الأمم المتحدة

A/76/135

الجمعية العامة

Distr.: General
14 July 2021
Arabic
Original: English

الدورة السادسة والسبعون

البند 96 من جدول الأعمال المؤقت*

التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي

فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي

مذكرة من الأمين العام

يتشرف الأمين العام بأن يحيل طي هذه المذكرة تقرير فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي. وقد أنشئ الفريق عملا بالفقرة 3 من قرار الجمعية العامة 266/73.

* A/76/50.

020821 270721 21-04030 (A)

تقرير فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي*

موجز

مع استمرار تزايد اعتماد العالم على تكنولوجيات المعلومات والاتصالات، أصبح السلوك المسؤول للدول في استخدام تكنولوجيات المعلومات والاتصالات ذا أهمية حيوية لصون السلام والأمن الدوليين.

وعملا بولاية فريق الخبراء الحكوميين المعني بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي للفترة 2019-2021، الواردة في قرار الجمعية العامة 266/73، واصل الفريق دراسة التدابير التعاونية الممكن اتخاذها للتصدي للتهديدات القائمة والمحتملة في ميدان أمن المعلومات، ابتغاء تعزيز الفهم المشترك والتنفيذ الفعال.

ويتضمن هذا التقرير النتائج التي توصل إليها الفريق بشأن التهديدات القائمة والناشئة؛ ومعايير سلوك الدول المسؤول وقواعده ومبادئه؛ والقانون الدولي؛ وتدابير بناء الثقة؛ والتعاون والمساعدة الدوليين في مجال أمن تكنولوجيات المعلومات والاتصالات وبناء القدرات في هذا المجال. وفيما يتعلق بكل موضوع من هذه المواضيع، يضيف التقرير مستوى إضافيا من الفهم إلى النتائج والتوصيات التي توصلت إليها أفرقة الخبراء الحكوميين السابقة.

* يصدر بغير تحرير رسمي.

المحتويات

الصفحة

تصدير بقلم الأمين العام

ما زالت تكنولوجيات المعلومات والاتصالات تحدث تحولا سريعا في المجتمعات، إذ تتيح فرصا عديدة في الوقت الذي تُسبب فيه أيضا مخاطر كبيرة. وقد زادت جائحة كوفيد-19 من تسريع تحول العديد من جوانب حياتنا إلى الفضاء الرقمي ومن تسريع اعتمادنا على التكنولوجيات الرقمية.

وفي الوقت نفسه، فإن المراقبة والتلاعب الرقميين آخذان في الازدياد، ويجري تشكيل عالم الإنترنت بطرق لا تخدم المصلحة العامة دائما. وإذا تركت هذه الاتجاهات بغير كابح، فيمكن أن يكون لها أثر مدمر على المجتمعات فضلا عن الأفراد. وقد باتت الحاجة إلى التصدي لهذه التحديات، وتسخير فوائد تكنولوجيات المعلومات والاتصالات، وتعزيز السلوك المسؤول للدول في سياق الأمن الدولي، أكثر إلحاحا منها في أي وقت مضى.

وقد أجرى فريق الخبراء الحكوميين للفترة 2019-2021، في إطار تنفيذ ولايته، مداولات مستفيضة على مدى ثمانية عشر شهرا. وأُثري هذا الجهد أيضا من خلال المشاورات غير الرسمية على الصعيد الإقليمي والاجتماعات غير الرسمية التي كانت مفتوحة أمام جميع الدول الأعضاء. وثمة تكاملٌ بين تقرير الفريق وعمل الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي الذي اعتمد تقريرا بتوافق الآراء في آذار/مارس 2021.

وفي السنوات الأخيرة، أولت الدول وغيرها من أصحاب المصلحة من القطاعين العام والخاص أهمية متزايدة لجهود الأمم المتحدة الرامية إلى تعزيز الاستخدام السلمي لتكنولوجيات المعلومات والاتصالات. وفي ظل هذه الروح، يمثل هذا التقرير مساهمة في سبيل تهيئة بيئة منفتحة وآمنة ومستقرة وميسرة لتكنولوجيات المعلومات والاتصالات. كما يمثل دعوة متجددة إلى مزيد من التعاون من أجل الحد من المخاطر السيبرانية على السلام والأمن الدوليين، وضمان حماية وتعزيز حقوق الإنسان والحريات الأساسية على الإنترنت وخارج الإنترنت.

كتاب الإحالة

28 أيار/مايو 2021

أتشرف بأن أحيل طيه تقرير فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي. وقد أنشئ الفريق في عام 2018 عملا بالفقرة 3 من قرار الجمعية العامة 266/73.

وقد طلبت الجمعية العامة، في ذلك القرار، إنشاء فريق من الخبراء الحكوميين في عام 2019 على أساس التوزيع الجغرافي العادل، وانطلاقا من التقييمات والتوصيات الواردة في تقارير فريق الخبراء الحكوميين الصادرة بتوافق الآراء للأعوام 2010 و 2013 و 2015 ليواصل، ابتغاء تعزيز الفهم المشترك والتنفيذ الفعال، دراسة التدابير التعاونية الممكن اتخاذها للتصدي للتهديدات القائمة والمحتملة في ميدان أمن المعلومات، بما في ذلك معايير وقواعد ومبادئ السلوك المسؤول للدول، وتدابير بناء الثقة وبناء القدرات، وكذلك كيفية انطباق القانون الدولي على استخدام الدول لتكنولوجيات المعلومات والاتصالات. وطُلب إلى الأمين العام أن يقدم تقريرا عن نتائج الدراسة إلى الجمعية العامة في دورتها السادسة والسبعين.

ووفقا لولاية الفريق، سيتاح ثبتٌ رسمي بالمساهمات الوطنية الطوعية المتعلقة بموضوع كيفية انطباق القانون الدولي على استخدام الدول لتكنولوجيات المعلومات والاتصالات، التي قدمها الخبراء الحكوميون المشاركون في الفريق، وذلك على الموقع الشبكي لمكتب الأمم المتحدة لشؤون نزع السلاح باللغات الأصلية التي قدمت بها دون ترجمة [سيجري توفير رمز الوثيقة].

ووفقا لأحكام القرار، عُين خبراء من 25 دولة هي: الاتحاد الروسي، والأردن، وأستراليا، وإستونيا، وألمانيا، وإندونيسيا، وأوروغواي، والبرازيل، وجنوب أفريقيا، ورومانيا، وسنغافورة، وسويسرا، والصين، وفرنسا، وكازاخستان، وكينيا، والمغرب، والمكسيك، والمملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية، وموريشيوس، والنرويج، والهند، وهولندا، والولايات المتحدة الأمريكية، واليابان. وترد قائمة الخبراء في نهاية التقرير.

وعقد الفريق أربع دورات رسمية: الأولى في الفترة من 9 إلى 13 كانون الأول/ديسمبر 2019 في مقر الأمم المتحدة، والثانية في الفترة من 24 إلى 28 شباط/فبراير 2020 في جنيف، والثالثة بالوسائل الإلكترونية في الفترة من 5 إلى 9 نيسان/أبريل 2021، والرابعة بالوسائل الإلكترونية في الفترة من 24 إلى 28 أيار/مايو 2021. وأجلت الدورة الثالثة للفريق عملا بقرار الجمعية العامة 551/75 بسبب جائحة كوفيد-19. ومع ذلك، واصل الفريق عمله خلال هذه الفترة من خلال سلسلة من عدة مشاورات غير رسمية جرت فيما بين الدورتين. وعقد الفريق أيضا، وفقا لولايته، مجموعة من المشاورات مع المنظمات الإقليمية المعنية واجتماعات تشاورية مفتوحة مع الدول الأعضاء لإجراء مناقشات تحاورية وتبادل الآراء.

ويود الفريق أن يعرب عن تقديره لمساهمة فريق الدعم المشترك التابع لمكتب الأمم المتحدة لشؤون نزع السلاح ومعهد الأمم المتحدة لبحوث نزع السلاح.

وأغتنم هذه الفرصة أيضا لأعرب عن امتناني الشخصي لحكومة البرازيل لتكليفي بهذه المهمة وعن امتناني للفريق على شرف الرئاسة. كما أشكر زملائي الخبراء وزملائي البرازيليين وأعضاء فريق الدعم المشترك والأمانة العامة للأمم المتحدة، ولا سيما الممثلة السامية لشؤون نزع السلاح، على دعمهم وعلى المساهمة بخبراتهم العظيمة بروح تعاونية بناءة.

(توقيع) غيليهرمي **دي أغيار باتريوتا**
رئيس الفريق

أولا - مقدمة

1 - يجسد هذا التقرير نتائج المناقشات التي أجراها فريق الخبراء الحكوميين عملا بقرار الجمعية العامة 266/73 بشأن 'الارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي'. وقد جرى جزء رئيسي من عمل الفريق أثناء جائحة مرض فيروس كورونا (كوفيد-19)، التي أبرزت الإمكانات الهائلة للتكنولوجيات الرقمية وعجلت في الوقت نفسه من وتيرة اعتماد العالم عليها، مما يزيد من تأكيد أهمية السلوك المسؤول في استخدام تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي.

2 - ويستند التقرير إلى تقييمات وتوصيات تقارير أفرقة خبراء الأمم المتحدة الحكوميين الصادرة بتوافق الآراء للسنوات 2010 و 2013 و 2015 بشأن التهديدات القائمة والناشئة والمعايير والقواعد والمبادئ المنظمة للسلوك المسؤول للدول، والقانون الدولي، وبناء الثقة، والتعاون الدولي، وبناء القدرات، التي تمثل مجتمعة إطارا تراكميا ومتطورا للسلوك المسؤول للدول في استخدامها لتكنولوجيات المعلومات والاتصالات. ويرحب الفريق باعتماد التقرير الصادر بتوافق الآراء لفريق الأمم المتحدة العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي (الفريق العامل المفتوح العضوية)، المنشأ عملا بقرار الجمعية العامة 27/73[(1)]، الذي يؤكد هذا الإطار ويستند إليه.

3 - وقد نظر فريق الخبراء الحكوميين في المسائل المشمولة بولايته في ضوء صلتها بالسلام والأمن الدوليين. وسعى، فضلا عن ذلك، إلى توفير مستوى إضافي من الفهم لتقييمات وتوصيات تقارير أفرقة الخبراء الحكوميين السابقة، من أجل توفير التوجيه لدعم تنفيذها. ويؤكد هذا المستوى الإضافي من الفهم مجددا الروابط بين مختلف العناصر الموضوعية في ولاية الفريق وأهمية إشراك الجهات الفاعلة الأخرى، بما في ذلك القطاع الخاص والمجتمع المدني والأوساط الأكاديمية والأوساط التقنية، عند الاقتضاء، في جهود الدول لتنفيذ هذه التوصيات.

4 - ويقر الفريق بالدور الهام الذي تضطلع به الهيئات الإقليمية ودون الإقليمية في المضي قدماً بالتقييمات والتوصيات الواردة في تقارير أفرقة الخبراء الحكوميين التابعة للأمم المتحدة وفي إنشاء آليات خاصة بكل منطقة على حدة وتعزيز جهود بناء القدرات دعماً لتنفيذها. ووفقا لولاية الفريق، جرى إطلاع الفريق على هذه الرؤى والتجارب وغيرها من الرؤى والتجارب ذات الصلة خلال الاجتماعات التشاورية غير الرسمية التي عقدها الفريق مع الدول الأعضاء في نيويورك ومن خلال مجموعة من المشاورات عقدت بالتعاون مع المنظمات الإقليمية[(2)].

5 - ويؤكد الفريق من جديد أن تهيئة بيئة منفتحة وآمنة ومستقرة وميسَّرة وسلمية لتكنولوجيا المعلومات والاتصالات هي أمرٌ ضروري للجميع، وتتطلب تعاونا فعالا بين الدول للحد من المخاطر التي تهدد السلام والأمن الدوليين. ويشكل تعزيز استخدام تكنولوجيات المعلومات والاتصالات للأغراض السلمية منفعة عامة

(1) A/75/816.

(2) يمكن الاطلاع على التقارير المتعلقة بمختلف المشاورات عن طريق الرابط https://www.un.org/disarmament/wp-content/uploads/2019/12/gge-chair-summary-informal-consultative-meeting-5-6-dec-20191.pdf، والرابط https://www.un.org/disarmament/wp-content/uploads/2019/12/collated-summaries-regional-gge-consultations-12-3-2019.pdf.

أساسية تصب في مصلحة الجميع. وما زال احترام السيادة وحقوق الإنسان والحريات الأساسية، فضلا التنمية المستدامة والرقمية، في صميم هذه الجهود.

