكن تفويت هذه الفرصة السانحة لتمتين جسور الثقة وترسيخ مناخ الاطمئنان. فإن وضع آلية دائمة تعمل تحت رعاية الأمم المتحدة هي الخطوة المنطقية التالية من النظر في هذه المسائل على مستوى متعدد الأطراف، وذلك بالاعتماد على ما أُحرز من نجاح في الماضي، مع القيام في الوقت نفسه بتمهيد الطريق لإحراز التقدم في المستقبل.

المرفق

الردود الواردة من الحكومات

أستراليا

[الأصل: بالإنكليزية
1 أيار/مايو 2024]

ترحب أستراليا بفرصة الردّ على الدعوة الواردة في قرار الجمعية العامة 237/78 بتقديم وجهات نظرها بشأن الارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي ومواصلة الحوار المؤسسي المنتظم.

وتستند هذه المذكرة إلى المذكرات التي قدمتها أستراليا في عام 2023 عملا بالقرار 37/77، وفي عام 2022 عملا بالقرار 19/76، وفي عام 2021 عملا بالقرار 32/75، وفي عام 2020 عملا بالقرار 28/74، ووفي 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.

استراتيجية الأمن السيبراني الأسترالية 2023-2030

في 22 تشرين الثاني/نوفمبر 2023، أعلنت كلير أونيل، وزيرة الأمن السيبراني، عن استراتيجية الأمن السيبراني الأسترالية للفترة 2023-2030، وهي تحدد رؤية أستراليا للأمن السيبراني المحلي والدولي من خلال نهج لبناء المرونة السيبرانية تشارك فيه الأمة بأكملها.

وحددت الاستراتيجية ستة دروع لتمتين الدفاعات السيبرانية وكفالة سرعة التعافي بعد وقوع أي حادث سيبراني :(أ) مؤسسات تجارية قوية ومواطنون أقوياء؛ (ب) تكنولوجيا آمنة؛ (ج) تبادل المعلومات عن التهديدات وحظرها بأرفع الطرق الممكنة؛ (د) حماية البنى التحتية الحيوية؛ (هـ) القدرات السيادية؛ (و) المرونة الإقليمية والقيادة العالمية.

وتكرس الاستراتيجية التزام أستراليا المستمر بصياغة القواعد والمبادئ والمعايير السيبرانية الدولية وبإعمالها والدفاع عنها، بما في ذلك من خلال التمسك بالقانون الدولي ومعايير سلوك الدول المسؤول في الفضاء السيبراني، واستخدام جميع قدرات الدولة لردع الجهات الفاعلة الخبيثة والتصدي لها.

التمسك بالقانون الدولي ومعايير سلوك الدول المسؤول في الفضاء السيبراني

نحن في أستراليا سنتعاون مع شركائنا الحاليين وسنقيم شراكات جديدة لصون القانون الدولي والإطار المتفق عليه لسلوك الدول المسؤول الذي يضمن استقرارنا وازدهارنا واستقلالنا وسيادتنا في الفضاء السيبراني.

وقد اتفقت جميع البلدان على أن يكون الفضاء السيبراني محكوما بقواعد، ويستند إلى القانون الدولي والمعايير الدولية القائمة. فالقانون الدولي، إلى جانب المعايير الطوعية المتفق عليها لسلوك الدول المسؤول، وتدابير بناء الثقة، وبناء القدرات، يوفر إطارا قويا يضفي على الفضاء السيبراني طابع الاستقرار

ووضـــوح الرؤية. وهذا الإطار، إذا تم تنفيذه والتقيد به، يوفر مجموعة أدوات للتصـــدي لتهديدات الأنشـــطة السيبرانية الخبيثة التي تقوم بها الدول وترعاها.

ونحن في أستراليا سنعمل مع شركائنا الدوليين في المناقشات التي تجري في إطار الأمم المتحدة لتوضـيح الكيفية التي ينطبق بها القانون الدولي في الفضـاء السـيبراني وللدفع قُدما بتنفيذ إطار سـلوك الدول المســؤول في الفضـــاء الســـيبراني. وســـتشـــمل هذه الجهود تعزيز التعاون من خلال المنتديات الإقليمية، بما في ذلك التعاون في إطار منتدى جزر المحيط الهادئ، ومن خلال التعاون مع المنتدى الإقليمي لرابطة أمم جنوب شرق آسيا.

استخدام جميع قدرات الدولة لردع الجهات الفاعلة الخبيثة والتصدي لها

سوف تستخدم أستراليا جميع قدرات الدولة لردع الجهات الفاعلة السيبرانية الخبيثة والتصدي لها. فنحن في أستراليا سنعمل مع شركائنا الدوليين لاتخاذ الإجراءات اللازمة لترتيب عواقب على كل من تسول له نفسه من الأفراد أو المؤسسات أن يمس بأمن وسلامة الفضاء السيبراني. ويشمل ذلك فضح الحالات التي تعمل فيها الدول على تقويض أو خرق القانون الدولي والمعايير الدولية، وفرض جزاءات على من يتســببون في حوادث ســيبرانية مؤثرة أو يســهلون وقوعها – متى توفرت لدينا أدلة كافية وكان من مصــلحتنا الوطنية القيام بذلك.

وســـتكون أســـتراليا، في كل ما تقوم به من إجراءات، متمســـكة بالقانون الدولي القائم وبالمعايير الطوعية المتفق عليها لسلوك الدول المسؤول في الفضاء السيبراني.

تقديم الدعم لإكساب منطقتنا الإقليمية المرونة السيبرانية

سنواصل في أستراليا العمل مع جيراننا على صعيد المحيط الهادئ وجنوب شرق آسيا حتى تكون منطقتها أكثر مرونة في الجانب السيبراني. وسيواصل سفير أستراليا للشؤون السيبرانية والتكنولوجيا الحيوية تنسيق أنشطتنا في مجالي التعاون والمساعدة.

وأستراليا بصدد إعادة تركيز جهودها في مجال التعاون السيبراني وبناء القدرات لتكون أهدافها أكثر وضـوحا، ولتكون أكثر تأثيرا واسـتدامة، ولإعطاء جيراننا المزيد من القدرة على منع الحوادث السـيبرانية وعلى التعافي منها بســـرعة عند حدوثها. وإدراكا منا بأن الناس يختلفون في طرق تعاملهم مع قضـــايا الأمن السيبراني، سنظل فيما نبذله من جهود نراعي اعتبارات المساواة بين الجنسين والإعاقة والإدماج الاجتماعي. وهذا يشمل مواصلة تقديم الدعم لخطة الأمم المتحدة المتعلقة بالمرأة والسلام والأمن، فضلا عن خطة العمل الوطنية الأسترالية بشأن المرأة والسلام والأمن 2021–2031.

ومتى وقعت حوادث سـيبرانية خطيرة في منطقتنا، سـتكون أسـتراليا في وضـع أفضـل للاسـتجابة لطلبات المساعدة. فأستراليا بصدد إنشاء فريق للاستجابة للأزمات السيبرانية على الصعيد الإقليمي في وزارة الخارجية والتجارة، معتمدة في ذلك على خبرات القطاعات الحكومية والصـــناعية والتقنية. ومتى كانت هناك طلبات حكومية عند وقوع حوادث سـيبرانية كبرى على صـعيد المنطقة، سـيبادر الفريق إلى تقديم المسـاعدة اللازمة لاحتواء الحوادث السيبرانية من حيث انتشارها وآثارها، ولاستعادة الخدمات والبنى التحتية الحيوية.

الحوار المؤسسي المنتظم

برنامج العمل للارتقاء بسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي

تؤيد أستراليا إنشاء آلية وحيدة ودائمة ومرنة، وتتسم بالشمول والشفافية، وتكون عملية المنحى، برعاية اللجنة الأولى، لمناقشة إطار سلوك الدول المسؤول في الفضاء السيبراني وتنفيذه والارتقاء به، وهو الإطار الذي وافقت عليه الجمعية العامة وأعادت تأكيده بتوافق الآراء. ويتألف الإطار من القانون الدولي، ومعايير وتدابير لبناء الثقة، ويحظى بالدعم من خلال بناء القدرات بطريقة منسقة. وينبغي أن يوفر برنامج العمل منتدى يمكن فيه لجميع الدول الأعضاء البالغ عددها 193 دولة أن تشارك مشاركة مجدية في كل من المناقشة والعمل على أساس منتظم ومستمر. ويُتوخى أن يكون برنامج العمل قابلا للتوسع والتكيف والتطور – إذ ينبغي له أن يدعم تنفيذَ الإطار الحالي المتفق عليه ويتيح إمكانية مواصلة تطويره، بتوافق الآراء، في ضوء ظهور تهديدات وتحديات جديدة.

وقد رحبت الجمعية العامة في قرارها 37/77 بالاقتراح الداعي إلى وضع برنامج العمل، وطلبت إلى الأمين العام أن يلتمس آراء الدول الأعضاء بشأن نطاق برنامج العمل وهيكله ومضمونه. وورد في ذلك التقرير (A/78/76) التوصية بأن تواصل الدول، تحت رعاية الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021–2025، مناقشة برنامج العمل المقترح من حيث إمكانات نطاقه وهيكله ومبادئه ومضمونه ووظائفه وآلية متابعته، مستفيدة في ذلك من الآراء المعرب عنها في التقرير، مع أخذها في الاعتبار أيضا المشاورات الإقليمية ودون الإقليمية التي ينظمها مكتب شؤون نزع السلاح عملا بقرار الجمعية العامة 37/77.

ويضطلع الفريق العامل المفتوح العضوية بدور رئيسي في أعمال الصياغة والتحضير لبرنامج العمل. وينبغي أن يستند برنامج العمل إلى المكاسب التي تحققت بشق الأنفس بتوافق الآراء والمناقشات التراكمية التي أجرتها أفرقة الخبراء الحكوميين الستة السابقة المتعاقبة والفريقين العاملين المفتوحَي العضوية الأول والحالي. وتمثل آليةٌ دائمة المرحلةَ التالية أو التطور في الهيكل السيبراني للأمم المتحدة الذي يقوم على ما سبقه ويضمن أن يُعطى في المستقبل لهذه المسائل ما تستحقه من اهتمام وأهمية.

وقررت الجمعية العامة في قرارها 16/78 إنشاء آلية تحت رعاية الأمم المتحدة، عند اختتام أعمال الفريق العامل المفتوح العضوية للفترة 2021–2025، وفي موعد أقصاه عام 2026، تكون آلية دائمة وشاملة وعملية المنحى، وفقا للأهداف المحددة المؤكدة في قرار الجمعية العامة 37/77، وللعناصر المشتركة للجولة المقبلة من الحوار المؤسسي المنتظم المتفق عليه بتوافق الآراء في التقرير المرحلي السنوي لعام 2023 للفريق العامل المفتوح العضوية للفترة 2021–2025.

وتؤيد أستراليا الاقتراح الداعي إلى عقد مؤتمر دولي في عام 2025 لاعتماد الوثيقة التأسيسية لبرنامج العمل، على أساس العمل التحضيري الذي أُنجز في إطار الفريق العامل المفتوح العضوية للفترة 2021–2025.

وتؤيد أستراليا أي وثيقة تأسيسية لبرنامج العمل تحدد التزامات الدول وتنشئ آلية يمكن إقرارها بقرار تتخذه الجمعية العامة. والوثيقة التأسيسية يمكن أن تصدر في صيغة إعلان سياسي وينبغي فيها ما يلي:

- تأييد وإعادة تأكيد التزام الدول سياسيا بالإطار (بما في ذلك تطبيق القانون الدولي القائم في الفضاء السيبراني) على النحو المتفق عليه في تقارير أفرقة الخبراء الحكوميين[1] وتقرير الفريق العامل المفتوح العضوية[2].

- التذكير بما يتعرض له الأمن الدولي من تهديدات قائمة وناشئة تتعلق باستخدام تكنولوجيات المعلومات والاتصالات لأغراض خبيثة، استنادا إلى تقييمات التهديدات الواردة في تقارير أفرقة الخبراء الحكوميين والفريق العامل المفتوح العضوية.

- إنشاء آلية مؤسسية دائمة للنهوض بتنفيذ هذا الإطار (بما في ذلك دعم قدرات الدول على القيام بذلك) والطرائق ذات الصلة.

- السماح بمواصلة تطوير وتحديث الإطار، حسب الاقتضاء، ليشمل مبادئ وتوصيات والتزامات متوافَق عليها في حالة إقرار الجمعية العامة، بتوافق الآراء، تقريراً يعده الفريق العامل المفتوح العضوية أو فريق الخبراء الحكوميين أو عمليات أخرى من عمليات الأمم المتحدة، أو من خلال اتفاق يُتوصل إليه بتوافق الآراء في مؤتمر يُعقد لاستعراض برنامج العمل.

- تحديد مجالات تركيز برنامج العمل استنادا إلى المسائل التي يتفق المجتمع الدولي على مناقشتها ومعالجتها.

- تعزيز وتشجيع التعاون، بوضوح، مع الأعضاء المعنيين من دوائر الجهات المتعددة صاحبة المصلحة في المجالات ذات الصلة.

وفيما يتعلق بالنظام الداخلي، تكرر أستراليا التأكيد على أن يتطلب برنامج العمل الاتفاق على جميع المسائل بتوافق الآراء (بما في ذلك التقارير والتوصيات والإعلانات).

وحتى تكون أنشطة برنامج العمل مرتكزة على الأدلة ومستندة إلى البيانات، ينبغي أن يركز برنامج العمل على دعم جهود التنفيذ، بسبل منها بناء القدرات على نحو محدد وهادف ومنسق. وينبغي توخي الوضوح لدى وضع تدابير بناء القدرات المخصصة في إطار برنامج العمل. ومن أجل المساعدة على بناء القدرات بطريقة هادفة تستند إلى الاحتياجات وتقوم على قاعدة من الأدلة، يمكن أن يشجع برنامج العمل الدول الأعضاء على إجراء دراسات استقصائية دورية وعلى الإبلاغ الذاتي عن تنفيذها للإطار (كل ثلاث سنوات مثلا، وإلا فبالتوازي مع دورة مؤتمر الاستعراض)، باستخدام آلية إبلاغ موحدة، هي الدراسة الاستقصائية الوطنية لتنفيذ توصيات الأمم المتحدة بشأن استخدام الدول المسؤول لتكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي (متاحة على هذا الرابط https://nationalcybersurvey.cyberpolicyportal.org/).

وتدرك أستراليا أهمية دوائر الجهات المعنية المتعددة، التي تشمل المجتمع المدني والقطاع الخاص والأوساط الأكاديمية والتقنية، في الإسهام في قيام فضاء سيبراني حر ومفتوح وآمن ومستقر وميسَّر وسلمي. وتقترح أستراليا أن يسمح برنامج العمل بإجراء مشاورات منتظمة ومؤسسية مع الجهات المعنية صاحبة المصلحة.

(1) انظر: A/65/201، و A/68/98، و A/70/174، و A/76/135.

(2) A/75/816.

بإيجاز، تشدد أستراليا على أن يكون لبرنامج العمل ولاية واضحة تستند إلى الإطار المتفق عليه وتعيد تأكيده؛ وأن يكون مرنا، سواء من الناحية الموضوعية أي إمكانية مواصلة تطوير الإطار بتوافق الآراء، أو من الناحية الإجرائية؛ وأن يدعم جهود التنفيذ من خلال الإبلاغ الطوعي ولدى تنفيذ الإطار من خلال بناء القدرات؛ وأن يكون شاملا، أي أن تظل القرارات المتعلقة بالمسائل ذات الصلة بالأمن الدولي من اختصاص الدول، مع فتح أبواب المناقشات والأفرقة العاملة أمام الجهات المتعددة صاحبة المصلحة.

وتتطلع أستراليا إلى مواصلة العمل مع الأمين العام ومكتب شؤون نزع السلاح والدول الأعضاء لوضع برنامج عمل يكون فعالا ويتسم بالمرونة والشمول.

أذربيجان

[الأصل: بالإنكليزية
1 أيار/مايو 2024]

في السنوات الأخيرة، شهد الفضاء السيبراني تطورا كبيرا، الأمر الذي فتح آفاقا لتحسين حياتنا اليومية، بدءا من السلامة والأمن، وإلى سرعة الاتصال واستخدام التكنولوجيات الرقمية. فأوجه التقدم في التكنولوجيا السيبرانية والحيوية تدعم ازدهار العالم في المستقبل، وهي في الوقت نفسه قادرة على تقويض الاستقرار ووضوح الرؤية. ولذلك، يلزم تعزيز تدابير بناء القدرات، والقدرات الوقائية الكافية، والخدمات الرقمية التي ستسهم في زيادة أمن الفضاء السيبراني.

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

تدعم أذربيجان عمل الفريق العامل المفتوح العضوية للفترة 2021-2025 المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها، المنشأ عملا بقرار الجمعية العامة 240/75. وقد اتخذت أذربيجان، باعتبارها من مقدمي قرار الجمعية العامة 237/78، عدة خطوات لتعزيز أمنها المعلوماتي وتشجيع التعاون الدولي في مجال الأمن السيبراني.

وتجدر الإشارة إلى أن استراتيجية جمهورية أذربيجان لأمن المعلومات والأمن السيبراني للفترة 2023-2027 المعتمدة بموجب مرسوم رئيس جمهورية أذربيجان المؤرخ 28 آب/أغسطس 2023، ترمي إلى تعزيز الأمن الوطني للمعلومات من أجل الاستخدام الآمن لتكنولوجيات المعلومات والاتصالات الحديثة من قبل الدولة والمجتمع والأفراد، وهو ما يستلزم تحديد وتنفيذ تدابير لضمان أمن شبكات الدولة والشبكات الخاصة، والبنى التحتية الحيوية للمعلومات، فضلا عن حماية البيانات الشخصية، ومن ثَم الإسهام في تهيئة ظروف أكثر ملاءمة لدعم حقوق الإنسان والحريات المكرسة في دستور جمهورية أذربيجان. وهذه الاستراتيجية، وهي الأولى من نوعها في مجال أمن المعلومات والأمن السيبراني في جمهورية أذربيجان، جزء لا يتجزأ من سياسة الدولة فيما يتعلق بتكنولوجيا المعلومات والاتصالات، وتتضمن الأهداف الأساسية للدولة وتوجهاتها ومهامها ذات الأولوية والحلول ذات الصلة وخطة من التدابير الشاملة المعمول بها في هذا المجال.

وعلاوة على ذلك، يرد ضمن خطة عمل الاستراتيجية، في الجزء 8-9-2-3، الإشارة إلى "تدبير مستمر لتنظيم تطوير التعاون الدولي ودراسة الخبرات الدولية في مجال الأمن السيبراني على مستوى كيانات أمن المعلومات، بما في ذلك الفريق الوطني للتصدي للطوارئ الحاسوبية والأفرقة الأخرى للتصدي للطوارئ الحاسوبية"، على أن الهدف الأساسي هو تطوير التعاون مع المراكز الدولية لأفرقة التصدي للطوارئ

الحاسوبية وتأمين العضوية في هذه المراكز. والعمل الفعلي جار حاليا من أجل توسيع نطاق الأنشطة المتبادلة وتبادل الخبرات.

وتجدر الإشارة إلى أنه تمت الموافقة على قواعد ضمان أمن البنية التحتية للمعلومات الحيوية في جمهورية أذربيجان والقواعد المنظمة لهيكل وإنشاء وإدارة سجل مكونات البنية التحتية للمعلومات الحيوية بموجب القرارين ذوي الصلة الصادرين عن مجلس وزراء جمهورية أذربيجان في عام 2023.

وبالإضافة إلى ذلك، ونتيجة للإجراءات المشتركة التي نفذها جهاز أمن الدولة في جمهورية أذربيجان ورابطة منظمات الأمن السيبراني في أذربيجان، انتقل موقع بلدنا في جدول الترتيب الدولي لمؤشر الأمن السيبراني الوطني من المركز السادس والثمانين إلى المركز الخمسين في عام 2023.

وأعد جهاز الدولة للاتصالات الخاصة وأمن المعلومات في جمهورية أذربيجان مشروع مبادئ توجيهية لضمان أمن المعلومات لتقديمه إلى الوكالات الحكومية بهدف ضمان أمن المعلومات في مؤسسات الدولة، بما في ذلك تحديد التدابير الوقائية والتصحيحية لمواجهة التهديدات المحتملة في بيئة معلومات الشركات.

ونُفذ مشروع للوقاية السيبرانية بهدف تعزيز المرونة السيبرانية ضد التهديدات السيبرانية وزيادة الوعي في هذا المجال لدى موظفي مؤسسات الدولة، وكذلك في القطاع الخاص ولدى أصحاب الأعمال التجارية.

وأقيم مهرجان سيبراني، تحدي الدفاع عن البنية التحتية الحيوية 2023، شارك في تنظيمه جهاز الدولة للاتصالات الخاصة وأمن المعلومات وجهاز أمن الدولة، يومي 26 و 27 تشرين الأول/أكتوبر 2023، وكان الهدف منه هو تعزيز خبرات ومعارف ومهارات الشركات المحلية والأجنبية ومؤسسات القطاعين العام والخاص العاملة في مجال الأمن السيبراني والبنى التحتية الحيوية والقطاع المالي وقطاع الاتصالات.

وفي المؤتمر الدولي للدبلوماسية السيبرانية الذي نظمه المعهد الوطني للبحث والتطوير في المعلوماتية في نيسان/أبريل 2023 برومانيا، تقرر أن تستضيف أذربيجان المؤتمر القادم في عام 2024.

ونتيجة للأنشطة العملية التي اضطُلع بها بهدف تشكيل وتطوير النظام الإيكولوجي الوطني للأمن السيبراني، تحسن كثيرا مركز أذربيجان في التصنيف العالمي. فبحسب المؤشر العالمي للأمن السيبراني 2020 الذي يتعهده الاتحاد الدولي للاتصالات، حسّنت أذربيجان مركزها بمقدار 15 نقطة، لتحتل المرتبة الأربعين من بين 194 بلدا، محققة درجة 89,31.

وأما من حيث التعاون الدولي في المجال المذكور، فقد حضر مشاركون من مختلف وكالات جمهورية أذربيجان الفعاليات الدولية المكرسة للتعاون في مكافحة التهديدات السيبرانية، ولتبادل المعلومات والخبرات بشأن حوادث الأمن السيبراني، وتطوير السياسات والاستراتيجيات في مجال الأمن السيبراني. ويشمل ذلك اجتماعات اللجنة الحكومية الدولية المخصصة المفتوحة العضوية المعنية بوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات لأغراض إجرامية، والمناسبات المعقودة في إطار مشاريع CyberEast، ووكالة الاتحاد الأوروبي للتدريب على إنفاذ القانون، والشراكة التدريبية والعملياتية لمكافحة الجريمة المنظمة، التي يشترك في تمويلها كل من الاتحاد الأوروبي ومجلس أوروبا.

كندا

[الأصل: بالإنكليزية
16 نيسان/أبريل 2024]

إن تنامي النشاطات الخبيثة في الفضاء السيبراني في السنوات الأخيرة يزيد من الحاجة إلى العمل بكفاءة للتخفيف من حدة التهديدات التي يمكن أن تقوض الأمن والاستقرار الدوليين.

والحاجة إلى تعزيز التعاون وتكثيف الجهود وفق منحى عملي تستدعي وجود آلية مناسبة تابعة للأمم المتحدة تُعنى بالأمن السيبراني. وتشدد كندا على ضرورة الاستفادة من المكتسبات الجماعية (القواعد القائمة وتفاهماتنا المشتركة بشأن كيفية تطبيق القانون الدولي)، وإفساح مجال يمكن أن يُجرى فيه المزيد من المناقشات المتعمقة والواقعية والتقنية، بطريقة تتكامل بالضرورة مع المناقشات التي نجريها في الجلسات العامة. وترى كندا أن الجولة المقبلة من الحوار المؤسسي المنتظم ينبغي أن تكون بمثابة حلقة حميدة من عمليات تقييم التهديدات، ومناقشات بشأن تنفيذ أطر العمل، وبناء القدرات، واستعراض أي ثغرات مخصوصة يتعين معالجتها. والعمل على أمور الواقع الحقيقي، أو على سيناريوهات تحاكي مثل هذه الأمور، هو أولى بأن يلقي الضوء على حلول ملموسة للتخفيف من حدة المخاطر. وينبغي أن تكون الجولة المقبلة من الحوار المؤسسي المنتظم عملية المنحى وموجهة نحو تحقيق نتائج، وأن تظهر تقدما مطردا وقابلا للقياس.

ومجتمع أصحاب المصلحة المتعددين، بصفتهم مالكي البنية التحتية للفضاء السيبراني ومشغليها، وباعتبارهم أعيننا وآذاننا على أرض الواقع، يوجد في وضع جيد بشكل خاص لتقديم إسهامات في عملنا عالية الجودة وفريدة من نوعها، بطريقة تشاورية. وضمان المشاركة الهادفة من قبل أصحاب المصلحة في الجولة المقبلة من الحوار المؤسسي المنتظم سيكون مفيدا لتحقيق هدفنا المشترك المتمثل في الحفاظ على الاستقرار السيبراني. وإشراك مجتمع أصحاب المصلحة المتعددين بهذه الطريقة هو أيضا أكثر النهج نجاعة لتعزيز وتيسير فرص إشراك الدول الصغيرة والنامية في عملنا. وهذا بدوره يرفع من إمكانية زيادة المرونة السيبرانية للجميع على صعيد العالم. والجولة المقبلة من الحوار المؤسسي المنتظم، إذا كانت شاملة حقا، فإنها ستوفر إمكانية أقوى للحصول على التأييد الذي يمكن أن يساعد على تنفيذ وتطوير سلوك الدول المسؤول في الفضاء السيبراني بحسن نية.

وينبغي مراعاة شواغل ومصالح جميع الدول في الجولة المقبلة من الحوار المؤسسي المنتظم، بما في ذلك ما يتعلق منها بمواصلة تطوير إطار العمل، وذلك من خلال مشاركة الدول على قدم المساواة في الأمم المتحدة. وينبغي اتخاذ القرارات المتعلقة بالمسائل الموضوعية بتوافق الآراء.

وتشير كندا إلى الآراء التي أعربت عنها بشأن الجولة المقبلة من الحوار المؤسسي المنتظم في سياق تقرير الأمين العام عن برنامج العمل، الصادر عملا بقرار الجمعية العامة 37/77، في نيسان/أبريل 2023، وتكرر تأكيد آرائها تلك. وتبين هذه الآراء بشكل خاص أن كندا تعترف وترحب بالتقارير والتوصيات المعتمدة بتوافق الآراء حتى الآن (مثل تقريري عام 2021 لفريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء السيبراني في سياق الأمن الدولي والفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي). وترى كندا أن أفضل مسار لعمل هذا الفريق العامل المفتوح العضوية لتنفيذ الولاية المنوطة به،

كما هي منصوص عليها في قرار الجمعية العامة 240/75، هو اتخاذ قرار بشأن إجراء حوار مؤسسي منتظم، أحادي المسار، دائم وعملي المنحى وشامل.

وترحب كندا بفرصة تقديم الآراء، مرة أخرى، بشأن الجولة المقبلة من الحوار المؤسسي المنتظم. فكندا تعتبر أن الآلية الحالية للفريق العامل المفتوح العضوية ليست مثالية ولا هي بالكافية لتحقيق أهدافنا الجماعية. ولن تؤيد كندا تكرار الآلية الحالية للفريق العامل المفتوح العضوية أو تجديدها بشكل دائم. وبدلا من ذلك، تؤمن كندا إيمانا راسخا بأن برنامج عمل يوضع في إطار الفريق العامل المفتوح العضوية ويُتَّفق عليه، في الحالات المثالية، بتوافق الآراء، هو أفضل السبل لضمان إجراء حوار مؤسسي منتظم أحادي المسار ودائم وعملي المنحى وشامل بشأن الأمن السيبراني. فعملية من هذا القبيل ستسمح بمشاركة أكثر تركيزا على تنفيذ القواعد وإجراء مناقشة أعمق بشأن كيفية تطبيق القانون الدولي. وستضمن أيضا تنسيقا أفضل وعملي المنحى (لا يوجد مثل هذا التنسيق داخل الفريق العامل المفتوح العضوية الحالي) بين المناقشة بشأن التنفيذ العملي للمكتسبات وبناء القدرات المستهدفة.

وتشير كندا إلى أن المناقشات الموضوعية بشأن برنامج عمل الجولة المقبلة من الحوار المؤسسي المنتظم جارية منذ عام 2021، بما في ذلك في سياق ورقة العمل المعممة في إطار هذا الفريق العامل المفتوح العضوية[3]. وتسلم كندا وتؤيد دعوات دول أعضاء أخرى إلى عملية أحادية المسار لمناقشة الأمن السيبراني في إطار الأمم المتحدة. والحالة هذه، تحذر كندا من إنشاء عملية موازية منفصلة للحوار المؤسسي المنتظم من شأنها أن تزاحم برنامج العمل الذي تؤيده 161 دولة عضوا من خلال قرار الجمعية العامة 16/78. فإن ذلك سيشكل ازدواجية لا مبرر لها ولا لزوم لها، وسيفرض على الدول الأعضاء تكاليف من العمالة والأموال لا لزوم لها.

وسيتقرر هيكل برنامج العمل وأداؤه من خلال مؤتمر دولي يعتمد فيه إعلان سياسي. ومن المتوخى أن يقوم مكتب شؤون نزع السلاح بتقديم الخدمات لبرنامج العمل بوصفه أمانته. وستعقد مؤتمرات استعراضية لتقديم التوجيه الاستراتيجي، ومناقشات عامة مفتوحة مماثلة لتلك التي تجري في إطار الآلية الحالية للفريق العامل المفتوح العضوية، واجتماعات أو أفرقة عاملة تقنية لتنسيق عناصر المناقشات المواضيعية ذات الصلة بالتصدي لتهديدات محددة (مثل تحديد أنشطة بناء القدرات الأكثر صلة بتنفيذ المعايير وتطبيق القانون الدولي وبرمجيات انتزاع الفدية).

وسيعزز برنامج العمل الاستثمارات في بناء القدرات والمساعدة التقنية باعتبارهما عنصرين أساسيين لتعزيز سلوك الدول المسؤول في الفضاء السيبراني ولتيسير التعاون فيما بين الدول. وسيرسي برنامج العمل مشاركة إقليمية من خلال التعاون مع المنظمات الإقليمية لتعزيز أوجه التآزر وتنسيق المبادرات.

ولن يكتفي برنامج العمل بمجرد إصدار تقارير الرئيس. بل سيبدي، فوق ذلك، تقدما مطردا وقابلا للقياس. وسيسعى إلى سد الفجوة القائمة في المساءلة بين المكتسبات والممارسة الفعلية من خلال ترسيخ الالتزامات والمشاركة في آليات الإبلاغ أو الاستعراض ليتسنى القيام بأفضل ما يمكن من أنشطة بناء القدرات لتعزيز سلوك الدول المسؤول في جميع أنحاء العالم.

(3) انظر: https://documents.unoda.org/wp-content/uploads/2021/11/Working-paper-on-the-proposal-for-a-Cyber-PoA.pdf.

الصين

[الأصل: بالصينية
29 نيسان/أبريل 2024]

ورقة تعرض وجهة نظر الصين بشأن الآلية الدائمة المقبلة

وفقا لقرار الجمعية العامة 237/78 المعنون "التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي"، يرد أدناه موقف الحكومة الصينية وآراؤها بشأن الآلية الدائمة المقبلة:

تمثل الآلية الدائمة المقبلة مسألة رئيسية لها تأثير كبير على التطور الطويل الأجل لعملية أمن المعلومات في الأمم المتحدة. وتؤيد الصين إنشاء آلية دائمة فريدة في المستقبل للأمن الإلكتروني في إطار الأمم المتحدة بمشاركة واسعة النطاق من جميع الأطراف. ويشكل التوصل إلى توافق في الآراء بشأن الآلية الدائمة المقبلة في إطار الفريق العامل المفتوح باب العضوية الخيار الوحيد لجميع الأطراف. ولا تؤيد الصين أي محاولة لإنشاء آلية دائمة خارج إطار الفريق العامل، وتعارض فكرة "البدء من نقطة الصفر" التي ستؤدي إلى انقسام في عملية أمن المعلومات في الأمم المتحدة وتغذي زخم المواجهة الجيوسياسية والمواجهة بين الكتل، وهو ما يتعارض مع مصالح جميع الدول الأعضاء.

وفيما يتعلق بهيكل الآلية الدائمة المقبلة ومهامها، ينبغي ألا يقتصر الأمر على تعزيز الإنجازات الهامة التي حققتها عملية أمن المعلومات في الأمم المتحدة على مدى السنوات الـ 26 الماضية والحفاظ عليها فحسب، بل ينبغي التطلع إلى المستقبل والسعي إلى تحقيق تطور طويل الأجل. ويمكن أن يتألف الهيكل من جزأين: الأول هو "النظر إلى الوراء"، مع التركيز على الامتثال للإطار الحالي المتفق عليه لسلوك الدول المسؤول في الفضاء الإلكتروني وتنفيذه، ولا سيما إثراء وتحسين خطط العمل لبناء القدرات. والثاني هو "التطلع إلى الأمام"، مع التركيز على مواكبة العصر في صياغة معايير جديدة، بما في ذلك تلك المتعلقة بأمن البيانات، وتعزيز صياغة الصكوك القانونية ذات الصلة، واقتراح خطط عمل جديدة لبناء القدرات. وقد طرحت الصين المبادرة العالمية بشأن أمن البيانات، التي تقترح حلولا عملية لمسألة أمن البيانات. وتقترح المبادرة ألا تطلب البلدان من مؤسساتها تخزين البيانات التي تم إنشاؤها أو الحصول عليها في الخارج داخل حدودها، واحترام السيادة والولاية القضائية وحقوق إدارة أمن البيانات في البلدان الأخرى، وألا تحصل مباشرة على البيانات الموجودة في بلدان أخرى عن طريق الشركات أو الأفراد دون إذن وفقا لقوانين تلك البلدان. وتطرح المبادرة أيضا مقترحات محددة بشأن حماية البنية التحتية الحيوية وأمن سلاسل التوريد. وقد عُممت هذه المبادرة رسميا بوصفها وثيقة من وثائق الجمعية العامة. والصين مستعدة للعمل مع جميع الأطراف لاستخدامها كمخطط للتعزيز المشترك لصياغة قواعد دولية بشأن الحوكمة السيبرانية والرقمية تعكس رغبات جميع الأطراف وتحترم مصالحها.

وينبغي للدول الأعضاء أن تقود الآلية الدائمة المقبلة، مع ضمان مشاركة أصحاب المصلحة المتعددين وفقا للطرائق الحالية للفريق العامل المفتوح باب العضوية. ويمكن عقد مؤتمر استعراض كل خمس سنوات، مع عقد جلستين أو ثلاث جلسات عامة في السنة. وينبغي أن تركز السنوات الثلاث الأولى من دورة الاستعراض على المناقشات الموضوعية واعتماد التقارير الإجرائية السنوية، مع اتخاذ القرارات بشأن المسائل التي تهم الدول الأعضاء على نطاق واسع بتوافق الآراء. وفي السنة الرابعة من دورة الاستعراض، يمكن الشروع في العملية التحضيرية للمؤتمر الاستعراضي وصياغة نص متداول باسم الرئيس. وفي السنة

الخامسة من دورة الاستعراض، سيكون التركيز الرئيسي على المناقشات الموضوعية بشأن النص المتداول للرئيس، وتلخيص توافق الآراء الموضوعي أو التفاوض بشأنه، والتخطيط للسنوات الخمس المقبلة.

والصين مستعدة لمواصلة المشاركة بنشاط في العمليات ذات الصلة والإسهام في إنشاء الآلية الدائمة المقبلة.

وتأمل الصين أن تنعكس الآراء المذكورة أعلاه في تقارير الأمين العام ذات الصلة.

كوبا

[الأصل: بالإسبانية
29 نيسان/أبريل 2024]

لتطور تكنولوجيا المعلومات والاتصالات تأثيرٌ متزايد على كافة مناحي المجتمع. وعلينا أن نمنع مساس هذا التقدّم بأمن الدول.

وتؤكد كوبا من جديد أن تكنولوجيا المعلومات والاتصالات ينبغي أن تستخدم في الأغراض السلمية وأن الدول يجب أن تتصرف على نحو مسؤول، بما يحقق الصالح العام للبشرية ومن أجل تعزيز التنمية المستدامة لجميع البلدان.

ونؤكد من جديد أن السبيل الوحيد لضمان عدم تحول الفضاء السيبراني إلى مسرح للعمليات العسكرية هو التعاون المشترك بين الدول كافة.

ومن الضروري لذلك أن يُعتمد، في إطار الجمعية العامة للأمم المتحدة، صكٌ دولي ملزِم قانوناً يكمل القانون الدولي المنطبق، ويوفر حلولاً للثغرات القانونية في مجال الأمن السيبراني، ويسمح بمعالجة فعالة للتحديات والتهديدات المتزايدة التي نواجهها.

