الأمم المتحدة S/2021/621

مجلس الأمن

Distr.: General
1 July 2021
Arabic
Original: English

رسالة مؤرخة 1 تموز/يوليه 2021 موجهة من رئيس مجلس الأمن إلى الأمين العام والممثلين الدائمين لأعضاء مجلس الأمن

أتشرف بإرفاق نسخة من الإحاطة الإعلامية التي قدمتها إيزومي ناكاميتسو، الممثلة السامية لشؤون نزع السلاح، وكذلك البيانات التي أدلى بها كل من كايا كالاس، رئيسة وزراء إستونيا؛ محمودو أوهومودو، رئيس وزراء النيجر؛ وسايمون كوفني، وزير الخارجية والدفاع في أيرلندا؛ وبوي ثانه سون، وزير خارجية فييت نام؛ وجو موشيرو، أمين مجلس الوزراء لشؤون الاتصالات والمعلومات والتكنولوجيا والابتكار والشباب في كينيا؛ وليندا توماس – غرينفيلد، الممثلة الدائمة للولايات المتحدة وعضوة في حكومة الرئيس بايدن؛ وهارش فاردان شرينغلا، وزير خارجية الهند؛ وكيسال م. بيترز، وزيرة الدولة المسؤولة عن الشؤون الخارجية والتجارة الخارجية في سانت فنسنت وجزر غرينادين؛ وآودون هالفورسن، نائب وزير خارجية النرويج؛ واللورد طارق أحمد، لورد ويمبلدون، ووزير الدولة لشؤون الكومنولث والأمم المتحدة وجنوب آسيا في المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية؛ وفرانك ريستر، وزير التجارة الخارجية والجاذبية الاقتصادية المنتدب الملحق بوزير شؤون أوروبا والشؤون الخارجية في فرنسا، وكذلك ممثلو الاتحاد الروسي، وتونس، والصين، والمكسيك فيما يتعلق بالجلسة المعقودة عبر التداول بالفيديو حول موضوع "صون السلام والأمن الدوليين: أمن الفضاء الإلكتروني" يوم الثلاثاء 29 حزيران/يونيه 2021.

ووفقا للتفاهم الذي تم التوصل إليه بين أعضاء المجلس بشأن هذه الجلسة المعقودة عبر التداول بالفيديو، قدمت الوفود والكيانات التالية بيانات خطية أُرفقت نسخ منها أيضا: الاتحاد الأوروبي والأرجنتين وأستراليا وإكوادور وألمانيا والإمارات العربية المتحدة وإندونيسيا وأوكرانيا وجمهورية إيران الإسلامية وإيطاليا وباكستان والبحرين والبرازيل وبلجيكا وبولندا وبيرو وتايلند وتركيا وتشيكيا وجمهورية كوريا وجنوب أفريقيا وجورجيا والدانمرك ورومانيا والسلفادور وسلوفاكيا وسلوفينيا وسنغافورة والسنغال وسويسرا وشيلي وغواتيمالا وقطر وكازاخستان وكندا ولاتفيا واللجنة الدولية للصليب الأحمر وليختنشتاين ومالطة ومصر والمغرب والمنظمة الدولية للشرطة الجنائية والنمسا ونيوزيلندا وهولندا واليابان واليونان.

290921 280921 21-09125 (A)

ووفقا للإجراء المبين في الرسالة المؤرخة 7 أيار/مايو 2020 (S/2020/372) الموجهة من رئيس مجلس الأمن إلى الممثلين الدائمين لأعضاء مجلس الأمن والذي تم الاتفاق عليه في ضوء الظروف الاستثنائية الناجمة عن جائحة مرض فيروس كورونا (كوفيد-19)، ستصدر هذه الإحاطات والبيانات باعتبارها وثيقة من وثائق مجلس الأمن.

(توقيع) نيكولا **دو ريفيير**
رئيس مجلس الأمن

المرفق الأول

بيان الممثلة السامية لشؤون نزع السلاح، إيزومي ناكاميتسو

أود أن أعرب عن تقديري لإستونيا لتنظيمها هذا الجلسة ودعوتي لتقديم إحاطة في هذه المناقشة المفتوحة حول صون السلام والأمن الدوليين في الفضاء الإلكتروني.

وحتى كانون الثاني/يناير من هذا العام، بلغ عدد مستخدمي الإنترنت النشطين أكثر من 4,6 بلايين مستخدم في جميع أنحاء العالم. وتشير التقديرات إلى أنه سيكون هناك 28,5 بليون جهاز موصول بشبكات ومتصل بالإنترنت بحلول عام 2022، بزيادة كبيرة عن 18 بليون في عام 2017.

ومع استمرار الثورة التي يحدثها التقدم في عالم التكنولوجيات الرقمية في حياة الإنسان، يجب أن نظل يقظين في فهمنا للاستخدام الخبيث لهذه التكنولوجيات التي يمكن أن تعرض أمن الأجيال المقبلة للخطر.

وتشكل التكنولوجيات الرقمية بشكل متزايد عبئا مجهدا على القواعد القانونية والإنسانية والأخلاقية القائمة، وعدم الانتشار، والاستقرار الدولي، والسلام والأمن.

كما أنها تقلل العوائق التي تحول دون الوصول إلى الفضاء الإلكتروني وتؤدي إلى فتح مجالات محتملة جديدة للنزاع وتمكين الجهات من الدول وغير الدول من شن هجمات، بما في ذلك عبر الحدود الدولية.

وفيما يتعلق بتكنولوجيا المعلومات والاتصالات على وجه التحديد، شهدنا زيادة هائلة في وتيرة الحوادث الخبيثة في السنوات الأخيرة. واتخذت هذه الحوادث أشكالا عديدة، تتراوح بين التضليل الإعلامي وتعطيل شبكات الحاسوب. وتسهم هذه الأعمال في تضاؤل الثقة والارتياح بين الدول.

وتشكل هذه التطورات أيضا خطرا محددا على البنى التحتية الحيوية التي تتيحها تكنولوجيا المعلومات والاتصالات، مثل القطاع المالي وشبكات الطاقة الكهربائية والمرافق النووية. وقد وجه الأمين العام الانتباه إلى الهجمات السيبرانية على مرافق الرعاية الصحية أثناء انتشار الجائحة، ودعا المجتمع الدولي إلى بذل المزيد من الجهود لمنع وإنهاء هذه الأشكال الجديدة من العدوان، التي يمكن أن تسبب مزيدا من الضرر الشديد للمدنيين[1].

ولهذه التهديدات التي تشكلها تكنولوجيا المعلومات والاتصالات تأثير جنساني ويجب دراستها من خلال هذا المنظور. وللتطرف العنيف والاتجار عبر الإنترنت آثار متباينة على النساء والرجال والأطفال كثيرا ما يتم تجاهلها، وهي تماثل أثر الأخطار الأخرى المتصلة بتكنولوجيا المعلومات والاتصالات مثل المطاردة السيبرانية وعنف العشير والنشر غير التوافقي للمعلومات والصور الحميمية. ولهذا السبب أيضا، نحن بحاجة إلى بذل كل جهد ممكن لضمان المشاركة المتساوية والكاملة والفعالة للنساء والرجال على حد سواء في صنع القرار في المجال الرقمي.

(1) انظر www.un.org/sg/en/content/sg/statement/2020-05-27/secretary-generals-remarks-the-security-council-open-debate-the-protection-of-civilians-armed-conflict-delivered.

وتتزايد الأخطار الناجمة عن تكنولوجيا المعلومات والاتصالات، ولكن يجري أيضا بذل الجهود اللازمة للتصدي لها. وخلال العقد ونصف العقد الماضيين في الأمم المتحدة، درست مجموعة مكونة من خمسة أفرقة من الخبراء الحكوميين الأخطار القائمة والمستجدة الناجمة عن استخدام تكنولوجيا المعلومات والاتصالات والتي تهدد الأمن الدولي وأوصت باتخاذ تدابير للتصدي لها. وقد اختتمت عمليتان إضافيتان للأمم المتحدة عملهما بنجاح، هما فريق عامل مفتوح العضوية وفريق سادس من الخبراء الحكوميين، أنشئ كلاهما في عام 2018، واتخذا خطوات هامة للمضي قدما بشأن هذا الموضوع من خلال اعتماد توصيات ملموسة وعملية المنحى.

وأوصى هذان الفريقان بحزمة من المعايير الطوعية وغير الملزمة للسلوك المسؤول للدول، وأقرا بأنه يمكن وضع معايير إضافية مع مرور الوقت. وأكدا أيضا من جديد أن القانون الدولي، ولا سيما ميثاق الأمم المتحدة، ينطبق على صون السلام والأمن والاستقرار في بيئة تكنولوجيا المعلومات والاتصالات، وله دور أساسي في هذا الصدد. وأوصى الفريقان باتخاذ تدابير لبناء الثقة وبناء القدرات والتعاون، استنادا إلى الأعمال التي اضطلع بها في إطار العمليات السابقة. وبالإضافة إلى ذلك، توصل الفريق العامل المفتوح العضوية، وفقا لولايته، إلى استنتاجات وتوصيات بشأن إقامة حوار مؤسسي منتظم بشأن مسألة تكنولوجيا المعلومات والاتصالات.

كما لاحظ أحدث فريق للخبراء الحكوميين في تقريره، فإن التدابير التي أوصى بها فريق الخبراء الحكوميين السابق والفريق العامل المفتوح العضوية تمثل معا إطارا أوليا لسلوك الدولة المسؤول في مجال استخدام تكنولوجيا المعلومات والاتصالات[2].

كما عقد فريق عامل مفتوح العضوية ثان جديد دورته التنظيمية منذ فترة قصيرة وسيبدأ عمله الموضوعي في وقت لاحق من هذا العام.

وعلى الصعيد الإقليمي، تبذل المنظمات الإقليمية الآن جهودا رئيسية بشأن المسائل المتعلقة بتكنولوجيا المعلومات والاتصالات. واتخذت النهج الإقليمية أشكالا مختلفة تحدد بحسب تفاوت الأولويات والاحتياجات. وقد ركز بعض المناطق بشكل أكبر على تنفيذ المعايير الطوعية غير الملزمة لسلوك الدولة المسؤول من خلال جهود بناء القدرات، بينما قامت مناطق أخرى بجهود رائدة في اتخاذ تدابيرها الخاصة لبناء الثقة على الصعيد الإقليمي للحد من مخاطر النزاع الناجمة عن أنشطة تكنولوجيا المعلومات والاتصالات أو اعتمدت أدوات إقليمية أخرى للتصدي لأخطار تكنولوجيا المعلومات والاتصالات. وتوجد أيضا صكوك إقليمية مختلفة تتناول جوانب محددة لتكنولوجيا المعلومات والاتصالات.

وبينما تتحمل الدول المسؤولية الرئيسية عن صون الأمن الدولي، تشكل تكنولوجيا المعلومات والاتصالات جزءاً لا يتجزأ من مجتمعاتنا، كما أن الجهات الأخرى صاحبة المصلحة يقع على عاتقها دور رئيسي في تأمين الفضاء الإلكتروني ولها مصلحة كبرى في تأمينه، إضافة إلى مسؤوليتها عن هذا التأمين.

(2) انظر الفقرة 21 من تقرير فريق الخبراء الحكوميين. ويمكن الاطلاع على نسخة مسبقة من خلال الرابط https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf.

وتم إطلاق العديد من المبادرات السيبرانية الممتازة التي يقودها القطاع الخاص، مثل اتفاق تكنولوجيا الأمن السيبراني بقيادة مايكروسوفت، وميثاق الثقة الذي تتولى قيادته شركة سيمنز ومؤتمر ميونيخ للأمن، ومبادرة الشفافية العالمية التي أطلقها معمل كاسبرسكي.

وجمع نداء باريس من أجل الثقة والأمن في الفضاء الإلكتروني لعام 2018 قطاع الصناعة والدول والمجتمع المدني والأوساط الأكاديمية في إطار من الالتزام بتسعة من مبادئ الأمن السيبراني. وتغطي هذه المبادئ مجموعة من المسائل تتراوح من استحداث سبل لمنع انتشار الأدوات والممارسات الخبيثة في مجال تكنولوجيا المعلومات والاتصالات، إلى تشجيع القبول الواسع النطاق للمعايير الدولية للسلوك المسؤول ووضعها موضع التنفيذ، فضلا عن اتخاذ تدابير بناء الثقة في الفضاء الإلكتروني.

وتساهم وجهات نظر القطاع الخاص والمجتمع المدني والأوساط الأكاديمية في جزء فريد ومهم من الحل الجماعي الذي ينشده المجتمع الدولي في مجال الأمن السيبراني.

والأمم المتحدة، من جانبها، على استعداد لدعم الدول إلى جانب الجهات الأخرى صاحبة المصلحة في تعزيز بيئة سلمية في مجال تكنولوجيا المعلومات والاتصالات. ودعا الأمين العام إلى عقد اجتماع لفريق رفيع المستوى معني بالتعاون الرقمي، أصدر تقريره في عام 2019. ومن خلال سلسلة لاحقة من مناقشات المائدة المستديرة مع الدول وغيرها من الجهات صاحبة المصلحة الرئيسية الأخرى، وضعت خريطة طريق أوصت باتخاذ المزيد من الإجراءات للمضي قدما بالتعاون في المجالات الرئيسية في الفضاء الرقمي.

وفي سياق السلام والأمن، أطلق الأمين العام أيضا خطة لنزع السلاح تركز على فهم ومعالجة تكنولوجيات الجيل الجديد التي تشكل تحديات محتملة للقواعد القانونية والإنسانية والأخلاقية القائمة؛ وعدم الانتشار ؛ والسلام والأمن.

ويلتزم الأمين العام في جدول أعماله بالمشاركة والعمل مع العلماء والمهندسين وقطاع الصناعة لتشجيع الابتكار المسؤول في مجال العلم والتكنولوجيا وكفالة تطبيقهما للأغراض السلمية.

ويؤكد التزامه للمرة الثانية بالعمل مع الدول الأعضاء على تعزيز ثقافة المساءلة والالتزام بما يستجد من معايير وقواعد ومبادئ بشأن السلوك المسؤول في الفضاء الإلكتروني.

وفي حين أن الفضاء الرقمي يكاد يشكل اليوم أساس جميع جوانب حياتنا اليومية، فإن حجم "انعدام الأمن" وانتشاره في مجال تكنولوجيا المعلومات والاتصالات يعتبران الآن أيضا مصدري قلق رئيسيين. وقد تؤدي الصعوبات السياسية والتقنية في عزو وإسناد المسؤولية عن الهجمات التي تشن باستخدام تكنولوجيا المعلومات والاتصالات إلى عواقب وخيمة، تتخذ أشكالا من بينها استجابات مسلحة غير مقصودة وعمليات تصعيد.

ويمكن أن تشجع هذه الديناميات الدول على اتخاذ مواقف هجومية في وجه الاستخدام العدائي لهذه التكنولوجيات. كما يمكن أن تؤدي إلى تمكين جهات مسلحة وإجرامية غير تابعة للدولة، فرادى وجماعات، تسعى إلى تطوير قدرات يمكن أن تزعزع الاستقرار أو الحصول عليها دون عقاب يذكر. ونظرا لما لهذه الآثار الناجمة عن أخطار تكنولوجيا المعلومات والاتصالات من عواقب على صون السلام والأمن الدوليين، تكتسي مشاركة مجلس الأمن في هذه المسألة أهمية بالغة.

ولذلك، فإنني أرحب بهذه الفرصة لتقديم إحاطة إعلامية إلى المجلس، وأتطلع إلى المناقشة التي ستعقب ذلك.

المرفق الثاني

بيان رئيسة وزراء إستونيا، كايا كالاس

لقد أنشئت الأمم المتحدة من منظور المستقبل. ورغم أننا نواجه عددا من التحديات الجديدة، فإن القيم والمبادئ المتفق عليها في ميثاق الأمم المتحدة قبل 76 عاما ما زالت صالحة اليوم. وقد أصبح التمسك بها في مستقبلنا الذي يغلب عليه الطابع الرقمي بصورة متزايدة واحدا من المهام العالمية الأكثر إلحاحا. واليوم، أريد أن أتحدث عن ما لدينا من فرص وآليات تمكننا من الاضطلاع بها وما يحيق بنا من أخطار ونحن بصدد القيام بذلك.

ولنتناول الفرص أولا: فقد برهنت السنة ونصف السنة الأخيرة من العمل والدراسة عن بعد والحياة بوضوح أن اعتمادنا على التكنولوجيا الرقمية وتكنولوجيات الاتصالات لن يكون من شأنه إلا أن يتزايد مع مرور الوقت. ونحن مسؤولون عن بناء مستقبل تتبع فيه جميع الجهات الفاعلة التزامات معينة فيما يتعلق بسلوكها في الفضاء الإلكتروني.

ولهذا السبب فإن المناقشة التي تدور اليوم ليست عن التكنولوجيا، بل هي مناقشة بشأن كيفية استخدام الفضاء الإلكتروني. لقد أحسن ستيف جوبز وصف التكنولوجيا حينما قال: "التكنولوجيا لا تمثل شيئا. المهم هو أن تؤمن بالناس، وبأنهم في الأساس ماهرون وأذكياء، وأنهم إذا ما أوتوا الأدوات، فسوف يفعلون بها أشياء رائعة".

وإستونيا، بوصفها مجتمعا رقميا مزدهراً، مرت بهذه التجربة بصورة مباشرة. إن الفضاء الإلكتروني الحر والمفتوح والمستقر والآمن هو جزء من شريان حياتنا. وقد وفرنا نسبة إضافية من ناتجنا المحلي الإجمالي تتراوح بين 2 و 3 في المائة كل عام بفضل نقل معظم الخدمات الحكومية إلى فضاء الإنترنت. لقد ظلت إدارتنا العامة الروتينية غير ورقية لأكثر من 15 عاما حتى الآن. كما أنتجت إستونيا أكبر عدد من شركات التكنولوجيا العملاقة الناشئة قياسا إلى عدد السكان.

ثانيا، الأخطار: يجب أن ندرك أن الرقمنة السريعة لها أيضا جانب مظلم. فالجهات الفاعلة الخبيثة يمكنها أن تتخذ من الفضاء الإلكتروني ميدانا آخر تعيث من خلاله الفساد. وعلى سبيل المثال، تخيل ماذا سيحدث إذا توقفت سلسلة إمدادات المياه في بلد ما عن العمل في منتصف فترة جفاف، أو تعطلت شبكة الكهرباء في بلد ما خلال أشهر الشتاء الباردة.

لقد شهدنا خلال العام الماضي كيف يمكن أن تشكل الأنشطة السيبرانية الضارة التي تستهدف قطاع الرعاية الصحية خطرا حقيقيا وملموسا. وقد تترتب آثار إنسانية مدمرة على العبث بالبنية التحتية الحيوية.

وبينما يمكننا إقامة أسوار عالية ووضع حراس حول محطات الطاقة التي نملكها وغيرها من البنى التحتية الحيوية، لا يمكن أن يكون هذا أبدا جزءا من الحل في الفضاء الإلكتروني. وبدلا من ذلك، يجب أن نتولى دور الحراس بصورة جماعية.

وأخيرا، لنتناول كيفية التصدي لهذه الأخطار: فلحسن الحظ، وكما أوضحت أيضا مقدمة الإحاطة البارزة، السيدة ناكاميتسو، فإن لدينا أساسا متينا ننطلق منه في عملنا.

فقد اتفقت الدول الأعضاء خلال العقد الماضي على إطار معياري فعال للاستقرار في الفضاء الإلكتروني ومنع نشوب النزاعات. وقوام هذا الإطار هو تطبيق القانون الدولي القائم و 11 من المعايير الطوعية لسلوك الدولة المسؤول وتدابير بناء الثقة وبناء القدرات.

وتعتقد إستونيا اعتقادا راسخا أن القانون الدولي القائم ينطبق في الفضاء الإلكتروني، بما في ذلك ميثاق الأمم المتحدة في مجمله، والقانون الدولي الإنساني والقانون الدولي لحقوق الإنسان.

واسمحوا لي أن أؤكد أن الدول مسؤولة عن أي أفعال ترتكب خلافا لالتزاماتها بموجب القانون الدولي.

ولضمان حماية المدنيين والأعيان المدنية في حالات النزاع المسلح على وجه الخصوص، التي يناقشها مجلس الأمن أيضا بانتظام، من المهم للغاية أن يخضع أي استخدام للقدرات السيبرانية في هذا السياق لالتزامات مستمدة من القانون الدولي الإنساني.

وتعكس المعايير الـ 11 لسلوك الدول المسؤول التي اتفقنا عليها توقعات المجتمع الدولي، وترسي مبادئ توجيهية إضافية هامة لأنشطة الدول في الفضاء الإلكتروني.

وفي ربيع هذا العام، قدم المجتمع الدولي تأكيدا قويا جدا للمرة الثانية على هذا الإطار المعياري. وتشكل النتائج الناجحة التي توصل إليها بتوافق الآراء كل من آخر فريق للخبراء الحكوميين والفريق العامل المفتوح العضوية مصدرا للتشجيع والتوجيه. وتنفيذ هذا الإطار هدف رئيسي للمجتمع الدولي.

وينبغي أيضا أن تكون الجهود العالمية مصحوبة بأنشطة إقليمية وبناءٍ للقدرات. وفي هذا الصدد، نسلط الضوء على العمل الهام الذي تقوم به المنظمات الإقليمية لتعزيز الثقة والدفع قدما بجهود التعاون. كما تعطي إستونيا الأولوية للجهود الرامية إلى سد الفجوة الرقمية، التي يجب أن تسير جنبا إلى جنب مع بناء القدرات في مجال قدرة النظم الإلكترونية على الصمود، ومع حماية حقوق الإنسان على الإنترنت.

ويجب أن نعترف أيضا بأننا نتصدى للتهديدات السيبرانية بالتعاون مع القطاع الخاص والمجتمع المدني والأوساط الأكاديمية. وللشركات على وجه الخصوص دور هام يتعين عليها أن تؤديه من خلال الاستثمار في الأمن السيبراني والمساعدة في القضاء على أوجه الضعف.

وإنني على ثقة بأن مناقشة اليوم ستكون علامة فارقة في تاريخ مجلس الأمن ونحن بصدد معالجة المسائل التي ستكون هي الأكثر أهمية من أجل الحفاظ على السلام والاستقرار الدوليين لسنوات قادمة.

ولن يتم تأمين مستقبلنا الرقمي إلا إذا اتبعنا قواعد الطريق بشأن العمليات الفضائية في المستقبل.

المرفق الثالث

بيان رئيس وزراء جمهورية النيجر، أوهومودو محمودو

[الأصل: بالفرنسية]

اسمحوا لي أولا وقبل كل شيء أن أشيد بإستونيا لالتزامها بإدراج مسألة المخاطر الأمنية المتصلة بالفضاء الإلكتروني في جدول أعمال المجلس.

وأود أيضا أن أشكر السيدة إيزومي ناكاميتسو على إحاطتها وعلى التزامها الشديد بهذه المسألة.

لقد ازداد تغلغل الإنترنت واستخدام تكنولوجيات المعلومات والاتصالات بسرعة البرق على مدى العقدين الماضيين. واليوم، أصبح الفضاء الإلكتروني عاملا جيوسياسيا يسمح لمختلف الدول بتوسيع نطاق نفوذها على المستويات الاقتصادية والسياسية والثقافية.

كما أن الثورة الرقمية، التي قربتنا من بعضنا البعض بإزالة الحدود القائمة بيننا، فتحت الطريق لتحديات جديدة تواجه السيادة بسبب الطابع المتجاوز للحدود الإقليمية الذي تتسم به القوانين المتعلقة بالسيادة. ومثلما يمكن لهذا الفضاء أن يعزز ديمقراطياتنا بتوفير منبر ووسائل تتيح إيصال جميع الأصوات، حتى أصوات المنشقين، فقد يثبت أيضا أنه ملاذ لجهات فاعلة وجماعات إجرامية يتمثل هدفها الوحيد في زعزعة استقرار أممنا.

لقد كشفت لنا جائحة مرض فيروس كورونا (كوفيد-19) وجهين للفضاء الإلكتروني: فمن ناحية أظهرت اعتمادنا المتزايد على التكنولوجيات الرقمية، الذي يعد هذا الاجتماع الافتراضي مثالا له، ومن ناحية أخرى، فقد أثبتت هشاشة أنظمتنا عندما نواجه جرائم سيبرانية محتملة وتجسسا سيبرانيا، وهو ما يتضح من خلال هجمات فيروسات الفدية على النظم الصحية وحملات التضليل التي تهدف إلى تقويض ثقة مواطني بلداننا في جهود التطعيم.

وعلاوة على ذلك، أدى ازدهار شبكات التواصل الاجتماعي وغيرها من منابر النقاش إلى انتشار أنواع معينة من الخطابات التي تحرض على أعمال العصيان والإرهاب والاعتداء على القيم الأخلاقية والأسس التي تقوم عليها ديمقراطياتنا.

وبالنظر إلى كل ما سبق، اسمحوا لي أن أقدم بعض التوصيات التي أعتقد أنها قد تعزز احترام القانون الدولي، فضلا عن تنفيذ قواعد مسؤولة لاشتراك الدول في أنشطة الفضاء الإلكتروني.

أولا، يجب سد الفجوة الرقمية بين الأمم، ولا سيما مع القارة الأفريقية، حيث لا تتوافر لثلاثة أرباع السكان إمكانية الحصول على خدمات الإنترنت بصورة كافية، أو لا تتوافر لهم إمكانية الحصول عليها على الإطلاق.

وكما ذكر الخبراء، تشكل هذه الحالة عاملا من عوامل ترسيخ الفقر، وتحمل تداعيات تنعكس آثارها على الجميع وعلى كل مكون من مكونات المجتمع، من الرعاية الصحية إلى الازدهار الاقتصادي وحتى التعليم؛ فهي تجعل تلك المجالات أكثر عرضة لحملات التضليل والأخطار الرقمية الأخرى. ولا يمكننا أن نأمل في فضاء إلكتروني سليم وآمن دون ضمان الإنصاف الرقمي.

وعلى هذا الأساس، فإن توصيتي الثانية هي وضع هيكل عالمي من خلال نهج متكامل ومنسق يسمح بتحديد واضح لقواعد القانون الدولي المنطبقة على الفضاء الإلكتروني، في مجالات رحبة مثل الرعاية الصحية والقانون الدولي الإنساني والعملية الانتخابية والنشاط الاقتصادي، على سبيل المثال لا الحصر.

بيد أنه يتعين علينا ونحن بصدد القيام بذلك أن ندرك أيضا أن هذا الهيكل يجب أن يكون منصفا، سواء في التنفيذ أو فيما يتعلق بجني ثماره، من أجل تجنب إنشاء آليات جديدة تطبق معايير مزدوجة لن تؤدي إلا إلى تعميق أوجه عدم المساواة بين الدول بإجبارها على التعامل مع الآثار السلبية الأخرى.

ووفقا لهذا النهج، سيكون من المناسب أن يسترشد أي هيكل تنظيمي جديد على الصعيد العالمي بالهياكل التي أنشئت بالفعل على الصعيد الإقليمي، والتي يلزم أن توائم اللوائح المعمول بها على الصعيد الوطني وعلى مستوى الدولة. ومن ثم ينبغي أن نذكر توجيه الجماعة الاقتصادية لدول غرب أفريقيا بشأن مكافحة الجرائم السيبرانية، الذي يفرض التزامات في ذلك المجال على الدول الأعضاء، بما في ذلك توقيع عقوبات على أفعال معينة، وينشئ إطارا لتيسير التعاون الإقليمي بشأن الأمن السيبراني.

وتوصيتي الأخيرة هي أن يعمل مجلس الأمن على تفسير ميثاق الأمم المتحدة تفسيرا أكثر شمولا للجميع وأقل تمييزا، بل وتفسير ولايته أيضا على هذا النحو، حتى تعكس مداولاتنا حقائق عالم اليوم، وبالتالي تتناول مواضيع مثل الأمن السيبراني وتغير المناخ والأوبئة، لأن هذه أخطار حقيقية لا تعترف بالحدود، مثلها في ذلك مثل كوفيد-19 تماما.

المرفق الرابع

بيان وزير الخارجية والدفاع في أيرلندا، سايمون كوفني

أود أن أزجي تهنئتي لإستونيا على رئاستها الناجحة للمجلس.