ثانيا - التهديدات القائمة والناشئة

6 - مع أن تكنولوجيات المعلومات والاتصالات والرقمنة والترابط المتزايدين للعالم تتيح فرصاً هائلة للمجتمعات في العالم أجمع، يؤكد الفريق مجددا أن التهديدات الجسيمة المتصلة بتكنولوجيات المعلومات والاتصالات المشار إليها في التقارير السابقة ما زالت قائمة. وقد طرأت زيادة على نطاق وحجم وشدة وتعقيد الحوادث المتصلة بالاستخدام الخبيث لتكنولوجيات المعلومات والاتصالات من قِبَل الدول والجهات الفاعلة من غير الدول. وبينما تتجلى التهديدات المرتبطة بتكنولوجيات المعلومات والاتصالات بأشكال مختلفة في مختلف المناطق، فإن آثارها يمكن أيضاً أن تكون عالمية.

7 - ويؤكد الفريق التقييمين اللذين خلص إليهما التقرير الصادر في عام 2015 ومفادهما قيام عدد من الدول حالياً باستحداث قدرات في مجال تكنولوجيا المعلومات والاتصالات للأغراض العسكرية؛ وتزايد احتمالات استخدام تكنولوجيات المعلومات والاتصالات في النزاعات التي قد تنشب بين الدول في المستقبل.

8 - ويمكن أن يشكل النشاط الخبيث باستخدام تكنولوجيات المعلومات والاتصالات من جانب الجهات الفاعلة التي تصدر عنها تهديدات مستمرة، بما في ذلك الدول والجهات الفاعلة الأخرى، خطرا كبيرا على الأمن والاستقرار الدوليين، وعلى التنمية الاقتصادية والاجتماعية، وكذلك على سلامة الأفراد ورفاههم.

9 - وبالإضافة إلى ذلك، تستخدم الدول والجهات الفاعلة الأخرى بنشاط حاليا قدرات أكثر تعقيدا وتطورا لتكنولوجيات المعلومات والاتصالات لأغراض سياسية وغيرها من الأغراض. ويلاحظ الفريق أيضا زيادة مقلقة في تنفيذ الدول حملات إعلامية سرية خبيثة باستخدام تكنولوجيات المعلومات والاتصالات للتأثير على العمليات والنظم والاستقرار العام لدولة أخرى. وهذه الاستخدامات تقوض الثقة، وقد تكون تصعيدية ويمكن أن تهدد السلام والأمن الدوليين. كما أنها قد تلحق ضررا مباشرا وغير مباشر بالأفراد.

10 - وغدا خطيرا بصورة متزايدة النشاطُ الضار لتكنولوجيات المعلومات والاتصالات على البنية التحتية الحيوية التي تقدم الخدمات محليا أو إقليميا أو عالميا، وهو ما نوقش في تقارير سابقة لأفرقة الخبراء الحكوميين. ومما يثير القلق بوجه خاص ذلك النشاط الخبيث لتكنولوجيات المعلومات والاتصالات الذي يؤثر على البنية التحتية الحيوية للمعلومات، والبنية التحتية التي تقدم الخدمات الأساسية للجمهور، والبنية التحتية التقنية الضرورية للتوافر العام لإمكانية استخدام الإنترنت والاستفادة من كيانات القطاع الصحي، أو لسلامتهما. وقد أظهرت جائحة كوفيد-19 مخاطر وعواقب الأنشطة الخبيثة لتكنولوجيات المعلومات والاتصالات التي تسعى إلى استغلال مواطن الضعف في الأوقات التي تتعرض فيها مجتمعاتنا لضغوط هائلة.

11 - وتؤدي التكنولوجيات الجديدة والناشئة حاليا إلى توسيع فرص التنمية. ومع ذلك، فإن سماتها وخصائصها التي لا تنفك تتطور توسع أيضا المساحة المعرضة للهجوم، مما يوجِد نواقل ونقاط ضعف جديدة يمكن استغلالها في نشاط تكنولوجيا المعلومات والاتصالات الخبيث. وأصبح ضمان ألا تستخدم لأغراض خبيثة نقاطُ الضعف في التكنولوجيا التشغيلية وفي أجهزة الحوسبة المترابطة أو المنصات أو الآلات أو الأشياء التي تتكون منها شبكة إنترنت الأشياء تحديا خطيرا.

12 - ولا تزال القدرات على تأمين نظم المعلومات تختلف في جميع أنحاء العالم، شـأنها شـأن القدرات على تطوير القدرة على الصـمود، وحماية البنية التحتية الحيوية للمعلومات، وتحديد التهديدات والتصـدي لها في الوقت المناسـب. وتترتب على هذه الاختلافات في القدرات والموارد، فضـلا عن تفاوت القوانين والأنظمة والممارسـات الوطنية المتصـلة باسـتخدام تكنولوجيات المعلومات والاتصـالات، وعدم تسـاوي الوعي بالتدابير التعاونية الإقليمية والعالمية القائمة المتاحة للتخفيف من هذه الحوادث أو التحقيق فيها أو التعافي منها، وعدم المساواة في إمكانية الاستفادة من تلك التدابير، زيادةُ مواطن الضعف والمخاطر بالنسبة لجميع الدول.

13 - ويؤكد الفريق من جديد أن اسـتخدام تكنولوجيات المعلومات والاتصـالات للأغراض الإرهابية، بما يتجاوز التجنيد والتمويل والتدريب والتحريض، بما في ذلك لأغراض شن هجمات إرهابية ضد تكنولوجيات المعلومات والاتصـالات أو ضـد البنية التحتية المعتمدة عليها، يمثل احتمالا آخذا في التزايد، وإن ترك على هذا النحو دون التصدي له، فإنه قد يشكل تهديداً للسلام والأمن الدوليين.

14 - ويؤكد الفريق من جديد أيضـاً أنه مما يزيد من هذه المخاطر التنوعُ الذي يصـبغ الجهات الفاعلة الخبيثة من غير الدول، بما فيها الجماعات الإجرامية والإرهابيون، واختلاف دوافعهم، والسرعة التي يمكن أن تحدث بها الأفعال الخبيثة باستخدام تكنولوجيات المعلومات والاتصالات، فضلاً عن صعوبة تحديد المصدر الذي يمكن أن تعزى إليه حادثة من حوادث تكنولوجيات المعلومات والاتصالات.

ثالثا - القواعد والمعايير والمبادئ

15 - يؤكد الفريق من جديد فيما يتعلق باسـتخدام الدول لتكنولوجيات المعلومات والاتصـالات أن القواعد الطوعية غير الملزمة لسلوك الدول المسؤول يمكن أن تقلل من المخاطر التي تهدد السلام والأمن والاستقرار على الصـعيد الدولي. وتتعايش هذه القواعد مع قواعد القانون الدولي القائمة. ولا تسـعى إلى الحد من العمل الذي يتسق مع القانون الدولي أو إلى حظره. إنما هي تجسد توقعات المجتمع الدولي، وترسي معايير لسلوك الدول المسـؤول. ويمكن أن تسـاعد تلك القواعد على منع نشـوب النزاعات في بيئة تكنولوجيات المعلومات والاتصـالات، وأن تسـهم في اسـتخدام تلك التكنولوجيات في الأغراض السلمية للتمكين من التطبيق التام لها من أجل زيادة التنمية الاجتماعية والاقتصادية على الصعيد العالمي.

16 - ويشـدد الفريق أيضـا على العلاقة المتبادلة بين القواعد وتدابير بناء الثقة والتعاون الدولي وبناء القدرات. وبالنظر إلى السمات الفريدة لتكنولوجيات المعلومات والاتصـالات، يؤكد الفريق من جديد الملاحظة التي وردت في تقرير عام 2015 بأنه يمكن وضع قواعد إضافية بمرور الوقت، ويلاحظ، في سياق منفصل، أن من الممكن وضع التزامات إضافية ملزمة في المستقبل، إذا كان ذلك مناسباً.

17 - وبالإضـافة إلى العمل في منظومة الأمم المتحدة، يقر الفريق بالتجارب القيمة التي ظهرت على الصـعيد الإقليمي في مجال تنفيذ القواعد، بما في ذلك التجارب التي أتيح الاطلاع عليها أثناء المشـاورات غير الرسـمية التي أجريت مع الدول الأعضـاء في نيويورك وبالتعاون مع المنظمات الإقليمية وفقا لولاية الفريق، ويشـير إلى أن الأعمال المقبلة المتعلقة بتكنولوجيات المعلومات والاتصـالات في سـياق الأمن الدولي ينبغي أن تأخذ تلك الجهود في الحسبان. ولاحظ الفريق أيضـا اقتراح الاتحاد الروسـي وأوزبكستان والصـين وطاجيكسـتان وقيرغيزسـتان وكازاخسـتان وضـع مدونة دولية لقواعد السـلوك في مجال أمن المعلومات (انظر A/69/723).

18 - وفي القرار 237/70 الصادر بتوافق الآراء، أهابت الجمعية العامة بالدول الأعضاء أن تسترشد في استخدامها لتكنولوجيات المعلومات والاتصالات بتقرير فريق الخبراء الحكوميين لعام 2015، الذي يتضمن إحدى عشرة قاعدة طوعية غير ملزمة لسلوك الدول المسؤول. وقد بلور الفريق، وفقا لولايته المتمثلة في الارتقاء بالسلوك المسؤول، مستوى إضافيا من الفهم لتلك القواعد، مؤكدا قيمتها فيما يتعلق بالسلوك المتوقع للدول في استخدامها لتكنولوجيات المعلومات والاتصالات في سياق السلام والأمن الدوليين، ومقدماً أمثلة لأنواع الترتيبات المؤسسية التي يمكن للدول أن تطبقها على الصعيدين الوطني والإقليمي لدعم تنفيذها. ويذكِّر الفريق الدول بأن هذه الجهود ينبغي أن تتم وفقا لالتزاماتها بموجب ميثاق الأمم المتحدة وقواعد القانون الدولي الأخرى، بغية الحفاظ على بيئة منفتحة وآمنة ومستقرة وميسَّرة وسلمية لتكنولوجيات المعلومات والاتصالات. ويُهاب بالدول أن تتجنب - وتمتنع عن - استخدام تكنولوجيات المعلومات والاتصالات على نحو لا يتماشى مع قواعد السلوك المسؤول للدول.

القاعدة 13 (أ): ينبغي للدول، تمشيا مع مقاصد الأمم المتحدة، بما في ذلك صون السلام والأمن الدوليين، أن تتعاون في وضع وتطبيق تدابير لزيادة الاستقرار والأمن في استخدام تكنولوجيات المعلومات والاتصالات، وأن تمنع الممارسات المعترف بضررها في مجال تكنولوجيا المعلومات والاتصالات أو التي قد تشكل تهديدا للسلام والأمن الدوليين.

19 - إن صون السلام والأمن الدوليين والتعاون الدولي من بين المقاصد التأسيسية للأمم المتحدة. وتذكِّر هذه القاعدة بأن من التطلعات المشتركة لجميع الدول ومن مصلحتها أن تتعاون وتعمل معاً على تعزيز استخدام تكنولوجيات المعلومات والاتصالات في الأغراض السلمية وأن تمنع نشوب النزاعات الناجمة عن استخدامها.

20 - وفي هذا الصدد، ودعما لتنفيذ تلك القاعدة، يشجع الفريق الدول على الامتناع عن استخدام تكنولوجيات المعلومات والاتصالات وشبكات تكنولوجيات المعلومات والاتصالات للقيام بأنشطة يمكن أن تهدد صون السلام والأمن الدوليين.

21 - وتمثل التدابير التي أوصت بها أفرقة الخبراء الحكوميين السابقة والفريق العامل المفتوح العضوية إطارا أوليا لسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات. وكإرشادات إضافية، ولتيسير هذا التعاون، يوصي الفريق بأن تنشئ الدول آليات وهياكل وإجراءات على الصعيد الوطني أو تعزيز القائم منها، مثل عمليات وضع السياسات والتشريعات ذات الصلة وعمليات الاستعراض المناظرة؛ وآليات إدارة الأزمات والحوادث؛ وترتيبات التعاون وإقامة الشراكات التي تشمل الحكومة بأكملها؛ وترتيبات التعاون والحوار مع القطاع الخاص والأوساط الأكاديمية والمجتمع المدني والأوساط التقنية. وتُشجَّع الدول أيضاً على تجميع وتبسيط المعلومات التي تقدمها بشأن تنفيذ القواعد، بوسائل منها المسح الطوعي لجهودها الوطنية وإتاحة خبراتها.

القاعدة 13 (ب): ينبغي للدول، في حالة وقوع حوادث في مجال تكنولوجيا المعلومات والاتصـــالات، أن تنظر في جميع المعلومات ذات الصـلة، بما يشـمل السـياق الأوسـع نطاقا للحادث، والتحديات المرتبطة بتحديد مصدر الحوادث التي تقع في بيئة تكنولوجيا المعلومات والاتصالات، وطبيعة نتائج الحادث ومداها

22 - تقر هذه القاعدة بأن تحديد الجهة الفاعلة عملية معقدة وبأنه ينبغي النظر في طائفة واســعة من العوامل قبل تحديد مصــدر أي حادثة من حوادث تكنولوجيات المعلومات والاتصــالات. وفي هذا الصــدد، يمكن أن يســاعد الحذر الذي دُعي إلى توخيه في الفقرة 71 (ز) من هذا التقرير وفي تقارير أفرقة الخبراء الحكوميين السابقة في تجنب سوء الفهم وتصاعد التوترات بين الدول.

