الأمم المتحدة

A/75/816

الجمعية العامة

Distr.: General
18 March 2021
Arabic
Original: English

الدورة الخامسة والسبعون

البند 98 من جدول الأعمال

التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي

التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي

مذكرة من الأمين العام

يتشرف الأمين العام بأن يحيل إلى أعضاء الجمعية العامة تقرير الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، عملا بقرار الجمعية العامة 27/73 ومقررها 550/75.

140421 050421 21-03673 (A)

تقرير الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي

أولا - مقدمة

1 - قرّرت الجمعية العامة، بموجب قرارها 27/73، أن يجتمع، ابتداء من عام 2019، فريقٌ عاملٌ مفتوح العضوية، يستند في عمله إلى توافق الآراء، ليُواصل، على سبيل الأولوية، صقل قواعد ومعايير ومبادئ السلوك المسؤول للدول وطرق تنفيذها؛ ويقوم عند اللزوم بإدخال تغييرات عليها أو وضع قواعد سلوك إضافية؛ ويدرس إمكانية إقامة حوار مؤسسي منتظم بمشاركة واسعة تحت رعاية الأمم المتحدة؛ ويُواصل، بغرض تعزيز الفهم المشترك، دراسةَ الأخطار القائمة والمحتملة في ميدان أمن المعلومات والتدابير التعاونية الممكن اتخاذها للتصدي لها، وكيفية انطباق القانون الدولي على استخدام الدول لتكنولوجيات المعلومات والاتصالات، وتدابير بناء الثقة وبناء القدرات، وُقدم تقريرا عن نتائج هذه الدراسة إلى الجمعية في دورتها الخامسة والسبعين، ويُتيح إمكانية عقد اجتماعات تشاورية فيما بين الدورات، في حدود التبرعات، مع الأطراف المهتمة ممثلةً في قطاع الأعمال والمنظمات غير الحكومية والأوساط الأكاديمية، لتبادل الآراء بشأن المسائل التي تدخل في نطاق ولاية الفريق. وقرّرت الجمعية أيضا أن يعقد الفريق دورته التنظيمية في حزيران/يونيه 2019 من أجل الاتفاق على ترتيباته التنظيمية.

2 - وقرّرت الجمعية العامة، في مقررها 550/75، وبعد إشارتها إلى إلغاء الدورة الموضوعية الثالثة والأخيرة التي كان مقررا عقدها في الفترة من 6 إلى 10 تموز/يوليه 2020، وذلك بسبب جائحة مرض فيروس كورونا (كوفيد-19)، أن يعقد الفريق العامل المفتوح العضوية دورته الموضوعية الثالثة والأخيرة في الفترة من 8 إلى 12 آذار/مارس 2021، بينما يواصل عمله وفق الولاية المنوطة به بموجب قرار الجمعية 27/73.

ثانيا - مسائل تنظيمية

ألف - افتتاح الدورات ومددها

3 - عقد الفريق العامل دورته التنظيمية في 3 حزيران/يونيه 2019، وعقد دورته الموضوعية الأولى في الفترة من 9 إلى 13 أيلول/سبتمبر 2019، ودورته الموضوعية الثانية في الفترة من 10 إلى 14 شباط/فبراير 2020، ودورته الموضوعية الثالثة في الفترة من 8 إلى 12 آذار/مارس 2021، وعقدت جميع هذه الدورات في المقر.

4 - وقدّم مكتب شؤون نزع السلاح ومعهد الأمم المتحدة لبحوث نزع السلاح الدعمَ الفني للفريق العامل. وقدّمت إدارة شؤون الجمعية العامة والمؤتمرات خدمات الأمانة.

باء - الحضور

5 - ترد أسماء المشاركين في الدورات الموضوعية في الوثائق A/AC.290/2019/INF/1 و A/AC.290/2020/INF/1 و A/AC.290/2021/INF/1.

جيم - أعضاء المكتب

6 - انتخب الفريق العامل، في دورته التنظيمية، المنعقدة في 3 حزيران/يونيه 2019، يويرغ لاوبر (سويسرا) رئيسا بالتزكية.

دال - إقرار جدول الأعمال

7 - أقرّ الفريق العامل، في الدورة نفسها، جدولَ الأعمال لجميع دوراته بصيغته الواردة في الوثيقة A/AC.290/2019/1. وفيما يلي نص جدول الأعمال:

1 - انتخاب أعضاء المكتب.

2 - إقرار جدول الأعمال.

3 - تنظيم الأعمال.

4 - تبادل عام للآراء.

5 - مناقشات بشأن المسائل الموضوعية الواردة في الفقرة 5 من قرار الجمعية العامة 27/73:

(أ) مواصلة صقل قواعد ومعايير ومبادئ السلوك المسؤول للدول المدرجة في الفقرة 1 من قرار الجمعية العامة 27/73، وطرق تنفيذها؛ وإدخال تغييرات عليها أو وضع قواعد سلوك إضافية، عند اللزوم؛

(ب) دراسة إمكانية إقامة حوار مؤسسي منتظم بمشاركة واسعة تحت رعاية الأمم المتحدة؛

(ج) مواصلة دراسة الأخطار القائمة والمحتملة في ميدان أمن المعلومات والتدابير التعاونية الممكن اتخاذها للتصدي لها، بغرض تعزيز الفهم المشترك؛

(د) كيفية انطباق القانون الدولي على استخدام الدول لتكنولوجيات المعلومات والاتصالات؛

(هـ) تدابير بناء الثقة؛

(و) بناءُ القدراتِ والمفاهيم المشار إليها في الفقرة 3 من قرار الجمعية العامة 27/73.

6 - مسائل أخرى.

7 - اعتماد التقرير النهائي.

8 - وقرّر الفريق العامل أيضا في الدورة نفسها أن يقوم بعمله وفقا للنظام الداخلي للجان الرئيسية التابعة للجمعية العامة، وأن يستند فيه إلى توافق الآراء وفقا لقرار الجمعية العامة 27/73. وقرّر الفريق كذلك أن لجميع الدول الأعضاء الحقّ في أن تكون ممثّلة في الفريق تمشياً مع النظام الداخلي والممارسات المعمول بها في الجمعية. وظلّت الدعوة مفتوحة على الدوام أمام الدول غير الأعضاء، والمنظمات الحكومية الدولية، والكيانات التي منحتها الجمعية العامة مركز المراقب، لتُشارك في دورات الفريق وعمله بصفة

مراقب. وتقرّر أن تُدعى الكيانات المعنية في منظومة الأمم المتحدة إلى المشاركة أيضا لأغراض المعلومات التقنية فحسب. وتقرّر أيضا أن تُبلغ المنظمات غير الحكومية المعنية ذات المركز الاستشاري لدى المجلس الاقتصادي والاجتماعي وفقا للقرار 31/1996 أمانةَ الفريق برغبتها في المشاركة في عمله. وتقرّر أيضا أن تقوم المنظمات غير الحكومية الأخرى المهتمة، في حال كانت معنية وكان اختصاصها يندرج ضمن نطاق ولاية الفريق والغرض منه، بإبلاغ أمانة الفريق برغبتها في المشاركة، ثم تُدعى، بناء على ذلك وإذا لم يُعترض عليها، إلى المشاركة بصفة مراقب.

هاء - تنظيم الأعمال

9 - في الجلسة الأولى من كل دورة من الدورات الموضوعية، أي الجلسات المعقودة في 9 أيلول/سبتمبر 2019 و 10 شباط/فبراير 2020 و 8 آذار/مارس 2021 على التوالي، اتّفق الفريق العامل على تنظيم أعماله بالشكل الوارد في الوثائق A/AC.290/2019/2 و A/AC.290/2020/1 و A/AC.290/2021/1.

واو - الوثائق

10 - يمكن الاطلاع على قائمة كاملة لجميع الوثائق وورقات العمل والورقات التقنية الرسمية وغيرها من الوثائق المعروضة على الفريق العامل على الموقع الشبكي التالي المخصص لهذا الغرض: www.un.org/disarmament/open-ended-working-group/.

زاي - أعمال الفريق العامل

11 - نظر الفريق العامل، في دورته الموضوعية الأولى، في بنود جدول الأعمال من 3 إلى 5 في جلساته العامة التسع.

12 - وواصل الفريق العامل، في دورته الموضوعية الثانية، النظر في البند 5 من جدول الأعمال في جلساته العامة التسع.

13 - ونظر الفريق العامل، في دورته الموضوعية الثالثة، في بنود جدول الأعمال من 5 إلى 7.

14 - وليُواصل الفريق العامل عملَه خلال جائحة مرض فيروس كورونا (كوفيد-19)، عقَد جلسات افتراضية غير رسمية في 15 و 17 و 19 حزيران/يونيه و 2 تموز/يوليه 2020؛ وفي الفترة من 29 أيلول/سبتمبر إلى 1 تشرين الأول/أكتوبر 2020؛ وفي الفترة من 17 إلى 19 تشرين الثاني/نوفمبر 2020؛ وفي الفترة من 1 إلى 3 كانون الأول/ديسمبر 2020؛ وفي 18 و 19 و 22 شباط/فبراير 2021.

15 - وعقد الفريق العامل اجتماعا تشاوريا غير رسمي بين الدورات لأصحاب المصلحة المتعددين في الفترة من 2 إلى 4 كانون الأول/ديسمبر 2019. وبناء على طلب رئيس الفريق، تولّى رئاسة الاجتماع الرئيسُ التنفيذي لوكالة الأمن السيبراني في سنغافورة، ديفيد كوه، وقد عُرض ملخّص مداولات الاجتماع الذي أعدّه على أعضاء الفريق وعُمّم عليهم[1].

(1) مُتاح على الرابط التالي: www.un.org/disarmament/open-ended-working-group/.

ثالثا - اعتماد التقرير

16 - نظر الفريق العامل في دورته الموضوعية الثالثة التي عقدت في 12 آذار/مارس 2021، في البند 7 من جدول الأعمال المعنون "اعتماد التقرير"، واعتمد تقريره بصيغته الواردة في الوثيقة A/AC.290/2021/L.1 بصيغتها المنقحة شفوياً والوثيقة A/AC.290/2021/CRP.2.

17 - وبالنظر إلى قيود كوفيد-19 المعمول بها في مقر الأمم المتحدة التي حدت من عدد جلسات الفريق العامل في دورته الموضوعية الثالثة، ستصدر خلاصة للبيانات التي تقدم تفسيرا للمواقف بوصفها الوثيقة A/AC.290/2021/INF.2.

المرفق الأول*

التقرير الموضوعي النهائي

ألف - مقدمة

1 - على الرغم من التحولات الجذرية التي شهدها العالم منذ تأسيس الأمم المتحدة قبل 75 عاما، فإن مقاصدها ومثلها الخالدة لا تزال ذات أهمية أساسية .فإلى جانب إعادة تأكيد الدول إيمانها بحقوق الإنسان الأساسية، والتزامها بتعزيز تقدم شعوب العالم قاطبة في المجالين الاقتصادي والاجتماعي وإرساء الظروف اللازمة للعدالة واحترام القانون الدولي، فقد عقدت العزم على ضم قواها لصون السلم والأمن الدوليين[2].

2 - وتترتب على التطورات في تكنولوجيا المعلومات والاتصالات آثار على جميع الركائز الثلاث لعمل الأمم المتحدة: السلام والأمن، وحقوق الإنسان، والتنمية المستدامة. وظلت تكنولوجيا المعلومات والاتصالات وإمكانية الاتصال الإلكتروني على الصعيد العالمي تشكلان حافزين لتقدم البشرية وتنميتها، مما أحدث تحولات في المجتمعات والاقتصادات، ووسع فرص التعاون.

3 - وتتضح أكثر من أي وقت مضى ضرورة بناء وصون السلام والأمن والثقة على الصعيد الدولي في بيئة تكنولوجيا المعلومات والاتصالات. إذ يمكن للاتجاهات السلبية في المجال الرقمي أن تقوض الأمن والاستقرار الدوليين، وتمارس ضغوطا على النمو الاقتصادي والتنمية المستدامة، وتعوق التمتع الكامل بحقوق الإنسان والحريات الأساسية. وتشمل هذه الاتجاهات تزايد استغلال تكنولوجيا المعلومات والاتصالات لأغراض خبيثة.

4 - وقد أبرزت الأزمة الصحية العالمية الراهنة الفوائد الأساسية لتكنولوجيا المعلومات والاتصالات واعتمادنا عليها، بما في ذلك في مجال توفير الخدمات الحكومية الحيوية، وإيصال رسائل السلامة العامة الأساسية، ووضع حلول مبتكرة لضمان استمرارية الأعمال، وتسريع البحوث، والمساعدة على ضمان مواصلة التعليم والتماسك الاجتماعي من خلال الوسائل الافتراضية. وفي هذا الوقت الذي يكتنفه عدم اليقين، سخرت الدول، إلى جانب القطاع الخاص والعلماء وغيرهم من الجهات الفاعلة، التكنولوجيا الرقمية لأجل التواصل المستمر بين الأفراد والمجتمعات والحفاظ على صحتهم. وفي الوقت نفسه، أظهرت جائحة كوفيد-19 مخاطر وعواقب الأنشطة الخبيثة التي تسعى إلى استغلال مواطن الضعف في الأوقات التي تتعرض فيها المجتمعات لضغوط هائلة. وسلطت الضوء أيضا على ضرورة سد الفجوات الرقمية، وبناء القدرة على الصمود في كل مجتمع وقطاع، والحفاظ على نهج يركز على الإنسان.

5 - وبما أنه يمكن استخدام تكنولوجيا المعلومات والاتصالات في أغراض لا تتفق مع أهداف صون السلام والاستقرار والأمن على الصعيد الدولي، فقد أقرت الجمعية العامة[3] بأن نشر واستخدام تكنولوجيا

---

* يصدر دون تحرير رسمي.

(2) ديباجة ميثاق الأمم المتحدة.

(3) انظر على سبيل المثال A/RES/53/70، الفقرة 6 من الديباجة.

المعلومات والاتصالات يؤثران في مصالح المجتمع الدولي بأكمله، وأن التعاون الدولي الواسع النطاق سيؤدي إلى الفعالية المثلى في الاستجابة.

6 - وفي ضوء ما تقدم، فإن الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي (الفريق العامل)، المنشأ عملا بقرار الجمعية العامة 27/73، يشكل فرصة للمضي قدما في النظر في هذه المسألة البالغة الأهمية. وهو يوفر منبرا ديمقراطيا وشفافا وشاملا لجميع الدول للمشاركة والتعبير عن آرائها وتوسيع نطاق التعاون بشأن البعد الأمني الدولي لتكنولوجيا المعلومات والاتصالات. وتدل المشاركة النشطة من جانب أعضاء الأمم المتحدة وإشراك مجموعة متنوعة من أصحاب المصلحة ذوي الصلة الآخرين على تطلع المجتمع الدولي المشترك إلى تهيئة بيئة لتكنولوجيا المعلومات والاتصالات تكون سلمية ومأمونة للجميع، واهتمامه الجماعي بذلك، وعزمه على التعاون لتحقيق ذلك.

7 - ويمثل الفريق العامل معلما هاما من معالم التعاون الدولي في سبيل تهيئة بيئة لتكنولوجيا المعلومات والاتصالات تكون مفتوحة ومأمونة ومستقرة وميسَّرة وسلمية. وقد أنشئت في ست مناسبات منذ عام 2003 أفرقة خبراء حكوميين لدراسة التهديدات القائمة والمحتملة في ميدان أمن المعلومات والتدابير التعاونية الممكن اتخاذها للتصدي لها[4]. وأوصت هذه الأفرقة، من خلال تقاريرها الثلاثة الصادرة بتوافق الآراء (2010 و 2013 و 2015[5])، والتي تتسم بطابع تراكمي، بوضع 11 معيارا من المعايير الطوعية وغير الملزمة للسلوك المسؤول للدول وأقرت بأنه يمكن وضع معايير إضافية مع مرور الوقت. وعلاوة على ذلك، أوصي باتخاذ تدابير محددة لبناء الثقة وبناء القدرات والتعاون. وأكدت أيضا من جديد أن القانون الدولي، ولا سيما ميثاق الأمم المتحدة، ينطبق على صون السلام والأمن والاستقرار في بيئة تكنولوجيا المعلومات والاتصالات، وهو يضطلع بدور أساسي في هذا الصدد. وفي قرار الجمعية العامة 237/70، اتفقت الدول الأعضاء بتوافق الآراء على أن تسترشد في استخدامها لتكنولوجيا المعلومات والاتصالات بتقرير عام 2015 الصادر عن فريق الخبراء الحكوميين، مما يعزز إطارا أوليا لسلوك الدول المسؤول في استخدام تكنولوجيا المعلومات والاتصالات. وفي هذا الصدد، أشار الفريق العامل أيضاً إلى قراري الجمعية العامة 27/73 و 266/73.

8 - وبناء على هذا الأساس وتأكيدا لهذا الإطار من جديد، سعى الفريق العامل إلى إيجاد أرضية مشتركة وتفاهم متبادل بين جميع الدول الأعضاء في الأمم المتحدة بشأن موضوع له عواقب عالمية. وناقش الفريق العامل، وفقا لولايته، التهديدات القائمة والمحتملة في ميدان أمن المعلومات والتدابير التعاونية الممكن اتخاذها للتصدي لها؛ ومواصلة صقل قواعد ومعايير ومبادئ السلوك المسؤول للدول؛ وكيفية انطباق القانون الدولي على استخدام الدول لتكنولوجيا المعلومات والاتصالات؛ وتدابير بناء الثقة؛ وبناء القدرات؛ وإمكانية إقامة حوار مؤسسي منتظم بمشاركة واسعة تحت رعاية الأمم المتحدة. واسترشدت مناقشات الفريق العامل بمبادئ الشمولية والشفافية في إطار الجهود التي يبذلها هذا الفريق لبناء توافق الآراء وتعزيز السلام والأمن والتعاون والثقة على الصعيد الدولي.

(4) A/RES/58/32، و A/RES/60/45، و A/RES/66/24، و A/RES/68/243، و A/RES/70/237، و A/RES/73/266.

(5) A/65/201 و A/68/98 و A/70/174.

9 - وينبغي للأمم المتحدة أن تواصل القيام بدور رائد في تعزيز الحوار بشأن استخدام الدول لتكنولوجيا المعلومات والاتصالات. ويسلم الفريق العامل بأهمية وتكامل المناقشات المتخصصة بشأن جوانب التكنولوجيات الرقمية التي تتناولها هيئات ومنتديات الأمم المتحدة الأخرى.

10 - وبينما تتحمل الدول المسؤولية الأولى عن صون السلام والأمن الدوليين، فإن مسؤولية استخدام تكنولوجيا المعلومات والاتصالات بطريقة لا تعرض السلام والأمن للخطر تقع على عاتق جميع الجهات صاحبة المصلحة. وبما أن بعد الأمن الدولي لتكنولوجيا المعلومات والاتصالات يشمل مجالات وتخصصات متعددة، فقد استفاد الفريق العامل من الخبرات والمعارف والتجارب التي أتاحها ممثلون عن المنظمات الحكومية الدولية والمنظمات الإقليمية والمجتمع المدني والقطاع الخاص والأوساط الأكاديمية والأوساط التقنية. وأسفر الاجتماع التشاوري غير الرسمي للفريق العامل الذي عقد في كانون الأول/ديسمبر 2019 على مدى ثلاثة أيام، عن مناقشة ثرية بين الدول ومجموعة واسعة من الجهات الأخرى صاحبة المصلحة[6]. وبالإضافة إلى ذلك، قدمت هذه الجهات مقترحات ملموسة وأمثلة للممارسات الجيدة عن طريق مساهمات خطية وتبادلات غير رسمية مع الفريق العامل. وأجرت بعض الوفود أيضا، بمبادرة منها، مشاورات بين الجهات المتعددة صاحبة المصلحة لتسترشد بها في مساهماتها في الفريق العامل.