كما أشكر الممثلة السامية على أفكارها الثمينة.

وأرحب بهذه المناقشة التي تجرى في الوقت المناسب، وهي الأولى من نوعها في مجلس الأمن.

ودعا الأمين العام، في معرض حديثه في العام الماضي، الدول إلى إحلال النظام في ما أسماه "العالم الموحش للفضاء الإلكتروني".

وبينما أحرز تقدم محمود في الأمم المتحدة في الأشهر الأخيرة، ما زالت التحديات التي تواجهها الدول فيما يتعلق بالأمن السيبراني في تزايد، مما يعرض السلام والأمن الدوليين للخطر.

وأود أن أركز ملاحظاتي اليوم على ثلاثة مناحي:

- التحديات والفرص
- ضرورة أن تنفذ الدول التدابير المتفق عليها في الأمم المتحدة
- أهمية اتباع نهج قائم على القيم في معالجة هذه المسألة

أولا، التحديات والفرص.

تواصل التكنولوجيات الرقمية وتكنولوجيات الاتصالات دفع عجلة النمو الاقتصادي وإحداث تحولات جذرية في أسلوب حياتنا وكيفية التواصل والعمل.

والابتكار هو المفتاح لمواجهة بعض التحديات العالمية الحرجة التي نواجهها اليوم، بما في ذلك تغير المناخ. كما أنه يسهل قطع أشواط هامة في البحوث الطبية، ويحسن فرص الحصول على التعليم، ويعزز قدرات حفظة السلام لدينا، ويساعدهم على الحفاظ على سلامتهم.

وسلطت الجائحة الضوء خلال العام الماضي على اعتمادنا المتزايد على تكنولوجيا المعلومات والاتصالات، ووحدت صفوف الناس معا في أوقات يتعين عليهم فيها الابتعاد عن بعضهم البعض، وكشفت في الوقت نفسه عن نقاط ضعفنا.

وأتكلم عن هذه النقطة الأخيرة من واقع التجربة التي شهدناها مؤخراً. فقد تعرضت أنظمة الرعاية الصحية العامة في أيرلندا لهجوم ضار للغاية من فيروسات الفدية الشهر الماضي أثر على الخدمات الطبية الحيوية.

إن هجوما من هذا النوع خلال جائحة عالمية لهو حادث مروع. ومن المؤسف أن تجربة أيرلندا ليست معزولة على الصعيد الدولي.

فقد تصاعد عدد الأنشطة السيبرانية الخبيثة في السنوات الأخيرة، بما في ذلك الهجمات المدمرة باستخدام فيروسات الفدية المكبلة، والجرائم السيبرانية، وسرقة الملكية الفكرية، ونشر المعلومات المضللة والكراهية.

ويجري استهداف البنية التحتية الحيوية على نحو متزايد.

ويساور أيرلندا قلق بالغ لأن هذا النشاط يشكل تهديدا للسلام والأمن الدوليين.

وتتفاقم التحديات الأمنية القائمة بسبب التهديدات السيبرانية، من قبيل ضعف منظومات القيادة والتحكم في مجال الأسلحة النووية في مواجهة الهجمات السيبرانية. وهذا يضفي طابعا جديدا ملحا على ضرورة إحراز تقدم في نزع السلاح النووي.

وليس بوسعنا أن نسمح للفضاء الإلكتروني بأن يكون غير مقيد بالقواعد أو القوانين كي ترتع فيه الجهات الفاعلة الخبيثة كيفما شاءت.

ويجب حل النزاعات الدولية في الفضاء الإلكتروني بالوسائل السلمية.

ويجب على المجلس أن يبث رسالة واضحة داعمة لفضاء إلكتروني عالمي سلمي وآمن يقوم على توافق الآراء والثقة المتبادلة.

وأنتقل الآن إلى نقطتي الثانية لأعرب عن ترحيب أيرلندا بالتقدم الذي أحرز مؤخرا في الأمم المتحدة بشأن الاتفاق على إطار لسلوك الدولة المسؤول في الفضاء الإلكتروني.

وقد أكدت الدول من جديد الآن أن القانون الدولي القائم، ولا سيما ميثاق الأمم المتحدة، يوفر أساسا متينا يستند إلى القواعد لجميع النهج المتبعة في مجال الأمن السيبراني.

وتؤيد أيرلندا الجهود الرامية إلى التوصل إلى فهم أعمق فيما بين الدول بشأن تطبيق القانون الدولي على الفضاء الإلكتروني.

وسننشر قريبا موقفنا الوطني، ونشجع الآخرين على أن يحذوا حذونا.

وبطبيعة الحال، فإن سلوك الدولة المسؤول أمر بالغ الأهمية أيضا.

وقد وافق جميع الدول الأعضاء على الاسترشاد بالمعايير الطوعية الـ 11 بشأن سلوك الدول في الفضاء الإلكتروني.

ويتعين علينا الآن أن نعمل على تعزيز فهم وتنفيذ هذه المعايير، استنادا إلى الأسس التي يقوم عليها القانون الدولي، لتعزيز الأمن السيبراني على الصعيد العالمي. وهذا من شأنه أن يؤدي إلى تقليل احتمالات نشوب النزاعات وتحسين العلاقات الدولية.

وتؤدي تدابير بناء الثقة، بما في ذلك الحوار، إلى غرس الطمأنينة والحد من التوترات بين الدول. وأنا أعلم أن هذا أمر واضح بذاته، ولكن لا بد من التصريح به.

ونرحب بالدور القيادي الذي تضطلع به المنظمات الإقليمية في هذا الصدد، بما في ذلك منظمة الأمن والتعاون في أوروبا. وتلتزم أيرلندا وشركاؤنا في الاتحاد الأوروبي بدعم مبادرات بناء القدرات.

وفي ظل وجود فضاء إلكتروني شديد الترابط، لن ينعم بلد بالأمان حتى تصبح جميع البلدان آمنة. وهذا بالتأكيد ما تعلمناه من جائحة مرض فيروس كورونا (كوفيد-19).

كما أننا مازلنا ملتزمين بمعالجة الفجوة الرقمية على الصعيد العالمي. وسيكون توفير إمكانية حصول الجميع على خدمات الإنترنت عنصرا رئيسيا في تحقيق أهداف التنمية المستدامة في العقد القادم.

والنقطة الثالثة التي أود أن أطرحها هي أن صون السلام والأمن الدوليين في الفضاء الإلكتروني يجب أن يكون محوره الإنسان وأن يستند إلى القيم.

وتدعم أيرلندا تهيئة فضاء إلكتروني آمن وميسر وتطبق فيها حقوق الإنسان والحريات الأساسية، سواء على الإنترنت أو خارجه.

ونحن نؤكد من جديد بقوة على انطباق القانون الدولي لحقوق الإنسان على الإجراءات التي تتخذها الدول في الفضاء الإلكتروني.

وتظل حماية المدنيين أولوية رئيسية في جميع جوانب عملنا. وفي هذا الصدد، تلتزم أيرلندا بضمان احترام القانون الدولي الإنساني في الفضاء الإلكتروني.

ومن الحقائق المحزنة أن العنف الجنساني الذي يتعرض له عدد كبير جدا من النساء والفتيات كثيرا ما يصاحبه حاليا عنف على الإنترنت وتهديدات سيبرانية تؤدي إلى تفاقمه.

وهذا يزيد من أهمية قيامنا، نحن معشر القادة، بوصفنا زعماء، بتشجيع واع لمشاركة المرأة في عمليات الأمم المتحدة وقراراتها وسياساتها المتعلقة بالفضاء الإلكتروني.

وعلينا أن نبذل مزيدا من الجهد للتغلب على الفجوة الرقمية بين الجنسين.

وقد دأبت أيرلندا على الدعوة إلى إشراك طائفة أوسع من ذوي الخبرات في مناقشات الأمم المتحدة بشأن الأمن السيبراني وبناء القدرات.

وتقع مسؤولية الحفاظ على فضاء إلكتروني آمن وحر على عاتق الحكومات، إلى جانب أولئك الذين يدفعون قاطرة الابتكار التكنولوجي ويقودون زمامه.

وقد أثرت مساهمات المجتمع المدني والخبراء التقنيين والأكاديميين والقطاع الخاص المناقشات السيبرانية السابقة التي أجريت في الأمم المتحدة. وما زال انخراطهم في مسألة الأمن السيبراني حتى الآن محدودا للغاية، في رأينا.

كما نؤيد المبادرات، بما في ذلك نداء باريس من أجل الثقة والاستقرار في الفضاء الإلكتروني، التي تجمع بين أصحاب المصلحة من الدول وغير الدول على هدف مشترك يتمثل في تعزيز السلام والأمن.

ويجب علينا جميعا أن نعمل معا للتوصل إلى حلول مشتركة أفضل.

وفي الختام، ستواصل أيرلندا دعم النهج البناءة والمتعددة الأطراف والمتعددة أصحاب المصلحة، المبنية على توافق الآراء، لتعزيز القدرة على الصمود في الفضاء الإلكتروني في جميع أنحاء العالم.

وندعو جميع الدول إلى التصرف بطريقة مسؤولة، في إطار من الامتثال التام للقانون الدولي، وتنفيذ الإطار المعياري.

ونحن نقدر دور مجلس الأمن في منع نشوب النزاعات والنهوض بالسلام والأمن، بما في ذلك النهوض بهما في الفضاء الإلكتروني.

ونحث جميع الدول على الاستفادة من الإنجازات التي تحققت في الأمم المتحدة خلال الأشهر الأخيرة.

وبهذه الطريقة يمكننا أن نكفل تهيئة فضاء إلكتروني عالمي أكثر أمنا وسلاما يستفيد منه الجميع.

المرفق الخامس

بيان وزير خارجية فييت نام، بوي ثانه سون

أشكر الرئيسة والرئاسة الإستونية على الدعوة إلى عقد هذه الجلسة بشأن مسألة هامة للغاية. وإنني ممتن لوكيلة الأمين العام ناكاميتسو لما أبدته من ملاحظات ثاقبة.

لقد أدى التطور الهائل في تكنولوجيا المعلومات والاتصـــالات إلى إحداث تحول كبير في طريقة عيش الناس وعملهم وتواصلهم مع بعضهم البعض. وأدى إلى تيسير الاتصالات العالمية وتبادل المعارف والتبادل الثقافي، وساعد الشعوب والبلدان على التقارب، كما أدى إلى تجديد الإنتاج بهدف الوصـول إلى أنماط إنتاج أكثر كفاءة واستدامة وشمولا.

ومن ناحية أخرى، يمكن أن تشـكل هذه التكنولوجيات المتقدمة، إذا وقعت في الأيدي الخطأ واسـتخدمت لأغراض خبيثة، تهديدات خطيرة لسـيادة الأمم وأمنها وازدهارها. ويقوم الإرهابيون أو مرتكبو الجرائم العابرة للحدود الوطنية بنشـر هذه التكنولوجيات القادرة على تخريب النظم الاقتصـادية، والعبث بالاستقرار الاجتماعي، وإهدار القيم الثقافية والإنسانية.

ولنذكر الخسـائر الاقتصـادية الناجمة عن الهجمات السـيبرانية كمثال. فقد بلغ الإنفاق العالمي السنوي على الأمن السيبراني تريليون دولار في عام 2020، بزيادة قدرها 50 في المائة مقارنة بعام 2018 وزيادة بمقدار ثلاثة أضعاف منذ عام 2013. ويوجه معظم النفقات إلى جبر الأضرار والتعافي من آثارها.

والأمر الأكثر إثارة للقلق هو ماورد من تقارير تفيد بوقوع هجمات سـيبرانية عابرة للحدود الوطنية قوضت الأمن على الصعيدين العالمي والوطني، بل وربما تحمل في طياتها احتمال اندلاع حرب سيبرانية.

ومن هذا المنطلق، يشكل الأمن السيبراني ضرورة ملحة للغاية ولا غنى عنه من أجل تحقيق السلام والأمن والتنمية والازدهار على الصـعيدين الوطني والعالمي على السـواء. وإزاء هذه الخلفية، أود أن أتطرق إلى النقاط التالية:

أولا، لكل دولة سـيادتها على الفضـاء الإلكتروني ومصـالحها الخاصـة فيه التي يتعين احترامها بصورة كاملة. وتتحمل كل دولة عضو المسؤولية الرئيسية عن إنشاء الإطار القانوني لتنظيم السلوك في الفضـاء الإلكتروني داخل إقليمها، وتطبيقه على مواطنيها. كما أن تنظيم السـلوكيات وفقا للقانون ومنع الأعمال الخبيثة غير المشروعة وتيسير الأنشطة الإيجابية هي مبادئ توجيهية لتهيئة فضاء إلكتروني آمن ومستقر من أجل السلام والتنمية والإنسانية.

وفييت نام بلد يتمتع بتغطية عالية بالإنترنت، حيث ينشـط ما يقرب من 70 في المائة من سـكاننا على شـبكة الإنترنت وشـبكات التواصـل الاجتماعي. ومكمن نجاحنا هو وجود إطار قانوني شـامل ييسـر تطوير تكنولوجيا المعلومات والاتصـالات ويحول دون إسـاءة اسـتخدامها. كما تعطي فييت نام الأولوية لتحسين الحماية الذاتية والاعتماد على الذات والقدرة على الصمود، إلى جانب التعاون الدولي الفعال.

ثانيا، إن الهجمات الإلكترونية ذات طبيعة عابرة للحدود الوطنية حيث تصـبح شـبكات الإنترنت العالمية هدفا للاسـتغلال المسـتمر من جانب الجناة. ويتطلب ذلك في المقابل حلولا عالمية وعابرة للحدود الوطنية للمشاكل المتعلقة بالأمن السيبراني. وتؤيد فييت نام وضع إطار دولي يحدد قواعد ومعايير السلوك المسؤول في الفضاء الإلكتروني، على أساس توافق الآراء، وبأوسع مشاركة من جانب البلدان، بما في ذلك

العمليات الجارية في الأمم المتحدة. إننا نشعر بالقلق ونعارض الاستخدام الخبيث والضار لتكنولوجيا المعلومات والاتصالات، ولا سيما الهجمات السيبرانية على المرافق الطبية ومرافق الكهرباء والمياه والمرافق الغذائية التي تمثل ضرورة لا غنى عنها للناس. وينبغي أن تمتثل الأنشطة التي تجري في الفضاء الإلكتروني لمبادئ ميثاق الأمم المتحدة والقانون الدولي، ولا سيما احترام السيادة، وعدم التدخل في الشؤون الداخلية للدول، وعدم استخدام القوة وتسوية المنازعات بالوسائل السلمية.

ثالثا، لا غنى عن تعزيز التعاون الدولي وبناء الثقة والمساءلة من أجل تعزيز الأمن السيبراني. ويستفيد جميع البلدان، بغض النظر عن حجمها ومستوى تنميتها، من وجود فضاء إلكتروني عالمي مأمون وآمن. ولذلك، فإنها تحتاج إلى المشاركة بنشاط وتقديم مساهمات أكثر مسؤولية واتصافا بالطابع العملي في الجهود الرامية إلى ضمان السلامة والأمن في الفضاء الإلكتروني العالمي من أجل تحقيق السلام والاستقرار والتنمية المستدامة لجميع الدول.

إن تطوير تكنولوجيا المعلومات والاتصالات هو نقطة انطلاق هامة في سعينا المشترك لتحقيق الرخاء. وقد نفذت فييت نام بنشاط استراتيجية وطنية للتحول الرقمي. ونحن نهدف إلى جعل الاقتصاد الرقمي يمثل 30 في المائة من الناتج المحلي الإجمالي بحلول عام 2030. وفي جنوب شرق آسيا، شاركت فييت نام بصورة نشطة في آليات الأمن السيبراني على الصعيد الإقليمي، بما في ذلك استراتيجية رابطة أمم جنوب شرق آسيا للتعاون في مجال الأمن السيبراني. كما أننا نتعاون تعاونا ثنائيا فعالا مع العديد من البلدان والشركاء الدوليين في هذا الميدان. وفييت نام على استعداد لزيادة الإسهام في تعزيز التعاون الدولي من أجل تهيئة فضاء إلكتروني سلمي ومستقر وآمن ومن أجل ازدهارنا المشترك وتحقيق التنمية المستدامة.

المرفق السادس

بيان من أمين مجلس الوزراء لشـــؤون تكنولوجيات المعلومات والاتصـــالات والابتكار والشباب في كينيا، جو موشيرو

أهنئ الرئيسة على عقد مناقشة مستقلة، لأول مرة في مجلس الأمن، بشأن الأمن السيبراني. وأشكر الممثلة السامية لشؤون نزع السلاح، السيدة ناكاميتسو، على إحاطتها الوافية.

إن اعتمادنا المتزايد على تكنولوجيا المعلومات والاتصالات يجلب لنا منافع ويعرضنا لأوجه ضعف في آن واحد.

وتقابل جهود أولئك الذين يطورون ويسـتخدمون تكنولوجيا المعلومات والاتصـالات والتكنولوجيات الناشئة للأغراض السلمية بشكل وثيق جهود مخالفيهم الذين يستخدمونها للسيطرة والمراقبة غير المشروعة والاحتيال وتغذية نزعة التطرف وزعزعة الاستقرار.

وكينيا ملتزمة بالمحافظة على نطاق إنترنت حر ومفتوح وحمايته. فنحن نعتبره محركا رئيسيا للتنمية الوطنية، ونسعى إلى تمكين شبابنا من استخدامه وتنافسهم في ذلك.

وقد حققنا ســـبقاً عالميا في مجال العملة الرقمية بريادتنا نظام الدفع بالهاتف المحمول (M-PESA) – الذي يعد أول منصـة أموال متنقلة مسـتخدمة على نطاق واسـع. كما تبنت حكومتنا توفير منصـــات الخدمات العامة الرقمية من خلال مرافقنا للخدمات الشـــاملة، المعروفة باســـم "مراكز هودوما"، المنتشرة في جميع أنحاء البلد.

ويقوم الشباب الكينيون بابتكار وإنشاء شركات تحويلية. وقد اعترف المستثمرون بذلك على مستوى العالم حيث جذبت شركتنا "سيليكون سافانا" أكبر قدر من الاستثمارات في منطقتنا. ونحن نعتقد أن العديد من فرص العمل اللائق التي ستتاح لنا في المستقبل سوف تأتي من هذه الشركات.

وفي ظل هذا التعرض الواســـع النطاق للمجال الرقمي، ترى كينيا أن تأمين تكنولوجيا المعلومات والاتصالات هدف أمني وطني لا غنى عنه.

وتحقيقا لهذه الغاية، يوجد لدينا إطار تنظيمي محكم. ولدينا أيضـــا قدرات متزايدة على مجابهة الأخطار. ويتعاون الفريق المعني بالحوادث الحاســـوبية الطارئة والتصـــدي لها مع الأفرقة الأخرى المعنية بالاســتجابة لحوادث الطوارئ الحاســوبية على الصــعيد الوطني، وعلى الصــعيد الدولي من خلال المنتدى العالمي لفرق التصدي للحوادث والأمن.

ومهمتنا اليوم هي تقديم مقترحات بشـــأن الكيفية التي يمكن بها لمجلس الأمن أن يكفل تحقيق الســلام والأمن الدوليين على نحو أفضــل في مواجهة الأخطار التي تصــلنا من خلال الفضــاء الإلكتروني أو أخطار استغلاله.

وسأسلط الضوء على ثلاث مجالات نعتقد أنها يمكن أن تستفيد من تحسين التعاون الدولي.

يتعلق المجال الأول بتكنولوجيا المعلومات والاتصالات والاقتصادات الناشئة. فقد أصبحت الجرائم السيبرانية تركز بشكل متزايد على الاقتصادات الناشئة. ومن الضروري تعزيز التعاون في النهوض بآليات تســـوية النزاعات الاقتصـــادية الإقليمية والدولية القائمة، بما في ذلك بذل جهود منســـقة لتحديد المخاطر

المرتبطة بالأنشطة ذات الصلة بتكنولوجيا المعلومات والاتصالات والحد منها من قبيل الاحتيال الرقمي، وتأثير العملات المشفرة على النظم المصرفية المركزية الوطنية، والهجمات السيبرانية على البنية التحتية الحيوية.

ومع تسارع وتيرة التشغيل الآلي في القطاع الصناعي، يجب استبدال فرص العمل المفقودة بفرص عمل لائقة أخرى وإلا فسيعاني السلام والأمن. وسيتعين بذل المزيد من الجهود للاستثمار في المهارات الرقمية التي تسمح للبلدان المتخلفة في مجال الصناعة باجتذاب الاستثمارات التي توفر الملايين من فرص العمل الجديدة.

ويتعلق المجال الثاني بتكنولوجيا المعلومات والاتصالات والتطرف العنيف. ورغم أن التكنولوجيات الناشئة التي تتسم بالانتشار الواسع النطاق والقابلية للبرمجة والاعتماد على البيانات مفيدة بحكم طبيعتها، فقد فتحت أيضا الباب أمام إساءة الاستخدام من جانب الجماعات المسلحة والإرهابيين. وتستفيد هذه الجماعات من آليات المراقبة المبهمة، والخوارزميات، والطباعة الثلاثية الأبعاد، وتطبيق علم التشفير، وواجهات المستخدم المبسطة لتجنيد مرتكبي الأعمال الإرهابية والتخطيط لها وتنفيذها. وقد أدى ذلك إلى تعزيز تغذية نزعة التطرف والعسكرة.

وتدعو كينيا إلى تعزيز التعاون بين مجلس الأمن ومكتب مكافحة الإرهاب لبناء قدرة أمنية في سيبرانية تكون فاعلة ومستجيبة لتلبية احتياجات الدول الأعضاء في مجال بناء القدرات.

كما سيتعين على ولايات عمليات الأمم المتحدة للسلام أن تنظر في استخدام الفضاء الإلكتروني من قبل جهات عسكرية معادية.

أما مجال التركيز الثالث الذي أود تسليط الضوء عليه فهو تكنولوجيا المعلومات والاتصالات ووسائل التواصل الاجتماعي. ولا يمكن المبالغة في تقدير الأثر المتزايد للأخبار المزيفة، وممارسات تزييف الوجوه باستخدام خوارزميات التعلم العميق، والمعلومات المغلوطة والمضللة على السلام والأمن. وقد شهدنا مؤخرا تأثير الأخبار المزيفة التي أبطأت جهود التصدي لخطر جائحة مرض فيروس كورونا (كوفيد-19) من خلال تقوية نزعة التردد في أخذ اللقاح.

وسيتعين محاسبة شركات وسائل التواصل الاجتماعي وإرغامها على كفالة عدم انتشار الأخبار المزيفة على منصاتها، ولا سيما الأخبار التي تروج لها جهات فاعلة متطورة، بعضها مدعوم من دول. وسوف يتعين أن يؤسس هذا الجهد التنظيمي استنادا إلى برنامج متعدد الأطراف لضمان اتساق الأثر.

وأختتم بياني بالتأكيد على استعداد كينيا للمساهمة في تعزيز الجهود العالمية والأطر والمعايير المؤسسية التي من شأنها أن تزيد من إمكانات وجود مجال سيبراني حر وسلمي ومستقر، وتؤدي إلى الحد من الأخطار في الوقت نفسه.

المرفق السابع

بيان الممثلة الدائمة للولايات المتحدة الأمريكية لدى الأمم المتحدة، ليندا توماس – غرينفيلد

أشكر الرئيسة وأشكر إستونيا على تنظيم هذه المناقشة الهامة اليوم. ونحن ممتنون جدا لإستونيا على توجيه انتباه المجلس إلى هذه المسألة. وأشكر أيضا الممثلة السامية ناكاميتسو على إحاطتها ذات الرؤية الثاقبة.

وتأتي هذه المناقشة في الوقت المناسب. وفي ظل انتشار جائحة مرض فيروس كورونا (كوفيد-19) على وجه الخصوص، أصبحنا نعتمد على التكنولوجيا أكثر من أي وقت مضى، وها نحن نشهد ذلك بأنفسنا في هذا اليوم. ولكن الجهات من الدول ومن غير الدول على حد سواء تستغل هذا الاعتماد المتزايد. في الولايات المتحدة، أدت حوادث بارزة منفصلة استخدمت فيها فيروسات الفدية إلى تعطيل شركة JBS، وهي شركة كبرى في مجال صناعة الأغذية، وشركة Colonial Pipeline، وهي شركة توفر الوقود لجزء كبير من ساحلنا الشرقي. وتبين هذه الحوادث الخطر الجسيم وغير المقبول الذي تشكله الجرائم السيبرانية للبنية التحتية الحيوية. وغالبا ما لا يتم احتواء آثار هذه الأنشطة الخبيثة داخل الحدود أيضا. وعلى سبيل المثال استهدف النشاط السيبراني الخبيث شركة البرامج SolarWinds، وبرمجيات نظام البريد الإلكتروني Microsoft's Exchange Server.

لقد أضحت المخاطر واضحة. فبنيتنا التحتية – عبر الإنترنت وخارجها – معرضة للخطر. وأصبحت أهم خدماتنا الأساسية والحيوية، ابتداء من الطعام الذي نأكله، والماء الذي نشربه، وانتهاء إلى خدمات الرعاية الصحية التي اعتمدنا عليها جميعا أثناء الجائحة، أهدافا لتلك الأنشطة. لذا فعندما نتحدث عن الأمن العالمي في عالم اليوم، علينا أن نتحدث عن الأمن السيبراني. ولحسن الحظ، وعلى الرغم من اختلافاتنا الأيديولوجية، اجتمعت الدول الأعضاء مرارا وتكرارا على مدى العقد الماضي لمحاولة منع نشوب النزاعات الناجمة عن القدرات السيبرانية. وقد وضعنا معا إطارا لسلوك الدولة المسؤول في الفضاء الإلكتروني من خلال عملية فريق الخبراء الحكوميين. ويوضح الإطار أن القانون الدولي ينطبق على الفضاء الإلكتروني. كما أنه يحدد المعايير الطوعية والتدابير التعاونية العملية التي ينبغي للدول أن تتخذها.

وفي الأشهر الأخيرة، توصل الفريق العامل المفتوح العضوية، المؤلف من جميع الدول الأعضاء، إلى توافق في الآراء بشأن تقرير جديد يؤيد صراحة إطار سلوك الدول المسؤول في الفضاء الإلكتروني. وفي الشهر الماضي تحديداً، نجح فريق الخبراء الحكوميين السادس التابع للأمم المتحدة في اختتام أعماله بإصدار مجموعة قوية من التوصيات والتوجيهات الجديدة بشأن الإطار. وهذا تقدم. فهذه التقارير توفر توجيها حقيقيا، بدءا من استخدام الدولة للقدرات السيبرانية إلى معالجة المسألة المعقدة المتمثلة في إسناد المسؤولية عن الحوادث السيبرانية. كما ينظر الإطار في الكيفية التي ينبغي أن تتعاون بها الدول للتخفيف من آثار الكم الهائل من أنشطة الفضاء الإلكتروني الخبيثة الصادرة من إقليم دولة معينة، بما في ذلك الأنشطة التي يقوم بها المجرمون.

ونحن جميعا نتشاطر هذه المسؤولية. وكما أشار الرئيس بايدن مؤخرا، وأقتبس منه ذلك، "يتعين على البلدان اتخاذ إجراءات ضد المجرمين الذين يقومون بأنشطة على أراضيها تستخدم فيها فيروسات الفدية". لذا، اسمحوا لي أن أكون واضحة: عندما تخطر دولة ما بانبعاث نشاط خبيث من أراضيها، يجب أن تتخذ خطوات معقولة للتصدي له. ونظرا لطبيعة الفضاء الإلكتروني العابرة للحدود الوطنية، فإن هذا التعاون ضروري.

وها هو الإطار الذي عملت الدول الأعضـــاء جاهدة على وضـــعه يوفر الآن قواعد الطريق. وقد التزمنا جميعا بهذا الإطار. والآن، حان الوقت لوضــعه موضــع التنفيذ. ولدينا كثير من الأعمال التي يتعين علينا أن نقوم بها لضمان معرفة جميع الدول التي تريد أن تتصرف على نحو مسؤول في الفضاء الإلكتروني بالسياسات وامتلاكها القدرة التقنية اللازمة للتصرف على هذا النحو في الوقت نفسه. وبينما نقوم بهذا العمل، نحتاج أيضـــا إلى مواصـــلة حماية حرية الإنترنت. فالحقوق نفســـها التي يتمتع بها الأشـــخاص خارج عالم الإنترنت – بما في ذلك الحق في حرية التعبير وتكوين الجمعيات والتجمع الســلمي يجب أن تكون مشــمولة بالحماية عبر الإنترنت.