23 - وتشجَّع الدول التي تتعرض لنشاط خبيث في مجال تكنولوجيا المعلومات والاتصالات والدول التي يشتبه في أن هذا النشاط الخبيث قد نشأ من أراضيها، على التشاور فيما بين السلطات المختصة المعنية.

24 - وينبغي للدولة التي تقع ضحية حادث خبيث في مجال تكنولوجيا المعلومات والاتصالات أن تنظر في جميع الجوانب لدى تقييمها للحادث. ويمكن أن تشـمل هذه الجوانب، مع الاسـتناد إلى وقائع مؤكدة بالأدلة، السمات التقنية للحادث؛ ونطاقه وحجمه وتأثيره؛ والسياق الأوسع، بما في ذلك تأثير الحادث على السلام والأمن الدوليين؛ ونتائج المشاورات بين الدول المعنية.

25 - وينبغي أن يكون رد الدولة المتضررة على نشاط تكنولوجيا المعلومات والاتصالات الخبيث الذي يعزى إلى دولة أخرى متفقا مع التزاماتها بموجب ميثاق الأمم المتحدة وقواعد القانون الدولي الأخرى، بما في ذلك الالتزامات المتعلقة بتسوية المنازعات بالوسائل السلمية وبالأفعال غير المشروعة دوليا. ويمكن للدول أيضا أن تستفيد من كامل تشكيلة الخيارات الدبلوماسية والقانونية وغيرها من الخيارات التشاورية المتاحة لها، فضلا عن الآليات الطوعية وغيرها من الالتزامات السياسية التي تسمح بتسوية الخلافات والمنازعات من خلال التشاور والوسائل السلمية الأخرى.

26 - ولتفعيل هذه القاعدة على الصـعيد الوطني وتيسـير التحقيق في حوادث تكنولوجيا المعلومات والاتصالات التي تشمل دولا أخرى وعلاجها، يمكن للدول أن تنشئ أو تعزز الهياكل الوطنية ذات الصلة، والسياسات والعمليات والأطر التشريعية وآليات التنسيق المتعلقة بتكنولوجيات المعلومات والاتصالات، فضلا عن الشراكات وغيرها من أشكال التفاعل مع أصحاب المصلحة المعنيين لتقييم خطورة حادث تكنولوجيا المعلومات والاتصالات وقابليته للتكرار.

27 - ويمكن للتعاون على الصـعيدين الإقليمي والدولي، بما في ذلك بين الأفرقة الوطنية للتصـدي للطوارئ الحاسوبية/الأفرقة الوطنية للاستجابة لحوادث أمن الفضاء الإلكتروني، وسلطات الدول المعنية بتكنولوجيات المعلومات والاتصالات والأوساط الدبلوماسية، أن يعزز قدرة الدول على اكتشاف الحوادث الخبيثة في مجال تكنولوجيا المعلومات والاتصالات والتحقيق فيها وإثبات شواغلها واستنتاجاتها بالأدلة قبل التوصل إلى نتيجة بشأن حادث ما.

28 - ويمكن للدول أيضا أن تستخدم منابر متعددة الأطراف وإقليمية وثنائية ومتعددة أصحاب المصلحة لإطلاع بعضها بعضا على ممارساتها وتبادل المعلومات بشأن النهج الوطنية المتبعة في تحديد الجهة الفاعلة، بما في ذلك كيفية التمييز بين مختلف أنواع هذا التحديد، وبشـأن التهديدات والحوادث المتعلقة بتكنولوجيا المعلومات والاتصالات. ويوصي الفريق أيضا بأن ينظر العمل المقبل في الأمم المتحدة أيضا في كيفية تعزيز الفهم المشترك بشأن تحديد الجهة الفاعلة وتبادل الممارسات بهذا الخصوص.

القاعدة 13 (ج): ينبغي ألا تسمح الدول عن علم باستخدام أراضيها لارتكاب أفعال غير مشروعة دولياً باستخدام تكنولوجيات المعلومات والاتصالات.

29 - تعكس هذه القاعدة توقعاً بأن تتخذ الدولة، إذا علمت أن فعلاً غير مشروع دولياً يجري بواسطة تكنولوجيات المعلومات والاتصالات ينطلق من إقليمها أو يمر عبره، أو أُخطرت بذلك بحسن نية، كل الخطوات المناسبة والمتاحة بصورة معقولة والممكنة لاكتشاف الحالة والتحقيق فيها ومعالجتها. وتشير القاعدة إلى فهمٍ مؤداه أن الدولة ينبغي ألا تسمح لدولة أخرى أو لجهة فاعلة من غير الدول بأن تستخدم في أراضيها تكنولوجيات المعلومات والاتصالات لارتكاب أفعال غير مشروعة دوليا.

30 - ولدى النظر في كيفية تحقيق أهداف هذه القاعدة، ينبغي للدول أن تضع في اعتبارها ما يلي:

(أ) تثير هذه القاعدة توقع أن تتخذ الدولة خطوات معقولة في حدود قدرتها لإنهاء النشاط الجاري في أراضيها بوسائل متناسبة وملائمة وفعالة وبطريقة تتسق مع القانون الدولي والمحلي. ومع ذلك، لا يتوقع أن يكون من الممكن أو الواجب أن ترصد الدول جميع أنشطة تكنولوجيا المعلومات والاتصالات داخل أراضيها.

(ب) يجوز للدولة التي تعلم بارتكاب أفعال غير مشروعة دوليا في أراضيها باستخدام تكنولوجيات المعلومات والاتصالات، ولكنها تفتقر إلى القدرة على التصدي لتلك الأفعال، أن تنظر في طلب المساعدة من دول أخرى أو من القطاع الخاص بطريقة تتفق مع القانون الدولي والمحلي. وقد يدعم إنشاء هياكل وآليات ذات صلة لصياغة طلبات المساعدة والاستجابة لها تنفيذ هذه القاعدة. وينبغي للدول عند تقديم المساعدة أن تتصرف بحسن نية ووفقا للقانون الدولي وألا تستغل الفرصة للقيام بأنشطة خبيثة ضد الدولة التي تلتمس المساعدة أو ضد دولة ثالثة.

(ج) ينبغي للدولة المتضررة أن تخطر الدولة التي يصدر عنها النشاط. وينبغي للدولة المخطَرة أن تفيد بتلقي الإخطار لتيسير التعاون والتوضيح وأن تبذل كل جهد معقول للمساعدة في تحديد ما إذا كان فعل غير مشروع دوليا قد ارتكب. ولا تشير الإفادة باستلام هذا الإخطار إلى الموافقة على المعلومات الواردة فيه.

(د) لا يعني صدور حادث تكنولوجيا المعلومات والاتصالات من إقليم دولة ثالثة أو بنيتها التحتية، في حد ذاته، مسؤولية تلك الدولة عن الحادث. كما أن إخطار دولة ما بأن إقليمها يُستخدم في ارتكاب فعل غير مشروع لا يعني في حد ذاته أنها مسؤولة عن ذلك الفعل ذاته.

القاعدة 13 (د): ينبغي للدول أن تنظر في أفضل سبل التعاون على تبادل المعلومات، ومساعدة بعضها البعض، ومقاضاة 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.

31 - هذه القاعدة تذكر الدول بأهمية التعاون الدولي على التصدي للتهديدات العابرة للحدود التي يشكلها استخدام شبكة الإنترنت وتكنولوجيات المعلومات والاتصالات لأغراض إجرامية وإرهابية، بما في ذلك التجنيد والتمويل والتدريب والتحريض والتخطيط للهجمات وتنسيقها والترويج للأفكار والأعمال ذات الصلة، وغير ذلك من الأغراض التي يبرزها هذا التقرير. وتسلم القاعدة بأن التقدم المحرز في التصدي لهذه

التهديدات وغيرها من التهديدات التي تشمل الجماعات الإرهابية والإجرامية والإرهابيين والمجرمين الأفراد من خلال التدابير القائمة وغيرها من التدابير يمكن أن يسهم في استتباب السلام والأمن الدوليين.

32 - ويعني التقيد بهذه القاعدة وجود سياسات وتشريعات وهياكل وآليات وطنية تيسر التعاون عبر الحدود بشأن المسائل التقنية، ومسائل إنفاذ القانون، والمسائل القانونية والدبلوماسية ذات الصلة بمعالجة الاستخدام الإجرامي والإرهابي لتكنولوجيات المعلومات والاتصالات.

33 - وتُشجَّع الدول على تعزيز ومواصلة تطوير آليات من شأنها تيسير تبادل المعلومات والمساعدة بين المنظمات الوطنية والإقليمية والدولية ذات الصلة من أجل إذكاء الوعي بأمن تكنولوجيات المعلومات والاتصالات بين الدول وتقليص حيز العمل المتاح للأنشطة الإرهابية والإجرامية على الإنترنت. ويمكن لهذه الآليات أن تعزز قدرة المنظمات والوكالات ذات الصلة، وأن تعمل في الوقت نفسه على بناء الثقة بين الدول وتعزيز سلوك الدول المسؤول. وتُشجَّع الدول أيضا على وضع بروتوكولات وإجراءات مناسبة لجمع وتجهيز وتخزين الأدلة الموجودة على الإنترنت بشأن استخدام تكنولوجيات المعلومات والاتصالات لأغراض إجرامية وإرهابية، وعلى تقديم المساعدة في التحقيقات في الوقت المناسب، بما يكفل اتخاذ هذه الإجراءات وفقاً لالتزامات الدولة بموجب القانون الدولي.

34 - وفي إطار الأمم المتحدة، يتصدى عدد من المحافل المكرسة والعمليات والقرارات تحديدا للتهديدات التي يشكلها استخدام تكنولوجيات المعلومات والاتصالات في أغراض إرهابية وإجرامية والنهج التعاونية اللازمة للتصدي لهذه التهديدات. وتشمل قرارات الجمعية العامة ذات الصلة القرار 230/65 بشأن مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية الذي يقضي بإنشاء فريق خبراء حكومي دولي مفتوح العضوية لإجراء دراسة شاملة لمشكلة الجريمة السيبرانية؛ والقرار 173/74 بشأن تعزيز المساعدة التقنية وبناء القدرات لتدعيم التدابير الوطنية والتعاون الدولي في مكافحة استخدام تكنولوجيات المعلومات والاتصالات لأغراض إجرامية، بما يشمل تبادل المعلومات؛ والقرار 247/74 بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية.

35 - ويمكن للدول أيضا أن تستخدم العمليات والمبادرات والصكوك القانونية القائمة وأن تنظر في إنشاء إجراءات أو قنوات اتصال إضافية لتيسير تبادل المعلومات والمساعدة للتصدي لاستخدام تكنولوجيات المعلومات والاتصالات في أغراض إرهابية وإجرامية. وفي هذا الصدد، تشجَّع الدول على مواصلة تعزيز الجهود الجارية على مستوى الأمم المتحدة وعلى الصعيد الإقليمي للتصدي لاستخدام الإنترنت وتكنولوجيات المعلومات والاتصالات في أغراض إرهابية وإجرامية، وإقامة شراكات تعاونية مع المنظمات الدولية والجهات الفاعلة في القطاع المعني والأوساط الأكاديمية والمجتمع المدني لتحقيق هذه الغاية.

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

36 - تذكِّر هذه القاعدة الدول باحترام وحماية حقوق الإنسان والحريات الأساسية، سواء على الإنترنت أو خارجها وفقا لالتزامات كل منها. ومما يتطلب اهتماما خاصا في هذا الصدد الحقُ في حرية التعبير، بما في ذلك حرية التماس المعلومات وتلقيها ونقلها إلى الآخرين بغض النظر عن الحدود وباستخدام أي

وسيلة، وغير ذلك من الأحكام ذات الصلة المنصوص عليها في العهد الدولي الخاص بالحقوق المدنية والسياسية، والعهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية، وكما هو منصوص عليه في الإعلان العالمي لحقوق الإنسان. ويمكن أن يسهم التقيد بهذه القاعدة أيضا في تعزيز عدم التمييز وتضييق الفجوة الرقمية، بما في ذلك ما يتعلق بنوع الجنس.