11 - ويقر الفريق العامل، إدراكا منه لاختلاف حالات الدول والمناطق وقدراتها وأولوياتها، بأن فوائد التكنولوجيا الرقمية ليست موزعة بالتساوي وأن تضييق الفجوات الرقمية، بسبل منها تعميم الوصول إلى تكنولوجيا المعلومات والاتصالات وإمكانية الاتصال الإلكتروني بصورة شاملة للجميع وغير تمييزية، يظل أولوية ملحة لدى المجتمع الدولي.

12 - ويرحب الفريق العامل بالمستوى الرفيع لمشاركة المندوبات في دوراته وبصدارة المنظورات الجنسانية في مناقشاته. ويشدد الفريق العامل على أهمية تضييق "الفجوة الرقمية بين الجنسين" وتعزيز مشاركة المرأة مشاركة فعالة ومؤثرة وتوليها أدوارا قيادية في عمليات صنع القرار المتعلقة باستخدام تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي.

13 - ويشدد الفريق العامل على أن العناصر الفردية التي تشكل ولايته مترابطة ويعزز بعضها بعضا، وتنهض معا ببيئة مفتوحة ومأمونة ومستقرة وميسَّرة وسلمية لتكنولوجيا المعلومات والاتصالات.

باء - استنتاجات وتوصيات

14 - إن الدول، وقد نظرت في الجوانب الموضوعية لولاية الفريق العامل، وإذ تشير إلى أن قرار الجمعية العامة 27/73 رحب بالعمل الفعال الذي قام به في الأعوام 2010 و 2013 و 2015 فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي والتقارير الختامية ذات الصلة التي أحالها الأمين العام[7]، توصلت إلى الاستنتاجات والتوصيات التالية التي

(6) انظر "موجز الرئيس للاجتماع التشاوري غير الرسمي الذي عقده بين الدورات الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي" المتاح على الرابط التالي: https://www.un.org/disarmament/open-ended-working-group/.

(7) A/65/201 و A/68/98 و A/70/174.

تشمل إجراءات ملموسة وتدابير تعاونية للتصدي للتهديدات في مجال تكنولوجيا المعلومات والاتصالات، والنهوض ببيئة لتكنولوجيا المعلومات والاتصالات تكون مفتوحة ومأمونة ومستقرة وميسَّرة وسلمية.

التهديدات القائمة والمحتملة

15 - خلصت الدول إلى أنها تشعر بقلق متزايد إزاء آثار الاستخدام الخبيث لتكنولوجيا المعلومات والاتصالات على صون السلام والأمن الدوليين، وبالتالي على حقوق الإنسان والتنمية. وأُعرب عن القلق بوجه خاص إزاء تطوير قدرات تكنولوجيا المعلومات والاتصالات لأغراض تقوض السلام والأمن الدوليين. فحوادث تكنولوجيا المعلومات والاتصالات الضارة تزداد من حيث التواتر والتعقيد، وهي تتطور وتتنوع باستمرار. ويمكن أن تؤدي زيادة الاتصال الإلكتروني والاعتماد على تكنولوجيا المعلومات والاتصالات بدون تدابير مصاحبة تكفل أمن هذه التكنولوجيا إلى مخاطر غير متوقعة، مما يجعل المجتمعات أكثر عرضة لأنشطة تكنولوجيا المعلومات والاتصالات الخبيثة. وعلى الرغم من أن تكنولوجيا المعلومات والاتصالات تعود بفوائد لا تقدر بثمن على البشرية، فإن استخدامها الخبيث يمكن أن تكون له آثار سلبية كبيرة وبعيدة المدى.

16 - وأشارت الدول إلى أن عدداً من الدول يطور قدرات في مجال تكنولوجيا المعلومات والاتصالات للأغراض العسكرية. وأشارت أيضاً إلى أن استخدام تكنولوجيا المعلومات والاتصالات في النزاعات بين الدول في المستقبل أصبح أكثر احتمالاً. فاستمرار تزايد الحوادث التي تنطوي على استخدام خبيث لتكنولوجيا المعلومات والاتصالات من جانب جهات من الدول ومن غير الدول، بما في ذلك الإرهابيون والجماعات الإجرامية، هو اتجاه مثير للقلق. وقد أثبتت بعض الجهات من غير الدول أنها تملك قدرات في مجال تكنولوجيا المعلومات والاتصالات كانت متاحة في السابق للدول فقط.

17 - وخلصت الدول أيضاً إلى أن أي استخدام لتكنولوجيا المعلومات والاتصالات من جانب الدول بطريقة لا تتفق مع التزاماتها بموجب الإطار الذي يشمل القواعد الطوعية والقانون الدولي وتدابير بناء الثقة، هو استخدام يقوض السلام والأمن الدوليين، والثقة والاستقرار بين الدول، وقد يزيد من احتمال نشوب نزاعات بين الدول في المستقبل.

18 - وخلصت الدول إلى أن هناك عواقب أمنية واقتصادية واجتماعية وإنسانية مدمرة محتملة لأنشطة تكنولوجيا المعلومات والاتصالات الخبيثة على البنية التحتية الحيوية والبنية التحتية الحيوية للمعلومات التي تدعم تقديم الخدمات الأساسية للجمهور. وفي حين أن من حق كل دولة أن تحدد البنية التحتية التي تعتبرها حيوية، فإن هذه البنية التحتية قد تشمل المرافق الطبية، والخدمات المالية، والطاقة، والمياه، والنقل، والمرافق الصحية. ثم إن أنشطة تكنولوجيا المعلومات والاتصالات الخبيثة الموجهة ضد البنية التحتية الحيوية والبنية التحتية الحيوية للمعلومات، التي تقوض الثقة في العمليات السياسية والانتخابية والمؤسسات العامة، أو التي تؤثر في توافر الإنترنت وسلامتها بوجه عام، هي أنشطة تشكل أيضا مصدر قلق حقيقي ومتزايد. ويمكن أن تكون هذه البنية التحتية مملوكة للقطاع الخاص أو تحت إدارته أو تشغيله، أو متقاسمة مع دولة أخرى أو مربوطة بها شبكيا، أو تعمل عبر دول مختلفة. ونتيجة لذلك، قد يكون التعاون بين الدول أو بين القطاعين العام والخاص ضروريا لحماية سلامتها وأدائها وتوافرها.

19 - وخلصت الدول أيضاً إلى أن نشاط تكنولوجيا المعلومات والاتصالات الذي يتعارض مع الالتزامات بموجب القانون الدولي، والذي يلحق الضرر عمداً بالبنية التحتية الحيوية أو يضر بطريقة أخرى باستخدام

وتشغيل البنية التحتية الحيوية لتقديم الخدمات إلى الجمهور، قد لا يشكل تهديداً للأمن فحسب وإنما أيضاً لسيادة الدولة، وكذلك للتنمية الاقتصادية وسبل العيش، وفي نهاية المطاف لسلامة الأفراد ورفاههم.

20 - وبما أن جميع الدول تعتمد بشكل متزايد على التكنولوجيات الرقمية، فقد خلصت الدول إلى أن الافتقار إلى الوعي والقدرات الكافية للكشف عن أنشطة تكنولوجيا المعلومات والاتصالات الخبيثة أو الحماية منها أو التصدي لها قد يجعلها أكثر ضعفا .وكما شهدنا خلال حالة الطوارئ الصحية العالمية الراهنة، يمكن أن تتضخم أوجه الضعف القائمة في أوقات الأزمات.

21 - وخلصت الدول إلى أن التهديدات قد يكون وقعها على الدول مختلفا وفقا لمستويات الرقمنة فيها، وقدراتها، وأمنها وقدرتها على الصمود في مجال تكنولوجيا المعلومات والاتصالات، وبنيتها التحتية، وتنميتها. وقد يكون للتهديدات أيضا أثر مختلف باختلاف الفئات والكيانات، بما في ذلك على الشباب والمسنين والنساء والرجال، وعلى الفئات الضعيفة من السكان، وعلى أصحاب مهن خاصة، والمؤسسات الصغيرة والمتوسطة، وغيرها.

22 - وفي ضوء مشهد التهديدات الرقمية المثير لقدر متزايد من القلق، وتسليما بأنه لا توجد أي دولة بمنأى عن هذه التهديدات، شددت الدول على الحاجة الملحة إلى تنفيذ ومواصلة وضع تدابير تعاونية للتصدي لهذه التهديدات. وجرى التأكيد على أن العمل معا وعلى نحو شامل كلما أمكن من شأنه أن يؤدي إلى تحقيق نتائج أكثر فعالية وبعيدة المدى. وجرى التشديد أيضا في هذا الصدد على أهمية مواصلة توثيق التعاون، عند الاقتضاء، مع المجتمع المدني والقطاع الخاص والأوساط الأكاديمية والأوساط التقنية.

23 - وشددت الدول على الفرص الاقتصادية والاجتماعية الإيجابية التي يمكن أن تُستمد من تكنولوجيا المعلومات والاتصالات، وخلصت إلى أن إساءة استخدام هذه التكنولوجيات، وليس التكنولوجيات ذاتها، هي التي تثير القلق.

قواعد ومعايير ومبادئ السلوك المسؤول للدول

24 - يمكن أن تحد المعايير الطوعية وغير الملزمة للسلوك المسؤول للدول من المخاطر التي تهدد السلام والأمن والاستقرار على الصعيد الدولي وأن تؤدي دورا هاما في زيادة القدرة على التنبؤ والحد من مخاطر التصورات الخاطئة، مما يسهم في منع نشوب النزاعات. وشددت الدول على أن هذه المعايير تعكس توقعات ومقاييس المجتمع الدولي فيما يتعلق بسلوك الدول في استخدامها لتكنولوجيا المعلومات والاتصالات، وتتيح للمجتمع الدولي تقييم أنشطة الدول. ووفقا لقرار الجمعية العامة 237/70، واعترافا بقرار الجمعية العامة 27/73، أُهيب بالدول أن تتجنب استخدام تكنولوجيا المعلومات والاتصالات بما لا يتماشى مع معايير السلوك المسؤول للدول وأن تمتنع عن القيام بذلك.

25 - وأكدت الدول من جديد أن المعايير لا تحل محل التزامات أو حقوق الدول بموجب القانون الدولي أو تغيرها، علما أنها التزامات وحقوق ملزمة، بل توفر إرشادات محددة إضافية بشأن ما يشكل سلوكا مسؤولا من جانب الدول في استخدام تكنولوجيا المعلومات والاتصالات. فالمعايير لا تسعى إلى الحد من العمل الذي يتسق مع القانون الدولي أو حظره.

26 - وفي حين اتفقت الدول على ضرورة حماية جميع البنى التحتية الحيوية والبنى التحتية الحيوية للمعلومات التي تدعم تقديم الخدمات الأساسية للجمهور، إلى جانب السعي إلى كفالة توافر الإنترنت

وسلامتها بوجه عام، خلصت كذلك إلى أن جائحة كوفيد-19 قد أبرزت أهمية حماية البنية التحتية للرعاية الصحية بما في ذلك الخدمات والمرافق الطبية من خلال تنفيذ المعايير التي تعالج مسألة البنية التحتية الحيوية، من قبيل المعايير التي أكدها قرار الجمعية العامة للأمم المتحدة 237/70 بتوافق الآراء.

27 - وأكدت الدول أهمية مساندة وتعزيز الجهود الرامية إلى تنفيذ المعايير التي تعهدت الدول بالاسترشاد بها على الصعد العالمي والإقليمي والوطني.

28 - وينبغي للدول، إذ تؤكد من جديد قرار الجمعية العامة 237/70 وتعترف بقرار الجمعية العامة 27/73، أن تقوم بما يلي: أن تتخذ خطوات معقولة لضمان سلامة سلسلة الإمداد، بسبل منها وضع تدابير تعاونية موضوعية حتى يتسنى للمستخدمين النهائيين الوثوق بأمن منتجات تكنولوجيا المعلومات والاتصالات؛ وأن تسعى إلى منع انتشار أدوات وتقنيات تكنولوجيا المعلومات والاتصالات الخبيثة واستخدام الوظائف الخفية الضارة؛ وأن تشجع على الإبلاغ المسؤول عن مواطن الضعف.

29 - وبالنظر إلى الخصائص الفريدة لتكنولوجيا المعلومات والاتصالات، أكدت الدول من جديد أنه يمكن، مع مراعاة المقترحات المقدمة بشأن المعايير في إطار الفريق العامل، مواصلة وضع معايير إضافية مع مرور الوقت. وخلصت الدول أيضا إلى أن مواصلة وضع المعايير وتنفيذ المعايير القائمة لا يستبعد أحدهما الآخر، بل يمكن أن يجريا بالتوازي.

ويوصي الفريق العامل بما يلي:

30 - أن تُجري الدول، على أساس طوعي، مسحا لجهودها الوطنية الرامية إلى تنفيذ المعايير، وأن تطور الخبرات والممارسات الجيدة في مجال تنفيذ المعايير وأن تتبادلها، وأن تواصل إبلاغ الأمين العام بآرائها وتقييماتها الوطنية في هذا الصدد.

31 - وينبغي للدول ألا تقوم بأنشطة في مجال تكنولوجيا المعلومات والاتصالات تتعارض مع التزاماتها بموجب القانون الدولي وتضر عن قصد بالبنية التحتية الحيوية أو تعطل، بأي شكل آخر، استخدام وتشغيل البنية التحتية الحيوية المستخدمة في تقديم الخدمات إلى الجمهور، وألا تدعم تلك الأنشطة عن عِلم. وعلاوة على ذلك، ينبغي أن تواصل الدول تعزيز التدابير الرامية إلى حماية جميع البنى التحتية الحيوية من التهديدات المتصلة بتكنولوجيا المعلومات والاتصالات، وأن تكثف تبادل الآراء بشأن أفضل الممارسات فيما يتعلق بحماية البنية التحتية الحيوية.

32 - وأن تواصل الدول دعمها لكي تنفذ وتضع جميع الدول معايير السلوك المسؤول للدول، وذلك في شراكة مع المنظمات المعنية، بما فيها الأمم المتحدة. وأن تُشجَّع الدول التي هي في وضع يسمح لها بالمساهمة بالخبرات أو الموارد على القيام بذلك.

33 - وأن تحيط الدول علما، مع الإشارة إلى قرار الجمعية العامة 237/70 والاعتراف بقرار الجمعية العامة 27/73، بالمقترحات التي قدمتها الدول بشأن وضع قواعد ومعايير ومبادئ السلوك المسؤول للدول في المناقشات المقبلة المتعلقة بتكنولوجيا المعلومات والاتصالات داخل الأمم المتحدة، مع الإشارة إلى أن القرار 240/75 قد أنشأ فريقا عاملا مفتوح العضوية معنيا بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025.

القانون الدولي

34 - أكدت الدول من جديد، مع التسليم بقرار الجمعية العامة 237/70 والاعتراف أيضا بقرار الجمعية العامة 27/73 الذي أنشأ الفريق العامل، أن القانون الدولي، وبخاصة ميثاق الأمم المتحدة، ينطبق على صون السلام والاستقرار والنهوض ببيئة لتكنولوجيات المعلومات والاتصالات تكون مفتوحة ومأمونة ومستقرة وميسَّرة وسلمية، وهو يضطلع بدور أساسي في هذا الصدد. وفي هذا الصدد، أُهيب بالدول تجنب اتخاذ أي تدابير لا تتفق مع القانون الدولي، ولا سيما ميثاق الأمم المتحدة، والامتناع عن ذلك. وخلصت الدول أيضا إلى ضرورة بلورة المزيد من أوجه الفهم المشترك بشأن كيفية انطباق القانون الدولي على استخدام الدول لتكنولوجيا المعلومات والاتصالات.

35 - وأكدت الدول أيضا من جديد أنه ينبغي للدول أن تسعى إلى تسوية المنازعات بالوسائل السلمية مثل التفاوض، وإجراء التحقيقات، والوساطة، والتوفيق، والتحكيم، والتسوية القضائية، واللجوء إلى الوكالات أو التنظيمات الإقليمية، أو غيرها من الوسائل السلمية التي تختارها بنفسها.

36 - وخلصت الدول إلى أنه يمكن، بالنظر لما لبيئة تكنولوجيا المعلومات والاتصالات من سمات فريدة، تعزيز الفهم المشترك المعمّق بشأن كيفية انطباق القانون الدولي على استخدام الدول لتكنولوجيا المعلومات والاتصالات عن طريق التشجيع على تبادل الآراء بشأن هذه المسألة فيما بين الدول، وعن طريق تحديد مواضيع معينة في القانون الدولي لإجراء المزيد من المناقشات المتعمقة بشأنها في الأمم المتحدة.

37 - ولكي تُعمّق جميع الدول فهمها لكيفية انطباق القانون الدولي على استخدام الدول لتكنولوجيا المعلومات والاتصالات، وللإسهام في بناء توافق في الآراء والفهم المشترك داخل المجتمع الدولي، خلصت الدول إلى أن الحاجة تقتضي بذل جهود إضافية محايدة وموضوعية لبناء القدرات في مجالات القانون الدولي والتشريعات الوطنية والسياسات.

ويوصي الفريق العامل بما يلي:

38 - أن تواصل الدول، على أساس طوعي، إبلاغ الأمين العام بآرائها وتقييماتها الوطنية بشأن كيفية انطباق القانون الدولي على استخدامها لتكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي، وأن تواصل تبادل الآراء والممارسات الوطنية طواعية من خلال طرق أخرى حسب الاقتضاء.

39 - وأن تواصل الدول التي بوسعها أن تدعم، بطريقة محايدة وموضوعية، بذل جهود إضافية لبناء القدرات، وفقا للمبادئ الواردة في الفقرة 56 من هذا التقرير، في مجالات القانون الدولي والتشريعات الوطنية والسياسات، القيام بذلك، لكي تسهم جميع الدول في بناء فهم مشترك لكيفية انطباق القانون الدولي على استخدام الدول لتكنولوجيا المعلومات والاتصالات، وتسهم في بناء توافق في الآراء داخل المجتمع الدولي.

40 - وأن تواصل الدول دراسة كيفية انطباق القانون الدولي على استخدام الدول لتكنولوجيا المعلومات والاتصالات، والاضطلاع بمناقشات بشأنها في إطار عمليات الأمم المتحدة المقبلة، كخطوة رئيسية لتوضيح الفهم المشترك بشأن هذه المسألة ومواصلة تعزيزه.

تدابير بناء الثقة

41 - يمكن لتدابير بناء الثقة، التي تشمل تدابير الشفافية والتعاون والاستقرار، أن تسهم في منع نشوب النزاعات، وتجنب التصورات الخاطئة وحالات سوء الفهم، والحد من التوترات. وهي تعبير ملموس عن التعاون الدولي. ويمكن لتدابير بناء الثقة، من خلال ما يلزم من موارد وقدرات ومشاركة، أن تعزز أمن تكنولوجيا المعلومات والاتصالات وقدرتها على الصمود واستخدامها في الأغراض السلمية. ويمكن أن تدعم تدابير بناء الثقة أيضا تنفيذ معايير السلوك المسؤول للدول، حيث إنها تعزز الثقة وتكفل قدراً أكبر من الوضوح والقدرة على التنبؤ والاستقرار في استخدام الدول لتكنولوجيا المعلومات والاتصالات. ويمكن لتدابير بناء الثقة، إلى جانب الركائز الأخرى لإطار السلوك المسؤول للدول، أن تساعد أيضا على بناء أوجه فهم مشتركة بين الدول، مما يسهم في تهيئة بيئة دولية سلمية بقدر أكبر.

42 - وبالنظر إلى أن تدابير بناء الثقة هي التزامات طوعية يتعهد بها تدريجيا، فإنها يمكن أن تكون خطوة أولى لمعالجة انعدام الثقة الناجم عن سوء التفاهم بين الدول عن طريق إقامة الاتصالات وبناء الجسور والشروع في التعاون على تحقيق هدف مشترك ذي مصلحة متبادلة. وبذلك، قد ترسي تدابير بناء الثقة الأسس لترتيبات واتفاقات موسعة إضافية في المستقبل.