والإطار المناسب لتحقيق ذلك هو الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها (2021-2025).

وهذا الفريق الذي يتسم بشموله وشفافيته ينبغي أن يُحترَم دوره في إرساء حوار حكومي دولي منتظم في ميدان أمن تكنولوجيا المعلومات والاتصالات وأمن استخدامها وأن يصان. ونحن نؤيد استمرار العمل بتلك الصيغة حتى يتسنى التوصل إلى نتائج ترتكز على توافق الآراء بين جميع الدول.

ويجب على جميع الدول أن تحترم المعايير الدولية القائمة في هذا المجال. وينبغي أن يكون الوصول إلى نظم المعلومات أو الاتصالات الخاصة بدولة أخرى متسقاً مع اتفاقات التعاون الدولي، استناداً إلى مبدأ موافقة الدولة المعنية. وينبغي أن يكون التبادل متوافقاً من حيث شكله ونطاقه مع تشريعات الدولة التي يراد الوصول إلى نظمها.

ويشكّل الاستخدام العدائي للاتصالات، الذي يكون غرضه المعلن أو المستتر هو تقويض النظام القانوني والسياسي للدول، انتهاكاً للمعايير المتفق عليها دولياً في هذا المجال كما يشكّل استخداماً غير قانوني وغير مسؤول لهذه الوسائل.

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

وفي المتوسط، جرى خلال عام 2023 وبشكل غير قانوني بث برامج مناوئة لكوبا بمعدل يزيد على 000 7 ساعة في الشهر وباستخدام 21 تردداً مختلفاً انطلاقاً من أراضي الولايات المتحدة، وهو ما يتعارض مع مقاصد ومبادئ ميثاق الأمم المتحدة والقانون الدولي وأحكام الاتحاد الدولي للاتصالات.

ولقد تسبَّب الحصار الاقتصادي والتجاري والمالي الذي تفرضه حكومة الولايات المتحدة على كوبا منذ أكثر من 60 عاماً في إلحاق أضرار جسيمة بالشعب الكوبي، بما في ذلك فيما يتعلق باستخدام تكنولوجيات المعلومات والاتصالات والتمتع بما توفره من مزايا.

ونحن نؤكد مجدداً رفضنا الشديد لفرض تدابير قسرية انفرادية تتعارض مع القانون الدولي وتضع عقبات تعترض المساعدة والتعاون ونقل التكنولوجيا.

ويُعترف، في منطقتنا، بإمكانات تكنولوجيا المعلومات والاتصالات من حيث قدرتها على توفير حلول جديدة لمواجهة تحديات التنمية وتعزيز النمو الاقتصادي المطرد والعادل والشامل للجميع، فضلا عن تحقيق خطة التنمية المستدامة لعام 2030.

وإضافة إلى ذلك، تبرُز الحاجة إلى تعزيز بيئة لتكنولوجيا المعلومات والاتصالات تكون منفتحة وآمنة ومستقرة وميسّرة وسلمية، على النحو المنصوص عليه في الإعلان الصادر عن مؤتمر القمة الثامن لجماعة دول أمريكا اللاتينية ومنطقة البحر الكاريبي الذي انعقد في كنغستاون في عام 2024.

وتؤكد كوبا مجدداً الأهمية الحاسمة للتعاون الدولي في مواجهة مخاطر إساءة استخدام تكنولوجيات المعلومات والاتصالات.

تشيكيا

[الأصل: بالإنكليزية
30 نيسان/أبريل 2024]

تشيكيا ملتزمة التزاما تاما بأن تدفع قُدما بالنقاش العالمي حول الأمن السيبراني في الأمم المتحدة، وهي ممتنة للتقدم الذي أحرزه حتى الآن كل من الأفرقة العاملة المفتوحة العضوية وأفرقة الخبراء الحكوميين.

ومن الإنجازات الرئيسية للفريق العامل المفتوح العضوية وفريق الخبراء الحكوميين قيامهما بوضع وتوحيد إطار لسلوك الدول المسؤول في الفضاء السيبراني.

وفي هذا السياق، ترى تشيكيا أن تنفيذ إطار سلوك الدول المسؤول في الفضاء السيبراني ينبغي أن يكون الموضوع الرئيسي للجولة المقبلة من الحوار المؤسسي. وعلاوة على ذلك، تؤيد تشيكيا إنشاء آلية دائمة أحادية المسار وشاملة وعملية المنحى تحت رعاية الأمم المتحدة عند اختتام أعمال الفريق العامل المفتوح العضوية الحالي في عام 2025.

وفي الوقت نفسه، نرى أنه لكي تكون الجولة المقبلة من الحوار المؤسسي بالفعل في مصلحتنا جميعا، ينبغي مواصلة النقاش بشأن شكلها العملي في إطار الفريق العامل المفتوح العضوية الحالي. وليس أمامنا اليوم، كمجتمع دولي، سوى أكثر قليلا من عام واحد لإجراء هذه النقاش.

وفيما يتعلق بالنقاش الدائر ضمن الفريق العامل المفتوح العضوية، تود تشيكيا أن توجه انتباهكم إلى أن الاقتراح الذي حظي بأكبر قدر من التطوير والمناقشة والتوافق أيضا لإجراء جولة من الحوار المؤسسي هو برنامج العمل للارتقاء بسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات.

وعلى النقيض من ذلك، نرى أن القرار 237/78 المتعلق بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي لا يبني على النهج التدريجي وتوافق الآراء اللذين تم التوصل إليهما في الفريق العامل المفتوح العضوية في السنوات الأخيرة. ويبدو أن القرار يعطي الأولوية لمصالح مجموعة ضيقة من الدول.

وقد ظل النقاش حول برنامج العمل متواصلا منذ عام 2020، وشاركت فيه تشيكيا بنشاط. ونحن ندرك قيمة النقاش الجاري بشأن برنامج العمل داخل الفريق العامل المفتوح العضوية في تحديد اتجاه برنامج العمل وفي توضيح عدد من النقاط التي يحتمل أن تكون مثيرة للجدل. ونرى أنه من المهم مواصلة هذا النقاش لتحديد مضمون وطرائق عمل الآلية التي سيتم استحداثها. وفي ضوء ما سبق، نقترح تنظيم اجتماعات بين الدورات ودورات مخصصة للفريق العامل المفتوح العضوية في عامي 2024 و 2025 للتركيز على جوانب معينة من برنامج العمل، بما في ذلك الآثار المترتبة في الميزانية.

وبالإضافة إلى ذلك، تود تشيكيا أن توجه الانتباه إلى جوانب معينة من برنامج العمل انبثقت عن المناقشة المتعلقة ببرنامج العمل والتي تعتبرها تشيكيا أهم مزايا برنامج العمل:

- برنامج العمل سيحقق الاستقرار المؤسسي للنقاش الدولي المتعلق بتكنولوجيات المعلومات والاتصالات. وسيكون برنامج العمل إطارا مؤسسيا دائما تقوم عليه جميع النقاشات المتصلة بالفضاء السيبراني التي تجري في إطار الأمم المتحدة. ومن شأن ذلك أن يحول دون ظهور الحاجة إلى إجراء مناقشات دورية بشأن إنشاء فريق عامل جديد يكرّس لاستخدام تكنولوجيات المعلومات والاتصالات.

- سيدعم برنامج العمل تنفيذ إطار سلوك الدول المسؤول وسيسمح بإجراء مزيد من المناقشات بشأن تطوير الإطار، إذا لزم الأمر.

- سيؤدي برنامج العمل إلى تفعيل مبادئ بناء القدرات في إطار أهدافه العملية المنحى وتعزيز التنفيذ في إطار مشاريع بناء القدرات السيبرانية. ويمكن لبرنامج العمل أن يعزز الجهود القائمة والمحتملة لبناء القدرات، وأن يزيد من التعريف بها ويحسن تنسيقها. فعلى سبيل المثال، قد يكون من المفيد استكشاف إمكانية التنسيق مع أنشطة بناء القدرات السيبرانية المضطلع بها في أماكن أخرى، من قبيل الاتحاد الدولي للاتصالات.

- سييسر برنامج العمل المشاركة والتعاون الهادفين مع الجهات غير الحكومية صاحبة المصلحة. ومن شأن إشراك القطاع الخاص والأوساط الأكاديمية والمجتمع المدني أن يقدم خبرة قيّمة بخصوص مسائل من قبيل تقييم التهديدات، وتنفيذ المعايير، بما في ذلك قياس التقدم المحرز.

- برنامج العمل مصمم ليكون بمثابة إطار شامل يمكن أن يشمل مبادرات أخرى تمت مناقشتها أو الاتفاق عليها داخل الفريق العامل المفتوح العضوية.

وفيما يتعلق بالطرائق المحددة، تحبذ تشيكيا فكرة عقد دورات عامة سنوية واجتماعات للأفرقة العاملة التقنية المتخصصة في الفترة الممتدة بين الدورات.

- عملية إنشاء فريق عامل معين وإنهائه ستكون برمتها من اختصاص الدول.
- سيقتصر نطاق هذه المناقشات التقنية وأعمالها التحضيرية على المواضيع المحددة في الجلسات العامة. وسيحضر هذه المناقشات، على سبيل المثال، عدد محدود من الخبراء من الحكومات، وعند الاقتضاء جهات أخرى من الجهات صاحبة المصلحة، مثل الأوساط الأكاديمية. وعلى وجه الخصوص، يمكن أن تركز هذه الأفرقة العاملة على مواضيع من قبيل حماية البنية التحتية الحيوية، والاستجابة للحوادث السيبرانية، وإمكانية تطبيق أحكام مخصوصة على قضايا محددة بموجب القانون الدولي في الفضاء السيبراني.
- إذا تم ذلك بشكل جيد، نعتقد أن وجود أفرقة عاملة تقنية لفترات ما بين الدورات يمكن أن يزيد من كفاءة عملنا إلى حد بعيد وأن يخفف أيضا من أعباء فرادى الوفود.
- قد يكون من المفيد النظر في ألا تُعقد في نيويورك كل اجتماعات الأفرقة العاملة لما بين الدورات، وأن تُناقَش إمكانية عقدها في أماكن أخرى أيضا.

الدانمرك

[الأصل: بالإنكليزية
1 أيار/مايو 2024]

تعتبر الدانمرك تنفيذ إطار الأمم المتحدة لسلوك الدول المسؤول في استخدام تكنولوجيا المعلومات والاتصالات أمرا محوريا لضمان فضاء سيبراني عالمي ومفتوح ومستقر وآمن. فالمجتمع الدولي يعترف بأن القانون الدولي القائم وميثاق الأمم المتحدة في مجمله ينطبقان في بيئة تكنولوجيا المعلومات والاتصالات، والدانمرك ملتزمة بتنفيذ هذا الإطار فيما يتعلق بالفضاء السيبراني.

وقد أُحرز تقدم كبير على مدى العشرين سنة الماضية في وضع إطار موحد لسلوك الدول المسؤول في الفضاء السيبراني، بما في ذلك تطبيق القانون الدولي والمعايير الطوعية وبناء القدرات وتدابير بناء الثقة. وقد أقرت الجمعية العامة الإطار بتوافق الآراء مرات عديدة، كان آخرها في التقرير المرحلي السنوي لعام 2023 الصادر بتوافق الآراء عن الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025.

والدانمرك، إلى جانب الاتحاد الأوروبي، ترى أن أجزاء من القرار 237/78 المتعلق بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، الذي اعتمدته الجمعية العامة في 22 كانون الأول/ديسمبر 2023، تستند إلى نص غير توافقي. وبشكل أكثر تحديدا، فإن الفقرة السادسة عشرة من الديباجة والفقرة 5 من المنطوق تستندان إلى مقترحات لا يؤيدها سوى مجموعة محدودة من الدول.

ويساور الدانمرك القلق من أن يؤدي ذلك إلى إعادة تفسير الوثائق التوافقية القائمة. ولذلك، لم تكن الدانمرك في وضع يتيح لها أن تؤيد القرار 237/78.

فيما يتعلق بالطلب المقدم عملا بالفقرة 8 من منطوق القرار

لقد دعت الأمم المتحدة مرارا إلى إنشاء آلية دائمة تابعة للأمم المتحدة تُعنى بالقضايا السيبرانية في سياق الأمن الدولي. وباتخاذ الجمعية العامة في تشرين الأول/أكتوبر 2023 قرار وضع برنامج عمل للارتقاء بسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي، نكون قد استجبنا للدعوة المذكورة أعلاه.

وقد أُحرز تقدم كبير في المناقشات بشأن الآلية المقبلة، وتود الدانمرك أن تعرب عن الآراء الإضافية التالية فيما يتعلق بالجولة المقبلة من الحوار المؤسسي المنتظم.

ينبغي أن يركز هذا الحوار المؤسسي على دعم تنفيذ الإطار المعياري، على نحو ما أوضحه أيضا الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي للفترة 2019-2021، الذي خلص إلى أن الجولة المقبلة من الحوار المؤسسي المنتظم "ينبغي أن تتخذ شكل إجراء عملي المنحى ومحدد الأهداف ومستند إلى النتائج السابقة، وأن تكون شاملة للجميع، وشفافة، ومدفوعة بتوافق الآراء، وقائمة على النتائج"[4].

وينبغي لبرنامج العمل أن يوفر آلية دائمة ومؤسسية لمتابعة تنفيذ المعايير المتفق عليها، ولدعم وتعزيز بناء القدرات، وتقديم التوصيات وتحديثها بانتظام. وفي الوقت نفسه، ينبغي أن يكون برنامج العمل مرنا وأن يسمح بمواصلة تطوير الإطار، استنادا إلى الدروس المستفادة أثناء تنفيذ الالتزامات القائمة.

وترى الدانمرك أنه من الأهمية بمكان الاعتراف بأن جميع أصحاب المصلحة لهم دور هادف في تشكيل مستقبل الأمن السيبراني. وحتى يكون الحوار شاملا، يلزم السماح للجهات المعنية صاحبة المصلحة، مثل الشركات والمنظمات غير الحكومية والأوساط الأكاديمية، بأن تشارك بصفة رسمية في المشاورات وأن تعرض وجهات نظرها باستمرار. وهذا يدل على الالتزام بتسخير الحكمة الجماعية المتأتية من تنوُّع وجهات النظر. وهذه الشمولية أمر حيوي لخلق حوار فعال وشامل يعالج التحديات المتعددة الأوجه للأمن السيبراني.

ويمكن لبرنامج العمل أن يعقد اجتماعات سنوية رسمية وأن يسمح بعقد اجتماعات تقنية وأفرقة عاملة تركز على الجوانب ذات الصلة على مدار السنة. وينبغي للآلية المقبلة أن تعقد مؤتمرات استعراضية دورية لاستعراض إطار سلوك الدول المسؤول، وتحديث الإطار حسب الاقتضاء، وتوفير التوجيه الاستراتيجي لعمل الآلية.

وفي الجزء المتبقي من دورة الفريق العامل المفتوح العضوية الحالي، ينبغي تكريس الوقت والجهد لمواصلة التوسع في جوانب من برنامج العمل. ولضمان انتقال سلس إلى برنامج العمل، من المهم مناقشة الآثار المترتبة في الميزانية على آلية دائمة وتحديد الجهات الفاعلة المعنية ضمن الأمم المتحدة للاضطلاع بهذه الوظائف في المستقبل.

(4) A/75/816، الفقرة 74.

مصر

[الأصل: بالإنكليزية
26 شباط/فبراير 2024]

أولا - مقدمة

1 - تتقاسم الدول الأعضاء الشواغل الدولية المتزايدة إزاء انتشار الاستخدامات الخبيثة لتكنولوجيات المعلومات والاتصالات وإفراط عدد من الدول في تطوير قدرات تكنولوجيا المعلومات والاتصالات لأغراض لا تنسجم مع القانون الدولي ومع أهداف الحفاظ على الاستقرار والأمن الدوليين، ويمكن أن تؤثر سلبا على سلامة البنية التحتية لدول أخرى، بما يضر بأمن هذه الدول في المجالين المدني والعسكري.

2 - وقد أحرزت الأمم المتحدة بالفعل تقدما نحو معالجة هذه الشواغل من خلال تقييمات وتوصيات أفرقة الخبراء الحكوميين للأعوام 2010 و 2013 و 2015 و 2021، وكذلك تقييمات وتوصيات الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي[5]، مما سمح بإنشاء إطار ذي طابع تراكمي ومتطور لسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات تمت بلورته بفضل تلك العمليات.

3 - وقد دُعيت الدول الأعضاء إلى الاسترشاد في استخدامها لتكنولوجيات المعلومات والاتصالات بتقارير أفرقة الخبراء الحكوميين للأعوام 2010 و 2013 و 2015 و 2021 وتقرير الفريق العامل المفتوح العضوية لعام 2021، وكذلك بالتقريرين المرحليين السنويين الأول والثاني للفريق العامل المفتوح العضوية الحالي المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025. وعلاوة على ذلك، شدد هذا الإطار المتفق عليه على أن القانون الدولي، ولا سيما ميثاق الأمم المتحدة، ينطبق في سياق صون السلام والاستقرار ولا غنى عنه من أجل المحافظة عليهما، وتعزيز بيئة منفتحة وآمنة ومستقرة وميسّرة وسلمية لتكنولوجيا المعلومات والاتصالات.

4 - ويمكن للإطار القائم للمعايير والقواعد والمبادئ التي تضبط سلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات أن يحد من المخاطر التي تهدد السلام والأمن والاستقرار على الصعيد الدولي دون تقييد أو حظر الأعمال التي تتسق مع القانون الدولي.

5 - وقد طرحت مصر وفرنسا في عام 2020 مقترحا لبرنامج عمل للأمم المتحدة للارتقاء بسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي، ثم طُور المقترح منذ ذلك الحين على يد مجموعة من الدول من عدة أقاليم، كما هو موضح في التقارير النهائية لأفرقة الخبراء الحكوميين وتقرير عام 2021 للفريق العامل المفتوح العضوية، بالإضافة إلى التقريرين المرحليين السنويين الأول والثاني للفريق العامل المفتوح العضوية الحالي.

6 - وأصدر الأمين العام تقريرا (A/78/76) فيه تجميع لآراء الدول بشأن نطاق برنامج العمل وهيكله ومبادئه ومضمونه والأعمال التحضيرية وطرائق إنشائه وطرائق.

(5) انظر A/65/201 و A/68/98 و A/70/174 و A/75/816 و A/76/135.

7 - ويجب أن تستند أي آلية توضع في المستقبل بشأن الحوار المؤسسي المنتظم إلى المكتسبات والإطار القائم المتفق عليه الذي أقرته الجمعية العامة بتوافق الآراء.

8 - وينبغي إنشاء الآلية أو المنصة الجديدة بعد انتهاء ولاية الفريق العامل المفتوح العضوية الحالي بعد عام 2025. وهذا يعني تفادي أي احتمال لازدواجية الجهود أو لوجود مسارات موازية. وينبغي أن تكون الآلية "وحدة متكاملة" ومنصة شاملة تحت رعاية الأمم المتحدة، تعالج المسائل المتصلة بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وترتقي بسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات.

9 - واتفقت الدول الأعضاء من حيث المبدأ على أن تكون آلية الحوار المؤسسي المنتظم أحادثة المسار، تقودها الدول، ودائمة، وشاملة، وشفافة، ومرنة[6].

ثانيا - أهداف ونطاق آلية الأمم المتحدة المقبلة للحوار المؤسسي المنتظم

10 - تشكيل منبر للحوار المؤسسي المنتظم يسمح بمشاركة جميع الدول الأعضاء في عملية أحادية المسار ودائمة وشاملة وشفافة وعملية المنحى وقائمة على النتائج ومدفوعة بتوافق الآراء تستند إلى الإطار الحالي.

11 - تعزيز بيئة لتكنولوجيا المعلومات والاتصالات تكون منفتحة وآمنة ومستقرة ويمكن الوصول إليها وسلمية وقابلة للتشغيل البيني.

12 - منع نشوب النزاعات الناشئة عن استخدام تكنولوجيات المعلومات والاتصالات والسعي إلى تسوية المنازعات ذات الصلة بالوسائل السلمية.

13 - ترسيخ الأدوات السيبرانية القائمة (دليل جهات الاتصال وجميع المقترحات الأخرى التي سيعتمدها الفريق العامل المفتوح العضوية) بهدف الحفاظ على الأداء والاستعراض الفعالين، حسب الاقتضاء.

14 - إعداد إرشادات ملموسة لدعم الدول الأعضاء في تنفيذها للمعايير والقواعد والمبادئ المتفق عليها، بما في ذلك عن طريق تشجيع التعاون والمساعدة الدوليين.

15 - وينبغي أن يركز نطاق الآلية على الركائز الثلاث التالية:

(أ) **تنفيذ النتائج الحالية المتفق عليها** - إجراء تقييم دوري لتنفيذ الدول الأعضاء للإطار المتفق عليه من خلال استعراض تقارير التنفيذ الوطنية الطوعية التي ينبغي أن تتبع نموذجا موحدا متفقا عليه للإبلاغ؛

(ب) **تطوير الإطار الحالي** - تحديد الثغرات والتحديات المتنوعة التي تواجهها الدول الأعضاء أثناء تنفيذها للإطار والترويج للتوصيات القابلة للتنفيذ ذات الصلة بهدف التصدي لتلك التحديات، فضلا عن استئناف المداولات حول القضايا المفاهيمية، مثل انطباق قانون الأعمال العمدية أو الحاجة إلى وضع قواعد جديدة والتزامات ملزمة قانونا في هذا المجال؛

(ج) **تعزيز بناء القدرات** - اتخاذ خطوات عملية لتعزيز التعاون الدولي وإجراء تقييمات دورية لمعرفة ما إذا كان يتعين اتخاذ إجراءات إضافية للتصدي للتحديات الحالية والناشئة، مع مراعاة سرعة تطوّر

(6) A/78/265، الفقرة 55.

بيئة تكنولوجيا المعلومات والاتصالات؛ وتبادل المعلومات بشأن أفضل الممارسات التي يمكن تنفيذها على الصعد الوطني والإقليمي والدولي (بما في ذلك الأطر التشريعية والإدارية والتدابير المتخذة لحماية البنية التحتية الحيوية)؛ وتقديم دعم ملموس لبناء القدرات استنادا إلى تقييم احتياجات الدولة المستفيدة ووفقا لمبادئ بناء القدرات الواردة في الوثيقة A/76/135. وينبغي النظر في إنشاء آلية تمويل مكرسة للأنشطة ذات الصلة، بما في ذلك إمكانية الاعتماد على كل من الأدوات القائمة والأدوات الجديدة، مثل الصندوق الاستئماني المتعدد المانحين للأمن السيبراني التابع للبنك الدولي.

ثالثا - إنشاء الآلية المستقبلية للحوار المؤسسي المنتظم

16 - إن الآراء والمساهمات المقدّمة من الدول الأعضاء في إطار الفريق العامل المفتوح العضوية الحالي بشأن برنامج العمل المقترح وتقريري الأمين العام المقدّمين عملا بقراري الجمعية العامة 380/77 و 237/87، فضلا عن التوصيات الممكنة ذات الصلة الواردة في تقارير الفريق العامل المفتوح العضوية، ستشكل ركيزة إنشاء الآلية من حيث نطاقها وهيكلها وطرائق عملها.

17 - وينبغي للدول الأعضاء أن تواصل مشاركتها النشطة في الفريق العامل المفتوح العضوية الحالي المنشأ عملا بقرار الجمعية العامة 240/75 بغية إعداد تقارير بتوافق الآراء، بما في ذلك التوصيات المتعلقة بإنشاء آلية مستقبلية للحوار المؤسسي المنتظم.

18 - وينبغي زيادة تفصيل الآلية وتطويرها في إطار الفريق العامل المفتوح العضوية الحالي بطريقة تتجنب أي ازدواجية في الجهود أو إنشاء عمليات متنافسة وتحافظ على الروح التوافقية أثناء تناول الجوانب المتصلة بالأمن الدولي لاستخدام تكنولوجيات المعلومات والاتصالات داخل الأمم المتحدة.

19 - وستوضع الآلية بعد انتهاء ولاية الفريق العامل المفتوح العضوية الحالي في عام 2025 باتباع توصيات التقرير النهائي للفريق العامل المفتوح العضوية الحالي، بينما يمكن النظر في إمكانية إرساء حوار مؤسسي منتظم في المستقبل من خلال قرار توافقي تتخذه الجمعية العامة بناء على مشاورات وأعمال تحضيرية شاملة وشفافة. ويمكن أن تتفق الدول الأعضاء في إطار الفريق العامل المفتوح العضوية الحالي على إنشاء الآلية من خلال إعلان سياسي يمكن إقراره بقرار تتخذه الجمعية العامة، بما في ذلك طرائق العمل المقترحة للآلية. ويمكن أن تتضمن الوثيقة الختامية لمؤتمر القمة المعني بالمستقبل إشارة إلى اتفاق أولي بشأن هذه المسألة.

رابعا - الهيكل والطرائق الممكنة

الاجتماعات الدورية

20 - إن الآلية، وهي يمكن أن تتخذ شكل برنامج عمل، ينبغي أن تعقد كل ست سنوات مؤتمر استعراض يركز على ما يلي:

(أ) بحث واستعراض تنفيذ الآلية، وتحديد أولويات العمل الرئيسية للسنوات التالية، ومن ثَم اعتماد خطة عمل للاجتماعات اللاحقة؛

(ب) النظر فيما إذا كان ينبغي وضع معايير أو قواعد أو مبادئ إضافية أو التزامات ملزمة على أساس توافق الآراء لتحديث الإطار.

21 - وينبغي للآلية أن تعقد اجتماعات منتظمة كل سنتين لتنفيذ خطة العمل التي يعتمدها مؤتمر الاستعراض ولمتابعة تنفيذ الدول الأعضاء للمعايير والقواعد والمبادئ المتفق عليها من خلال استعراض تقارير التنفيذ الوطنية الطوعية التي تعدّها.

22 - ويعقد رئيس كل دورة اجتماعات استشارية تحضيرية قبل كل مؤتمر من مؤتمرات الاستعراض وقبل كل اجتماع من اجتماعات المتابعة التي تُعقد كل سنتين.

23 - والآلية المتفق عليها يمكن أن تقرر، بتوافق الآراء، عقد اجتماعات بين الدورات أو إنشاء أفرقة عاملة غير رسمية للتركيز على مسائل محددة ذات صلة، بما في ذلك انطباق القانون الدولي ووضع معايير وقواعد ومبادئ جديدة، فضلا عن التزامات أو صكوك ملزمة قانونا، حسب الاقتضاء.

التقارير

24 - في إطار الآلية المتفق عليها، ستُشجَّع الدول الأعضاء على تقديم تقارير التنفيذ الوطنية الطوعية التي تعدها مرة كل سنتين على أساس التناوب، بشرط تقديم تقرير واحد على الأقل كل ثلاث دورات (أي كل ست سنوات). ويمكن الاسترشاد في هذه العملية بنموذج الدراسة الاستقصائية الوطنية لتنفيذ توصيات الأمم المتحدة بشأن استخدام الدول المسؤول لتكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي. وقد ترغب الدول الأعضاء أيضا في أن تدرج في تقارير التنفيذ الوطنية الطوعية التي تعدّها فرعًا يعرض تفاصيل أولوياتها واحتياجاتها في مجال بناء القدرات.

25 - ويجب أن يعتمد كل اجتماع من الاجتماعات التي تُعقد مرة كل سنتين وكل مؤتمر من مؤتمرات الاستعراض تقريرا نهائيا بتوافق الآراء، بما في ذلك وثيقة ختامية تُقدَّم أثناء الدورة التالية للجنة الأولى لكي تنظر فيها وتقرّها.

اتخاذ القرارات

26 - يعتمد برنامج العمل قراراته بشأن المسائل الموضوعية بتوافق الآراء.

الأمانة

27 - ينبغي لمكتب الأمم المتحدة لشؤون نزع السلاح أن يقدم خدمات الأمانة للآلية.

مشاركة الجهات صاحبة المصلحة

28 - الآلية عملية حكومية دولية يكون فيها التفاوض واتخاذ القرارات من الصلاحيات الحصرية للدول الأعضاء.

29 - وستلتزم الآلية بالتفاعل مع الجهات المعنية صاحبة المصلحة بطريقة منهجية ومستدامة وموضوعية.

30 - والمنظمات غير الحكومية ذات الصلة التي تتمتع بالمركز الاستشاري لدى المجلس الاقتصادي والاجتماعي وفقا لقرار المجلس 31/1996 تبلغ الأمانة برغبتها في المشاركة في أعمال الآلية.

31 - ينبغي أيضا للمنظمات غير الحكومية الأخرى المهتمة ذات الصلة بمجال عمل الآلية وغرضها والمختصة فيهما أن تبلغ الأمانة باهتمامها بالمشاركة عن طريق تقديم معلومات عن غرض المنظمة

وبرامجها وأنشـــطتها في المجالات ذات الصـــلة بمجال عمل الآلية. وتدعى هذه المنظمات بناء على تلك المعلومات إلى المشاركة، على أساس عدم الاعتراض، بصفة مراقب في الجلسات الرسمية للآلية.

32 - ويُسمح للجهات صاحبة المصلحة المعتمدة بأن تحضر الاجتماعات الرسمية لبرنامج العمل، وبأن تدلي ببيانات شفوية خلال جلسة مكرسة للجهات صاحبة المصلحة، وتقديم مدخلات خطية. وتشجَّع الدول الأعضاء على استخدام آلية عدم الاعتراض بحصافة، مع مراعاة مبدأ استيعاب الجميع.

33 - وفي حالة وجود اعتراض على منظمة غير حكومية، تبلغ الدولة العضـــو المعترضـــة رئيس الآلية باعتراضـــها وتوافيه، طوعا، بالاعتبارات العامة التي تســـتند إليها في اعتراضـــاتها. ويطلع الرئيس أي دولة عضو، بناء على طلبها، على أي معلومات يتلقّاها.

34 - وينظم الرئيس اجتماعات تشاورية غير رسمية مع الجهات صاحبة المصلحة خلال فترة ما بين الدورات.

35 - ويمكن للآلية أن تيســـر التنســـيق مع المبادرات الإقليمية ودون الإقليمية المعنية، بما في ذلك من خلال تيسير إمكانية مشاركتها ومساهمتها.

إستونيا

[الأصل: بالإنكليزية
30 نيسان/أبريل 2024]

وفقا للتكليف الوارد في قرار الجمعية العامة 237/78، تود إســـتونيا أن تدلي بموقف وطني إزاء الجولة المقبلة من الحوار المؤسسي المنتظم بشأن أمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها.

وخلال الســـنوات الأخيرة، تواصـــلت حدة التهديدات المتصـــلة باســـتخدام تكنولوجيات المعلومات والاتصـــالات في ســـياق الأمن الدولي، وشـــهدت تطوّرا كبيرا في ظل البيئة الجيوســـياســـية الصـــعبة الحالية. ويتسبب تنامي التهديدات المتصلة باستخدام تكنولوجيات المعلومات والاتصالات في إثارة تحديات متزايدة لها آثار سلبية في التنمية الاقتصادية والاجتماعية، فضلا عما لها من تداعيات على الاستقرار الوطني والدولي. ولا تزال هذه التداعيات في صـــدارة المناقشـــات المتعددة الأطراف، كما يتضـــح من عمل فريق الخبراء الحكوميين والفريق العامل المفتوح العضوية.

وفي أعقاب التأييد الواسع الذي قدمته مجموعة من البلدان من مختلف الأقاليم لوضع برنامج عمل، نؤيد برنامج العمل باعتباره آلية مؤســـسية دائمة في إطار اللجنة الأولى تركز على تنفيذ الإطار المتفق عليه لسلوك الدول المسؤول في الفضاء السيبراني، مع السماح أيضا بمواصلة تطوير الإطار، حسب الاقتضاء. ونحن نرى أن هذا الحوار المؤسسي المنتظم من شأنه أن يسهم في التخفيف من حدة التوترات، فيحول بذلك دون نشوب النزاعات ويعزز استخدامها للأغراض السلمية.

وهذا الموقف الوطني هو تحديث لمســـاهمة إســـتونيا الوطنية المدرجة في تقرير الأمين العام عن برنامج العمل (A/78/76) الذي يعتمد على جملة أمور منها التقدم المكرس في قرار الجمعية العامة 16/78 والمناقشات التي جرت في إطار الفريق العامل المفتوح العضوية للفترة 2021-2025.

1 - **ينبغي أن يســـتند برنامج العمل إلى المكتســـبات القائمة وإلى إطار ســـلوك الدول المســـؤول، مع التركيز على استخدام الدول لتكنولوجيات المعلومات والاتصالات في سياق السلام والأمن الدوليين -**

فإستونيا ترى أن تكنولوجيات المعلومات والاتصالات يجب أن تُستخدم بطريقة تتسق مع أهداف الحفاظ على الاستقرار والأمن الدوليين ووفقا للمكتسبات المتفق عليها وإطار سلوك الدول المسؤول. ونحن نشدد على أن الدول الأعضاء ينبغي لها أن تسترشد في استخدامها لتكنولوجيات المعلومات والاتصالات بتقارير أفرقة الخبراء الحكوميين للأعوام 2010 و 2013 و 2015 و 2021 وبتقرير عام 2021 للفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي. وينبغي أن تُقام آلية برنامج العمل على هذه الركائز وأن تسترشد بهدف الحفاظ على بيئة منفتحة ومستقرة وآمنة وميسرة وسلميّة لتكنولوجيا المعلومات والاتصالات. وترى إستونيا أن عددا من المبادرات القائمة أو المقترحة، مثل الدليل العالمي لجهات الاتصال، كفيلة بتقديم دعم مفيد ليعمل برنامج العمل بفعالية.

2 - **ينبغي أن يكون برنامج العمل شكلا محايدا يوفر الاستقرار المؤسسي** - فمن وجهة نظر دولة صغيرة، من الضروري أن تتسم العمليات الأخرى المتصلة بالمناقشات بشأن استخدام الدول لتكنولوجيات المعلومات والاتصالات بالوضوح والاستقرار المؤسسي. ولهذا، تدعو إستونيا إلى إنشاء هيكل دائم واحد لمواصلة مناقشات الفريق العامل المفتوح العضوية، بعد انتهاء ولاية الفريق العامل المفتوح العضوية الحالي المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025. ونحن نؤيد مواصلة المناقشات بشأن هيكل برنامج العمل وطرائقه وجدوله الزمني بوصفه آلية للارتقاء بسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات، مع مراعاة آراء جميع الدول الأعضاء. وتؤيد إستونيا خيار إنشاء الآلية بعقد مؤتمر دولي، في موعد أقصاه عام 2026، على النحو المتفق عليه في قرار الجمعية العامة 37/77. وتعتقد إستونيا أنه بفضل الشكل المقترح لبرنامج العمل، لن تحتاج الجمعية العامة بعد ذلك إلى مناقشة إنشاء عمليات جديدة متصلة بالفضاء السيبراني كل سنتين أو ثلاث أو أربع سنوات. ونحن نأمل أن تنظر الدول الأعضاء إلى إطار برنامج العمل باعتباره إطارا مفيدا ومحايدا وأن يُغني عن أي عمليات موازية.

3 - **ينبغي أن يوفر برنامج العمل إطارا شاملا لتناول مختلف المواضيع المقترحة خلال دورات الفريق العامل المفتوح العضوية بطريقة شاملة** - فنحن نرحب بالاهتمام المتزايد الذي توليه الدول الأعضاء للإسهام في مختلف المواضيع التي يتم التركيز عليها خلال المناقشات التي تجري في دورات الفريق العامل المفتوح العضوية. وقد كانت مناقشات الفريق العامل الحالية كثيفة، حيث طُرحت مجموعة متنوعة من الأفكار التي اقترحتها العديد من الدول الأعضاء. ونحن نعتقد أن إطار برنامج العمل يمكن أن يوفر منبرا "تتردد" عليه الدول الأعضاء لإثارة المسائل المتعلقة بتكنولوجيات المعلومات والاتصالات والسلام والأمن الدوليين. ولذلك يمكن أن يوفر برنامج العمل إطارا شاملا لطرح هذه الأفكار وتحليلها بمزيد من الدقة.

4 - **ينبغي أن يتضمن برنامج العمل أيضا طرائق واضحة وشفافة لإشراك العديد من الأطراف المعنية بشكل ملموس من أجل الاستفادة أكثر من خبراتها ومعارفها** - فإشراك أصحاب المصلحة المتعددين سيكون فيه دعم للدول الأعضاء في تنفيذ إطار سلوك الدول المسؤول وتصميم وتنفيذ جهود بناء القدرات القائمة على الاحتياجات لزيادة المرونة السيبرانية على الصعيد العالمي. وبالمثل، يمكن لبرنامج العمل أيضا أن يعزز المشاركة الإقليمية من خلال التعاون مع المنظمات الإقليمية والمواضيعية للاستفادة من المبادرات القائمة ذات الصلة والبناء عليها.