37 - ويشكل اتخاذ القرارات المشار إليها في هذه القاعدة وغيرها من القرارات التي اتخذت منذ ذلك الحين إقرارا بالتحديات والمعضلات الجديدة التي ظهرت حول استخدام الدول لتكنولوجيات المعلومات والاتصالات وبما يقترن بذلك من حاجة إلى التصدي لها. وقد يكون لممارسات الدول، مثل المراقبة الجماعية التعسفية أو غير القانونية، آثار سلبية للغاية على ممارسة حقوق الإنسان والتمتع بها، ولا سيما الحق في الخصوصية.

38 - وينبغي للدول، لدى تنفيذ هذه القاعدة، أن تنظر في توجيهات محددة واردة في القرارات المذكورة. وينبغي لها أيضا أن تحيط علما بالقرارات الجديدة التي اتخذت منذ تقرير فريق الخبراء الحكوميين لعام 2015 وأن تسهم في قرارات جديدة قد يلزم طرحها في ضوء التطورات الجارية.

39 - وينبغي أن تكون الجهود التي تبذلها الدول لتشجيع احترام ومراعاة حقوق الإنسان وضمان الاستخدام المسؤول والمأمون لتكنولوجيات المعلومات والاتصالات جهوداً متكاملة ومتعاضدة ومترابطة. فهذا النهج يشجع على تهيئة بيئة منفتحة وآمنة ومستقرة وميسَّرة وسلمية لهذه التكنولوجيات. ويمكنه أيضا الإسهام في تحقيق أهداف التنمية المستدامة.

40 - ومع التسليم بأهمية الابتكار التكنولوجي بالنسبة لجميع الدول، فقد تترتب على التكنولوجيات الجديدة والناشئة أيضا آثار هامة في مجال حقوق الإنسان وأمن تكنولوجيات المعلومات والاتصالات. ولمعالجة هذا الأمر، قد تنظر الدول في الاستثمار في وضع تدابير تقنية وقانونية لتوجيه تطوير واستخدام تكنولوجيات المعلومات والاتصالات، وفي تعزيز تلك التدابير، وذلك على نحو أكثر شمولاً وتيسُّرا ولا يؤثر سلبا على فرادى المجتمعات أو الفئات.

41 - ويلاحظ الفريق أن عدداً من المنتديات مكرس في الأمم المتحدة لمعالجة قضايا حقوق الإنسان على وجه التحديد. وبالإضافة إلى ذلك، يقر الفريق بأن مجموعة متنوعة من أصحاب المصلحة تسهم بطرق مختلفة في حماية وتعزيز حقوق الإنسان والحريات الأساسية على الإنترنت وخارجها. ويمكن لإشراك هذه الأصوات في عمليات صنع السياسات ذات الصلة بأمن تكنولوجيات المعلومات والاتصالات أن يدعم الجهود المبذولة لتعزيز حقوق الإنسان وحمايتها والتمتع بها على الإنترنت، وأن يساعد على توضيح وتقليل الآثار السلبية المحتملة للسياسات على الأشخاص، بمن فيهم الأشخاص الذين يعيشون في أوضاع هشة.

القاعدة 13 (و): ينبغي للدولة ألا تنفذ، أو تدعم عن علم، أي نشاط من أنشطة تكنولوجيات المعلومات والاتصالات يتعارض مع التزاماتها بموجب القانون الدولي ويضر عمدا بالبنية التحتية الحيوية المستخدمة في تقديم الخدمات إلى الجمهور أو يعطل، بأي شكل آخر، استخدام تلك البنية التحتية الحيوية وتشغيلها.

42 - فيما يتعلق بهذه القاعدة، فإن النشاط الذي يمارَس باستخدام تكنولوجيات الاتصالات والمعلومات ويُقصد به الإضرار بالبنية التحتية الحيوية المستخدمة في تقديم الخدمات إلى الجمهور أو يعطل، بأي شكل آخر، استخدام تلك البنية التحتية الحيوية وتشغيلها، يمكن أن تكون له آثار محلية وإقليمية وعالمية متتالية. ويهدد هذا النشاط بشدة بإلحاق ضرر بالسكان، ويمكن أن يكون تصعيديا، وقد يفضي إلى نشوب نزاع.

43 - وتشير القاعدة أيضا إلى الأهمية القصوى للبنية التحتية الحيوية بوصفها ثروة وطنية، نظرا إلى أن هذه البنية التحتية تشكل العمود الفقري للوظائف والخدمات والأنشطة الحيوية للمجتمع. وإذا ما لحقها تعطل أو تلف، فإن التكلفة البشرية والآثار على اقتصاد الدولة وتنميتها وأدائها السياسي والاجتماعي وأمنها الوطني قد تكون باهظة.

44 - وعلى نحو ما أشارت إليه القاعدة 13 (ز)، ينبغي أن تتخذ الدول التدابير المناسبة لحماية بنيتها التحتية الحيوية. وفي هذا الصدد، تحدد كل دولة البنية التحتية أو القطاعات التي تعتبرها حيوية في نطاق ولايتها، بما يتفق مع أولوياتها الوطنية والطرق التي تتبعها في تصنيف البنية التحتية الحيوية.

45 - وقد أدت جائحة كوفيد-19 إلى زيادة الوعي بالأهمية الحاسمة لحماية البنى التحتية والمرافق الطبية والمتعلقة بالرعاية الصحية، بما في ذلك حمايتها من خلال تنفيذ القواعد التي تتناول البنية التحتية الحيوية (مثل هذه القاعدة والقاعدتين (ز) و(ح)). ومن بين الأمثلة على قطاعات البنية التحتية الحيوية التي تقدم خدمات أساسية للجمهور قطاعات الصحة، وتوليد الكهرباء، والمياه والصرف الصحي، والتعليم، والخدمات التجارية والمالية، والنقل، والاتصالات، والعمليات الانتخابية. وقد تشير البنية التحتية الحيوية أيضا إلى البنى التحتية التي توفر خدمات عبر عدة دول، مثل البنية التحتية التقنية الضرورية للتوافر العام لشبكة الإنترنت وسلامتها. ويمكن أن تكون تلك البنية التحتية ذات أهمية قصوى للتجارة الدولية، أو الأسواق المالية، أو قطاع النقل العالمي، أو الاتصالات، أو الصحة، أو العمل الإنساني. وإبراز هذه البنى التحتية بوصفها أمثلة لا يمنع، بأي حال من الأحوال، الدول من تحديد بنى تحتية أخرى على أنها حيوية، ولا يُعتبر غضاً للطرف عن الأنشطة الخبيثة التي تستهدف فئات البنية التحتية التي لم تحدَّد أعلاه.

46 - ومن أجل دعم تنفيذ القاعدة، تُشجع الدول، إلى جانب مراعاة العوامل المحددة أعلاه، على أن تتخذ تدابير ذات صلة على الصعيد الوطني في مجال السياسات العامة والمجال التشريعي لضمان أن تكون أنشطة تكنولوجيات المعلومات والاتصالات التي تنفذها أو تدعمها دولة ما، والتي قد تؤثر على البنية التحتية الحيوية لدولة أخرى أو على تقديم الخدمات العامة الأساسية فيها، متسقة مع هذه القاعدة، وأن تُستخدم وفقا لالتزاماتها القانونية الدولية، وأن تخضع لاستعراض ورقابة شاملين.

القاعدة 13 (ز): ينبغي أن تتخذ الدول التدابير المناسبة لحماية بنيتها التحتية الحيوية من التهديدات المرتبطة بتكنولوجيات المعلومات والاتصالات، آخذة في اعتبارها قرار الجمعية العامة 199/58.

47 - تؤكد هذه القاعدة من جديد التزام جميع الدول بحماية البنية التحتية الحيوية الخاضعة لولايتها من التهديدات المرتبطة بتكنولوجيات المعلومات والاتصالات، وأهمية التعاون الدولي في هذا الصدد.

48 - وتحديد الدولة لبنيةٍ تحتية أو قطاعٍ من القطاعات على أنهما حيويان يمكن أن يكون مفيدا لحماية تلك البنية التحتية أو ذلك القطاع. وبالإضافة إلى قيام كل دولة بتحديد البنى التحتية أو قطاعاتها اللتين تعتبرهما حيويتين، فإنها تحدد التدابير الهيكلية والتقنية والمؤسسية والتشريعية والتنظيمية الضرورية لحماية بنيتها التحتية الحيوية وإعادتها إلى العمل في حال وقوع حادث ما. ويبرز قرار الجمعية العامة 199/58 بشأن إرساء ثقافة عالمية لأمن الفضاء الإلكتروني وحماية البنية التحتية الحيوية للمعلومات ومرفقه[3]، الإجراءات التي يمكن للدول أن تتخذها على الصعيد الوطني لهذا الغرض.

(3) A/RES/58/199، وهو جزء من مجموعة من ثلاثة قرارات منها قرارا الجمعية العامة A/RES/57/239 و A/RES/64/211.

49 - وتوجد في بعض الدول بنى تحتية تقدم خدمات على الصعيد الإقليمي أو الدولي. وتهديدات تكنولوجيات المعلومات والاتصالات لتلك البنية التحتية يمكن أن يكون لها آثار مزعزِعة للاستقرار. ويمكن للدول المشاركة في هذه الترتيبات أن تشجع التعاون عبر الحدود مع مالكي البنية التحتية ومشغليها المعنيين من أجل تعزيز تدابير أمن تكنولوجيات المعلومات والاتصالات المخصصة لتلك البنية التحتية، وتقوية العمليات والإجراءات القائمة - أو وضع عمليات وإجراءات مكملة لها - لكشف وتخفيف وطأة الحوادث المرتبطة بتكنولوجيات المعلومات والاتصالات التي تؤثر على تلك البنية التحتية.

50 - ومن شأن تشجيع اتخاذ تدابير لضمان سلامة وأمن منتجات تكنولوجيا المعلومات والاتصالات طوال دورة حياتها أو لتصنيف حوادث تكنولوجيا المعلومات والاتصالات من حيث حجمها وخطورتها أن يسهم أيضا في تحقيق هدف هذه القاعدة.

القاعدة 13 (ح): ينبغي أن تستجيب الدول لطلبات ا لمساعدة المناسبة التي تأتيها من دولة أخرى تتعرض بنيتها التحتية الحيوية لأعمال خبيثة باستخدام تكنولوجيات المعلومات والاتصالات. وينبغي أن تستجيب الدول أيضا للطلبات المناسبة للتخفيف من ضرر نشاط من أنشطة تكنولوجيات المعلومات والاتصالات ينطلق من أراضيها ويستهدف البنية التحتية الحيوية لدولة أخرى، مع مراعاة السيادة على النحو الواجب.

51 - تذكِّر هذه القاعدة الدول بأن التعاون والحوار الدوليين، وإيلاء الاعتبار الواجب لسيادة جميع الدول، أمور أساسية للاستجابة لطلبات المساعدة التي تقدمها دولة أخرى تتعرض بنيتها التحتية الحيوية لأعمال خبيثة باستخدام تكنولوجيات المعلومات والاتصالات. وتكتسي هذه القاعدة أهمية خاصة عندما يتصل الأمر بالأعمال التي يمكن أن تهدد السلام والأمن الدوليين.

52 - وينبغي للدول، لدى تلقيها طلب المساعدة، أن تقدم أي مساعدة تكون لديها القدرة والموارد اللازمة لتقديمها، وأن تكون تلك المساعدة متاحة على نحو معقول وعملية في ظل الظروف السائدة. ويجوز للدولة أن تختار المساعدة على صعيد ثنائي، أو من خلال ترتيبات إقليمية أو دولية. ويجوز للدول أيضا أن تسعى للحصول على خدمات القطاع الخاص للاستعانة بها في الاستجابة لطلبات المساعدة.

53 - وامتلاك الهياكل والآليات الوطنية الضرورية لاكتشاف وتخفيف ضرر حوادث تكنولوجيات المعلومات والاتصالات المحتمل أن تهدد السلام والأمن الدوليين يمكِّن من التنفيذ الفعال لهذه القاعدة. وتكمّل هذه الآلياتُ الآليات القائمة التي تضطلع بالإدارة والمعالجة اليوميتين للحوادث المرتبطة بتكنولوجيات المعلومات والاتصالات. فعلى سبيل المثال، ستعود على الدولة التي ترغب في طلب مساعدة دولة أخرى فائدة من معرفة الجهة المناسبة التي ينبغي أن تتصل بها وكذلك قناة الاتصال التي يجب أن تستخدمها لذلك الغرض. ويتعين على الدولة التي تتلقى طلب مساعدة أن تحدد، على نحو شفاف وفي الوقت المناسب قدر المستطاع، ومع احترام الطابع الملح والحساس للطلب، ما إذا كانت تملك القدرات والإمكانيات والموارد التي تتيح لها تقديم المساعدة المطلوبة. ولا يُتوقع من الدول التي تُطلب مساعدتها أن تضمن تحقيق نتيجة معينة.