وقد أبدت الدول الأعضاء استعدادا ملحوظا لتجاوز الخلافات والتوصل إلى توافق في الآراء بشأن هذه المسائل. فلنواصل إظهار حسن النية ولنقدم للعالم جبهة موحدة بشأن الأمن السيبراني. وسوف نبني معا فضاءً إلكترونيا مفتوحا وآمنا ومستقرا يفيد الجميع.

المرفق الثامن

بيان وزير خارجية الهند، هارش فاردان شرينغلا

أتوجه بالشكر للرئيسة وأرحب بمبادرة إستونيا بتنظيم هذه المناقشة المفتوحة لتسليط الضوء على أحد المجالات المستجدة الهامة على صعيد الأمن السيبراني. وأشكر أيضا وكيلة الأمين العام ناكاميتسو على إحاطتها.

لقد ظل معنى السلام ثابتا منذ إنشاء مجلس الأمن، بيد أن طبيعة النزاع وأدواته الأساسية تغيرت بشكل هائل على مر العقود. واليوم أصبحنا نشهد تهديدات أمنية متزايدة للدول الأعضاء ناشئة عن الفضاء الإلكتروني، لم يعد من الممكن تجاهلها. ومن ثم، فإن هذه المناقشة المفتوحة تعقد في الوقت المناسب.

وقد أدى الاستخدام المتزايد لتكنولوجيات الفضاء الإلكتروني وتكنولوجيا المعلومات والاتصالات إلى تسريع وتيرة التنمية الاقتصادية، وتحسين تقديم الخدمات للمواطنين، وزيادة الوعي الاجتماعي، ووضع المعلومات والمعارف في متناول الجميع. فمعظم الأنشطة في هذا العصر السيبراني – السياسية والاجتماعية والاقتصادية والإنسانية والإنمائية (بما في ذلك هذه الجلسة الرفيعة المستوى لمجلس الأمن) – تجري الآن في الفضاء الإلكتروني أو ترتبط به. ولم تسفر جائحة مرض فيروس كورونا (كوفيد-19) إلا عن تسريع وتيرة رقمنة هذه الأنشطة وتوسيع نطاقها.

كما أن السمة الدينامية والمتطورة باستمرار للفضاء الإلكتروني قد جعلت أمن هذا الفضاء جزءاً من خطاب السلام والأمن. وقد شكل طابع الفضاء الإلكتروني الذي لا يعترف بالحدود، ولا سيما ما يتصف به من عدم الكشف عن هوية الجهات الفاعلة المعنية، تحديا للمفاهيم التقليدية السائدة بشأن السيادة والولاية القضائية والخصوصية. وهذه السمات الفريدة للفضاء الإلكتروني تطرح مجموعة متفردة من التحديات العديدة التي تواجه الدول الأعضاء. وسأركز في مداخلتي على ثلاثة تحديات رئيسية:

أولا، يستفيد بعض الدول من خبرتها في الفضاء الإلكتروني لتحقيق أهدافها السياسية والأمنية والانغماس في أشكال معاصرة للإرهاب العابر للحدود. ويشهد العالم بالفعل استخدام أدوات سيبرانية للإضرار بأمن الدول، من خلال جملة أمور منها مهاجمة البنى التحتية الوطنية الحيوية، بما في ذلك المرافق الصحية ومرافق الطاقة، بل وإفساد الوئام الاجتماعي من خلال تغذية نزعة التطرف. ولقد تعرضت المجتمعات المفتوحة بوجه خاص لهجمات سيبرانية وحملات تضليل.

ثانيا، نشهد استخدام الإرهابيين المتطور للفضاء الإلكتروني في جميع أنحاء العالم لتوسيع نطاق دعوتهم، ونشر الدعاية الخبيثة، والتحريض على الكراهية والعنف، وتجنيد الشباب وجمع الأموال. كما استخدم الإرهابيون وسائل التواصل الاجتماعي للتخطيط لهجماتهم الإرهابية وتنفيذها وإلحاق الدمار. والهند، بوصفها ضحية للإرهاب، تؤكد دائما على ضرورة أن تتصدى الدول الأعضاء للآثار المترتبة على الاستغلال الإرهابي لمجال الفضاء الإلكتروني وأن تواجهها على نحو أكثر استراتيجية.

ثالثا، تتعرض سلامة وأمن منتجات تكنولوجيا المعلومات والاتصالات، التي تشكل اللبنات الأساسية للفضاء الإلكتروني، للخطر. وثمة شواغل واسعة النطاق إزاء قيام جهات من الدول ومن غير الدول بتعريض شبكات ومنتجات تكنولوجيا المعلومات والاتصالات لمواطن الضعف وإقحام وظائف خفية ضارة عليها، بطرق من بينها استخدام قنوات مستترة. وهذه الأعمال الشائنة تقوض الثقة في سلسلة الإمداد

العالمية بتكنولوجيا المعلومات والاتصالات، وتضر بالأمن، ويمكن أن تصبح بقعة ساخنة بين الدول. ومن مصلحة المجتمع الدولي أن يكفل التزام جميع الجهات الفاعلة بالتزاماتها وتعهداتها الدولية وعدم الانغماس في ممارسات يمكن أن تكون لها آثار مدمرة على سلاسل التوريد العالمية وعلى التجارة في منتجات تكنولوجيا المعلومات والاتصالات.

ويتطلب الترابط داخل مجال الفضاء الإلكتروني عدم إيجاد حلول للمشاكل والأخطار المعقدة الناشئة عن الفضاء الإلكتروني بمعزل عن غيرها. ونحن، كدول أعضاء، نحتاج إلى اعتماد نهج تعاوني قائم على القواعد في الفضاء الإلكتروني والعمل على ضمان انفتاحه واستقراره وأمنه. وينبغي الاستفادة من الزخم الذي تولد عن النتائج الإيجابية التي توصل إليها فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي والفريق العامل المفتوح العضوية المعني بالتطورات في مجال تكنولوجيا المعلومات والاتصالات لإيجاد مزيد من الأرضية المشتركة وتحسين المعايير والقواعد السيبرانية المتفق عليها بالفعل. ويجب أن تسعى هذه القواعد إلى ضمان الأمن الجماعي للفضاء الإلكتروني من خلال التعاون الدولي. ومن شأن مشاركة الجهات صاحبة المصلحة المتعددة أن تؤدي دورا أساسيا في تحقيق هذا الهدف.

وينبغي أن يشكل تعزيز إمكانية الوصول إلى الفضاء الإلكتروني والاستفادة منه على قدم المساواة عنصرا هاما من عناصر هذا التعاون الدولي. ويؤدي اتساع "الفجوات الرقمية" و "فجوات المعرفة الرقمية" الآخذة في الاتساع بين البلدان إلى خلق بيئة غير مستدامة في مجال الفضاء الإلكتروني. وأدى الاعتماد الرقمي المتزايد في عصر ما بعد مرض فيروس كورونا (كوفيد) إلى تفاقم المخاطر وكشف هذه التصدعات التي تجسدها أوجه انعدام المساواة الرقمية. ويجب سد هذه الفجوات من خلال بناء القدرات. فالفضاء الإلكتروني المترامي الأطراف والذي لا يعرف الحدود بحكم طبيعته لا يعني سوى أن قوتنا لا تتجاوز قوة أضعف حلقة في الشبكة العالمية. ولن نتمكن من تحقيق هدف تهيئة فضاء إلكتروني قادر على الصمود وآمن على الصعيد العالمي إلا بالعمل سوياً، ويجب أن نضمن عدم تخلف أي بلد عن الركب في هذا المسعى الجماعي.

والهند ملتزمة بتهيئة بيئة حاضنة لفضاء إلكتروني مفتوح وآمن وحر وميسر ومستقر، من شأنها أن تصبح محركا للابتكار والنمو الاقتصادي والتنمية المستدامة، وأن تضمن التدفق الحر للمعلومات وتحترم التنوع الثقافي واللغوي. ومن خلال مبادراتنا التكنولوجية التحويلية التي أطلقت في السنوات الأخيرة مثل IndiaStack و Aadhar و UPI، نجحنا في الاستفادة من الإمكانات الهائلة للتكنولوجيات السيبرانية في تنفيذ خطة التنمية المستدامة لعام 2030 وتحسين الحوكمة. وكجزء من حملة التطعيم ضد كوفيد-19 التي أطلقتها الهند، التي تشكل واحدة من أكبر حملات التطعيم ضد كوفيد-19 على مستوى العالم، طورت الهند منصة Co-WIN وهي عبارة عن منصة تكنولوجية قابلة للتطوير وشاملة ومفتوحة. ويمكن تعديل منصة Co-WIN وتوسيع نطاقها لأغراض التدخلات الصحية في جميع أنحاء العالم. ونحن نعمل على تقاسم هذه المنصة مع البلدان الشريكة.

وهدفنا الرئيسي هو تسخير الفضاء الإلكتروني من أجل نماء الأفراد وتمكينهم، لا من أجل بلدنا فقط، ولكن من أجل البشرية جمعاء. والهند على استعداد للمساهمة بما لديها من دراية فنية وتقاسم خبراتها في هذا المسعى.

المرفق التاسع

بيان وزيرة الدولة المسؤولة عن الشؤون الخارجية والتجارة الخارجية لسانت فنسنت وجزر غرينادين، كيسال م. بيترز

نود أن نعرب عن تقديرنا للرئاسة الإستونية لمبادرتها بعقد مناقشة اليوم المفتوحة الرفيعة المستوى بشأن موضوع بالغ الأهمية، لتقييم أداء مجلس الأمن فيما يتعلق بمهمته المتمثلة في صون السلام والأمن الدوليين. وأعرب كذلك عن خالص تقديري لجميع مقدمي الإحاطات اليوم لما أدلوا به من بيانات تحمل رؤى ثاقبة.

يكاد الفضاء الإلكتروني في عالمنا المعاصر أن يمس جميع جوانب حياتنا اليومية. لقد بات دور تكنولوجيا المعلومات والاتصالات في تهيئة الحصول على المنافع الاقتصادية والاجتماعية واضحا. ومع ذلك، وعلى الرغم من هذه الفوائد، يجب أن يظل العالم مدركا للمشاكل الخطيرة القائمة في مجال تكنولوجيا المعلومات والاتصالات. فالبيئة العالمية لتكنولوجيا المعلومات والاتصالات تواجه زيادة هائلة في الاستخدام الخبيث لتكنولوجيا المعلومات والاتصالات من جانب الجهات من الدول ومن غير الدول. ومن المؤكد أن إساءة استخدام تكنولوجيا المعلومات والاتصالات تشكل خطرا على جميع الدول ويمكن أن تؤثر سلبا على السلام والأمن الدوليين. ولذلك، من الضروري أن ننطلق في رحلة البناء من التزام سابق باستحداث تدابير لبناء الثقة تعزز السلام والأمن الدوليين وتزيد من التعاون والشفافية والقدرة على التنبؤ والاستقرار فيما بين الدول الأعضاء في هذا الميدان.

إن 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. وبالإضافة إلى ذلك، فإن الجهات الفاعلة الأخرى ذات القدرات المتباينة وكذلك القدرات التي تتفاوت عبر مختلف القطاعات على جميع مستويات السلسلة العالمية لتكنولوجيا المعلومات والاتصالات لها دور رئيسي في ضمان الأمن السيبراني. ويجب أن نستكشف إمكانيات زيادة بناء القدرات وموارد المساعدة التقنية. وتحتاج الأمم المتحدة إلى تعزيز المساعدة المقدمة إلى الدول الأعضاء وزيادة المساعدة على كفالة اتساق الجهود بين مجموعة كيانات الأمم المتحدة المشاركة في أنشطة الفضاء السيبراني. وينبغي ربط هذه الجهود بأهداف المنظمة الأوسع نطاقا.

وعلى الرغم من التحديات العديدة التي تواجهنا كدولة جزرية صغيرة نامية، اتخذت سانت فنسنت وجزر غرينادين خطوات ملموسة لتحسين قدرتها على التصدي لآفة الجرائم السيبرانية. وهناك قانونان يقوم عليهما إطار تشريعي أساسي للأمن السيبراني في البلد، هما قانون الأدلة السيبرانية (2004) وقانون المعاملات السيبرانية (2007). وفي آب/أغسطس 2016، أقر المشرعون مشروع قانون الجرائم السيبرانية لعام 2016 ليصبح قانونا، فوفروا بذلك للبلد قانونا موضوعيا وإجرائيا ليتمكن من التعامل مع الجرائم السيبرانية بشكل أكثر فعالية. كما أننا ملتزمون باتفاقات الأمن السيبراني الإقليمية التي أبرمناها في إطار منظمة الدول الأمريكية والجماعة الكاريبية.

وبسبب جائحة مرض فيروس كورونا (كوفيد-19) وزيادة التعطيلات الناجمة عن الثوران البركاني الذي دهمنا مؤخرا، تحولت المدارس داخل بلدنا إلى التعليم عن بعد، كما هو الحال في جميع أنحاء العالم. ومع تلقي آلاف الأطفال حواسيب لوحية من الحكومة لتسهيل هذا الانتقال، ازداد حجم

استخدام الإنترنت والوقت المنفق أمام الشاشة. وبالنظر إلى ذلك، شرعت وزارة التعليم والمصالحة الوطنية في إطلاق حملة #GoCyberSmart لتعزيز الأمان السيبراني. والحملة هي مبادرة لبناء الوعي تهدف إلى تمكين الطلاب من اتخاذ القرارات الرقمية الصحيحة. ومجالات التركيز الثلاثة هي أمن المعلومات وسلامة الأجهزة والتنقل بأمان عبر الإنترنت.

ويكتسي تبادل المعلومات بين الدول الأعضاء والمنظمات الإقليمية والدولية أهمية بالغة لضمان الاستقرار ومنع تصاعد الحوادث المتعلقة بالأمن السيبراني. وعلاوة على ذلك، ندعو الدول الأعضاء إلى مواصلة الالتزام بالقانون الدولي وإطار سلوك الدول المسؤول في الفضاء الإلكتروني.

وفي إطار جهودنا الرامية إلى تعزيز سلوك الدول المسؤول في الفضاء الإلكتروني في سياق السلام والأمن الدوليين، يجب أن نسترشد بالتقييمات والتوصيات الواردة في تقارير فريق الخبراء الحكوميين الصادرة بتوافق الآراء في الأعوام 2010 و 2013 و 2015 وآخرها في عام 2021، فضلا عن الاستنتاجات والتوصيات الواردة في التقرير النهائي للفريق العامل المفتوح العضوية التابع للأمم المتحدة.

وفي الختام، فإن عدم الاتفاق على قواعد الاشتباك، ومعايير السياسات، وآليات التعاون الدولي لتهيئة بيئة سلمية لتكنولوجيا المعلومات والاتصالات لن يؤدي إلا إلى إيجاد مصادر جديدة لعدم الاستقرار والنزاع. وعلى صعيد الفضاء السيبراني، نشجع جميع الجهات الفاعلة في المجتمع الدولي على الامتثال لالتزاماتها القانونية الدولية، بما في ذلك احترام السيادة والاستقلال السياسي على النحو المنصوص عليه في ميثاق الأمم المتحدة، ومبادئ التسوية السلمية للمنازعات بنفس الأسلوب المتبع في العالم المادي. ويجب ألا تتوقف أبدا الحملة العاجلة للحفاظ على السلام والأمن الدوليين في الفضاء الإلكتروني.

المرفق العاشر

بيان نائب وزير خارجية النرويج، آودون هالفورسن

إن وجود فضاء إلكتروني متاح للجميع وحر ومفتوح وآمن أمر ضروري للحفاظ على السلام والأمن الدوليين. ونرحب بما قامت به إستونيا من لفت انتباه مجلس الأمن إلى هذا الموضوع – فهو الهيئة الرئيسية في الأمم المتحدة المسؤولة عن صون السلام والأمن الدوليين، وفقا لميثاق الأمم المتحدة.

وتشكل تكنولوجيات المعلومات والاتصالات جزءا أساسيا من البنية التحتية العالمية. فهي في صميم التنمية والاستقرار والأمن لجميع الدول. ومع ذلك، فإن الفضاء الإلكتروني يتحول بصورة مطردة أيضا إلى ساحة للتنافس والنزاع المحتمل بين الدول.

لقد شهدنا على مدى العقد الماضي كيف أن العمليات السيبرانية الخبيثة، من جانب الدول والجهات الفاعلة من غير الدول على حد سواء، قد زادت من حيث النطاق والحجم والشدة والتعقد. وإننا نجد أنفسنا في خضم جائحة عالمية لم تسلم فيها حتى البنية التحتية الصحية الحيوية من استهداف هذا النشاط الخبيث – مما يعرض سلامة المواطنين وجهودنا العالمية الرامية إلى إدارة أزمة كوفيد-19 للخطر.

ومع ذلك، هناك أيضا ما يدعو إلى التفاؤل. فقد برهنت أحداث العام الماضي على استعداد المجتمع الدولي للارتقاء إلى مستوى الحدث والعمل معا على تعزيز سلوك الدول المسؤول في الفضاء الإلكتروني. وتبين التقارير الصادرة بتوافق الآراء عن الفريق العامل المفتوح العضوية والفريق الحكومي للخبراء (فريق الخبراء الحكوميين) التزام جميع الدول الأعضاء بالتمسك بالنظام الدولي القائم على القواعد في الفضاء الإلكتروني. وهذا يمثل انتصارا للتعددية.

ويشكل تأكيد انطباق القانون الدولي على الفضاء الإلكتروني حجر الزاوية في تقريري كل من فريق الخبراء الحكوميين والفريق العامل المفتوح العضوية الصادرين بتوافق الآراء. فالقانون الدولي هو أساس التزام الدول المشترك بمنع نشوب النزاعات وصون السلام والأمن الدوليين. وهو ركيزة أساسية لتعزيز الثقة بين الدول. ويؤكد التقريران من جديد أن القانون الدولي، ولا سيما ميثاق الأمم المتحدة، ينطبق في سياق صون السلام والاستقرار ولا غنى عنه من أجل المحافظة عليهما، وتعزيز بيئة لتكنولوجيا المعلومات والاتصالات مفتوحة وآمنة ومستقرة وميسرة وسلمية.

ونرى أن إقرار فريق الخبراء الحكوميين بأن القانون الدولي الإنساني ينطبق في جميع النزاعات المسلحة، وفي سياق سيبراني أيضا، يشكل خطوة كبيرة إلى الأمام.

ويهدف القانون الدولي الإنساني إلى تقليل المعاناة الإنسانية الناجمة عن النزاع المسلح إلى أدنى حد. فهو ينظم العمليات السيبرانية ويقيدها أثناء النزاعات المسلحة، مثلما هو الحال تماما في تنظيمه وتقييده لأي وسائل وأساليب أخرى للحرب. وبالتالي، يحظر شن هجمات على المدنيين أو الأعيان المدنية، ويجب حماية الخدمات الطبية واحترامها. وبالتالي، تحظر مهاجمة البنى التحتية الوطنية الحيوية، مثل منشآت الإمداد بالطاقة، وإنتاج الأغذية، ومياه الشرب، أو غيرها من الأعيان التي لا غنى عنها لبقاء السكان.

إن الاعتراف بانطباق القانون الدولي الإنساني في الفضاء الإلكتروني لا يضفي الشرعية على الحرب السيبرانية. ويظل أي استخدام للقوة من جانب الدول محكوما بميثاق الأمم المتحدة وبالقواعد

ذات الصلة من القانون الدولي العرفي. ويجب تسوية المنازعات الدولية بالوسائل السلمية، في الفضاء الإلكتروني كما هو الحال في جميع المجالات الأخرى.

السيدة الرئيسة،

لقد أيد جميع الدول الأعضاء إطارا لسلوك الدول المسؤول في الفضاء الإلكتروني. وهو إطار يقوم على ما يلي: انطباق القانون الدولي، والالتزام بالمعايير الطوعية المتفق عليها، والتدابير العملية لبناء الثقة، وجهود بناء القدرات لتعزيز قدرة الجميع على الصمود وأمنهم. وذلك إنجاز كبير؛ ولكن قيمته لا يمكن تحقيقها إلا من خلال التنفيذ والامتثال من جانب جميع الدول.

وتشكل جلسة اليوم اعترافا بأن الأنشطة الخبيثة في الفضاء الإلكتروني يمكن أن تؤثر تأثيرا شديدا على السلام والأمن الدوليين. وتحمل جلسة اليوم أيضا إشارة واضحة لجميع الدول بأنه يتوقع منا أن نلتزم بإطار سلوك الدول المسؤول في الفضاء الإلكتروني الذي اتفقنا عليه: وأنه يجب علينا أن نتقيد بالتزاماتنا بموجب القانون الدولي وأن نلتزم بالمعايير التي اتفقنا عليها.

المرفق الحادي عشر

بيان وزير الدولة لشؤون جنوب آسيا والكومنولث في المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية، اللورد أحمد، لورد ويمبلدون

يكاد أن يكون لكل شيء بعد رقمي في عالم اليوم.

ويتعين على المجتمع الدولي أن يغتنم الفرص الهائلة التي تتيحها شبكة الإنترنت للتعلم، وإقامة الأعمال التجارية، والتواصل، بل والترفيه.

ولكننا نحتاج أيضا إلى التعامل مع التهديدات التي تقترن بهذه الفرص، بالجدية التي تليق بها.

وقد أصبحت الأخطار التي تشكلها الأنشطة الخبيثة والخطيرة التي تجري في الفضاء الإلكتروني الآن أكثر وضوحا من أي وقت مضى.

والواقع أن عصابة إجرامية استهدفت الشهر الماضي فقط شركة Colonial Pipeline، وجعلت أكبر خط أنابيب للوقود في أميركا مرهونا بدفع فدية، وهددت بإحداث إرباك اقتصادي شديد.

ويهدف بعض هذه الأنشطة إلى السرقة أو الابتزاز. ويهدف في كثير من الأحيان إلى مجرد التخريب والتعطيل.

بيد أننا كمجتمع دولي تقع على عاتقنا مسؤولية جماعية عن تهيئة فضاء إلكتروني يعود بالفائدة على جميع البلدان، بل وعلى جميع الناس. وينبغي لنا معا أن نصوغ القواعد التي تخدم الصالح العام.

ونحن بالطبع لا نبدأ من الصفر في هذا الصدد.

فقبل عشر سنوات جمعت المملكة المتحدة أكثر من 60 بلدا في لندن لوضع مبادئ أساسية من قبيل تعميم الوصول إلى خدمات الإنترنت، وحماية حقوق الأفراد عبر الإنترنت.

لقد قطعنا شوطاً طويلاً بعد مرور عشر سنوات منذ ذلك الحين.

وفي هذا العام فقط، أعادت الجمعية العامة بالإجماع التأكيد على تطبيق القانون الدولي في الفضاء الإلكتروني ووافقت على مجموعة من المبادئ الطوعية، بما في ذلك أهمية حماية البنية التحتية الصحية.

وقد قطع فريق من الخبراء الحكوميين شوطاً إلى الأمام في فهمنا لمعايير الفضاء الإلكتروني وقواعده ومبادئه، وبلور تفسيرات واضحة لكيفية انطباق القانون الدولي.

غير أننا بحاجة إلى أن نذهب إلى أبعد من ذلك. فليس سرا أن الدول تطور عمليات سيبرانية لدعم قدراتها العسكرية وقدراتها الأمنية الوطنية. والمملكة المتحدة هي في الواقع واحدة منها.

واسمحوا لي أن أكون واضحا: إننا سنستخدم هذه القدرات للدفاع عن أنفسنا ضد أولئك الذين يسعون إلى إلحاق الأذى بنا. ونحن ملتزمون باستخدام هذه القدرات عند الضرورة، بطريقة متناسبة، وتمشيا مع القانون الدولي.

والتحدي الجماعي الذي نواجهه هنا هو توضيح كيفية انطباق قواعد القانون الدولي على أنشطة الدول في الفضاء الإلكتروني، والاحتراز من الجهات الفاعلة الخبيثة التي تتحايل على هذه القواعد، وإذاقة أولئك الذين يقومون بأنشطة خبيثة في الفضاء الإلكتروني وبال أمرهم.

والمملكة المتحدة ملتزمة بالعمل مع جميع البلدان ومع جميع الجهات صاحبة المصلحة المتعددة فيها لكفالة خضوع الفضاء الإلكتروني لقواعد ومعايير تعزز أمننا الجماعي.

ويجب أن تعزز هذه القواعد والمعايير القيم الديمقراطية وأن تدعم النمو الاقتصادي العالمي، وأن تتصدى لانتشار السلطوية الرقمية.

ويجب أن نتمسك بسيادة القانون في الفضاء الإلكتروني من خلال ما يلي: تجسيد سلوك الدول المسؤول، وتحفيز الامتثال، وردع الهجمات، بل ومحاسبة الآخرين على سلوك الدول غير المسؤول.

ويجب علينا أيضا أن نعطي الأولوية المطلقة لحقوق الإنسان وأن نضمن حمايتها على الإنترنت، على غرار ما نكفله لها من حماية خارج عالم الإنترنت، لضمان بناء فضاء إلكتروني حر ومفتوح وسلمي وآمن، ومتاح للجميع.

ويشكل إطار الأمم المتحدة لسلوك الدول المسؤول في الفضاء الإلكتروني نقطة انطلاقنا. ويجب أن ندعم جميع الدول في تنفيذه الآن.

وقد سر المملكة المتحدة أن تعلن الشهر الماضي أننا سنستثمر أكثر من 30 مليون دولار لدعم بناء القدرات المرتبط بالفضاء الإلكتروني في البلدان الضعيفة – وخاصة في جميع أنحاء أفريقيا ومنطقة المحيطين الهندي والهادي.

وسيساعد عملنا مع المنظمة الدولية للشرطة الجنائية (الإنتربول) البلدان، بما في ذلك إثيوبيا، ورواندا، وغانا، وكينيا، ونيجيريا، على دعم العمليات المشتركة ضد مجرمي الفضاء الإلكتروني.

وسيساعد التمويل البريطاني في أماكن أخرى على بناء أفرقة وطنية للاستجابة لحالات الطوارئ لحماية البلدان من هذه الأخطار.

ولا يمكننا بالطبع أن نفعل شيئا من هذا دون شركائنا في القطاع الخاص، وبالطبع في الدوائر الأكاديمية والمجتمع المدني.

ولكن لمجلس الأمن أيضا دور محوري وهام في كل هذا عليه أن يؤديه بينما نجتمع هنا معا اليوم.

فحيثما شكلت الأنشطة الخبيثة تهديدا للسلام والأمن الدوليين – من خلال تسببها في تفاقم النزاع أو إحداث معاناة إنسانية – يجب أن يكون مجلس الأمن مستعدا للاستجابة.

وينبغي للمجلس أن يتصدى لهذه التهديدات مثلما هو الحال تماما في تصديه للتهديدات التي تشكلها الوسائل التقليدية.

ولدينا فرصة لاغتنام الفرص التي يتيحها الفضاء الإلكتروني وضمان بقائه قوة للازدهار والتقدم للجميع.

ولتحقيق ذلك، من المهم للغاية أن نعمل معا لمواجهة أولئك الذين يخاطرون بأمننا الجماعي.

واسمحوا لي أن أؤكد لكم ذلك: إن المملكة المتحدة ملتزمة التزاما كاملا بحماية فضاء إلكتروني حر ومفتوح وسلمي وآمن للأجيال القادمة.

المرفق الثاني عشر

بيان الوزير المنتدب لدى وزير شؤون أوروبا والشؤون الخارجية في فرنسا، فرانك ريستر

[الأصل: بالفرنسية]

أود أن أشكر رئيسة وزراء إستونيا على هذا الحدث. إن مجلس الأمن يشرف على صون السلام والأمن الدوليين وينبغي أن يكون قادرا على القيام بذلك في الفضاء الإلكتروني.

فالفضاء الإلكتروني هو حيز للفرص ولكنه أيضا مصدر لأخطار جديدة. فقد أصبح منطقة للتنافس الاستراتيجي بين القوى. والاستخدامات الخبيثة لتكنولوجيا المعلومات والاتصالات من جانب الجهات من الدول وغير الدول على السواء آخذة في الانتشار.