5 - **ينبغي أن يتيح برنامج العمل شكلا أكثر مرونة، ولكن أكثر تركيزا، لمواصلة المناقشات بشأن إطار سلوك الدول المسؤول** - وتود إستونيا أن تشدد على أن تصميم إطار برنامج العمل ينبغي أن يراعي

أيضـــا التحديات المتعلقة بمحدودية قدرات الدول الصـــغيرة، ولهذا ينبغي أن يقوم على توقعات معقولة فيما يتعلق بعبء العمل المتوقع:

(أ) نقترح أن تشـمل عناصـر آلية برنامج العمل عقد جلسـات عامة سـنوية لتناول مواضـيع تندرج ضمن الركائز الأساسية لإطار سلوك الدول المسؤول؛

(ب) نؤيد أيضـا إجراء مناقشـة مركزة في شكل افرقة عاملة مفتوحة لجميع المشاركين المهتمين وتتناول، على سبيل المثال لا الحصر، التهديدات وبناء القدرات وبناء الثقة والمعايير، والقانون الدولي أيضـا. ويتمثل خيار آخر في أن تركّز هذه الأفرقة العاملة على محاور ذات مواضيع أدق، مثل حماية البنية التحتية الحيوية. وينبغي أن تكون المشـاركة في الأفرقة العاملة طوعية، وأن تقرر الدول إنشـاء مسـارات العمل هذه في جلسات عامة سنوية؛

(ج) نؤيد أيضـا تنظيم مؤتمرات اسـتعراض (كل أربع سـنوات، على سـبيل المثال) تسـمح للمشـاركين بتقييم التقدم المحرز والنظر في أي تعديلات أخرى يمكن إدخالها على الولاية وعلى تنظيم العمل أو برنامج العمل.

6 - **ينبغي أن يوفر برنامج العمل إطارا شاملا للجميع لإجراء مناقشات بشأن القانون الدولي، ضمن مواضيع أخرى** - فإستونيا ترحب بتزايد نشاط المناقشات الموضوعية الجارية بشأن القانون الدولي وكيفية تطبيقه على اسـتخدام الدول لتكنولوجيات المعلومات والاتصـالات. وسـتسـتفيد الدول الأعضـاء من تحسـين فهمها لكيفية تطبيق القواعد القائمة ومن تبادل الآراء بشـأنها، ومن تحليل أكثر تفصـيلا لأي ثغرات محتملة. وسيكون برنامج العمل في وضع جيد يتيح له توفير منبر شامل للجميع لمواصلة هذه المناقشات. وعلى وجه الخصـوص، يمكن أن يوفر برنامج العمل منبرا للعناصـر التالية في مناقشـة القانون الدولي: (أ) مواصـلة المناقشـات بشـأن كيفية انطباق القانون الدولي على الفضـاء السـيبراني؛ (ب) تبادل وجهات النظر الوطنية؛ (ج) عقد اجتماعات تكرس لمناقشـــة كيفية تطبيق القانون الدولي في اســـتخدام تكنولوجيات المعلومات والاتصـــالات، مع التركيز على مواضـــيع محددة ليتســـنى تعميق النقاش؛ (د) إحاطات الخبراء؛ (هـ) إجراء مناقشات على أساس سيناريوهات؛ (و) بناء القدرات في مجال القانون الدولي.

7 - **ينبغي أن يكون برنامج العمل عملي المنحى وأن يركز بقوة على بناء القدرات** - ينبغي أن يكون تنفيذ الإطار المتفق عليه لسلوك الدول المسؤول جزءا لا يتجزأ من المناقشات في المستقبل. ويمكن أن يشجع برنامج العمل أيضـــا على الإبلاغ الطوعي عن جهود التنفيذ الوطنية التي من شـــأنها أن تســـهم في تحقيق العديد من الأهداف، مثل بناء الثقة، والشـــفافية، فضـــلا عن تحديد القدرات والاحتياجات. وينبغي لبرنامج العمل أن يقيّم المبادرات القائمة لبناء القدرات بطريقة جيدة التنســـيق ومتكاملة. فعلى ســـبيل المثال، ينبغي أن يراعي تصـميم برنامج العمل عمليات وموارد المسـح القائمة، مثل بوابة سـيبيل (Cybil) وعمليات المسـح التي تجريها شبكة CyberNet لمشاريع بناء القدرات السيبرانية للدول الأعضاء في الاتحاد الأوروبي.

فرنسا

[الأصل: بالفرنسية
30 نيسان/أبريل 2024]

أولا - مقدمة

لقد اعترفت الدول منذ أكثر من 20 عاما بأن تكنولوجيات المعلومات والاتصالات تشكّل عاملا يحفز التقدم البشري والتنمية، ولكنها اعترفت أيضا بأنه يمكن استخدامها في أغراض لا تتفق مع هدف صون الاستقرار والأمن الدوليين.

ومنذ عام 2003، أنشأت اللجنة الأولى للجمعية العامة مجموعة من الأفرقة العاملة التي سعت إلى صون السلام والأمن والاستقرار الدوليين في البيئة الرقمية. وتحقيقا لهذه الغاية، قامت تلك الأفرقة العاملة بتعزيز إطار سلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات، الذي أيدته الجمعية العامة بتوافق الآراء في العديد من القرارات[7].

وناقشت تلك الأفرقة العاملة أيضا إقامة حوار مؤسسي منتظم لتناول المسائل المتعلقة باستخدام تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي.

وجرى التشديد على أن هذا الحوار ينبغي أن يولي اهتماما خاصا لدعم تنفيذ الإطار. وعلى وجه الخصوص، خلص الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي للفترة 2019-2021 إلى أن آلية الحوار المؤسسي المنتظم المستقبلي "ينبغي أن تتخذ شكل إجراء عملي المنحى ومحدد الأهداف ومستند إلى النتائج السابقة، وأن تكون شاملة للجميع، وشفافة، ومدفوعة بتوافق الآراء، وقائمة على النتائج"[8]. وشددت الدول أيضا على "جدوى استكشاف آليات مكرسة لمتابعة تنفيذ المعايير [...] المتفق عليها"[9].

ولاحظت الدول أيضا أن للإطار طابع تراكمي ومتطور وأنه يمكن وضع معايير إضافية مع مرور الوقت. كما أشارت الدول إلى إمكانية وضع التزامات ملزمة إضافية في المستقبل، عند الاقتضاء[10]. وينبغي للحوار المؤسسي المنتظم المستقبلي أن يدعم تنفيذ الإطار المتفق عليه بالفعل، وأن يتيح أيضا إمكانية تطوير هذا الإطار في المستقبل، ولا سيما في سياق نشأة تحديات وتهديدات جديدة.

وفي هذا السياق، من شأن الاقتراح الذي قدمته منذ عام 2020 مجموعة عبر إقليمية من الدول الداعي إلى وضع برنامج عمل أن يزود اللجنة الأولى بآلية مؤسسية دائمة تقوم برصد تنفيذ الإطار المتفق عليه بالفعل وتتيح تطويره عند الاقتضاء.

وفي تقرير الأمين العام عن برنامج العمل للارتقاء بسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي (A/78/76)، أوصى الأمين العام بأن تواصل الدول النظر

(7) انظر قراري الجمعية العامة 237/70 و 19/76.

(8) A/75/816، المرفق الأول، الفقرة 74.

(9) A/75/816، المرفق الأول، الفقرة 73.

(10) قرار الجمعية العامة 19/76، الفقرة العاشرة من الديباجة.

في نطاق الاقتراح الداعي إلى إنشـــاء برنامج العمل وهيكله ومبادئه ومحتواه ووظائفه وآلية متابعته المحتملة برعاية الفريق العامل المفتوح العضوية للفترة 2021–2025، بالاستفادة من الآراء المعرب عنها في التقرير، مع مراعاة أيضـــا المشـــاورات الإقليمية ودون الإقليمية التي ينظمها مكتب شـــؤون نزع الســـلاح عملا بقرار الجمعية العامة 37/77.

وتشـــكل هذه المســـاهمة تحديثا للمســـاهمة الوطنية الفرنســـية الواردة في الوثيقة A/78/76، وهي تعكس التقدم المحرز بفضل قرار الجمعية العامة 16/78 ومتابعة المناقشات في إطار الفريق العامل المفتوح العضوية للفترة 2021–2025.

ثانيا – النطاق والأهداف

سـيتطرق برنامج العمل، بوصـفه آلية من آليات اللجنة الأولى، إلى المسـائل المتصـلة باسـتخدام تكنولوجيات المعلومات والاتصـــالات في ســـياق الأمن الدولي. وســـيتمثل الهدف الرئيســـي لبرنامج العمل في المساهمة في صون السلام والأمن الدوليين من خلال الحفاظ على بيئة منفتحة ومأمونة ومستقرة وميسَّرة وسلمية لتكنولوجيا المعلومات والاتصالات.

وتحقيقا لهذه الغاية، ينبغي أن تكون أهداف برنامج العمل كما يلي:

- التعاون: التخفيف من حدة التوترات ومنع نشوب النزاعات وتعزيز استخدام تكنولوجيات المعلومات والاتصـالات في الأغراض السـلمية باتباع نهج تعاوني للتصـدي للتهديدات السـيبرانية، إلى جانب إجراء حوار شامل للجميع بين الدول ومع الجهات صاحبة المصلحة؛
- الاسـتقرار: تعزيز الاسـتقرار في الفضـاء الإلكتروني من خلال دعم تنفيذ إطار سـلوك الدول المسـؤول استنادا إلى القانون الدولي، بما في ذلك القانون الدولي الإنساني وقانون حقوق الإنسان، ومعايير سلوك الدول المسؤول، وتدابير بناء الثقة وتعزيز القدرات، ومن خلال تطوير هذا الإطار عند الاقتضاء؛
- القدرة على الصـمود: المساهمة في سد الفجوة الرقمية وفي بناء القدرة على الصـمود على المستوى العالمي من خلال تنفيذ إطار سلوك الدول المسؤول.

ثالثا – الهيكل والمحتوى

الهيكل المؤسسي

يمكن أن يعتمد برنامج العمل على وثيقة سياسية تتضمن أهدافها أمورا من بينها ما يلي:

(أ) إعادة تأكيد الالتزام السياسي للدول بإطار سلوك الدول المسؤول، على النحو الذي تؤكده القرارات والتقارير ذات الصـــلة[11]. وســـيراعي هذا الالتزام التأســـيســـي النتائج القائمة على توافق الآراء التي اعتمدها الفريق العامل المفتوح العضـوية المعني بأمن تكنولوجيات المعلومات والاتصـالات وأمن اسـتخدامها للفترة 2021–2025، مثل إنشاء دليل حكومي دولي عالمي لجهات الاتصال، أو إمكانية إنشاء بوابة عالمية

(11) تتضـــمن بشـــكل خاص قرار الجمعية العامة 19/76، وتقارير أفرقة الخبراء الحكوميين التي تم الاتفاق عليها بتوافق الآراء للأعوام 2010 و 2013 و 2015 و 2021، وتقرير عام 2021 الذي أعده الفريق العامل المفتوح العضوية للفترة 2019–2021، وأول تقرير مرحلي للفريق العامل المفتوح العضـوية للفترة 2021–2025، نظرا إلى أن النتائج التي سـيتوصـل إليها الفريق الحالي بتوافق الآراء في المستقبل ستثري هذا الإطار التراكمي والمتطور.

للتعاون أو إمكانية إنشاء سجل بالتهديدات. وينبغي أن يعتمد أي برنامج عمل مستقبلي على هذه النتائج التي اعتُمِدت بتوافق الآراء[12]؛

(ب) إنشاء آلية مؤسسية دائمة تهدف إلى ما يلي: '1' تعزيز تنفيذ هذا الإطار، ولا سيما بدعم قدرات الدول في هذا المجال؛ '2' مواصلة تطوير الإطار، عند الاقتضاء؛ '3' تشجيع التعاون المتعدد الأطراف في المجالات ذات الصلة.

ويمكن لبرنامج العمل، بوصفه آلية دائمة، أن يعتمد الهيكل المؤسسي التالي:

- تنظيم اجتماعات عامة منتظمة بمعدل سنوي أو نصف سنوي على سبيل المثال (فرنسا مستعدة لمتابعة المناقشات بشأن الوتيرة الأمثل لعقد اجتماعات برنامج العمل، مع مراعاة إمكانات الدول وضرورة أن يواكب برنامج العمل التطورات الرقمية). وستتيح تلك الاجتماعات فرصة للقيام بما يلي: (أ) مناقشة التهديدات القائمة والناشئة؛ (ب) والنظر في تنفيذ القواعد والمعايير والمبادئ؛ (ج) ومتابعة المناقشات المتعلقة بكيفية انطباق القانون الدولي على استخدام تكنولوجيات المعلومات والاتصالات وتحديد الثغرات المحتملة؛ (د) ومناقشة تنفيذ تدابير بناء الثقة؛ (هـ) وتحديد الأولويات المتعلقة بتنمية القدرات، بما في ذلك بالاعتماد على المعلومات المقدمة طوعًا؛ (و) وتحديد الإجراءات التي يتعين اتخاذها في المستقبل ووضع خطة عمل للاجتماعات المعقودة بين الدورات. ويمكن اتخاذ قرار بتوافق الآراء أثناء الاجتماعات السنوية بإنشاء مسارات عمل تقنية تكون مفتوحة لجميع الدول والجهات الفاعلة المعنية وتعنى بمسائل محددة (انظر أدناه). وسيتم تشجيع مشاركة الخبراء في المجالين التقني والقانوني.
- تنظيم اجتماعات بين الدورات للنهوض بخطة العمل المتفق عليها أثناء الاجتماعات السنوية. ويمكن أن تُعقد تلك الاجتماعات على شكل اجتماعات أو أفرقة عاملة تقنية مفتوحة العضوية حول مسارات عمل تعنى بمسائل محددة، وذلك وفقًا للأولويات ومجالات العمل التي يتم تحديدها خلال الاجتماعات السنوية.
- تنظيم مؤتمرات استعراض، بمعدل مرة كل أربع سنوات على سبيل المثال، لتقييم ما إذا كان الإطار بحاجة إلى تحديث، وتطوير الإطار عند الاقتضاء (انظر أدناه). ويمكن إنشاء مسار عمل خاص لتعميق المناقشات حول كيفية انطباق القانون الدولي على استخدام تكنولوجيات المعلومات والاتصالات ولمعرفة إذا ما كان الإطار يتضمن ثغرات تبرر تطويره.

المحتوى

(أ) الترويج لتنفيذ الإطار

سيشجع برنامج العمل على الإبلاغ الطوعي عن التدابير المتخذة على الصعيد الوطني لتنفيذ الإطار، إما بإنشاء نظام إبلاغ خاص بالإطار أو بتعزيز الآليات القائمة (مثل الدراسة الاستقصائية النموذجية الوطنية بشأن التنفيذ التي أجراها معهد الأمم المتحدة لبحوث نزع السلاح، أو التقارير الوطنية

(12) انظر قرار الجمعية العامة 37/77، الفقرة الثانية من الديباجة، وقرار الجمعية العامة 16/78، الفقرة الثانية من الديباجة.

المقدّمة إلى الأمين العام). وسيسمح ذلك الإبلاغ بتحديد الأولويات المتعلقة بتنفيذ الإطار وبتقييم الاحتياجات في مجال بناء القدرات.

وخلال الاجتماعات السنوية لبرنامج العمل، يمكن اعتماد توصيات ملموسة بشأن جهود التنفيذ على المستوى الوطني ويمكن تحديث تلك التوصيات بانتظام. ووفقا للهيكل المؤسسي المبين أعلاه، يمكن للاجتماعات السنوية لبرنامج العمل أن تنشئ اجتماعات أو أفرقة عاملة تقنية مفتوحة العضوية تهدف إلى تعزيز تبادل الآراء بشأن جوانب محددة متصلة بتنفيذ الإطار.

فعلى سبيل المثال، يمكن تحديد أولوية مواضيعية لتنفيذ الإطار خلال اجتماع سنوي (مثل تنفيذ معيار معين أو إجراء معين لبناء الثقة، وأمن المنتجات والخدمات الرقمية، وحماية البنية التحتية الحيوية، وما إلى ذلك). ومن أجل مواصلة تبادل الآراء بشأن هذه المسألة، والمساهمة بالخبرات الفنية، ومناقشة أفضل الممارسات والصعوبات القائمة، يمكن للاجتماع السنوي عندئذ أن يقرر إنشاء مسار عمل محدد تكون أعماله مفتوحة أمام جميع الدول وتجري أثناء اجتماعات برنامج العمل المعقودة بين الدورات. وستُعرض نتائج وتوصيات تلك الاجتماعات أو الأفرقة العاملة التقنية المفتوحة العضوية خلال الاجتماع العام التالي.

وسيدعم برنامج العمل التدابير الرامية لبناء القدرات فيما يتعلق بتنفيذ الإطار، وسيهدف إلى تعزيز التعاون المتعدد الأطراف في هذا المجال وكذلك إلى تنسيق الجهود مع المبادرات الأخرى ذات الصلة.

ويمكن للدول أن تنظر في إنشاء صندوق تبرعات، في إطار برنامج العمل المستقبلي، لتمويل أنشطة معينة تهدف إلى تعزيز إطار سلوك الدول المسؤول. ويمكن أن يتبع هذا الصندوق مثالَ مرفق الأمم المتحدة الاستئماني لدعم التعاون في مجال تنظيم الأسلحة[13]. وينبغي أن تعتمد المبادرات أو المشاريع المموّلة من هذا المرفق على ولاية يمكن أن يحددها الاجتماعُ الأول لبرنامج العمل (الترويج للانضمام إلى الإطار، والتقيد بالمبادئ التوجيهية لبناء القدرات المتفق عليها في التقرير النهائي للفريق العامل المفتوح العضوية للفترة 2019-2021، وما إلى ذلك).

وسيهدف برنامج العمل أيضا إلى الاستفادة من الإجراءات والمبادرات القائمة. وستتيح اجتماعات برنامج العمل والاجتماعات المعقودة بين الدورات لفريق عامل تقني معني ببناء القدرات فرصةً أمام الدول لتبادل الآراء بشأن الأولويات في هذا المجال (على أساس الاحتياجات المحددة بفضل المعلومات المقدّمة طوعا)، وأمام الجهات صاحبة المصلحة لعرض المبادرات ذات الصلة. ويمكن لبرنامج العمل أيضا أن يعد نظاما يتيح "إصدار شهادات" للتصديق على الأنشطة المتّسقة مع أهدافه ولتعزيزها.

ويمكن لممثلي المنظمات الأخرى (الاتحاد الدولي للاتصالات، والصندوق الاستئماني للأمن السيبراني التابع للبنك الدولي) أن يقدموا عروضا أثناء اجتماعات برنامج العمل لضمان تنسيق وتكامل تدابير بناء القدرات التي تتخذها مختلف الهياكل (التي يعمل كل هيكل منها في إطار ولايته ومجال اختصاصه).

(ب) تطور الإطار

عند الضرورة وللتصدي للتحديات الناشئة، ستسمح الاجتماعات المنتظمة أو مؤتمرات الاستعراض بتحديث الإطار (بإتاحة الإمكانية لإجراء مناقشات بشأن مواصلة تطوير الإطار، بما في ذلك عن طريق

(13) مرفق الأمم المتحدة الاستئماني لدعم التعاون في مجال تنظيم الأسلحة، انظر https://disarmament.unoda.org/unscar/.

تعميق نقاط الفهم المشـــترك للمعايير وكيفية انطباق القانون الدولي على اســـتخدام تكنولوجيات المعلومات والاتصـالات، وتحديد أي ثغرات في نقاط الفهم المشترك تلك، والنظر، عند الاقتضاء، في ما إذا كانت هناك حاجة إلى معايير طوعية إضـــافية غير ملزمة أو إلى تعهدات إضـــافية ملزمة قانونا)، على أســـاس التوافق في الآراء[14].

(ج) مشاركة متعددة الأطراف

تسلّم فرنسا بأن الدول "تتحمل [...] المسؤولية الأولى عن صون السلام والأمن الدوليين"[15]، وبأنه يجب عليها أن تحافظ على دورها المحوري (الذي يشـــمل الممارســـة الحصـــرية لســـلطة اتخاذ القرار) في أي عملية من عمليات اللجنة الأولى، ولذلك فهي تؤيد تعزيز الحوار والتعاون مع الجهات صـــاحبة المصلحة في سياق برنامج عمل مستقبلي.

- وسيظل اتخاذ القرار والتفاوض بشأن الوثائق الختامية من اختصاص الدول وحدها.
- بيد أن الأفرقة العاملة المعنية التابعة للجنة الأولى شـــددت في العديد من المناســـبات على أهمية مواصلة توثيق التعاون، عند الاقتضاء، مع المجتمع المدني والقطاع الخاص والأوساط الأكاديمية والأوســـاط التقنية[16]. وقد يكون التعاون مع تلك الجهات الفاعلة ضـــروريا لتتمكن الدول من تنفيذ التزاماتها بموجب إطار السلوك المسؤول. وبالإضافة إلى ذلك، تتحمل الجهات صاحبة المصلحة "مسؤولية استخدام تكنولوجيا المعلومات والاتصالات بطريقة لا تعرّض السلام والأمن للخطر"[17]. ويمكن للجهات الفاعلة الخاصـــة أيضـــا أن تســـاهم بمعارف قيّمة في عمليات التبادل وأن تســـاهم في جهود بناء القدرات.
- ولذلك، ينبغي أن تســـمح طرائق تنظيم اجتماعات برنامج العمل للجهات صـــاحبة المصـــلحة بالمشاركة في الجلسات الرسمية وبالإدلاء ببيانات وبتقديم مدخلات، كما هو الحال أثناء عمليات اللجنة الأولى الأخرى التي تكون فيها خبراتها مفيدة، ولا ســـيما فريق الخبراء الحكومي المعني بالأســـلحة الفتاكة الذاتية التشـــغيل الذي يعقد اجتماعات في إطار اتفاقية حظر أو تقييد اســـتعمال أسلحة تقليدية معينة يمكن اعتبارها مفرطة الضرر أو عشوائية الأثر[18]. وستضفي تلك الطرائق، التي تسمح بإجراء حوار متعدد الأطراف في إطار رسمي، شفافية أكبر على العملية.
- ولضـــمان شـــمولية تلك الاجتماعات، ينبغي تشـــجيع ودعم مشـــاركة الجهات صـــاحبة المصـــلحة من كل مجموعة إقليمية، بما في ذلك بالاعتماد على برامج رعاية محددة.

(14) انظر قرار الجمعية العامة 16/78، الفقرة 3 (ب).

(15) A/75/816، المرفق الأول، الفقرة 10.

(16) A/75/816، المرفق الأول، الفقرة 22.

(17) A/75/816، المرفق الأول، الفقرة 10.

(18) المادة 49 من النظام الداخلي لاتفاقية حظر أو تقييد استعمال أسلحة تقليدية معينة يمكن اعتبارها مفرطة الضرر أو عشوائية الأثر (اعتُمد النظام الداخلي أثناء المؤتمر الاستعراضي الخامس للأطراف المتعاقدة السامية في الاتفاقية المعقود في عام 2016).

رابعا - الأعمال التحضيرية لإنشاء برنامج العمل وطرائق الإنشاء

الأعمال التحضيرية

تؤيد فرنسا مواصلة إجراء مناقشات مركّزة ومكرّسة في إطار الفريق العامل المفتوح العضوية للفترة 2021-2025 بهدف متابعة بلورة برنامج العمل والسعي إلى التوصل إلى توافق في الآراء بشأن إنشائه.

ويوصي التقريران النهائيان للفريق العامل المفتوح العضوية للفترة 2019-2021 ولفريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي بمواصلة بلورة برنامج العمل، بما في ذلك في إطار الفريق العامل المفتوح العضوية للفترة 2021-2025. كما يدعو التقرير المرحلي لعام 2022 الذي أعده الفريق العامل الحالي المفتوح العضوية للفترة 2021-2025 إلى إجراء مناقشات مركّزة بشأن برنامج العمل.

وقد سمح كل من المشاورات الإقليمية التي أجريت في عام 2023 وتقرير الأمين العام (A/78/76) بجمع آراء مجموعة كبيرة ومتنوعة من الدول. وجرت الإشارة في تقرير الأمين العام إلى أن النظر في الاقتراح الداعي إلى إنشاء برنامج العمل بطريقة شاملة وشفافة، المستند بقوة إلى الاتفاقات السابقة التي اتُّخذت بتوافق الآراء والتقدم المحرز في الجمعية العامة، يمثل مسعى جديرا بالاهتمام. وقد سمح التقرير المرحلي السنوي الثاني للفريق العامل المفتوح العضوية للفترة 2021-2025 بمواصلة هذا المسعى، من خلال الاتفاق من حيث المبدأ على "العناصر المشتركة" التوافقية لكي تفضي، بطريقة بناءة، إلى رؤية مشتركة للآلية المقبلة للحوار المؤسسي المنتظم[19].

وفي القرار 37/77، طلبت الجمعية العامة أيضا أن يُعرض عليها تقرير الأمين العام عن برنامج العمل وأن ينظر فيه الفريق العامل المفتوح العضوية للفترة 2021-2025 لإجراء مزيد من المناقشات. وفي القرار 16/78، شددت الجمعية العامة على أن الفريق العامل المفتوح العضوية ينبغي أن يكون المحفل الرئيسي لبلورة برنامج العمل بغية إنشائه عند اختتام أعمال الفريق العامل المفتوح العضوية للفترة 2021-2025، وفي موعد أقصاه عام 2026.

ولذلك، ينبغي عقد اجتماعات بين الدورات ودورات محددة للفريق العامل المفتوح العضوية للفترة 2021-2025 في عامي 2024 و 2025 من أجل القيام بأمور من بينها مواصلة بلورة مختلف جوانب برنامج العمل وصياغة نصه التأسيسي.

طرائق الإنشاء

تؤيد فرنسا إجراء مزيد من المناقشات بشأن الطريقة الدقيقة التي ستُتَّبع لإنشاء الآلية المقبلة.

وقد أشارت الجمعية العامة في قرارها 37/77 إلى "مؤتمر دولي" باعتباره خيارا لإنشاء برنامج العمل (كما حدث مثلاً بالنسبة لبرنامج العمل المتعلق بمنع الاتجار غير المشروع بالأسلحة الصغيرة والأسلحة الخفيفة من جميع جوانبه ومكافحته والقضاء عليه). وفي القرار 16/78، قررت الجمعية العامة إنشاء آلية، تحت رعاية الأمم المتحدة، عند اختتام أعمال الفريق العامل المفتوح العضوية للفترة 2021-2025، وفي موعد أقصاه عام 2026، تكون آلية دائمة وشاملة وعملية المنحى، وفقا للأهداف

(19) A/78/265، الفقرة 55.

المحددة والمؤكدة في قرار الجمعية العامة 37/77، وللعناصر المشتركة للحوار المؤسسي المنتظم في المستقبل حسبما اتُّفق عليه بالإجماع في التقرير المرحلي السنوي الثاني للفريق العامل المفتوح العضوية للفترة 2021-2025. وإذا قررت الدول ذلك، يمكن عقد مؤتمر دولي في عام 2025 من أجل اعتماد النص التأسيسي للآلية المذكورة، استنادا إلى الأعمال التحضيرية المنجزة في إطار الفريق العامل المفتوح العضوية للفترة 2021-2025.

وينبغي لهذا المؤتمر الدولي أن يتخذ قراراته بتوافق الآراء، وذلك على الأقل بشأن المسائل الموضوعية. وينبغي أن يسمح المؤتمر بمشاركة الجهات صاحبة المصلحة (يمكن أن يتبع اعتماد تلك الجهات طرائق مماثلة لتلك المتّبعة في القرار 282/75 بالنسبة للجنة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية).

ويمكن للجمعية العامة عندئذ أن تتخذ قرارا يرحب بنتائج المؤتمر وأن تقرر عقد الاجتماع الأول للآلية المنشأة حديثا.

جورجيا

[الأصل: بالإنكليزية
20 آذار/مارس 2024]

فيما يتعلق بالجولة المقبلة من الحوار المؤسسي المنتظم بشأن استخدام تكنولوجيات المعلومات والاتصالات، تحت رعاية الأمم المتحدة: ترى جورجيا أن برنامج العمل للارتقاء بسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي هو النهج الأمثل للنهوض بمبادرات الأمم المتحدة المتعلقة بالأمن السيبراني وسلوك الدول المسؤول في الفضاء السيبراني.

ففي البيئة الأمنية الحالية التي تشهد تطورات جيوسياسية سريعة لا يمكن التنبؤ بها، تهدد بعض الجهات الفاعلة النظام الدولي القائم على القواعد باستخدام مزيج من وسائل الحرب التقليدية وغير التقليدية. ومما يؤسف له أن ثمة حالات تنتهك فيها بعض الجهات الفاعلة القانون الدولي من خلال العمليات السيبرانية. ويجب على المجتمع العالمي أن يصر على مساءلة هذه الجهات الفاعلة عن سلوكها غير المشروع وغير المقبول في الفضاء السيبراني، وأن يكون حريصا على أن يكون لمثل هذه الأعمال عواقب قانونية.

ويمكن أن يكون برنامج العمل منصة مناسبة لإجراء حوارات محددة الأهداف بشأن تطبيق القانون الدولي في الفضاء السيبراني بعد اختتام أعمال الفريق العامل المفتوح العضوية الحالي المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025، في عام 2025.

ونحن ندعو إلى أن يكون برنامج العمل بمثابة إطار موحد داخل اللجنة الأولى للجمعية العامة مكرس لمعالجة شواغل الأمن السيبراني، مع توفير هيكل موثوق به يفضي إلى مبادرات عملية المنحى وإلى إحراز تقدم ملموس.

ويمثل غياب القدرات على المستويات الوطني والإقليمي والعالمي تحديا كبيرا. ولذلك ينبغي لبرنامج العمل أن يساعد المساعي الوطنية في سن الإطار المعياري وأن يقدم المساعدة في بناء القدرات لتضييق الفجوة الرقمية.

وترحب جورجيا بوضع دليل حكومي دولي عالمي لجهات الاتصال. فهذه المبادرة خطوة مهمة إلى الأمام في تعزيز التعاون والتنسيق الدوليين في مجال الأمن السيبراني في سياق الأمم المتحدة.

وبالنظر إلى الوتيرة السريعة لتطور تكنولوجيا المعلومات والاتصالات، يجب أن يتمتع الإطار الدولي المقبل بمرونة كبيرة لضمان أهميته في المستقبل. وينبغي أن يتضمن هذا المحفل الدولي آلية تمكن من إجراء تنقيح دوري لإطاره من خلال توافق في الآراء ييسره عقد جلسات عامة عادية أو مؤتمرات استعراض. ويمكن لهذه التجمعات أن تعيد تقييم الإطار القائم، وأن تقرر، متى تعين، تعزيزه أو مواصلة تطويره.

وتؤيد جورجيا بقوة النهج الشفاف والشامل المتعدد أصحاب المصلحة، مع التأكيد على المشاركة النشطة لكل من الجهات الفاعلة الحكومية وغير الحكومية في إطار الحوار المؤسسي بشأن هذه المسائل.

ألمانيا

[الأصل: بالإنكليزية
30 نيسان/أبريل 2024]

ألف - المبادئ الأساسية لبرنامج العمل

تنادي ألمانيا بوضع برنامج عمل باعتباره محفلا عمليا ودائما وشفافا ومرنا وشاملا لإجراء حوار مؤسسي منتظم بشأن أمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها في إطار اللجنة الأولى. وينبغي أن يكون برنامج العمل هو آلية المتابعة الأحادية المسار للفريق العامل الحالي المفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات وأمن استخدامها، للفترة 2021-2025. وينبغي أن يبدأ في أداء وظائفه في موعد لا يتجاوز عام 2026 لتنفيذ نتائج الفريق العامل بعد الانتهاء من ولايته، مع تكرار التأكيد على ما تقرر في قرار الجمعية العامة 16/78 من إنشاء آلية تحت رعاية الأمم المتحدة، وإعادة تأكيد الأهداف المحددة في القرار 37/78، بما في ذلك العناصر المشتركة المتفق عليها في التقرير المرحلي السنوي الثاني الذي أعده بتوافق الآراء الفريق العامل المفتوح العضوية للفترة 2021-2025 (A/78/265).

ويتعين تفادي العمليات الموازية أو الهياكل المزدوجة، بهدف عدم إرهاق الدول على نحو يمنعها من المشاركة الهادفة وحتى تكون المناقشات عملية المنحى. وفي إطار التحضير لانتقال سلس، يلزم مواصلة المناقشات بين الدول بشأن نطاق برنامج العمل وهيكله ومضمونه في إطار الفريق العامل المفتوح العضوية الحالي، بهدف التوصل إلى توافق في الآراء بشأن جوهر برنامج العمل وطرائقه. وينبغي أن يكون الهدف هو أن تؤيد جميع الدول الأعضاء برنامج العمل هذا في مؤتمر مكرس يُعقد مباشرة بعد الدورة الأخيرة للفريق العامل التي ستُعقد في عام 2025.

والغرض العام لبرنامج العمل هو المساهمة في السلام والأمن الدوليين في الفضاء السيبراني عن طريق تيسير الحوار والتعاون بين الدول بشأن تنفيذ الإطار الدولي القائم لسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات. وهذا يتطلب ما يلي:

- بناء القدرات السيبرانية وفقا للمبادئ التوجيهية المتفق عليها في التقرير النهائي لعام 2021 الذي أعده الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، فضلا عن المبادئ المتفق عليها لبناء القدرات المؤكدة

في المرفق جيم للتقرير المرحلي السنوي الثاني. وستكون الاستفادة من أوجه التآزر مع الآليات الواردة في المحافل الأخرى مفيدا في تجنب ازدواجية الهياكل والتخفيف من استخدام الموارد.

- تدابير بناء الثقة، بما في ذلك التنفيذ الفعال للقائمة الأولية غير الحصرية لتدابير بناء الثقة المتفق عليها في التقرير المرحلي السنوي الثاني (A/78/265، المرفق باء)، لاسيما الدليل العالمي لجهات الاتصال.
- تبادل أفضل الممارسات على المستوى الدولي والأقاليمي والإقليمي.
- المشاركة الهادفة للجهات المعنية صاحبة المصلحة.

وعلاوة على ذلك، ينبغي أن يشكل برنامج العمل منبرا دائما لإعطاء دفع للمناقشات بشأن التهديدات القائمة والناشئة، وكذلك بشأن كيفية تطبيق القانون الدولي، بما في ذلك القانون الدولي الإنساني وقانون حقوق الإنسان، على استخدام الدول لتكنولوجيات المعلومات والاتصالات. وينبغي أن تُتاح الفرصة لإجراء مزيد من المناقشات بشأن الإطار الدولي لسلوك الدول المسؤول في الفضاء السيبراني، ولمواصلة تطويره، عند الاقتضاء، ضمن برنامج العمل من أجل التكيف مع التهديدات الجديدة والتصدي لها في ظل تغيُّرها بمرور الوقت.

وينبغي أن يوفر برنامج العمل إطارا مؤسسيا عاما لآليات الأمن السيبراني الأخرى الجاري إعدادها حاليا في إطار الفريق العامل، مثل البوابة السيبرانية، على النحو الذي اقترحته الهند، والمستودع السيبراني، على النحو الذي اقترحته كينيا.

وينبغي أن يقوم الهدف العام والأهداف المحددة والمبادئ الأساسية لبرنامج العمل على شكل إعلان سياسي توافق عليه الجمعية العامة. وينبغي أن يكمّل الإعلانَ قرارٌ تعده اللجنة الأولى يصف مهام برنامج العمل وهيكله وطرائقه. وينبغي أن يستند كل من الإعلان السياسي وقرار اللجنة الأولى إلى الوثيقة الختامية للمؤتمر المكرس لهذا الغرض المقرر عقده في عام 2025، كما ذكر أعلاه.

باء - مهام برنامج العمل وهيكله وطرائقه

استنادا إلى الدروس المستفادة من الصكوك السابقة والقائمة، ينبغي تصميم مهام برنامج العمل بطريقة تضمن مشاركة الدول مشاركةً فعالة وشاملة وشفافة وتسمح بقياس التقدم المحرز نحو تنفيذ إطار سلوك الدول المسؤول، بما في ذلك من خلال آلية إبلاغ طوعية، مثل الدراسة الاستقصائية الوطنية بشأن تنفيذ توصيات الأمم المتحدة المتعلقة باستخدام الدول المسؤول لتكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي التي أجراها معهد الأمم المتحدة لبحوث نزع السلاح. ويكتسي بناء القدرات والتعاون، فيما بين الدول وكذلك مع المنظمات الإقليمية والجهات الفاعلة من غير الدول، أهمية حاسمة لمعالجة المجالات التي يتأخر فيها التنفيذ على المستوى الوطني.