43 - وخلصت الدول إلى أن الحوار داخل الفريق العامل المفتوح العضوية هو في حد ذاته من تدابير بناء الثقة، لأنه يحفز على تبادل مفتوح وشفاف للآراء بشأن تصورات التهديدات ومواطن الضعف، والسلوك المسؤول للدول والجهات الفاعلة الأخرى، والممارسات الجيدة، وذلك ما يدعم في نهاية المطاف العمل الجماعي على وضع وتنفيذ إطار السلوك المسؤول للدول في استخدامها لتكنولوجيا المعلومات والاتصالات.

44 - وبالإضافة إلى ذلك، خلصت الدول إلى أن للأمم المتحدة دورا حاسما في وضع تدابير بناء الثقة العالمية ودعم تنفيذها. وقد أوصي باتخاذ تدابير عملية لبناء الثقة في كل تقرير من تقارير فريق الخبراء الحكوميين الصادرة بتوافق الآراء. وبالإضافة إلى هذه التوصيات الخاصة بتكنولوجيا المعلومات والاتصالات، أيدت الجمعية العامة، في قرارها 78/43 (جاء) المتخذ بتوافق الآراء، المبادئ التوجيهية لتدابير بناء الثقة التي وضعت في إطار هيئة نزع السلاح التابعة للأمم المتحدة، والتي حددت مبادئ وأهدافاً وخصائص قيّمة لتدابير بناء الثقة يمكن النظر فيها عند وضع تدابير جديدة خاصة بتكنولوجيا المعلومات والاتصالات.

45 - وخلصت الدول، استناداً إلى ما لديها من رصيد أساسي من الثقة والعلاقات الراسخة، إلى أن المنظمات الإقليمية ودون الإقليمية بذلت جهودا كبيرة في وضع تدابير بناء الثقة، وتكييفها مع سياقاتها وأولوياتها المحددة، وإذكاء الوعي، وتبادل المعلومات بين أعضائها. وبالإضافة إلى ذلك، يمكن أن تُرسي عمليات التبادل الإقليمية والأقاليمية وفيما بين المنظمات سبلا جديدة للتآزر والتعاون والتعلم المتبادل. وبالنظر إلى أن الدول ليست جميعها أعضاء في منظمة إقليمية وليس لدى جميع المنظمات الإقليمية تدابير لبناء الثقة، فقد لوحظ أن هذه التدابير مكملة لعمل الأمم المتحدة والمنظمات الأخرى في مجال تعزيز تدابير بناء الثقة.

46 - واستناداً إلى الدروس والممارسات التي تم تبادلها في إطار الفريق العامل، خلصت الدول إلى أن الوجود المسبق للآليات والهياكل الوطنية والإقليمية، إضافة إلى بناء الموارد والقدرات الكافية، مثل الأفرقة الوطنية لمواجهة الطوارئ الحاسوبية، أمران أساسيان لكفالة أن تفي تدابير بناء الثقة بالغرض المنشود منها.

47 - وكإجراء محدد، خلصت الدول إلى أن إنشاء نقاط اتصال وطنية هو في حد ذاته من تدابير بناء الثقة، ولكنه أيضا تدبير مفيد لتنفيذ العديد من تدابير بناء الثقة الأخرى، وهو أمر لا يُقدر بثمن في أوقات الأزمات. وقد تجد الدول أنه من المفيد إنشاء نقاط اتصال لجملة أمور منها التبادل الدبلوماسي والسياساتي والقانوني والتقني، إضافة إلى الإبلاغ عن الحوادث والتصدي لها.

ويوصي الفريق العامل بما يلي:

48 - أن تواصل الدول، على أساس طوعي، إبلاغ الأمين العام بآرائها وتقييماتها وإدراج معلومات إضافية عن الدروس المستفادة والممارسات الجيدة المتعلقة بتدابير بناء الثقة ذات الصلة على المستوى الثنائي أو الإقليمي أو المتعدد الأطراف.

49 - وأن تقوم الدول طوعا بتحديد تدابير بناء الثقة الملائمة لسياقاتها المحددة والنظر فيها، وتتعاون مع الدول الأخرى في تنفيذها.

50 - وأن تشارك الدول طوعا في تدابير تحقيق الشفافية عن طريق تبادل المعلومات والدروس المستفادة ذات الصلة، بالشكل الذي تختاره وفي المنتديات التي تختارها، حسب الاقتضاء، بما في ذلك من خلال بوابة السياسات السيبرانية التابعة لمعهد الأمم المتحدة لبحوث نزع السلاح.

51 - وأن تنظر الدول التي لم تعين بعدُ نقاط اتصال وطنية على مستويات منها المستويات التقنية والسياساتية والدبلوماسية في تعيينها، مع مراعاة القدرات المتباينة. وتُشجَّع الدول أيضا على مواصلة النظر في طرائق إنشاء دليل لنقاط الاتصال على الصعيد العالمي.

52 - وأن تستكشف الدول آليات للتبادل الأقاليمي المنتظم للدروس المستفادة والممارسات الجيدة فيما يتعلق بتدابير بناء الثقة، مع مراعاة الاختلافات في السياقات الإقليمية وهياكل المنظمات ذات الصلة.

53 - وأن تواصل الدول النظر في تدابير بناء الثقة على المستويات الثنائية والإقليمية والمتعددة الأطراف، وفرص التعاون في ممارسة تدابير بناء الثقة التي يتم تشجيعها.

بناء القدرات

54 - تتوقف قدرة المجتمع الدولي في مجال منع أو تخفيف أثر أنشطة تكنولوجيا المعلومات والاتصالات الخبيثة على قدرة كل دولة على الاستعداد والاستجابة. وبناء القدرات يكتسي أهمية خاصة بالنسبة للدول النامية، من أجل تيسير مشاركتها الحقيقية في المناقشات المتعلقة بتكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي وقدرتها على معالجة أوجه الضعف في بنيتها التحتية الحيوية. ويساعد بناء القدرات على تطوير المهارات والموارد البشرية والسياسات والمؤسسات التي تزيد من قدرة الدول على الصمود وتزيد من أمنها حتى تتمكن من التمتع الكامل بفوائد التكنولوجيا الرقمية. وهو يؤدي وظيفة تمكينية هامة لتعزيز التقيد بالقانون الدولي وتنفيذ معايير السلوك المسؤول للدول، إضافة إلى دعم تنفيذ تدابير بناء الثقة. وفي عالم مترابط رقميا، تتجاوز فوائد بناء القدرات المستفيدين الأصليين، وتسهم في تهيئة بيئة أكثر أمنا واستقرارا للجميع في مجال تكنولوجيا المعلومات والاتصالات.

55 - وتتطلب كفالة تهيئة بيئة مفتوحة ومأمونة ومستقرة وميسَّرة وسلمية لتكنولوجيا المعلومات والاتصالات تعاونا فعالا بين الدول للحد من المخاطر التي تهدد السلام والأمن الدوليين. ويشكل بناء القدرات جانبا هاما من جوانب هذا التعاون، وهو عمل طوعي من جانب كل من المانح والمتلقي.

56 - وخلصت الدول، مع مراعاة المبادئ المقبولة على نطاق واسع، وبعد التعمق في تفاصيلها، إلى أن بناء القدرات فيما يتعلق باستخدام الدول لتكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي ينبغي أن يسترشد بالمبادئ التالية:

العملية والغرض

- ينبغي أن يكون بناء القدرات عملية مستدامة، تشمل أنشطة محددة من جانب مختلف الجهات الفاعلة ومن أجلها.
- ينبغي أن يكون للأنشطة المحددة هدف واضح، وأن تركز على النتائج، مع دعم الهدف المشترك المتمثل في تهيئة بيئة لتكنولوجيا المعلومات والاتصالات تكون مفتوحة ومأمونة ومستقرة وميسَّرة وسلمية.
- ينبغي أن تكون أنشطة بناء القدرات قائمة على الأدلة ومحايدة سياسيا وشفافة وخاضعة للمساءلة ودون شروط.
- ينبغي الاضطلاع ببناء القدرات مع الاحترام الكامل لمبدأ سيادة الدول.
- قد يلزم تيسير الوصول إلى التكنولوجيات ذات الصلة.

الشراكات

- ينبغي أن يستند بناء القدرات إلى الثقة المتبادلة، وأن يكون قائما على الطلب، وأن يتوافق مع الاحتياجات والأولويات المحددة وطنيا، وأن يتم الاضطلاع به في اعتراف كامل بمبدأ تولي مقاليد الأمور على الصعيد الوطني. ويشارك الشركاء في بناء القدرات طوعاً.
- وبالنظر إلى أن أنشطة بناء القدرات ينبغي أن تُصمَّم وفقا للاحتياجات والسياقات المحددة، فإن جميع الأطراف شركاء نشطون لهم مسؤوليات مشتركة ولكنها متباينة، بما في ذلك التعاون في تصميم أنشطة بناء القدرات وتنفيذها ورصدها وتقييمها.
- ينبغي لجميع الشركاء حماية سرية السياسات والخطط الوطنية واحترامها.

الناس

- ينبغي أن يحترم بناء القدرات حقوق الإنسان والحريات الأساسية، وأن يراعي الاعتبارات الجنسانية، وأن يكون شاملا للجميع وعالميا وغير تمييزي.
- ينبغي ضمان سرية المعلومات الحساسة.

57 - وخلصت الدول إلى أن بناء القدرات مسعى متبادل، وهو ما يسمى "طريق ذو اتجاهين"، يتعلم فيه المشاركون من بعضهم البعض، ويستفيد فيه جميع الأطراف من التحسن العام في أمن تكنولوجيا المعلومات

والاتصالات على الصعيد العالمي. وأشيرَ أيضا إلى قيمة التعاون بين بلدان الجنوب، وبين بلدان الجنوب والشمال، والتعاون الثلاثي، والتعاون المركّز على الصعيد الإقليمي.

58 - وخلصت الدول إلى أن بناء القدرات ينبغي أن يساهم في تحويل الفجوة الرقمية إلى فرص رقمية. وينبغي أن يستهدف على وجه الخصوص تيسير المشاركة الحقيقية للبلدان النامية في المناقشات والمحافل ذات الصلة وتعزيز قدرة البلدان النامية على الصمود في بيئة تكنولوجيا المعلومات والاتصالات.

59 - وخلصت الدول إلى أن بناء القدرات يمكن أن يساعد على تعزيز فهم المخاطر النظامية وغيرها من المخاطر الناشئة عن انعدام أمن تكنولوجيا المعلومات والاتصالات، وعدم كفاية التنسيق بين القدرات التقنية وقدرات السياسات على الصعيد الوطني، وما يتصل بذلك من تحديات مرتبطة بعدم المساواة والفجوات الرقمية، والتصدي لهذه المخاطر. واعتُبر أن بناء القدرات الرامي إلى تمكين الدول من تحديد وحماية البنية التحتية الوطنية الحيوية، والتعاون في حماية البنية التحتية الحيوية للمعلومات، يتسم بأهمية خاصة. وقد يساعد بناء القدرات الدولَ أيضاً على تعميق فهمها لكيفية انطباق القانون الدولي. ويمكن أن يؤدي تبادل المعلومات والتنسيق على الصعد الوطني والإقليمي والدولي إلى جعل أنشطة بناء القدرات أكثر فعالية واستراتيجية ومواءمة مع الأولويات الوطنية.

60 - وبالإضافة إلى الحاجة إلى المهارات التقنية وبناء المؤسسات والآليات التعاونية، خلصت الدول إلى أن هناك حاجة ملحة لبناء الخبرات في طائفة من المجالات الدبلوماسية والقانونية والسياساتية والتشريعية والتنظيمية. وفي هذا السياق، تم إبراز أهمية تنمية القدرات الدبلوماسية للمشاركة في العمليات الدولية والحكومية الدولية.

61 - وأشارت الدول إلى الحاجة إلى نهج عملي المنحى وملموس في مجال بناء القدرات. وخلصت إلى أن هذه التدابير الملموسة يمكن أن تشمل تقديم الدعم على صعيد السياسات العامة وعلى الصعيد التقني، مثل وضع استراتيجيات وطنية للأمن السيبراني، وتوفير سبل الوصول إلى التكنولوجيات ذات الصلة، ودعم أفرقة مواجهة الطوارئ الحاسوبية أو أفرقة الاستجابة لحوادث أمن الفضاء الإلكتروني، ووضع برامج تدريبية متخصصة ومناهج مصممة خصيصا، بما في ذلك برامج "تدريب المدربين" وإصدار شهادات مهنية. وتم الاعتراف بفوائد إنشاء منابر لتبادل المعلومات، بما في ذلك الممارسات القانونية والإدارية الجيدة، وكذلك بالمساهمات القيمة التي تقدمها الجهات الأخرى ذات الصلة صاحبة المصلحة لأنشطة بناء القدرات.

62 - وخلصت الدول إلى أن تقييم الجهود الوطنية فيما يتعلق بالاستنتاجات والتوصيات الواردة في هذا التقرير، وكذلك التقييمات والتوصيات التي اتفقت الدول الأعضاء على أن يسترشد فيها بالقرار 237/70 المتخذ بتوافق الآراء، عمليةٌ قيّمة لتحديد التقدم المحرز وتحديد المواطن التي يلزم فيها زيادة بناء القدرات.

ويوصي الفريق العامل بما يلي:

63 - أن تسترشد الدول بالمبادئ الواردة في الفقرة 56 في جهودها الرامية إلى بناء القدرات المتعلقة بتكنولوجيا المعلومات والاتصالات في ميدان الأمن الدولي، وأن تُشجِّع الجهات الفاعلة الأخرى على مراعاة هذه المبادئ في أنشطتها الخاصة ببناء القدرات.

64 - وأن تواصل الدول، على أساس طوعي، إبلاغ الأمين العام بآرائها وتقييماتها بشأن التطورات في ميدان تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي، وإدراج معلومات إضافية عن الدروس المستفادة والممارسات الجيدة المتصلة ببرامج ومبادرات بناء القدرات.

65 - وأن تستخدم الدول، على أساس طوعي "الدراسة الاستقصائية النموذجية الوطنية بشأن تنفيذ قرار الجمعية العامة للأمم المتحدة 237/70" (التي ستتاح على الإنترنت) من أجل مساعدتها على القيام بذلك. وقد ترغب الدول الأعضاء أيضا في استخدام الدراسة الاستقصائية النموذجية، على أساس طوعي، في هيكلة ما تقدمه من إفادات حسب ما ذكر أعلاه لإبلاغ الأمين العام بآرائها وتقييماتها.

66 - وأن تُشجَّع الدول وغيرها من الجهات الفاعلة التي يمكنها تقديم المساعدة المالية أو العينية أو التقنية من أجل بناء القدرات على القيام بذلك. وينبغي مواصلة تعزيز تنسيق جهود بناء القدرات وتوفير الموارد لها، بما في ذلك بين المنظمات ذات الصلة والأمم المتحدة.

67 - وأن تواصل الدول النظر في بناء القدرات على الصعيد المتعدد الأطراف، بما في ذلك تبادل الآراء والمعلومات والممارسات الجيدة.

الحوار المؤسسي المنتظم

68 - أتاح الفريق العامل المنشأ بموجب قرار الجمعية العامة 27/73، لأول مرة تحت رعاية الأمم المتحدة، منبرا مخصصا للحوار فيما بين جميع الدول بشأن التطورات في ميدان تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي.

69 - وبالإضافة إلى هدف الفريق العامل المتمثل في السعي إلى التوصل إلى أوجه فهم مشتركة بين جميع الدول، فقد عزز الفريق الشبكات الدبلوماسية وشجع الثقة بين المشاركين. وأظهرت المشاركة الواسعة لأصحاب المصلحة غير الحكوميين أن هناك مجتمعا أوسع من الجهات الفاعلة على استعداد لتسخير خبرته لدعم الدول في تحقيق هدفها المتمثل في كفالة تهيئة بيئة لتكنولوجيا المعلومات والاتصالات تكون مفتوحة ومأمونة ومستقرة وميسَّرة وسلمية. وشكلت مناقشات الفريق العامل تأكيدا لأهمية المناقشات المتكررة والمنظمة التي تجرى تحت رعاية الأمم المتحدة بشأن استخدام تكنولوجيا المعلومات والاتصالات.

70 - وخلصت الدول إلى أن الحوار المنتظم تحت رعاية الأمم المتحدة يدعم الأهداف المشتركة المتمثلة في تعزيز السلام والاستقرار ومنع نشوب النزاعات على الصعيد الدولي في بيئة تكنولوجيا المعلومات والاتصالات. وخلصت الدول أيضاً إلى أنه في ضوء تزايد الاعتماد على تكنولوجيا المعلومات والاتصالات ونطاق التهديدات الناجمة عن استخدامها لأغراض خبيثة، فإن هناك حاجة ملحة إلى مواصلة تعزيز الفهم المشترك وبناء الثقة وتكثيف التعاون الدولي.

71 - وبالنظر إلى أن الدول تتحمل المسؤولية الرئيسية عن الأمن الوطني والسلامة العامة وسيادة القانون، فإن الدول أكدت أهمية الحوار الحكومي الدولي المنتظم، وأهمية تحديد الآليات المناسبة للعمل مع المجموعات الأخرى من أصحاب المصلحة في العمليات المقبلة.

72 - ويركز النظر في تطورات تكنولوجيا المعلومات والاتصالات والأمن الدولي في الأمم المتحدة على أبعادها المتعلقة بالسلام والاستقرار ومنع نشوب النزاعات على الصعيد الدولي. وخلصت الدول إلى أن الحوار المؤسسي المنتظم في المستقبل ينبغي ألا يكرر ولايات الأمم المتحدة وجهودها وأنشطتها القائمة التي

تركز على الأبعاد الرقمية لمسائل أخرى[8]. وخلصت الدول إلى أن زيادة التبادل بين هذه المنتديات والعمليات التي أنشأتها اللجنة الأولى يمكن أن تساعد على تعزيز التآزر وتحسين الاتساق، مع احترام الطبيعة الفنية أو الولاية المتخصصة لكل هيئة.

73 - وخلصت الدول إلى أن الحوار الذي سيجرى في المستقبل فيما يتعلق بالتعاون الدولي بشأن تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي ينبغي أن يتوخى، في جملة أمور، زيادة الوعي وبناء الثقة وتشجيع مزيد من الدراسة والمناقشة بشأن المجالات التي لم يتبلور فيها بعد فهم مشترك. وأقرت الدول بجدوى استكشاف آليات مكرسة لمتابعة تنفيذ المعايير والقواعد المتفق عليها ووضع معايير وقواعد أخرى.

74 - وخلصت الدول إلى أن أي آلية تُعتمد في المستقبل للحوار المؤسسي المنتظم تحت رعاية الأمم المتحدة ينبغي أن تتخذ شكل إجراء عملي المنحى ومحدد الأهداف محددة ومستند إلى النتائج السابقة، وأن تكون شاملةً للجميع، وشفافة، ومدفوعة بتوافق الآراء، وقائمة على النتائج.

ويوصي الفريق العامل بما يلي:

75 - أن تواصل الدول المشاركة بنشاط في الحوار المؤسسي المنتظم تحت رعاية الأمم المتحدة.

76 - أن تكفل الدول استمرار عملية تفاوض شفافة وشاملة للجميع بشأن تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي تحت رعاية الأمم المتحدة، تشمل الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025، الذي أنشئ عملا بقرار الجمعية العامة 240/75، وتعترف بهذا الفريق.

77 - وأن تحيط الدول علماً بمجموعة متنوعة من المقترحات الرامية إلى النهوض بسلوك الدول المسؤول في مجال تكنولوجيا المعلومات والاتصالات، وهو ما من شأنه، في جملة أمور، أن يدعم قدرة الدول على تنفيذ الالتزامات في استخدامها لتكنولوجيا المعلومات والاتصالات، ولا سيما برنامج العمل. وعند النظر في هذه المقترحات، ينبغي أن تؤخذ في الاعتبار شواغل جميع الدول ومصالحها من خلال مشاركة الدول على قدم المساواة في الأمم المتحدة. وفي هذا الصدد، ينبغي زيادة تفصيل برنامج العمل بما في ذلك على صعيد عملية الفريق العامل المفتوح العضوية المنشأ عملا بقرار الجمعية العامة 240/75.