54 - ويمكن أن يتيسر التعاون الذي تصفه هذه القاعدة باتباع عمليات وإجراءات موحدة وشفافة لطلب المساعدة من دولة أخرى وللاستجابة لطلبات المساعدة. ويمكن في هذا الصدد أن يكفل استخدام نماذج موحدة لطلب المساعدة والاستجابة لها قيام الدولة التي تطلب المساعدة بموافاة الدولة التي تسعى إلى الحصول على مساعدتها، بمعلومات كاملة ودقيقة قدر الإمكان، مما ييسر التعاون وحسن توقيت

الاستجابة للطلب. ويمكن وضع هذه النماذج طوعا على المستويات الثنائي أو المتعدد الأطراف أو الإقليمي. ويمكن أن يتضمن نموذج موحد للاستجابة لطلبات المساعدة مكاناً يُفاد فيه بتلقي الطلب، وفي حالة تيسُّر تقديم المساعدة، أماكنَ يبيَّن فيها الإطار الزمني للمساعدة التي يمكن تقديمها وطبيعتها ونطاقها وشروطها.

55 - وحيثما يكون النشاط الخبيث صادرا عن إقليم دولة معينة، فمن شأن عرضها تقديم المساعدة المطلوبة وتقديمها فعلا أن يساهما في التقليل إلى أدنى حد ممكن من الأضرار، وتفادي التصورات الخاطئة، وتقليص خطر التصعيد والمساعدة على استعادة الثقة. ويمكن أن يتعزز الامتثال لهذه القاعدة من خلال المشاركة في آليات تعاونية تُحدد وسائل وطرق الاتصال في حالات الأزمات ووسائل وطرق التعامل مع الحوادث ومعالجتها.

القاعدة 13 (ط): ينبغي أن تتخذ الدول خطوات معقولة لكفالة سلامة سلسلة الإمداد حتى يمكن للمستخدمين النهائيين الوثوق بأمن منتجات تكنولوجيات المعلومات والاتصالات. وينبغي للدول أن تسعى إلى منع انتشار أدوات وتقنيات تكنولوجيات المعلومات والاتصالات الخبيثة واستخدام الوظائف الخفية الضارة.

56 - تسلم هذه القاعدة بالحاجة إلى تعزيز ثقة المستعمل النهائي في بيئة تكنولوجيا المعلومات والاتصالات المنفتحة والآمنة والمستقرة والميسرة والسلمية واطمئنانه إليها. ويشكل ضمان سلامة سلسلة إمداد تكنولوجيات المعلومات والاتصالات وأمن منتجات تكنولوجيات المعلومات والاتصالات، ومنع انتشار الأدوات والتقنيات الخبيثة لهذه التكنولوجيات واستخدام الوظائف الخفية الضارة، أمرين حاسمين بشكل متزايد في هذا الصدد، ويشكلان كذلك أمرين حاسمين بشكل متزايد للأمن الدولي والتنمية الرقمية والتنمية الاقتصادية الأوسع نطاقا.

57 - وسلاسل الإمداد العالمية لتكنولوجيات المعلومات والاتصالات واسعة النطاق، وتزداد تعقيدا وترابطا، وتشمل أطرافا مختلفة كثيرة. ويمكن أن تشمل الخطوات المعقولة لتعزيز انفتاح سلسلة الإمداد وضمان سلامتها واستقرارها وأمنها ما يلي:

(أ) وضع أطر وآليات شاملة وشفافة وموضوعية ومحايدة على الصعيد الوطني بشأن إدارة مخاطر سلسلة الإمداد، بما يتماشى مع الالتزامات الدولية للدولة. ويمكن أن تشمل هذه الأطر تقييمات مخاطر تأخذ في الحسبان طائفة من العوامل، بما في ذلك فوائد التكنولوجيات الجديدة.

(ب) وضع سياسات وبرامج للتشجيع بصورة موضوعية على اعتماد موردي وبائعي معدات ونظم تكنولوجيا المعلومات والاتصالات للممارسات الجيدة من أجل بناء الثقة الدولية في سلامة وأمن منتجات وخدمات تكنولوجيات المعلومات والاتصالات، وتعزيز الجودة، وتشجيع الاختيار.

(ج) إيلاء اهتمام أكبر، في السياسات الوطنية والحوار مع الدول والجهات الفاعلة المعنية في الأمم المتحدة وغيرها من المنتديات، لمسألة كفالة أن تتنافس جميع الدول وتبتكر على قدم المساواة، بهدف التمكين من الاستفادة الكاملة من تكنولوجيات المعلومات والاتصالات في زيادة التنمية الاجتماعية والاقتصادية على الصعيد العالمي والإسهام في صون السلام والأمن الدوليين، مع حماية الأمن الوطني والمصلحة العامة في الوقت نفسه.

(د) اتخاذ تدابير تعاونية من قبيل تبادل الممارسات الجيدة، على الصعد الثنائي والإقليمي والمتعدد الأطراف، بشأن إدارة مخاطر سلسلة الإمداد؛ ووضع وتنفيذ قواعد ومعايير موحدة لأمن سلسلة الإمداد قابلة للتطبيق المشترك على الصعيد العالمي؛ ووضع نهج أخرى رامية إلى تقليص مواطن الضعف في سلسلة الإمداد.

58 - ولمنع استحداث وانتشار أدوات وتقنيات تكنولوجيا المعلومات والاتصالات الخبيثة واستخدام الوظائف الخفية الضارة، بما في ذلك الأبواب الخلفية، يمكن للدول أن تنظر في تطبيق ما يلي على الصعيد الوطني:

(أ) تدابير لتعزيز سلامة سلسلة الإمداد، بما في ذلك تعزيزها عن طريق إلزام بائعي تكنولوجيات المعلومات والاتصالات بجعل السلامة والأمن عنصرا أساسيا في تصميم منتجات تكنولوجيا المعلومات والاتصالات وإنشائها وطوال دورة حياتها. وتحقيقا لهذه الغاية، يمكن للدول أيضا أن تنظر في وضع إجراءات مستقلة ومحايدة لمنح التراخيص.

(ب) ضمانات تشريعية وضمانات أخرى تعزز حماية البيانات والخصوصية.

(ج) تدابير لحظر إدخال وظائف سرية ضارة واستغلال مواطن الضعف في منتجات تكنولوجيا المعلومات والاتصالات اللذين قد يقوضان سرية النظم والشبكات وسلامتها وبقاءها قيد التشغيل، بما يشمل البنية التحتية الحيوية.

59 - وبالإضافة إلى الخطوات والتدابير الموجزة أعلاه، ينبغي للدول أن تواصل تشجيع القطاع الخاص والمجتمع المدني على القيام بدور مناسب لتحسين أمن تكنولوجيات المعلومات والاتصالات وبدور ملائم في تحسين مأمونية استخدامها، بما في ذلك أمن سلسلة الإمداد بمنتجات تكنولوجيات المعلومات والاتصالات، لتسهم بذلك في الوفاء بأهداف هذه القاعدة.

القاعدة 13 (ي): ينبغي للدول تشجيع الإبلاغ المسؤول عن مواطن الضعف في تكنولوجيات المعلومات والاتصالات وأن تقدم ما لديها من معلومات ذات صلة حول الوسائل المتاحة لعلاجها من أجل تقليل، وربما استئصال، التهديدات المحتملة التي تتعرض لها تكنولوجيات المعلومات والاتصالات والبنية التحتية المعتمِدة على هذه التكنولوجيات.

60 - تذكّر هذه القاعدة الدول بأهمية ضمان التعجيل بمعالجة مواطن الضعف في تكنولوجيات المعلومات والاتصالات من أجل تقليص إمكانية استغلالها من جانب جهات فاعلة خبيثة. ومن شأن اكتشاف مواطن الضعف في تكنولوجيات المعلومات والاتصالات والكشف والإبلاغ عنها بشكل مسؤول أن يمنع الممارسات الضارة أو الخطرة، ويزيد من مستوى الاطمئنان والثقة، ويقلص الأخطار ذات الصلة التي تهدد الأمن والاستقرار الدوليين.

61 - وتهدف سياسات وبرامج الكشف عن مواطن الضعف، إلى جانب التعاون الدولي ذي الصلة، إلى توفير إجراءات موثوقة ومتسقة لجعل عمليات الكشف تلك عمليات روتينية. ومن شأن عملية منسقة للكشف عن مواطن الضعف التقليلُ إلى أدنى حد من الضرر الذي تُلحقه المنتجات السهلة الاختراق بالمجتمع، وتنظيمُ الإبلاغ عن مواطن الضعف في تكنولوجيات المعلومات والاتصالات وطلبات المساعدة بين البلدان وأفرقة الاستجابة لحالات الطوارئ. وينبغي أن تكون تلك العمليات متسقة مع التشريعات المحلية.

62 - وعلى الصعد الوطني والإقليمي والدولي، يمكن للدول أن تنظر في تطبيق أطر قانونية وسياسات وبرامج لتوجيه عملية اتخاذ القرارات بشأن التعامل مع مواطن الضعف في تكنولوجيات المعلومات والاتصالات وكبح استغلالها تجارياً، بوصف ذلك وسيلة للحماية من سوء الاستخدام الذي قد يشكل خطرا على السلام والأمن الدوليين أو حقوق الإنسان والحريات الأساسية. ويمكن للدول أيضا أن تنظر في إتاحة سبل حماية قانونية للباحثين وللخبراء في مجال اختبار الاختراق.

63 - وبالإضافة إلى ذلك، وبالتشاور مع القطاع المعني والجهات الفاعلة الأخرى في مجال أمن تكنولوجيات المعلومات والاتصالات، تستطيع الدول وضع توجيهات وحوافز، بما يتسق مع المعايير التقنية الدولية ذات الصلة، بشأن الإبلاغ المسؤول عن مواطن الضعف وإدارتها ودور كلٍ من أصحاب المصلحة المختلفين ومسؤولياته فيما يخص عمليات الإبلاغ؛ وأنواع المعلومات التقنية التي يجب الكشف عنها أو مشاركتها علنا، بما في ذلك مشاركة المعلومات التقنية بشأن الحوادث الخطيرة المرتبطة بتكنولوجيات المعلومات والاتصالات؛ وكيفية التعامل مع البيانات الحساسة وضمان أمن المعلومات وسريتها.

64 - ومن الممكن أن تكون توصياتُ أفرقة الخبراء الحكوميين السابقة المتعلقة ببناء الثقة والتعاون الدولي، والمساعدة وبناء القدرات، مفيدة بشكل خاص في تطوير فهم مشترك للآليات والعمليات التي يمكن أن تطبقها الدول للكشف المسؤول عن مواطن الضعف. ويمكن للدول أن تنظر في أن تستخدم لهذا الغرض الهيئات المتعددة الأطراف والإقليمية ودون الإقليمية القائمة وغيرها من القنوات والمنابر ذات الصلة التي تشارك فيها جهات مختلفة من أصحاب المصلحة.

القاعدة 13 (ك): ينبغي للدول ألا تنفذ، أو تدعم عن علم، أي نشاط يُلحق الضرر بنظم المعلومات الخاصة بالأفرقة المفوضة للاستجابة لحالات الطوارئ (المعروفة أحياناً بأفرقة مواجهة الطوارئ الحاسوبية أو أفرقة الاستجابة لحوادث أمن الفضاء الإلكتروني) التابعة لدولة أخرى. وينبغي ألا تستخدم أي دولة الأفرقة المفوضة للاستجابة لحالات الطوارئ في القيام بأنشطة دولية خبيثة.

65 - تعكس هذه القاعدة واقع أن لأفرقة مواجهة الطوارئ الحاسوبية/أفرقة الاستجابة لحوادث أمن الفضاء الإلكتروني أو غيرها من هيئات الاستجابة المفوضة، مسؤولياتٍ ووظائفَ في إدارة وعلاج الحوادث المرتبطة بتكنولوجيات المعلومات والاتصالات، وهي بذلك تضطلع بدور مهم في المساهمة في صون السلام والأمن الدوليين. وهذه الأفرقة والهيئات ضرورية للاكتشاف والتخفيف الفعالين للآثار السلبية الفورية والطويلة الأمد للحوادث المرتبطة بتكنولوجيات المعلومات والاتصالات. ومن شأن الضرر الذي يَلحق بأفرقة مواجهة الطوارئ أن يقوض الثقة ويعوق قدرتها على أداء وظائفها، وقد يكون له عواقب أوسع نطاقا وغير متوقعة في الغالب على جميع القطاعات، وربما على السلام والأمن الدوليين. ويؤكد الفريق أهمية تجنب تسييس أفرقة مواجهة الطوارئ الحاسوبية/أفرقة الاستجابة لحوادث أمن الفضاء الإلكتروني واحترام الطابع المستقل لوظائفها.

66 - واعترافا بالدور الحاسم الذي تؤديه أفرقة مواجهة الطوارئ الحاسوبية/أفرقة الاستجابة لحوادث أمن الفضاء الإلكتروني في حماية الأمن القومي والجمهور ومنع حدوث خسائر اقتصادية ناجمة عن الحوادث المرتبطة بتكنولوجيات المعلومات والاتصالات، فإن العديد من الدول تصنف تلك الأفرقة على أنها جزء من بنيتها التحتية الحيوية.