واستنادا إلى العناصر المشتركة المتفق عليها في التقرير المرحلي السنوي الثاني الصادر بتوافق الآراء، ينبغي أن يشمل هيكل وطرائق برنامج العمل ما يلي:

(أ) مؤتمرات سنوية تُعقد في المقر بنيويورك:

'1' لاستعراض وقياس التقدم المحرز صوب تنفيذ الإطار والمهام المحددة؛

’2‘ لمناقشة إمكانية تطوير الإطار، بما في ذلك بمواصلة تعزيز الفهم المشترك لتطبيق القانون الدولي في الفضاء السيبراني؛

’3‘ لاتخاذ قرارات بشأن مواضيع محددة؛

’4‘ لتبادل المعلومات بشأن التهديدات الحالية والناشئة المحدقة بالسلام والأمن الدوليين الناجمة عن استخدام تكنولوجيات المعلومات والاتصالات؛

’5‘ لمواصلة بلورة التدابير الهادفة لبناء القدرات السيبرانية؛

’6‘ للنظر في إمكانية مواصلة تطوير برنامج العمل بطريقة تدريجية، استنادا إلى احتياجات الدول الأعضاء، ومع مراعاة التغيرات التي تطرأ على مشهد التهديدات، وعلى أساس فهم أن برنامج العمل صك يتسم بالمرونة؛

(ب) تنفيذ تدابير لبناء الثقة ومواصلة بلورتها استنادا إلى الدليل العالمي لجهات الاتصال الذي أعدّه الفريق العامل المفتوح العضوية الحالي. والدليل، بالإضافة إلى كونه تدبيرا لبناء الثقة في حد ذاته، ينبغي أن يوفر الأساس لتنفيذ القائمة العالمية غير الحصرية لتدابير بناء الثقة المتفق عليها في التقرير المرحلي السنوي الثاني، بغية تحقيق الهدف العام المتمثل في الحد من احتمالات سوء الفهم والصراع في الفضاء السيبراني. وينبغي أن يُستخدم أيضا لمناقشة واعتماد وتنفيذ تدابير إضافية لبناء الثقة على الصعيد العالمي. وبتيسير وضع وتنفيذ تدابير مكرسة لبناء الثقة، سيكون الدليل دعامة أساسية لبرنامج العمل تركز على تنفيذ الإطار القائم؛

(ج) عقد مؤتمرات استعراض كل أربع إلى ست سنوات لإتاحة إمكانية تكييف برنامج العمل مع التطورات الديناميكية التي تحدث في الفضاء السيبراني وما يرتبط بها من تهديدات محدقة بالسلام والأمن الدوليين؛

(د) اضطلاع مكتب شؤون نزع السلاح بدور أمانة برنامج العمل. وبالإضافة إلى التحضير للاجتماعات السنوية ومؤتمرات الاستعراض، سيكون المكتب مسؤولا أيضا عن إدارة الدليل العالمي لجهات الاتصال وغيره من تدابير بناء الثقة؛

(هـ) قيام معهد الأمم المتحدة لبحوث نزع السلاح بتزويد الدول بأدوات الرصد والاستعراض ذات الصلة (مثل القوائم المرجعية لتنفيذ المعايير على النحو المتفق عليه في التقرير المرحلي السنوي الثاني الصادر بتوافق الآراء) وإجراء أنشطة بحثية متصلة بتنفيذ الإطار؛

(و) إمكانية عقد اجتماعات إضافية لمجموعات العمل التقنية خلال فترة ما بين الدورات. ويمكن أن تركّز مجموعات العمل التقنية المخصصة على مواضيع من قبيل النهوض ببناء القدرات السيبرانية، وتدابير بناء الثقة، وتطبيق القانون الدولي، بما في ذلك القانون الدولي الإنساني، والتهديدات القائمة والناشئة. وينبغي أن تكون المشاركة في مجموعات العمل طوعية ومفتوحة لجميع الدول ومتوازنة من حيث التمثيل الإقليمي. وينبغي أن يراعي عدد مجموعات العمل وتشكيلها، بما في ذلك مشاركة الجهات صاحبة المصلحة ووتيرة عقد الاجتماعات، وطرائق العمل المختلطة المحتملة، قدرة الدول على المشاركة بصورة مجدية وينبغي اتخاذ قرارات بشأن تلك المسائل بتوافق الآراء خلال الاجتماعات السنوية.

وستحتفظ الدول بالحق الحصري في التفاوض على النتائج وفي اتخاذ القرارات في إطار برنامج العمل. وفي الوقت نفسه، ينبغي أن يوفر البرنامج آليات للتعامل مع الجهات صاحبة المصلحة

من غير الدول (المنظمات المتعددة الأطراف والمنظمات الإقليمية، والمجتمع المدني، والقطاع الخاص، والأوساط الأكاديمية). وينبغي أن يتيح برنامج العمل فرصا لمشاركة الجهات صاحبة المصلحة بطريقة شاملة ومجدية على نحو مماثل لطرائق اللجنة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية (وعلى وجه الخصوص، ينبغي تقديم تبرير علني لأي اعتراض من جانب دولة عضو على مشاركة أي جهة من الجهات صاحبة المصلحة؛ ويتقرر إقصاء الجهات صاحبة المصلحة بالتصويت). ويشمل ذلك الحق في أخذ الكلمة وتقديم مدخلات كتابية في الاجتماعات ومؤتمرات الاستعراض والاجتماعات الإضافية لمجموعات العمل التقنية التي تُعقد خلال فترة ما بين الدورات. وعلاوة على ذلك، ينبغي إتاحة خيارات مختلطة للمشاركة بالنسبة لغالبية الأشكال من أجل زيادة شمولية المداولات.

وفي مجال تدابير بناء الثقة وبناء القدرات بشكل خاص، ينبغي الاستفادة من المبادرات والهياكل القائمة على الصعيدين الإقليمي ودون الإقليمي أو في المحافل الأخرى وتعزيز أوجه التآزر (على سبيل المثال مع المنظمات الإقليمية، والصندوق الاستئماني المتعدد المانحين للأمن السيبراني التابع للبنك الدولي، والمنتدى العالمي للخبرات السيبرانية).

ويمكن لمرافق التمويل القائمة في محافل الأمم المتحدة الأخرى، مثل صندوق كيان إنقاذ الأرواح أو مرفق الأمم المتحدة الاستئماني لدعم التعاون في مجال تنظيم الأسلحة في ميدان تحديد الأسلحة، أن توفر مبادئ توجيهية مفيدة لإنشاء آلية لدعم جهود بناء القدرات السيبرانية على شكل مواد تدريبية وتبادل أفضل الممارسات. وعلاوة على ذلك، يمكن التفكير في برنامج للزمالات لتيسير تمثيل عواصم وفود البلدان النامية على نطاق واسع.

ويمكن إنشاء "نظام شراكة" طوعي بين الأقاليم، تتم فيه توأمة أي دولة لديها قدرات عالية من حيث تنفيذ إطار سلوك الدول المسؤول في الفضاء السيبراني مع دولة أو أكثر لديها قدرات أقل. ويمكن لهذه الآلية أن تعزز التعاون بين الدول، وتيسر الحوار وتبادل أفضل الممارسات، وتحسّن قدرات الدول على تنفيذ المعايير إجمالا. ويمكن استخدام نهج "اعتماد تدبير لبناء الثقة" الذي تتبعه منظمة الأمن والتعاون في أوروبا كنموذج مرجعي في هذا الصدد.

أيرلندا

[الأصل: بالإنكليزية
1 أيار/مايو 2024]

إن أيرلندا، باعتبار مجتمعها مجتمعا مفتوحا له اقتصاد مرقمن عالي الترابط، تدرك تماما البيئة الأمنية الدولية المتدهورة، لا سيما فيما يتعلق بزيادة الأنشطة السيبرانية الخبيثة. وإدراكا لذلك، اتخذنا إجراءات محلية ومع شركائنا في الاتحاد الأوروبي، لزيادة القدرة على الصمود، وبناء قدرتنا على تحديد التهديدات ومنعها وردعها، وتعزيز فضاء سيبراني عالمي مفتوح وآمن عماده القانون الدولي وحقوق الإنسان.

غير أننا بقينا واضحين في موقفنا بأن الطابع العالمي لهذا التحدي يتطلب استجابة دولية شاملة. وأيدت أيرلندا التوصل بتوافق الآراء إلى وضع إطار الأمم المتحدة المعياري لسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات، وكان التوصل إلى ذلك من دواعي تفاؤلها. وكان الإطار

نتاجا حاسما لتوصيات متعددة صدرت بتوافق الآراء من كل من أفرقة الخبراء الحكوميين (2010 و 2013 و 2015 و 2021)، والفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي (2021). كما حظي الإطار بالتأييد في أحدث تقريرين مرحليين سنويين أعدهما الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025.

وقد نشرت أيرلندا في العام الماضي موقفها الوطني الداعم لتطبيق القانون الدولي في الفضاء السيبراني، وهو أحد الركائز الأربع للإطار المعياري. وأيرلندا ملتزمة بالعمل مع الدول الأخرى الأعضاء في الاتحاد الأوروبي ومع الشركاء الدوليين للعمل وفقا للإطار المعياري وتعزيز السلام والاستقرار من خلال تنفيذه على صعيد العالم.

وترى أيرلندا أن تنفيذ الإطار المعياري وتعزيزه أمر أساسي لصون الأمن الدولي في الفضاء السيبراني، ولذلك ينبغي أن يكون محوريا في أي آلية للحوار المؤسسي المنتظم. والإطار المستقبلي المقترح للحوار المؤسسي المنتظم الذي يمكن استحداثه بعد انتهاء ولاية الفريق العامل المفتوح العضوية الحالي، على النحو المتوخى تحديدا في مقترحات وضع برنامج عمل، يقرّ بأن الإطار المعياري ضروري، ويسمح بعقد مؤتمرات استعراض دورية لبحث الإطار.

وقد ظلت أيرلندا تبدي تأييدها الكامل للنهج الخاص للحوار المؤسسي المنتظم المتعلق بأمن تكنولوجيا المعلومات والاتصالات على النحو الذي يدعو إليه برنامج العمل، حيث يقترح آلية شاملة وعملية المنحى لحوار دائم في المستقبل. ومن شأن نهج برنامج العمل أن يتيح إجراء حوار دائم وشامل إقليميا ومتعدد أصحاب المصلحة وشفاف تحت رعاية الأمم المتحدة. وقد كان الدعم الواسع النطاق لبرنامج العمل، على النحو المنصوص عليه في قرارات اللجنة الأولى للجمعية العامة، واضحا باستمرار، سواء خلال مداولات الفريق العامل المفتوح العضوية أو من خلال تصويت مجموعة واسعة ومتنوعة إقليميا من الدول في الجمعية العامة.

ويُعد ضمان قدرة جميع الدول على الاستفادة من منافع تكنولوجيات المعلومات والاتصالات، مع التخفيف من المخاطر من خلال تدابير بناء القدرات، ركيزةً أساسية في الإطار المعياري، وهو أولوية بالنسبة لأيرلندا. ويتعين على الدول أن تقرّب الفجوات الرقمية وأن تبني القدرة على الصمود في مواجهة الأنشطة السيبرانية الخبيثة.

وقرار اللجنة الأولى 237/78، المعنون "التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي"، لا يعبر عن أهمية الإطار المعياري، أو عن النطاق الواسع للمنظورات التي أعرب عنها العديد من الدول الأعضاء، ولذلك لم يكن بوسع أيرلندا أن تؤيد القرار. ولا تعتقد أيرلندا أن النهج المقترح في هذا القرار يمكن أن يلبي احتياجات غالبية الدول الأعضاء. بل إن أيرلندا خلصت إلى أن القرار قد يؤدي إلى تقويض الطريقة القائمة على التدرج وتوافق الآراء التي بفضلها تمكن الفريق العامل المفتوح العضوية من إحراز ما أحرز من تقدم خلال السنوات الماضية.

ولا يزال الأمل يحدو أيرلندا في التوصل بتوافق الآراء إلى إنشاء آلية مستقبلية للجولة المقبلة من الحوار المؤسسي المنتظم قبل نهاية مهمة الفريق العامل المفتوح العضوية الحالي، وستعمل مع جميع الدول لطرح نموذج شامل عملي المنحى يجسد الإطار المعياري.

وشـــملت المناقشـــات حول كيفية تنظيم نهج برنامج العمل على وجه الخصـــوص مقترحات لعقد دورات رسـمية سـنوية تُجرى فيها مناقشـات مفصـلة مفتوحة واجتماعات تقنية بشـأن قضـايا محددة تتعلق بالسـياسـات على مدار العام. ويمكن للأفرقة التقنية أن تعالج قضـايا من قبيل القضـايا الجنسـانية والفجوات الرقمية ودور الكيانات غير الحكومية في تنفيذ الإطار المعياري. وينبغي أن تكون مســـارات العمل التقني طوعية ومفتوحة أمام جميع الدول، وأن تفضي إلى استنتاجات تشغيلية تستند إلى الدروس المستفادة من تنفيذ الإطار المعياري.

واســتنادا إلى التأييد العابر للحدود الإقليمية الذي نالته قرارات اللجنة الأولى الداعية إلى اتباع نهج برنامج العمل، فإن هذه الآلية الخاصـــة يمكن أن تعزز المشـــاركة والتعاون على الصـــعيد الإقليمي مع المنظمات الإقليمية لتقديم الدعم في بناء القدرات وفق ما يكون من احتياجات.

ومن الأمور المشـجعة أن برنامج العمل بالصـيغة المقترحة سـيتيح أيضـا للجهات المعنية صـاحبة المصـلحة أن تشـارك بصـفة رسـمية، كما سـيتيح المجال للتشـاور مع تلك الجهات، بما في ذلك مع القطاع الخاص والأوساط الأكاديمية والمجتمع المدني، لتقديم مساهمات بشأن القضايا ذات الصلة. وتؤيد أيرلندا بقوة مشـاركة الجهات المتعددة صـاحبة المصـلحة في الحوار المؤسـسـي المنتظم، وتؤمن إيمانا راسـخا بأن ذلك سـيركز الجهود بشـكل أفضـل على دعم الدول في تنفيذ إطار سـلوك الدول المسـؤول وبناء القدرات وفقا لما يكون من احتياجات من أجل زيادة المرونة السيبرانية.

ولإجراء حوار مؤســـســـي منتظم يؤدي وظائفه كاملة بحلول نهاية فترة ولاية الفريق العامل المفتوح العضوية، تؤيد أيرلندا تنظيم اجتماعات فيما بين الدورات ودورات مخصصة للفريق العامل المفتوح العضوية في عامي 2024 و 2025، بما في ذلك عن الآثار المترتبة في الميزانية.

اليابان

[الأصل: بالإنكليزية
30 نيسان/أبريل 2024]

1 - مقدمة

تؤيد اليابان وضـع برنامج عمل للارتقاء بسـلوك الدول المسـؤول في الفضـاء السـيبراني باعتبار برنامج العمل آلية للمسـتقبل. وترى اليابان أن برنامج العمل هو المحفل الملائم لمواصـلة مناقشـاتنا بشـأن سلوك الدول المسؤول في الفضـاء السيبراني. وينبغي أن يكون برنامج العمل، بوصـفه إطارا عملي المنحى، بمثابة منبر لدعم الجهود التي يبذلها كل بلد لتنفيذ المعايير والمبادئ المتفق عليها بشـــأن ســـلوك الدول المسؤول، وذلك بالتشجيع على تبادل أفضل الممارسات وتحديد التحديات الخاصة التي يواجهها كل بلد.

وسـيكون برنامج العمل آلية المتابعة الوحيدة للفريق العامل المفتوح العضـوية الحالي المعني بأمن تكنولوجيات المعلومات والاتصـالات وأمن استخدامها للفترة 2021-2025، وسيصـبح قادرا على تنفيذ نتائج الفريق العامل المفتوح العضوية بعد انتهاء ولاية هذا الأخير. وسيوضـع برنامج العمل بعد انتهاء ولاية الفريق العامل المفتوح العضوية الحالي ولن يشكّل مسارا مزدوجا.

وتود اليابان أن تقدم أقصـى ما يمكن من إسـهامات في المناقشـات، آخذة في الاعتبار أن برنامج العمل يُتوخى منه أن يكون بمثابة صيغة للتنفيذ الفعلي للمعايير والمبادئ المتفق عليها دوليا.

وهذه المساهمة هي تحديث للمساهمة الوطنية لليابان المدرجة في التقرير A/78/76 لمراعاة التقدم الذي أمكن إحرازه بفضل قرار الجمعية العامة 16/78 ومواصلة المناقشات في إطار الفريق العامل المفتوح العضوية للفترة 2021-2025.

2 - النطاق/الأهداف

الغرض من برنامج العمل هو المساهمة في الحفاظ على السلام والاستقرار وتعزيز بيئة منفتحة وآمنة ومستقرة وميسّرة وسلمية لتكنولوجيا المعلومات والاتصالات.

وتحقيقا لهذه الغاية، ينبغي أن يسعى برنامج العمل، على وجه الخصوص، إلى تحقيق الأهداف التالية:

(أ) تقديم توصيات لتوجيه الجهود الوطنية الرامية إلى تنفيذ معايير ومبادئ سلوك الدول المسؤول؛

(ب) تشجيع الإبلاغ الطوعي عن الممارسات الوطنية من أجل تحديد احتياجات كل دولة عضو والتحديات التي تواجهها؛

(ج) تقديم دعم لبناء القدرات، يكون مصمما خصيصا لتلبية الاحتياجات ومواجهة التحديات، بناء على طلب البلدان المستفيدة؛

(د) أن يكون برنامج العمل شاملا ويضمن مشاركة واسعة من الدول الأعضاء ومن جهات متعددة من أصحاب المصلحة.

وعلاوة على ذلك، سيكون برنامج العمل منبرا دائما لإعطاء دفع للبنود المتكررة عن طريق تيسير المناقشات بشأن التهديدات القائمة والناشئة، وبشأن بلورة تدابير لبناء الثقة، وكذلك بشأن كيفية تطبيق القانون الدولي القائم على الفضاء السيبراني.

3 - الهيكل والمضمون

(أ) هيكل للنهوض بتنفيذ الإطار

عند تحديد نطاق برنامج العمل وهيكله ومضمونه، يمكن أن تكون جهود برنامج العمل المتعلق بمنع الاتجار غير المشروع بالأسلحة الصغيرة والأسلحة الخفيفة من جميع جوانبه ومكافحته والقضاء عليه مرجعا مفيدا. فبرنامج العمل المتعلق بالأسلحة الصغيرة يتضمن تدابير محددة على الصعيد الوطني والإقليمي والدولي. ويقدم كل بلد تقريرا طوعيا عما يشهده من تطورات قانونية ومؤسسية وعن ممارساته الأخرى، ويعقد اجتماعا سنويا للاستعراض.

أما بالنسبة لبرنامج العمل المتعلق بالمسائل السيبرانية، فينبغي أن يتضمن التقرير الطوعي قائمة مرجعية عن حالة تنفيذ المعايير في كل بلد، مثل حالة الجهود الرامية إلى وضع سياسات وقوانين ومبادئ توجيهية لحماية البنية التحتية الحيوية وحالة الاستجابة للحوادث في كل بلد أو منطقة. وسيكون من المفيد أن تحدد كل دولة عضو أيضا نوع بناء القدرات الذي تحتاجه وأن تذكره في تقريرها. ومن شأن هذه العملية أن تيسّر توفير إطار لدعم الممارسة الوطنية الرامية إلى تنفيذ المعايير في كل بلد.

وينبغي أن يشمل هيكل وطرائق برنامج العمل اجتماعات عامة منتظمة تُعقد سنويا أو مرتين في السنة في الأمم المتحدة. ويمكن للاجتماعات العامة لبرنامج العمل أن تعتمد توصيات قابلة للتنفيذ بشأن

جهود التنفيذ الوطنية، وأن تحدّث تلك التوصيات بانتظام. فعلى سبيل المثال، يمكن أن تحدد الاجتماعات العامة أولوية مواضيعية لتنفيذ الإطار، مثل تنفيذ معيار معيّن، والتهديدات القائمة والناشئة، وحماية البنية التحتية الحيوية، وما إلى ذلك.

ولدعم المزيد من تبادل الآراء بشأن هذا الموضوع، يمكن أن تقرر الاجتماعات العامة إنشاء مسارات عمل مكرسة، أو اجتماعات تقنية أو أفرقة عاملة مفتوحة العضوية، تنعقد في اجتماعات ما بين الدورات للاجتماعات العامة لبرنامج العمل وتقدم استنتاجاتها إلى الاجتماعات العامة التي تليها.

واستكمالا للمناقشات المتعلقة بتطور الإطار في المستقبل، ستعقد مؤتمرات استعراض في إطار برنامج العمل بوتيرة تحدد لاحقا لمراعاة التطور السريع للتكنولوجيا وتفادي تحولها إلى عبء ثقيل، لا سيما بالنسبة للوفود من البلدان النامية.

وسيكون الدليل العالمي لجهات الاتصال الذي وضعه الفريق العامل المفتوح العضوية الحالي جزءا لا يتجزأ من برنامج العمل لتنفيذ تدابير بناء الثقة وزيادة تطويرها.

(ب) بناء القدرات

سيدعم برنامج العمل جهود بناء القدرات المتصلة بتنفيذ الإطار، مع ضمان مشاركة العديد من الجهات صاحبة المصلحة.

وسيكون من المفيد أن يحدد برنامج العمل ما يوجد من ثغرات في قدرة الدول الأعضاء على تنفيذ الإطار وأن يستفيد من المبادرات القائمة في مجال بناء القدرات لكي يتسنى سد تلك الثغرات.

وخلال اجتماعات برنامج العمل، يمكن لممثلي منظمات أخرى (مثل مركز بناء القدرات في مجال الأمن السيبراني التابع لرابطة أمم جنوب شرق آسيا واليابان، والاتحاد الدولي للاتصالات، والصندوق الاستئماني المتعدد المانحين للأمن السيبراني التابع للبنك الدولي) أن يقدموا إحاطات من أجل ضمان التنسيق والتكامل بين أنشطة بناء القدرات التي يضطلع بها كل واحد من تلك الهياكل.

وينبغي أن يضطلع برنامج العمل بدور منبر تحت رعاية الأمم المتحدة من أجل بناء علاقات تآزر مع المنظمات الإقليمية الأخرى والاستفادة من الجهود التي تبذلها، بدلا من تنفيذ برامج لبناء القدرات بمعزل عنها.

(ج) القانون الدولي والقواعد الدولية

في أيار/مايو 2021، قامت اليابان بعرض ونشر الموقف الأساسي لحكومة اليابان من انطباق القانون الدولي على العمليات السيبرانية، وهي تؤكد من جديد أن القانون الدولي القائم، بما في ذلك ميثاق الأمم المتحدة بأكمله، ينطبق على العمليات السيبرانية. وهي تعرض موقفها الحالي من كيفية تطبيق القانون الدولي القائم على العمليات السيبرانية، مع التركيز على وجهات نظرها بشأن أهم المسائل وأبسطها. ولا تزال اليابان تأمل أن يؤدي إعلان حكومات مختلف الدول عن مواقفها الأساسية من انطباق القانون الدولي على العمليات السيبرانية ومن تطبيق القانون الدولي في المحاكم والهيئات القضائية الدولية والمحلية إلى تعميق الفهم الدولي المشترك لكيفية تطبيق القانون الدولي على العمليات السيبرانية في إطار برنامج العمل.

وسيشجع برنامج العمل أيضا الإبلاغ الطوعي عن جهود التنفيذ الوطنية، إما عن طريق إنشاء نظام إبلاغ خاص ببرنامج العمل أو عن طريق تعزيز الآليات القائمة (مثل الدراسة الاستقصائية الوطنية

لتنفيذ توصيات الأمم المتحدة بشأن استخدام الدول المسؤول لتكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي التي أعدها معهد الأمم المتحدة لبحوث نزع السلاح، أو التقارير الوطنية المقدّمة إلى الأمين العام). وسيشكل هذا الإبلاغ أساسا لتحديد الأولويات المتعلقة بتنفيذ الإطار ولمعرفة الاحتياجات من حيث بناء القدرات.

ويمكن أن تُجرى مناقشات في الاجتماعات العامة لبرنامج العمل بهدف تعميق فهم تطبيق القانون الدولي في الفضاء السيبراني. ويمكن أيضا إنشاء مسارات عمل مكرسة لتعزيز تبادل الآراء بشأن كيفية تطبيق القانون الدولي الحالي على العمليات السيبرانية. ويمكن استخدام مسار العمل المكرس، استنادا إلى الولاية التي تقررها الدول الأعضاء، لتبادل وجهات النظر الوطنية وإجراء مناقشات على أساس سيناريوهات. ويمكن أن تركز مسارات العمل المكرسة على القضايا العامة أو المفاهيم المحددة للقانون الدولي أو المجالات المواضيعية، مثل العمليات السيبرانية ضد البنية التحتية الحيوية، مع تغطية مبادئ القانون الدولي ذات الصلة.

(د) إشراك الجهات المتعددة صاحبة المصلحة

توجد الجهات صاحبة المصلحة في مكانة محورية من الفضاء السيبراني، سواء باعتبارها من المالكين أو المشغلين لعناصر البنية التحتية، أو باعتبارها تنوب عن المجتمعات المحلية في التعبير نفسها. وبالنظر إلى طابع الترابط في الفضاء السيبراني، يتعين إشراك الجهات المتعددة صاحبة المصلحة في مناقشات الأمم المتحدة.

وسيتيح برنامج العمل التفاعل والتعاون مع الجهات المتعددة صاحبة المصلحة، بما في ذلك من أجل السماح بأنشطة بناء القدرات على أفضل وجه ممكن.

4 - الأعمال التحضيرية وطرائق إنشاء الآلية المقبلة

تؤيد اليابان إجراء مزيد من المناقشات المركزة في إطار الفريق العامل المفتوح العضوية للفترة 2021-2025 لمواصلة بلورة الآلية المقبلة.

لاتفيا

[الأصل: بالإنكليزية
30 نيسان/أبريل 2024]

ظل إطار سلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات لفترة طويلة، منذ عام 2003، مدرجا في جدول أعمال اللجنة الأولى للجمعية العامة، ونوقِش في عدد من أفرقة الخبراء الحكوميين، وكذلك في أفرقة عاملة مفتوحة العضوية، مما يؤكد الأهمية المتزايدة للاستخدام المسؤول لتكنولوجيات المعلومات والاتصالات من أجل صون الاستقرار والأمن الدوليين. والتعاون بين الدول أمر حيوي للتصدي بفعالية للتهديدات المتزايدة في الفضاء السيبراني ولمد جسور الثقة بين الدول. ولهذه الأسباب، حان الوقت لاتخاذ قرار بشأن إنشاء آلية دائمة داخل الأمم المتحدة لمعالجة مسائل الأمن السيبراني في الأمد البعيد.

فالهجمات السيبرانية صارت أكثر تعقيدا وتدميرا وتواترا من أي وقت مضى في العالم الحديث المطبوع بالترابط. والمشهد السيبراني يتطور باستمرار. فالهجمات السيبرانية ضد البنية التحتية الحيوية

والهجمات ذات الدوافع السياسية والهجمات ببرمجيات انتزاع الفدية والاستخدام الخبيث للذكاء الاصطناعي آخذة في الازدياد. لذلك، لا أحد يمكن أن ينكر أهمية الأمن السيبراني في سياق مناقشة مسألة الأمن الدولي.

ومن أجل التصدي للأنشطة الخبيثة التي وصلت إلى مستوى غير مسبوق في الفضاء السيبراني، تعمل لاتفيا على زيادة أمنها السيبراني ومرونتها السيبرانية. ومن بين ما نقوم به في لاتفيا تنظيم وتنفيذ عمليات لضبط التهديدات السيبرانية على المستوى الوطني وداخل الاتحاد الأوروبي، وتبادُل مؤسساتنا الحكومية المعارف والخبرات مع المواطنين والكيانات العامة والخاصة. وفي عامي 2023 و 2024، أدانت لاتفيا مرارا، إلى جانب الدول الأعضاء الأخرى في الاتحاد الأوروبي، الأنشطة السيبرانية الخبيثة، بما في ذلك الهجمات السيبرانية التي تستهدف العمليات والمؤسسات الديمقراطية.

إن اقتراح إقامة "حوار مؤسسي منتظم" تحت رعاية الأمم المتحدة سبق أن نوقش في اللجنة الأولى، ووردت الإشارة إليه في التقرير النهائي للفريق العامل المفتوح العضوية للفترة 2019-2021[20]. وخلص الفريق العامل المفتوح العضوية للفترة 2019-2021 إلى أن أي آلية تُعتمد في المستقبل للحوار المؤسسي المنتظم ينبغي "أن تتخذ شكل إجراء عملي المنحى ومحدد الأهداف ومستند إلى النتائج السابقة، وأن تكون شاملة للجميع، وشفافة، ومدفوعة بتوافق الآراء، وقائمة على النتائج"[21]. وورد في التقرير المرحلي السنوي لعام 2023 الذي أعده الفريق العامل المفتوح العضوية للفترة 2021-2025، أن الدول اتفقت على عناصر مشتركة، أبرزها عناصر بشأن آلية دائمة أحادية المسار تتولى فيها الدول زمام الأمور[22].

والتهديدات السيبرانية المتنامية تتطلب تركيز قدرة الدول ومواردها على تعزيز أواصر التعاون والثقة بين الدول على المدى الطويل، بدلا من التركيز على مناقشات بشأن طرائق آلية جديدة تجري كل بضع سنوات وتنطوي على خطر تجزئة التقدم في المستقبل. ولاتفيا، بوصفها دولة صغيرة، تؤيد اتباع نهج أحادي المسار من شأنه أن ييسر الاستخدام الفعال للموارد المحدودة.

واستجابة للدعوة إلى إنشاء آلية دائمة للارتقاء بسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات وفق نهج متسق وطويل الأمد، اقتُرح وضع برنامج عمل[23]. وحظي قرار الجمعية العامة 37/77[24] بشأن برنامج العمل في عام 2022 وقرارها 16/78[25] بشأن برنامج العمل في عام 2023 بتأييد واسع من الدول في الجمعية العامة، وتم تطوير هذه المبادرة بطريقة شفافة وشاملة وتدريجية.

(20) التقرير النهائي للفريق العامل المفتوح العضوية للفترة 2019-2021، الفقرات 68 إلى 74.

(21) المرجع نفسه، الفقرة 74.

(22) التقرير المرحلي السنوي الثاني للفريق العامل المفتوح العضوية للفترة 2021-2025 (A/78/265)، الفقرة 55 (أ).

(23) https://documents.unoda.org/wp-content/uploads/2021/11/Working-paper-on-the-proposal-for-a-Cyber-PoA.pdf.

(24) قرار الجمعية العامة 37/77، برنامج العمل للارتقاء بسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي.

(25) قرار الجمعية العامة 16/78، برنامج العمل للارتقاء بسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي.

برنامج العمل باعتباره آلية دائمة للأمم المتحدة

ترى لاتفيا أن الجمعية العامة منحت، بموجب القرارين 37/77 و 16/78، ولاية قوية للمضي قدما في وضع برنامج العمل. وينبغي أن يكون برنامج العمل آلية دائمة وشاملة وعملية المنحى تقودها الدول داخل اللجنة الأولى ومنبرا تشارك من خلاله جميع الدول. وسيكون برنامج العمل موجها نحو تحقيق الهدف الأسمى المتمثل في الإسهام في تعزيز السلام والأمن الدوليين ومنع نشوب النزاعات وحالات سوء التفاهم بين الدول. وينبغي أن يشمل نطاق برنامج العمل المسائل المتعلقة باستخدام تكنولوجيات المعلومات والاتصالات وفقا للقانون الدولي وتنفيذ إطار الأمم المتحدة لسلوك الدول المسؤول في الفضاء السيبراني. وكما هو مذكور في قرار الجمعية العامة 37/77، فإن برنامج العمل "سيأخذ في الاعتبار النتائج القائمة على توافق الآراء التي اعتمدها الفريق العامل المفتوح العضوية للفترة 2021-2025"[26].

وسيتم تعزيز الاستقرار والأمن في الفضاء السيبراني من خلال دعم تنفيذ إطار سلوك الدول المسؤول، ومواصلة تطويره، متى تعين[27]، استنادا إلى القانون الدولي، بما في ذلك ميثاق الأمم المتحدة برمته. وعلى نحو ما حصل عليه الاتفاق في تقارير فريق الخبراء الحكوميين للأعوام 2013 و 2015 و 2021، وفي تقريري الفريق العامل المفتوح العضوية لعامي 2021 و 2022، فإن القانون الدولي، بما في ذلك القانون الدولي الإنساني، ينطبق وضروري لصون السلام والأمن والاستقرار في الفضاء السيبراني.

ومن أجل النهوض بتنفيذ إطار سلوك الدول المسؤول، سيدعم برنامج العمل أنشطة بناء القدرات ذات الصلة وبحسب الحاجة. ومن المهم النهوض بالعمل الجماعي بشأن بناء القدرات وتبادل الخبرات وأفضل الممارسات لتحسين القدرة على الصمود على الصعيدين الوطني والعالمي في وجه التهديدات السيبرانية.

ويمكن أن تعقد دورات رسمية سنوية في إطار برنامج العمل. وفي الفترات الفاصلة بين الدورات الرسمية، يمكن تنظيم عمل برنامج العمل في إطار أفرقة عاملة تقنية تُكرَّس لقضايا محددة. فعلى سبيل المثال، يمكن أن يُعنى فريق عامل تقني بزيادة تحسين فهم كيفية انطباق القانون الدولي على استخدام تكنولوجيات المعلومات والاتصالات. وتُعتمَد في الدورات الرسمية التوصيات التي تعدها الأفرقة العاملة التقنية. وينبغي القيام بشكل دوري باستعراض الأولويات الأخرى لبرنامج العمل خلال مؤتمرات الاستعراض.

ويمكن إنشاء الأفرقة التقنية وإنهاؤها بقرارات تُتخذ في الدورات الرسمية. ويجب أن تكون الأفرقة العاملة التقنية شاملة ومفتوحة أمام جميع الدول، على نحو يكفل مشاركة الخبراء الوطنيين عبر الإنترنت أو حضوريا (بشكل هجين). وينبغي أن تتخذ القرارات بشأن الأفرقة التقنية وطرائق عملها مع مراعاة قدرات الدول الصغيرة ومواردها.

ويعد الحوار المنتظم والكامل مع الجهات صاحبة المصلحة – المجتمع المدني والقطاع الخاص والأوساط الأكاديمية – أمرا ضروريا وينبغي تيسيره من خلال برنامج العمل. فخبرات هذه الجهات في المجال السيبراني الدائب التطور لا تقدر بثمن، وبالتالي فإن مدخلاتها مهمة للنهوض بإعمال سلوك الدول المسؤول.

(26) قرار الجمعية العامة 37/77، الفقرة 2.

(27) قرار الجمعية العامة 19/76، الفقرة 10 من الديباجة.

وتقع أيضا على الجهات صاحبة المصلحة "مسؤولية استخدام تكنولوجيا المعلومات والاتصالات بطريقة لا تعرِّض السلام والأمن للخطر"[28] كما أنها هي من يقود تطوير التكنولوجيات الجديدة.

وينبغي أن يُنظَّم في عامي 2024 و 2025 المزيد من المناقشات المركزة في الدورات المتبقية والاجتماعات التي تعقد فيما بين الدورات للفريق العامل المفتوح العضوية للفترة 2021-2025 بهدف مواصلة بلورة الجوانب المختلفة لبرنامج العمل، بما في ذلك طرائق وضع برنامج العمل. وينبغي أن يكون برنامج العمل جاهزا لأداء وظائفه عند اختتام أعمال الفريق العامل المفتوح العضوية للفترة 2021-2025.

هولندا (مملكة -)

[الأصل: بالإنكليزية
1 أيار/مايو 2024]

مقدمة

لا تزال هولندا يساورها قلق بالغ من تنامي الأخطار المحدقة بالأمن والاستقرار الدوليين والتنمية الاقتصادية والاجتماعية وسلامة ورفاه الأفراد من جراء استخدام الجهات الفاعلة من الدول ومن غير الدول لتكنولوجيات المعلومات والاتصالات في أغراض خبيثة. ومن الملاحظ أيضا أن تفاوت الدول من حيث مستويات القدرات المتصلة بأمن تكنولوجيا المعلومات والاتصالات يمكن أن يزيد من الهشاشة في عالم يزداد ترابطا.

وللتصدي هذه التحديات، ومن خلال عمل سلسلة من العمليات الحكومية الدولية، وضعت الدول إطارا تراكميا ومتطورا لسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي. وقد أيدت الجمعية العامة هذا الإطار عدة مرات في قرارات اتُّخذت بتوافق الآراء.