وعلى مدى الأشهر القليلة الماضية، ولا سيما في سياق جائحة مرض فيروس كورونا (كوفيد-19)، لاحظنا زيادة اعتمادنا على هذه التكنولوجيات. وأعني أولا وقبل كل شيء الهجمات السيبرانية الشنيعة باستخدام فيروسات الفدية التي شنت ضد المستشفيات وغيرها من البنى التحتية الحيوية. وأود أن أعرب عن تضامن فرنسا الكامل مع ضحايا تلك الهجمات. وتجول بخاطري أيضا الحملات الرامية إلى التلاعب بالمعلومات من خلال نشر "الوباء المعلوماتي" أو التجزئة المتزايدة للإنترنت، وهي ممارسات تتعارض مع القيم الديمقراطية. إن الإجراءات التي تجري في الفضاء الإلكتروني لها عواقب حقيقية جدا يمكن أن تكون وخيمة في حياتنا ومجتمعاتنا.

ويتمثل التحدي الذي سنواجهه خلال القرن القادم في بناء حوكمة وتنظيم جماعيين للفضاء الإلكتروني. إننا لا نريد "عالما موحشا من الفوضى الرقمية"، ولا فضاء إلكترونيا معزولاً. وقد أكدنا ذلك في نداء باريس من أجل الثقة والأمن في الفضاء الإلكتروني، وكذلك من خلال إطار مجموعة السبعة في إعلان دينارد بشأن مبادرة معايير الفضاء الإلكتروني. إن فرنسا مصممة على أن تبني مع شركائها فضاء إلكترونيا مفتوحا وآمنا ومستقرا وسلميا وغير مجزأ وميسرا.

وينطبق القانون الدولي، بما في ذلك ميثاق الأمم المتحدة، انطباقا كاملا على الفضاء الإلكتروني. وهذا يعني أيضا تقيد العمليات السيبرانية التي تجري أثناء النزاع المسلح بالقانون الدولي الإنساني.

وفي مواجهة تزايد عدد التهديدات في الفضاء الإلكتروني والهجمات السيبرانية، ينبغي للحكومات أن تتصدى لها من خلال التعاون والقانون. لقد اضطلعت فرنسا، على مدى أكثر من عقد من الزمن، بدور رائد في مختلف الجهود المتعددة الأطراف. وأدت هذه الجهود إلى انبثاق إطار لسلوك الدول المسؤول تتقيد به هذه الدول في استخدامها لتكنولوجيا المعلومات والاتصالات. ويستند هذا الإطار إلى القانون الدولي، وإلى مجموعة متسقة من معايير السلوك غير الملزمة، وإلى تدابير الشفافية والثقة. وقد أتاح إحراز تقدم في التعاون والتفاهم المتبادلين بين الدول في الفضاء الإلكتروني. وأود أن أشيد بالنجاح الذي حققه مؤخرا الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي وفريق الخبراء الحكوميين السادس المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي اللذين اعتمدا تقريرين متوازنين ومفيدين بتوافق الآراء. وفرنسا مستعدة لمواصلة المشاركة البناءة في المناقشات المتعددة الأطراف داخل الأمم المتحدة، بما في ذلك في سياق الفريق العامل الجديد المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها، الذي أنشئ بموجب قرار الجمعية العامة 240/75.

وفي المستقبل، يجب أن توضع القواعد والمبادئ المتفق عليها موضع التنفيذ على نحو فعال قبل كل شيء. وتقترح فرنسا، مع 52 شريكا، أن تنشئ الأمم المتحدة برنامج عمل بشأن الأمن السيبراني. وستسمح هذه الأداة الجديدة، التي تكمل الفريق العامل المفتوح العضوية الجديد، بإنشاء هيكل دائم. وسيكون الغرض منها دعم بناء القدرات وتهيئة مساحات للحوار مع المجتمع المدني والباحثين والجهات الفاعلة الخاصة. وفرنسا منفتحة على الحوار مع جميع الدول وأصحاب المصلحة المهتمين بتنقيح هذا الاقتراح العملي المنحى والانطلاق منه.

وهذا الالتزام الجماعي من جانب جهات فاعلة متعددة أمر ضروري. فلا شك أن الدول تتحمل في الفضاء الإلكتروني مسؤوليات لا يمكن أن تقدم جهات فاعلة أخرى على الاضطلاع بها، بيد أن الدول لا تستطيع أن تتصرف بمفردها. لذا وجب أن نطبق هذا الشكل الجديد من أشكال الدبلوماسية تطبيقا تاماً.

المرفق الثالث عشر

بيان الممثل الدائم للصين لدى الأمم المتحدة، دجانغ جون

[الأصل: بالصينية]

في عالم اليوم، تبدأ حاليا دورة جديدة من الثورة التكنولوجية والتحول الصناعي، وتتطور التكنولوجيات الرقمية والسيبرانية بسرعة، فتُغيِّر إلى حد كبير أساليب إنتاج البشرية وطرق حياتها، وتحفز التنمية الاقتصادية والاجتماعية لجميع البلدان. وفي الوقت نفسه، أصبحت المراقبة والهجمات والجرائم والعمليات الإرهابية السيبرانية مخاطر عامة عالمية، واصطبغ الفضاء الإلكتروني على نحو متزايد بصبغة عسكرية وسياسية وغير آمنة وأيديولوجية. وفي العالم السيبراني، لا تتمتع البلدان بالفرص والمصالح المشتركة فحسب، وإنما تواجه أيضا تحديات مشتركة وتتحمل مسؤوليات مشتركة. وأصبحت تشكل على نحو متزايد مجتمعا له مستقبل مشترك في السراء والضراء.

وقد صرح الرئيس الصيني شي جينبينغ بأن البلدان تشترك في نفس الرغبة في الارتقاء بالاقتصاد الرقمي، ونفس الاهتمام بالتصدي لتحديات الأمن السيبراني، ونفس الحاجة إلى تعزيز حوكمة الفضاء الإلكتروني، وذلك على الرغم من اختلاف ظروفها والمراحل التي قطعتها على المستوى الوطني لتطوير الإنترنت، وعلى الرغم مما تواجهه من تحديات مختلفة على أرض الواقع. وما فتئت الصين تدعو المجتمع الدولي دائما إلى تضافر جهوده في العمل معا من أجل حماية الأمن السيبراني والحفاظ على السلام الدولي.

- فينبغي لنا أن نعزز الأمن من خلال الحفاظ على السلام والحيلولة دون أن يصبح الفضاء الإلكتروني ساحة معركة جديدة. وينبغي للمجتمع الدولي أن يلتزم بمقاصد ميثاق الأمم المتحدة ومبادئها، ولا سيما مبادئ المساواة في السيادة، وحظر استخدام القوة، وعدم التدخل في الشؤون الداخلية، وتسوية المنازعات بالوسائل السلمية. ومن الضروري احترام حق كل بلد في اختيار مسار تطوير شبكته ونموذج إدارتها بصورة مستقلة، والمشاركة في إدارة الفضاء الإلكتروني على قدم المساواة. وينبغي للبلدان أن تمتنع عن القيام بأنشطة سيبرانية تعرض أمن البلدان الأخرى للخطر. وينبغي توخي الحذر في تطبيق قانون النزاعات المسلحة على الفضاء الإلكتروني، ومنع سباقات التسلح في الفضاء الإلكتروني.

- وينبغي لنا أن نعزز الأمن من خلال التبادلات والتعاون وأن نهيئ بيئة مؤاتية للفضاء الإلكتروني. فحماية الأمن السيبراني قضية عالمية، ولا يمكن لأي بلد أن ينأى بنفسه عنها أو أن يتعامل معها بمفرده. والهيمنة والنزعة الانفرادية والحمائية في الفضاء الإلكتروني لن تؤدي إلا إلى تكثيف المواجهات وتسميم مناخ التعاون، وينبغي أن يرفضها ويعارضها المجتمع الدولي بصورة جماعية. وينبغي للبلدان أن تعمل معا لتوسيع نطاق التبادلات والتعاون فيما يتعلق بالبحث والتطوير في مجال التكنولوجيا، ووضع القواعد، وتبادل المعلومات، وينبغي أن تحد بصورة مشتركة من إساءة استخدام تكنولوجيا المعلومات. وينبغي لنا أن نعارض بصورة مشتركة المراقبة والهجمات السيبرانية، ومكافحة الإرهاب السيبراني والجرائم السيبرانية، وتعزيز قدرات حماية الأمن السيبراني. ومن الضروري أن نوفر للشركات بيئة أعمال مفتوحة وعادلة وغير تمييزية، وضمان انفتاح سلاسل التوريد العالمية لقطاع تكنولوجيا المعلومات واستقرارها وأمنها، وتعزيز التنمية الصحية للاقتصاد العالمي، ومعارضة التدخل البشري في العمليات التجارية العادية للشركات، مهما كانت الذرائع.

- وينبغي لنا أن نعزز الأمن من خلال تعزيز الحوكمة والنهوض بالإنصاف والعدالة في الفضاء الإلكتروني. وينبغي لجميع البلدان أن تتمسك بالتعددية الفعالة، وأن تنشئ عملية حوكمة مفتوحة وشاملة للجميع ومستدامة لإدارة الأمن السيبراني في إطار الأمم المتحدة وبمشاركة الجميع بالتساوي، وأن تضع قواعد دولية للفضاء الإلكتروني تقبلها جميع البلدان عموما، وأن تعارض السياسة التي تقوم على التكتلات والمجموعات. وتشيد الصين بشدة بنجاح فريق الأمم المتحدة العامل المفتوح العضوية وفريق الخبراء الحكوميين في إنجاز التقارير عن الأمن السيبراني، وتتطلع إلى مساهمات الفريق العامل المفتوح العضوية الجديد في الحفاظ على الأمن السيبراني. ونحن على استعداد للعمل مع جميع الأطراف لتعزيز وضع اتفاقية دولية لمكافحة الجريمة السيبرانية في إطار الأمم المتحدة. وينبغي أن تعطى الفرصة للجهات المتعددة صاحبة المصلحة مثل الحكومات وشركات الإنترنت والدوائر التكنولوجية والمجتمع المدني وفرادى المواطنين للقيام بدور على أساس المشاورات الواسعة النطاق والمساهمة المشتركة وتقاسم الفوائد.

- وينبغي لنا أن نعزز الأمن من خلال التنمية الشاملة للجميع وأن نحقق الرخاء المشترك في الفضاء الإلكتروني. فالتنمية الاقتصادية العالمية الراهنة متباطئة. ويمكن أن تصبح التكنولوجيا الرقمية والسيبرانية عوامل دفع هامة للبلدان لكي تتعافى وتستأنف التنمية الاقتصادية والاجتماعية عقب انتهاء هذه الجائحة. وينبغي للبلدان أن تعتمد سياسات أكثر استباقية وكلية وتنسيقا وشمولا للجميع من أجل تعزيز التنمية المتوازنة لتكنولوجيات المعلومات والاتصالات على الصعيد العالمي، وأن تطور بقوة نماذج وأشكالا جديدة مثل الاقتصاد الرقمي، وأن تعارض محاولات السعي إلى الهيمنة العلمية والتكنولوجية. وينبغي لنا أن ننهض بتطوير البنية التحتية الرقمية والقدرة على الاتصال الإلكتروني، وأن نكسر الحواجز الإعلامية، وأن نسد الفجوات الرقمية، وأن نساعد البلدان النامية على رفع مستويات الرقمنة، والقدرة على الاتصال الإلكتروني، وتنمية المعارف، بغية تنفيذ خطة التنمية المستدامة لعام 2030. وينبغي لنا أن نكثف التعاون مع البلدان النامية ونساعدها في مجال الأمن السيبراني، وأن نحسن قدراتها على الإنذار المبكر والوقاية والاستجابة لحالات الطوارئ في حوادث الأمن السيبراني.

وتولي الصين أهمية قصوى للأمن السيبراني والحوسبة، وهي ملتزمة ببناء اقتصاد رقمي ومجتمع رقمي وحكومة رقمية، باستخدام التحول الرقمي الشامل لدفع التغييرات في أساليب الإنتاج وأساليب الحياة ونماذج الحوكمة. وستواصل الصين تحسين قوانينها ولوائحها ومعاييرها المؤسسية الوطنية المتعلقة بالأمن السيبراني بالاستناد إلى قانون الأمن السيبراني وقانون أمن البيانات.

وفي العام الماضي، طرحت الصين المبادرة العالمية لأمن البيانات، مع التركيز على قضايا مثل البنية التحتية الحيوية وحماية المعلومات الشخصية، وتخزين البيانات واسترجاعها للشركات في الخارج، وأمن سلاسل الإمداد، وتوفير حلول بنّاءة للحفاظ على البيانات العالمية والأمن السيبراني. وفي الآونة الأخيرة، أصدرت الصين، بالاشتراك مع جامعة الدول العربية، مبادرة التعاون بين الصين وجامعة الدول العربية بشأن أمن البيانات، والتي جسدت النداء المشترك بين الطرفين للحفاظ على الأمن السيبراني وأمن البيانات. وإننا نرحب باستجابات جميع الأطراف النشطة للمبادرة ومشاركتها فيها، وذلك من أجل الاشتراك في صياغة قواعد عالمية للإدارة الرقمية. وتسعى الصين أيضا حثيثا لبناء طريق الحرير الرقمي، والعمل مع بلدان أخرى لبناء نمط جديد من الترابط الذكي موجه نحو المستقبل.

فالفضاء الإلكتروني يجسد حلم الإنسانية الذي يشمل رفاه الناس وسلامهم وأمنهم. والصين على استعداد للعمل مع جميع البلدان لاغتنام الفرصة التي تتيحها ثورة المعلومات من أجل إحداث زخم جديد للابتكار والتنمية، وفتح مشهد جديد للتعاون الرقمي، وبلورة نمط جديد للأمن السيبراني، وبناء مجتمع له مستقبل مشترك في الفضاء الإلكتروني، والاشتراك في بناء مستقبل أفضل للبشرية.

المرفق الرابع عشر

بيان البعثة الدائمة للمكسيك لدى الأمم المتحدة

[الأصل: بالإسبانية]

ترحب المكسيك بعقد هذه المناقشة المفتوحة والإحاطة التي قدمتها وكيلة الأمين العام والممثلة السامية لشؤون نزع السلاح، إيزومي ناكاميتسو.

وكما استمعنا إلى ذلك في هذا المحفل وفي العديد من المحافل الأخرى، فإن الأهمية المتزايدة للفضاء الإلكتروني لا يمكن إنكارها. فالعالم أصبح يعتمد بصورة متزايدة على تكنولوجيا المعلومات والاتصالات، ولا سيما في سياق الجائحة. وسرعان ما دخلت العلاقات الدولية أيضا المجال الافتراضي، ولا يمكن لمجلس الأمن، ولا ينبغي له، أن يتجاهل آثارها على السلام والأمن الدوليين.

وعلى الرغم من أن ما يقرب من نصف سكان العالم لا تتاح لهم إمكانية الوصول إلى الإنترنت، فإن ذلك لا ينجيهم من الوقوع ضحايا لبعض آلاف الهجمات السيبرانية التي تحدث يوميا ضد الشبكات الحكومية والمؤسسات المصرفية والمالية ومؤسسات البحوث والصحة.

وقد دفعت هذه المخاطر المحتملة الهيئات المختلفة لمنظومة الأمم المتحدة إلى التصدي للتهديدات والسعي إلى إبرام اتفاقات بين الدول لضمان عدم استخدام الفضاء الإلكتروني لأغراض إجرامية وكيدية بل وحتى إرهابية، دون إغفال التوازن مع استخداماته السلمية والفرص الهائلة التي يوفرها للتنمية المستدامة.

وترى المكسيك أن من الضروري منع أي تصعيد للمخاطر في الفضاء الإلكتروني. وينبغي تنظيم استخدام الفضاء الإلكتروني، شأنه في ذلك شأن أي بيئة مادية أخرى، وفقا لمبادئ توجيهية ومعايير واضحة جدا، بينما من الضروري المساعدة على تعزيز إقامة فضاء إلكتروني مفتوح وحر وآمن ومستقر وميسَّر ومرن.

ولذلك تشيد المكسيك بالاختتام الناجح لأعمال فريق الخبراء الحكوميين والفريق العامل المفتوح العضوية التي أدت إلى اعتماد تقارير موضوعية بتوافق الآراء، تمثل سوابق أساسية للجهود المتعددة الأطراف. ومن وجهة نظر بلدي، تؤكد هذه الحقيقة من جديد الثقة المتجددة في تعددية الأطراف، والدور البنّاء الذي يمكن أن تؤديه الأمم المتحدة في تحقيق استجابات متكاملة ومشروعة وطويلة الأجل لتحديات الفضاء الإلكتروني وتكنولوجيا المعلومات والاتصالات.

غير أن ذلك ليس كافيا. وإنما يجب إحراز تقدم نحو التطبيق الكامل للقانون الدولي في الفضاء الإلكتروني، بما في ذلك ميثاق الأمم المتحدة، والقانون الدولي لحقوق الإنسان، والقانون الدولي الإنساني، وتطوير الفقه القانوني في تلك المجالات.

ونحن نؤمن إيمانا راسخا بتحقيق مزيد من الشفافية في أنشطة الفضاء الإلكتروني، والمساءلة، والدعوة التي اعتمدتها الجمعية العامة نفسها إلى وضع معايير لسلوك الدول المسؤول تستكمل باتخاذ التدابير الرامية إلى تعزيز التعاون الدولي من أجل بناء القدرات السيبرانية للدول وتعزيزها.

وتأمل المكسيك أن يُستمع في مداولات مجلس الأمن وأعماله في المستقبل إلى المزيد من أصوات المجتمع المدني والأوساط الأكاديمية والقطاع الخاص. فهذه الأطراف متمسكة بتحقيق هدف مشترك ألا وهو: ضمان الاستخدام السلمي للفضاء الإلكتروني ابتغاء تطوير التكنولوجيات الرقمية واستخدامها.

المرفق الخامس عشر

بيان الممثل الدائم للاتحاد الروسي لدى الأمم المتحدة، ف. أ. نيبنزيا

[الأصل: بالروسية]

مثلت السنة التي أعقبت تفشي جائحة مرض فيروس كورونا (كوفيد-19) محنة كبيرة للعالم بأسره، ستبقى في الذاكرة على أنها أساسا سنة تحديات وخسائر. وقد تأثرت جهود دبلوماسية كثيرة، وتوقفت المفاوضات على جبهات عديدة.

وتبرز في هذا الصدد المناقشات المتعددة الأطراف بشأن أمن المعلومات الدولي في الأمم المتحدة، لأنها لم تحافظ على الزخم فحسب وإنما حققت أيضا، دون مبالغة، نتائج تاريخية. وتسنى لكل من منتدبي خبراء الجمعية العامة للأمم المتحدة المعنيين – فريق الخبراء الحكوميين والفريق العامل المفتوح العضوية – اعتماد تقريريهما النهائيين بتوافق الآراء.

ولم تكن المفاوضات في هذين الفريقين سهلة، مما أكسب النتائج التي تم التوصل إليها بشق الأنفس قيمة أكبر. وقد أظهرت هذه النتائج بوضوح أن المجتمع الدولي قادر على الاتفاق على القضايا الرئيسية عندما يكون الحوار عمليا وغير مسيس وبنّاء. وبفضل هذه الجهود، ندخل الآن مرحلة جديدة هامة، بدأت في حزيران/يونيه 2021 مع عقد الدورة التنظيمية للفريق العامل المفتوح العضوية الجديد للفترة 2021-2025.

وتمثل هذه النتائج إنجازا مشتركا من إنجازات المجتمع الدولي. ونحن من جانبنا، ما فتئنا نسعى منذ عقود إلى الإسهام في إنشاء نظام عالمي لضمان أمن المعلومات على الصعيد الدولي. ففي عام 1998، أثار الاتحاد الروسي، لأول مرة في الأمم المتحدة، مسألة الحاجة إلى التصدي للتهديدات التي يتعرض لها أمن المعلومات على الصعيد الدولي واقترح على الجمعية العامة أن تتخذ قرارا بهذا الشأن. وفي أوائل القرن الحادي والعشرين، اقترحنا إنشاء فريق الخبراء الحكوميين ليكون بمثابة منتدى للخبراء تُناقش فيه مسألة أمن المعلومات على الصعيد الدولي. وفي عام 2019، عندما أصبح من الواضح أن هذا الموضوع قد تجاوز التركيز الضيق للفريق، لبينا نحن والوفود التي تتوافق آراؤها مع آرائنا احتياجات المجتمع الدولي بإطلاق عملية التفاوض المفتوح والديمقراطي حول أمن المعلومات على الصعيد الدولي بمشاركة جميع الدول الأعضاء بصيغة فريق عامل مفتوح العضوية.

فهذه المسألة تشكل معلما تاريخيا هاما للغاية. ولأول مرة، كانت المناقشات المتعلقة بالأمن الرقمي مفتوحة لغالبية الدول الأعضاء في الأمم المتحدة. ونحن نتمسك بمبدأ واضح جدا: إننا نؤمن بالحوار المتساوي الذي يقوم على الاحترام المتبادل. فإذا كنا جميعا متساوين في مواجهة التهديدات التي يتعرض لها أمن المعلومات على الصعيد الدولي، فينبغي ألا تُناقش هذه التهديدات دائرة ضيقة من الدول المتقدمة تكنولوجيا، بل جميع الدول الأعضاء في الأمم المتحدة. وينبغي للدول التي تعتبر نفسها أكثر "تقدما" ألا تفرض إرادتها.

ولم يكن المقترحان اللذان قدمناهما لإنشاء فريق الخبراء الحكوميين، ثم الفريق العامل المفتوح باب العضوية، يروقان للجميع في البداية. فعدة دول، بما فيها دول مشاركة في جلسة اليوم، صوتت ضد إنشائهما. بيد أنها، بدأت تدريجيا تلتحق بالمحادثات، وأصبحت في نهاية المطاف أطرافا مشاركة نشطة وبنّاءة.

وتقدم الدبلوماسية المتعددة الأطراف الفعالة في مجال أمن المعلومات على الصعيد الدولي في الأمم المتحدة، التي تكمل التعاون الثنائي بين الدول بشأن هذا الموضوع، مثالا ممتازا على كيفية معالجة هذه المسائل بغية التغلب على انعدام الثقة المتبادل وتبديد المخاوف. وهذا يتناقض مع "دبلوماسية المنابر" السيئة السمعة التي يلجأ إليها، للأسف، بعض أطرافنا الشريكة في بعض الأحيان.

وفي الوقت نفسه، نشهد للأسف اتجاها خطيرا يحاول فيه مجلس الأمن التابع للأمم المتحدة فرض تفسيرات أحادية الجانب للاتفاقات التي تم التوصل إليها في إطار فريق الخبراء الحكوميين والفريق العامل المفتوح العضوية، داعيا فعليا إلى دعم نتائج المناقشات التي دارت في هذين المنتديين اللذين عينتهما الجمعية العامة أو الأسوأ من ذلك مراجعة هذه النتائج. ونحن نعتبر هذه المحاولات هدامة. فهي تدفع المجتمع الدولي نحو مواجهات لا يمكن التنبؤ بها ومرفوضة.

ويسعى بعض البلدان على وجه التحديد، عن طريق تحريف الاتفاقات، بما في ذلك الاتفاقات المتعلقة بالجوانب القانونية الدولية لاستخدام تكنولوجيا المعلومات والاتصالات، إلى تبرير الضغط والجزاءات من جانب واحد ضد الدول الأعضاء الأخرى وإمكانية استخدام القوة ضدها. ومن دواعي القلق البالغ أن عدة دول متقدمة تكنولوجيا تسعى جاهدة إلى عسكرة الفضاء المعلوماتي عن طريق الدفع بمفهوم "الضربات السيبرانية العسكرية الوقائية"، بما في ذلك ضد الهياكل الأساسية الحيوية. وتتناقض هذه المذاهب الصدامية مع الالتزام الذي قطعته سابقا وتتعهد به اليوم أيضا، بمنع نشوب النزاعات الناشئة عن استخدام تكنولوجيا المعلومات والاتصالات. وهذا كمحاولة لاستخدام موقع قوتهم لفرض "قواعد اللعبة" الخاصة بهم في مجال المعلومات.

وأود أن أؤكد أن النقاش حول كيفية تطبيق القانون الدولي تطبيقا دقيقا لم ينته بعد على الرغم من أن المجال الرقمي لا يتسم بعدم التنظيم. وستناقش هذه المسائل لمدة خمس سنوات أخرى على الأقل في إطار المنتدى الذي عينته الجمعية العامة – أي الفريق العامل المفتوح العضوية الجديد.

وفي هذا الصدد، تمثل التقارير النهائية لفريق الخبراء الحكوميين والفريق العامل المفتوح العضوية مجموعة من الاتفاقات الدقيقة والمتوازنة، بما في ذلك بشأن ضرورة وضع معايير جديدة للسلوك المسؤول الذي يتعين أن تتوخاه الدول في مجال المعلومات، مع مراعاة خصائصها. وقد أُدرجت القائمة الأولية لهذه القواعد في القرار المتعلق بأمن المعلومات على الصعيد الدولي الذي اتخذته الجمعية العامة في عام 2018 بمبادرة من الاتحاد الروسي. ومن المؤسف أن زملاءنا الغربيين يحاولون الآن أن يختاروا من هذه القائمة الأحكام التي تعود عليهم بأكبر فائدة، بينما يجانبون الصواب في تفسير انطباق القانون الدولي في المجال الرقمي بالقول إنه "تلقائي"، مما يسمح باستخدام القوة فيه، وأن يقدموا وجهات نظرهم الوطنية كما لو كانت نتاج توافق عالمي في الآراء. ولذلك، فإننا سنعارض أي محاولات لتنقيح الاتفاقات المتوازنة التي تم التوصل إليها في إطار المنتديات التي عينتها الجمعية العامة، من خلال مجلس الأمن التابع للأمم المتحدة.

وكما ذكر رئيس الاتحاد الروسي، ف. ف. بوتين، في اجتماع مجلس الأمن التابع للاتحاد الروسي في 26 آذار/مارس 2021، فإن النهج المذهبية الروسية إزاء وضع نظام عالمي لضمان أمن المعلومات على الصعيد الدولي تظل مفتوحة وشفافة وغير متغيرة. وهي مكرسة في المبادئ الأساسية لسياسة الدولة بشأن أمن المعلومات الدولية التي وافق عليها الرئيس في نيسان/أبريل 2021. وهذه الوثيقة هي وثيقة عامة، وأشجع الجميع على الاطلاع عليها.

ويقوم مذهبنا على فرضية استخدام تكنولوجيا المعلومات والاتصالات للأغراض السلمية فقط، وضرورة منع نشوب النزاعات في الفضاء الإعلامي، وأهمية تعزيز التعاون المتعدد الأطراف والثنائي تحقيقا لتلك الغاية. ونعتقد أنه ينبغي إبرام اتفاقات قانونية دولية على الصعيد العالمي من أجل التصدي لتلك المهام بفعالية. ولتحقيق هذا الهدف، يجب بذل جهود مشتركة لوضع قواعد عالمية وعادلة وشاملة لسلوك الدول والاتفاق عليها في الفضاء الإعلامي تأخذ في الاعتبار الحقائق الراهنة؛ والتمييز بوضوح بين الأنشطة المسموح بها وغير المسموح بها في الفضاء الإعلامي؛ وجعل هذه القواعد ملزمة قانونا لضمان أن تحرص جميع الدول على التقيد بها بصرامة.

وفي الوقت نفسه، فإننا نتمسك بحرمة سيادة الدول في المجال الرقمي. والأمر متروك لكل بلد لتحديد معايير تنظيم مجال المعلومات الخاص به والهياكل الأساسية ذات الصلة.

ومن المهام التي لا تقل أهمية بناء نظام سلمي ومنصف وعادل لضمان أمن المعلومات على الصعيد الدولي يأخذ في الاعتبار مصالح جميع البلدان، بغض النظر عن إمكاناتها الرقمية. وينبغي دعم الجهود التي تقودها الأمم المتحدة لبناء هذه القدرات بهدف سد الفجوة الرقمية دعما قويا. ونحن نأمل أن الفريق العامل المفتوح العضوية الجديد، وفقا لولايته، سيتمكن من مواصلة دراسة هذه المسألة بالتفصيل وتقديم توصيات مفيدة.