67 - ولدى النظر في الكيفية التي قد تسهم بها الإجراءات التي تتخذها الدول فيما يخص أفرقة مواجهة الطوارئ في السلام والأمن الدوليين، فإن بإمكانها أن تعلن أو تتخذ تدابير تؤكد أنها لن تستخدم أفرقة

مواجهة الطوارئ المفوضة في القيام بأنشطة دولية خبيثة، وأنها تدرك وتحترم ميادين عمل تلك الأفرقة والمبادئ الأخلاقية التي توجه ذلك العمل. ويحيط الفريق علما بالمبادرات الناشئة في هذا الصدد.

68 - ويمكن للدول أن تنظر أيضا في اتخاذ تدابير أخرى مثل إنشاء إطار وطني لإدارة حوادث أمن تكنولوجيات المعلومات والاتصالات تحدد فيه الأدوار والمسؤوليات المعينة، بما في ذلك تلك التي تخص أفرقة مواجهة الطوارئ الحاسوبية/أفرقة الاستجابة لحوادث أمن الفضاء الإلكتروني، وذلك لتيسير التعاون والتنسيق بين هذه الأفرقة وغيرها من الهيئات الأمنية والتقنية ذات الصلة على الصعد الوطني والإقليمي والدولي. ويمكن أن يشمل هذا الإطار سياسات أو تدابير تنظيمية أو إجراءات توضح مركز هذه الأفرقة وسلطتها وولايتها، وتميز الوظائفَ الفريدة التي تؤديها عن الوظائف الأخرى التي تؤديها الحكومة.

رابعا - القانون الدولي

69 - القانون الدولي هو أساس التزام الدول المشترك بمنع نشوب النزاعات وصون السلام والأمن الدوليين، وهو مفتاح تعزيز الثقة بين الدول. ويعيد الفريق، لدى نظره في كيفية انطباق القانون الدولي على استخدام الدول لتكنولوجيات المعلومات والاتصالات، تأكيد التقييمات والتوصيات المتعلقة بالقانون الدولي الواردة في تقارير أفرقة الخبراء الحكوميين السابقة، ولا سيما أن القانون الدولي، وخصوصا ميثاق الأمم المتحدة، قابل للتطبيق وضروري لصون السلام والاستقرار والتشجيع على توافر بيئة منفتحة وآمنة ومستقرة وميسرة وسلمية لتكنولوجيات المعلومات والاتصالات. وتؤكد هذه التقييمات والتوصيات، بالاقتران مع عناصر موضوعية أخرى في التقارير السابقة، أن تقيد الدول بالقانون الدولي، ولا سيما التزاماتها بموجب الميثاق، هو إطار أساسي للإجراءات التي تتخذها عند استخدامها لتكنولوجيات المعلومات والاتصالات.

70 - وفي هذا الصدد، أكد الفريق من جديد التزامات الدول بالمبادئ التالية للميثاق وغيره من قواعد القانون الدولي: المساواة 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 لأية دولة، أو بأية طريقة أخرى تتعارض مع مقاصد الأمم المتحدة؛ واحترام حقوق الإنسان والحريات الأساسية؛ وعدم التدخل في الشؤون الداخلية للدول الأخرى.

71 - وإضافة إلى عمل أفرقة الخبراء الحكوميين السابقة، يقدم الفريق الحالي، مسترشدا بالميثاق والولاية الواردة في القرار 266/73، مستوى إضافيا من الفهم لتقييمات وتوصيات فريق الخبراء الحكوميين لعام 2015 بشأن كيفية انطباق القانون الدولي على استخدام الدول لتكنولوجيات المعلومات والاتصالات، وذلك على النحو التالي:

(أ) يلاحظ الفريق أن الدول الأطراف في أي نزاعات دولية، بما فيها تلك المتعلقة باستخدام تكنولوجيات المعلومات والاتصالات، يحتمل أن يعرض استمرارها صون السلام والأمن الدوليين للخطر، يتعين عليها، وفقا لالتزاماتها بموجب المادة 2 (3) والفصل السادس من ميثاق الأمم المتحدة، أن تسعى أولا وقبل كل شيء إلى إيجاد حل بالوسائل المبينة في المادة 33 من الميثاق، وهي المفاوضة والتحقيق والوساطة والتوفيق والتحكيم والتسوية القضائية، أو أن تلجأ إلى الوكالات والترتيبات الإقليمية أو غيرها من الوسائل السلمية التي يقع عليها اختيارها. ويلاحظ الفريق أيضا أهمية أحكام الميثاق الأخرى ذات الصلة بتسوية المنازعات بالوسائل السلمية.

(ب) يؤكد الفريق أن سيادة الدول والمعايير والمبادئ الدولية التي تنبع من السيادة تنطبق على قيام الدول بالأنشطة المتصلة بتكنولوجيات المعلومات والاتصالات، وعلى ولايتها على البنية التحتية لتلك التكنولوجيات داخل أراضيها. وتنطبق الالتزامات القائمة التي يقضي بها القانون الدولي على الأنشطة المتصلة بتكنولوجيات المعلومات والاتصالات التي تقوم بها الدول. وتمارس الدول ولايتها على البنية التحتية لتكنولوجيات المعلومات والاتصالات داخل أراضيها بوسائل منها وضع السياسات والقوانين وإنشاء الآليات اللازمة لحماية البنى التحتية لتكنولوجيات المعلومات والاتصالات على أراضيها من التهديدات المتصلة بتلك التكنولوجيات.

(ج) وفقا لمبدأ عدم التدخل، يجب ألا تتدخل الدول بشكل مباشر أو غير مباشر في الشؤون الداخلية لدولة أخرى، بما في ذلك عن طريق تكنولوجيات المعلومات والاتصالات.

(د) يجب على الدول، لدى استخدامها لتكنولوجيات المعلومات والاتصالات ووفقا لميثاق الأمم المتحدة، أن تمتنع في علاقاتها الدولية عن التهديد باستعمال القوة أو استعمالها ضد السلامة الإقليمية أو الاستقلال السياسي لأية دولة، أو بأية طريقة أخرى تتعارض مع مقاصد الأمم المتحدة.

(هـ) لاحظ الفريق مرة أخرى، مؤكِّدا تطلعات المجتمع الدولي إلى الاستخدام السلمي لتكنولوجيات المعلومات والاتصالات من أجل الصالح العام للبشرية، ومشيرا إلى أن الميثاق ينطبق برمته، الحق الأصيل للدول في اتخاذ تدابير تتسق مع القانون الدولي وعلى النحو المعترف به في الميثاق، والحاجة إلى مواصلة الدراسة في هذا الشأن.

(و) لاحظ الفريق أن القانون الدولي الإنساني لا ينطبق إلا في حالات النزاع المسلح. وهو يذكِّر بالمبادئ القانونية الدولية الراسخة، بما فيها مبادئ الإنسانية والضرورة والتناسب والتمييز التي أشير إليها في تقرير عام 2015، حيثما انطبقت هذه المبادئ. وأقر الفريق بالحاجة إلى إجراء مزيد من الدراسة بشأن كيف ومتى تنطبق هذه المبادئ على استخدام الدول لتكنولوجيات المعلومات والاتصالات، وشدد على أن التذكير بهذه المبادئ لا يضفي الشرعية على النزاع أو يشجعه بأي حال من الأحوال.

(ز) أكد الفريق مجددا أنه يجب على الدول الوفاء بالتزاماتها الدولية فيما يتعلق بالأفعال غير المشروعة دوليا المنسوبة إليها بموجب القانون الدولي. ويؤكد الفريق أيضا أنه يجب على الدول ألا تستخدم وكلاء عنها لارتكاب أفعال غير مشروعة دولياً باستخدام تكنولوجيات المعلومات والاتصالات، وينبغي أن تسعى إلى ضمان عدم استخدام إقليمها من قبل جهات من غير الدول لارتكاب أفعال من هذا القبيل. وفي الوقت ذاته، يذكِّر الفريق بأن الإشارة إلى أن نشاطا من أنشطة تكنولوجيات المعلومات والاتصالات قد انطلق من إقليم دولة من الدول أو من بنيتها التحتية لتكنولوجيات المعلومات والاتصالات أو نبَع من ذلك الإقليم أو تلك البنية التحتية بطريقة أخرى، قد لا يكون كافياً في حد ذاته لنسبة النشاط إلى تلك الدولة؛ ويلاحظ أنه ينبغي أن تكون الاتهامات الموجهة ضد الدول بتنظيم أفعال غير مشروعة وتنفيذها مدعومة بالأدلة. والاحتجاج بمسؤولية الدولة عن فعل غير مشروع دوليا ينطوي على اعتبارات تقنية وقانونية وسياسية معقدة.

72 - ودون المساس بقواعد القانون الدولي القائمة أو التطوير الإضافي للقانون الدولي في المستقبل، أقر الفريق بأن استمرار الدول في المناقشة وتبادل الآراء، بصورة جماعية في الأمم المتحدة، بشأن كيفية انطباق قواعد ومبادئ محددة في القانون الدولي على استخدام الدول لتكنولوجيات المعلومات والاتصالات أمر

أساسي لتعميق الفهم المشترك وتجنب سوء الفهم وزيادة القدرة على التنبؤ والاستقرار. ويمكن أن تستمد هذه المناقشات الاستنارة والدعم من وجهات النظر الإقليمية والثنائية المتبادلة بين الدول.

73 - ووفقا لولاية الفريق، سيتاح ثبتٌ رسمي [سيجري توفير رمز الوثيقة] بالمساهمات الوطنية الطوعية المتعلقة بموضوع كيفية انطباق القانون الدولي على استخدام الدول لتكنولوجيات المعلومات والاتصالات، التي قدمها الخبراء الحكوميون المشاركون في الفريق، على الموقع الشبكي لمكتب الأمم المتحدة لشؤون نزع السلاح. ويشجع الفريق جميع الدول على مواصلة تبادل آرائها وتقييماتها الوطنية طوعا عن طريق الأمين العام للأمم المتحدة وقنوات أخرى حسب الاقتضاء.

خامسا - تدابير بناء الثقة

74 - يلاحظ الفريق أن تدابير بناء الثقة يمكنها، من خلال تعزيز الثقة والتعاون والشفافية وإمكانية التنبؤ، أن تعزز الاستقرار وأن تساعد على الحد من خطر سوء الفهم والتصعيد والنزاع. وبناء الثقة التزام طويل الأجل وتصاعدي يتطلب انخراطا متواصلا من جانب الدول. ويمكن أن يسهم دعم الأمم المتحدة والهيئات الإقليمية ودون الإقليمية وغيرها من الجهات صاحبة المصلحة في تطبيق وتعزيز تدابير بناء الثقة بفعالية.

75 - وتشجَّع الدول، تأكيدا لجهودها الرامية إلى بناء الثقة وضمان توافر بيئة سلمية لتكنولوجيات المعلومات والاتصالات، على أن تكرر علنا التزامها بإطار سلوك الدول المسؤول المشار إليه في الفقرة 2 وعلى أن تتصرف وفقا له. وتشجَّع الدول أيضا على أن تأخذ في الاعتبار المبادئ التوجيهية لتدابير بناء الثقة التي اعتمدتها هيئة نزع السلاح التابعة للأمم المتحدة في عام 1988 وأيدتها الجمعية العامة بتوافق الآراء في القرار 78/43 حاء، فضلا عن الممارسات الناشئة على الصعيدين الإقليمي ودون الإقليمي بشأن تدابير بناء الثقة وتفعيلها.

التدابير التعاونية

نقاط الاتصال

76 - يمكن أن ييسّر تحديد نقاط اتصال مناسبة على مستوى السياسات وعلى المستوى التقني إجراء اتصالات آمنة ومباشرة بين الدول للمساعدة في منع ومعالجة الحوادث الخطيرة المرتبطة بتكنولوجيات المعلومات والاتصالات وتهدئة التوترات في حالات الأزمات. ويمكن أن يساعد التواصل بين نقاط الاتصال في الحد من التوترات ومنع حالات سوء الفهم والتصورات الخاطئة التي قد تنشأ عن الحوادث المرتبطة بتكنولوجيات المعلومات والاتصالات، بما فيها الحوادث التي تؤثر على البنية التحتية الحيوية والحوادث ذات التأثير الوطني أو الإقليمي أو العالمي. ويمكن أيضا أن تزيد نقاط الاتصال هذه من تبادل المعلومات وأن تمكن الدول من إدارة وعلاج الحوادث المرتبطة بتكنولوجيا المعلومات والاتصالات بشكل أكثر فعالية.