ولمواصلة هذه الإنجازات، تشدد هولندا على ضرورة إقامة حوار مؤسسي منتظم بعد اختتام أعمال الفريق العامل الحالي المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025، المنشأ عملا بقرار الجمعية العامة 240/75 وتحقيقا لهذه الغاية، تؤيد هولندا المبادرة الرامية إلى وضع برنامج عمل في المستقبل للارتقاء بسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي، الذي رحبت به الجمعية العامة في قراريها 37/77 و 16/78.

وعملا بالفقرة 8 من منطوق القرار 237/78 المعنون "التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي"، تقدم هولندا هنا آراءها وتقييماتها بشأن أمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها، ولا سيما بشأن الجولة المقبلة للحوار المؤسسي المنتظم حول هذه المسائل المتوخى أن تُعقد برعاية الأمم المتحدة. وتستند الآراء الواردة أدناه إلى المذكرة التي قدمتها هولندا إسهاما في إعداد تقرير الأمين العام المقدم عملا بالقرار 37/77 (A/78/76).

وقد أُحرز في إطار الفريق العامل المفتوح العضوية للفترة 2021-2025 تقدم ذو بال نحو إيجاد أرضية مشتركة بشأن الآلية المستقبلية للحوار المؤسسي المنتظم بشأن الأمن الدولي لتكنولوجيا المعلومات والاتصالات. وترحب هولندا في هذا الصدد بالعناصر المشتركة للحوار المؤسسي المنتظم الواردة في التقرير

(28) التقرير النهائي للفريق العامل المفتوح العضوية للفترة 2019-2021، الفقرة 10.

المرحلي السنوي لعام 2023 للفريق العامل المفتوح العضوية. وتبقى هولندا ملتزمة بإحراز مزيد من التقدم في هذا الشأن في إطار الفريق العامل المفتوح العضوية للفترة 2021-2025.

النطاق والأهداف

إن هولندا، وإذ تعيد تأكيد الفقرة 4 من منطوق قرار الجمعية العامة 16/78، ترى أنه ينبغي إنشاء آلية تحت رعاية الأمم المتحدة، عند اختتام أعمال الفريق العامل المفتوح العضوية للفترة 2021-2025 وفي موعد أقصاه عام 2026، تكون آلية دائمة وشاملة وعملية المنحى، وتكون شاملة للأهداف المحددة المؤكدة في قرار الجمعية العامة 37/77 وللعناصر المشتركة للحوار المؤسسي المنتظم في المستقبل حسبما اتُّفق عليه بتوافق الآراء في التقرير المرحلي السنوي لعام 2023 للفريق العامل المفتوح العضوية للفترة 2021-2025.

وتؤيد هولندا المبادرة الرامية إلى وضع برنامج عمل تحت رعاية الأمم المتحدة للارتقاء بسلوك الدول المسؤول في الفضاء السيبراني في سياق الأمن الدولي. وينبغي أن يستند برنامج العمل إلى العناصر المشتركة للجولة المقبلة من الحوار المؤسسي المنتظم المتفق عليها بتوافق الآراء في التقرير المرحلي السنوي لعام 2023 للفريق العامل المفتوح العضوية، وإلى القرارات الأساسية المتعلقة بالنطاق والهيكل والمضامين والطرائق وفق النتائج التي يتوصل إليها الفريق العامل المفتوح العضوية للفترة 2021-2025.

الهيكل والطرائق

تشاطر هولندا الرأي القائل بأن برنامج العمل ينبغي أن يكون عملية شاملة للجميع، وشفافة، ومدفوعة بتوافق الآراء، وقائمة على النتائج. ويمكن أن يستمد برنامج العمل ولايته من وثيقة تأسيسية تؤكد الالتزام السياسي للدول بالاسترشاد بإطار سلوك الدول المسؤول في الفضاء السيبراني، وينشئ آلية لمواصلة تفعيل أهدافه.

وينبغي أن يكون برنامج العمل مفتوحا لمشاركة جميع الدول الأعضاء في الأمم المتحدة والمراقبين الدائمين والمنظمات الحكومية الدولية وغيرها من المنظمات والوكالات المتخصصة. فبينما تتحمل الدول المسؤولية الرئيسية عن صون السلام والأمن الدوليين، ينبغي أن يسمح برنامج العمل أيضا بالمشاركة المجدية، بما في ذلك في المحافل الرسمية، للجهات المعنية غير الحكومية صاحبة المصلحة، بما في ذلك القطاع الخاص والأوساط الأكاديمية والمجتمع المدني.

ويمكن أن يتألف هيكل برنامج العمل مما يلي:

(أ) مؤتمرات استعراض دورية لتقييم المشهد المتطور للتهديدات السيبرانية ومبادرات برنامج العمل، وتحديث الإطار حسب الاقتضاء، وتقديم التوجيه الاستراتيجي؛

(ب) مناقشات عامة مفتوحة العضوية لمناقشة التهديدات القائمة والناشئة، ولمواصلة مناقشة كيفية تطبيق القانون الدولي، ومناقشة تنفيذ تدابير بناء الثقة، وتحديد أولويات بناء القدرات، والنظر في تنفيذ المعايير والقواعد والمبادئ، وتقديم التوجيه للاجتماعات التقنية المفتوحة والمبادرات العملية؛

(ج) اجتماعات تقنية مفتوحة و/أو أفرقة عاملة لإجراء مناقشات عملية المنحى مفتوحة لمشاركة الجهات المعنية صاحبة المصلحة، ومكرسة لقضايا محددة.

الأعمال التحضيرية وطرائق وضع برنامج العمل

يقدم قرارا الجمعية العامة 16/78 و 37/77 وتقرير الأمين العام (A/78/76) خريطة طريق أولية نحو إنشاء برنامج العمل. ففي الفترة 2025-2026، وبعد اختتام أعمال الفريق العامل المفتوح العضوية، تعتزم هولندا عقد مؤتمر دولي، يكون مفتوحا للجهات غير الحكومية صاحبة المصلحة، ويستند إلى الأعمال التحضيرية المنجزة، بما في ذلك في إطار الفريق العامل المفتوح العضوية للفترة 2021-2025، بغية اعتماد الوثيقة التأسيسية و/أو الإعلان السياسي.

بناء القدرات ضمن آلية مستقبلية

دون المساس بالنتائج التي سيخلص إليها الفريق العامل المفتوح العضوية وما تقرره الجمعية العامة بشأن إنشاء آلية مستقبلية، تقترح هولندا العناصر التالية لتيسير بناء القدرات السيبرانية من أجل النهوض بتنفيذ الإطار المتطور والتراكمي وتعزيز التعاون الدولي في هذا الصدد. ويتمحور هذا الاقتراح حول دورة من أربع خطوات:

(أ) تبادل الآراء بشأن واقع التهديدات من خلال تبادل الخبرات التقنية بشأن التهديدات والنظر في كيفية التصدي لهذه التهديدات من منظور الإطار التوافقي لسلوك الدول المسؤول في الفضاء السيبراني؛

(ب) التحديد الذاتي للاحتياجات من القدرات من خلال الإبلاغ الطوعي في ضوء الإطار التراكمي والمتطور لسلوك الدول المسؤول. ويمكن استخدام الأساليب القائمة للإبلاغ الطوعي، مثل الدراسة الاستقصائية الوطنية لتنفيذ توصيات الأمم المتحدة بشأن استخدام الدول المسؤول لتكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي التي أعدها معهد الأمم المتحدة لبحوث نزع السلاح (مبادرة مشتركة بين المكسيك وأستراليا)؛

(ج) التوفيق بين الاحتياجات والموارد. فالآلية المقبلة يمكن أن تعمل باعتبارها منبرا لعقد الاجتماعات. وعلاوة على ذلك، وبالنظر إلى الطابع العالمي للأمم المتحدة والاعتراف بها، يمكن للأمانة العامة للأمم المتحدة أن تقوم بدور في تيسير التنسيق بشأن عمل المنظمات والهياكل في مجال بناء القدرات السيبرانية. ويمكن أن تستند الآلية المقبلة إلى الأدوات القائمة مثل بوابة سيبيل (Cybil) التابعة للمنتدى العالمي للخبرات السيبرانية، وربما أيضا إلى المقترحات التي ينظر فيها حاليا الفريق العامل المفتوح العضوية للفترة 2021-2025، مثل فهرس بناء القدرات والبوابة العالمية للتعاون في مجال الأمن السيبراني التي اقترحت الدول الأعضاء إنشاءها؛

(د) حلقة لإبداء التعليقات تتبادل من خلالها الدول خبراتها فيما تبذله من جهود التنفيذ وأنشطة بناء القدرات السيبرانية، ويمكن أن تفيد في إجراء مزيد من المناقشات بشأن استخدام الدول لتكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي.

وجهود بناء القدرات التي ستُبذل في إطار الآلية المقبلة ينبغي أن تكون منسجمة مع مبادئ بناء القدرات المتفق عليها في التقرير المرحلي السنوي لعام 2023 للفريق العامل المفتوح العضوية.

نيوزيلندا

[الأصل: بالإنكليزية
30 نيسان/أبريل 2024]

1 - لقد ظل موضوع الأمن السيبراني مطروحا للنقاش بين الدول، تحت رعاية الأمم المتحدة، لمدة أكثر من 20 عاما. وقد أتاحت الأفرقة العاملة المتعاقبة - أي أفرقة الخبراء الحكوميين والأفرقة العاملة المفتوحة العضوية - الفرصة لتبادل الآراء بانتظام بشأن المسائل المتعلقة بالأمن السيبراني في سياق الأمن الدولي.

2 - وقد أحرزت هذه الأفرقة العاملة نتائج تأسيسية مهمة تسهم مجتمعة في الأمن والاستقرار الدوليين من خلال وضع إطار لسلوك الدول المسؤول في الفضاء السيبراني، إطار أقرته الجمعية العامة للأمم المتحدة ويقوم على أربع ركائز:

- القانون الدولي: يتفق أعضاء الأمم المتحدة جميعهم على أن القانون الدولي ينطبق على سلوك الدول في الفضاء السيبراني
- معايير سلوك الدول المسؤول على الإنترنت في وقت السلم
- تدابير بناء الثقة لدعم الشفافية ووضوح الرؤية والاستقرار
- تدابير بناء الثقة حتى تتمكن جميع الدول من الحد من المخاطر المرتبطة بزيادة الاتصال الإلكتروني، مع الاستمرار في الاستفادة من هذه الزيادة

3 - وتؤيد نيوزيلندا كل التأييد ما قررته الجمعية العامة في قرارها 237/78 من إنشاء لآلية تحت رعاية الأمم المتحدة، عند اختتام أعمال الفريق العامل المفتوح العضوية للفترة 2021-2025، وفي موعد أقصاه عام 2026، تكون آلية دائمة وشاملة وعملية المنحى، وتشمل الأهداف المحددة المؤكدة في قرار الجمعية العامة 37/77، والعناصر المشتركة للحوار المؤسسي المنتظم في المستقبل حسبما اتُّفق عليه بتوافق الآراء في التقرير المرحلي السنوي لعام 2023 للفريق العامل المفتوح العضوية للفترة 2021-2025.

4 - ونتوقع أن تكون هذه الآلية بمثابة "المقر الدائم" لمناقشات الأمن السيبراني في سياق الأمن الدولي في الأمم المتحدة، في ختام أعمال الفريق العامل المفتوح العضوية الحالي للفترة 2021-2025، وبناء على الاقتراح المعتمد في قراري الجمعية العام 37/77 و 237/78. ونحن نرحب بالقرار الذي عرضته فرنسا، باسم مجموعة عبر إقليمية، ونؤيده، إذ يتيح القرار مسارا واضحا وشفافا لجميع الدول لتنظر في نطاق الآلية المقبلة وهيكلها ومضمونها وطرائقها على نحو مكمل للفريق العامل المفتوح العضوية الحالي. وفي هذا الصدد، نؤيد وضع برنامج عمل يكون:

(أ) الآلية الدائمة الوحيدة لإجراء مناقشات الأمم المتحدة بشأن الأمن السيبراني بعد عام 2025، مما يضمن القدرة على التنبؤ والاستقرار المؤسسي. ومن شأن التفاوض على طرائق متفق عليها لإنشاء آلية دائمة أن يحقق أيضا مكاسب من حيث الكفاءة في الأجل الطويل. وقد تطلبت إعادة النظر في طرائق عمل الأفرقة العاملة المتعاقبة والاتفاق عليها مفاوضات مطوّلة ومتكررة، مما استغرق الكثير من الوقت الذي كان ينبغي تخصيصه للمناقشات الموضوعية الهامة؛

(ب) قائمًا على الإطار المتفق عليه لسلوك الدول المسؤول في الفضاء السيبراني، بما في ذلك الانسجام مع التزامات القانون الدولي والقانون الدولي لحقوق الإنسان، بما يكفل أن يكون برنامج العمل معتمدا على ومعززا للعمل التأسيسي الذي قامت به أفرقة الخبراء الحكوميين والأفرقة العاملة المفتوحة العضوية المتعاقبة للارتقاء بسلوك الدول المسؤول على الإنترنت؛

(ج) شاملًا لمشاركة العديد من الجهات صاحبة المصلحة بما في ذلك الحكومات (التي تتحمل المسؤولية عن صون السلام والأمن الدوليين في الفضاء السيبراني) والشركات والمجتمع المدني والخبراء التقنيون والأكاديميون والمنظمات الأخرى الذين يساهمون في شبكة إنترنت حرة ومفتوحة وآمنة وقابلة للتشغيل البيني. وتؤيد نيوزيلندا الطرائق التي تتيح مشاركة الجهات صاحبة المصلحة غير الحكومية (بما في ذلك بتقديم بيانات وتقارير خطية) في المناقشات، بما في ذلك في أي اجتماع رسمي وغير رسمي وفي مؤتمرات الاستعراض؛

(د) عمليَّ المنحى، بما في ذلك بالتركيز على التدابير العملية للدفع قُدما بإطار سلوك الدول المسؤول وتعزيز تدابير بناء القدرات التي تدعم الدول في تنفيذ الإطار وآليات المساءلة والرصد؛

(هـ) مرنًا وقابلا للتكييف، للتعامل مع التهديدات الناشئة.

الاتحاد الروسي

[الأصل: بالروسية
9 نيسان/أبريل 2024]

ورقة مفاهيمية بشأن إنشاء فريق عامل دائم مفتوح العضوية له صلاحية صنع القرار بشأن أمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها

من إعداد: الاتحاد الروسي، ودولة إريتريا، وبوركينا فاسو، وجمهورية بوروندي، وجمهورية بيلاروس، والجمهورية العربية السورية، وجمهورية كوريا الشعبية الديمقراطية، وجمهورية زمبابوي، وجمهورية السودان، وفنزويلا (جمهورية – البوليفارية)، وجمهورية كوبا، وجمهورية مالي، وجمهورية اتحاد ميانمار، وجمهورية نيكاراغوا

تبيّن من المناقشات التي دارت في إطار فريق الأمم المتحدة العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021–2025 أن المجتمع الدولي يطالب بإنشاء آلية دائمة وحيدة لصنع القرار بشأن هذه المسألة تعمل برعاية الأمم المتحدة. ونحن نعتقد أن الشكل الأمثل الذي يمكن أن تتخذه هذه الآلية هو شكل الفريق العامل المفتوح العضوية الذي ثبتت عملياً فعاليته وأهميته.

وأيّ فريق عامل دائم ومفتوح العضوية يُنشأ في المستقبل وتكون له صلاحية صنع القرار ينبغي أن تركّز ولايته على مواصلة تعزيز بيئة منفتحة وآمنة ومستقرة وميسّرة وسلمية لتكنولوجيا المعلومات والاتصالات من خلال التنفيذ العملي للاتفاقات التي تم التوصل إليها في إطار الفريق العامل المفتوح العضوية للفترة 2021–2025. وتشمل المسائل المندرجة في إطار تلك الولاية ما يلي:

- مواصلة وضع قواعد ومعايير ومبادئ ملزِمة قانوناً بشأن السلوك المسؤول للدول وإنشاء آليات فعالة لتنفيذها، بوصف ذلك عنصرا في معاهدة عالمية تُبرم في المستقبل بشأن ضمان أمن المعلومات على الصعيد الدولي؛

- التوصل إلى فهم مشترك لكيفية انطباق القانون الدولي على استخدام تكنولوجيات المعلومات والاتصالات وكيفية تكييف المعايير القائمة لتتوافق مع خصوصيات فضاء المعلومات (من حيث بُعده العابر للحدود، وخاصيات إخفاء الهوية، وإمكانية إدخال خاصيات غير معلنة)؛

- وضع وتنفيذ تدابير وآليات لبناء الثقة لأغراض التعاون العملي بين الدول، بما في ذلك من خلال قنوات الاتصال القائمة بين الكيانات/الهيئات المأذون لها وعن طريق دليل حكومي دولي عالمي لجهات الاتصال، من أجل التصدي لمخاطر أمن المعلومات المرتبطة بتكنولوجيات المعلومات والاتصالات واستخدامها ومن أجل منع نشوب النزاعات بين الدول في فضاء المعلومات العالمي؛

- إنشاء آليات وبرامج لمساعدة الدول في تحسين قدرتها على حماية مواردها الوطنية من المعلومات، مع مراعاة الاحتياجات الخاصة لكل منها.

وينبغي أن تشكّل المبادئ التالية الأساسَ الذي يقوم عليه أي فريق عامل دائم مفتوح العضوية يُنشأ في المستقبل:

- الانفتاح وشمول الجميع والديمقراطية والشفافية؛

- اضطلاع الدول بدور قيادي في تعزيز الحوار بشأن أمن استخدام الدول لتكنولوجيات المعلومات والاتصالات، برعاية اللجنة الأولى التابعة للجمعية العامة للأمم المتحدة؛

- الامتثال لمبادئ ميثاق الأمم المتحدة (المساواة في السيادة بين الدول، والامتناع عن استخدام القوة والتهديد باستخدامها، والتسوية السلمية للمنازعات الدولية)؛

- أن تختص الدول دون سواها باتخاذ أي قرارات وأن يكون ذلك بتوافق الآراء؛

- ألا تكون هناك ازدواجية في الجهود الدولية الرامية إلى ضمان أمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها بحيث تتكرر الجهود نفسها في عدة محافل تفاوضية للأمم المتحدة؛

- الاستمرارية في تنفيذ النتائج والتوصيات المعتمدة بتوافق الآراء في إطار ما أُنشئ سابقاً من أفرقة عاملة مفتوحة العضوية وأفرقة للخبراء الحكوميين؛

- المرونة وقابلية التطور للتوافق مع التغير في احتياجات الدول والتحديات الجديدة التي تنشأ في مجال أمن تكنولوجيا المعلومات والاتصالات.

مسائل إجرائية:

- أي قرارات تتخذ في إطار الفريق العامل الدائم المفتوح العضوية ينبغي اعتمادها بتوافق الآراء بين الدول (ينبغي أن يُذكر هذا المعيار بوضوح في قرار الجمعية العامة المنشئ للفريق العامل الدائم المفتوح العضوية)؛

- الإطار الزمني: ينبغي أن يستهل الفريق العامل الدائم المفتوح العضوية أعماله عند اختتام الفريق العامل الحالي المفتوح العضوية أعماله، وينبغي أن يعقد دورتين رسميتين في السنة في مقر الأمم المتحدة بنيويورك (تكون جميع الدول الأعضاء دون استثناء ممثَّلة فيهما)؛

- شكل التقارير: تقارير مرحلية تقدم إلى الجمعية العامة للأمم المتحدة، وتعتمد بتوافق الآراء مرة كل سنتين؛

- الهيكل: يجوز للدول الأعضاء في الأمم المتحدة، حسب الاقتضاء، أن تقرر إنشاء أفرقة فرعية تتناول جوانب محدّدة من الولاية بشكل أكثر تفصيلا وتعمّقا. غير أن اجتماعات هذه الأفرقة الفرعية ينبغي ألا تكون متزامنة حتى يتسنى ضمان المشاركة الكاملة لجميع الوفود؛

- إدارة العمل: يتولى إدارة أعمال الفريق العامل الدائم المفتوح العضوية مكتبٌ يتألف من رئيس ونائبين للرئيس ومقرِّر، ويضم إذا لزم الأمر رؤساءَ الأفرقة الفرعية (ويكون لهم أيضا مركز نواب الرئيس). وتوافق الدول على تشكيلة المكتب كل سنتين بتوافق الآراء، وتقوم هذه التشكيلة على أساس التوزيع الجغرافي العادل وعلى أساس التناوب بين المجموعات الإقليمية.

ويُستصوب أن يُجهَّز الفريق العامل الدائم المفتوح العضوية بآلية لإضفاء الطابع الرسمي سريعاً على القرارات التي يُتفق عليها (بموجب إجراء الموافقة الصامتة ثم الموافقة اللاحقة في الدورة التالية). وينبغي اتخاذ خطوات عملية لضمان استمرارية تبادل المعلومات بين الدول من خلال بوابة إلكترونية مناسبة.

ويكون من المفيد توخي قيام علاقة تعاون بين الفريق العامل الدائم المفتوح العضوية وبين المنظمات والرابطات الإقليمية ذات الصلة عن طريق مشاورات يجريها رئيسه مع مجموعات البلدان ومن خلال اجتماعات لما بين الدورات تُعقد مع ممثليها مرة في السنة.

وينبغي أن تكون مشاركة الجهات غير الحكومية (المنظمات غير الحكومية، ودوائر الأعمال التجارية، والأوساط العلمية والأكاديمية) في أعمال الفريق العامل الدائم المفتوح العضوية ذات طابع تشاوري بحت وغير رسمية بالمرة؛ ويكون ذلك، على سبيل المثال، من خلال اجتماعات لما بين الدورات تُعقد مرة واحدة في السنة. ولا يُمنَح حق حضور المناسبات الرسمية بصفة مراقب إلا الجهات غير الحكومية المعتمدة (ويكون اعتمادها بتوافق الآراء بين الدول).

سنغافورة

[الأصل: بالإنكليزية
1 أيار/مايو 2024]

لا تزال سنغافورة ملتزمة بإجراء حوار عالمي مفتوح وشامل بشأن الأمن السيبراني، وفي هذا الصدد نرى أن التزام جميع الدول بعقد جولة مقبلة أحادية المسار للحوار المؤسسي المنتظم يكتسي أهمية قصوى. ومن الأهمية بمكان عقدُ جولة مقبلة أحادية المسار للحوار المؤسسي المنتظم لتعزيز القبول والاعتراف على نطاق عالمي بالإطار التراكمي والمتطور لسلوك الدول المسؤول في استخدام تكنولوجيا المعلومات والاتصالات الذي وافقت عليه جميع الدول الأعضاء في الأمم المتحدة منذ عام 1998، وتوفيرُ منصة عالمية مشتركة لمواصلة تطوير وتنفيذ هذا الإطار. وفي هذا الصدد، من المهم أن تتمكن جميع الدول من تركيز جهودها على عملية واحدة لضمان أن تظل المناقشات موضوعية وألا تكون عرضة للتشتت.

كما أن الدول الصغيرة والنامية المحدودة الموارد لن تكون قادرة على المشاركة على نحو مستدام في عمليات موازية مزدوجة المسار.

وتعتقد سنغافورة أنه ينبغي لنا أن نواصل البناء على العناصر الأربعة المشتركة لجولة الحوار المؤسسي المنتظم المتفق عليها في التقرير المرحلي السنوي الثاني للفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025 (A/78/265، الفقرة 55) لبناء الثقة والاطمئنان اللذين نحتاجهما للتوصل إلى توافق على آلية دائمة أحادية المسار.

ومن المهم أن تستخدم الدول الوقت والحيز المتبقيين المحدودين للعمل على بناء رؤية مشتركة بشأن سبل المضي قدما لعقد جولة مقبلة للحوار المؤسسي المنتظم في إطار الفريق العامل الحالي. وينبغي للمهمة المطروحة ذات الأولوية أن تكون بناء توافُق. وفي هذا الصدد، تؤيد سنغافورة الاقتراح الذي قدمته البرازيل في الدورة الموضوعية السابعة للفريق العامل الداعي إلى وقف اختياري لطرح القرارات المتصلة بأمن تكنولوجيا المعلومات والاتصالات في اللجنة الأولى للجمعية العامة للأمم المتحدة إلى أن يختتم الفريق العامل الحالي أعماله في عام 2025. ونؤيد أن يواصل رئيس الفريق العامل إجراء مناقشات حول سبل المضي في جولة الحوار المؤسسي المنتظم بهدف مواصلة تطوير وتعديل اقتراح توافقي حول هذا الحوار.

وكخطوة تالية، نعتقد أنه سيكون من المفيد للفريق العامل الحالي أن يتفق على نطاق الاجتماعات وتنظيمها وأهدافها ووتيرتها في إطار الآلية المقبلة. والإجابة على هذه الأسئلة العملية هي طريقة منطقية للبناء على العناصر المشتركة التي سبق لجميع الدول أن وافقت عليها. وسيوفر القيام بذلك أيضا للوفود، ولا سيما الوفود الأصغر حجما المحدودة الموارد، وضوحا مبكرا بشأن عملها بعد عام 2025، ما يتيح لها البدء في التخطيط اللازم لتحسين مشاركتها المثلى بطريقة مجدية. ولضمان أساس مستدام لآلية عالمية دائمة أحادية المسار، تشدد سنغافورة أيضا على أن تصميم الآلية المقبلة يجب أن يكون واسعا وملائما بما فيه الكفاية لتيسير المناقشات المستمرة والمقبلة بشأن مقترحات وأولويات جميع الوفود. وعلى وجه الخصوص، سيكون من المفيد إجراء استعراض دوري لعمليات الآلية الدائمة للتأكد من أن النهُج التي نتّبعها هي ذات صلة بالمشهد الدينامي للتهديدات التشغيلية. وفي هذا الصدد، تؤيد سنغافورة النهج والهيكل المعروضين في ورقة المناقشة التي أعدها الرئيس المؤرخة 20 شباط/فبراير 2024 بشأن مشاريع عناصر الآلية الدائمة. وتتطلع سنغافورة إلى العمل بشكل بنّاء مع جميع الوفود على مواصلة تعديل مشاريع العناصر هذه تمهيدا لاعتمادها بالتوافق في التقرير المرحلي السنوي الثالث للفريق العامل الحالي.

تركيا

[الأصل: بالإنكليزية]
[1 أيار/مايو 2024]

أصبحت تكنولوجيا المعلومات والاتصالات جزءا لا غنى عنه من المجتمع والاقتصاد بما لها من تأثير على كل جانب من جوانب الحياة. ويستخدم الأفراد والدول هذه التكنولوجيا في العديد من المجالات. واليوم، تؤدي مهارات الدول في تطوير واستخدام التكنولوجيا دورا هاما في التنمية والنمو. وباتت تكنولوجيا المعلومات العاملَ الرئيسي للتنمية في كل مجال تقريبا، بدءاً من النقل والاتصالات، ومرورا بالصناعات الدفاعية والعلوم الطبية، ووصولا إلى الإنتاج والتعليم والتجارة.

وتشير الدراسات إلى أن الاتجاهات التكنولوجية ستتسارع في السنوات القليلة المقبلة. ومن هذه الاتجاهات، تلك القادرة على استحداث معايير تكنولوجية وخطوط أعمال وإجراء تغييرات بارزة في المعايير الحالية. وتُعتبر إنترنت الأشياء، والجيل الخامس للاتصالات 5G، والبيانات الضخمة وتقنية سلسلة الكتل blockchain، والذكاء الاصطناعي والمركبات الذاتية القيادة، والروبوتات الذكية، تكنولوجيات ستلقي الضوء على المسار الذي سيسلكه حاضرنا ومستقبلنا.

ومن ناحية أخرى، ومع أن هذه التكنولوجيات تتيح لنا العديد من الفرص، فإنها تحمل في طياتها أيضا مخاطر الأمن السيبراني. وأصبحت هياكل التهديدات السيبرانية أكثر تعقيدا وباتت أعدادها تتزايد يوما بعد يوم، وتبيَّن، وفقا للبحوث، أنه سيكون هناك أكثر من 493 مليون محاولة تستخدم برمجيات انتزاع الفدية في أنحاء العالم خلال عام 2022[29].

وفي هذا الصدد، يشكل الأمن السيبراني مسألة تتعين معالجتها في كل مرحلة من أجل تطوير التكنولوجيا وإدماجها على نحو سليم. فقد تتسبب مواطن الضعف الأمنية التي تشوب نظُم المعلومات والاتصالات في خروج هذه النظم من الخدمة أو إساءة استخدامها، و/أو فقدان الأرواح، و/أو إلحاق أضرار اقتصادية واسعة النطاق، و/أو تعطيل النظام العام، و/أو انتهاك الأمن القومي.

وعليه، فإن ضمان الأمن السيبراني ليس فقط ضرورةً لمكافحة التهديدات في المجالات التي تستخدم التكنولوجيا بكثافة، بل هو أيضا عامل هام يمسّ برفاه البلدان وأمنها القومي بسبب ما تحمله من مخاطر على مسار الحياة الاجتماعية والاقتصادية. وفي ضوء كل هذه التطورات، تنفق البلدان مبالغ طائلة في مجال الأمن السيبراني، وتطوِّر تكنولوجيا الأمن السيبراني، وتوجه جهودها لضمان أمنها في البيئة السيبرانية وزيادة مقاومتها للهجمات.

إن مسألة مكافحة التهديدات السيبرانية تُعتبر سياسة وطنية في بلدنا. وفي هذا السياق، تجري وزارة النقل والبنية التحتية دراسات لضمان الأمن السيبراني الوطني على المستوى الاستراتيجي كما تجري هيئة تكنولوجيا المعلومات والاتصالات دراسات على المستوى التقني. وإضافة إلى ذلك، تسهم مؤسسات ومنظمات أخرى أيضا في هذه الدراسات.

وفي إطار الدراسات التي تجرى منذ عام 2012، أُعدت ونُفذت "الاستراتيجية وخطط العمل الوطنيتان للأمن السيبراني". وفي الآونة الأخيرة، ووفقا لـ "الاستراتيجية وخطة العمل الوطنيتان للأمن السيبراني (2020–2023)"، أُجريت دراسات لحماية الأمن السيبراني للبنى التحتية الحيوية على مدار الساعة، وزيادة كفاءة فرق الاستجابة للحوادث السيبرانية، والاستخدام الآمن للفضاء السيبراني من قبل جميع شرائح المجتمع، وإبقاء التوعية بالأمن السيبراني على مستوى عال، وتبادُل المعلومات والتعاون مع الجهات المعنية الوطنية والدولية، واستحداث آليات تضمن الحماية، وتقليل الجرائم السيبرانية إلى الحد الأدنى، وزيادة الردع.

وإضافة إلى ذلك، شرعت وزارة النقل والبنى التحتية في دراسات لوضع استراتيجية وخطة عمل جديدتين للأمن السيبراني تغطيان الفترة 2024–2028. وفي هذا السياق، تتواصل الدراسات لضمان التعاون الفعال بين جميع الجهات المعنية، وزيادة اكتساب وإنتاج وتبادل المعلومات الاستخبارية عن تهديدات الأمن

(29) www.statista.com/statistics/494947/ransomware-attempts-per-year-worldwide.

السيبراني، ورفع مستوى التأهب الوطني للحوادث السيبرانية، وتطوير الموارد البشرية المتخصصة، وإتاحة فرص الكشف السريع والاستجابة المبكرة، وإجراء تحليلات المخاطر للقطاعات والبنى التحتية الحيوية.

ويتولى فريق تركيا الوطني للتصدي للطوارئ السيبرانية (الفريق الوطني) ضمن هيئة تكنولوجيا المعلومات والاتصالات تنسيق الاستجابة للحوادث السيبرانية في تركيا منذ عام 2013. وإلى جانب كشف التهديدات السيبرانية والاستجابة للحوادث السيبرانية بما في ذلك قبل الحوادث وخلالها وبعدها، يتأكد الفريق الوطني من تنفيذ التدابير الوقائية ضد التهديدات السيبرانية ويضمن الردع السيبراني.

وينصبّ تركيز الفريق الوطني في مجال الأمن السيبراني على ما يلي:

- بناء القدرات السيبرانية
- التدابير التكنولوجية
- جمع وتعميم المعلومات الاستخبارية عن التهديدات
- حماية البنى التحتية الحيوية.

وفي سياق تحسين الأمن السيبراني الوطني، أنشئ أيضاً منذ عام 2013 ما مجموعه 14 فريقا قطاعيا للتصدي للطوارئ السيبرانية في القطاعات/البنى التحتية الحيوية (كالطاقة، والصحة، والمصارف والمالية، وإدارة المياه، والاتصالات الإلكترونية، والخدمات العامة الحيوية)، وما يزيد عن 200 2 فريق مؤسَّسي للتصدي للطوارئ السيبرانية. وتعمل جميع أفرقة التصدي للطوارئ السيبرانية على مدار الساعة، ويتولى الفريق الوطني التنسيق بينها من أجل التخفيف من حدة المخاطر السيبرانية ومكافحة التهديدات السيبرانية. ويستخدم الفريق الوطني أدوات الكشف والوقاية لأغراض الرصد، وأدوات الإبلاغ من أجل تبادل المعلومات مع الأطراف المعنية. واستحدث الفريق الوطني منصة تبادل المعلومات لجميع أفرقة التصدي للطوارئ السيبرانية داخل تركيا من أجل تعميم الإنذارات والتحذيرات والإشعارات الأمنية، ما يوفر قناة اتصالات تتسم بالكفاءة والأمن.

ويشكل التمرين الخاص بالأمن السيبراني نشاطا هاما آخر للتعاون والتأهب. ويسهم هذا النوع من التمارين التي تُجرى على الصعيدين الوطني والدولي في تعزيز الحيز السيبراني واختبار التدابير المزمع اتخاذها ضد التهديدات السيبرانية المحتملة. ومنذ عام 2011، نظمت وزارة النقل والبنية التحتية سبعة تمارين وطنية وتمرينين دوليين في مجال الأمن السيبراني. وفي الآونة الأخيرة، أُجريت على الصعيد الوطني تمارين الدرع السيبرانية 2022. وبعد الدرع السيبرانية 2022، نُفذت بالتعاون مع وزارة النقل والبنية التحتية وهيئة تكنولوجيا المعلومات والاتصالات، الدرع السيبرانية 2022 للقطاع المالي يومي 20 و 21 تشرين الأول/أكتوبر 2022 بمشاركة مؤسسات وهيئات عامة. وفي هذه التمارين؛ ومن خلال البنية التحتية التقنية والسيناريوهات التي استُحدثت داخل الفريق الوطني، مُنح المشاركون تجربة عملية في مجال الأمن السيبراني، وجرى تبادل المعلومات حول الخطوات التي يتعين القيام بها في حال وقوع هجمات سيبرانية محتملة. ومن المقرر تنظيم تمرين دولي في مجال الأمن السيبراني في الفترة المقبلة.

والأمن السيبراني قضية مدرجة في جدول أعمال العالم بأسره تتطلب جهودا على المستوى الدولي. ويؤدي التعاون على الصعيدين الإقليمي والعالمي وتبادلُ المعلومات والاستخبارات في مجال الأمن السيبراني دورا هاما في مساعدة البلدان على مواجهة المخاطر والتهديدات السيبرانية. وفي هذا السياق، تعكف تركيا

على تطوير التعاون الثنائي والإقليمي والدولي في هذا المجال؛ وتشارك وتسهم في أنشطة صنع السياسات والاستراتيجيات لمنظمات دولية مثل الأمم المتحدة ومنظمة حلف شمال الأطلسي ومنظمة الأمن والتعاون في أوروبا ومجموعة العشرين ومنظمة التعاون والتنمية في الميدان الاقتصادي ومنظمة التعاون الاقتصادي والبلدان النامية الثمانية والمركز الإقليمي للمساعدة على التحقق من تحديد الأسلحة وتنفيذه ومنظمة الدول التركية، وغيرها. وإضافة إلى ذلك، يواصل الفريق الوطني أنشطته في تبادل المعلومات الاستخبارية عن التهديدات السيبرانية من خلال عضويته في محافل دولية من قبيل منتدى أفرقة الأمن والتصدي للحوادث ومؤسسة تراستد إنترود يوسرز، والاتحاد الدولي للاتصالات، وتحالف الأمن السيبراني من أجل التقدم المشترك، والمنتدى المتعدد الجنسيات لتبادل المعلومات عن البرامجيات الخبيثة التابع للناتو، وفريق التصدي للطوارئ السيبرانية التابع لمنظمة التعاون الإسلامي. ويشارك بلدنا أيضا في مركز المعارف المتفوقة التابع للناتو باعتباره بلدا راعيا وهو عضو في آلية الناتو للقدرات الافتراضية على دعم مواجهة الحوادث السيبرانية. وإضافة إلى ذلك، وُقعت مذكرات تفاهم وتعاون ثنائي مع العديد من البلدان في مجال الأمن السيبراني.

وقُبل الفريق الوطني في برنامج الثغرات والمخاطر الأمنية الشائعة التابع لشركة ميتر كوربوريشن، وفي هذا السياق، يحدد الفريق أرقاماً خاصة بالثغرات والمخاطر الأمنية الشائعة لمكامن الضعف في برامج أو أجهزة أو منتجات الأطراف الثالثة ويوفر تنسيق العمليات في معالجتها.