78 - وأن تنظر الدول في استنتاجات وتوصيات هذا التقرير في أي عمليات مقبلة لإجراء حوار مؤسسي منتظم تحت رعاية الأمم المتحدة.

79 - وأن تنظر الدول التي بوسعها إنشاء أو دعم برامج الرعاية وغيرها من الآليات لضمان المشاركة الواسعة في عمليات الأمم المتحدة المذكورة أعلاه في القيام بذلك.

(8) انظر ورقة المعلومات الأساسية الصادرة عن رئيس الفريق العامل، "An Initial Overview of UN System Actors, Processes and Activities on ICT-related issues of Interest to the OEWG, By Theme", December 2019, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/background-paper-on-existing-un-bodies-processes-related-to-mandate.pdf.

جيم - ملاحظات ختامية

80 - طوال عملية الفريق العامل المفتوح العضوية، شاركت الدول بصورة متسقة ونشطة، وأسفر ذلك عن تبادل جد غزير للآراء. ومن الجوانب القيمة التي يكتسيها هذا التبادل تقديم وجهات نظر متنوعة وأفكار جديدة ومقترحات هامة، حتى وإن لم تتفق بالضرورة جميع الدول بشأنها، بما في ذلك إمكانية وضع مزيد من الالتزامات الملزمة قانوناً. وترد وجهات النظر المتنوعة في الموجز المرفق الذي أعده الرئيس بشأن المناقشات ومقترحات الصياغات المحددة في إطار بند جدول الأعمال "القواعد والمعايير والمبادئ". وينبغي مواصلة النظر في وجهات النظر المذكورة في عمليات الأمم المتحدة المقبلة، بما في ذلك في الفريق العامل المفتوح العضوية المنشأ عملا بقرار الجمعية العامة 240/75.

المرفق الثاني*

موجز الرئيس

ألف - السياق

1 - أتاح الفريق العامل المفتوح العضوية فرصة تاريخية لجميع الدول للمشاركة على قدم المساواة تحت رعاية الأمم المتحدة في مناقشات مركزة ومتواصلة بشأن مسائل متعلقة بتكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي. وبالإضافة إلى مجالات الاتفاق العديدة التي يجسدها تقرير الفريق العامل، فقد كان الفريق العامل، من خلال مناقشاته الشاملة والشفافة، بمثابة تدبير قيّم لتعزيز السلام والأمن الدوليين من خلال بناء الثقة والتفاهمات بين الدول، والمساعدة في إنشاء شبكة دبلوماسية عالمية من الخبراء الوطنيين. وأظهرت المشاركة النشطة والواسعة النطاق من جانب جميع الوفود تصميم الدول على مواصلة العمل معا بشأن هذا الموضوع ذي الأهمية الأساسية للجميع.

2 - وتميزت جميع دورات الفريق العامل بتبادلات موضوعية وتفاعلية بين الدول، وكذلك مع المجتمع المدني والقطاع الخاص والأوساط الأكاديمية والأوساط التقنية. ويشكل الالتزام الذي أبدته الدول وأصحاب المصلحة الآخرون طوال أعمال الفريق العامل، مع مشاركة متزايدة حتى مع تحول بعض اجتماعاته إلى شكل افتراضي، مؤشرا لا يمكن إنكاره على الأهمية العالمية المتزايدة للمواضيع قيد النظر، وعلى الاعتراف المتزايد بالحاجة الملحة إلى التصدي الجماعي للتهديدات التي يتعرض لها الأمن الدولي بسبب الاستخدام الخبيث لتكنولوجيا المعلومات والاتصالات.

3 - ويصدر هذا الموجز تحت مسؤولية الرئيس ويعكس فهمه للنقاط الرئيسية التي نوقشت خلال اجتماعات الفريق العامل المفتوح العضوية. وقد لا يعكس الموجز المساهمة الكاملة لجميع الوفود وينبغي ألا ينظر إليه بوصفه يعكس توافق آراء الدول بشأن أي نقاط محددة مشمولة فيه. ويمكن الاطلاع على الخلاصة الكاملة للبيانات والمقترحات الوطنية التي قُدمت بغرض تعميمها على الرابط التالي: https://www.un.org/disarmament/open-ended-working-group.

باء - استعراض عام للمناقشات

4 - أتاحت عملية الفريق العامل المفتوح العضوية فرصةً لجميع الدول للإعراب عن آرائها وشواغلها وتطلعاتها بطريقة ديمقراطية وشفافة وشاملة للجميع. وفي حين سعى الفريق العامل إلى تحديد مجالات التقارب وتوافق الآراء، فإن مناقشاته كانت أيضاً سجلاً لتنوع وجهات نظر الدول الأعضاء وأفكارها ومقترحاتها، وقد تكون بمثابة أساس مفيد للعمل في المستقبل سعياً إلى زيادة بلورة أوجه فهم مشتركة بشأن استخدام الدول لتكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي.

5 - وشددت الدول، طوال مداولاتها في إطار الفريق العامل المفتوح العضوية، على الروابط وأوجه التآزر بين كل عنصر من عناصر ولايته: فالقانون الدولي يحكم الإجراءات والعلاقات بين الدول، والقواعد الطوعية غير الملزمة توفر إرشادات إضافية بشأن ما يشكل سلوك الدول المسؤول. ويعكس هذان العنصران معا توقعات نهج سلوك معين فيما يتعلق باستخدامات الدول لتكنولوجيا المعلومات والاتصالات في سياق

* يصدر دون تحرير رسمي.

الأمن الدولي. وبهذه الطريقة، فهما يسهمان أيضا في بناء الثقة بزيادة الشفافية والتعاون بين الدول، وفي الحد من خطر نشوب النزاعات. ويشكل بناء القدرات بدوره أداة تمكين لجميع الدول من أجل المساهمة في زيادة الاستقرار والأمن على الصعيد العالمي. وتشكل هذه العناصر مجتمعة إطارا عالميا للتدابير التعاونية بغرض التصدي للتهديدات القائمة والمحتملة في ميدان تكنولوجيا المعلومات والاتصالات. وسيتيح الحوار المؤسسي المنتظم الفرصة لزيادة تطوير وتفعيل هذا الإطار عن طريق تعزيز أوجه الفهم المشتركة، وتبادل الدروس المستفادة والممارسات الجيدة في مجال التنفيذ، وبناء الثقة، وزيادة القدرات لدى الدول.

التهديدات القائمة والمحتملة

6 - أبرزت الدول، في مناقشاتها في إطار الفريق العامل، مجموعة واسعة من التهديدات القائمة والمحتملة، مما أكد على أن الدول قد تبدو لها التهديدات الناشئة عن بيئة تكنولوجيا المعلومات والاتصالات بطرق مختلفة. وقد أتاح الشكل الشامل للفريق العامل فرصة للدول لتعميق فهمها لكيفية إدراك الآخرين للأفعال والسلوكيات في بيئة تكنولوجيا المعلومات والاتصالات، والاستماع إلى ما يعتبره الآخرون أهم التهديدات والمخاطر.

7 - وأعربت بعض الدول عن قلقها إزاء تطوير أو استخدام قدرات تكنولوجيا المعلومات والاتصالات لأغراض لا تتفق مع أهداف صون السلام والأمن الدوليين. وأعرب البعض عن القلق من أن خصائص بيئة تكنولوجيا المعلومات والاتصالات قد تشجع على اتخاذ تدابير انفرادية بدلا من تسوية المنازعات بالوسائل السلمية. وأشارت بعض الدول إلى قلقها إزاء تطوير قدرات تكنولوجيا المعلومات والاتصالات لأغراض عسكرية وغيرها من الأغراض التي يمكن أن تقوض السلام والأمن الدوليين. وأشارت دول أخرى إلى أن التهديد يكمن في استخدام الدول لهذه القدرات بما يتعارض مع التزاماتها بموجب القانون الدولي. وأُثيرت أيضاً شواغل بشأن تراكم مواطن الضعف وانعدام الشفافية والعمليات المحددة للكشف عنها، واستغلال الوظائف الخفية الضارة، وسلامة سلاسل الإمداد العالمية لتكنولوجيا المعلومات والاتصالات، وضمان أمن البيانات. وأثارت بعض الدول شواغل بشأن إمكانية استخدام تكنولوجيا المعلومات والاتصالات للتدخل في شؤونها الداخلية، بما في ذلك عن طريق العمليات الإعلامية وحملات التضليل الإعلامي. وأشير أيضاً إلى مساعي زيادة التشغيل الآلي والتشغيل الذاتي في عمليات تكنولوجيا المعلومات والاتصالات باعتبارها شاغلا محددا، شأنها شأن الإجراءات التي يمكن أن تؤدي إلى خفض أو تعطيل القدرة على الاتصال الإلكتروني، أو التصعيد غير المقصود، أو الآثار التي تؤثر سلبا على أطراف ثالثة. ولاحظت بعض الدول أيضا أن عدم الوضوح فيما يتعلق بمسؤوليات القطاع الخاص هو مصدر قلق في حد ذاته.

8 - وشددت الدول على أن التدابير الرامية إلى تعزيز السلوك المسؤول للدول ينبغي أن تظل محايدة من الناحية التكنولوجية، مؤكدة أن إساءة استخدام التكنولوجيات، وليس التكنولوجيات ذاتها، هي التي تثير القلق. وأقرت الدول أن أوجه التقدم التكنولوجي والتطبيقات الجديدة، وإن كان من الممكن أن تتيح فرصا إنمائية، فإنها قد توسع أيضا نطاق الهجمات، أو تزيد من مواطن الضعف في بيئة تكنولوجيا المعلومات والاتصالات، أو تُستخدم لأنشطة خبيثة جديدة. وسُلط الضوء على اتجاهات وتطورات تكنولوجية معينة في هذا الصدد، بما في ذلك التقدم المحرز في تعلّم الآلة والحوسبة الكمية؛ وانتشار الأجهزة الموصولة ("إنترنت الأشياء")؛ والطرق الجديدة لتخزين البيانات والوصول إليها من خلال تقنية الحسابات الموزعة والحوسبة السحابية؛ وتوسع البيانات الضخمة والبيانات الشخصية الرقمية.

القانون الدولي

9 - استرشاداً بولاية الفريق، وبهدف صون السلام والاستقرار وتعزيز بيئة لتكنولوجيا المعلومات والاتصالات تكون مفتوحة ومأمونة ومستقرة وميسَّرة وسلمية، وتعزيز أوجه الفهم المشتركة، تبادلت الدول الآراء بشأن كيفية انطباق القانون الدولي على البعد الأمني الدولي لتكنولوجيا المعلومات والاتصالات.

10 - وأشارت الدول، في مناقشاتها في إطار الفريق العامل، إلى أن القانون الدولي، وبخاصة ميثاق الأمم المتحدة برمته، ينطبق في هذا الصدد، وهو عنصر لا بد منه لصون السلام والاستقرار والنهوض ببيئة لتكنولوجيا المعلومات والاتصالات تكون مفتوحة ومأمونة ومستقرة وميسَّرة وسلمية. وفي هذا الصدد، شددت الدول على الحاجة إلى اتخاذ خطوات من أجل النأي أو الامتناع عن اتخاذ، أي تدابير لا تتوافق مع ميثاق الأمم المتحدة والقانون الدولي على نحو يعوق التحقيق الكامل للتنمية الاقتصادية والاجتماعية لشعوب البلدان المتضررة ويعرقل رفاهها. وفي الوقت نفسه، أبرزت الدول أيضاً أن الأمر يتطلب مزيدا من الفهم بشأن كيفية انطباق القانون الدولي على استخدام الدول لتكنولوجيا المعلومات والاتصالات.

11 - ومن بين مبادئ القانون الدولي المحددة التي أعيد تأكيدها سيادة الدول؛ والتساوي في السيادة؛ وتسوية المنازعات الدولية بالوسائل السلمية بطريقة لا تعرّض السلام والأمن الدوليين والعدالة للخطر؛ والامتناع في علاقاتها الدولية عن التهديد باستعمال القوة أو استعمالها ضد السلامة الإقليمية أو الاستقلال السياسي لأي دولة، أو بأي طريقة أخرى تتعارض مع مقاصد الأمم المتحدة؛ واحترام حقوق الإنسان والحريات الأساسية؛ وعدم التدخل في الشؤون الداخلية للدول الأخرى.

12 - وأشيرَ إلى أن القانون الدولي هو أساس الاستقرار وإمكانية التنبؤ في العلاقات بين الدول. وعلى وجه الخصوص، يحد القانون الدولي الإنساني من المخاطر والأضرار التي يمكن أن يتعرض لها المدنيون والأعيان المدنية والمقاتلون في سياق نزاع مسلح. وفي الوقت نفسه، أكدت الدول أن القانون الدولي الإنساني لا يشجع على العسكرة ولا يضفي الشرعية على اللجوء إلى النزاع في أي مجال من المجالات.

13 - ولوحظ أيضا أن مسؤوليات الدول فيما يتعلق بالأفعال غير المشروعة دوليا تمتد، بموجب القانون الدولي العرفي، إلى استخدامها لتكنولوجيا المعلومات والاتصالات.

14 - وأشير إلى أنه يجب على الدول ألا تستخدم وكلاء عنها لارتكاب أفعال غير مشروعة دوليا باستخدام تكنولوجيا المعلومات والاتصالات، وينبغي لها أن تسعى إلى ضمان عدم استخدام إقليمها من قبل جهات من غير الدول تعمل بناء على تعليمات دولة ما أو تحت سيطرتها لارتكاب أفعال من هذا القبيل. وأشير أيضا إلى مسؤولية الدول فيما يتعلق بالكيانات التي تملكها الدولة أو التي تخضع لسيطرتها.

15 - وأوضحت الدول أن الإشارة إلى إطلاق نشاط من أنشطة تكنولوجيا المعلومات والاتصالات من إقليم دولة من الدول أو من بنيتها التحتية لتكنولوجيا المعلومات والاتصالات أو صدور هذا النشاط من ذلك الإقليم أو تلك البنية التحتية بطريقة أخرى قد لا يكون كافيا في حد ذاته لنسبة النشاط إلى تلك الدولة، وأنه ينبغي أن تكون الاتهامات الموجهة ضد الدول بتنظيم أفعال غير مشروعة وتنفيذها مدعومة بالأدلة. وأبرزت بعض الدول أهمية تقديم دليل حقيقي وموثوق وكاف في هذا السياق.

16 - وأعربت بعض الدول عن رأي مفاده أن القانون الدولي القائم، الذي تكمله القواعد الطوعية غير الملزمة التي تعكس توافق الآراء بين الدول، يكفي حاليا لمعالجة استخدام الدول لتكنولوجيا المعلومات والاتصالات. واقتُرح أيضا أن تركز الجهود على التوصل إلى فهم مشترك بشأن كيفية تطبيق الإطار المعياري المتفق عليه بالفعل من خلال وضع توجيهات إضافية، وإمكانية تفعيله من خلال تعزيز التنفيذ من جانب جميع الدول. وفي الوقت نفسه، أعربت دول أخرى عن رأي مفاده أنه بالنظر إلى الطبيعة السريعة التطور لبيئة التهديدات وشدة الخطر، فإن الحاجة تدعو إلى وضع إطار دولي ملزم قانونا بشأن تكنولوجيا المعلومات والاتصالات. وأشير أيضا إلى أن هذا الإطار الملزم قد يؤدي إلى تنفيذ الالتزامات على الصعيد العالمي بمزيد من الفعالية، وإلى إيجاد قاعدة أقوى لمساءلة الجهات الفاعلة عن أفعالها. وشددت الدول على أن عملية وضع أي إطار قانوني دولي لمعالجة المسائل المتعلقة باستخدام تكنولوجيا المعلومات والاتصالات الذي تكون له آثار على السلام والأمن الدوليين ينبغي أن تراعي شواغل جميع الدول ومصالحها، وأن تستند إلى توافق الآراء، وأن تتوخى داخل الأمم المتحدة بمشاركة نشطة من جميع الدول على قدم المساواة.

17 - وأُبرز أنه في حين أن هيئات القانون الدولي القائمة لا تدرج إشارة محددة إلى استخدام تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي، فإن القانون الدولي يمكن أن يتطور تدريجيا، بما في ذلك من خلال الاعتقاد بالإلزام وممارسات الدول. وأثيرت إمكانية القيام، مع مرور الوقت، بوضع تدابير ملزمة تكميلية بالتزامن مع تنفيذ القواعد. وعلاوة على ذلك، اقتُرح إبداء التزام سياسي كإحدى الوسائل المحتملة للمضي قدما.

18 - ومع الإشارة إلى أن القانون الدولي، وبخاصة ميثاق الأمم المتحدة، ينطبق على استخدام تكنولوجيا المعلومات والاتصالات، سُلط الضوء على أن بعض المسائل المتعلقة بكيفية انطباق القانون الدولي على استخدام تكنولوجيا المعلومات والاتصالات لم تتضح بعد بصورة كاملة. وأشارت بعض الدول إلى أن هذه المسائل تشمل في جملة أمور نوع النشاط المتصل بتكنولوجيا المعلومات والاتصالات الذي قد تفسره دول أخرى على أنه ينطوي على التهديد باستعمال القوة أو استعمالها (المادة 2 (4) من الميثاق) أو الذي قد يعطي دولة ما سببا للاحتجاج بحقها الطبيعي في الدفاع عن النفس (المادة 51 من الميثاق). وهي تشمل أيضا مسائل تتصل بكيفية انطباق مبادئ القانون الدولي الإنساني، مثل مبادئ الإنسانية، والضرورة، والتناسب، والتمييز، والحيطة، على عمليات تكنولوجيا المعلومات والاتصالات. وفي هذا الصدد، لاحظت بعض الدول أن المناقشات بشأن انطباق القانون الدولي الإنساني على استخدام الدول لتكنولوجيا المعلومات والاتصالات ينبغي تناولها بحذر. ولاحظت الدول أنه يلزم إجراء مزيد من الدراسة بشأن هذه المواضيع الهامة في المناقشات المقبلة.

19 - وفيما يتعلق أيضا بسبل المضي قدما، أشارت الدول إلى أن الخطوة الأولى الرئيسية لتوضيح أوجه الفهم المشتركة ومواصلة تطويرها قد تنشأ عن زيادة تبادل الآراء والمناقشات المتعمقة من جانب الدول بشأن كيفية انطباق القانون الدولي على استخدام الدول لتكنولوجيا المعلومات والاتصالات. ولوحظ أن تبادل الآراء هذا يمكن أن يكون في حد ذاته تدبيرا هاما من تدابير بناء الثقة. وعلاوة على ذلك، اقترحت بعض الدول عدة طرق لتبادل آرائها الوطنية طوعا بشأن كيفية انطباق القانون الدولي، بما في ذلك استخدام التقرير السنوي للأمين العام عن التطورات في ميدان المعلومات والاتصالات السلكية

واللاسلكية في سياق الأمن الدولي[9]، أو بوابة السياسات السيبرانية التابعة لمعهد الأمم المتحدة لبحوث نزع السلاح، أو استخدام دراسة استقصائية للممارسات الوطنية في مجال تطبيق القانون الدولي. وجرى أيضا إبراز التقدم المحرز في الترتيبات الإقليمية وغيرها من الترتيبات لتبادل الآراء ووضع فهم مشترك بشأن كيفية انطباق القانون الدولي.

20 - ومن منظور صون السلام ومنع نشوب النزاعات، أكدت الدول ضرورة تسوية المنازعات بالوسائل السلمية والامتناع عن التهديد باستعمال القوة أو استعمالها. وفي هذا السياق، أشارت الدول إلى الهيئات والآليات والأدوات القائمة لمنع نشوب المنازعات وتسويتها بالوسائل السلمية. وأشارت بعض الدول إلى أن وضع نهج وفهم مشتركين ومقبولين عالميا لمصدر حوادث تكنولوجيا المعلومات والاتصالات على المستوى التقني تحت رعاية الأمم المتحدة، من خلال تبادل الممارسات الجيدة، مع مراعاة احترام مبدأ سيادة الدول، يمكن أن يؤدي إلى مزيد من المساءلة والشفافية، ويمكن أن يساعد على دعم إمكانية لجوء المتضررين من الأفعال الخبيثة إلى القضاء.