77 - وعند إنشاء نقاط الاتصال أو المشاركة في شبكات نقاط الاتصال، يمكن للدول أن تنظر فيما يلي:

(أ) تعيين نقاط اتصال مكرسة على مستوى السياسات والمستويين الدبلوماسي والتقني وتوفير التوجيه بشأن الخصائص المحددة لنقاط الاتصال، بما في ذلك الأدوار والمسؤوليات المتوقعة ومهام التنسيق ومتطلبات الاستعداد.

(ب) إنشاء إجراءات فيما بين الحكومات وداخل الحكومات لضمان التواصل الفعال بين نقاط الاتصال أثناء الأزمات. ويمكن أن تبين النماذج الموحدة أنواع المعلومات المطلوبة، بما في ذلك البيانات التقنية وطبيعة الطلب، ولكنها يمكن أن تكون مرنة بما يكفي للسماح بالاتصال، حتى لو كانت بعض المعلومات غير متوفرة.

(ج) استخلاص الدروس والممارسات الجيدة من الشبكات الإقليمية لنقاط الاتصال، بما يشمل ما يتعلق بمناقشة وتطوير وتنفيذ نُهج عملية لاستخدام شبكات نقاط الاتصال في السياقات الوطني والإقليمي والدولي، لأغراض منها التوعية المبكرة بحوادث تكنولوجيات المعلومات والاتصالات الخطيرة، بهدف تعزيز التنسيق وتبادل المعلومات بين نقاط الاتصال المكلَّفة.

78 - والتصدي للتهديدات الأمنية العالمية المرتبطة بتكنولوجيات المعلومات والاتصالات يتطلب أيضا اتباع نهج جامعة وعالمية. ويمكن للدول أن تدعو الأمين العام للأمم المتحدة إلى تيسير عمليات تبادل طوعية بين جميع الدول الأعضاء فيما يتعلق بالدروس والممارسات الجيدة والتوجيهات المتصلة بشبكات نقاط الاتصال ذات الصلة القائمة بالفعل على الصعيدين الإقليمي ودون الإقليمي. ويمكن أن يسهم هذا العمل في المناقشات ذات الصلة بإنشاء دليل لنقاط الاتصال هذه على الصعيد العالمي.

الحوار والمشاورات

79 - يمكن للحوار من خلال المشاورات والمشاركة الثنائية ودون الإقليمية والإقليمية والمتعددة الأطراف أن يعزز التفاهم بين الدول ويشجع على زيادة الثقة ويسهم في توثيق التعاون بين الدول في التخفيف من ضرر الحوادث المتعلقة بتكنولوجيا المعلومات والاتصالات، مع الحد في الوقت نفسه من مخاطر التصورات الخاطئة والتصعيد. ويمكن لأصحاب المصلحة الآخرين، من قبيل القطاع الخاص والأوساط الأكاديمية والمجتمع المدني والأوساط التقنية، أن يسهموا إسهاما كبيرا في تيسير هذه المشاورات والمشاركة.

80 - وقد اتخذت الهيئات الإقليمية خطوات هامة في وضع وتنفيذ تدابير لبناء الثقة يمكن أن تحد من خطر التصورات الخاطئة والتصعيد والنزاع الذي قد ينشأ عن حوادث تكنولوجيات المعلومات والاتصالات. وتتيح المشاركة في هذه الهيئات التركيز على الخصائص والشواغل الإقليمية، بينما تتيح عمليات التبادل بين المناطق أن يكون هناك تعلم متبادل بين هذه المنظمات. وتُشجَّع الدول على مواصلة هذا العمل، وعلى التواصل النشط مع الدول التي ليست حاليا أعضاء في منظمة إقليمية أو دون إقليمية ذات صلة.

81 - ولمواصلة تعزيز التدابير التعاونية ذات الصلة بالأفرقة الوطنية لمواجهة الطوارئ الحاسوبية وغيرها من الهيئات المفوضة، يمكن للدول أن تشجِّع على تبادل ونشر المعلومات والممارسات الجيدة بشأن إنشاء ومواصلة عمل الأفرقة الوطنية لمواجهة الطوارئ الحاسوبية/الأفرقة الوطنية للاستجابة لحوادث أمن الفضاء الإلكتروني، وبشأن التعامل مع الحوادث من خلال المنظمات والشبكات الإقليمية والعالمية القائمة المعنية بمواجهة الطوارئ. وهذا التشجيع والدعم المقدمان للأفرقة الوطنية لمواجهة الطوارئ الحاسوبية/الأفرقة الوطنية للاستجابة لحوادث أمن الفضاء الإلكتروني سيساعدان أيضاً في زيادة الوعي لدى الدول بالتزاماتها تجاه هذه الأفرقة وغيرها من الهيئات ذات الصلة بموجب القاعدة 13 (ك).

تدابير تحقيق الشفافية

82 - تمثل ممارسة الشفافية على أساس طوعي من خلال تبادل الآراء والممارسات الوطنية بشأن الحوادث الأمنية المتعلقة بتكنولوجيات المعلومات والاتصالات وغيرها من التهديدات ذات الصلة، ومن خلال جعل المشورة والتوجيه وقاعدة الأدلة والبيانات الداعمة للقرارات فيما يتعلق بأمن تكنولوجيات المعلومات والاتصالات متاحة للعموم، أمرا مهماً لبناء الثقة والقدرة على التنبؤ، والحد من احتمال سوء التفسير والتصعيد، ومساعدة المنظمات والوكالات على اتخاذ قرارات جيدة بشأن إدارة المخاطر.

83 - ولزيادة تعزيز الشفافية وإمكانية التنبؤ بسلوك الدول، وإتاحة إمكانية الاطلاع على طائفة أوسع من الآراء والخبرات، وتعزيز استعداد الدول ووعيها المبكر بالتهديدات المتزايدة، يمكن للدول أن تنظر في استخدام المحافل الثنائية ودون الإقليمية والإقليمية والمتعددة الأطراف والمشاورات غير الرسمية لتبادل المعلومات والممارسات الجيدة والدروس أو الورقات البيضاء طوعاً بشأن التهديدات والحوادث القائمة والناشئة المتصلة بأمن تكنولوجيات المعلومات والاتصالات؛ وبشأن النهج الوطنية والإقليمية لإدارة المخاطر ومنع نشوب النزاعات، بما في ذلك النهج الوطنية لتصنيف حوادث تكنولوجيات المعلومات والاتصالات من حيث حجم الحادث وخطورته.

84 - ويمكن للدول أيضا الاستفادة من هذه المنتديات القائمة لتوضيح المواقف وتبادل المعلومات طوعا حول: النهج الوطنية لأمن تكنولوجيات المعلومات والاتصالات؛ وحماية البيانات؛ وحماية البنية التحتية الحيوية المستندة إلى تكنولوجيات المعلومات والاتصالات؛ ومهمة الوكالة المعنية بأمن تكنولوجيات المعلومات والاتصالات ووظائفها، والاستراتيجية المتعلقة بتكنولوجيات المعلومات والاتصالات على الصعيد الوطني أو المؤسسي، والأنظمة القانونية والرقابية التي تعمل في ظلها.

85 - وتوفر التوصيات المتعلقة بتدابير بناء الثقة الواردة في التقارير السابقة لأفرقة الخبراء الحكوميين أساساً تعاونياً للتصدي للتهديدات المتزايدة التي تواجه البنية التحتية الحيوية ولتنفيذ القواعد ذات الصلة. وتُشجَّع الدول على مواصلة التوعية بأهمية حماية البنية التحتية الحيوية، وتعزيز تبادل المعلومات فيما بين الجهات صاحبة المصلحة في البنية التحتية الحيوية، وتبادل الممارسات الجيدة والتوجيهات. ويمكنها، عند الاقتضاء، أن تستخدم المنابر القائمة وطرائق الإبلاغ القائمة (انظر الفقرة 86) لتبادل الآراء الوطنية طوعا بشأن تصنيف البنية التحتية الحيوية الوطنية والبنية التحتية الحيوية التي توفر خدمات أساسية على الصعيد الإقليمي أو الدولي، والسياسات والتشريعات الوطنية ذات الصلة، وأطر تقييم المخاطر وتحديد وتصنيف وإدارة الحوادث المتعلقة بتكنولوجيات المعلومات والاتصالات التي تؤثر على البنية التحتية الحيوية.

86 - ويمكن للدول أيضا أن تستخدم موارد الأمم المتحدة مثل تقديم التقارير طوعا إلى الأمين العام، وبوابة السياسات السيبرانية التابعة لمعهد الأمم المتحدة لبحوث نزع السلاح، فضلا عن موارد المنظمات الدولية والإقليمية الأخرى ذات الصلة لتجميع المعلومات والممارسات الجيدة التي تقدمها الدول طوعا بشأن الاستراتيجيات والسياسات والتشريعات والبرامج الوطنية التي تعالج مسائل أمن تكنولوجيات المعلومات والاتصالات ذات الصلة بالأمن والاستقرار الدوليين.

سادسا - التعاون والمساعدة الدوليان في مجال أمن تكنولوجيات المعلومات والاتصالات وبناء القدرات في هذا المجال

87 - يؤكد الفريق ما يتسم به التعاون والمساعدة في مجال أمن تكنولوجيات المعلومات والاتصالات وبناء القدرات في هذا المجال من أهمية لجميع عناصر ولاية الفريق. فزيادة التعاون وفعالية المساعدة وبناء القدرات في مجال أمن تكنولوجيات المعلومات والاتصالات، بمشاركة أصحاب المصلحة الآخرين، من قبيل القطاع الخاص والأوساط الأكاديمية والمجتمع المدني والأوساط التقنية، يمكن أن تساعد الدول على تطبيق إطار النهوض بالسلوك المسؤول للدول في استخداماتها لتكنولوجيات المعلومات والاتصالات. والتعاون والمساعدة لهما أهمية حاسمة في سد الفجوات القائمة داخل الدول وفيما بينها بشأن المسائل المتعلقة بالسياسات والمسائل القانونية والتقنية ذات الصلة بأمن تكنولوجيات المعلومات والاتصالات. وقد يسهمان أيضا في تحقيق أهداف أخرى للمجتمع الدولي مثل أهداف التنمية المستدامة.

88 - ويمكن للتعاون والمساعدة الدوليين في مجال أمن تكنولوجيات المعلومات والاتصالات وبناء القدرات في هذا المجال أن يعززا قدرة الدول على اكتشاف التهديدات والتصدي لها، وأن يكفلا قدرة جميع الدول على التصرف بمسؤولية في استخدامها لتكنولوجيات المعلومات والاتصالات. ويمكن أن يساعدا أيضا في ضمان أن تحقق جميع الدول المستويات الضرورية من الحماية والأمن للبنية التحتية الحيوية، وأن يكون لديها قدرات كافية على إدارة الحوادث، وأن تطلب المساعدة أو تستجيب لنداءات المساعدة في حالة وجود أنشطة خبيثة في مجال تكنولوجيات المعلومات والاتصالات تنبع من إقليمها أو تؤثر عليه.

89 - ويوصي الفريق بمواصلة تعزيز التعاون والمساعدة الدوليين في مجال أمن تكنولوجيات المعلومات والاتصالات وبناء القدرات ذات الصلة في المجالات التالية:

(أ) وضع وتنفيذ السياسات والاستراتيجيات والبرامج الوطنية المتعلقة بتكنولوجيات المعلومات والاتصالات.

(ب) إنشاء أفرقة وطنية لمواجهة الطوارئ الحاسوبية/أفرقة وطنية للاستجابة لحوادث أمن الفضاء الإلكتروني وتعزيز قدرات الأفرقة الموجودة منها وتدعيم ترتيبات التعاون فيما بين هذه الأفرقة.

(ج) تحسين أمن البنية التحتية الحيوية وصلابتها وحمايتها.

(د) بناء أو تعزيز قدرات الدول التقنية والقانونية وفي مجال السياسات على اكتشاف حوادث تكنولوجيات المعلومات والاتصالات والتحقيق فيها وعلاجها، بوسائل منها الاستثمار في تنمية الموارد البشرية والمؤسسات وفي التكنولوجيا المتينة والبرامج التثقيفية.

(هـ) تعميق الفهم المشترك لكيفية انطباق القانون الدولي على استخدام الدول لتكنولوجيات المعلومات والاتصالات وتعزيز التبادلات بين الدول، بوسائل منها إجراء مناقشات في الأمم المتحدة بهذا الشأن.

(و) تعزيز القدرات التقنية والقانونية لجميع الدول على التحقيق في حوادث تكنولوجيات المعلومات والاتصالات الخطيرة وعلاجها.

(ز) تنفيذ القواعد الطوعية غير الملزمة المتفق عليها المنظمة للسلوك المسؤول للدول.

(ح) تشجَّع الدول في سبيل تحقيق هذه الغاية، وكوسيلة لتقييم أولوياتها واحتياجاتها ومواردها، على استخدام الدراسة الاستقصائية الطوعية للتنفيذ الوطني التي أوصى بها فريق الأمم المتحدة العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي[4].