كما أن تركيا هي طرف في العديد من الاتفاقات المتعددة الأطراف المتعلقة بالأمن السيبراني. فقد صادقت تركيا على اتفاقية مجلس أوروبا بشأن الجريمة الإلكترونية (مجموعة المعاهدات الأوروبية رقم 185). وتسهم تركيا أيضا في دراسات تجرى برعاية لجنة الأمم المتحدة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية. وإضافة إلى ذلك، فإن تركيا هي إحدى الدول المشاركة في رعاية برنامج العمل لتعزيز السلوك المسؤول للدول في استخدام تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي، وهي تؤيد بقوةٍ قرارَ الجمعية العامة للأمم المتحدة 37/77 والجهود الأخرى الرامية إلى إنشاء برنامج العمل كآليةٍ دائمة وشاملة للجميع وعملية المنحى.

1 - المنظمة الوطنية للأمن السيبراني في تركيا

في ما يتعلق بأمن المعلومات والاتصالات، ولا سيما الأمن السيبراني في تركيا، من الجدير بالذكر أن التقدم في هذا المجال يعود إلى عام 1991. فقد بدأت مسيرة تركيا في مجال الأمن السيبراني بإدراج الجرائم السيبرانية في القانون الجنائي التركي رقم 765 في عام 1991[30]. وهي ما برحت منذ ذلك الحين تحقق إنجازات هامة في مجالات مختلفة من الأمن السيبراني الذي يشكل جزء أساسي من أمنها القومي. وفي ما يلي قائمة غير حصرية بالمبادرات المنفذة حتى عام 2012:

- وضع الخطة الرئيسية للبنى التحتية الوطنية الخاصة بالمعلومات[31] في تركيا عام 1999.
- إطلاق خطة عمل مبادرة تركيا الإلكترونية E-Türkiye[32] في عام 2002.

(30) https://www.mevzuat.gov.tr/MevzuatMetin/5.3.765.pdf.

(31) http://www.bilgitoplumu.gov.tr/Documents/1/Yayinlar/991000_TuenaRapor.pdf.

(32) http://www.bilgitoplumu.gov.tr/Documents/1/Yayinlar/020800_E-TurkiyeEylemPlani.pdf.

- تحديد مشـــروع التحول الإلكتروني لتركيا في عام 2003 إلى جانب خطة العمل القصـــيرة الأجل للفترة 2003–2004[33].
- بـدء تطبيق قـانون التوقيع الإلكتروني رقم 5070[34] وقـانون العقوبـات التركي رقم 5237[35] في عام 2004.
- إصدار استراتيجية وخطة عمل مجتمع المعلومات للفترة 2006–2010[36] في عام 2006.
- إنشاء المركز التركي للتنسيق بين أفرقة الاستجابة لحوادث الحاسوب في عام 2007.
- سـنّ القانون رقم 5651 بشـأن المنشـورات على الإنترنت ومكافحة الجرائم المرتكبة عن طريق هذه المنشورات[37] في عام 2007.
- تنفيذ قانون الاتصـــالات الإلكترونية رقم 5809[38] في عام 2008 إلى جانب أول مناورة وطنية للأمن السيبراني في تركيا.
- صـــدور إعلان مجلس الأمن القومي في عام 2010 الذي يعترف بالانتشـــار العالمي للتهديدات السيبرانية وآثارها على الأمن القومي.
- مواءمة تشـــريعات تركيا مع اتفاقية بودابســـت المتعلقة بالجريمة الإلكترونية التي وضـــعها مجلس أوروبا (ETS No. 185) في العام نفسه.
- أدى قرار مجلس الوزراء بإدارة وتنسـيق الجهود الوطنية للأمن السـيبراني إلى إنشـاء مجلس الأمن السـيبراني في عام 2012[39]، ومعهد الأمن السـيبراني[40] التابع لمركز أبحاث المعلوماتية وأمن المعلومات بمجلس تركيا للبحوث العلمية والتكنولوجية في العام نفسه.

وتمثل هذه المحطات الهامة تقدما كبيرا في هذا المجال. وكما ذُكر أعلاه، ففي ظل نظام الحكم البرلماني في تركيا، وافق مجلس الوزراء على قرار بشـأن تنفيذ وإدارة وتنسـيق الدراسـات الوطنية في مجال الأمن السـيبراني في 11 حزيران/يونيه 2012[41]. وبموجب هذا القرار، أنشـئ مجلس الأمن السـيبراني[42]

(33) https://webdosya.csb.gov.tr/db/cbs/icerikler/2005-20180522115122.pdf.

(34) https://kamusm.bilgem.tubitak.gov.tr/dosyalar/mevzuat/kanunlar/kanun.pdf.

(35) www.resmigazete.gov.tr/eskiler/2004/10/20041012.htm#1.

(36) http://www.bilgitoplumu.gov.tr/Documents/1/BT_Strateji/Diger/060500_BilgiToplumuStratejisi.pdf.

(37) www.mevzuat.gov.tr/mevzuatmetin/1.5.5651.pdf.

(38) https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5809.pdf.

(39) www.btk.gov.tr/siber-guvenlik-kurulu.

(40) https://bilgem.tubitak.gov.tr/en/sge/.

(41) https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf.

(42) www.btk.gov.tr/siber-guvenlik-kurulu.

وكُلفت وزارة النقل والشؤون البحرية والاتصالات (أصبحت الآن وزارة النقل والبنية التحتية[43])، كما كانت تُعرف آنئذ، بالاضطلاع بعمل أمانة المجلس وبتنسيق أنشطة الأمن السيبراني مع المؤسسات ذات الصلة.

وعلى مدى العقد الماضي، سُجلت زيادة ملحوظة في وتيرة التطورات في قطاع الأمن السيبراني في تركيا. وتشمل الإنجازات الرئيسية إطلاق أول استراتيجية وخطة عمل وطنيتين للأمن السيبراني في البلاد للفترة 2013-2014[44]، وإنشاء المركز الوطني للتصدي للحوادث السيبرانية (المركز الوطني)[45] ضمن هيئة تكنولوجيا لمعلومات والاتصالات[46]، ونشر إعلان يحدد إنشاء أفرقة التصدي للحوادث السيبرانية وأدوارها ومبادئ عملها[47]. وإضافة إلى ذلك، أنشئت أفرقة التصدي للحوادث السيبرانية (الأفرقة المؤسسية للتصدي للحوادث السيبرانية، والأفرقة القطاعية التصدي للحوادث السيبرانية) داخل المؤسسات والمنظمات العامة في إطار الاستراتيجية وخطة العمل الوطنيتين للأمن السيبراني للفترة 2013-2014. وأفرقة التصدي للحوادث السيبرانية هي منظمات مؤسسية وقطاعية أنشئت للعمل سريعا على تحديد التهديدات والهجمات المحتملة في البيئة السيبرانية، ولوضع وتبادل التدابير اللازمة لحل المشاكل التي تسببها هذه الهجمات. وعليه، فإن هدف هذه الأفرقة هو توفير مهارات التصدي السيبراني لدى المؤسسات والمنظمات. ويعمل حاليا 14 فريقا التصدي للحوادث السيبرانية يتولى المركزُ الوطني للتصدي للحوادث السيبرانية التنسيق بينها، ويعمل أكثر من 100 2 فريق مؤسسي للتصدي للحوادث السيبرانية بجد لحماية المجال السيبراني لتركيا.

وما برح مركز الدفاع السيبراني، الذي أنشئ ضمن القوات المسلحة التركية في عام 2012، يتطور منذ ذلك الحين حتى أصبح قيادة الدفاع السيبراني. وعلى غرار ذلك، أعيدت لاحقا في عام 2013 هيكلة قسم مكافحة الجرائم السيبرانية، الذي أنشئ ضمن المديرية العامة للأمن في عام 2011.

وأدخل القانون رقم 6518 الذي نُشر في عام 2014 بعضَ الأنظمة في مجال الأمن السيبراني بإضافة مواد إلى القانون رقم 5809 الذي نُشر في عام 2008 والذي ينظم قطاع الاتصالات الإلكترونية[48]. ومع إضافة مواد إلى القانون رقم 5809، أنشئ مجلس الأمن السيبراني، المكون من كبار المسؤولين التنفيذيين في المؤسسات العامة، برئاسة وزير النقل والشؤون البحرية والاتصالات. ومع إضافة الفقرة الفرعية (ح) إلى المادة 5 من القانون المذكور أعلاه، كُلفت وزارة النقل والشؤون البحرية والاتصالات بمهام "تحديد السياسات والاستراتيجيات والأهداف لضمان الأمن السيبراني الوطني، وإعداد خطط العمل، والقيام بأنشطة التعليم والتوعية في مجال الأمن السيبراني".

وبموجب هذه القاعدة التنظيمية، عُينَ مجلس الأمن السيبراني باعتباره السلطة الرئيسية المسؤولة عن الموافقة النهائية والتنفيذ الفعلي للسياسات والاستراتيجيات وخطط العمل في الدولة حسبما تحددها وزارة النقل والشؤون البحرية والاتصالات. كما كُلف المجلس بالبت في المقترحات المتصلة بتبيان البنى التحتية الحيوية وتحديد المؤسسات والمنظمات التي من المزمع إعفاؤها كليا أو جزئيا من الأحكام المتعلقة بالأمن السيبراني.

(43) www.uab.gov.tr/.

(44) https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/actionplan2013-2014.pdf.

(45) www.usom.gov.t/r.

(46) www.btk.gov.tr/.

(47) www.usom.gov.tr/hakkimizda.

(48) https://www.resmigazete.gov.tr/eskiler/2014/02/20140219-1.htm.

وفي عام 2016، نُشر القانونُ رقم 6698 بشأن حماية البيانات الشخصية[49] والاستراتيجيةُ وخطة العمل الوطنيتان للأمن السيبراني للفترة 2016–2019[50]. وإضافة إلى ذلك، ومع مرسوم القانون رقم 671[51]، الذي أُعدَّ بما يتماشى مع مقتضيات الفترة، أُذنَ لهيئة تكنولوجيا المعلومات والاتصالات بأن "تتخذ أو تطلب اتخاذ كل أنواع التدابير لحماية المؤسسات والمنظمات العامة والأشخاص الحقيقيين والاعتباريين من الهجمات السيبرانية وتوفير الردع ضد هذه الهجمات". ولاحقا، في عام 2017، وبتنسيق من قبل رئاسة الصناعات الدفاعية (التي أصبحت الآن أمانة الصناعات الدفاعية[52])، بدأ إنشاء المجموعة التركية للأمن السيبراني، وأُنجزت تعيينات مجلس حماية البيانات الشخصية وبدأ المجلس أنشطته.

وفي عام 2018، ألغيَ مجلس الأمن السيبراني في أعقاب نشر مرسوم القانون رقم 703[53]. وأُعلنَ أن مسؤوليات المجلس وولايته ستناط بـ"مجلس أو هيئة يعينها الرئيس". بيد أنه، رغم بعض التعيينات الجزئية المتصلة بهذه المسؤوليات، لم يُنقل أيٌّ منها رسميا إلى أي مجلس أو هيئة حتى تاريخه. ومع الانتقال إلى نظام الحكم الرئاسي، حدثت أيضا تغييرات في عملية صنع السياسات. ونُقلت سلطة صياغة السياسات إلى رئيس الجمهورية. وكُلفت مجالس السياسات بصوغ وتطوير هذه السياسات (المرسوم الرئاسي رقم 1[54]، المواد 20 إلى 22)، في حين أنيطت بالوزارات المسؤولية عن تنفيذها.

واعتبارا من 10 تموز/يوليه 2018، ومع تنفيذ المرسوم الرئاسي رقم 1 لنظام الحكومة الرئاسية، أنيطت المسؤولية عن "وضع مقترحات السياسات والاستراتيجية في ما يتصل بالأمن السيبراني" بمجلس السياسات الأمنية والخارجية الذي يعمل تحت إشراف الرئيس (المرسوم الرئاسي رقم 1، المادة 36/1 ğ). وبموجب المرسوم الرئاسي رقم 1، أُسندت المسؤولية عن "تنفيذ مشاريع لتعزيز أمن المعلومات والأمن السيبراني" إلى مكتب التحول الرقمي[55] التابع لرئاسة جمهورية تركيا، وعلى وجه الخصوص إلى قسم الأمن السيبراني[56] التابع للمكتب. وتشمل مهام هذا القسم ما يلي:

- وضع استراتيجيات الأمن السيبراني للمؤسسات العامة والبنى التحتية الحيوية، بما يتماشى مع السياسات التي يضعها الرئيس.
- مراقبة أوجه التقدم المحرز في تنفيذ متسم بالكفاءة للسياسات والاستراتيجيات وخطط العمل في مجال الأمن السيبراني على نطاق البلد.
- إجراء بحوث لتحديد البنى التحتية الحيوية.
- إعطاء زخم للتعاون بين القطاعين العام والخاص والجامعات بغية تعزيز بيئة وطنية للأمن السيبراني.

(49) https://kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law.

(50) https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/ulusalsibereng.pdf.

(51) www.resmigazete.gov.tr/eskiler/2016/08/20160817-18..htm.

(52) www.ssb.gov.tr/Default.aspx?LangID=2.

(53) www.resmigazete.gov.tr/eskiler/2018/07/20180709M3-1.pdf.

(54) https://www.mevzuat.gov.tr/mevzuatmetin/19.5.1.pdf.

(55) https://cbddo.gov.tr/en/.

(56) https://cbddo.gov.tr/en/department-of-cyber-security/.

- إجراء دراسات لتطوير منتجات الأمن السيبراني المحلية والوطنية في جميع القطاعات، وبخاصة البنى التحتية الحيوية، والترويج لاستخدامها داخل القطاع العام.
- الاضطلاع بأنشطة وقائية وبتوفير الحماية لصون أصول التكنولوجيا والمعلومات الحيوية.
- إجراء دراسات عن إنشاء وإدارة نظام أمن المعلومات في المؤسسات والمنظمات العامة التي تشغّل البنية التحتية الحيوية؛ ويشمل ذلك وضع المعايير والإجراءات الفنية، فضلا عن مبادئ مراقبة وتوجيه التطبيقات.

وإضافة إلى ذلك، أنشئت مديرية التكنولوجيا الوطنية[57] التابعة لوزارة الصناعة والتكنولوجيا[58]، على النحو المبين في المرسوم الرئاسي رقم 1 المنشور في الجريدة الرسمية الصادرة في 10 تموز/يوليه 2018. وأنيطَت بالمديرية المسؤوليات التالية في ما يتعلق بالأمن السيبراني:

- تعزيز مستوى تطور الأمن السيبراني وأمن المعلومات لمنتجات ونظم تكنولوجيا المعلومات والتكنولوجيا المتطورة.
- تطوير المنتجات المحلية والوطنية في مجال الأمن السيبراني.
- التوسع في استخدام المنتجات المحلية والوطنية على الصعيد الوطني.
- تعزيز مركز البيانات والبنية التحتية لتجهيز البيانات.
- دعم منظومة الأمن السيبراني من خلال برامج الحوافز المختلفة.

وباختصار، حددت العديد من القوانين والأنظمة والتشريعات الأخرى مؤسسات عدة للإشراف على الأمن السيبراني الوطني. وتستمد هذه المؤسسات مهامها المتصلة بالأمن السيبراني من هذه التشريعات المختلفة. وعلى غرار معظم البلدان الأخرى، يُعتبر الأمن السيبراني في تركيا مسؤولية مشتركة بين كيانات حكومية متعددة. فقد أجرى مكتب التحول الرقمي ووزارة النقل والبنية التحتية دراسات تتعلق بوضع استراتيجيات وسياسات الأمن السيبراني. ولكل منظمة مجموعتها الخاصة من الأدوار والمسؤوليات في مجال اختصاصها.

2 - أدوار ومسؤوليات مكتب التحول الرقمي في مجال الأمن السيبراني

بعد الانتقال إلى نظام الحكومة الرئاسية في عام 2018، أنشئ مكتب التحول الرقمي التابع لرئاسة الجمهورية التركية بموجب المرسوم الرئاسي رقم 1 الذي دخل حيز النفاذ بعد نشره في الجريدة الرسمية الصادرة في 10 تموز/يوليه 2018. وجرى توسيع ولاية مكتب التحول الرقمي لاحقا بموجب المرسوم الرئاسي رقم 48 الصادر في 24 تشرين الأول/أكتوبر 2019[59].

وشكّل إنشاء مكتب التحول الرقمي بداية حقبة جديدة وتغييرا في العقلية إزاء الجهود المبذولة في مجال الرقمنة في تركيا. ومنذ إنشاء هذا المكتب، بدأ اتّباع نهج أكثر اتساقا وشمولا بين المؤسسات إزاء التحول الرقمي في القطاع العام. وعليه، وإضافة إلى تحقيق إدارة أسرع وأكثر شفافية وفعالية، فهو يهدف

(57) www.sanayi.gov.tr/merkez-birimi/c03f1f3bae27/hakkimizda.

(58) www.sanayi.gov.tr/anasayfa.

(59) https://cbddo.gov.tr/en/governance-and-responsibilities.

إلى تنسيق وإدارة وتشغيل أنشطة التحول الرقمي التي تنفَّذ بشكل منفصل في إطار مؤسسات مختلفة بما يتماشى مع التكنولوجيات المتطورة والمطالب الاجتماعية واتجاهات الإصلاح في القطاع العام. وإضافة إلى ذلك، يهدف إلى تنسيق الأنشطة المتصلة بالأمن السيبراني والتكنولوجيات الوطنية والبيانات الضخمة والذكاء الاصطناعي على الصعيدين الاستراتيجي أو العملي تحت سقف واحد، والتنفيذ الفعال لاستراتيجيات عالية المستوى. ونتيجة لذلك، وبتنسيق من مكتب التحول الرقمي، تُحدَّد أهداف على المستوى الكلي وتنفَّذ مبادرات لحماية البنى التحتية الرقمية لتركيا ولتحويلها إلى قوة سيبرانية رادعة.

ويضطلع مكتب التحول الرقمي بالمسؤوليات التالية في مجال الأمن السيبراني بما في ذلك وضع السياسات والأنظمة وبناء بيئة للأمن السيبراني وتوعية الجمهور وبناء القدرات وتعزيز البنية التحتية العمومية ووضع المعايير:

- وضع استراتيجيات الأمن السيبراني للمؤسسات العامة والبنى التحتية الحيوية، عملا بالسياسات التي يحددها الرئيس.
- تنفيذ المشاريع الداعمة للأمن السيبراني وأمن المعلومات على الصعيد الوطني.
- متابعة التطورات في التنفيذ الفعال على الصعيد الوطني للسياسات والاستراتيجيات وخطط العمل المتعلقة بالأمن السيبراني.
- العمل على تحديد البنى التحتية الحيوية.
- تقديم مقترحات إلى الوكالات المختصة بشأن المؤسسات والمنظمات التي ستُعفى كليا أو جزئيا من الأحكام المتعلقة بالأمن السيبراني.
- الإسهام في إنشاء بيئة وطنية للأمن السيبراني من خلال تعزيز التعاون بين القطاع العام والقطاع الخاص والجامعات.
- تحديد مجالات الأمن السيبراني ذات الأولوية تمهيدا لتوجيه قدرات القطاع الخاص نحو المجالات الحيوية ومنع الاستثمارات المتكررة.
- العمل على تطوير المنتجات المحلية والوطنية للأمن السيبراني في كل مجال بما في ذلك البنية التحتية الحيوية في المقام الأول، وتوسيع نطاق استخدام هذه المنتجات في القطاع العام.
- الاضطلاع بأنشطة وقائية وبأنشطة توفير الحماية بغية صون الأصول الحيوية للتكنولوجيا والمعلومات.
- إنشاء وتشغيل نظام إدارة أمن المعلومات في المؤسسات العامة والمنظمات التي تشغّل البنية التحتية الحيوية، وتحديد المعايير والإجراءات والمبادئ الفنية، ومراقبة التنفيذ وتوجيهه.

ومكتب التحول الرقمي هو حاليا السلطة الرائدة في إدارة قضايا الأمن السيبراني للمؤسسات العامة والقطاعات الحيوية في بلدنا. وهو، إلى جانب اضطلاعه بمسؤوليات مجلس الأمن السيبراني، يتعاون مع جميع المؤسسات لتنسيق وضع الاستراتيجيات وخطط العمل وتنفيذها على نحو فعال على الصعيد الوطني.

3 - أنشطة مكتب التحول الرقمي ومشاريعه في مجال وضع السياسات

رغم وجود تعاريف مختلفة لمفهوم الأمن السيبراني، فبالإمكان التعبير عن تعريفه البسيط والشامل باعتباره نظاما أمنيا يطبَّق على كل نقطة في الفضاء السيبراني الذي يغطي مكونات تكنولوجيا المعلومات. وبالنظر إلى أن الثورة الصناعية الرابعة تُعتبر ثورة تهدف إلى الجمع بين تكنولوجيا المعلومات وكل الآليات الحيوية، فمن المتوقع أن يتم دمج نظام الأمن السيبراني في نظام حياتنا باعتباره تكيفا أمنيا لهذه الثورة.

وعندما لا يطبَّق النظام الأمني وفقا للانضباط الأمني، تنشأ مشاكل متعلقة بالأمن والخصوصية. وعند النظر إلى الأهداف الاستراتيجية المتمثلة في حماية البنى التحتية الحيوية، وضمان تبادل البيانات بشكل آمن بين المؤسسات والمنظمات، والحفاظ على حركة البيانات التي يكون مصدرها ووجهتها محليين داخل البلاد، على المستوى الوطني فهي تحتل الصدارة. وهو يهدف إلى رفع مستوى التأهب لمواجهة الحوادث السيبرانية على أساس مؤسسي وقطاعي ووطني من خلال نهُج تستند إلى التحليل والتخطيط القائمين على المخاطر.

وبغية ضمان الأمن في العالم الرقمي، تعكف الحكومات على إعداد ونشر استراتيجيات الأمن السيبراني وضمان تحقيقها والإشراف عليها من خلال تحديد المؤسسات المختصة. ويقوم بلدنا أيضا بواجبه في هذا الصدد. ونتيجةً لعمل بلدنا في هذا الشأن بتنسيق من وزارة النقل والبنى التحتية، أُدرجت الاستراتيجيات أدناه:

- الاستراتيجية وخطة العمل الوطنيتان للأمن السيبراني للفترة 2013-2014[60]
- الاستراتيجية وخطة العمل الوطنيتان للأمن السيبراني للفترة 2016-2019[61]
- الاستراتيجية وخطة العمل الوطنيتان للأمن السيبراني للفترة 2020-2023[62]

ويُحرَز تقدم في الاستراتيجيات وخطط العمل الوطنية للأمن السيبراني المذكورة أعلاه باتّباع نهج شامل يضمن الاستمرارية، وهي تشمل تدابير لضمان أمن التكنولوجيات الجديدة التي دخلت حياتنا.

ونُشرت أحدث استراتيجية وخطة عمل وطنيتين للأمن السيبراني (2020-2023)[63] في 28 كانون الأول/ديسمبر 2020 بدعم من مكتب التحول الرقمي. وهما تهدفان إلى دعم التنمية الاقتصادية لبلدنا وحماية الحياة الاجتماعية والأمن القومي وإلى جعل بلدنا علامة تجارية دولية في مجال الأمن السيبراني. وفي هذا الصدد، تركز الاستراتيجية على السياسات المتصلة بفترة الأربع سنوات بما يتماشى مع رؤية تركيا ورسالتها في مجال الأمن السيبراني، وتهدف إلى مواصلة الإنجازات التي تحققت من خلال الاستراتيجيات السابقة. وجُمعت كل الأهداف الاستراتيجية التي حددتها الاستراتيجية وخطة العمل الوطنيتان للأمن السيبراني (2020-2023) ضمن ثماني ركائز:

(60) https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/actionplan2013-2014.pdf.

(61) https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/ulusalsibereng.pdf.

(62) https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/national-cyber-security-strategy-2020-2023.pdf.

(63) https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/national-cyber-security-strategy-2020-2023.pdf.

- حماية البنية التحتية الحيوية وزيادة المنعة
- بناء القدرات الوطنية
- الشبكة العضوية للأمن السيبراني
- أمن تكنولوجيات الجيل الجديد
- مكافحة الجريمة السيبرانية
- تطوير التكنولوجيات المحلية والوطنية والترويج لها
- دمج الأمن السيبراني في الأمن القومي
- تحسين التعاون الدولي

3-1 نظام رصد الاستراتيجية وخطة العمل

وُضع نظام رصد الاستراتيجية وخطة العمل بغية العمل بشكل فعال على إدارة ورصد الاستراتيجية وخطط العمل التي أعدتها الرئاسة، وكذلك أنشطة المجموعة التركية للأمن السيبراني في نطاق مكتب التحول الرقمي. كما يتتبع النظام التقدم المحرز في الإجراءات ويقيم أداءها وإنجازاتها بناء على أهداف محددة مسبقا.

وعلاوة على ذلك، فإن مكتب التحول الرقمي مسؤول عن دعم أنشطة وضع السياسات التي يتولى مجلس سياسات العلوم والتكنولوجيا والابتكار تنسيقها بما في ذلك:

- اقتراح السياسة الوطنية للأمن السيبراني وتكنولوجيات البنية التحتية للاتصالات
- اقتراح السياسة الوطنية لجيل الاتصالات 5G والجيل الذي يليه من تكنولوجيا الاتصالات
- خرطة الطريق الوطنية لتكنولوجيات الأمن السيبراني

3-2 التدابير المتخذة في إطار البرنامج الرئاسي السنوي لعام 2023

استنادا إلى الاستراتيجية وخطة العمل الوطنيتين للأمن السيبراني (2020-2023)، التدابير الواردة في البرنامج السنوي الرئاسي لعام 2023[64] التي أنيطت المسؤولية المباشرة عنها بمكتب التحول الرقمي أو التابعة له هي كما يلي:

- تحديث الاستراتيجية الوطنية للأمن السيبراني، وتعزيز القواعد التنظيمية والبنية التحتية التقنية للأمن السيبراني، وإنشاء هيكل تنسيقي قوي.
  - إعداد تشريع إطاري للأمن السيبراني.
  - إعداد الاستراتيجية وخطة العمل الوطنيتين للأمن السيبراني للفترة 2024-2027.
- تحديدُ إجراءات ومبادئ إنشاء نظم إدارة أمن المعلومات في البنى التحتية الحيوية، ووضعُها موضع التنفيذ.

(64) https://www.sbb.gov.tr/wp-content/uploads/2022/11/2023-Yili-Cumhurbaskanligi-Yillik-Programi.pdf.

- تحديث دليل أمن المعلومات والاتصالات.

- بغية إفادة النظام البيئي للأمن السيبراني وتطوير منتجات وبرمجيات ذات قيمة مضافة أعلى في هذا المجال، سيجرى تطوير منتجات الأمن السيبراني ومشاريع التكنولوجيا التي تشمل مؤسسات البحوث الحكومية والجامعات، وسيتم تبادل نواتج هذه المشاريع مع بيئة الأمن السيبراني في شفرة مصدرية مفتوحة.

- بذل جهود لتعزيز البيئة الوطنية للأمن السيبراني وزيادة قدرتها التنافسية الدولية.

  - تنظيم منتدى دولي للأعمال التجارية في مجال الأمن السيبراني.

  - إطلاق منصة نشر منتجات الأمن السيبراني المحلية بغية تنمية بيئة تتيح تطوير وتصدير منتجات الأمن السيبراني المحلية اللازمة.

- بغية تدريب قوة عاملة مؤهلة في مجال الأمن السيبراني، ستوضع مناهج الأمن السيبراني للكليات المهنية وستحدَّد معايير مهنية.

  - تحسين مناهج الأمن السيبراني الحالية للمدارس المهنية مع مناهج الأمن السيبراني.

  - تخرُّج طلاب يحملون ألقابا وظيفية من مدارس مهنية تقدم مناهج دراسية في مجال الأمن السيبراني ووضع معايير.

3-3 التدابير المتخذة في إطار البرنامج الرئاسي السنوي لعام 2024

استنادا إلى الاستراتيجية وخطة العمل الوطنيتين للأمن السيبراني (2020-2023)، إن التدابير الواردة في البرنامج السنوي الرئاسي لعام 2024[(65)] التي أنيطت المسؤولية المباشرة عنها بمكتب التحول الرقمي أو التابعة له هي كما يلي:

- زيادة المنعة السيبرانية ومستوى التطور الأمني إزاء تهديدات الأمن السيبراني للأسواق المالية.

  - نشر قاعدة تنظيمية بشأن ضمان الأمن السيبراني الوطني وتعزيز الردع السيبراني بحيث يشمل القطاع المالي.

- دعم المواءمة مع المعايير الدولية في مجال الأمن السيبراني ومشاركة تركيا في مشاريع دولية مشتركة.

  - العمل، في سياق مراعاة المعايير الدولية وتشريعات الاتحاد الأوروبي، على إنجاز تشريعات ثانوية بشأن أمن إنترنت الأشياء.

- إصدار قواعد تنظيمية تضمن الأمن السيبراني الوطني من خلال مراعاة الأمر التوجيهي للاتحاد الأوروبي المتعلق بأمن الشبكات والمعلومات (NIS2) وجهوده الجديدة في مجال الأمن السيبراني وأفضل الممارسات الدولية.

  - نشر قاعدة تنظيمية بشأن ضمان الأمن السيبراني الوطني وزيادة الردع السيبراني.

(65) https://www.sbb.gov.tr/wp-content/uploads/2023/10/2024-Yili-Cumhurbaskanligi-Yillik-Programi.pdf.

- إجراء دراسات تتعلق بالقواعد التنظيمية لأمن إنترنت الأشياء.
- إجراء عمليات تفتيش في مجال الأمن السيبراني لأجهزة إنترنت الأشياء.
- تحديد القواعد التنظيمية الثانوية اللازمة في ما يتعلق بالتشريع الإطاري الوطني للأمن السيبراني، الذي لا يزال العمل التحضيري جاريا بشأنه.
- بذل جهود بشأن القانون رقم 5070 المتعلق بالتوقيع الإلكتروني والتشريعات الأخرى ذات الصلة لتوفير أساس قانوني لخدمة التوقيع من بُعد.
- تنفيذ أنشطة توعية لتوسيع نطاق استخدام خدمة التوقيع من بُعد في المؤسسات العامة والقطاع الخاص.

• التأكد من التنسيق على أعلى مستوى لأنشطة الأمن السيبراني الوطنية، وإنشاء هيكل فعال للتنسيق والإدارة لتعزيز التعاون بين المؤسسات.

- نشر تشريعات حصرية للأمن السيبراني تنظم وظائف وواجبات ومسؤوليات المنظمة الوطنية للأمن السيبراني.
- تنسيق الأعمال التحضيرية للاستراتيجية وخطة العمل الوطنيتين للأمن السيبراني للفترة 2024–2028 ووضع آلية لرصد الإجراءات والأنشطة في البيئة الرقمية.
- بذل جهود لوضع خطة وطنية لإدارة حالات الطوارئ والأزمات في مجال الأمن السيبراني.
- تعزيز شبكة تبادل المعلومات الاستخباراتية عن التهديدات السيبرانية.

• تعزيز آليات الحصول على معلومات عن التهديدات السيبرانية وتبادلها من خلال زيادة تنوع الموارد وتطوير تطبيقات الذكاء الاصطناعي وتحليل البيانات الضخمة، وبذل الجهود للكشف المبكر عن الأخطار التي تهدد الأمن السيبراني الوطني والوقاية منها.

- إجراء تحليل للاحتياجات لموارد المعلومات الاستخبارية عن التهديدات السيبرانية.
- زيادة القدرات على مواجهة الحوادث والتنسيق.
- مباشرة العمل في مشاريع الأمن السيبراني المدعومة بالذكاء الاصطناعي وتحليلات البيانات الضخمة لكشف مراكز القيادة والتحكم لمجالات التصيد الإلكتروني والبرامجيات الخبيثة وشبكات الحواسيب المصابة.

• تحديدُ إجراءات ومبادئ إنشاء نظم إدارة أمن المعلومات في البنى التحتية الحيوية، ووضعُها موضع التنفيذ.

- إجراء تحليل العمليات لإنشاء نظام إدارة أمن المعلومات في البنى التحتية الحيوية.
- تنفيذ الأعمال التنظيمية لإنشاء نظام لإدارة أمن المعلومات في البنى التحتية الحيوية.

• وضع معايير الأمن السيبراني في المجالات التي تشكل مدعاة للقلق.

- درس إطار الاعتماد الذي أنشئ بموجب قانون الأمن السيبراني للاتحاد الأوروبي، وتحديد المعايير اللازمة لمنتجات وخدمات وعمليات الأمن السيبراني.
- إدماج المواد المتصلة بالمبادئ التوجيهية لأمن المعلومات والاتصالات في دليل أمن المعلومات والاتصالات.
- وضع نموذج لتحديد المؤسسات الحيوية المزمع إخضاعها للتدقيق بموجب دليل أمن المعلومات والاتصالات.
- إجراء الاستعدادات لعملية التدقيق وفقا لدليل أمن المعلومات والاتصالات.
- تنفيذ أنشطة توعية بدليل أمن المعلومات والاتصالات.

• تطوير البنى التحتية التجريبية للأمن السيبراني.

- إجراء تحليل للوضع الحالي لمراكز تطبيقات وبحوث الأمن السيبراني، ومنصات اختبار الأمن السيبراني ومختبرات الدمج التابعة للجامعات.

• زيادة استخدام منتجات الأمن السيبراني المحلية، لا سيما من جانب المؤسسات العامة.

- إعداد خريطة طريق لتطوير قطاع الأمن السيبراني ومشاركته في السوق العالمية.

• وضع برامج لتدريب قوة عاملة مؤهلة وتحسين الفرص الوظيفية في مجال الأمن السيبراني.

- تنظيم مسابقات الأمن السيبراني للموظفين الشباب المؤهلين.
- تنفيذ أنشطة التعاون والتنسيق لتحديد المعايير المهنية للموظفين العاملين في مجال الأمن السيبراني.

• تحسين محتوى التدريب وجودته وبيئته من أجل تدريب القوة العاملة بما يتماشى واحتياجات قطاع الأمن السيبراني.

- إجراء تدريبات في مجال الأمن السيبراني عبر الإنترنت وفي المختبرات.
- مواصلة التدريبات في مجال الأمن السيبراني عبر الإنترنت عن طريق أكاديمية هيئة المعلومات وتكنولوجيا المعلومات والاتصالات.
- تنظيم تدريبات في مجال الأمن السيبراني التطبيقي في مركز FETIH للتدريب السيبراني.

• إجراء دراسات لتوعية الجمهور بالأمن السيبراني.

- إجراء دراسات لتطوير محتوى الدورات التدريبية في مجال الأمن السيبراني على مستويي التعليم الابتدائي والثانوي.
- وضع آلية الامتثال لدليل أمن المعلومات والاتصالات والتدقيق فيه وبرنامج تدريبي حول التوعية بأمن المعلومات.
- تنظيم أنشطة من قبيل الحلقات الدراسية والدورات التدريبية والمسابقات للتوعية بالأمن السيبراني.

- تعزيز آليات تنفيذ تدابير أمن المعلومات والاتصالات وإنشاء نظم لإدارة أمن المعلومات في المؤسسات العامة ولتشغيلها والتدقيق فيها.

  - وضع قواعد تنظيمية ثانوية للإجراءات والمبادئ المتعلقة بضمان أمن المعلومات والاتصالات.

  - إجراء دراسات حول التشريعات والبنى التحتية في ما يتعلق باستخدام ورصد أسماء النطاقات التابعة لمؤسسات ومنظمات القطاع العام.

4 - أنشطة ومشاريع مكتب التحول الرقمي في ما يتعلق بالقواعد التنظيمية وبالمبادئ التوجيهية للأمن السيبراني

يضطلع مكتب التحول الرقمي بأنشطة هامة لزيادة المنعة الوطنية باتخاذ تدابير لحماية القطاعين العام والخاص من التهديدات السيبرانية. وتشمل الأهداف الرئيسية لهذه الجهود تحسينَ القواعدَ التنظيمية وسياسات الأمن السيبراني، وإنشاء آليات للتدقيق، ومنع الاستعانة بنفس البائعين في البنى التحتية الحيوية، وضمان التحول التكنولوجي الآمن، وحماية بيانات البلد. ويرد أدناه موجز لبعض الدراسات الجارية:

- أعدَّ مشروع قواعد تنظيمية لتحديد الإجراءات والمبادئ المتعلقة بأمن المواقع الشبكية التي تستضيفها مؤسسات ومنظمات القطاع العام وتخصيص النطاقات الفرعية "gov.tr".