قواعد ومعايير ومبادئ السلوك المسؤول للدول

21 - أشارت الدول، في مناقشاتها في إطار الفريق العامل، إلى أن المعايير الطوعية وغير الملزمة للسلوك المسؤول للدول لا تغير أو تحل محل أحكام القانون الدولي ومقاصد الأمم المتحدة ومبادئها، بما في ذلك صون السلام والأمن الدوليين وتعزيز حقوق الإنسان، بل ينبغي أن ينظر إليها على أنها تتسق معها. وأشارت الدول أيضا إلى قرار الجمعية العامة 2131 (د-20) لعام 1965 المعنون "إعلان عدم جواز التدخل في الشؤون الداخلية للدول، وحماية استقلالها وسيادتها".

22 - وأشارت الدول إلى أنه في حين يقدم قرار الجمعية العامة 23/73 مجموعة من 13 من قواعد ومعايير ومبادئ السلوك المسؤول للدول، فإنه يؤكد، في جملة أمور، على المعايير الإحدى عشر الطوعية وغير الملزمة "الواردة في تقريري فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي لعامي 2013 و 2015، التي اعتمدت بتوافق الآراء وأوصي بها في القرار 28/71"[10].

23 - وشددت الدول على ضرورة تعزيز الوعي بالمعايير القائمة ودعم تفعيلها بالتوازي مع وضع معايير جديدة. وأكدت الدول على الحاجة إلى التوجيه بشأن كيفية تفعيل المعايير. وفي هذا الصدد، دعت الدول إلى تبادل ونشر الممارسات الجيدة والدروس المستفادة بشأن تنفيذ المعايير. واقترحت نُهج تعاونية مختلفة، مثل قيام الدول بوضع خارطة طريق للمساعدة في جهودها في مجال التنفيذ، وكذلك إجراء دراسات استقصائية طوعية لتبادل الدروس المستفادة والممارسات الجيدة.

24 - وسلّمت الدول بأن المعايير يمكن أن تساعد على منع نشوب النزاعات في بيئة تكنولوجيا المعلومات والاتصالات، وتسهم في استخدام تكنولوجيا المعلومات والاتصالات في الأغراض السلمية والإعمال التام لها من أجل زيادة التنمية الاجتماعية والاقتصادية على الصعيد العالمي. وأبرزت الدول أن تنفيذ المعايير ينبغي ألا يؤدي إلى فرض قيود لا مبرر لها على التعاون الدولي ونقل التكنولوجيا، وألا يعوق

(9) A/RES/75/32.

(10) A/RES/73/27، الفقرة 1 من المنطوق.

الابتكار للأغراض السلمية والتنمية الاقتصادية للدول في بيئة عادلة وغير تمييزية. وشددت الدول أيضا على الروابط بين المعايير وبناء الثقة وبناء القدرات، وأكدت على ضـــرورة تعميم المنظور الجنســـاني في عملية تنفيذ المعايير.

25 - وأثناء المناقشـــات، قُدمت مقترحات لزيادة بلورة المعايير القائمة. وكررت الدول التأكيد على إيلاء نفس القدر من الاهتمام لحماية جميع البنى التحتية الحيوية التي تدعم تقديم الخدمات الأســاســية للجمهور، والتي ينبغي أن تشــمل المرافق الطبية ومرافق الرعاية الصــحية. ووجهت أيضــا الانتباه إلى أهمية التعاون لحماية البنى التحتية الحيوية التي توفر الخدمات العابرة للحدود أو الولايات الوطنية، بالنظر إلى الأثر المحتمل لأي ضـرر يصـيب هذه البنى التحتية، وأهمية كفالة توافر الإنترنت وضـمان سـلامتها بوجه عام. وأشارت الدول إلى قرار الجمعية العامة 211/64 المعنون "إرساء ثقافة عالمية تكفل أمن الفضاء الإلكتروني وتقييم الجهود الوطنية الرامية إلى حماية الهياكل الأســاســية الحيوية للمعلومات"[(11)]. وبالإضــافة إلى ذلك، اقترحت الدول أيضا زيادة ضمان سلامة سلسلة الإمداد في مجال تكنولوجيا المعلومات والاتصالات، معربة عن قلقها إزاء إنشــاء وظائف خفية ضــارة في منتجات تكنولوجيا المعلومات والاتصــالات، والمسـؤولية عن إخطار المســـتخدمين عند تحديد مواطن ضـــعف كبيرة. وأعربت الدول كذلك عن قلقها إزاء تراكم مواطن الضعف. واقترحت بعض الدول صياغة قواعد ومعايير دولية موضوعية بشأن أمن سلسلة الإمداد.

26 - وإضـــافة إلى الفقرة الواردة أعلاه، ترد مرفقة بهذا الموجز المقترحات الخطية التي قدمتها الدول في إطار الفريق العامل بشأن بلورة المعايير القائمة والتوجيهات المتعلقة بالتنفيذ، إضافة إلى المعايير الجديدة.

27 - وأشـــارت بعض الدول أيضـــا إلى الاقتراح الداعي إلى وضـــع مدونة قواعد ســـلوك دولية لأمن المعلومات، الذي قُدّم في عام 2015[(12)].

28 - وأقرت بعض الدول بالحاجة إلى تشــجيع ودعم المزيد من الجهود الإقليمية، وكذلك إقامة شــراكات مع أصحاب المصلحة الآخرين، مثل القطاع الخاص والأوساط التقنية، بشأن تنفيذ المعايير. ويمكن بناء هذه الشـراكات، على سـبيل المثال، لضـمان اسـتدامة جهود بناء القدرات لمعالجة الاختلافات في قدرات التنفيذ. وفي هذا الصـدد، أشـارت الدول إلى الفقرة 1-13 من منطوق قرار الجمعية العامة 27/73، التي تبرز، في جملة أمور، أنه "ينبغي للدول أن تشـجع القطاع الخاص والمجتمع المدني على القيام بدور مناسـب لتحسـين أمن تكنولوجيا المعلومات والاتصالات وبدور ملائم في استخدامها، بما في ذلك أمن سلسلة التوريد لمنتجات وخدمات تكنولوجيا المعلومات والاتصــالات". وأشــارت الدول إلى أهمية اتخاذ خطوات في مجالي التواصــل والتعاون لكفالة أن تضـــطلع مختلف الجهات صـــاحبة المصـــلحة، بما في ذلك القطاعان العام والخاص والمجتمع المدني، بمسؤولياتها في استخدام تكنولوجيا المعلومات والاتصالات.

تدابير بناء الثقة

29 - أشارت الدول، في مناقشاتها في إطار الفريق العامل، إلى استمرار أهمية تدابير بناء الثقة الموصى بها في تقارير فريق الخبراء الحكوميين الصـــادرة بتوافق الآراء. وسُـــلِّط الضـــوء على عدة تدابير باعتبارها تتطلب اهتماما على سـبيل الأولوية، مثل الحوار المنتظم وتبادل المعلومات الطوعي بشـأن التهديدات القائمة

(11) ترد مرفقة بهذا القرار أداة طوعية للتقييم الذاتي للجهود الوطنية الرامية إلى حماية الهياكل الأساسية الحيوية للمعلومات.

(12) A/69/723، وأشير إليه في الوثيقة A/70/174، الفقرة 12.

والناشئة، والسياسات الوطنية، والأطر أو المبادئ التشريعية، والآراء الوطنية بشأن كيفية انطباق القانون الدولي على استخدام الدول لتكنولوجيا المعلومات والاتصالات، والنُهُج الوطنية لتحديد البنية التحتية الحيوية وتصنيف الحوادث المتصلة بتكنولوجيا المعلومات والاتصالات. وأشير إلى أنه من الممكن أن يؤدي تبادل الممارسات الجيدة في النُهج المتبعة في مجال الاستدلال الرقمي الجنائي والتحقيق في الحوادث الإلكترونية الخبيثة إلى زيادة التعاون وبناء القدرات. كما تم إبراز أهمية التوصل إلى فهم مشترك للمفاهيم والمصطلحات كخطوة عملية لتعزيز التعاون الدولي وبناء الثقة. وشملت التدابير الأخرى المماثلة وضع توجيهات بشأن تنفيذ تدابير بناء الثقة، وتدريب الدبلوماسيين، وتبادل الدروس بشأن إنشاء قنوات اتصالات آمنة في الأزمات وممارستها، وتبادل الموظفين، وتمارين قائمة على سيناريوهات محتملة على مستوى السياسات، إضافة إلى تمارين تشغيلية على المستوى التقني بين أفرقة مواجهة الطوارئ الحاسوبية أو أفرقة الاستجابة لحوادث أمن الفضاء الإلكتروني. واقترح اتباع تدابير الشفافية على الصعيد الوطني، مثل تبادل الردود طوعا على الدراسات الاستقصائية للتنفيذ أو إصدار إعلانات وطنية بشأن التقيد بإطار السلوك المسؤول للدول، بوصفها سبلا أخرى لبناء الثقة والاطمئنان فيما يتعلق بنوايا الدول والتزاماتها.

30 - ومع وضع تجارب الهيئات الإقليمية في إنشاء شبكات نقاط الاتصال وصيانتها في الاعتبار، واستنادا إلى الشبكات القائمة، نوقشت جدوى إنشاء دليل عالمي مركزي لنقاط الاتصال. وفي الوقت نفسه، لوحظ أن أمن هذا الدليل وطرائقه التشغيلية سيكونان حاسمين بالنسبة لفعاليته، وكذلك تجنب وجود ترتيبات مزدوجة أو مفرطة في التفصيل. وجرى التأكيد أيضا على قيمة إجراء تمارين منتظمة داخل شبكة لنقاط الاتصال، لأنها يمكن أن تساعد في الحفاظ على الاستعداد والقدرة على الاستجابة وتكفل أن تظل دلائل نقاط الاتصال محدثة.

31 - وبما أن تدابير بناء الثقة يمكن أن توضع على المستويات الثنائية أو الإقليمية أو المتعددة الأطراف، ناقشت الدول أيضا استصواب وجدوى إنشاء مستودع عالمي لتدابير بناء الثقة تحت رعاية الأمم المتحدة، بهدف تبادل السياسات والممارسات الجيدة والتجارب والتقييمات المتعلقة بتنفيذ تدابير بناء الثقة، وتشجيع التعلم من الأقران والاستثمار في بناء القدرات. ويمكن أن يساعد هذا المستودع الدول أيضا على تحديد تدابير بناء الثقة الإضافية الملائمة لسياقها الوطني والإقليمي، وتقديم نماذج محتملة للتكيف في أماكن أخرى. ولوحظ أن أي مستودع عالمي جديد ينبغي ألا يكرر الترتيبات القائمة، وأن الطرائق التشغيلية تحتاج إلى مزيد من المناقشة.

32 - ووجهت الدول الانتباه أيضا إلى أدوار ومسؤوليات الجهات الفاعلة الأخرى، بما فيها المجتمع المدني والقطاع الخاص والأوساط الأكاديمية والأوساط التقنية، في المساهمة في بناء الثقة في استخدام تكنولوجيا المعلومات والاتصالات على الصعد الوطني والإقليمي والعالمي. ولاحظت الدول تنوع المبادرات التي تضم أصحاب مصلحة متعددين، والتي أنشأت، عن طريق وضع المبادئ والالتزامات، شبكات جديدة للتبادل والتآزر والتعاون. وفي نفس السياق، أظهرت المبادرات الخاصة بقطاعات أو مجالات محددة الوعي المتزايد بأدوار ومسؤوليات الجهات الفاعلة الأخرى والمساهمات الفريدة التي يمكن أن تقدمها في أمن تكنولوجيا المعلومات والاتصالات عن طريق الالتزامات الطوعية والمدونات المهنية والمعايير.

بناء القدرات

33 - شددت الدول، في مناقشاتها في إطار الفريق العامل، على الوظيفة الهامة التي يمكن أن يؤديها بناء القدرات في تمكين جميع الدول من المشاركة الكاملة في المناقشات الدولية بشأن إطار السلوك المسؤول للدول، مع المساهمة في الوقت ذاته في الالتزامات المشتركة مثل خطة التنمية المستدامة لعام 2030[13]. وفي هذا الصدد، شددت الدول على الحاجة إلى تخصيص موارد مالية وبشرية كافية لبرامج بناء القدرات.

34 - وأبرزت الدول العمل الهام الذي اضطلعت به جهات فاعلة أخرى في مجال بناء القدرات المتصلة بتكنولوجيا المعلومات والاتصالات، بما في ذلك المنظمات الدولية، والهيئات الإقليمية ودون الإقليمية، والمجتمع المدني، والقطاع الخاص، والأوساط الأكاديمية، والهيئات التقنية المتخصصة، وشجعت على التفكير في كيفية تعزيز التنسيق والاستدامة والفعالية والحد من الازدواجية في جميع هذه الجهود.

35 - ويتعين على الأمم المتحدة أن تؤدي دورا أساسيا في دعم الدول في إبراز أهمية بناء القدرات، ومن خلال الاستفادة من صلاحيتها للدعوة للاجتماع لحشد الدعم من أجل زيادة التنسيق بين مختلف الجهات الفاعلة النشطة في مجال بناء القدرات. واقترحت الدول أن تُستخدم المنابر القائمة داخل الأمم المتحدة ووكالاتها المتخصصة وفي المجتمع الدولي الأوسع نطاقا لتعزيز التنسيق القائم بالفعل. ويمكن استخدام هذه المنابر لتبادل الآراء الوطنية بشأن متطلبات بناء القدرات، وتشجيع تبادل الدروس والخبرات من جانب كل من متلقي الدعم ومقدميه، وتيسير الحصول على المعلومات المتعلقة ببرامج بناء القدرات وتقديم المساعدة التقنية. ويمكن لهذه المنابر أيضا أن تدعم تعبئة الموارد أو تساعد في الجمع بين الموارد المتاحة وطلبات الدعم في مجال بناء القدرات وتقديم المساعدة التقنية. وأُشير إلى أن وضع خطة عالمية لبناء القدرات السيبرانية تحت رعاية الأمم المتحدة يمكن أن يساعد على كفالة مزيد من الاتساق في جهود بناء القدرات، وأن الدراسات الاستقصائية الطوعية للتقييم الذاتي قد تساعد الدول على تحديد احتياجاتها وأولوياتها في مجال بناء القدرات أو قدرتها على تقديم الدعم.

36 - وبينما أشير إلى المسؤولية الرئيسية للدول عن الحفاظ على بيئة منيعة وآمنة وموثوق بها لتكنولوجيا المعلومات والاتصالات، جرى التأكيد أيضا على أهمية اتباع نهج متعدد أصحاب المصلحة في بناء القدرات يعالج الثغرات التقنية والسياساتية في جميع قطاعات المجتمع ذات الصلة. ولاحظت الدول على وجه الخصوص أن الاستدامة في بناء القدرات يمكن تعزيزها باتباع نهج ينطوي على المشاركة والشراكة مع المجتمع المدني المحلي والأوساط التقنية والمؤسسات الأكاديمية والجهات الفاعلة في القطاع الخاص، وعن طريق وضع قوائم ومراكز للخبراء. وفي هذا الصدد، تم التأكيد أيضا على أن النهج الوطنية إزاء أمن تكنولوجيا المعلومات والاتصالات يمكن أن تستفيد من اعتماد نهج شامل ومتعدد التخصصات في بناء القدرات يشمل عدة قطاعات، بما في ذلك عن طريق تعزيز هيئات التنسيق الوطنية بمشاركة أصحاب المصلحة ذوي الصلة لتقييم فعالية البرامج. وقد يساعد هذا النهج أيضا في التصدي للتحديات التي تطرحها التكنولوجيات الناشئة حديثا.

(13) تشمل الأمثلة على أهداف التنمية المستدامة وغاياتها ذات الصلة، على سبيل المثال لا الحصر، ما يلي: تحقيق زيادة كبيرة في فرص الحصول على تكنولوجيا المعلومات والاتصالات (9-ج)؛ وتعزيز التعاون الإقليمي والدولي بين الشمال والجنوب وفيما بين بلدان الجنوب والتعاون الثلاثي فيما يتعلق بالعلوم والتكنولوجيا والابتكار والوصول إليها (الغاية 17-6)؛ وتعزيز الدعم الدولي لتنفيذ بناء القدرات تنفيذا فعالا ومحدد الأهداف (الغاية 17-9).

37 - ووجهت الدول الانتباه إلى "الفجوة الرقمية بين الجنسين" وحثت على اتخاذ تدابير محددة على الصعيدين الوطني والدولي لمعالجة مسألة المساواة بين الجنسين والمشاركة المجدية للمرأة في المناقشات الدولية وبرامج بناء القدرات في مجال تكنولوجيا المعلومات والاتصالات والأمن الدولي، بما في ذلك من خلال جمع البيانات المصنفة حسب نوع الجنس. وأعربت الدول عن تقديرها للبرامج التي يسرت مشاركة المرأة في المناقشات المتعددة الأطراف بشأن أمن تكنولوجيا المعلومات والاتصالات. وجرى التأكيد أيضا على ضرورة تعزيز الروابط بين هذا الموضوع وخطة الأمم المتحدة المتعلقة بالمرأة والسلام والأمن.

38 - ولاحظت الدول أن هناك عقبات كثيرة تعوق فعالية بناء القدرات أو تحد منها. وسُلط الضوء على عدم كفاية التنسيق والتكامل في تحديد وتنفيذ جهود بناء القدرات باعتبار ذلك من الشواغل الهامة. وأثارت الدول أيضا شواغل عملية تتعلق بتحديد الاحتياجات في مجال بناء القدرات، وحسن توقيت تلبية طلبات المساعدة في مجال بناء القدرات، وكذلك فيما يتعلق بتصميم أنشطة بناء القدرات وتنفيذها واستدامتها وإمكانية الوصول إليها، وعدم وجود مقاييس محددة لقياس أثرها. وفي سياقات كثيرة، يعوق عدم كفاية الموارد البشرية والمالية والتقنية جهود بناء القدرات والتقدم في تضييق الفجوة الرقمية. وبمجرد إتمام بناء القدرات، تواجه بعض البلدان التحدي المتمثل في الاحتفاظ بالمواهب في سوق تنافسية للمهنيين في مجال تكنولوجيا المعلومات والاتصالات. وذكرت الدول أن عدم إمكانية الوصول إلى التكنولوجيات المتصلة بأمن تكنولوجيا المعلومات والاتصالات يمثل مشكلة أيضا.

الحوار المؤسسي المنتظم

39 - أشارت الدول، في مناقشاتها في إطار الفريق العامل، إلى ولاية الفريق في قرار الجمعية العامة 27/73 المتمثلة في دراسة إمكانية إقامة حوار مؤسسي منتظم، وأكدت أن تقييمات الفريق وتوصياته في هذا الصدد ستكون نتيجة رئيسية لعمله.

40 - وأعربت الدول عن طائفة من الآراء بشأن الأهداف التي ينبغي أن تكون لها الأولوية في الحوار المؤسسي المنتظم في المستقبل، والشكل الذي يمكن أن يدعم فيه الحوار المنتظم هذه الأهداف على أفضل نحو. وأعربت بعض الدول عن رغبتها في إجراء حوار منتظم لتحديد أولويات تنفيذ الالتزامات والتوصيات القائمة، بما في ذلك وضع توجيهات لدعم ورصد تنفيذها؛ وتنسيق وتعزيز فعالية بناء القدرات؛ وتحديد الممارسات الجيدة وتبادلها. وأعربت دول أخرى عن رغبتها في أن تكون الأولوية في الحوار المنتظم هي مواصلة تطوير الالتزامات القائمة ووضع التزامات إضافية، بما في ذلك التفاوض على صك ملزم قانونا والهياكل المؤسسية لدعمه.