وبالإضافة إلى ذلك، يجب أن نتصدى بصورة جماعية لاستخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية. ونهيب بالدول الأعضاء أن تسهم على نحو بنّاء في عمل اللجنة الخاصة المكلفة بإعداد مشروع اتفاقية بشأن هذه المسألة بحلول عام 2023.

وتظل الجمعية العامة المحفل الرئيسي لمناقشة أمن المعلومات على الصعيد الدولي. وفي هذا المحفل ستجري مناقشات الخبراء بشأن جميع جوانب هذا الموضوع على مدى السنوات الخمس القادمة. فنركز على دعم هذه العملية الفريدة. ويجب أن نحافظ على المناخ البناء للتعاون المتعدد الأطراف في مجال أمن المعلومات على الصعيد الدولي تحت رعاية الأمم المتحدة بصيغة الفريق العامل المفتوح باب العضوية، الذي أثبت حقا فعاليته وأهميته. وهذا من شأنه أن يتيح لهذا الفريق فرصة حقيقية لتحقيق نتائج ملموسة وعملية. ومن واجبنا الجماعي، كأعضاء في مجلس الأمن التابع للأمم المتحدة، أن نسهم إسهاما كاملا في هذا الجهد.

المرفق السادس عشر

بيان الممثل الدائم لتونس لدى الأمم المتحدة، طارق الأدب

أود، بادئ ذي بدء، أن أعرب عن تقديرنا للرئاسة الإستونية لتنظيمها هذا الاجتماع بشأن الأمن السيبراني وصون السلام والأمن الدوليين في الفضاء الإلكتروني.

وأود أن أتوجه بالشكر إلى وكيلة الأمين العام والممثلة السامية لشؤون نزع السلاح، السيدة ناكاميتسو، على إحاطتها الثرة بالمعلومات.

إن تونس تشعر بقلق بالغ إزاء الزيادة الكبيرة في السنوات الأخيرة في الأنشطة الكيدية في الفضاء الإلكتروني التي يمكن أن تشكل تهديدا خطيرا للسلام والأمن الدوليين، ولا سيما عندما تستهدف البنى التحتية الحيوية.

ثم إن العديد من الدول تعمل علنا أيضا على تطوير قدرات سيبرانية لأغراض عسكرية، وهذا التوجه يمكن أن يطلق العنان لسباق تسلح سيبراني ويزيد من عدد الهجمات والهجمات المضادة السيبرانية، فضلا عن مخاطر الحسابات الخاطئة التي يمكن أن تؤدي إلى نشوب نزاعات مسلحة.

وتشعر تونس بالقلق أيضا من أن القدرات السيبرانية، التي كانت متاحة في السابق للدول فقط، أصبحت في متناول الجهات الفاعلة من غير الدول، بما فيها المنظمات الإرهابية التي تستخدمها لأغراض خبيثة. وتفيد التقارير بأن هذه القدرات كثيرا ما اكتسبت عن طريق التسرب أو السرقة من الكيانات الحكومية، مما يثير مسألة مسؤولية الدول.

ولم يعد من الممكن استبعاد إمكانية قيام الجماعات الإرهابية بشن هجمات سيبرانية مدمرة ضد الهياكل الأساسية الحيوية مثل محطات الطاقة النووية، ولذلك ينبغي التصدي لها بجدية.

وتؤكد تونس من جديد انطباق القانون الدولي في التصدي لاستخدام الدول لتكنولوجيات المعلومات والاتصالات، وتشدد في هذا الصدد على أهمية احترام المبدأ المكرس في ميثاق الأمم المتحدة، بما في ذلك تسوية المنازعات الدولية بالوسائل السلمية، والامتناع عن التهديد باستخدام القوة أو استخدامها، واحترام حقوق الإنسان والحريات الأساسية.

ونود أيضا أن نشدد مرة أخرى على إمكانية تطبيق القانون الدولي الإنساني على العمليات السيبرانية التي تجرى أثناء النزاعات المسلحة.

ويرحب وفد بلدي باعتماد تقرير الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي العام، وتقرير فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي، وهو اعتماد تم في وقت سابق من هذا العام بتوافق الآراء، وقد أسهم هذان التقريران كلاهما في تعميق فهم الدول الأعضاء لكيفية تطبيق القانون الدولي وقدما توجيهات إضافية بشأن الطريقة التي يمكن للمعايير الطوعية غير الملزمة أيضا أن تؤدي دورا هاما في منع نشوب النزاعات والتشجيع على إقامة فضاء إلكتروني مفتوح وآمن ومستقر وميسَّر وسلمي.

وإننا نتطلع إلى مواصلة إجراء حوار مفتوح وشامل للجميع بشأن الأمن السيبراني خلال دورات الفريق العامل المفتوح العضوية الجديد (المعني بأمن تكنولوجيا المعلومات والاتصالات واستخدامها للفترة 2021-2025) من أجل تعزيز قدرات جميع الدول ومنع آثار الأنشطة السيبرانية الخبيثة والتهديدات والهجمات السيبرانية أو التخفيف من حدتها.

أما تونس فقد اعتمدت من جانبها وتحت إشراف مجلس الأمن القومي وبمشاركة القطاع الخاص والمجتمع المدني في تشرين الأول/أكتوبر 2019 استراتيجية وطنية للأمن السيبراني تهدف إلى تحسين قدرتها على الصمود أمام التهديدات السيبرانية من خلال تنمية قدراتها الوطنية ونظامها القانوني، مع الاحترام الكامل للحقوق والحريات الأساسية، ومن خلال تعزيز التعاون الدولي.

وأخيرا، ونظرا للطبيعة المترابطة للفضاء الإلكتروني، نعتقد أن تبادل المعلومات عن مواطن الضعف المعروفة وبناء القدرات لأولئك الذين يطلبونها يكتسي أهمية حاسمة للحد من المخاطر التي تشكلها التهديدات السيبرانية على السلام والأمن الدوليين.

المرفق السابع عشر

بيان البعثة الدائمة للأرجنتين لدى الأمم المتحدة

[الأصل: بالإسبانية]

تود الأرجنتين أن تتوجه بالشكر إلى إستونيا على مبادرتها بعقد مناقشة مفتوحة لزيادة فهم المخاطر المتزايدة الناجمة عن الأعمال الكيدية في الفضاء الإلكتروني وتأثيرها على السلام والأمن الدوليين. ومجلس الأمن، بحكم ولايته وطبيعته، قادر على معالجة الموضوع وإيلائه ما يستحق من أهمية وعناية.

إن العدد المنتظم والمتزايد من التقارير عن وقوع حوادث سيبرانية خطيرة في مختلف أنحاء العالم يلفت نظر الجميع إلى ضرورة مواصلة بناء فهم أكبر لكيفية إدارة حوادث من هذا القبيل قد يعرض بعضها السلام والأمن الدوليين للخطر، وضرورة إنشاء أطر للتعاون وتعزيز بناء القدرات الوطنية لمواجهة التحديات التي تؤثر في المجتمع الدولي برمته. ولذلك، لا بد من اتخاذ إجراءات على الصعيد الوطني والإقليمي والدولي.

فعلى الصعيد الدولي، وبهدف معالجة أحد أهم جوانب المسألة، ترى الأرجنتين أن من الأهمية بمكان الحفاظ على مساحات واسعة وشاملة للجميع يمكن فيها لبلدان من جميع المناطق وذات وجهات نظر متنوعة أن تشارك بنشاط في جملة أعمال منها بناء توافق في الآراء بشأن قواعد ومعايير ومبادئ سلوك الدول المسؤول وكيفية تطبيق القانون الدولي في الفضاء الإلكتروني. وتدرك الأرجنتين أن ثمة مجموعة كبيرة من المعايير والقواعد والمبادئ الطوعية التي قبلها بتوافق الآراء جميع أعضاء الجمعية العامة للأمم المتحدة لتوجيه استخدام الدول لتكنولوجيا المعلومات والاتصالات وسلوك الدول المسؤول في الفضاء الإلكتروني، وهي أمور أساسية للحفاظ على الاستخدام السلمي للفضاء الإلكتروني واستقراره. وهذه نقطة انطلاق وأحد الأركان اللذين ينبغي الحفاظ عليهما وتطويرهما.

ونحن نقدر بصفة خاصة توافق الآراء الذي حصل عليه الفريق العامل المفتوح العضوية الأول المعني بالتطورات في مجال المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، الذي يقوم على خصائص الانفتاح هذه. ونقدر أيضا عمل فريقي الخبراء الحكوميين السابق والحالي المعنيين بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي. وتجدر الإشارة إلى أن الفريقين كليهما أصدرا هذا العام تقريرين بتوافق الآراء، مشفوعين بتوصيات ومساهمات هامة لمواصلة البناء على توافق الآراء الذي تم التوصل إليه بالفعل في الماضي.

ويكتسي استمرار منتدى المناقشة المفتوح والشامل للجميع وذي الآفاق الأوسع أهمية بالغة بهدف مواصلة توطيد الاتفاقات التي تم التوصل إليها وإبرام اتفاقات جديدة. ولذلك نرحب بإنشاء فريق عامل مفتوح العضوية جديد معني بأمن تكنولوجيا المعلومات والاتصالات واستخدامها، تمتد ولايته حتى عام 2025، وسيواصل بلدنا المشاركة فيه بنشاط وبصورة بنّاءة.

وفي هذا الصدد، وفيما يتعلق باتباع نهج أكثر فعالية، تؤيد الأرجنتين، إلى جانب عدد من البلدان الأخرى من جميع المناطق، المبادرة الدولية لبرنامج عمل بشأن تطوير تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي. ويقترح برنامج العمل هذا، الذي يمر بمرحلة تطوير مفاهيمي كامل، إطارا مفتوحا وشاملا للجميع ومرنا ومتواصلا للمناقشة تحت رعاية الأمم المتحدة تجريه الدول وبمشاركة مناسبة من جانب الجهات الفاعلة المتعددة المنخرطة في الفضاء الإلكتروني. وندعو جميع البلدان إلى إبداء اهتمام بهذه المبادرة.

وتعتقد الأرجنتين أن الأســـاس والمبدأ اللذين تقوم عليهما تفاهماتنا ينبغي أن يتمثلا في حماية وضـمان حقوق الإنسـان والحريات الأسـاسـية المكرسـة في ميثاق الأمم المتحدة والمعاهدات الدولية. ويجب أن تكون مسألة نوع الجنس والضمانات الخاصة للفئات الضعيفة عنصرا شاملا في جميع الإجراءات التي نتخذها.

وفي سـياق الابتكار المسـتمر في الميدان، يجب أن نعمل بنشـاط لضـمان تمتع جميع الدول بفوائد تلك التكنولوجيات على نحو منصـــف. ولذلك، نعتقد أن تقليص الفجوة الرقمية بين الدول وداخلها ينبغي أن يكون شاغلا مستمرا في المناقشة.

وثمة ارتباط وثيق بين هذا الشـاغل وتنمية القدرات الوطنية. وهناك مجال واسـع جدا للعمل في هذا المجال وهو أحد المبادئ لتنمية أوجه التآزر مع الجهات الفاعلة الأخرى التي تشارك في الفضاء الإلكتروني، مثل القطاع الخاص والمجتمع المدني والأوساط الأكاديمية والقطاع التقني.

وقد أثبتت المنظمات الإقليمية ودون الإقليمية أنها جهات فاعلة هامة وحاسـمة باعتبارها عوامل محفزة لتنمية القدرات الوطنية، وتعزيز التفاهمات المشتركة، وتيسير التعاون الدولي.

ولا شـــك في أنه يجب على الدول أن تبذل جهودا كبيرة على الصـــعيد الوطني لتنمية القدرات واســـتحداث المعايير والهياكل الفعالة لإعطاء المسألة الأهمية والأولوية اللتين تستحقهما.

ونحن نأمل أن تتيح لنا هذه المناسبة تحديد سبل جديدة للتفاهم من شأنها أن تساعدنا على تحقيق فضاء إلكتروني يتسم بالحرية والانفتاح والأمان والاستقرار وإمكانية تشغيله المتبادل.

المرفق الثامن عشر

بيان الممثل الدائم لأستراليا لدى الأمم المتحدة، ميتشل فيفيلد

تتوجه أستراليا بالشكر إلى إستونيا على الفرصة التي أتيحت لها لتقديم بيان إلى مجلس الأمن يتناول مسألة السلام والأمن الدوليين في الفضاء الإلكتروني. ومع تزايد الأهمية الاستراتيجية للفضاء الإلكتروني، سيحاول المزيد من المجموعات ممارسة السلطة من خلاله. فالقضايا السيبرانية أصبحت قضايا استراتيجية للسياسة الخارجية تكتسي أهمية ملحة لجميع البلدان ومن الحيوي أن يعاملها المجتمع الدولي على هذا النحو.

وعلى الرغم من أن وتيرة الحوادث السيبرانية الخبيثة ونطاقها وتطورها وخطورتها آخذة في الازدياد، فإن للأمم المتحدة تاريخا حافلا بالأعمال المتعلقة بتوثيق التعاون الدولي لفهم هذه التهديدات وتعزيز إقامة فضاء إلكتروني مفتوح وحر وآمن وسلمي وقابل للتشغيل المتبادل.

وقد اتفق جميع أعضاء الأمم المتحدة، بتوافق الآراء، على أن القانون الدولي الساري – وبخاصة ميثاق الأمم المتحدة برمته – ينطبق على الفضاء الإلكتروني وهو ضروري للحفاظ على السلام والاستقرار في إطار تهيئة بيئة لتكنولوجيا المعلومات والاتصالات منفتحة وآمنة ومستقرة وميسَّرة وسلمية[3].

وقد بيّنت أستراليا آراءها بشأن كيفية تطبيق مبادئ معينة من القانون الدولي على سلوك الدول في الفضاء الإلكتروني (2017؛ و 2019؛ و 2021) ونشرت دراسات حالات إفرادية قانونية افتراضية (2020)[4].

وينطبق القانون الدولي الإنساني (بما في ذلك مبادئ الإنسانية والضرورة والتناسب والتمييز) على الأنشطة السيبرانية خلال النزاعات المسلحة. وينص القانون الدولي الإنساني على قواعد تنطبق على الأنشطة السيبرانية في أي نزاع مسلح لا تشكل أو ترقى إلى مستوى "الهجوم"، بما في ذلك أوجه الحماية العامة الممنوحة للسكان المدنيين وفرادى المدنيين ضد الأخطار الناشئة عن العمليات العسكرية.

وينطبق القانون الدولي لحقوق الإنسان أيضا على سلوك الدول في الفضاء الإلكتروني. وبموجب القانون الدولي لحقوق الإنسان، تقع على عاتق الدول التزامات بحماية حقوق الإنسان ذات الصلة للأفراد الخاضعين لولايتها القضائية، بما في ذلك الحق في الخصوصية، حيثما تمارس تلك الحقوق أو تتحقق من خلال الفضاء الإلكتروني أو فيه.

واعترافا بالسمات الفريدة للفضاء الإلكتروني، وافقت جميع الدول الأعضاء في عام 2015 على أن تسترشد في استخدامها لتكنولوجيا المعلومات والاتصالات بالمعايير الأحد عشر الطوعية وغير الملزمة لسلوك الدول المسؤول في الفضاء الإلكتروني[5]. وتكمل هذه المعايير الالتزامات القانونية القائمة للدول، ولكنها لا تحل محلها. فالقانون الدولي والقواعد الدولية مجتمعة تضع توقعات واضحة لسلوك الدول المسؤول، وبالتالي تعزز القدرة على التنبؤ والاستقرار والأمن.

(3) انظر قراري الجمعية العامة 243/68 و 237/70 ومقررها 75/265.

(4) انظر www.internationalcybertech.gov.au/international-security-at-the-un.

(5) انظر قرار الجمعية العامة 237/70.

وأقرت جميع الدول أيضا بضرورة وضع تدابير لبناء الثقة وبناء قدرات منسقة[6]. وتكتسي هذه التدابير، التي تهدف إلى منع سوء الفهم الذي يؤدي إلى نشوب النزاعات، أهمية الآن أكثر من أي وقت مضى، ويلزم بناء القدرات المستهدفة لضمان اكتساب جميع البلدان القدرة على التصدي للتحديات واغتنام الفرص لزيادة الاتصال.

وتُتيح هذه التدابير مجتمعة (القانون الدولي، والمعايير، وتدابير بناء الثقة، وبناء القدرات) المرتكز الذي يكفل انفتاح الفضاء الإلكتروني وأمانه واستقراره وازدهاره، وكثيرا ما يشار إليها على أنها إطار الأمم المتحدة لسلوك الدول المسؤول في الفضاء الإلكتروني (الإطار). وكل عنصر من عناصر الإطار يعزز بعضه بعضا وينبغي ألا ينظر إلى عنصر واحد بمعزل عن الآخر.

ويمثل إقرار جميع الدول الأعضاء للإطار[7] على الصعيد العالمي تقدما كبيرا نحو تعزيز السلام والاستقرار الدوليين في الفضاء الإلكتروني. ويوفر الإطار، إذا ما تم التقيد به، مرتكزا قويا من أجل التصدي للتهديدات التي تشكلها الأنشطة السيبرانية الخبيثة التي تقوم بها الدول وترعاها.

وتؤكد أستراليا من جديد التزامها بالعمل وفقا لإطار سلوك الدول المسؤول في الفضاء الإلكتروني، على النحو المفصل في التقارير المجمعة لأفرقة الخبراء الحكوميين في الأعوام 2010 و 2013 و 2015 و 2021[8] وتقرير الفريق العامل المفتوح العضوية لعام 2021[9] وتدعو جميع البلدان إلى أن تفعل الشيء نفسه.

بيد أن عددا صغيرا من الدول والجهات الفاعلة التي ترعاها الدول يخرق بصورة متزايدة القانون والقواعد الدولية، على الرغم من التوقعات الواضحة التي حددها المجتمع الدولي. وهي بذلك تهدد السلام والاستقرار الدوليين.

إن ما نحتاج إليه ليس المزيد من القواعد – أو قواعد جديدة – بل الالتزام بالقواعد التي اتفقنا عليها بالفعل، والمزيد من المساءلة عندما يتم خرقها. ولردع أي نشاط خبيث، يجب أن تكون هناك عواقب فعّالة على من يتصرف خلافا للقانون الدولي القائم وللمعايير المتفق عليها لسلوك الدول المسؤول.

وأستراليا ملتزمة بالتصدي للأنشطة السيبرانية الخبيثة وردعها وتثبيطها، ولا سيما من قِبل الدول ووكلائها. وستعمل أستراليا مع الجهات الشريكة على تعزيز الاستجابات المنسقة للسلوك غير المقبول في الفضاء الإلكتروني. فردع الأنشطة الخبيثة يحمي الاستقرار الدولي. ويتمثل الهدف من سياسة الردع السيبراني في أستراليا في منع الهجمات السيبرانية الكبيرة التي تضر بمصالح أستراليا وشركائها الدوليين.

إن التعاون الفعال بين الدول وأوساط الجهات المتعددة صاحبة المصلحة (بما في ذلك المجتمع المدني والقطاع الخاص والأوساط الأكاديمية والتقنية) يؤثر عمليا في الأمن ويرفع من مستوى القدرات ويخلق دورة معززة للتنمية والانفتاح والاستقرار في الفضاء الإلكتروني. وبما أن الجهات الحامية للبنى التحتية الحيوية، والجهات المقدمة للخبرة التقنية والجهات المستفيدة منها، والجهات المعنية غير الحكومية ذات

(6) المرجع نفسه.

(7) A/DEC/75/564؛ و A/75/816.

(8) A/65/201؛ و A/68/98؛ و A/70/174.

(9) A/75/816.

الأصول المتنامية في الفضاء الإلكتروني هي أولى الجهات المتضررة من الحوادث السيبرانية في كثير من الأحيان، فإن لها مصالح متشابكة في الحفاظ على بيئة شبكية سلمية.

ويقوض انعدام المساواة بين الجنسين السلام والاستقرار والأمن العالميين في الفضاء الإلكتروني. وهو يسهم في طائفة من التحديات، من بينها الفقر والحوكمة الضعيفة والنزاعات والتطرف العنيف، وكثيرا ما يؤدي إلى تفاقمها. ولا جدال في قيمة المساواة بين الجنسين ومشاركة المرأة في صنع القرار والقيادة وبناء السلام المرتبطين بالسلام والأمن الدوليين في الفضاء الإلكتروني. ولذلك ستواصل أستراليا اتخاذ خطوات ملموسة لدعم المشاركة الفعالة والمجدية للمرأة في جميع المحافل التي تناقش المسائل المتصلة بالسلام والأمن الدوليين في الفضاء الإلكتروني.

إن الضرر أو الخلل المحتمل الناجم عن الأنشطة السيبرانية الخبيثة هام ومتزايد. فينبغي عدم تبديد الاهتمام والوعي المتزايدين من جانب المجتمع الدولي بهذه المسائل. وينبغي اغتنام هذه الفرصة – لتعميق فهم كيفية تطبيق القانون الدولي في الفضاء الإلكتروني، وتعزيز التنفيذ العملي لمعايير سلوك الدول المسؤول وتدابير بناء الثقة، وتنسيق بناء القدرات حتى تفهم جميع البلدان الإطار ويتسنى لها تنفيذه، وكفالة الإصغاء لأصوات متنوعة.

المرفق التاسع عشر

بيان البعثة الدائمة للنمسا لدى الأمم المتحدة

تود النمسا أن تتوجه بالشكر إلى إستونيا بصفتها رئيسة مجلس الأمن لشهر حزيران/يونيه 2021 على عقد هذه المناقشة المفتوحة بشأن السلام والأمن الدوليين في الفضاء الإلكتروني. والنمسا تؤيد بيان الاتحاد الأوروبي. ونود، بصفتنا الوطنية، أن نضيف الملاحظات التالية:

اليوم يمثل المرة الأولى التي يتناول فيها مجلس الأمن مسألة الأمن السيبراني باعتبارها مسألة مستقلة – وهذا تطور جدير بالترحيب. ولكي يبقى مجلس الأمن على إلمام بالموضوع ويضطلع بولايته، من الضروري أن يواصل التصدي للتهديدات المعاصرة للسلام والأمن الدوليين.

فقد فاقم عدد متزايد من الأنشطة السيبرانية الخبيثة من التهديدات في الفضاء الإلكتروني على مدى السنوات الماضية. وفي عالم اليوم المترابط، عندما تعتمد البنية التحتية بصورة متزايد على أنظمة التحكّم الرقمي، يمكن أن تحدث الهجمات السيبرانية آثارا مماثلة أو أسوأ في بعض الأحيان من الهجمات التقليدية. وهذه التطورات، إلى جانب التحديات التي تطرحها الهجمات السيبرانية، تزيد من انعدام الأمن، ومخاطر الحسابات الخاطئة واحتمال وقوع خطأ بشري عند اتخاذ قرار بشأن كيفية الرد على هجوم قادم.

وعلى الرغم من أن الفضاء الإلكتروني يختلف عن العالم المادي في طريقة عمله، فلن نجانب الصواب إذا قلنا إن ثمة حقيقة واحدة بسيطة مفادها أن القانون الدولي بأكمله ينطبق تماما أيضا في الفضاء الإلكتروني. وقد أُعيد تأكيد هذا الأمر، وحصل ذلك مؤخرا في الوثائق الختامية للفريق العامل المفتوح العضوية المعني بتكنولوجيا المعلومات والاتصالات، وكذلك لفريق الخبراء الحكوميين المعني بالأمن السيبراني، اللذين اتفقا بتوافق الآراء على وثائق ختامية هامة تعزز فهمنا للتحديات التي نواجهها في الفضاء الإلكتروني. ومع تزايد عدد الدول التي لا تكتفي بتطوير قدرات دفاعية فحسب، وإنما تطور أيضا قدرات سيبرانية هجومية، من المهم أن تلتزم جميع الدول في استخدامها لتكنولوجيا المعلومات والاتصالات بالقانون الدولي الساري وكذلك بالمعايير المتعلقة بالسلوك المسؤول في الفضاء الإلكتروني. ونأمل أن تذكّر هذه الوثائق الدول بالتزاماتها، ولذلك فإنها ستسهم في تحقيق المزيد من الاستقرار في الفضاء الإلكتروني.

وغني عن القول إن الأحكام الأساسية لميثاق الأمم المتحدة ينبغي أن توجّه جميع الدول في سلوكها في الفضاء الإلكتروني. والدول ملزمة، على وجه الخصوص، بالتقيد بحظر استخدام القوة باعتبارها الركيزة الأساسية لنظام الأمن الدولي. وبالإضافة إلى ذلك، اتفقت أفرقة الخبراء الحكوميين السابقة على معايير لسلوك الدول المسؤول في الفضاء الإلكتروني أقرتها جميع الدول الأعضاء. وبناء عليه، من الواضح أن عدم وجود قواعد ومعايير ليس هو الذي يسهم في عدم الاستقرار وانعدام الأمن بل عدم تنفيذها. ولذلك، فإننا ندعو جميع الدول إلى الامتثال الكامل للقانون الدولي واتباع معايير السلوك المسؤول للدول برمتها.

وفي حالة نشوب نزاع مسلح أو ما يتصل به من عناصر في الفضاء الإلكتروني، لا بد من احترام القانون الإنساني الدولي والتقيد به حيث تنطبق مبادئ الإنسانية والضرورة والتناسب والتمييز بصورة كاملة في الفضاء الإلكتروني.

وفي سياق جائحة كوفيد-19، نلاحظ بقلق الزيادة الأخيرة في الهجمات السيبرانية على المرافق الطبية والصحية التي تنتهك انتهاكا صارخا المعايير التي تدعو إلى أن تكون البنية التحتية الحيوية، بما في ذلك البنية التحتية الطبية، بمنأى دائما عن الأنشطة السيبرانية الخبيثة.

ومن أجل تجنب سيناريوهات النزاع، لا بد من بناء الثقة – وينبغي للدول أن تشارك بطريقة بنّاءة في تقاسم فهمها للفضاء الإلكتروني والسبل التي تشارك بها عسكريا من أجل تجنب الحسابات الخاطئة. وفي هذا الصدد، لا يمكن التقليل من قيمة الدور الذي تقوم به المنظمات الإقليمية التي نفذت العديد منها أنشطة لبناء الثقة. ونرحب بوجه خاص بمشاركة منظمة الأمن والتعاون في أوروبا في هذا الشأن، ونأمل في أن الاستفادة من خبرتها في مجال شبكات جهات الاتصال لشؤون الأمن الإلكتروني ستتيح لنا أيضا إنشاء شبكة عالمية على مستوى الأمم المتحدة.

وعلى الرغم من أن الدول والمنظمات الدولية والإقليمية كانت في طليعة الدول التي وضعت القانون الدولي ومعايير سلوك الدول المسؤول، فإنها لا تستطيع أن تتصدى للتحديات الماثلة أمامنا بنفسها. فالجهات الفاعلة التجارية تضطلع بدور ومسؤولية كبيرين في الفضاء الإلكتروني، والمجتمع المدني والأوساط الأكاديمية يساعداننا في إدراج وجهات نظر مختلفة في مناقشاتنا. ولهذا السبب ينبغي أن تسترشد المناقشات المقبلة المتعلقة بالفضاء الإلكتروني بنهج شامل ومتعدد الجهات صاحبة المصلحة يكفل الاستماع إلى أولئك الذين يقومون بدور في الحفاظ على فضاء إلكتروني حر وآمن ومفتوح ومستقر والمساهمة في الأهداف المشتركة التي نسعى إلى تحقيقها.

وعلى الرغم من كل التقدم المحرز في مجال الأمن السيبراني، لا تزال هناك أسئلة كثيرة مفتوحة تلوح في الأفق، وسيتعين على المجتمع الدولي أن يجد إجابات مشتركة على هذه الأسئلة. وسيظل التعاون أساسيا وستقف النمسا على أهبة الاستعداد للمساهمة البناءة في العمليات ذات الصلة. وفي هذا السياق، نأمل أن تعود المناقشات المفتوحة في المجلس في المستقبل إلى الممارسة السابقة المتمثلة في السماح لغير الأعضاء بالإدلاء ببيانات شفوية من أجل تسليط الضوء على وجهات نظر جميع الدول المهتمة.