- أُعدَّ مشروع قاعدة تنظيمية بشأن ضمان أمن المعلومات والاتصالات لتوفير المتطلبات التقنية لتنفيذ تدابير أمن المعلومات والاتصالات. وإضافة إلى ذلك، أُدرجت في مشروع القاعدة التنظيمية أحكام لإنشاء نظام لإدارة أمن المعلومات وتنفيذه وتعهده والتدقيق فيه وتحسينه بشكل مستمر لمنع أو تخفيف حدة مخاطر أمن المعلومات. والغرض من الشروط المنصوص عليها في مشروع القاعدة التنظيمية هذا هو تطبيقها على جميع المؤسسات العامة.

- والعمل جارٍ حاليا على إعداد قانون وطني للأمن السيبراني. ويتناول هذا القانون إدارة وتنظيم الأمن السيبراني الوطني من خلال "إطار إدارة الأمن السيبراني" الفريد الذي يتوافق مع التطورات التكنولوجية ويزيد من المنعة الوطنية إزاء التهديدات السيبرانية الحالية.

ويلخص الجزء المتبقي من هذا الفرع المبادرات التي نُفذت أو أُنجزت.

4-1 التعميم الرئاسي بشأن تدابير أمن المعلومات 12/2019

إن الرقمنة المتزايدة للمعلومات، وسهولة الوصول المباشر إلى المعلومات، ورقمنة البنى التحتية وانتشار نظم إدارة المعلومات تحمل معها مخاطر أمنية جدّية. وفي هذا السياق، صدر التعميم الرئاسي بشأن تدابير أمن المعلومات 12/2019[66] للحد من المخاطر الأمنية المصادَفة وضمان أمن الأنواع الحرجة من البيانات التي قد تهدد الأمن القومي أو تخل بالنظام العام. ويتضمن التعميم 21 تدبيرا أساسيا لأمن المعلومات والاتصالات[67] ينبغي للمؤسسات العامة والقطاع الخاص اللذين يقدمان خدمات البنية التحتية الحيوية أن يتبعاها. ولكفالة حماية البيانات، يهدف التعميم الرئاسي إلى ضمان بقاء البيانات التي يملكها بلد ما داخل حدود ذلك البلد. وإضافة إلى ذلك، فهو يسلط الضوء على أن إنتاج واستخدام برمجيات الأمن

(66) https://www.mevzuat.gov.tr/MevzuatMetin/CumhurbaskanligiGenelgeleri/20190706-12.pdf.

(67) https://cbddo.gov.tr/en/presidential-circular-no-2019-12-on-information-security-measures.

السـيبراني الوطنية هما من الأولويات الرئيسـية لتركيا. وأخيرا، ينص التعميم أيضـا على "إعداد دليل لأمن المعلومات والاتصـالات بتنسـيقٍ يتولاه مكتب التحول الرقمي من أجل التخفيف من حدة المخاطر الأمنية وإزالتها وبخاصة ضمان أمن البيانات الهامة".

2-4 دليل أمن المعلومات والاتصالات

عطفا على التعميم الرئاسـي بشـأن تدابير أمن المعلومات 12/2019 المذكور أعلاه، نُشـرت وثيقة دليل أمن المعلومات والاتصـالات[68] في عام 2020. والغرض الرئيسي من الدليل هو تحديد تدابير مفصـلة في مجال الأمن السـيبراني لضـمان أمن المعلومات/البيانات والبنى التحتية الحيوية التي قد يؤدي المسّ بها إلى الإخلال بالنظام العام أو تهديد الأمن القومي. وهذا الدليل هو أول وثيقة مرجعية وطنية تُنشـر في هذا المجال، وهو يؤكد على الحاجة إلى اسـتراتيجية أمنية شـاملة تغطي جميع جوانب أمن المعلومات والاتصـالات. وهو يؤدي دوراً هاماً في تعزيز قدرات الدفاع السـيبراني للمؤسـسـات العامة ومقدمي خدمات البنى التحتية الحيوية. وعلاوة على ذلك، يشـترط التعميم الرئاسـي بشـأن تدابير أمن المعلومات 12/2019 ودليلُ أمن المعلومات والاتصـالات على بائعي المنتجات تقديم إفصـاح بأن منتجاتهم عصـيّة على التسـلل إليها من أي أبواب خلفية.

3-4 دليل التدقيق في أمن المعلومات والاتصالات

بغية تحقيق وضمان استمرارية الإنجازات المستهدفة في دليل أمن المعلومات والاتصالات[69]، أعد مكتبُ التحول الرقمي دليلَ التدقيق في أمن المعلومات والاتصـالات ونشرَه في تشرين الأول/أكتوبر 2021، مع الاعتراف بأن أمن المعلومات والاتصالات ممكن تحقيقه من خلال أنشطة التدقيق والمراقبة الفعالة.

ومن المتوقع أن تسـتكمل المؤسـسـات والهيئات العامة والشـركات التي تقدم خدمات البنية التحتية الحيوية أنشـطة الامتثال الخاصـة بها خلال الفترة المحددة في دليل أمن المعلومات والاتصـالات، وأن تجري دراسات تدقيق مرة واحدة على الأقل في السنة من أجل ضمان الامتثال لأنشطتها المنفذة والتدابير المتخذة.

ولا يُطلب من المنظمات ضمن النطاق الامتثالُ لشروط دليل أمن المعلومات والاتصـالات فحسب، بل يطلب منها أيضـا إجراء عمليات تدقيق وتقييم منتظمة لمدى فعالية تنفيذ التدابير الأمنية وما إذا كانت عملية التنفيذ تتماشـى مع الشـروط ذات الصـلة. لذا، ينبغي إجراء عمليات تدقيق منتظمة مرة واحدة على الأقل في السـنة إما من قبل وظيفة التدقيق الداخلي أو شـركات تدقيق طرف ثالث معتمدة. وتوثَّق سـياسـات وإجراءات التدقيق التي يجب أن تقوم بها المؤسـسـات في هذا الصـدد في دليل التدقيق في أمن المعلومات والاتصالات الذي نشره مكتب التحول الرقمي في عام 2021.

4-4 برنامج اعتماد مدقق/شركة أمن المعلومات والاتصالات

صُـمم برنامج اعتماد مدقق/شـركة أمن المعلومات والاتصـالات لتوفير المهارات اللازمة لتحديد مؤهلات وكفاءات الشركات والمدققين الذين سيقومون بعمليات التدقيق في الامتثال وفقا لدليل أمن المعلومات

(68) https://cbddo.gov.tr/en/icsguide/.

(69) https://cbddo.gov.tr/en/icsaguide/.

والاتصـــالات. وينفَّذ البرنامج بالتعاون مع المؤســـسـة التركية للمعايير ومجلس تركيا للبحوث العلمية والتكنولوجية. واعتُمد ما مجموعه 163 مدققا و 23 شركة وأُذن لهم بموجب برنامج الاعتماد منذ عام 2021.

4-5 نظام رصد الامتثال لأمن المعلومات والاتصالات والتدقيق فيه

وُضـــع نظام مراقبة الامتثال لأمن المعلومات والاتصـــالات والتدقيق فيه[70] ودخل قيد الخدمة في 4 كانون الثاني/يناير 2023. ويتيح هذا النظام رصـد نتائج التدقيق لجميع المنظمات التي يشـملها دليل أمن المعلومات والاتصـــالات. ومنذ ذلك الحين، تســـجَّلَ في النظام 945 2 مســـتخدما و 191 1 منظمة. ويمكن للمؤســـســـات أن تقدم معلومات عن التقدم المحرز في امتثالها لدليل أمن المعلومات والاتصـــالات وأنشـــطة التدقيق التي تقوم بها. ويمكن أيضـــا تتبّع المســـتوى الحالي لامتثال المنظمات لنظم إدارة أمن المعلومات من خلال هذه المنصة الرقمية.

4-6 المشروع الوطني لتحليل نموذج إدارة الأمن السيبراني والإبلاغ عنه

أُنجزَ المشـروع الوطني لتحليل نموذج إدارة الأمن السـيبراني والإبلاغ عنه، الذي أُطلق بدايةً لدرس نموذج إدارة الأمن الســـيبراني في تركيا. وأجريَ تحليل مقارن من خلال اســـتعراض حالات بلدان مختلفة، وقُدمت توصيات لتحسينه. ووُضع بنتيجة ذلك "إطار إدارة الأمن السيبراني" لتركيا.

وبعد الانتهاء من المشـروع، نُظمت حلقة عمل وطنية للأمن السـيبراني في 13 كانون الأول/ديسـمبر 2022 لتبادل منتجات المشـــروع الوطني لتحليل نموذج إدارة الأمن الســـيبراني والإبلاغ عنه. وتبادل أكثرُ من 40 مؤسسة عامة وأكثرُ من 100 مشارك آراءهم ومقترحاتهم خلال حلقة العمل. ووفقا لنتائج حلقة العمل، تبيّن أن من الضروري سن قانون وطني للأمن السيبراني. والعمل جارٍ على وضع الصيغة النهائية لهذا القانون.

5 - أنشطة ومشاريع مكتب التحول الرقمي في ما يتعلق ببيئة الأمن السيبراني

5-1 المجموعة المعنية بالأمن السيبراني التركي

في تشـرين الأول/أكتوبر 2017، دُعيت مؤسـسـات القطاع العام والأوسـاط الأكاديمية وشـركات الأمن السـيبراني الكبرى في القطاع الخاص إلى مناقشـة التعاون المحتمل بين هذه الهيئات، ما أفضـى إلى إنشـاء المجموعة المعنية بالأمن السـيبراني التركي[71]. واليوم، تعمل المجموعة بتنسـيق يتولاه مكتب التحول الرقمي وأمانة الصـناعات الدفاعية مع أكثر من 200 عضـو لديهم أكثر من 400 من المنتجات والخدمات. ومجموعة الأمن الســـيبراني التركي هي أيضـــا عضـــو في البيئات العالمية الشـــريكة في الابتكار والأمن السيبراني (Global EPIC) منذ عام 2018.

وتسعى المجموعة المعنية بالأمن السيبراني التركي إلى تحقيق عدة أهداف، منها:

- زيادة عدد شركات الأمن السيبراني
- دعم تنمية القدرات الفنية والإدارية والمالية للشركات الأعضاء

(70) https://cbddo.gov.tr/en/bigdes/.

(71) https://siberkume.org.tr/.

- تحسين العلامة التجارية للمنتجات والخدمات
- تحسين معايير بيئة الأمن السيبراني
- زيادة القدرة التنافسية للشركات الأعضاء في الأسواق الوطنية والعالمية
- تحسين رأس المال البشري في مجال الأمن السيبراني
- التوعية بالأمن السيبراني في المجتمع

ورغم عدم وجود التزام قانوني من جانب القطاع الخاص بالمشـــاركة في هذا التعاون، فإن التركيز يظل منصبا على الثقة المتبادلة والتعاون بين القطاع العام والمؤسسات الخاصة. والدافع الرئيسي لهذا الجهد هو تعزيز العلاقات بين المشـتري والمورّد، وقنوات التوزيع المشـتركة، وفرص التواصـل المشـترك، وأنشـطة البحث والتطوير التي تجريها الجامعات مع الشـركات التي يمكن أن تخلق فرصـا وفوائد أفضـل للطرفين. وبسبب المصالح الاقتصادية المشتركة، أصبحت الشركات في المجموعة أكثر إنتاجية وأكثر ابتكارا، وبالتالي أكثر قدرة على المنافسة من الشركات التي تعمل بمفردها.

ولا يمكن عادةً إحراز نجاح في مجال الأمن السـيبراني دون دعم على أعلى المسـتويات من السـلطة العامة. ولدى تركيا شـركات توسـعت في الخارج ومنتجات ناجحة وفريدة في مجال الأمن السـيبراني يتم تداولها في الخارج. وبعض هذه المنتجات مدرج أيضا في تقارير غارتنر. وفئة محاكاة الاختراق والهجوم هي واحدة منها.

2-5 مجلس العلاقات الاقتصادية الخارجية – مجلس أعمال التكنولوجيا الرقمية – لجنة الأمن السيبراني

بغية زيادة فعالية شـركاتنا المحلية والوطنية في الخارج، أُطلقَ مجلس أعمال التكنولوجيا الرقمية[72] في حزيران/يونيه 2022 بدعم من مكتب التحول الرقمي وبتنسـيقٍ تولاه مجلس العلاقات الاقتصـادية الخارجية. ومجلس أعمال التكنولوجيا الرقمية ملتزم بتنفيذ مشاريع تتعلق بما يلي:

- عولمة بيئة التكنولوجيا الرقمية لتركيا
- التكيف مع الاتجاهات الجديدة
- الوصول إلى التمويل الدولي والتحول الرقمي والقواعد التنظيمية

وهدف مجلس أعمال التكنولوجيا الرقمية هو ما يلي:

- زيادة عدد الشركات التركية المدرجة في قائمة فورتشن 500 وعدد الشركات البليونية التركية
- جعل تركيا مركزا محوريا للتكنولوجيا وإنشاء ممرات رقمية مع بلدان أخرى
- تعزيز صادرات تركيا من منتجات التكنولوجيا المتطورة
- الترويج لتدويل شركات التكنولوجيا من خلال 144 مجلسا من مجالس الأعمال الثنائية في مجلس العلاقات الاقتصادية الخارجية
- دعم التحول الرقمي للشركات الصناعية من خلال العمل في شراكة مع الشركات الناشئة

(72) https://www.deik.org.tr/sectoral-business-councils-digital-technologies-business-council?pm=65.

- زيادة رأس المال المخاطر في القطاع من حيث الحجم والعدد من خلال إنشاء منصات للجمع بين رساميل الاستثمار العالمية ورساميل الاستثمار المحلية وعمليات التوسع والشركات الناشئة
- تحديد المشاكل التي يواجهها القطاع وإبلاغ الجهات الحكومية المختصة بتلك المشاكل

واللجان الفرعية التابعة لمجلس أعمال التكنولوجيا الرقمية هي التالية: التكنولوجيا السحابية، التكنولوجيا المالية، التكنولوجيا الجوالة، الألعاب، الأمن السيبراني، تقنيات البرامجيات، التقنيات الابتكارية، رأس مال الاستثمار، التكنولوجيا الصحية، الويب-3 تقنية سلسلة الكتل. وكما يتضح، ففي هذا الهيكل، حيث للأمن السيبراني أيضا لجنة فرعية، يؤخذ بمنظور قطاعي.

ويتسم تطوير التكنولوجيا المحلية في مجال الأمن السيبراني بأهمية استراتيجية في تركيا وهو معترف به باعتباره مسألة أمن قومي. وبالتالي، فإن التركيز منصبّ على إنشاء منتجات وخدمات معززة وواسعة النطاق قادرة على أن تنافس نظيراتها الأجنبية. وسجلت السوق العالمية للأمن السيبراني، بفضل إدراك متزايد للمخاطر والتهديدات المرتبطة بالبيانات، نموا كبيرا في الآونة الأخيرة. ومن المتوقع أن تظل حصة منتجات وخدمات الأمن السيبراني في السوق آخذة في الازدياد.

وتركيا هي جزء من هذا الاقتصاد الآخذ في التوسع، وهي تتعاون مع القطاع الخاص والمؤسسات الحكومية لتطوير حلولها على نطاق عالمي. وعليه، يعمل مكتب التحول الرقمي على تعزيز التكنولوجيا المحلية للأمن السيبراني. ويشكل هذا المسعى جزءا من الولاية الممنوحة بموجب المرسوم الرئاسي رقم 1 الذي ينص على إجراء دراسات لتطوير منتجات الأمن السيبراني المحلية والوطنية في جميع القطاعات، وبخاصة البنى التحتية الحيوية، وتوسيع نطاق استخدامها في القطاع العام.

وبغية تشجيع نمو البيئة المحلية للأمن السيبراني، أُطلقَ نهج منتظم بتنسيقٍ تولاه مكتب التحول الرقمي. ويهدف هذا النهج إلى دمج نظام الحوافز مع المشتريات العامة، وتقييم مستويات تطوُّر منتجات الأمن السيبراني المحلية وتحسينها وتوسيعها تدريجا.

وشُكل "فريق التنسيق السيبراني على المستوى المحلي" في عام 2021 بتنسيق تولاه مكتب التحول الرقمي وبقيادة أمانة الصناعات الدفاعية ووزارة الصناعة والتكنولوجيا ومكتب الإمداد الحكومي ووكالة المشتريات العامة ورئاسة الاستراتيجية والميزانية. وانضم لاحقا إلى هذا الفريق كل من وزارة الخزانة والمالية ومجلس تركيا للبحث العلمي والتكنولوجي ومؤسسة المعايير التركية وسواتل الاتصالات التركية ووزارة النقل والبنية التحتية وهيئة تكنولوجيا المعلومات والاتصالات. والهدف الرئيسي هو التشجيع على استخدام منتجات الأمن السيبراني المحلية والوطنية في جميع القطاعات، محليا ودوليا، مع التركيز بشكل أساسي على القطاع العام. وتنقسم أنشطة الفريق إلى خمس ركائز رئيسية هي: السياسات، والتشريعات، والتوحيد القياسي/التطور، والحوافز/الدعم/التمويل، والتدويل.

6 - أنشطة ومشاريع مكتب التحول الرقمي في مجال التوعية بالأمن السيبراني

6-1 مسابقات TeknoFest للأمن السيبراني

يدرك مكتب التحول الرقمي أن الحاجة إلى التوعية واكتساب المهارات في مجال الأمن السيبراني أصبحت ملحة بشكل متزايد نظرا للأهمية التي تولى لتكنولوجيا المعلومات والاتصالات. وفي هذا الصدد، ينظم مكتب التحول الرقمي أيضا مسابقات للتوعية بالأمن السيبراني. ومن المشاريع المتميزة مشروع

HackIstanbul المعترف به في جميع أنحاء العالم كمسابقة استثنائية تنظَّم في إطار مهرجان TeknoFest للطيران والفضاء والتكنولوجيا[73] منذ عام 2018. وقد فتحت هذه المسابقات أبوابها لجميع قراصنة الحواسيب حول العالم لإبراز مواهبهم في اسطنبول، وأقيمت المسابقات تحت اسم HackIstanbul، وفي عام 2020 فقط أقيمت المسابقة في غازيانتب تحت اسم HackZeugma. وفي عام 2022، نظم مكتب التحول الرقمي HackBlackSea 2022 في زونغولداك في آب/أغسطس.

وأُغلق باب تقديم الطلبات للمشاركة في مسابقة HackMasters 2023، التي نُظمت في 23 نيسان/أبريل 2023 من هذا العام، في آذار/مارس 2023. وحُدد المتأهلون للتصفيات النهائية خلال مرحلة البحث عن الفدية عبر الإنترنت. وفي المرحلة النهائية، التي نُظمت في 28 نيسان/أبريل، عُرِضَ على المتسابقين سيناريو يركز على الأمن السيبراني للأجهزة الذكية. وحاول قراصنة الحواسيب اختراق النظم من خلال البحث عن مواطن الضعف في الأجهزة المنزلية الذكية وتطبيقات الهاتف الخلوي التي تديرها والبنى التحتية السحابية التي تتلقى بيانات من هذه الأجهزة، في محاولة للتحكم بالنظم.

وفي كل عام، كانت محتويات المسابقة تتناول مفاهيم مختلفة مثل أمن نظم التكنولوجيا التشغيلية، أو المكافأة على زرع برامجيات خبيثة أو تحدي الأمن السيبراني المتمثل في "خطف العلَم". وتهدف هذه المسابقات إلى التوعية بالأمن السيبراني واستقطاب مواهب جديدة إلى القطاع. ومن ناحية أخرى، يحقق هذا المشروع فائدة غير مباشرة هي الترويج لتركيا على النطاق العالمي في مجال الأمن السيبراني.

والموعد النهائي لتقديم الطلبات للمشاركة في مسابقة HackMasters 2024[74] هو 31 أيار/مايو 2024، وستنظَّم المرحلة النهائية في آب/أغسطس 2024 في اسطنبول في إطار TeknoFest[75].

6-2 مسابقة الذكاء السيبراني

ينظم مكتب التحول الرقمي العديد من الخلوات التدريبية وبرامج التدريب في مجال الأمن السيبراني، إلى جانب أنشطة "خطف العلَم" مع المؤسسات العامة المختصة، مثل وزارة التربية الوطنية ووزارة الشباب والرياضة والقطاع الخاص والمنظمات غير الحكومية. وتضمن هذه الخلوات والبرامج التدريبية إلهام عدد كاف من الشباب كي يستفيدوا من مواهبهم في مجال الأمن السيبراني. ومن المهم أيضا ملاحظة أن عدد الطلاب المشاركين في هذه الأنشطة يفوق المليون مشارك.

وعلاوة على ذلك، فإن الحدث البارز الآخر هو مسابقة الذكاء السيبراني[76]. وتندرج هذه المسابقات في إطار أنشطة التدريب والتوعية التي تهدف إلى زيادة عدد الأفراد المدركين لأهمية الأمن السيبراني، وهي فعالة جدا في هذا الصدد. وشارك في المسابقة ما مجموعه 1,5 مليون طالب من المراحل الابتدائية والمتوسطة والثانوية.

والمسابقة هي نشاط عبر الإنترنت ينظَّم بشكل منفصل لكل من المراحل الدراسية الابتدائية والمتوسطة والثانوية. ويعدّ الأسئلةَ مكتبُ التحول الرقمي وتوضع صيغتها النهائية بدعم من وزارة التربية

(73) https://www.teknofest.org/en/.

(74) https://hackmasters.com.tr/.

(75) https://www.teknofest.org/en/competitions/hack-masters/.

(76) https://cbddo.gov.tr/en/projects/cyberintelligencecontest/.

الوطنية بما يراعي المناهج الدراسية الحالية. ويتم الإعلان عنها عبر حسابات وسائل التواصل الاجتماعي لمكتب التحول الرقمي ووزارة التربية الوطنية ومنصة شبكة معلومات التعليم. وفي المسابقة، يتلقى الطلاب الذين يقدمون الإجابات الصحيحة في أقصر وقت ممكن هدايا ومكافآت مفاجِئة بهدف زيادة اندفاعهم في هذا المجال.

ونُظمت المسابقة المعرفية الرابعة للذكاء السيبراني في عام 2023. وتستهدف هذه المسابقة، التي نُظمت لأول مرة في تشرين الأول/أكتوبر 2020 بالتعاون مع رئاسة الجمهورية ووزارة التربية الوطنية، المستويات الدراسية الابتدائية والمتوسطة والثانوية. ونُظمت المسابقة في 27 كانون الأول/ديسمبر 2023 لطلاب المدارس الابتدائية، وفي 28 كانون الأول/ديسمبر 2023 لطلاب المدارس المتوسطة، وفي 29 كانون الأول/ديسمبر 2023 لطلاب المدارس الثانوية. وتسجّل في المسابقة ما مجموعه 915 16 طالبا من المدارس الابتدائية و 955 15 طالبا من المدارس المتوسطة و 528 4 طالبا من المدارس الثانوية.

3-6 الرسوم المتحركة Digital Crew

يسلّم مكتب التحول الرقمي أيضا، بعدما أجرى العديد من الدراسات حول التوعية بالأمن السيبراني على المستوى الوطني، بالحاجة إلى زيادة الإلمام بالتكنولوجيا الرقمية حتى عندما لا يكون الأطفال متصلين بالإنترنت. ويتجاوز ذلك مجرد الدراية التقنية. فالمقصود هنا هو المعارف والمهارات والمواقف التي تتيح للأطفال أن يكونوا آمنين ومقتدِرين في عالم رقمي. ومن أبرز المشاريع الهامة التي نُفذت لهذا الغرض والتي تستهدف الأطفال هي سلسلة شهيرة من الرسوم المتحركة اسمها *Digital Crew*[77]. وهي تُبث عبر الإذاعة التركية وتلفزيون جوجوك ("طفل") منذ عام 2020. والهدف الرئيسي لهذا المشروع هو زيادة الإدراك الرقمي والإلمام بالتكنولوجيا الرقمية والتوعية بها بين الأطفال. وأُعدَّ محتوى سلسلة *Digital Crew*، التي تتكون من 10 حلقات، بالتعاون مع مكتب التحول الرقمي. وتغطي الحلقات طائفة واسعة من المواضيع بدءاً من الإنترنت الآمن للأطفال إلى التنمر السيبراني، ومن إدمان استخدام الإنترنت إلى الذكاء الاصطناعي، ومن إنترنت الأشياء إلى تأثير الرقمنة على الحياة والتكنولوجيا الوطنية.

7 - أنشطة ومشاريع مكتب التحول الرقمي في مجال التثقيف بالأمن السيبراني

ما لا شك فيه أن أحد أهم عناصر ضمان الأمن السيبراني الوطني هو الموارد البشرية ذات الكفاءة والخبرة الكافية. وبغية تلبية احتياجات بلدنا في هذا المجال، يضطلع مكتب التحول الرقمي بأنشطة لزيادة مستوى كفاءة الموارد البشرية الحالية. ويرد أدناه عرض مفصَّل لهذه المبادرات.

1-7 الثانوية المهنية للأمن السيبراني بالتعاون مع وزارة التربية الوطنية في جمهورية تركيا

اتُخذت خطوات محددة لتطوير المهارات والقدرات في مجال الأمن السيبراني في التعليم الرسمي، ونتيجة لذلك، بدأ وضع المناهج الدراسية لمرحلة التعليم الثانوي في عام 2020.

وأنشأت وزارةُ التعليم الوطني بمساهمات من المجموعة المعنية بالأمن السيبراني التركي وأمانة الصناعات الدفاعية ومكتب التحول الرقمي وتكنوبارك اسطنبول ثانويةَ تكنوبارك اسطنبول الأناضولية المهنية

(77) https://www.youtube.com/watch?v=YnuLs6GAogM&ab_channel=CBDijitalD%C3%B6n%C3%BC%C5%9F%C3%BCmOfisi.

والتقنية، وهي أول مدرسة ثانوية للأمن السيبراني في تركيا. وتوفر هذه الثانوية الكائنةُ في تكنوبارك اسطنبول التعليمَ في مجالات تكنولوجيا المعلومات وإدارة الشبكات والأمن السيبراني.

وتتصدر الثانوية المهنية للأمن السيبراني قائمة الثانويات المفضَّلة منذ افتتاحها.

2-7 إنشاء الكليات المهنية للأمن السيبراني بالتعاون مع مجلس التعليم العالي في جمهورية تركيا

شرع مكتب التحول الرقمي في مشروع جديد لتدريب الموظفين المؤهلين في مجال الأمن السيبراني من خلال مواصلة تطوير النموذج المطبَّق في الثانوية المهنية للأمن السيبراني المذكورة أعلاه. وشكّل توقيعُ بروتوكول التعاون بين مكتب التحول الرقمي ومجلس التعليم العالي[78] في عام 2022، الخطوةَ الأولى على طريق إنشاء الكليات المهنية للأمن السيبراني.

وافتُتحت الكليات المهنية للأمن السيبراني، التي ستقدم برامج تعليمية فقط في مجال الأمن السيبراني، في عام 2023. والبرنامج الأول المقدَّم في هذه المدارس هو "محلل ومشغِّل الأمن السيبراني"[79]. وأُطلقَ هذا البرنامج في أربع من كبريات الجامعات في تركيا هي: جامعة أنقرة وجامعة إيجه وجامعة غبزي التقنية وجامعة اسطنبول التقنية.

8 - تركيا في المؤشرات العالمية

نتيجة لاعتماد التقنيات الرقمية على الصعيدين المحلي والوطني، بات الأمن السيبراني لا يقل أهمية عن الأمن المادي للبلاد. ونظراً للتهديد المتزايد، وُظفت استثمارات كافية في مجال الأمن السيبراني في القطاعين العام والخاص. ونُفذ العديد من المشاريع المنسقة في كلٍ من المجالات العام والخاص والعسكري؛ ووظفت منظمات الصناعات الدفاعية الهامة استثمارات كبيرة؛ وأنشئت معاهد خاصة بالأمن السيبراني في المجال الأكاديمي؛ وطُورت منتجات وتكنولوجيات جديدة بقدرات وطنية. ونتيجة لهذه الجهود، أصبحت تركيا مؤخرا واحدة من أنجح البلدان في مجال الأمن السيبراني.

وانعكست الجهود التي تبذلها الجهات الفاعلة الحكومية والقطاع العام لتحقيق هذه الأهداف، إيجابا على ترتيب تركيا في مؤشرات الأمن السيبراني العالمية.

وتتمتع تركيا بمرتبة عالية في مؤشر الأمن السيبراني العالمي، ما يعكس إنجازات البلاد حتى تاريخه.

ووفقا لمؤشر الأمن السيبراني العالمي الذي نشره الاتحاد الدولي للاتصالات في عام 2021[80]، احتلت تركيا المرتبة الحادية عشرة في العالم، بارتفاعٍ بتسع مرتبات مقارنة بالعام السابق وحلت سادسة في أوروبا.

وفي المشهد العالمي اليوم، تؤدي تكنولوجيا المعلومات والاتصالات دورا لا غنى عنه. فهي عصب مجتمعاتنا، الذي يربط بشكل معقد بين الاقتصادات والحكومات والأفراد في أنحاء العالم الشاسع. وتخيُّل عالم خالٍ من الاتصال الفوري أو من الوصول السلس إلى المعلومات أو من القدرة على إدارة الأعمال إلكترونيا

(78) https://cbddo.gov.tr/projeler/siber-myo/.

(79) https://cbddo.gov.tr/sss/siber-myo/.

(80) www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

هو تخيُّل واقع مختلف تماما. وقد أثرت تكنولوجيا المعلومات والاتصالات بشكل واضح على كل جانب من جوانب التجربة الإنسانية، بدءاً من نشر المعرفة وتقديم الرعاية الصحية وصولا إلى مجالات الترفيه والتفاعل الاجتماعي. فهي تعمل على تمكين المواطنين، ورعاية الابتكارات السبّاقة ودفع عجلة النمو الاقتصادي بمعدلات غير مسبوقة. وإضافة إلى ذلك، يمكن للحكومات أن تسخّر قوة تكنولوجيا المعلومات والاتصالات لتقديم الخدمات بمزيد من الكفاءة والشفافية والشمول، معززة بذلك إطارا ديمقراطيا أكثر تشاركية وقوة.

بيد أنه رغم توفير هذا النموذج من الترابط فوائد هائلة، فهو يحمل معه أيضا محذورا هاما هو: الأمن. فمع توسُّع اعتمادنا على تكنولوجيا المعلومات والاتصالات بلا هوادة، تزداد أيضا درجة الضعف التي نعرض أنفسنا لها. وتستغل الجهات الفاعلة الخبيثة، التي تراوح بين المجرمين السيبرانيين الساعين إلى تحقيق مكاسب شخصية والكيانات التي ترعاها الدول والتي لديها نوايا جيوسياسية مبيتة، نقاطَ الضعف هذه لاستهداف البنية التحتية الحيوية والنظم الحكومية التي تحوي بيانات حساسة ومعلومات شخصية للمواطنين. ويخلق الطابع المترابط عالميا للبنية التحتية لتكنولوجيا المعلومات والاتصالات شبكةً معقدة من أوجه الاعتماد المتبادل، حيث يمكن أن تكون لخرق أمني وحيد في ركن ناء من العالم آثار متتالية في أماكن أخرى، ما يمكن أن يؤدي إلى تعطيل الخدمات الأساسية والتسبب في مشاق اقتصادية وتقويض ثقة الجمهور. ويقدم ظهور تكنولوجيات جديدة، مثل الذكاء الاصطناعي وإنترنت الأشياء بعدا جديدا تماما للتحديات الأمنية يتطلب اهتماما فوريا وإيجاد حلول مبتكرة حيث غالبا ما تقدم هذه التكنولوجيات وسائل شن هجوم جديد وتعقيدات في توفير الأمن لشبكات واسعة من الأجهزة المترابطة.

لذا يتحتم توخي الحرص في سلوك مسار يعزز توازنا حصيفا بين تسخير الإمكانات الهائلة لتكنولوجيا المعلومات والاتصالات والتخفيف من حدة المخاطر المرتبطة بها. ويجب على الدول أن تولي الأولوية لأمن تكنولوجيا المعلومات والاتصالات وأن تعترف به باعتباره ضرورة حتمية للأمن القومي. ويتطلب ذلك نهجاً متعدد الأوجه. إن من الأهمية بمكان وضع استراتيجيات وطنية معزَّزة للأمن السيبراني، مدعومة بشراكات قوية بين القطاعين العام والخاص تستفيد من خبرات وموارد الحكومة والقطاع.

كما أن الجهود التعاونية بين الحكومات والشركات للاستثمار في تثقيف وتوعية المواطنين والمسؤولين الحكوميين بالأمن السيبراني لا تقل عن ذلك أهمية. ولا ينبغي لهذا التثقيف أن يشمل المهارات التقنية اللازمة لتحديد التهديدات السيبرانية والتخفيف من حدتها فحسب، بل أن يعزز أيضا ثقافة النظافة السيبرانية بين المواطنين.

وعلاوة على ذلك، فإن تعزيز التعاون الدولي في مجال أمن تكنولوجيا المعلومات والاتصالات هو أمر أساسي لا يمكن إنكاره. وفي هذا السياق، يكتسي الحوار المنتظم بين المؤسسات تحت مظلة الأمم المتحدة أهمية كبرى. ويجب على الدول الأعضاء أن تعمل معا لوضع إطار للقواعد والمعايير والأطر القانونية الدولية التي تشجع السلوك المسؤول في الفضاء السيبراني. وينبغي لهذا الإطار أن يشمل بروتوكولات لتبادل المعلومات تيسر الاستجابةَ السريعة للتهديدات السيبرانية، وبذل جهود تعاونية لإنفاذ القانون من أجل مكافحة الجريمة السيبرانية بمزيد من الفعالية، ووضع معاهدات دولية تحدد معايير للسلوك المقبول في الفضاء السيبراني. وفي نهاية المطاف، يتجاوز الهدف التدابير الدفاعية البحت لبناء بنية تحتية مرنة لتكنولوجيا المعلومات والاتصالات. ويشمل ذلك تصميم نظم لا تتمتع فقط بالقوة اللازمة لمواجهة الهجمات السيبرانية ولكن أيضا القدرة على التعافي بسرعة وتقليل الاضطرابات إلى الحد الأدنى والحفاظ على سلامة البيانات. وإضافة إلى ذلك، من المهم تشجيع التطوير والاستخدام الأخلاقيين لتكنولوجيا المعلومات والاتصالات. وفي وسع الدول الأعضاء أن تضمن

أن هذه التكنولوجيا القوية تخدم الصالحَ العام للقيم الإنسانية من خلال إيلاء الأولوية لخصوصية المستعملين، والدعوة من أجل ممارسات بحثية مسؤولة تقلل إلى أدنى حد من احتمال إساءة الاستخدام، وضمان الشفافية في تطوير ونشر نظم تكنولوجيا المعلومات والاتصالات.

ومن خلال إيلاء الأولوية للأمن مع تشجيع الابتكار، يمكن للدول الأعضاء ضمان استمرار تكنولوجيا المعلومات والاتصالات في أداء دور تحويلي وإيجابي في رسم ملامح عالمنا. إن اتّباع هذا النهج التعاوني، إلى جانب التحلي باليقظة والتكيف المستمرين، أساسي لضمان مستقبل رقمي آمن ومزدهر للجميع.

الولايات المتحدة الأمريكية

[الأصل: بالإنكليزية
1 أيار/مايو 2024]

مقدمة

أقرت الدول الأعضاء في الأمم المتحدة بأن تكنولوجيات المعلومات والاتصالات يمكن أن تستخدم لأغراض تنافي الهدف المتمثل في صون السلام والاستقرار الدوليين. فعلى مدار سنوات عديدة، اجتمعت الدول برعاية الأمم المتحدة لمناقشة هذه المسألة ومعالجتها. ومن خلال التأكيد بالتوافق على تقارير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي والفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021–2025، تجمعت الدول حول إطار للسلوك المسؤول للدول في استخدام تكنولوجيا المعلومات والاتصالات. وانطوى هذا الإطار المتعلق بتعزيز الاستقرار الدولي على تطبيق القانون الدولي ذي الصلة، بما في ذلك ميثاق الأمم المتحدة، وكذلك على مجموعة من القواعد غير الملزمة وتدابير بناء الثقة.

ومع أن الإطار حظي بتأييد عالمي، فإن نجاحه يتوقف على التزام الدول بعناصره وتنفيذها. وكما ورد لأول مرة في تقرير فريق الخبراء الحكوميين الذي حظي بالتوافق في عام 2015، أكدت الدول ضرورة إقامة حوار منتظم بين المؤسسات بمشاركة واسعة تحت رعاية الأمم المتحدة[81]. وبناء على ذلك الجهد، ما برح الفريق العامل المفتوح العضوية يؤكد مجددا بشكل مستمر الحاجة إلى أن تسعى الدول إلى إنشاء آلية للحوار المؤسسي في المستقبل[82].