41 - وقدمت بعض الدول اقتراحا محددا بشأن وضع برنامج عمل للارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني بهدف إنشاء منتدى دائم للأمم المتحدة للنظر في استخدام الدول لتكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي. واقتُرح أن يشكل برنامج العمل التزاما سياسيا من جانب الدول بالتوصيات والمعايير والمبادئ المتفق عليها؛ وأن يدعو إلى عقد اجتماعات منتظمة تركز على التنفيذ؛ ويعزز التعاون وبناء القدرات فيما بين الدول؛ ويعقد مؤتمرات استعراضية منتظمة. ومن المتوقع أيضا أن تكون ثمة مشاركة ومشاورات واسعة النطاق في إطار مقترح برنامج العمل.

42 - وأشارت الدول إلى إنشاء فريق عامل جديد مفتوح العضوية معني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025، بموجب القرار 240/75 المؤرخ 31 كانون الأول/ديسمبر 2020، سيبدأ أنشطته عند اختتام أعمال الفريق العامل المفتوح باب العضوية المنشأ عملا بالقرار 27/73 وسينظر في نتائجه.

43 - وأعربت الدول أيضاً عن رغبتها في أن يعود المجتمع الدولي في نهاية المطاف إلى عملية واحدة قائمة على توافق الآراء برعاية الأمم المتحدة. وفي هذا الصدد، لاحظت الدول أن مختلف الأشكال المقترحة للحوار ليست متنافية بالضرورة. واقتُرح أن تكون الأشكال المختلفة متكاملة، أو أن تدمج للاستفادة من السمات الفريدة لكل منها والحد من ازدواجية الجهود.

44 - وبالإضافة إلى ذلك، أثيرت أيضا الحاجة إلى مواصلة النظر في مدة الحوار المقبل واستدامته، وما إذا كان ينبغي أن يكون ذا طابع تداولي أو عملي المنحى، وتوقيته، والأماكن المحتملة لإجرائه، واعتبارات الميزانية.

45 - وأكدت الدول، مع التسليم بالدور الفريد للدول ومسؤوليتها فيما يتعلق بالأمن الوطني والدولي، على ما لتحلي الجهات الفاعلة الأخرى بسلوك مسؤول من مساهمة هامة في تهيئة بيئة لتكنولوجيا المعلومات والاتصالات تكون مفتوحة ومأمونة وميسَّرة وسلمية. وفي هذا الصدد، أشير إلى أنه يمكن تيسير بناء بيئة لتكنولوجيا المعلومات والاتصالات أكثر أمنا وقدرة على الصمود من خلال زيادة التعاون والشراكات بين أصحاب المصلحة المتعددين.

مرفق لموجز الرئيس

مقترحات صـــياغات محددة في إطار بند جدول الأعمال "القواعد والمعايير والمبادئ" واردة في الإفادات الخطية المقدمة من الوفود

يلاحظ أن وفودا كثيرة أشارت، في مساهماتها الخطية، إلى المعايير القائمة، لذا لا يتضمن ما يلي سوى مقترحات الصياغات الإضافية.

أرمينيا

- تمتنع الدول عن اتخاذ أي إجراء قد يؤدي إلى محاولة تعطيل ســـلامة البنى التحتية الحيوية والأنشطة الحكومية، وتقدم من خلال قنوات آمنة توضيحات في الوقت المناسب للحيلولة دون تزايد احتمال التصعيد.

أستراليا وإستونيا والجمهورية التشيكية وكازاخستان والولايات المتحدة الأمريكية واليابان

نص يتضمن توجيهات بشأن تنفيذ معياري عام 2015، 13 (و) و (ز)

- ينبغي للدول، عند تقديمها توجيهات لتنفيذ هذين المعيارين، أن تشير إلى أن التركيز على قطاعات معينة بوصفها بنى تحتية حيوية لا يقصد به أن تلك القطاعات تشكل قائمة حصرية، وهو لا يؤثر على تعيين أو عدم تعيين أي قطاع آخر على الصـعيد الوطني، كما أنه لا يؤيد ضـمناً أي نشـاط ضار ضد فئة غير محددة.
- وقد وضـــع الفريق العامل تقريره في ســياق جائحة كوفيد-19. وفي ظل هذه الظروف، أكد الفريق العامل أن جميع الدول تعتبر الخدمات الطبية والمرافق الطبية بمثابة بنى تحتية حيوية لأغراض المعيارين (و) و (ز).

بيلاروس

- ينبغي للدول أن تعيد تأكيد التزاماتها بمبدأ التخلي عن عســكرة تكنولوجيا المعلومات والاتصـــالات القائمة وعن إنشـاء تكنولوجيا جديدة للمعلومات والاتصـالات مصـممة خصـيصـاً للإضـرار بموارد المعلومات والبنى التحتية والمرافق الحيوية للبلدان الأخرى.

كندا

نص التوجيهات المتعلقة بالمعايير المقترح إدراجه في الفقرة 41

في حين أن معايير فريق الخبراء الحكوميين لعام 2015 تبين الإجراءات التي ينبغي للدول اتخاذها أو عدم اتخاذها، أكدت الدول على الحاجة إلى توجيهات بشأن كيفية تفعيل هذه المعايير، وقدمت التوجيهات التالية بشـأنها. ووفقاً لفهم الفريق العامل المفتوح العضـوية، لا تخل المعايير والتوجيهات بالحقوق والالتزامات القائمة للدول بموجب القانون الدولي، ولا تغيرها أو تنتقص منها بأي شكل من الأشكال.

أ - ينبغي للدول، بما يتفق ومقاصد الأمم المتحدة، بما فيها مقصد صون السلام والأمن الدوليين، أن تتعاون في وضع وتطبيق تدابير لزيادة استقرار وأمن استخدام تكنولوجيات المعلومات والاتصالات ولمنع ما يتصل بتلك التكنولوجيات من ممارسات يسلَّم بأنها ضارة أو قد تشكل تهديدات للسلام والأمن الدوليين؛ (الفقرة 13 (أ) من تقرير عام 2015).

'1' هذا المعيار عام في طبيعته. وسيسهم تنفيذ المجموعة الكاملة من المعايير، فضلا عن التوجيهات المحددة الواردة أدناه، في مواصلة تفعيل هذا المعيار. وينبغي أن تتخذ الدول نهجا تعاونيا في العمل فيما بينها ومع أصحاب المصلحة غير الحكوميين، بما في ذلك الصناعة والأوساط الأكاديمية والمجتمع المدني.

'2' وينبغي للدول، لكي تفعل ذلك، أن تقوم، حسب الاقتضاء وحيثما يمكن، بما يلي:

- اعتماد وتنفيذ استراتيجيات وطنية شاملة للأمن السيبراني. وينبغي لهذه الاستراتيجيات أن تعزز التعاون الدولي حيثما أمكن في مجال الأمن السيبراني.
- إنشاء وصيانة وظائف للتصدي للحوادث، مثل أفرقة مواجهة الطوارئ الحاسوبية على سبيل المثال، التي تستطيع تولي التنسيق وتبادل الممارسات الجيدة والتعاون في مواجهة حوادث تكنولوجيا المعلومات والاتصالات.
- نشر بيانات تفيد بأنها ستعمل وفقاً لإطار السلوك المسؤول للدول في مجال الفضاء الإلكتروني، على النحو المبين في تقرير فريق الخبراء الحكوميين للأمم المتحدة لعام 2015.
- المشاركة في المبادرات الإقليمية والثنائية الرامية إلى وضع وتنفيذ تدابير بناء الثقة.

'3' وينبغي تشجيع الدول الأعضاء على تجميع وتبسيط المعلومات التي تقدمها بشأن تنفيذها للمعايير المقبولة.

ب - ينبغي للدول، في حالة وقوع حوادث في مجال تكنولوجيا المعلومات والاتصالات، أن تنظر في جميع المعلومات ذات الصلة، بما في ذلك في إطار السياق الأوسع نطاقا للحادث، والتحديات المرتبطة بعزو المسؤولية عن الحادث في بيئة تكنولوجيا المعلومات والاتصالات، وطبيعة نتائج الحادث ومداها (الفقرة 13 (ب) من تقرير عام 2015).

'1' يمكن للدول أن تنشئ الهياكل والسياسات والعمليات وآليات التنسيق الوطنية اللازمة لتيسير النظر بعناية في الحوادث الخطيرة المتعلقة بتكنولوجيا المعلومات والاتصالات وتحديد الاستجابات المناسبة.

'2' وبمجرد أن يتم وضع هذه الهياكل والعمليات، يمكن للدول أن تضع نماذج لتقييم حوادث تكنولوجيا المعلومات والاتصالات أو تحديد مدى فداحتها بهدف تقييم حوادث تكنولوجيا المعلومات والاتصالات.

'3' ويمكن أن يضمن توخي المنظمات الإقليمية الشفافية بشأن هذه النماذج وقيامها بالمواءمة بينها وجود قواسم مشتركة في كيفية نظر الدول في حوادث تكنولوجيا المعلومات والاتصالات وتحسين التواصل فيما بينها. وينبغي أن تتماشى النماذج، حيثما أمكن، مع الممارسات القائمة، وتجنب الازدواجية فيها.

‘4’ وعند النظر في جميع المعلومات ذات الصلة في حالة وقوع حادث من حوادث تكنولوجيا المعلومات والاتصالات، ينبغي للدول أن تجري بحوثاً عن الآثار الجنسانية المحتملة، وأن تعمل بشكل شامل مع جميع أصحاب المصلحة لفهم السياق الأوسع للحادث، بما في ذلك تأثيره على تمتع المثليات والمثليين ومزدوجي الميل الجنسي ومغايري الهوية الجنسانية والنساء بحقوقهم.

‘5’ وينبغي للدول أن تنظر في أثر حوادث تكنولوجيا المعلومات والاتصالات على حقوق الإنسان، بما في ذلك الحق في حرية التعبير وتكوين الجمعيات والتجمع السلمي، والحق في حماية الخصوصية من التدخل التعسفي أو غير القانوني، فضلاً عن حقوق الأشخاص ذوي الإعاقة.

‘6’ وينبغي أن تدرك الدول أن تدابير مواجهة الحوادث الأمنية تتطلب في كثير من الأحيان مشاركة مختلف أصحاب المصلحة، وليس فقط أفرقة مواجهة الطوارئ الحاسوبية/أفرقة الاستجابة لحوادث أمن الفضاء الإلكتروني الوطنية، وتحسين التعاون من خلال التدريب وبناء القدرات مع جميع مجموعات أصحاب المصلحة. وينبغي للدول أن تشجع التدريب على الأمن الرقمي وغير ذلك من بناء القدرات والمساعدة من جانب أصحاب المصلحة، بما في ذلك المجتمع المدني، بهدف منع وقوع حوادث أمنية، ولا سيما على مستوى المجتمعات الضعيفة والمستخدمين الآخرين المعرضين للخطر.

ج – ينبغي للدول ألا تسمح، عن علم، باستخدام إقليمها لارتكاب أفعال غير مشروعة دولياً باستخدام تكنولوجيات المعلومات والاتصالات (الفقرة 13 (ج) من تقرير عام).

‘1’ فيما يتعلق بتنفيذ هذا المعيار:

- إذا حددت دولة ما نشاطاً خبيثاً في الفضاء الإلكتروني ينبثق من إقليم دولة أخرى أو من بنيتها التحتية السيبرانية، يمكن اتخاذ خطوة أولى تتمثل في إخطار تلك الدولة. وتعد أهمية أفرقة مواجهة الطوارئ الحاسوبية حاسمة لتوفير القدرة على تحديد هذا النشاط.
- بما أن حوادث تكنولوجيا المعلومات والاتصالات يمكن أن تنشأ عن دول ثالثة أو أن تشملها، فمن المفهوم أن إخطار دولة ما لا يعني ضمناً مسؤولية تلك الدولة عن الحادث.
- ينبغي للدولة التي تم إخطارها أن تعترف باستلام الطلب عن طريق نقطة الاتصال الوطنية المعنية.
- عندما تكون دولة ما على علم باستخدام إقليمها أو بنيتها التحتية السيبرانية لارتكاب فعل غير مشروع دولياً عن طريق استخدام تكنولوجيا المعلومات والاتصالات وأنه من المرجح أن تترتب على هذا الفعل عواقب وخيمة في دولة ثانية، ينبغي للدولة الأولى أن تسعى إلى اتخاذ تدابير معقولة ومتاحة وعملية داخل إقليمها وضمن قدراتها، بما يتفق مع التزاماتها بموجب القانون المحلي والدولي، للعمل على وقف الفعل غير المشروع دولياً، أو للتخفيف من عواقبه.
- قد تعلم دولة ما بهذا الفعل عقب إخطار من إحدى الدول المتأثرة. ويجب أن يتم هذا الإخطار بحسن نية وأن يكون مصحوبا بمعلومات داعمة. وقد تتضمن المعلومات الداعمة إتاحة مؤشرات الاختراق المحتملة، مثل عنوان بروتوكول الإنترنت وأجهزة الحاسوب المستخدمة في أعمال تكنولوجيا المعلومات والاتصالات الخبيثة ومعلومات البرامجيات الضارة.

- ينبغي تشجيع الدول على ضمان منع الجهات من غير الدول، بما في ذلك القطاع الخاص، من القيام بأنشطة خبيثة في مجال تكنولوجيا المعلومات والاتصالات لأغراضها الخاصة أو لأغراض الدولة أو غيرها من الجهات من غير الدول، وذلك على حساب أطراف ثالثة، بما فيها تلك الموجودة في إقليم دولة أخرى. ويمكن تحقيق هذا الهدف بالعمل مع القطاع الخاص لتحديد الإجراءات المسموح بها باستخدام نهج قائم على المخاطر، واستحداث أدوات ملموسة أي عمليات التصديق، وأدلة أفضل الممارسات، وآليات التصدي للحوادث، وحسب الاقتضاء، اللوائح الوطنية.

- ينبغي ألا يفسر هذا المعيار على أنه يتطلب من الدولة أن ترصد بصورة استباقية جميع تكنولوجيات المعلومات والاتصالات داخل أراضيها، أو أن تتخذ خطوات وقائية أخرى.

'2' وقد تختار الدولة التي تعلم بأنشطة ضارة في مجال تكنولوجيا المعلومات والاتصالات نابعة من إقليمها والتي تفتقر إلى القدرة على الاستجابة التماس المساعدة من دول أخرى، بما في ذلك عن طريق نماذج موحدة لطلب المساعدة.

- في مثل هذه الحالات، يجوز التماس المساعدة من دول أخرى، أو من كيان من القطاع الخاص، وينبغي أن يتم ذلك، في حال تقديم المساعدة، بطريقة تتفق مع القانون الوطني والقانون الدولي لحقوق الإنسان.

د - ينبغي للدول أن تنظر في أفضل سبل التعاون على تبادل المعلومات، ومساعدة بعضها البعض، ومحاكمة المسؤولين عن استخدام تكنولوجيات المعلومات والاتصالات لأغراض إرهابية وإجرامية، وتنفيذ تدابير تعاونية أخرى للتصدي لهذه التهديدات. وقد تحتاج الدول إلى النظر فيما إذا كان من الضروري وضع تدابير جديدة في هذا الصدد. (الفقرة 13 (د) من تقرير عام 2015).

'1' عند تنفيذ هذه المعيار، ينبغي للدول أن تقوم بما يلي:

- النظر، حسب الاقتضاء، في دعم عمل لجنة الأمم المتحدة لمنع الجريمة والعدالة الجنائية، بسبل منها تجديد ولاية فريق الخبراء الحكومي الدولي المفتوح العضوية، ودعم الجهود الجارية التي يبذلها من أجل أن يدرس، بطريقة شاملة، مشكلة الجريمة السيبرانية.

- دعم جهود مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة من أجل أن يواصل تزويد الدول الأعضاء، بناء على طلبها ووفقاً لاحتياجاتها الوطنية، بمساعدات تقنية وبرامج لبناء القدرات المستدامة على التصدي للجريمة السيبرانية، من خلال البرنامج العالمي المعني بالجريمة السيبرانية وعن طريق مكاتبه الإقليمية وغيرها، ابتغاء منع الجريمة السيبرانية بكل أشكالها والكشف عنها والتحقيق فيها وملاحقة مرتكبيها، مع التسليم بأن التعاون مع الدول الأعضاء والمنظمات الدولية والإقليمية ذات الصلة والقطاع الخاص والمجتمع المدني والجهات ذات الصلة صاحبة المصلحة الأخرى من شأنه أن يُيسِّر هذا النشاط.

- تنفيذ التدابير القائمة بطريقة تتسق مع التزاماتها والنظر في اتخاذ تدابير جديدة، مثل اعتماد تشريعات وطنية لمكافحة الجريمة السيبرانية، بطريقة تتسق مع التزامات الدول في مجال حقوق الإنسان وتكفل الضمانات القضائية.

هـ - ينبغي للدول، في سعيها لكفالة الاستخدام الآمن لتكنولوجيات المعلومات والاتصالات، أن تلتزم بقراري لجنة حقوق الإنسان A/HRC/RES/20/8 و A/HRC/RES/26/13 بشأن تعزيز وحماية حقوق الإنسان على الإنترنت والتمتع بها، وقراري الجمعية العامة A/RES/68/167 و A/RES/69/166 (الحق في الخصوصية في العصر الرقمي)، لضمان الاحترام الكامل لحقوق الإنسان، بما في ذلك الحق في حرية التعبير. (الفقرة 13 (هـ) من تقرير عام 2015)

'1' ينبغي للدول أن تقوم بما يلي:

- الامتثال للالتزامات الواقعة عليها بموجب القانون الوطني والقانون الدولي، عند النظر في السياسات أو التشريعات الوطنية المتعلقة بالأمن السيبراني أو وضعها أو تطبيقها أو عند إعداد مبادرات أو هياكل تتعلق بالأمن السيبراني وتنفيذها، بما يشمل اتخاذ التدابير اللازمة لضمان حماية جميع حقوق الإنسان.

- وينبغي للدول، وهي تقوم بذلك، أن تدمج وجهات نظر جميع أصحاب المصلحة ذوي الصلة والمتأثرين في المراحل الأولى من وضع السياسات المتعلقة بالأمن السيبراني وتنفيذها من أجل أن تضمن النظر من منظور كلي في الآثار المترتبة على هذه التدابير.

- وتكتسي مشاركة المجتمع المدني أهمية خاصة بالنظر إلى دوره كعنصر فاعل رئيسي في تعزيز امتثال الدولة لواجباتها والتزاماتها في مجال حقوق الإنسان.

- وينبغي للدول أن تراعي بأن الأفراد يتمتعون بالحقوق نفسها داخل شبكة الإنترنت وخارجها، وأن تأخذ في الاعتبار التهديدات المتباينة التي قد تواجه النساء والأفراد المنتمين إلى الأقليات والفئات الضعيفة في سياق حقوق الإنسان.

- الاضطلاع بعمليات مراجعة جنسانية لسياسات الأمن السيبراني الوطنية أو الإقليمية لتحديد المجالات التي تحتاج إلى تحسين.

- النظر في أن تدمج تدابير ترمي إلى معالجة آثار تكنولوجيات المعلومات والاتصالات على حقوق الإنسان في خطط عملها الوطنية المتعلقة بالأعمال التجارية وبحقوق الإنسان.

و - ينبغي لأي دولة ألا تمارس أو تدعم عن علم أنشطة في مجال تكنولوجيا المعلومات والاتصالات تتعارض مع التزاماتها بموجب القانون الدولي وتضر عن قصد بالبنية التحتية الحيوية أو تعطل، بأي شكل آخر، استخدام وتشغيل البنية التحتية الحيوية المستخدمة في تقديم الخدمات إلى الجمهور. (الفقرة 13 (و) من تقرير عام 2015).

'1' تحدد كل دولة البنى التحتية أو القطاعات التي تعتبرها حيوية، وفقا للأولويات الوطنية وأساليب تصنيف البنى التحتية الحيوية. ويمكن أن تشمل الأمثلة على قطاعات البنى التحتية الحيوية التي توفر الخدمات العامة الأساسية المؤسسات المعنية بالطاقة والمياه والصرف الصحي والصحة والتعليم والمالية والنقل والاتصالات السلكية واللاسلكية والتصدي للأزمات. ويمكن أن تشمل البنى الحيوية أيضا البنى التحتية التقنية الضرورية لإجراء الانتخابات أو الاستفتاءات بأنواعها، والبنى التحتية التقنية الضرورية لتوافر الإنترنت وضمان سلامتها بوجه عام. وإبراز هذه البنى التحتية

كأمثلة لا يمنع الدول بأي حال من تعيين بنى تحتية أخرى باعتبارها حيوية، ولا يمثل أيضا تأييدا لأي نشاط خبيث يستهدف فئات البنى التحتية الحيوية غير المحددة أعلاه.