المرفق العشرون

بيان الممثل الدائم للبحرين لدى الأمم المتحدة، جمال فارس الرويعي

[الأصل: بالعربية]

بدايةً يطيب لي أن أتقدم بالشكر إلى البعثة الدائمة لإستونيا على عقد الجلسة الرسمية الأولى لمجلس الأمن بشأن الأمن السيبراني والتي تتزامن مع ازدياد اعتماد الدول والأفراد على تكنولوجيا العالم الرقمي في ظل استمرار التحديات المرتبطة بتفشي جائحة كوفيد-19.

كما أود أن أرحب بترؤس سعادة السيدة كايا كالاس، رئيسة وزراء إستونيا، لهذه الجلسة، وبالسيدة إيزومي ناكاميتسو، وكيلة الأمين العام للأمم المتحدة والممثلة السامية لشؤون نزع السلاح، على إحاطتها القيمة.

وإن التحول التكنولوجي والرقمي وظهور التقنيات الحديثة يساهمان في تحقيق التقدم والرخي والنماء للبشرية جمعاء، وتجلّت هذه الأهمية على خلفية الاعتماد على العمل والدراسة وتقديم الخدمات عن بعد في مختلف القطاعات نظرا لتفشي جائحة كوفيد-19. وعلى الرغم من المنافع العديدة للتطور التكنولوجي، فإنه يرتبط كذلك بالعديد من المخاطر خاصة في حال لم تكن هناك منظومة واضحة لحماية أمن المعلومات والفضاء الإلكتروني، وهو ما نراه في الهجمات السيبرانية المختلفة التي قد تستهدف البنى التحتية الأساسية للدول بما يهدد قطاعاتها الحيوية، أو المؤسسات، أو الأفراد.

وأولت الأمم المتحدة اهتماما بالغا لهذه المسألة، حيث تطرق مجلس الأمن إليها بشكل غير مباشر في عدد من الجلسات المتصلة بصون السلم والأمن الدوليين إلى جانب عقد اجتماعات بصيغة آريا. كما أنشأت الجمعية العامة عددا من الآليات، من ضمنها الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات (2021-2025) في 2020، والتي تهدف إلى دراسة التهديدات التي يشكلها استخدام تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي وكيفية معالجة هذه التهديدات، إلى جانب صياغة المعايير السلوكية للدول في الفضاء الإلكتروني، وتطبيق القانون الدولي في استخدام تكنولوجيا المعلومات والاتصالات، وتدابير بناء الثقة، وبناء القدرات.

وانطلاقا من إيمانها بأهمية حماية الفضاء الإلكتروني من الهجمات والاعتداءات بما يضمن مصالح الدول والشعوب، أيدت مملكة البحرين إنشاء هذه الآليات، كما شاركت في أعمال الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي الذي انتهى من أعماله في عام 2021، وتتطلع للمشاركة الفعّالة في أعمال الفريق العامل المنشأ حديثا.

وفي إطار اهتمامها الكبير بالأمن السيبراني على خلفية التحول الرقمي والنقلة النوعية التي يشهدها قطاع تقنية المعلومات والاتصالات، عملت مملكة البحرين على بناء نظام حوكمة واضح وشامل لحماية الفضاء الإلكتروني من خلال المركز الوطني للأمن السيبراني التابع لوزارة الداخلية والذي يعنى بالأمن الإلكتروني في مختلف القطاعات بالمملكة، إلى جانب هيئة المعلومات والحكومة الإلكترونية المعنية بحماية أمن المعلومات في شبكة البيانات الحكومية في مملكة البحرين. كما تسعى هيئة تنظيم الاتصالات إلى تعزيز التعاون بين القطاعين العام والخاص لضمان جاهزيتهما لمواجهة تهديدات الأمن السيبراني.

ومن جهة أخرى، حرصت مملكة البحرين على وضع التشريعات والأطر القانونية المتصلة بأمن المعلومات لحماية الأفراد والمؤسسات وأبرزها القانون رقم (30) لسنة 2018 بشأن إصدار قانون حماية البيانات الشخصية والقانون رقم (16) لعام 2014 بشأن حماية المعلومات ووثائق الدولة والقانون رقم (60) لعام 2014 بشأن جرائم تقنية المعلومات.

وعلى الصعيد الإقليمي، تشارك مملكة البحرين بفعالية في أعمال اللجنة الدائمة للأمن السيبراني بدول مجلس التعاون لدول الخليج العربية، حيث اقترحت إنشاء منصة إلكترونية لتبادل المعلومات والبيانات فيما يخص مجال الأمن السيبراني بين الدول الأعضاء، وقد قامت كل من الدول الأعضاء بتعيين ضابط اتصال لتبادل المعلومات المتعلقة بالأمن السيبراني كالتهديدات وأفضل الممارسات.

كما صادقت مملكة البحرين على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في عام 2017.

وختاماً، تؤكد مملكة البحرين دعمها للتعاون الدولي في مجال الأمن السيبراني، بما يلبي تطلعات شعوب العالم ويحقق التقدم والازدهار والنمو ويصب في تنفيذ أهداف التنمية المستدامة لعام 2030.

المرفق الحادي والعشرون

بيان الممثل الدائم لبلجيكا لدى الأمم المتحدة، فيليب كريدلكا

بادئ ذي بدء، أود أن أعرب عن امتناني للرئاسة الإستونية على استضافتها هذه المناقشة المفتوحة الأولى لمجلس الأمن بشأن السلام والأمن في الفضاء الإلكتروني. وهذه المناقشة التي تجري في الوقت المناسب تدل على أن الحاجة ماسة إلى معالجة هذا الموضوع وإلى أهمية قيام مجلس الأمن بذلك. إن المخاطر الناجمة عن الأنشطة الكيدية في الفضاء الإلكتروني آخذة في التزايد بالفعل، وتأثيرها على السلام والأمن الدوليين أكثر ضررا من أي وقت مضى. ولذلك من الأهمية بمكان إعادة تأكيد التزام الدول الأعضاء بالقانون الدولي وبإطار سلوك الدول المسؤول باعتبارهما عنصرين رئيسيين لمنع نشوب النزاعات وصون السلام والأمن في الفضاء الإلكتروني.

ويتطلب تحقيق هذا الهدف على السواء تفاهما دوليا مشتركا بشأن إدارة الفضاء الإلكتروني وإجراءات حقيقية لتنفيذ هذه الرؤية على أرض الواقع.

فالمناقشة الدولية بشأن إدارة الفضاء الإلكتروني تمر بمرحلة حاسمة. وتؤيد بلجيكا بقوة المناقشات الجارية في إطار الأمم المتحدة، ومن بينها اللجنة الأولى، ومختلف الأفرقة العاملة المفتوحة العضوية وأفرقة الخبراء الحكوميين. وتكتسي العناصر التالية أهمية كبرى:

فأولا، تدعو بلجيكا إلى رؤية مشتركة بشأن فضاء إلكتروني عالمي حر ومفتوح ومستقر وسلمي وآمن، تُطبَّق فيه حقوق الإنسان والحريات الأساسية وسيادة القانون. ويستند هذا الفهم المشترك إلى نهج شامل للجميع يُستمع فيه إلى صوت جميع الجهات المعنية صاحبة المصلحة، بما في ذلك المجتمع المدني والقطاع الخاص والأوساط الأكاديمية.

وثانيا، يجب على المجتمع الدولي أن يواصل السعي من أجل وضع إطار عالمي حقيقي للأمن السيبراني لسلوك الدول المسؤول. وهذا العمل ينبغي أن يستند إلى القانون الدولي الساري، بما في ذلك ميثاق الأمم المتحدة كله، والقانون الدولي الإنساني، والقانون الدولي لحقوق الإنسان. وفي العام الماضي، شاركت بلجيكا، بصفتها عضوا غير دائم في مجلس الأمن، في اجتماع لمجلس الأمن عقد بصيغة آريا بشأن الهجمات السيبرانية على الهياكل الأساسية الحيوية. وتعرض هذه الهجمات التي تستهدف الهياكل الأساسية الحيوية حياة البشر للخطر ويتعين على المجتمع الدولي أن يدينها. وتظل الهجمات السيبرانية على المرافق الطبية مثل المستشفيات مرفوضة.

وفيما يتعلق بإطار الأمم المتحدة المتعلق بسلوك الدول المسؤول في الفضاء الإلكتروني، لا بد من التأكيد على أن الدول الأعضاء في الأمم المتحدة قد أيدت – من خلال اتخاذ قرار الأمم المتحدة 237/70 – استنتاجات تقارير فريق الخبراء الحكوميين للأعوام 2010 و 2013 و 2015، التي تشكل أساسا متينا وتوافقيا لمزيد من العمل. وقد بذلت الأمم المتحدة والدول الأعضاء فيها جهودا كبيرة لبناء تفاهم دولي مشترك بشأن إدارة الفضاء الإلكتروني ووضع إجراءات حقيقية لتنفيذ هذه الرؤية المشتركة على أرض الواقع. وفي إطار نظام متعدد الأطراف يتسم بالكفاءة والفعالية، من الضروري أن نمضي قدما في أي مناقشة أخرى تبدأ من هذا الأساس التوافقي، من أجل تجنب إعادة النظر في الحلول التوفيقية الشاقة في الماضي مع تعطيل الجهود في المستقبل.

وثالثا، نعتقد أنه ينبغي لنا أن نعمل على مواءمة العدالة الجنائية الدولية بطريقة أفضل مع تحديات القرن الحادي والعشرين. ولهذا السبب انضمت بلجيكا إلى ليختنشتاين في مبادرتها لإنشاء مجلس للمستشارين معني بتطبيق نظام روما الأساسي على الحرب السيبرانية من أجل استكشاف الدور الذي يمكن أن تؤديه المحكمة الجنائية الدولية في هذا الإطار التنظيمي الجديد. ونحن نتطلع إلى تلقي التقرير النهائي لمجلس المستشارين المقرر تقديمه هذا العام.

وينبغي أن تتبع المبادئ التوجيهية إجراءات لإحداث تغيير. وفي هذا الصدد، فإن بلجيكا مقتنعة بأن اقتراح مصر وفرنسا المتمثل في وضع برنامج عمل يشكل الهيكل الصحيح لتنفيذ رؤيتنا. وتفخر بلجيكا بدعم هذه المبادرة مع أكثر من 50 بلدا آخر، ونأمل أن تنضم دول أخرى كثيرة.

وعلى الصعيد الوطني، اعتمدت بلجيكا مؤخرا، في أيار/مايو 2021، النسخة 2,0 من الاستراتيجية الوطنية الجديدة للأمن السيبراني للفترة 2021-2025 التي تحدد النهج الشامل لبلدنا من حيث تنمية قدرتنا على المجابهة السيبرانية ومكافحة التهديدات السيبرانية. ويتمثل الهدف الرئيسي لهذه الاستراتيجية الوطنية في "دفع بلجيكا إلى مصاف أقل البلدان هشاشة في أوروبا".

وتنص سياسة الأمن السيبراني في بلجيكا أيضا على استحداث آلية جديدة لإسناد المسؤولية ينظر إليها على أنها أداة ردع. فإذا أردنا منع الأنشطة السيبرانية الخبيثة وردعها بصورة فعالة في بيئة يتزايد فيها عدد الهجمات السيبرانية وتعقيدها، فإن عملية إسناد المسؤولية رسميا عن الأنشطة السيبرانية الخبيثة التي تستهدف أي منظمة حيوية في بلجيكا هي عملية تشكل أداة هامة. ويمكن أيضا تفعيل الإجراء الوطني لإسناد المسؤولية بهدف دعم بلد حليف يقع ضحية لهجمات مماثلة.

وعلاوة على ذلك، تنص الاستراتيجية الوطنية على التزام دولي واضح. وذلك لأن بلجيكا تقول وتفعل، فهي مقتنعة بأن الحاجة تقتضي زيادة التعاون الدولي لتعزيز الأمن والاستقرار في الفضاء الإلكتروني.

ثم إن زيادة التعاون الدولي تعني المزيد من بناء القدرات والمزيد من الدعم لتدابير بناء الثقة، بطرق منها جهود المنظمات الإقليمية مثل منظمة الأمن والتعاون في أوروبا. وتباشر بلجيكا دورا نشطا في عمل هذه المنظمة لجعل تدابير بناء الثقة هذه ملموسة وعملية. وفيما يتعلق ببناء القدرات، فإن الاحتياجات هامة وملحة على الصعيد العالمي. وينبغي تعزيز برامج التعاون أو بناء القدرات القائمة، مثل تلك التي يقدمها الاتحاد الأوروبي أو المنتدى العالمي للخبرات السيبرانية وتوسيع نطاقها. فمن مصلحتنا جميعا تعزيز القدرة العالمية على الصمود في وجه التهديدات السيبرانية.

المرفق الثاني والعشرون

بيان البعثة الدائمة للبرازيل لدى الأمم المتحدة

أود في البداية أن أهنئ إستونيا على المبادرة الهامة المتمثلة في تشجيع إجراء مجلس الأمن لأول مرة مناقشة مفتوحة رسمية بشأن الأمن الإلكتروني في السياق الأوسع المتصل بصون السلام والأمن الدوليين. إن التطور السريع لتكنولوجيات المعلومات والاتصالات التي أصبحت تتغلغل في جميع مجالات الوجود البشري، يدفعنا إلى تحديث مفهوم التهديدات، وتكييف الإطار المعياري القائم مع هذا الواقع الجديد، ووضع أنماط جديدة لسلوك الدول المسؤول بغية التغلب على التحديات الحديثة والحد من نشوب النزاعات.

فعلى الرغم من أن موضوع الأمن الإلكتروني قد أثير للتو في الهيئة التي تتحمل المسؤولية الرئيسية عن صون السلام والأمن الدوليين، فإن الدول الأعضاء تناقشه منذ أكثر من عقدين – على الأقل منذ عام 1998، عندما أدرج هذا الموضوع لأول مرة في جدول أعمال الجمعية العامة. وخلال هذه الفترة، شهدنا اعتماد أربعة تقارير توافقية قدمتها أفرقة الخبراء الحكوميين – اثنان منها برئاسة خبيرين برازيليين – وتقرير توافقي مماثل قدمه فريق عامل مفتوح العضوية. وتشكل هذه الوثائق مجتمعة نصا تشريعيا ومدونة مشتركة من التفاهمات والمعايير والقواعد والمبادئ الطوعية غير الملزمة التي تساعد على إرشاد الدول بشأن استخدام تكنولوجيا المعلومات والاتصالات.

ومن أكبر إسهامات هذا النص التشريعي في صون السلام والأمن الدوليين توكيد أن القانون الدولي، بما في ذلك القانون الدولي الإنساني، ينطبق على الفضاء الإلكتروني. ومن خلال إسهامنا الوطني الطوعي في الخلاصة الرسمية التي أصدرها فريق الخبراء الحكوميين الأخير، أكدنا من جديد إيمان البرازيل الراسخ بأن الدول، في استخدامها لتكنولوجيا المعلومات والاتصالات، يجب أن تمتثل للقانون الدولي، بما في ذلك ميثاق الأمم المتحدة والقانون الدولي لحقوق الإنسان والقانون الدولي الإنساني. وأقرت الأمم المتحدة والمنظمات الإقليمية الأخرى بأن القانون الدولي، ولا سيما ميثاق الأمم المتحدة، ينطبق على الفضاء الإلكتروني، وهو ضروري لصون السلام والاستقرار وتعزيز بيئة مفتوحة وآمنة وسلمية وميسّرة في مجال تكنولوجيا المعلومات والاتصالات. ومن ثم، فإن المسألة لم تعد، في المناقشات الحالية، تتعلق بما إذا كان القانون الدولي ينطبق على استخدام الدول لتكنولوجيا المعلومات والاتصالات، وإنما بكيفية انطباقه.

وفي حين أن أوجه التماثل فيما يتصل بالعالم المادي قد تنجح في معظم الأحيان في تحديد هذا الانطباق، فإن خصائص الفضاء الإلكتروني الفريدة توجد حالات جديدة لم يصمم القانون الدولي أصلا لتنظيمها. فالترابط بين نظم المعلومات، والطابع غير الملموس لبيئة تكنولوجيا المعلومات والاتصالات، وتشعبات مشكلة إسناد المسؤولية عن الأعمال الخبيثة والهجومية في الفضاء الإلكتروني، هي من بين العوامل التي تشكل تحديات جديدة للقانون الدولي الذي يقوم تطوره على نظام دولي مادي وإقليمي.

وتزيد الاختلافات في تفسيرات الدول لكيفية انطباق القانون الدولي على استخدام تكنولوجيا المعلومات والاتصالات من خطر السلوك غير المتوقع وسوء الفهم وتصاعد التوترات. ولذلك، من المهم أن نحدد تدريجيا مجالات التقارب بين الدول بشأن هذه المسألة، وأن نعمل معا، حيثما يتبين وجود اختلافات، من أجل زيادة الاتساق في تفسير القواعد السارية. وإذا لزم الأمر، ينبغي أيضا اعتبار وضع معايير إضافية وسيلة لسد الثغرات القانونية المحتملة وإيجاد حل لأوجه الشك المتبقية.

ويعتمد صون السلام والأمن الدوليين اعتمادا كبيرا على مستوى الثقة السائد بين الدول. ولذلك، فبالإضافة إلى الاعتراف بانطباق القانون الدولي ووضع المعايير والقواعد والمبادئ المتعلقة بأنماط سلوك الدول المسؤول وتنفيذها، من الأهمية بمكان أن تنفذ الحكومات تدابير لبناء الثقة. ويشكل إنشاء شبكة من نقاط الاتصال على المستويين التقني والسياسي، فضلا عن تبادل الآراء الوطنية بشأن التهديدات وإدارة حوادث تكنولوجيا المعلومات والاتصالات، تدابير تعاونية وشفافة هامة. وهذه المبادرات لا تساعد على منع سوء الفهم والتصورات الخاطئة فحسب، وإنما هي مبادرات مفيدة أيضا في التصدي لحوادث تكنولوجيا المعلومات والاتصالات الخطرة وتهدئة التوترات في حالات الأزمات.

كما يمثّل بناء القدرات أداة أساسية في تهيئة بيئة سلمية لتكنولوجيا المعلومات والاتصالات. وكما هو الحال في مجالات أخرى، يمكن أن يؤدي عدم المساواة بين الأمم إلى انعدام الأمن أيضا في الفضاء الإلكتروني، مع التأثير تأثيرا مباشرا في عالم يتسم بالحركية. ويسهم التعاون الدولي الرامي إلى تطوير المؤسسات الوطنية والموارد البشرية والسياسات العامة في الحد من أوجه ضعف الدول، وهو أساسي لتحقيق عالمية تنفيذ القانون الدولي والمعايير والقواعد والمبادئ المتعلقة بأنماط سلوك الدول المسؤول في الفضاء الإلكتروني. وإذا كان هناك درس واحد لقنتنا إياه الجائحة فهو أنه لن ينعم أحد بالأمان ما لم يحظ الجميع بالأمان، والأمر نفسه يصدق على الفضاء الإلكتروني المترابط والمتكافل للغاية.

ونظرا لطبيعة الفضاء الإلكتروني المتعدد الجهات صاحبة المصلحة، ترى البرازيل أنه لا يمكن أن تنجح أي مناقشات فعالة بشأن الأمن السيبراني بدون إسهامات المجتمع المدني والأوساط الأكاديمية والقطاع الخاص. ومن الضروري اتباع نهج متعدد الجهات صاحبة المصلحة لتحديد التهديدات ومكافحتها، ومنع نشوب النزاعات، وتعزيز التفاهمات المشتركة، وزيادة القدرة على الصمود في وجه التهديدات السيبرانية، وتوثيق التعاون. ويكتسي توسيع نطاق التواصل بين الجهات الفاعلة العامة والخاصة من مختلف البلدان، وتبادل الخبرات وأفضل الممارسات، أهمية بالغة لتحقيق بيئة أكثر انفتاحا وأمنا وسلاما ونفاذا إلى تكنولوجيا المعلومات والاتصالات.

وما فتئت البرازيل تشارك بنشاط في المناقشات الدائرة بشأن الأمن السيبراني في الأمم المتحدة. وقد سعينا دائما إلى أن نكون استباقيين في كل من أفرقة الخبراء الحكوميين وآخر فريق عامل مفتوح العضوية. وستواصل البرازيل نهجها البنّاء في مناقشات الفريق العامل المفتوح العضوية الجديد الذي سيعقد دورته الموضوعية الأولى في كانون الأول/ديسمبر، وكذلك في آليات أخرى للحوار المؤسسي المنتظم الذي يمكن إنشاؤه، مثل برنامج العمل المتعلق بالأمن السيبراني. وفي الوقت نفسه، فإننا، بصفتنا عضوا غير دائم انتُخب حديثا في مجلس الأمن، نعتزم الإسهام في المضي قدما بالمناقشات المتعلقة بأثر استخدام تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي في صلب هذه الهيئة أيضا. وترى البرازيل أنه ينبغي للمجلس أن يسترشد أولا وقبل كل شيء بهدف تعزيز التقيد بالتوصيات السابقة التي اعتمدتها الجمعية العامة وبالتوصيات التي ستعتمدها مستقبلا بشأن مسألة الأمن السيبراني.

وشكرا لكم.

المرفق الثالث والعشرون

بيان البعثة الدائمة لكندا لدى الأمم المتحدة

[الأصل: بالفرنسية]

نشكر إستونيا على عقد جلسة مجلس الأمن هذه بشأن موضوع يتسم بمثل هذه الأهمية ويُطرح في إبانه. ويسرّ كندا اغتنام هذه الفرصة للمساهمة في المناقشات الجارية.

إن العالم يعتمد بصورة متزايدة على التكنولوجيات الرقمية وعلى الإنترنت. والفضاء الإلكتروني يشكل تهديدات على السلام والأمن الدوليين. والتدخل في الحياة الديمقراطية يعتبر مجال انشغال بوجه خاص. والزيادة المسجلة مؤخرا في الهجمات ببرامجيات طلب الفدية تبعث على الانشغال أيضا. لذلك يجب علينا أن نواصل اتخاذ الخطوات لضمان بقاء الفضاء الإلكتروني حرا ومفتوحا وآمنا.

ويشكل الإطار المتفق عليه لتعزيز سلوك الدول المسؤول في الفضاء الإلكتروني الأساس الذي يقوم عليه السلام والاستقرار في هذا الفضاء. ويتضمن هذا الإطار الاعتراف بإمكانية تطبيق القانون الدولي على الفضاء الإلكتروني، والتقيد بالمعايير المتفق عليها دوليًا، وبناء القدرات، وكذلك تنفيذ تدابير بناء الثقة. وتتضافر هذه العناصر لتقليل مخاطر التصعيد والنزاعات.

وقد أعادت تقارير التوافق التي اعتمدها مؤخرًا فريق الأمم المتحدة العامل المفتوح العضوية وفريق الأمم المتحدة للخبراء الحكوميين تأكيد هذا الإطار. وجميع الدول الأعضاء في الأمم المتحدة ملتزمة الآن بأن تسترشد بهذا الإطار.

ويمثل القانون الدولي عنصرا أساسيا لتطبيق النظام الدولي القائم على القواعد على الفضاء الإلكتروني. وتؤكد مجددا التقارير الصادرة مؤخرا عن الفريق العامل المفتوح العضوية وفريق الخبراء الحكوميين انطباق القانون الدولي على الفضاء الإلكتروني وتتخذ خطوات هامة في هذا الصدد. ويوصي تقرير الفريق العامل المفتوح العضوية بمزيد من التعاون في بناء القدرات في القانون الدولي، بحيث يمكن لعدد أكبر من الدول بلورة تصورات خاصة بها وبناء منظور مشترك. وفي تقرير فريق الخبراء الحكوميين، أُعيد تأكيد إمكانية انطباق القانون الدولي وأُشير بوضوح إلى القانون الدولي الإنساني.

ويوجه التقرير الصادر عن فريق الخبراء الحكوميين في أيار/مايو 2021 تنفيذ المعايير الأحد عشر غير الملزمة المتعلقة بسلوك الدول المسؤول. واعتمد فريق الخبراء الحكوميين هذه المعايير في عام 2015 وأيدتها جميع الدول الأعضاء في قرار الجمعية العامة للأمم المتحدة 237/70. وتعتبر كندا أن هذه المعايير وأحكام القانون الدولي تكفي وحدها لتوجيه سلوك الدول في الفضاء الإلكتروني. ومع ذلك، لا يزال هناك عمل يتعين القيام به لنشرها وتطبيقها. ونذكر على سبيل المثال الهجمات البارزة ببرامجيات طلب الفدية التي شنتها مؤخرا جماعات إجرامية. فقد عطلت قطاعات رئيسية من قبيل إمدادات الطاقة والغذاء على نطاق واسع. وألحقت أيضًا أضرارا بالأسواق المالية.

وعلى الرغم من أن الجماعات الإجرامية مسؤولة عن هذه الأعمال، فإن هذه الأمثلة تؤكد أهمية القانون الدولي والمعايير الأحد عشر لفريق الخبراء الحكوميين. ويتناول العديد من هذه المعايير بصورة مباشرة أو غير مباشرة التهديدات التي تتعرض لها البنى التحتية الحيوية لتكنولوجيا المعلومات والاتصالات. وينص أحد المعايير على أن الدول يجب أن تستجيب لطلبات المساعدة من أي دولة تقع بنيتها التحتية

الحيوية ضحية أعمال خبيثة عن طريق تكنولوجيا المعلومات والاتصالات. وينص معيار آخر على أنه يجب على الدول ألا تسمح عن علم باستخدام أراضيها لارتكاب أعمال غير مشروعة على الصعيد الدولي باستخدام تكنولوجيا المعلومات والاتصالات.

إن الجماعات التي تشارك في أعمال إجرامية، بما في ذلك الهجمات ببرامجيات طلب الفدية، تعيش وتعمل في دول. وهي تستخدم البنية التحتية الرقمية لهذه الدول لتنفيذ أعمالها الخبيثة. وهي تخضع لقوانين هذه الدول. وتقع على عاتق الدول، التي تُبلغ بوقوع عمل خبيث صادر من أراضيها، مسؤولية التصرف وإنفاذ قوانينها والتعاون مع الدول الأخرى. ومن خلال الموافقة على الاسترشاد بمعايير فريق الخبراء الحكوميين، تعهدنا جميعًا بالقيام بذلك. وهذا أيضًا هو السبب وراء اعتماد عدد متزايد من الدول لقوانين صارمة من أجل مكافحة الجرائم السيبرانية. وفي كثير من الحالات، استندت هذه الدول في صياغة هذه القوانين على اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، التي تضم الآن أطرافًا من جميع مناطق العالم.

ولسوء الحظ، كما لاحظنا ذلك مؤخرًا، لا تتقيد جميع الدول دائمًا بمعايير إطار سلوك الدول المسؤول. فبعض البلدان تسمح لمجرمي الفضاء الإلكتروني بالعمل انطلاقا من أراضيها دون عقاب. ويمر آخرون عبر وسطاء أو ينخرطون عمدًا في أنشطة سيبرانية خبيثة تتعارض مع معايير الإطار. وفي عدة مناسبات، انضمت كندا إلى شركائها الدوليين لإدانة هذه السلوكيات والتصدي للتهديد الذي تمثله للسلام والأمن الدوليين.

وكندا هي أحد الأطراف الـ 27 الموقّعين على الإعلان المشترك الصادر في أيلول/سبتمبر 2019 والمتعلق بتعزيز سلوك الدول المسؤول في الفضاء الإلكتروني. وبالإضافة إلى إعادة تأكيد الإطار المتعلق بتعزيز سلوك الدول المسؤول في الفضاء الإلكتروني، نحن ملتزمون بالعمل معًا وعن طواعية لمساءلة الدول عندما تتصرف بشكل مخالف لهذا الإطار، بما في ذلك اتخاذ تدابير شفافة وفقًا للقانون الدولي.

وهذا ما فعلناه حتى الآن، وهذا ما سنواصل القيام به. ومن المهم تسليط الضوء على التصرفات المخالفة للمعايير، وذلك من أجل إنفاذ الإطار المتفق عليه لتعزيز الإطار المتعلق بالسلوك المسؤول. ونحن نشجع الآخرين على أن يحذوا حذونا.