وإضافة إلى ذلك، وكما لوحظ في أحدث تقرير مرحلي سنوي للفريق العامل المفتوح العضوية صدر بالتوافق، اتفقت الدول على مجموعة أولية من العناصر المشتركة للحوار المؤسسي المنتظم، واتفقت أيضا على مواصلة المناقشات بشأن برنامج عمل مقبل. والمهم في الأمر هو أن الدول اتفقت على أنه ينبغي للحوار المؤسسي المنتظم المقبل أن يتخذ "أساسا لعمله الاتفاقات المتخذة بالتوافق بشأن إطار سلوك الدول المسؤول"[83]. واتفقت الدول أيضا على أنه ينبغي للحوار المقبل أن يكون دائما وأحادي المسار وبقيادة الدول[84]. وخلصت الدول كذلك إلى أنه ينبغي للآلية أن تكون مفتوحة وشاملة للجميع وشفافة ومستدامة

(81) A/70/174، الفقرة 18.

(82) A/75/816، الفقرات 70 إلى 74، و A/78/265، الفقرة 52.

(83) A/78/265، الفقرة 55 (ج).

(84) المرجع نفسه، الفقرة 55 (أ).

ومرنة[85] حتى تتمكن من التكيف حسب الضرورة مع مشهد التهديدات السيبرانية السريع التطور. وشدد الأمين العام في تقريره الصادر في نيسان/أبريل 2023 (A/78/76) على الحاجة الملحة إلى إنشاء البرنامج وسلط الضوء على العديد من القضايا نفسها التي تتناولها العناصر المشتركة المحددة في التقرير المرحلي السنوي للفريق العامل المفتوح العضوية لعام 2023، بما في ذلك أن الإطار "يجب أن يكون بمثابة خط أساس" لبرنامج العمل[86]. وفي التقرير، خلص الأمين العام أيضا إلى أن العديد من الدول تثمّن المشاركة الشاملة للجميع والهادفة للجهات المعنية غير الحكومية[87]. وواصلت الدول الدعوةَ إلى مشاركة الجهات المعنية المتعددة مشاركة مُجدية في الاجتماعات الرسمية واجتماعات ما بين الدورات للفريق العامل المفتوح العضوية.

وعلى مدى العامين الماضيين، تجمعت الدول حول برنامج العمل بوصفه الآلية الدائمة المقبلة لمناقشات اللجنة الأولى للأمم المتحدة بشأن القضايا السيبرانية. وفي الآونة الأخيرة، صوتت جميع الدول الأعضاء في الأمم المتحدة تقريبا تأييدا للقرار 16/78 الذي أنشأت فيه الجمعية العامة بشكل حاسم الآلية تحت رعاية الأمم المتحدة عند اختتام أعمال الفريق العامل الحالي المفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات وباستخدامها.

وكما هو مبين في القرار، سيكون برنامج العمل بمثابة آلية دائمة، ولكن مرنة، في الأمم المتحدة للنهوض بعمل الإطار الرامي إلى تعزيز السلام والأمن في الفضاء السيبراني، بما في ذلك من خلال المشاركة الهادفة مع أوساط الجهات المعنية المتعددة وتيسير بناء القدرات من خلال دور الأمم المتحدة باعتبارها منبرا لتبادل المعلومات.

نطاق برنامج العمل

حددت الجمعية العامة في قرارها 37/77 نطاق وولاية برنامج العمل على النحو التالي:

"آلية دائمة وشاملة للجميع وعملية المنحى لمناقشة التهديدات القائمة والمحتملة؛ ودعم قدرات الدول وجهودها الرامية إلى التنفيذ واسترشاد تعزيز الالتزامات بإطار سلوك الدول المسؤول، الذي يتضمن قواعد طوعية وغير ملزمة لتطبيق القانون الدولي في استخدام تكنولوجيات المعلومات والاتصالات من جانب الدول، وتدابير بناء الثقة وبناء القدرات، على النحو الذي أكده قرار الجمعية العامة 19/76 وتقارير أفرقة الخبراء الحكوميين للأعوام 2010 و 2013 و 2015 و 2021، وتقرير الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي لعام 2021، والتقرير المرحلي السنوي الأول للفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025؛ ومناقشة هذا الإطار ومواصلة تطويره عند الاقتضاء؛ وتعزيز المشاركة

(85) المرجع نفسه، الفقرة 55 (د).

(86) A/78/76، الفقرة 42.

(87) A/78/76، الفقرة 40.

والتعاون مع أصحاب المصلحة المعنيين؛ والاستعراض الدوري للتقدم المحرز في تنفيذ برنامج العمل، وكذلك أعمال البرنامج في المستقبل"[88].

وأكدت الجمعية العامة من جديد، في قرارها 16/78، أهداف برنامج العمل على النحو المبين في القرار 77/37 وقررت أيضا أن تتضمن الآلية العناصر المشتركة المبينة في التقرير المرحلي للفريق العامل المفتوح العضوية لعام 2023. وعلاوة على ذلك، قررت الجمعية أن يستند نطاق برنامج العمل وهيكله ومحتواه وطرائقه إلى نتائج الفريق العامل المفتوح باب العضوية بالتوافق.

وفي القرارات المتعلقة ببرنامج العمل والقرارات المتخذة بالتوافق والتي أكدت تقريري فريق الخبراء الحكوميين والفريق العامل المفتوح العضوية، أكدت الدول مرارا توقّعها أنه ينبغي للدول أن تسترشد في إجراءاتها بتقييمات وتوصيات أفرقة الخبراء الحكوميين للأعوام 2010 و 2013 و 2015 و 2021، وكذلك بنتائج الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي لعام 2021، إلى جانب المنتجات التوافقية الحالية للفريق العامل المفتوح العضوية (مثل التقريرين المرحليين السنويين الأول والثاني)، ولا سيما "الإطار التراكمي والمتطور للسلوك المسؤول للدول في استخدام تكنولوجيا المعلومات والاتصالات الذي وُضع واعتُمد بالتوافق من خلال هذه العمليات"[89]. وهذا الإطار التوافقي، الذي صاغه فريق الخبراء الحكوميين بالتوافق، وتقارير الفريق العامل المفتوح باب العضوية وأيدته جميع الدول الأعضاء مرارا، هو الأساس الذي يقوم عليه برنامج العمل.

وستحدد الدول الأعضاء اتجاه برنامج العمل وتحدثه بمرور الوقت، مع إبقاء أولوية التركيز على التنفيذ العملي وأعمال بناء القدرات المخصصة لتنفيذ الإطار. فالطابع الدائم لبرنامج العمل سيجعل منه موردا دائما للدول في هذه الجهود.

وينبغي أيضا لبرنامج العمل، بوصفه آلية دائمة، أن يتمتع بالمرونة اللازمة للتصدي للتهديدات في المستقبل وبالسرعة اللازمة لتقييم الاحتياجات المتطورة للدول وأفضل الممارسات للتصدي لهذه التهديدات. وفي إطار برنامج العمل، ستتمكن الدول أيضا من النظر في ما إذا كان ينبغي لإطار التوافق أن يتطور بمرور الوقت وفي كيفية تطوره.

وستكون الجهات المعنية غير الحكومية جزءا لا يتجزأ من عملية برنامج العمل. وتشمل جميع جهود بناء القدرات تقريبا، سواء كانت دولية أو محلية، القطاع الخاص والمجتمع المدني والأوساط الأكاديمية وغيرها من أنشطة وخبرات الجهات المعنية غير الحكومية. ويجب أن يتضمن برنامج العمل طرائق لمشاركة الجهات صاحبة المصلحة تكون شاملة قدر الإمكان للاستفادة بشكل كامل من خبرات هذه الجهات.

إنشاء برنامج العمل

يجب أن تهدف الدول الأعضاء إلى تحقيق انتقال سلس إلى برنامج العمل في عام 2025 بعد اختتام أعمال الفريق العامل المفتوح العضوية للفترة 2021-2025. ويجب تيسير هذا الانتقال بتقرير نهائي للفريق العامل المفتوح باب العضوية يؤكد من جديد ولاية البرنامج على النحو المحدد في قرار الجمعية العامة 37/77 ويستند إلى إطار التوافق، ويحدد هيكله العملي المنحى وأساليب عمله، ويحدد مجالات العمل

(88) قرار الجمعية العامة 37/77، الفقرة 1.

(89) قرار الجمعية العامة 16/78، الفقرة 8 من الديباجة.

ذات الأولوية، ويؤكد اتباع نهج شامل إلى أقصى حد إزاء مشاركة الجهات المعنية، ويحدد الخطوات التالية والتوقيت التفصيلي للإطلاق الرسمي للبرنامج بحلول عام 2026.

ولتحديد طرائق برنامج العمل بشكل كامل، قد يكون من الضروري عقد اجتماع تحضيري إضافي أو تنظيم عملية تحضيرية إضافية. وإضافة إلى ذلك، إذا فشل الفريق العامل المفتوح باب العضوية في التوصل إلى توافق بشأن تقرير نهائي، سيتعين عقد "مؤتمر دولي"[90] أكثر شمولا أو عملية تحضيرية أخرى تنشأ من خلال الجمعية العامة لتنفيذ التوجيه المبين في القرار 16/78 لبدء البرنامج بحلول عام 2026. ويجب أن تبدأ اجتماعات البرنامج في عام 2026 لضمان استمرارية هذه المناقشات الهامة المتعددة الأطراف.

وبالنظر إلى ولاية برنامج العمل الرامية إلى معالجة بُعديْ السلام والأمن لاستخدام تكنولوجيات المعلومات والاتصالات، سيكون من الطبيعي إنشاؤه في إطار اللجنة الأولى للأمم المتحدة. وسيكون مكتب شؤون نزع السلاح بشكل منطقي أمانة هذه الآلية المقبلة. وينبغي للبرنامج أن يعمل، قدر المستطاع، في حدود موارد الميزانية المتاحة.

الهيكل

ينبغي أن يتألف هيكل برنامج العمل من أفرقة عاملة تقنية تجتمع ثلاث أو أربع مرات في السنة، ومن جلسات عامة سنوية ومؤتمرات استعراضية دورية. وسيدعم البرنامج مكتب أمانة داخل مكتب شؤون نزع السلاح.

إن مجموعات العمل الفنية لبرنامج العمل هي جوهر طبيعته العملية المنحى – وليست ميزة اختيارية. ولجعل هذه الأفرقة شاملة قدر الإمكان، ستدعى جميع الدول المهتمة إلى العمل معا في أفرقة مركزة لوضع توصيات ملموسة تدعم تنفيذ الإطار. وستدرج هذه التوصيات في تقارير لتنظر فيها الجلسة العامة، وفي نهاية المطاف، الجمعية العامة.

ويجب أن تكون هذه الأفرقة العاملة متعددة الأقاليم في تكوينها وأن تتبع نهجا شاملا لتنفيذ الإطار، ووضع التوصيات والتقييمات وأفضل الممارسات بشأن قضايا مثل:

- حماية البنى التحتية الحيوية
- تيسير التعاون بين الدول في أعقاب حادث سيبراني خطير
- سبل تحسين المساءلة عن سلوك الدول غير المسؤول في الفضاء السيبراني
- تبادل المعلومات حول مشهد التهديدات السيبرانية المتطور
- تحسين قدرة الدول على ردع تهديدات تكنولوجيا المعلومات والاتصالات وتعطيلها

ومن شأن المناقشات القائمة على القضايا أن تيسر إجراء مناقشة موضوعية شاملة بشأن تنفيذ الإطار الذي يخرج عن الصوامع التقليدية للتهديدات والمعايير والقانون الدولي وبناء القدرات. وفي الفريق العامل المفتوح باب العضوية، شددت الدول مرارا وتكرارا على أن هذه المواضيع تتسرب إلى بعضها البعض ويلزم النظر فيها بصورة كلية. وتتفق الدول أيضا على أن بناء القدرات، على وجه الخصوص، يشمل جميع

(90) قرار الجمعية العامة 37/77، الفقرة 3.

المواضـــيع. ومن شـــأن تحديد أولويات الحوار بشـــأن احتياجات بناء القدرات داخل الأفرقة العاملة المعنية بالتنفيذ أن يؤدي إلى توصيات واقعية وقابلة للتنفيذ وأن يسرع التنفيذ.

وينبغي تكليف الاجتماع العام الســـنوي بتقييم التقدم الذي تحرزه الأفرقة العاملة التقنية، والمضـــي قدما بأي توصيات من تلك الأفرقة، ومناقشة التهديدات المستمرة والناشئة، والنظر في حالة المبادرات العملية مثل تدابير بناء الثقة. ويجوز أن توفر الجلســـة العامة التوجيه للأفرقة العاملة التقنية والمبادرات العملية، حسب الاقتضاء.

وينبغي أن يجتمع مؤتمر الاستعراض الدوري مرة كل ثلاث أو أربع سنوات (ليحل محل الاجتماع العام السنوي خلال سنوات المؤتمر) لجميع الدول الأعضاء لتقييم المشهد المتطور للتهديدات السيبرانية ونتائج مبادرات برنامج العمل وأفرقته العاملة، وتحديث الإطار حسب الاقتضاء، وتوفير التوجيه الاستراتيجي والولايات للجلسات العامة المقبلة للبرنامج، الأفرقة العاملة وغيرها من المبادرات. وهذا الاستعراض الدوري للبرنامج سيمنح الدول المرونة اللازمة لتكييف البرنامج مع تطور الظروف.

وفي كل عام بعد إطلاق برنامج العمل في عام 2026، ســـتؤكد اللجنة الأولى أي نتائج توافقية للاجتماعات الســـنوية للبرنامج من خلال قرار أو مقرر. وســـتؤكد اللجنة الأولى أيضـــا نتائج مؤتمرات الاستعراض الدوري عند انعقادها.

وســـتكلف أمانة برنامج العمل، التي يديرها مكتب شـــؤون نزع الســـلاح، بدعم إدارة مختلف الاجتماعات البرنامجية؛ الحفاظ على منصـــات تبادل المعلومات وآليات الاتصـــال والمحفوظات؛ وإدارة المبادرات والمشاريع العملية مثل دليل نقاط الاتصال ومستودع التهديدات وبوابات تبادل المعلومات.

بناء القدرات

بالنظر إلى أن البلدان تمر بجميع مراحل تطوير خبراتها ومهاراتها الســـيبرانية، فقد اعترفت الأمم المتحـدة بـأن بنـاء القـدرات ضـــروري لتعـاون الـدول وبنـاء الثقـة في مجـال تكنولوجيـات المعلومـات والاتصـــالات[91]. وللأمم المتحدة دور رئيســـي في الدعوة إلى عقد الاجتماعات، والتنســـيق مع طائفة من الأطراف الفاعلة من الجهات المتعددة صـاحبة المصـلحة التي تشـارك بفعالية في بناء القدرات بشـأن المسائل السيبرانية ذات الصلة، وكذلك في تنفيذ برامج محددة لبناء القدرات وفقا لتوجيهات الدول الأعضاء، كما أن لها دورا رئيسيا في تسليط الضوء على تلك الطائفة من الأطراف الفاعلة.

ويجب أن ترتبط الوظيفة الرئيســـية لبرنامج العمل في مجال بناء القدرات ارتباطا مباشـــرا بالجهود التي تبذلها الدول على الصعيد الوطني لتنفيذ الإطار. وينبغي أن ييسر برنامج العمل أيضا إجراء مناقشات مخصصة بشأن أنواع بناء القدرات التي تحتاج إليها الدول من أجل تنفيذ الإطار لكفالة تماشي جهوده على نحو وثيق مع طائفة من احتياجات الدول. وبعبارة أخرى، ينبغي أن يهدف إلى إذكاء الوعي الدولي بأهمية بناء القدرات السيبرانية لدعم الإطار وتيسير التنسيق وتبادل المعلومات بشأن البرامج المتاحة لبناء القدرات السيبرانية إلى جانب أصحاب المصلحة الآخرين، مع توفير التوجيه وأفضل الممارسات التي يمكن للدول استخدامها محليا/وطنيا لتنفيذ الإطار.

(91) المرجع نفسه، الفقرة 20 من الديباجة.

وتدرك الولايات المتحدة أن دولا كثيرة ما زالت تفتقر إلى فهم عميق لماهية الإطار وأهميته. فالكثير منها يفتقر أيضا إلى القدرات في مجال الأمن السيبراني على الصعيد الوطني اللازمة لتنفيذ الإطار، بما في ذلك السلطات والقدرات المحلية المرتبطة بدعم المعايير وتدابير بناء الثقة. وهناك طائفة من الكيانات القائمة التابعة للأمم المتحدة وغير التابعة لها من ذات الخبرة في مجالات من قبيل السياسات والاستراتيجيات الوطنية في مجال الأمن السيبراني، وإدارة الحوادث السيبرانية وحماية البنى التحتية الحيوية، والتشريعات المحلية المتعلقة بالجرائم السيبرانية، وثقافة الأمن السيبراني، ومعايير الأمن السيبراني، والتنسيق بين الجهات المانحة، والتوفيق بين المساعدة الدولية في مجال الأمن السيبراني. ويجب ألا يكرر برنامج العمل هذه الجهود القائمة أو يلغيها. فكل هذه البرامج – التي هي بمعظمها ذات طابع متعدد الجهات المانحة – تعزز حالة الأمن الوطني للدول وتمكّن في نهاية المطاف من تنفيذ الإطار، وإن كانت لا تدخل في نطاق ولاية برنامج العمل.

مشاركة متعددة الأطراف

يجب أن تحتفظ الدول بسلطة حصرية لاتخاذ القرارات في إطار برنامج العمل. ومع ذلك، فإن الجهات غير الحكومية صاحبة المصلحة، بما في ذلك المجتمع المدني والأوساط الأكاديمية والهيئات الإقليمية والدولية والقطاع الخاص، تضطلع بدور إيجابي في المنتديات المتعددة الأطراف بالمساهمة بخبراتها في المناقشات الرسمية والمساهمة في جهود بناء القدرات. ويجب أن تتاح للجهات المعنية غير الحكومية فرصة للمشاركة والمساهمة بفعالية في برنامج العمل بصفة مراقب، دون أن يكون لها حق التصويت. وستكون خبرة أصحاب المصلحة غير الحكوميين ذات أهمية خاصة داخل الأفرقة التقنية أو العاملة. وستيسر هذه الأفرقة العاملة التقنية مشاركة أكثر تعمقا وعملية مع مجموعة من أصحاب المصلحة من غير الدول. ويمكن لأصحاب المصلحة أيضا أن يقدموا تقارير دورية عن جهودهم الرامية إلى تنفيذ المبادرات التي تركز على الإطار، بما في ذلك بناء القدرات.

ولكي يكون برنامج العمل شاملا قدر الإمكان لأصحاب المصلحة المهتمين، بما في ذلك داخل أفرقته العاملة التقنية الفرعية، ينبغي أن تستند الطرائق إلى المعايير الذهبية القائمة لمشاركة أصحاب المصلحة، بما في ذلك توفير الشفافية فيما يتعلق باعتراضات الدول وعملية لتقييم الاستبعادات المحتملة. فعلى سبيل المثال، يمكن للدول أن تنظر إلى الفريق العامل المفتوح العضوية المعني بالشيخوخة باعتباره نموذجا. فطرائق ذلك الفريق تتيح الفرصة للدول الأعضاء للاعتراض على مشاركة منظمة ما ولكنها تتطلب إبداء الاعتراضات علناً لتوعية الدول الأعضاء وإجراء تصويت لاحقاً لتحديد ما إذا كان ينبغي استبعاد المنظمات التي أبدي الاعتراض بشأنها. ويؤذن تلقائيا للمنظمات التي لا تعترض عليها أي دولة عضو في الجولة الأولى بالمشاركة في الدورة الرسمية[92].

وبالإضافة إلى الاعتبارات المتعلقة بكيفية اعتماد أصحاب المصلحة لحضور اجتماعات برنامج العمل، ينبغي أن توفر الطرائق أيضا إرشادات بشأن الكيفية التي يمكن بها لأصحاب المصلحة المعتمدين أن يساهموا في مناقشات البرنامج عمليا. وفي هذا المجال، يمكن للجنة المخصصة لوضع اتفاقية دولية

(92) على النحو المبين بوضوح في الفرع واو من الوثيقة A/AC.278/2011/2.

شـاملة بشـأن مكافحة اسـتخدام تكنولوجيات المعلومات والاتصـالات للأغراض الإجرامية أن تكون بمثابة نموذج. فطرائقها تتيح مشاركة الجهات المتعددة صاحبة المصلحة، بما في ذلك:

- حضور أي جلسة رسمية مفتوحة.
- الإدلاء ببيانات شـفوية، رهنا بالوقت المتاح، في نهاية مناقشـات الدول الأعضـاء، بشـأن كل بند موضـوعي من بنود جدول الأعمال. ونظرا لضـيق الوقت المتاح في الاجتماعات، يمكن للجهات المتعددة صـاحبة المصـلحة النظر في اختيار متحدثين رسـميين من بينها، بطريقة متوازنة وشـفافة، مع مراعاة التمثيل الجغرافي العادل، وتكافؤ الجنسـين، وتنوع الجهات المتعددة صـاحبة المصـلحة المُشاركِة في الاجتماعات.
- تقديم مواد خطية ومحدودة من حيث عدد الكلمات. وتُنشَـر هذه الإفادات بلغتها الأصـلية على الموقع الشبكي للجنة المخصصة[93].

وينبغي لبرنامج العمل أيضـا أن يستفيد من الخبرات القائمة والعمل الجاري على الصـعيد الإقليمي. وإن إتاحة المشـاركة لتلك الكيانات في مناقشـات برنامج العمل، بصـفتها جهات صـاحبة مصـلحة، سـتساعد العمل الجاري على صـعيد الأمم المتحدة على الاندماج بشكل أفضـل في الجهود الإقليمية ومراعاة التحديات والسياقات الإقليمية المحددة.

فنزويلا (جمهورية – البوليفارية)

[الأصل: بالإسبانية
26 نيسان/أبريل 2024]

في الفقرة 8 من القرار 237/78 الذي اتخذته الجمعية العامة في 22 كانون الأول/ديسمبر 2023، تدعو الجمعيةُ جميع الدول الأعضاء إلى مواصلة إعلام الأمين العام بآرائها وملاحظاتها بشأن أمن تكنولوجيا المعلومات والاتصـالات وأمن اسـتخدامها، ولا سـيما بشـأن الجولة المقبلة للحوار المنتظم حول هذه المسـائل المتوخى أن تُعقد برعاية الأمم المتحدة، كما تطلب إلى الأمين العام أن يحيل إليها في دورتها الثامنة والسـبعين تقريرا يعده بناء على تلك الآراء لمواصـلة المناقشـات بين الدول الأعضـاء في هذا الصـدد خلال اجتماعات الفريق العامل المفتوح العضوية في دورته الثامنة المقرر عقدها في عام 2024.

وفي هذا الصـدد، تعتقد جمهورية فنزويلا البوليفارية أن من الضـروري التأكيد على ما للدور الذي يقوم به الفريق العامل المفتوح العضوية والقالبِ الذي تتخذه أعماله من أهمية بالنسبة إلى تنفيذ ولاية الجمعية العامة على نحو ما نُص عليها في قرار الجمعية 240/75. وتبيّن الإنجازات التي تحقّقت في السـنوات الأخيرة – ومنها مثلا وضـع الدليل الحكومي الدولي العالمي لجهات الاتصـال – أن الشـكلَ الحالي للفريق العامل المفتوح العضوية أثبت نجاحه الملحوظ، لا سيما في ضوء اعتماده توافق الآراء وسيلة لاتخاذ القرارات واعتماد التقارير السنوية.

وتعتقد جمهورية فنزويلا البوليفارية أن الأمم المتحدة ينبغي أن تواصل القيام بدور جوهري ومحوري في تعزيز الحوار بشأن استخدام الدول لتكنولوجيا المعلومات والاتصالات. ويقتضي الطابع الفريد لتكنولوجيا

(93) A/AC.291/6، الفقرة 3.

المعلومات والاتصالات وضعَ مبادئ ومعايير جديدة – يُفضل أن تكون ملزِمة قانوناً – تتيح سد الثغرات القائمة بين القانون الدولي القائم وواقع العالم الافتراضي.

وفي ضوء ما تقدّم، تتبين الضرورة الملحة للإذن بأن تتواصل أعمال الفريق العامل المفتوح العضوية للفترة 2021 إلى 2025، من خلال فريق عامل دائم جديد مفتوح العضوية يُنشأ بعد عام 2025، وهو ما سيساعد على تعزيز قدرة الفريق العامل المفتوح العضوية بتشكيلته الجديدة على وضع وتكييف قواعد جديدة ملزِمة قانوناً تساعد في تحسين الأمن الدولي في استخدام تكنولوجيات الاتصالات والمعلومات.

وثمة حاجة ملحة أيضا إلى تزويد الفريق العامل المقبل المزمع إنشاؤه بعد عام 2025 كفريق مفتوح العضوية بالقدرة على معالجة التحديات الناشئة عن الفجوة الرقمية الواسعة التي تفصل بين البلدان الأعضاء، وهي فجوة تجعل تنفيذ الاستراتيجيات العالمية لتعزيز الأمن الدولي في استخدام تكنولوجيات الاتصالات والمعلومات أمرا عسيرا.

وأخيرا، تؤيد جمهورية فنزويلا البوليفارية تأييدا شديدا الجهود الواسعة التي تبذلها رئاسة الفريق العامل المفتوح العضوية للتوصل إلى توافق في الآراء في كل ما يضطلع به الفريق من أنشطة وتكرر التعبير عن استعدادها لمواصلة المشاركة في هذه العملية ودعمها.

الردود الواردة من المنظمات الحكومية الدولية

الاتحاد الأوروبي

[الأصل: بالإنكليزية
29 نيسان/أبريل 2024]

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

ويسلّم المجتمع الدولي بأن القانون الدولي الحالي، بما في ذلك ميثاق الأمم المتحدة بكامله، ينطبق على تصرف الدول في الفضاء السيبراني وأنه ضروري لصون السلام والاستقرار وتعزيز بيئة مفتوحة وآمنة وسلمية ويمكن الوصول إليها لتكنولوجيا المعلومات والاتصالات.

وقد جرى وضع وتوحيد إطار لسلوك الدول المسؤول في الفضاء الإلكتروني عملا بالتوصيات الصادرة بتوافق الآراء عن أفرقة الخبراء الحكوميين لأعوام 2010 و 2013 و 2015 و 2021، والتوصية بتوافق الآراء الصادرة عن الفريق العامل المعني بالتطورات في ميدان المعلومات والاتصالات لعام 2021، والتقرير المرحلي السنوي لعامي 2022 و 2023 الصادر بتوافق الآراء عن الفريق العامل المعني بأمن تكنولوجيات المعلومات والاتصالات 2021–2025 ويتألف الإطار تطبيق القانون الدولي على الفضاء الإلكتروني، ومعايير طوعية لسلوك الدول المسؤول، وتدابير لبناء الثقة، وبناء القدرات.

ويؤكد الاتحاد الأوروبي والدول الأعضاء فيه من جديد التزامنا بالعمل وفقا لهذه الاتفاقات القائمة، والتزامنا بالعمل وفقا للقانون الدولي، بما في ذلك الميثاق برمته، فضلا عن معايير السلوك المسؤول للدول في الفضاء الحاسوبي. نحن ملتزمون بتعزيز السلام والاستقرار السيبراني وتقدمهما من خلال المناقشات وفي المنتديات مثل مجموعة العمل المفتوحة العضوية الحالية.

وإزاء هذه الخلفية، واتساقا مع دعمنا لعمل الفريق العامل المفتوح باب العضوية، لم يكن الاتحاد الأوروبي في وضع يسمح له بتأييد القرار 237/78 المعنون "التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي"، الذي اتخذته الجمعية العامة في 22 كانون الأول/ديسمبر 2023.

ويرى الاتحاد الأوروبي أن القرار كان يمكن أن يمثل على نحو أفضل توافق الآراء الهش الذي تحقق في الفريق العامل المفتوح باب العضوية، وعملياته السابقة وقراراته السابقة بتوافق الآراء.

وبشكل أساسي، فشل القرار في الإشارة إلى الإطار التراكمي والمتطور للسلوك المسؤول للدولة في استخدام تكنولوجيا المعلومات والاتصالات – وهو إطار هو نتيجة لأكثر من 20 عاما من المفاوضات وأقرته الجمعية العامة مرارا وتكرارا بتوافق الآراء.

وبدلا من ذلك، يسلط التقرير، ولا سيما في الفقرة 16 من الديباجة والفقرة 5، الضوء على مقترحات موضوعية مختارة تؤيدها مجموعة صغيرة من الدول، يخشى الاتحاد الأوروبي أن تعرقل النهج التدريجي القائم على توافق الآراء الذي تمكن الفريق العامل المفتوح باب العضوية من إحراز تقدم خلال السنوات الماضية.

ويرى الاتحاد الأوروبي ودوله الأعضاء أن تنفيذ إطار الأمم المتحدة للسلوك المسؤول للدول في استخدام تكنولوجيا المعلومات والاتصالات يكتسي أهمية قصوى في ضمان بيئة مفتوحة وآمنة ومستقرة ويمكن الوصول إليها وسلمية لتكنولوجيا المعلومات والاتصالات، ويساورنا القلق لأن نرى أن هذا القرار يعتمد على نص غير توافقي يمكن أن يؤدي إلى إعادة تفسير عمل الفريق العامل المفتوح باب العضوية والوثائق القائمة بتوافق الآراء.

ولا يزال الاتحاد الأوروبي ملتزما تماما بإيجاد أرضية مشتركة بشأن تعزيز توافق الآراء في الفريق العامل الحالي المفتوح باب العضوية، فضلا عن الجهود الجماعية لتصميم آلية شاملة ودائمة وعملية المنحى لإجراء حوار مؤسسي منتظم بعد اختتام أعمال الفريق العامل الحالي المفتوح باب العضوية.

في الطلبات المقدمة عملا بالفقرة 8 من القرار

أحرز تقدم كبير في مناقشة آلية مستقبلية بعد اختتام الفريق العامل المفتوح العضوية للفترة 2021–2025. تضمّن تقرير الأمين العام (A/78/76) الذي أذنت به الجمعية العامة في قرارها 37/77، ملاحظات واستنتاجات بشأن نطاق برنامج عمل للارتقاء بسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي، وهيكله ومضمونه والأعمال التحضيرية لإنشائه وطرائق ذلك الإنشاء. بالإضافة إلى ذلك، وافق الفريق العامل مفتوح العضوية 2021–2025 على عناصر مشتركة لآلية مستقبلية للحوار المؤسسي المنتظم في تقريره المرحلي السنوي لعام 2023. وأخيرا، اقترح رئيس الفريق العامل المفتوح العضوية للفترة 2021–2025 المزيد من العناصر المشتركة في ورقة مناقشة، استنادا إلى مقترحات الوفود والمناقشات التي دارت في الدورة الموضوعية السادسة للفريق العامل مفتوح العضوية.

ومع مراعاة التقدم المحرز في تحديد العناصر المشتركة لآلية في المستقبل، سيعرب الاتحاد الأوروبي كذلك عن آرائه بشأن آلية مستقبلية للحوار المؤسسي المنتظم.

وينبغي أن يظل النهوض بالأمن والاستقرار الدوليين في الفضاء الحاسوبي، وتعزيز فهم وتنفيذ إطار الأمم المتحدة للسلوك المسؤول للدول في الفضاء الحاسوبي، من أولويات الحوار المؤسسي المنتظم بشأن هذه المسائل تحت رعاية الأمم المتحدة.

واستجابة للدعوة إلى إقامة حوار مؤسسي دائم وشامل وشفاف، بمشاركة واسعة، تحت رعاية الأمم المتحدة، على النحو المبين في تقرير الفريق العامل المفتوح العضوية لعام 2021 المعني بالتطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي وتقرير فريق الخبراء الحكوميين، برنامج العمل، وهو مقترح بادرت به مجموعة من البلدان عبر الإقليمية[94]، يمثل فرصة لوضع هيكل دائم للحوار المؤسسي المنتظم على مستوى الأمم المتحدة، وبالتالي السماح للمجتمع الدولي بتركيز مناقشاته على الجوهر بدلا من إجراء مناقشات متكررة بشأن العمليات المقبلة. وفي هذا السياق، يمكن أن يصبح البرنامج الآلية المتطورة للتعاون في المستقبل داخل اللجنة الأولى للجمعية العامة.

وتحقيقا لهذه الغاية، ينبغي أن ينصب التركيز الجماعي على السعي إلى تحقيق توازن بين جانبين متساويين في الأهمية من عملنا – تنفيذ الإطار القائم للسلوك المسؤول للدول في استخدام تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي، ومواصلة تطوير الإطار. وينبع وضع الإطار، في جملة أمور، من الدروس المستفادة أثناء تنفيذ الالتزامات القائمة.

وينبغي أن تكون الآلية شاملة وعملية المنحى وأن توفر منبرا للمناقشات والتبادلات التفصيلية، وأن تيسر بناء القدرات وتسمح بمواصلة تطوير الإطار المعياري وتحديثه وفقا للتطورات الجارية في بيئة تكنولوجيا المعلومات والاتصالات على أساس توافق الآراء.

كما ينبغي أن يسمح بالمشاركة الرسمية لأصحاب المصلحة المعنيين، بما في ذلك القطاع الخاص والأوساط الأكاديمية والمجتمع المدني، وإجراء مشاورات منتظمة معهم، حتى يتمكنوا من النظر في وجهات نظرهم وخبراتهم الفريدة بشأن القضايا ذات الصلة وتقديمها. وسيزيد ذلك من تركيز الجهود على دعم الدول في تعزيز تنفيذ إطار السلوك المسؤول للدول وبناء القدرات القائمة على الاحتياجات لزيادة القدرة على الصمود الحاسوبي على الصعيدين الوطني والعالمي.

وينبغي أن يستند برنامج العمل إلى الإطار المعياري على النحو الوارد في تقارير فريق الخبراء الحكوميين المتعاقبة وتقارير توافق الآراء الصادرة عن الأفرقة العاملة المفتوحة العضوية والالتزامات والإجراءات الناتجة عنها. وينبغي للآلية المقبلة أن تعقد مؤتمرات استعراضية دورية كل عدة سنوات (كل ثلاث أو أربع سنوات مثلا) لاستعراض إطار سلوك الدول المسؤول، وتحديث الإطار حسب الاقتضاء، وتوفير التوجيه الاستراتيجي لعمل الآلية.

ويمكن لبرنامج العمل أن يعقد دورات رسمية سنوية، لجمع أعمال المناقشات المفصلة المفتوحة العضوية المزمع إجراؤها على مدار العام. ويمكن للدورات الرسمية السنوية أن تقرر إنشاء اجتماعات تقنية

(94) انظر https://documents.unoda.org/wp-content/uploads/2021/11/Working-paper-on-the-proposal-for-a-Cyber- PoA.pdf.

مفتوحة العضوية أو أفرقة عاملة أو مسارات عمل للتركيز على قضايا محددة ذات أولوية للمضي قدما من خلال البرنامج.

وينبغي أن تكون المشاركة في مسارات العمل التقنية طوعية ومفتوحة لجميع الدول. وينبغي تحديد مسار العمل، بما في ذلك مشاركة أصحاب المصلحة، وتواتر الاجتماعات في الاجتماعات السنوية أو المؤتمرات الاستعراضية. وينبغي أن توجه هذه الاجتماعات نحو وضع وثيقة ختامية تتضمن استنتاجات عملية تستند إلى الدروس المستفادة من تنفيذ إطار السلوك المسؤول للدول، في دورة من التحسين المستمر.

ويمكن لبرنامج العمل أيضا أن يعزز المشاركة الإقليمية من خلال التعاون مع المنظمات الإقليمية للاستفادة من المبادرات القائمة ذات الصلة والاستفادة من الهياكل والمناهج القائمة لبناء القدرات. وهذه الجهود الجماعية ستساعد البلدان على توضيح احتياجاتها من بناء القدرات والحصول عليها. ومع التشديد على المسؤولية الرئيسية للدول عن صون السلم والأمن الدوليين ودورها المركزي في برنامج العمل، ينبغي تعزيز التبادل والتعاون مع أصحاب المصلحة من خلال توفير مكان للمشاركة الشاملة والهادفة.

وفيما يتعلق بالأعمال التحضيرية ووضع برنامج العمل، ينبغي تنظيم اجتماعات فيما بين الدورات ودورات مخصصة للفريق العامل المفتوح العضوية في عامي 2024 و 2025 لمواصلة بلورة الجوانب المختلفة لبرنامج العمل، بما في ذلك الآثار المترتبة في الميزانية على الآلية الدائمة وتحديد الجهات الفاعلة ذات الصلة داخل الأمم المتحدة للاضطلاع بهذه المهام. وينبغي أن تنعكس نتائج هذه الدورات في التقارير المرحلية السنوية للفريق العامل المعني المفتوح العضوية. وينبغي أن يبدأ تنفيذ برنامج العمل عند اختتام أعمال هذا الفريق العامل المفتوح العضوية للفترة 2021-2025.