90 - وبغية سد الفجوات الرقمية وضمان استفادة جميع الدول من هذه المجالات وغيرها من مجالات المساعدة وبناء القدرات، تشجَّع الدول على الالتزام، حيثما أمكن، بتدبير الموارد المالية وتوفير الخبرة التقنية والسياساتية، ودعم البلدان التي تطلب المساعدة في جهودها الرامية إلى تعزيز أمن تكنولوجيات المعلومات والاتصالات.

91 - وفي سياق النهوض بالتعاون والمساعدة الدوليين في مجال أمن تكنولوجيات المعلومات والاتصالات وبناء القدرات في هذا المجال، يؤكد الفريق طوعية بناء القدرات وحياده السياسي ومنافعه المتبادلة واستناده إلى مبدأ المعاملة بالمثل. وفي هذا الصدد، يرحب الفريق فيما يتعلق ببناء القدرات بمبادئه المتصلة بالإجراءات والغرض والشراكات والأشخاص التي أوصى بها الفريق العامل المفتوح العضوية، ويشجع جميع الدول على الاسترشاد بهذه المبادئ في جهودها الرامية إلى تعزيز التعاون والمساعدة[5].

92 - وتعزيز الفهم المشترك والتعلم المتبادل يمكن أيضا أن يعزز التعاون والمساعدة الدوليين في مجال أمن تكنولوجيات المعلومات والاتصالات وبناء القدرات ذات الصلة. وينبغي للدول أن تنظر في تناول مسألة التعاون في مجال أمن تكنولوجيا المعلومات والاتصالات وبناء القدرات ذات الصلة على نحو يتسم بتعدد التخصصات، وتعدد أصحاب المصلحة، وقابلية التكيف، وقابلية القياس. ويمكن تحقيق ذلك من خلال العمل مع الأمم المتحدة والهيئات العالمية والإقليمية ودون الإقليمية الأخرى ومع أصحاب المصلحة الآخرين المعنيين لتيسير فعالية تنسيق وتنفيذ برامج بناء القدرات ومن خلال تشجيع الشفافية وتبادل المعلومات بشأن فعالية هذه البرامج.

سابعاً - الاستنتاجات والتوصيات المتعلقة بالعمل في المستقبل

93 - مع تزايد اعتماد المجتمعات على تكنولوجيات المعلومات والاتصالات، أصبح وجود إطار مشترك لسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي أمراً أساسياً لاستفادة جميع الدول من التكنولوجيات وللحماية من إساءة استخدامها والتصدي لذلك.

94 - وقد قام الفريق، مركِّزا جهوده على تعزيز الفهم المشترك والتنفيذ الفعال ومستندا إلى التوصيات الواردة في التقارير السابقة، بتحديد - وزيادة توضيح - النُهج التي يمكن للدول أن تتبعها لضمان أن تتصدى التدابير التعاونية بفعالية للتهديدات القائمة والمحتملة في مجال أمن تكنولوجيات المعلومات والاتصالات، وبتوفير توجيه بشأن هذه النُهج. وهذه النُهج مبينة بوضوح في فروع التقرير المتعلقة بمعايير وقواعد ومبادئ السلوك المسؤول للدول؛ والقانون الدولي، وبناء الثقة؛ والتعاون الدولي، وبناء القدرات، وكل منها يطور العناصر الأساسية للسلوك المسؤول للدول التي تبلورت في تقارير فريق الخبراء الحكوميين السابقة.

95 - كما حدد الفريق مجالات محتملة للعمل في المستقبل، وهي تشمل ما يلي ولا تقتصر عليه:

(4) الفقرة 65 من التقرير الفني النهائي للفريق.

(5) الفقرة 56 من التقرير الفني النهائي للفريق العامل المفتوح العضوية.

(أ) زيادة التعاون على الصعيد الثنائي والإقليمي والمتعدد الأطراف لتعزيز الفهم المشترك بشأن التهديدات القائمة والناشئة والمخاطر المحتملة على السلام والأمن الدوليين التي يشكلها الاستخدام الخبيث لتكنولوجيات المعلومات والاتصالات، وبشأن أمن البنية التحتية المعتمدة على تلك التكنولوجيات.

(ب) زيادة إتاحة وتبادل الآراء بشأن المعايير والقواعد والمبادئ المتعلقة بسلوك الدول المسؤول والممارسات الوطنية والإقليمية المتبعة في تنفيذ القواعد وتدابير بناء الثقة؛ وبشأن كيفية انطباق القانون الدولي على استخدام الدول لتكنولوجيات المعلومات والاتصالات، بوسائل منها تحديد مواضيع معينة في القانون الدولي لإجراء المزيد من المناقشة المتعمقة بشأنها.

(ج) مواصلة تعزيز التعاون الدولي وبناء القدرات بشأن التقييمات والتوصيات الواردة في هذا التقرير بغية ضمان أن تتمكن جميع الدول من الإسهام في صون السلام والأمن الدوليين، مع مراعاة الفقرة 90 أعلاه.

(د) تحديد الآليات التي يمكن أن تيسر مشاركة أصحاب المصلحة الآخرين، بما في ذلك القطاع الخاص والأوساط الأكاديمية والمجتمع المدني والأوساط التقنية في الجهود الرامية إلى تنفيذ إطار السلوك المسؤول، عند الاقتضاء.

(هـ) الطلب إلى معهد الأمم المتحدة لبحوث نزع السلاح، الذي يخدم جميع الدول الأعضاء، إجراء دراسات ذات صلة حول الموضوعات التي نوقشت في هذا التقرير، وتشجيع مراكز الفكر والمؤسسات البحثية على إجراء تلك الدراسات.

96 - ويشجع الفريق على الاستمرار في عملية تفاوض جامعة وشفافة بشأن تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي تحت رعاية الأمم المتحدة، تشمل وتقدِّر الفريق العامل المفتوح العضوية المعني بمأمونية استخدام تكنولوجيات المعلومات والاتصالات للفترة 2021-2025، الذي أنشئ عملا بقرار الجمعية العامة 240/75. ويوصي الفريق بأن يبني العمل في المستقبل على العمل التراكمي الذي قامت به أفرقة الخبراء الحكوميين والفريق العامل المفتوح العضوية.

97 - ويشجع الفريق الدول على مواصلة الجهود الرامية إلى تعزيز إطار سلوك الدول المسؤول داخل الأمم المتحدة وغيرها من المحافل الإقليمية والمتعددة الأطراف لدعم الحوار المنتظم والتشاور وبناء القدرات بطريقة جامعة وشفافة وعملية المنحى ومدفوعة بتوافق الآراء. وفي هذا الصدد ووفقا للنتائج التي انتهى إليها الفريق العامل المفتوح العضوية، يلاحظ الفريق وجود مجموعة متنوعة من المقترحات الرامية إلى النهوض بسلوك الدول المسؤول في مجال تكنولوجيات المعلومات والاتصالات، وهي مقترحات من شأنها، في جملة أمور، أن تدعم قدرات 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.

98 - ويوصي الفريق بأن تسترشد الدول الأعضاء بالتقييمات والتوصيات الواردة في هذا التقرير وتقييمات وتوصيات أفرقة الخبراء الحكوميين السابقة، وكذلك بالاستنتاجات والتوصيات الواردة في التقرير النهائي للفريق العامل المفتوح العضوية (A/75/816)، وأن تنظر في كيفية مواصلة تطوير هذه الاستنتاجات والتقييمات وتنفيذها.

المرفق

قائمة بأعضـــاء فريق الخبراء الحكوميين المعني بالارتقاء بســـلوك الدول المســـؤول في الفضاء الإلكتروني في سياق الأمن الدولي

أستراليا

جوانا ويفر

المستشارة الخاصة لسفير أستراليا للشؤون السيبرانية

وزارة الشؤون الخارجية والتجارة

البرازيل

غيليرمي دي أغيار باتريوتا

السفير، القنصل العام للبرازيل في مومباي

الصين

وانغ لي

منسق الشؤون السيبرانية، وزارة الخارجية

إستونيا

هيلي تيرما – كلار

السفيرة المتجولة للدبلوماسية السيبرانية، مدير عام إدارة الدبلوماسية السيبرانية، وزارة الخارجية

فرنسا

أونري فيرديبه

سفير الشؤون الرقمية، وزارة شؤون أوروبا والشؤون الخارجية

ألمانيا

ريغين غرينبرغر (الدورتان الثالثة والرابعة)

سفيرة شؤون السياسة الخارجية السيبرانية، وزارة الخارجية الاتحادية

فولفرام فون هينيتز (الدورتان الأولى والثانية)

رئيس موظفي تنسيق السياسات السيبرانية الدولية، وزارة الخارجية الاتحادية

الهند

س. جاناكيرامان

السكرتير المشترك ورئيس شعبتي الحوكمة الإلكترونية وتكنولوجيا المعلومات، والدبلوماسية السيبرانية، وزارة الخارجية

إندونيسيا

روليانسياه سوميرات (الدورتان الثالثة والرابعة)

مدير شؤون الأمن الدولي ونزع السلاح، وزارة الخارجية

هارديتيا سورياوانتو (الدورة الثانية)

مستشار في شؤون التكنولوجيا والمسائل السيبرانية، مديرية الأمن الدولي ونزع السلاح، وزارة الخارجية

غراتا إنداه ويردانينغتياس (الدورة الأولى)
مدير شؤون الأمن الدولي ونزع السلاح، وزارة الخارجية

اليابان

تاكيشي أكاهوري
سفير شؤون الأمم المتحدة والسياسة السيبرانية، وزارة الخارجية

الأردن

فراس محمد عبد الله الزعبي
رئيس فرع البرنامج الوطني لأمن المعلومات، القوات المسلحة الأردنية

كازاخستان

أسيت نوسوبوف
رئيس القطاع بالمكتب التنفيذي لرئيس جمهورية كازاخستان

كينيا

كاثرين غيتاو
الرئيسة التنفيذية لهيئة تكنولوجيا المعلومات والاتصالات

موريشيوس

كليم أحمد عثماني
رئيس فريق موريشيوس للتصدي للطوارئ الحاسوبية

المكسيك

خيراردو إسحاق موراليس تينوريو
منسق الأمن المتعدد الأبعاد، وزارة الخارجية

المغرب

الكولونيل ماجور عبد الله بوطريك
مدير المساعدة والتدريب والمراقبة والخبرة، المديرية العامة لأمن نظم المعلومات، إدارة الدفاع الوطني

هولندا

كارمن غونسالفيس
رئيسة قسم السياسة المعلوماتية الدولية، وزارة الخارجية

النرويج

سيمين إكبلوم (الدورتان الثالثة والرابعة)
منسق السياسات السيبرانية، وزارة الخارجية

أنكين كروتنيس (الدورتان الأولى والثانية)
نائب المدير العام، إدارة السياسات الأمنية والشمال الأعلى، وزارة الخارجية

رومانيا

ميهايلا – أيونيليا بوبيسكو

منسقة السياسات الإلكترونية، وزارة الخارجية

الاتحاد الروسي

أندريه كروتسكيخ

الممثل الخاص لرئيس الاتحاد الروسي للتعاون الدولي في مجال أمن المعلومات، مدير إدارة أمن المعلومات الدولي، وزارة الخارجية

فلاديمير شين (الدورتان الثالثة والرابعة)

نائب مدير إدارة أمن المعلومات الدولي، وزارة الخارجية

سنغافورة

ديفيد كوه

الرئيس التنفيذي لوكالة الأمن السيبراني في سنغافورة ومفوض الأمن السيبراني

جنوب أفريقيا

دوك مشابان

المدير العام، إدارة شؤون العدالة والتطوير الدستوري

موليهي ماكومان (الدورتان الثالثة والرابعة)

مستشارة خاصة لممثل جنوب أفريقيا في فريق الخبراء الحكوميين

سويسرا

نادين أوليفييري لوزانو

سفيرة، رئيسة شعبة الأمن الدولي، وزارة الخارجية الاتحادية

المملكة المتحدة

كاثرين جونز

رئيسة شؤون الحوكمة السيبرانية الدولية، مديرية الأمن الوطني، وزارة الخارجية والكومنولث والتنمية

ألكسندر إيفانز (الدورة الأولى)

المدير السابق للشؤون السيبرانية، وزارة الخارجية والكومنولث والتنمية

الولايات المتحدة

ميشيل ماركوف

القائم بأعمال منسق القضايا السيبرانية، وزارة خارجية الولايات المتحدة

أوروغواي

نويليا مارتينيس فرانشي (الدورتان الثالثة والرابعة)

مديرة الشؤون المتعددة الأطراف، وزارة الخارجية

أليخاندرا إيراموسبي (الدورتان الأولى والثانية)

كبيرة موظفين، وكالة الحكومة الإلكترونية ومجتمع المعلومات، مكتب الرئيس