وفيما يتصل بالأمم المتحدة في المستقبل، تتطلع كندا إلى المشاركة البناءة في الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة (2021-2025). وسنساهم أيضا بنشاط في وضع برنامج عمل بشأن الأمن السيبراني. فكندا شاركت في الإشراف على برنامج العمل لأنها تعتقد أنه يمكن أن يكون بمثابة منتدى مفيد وعملي المنحى لتعزيز تنفيذ إطار العمل المتعلق بسلوك الدول المسؤول.

وسيعتمد نجاح هاتين العمليتين على قدرتهما على جمع الأصوات والتقريب بين وجهات النظر المتباينة في أساليب عملهما ونتائجهما. وفي إطار الفريق العامل المفتوح العضوية، تدعو كندا إلى المشاركة الهادفة للجهات غير الحكومية صاحبة المصلحة. وبالفعل، فإن لدى المجتمع المدني والأوساط الأكاديمية والدوائر التقنية والقطاع الخاص الكثير مما تسهم به في هذه المناقشات، لأنها أطراف تقوم بدور هام في تنفيذ توصيات فريق الخبراء الحكوميين والفريق العامل. وسندعو أيضًا إلى مشاركة الجهات صاحبة المصلحة بنشاط في برنامج العمل أثناء وضعه.

وسيكون من المهم أيضًا الحرص على الإصغاء إلى النساء حقًا، سواء داخل الفريق العامل المفتوح العضوية أو إدراج آرائهن في برنامج العمل. ويجب إدماج الاعتبارات الجنسانية في كلتا العمليتين منذ البداية، لضمان أن يعالج عمل كلا الفريقين جوانب الأمن السيبراني المتعلقة بالمنظور الجنساني. ومن الموثق جيدًا أن عمليات الوساطة التي تكون فيها مشاركة المرأة هامة تؤدي إلى نتائج أشد متانة، وتتميز بانخفاض مخاطر استئناف الأعمال العدائية بعد انتهاء عمليات السلام. ويمكن تعزيز العمليات السيبرانية للأمم المتحدة بنفس الأسلوب، وإشراك النساء بطريقة هادفة. والشمول هام لإنجاح كلتا العمليتين.

وباختصار، تظل كندا طرفا داعمًا ثابتًا للإطار المتفق عليه لتعزيز سلوك الدول المسؤول في الفضاء الإلكتروني. وسنواصل تعزيز تنفيذ التوصيات المنبثقة عن أفرقة الخبراء الحكوميين السابقة والفريق العامل المفتوح العضوية الأخير. وسنستمر أيضًا في التنديد بالأنشطة السيبرانية الخبيثة التي تتعارض مع هذا الإطار والتصدي لتلك الأنشطة قانونيا. وإننا نتطلع إلى مواصلة العمل مع المجتمع الدولي لتعزيز السلام والأمن الدوليين من خلال توطيد الاستقرار والأمن في الفضاء الإلكتروني.

المرفق الرابع والعشرون

بيان البعثة الدائمة لشيلي لدى الأمم المتحدة

تؤكد شيلي من جديد موقفها بأن أحكام القانون الدولي، وبخاصة ميثاق الأمم المتحدة، هي التي تنطبق على عملية صون السلام والاستقرار، وهي أساسية لهذه العملية وللارتقاء ببيئة لتكنولوجيا المعلومات والاتصالات منفتحة ومأمونة ومستقرة وميسَّرة وسلمية. وهذه الأحكام، إلى جانب مبادئ محددة من ميثاق الأمم المتحدة، وبخاصة تسوية المنازعات بالوسائل السلمية، وحظر اللجوء إلى التهديد باستخدام القوة أو استخدامها ضد السلامة الإقليمية أو الاستقلال السياسي لأي دولة، وعدم التدخل في الشؤون الداخلية للدول الأخرى، واحترام حقوق الإنسان والحريات الأساسية، لا يمكن الفصل بينها ماديا كما في المجالات الرقمية، وعلى هذا النحو سوف تستمر شيلي في التشجيع على تطبيقها.

ويمكن أن تشكل الأنشطة الخبيثة باستخدام تكنولوجيات المعلومات والاتصالات التي تقوم بها جهات فاعلة 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. فالأنشطة الخبيثة ضد الهياكل الأساسية الحيوية التي تقدم الخدمات محليا أو إقليميا أو عالميا أصبحت خطرة بصورة متزايدة، بما في ذلك الأنشطة الخبيثة لتكنولوجيات المعلومات والاتصالات التي تؤثر في البنية التحتية الحيوية للمعلومات، والبنية التحتية التي تقدم الخدمات الأساسية للجمهور، والبنية التحتية التقنية الضرورية لتوافر الإنترنت عموما وكيانات القطاع الصحي أو لسلامتهما. وفي النزاعات المستقبلية، يمكن أن تكون هذه الأنشطة الخبيثة أكثر تدميرا وتؤثر بصورة جسيمة على رفاه الناس وحياتهم. وبهذا المعنى، يمكن أن تتضرر البلدان تضررا كبيرا من الهجمات السيبرانية التي تقع في سياق النزاعات المسلحة.

وخلال النزاعات المسلحة، ينبغي للدول أن تخطط وتقود وتنفذ عملياتها في الفضاء الإلكتروني، وأن تتقيد تقيدا صارما بقواعد القانون الدولي، مع إيلاء اعتبار خاص للقانون الدولي في مجال حقوق الإنسان والقانون الدولي الإنساني.

وتؤيد شيلي بقوة عمل فريق الخبراء الحكوميين وتقاريره وتوصياته المعتمدة في الأعوام 2010 و 2013 و 2015 و 2021، لأنها تمثل تقدما هائلا فيما يتعلق بالقانون الدولي والمعايير وتدابير بناء الثقة في مجال تكنولوجيا المعلومات والاتصالات. وتؤيد شيلي أيضا عمل الفريق العامل المفتوح العضوية وتوصياته. وللحد من الاستخدام الخبيث للقدرات السيبرانية وبناء فضاء إلكتروني أكثر استقرارا، من المهم اتباع هذه التوصيات وتنفيذها، على جميع المستويات.

إن برنامج العمل الرامي إلى الارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني مبادرة إيجابية وبناءة وواقعية يمكن أن تساعدنا على المضي قدما وتحقيق نتائج ملموسة في إطار بيئة تكنولوجيا المعلومات والاتصالات. ويمكن أن يكون برنامج العمل أداة دولية دائمة وشاملة وقائمة على توافق الآراء وعملية المنحى للارتقاء بالسلوك المسؤول في استخدام تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي. وترى شيلي، باعتبارها أحد المشاركين في رعاية هذه المبادرة، أن برنامج العمل سيوفر منبرا لاعتماد توصيات تنفيذية، وتوثيق التعاون الدولي، وتعزيز برامج المساعدة المصممة خصيصا لتلبية احتياجات الدول المستفيدة، ولا سيما في مجال بناء القدرات.

وفيما يتعلق بالامتثال للقانون الدولي الساري وتنفيذ معايير سلوك الدول المسؤول في الفضاء الإلكتروني، من المهم أن تتمكن الدول من بلورة وجهات نظرها وتبادلها مع الدول الأخرى بشأن كيفية تطبيق القانون الدولي في الفضاء الإلكتروني. ويكتسي أيضا بناء القدرات في هذا المجال أهمية بالغة. ويشكل وجود مبادئ توجيهية لتنفيذ المعايير خطوة هامة ينبغي أن تساعد الدول على إحراز تقدم في معالجة هذه المسألة. ويمكن للمنظمات الإقليمية أن تؤدي دورا رئيسيا في مساعدة الدول على تنفيذ المعايير والامتثال للقانون الدولي، ووضع استراتيجيات إقليمية في هذا الصدد، فضلا عن التدريب وبناء القدرات.

وترى شيلي أن هذا الأمر أساسي لتعزيز تدابير بناء الثقة في الفضاء الإلكتروني وبناء القدرات التي يجب أن تضطلع المنظمات الإقليمية بدور رئيسي فيها. وفي هذا الصدد، يجدر بنا تسليط الضوء على العمل الذي تقوم به منظمة الدول الأمريكية من خلال فريقها العامل المعني بالتعاون وتدابير بناء الثقة في الفضاء الإلكتروني، وكذلك على الأعمال التي أنجزتها منظمة الأمن والتعاون في أوروبا ورابطة أمم جنوب شرق آسيا وما أحرزتاه من تقدم.

ومن المهم تعزيز الحوار بين المناطق بشأن هذه المسألة، ولكن أيضا في بناء القدرات أو تنفيذ المعايير. وينبغي أن ينظر هذا الحوار في تبادل الخبرات والمعلومات والمبادئ التوجيهية وأفضل الممارسات والدروس المستفادة ودعوة أعضاء المنظمات إلى المشاركة في هذه العمليات الإقليمية. وينبغي للدول أن تعزز جهات الاتصال الوطنية، فضلا عن دور وزارات خارجيتها فيما يتعلق بالسياسات المتصلة بالفضاء الإلكتروني وتكنولوجيا المعلومات والاتصالات. فالدبلوماسية السيبرانية أداة هامة يمكن أن تساعد الدول على تحسين التعاون فيما بينها وعلى بناء الثقة. وينبغي للدول أيضا أن تنظر في إنشاء آليات ثنائية للحوار والتعاون بشأن الأمن السيبراني والفضاء الإلكتروني.

وتعتقد شيلي أن العمليات المتعددة الأطراف يجب أن تتسم بالشمولية والشفافية قدر الإمكان. وينبغي أن تشمل المناقشة المتعلقة بتكنولوجيا المعلومات والاتصالات مجموعة من الأطراف منها القطاع الخاص، والأوساط الأكاديمية، والمجتمع المدني، وقطاع الصناعة، والدوائر التقنية. ولا يمكن بناء بيئة مستقرة وآمنة في الفضاء الإلكتروني إذا لم نضمن مشاركة جميع الجهات صاحبة المصلحة وتدخلاتها. فكلما زاد عدد الجهات الفاعلة التي تشارك في المناقشة، زاد احتمال تحقيقنا لنتائج تعود بالفائدة على الجميع. وفي هذا الشأن، نعتقد أنه من الضروري أن نستمع إلى جميع الأطراف المهتمة وأن يتسنى لها أيضا عرض آرائها ومساهماتها في الجلسات الرسمية. وبهذا المعنى، ينبغي للدول أن تشرك جميع الجهات صاحبة المصلحة عندما يتعلق الأمر ببلورة سياسات واستراتيجيات ومبادرات أخرى تهدف إلى منع نشوب النزاعات، وبناء تفاهمات مشتركة، وزيادة القدرة على الصمود في وجه التهديدات السيبرانية.

المرفق الخامس والعشرون

بيان البعثة الدائمة للجمهورية التشيكية لدى الأمم المتحدة

تود الجمهورية التشيكية أن تعرب عن تقديرها لجمهورية إستونيا لتنظيمها أول مناقشة مفتوحة تاريخيا لمجلس الأمن بشأن موضوع الأمن المعلوماتي في سياق السلام والأمن الدوليين. إن التزام الدول بالقانون الدولي وسلوك الدول المسؤول في الفضاء الإلكتروني عنصران رئيسيان لمنع نشوب النزاعات وصون السلام والأمن الدوليين.

وتؤيد الجمهورية التشيكية البيان الذي قدمه الاتحاد الأوروبي، وتود أن تؤكد على نقطتين إضافيتين على النحو التالي:

الأخطار السيبرانية الحالية والناشئة التي تهدد السلام والأمن الدوليين

يوفر الفضاء الإلكتروني فوائد هائلة للتنمية البشرية والاقتصادية ولكنه أصبح أيضا مجالا لزيادة عوامل التبعية والتحديات الأمنية. إن اعتمادنا المتزايد على تكنولوجيا المعلومات والاتصالات خلال جائحة مرض فيروس كورونا (كوفيد-19)، التي تستغلها باستمرار الجهات الفاعلة الخبيثة لمصلحتها الخاصة، هو تذكير واضح بالتحديات المتزايدة في الفضاء الإلكتروني. ومن الجدير بالذكر أننا شهدنا زيادة مثيرة للقلق في أنشطة تكنولوجيا المعلومات والاتصالات الخبيثة الموجهة ضد الهياكل الأساسية الحيوية التي تقدم الخدمات الأساسية للجمهور، بما في ذلك تلك التي تستهدف المرافق الطبية والمياه والطاقة والصرف الصحي والهياكل الأساسية الانتخابية والتوافر العام للإنترنت. وعلى وجه الخصوص، فإن العدد المتزايد من الهجمات السيبرانية التي تعطل توفير الرعاية الصحية يؤدي إلى مزيد من الخسائر في الأرواح، ويقوض قدرتنا الجماعية على الاستجابة لمرض فيروس كورونا (كوفيد-19)، ويهدد في نهاية المطاف السلام والاستقرار الدوليين.

كما أن أنشطة تكنولوجيا المعلومات والاتصالات المتهورة التي تهدف إلى إلحاق الضرر المتعمد بالهياكل الأساسية الحيوية تنطوي أيضا على مخاطر قد تكون لها عواقب إنسانية مدمرة، وإذا ما نسبت إلى دولة ما، فإنها تنتهك التزامات الدول بموجب القانون الدولي. ولذلك ترحب الجمهورية التشيكية بأن جميع الدول الأعضاء قد أكدت مؤخرا، من خلال التقريرين النهائيين لفريق الخبراء الحكوميين والفريق العامل المفتوح العضوية، أن أنشطة تكنولوجيا المعلومات والاتصالات الموجهة ضد الهياكل الأساسية الحيوية غير مقبولة. وفي حين أن الالتزام السياسي هو الخطوة الضرورية الأولى، فإن حماية الهياكل الأساسية الحيوية من تهديدات تكنولوجيا المعلومات والاتصالات ستتطلب أيضا جهودا عملية متواصلة من المجتمع الدولي، بما في ذلك من خلال تكثيف التعاون التقني ووضع برامج ملموسة متعلقة بالفضاء الإلكتروني لبناء القدرات. ويمكن لمجلس الأمن أيضا أن يؤدي دورا حاسما بضمان أن تكون هناك عواقب لأنشطة تكنولوجيا المعلومات والاتصالات التي ترعاها الدولة الموجهة ضد الهياكل الأساسية الحيوية.

ولا تؤثر التهديدات السيبرانية الجديدة والناشئة على الأمن القومي للدول فحسب، بل تهدد أيضا رفاه الأفراد وسلامتهم بشكل متزايد. ويساور الجمهورية التشيكية قلق خاص إزاء الانقسام السياسي المتزايد بين الدول التي تدعو إلى حماية الحريات الشخصية في الفضاء الإلكتروني والدول التي تدعو إلى زيادة المراقبة التكنولوجية. وفي رأينا أن توسيع نطاق تقنيات المراقبة الجماعية التي ترعاها الدولة من خلال تكنولوجيا المعلومات والاتصالات، والإغلاق الجزئي أو الكامل للإنترنت، والرقابة الواسعة النطاق على

المحتوى، تثير شواغل خطيرة تتعلق بحقوق الإنسان. ومن الضروري اتخاذ إجراءات حازمة لحماية المواطنين من الممارسات التعسفية وغير القانونية لسلطة الدولة في الفضاء الإلكتروني. وهذه الاتجاهات، مقترنة بمخاطر محتملة مرتبطة بإدخال الذكاء الاصطناعي في مختلف جوانب حياتنا، تثير تحديات أمنية جديدة، وتهدد بتقويض الثقة في الفضاء الإلكتروني والاطمئنان له، وقد تؤدي في نهاية المطاف إلى إضعاف قدرتنا على الحفاظ على السلام والأمن الدوليين.

تعزيز الامتثال للقانون الدولي العام ومعايير السلوك المسؤول للدول

تود الجمهورية التشيكية أن تؤكد من جديد أن امتثال الدول لالتزاماتها بموجب القانون الدولي عنصر أساسي للحفاظ على فضاء إلكتروني ينعم بالحرية والسلام والاستقرار والأمن وقابلية التشغيل البيني وإمكانية الوصول إليه. وأكدت جميع الدول انطباق القانون الدولي القائم على استخدام الدول لتكنولوجيا المعلومات والاتصالات، ولا سيما من خلال التأييد العالمي لتقريري فريق الخبراء الحكوميين لعامي 2013 و 2015 في قراري الجمعية العامة 243/68 و 237/70.

وفي هذا الصدد، تذكر الجمهورية التشيكية أيضا بأن حقوق الدول في ممارسة الولاية الحصرية على تكنولوجيا المعلومات والاتصالات الموجودة على أراضيها لا تنشأ عنها حقوق فحسب، بل التزامات محددة بموجب القانون الدولي أيضا. وتود الجمهورية التشيكية، على وجه الخصوص، أن تكرر التأكيد على أن الهيئات القانونية القائمة، بما في ذلك القانون الدولي الإنساني والقانون الدولي لحقوق الإنسان، تنطبق على سلوك الدول في الفضاء الإلكتروني دون استثناء.

ومما يؤسف له أن أقلية صغيرة من الدول لا تزال تشكك في إمكانية تطبيق القانون الدولي القائم على الفضاء الإلكتروني، بما في ذلك إمكانية تطبيق القانون الدولي الإنساني على استخدام تكنولوجيا المعلومات والاتصالات في سياق النزاع المسلح. وتود الجمهورية التشيكية أن تؤكد أن إمكانية تطبيق القانون الدولي الإنساني على عمليات تكنولوجيا المعلومات والاتصالات لا تشجع، في رأيها، على عسكرة الفضاء الإلكتروني، كما أنها لا تشجع على عسكرة أي مجال آخر. بل على العكس من ذلك، يفرض القانون الدولي الإنساني قيودا على استخدام القوة من خلال اشتراط استخدام جميع وسائل الحرب وأساليبها المستعملة في سياق النزاع المسلح وفقا لقواعده؛ بما في ذلك مبادئ الإنسانية والتمييز وقاعدة التناسب.

وبالإضافة إلى ذلك، تذكّر الجمهورية التشيكية بأن قانون المسؤولية عن الأفعال غير المشروعة الدولية ينص على أن جميع الدول ملزمة بممارسة العناية الواجبة وباتخاذ تدابير ملموسة في حدود قدرتها على ضمان عدم استخدام أراضيها في القيام بأنشطة سيبرانية خبيثة ضد دول أخرى.

وتسلم الجمهورية التشيكية بنفس القدر بأن قدرة الدولة على تنفيذ الإطار القائم لسلوك الدولة المسؤولة في الفضاء الإلكتروني، بما في ذلك قدرتها على ممارسة العناية الواجبة على نحو كاف، ترتبط ارتباطا جوهريا بقدرات تلك الدولة. وفي هذا الصدد، تشدد الجمهورية التشيكية على ضرورة تكثيف الجهود الدولية الرامية إلى بناء القدرات السيبرانية وزيادة قدرة النظم السيبرانية على الصمود على الصعيد العالمي، بما في ذلك من خلال الإسراع بإنشاء برنامج عمل الأمم المتحدة لسلوك الدول المسؤول في الفضاء الإلكتروني، مما سيسمح للدول الأعضاء بالنهوض بتنفيذ الالتزامات القائمة من خلال إجراءات عملية وموجهة نحو تحقيق النتائج.

وفي الختام، تلتزم الجمهورية التشـــيكية التزاما كاملا باتباع نهج يركز على الإنســـان إزاء الأمن السـيبراني يؤكد على ضـرورة حماية سـلامة وأمن الأفراد في بيئة تكنولوجيا المعلومات والاتصـالات، وذلك من خلال حماية الهياكل الأسـاسـية الحيوية من تهديدات تكنولوجيا المعلومات والاتصـالات، أو من خلال ضـمان عدم اسـتخدام تدابير الأمن السـيبراني كذريعة لتضـييق التمتع الكامل بحقوق الإنسـان والحريات الأساسية في الفضاء الإلكتروني.

المرفق السادس والعشرون

بيان مشترك صادر عن البعثات الدائمة لآيسلندا والدانمرك والسويد وفنلندا والنرويج لدى الأمم المتحدة

يسرني أن أتكلم باسم بلدان الشمال الأوروبي، وهي آيسلندا والسويد وفنلندا والنرويج وبلدي، الدانمرك. ونحن ممتنون للرئاسة الإستونية على إدراج هذا الموضوع الهام جدا على جدول أعمال المجلس. وإنها فرصة عظيمة لجميع الدول الأعضاء من أجل البناء على التزامنا بتطبيق القانون الدولي في الفضاء الإلكتروني وإطار السلوك المسؤول للدول في الفضاء الإلكتروني بهدف تعزيز السلام والاستقرار.

ويستفيد العالم بطرق لا حصر لها من تطوير تكنولوجيا المعلومات والاتصالات. وقد حقق تقدما اقتصاديا هائلا وتنمية مجتمعية كبيرة. وفي ظل الجائحة الحالية، سمح الفضاء الإلكتروني للكثيرين منا بالبقاء على اتصال بالعائلة والأصدقاء والزملاء والحفاظ على وظائف هامة لتسيير شؤون المجتمع، بما في ذلك تشغيل الهياكل الأساسية الحيوية الضرورية لإدارة الأزمة الصحية. ومع ذلك، فقد استخدم الفضاء الإلكتروني أيضا لنشر معلومات مضللة عن فيروس مرض كورونا (كوفيد-19)، مما يعرض للخطر مناعتنا الجماعية إزاء الآثار المعطلة والاستغلال المسيء لمجال المعلومات. وعلاوة على ذلك، كشفت الجائحة عن انقسامات رقمية عميقة، ليس أقلها الفجوة الرقمية بين الجنسين. ونحن، بلدان الشمال الأوروبي، نؤمن إيمانا قويا بأن الفضاء الإلكتروني الذي يمكن الوصول إليه عالميا ويتسم بالحرية والانفتاح والأمن أمر أساسي ليس فقط لكيفية عمل العالم اليوم، ولكن لطموحاتنا المشتركة نحو بناء مستقبل أفضل وأكثر مراعاة للبيئة وأكثر أمانا.

ولسوء الحظ، لا تزال الأنشطة السيبرانية الخبيثة تتحدى سلامة الفضاء الإلكتروني واستقراره. وقد كشفت السنة ونصف السنة الأخيرة أن الجهات الفاعلة من الدول وغير الدول سوف تستغل أي فرصة، حتى لو كانت جائحة عالمية، للقيام بأنشطة خبيثة في الفضاء الإلكتروني. وهي أنشطة غير مقبولة. فهي تهدد سلامة مجتمعاتنا وأمنها وازدهارها، وتقوض السلام والاستقرار الدوليين.

واسمحوا لي أن أبرز ثلاثة اتجاهات مترابطة تشكل تحديا للسلام والأمن الدوليين.

أولا، إن الزيادة الأخيرة في الهجمات السيبرانية ضد سلاسل الإمداد للشركات والمنظمات والحكومات قد تركت عشرات إن لم يكن مئات الآلاف من الأنظمة الحاسوبية مكشوفة. وتظهر هذه الهجمات تجاهلا صارخا للمتضررين. والهدف من ذلك هو في كثير من الأحيان سرقة المعلومات الحساسة والملكية الفكرية للحصول على ميزة في المنافسة الجيوسياسية. وقد تكون لهذه الهجمات آثار إضافية غير مقصودة حيث تُترك الأبواب الخلفية مفتوحة للجميع لاستغلالها.

ثانيا، أطلقت هجمات سيبرانية تخريبية ترعاها الدول من قبيل "ونا كراي" (WannaCry) و "نوتبتيا" (NotPetya) على العالم مع عدم اكتراث كامل بآثارها المنهجية السلبية في جميع أنحاء العالم. ولم تسفر هذه الهجمات عن خسائر مالية فادحة فحسب، بل شلت أيضا نظم تكنولوجيا المعلومات والاتصالات، بما في ذلك في المستشفيات ونظم المراقبة الصناعية التي تؤثر على إمدادات الكهرباء الحيوية. وتعرض هذه الأنشطة صحة مواطنينا وسلامتهم للخطر.

ثالثا، يتعين على الدول أن تتخذ إجراءات ضد الآثار المتزايدة الخطورة والمزعزعة للاستقرار المترتبة على الجريمة السيبرانية الناشئة من أراضيها. وتوضح الهجمات الأخيرة لبرامج فيروسات الفدية ضد إمدادات الوقود في الولايات المتحدة والمستشفيات في أيرلندا وإنتاج الأغذية في البرازيل والولايات المتحدة وأستراليا أن عواقب الجريمة السيبرانية أصبحت مصدر قلق للأمن الوطني مع ما قد يترتب على ذلك من آثار على السلام والأمن الدوليين. ويزيد الخلط المتزايد بين الجماعات التابعة للدول وغير التابعة لها من تعقيدات التهديد.

ويوما بعد يوم، تسير عتبة السلوك المقبول في الفضاء الإلكتروني في الاتجاه الخاطئ. ويجب أن نعود إلى هذا الاتجاه بالوفاء بالالتزام المشترك الذي قطعناه نحن، الدول الأعضاء، عندما أيدنا تقارير فريق الخبراء الحكوميين وتقرير الفريق العامل المفتوح العضوية بتوافق الآراء. وانطلاقا من هذه الروح، نؤكد من جديد على أن القانون الدولي، بما في ذلك ميثاق الأمم المتحدة في مجمله، والقانون الدولي الإنساني والقانون الدولي لحقوق الإنسان، ينطبق على سلوك الدول في الفضاء الإلكتروني. وندعو أيضا إلى الالتزام بقوة أكبر بالمعايير الطوعية الـ 11 غير الملزمة لسلوك الدول المسؤول في الفضاء الإلكتروني الواردة في تقرير فريق الخبراء الحكوميين لعام 2015 مع الأخذ في الاعتبار التوجيهات والطبقة الإضافية من الفهم لهذه المعايير، التي قدمت في تقرير فريق الخبراء الحكوميين لعام 2021. وهذا من شأنه أن يحقق الكثير في التصدي للتحديات المذكورة أعلاه.

ويجب علينا أن نرفع تكلفة النشاط السيبراني الخبيث من خلال محاسبة المسؤولين بشكل جماعي. ويجب على الدول أن تبذل العناية الواجبة وأن تتخذ إجراءات ملائمة من أجل التصدي للأنشطة السيبرانية الشريرة التي تنطلق من أراضيها. وينبغي عدم السماح لمجموعات القراصنة بالعمل دون عقاب.

وندعم مواصلة تبادل المعلومات والممارسات الفضلى في إطار الأمم المتحدة، لا سيما بشأن تنفيذ معايير سلوك الدولة المسؤول، وتدابير بناء الثقة وتطبيق القانون الدولي القائم في الفضاء الإلكتروني. وينبغي أن نتتبع مسارا عملي المنحى يستند إلى إطار توافق الآراء الذي اتفقنا عليه بالفعل بموافقة الجمعية العامة على تقرير الفريق العامل المفتوح العضوية وتقارير فريق الخبراء الحكوميين. ويشكل ذلك الأساس لأي نقاش آخر. واقتراح وضع برنامج عمل هو وسيلة جيدة للتحرك نحو التنفيذ الكامل للقواعد المتفق عليها بالفعل.

ويجب أن نعترف بأنه في حين أن التهديد السيبراني يشكل تحديا عالميا، فإن له مظاهر مختلفة باختلاف البلدان والمناطق. والتمسك بقدرة النظم السيبرانية القوية على الصمود في جميع مجتمعاتنا أمر بالغ الأهمية ليس لأمننا المشترك فحسب، بل من أجل التمتع بحقوق الإنسان أيضا. وعلينا أن نتعاون لبناء القدرات على الصعيد العالمي.

ولا تستطيع الدول أن تفعل ذلك بمفردها. وتتطلب مواجهة التهديدات في الفضاء الإلكتروني اتباع نهج متعدد أصحاب المصلحة للمساعدة في منع نشوب النزاعات وبناء فهم مشترك وزيادة الثقة وبناء القدرات. ونحن بحاجة إلى الأمم المتحدة بوصفها جهة منظمة للاجتماعات ومنتدى لإقامة تعاون فعال بين الحكومات والمجتمع المدني والأوساط الأكاديمية والقطاع الخاص. ونحن نؤيد خريطة الطريق من أجل التعاون الرقمي التي وضعها الأمين العام، ولا سيما عندما يتعلق الأمر بمشاركة القطاع الخاص، وهو أمر حيوي في إدارة الهياكل الأساسية الحيوية، وجمع المعلومات وحماية النظم والبيانات الشخصية.