’2‘ ينبغي للدول أن تنظر فيما يحتمل أن يترتب على أنشطة تكنولوجيا المعلومات والاتصالات التي تضطلع بها من آثار ضارة على البنى التحتية التقنية الضرورية لتوافر الإنترنت أو سلامتها بوجه عام.

ز - ينبغي للدول أن تتخذ التدابير المناسبة لحماية البنى التحتية الحيوية من التهديدات المتصلة بتكنولوجيا المعلومات والاتصالات وفقاً لقرار الجمعية العامة 199/58 بشأن إرساء ثقافة عالمية للأمن السيبراني وحماية البنى التحتية للمعلومات، والقرارات الأخرى ذات الصلة (الفقرة 13 (ز) من تقرير عام 2015).

’1‘ من أجل المساهمة في إرساء ثقافة عالمية للأمن السيبراني، ينبغي للدول أن تنظر، حسب الاقتضاء، في تبادل المعلومات بشأن أفضل الممارسات لحماية البنى التحتية الحيوية، بما في ذلك جميع العناصر المحددة في هذا القرار، وبشأن ما يلي:

- المتطلبات الأمنية الأساسية؛
- إجراءات الإخطار بالحوادث؛
- أدوات التعامل مع الحوادث ومنهجياته؛
- القدرة على الصمود في حالات الطوارئ؛
- الدروس المستفادة من الحوادث السابقة.

’2‘ ينبغي أن تتخذ تدابير بناء القدرات وغيرها من التدابير الرامية إلى إرساء ثقافة عالمية للأمن السيبراني بطريقة شاملة للجميع وأن يتوخى منها معالجة الأبعاد الجنسانية للأمن السيبراني.

’3‘ بالنظر إلى الطبيعة المتنوعة والموزعة لملكية البنى التحتية الحيوية، ينبغي للدول أن تقوم، حسب الاقتضاء، وبالتشاور مع أصحاب المصلحة ذوي الصلة، بتعزيز المعايير الدنيا لأمن البنى التحتية الحيوية وتعزيز التعاون مع القطاع الخاص والأوساط الأكاديمية والأوساط التقنية في جهود حماية البنى التحتية الحيوية.

’4‘ ينبغي للدول أن تشارك، حسب الاقتضاء، في مبادرات التخطيط للتقييم الطوعي للمخاطر واستمرارية تصريف الأعمال (القدرة على الصمود والإنعاش والطوارئ) التي تشمل أصحاب المصلحة الآخرين، وتهدف إلى تعزيز أمن البنى التحتية الحيوية التي تقدم خدمات على الصعيد الإقليمي أو الدولي وقدرتها على الصمود أمام التهديدات القائمة والناشئة.

’5‘ ينبغي بذل الجهود لحماية البنى التحتية الحيوية للمعلومات مع إيلاء الاعتبار الواجب للقوانين الوطنية المنطبقة فيما يتعلق بحماية الخصوصية والتشريعات الأخرى ذات الصلة.

’6‘ ينبغي للدول، عند تقديمها التوجيهات بشأن تنفيذ المعيارين (و) و (ز)، أن تلاحظ أن إبراز قطاعات معينة بوصفها بنى تحتية حيوية لا يُقصَد به أن يشكل قائمة حصرية، ولا يؤثر على

تعيين أو عدم تعيين أي قطاع آخر على الصعيد الوطني، ولا يؤيد ضمنا أي نشاط خبيث ضد فئة غير محددة.

’7‘ أكد الفريق العامل المفتوح العضوية أن جميع الدول تعتبر البنى التحتية للرعاية الصحية والخدمات والمرافق الطبية بنى تحتية حيوية لأغراض المعيارين (و) و (ز). وبرزت بشدة الحاجة إلى تأكيد حماية البنى التحتية الصحية بشكل خاص بالنظر إلى أن الفريق وضع تقريره في سياق جائحة كوفيد-19.

ح - ينبغي أن تستجيب الدول لطلبات المساعدة المناسبة المقدمة من الدول الأخرى التي تتعرض بناها التحتية الحيوية لأفعال ضارة في مجال تكنولوجيا المعلومات والاتصالات. وينبغي للدول أيضا أن تستجيب للطلبات المناسبة المقدمة للتخفيف من آثار الأنشطة الضارة في مجال تكنولوجيا المعلومات والاتصالات، المنبثقة من إقليمها، والتي تستهدف البنى التحتية الحيوية لدول أخرى، مع إيلاء الاعتبار الواجب لحقوق السيادة (الفقرة 13 (ح) من تقرير عام 2015.

’1‘ يشمل تنفيذ هذا المعيار النظر في الطلبات المناسبة للحصول على المساعدة والنظر في طبيعة المساعدة التي يمكن تقديمها في الوقت المناسب. وينبغي للدول التي تتلقى طلبا ملائما للمساعدة بعد حادث من حوادث تكنولوجيا المعلومات والاتصالات أن تنظر، حيثما كان ممكنا ومعقولا وملائما، في القيام بالآتي:

- الإقرار باستلام الطلب عن طريق نقطة الاتصال الوطنية المعنية؛
- البت، في الوقت المناسب، فيما إذا كانت لديها القدرة والموارد اللازمة لتقديم المساعدة المطلوبة. وقد يشمل ذلك تحديد الخبرات المتاحة في البلد من مجموعة متنوعة من أصحاب المصلحة؛
- الإشارة، في الرد الأولي، إلى طبيعة المساعدة التي يمكن توفيرها ونطاقها وشروطها، بما في ذلك الإطار الزمني لتقديمها؛
- في حالة الاتفاق على المساعدة، توفير المساعدة المتفق عليها على وجه السرعة؛
- ضمان أن تكون طلبات المساعدة، بما يشمل العمليات والموارد ذات الصلة مثل الأطر والنماذج، والردود متسقة مع الالتزامات المتعلقة بحقوق الإنسان.

’2‘ من شأن تنفيذ هذا المعيار أن يتيسر أكثر من خلال الوجود السابق للهياكل والآليات الوطنية، ومنها نقطة الاتصال الوطنية ونماذج طلبات المساعدة وتأكيد المساعدة المقرر توفيرها، ومن خلال أنشطة بناء القدرات والمساعدة التقنية المحددة الهدف. ويمكن أن تؤدي مبادرات التعاون الثنائي والمتعدد الأطراف والمنظمات والمنتديات الدولية والإقليمية دوراً في تيسير تطوير هذه الهياكل والأنشطة.

والنُهُج التي يمكن أن تسهم بشكل إيجابي في تنفيذ هذا المعيار يمكن أن تشمل: زيادة التعاون بين القطاعين العام والخاص ومنظمات المجتمع المدني، على الصعيدين الوطني والدولي، وخاصة من أجل اتخاذ الإجراءات الوقائية؛ وتحسين قدرة أفرقة التصدي للحوادث من خلال نهج مصمم خصيصا لتطوير

القدرات المتعلقة بالفضاء الإلكتروني؛ والتدريب المتخصص لبناء هذه القدرات على جميع مستويات الدول وعلى نطاق المجتمع.

ط - ينبغي للدول أن تتخذ الخطوات المعقولة لضمان سلامة سلسلة الإمداد بما يشعر المستعملين النهائيين بالثقة في منتجات تكنولوجيا المعلومات والاتصالات. وينبغي للدول أن تسعى إلى منع انتشار أدوات وتقنيات تكنولوجيا المعلومات والاتصالات الخبيثة ومنع استخدام الوظائف الخفية الضارة لهذه الأدوات والتقنيات (الفقرة 13 (ط) من تقرير عام 2015).

'1' من أجل تنفيذ هذه المعيار، ينبغي للدول أن تقوم بالآتي:

- اتخاذ خطوات، عبر سبل منها المنتديات القائمة، لمنع انتشار الأدوات والتقنيات الخبيثة في مجال تكنولوجيا المعلومات والاتصالات. وينبغي للدول، وهي تقوم بذلك، أن تشجع ما تمارسه الدوائر البحثية، والأوساط الأكاديمية، والصناعة، ووكالات إنفاذ القانون، وأفرقة مواجهة الطوارئ الحاسوبية/أفرقة الاستجابة لحوادث الأمن السيبراني وغيرها من الوكالات المعنية بحماية الفضاء الإلكتروني من أنشطة مشروعة في إطار ضمان أمن نظم تكنولوجيا المعلومات والاتصالات الخاصة بها؛
- النظر في تبادل المعلومات بشأن نقاط الضعف في تكنولوجيا المعلومات والاتصالات و/أو الخاصيات الضارة الخفية في منتجاتها؛
- العمل على تطبيق الضوابط الأمنية، القائمة على إدارة المخاطر.

ي - ينبغي للدول تشجيع الإبلاغ المسؤول عن نقاط الضعف المرتبطة بتكنولوجيا المعلومات والاتصالات وتبادل المعلومات ذات الصلة عن العلاجات المتاحة لنقاط الضعف هذه بغرض الحد من التهديدات المحتملة لتكنولوجيات المعلومات والاتصالات والهياكل المعتمدة على تكنولوجيا المعلومات والاتصالات وربما القضاء على هذه التهديدات (الفقرة 13 (ي) من تقرير عام 2015).

'1' من أجل تنفيذ هذه المعيار، ينبغي للدول أن تقوم بالآتي:

- إنشاء هياكل وطنية تتيح الإبلاغ عن نقاط الضعف في تكنولوجيا المعلومات والاتصالات والتعامل معها بطريقة مسؤولة؛
- تشجيع آليات التنسيق الملائمة بين كيانات القطاعين العام والخاص؛

'2' بالإضافة إلى ذلك، ولتجنب حالات سوء التفاهم أو سوء التفسير، بما فيها الحالات التي تنجم عن عدم الكشف عن المعلومات حول نقاط الضعف المحتمل أن تكون ضارة في تكنولوجيا المعلومات والاتصالات، تُشجَّع الدول على تبادل المعلومات التقنية، حسب الاقتضاء، وعلى أوسع نطاق ممكن، بشأن الحوادث الخطيرة المتعلقة بتكنولوجيا المعلومات والاتصالات، باستخدام الآليات القائمة للتنسيق فيما بين أفرقة مواجهة الطوارئ الحاسوبية وكذلك الآليات التي تنشئها

المنظمات الإقليمية (مثل شـــبكات نقاط الاتصـــال). وينبغي للدول أن تكفل التعامل مع هذه المعلومات بطريقة مسؤولة وبالتنسيق مع أصحاب المصلحة الآخرين، حسب الاقتضاء.

ك –	لا ينبغي للدول أن تمارس أو تدعم عن علم أي نشـــاط يضـــر بنظم المعلومات الخاصـــة بأفرقة التصـــدي للطوارئ المأذون بها (والتي تعرف أحيانا بأفرقة التصـــدي للطوارئ الحاســـوبية أو أفرقة الاستجابة لحوادث أمن الفضاء الإلكتروني) لأي دول أخرى. ولا ينبغي لأي دولة أن تستخدم أفرقة الاســـتجابة للطوارئ المأذون بها للمشـــاركة في أنشـــطة دولية ضـــارة. (الفقرة 13 (ك) من تقرير عام 2015).

الصين

- ينبغي للدول أن تتعهد بعدم اســـتخدام تكنولوجيا المعلومات والاتصـــالات وشـــبكاتها في ممارســـة أنشطة تتعارض مع مهمة صون السلام والأمن الدوليين.

سيادة الدولة في الفضاء الإلكتروني

- ينبغي للدول أن تمارس ولايتها على البنى التحتية لتكنولوجيا المعلومات والاتصـــالات ومواردها، وكذلك على الأنشطة المتعلقة بها في نطاق إقليمها.
- وللدول الحق في مواءمة السياسات العامة في مجال تكنولوجيا المعلومات والاتصالات مع الظروف الوطنية لإدارة شؤونها في هذا المجال وحماية المصالح المشروعة لمواطنيها في الفضاء الإلكتروني.
- ينبغي للدول أن تمتنع عن استخدام تكنولوجيا المعلومات والاتصالات للتدخل في الشؤون الداخلية للدول الأخرى وتقويض استقرارها السياسي والاقتصادي والاجتماعي.
- ينبغي أن تشارك الدول في إدارة موارد الإنترنت الدولية وتوزيعها على قدم المساواة.

حماية البنى التحتية الحيوية

- للدول حقوق وعليها مســـؤوليات فيما يتعلق بالحماية القانونية لبناها التحتية الحيوية لتكنولوجيا المعلومات والاتصالات من الأضرار الناجمة عن التهديدات والتدخل والاعتداء والتخريب.
- ينبغي أن تلتزم الدول بالامتناع عن شـــن هجمات إلكترونية على البنى التحتية الحيوية في الدول الأخرى.
- ينبغي للدول ألا تستغل ما تتمتع به من مزايا سياساتية وتقنية كي تقوض أمن البنى التحتية الحيوية للدول الأخرى وسلامتها.
- ينبغي للدول أن تزيد من عمليات تبادل الآراء بشأن المعايير وأفضل الممارسات فيما يتعلق بحماية البنى التحتية الحيوية وأن تشجع المؤسسات على الشروع في هذه العمليات.

أمن البيانات

- ينبغي للدول أن تتَّبع نهجا متوازنا فيما يتعلق بالتطور التقني، وتنمية الأعمال، وحماية الأمن الوطني والمصالح العامة.
- للدول الحق في كفالة أمن المعلومات الشخصية والبيانات الهامة ذات الصلة بأمنها القومي وأمنها العام وأمنها الاقتصادي واستقرارها الاجتماعي وهي المسؤولة عن ذلك.
- لا يجوز للدول أن تمارس أو تدعم التجسس بوسائل تكنولوجيا المعلومات والاتصالات على دول أخرى، بما في ذلك المراقبة الجماعية وسرقة البيانات والمعلومات الشخصية الهامة.
- ينبغي للدول أن تولي لكل من التنمية والأمن نفس القدر من الاهتمام، وأن تحفز تدفق البيانات بشكل قانوني ومنظم وحر. وينبغي للدول أن تيسر تبادل أفضل الممارسات والتعاون في هذا الصدد.

أمن سلسلة الإمداد

- ينبغي للدول ألا تستغل مركزها المهيمن في مجال تكنولوجيا المعلومات والاتصالات، بما يشمل الهيمنة فيما يتعلق بالموارد والبنى التحتية الحيوية والتكنولوجيات الأساسية والسلع والخدمات في هذا المجال لتقويض حق الدول الأخرى في التحكم المستقل في سلع تكنولوجيا المعلومات والاتصالات وخدماتها، فضلا عن أمنها.
- وينبغي للدول أن تحظر على موردي سلع وخدمات تكنولوجيا المعلومات والاتصالات الحصول غير القانوني على بيانات المستخدمين، ومراقبة أجهزة المستخدمين ونظمهم والتلاعب بها عن طريق تركيب أبواب خلفية في السلع. وينبغي للدول أيضا أن تحظر على موردي سلع وخدمات تكنولوجيا المعلومات والاتصالات السعي إلى تحقيق مصالح غير مشروعة باستغلال اعتماد المستخدمين على منتجاتهم، أو إجبار المستخدمين على تحديث نظمهم أو أجهزتهم. وينبغي للدول أن تطلب من موردي سلع وخدمات تكنولوجيا المعلومات والاتصالات أن يلتزموا بأن يتلقى الشركاء المتعاونون معهم ومستخدمو منتجاتهم إخطارا في الوقت المناسب إذا أُكتُشِفَت نقاط ضعف خطيرة في هذه المنتجات.
- ينبغي أن تلتزم الدول بالحفاظ على بيئة أعمال منصفة وعادلة وغير تمييزية. وينبغي للدول ألا تستخدم الأمن الوطني كذريعة لتقييد تطوير تكنولوجيا المعلومات والاتصالات وتقييد التعاون بشأنها والحد من وصول منتجات تكنولوجيا المعلومات والاتصالات إلى الأسواق ومن تصدير المنتجات ذات التكنولوجيا المتطورة.

مكافحة الإرهاب

- ينبغي للدول أن تحظر على المنظمات الإرهابية استخدام الإنترنت لإنشاء مواقع شبكية ومنتديات ومدونات إلكترونية للقيام بأنشطة إرهابية، بما في ذلك صنع وثائق سمعية وبصرية لأغراض إرهابية ونشرها وتخزينها وبثها، ونشر خطاب وفكر الإرهاب العنيف، وجمع الأموال، والتجنيد، والتحريض على الأنشطة الإرهابية، وما إلى ذلك.

- ينبغي للدول أن تضطلع بعمليات لتبادل المعلومات الاستخباراتية والتعاون على مستوى إنفاذ القانون في مجال مكافحة الإرهاب. فعلى سبيل المثال، ينبغي أن تقوم الدولة في الوقت المناسب بجمع البيانات والأدلة الإلكترونية ذات الصلة وتخزينها عندما تطلبها منها دول أخرى لاستخدامها في قضايا الإرهاب المتصل بالفضاء الإلكتروني، وأن توفر المساعدة في التحقيقات وأن ترد على الطلبات بسرعة.

- ينبغي للدول أن تقيم شراكة تعاونية مع المنظمات الدولية والمؤسسات والمواطنين في مكافحة الإرهاب الإلكتروني.

- ينبغي للدول أن تطلب إلى مقدمي خدمات الإنترنت أن يسدوا القناة التي يتدفق عبرها المحتوى الإرهابي الإلكتروني بأن يغلقوا المواقع الشبكية والحسابات الدعائية ويحذفوا المحتوى الإرهابي والمتطرف العنيف.

سلوفينيا وفرنسا وفنلندا وكرواتيا

- ينبغي أن تُشجَّع الدول على أن تتخذ تدابير من أجل أن تمنع الجهات من غير الدول، بما فيها القطاع الخاص، من أن تمارس أنشطة في مجال تكنولوجيا المعلومات والاتصالات، لأغراض خاصة بها أو بجهات أخرى من غير الدول، بطريقة تضر بأطراف ثالثة، بما فيها الأطراف الموجودة في إقليم دولة أخرى.

- ويمكن أن يتحقق هذا الهدف بالعمل مع القطاع الخاص على تحديد الإجراءات المسموح بها باستخدام نهج قائم على تقييم المخاطر، واستحداث أدوات ملموسة، أي عمليات التصديق، وأدلة أفضل الممارسات، وآليات التصدي للحوادث، وحسب الاقتضاء، اللوائح الوطنية.

كوبا

يستدعي هذا الوضع تنفيذ لوائح محددة مكملة للقانون الدولي، ترمي، في جملة أمور، إلى تحقيق العناصر التالية المتساوية في الأهمية:

- منع تطبيق تدابير انفرادية وتدابير مضادة لتدابير الدول تعرقل النفاذ العالمي إلى الفوائد التي توفرها تكنولوجيا المعلومات والاتصالات.

- التخفيف من التأثيرات الخبيثة لعزو المسؤولية عن الأفعال في مواجهة الهجمات الإلكترونية.

- منع عسكرة الفضاء الإلكتروني.

- حماية بيانات المواطنين الخاصة بمزيد من الفعالية بتعزيز اللوائح الدولية في هذا الصدد.

- استكمال التشريعات المتعلقة بـالإرهاب الإلكتروني لمواجهة حوادث الأمن السيبراني ومشاكله، مثل الهجمات الإلكترونية. وتعريف مفهوم الهجوم الإلكتروني بتوافق الآراء.
- تفعيل تطبيق مبادئ القانون الدولي في هذا المجال، بمزيد من الموضوعية.

الجمهورية التشيكية

- ينبغي للدول ألا تمارس أو تدعم عن علم نشاطا في الفضاء الإلكتروني من شأنه أن يضر بالخدمات الطبية أو المرافق الطبية، وينبغي لها أن تتخذ تدابير لحماية الخدمات الطبية من الضرر[14].
- الحاجة إلى الامتثال للالتزامات القائمة بموجب القانون الدولي لحقوق الإنسان عند النظر في السياسات والتشريعات الوطنية المتعلقة بالأمن السيبراني ووضعها وتطبيقها[15].
- الحاجة إلى إدماج وجهات نظر جميع أصحاب المصلحة ذوي الصلة والمتأثرين في المرحلة الأولى من وضع السياسات المتعلقة بالأمن السيبراني من أجل ضمان النظر من منظور كلي في آثار التدابير المتعلقة بالأمن السيبراني على حقوق الإنسان[16].

إكوادور

- توجيهات بشأن المعيار 13-ب (تقرير فريق الخبراء الحكوميين لعام 2015)[17]:

'1' يمكن للدول أن تنشئ الهياكل والسياسات والعمليات وآليات التنسيق الوطنية اللازمة لتيسير النظر بعناية في الحوادث الخطيرة المتعلقة بتكنولوجيا المعلومات والاتصالات وتحديد الاستجابات المناسبة؛

'2' يمكن للدول، بعد ذلك، أن تضع نماذج لتقييم حوادث تكنولوجيا المعلومات والاتصالات أو تحديد مداها بهدف تقييم حوادث تكنولوجيا المعلومات والاتصالات؛

'3' يمكن أن يضمن توخي المنظمات الإقليمية الشفافية بشأن هذه النماذج وقيامها بالمواءمة بينها وجود قواسم مشتركة في كيفية نظر الدول في حوادث تكنولوجيا المعلومات والاتصالات وتحسين التواصل فيما بينها؛

'4' عند النظر في جميع المعلومات ذات الصلة في حالة وقوع حادث متعلق بتكنولوجيا المعلومات والاتصالات، ينبغي للدول أن تجري بحوثا بشأن الآثار الجنسانية المحتملة، وأن تعمل مع جميع

(14) https://www.icrc.org/en/document/norms-responsible-state-behavior-cyber-operations-should-build-international-law.

(15) https://freedomonlinecoalition.com/wp-content/uploads/2020/02/FOC-Statement-on-Human-Rights-and-Cyber-Security-07.02.pdf.

(16) https://freedomonlinecoalition.com/wp-content/uploads/2020/02/FOC-Statement-on-Human-Rights-and-Cyber-Security-07.02.pdf.

(17) ينبغي للدول، في حالة وقوع حوادث في مجال تكنولوجيا المعلومات والاتصالات، أن تنظر في جميع المعلومات ذات الصلة، بما في ذلك في إطار السياق الأوسع نطاقا للحادث، والتحديات المرتبطة بعزو المسؤولية عن الحادث في بيئة تكنولوجيا المعلومات والاتصالات، وطبيعة نتائج الحادث ومداها.

أصحاب المصلحة في إطار شامل للجميع من أجل فهم السياق الأوسع لهذا الحادث، بما يشمل تأثيره على تمتع النساء بحقوقهن.

- تقتَرَح التوجيهات الآتية لتنفيذ المعيار 13-ج[18]:

'1' إذا حددت دولة ما نشاطا إلكترونيا خبيثا نابعا من إقليم دولة أخرى أو من بناها التحتية السيبرانية، يمكن اتخاذ خطوة أولى تتمثل في إخطار تلك الدولة. وتكون لأفرقة مواجهة الطوارئ الحاسوبية أهمية بالغة في التمكن من تحديد نشاط كهذا؛

'2' بالنظر إلى أن حوادث تكنولوجيا المعلومات والاتصالات يمكن أن تتبع من دول ثالثة أو أن تشملها، فمن المفهوم أن إخطار دولة ما لا يعني ضمنا مسؤولية تلك الدولة عن الحادث؛

'3' ينبغي للدولة التي تلقت الإخطار أن تقر باستلام الطلب عن طريق نقطة الاتصال الوطنية المعنية؛

'4' عندما تكون دولة ما على علم بأنه يجري استخدام إقليمها أو بناها التحتية السيبرانية لارتكاب فعل غير مشروع دوليا من المرجح أن تترتب عليه عواقب وخيمة في دولة ثانية، ينبغي للدولة الأولى أن تسعى إلى اتخاذ تدابير معقولة ومتاحة وعملية في نطاق إقليمها وقدراتها، بما يتفق مع التزاماتها بموجب القانون المحلي والدولي، للعمل على وقف الفعل غير المشروع دوليا، أو للتخفيف من عواقبه؛

'5' ينبغي ألا يفسر هذه المعيار على أنه يتطلب من الدولة أن ترصد بصورة استباقية جميع تكنولوجيات المعلومات والاتصالات الموجودة في نطاق إقليمها، أو أن تتخذ خطوات وقائية أخرى؛

'6' يجوز للدولة التي تصبح على دراية بوجود أنشطة ضارة نابعة من إقليمها في مجال تكنولوجيا المعلومات والاتصالات ولكنها تفتقر إلى القدرة على التصدي لها أن تختار التماس المساعدة من دول أخرى، بسبل منها نماذج طلب المساعدة الموحدة؛

'7' في هذه الحالات، يجوز التماس المساعدة من دول أخرى، أو من كيان من القطاع الخاص، بطريقة تتفق مع القانون الوطني. والتزام الدول بالتعاون مع الدول الأخرى ومساعدتها في حالة حدوث أزمة يعد أمرا أساسيا، وينبغي التركيز بشكل خاص على الآثار المتباينة التي يمكن أن يسببها حادث من حوادث تكنولوجيا المعلومات والاتصالات لبنى تحتية معينة في دولة نامية.

- وينبغي أن يتضمن المشروع أيضا معايير جديدة؛ من بينها ما يلي:

"ينبغي للدول ألا تضطلع بعمليات في مجال تكنولوجيا المعلومات والاتصالات يكون الهدف منها تعطيل البنى التحتية التقنية الضرورية للعمليات السياسية، مثل الانتخابات أو الاستفتاءات بأنواعها."

الهند

- (بشأن الفقرة 39): مقترح لمعيار جديد يتعلق بالحاجة إلى مقياس متفق عليه للأمن الأساسي في الفضاء الإلكتروني بشأن أكثر الطرق فعالية لتحسين التكنولوجيات الواعدة إلى أقصى درجة

(18) ينبغي للدول ألا تسمح، عن علم، باستخدام إقليمها لارتكاب أفعال غير مشروعة دوليا باستخدام تكنولوجيات المعلومات والاتصالات.

مع حماية الجمهور في الوقت نفسه. وتحقيقا لهذه الغاية، يجب على الدول أن تؤيد بقوة الاعتماد الواسع النطاق للنظافة الصحية الأساسية في الفضاء الإلكتروني والتنفيذ المُبَرهَن عليه لمتطلباتها.

- وتمثل حماية البنى التحتية الحيوية للمعلومات السلوك المسؤول للدول. فتهديد البنى التحتية الحيوية للمعلومات يمكن أن يفسد سلامة المعلومات ويضر باقتصاد الدولة وتنميتها الاقتصادية. ويجب على الدول أن تنظر في حماية هذه البنى التحتية بالشراكة بين القطاعين العام والخاص. وينبغي للدول ألا تضطلع بعمليات في مجال تكنولوجيا المعلومات والاتصالات يكون الهدف منها تعطيل البنى التحتية الحيوية للمعلومات. وينبغي للدول ألا تنشئ وظائف ضارة في منتجات تكنولوجيا المعلومات والاتصالات. وينبغي أن تكون الدول مسؤولة عن إخطار المستخدمين عند تحديد نقاط ضعف كبيرة وإخطار البائعين لعلاج نقاط الضعف. وينبغي أن تعمل الدول بشكل تعاوني في مجال البنى التحتية الحيوية للمعلومات وتتبادل المعلومات بشأن التهديدات وتتبادل أدوات وتقنيات التخفيف منها.

جمهورية إيران الإسلامية

- ينبغي تعزيز ما تضطلع به الدول، التي تقع على عاتقها المسؤولية الأساسية عن الحفاظ على بيئة لتكنولوجيا المعلومات والاتصالات تتسم بالأمن والسلامة والموثوقية، من أدوار في حوكمة هذه البيئة، بما يشمل دورها في صنع السياسات والقرارات على المستوى العالمي. وينبغي أن تتحقق الحوكمة المتوخاة بطريقة ترسخ سيادة الدول ولا تؤثر على حقوق الدول في اختيارها لنماذج التنمية والحوكمة والتشريع في هذه البيئة.

- وينبغي للدول أن تمتنع عن التهديد باستخدام القوة أو استخدامها ضد السلامة الإقليمية أو الاستقلال السياسي لأي دولة في نطاق بيئة تكنولوجيا المعلومات والاتصالات ومن خلالها.

- وليس لأي دولة الحق في التدخل من خلال الطرق والوسائل المتصلة بالفضاء الإلكتروني، بصورة مباشرة أو غير مباشرة ولأي سبب آخر، في الشؤون الداخلية أو الخارجية للدول الأخرى. وينبغي إدانة ومنع جميع أشكال التدخل والتطفل أو محاولات التهديد التي تستهدف النظم السياسية والاقتصادية والاجتماعية والثقافية للدول وكذلك بناها التحتية الحيوية المتصلة بالفضاء الإلكتروني. (قرار الجمعية العامة للأمم المتحدة 2131 المؤرخ 21 كانون الأول/ديسمبر 1965)

- لا يجوز للدول أن تستخدم أوجه التقدم في مجال تكنولوجيا المعلومات والاتصالات كأدوات لاتخاذ تدابير اقتصادية أو سياسية أو أي نوع آخر من التدابير القسرية، بما فيها تدابير فرض القيود والعرقلة التي تُتَّخَذ ضد دول مستهدفة. (قرار الجمعية العامة للأمم المتحدة 2131 المؤرخ 21 كانون الأول/ديسمبر 1965)

- ينبغي للدول أن تكفل اتخاذ التدابير المناسبة بغية إخضاع القطاع الخاص الذي تتجاوز آثاره الحدود الإقليمية، بما يشمل المنصات، للمساءلة عن سلوكه في بيئة تكنولوجيا المعلومات والاتصالات. ويجب على الدول أن تمارس الرقابة الواجبة على شركات ومنصات تكنولوجيا المعلومات والاتصالات الخاضعة لولايتها، وإن لم تفعل، فإنها تتحمل المسؤولية عن انتهاك السيادة الوطنية للدول الأخرى وأمنها ونظامها العام عن علم.

- ينبغي للدول أن تمتنع عن إساءة استخدام سلاسل الإمداد الخاصة بتكنولوجيا المعلومات والاتصالات التي تنشأ تحت رقابتها وولايتها من أجل إحداث، أو المساعدة في إيجاد، نقاط ضعف في المنتجات والخدمات والصيانة تنتهك سيادة الدول المستهدفة وحمايتها للبيانات، وينبغي لها أن تمنع حدوث ذلك.

اليابان

يتمثل المقترح الجديد المقدم من اليابان إلى الفريق العامل المفتوح العضوية في إضافة الصياغة التالية باعتبارها توجيها للمعيار '1' بشأن ضمان سلامة سلسلة الإمداد:

- "للدول الحق في التأكد من استخدام موردين وبائعين موثوق بهم لتوفير معدات ونظم تكنولوجيا المعلومات والاتصالات، ولا سيما من أجل معالجة شواغل الأمن الوطني وحماية الخصوصية، وهي المسؤولة عن ذلك. ويجوز أن تشمل الخطوات المعقولة في هذا الصدد وضع تشريعات أو تدابير إدارية ترمي إلى تأمين سلسلة الإمداد، ودعم تطوير تكنولوجيا وصناعة يمكن الاعتماد عليهما والوثوق بهما، وتنويع الموردين".

هولندا

- "ينبغي ألاّ تقوم الجهات من غير الدول، أو تسمح عن علم، بنشاط يضر ضررا متعمدا وجسيما بتوافر النواة الجماهيرية للإنترنت أو سلامتها بوجه عام، وبالتالي يضر باستقرار الفضاء الإلكتروني"، توجيه [محتمل] لتنفيذ التوصية 13 (و) من توصيات فريق الخبراء الحكوميين التابع للأمم المتحدة لعام 2015 وبالتالي يدرج ذلك أيضا في نطاق التوصية 13 (ز) من توصيات الفريق لعام 2015

- "يجب على الجهات من الدول ومن غير الدول ألا تنخرط في عمليات في الفضاء الإلكتروني يكون الهدف منها تعطيل البنى التحتية التقنية الضرورية للانتخابات أو مختلف أنواع الاستفتاءات، أو تدعم هذه العمليات أو تسمح بها"، توجيه [محتمل] لتنفيذ التوصية 13 (و) من توصيات فريق الخبراء الحكوميين التابع للأمم المتحدة لعام 2015 وبالتالي يدرج ذلك أيضا في نطاق التوصية 13 (ز) من توصيات الفريق لعام 2015

حركة عدم الانحياز

- ينبغي تشجيع الدول الأعضاء على تجميع وتبسيط المعلومات التي تقدمها عن تنفيذها للقواعد الدولية والمستودع المقترح ذي الصلة، بغية تنظيم جوانب محددة من استخدام الدول لتكنولوجيا المعلومات والاتصالات من منظور الأمن الدولي وتحديد المجالات ذات الاهتمام المشترك.

- ينبغي للدول الأعضاء ألا تمارس أو تدعم عن علم أي أنشطة في مجال تكنولوجيا المعلومات والاتصالات تضر عمدا بالبنى التحتية الحيوية للدول الأعضاء الأخرى أو تعوق استخدامها وتشغيلها على نحو يخالف القانون الدولي.

- ينبغي حث الدول الأعضاء على النظر في تبادل المعلومات بشأن نقاط الضعف ذات الصلة بتكنولوجيا المعلومات والاتصالات و/أو الوظائف الضارة الخفية في منتجات تكنولوجيا المعلومات والاتصالات وإخطار المستخدمين عند تحديد نقاط ضعف كبيرة.

- ينبغي للدول الأعضاء أيضا أن تأخذ في الاعتبار قرار الجمعية العامة للأمم المتحدة 27/73 في ممارسة جميع الأنشطة المتصلة بتكنولوجيا المعلومات والاتصالات.

- تعرب حركة عدم الانحياز من جديد عن قلقها الشديد إزاء اللجوء المتزايد إلى العمل الانفرادي، وتؤكد في هذا السياق أن تعددية الأطراف والحلول المتفق عليها على نحو متعدد الأطراف، وفقاً لميثاق الأمم المتحدة، توفر الطريقة المستدامة الوحيدة لمعالجة قضايا الأمن الدولي.

- تؤكد الحركة من جديد على أن جميع الدول ينبغي أن تمتنع عن التهديد باستخدام القوة أو استخدامها ضد السلامة الإقليمية أو الاستقلال السياسي لأي دولة في نطاق بيئة تكنولوجيا المعلومات والاتصالات ومن خلالها.

- تدعو الحركة إلى تكثيف الجهود في اتجاه حماية الفضاء الإلكتروني حتى لا يصبح ساحة نزاع وكفالة استخدامه بدلاً من ذلك في الأغراض السلمية الحصرية التي من شأنها أن تتيح تسخير إمكانات تكنولوجيا المعلومات والاتصالات بشكل كامل للمساهمة في التنمية الاجتماعية والاقتصادية.

- تشدد الحركة على أهمية تجنب فرض قيود لا مبرر لها، من بينها التدابير القسرية الانفرادية، على استخدام تكنولوجيا المعلومات والاتصالات في الأغراض السلمية أو التعاون الدولي أو نقل التكنولوجيا.

- تؤكد الحركة على أن الدول تتحمل المسؤولية الرئيسية عن صون بيئة مفتوحة ومأمونة وميسَّرة وسلمية لتكنولوجيا المعلومات والاتصالات.

- تشدد الحركة على أنه ينبغي لجميع الدول ألا تمارس أو تدعم عن علم أي نشاط في مجال تكنولوجيا المعلومات والاتصالات يتعارض مع التزاماتها بموجب القانون الدولي ويضر عمدا بالبنى التحتية الحيوية أو يعرقل استخدامها وتشغيلها.

باكستان

- ينبغي تشجيع الدول الأعضاء على مواصلة النظر، حسب الاقتضاء، في إمكانية اعتماد صك ملزم قانونا و/أو سياسيا (أو أكثر من صك واحد) من أجل تنظيم جوانب محددة من استخدام الدول لتكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي.

- ينبغي تشجيع الدول الأعضاء على التوصل إلى تعريف مشترك متفق عليه لما يشكل "البنى التحتية الحيوية"، بغية الاتفاق على حظر نشاط تكنولوجيا المعلومات والاتصالات الذي يضر عن علم أو عمدا بالبنى التحتية الحيوية أو يعطل بأي طريقة أخرى استخدام البنى التحتية الحيوية وتشغيلها.

- ينبغي تشجيع الدول الأعضاء على التعاون للتوصل إلى اتفاق بشأن حظر إنشاء وظائف ضارة خفية في منتجات تكنولوجيا المعلومات والاتصالات أو مراكمة نقاط ضعف في هذه المنتجات، وعلى الالتزام بالإبلاغ المسؤول وفي الوقت المناسب عن نقاط الضعف في تكنولوجيا المعلومات والاتصالات وتبادل ما يتصل بذلك من معلومات عن سبل العلاج المتاحة لأوجه الضعف هذه.

- ينبغي للدول الأعضاء أن تسعى إلى تيسير التعاون مع مقدمي منتجات وخدمات تكنولوجيا المعلومات والاتصالات لمنع استغلال أو انتهاك بيانات المستخدمين وخصوصيتهم.

- ينبغي للدول الأعضاء أن تلتزم بعدم استخدام تكنولوجيا المعلومات والاتصالات في ممارسة أنشطة تتعارض مع صون السلام والأمن الدوليين، وأن تمتنع عن استخدام تكنولوجيا المعلومات والاتصالات للتدخل في الشؤون الداخلية للدول الأخرى بأي شكل من الأشكال.

- ينبغي للدول الأعضاء أن تتعاون في التصدي للتحديات المرتبطة بعزو المسؤولية عن الأفعال في بيئة تكنولوجيا المعلومات والاتصالات. ولا يزال وضع نهج مشترك لعزو المسؤولية في إطار عالمي تحت رعاية الأمم المتحدة هو أكثر السبل فعالية للمضي قدما في هذا الصدد.

- يجب حث الدول الأعضاء على التوصل إلى اتفاق بشأن حظر نشاط تكنولوجيا المعلومات والاتصالات الذي يهدف إلى تعطيل البنى التحتية التقنية الضرورية لإجراء الانتخابات أو الاستفتاءات بأنواعها.

- ينبغي تشجيع الدول الأعضاء على وضع المعايير وتنفيذها بطريقة تتفادى فرض قيود غير مبررة على استخدام تكنولوجيا المعلومات والاتصالات في الأغراض السلمية، أو التعاون الدولي في هذا الميدان، أو نقل التكنولوجيا.

جمهورية كوريا

توجيهات مقترحة بشأن الفقرة 13 (ج) من تقرير فريق الخبراء الحكوميين لعام 2015:

- عندما تُخطِر دولة متضررة دولة أخرى بأن حوادث تكنولوجيا المعلومات والاتصالات قد نبعت من إقليم الدولة التي أُخطِرَت أو تتعلق به وفقا لمعلومات مؤهلة، ينبغي للدولة التي أُخطِرَت أن تتخذ، وفقا للقانون الدولي والمحلي وفي حدود قدراتها، جميع الخطوات المعقولة، في نطاق إقليمها، للعمل على وقف هذه الأنشطة أو للتخفيف من آثارها.

- ينبغي أن يكون مفهوما أن الإخطار المذكور لا يعني ضمنا أن الدولة التي أُخطِرَت مسؤولة عن الحادث.

- يجوز أن يتضمن الحد الأدنى المطلوب من المعلومات المؤهلة مؤشر الاختراق، مثل عنوان البروتوكول على الإنترنت وموقع الجناة والحواسيب المستخدمة في ارتكاب أفعال تكنولوجيا المعلومات والاتصالات الخبيثة، ومعلومات عن البرمجيات الخبيثة.