ويجب على جميع الدول أن تفي بمسؤولياتها وأن تمتثل للقانون الدولي وأن تحترم المعايير في الفضاء الإلكتروني. وإذا لم يكن الأمر كذلك، فإن التهديد الناجم عن النشاط السيبراني الخبيث على السلام والأمن الدوليين سوف يستمر في التزايد. وستستمر الهجمات السيبرانية في تعزيز خطر نشوب النزاعات، وتعريض حياة البشر للخطر، وانتهاك حقوق الإنسان، وخنق النشاط الاقتصادي، وتعميق الخطوط الفاصلة، والتسبب في النزاعات. ولجميع الدول دور تؤديه في مجالي تعزيز ودعم الفضاء الإلكتروني القائم على القواعد والذي يمكن التنبؤ به، والمتسم بالانفتاح والمساواة والحرية، والذي يمكن الوصول إليه ويوفر الاستقرار والأمن لصالح الجميع.

المرفق السابع والعشرون

بيان الممثل الدائم لإكوادور لدى الأمم المتحدة، كريستيان إسبينوزا

[الأصل: بالإسبانية]

اسمحوا لي أولا وقبل كل شيء أن أشكر إستونيا على إدراج هذا البند في جدول الأعمال الرسمي لمجلس الأمن بعد عام من الاجتماع المعقود بصيغة آريا بشأن هذا الموضوع. ونلاحظ أيضا قيادة رئيس الوزراء كالاس في هذا المجال، ونرحب بالعرض الذي قدمته وكيلة الأمين العام والممثلة السامية لشؤون نزع السلاح إيزومي ناكاميتسو.

وشكلت فترة السنتين 2020-2021 معلما بارزا في مجال الدبلوماسية السيبرانية ليس فقط بسبب الولاية والنتائج الموضوعية التي حققها في 12 آذار/مارس 2021 الفريقُ العامل الأول المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، والتوافق الذي توصل إليه في 28 أيار/مايو فريقُ الخبراء الحكوميين المعني بسلوك الدول المسؤول في الفضاء الإلكتروني، ولكن أيضا بسبب جائحة مرض فيروس كورونا (كوفيد-19) التي عجلت بالتحول الرقمي.

وكان للجائحة أثر على جميع أبعاد السلام والأمن بطرق مختلفة. ولم يكن الأمن السيبراني استثناء. وأصبح أمن الخدمات الأساسية مصدر قلق كبير، إلى جانب الحاجة إلى الحفاظ على الهياكل الأساسية الحيوية ضد الهجمات السيبرانية المحتملة التي يمكن أن تسبب أضرارا في العالم المادي.

إن التهديدات التي نواجهها اليوم هي في معظمها تهديدات عبر وطنية، والطريقة الوحيدة لمواجهتها، سواء في العالم المادي أو الافتراضي، هي من خلال التعاون والحوار الدوليين. وبالتالي، إذا لم تكن دولة عضو واحدة آمنة، فلا توجد دولة آمنة.

ولذلك تؤكد إكوادور من جديد التزامها بالقواعد السارية، كما يتبين من تقارير فريق الخبراء الحكوميين ونتائج الفريق العامل المفتوح العضوية، وفقا للقانون الدولي. ويود وفد بلدي أن يؤكد أنه لا يمكن أن يبقى أي مجال خارج نطاق القانون الدولي، بما في ذلك القانون الدولي لحقوق الإنسان والقانون الدولي الإنساني، وهذا لا يعني أن عسكرة الفضاء الإلكتروني ستكون مقبولة.

بل على العكس من ذلك، تدافع إكوادور عن الاستخدام السلمي الحصري للفضاء الإلكتروني. ويحظر ميثاق الأمم المتحدة استخدام القوة، ولذلك ينبغي تسوية جميع المنازعات الدولية في الفضاء الإلكتروني بالوسائل السلمية.

وبناء عليه، فإننا نعزز الثقة وبناء القدرات، ونعتقد أن ذلك يقتضي وجود منتدى تشغيلي لتيسير تنفيذ الدول للإطار القائم. ويمكن أن يتخذ هذا المنتدى شكل برنامج عمل.

وندافع عن أي آلية تعزز زيادة التعاون الدولي للحد من الاختلالات في القدرة على تنفيذ معايير السلوك المسؤول للدول، وندعم هذه الآلية.

وبالإضافة إلى ذلك، نعترف بالمساهمة التي يمكن للمنظمات الإقليمية أن تقدمها لتنمية القدرات وتنفيذ هذه المعايير. ومن الأمثلة على ذلك العمل القيّم الذي تقوم به منظمة الدول الأمريكية في هذا المجال، ولا سيما جهودها الرامية إلى مكافحة الجريمة السيبرانية والإرهاب.

وأختتم بياني بتذكر الحاجة إلى الحفاظ على الاستخدام المسؤول لتكنولوجيا المعلومات والاتصالات وتعزيزه بصفته ضمانا رئيسيا للاستقرار والأمن في الفضاء الإلكتروني. وبالمثل، نعتقد أنه ينبغي تعزيز المعايير القائمة، مع مراعاة التطور التكنولوجي السريع. ويجب على مجلس الأمن، من جانبه، أن ينظر في آليات لتعزيز استخدام التكنولوجيات بوصفها وسيلة لتعزيز السلام وعنصرا مكملا للجهود المنتظمة.

وشكرا لكم.

المرفق الثامن والعشرون

بيان البعثة الدائمة لمصر لدى الأمم المتحدة

تولي مصـــر أهمية كبيرة للجوانب الأمنية الدولية لتكنولوجيا المعلومات والاتصـــالات، وتدعو بقوة إلى أن تضـــطلع الأمم المتحدة بدور مركزي وقيادي في تعزيز وتطوير القواعد والمبادئ المتعلقة باســـتخدام الدول لتكنولوجيا المعلومات والاتصالات من خلال عملية منصفة وشاملة للجميع بمشاركة جميع الدول.

ويطور عدد من الدول قدرات تكنولوجيا المعلومات والاتصـــالات لاســـتخدامات خبيثة محتملة ولأغراض عسكرية هجومية. وأصبح استخدام تكنولوجيا المعلومات والاتصالات في النزاعات المستقبلية بين الدول حقيقة واقعة، ويشكل خطر وقوع هجمات تكنولوجيا معلومات واتصالات ضارة على الهياكل الأساسية الحيوية تهديدا حقيقيا وخطيرا على حد سواء. ويترتب على سباق التسلح الجديد هذا تداعيات بعيدة المدى على السلام والأمن والاستقرار الدوليين، خاصة وأن الخطوط الفاصلة بين الأسلحة التقليدية وغير التقليدية لا تزال تتآكل.

وعلاوة على ذلك، فإن التكنولوجيات ذات الصلة التي تطورها الدول يجري نقلها أو نسخها أو إعادة إنتاجها من قبل الإرهابيين والمجرمين. ويشـكل الاسـتخدام الخبيث لتكنولوجيا المعلومات والاتصـالات من جانب المنظمات الإرهابية والإجرامية تهديدا خطيرا للســلام والأمن الدوليين، لا ســيما في ضــوء التحديات المتصلة بإسناد المسؤولية.

وبموجب القانون الدولي وميثاق الأمم المتحدة، ينبغي أن تمتنع جميع الدول الأعضـــاء عن القيام بأي عمل يلحق ضررا باستخدام وتشغيل الهياكل الأساسية الحيوية للدول الأخرى، أو يعوق ذلك بأي شكل آخر، عن علم أو قصد، فضلا عن التدخل في شؤونها الداخلية.

ولا شك في أن الجوانب الأمنية الدولية لتكنولوجيا المعلومات والاتصـالات قد أصـبحت ذات أهمية واســتراتيجية كبيرتين بحيث لا يمكن تركها دون قواعد ملزمة واضــحة على الصــعيد الدولي. ويعد اســتخدام عملية شاملة للجميع داخل منظومة الأمم المتحدة أفضل الطرق وأكثرها كفاءة لوضع ترتيبات منصفة وشاملة وفعالة في هذا المجال.

وقد اتخذت الأمم المتحدة بالفعل بعض الخطوات نحو إنشـــاء إطار معياري يكمل مبادئ القانون الدولي. وباعتماد التقرير النهائي للفريق العامل المفتوح العضـــوية الذي أنشـــئ عملا بقرار الجمعية العامة 27/73 بشـأن التطورات في ميدان المعلومات والاتصـالات السـلكية واللاسـلكية في سـياق الأمن الدولي، بتوافق الآراء مؤخرا، وضـــعت الأمم المتحدة بالفعل العناصـــر الأولية لإطار منع نشـــوب النزاعات وتحقيق الاستقرار في الفضاء الإلكتروني.

ودعت الجمعية العامة الدول الأعضـــاء إلى أن تســـترشـــد في اســـتخدامها لتكنولوجيا المعلومات والاتصـــالات بمعايير الســـلوك المســـؤول للدول الواردة في التقارير المتتالية لأفرقة الخبراء الحكوميين التابعة للجنة الأولى. غير أن تنفيذ هذه المعايير المتواضـعة لا يزال ضـئيلا جدا في أحسـن الأحوال، وذلك بسـبب طابعها الطوعي وعدم وجود أي آلية للمتابعة.

ويمثل نجاح الفريق العامل المفتوح العضـــوية، الذي يعد أول عملية شـــاملة للجميع بشـــأن هذا الموضـــوع الهام، وإنشـــاء فريق عامل مفتوح العضـــوية جديد بموجب قرار الجمعية العامة 240/75، تقدما

واعدا نحو التوصل إلى اتفاق ممكن بشأن التفاهمات المتبادلة الهامة بين الدول الأعضاء بشأن عدد من الجوانب الرئيسية.

وتعد العمليات الشاملة للجميع داخل الأمم المتحدة، التي تتجري أساسا تحت رعاية الجمعية العامة، هي أنجع طريقة لوضع ترتيبات منصفة وشاملة وفعالة في هذا المجال. ويُشجّع مجلس الأمن، من جانبه، على أن يأخذ في الاعتبار الفرص التي تتيحها التكنولوجيات الناشئة مع النظر في مواضيع من قبيل حفظ السلام ومكافحة الإرهاب. ومع ذلك، ينبغي ألا يستخدم المجلس كهيئة تشريعية تحاول وضع معايير وقواعد باسم الدول الأعضاء بشأن المسائل التي تتطلب بالضرورة عمليات شفافة وشاملة للجميع.

ويمكن أن تشكل التوصيات التي أقرتها الجمعية العامة بتوافق الآراء الأساس لقواعد ملزمة سياسيا أو قانونيا، لا سيما أنها مستمدة من مبادئ القانون الدولي وميثاق الأمم المتحدة.

وشجعت مصر أيضا على النظر في إنشاء منتدى مؤسسي شامل للجميع مكرس للتعاون الدولي بشأن صون الاستخدامات السلمية لتكنولوجيا المعلومات والاتصالات وتخفيف المخاطر المرتبطة بها.

وبينما نعتقد أن القانون الدولي ومبادئ الميثاق تنطبق على جميع المجالات بما في ذلك الفضاء الإلكتروني، فإننا نعتقد أيضا أن هناك حاجة ملحة لتحديد التزامات محددة تجعل سلوك الدول في الفضاء الإلكتروني متسقا مع القانون الدولي وأهداف ميثاق الأمم المتحدة.

وفي عالم يزداد ترابطا، لن تكون قوة أي نظام دولي بشأن الأمن السيبراني إلا بمقدار قوة أضعف حلقاته. ولحسن الحظ، فهناك توافق في الآراء على ضرورة تكثيف جهود بناء القدرات وتعزيزها لمنع الهجمات المحتملة على الهياكل الأساسية الحيوية وتطوير القدرات والمهارات التقنية اللازمة في البلدان النامية. وينبغي للأمم المتحدة أن تقود جهدا منسقا من أجل تقديم المساعدة اللازمة للبلدان النامية.

وفي الختام، تتيح تكنولوجيا المعلومات والاتصالات فرصا وتحديات هائلة على حد سواء. ونشدد على أن هناك حاجة ملحة إلى تحديد معايير سلوك الدول المسؤول وتطويرها من أجل زيادة الاستقرار والأمن في البيئة العالمية لتكنولوجيا المعلومات والاتصالات ومنع الفضاء الإلكتروني من أن يصبح ساحة أخرى للنزاعات وسباقات التسلح.

المرفق التاسع والعشرون

بيان البعثة الدائمة للسلفادور لدى الأمم المتحدة

[الأصل: بالإسبانية]

تشكر السلفادور وفد إستونيا بصفتها رئيسة لمجلس الأمن في حزيران/يونيه 2021 على عقد هذه المناقشة المفتوحة، وهي المرة الأولى التي يتناول فيها مجلس الأمن مسألة الأمن السيبراني بطريقة موضوعية ورسمية. وهذه المبادرة تدبير بالغ الأهمية تفي بموجبه هذه الهيئة بالالتزام الدولي بالنظر على الصعيد المتعدد الأطراف في التهديدات القائمة والمحتملة للأمن في ميدان تكنولوجيا المعلومات والاتصالات.

ويمثل استحداث تكنولوجيات جديدة فرصة مهمة لتعزيز التنمية الاقتصادية والاجتماعية للدول. غير أن نظم المعلومات تلك معرضة لهجمات الأشخاص العازمين على التلاعب بشبكات الاتصال هذه لأغراض أيديولوجية أو لمصلحتهم الخاصة. ونظرا لأن المجرمين والإرهابيين يستغلون تكنولوجيات المعلومات والاتصالات الجديدة لتحقيق أهدافهم، يجب استثمار الجهود والموارد لإعداد مبادئ توجيهية متخصصة من أجل وضع معايير مشتركة وتطبيقها كي تساعدنا على منع هذا النوع من الجرائم وتيسير تقديم أولئك الذين يعملون خارجها إلى العدالة.

ولذلك نود أن نسلط الضوء على أهمية الصكوك الدولية والإقليمية المتصلة بمكافحة الجريمة السيبرانية، وكذلك على التقدم المحرز في ذلك المجال، مثل إنشاء الفريق العامل المفتوح العضوية بغرض وضع اتفاقية دولية شاملة لمكافحة استخدام تكنولوجيات المعلومات والاتصالات لأغراض إجرامية.

ونرحب بارتياح بجهود الدول الأعضاء في الأمم المتحدة في مجال الإرهاب في إطار جدول أعمال السلام والأمن الدوليين. ومع ذلك، نلاحظ أنه لا يزال من المستحيل العثور، فيما بين الصكوك الملزمة دوليا في هذا المجال، على أي ذكر مباشر للفضاء الإلكتروني. وهذه فجوة يجب علينا جميعا سدها في أقرب وقت ممكن. ونثني على جهود مجلس الأمن لمناقشة هذا التهديد المهم مناقشة موضوعية، بغية توفير حلول فعالة. ونحث هذه الهيئة على مواصلة تلك الجهود، مع تنحية جميع المصالح السياسية و/أو الشخصية جانبا، والتمسك بهدف منع نشوب نزاعات جديدة ووضع سيناريوهات لتنمية البلد.

وتذكّر السلفادور بقرار الجمعية العامة 199/58، الذي اتخذ في عام 2004، والذي تضمن قائمة بعناصر الهياكل الأساسية الحيوية للمعلومات في الدول، التي تتعرض لعدد آخذ في التزايد والتنوع من التهديدات بسبب تزايد الترابط التكنولوجي. واعترف ذلك القرار أيضا بأن مواطن الضعف في الهياكل الأساسية الحيوية للمعلومات لا تزال تطرح مشاكل أمنية كبيرة.

وعلاوة على ذلك، وبغية تهيئة الظروف لإحراز تقدم نحو الهدف المشترك المتمثل في السلام والأمن الدوليين، والممارسة الكاملة لحقوق الإنسان والتنمية الاقتصادية والاجتماعية، نعتقد أنه ينبغي توسيع الإطار المنصوص عليه في قرار الجمعية العامة 199/58 لتلبية الحاجة إلى حماية أنشطة الهياكل الأساسية الحيوية من الهجمات السيبرانية، بالإضافة إلى الجهود المبذولة حاليا لمنع الفضاء الإلكتروني من أن يصبح منتدى للدعاية من أجل تغذية نزعة التطرف والتجنيد وجمع الأموال للأنشطة الإجرامية.

وسيواصل العالم مواجهة أحد أكبر التحديات منذ إنشاء هذه المنظمة، وهو تفشي جائحة مرض فيروس كورونا (كوفيد-19) التي كشفت عن أوجه الضعف في النظم الأساسية في الدول. وقد رأينا كيف

زادت الهجمات السيبرانية أثناء جائحة كوفيد-19 ضد النظم الصحية الوطنية، مما عرّض للخطر حياة الملايين من الناس وأثر بشكل مباشر على المجتمعات والقطاعات الأكثر ضعفا. ونود أن نغتنم هذا المنتدى لإدانة الهجمات السيبرانية ضد منظمة الصحة العالمية ومحاولات انتحال الشخصية التي وقعت في الأشهر الأخيرة. ومما لا شك فيه أن زيادة الترابط تفترض أنه يمكن رؤية زيادة في تلك الهجمات في السنوات المقبلة.

وقد امتد نطاق الاستخدام الخبيث لتكنولوجيات المعلومات والاتصالات في الأشهر الأخيرة ليشمل الهجمات السيبرانية ضد قطاعات الطاقة والمالية والإمدادات الغذائية؛ ومن بين القطاعات الأخرى، فإن تلك القطاعات معرضة بشدة للهجمات السيبرانية. وبالمثل، رأينا كيف ازدادت أنشطة التضليل بهدف التأثير على تصور المسؤولين الحكوميين والمؤسسات الحكومية، التي كثيرا ما تكون قادرة على نزع الشرعية عن عملهم، وإطلاق العنان لعدم الاستقرار والنزاع الاجتماعي.

وكل ما سبق يحتم مواصلة العمل من أجل منع الهجمات السيبرانية وتدوين القانون الدولي الرامي إلى منع استخدامها الخبيث، وهو ما يعترف بالتداخل مع القانون الدولي الإنساني المنطبق، بما في ذلك مجال العمليات السيبرانية أثناء النزاعات المسلحة.

ونشدد على أهمية العمل على أساس توافق الآراء، دون نية فرض حلول تتعارض مع واقع الدول، وكذلك ضمان مراعاة التقدم الذي أحرزته الجمعية العامة من خلال مختلف الاتفاقات التوافقية التي توصل إليها فريق الخبراء الحكوميين والفريق العامل المفتوح العضوية المعني بالتطورات في مجال المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي. ونرحب بصفة خاصة باعتماد الاتفاق الذي توصل إليه الفريق العامل المفتوح العضوية بتوافق الآراء في عام 2021، بمشاركة 193 دولة عضوا في الأمم المتحدة، بما في ذلك الـ 15 عضواً في مجلس الأمن والأطراف الأخرى ذات الصلة في العملية.

وتتوقع السلفادور أن تعمل بشكل بناء في الفريق العامل المفتوح العضوية المعني بتطوير تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي، الذي سيقوم بعمله الموضوعي في الفترة من 2021 إلى 2025، ونشيد بعمل الممثل الدائم لسنغافورة لدى الأمم المتحدة، برهان غفور، بوصفه الرئيس المعيّن للعملية.

وينبغي الإشارة إلى الدور الأساسي للمنظمات الإقليمية والقطاع الخاص والمجتمع المدني والأوساط الأكاديمية والقطاعات الأخرى ذات الصلة في منع تلك التهديدات والتصدي لها. وثمة حاجة ملحة إلى مواصلة العمل على تعزيز آليات التعاون الإقليمي والدولي لمنع تلك التحديات والتصدي لها، من خلال تبادل دينامي للمعلومات والممارسات الجيدة، وبناء القدرات، وتوحيد الأطر القانونية، واستخدام التكنولوجيات الجديدة بوصفها الطريق نحو التنمية ومكافحة الجريمة المنظمة.

المرفق الثلاثون

بيان رئيس وفد الاتحاد الأوروبي لدى الأمم المتحدة، أولوف سكوغ

يشرفني أن أسهم في المناقشة المفتوحة بشأن الأمن المعلوماتي باسم الاتحاد الأوروبي ودوله الأعضاء.

ويحظى هذا البيان بتأييد البلدان المرشحة للعضوية، تركيا وجمهورية مقدونيا الشمالية* والجبل الأسود* وألبانيا*، وبلد عملية تحقيق الاستقرار والانتساب والمرشح المحتمل البوسنة والهرسك، فضلا عن أوكرانيا وجمهورية مولدوفا.

أولا، نود أن نشيد بإستونيا لعقدها هذه المناقشة المفتوحة بشأن هذا الموضوع الحاسم، في لحظة لا تزال فيها الأنشطة السيبرانية الخبيثة في ازدياد، وتشكل التحديات المتزايدة خطرا على الأمن والاستقرار الدوليين في الفضاء الإلكتروني، ولا سيما في ظل الظروف الخاصة لهذه الجائحة.

وتؤثر الرقمنة تأثيرا متزايدا على أمننا واقتصاداتنا ومجتمعاتنا ككل، مما يتيح فرصا وتحديات على حد سواء. وتعتمد مجالات النقل والطاقة والصحة والاتصالات السلكية واللاسلكية والمالية والأمن والعملية الديمقراطية والفضاء والدفاع اعتمادا كبيرا على نظم الشبكات والمعلومات التي تزداد ترابطا.

وفي ضوء ذلك، نشعر بالجزع بوجه خاص إزاء الزيادة الأخيرة في الأنشطة السيبرانية الخبيثة التي تستهدف المشغلين الأساسيين على الصعيد العالمي، بما في ذلك في قطاع الرعاية الصحية، وتؤثر على توافر منتجات وخدمات تكنولوجيا المعلومات والاتصالات وأمنها وسلامتها، وبالتالي استمرار العمليات، التي قد تكون لها آثار جانبية ومنهجية ومخاطر معززة للنزاع.

ولذلك نرحب بفرصة مناقشة هذه المسألة الهامة في مجلس الأمن، الذي يتحمل المسؤولية الرئيسية عن صون السلام والأمن الدوليين. وهي فرصة للتأكيد على عدد من التحديات التي تواجهنا، وتكرار الإنجازات التي حققها مجتمع الأمم المتحدة حتى الآن، وتوفير نظرة عن كيفية تناول هذه المسائل داخل الأمم المتحدة.

وفي هذا الصدد، يرحب الاتحاد الأوروبي والدول الأعضاء فيه بالتقارير المفيدة التي وافق عليها بتوافق الآراء الفريقُ العامل المفتوح باب العضوية المعني بالتطورات في ميدان تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي (الفريق العامل المفتوح العضوية) وفريق الخبراء الحكوميين التابع للأمم المتحدة المعني بتعزيز سلوك الدول المسؤول في الفضاء الإلكتروني.

وتساهم التقارير إسهاما كبيرا في زيادة الوعي، وتسمح بتعزيز القدرة على منع التهديدات السيبرانية والأنشطة السيبرانية الخبيثة والتصدي لها والتعافي منها. وهذا أمر تمس الحاجة إليه، لأن نقص الوعي والقدرات يشكل تهديدا بحد ذاته، نظرا لأن جميع البلدان تعتمد بشكل متزايد على تكنولوجيا المعلومات والاتصالات.

ولذلك، فإن زيادة قدرة النظم السيبرانية على الصمود على الصعيد العالمي أمر ضروري، لأنه يقلل من قدرة الجناة المحتملين على إساءة استخدام تكنولوجيا المعلومات والاتصالات لأغراض خبيثة. ويسمح أيضا للدول بممارسة العناية الواجبة واتخاذ الإجراءات المناسبة ضد الجهات الفاعلة التي تقوم بهذه الأنشطة من أراضيها، بما يتفق مع القانون الدولي وتقارير الأعوام 2010 و 2013 و 2015 و 2021 التي أعدَّتها

* لا تزال جمهورية مقدونيا الشمالية، والجبل الأسود، وصربيا، وألبانيا جزءاً من عملية تحقيق الاستقرار والانتساب.

بتوافق الآراء أفرقة الخبراء الحكوميين التابعة للأمم المتحدة في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي.

وتوفر تقارير أفرقة الخبراء الحكوميين المتعاقبة والفريق العامل المفتوح باب العضوية خط أساس لمنع نشوب النزاعات والتعاون والاستقرار في الفضاء الإلكتروني، أي إعادة تأكيد تطبيق القانون الدولي، ومعالجة معايير سلوك الدول المسؤول، وتدابير بناء الثقة في الفضاء الإلكتروني، وبناء القدرات السيبرانية.

ويؤكد الاتحاد الأوروبي ودوله الأعضاء من جديد أن إطار منع نشوب النزاعات والتعاون والاستقرار في الفضاء الإلكتروني لا يمكن أن يقوم إلا على القانون الدولي القائم، الذي يشمل ميثاق الأمم المتحدة برمته، والقانون الدولي الإنساني، والقانون الدولي لحقوق الإنسان، على النحو الذي أقرته الجمعية العامة منذ عام 2013.

ومن شأن تعميق الفهم حول كيفية تطبيق القانون الدولي في الفضاء الإلكتروني زيادة الحد من سوء الفهم وزيادة المساءلة في الفضاء الإلكتروني، وينبغي أن تواصل الدول الأعضاء بالأمم المتحدة النهوض بهذا الإطار وتنفيذه في ضوء الأمن والاستقرار الدوليين في الفضاء الإلكتروني.

وعلى سبيل المثال، يرى الاتحاد الأوروبي والدول الأعضاء فيه أن القانون الدولي الإنساني ينطبق تماما في الفضاء الإلكتروني في سياق النزاع المسلح. ونؤكد من جديد أن تطبيقه في الفضاء الإلكتروني ينبغي ألا يساء فهمه على أنه يضفي الشرعية على أي استخدام للقوة يتعارض مع ميثاق الأمم المتحدة. ويحدد القانون الدولي الإنساني تدابير الحماية الأساسية لأولئك الذين لا يشاركون في الأعمال العدائية أو لم يعودوا يشاركون فيها بعد الآن، وذلك في جملة أمور منها حماية المدنيين من آثار الأعمال العدائية والمقاتلين من المعاناة التي لا مبرر لها، من بين أمور أخرى. ويفرض أيضا قيودا على وسائل وأساليب القتال المسموح بها، بما في ذلك الوسائل والأساليب الجديدة.

ثانيا، إن التقيد بمعايير السلوك المسؤول للدول له أهمية قصوى. إذ تجسد مجموعة المعايير المتفق عليها التوقعات المشتركة للمجتمع الدولي، التي ترسي معايير لسلوك الدول المسؤول. وهو يتيح للمجتمع الدولي تقييم أنشطة الدول ونواياها من أجل منع نشوب النزاعات وزيادة الاستقرار والأمن في الفضاء الإلكتروني.

ثالثا، تشكل تدابير بناء الثقة المتعلقة بالفضاء الإلكتروني وسيلة عملية لمنع نشوب النزاعات. ومن خلال التعاون وتبادل المعلومات، أثبتت تدابير بناء الثقة على الصعيد الإقليمي أنها تقلل من خطر سوء التفسير والتصعيد والنزاع الذي قد ينشأ عن حوادث تكنولوجيا المعلومات والاتصالات.

وأخيرا، يتضمن الإطار المسألة الهامة التي تتعلق ببناء القدرات. ونؤيد بشدة الدعوة إلى تحسين التنسيق من أجل تعزيز الاتساق في جهود بناء القدرات في استخدام تكنولوجيا المعلومات والاتصالات لسد الفجوة الرقمية، بما في ذلك جهودنا العديدة مع الشركاء في جميع أنحاء العالم.

ويدعم الاتحاد الأوروبي أعمال بناء القدرات السيبرانية من خلال أدوات التمويل الخارجي التي تشمل مجموعة من البرامج ذات النطاق العالمي، بما في ذلك الإجراءات المنفذة في أفريقيا وآسيا وأمريكا اللاتينية، فضلا عن جوار الاتحاد الأوروبي وغرب البلقان. ومن الناحية العملية، يستثمر الاتحاد الأوروبي حاليا في الأنشطة في جميع أنحاء العالم، لدعم التنفيذ بالتعاون مع شركائه المنفذين، من خلال مشاريع مثل مبادرة الاتحاد الأوروبي لتعزيز قدرة النظم السيبرانية على الصمود من أجل التنمية، ومبادرة الاجراءات

العالمية الموسعة المعنية بالجريمة السيبرانية (غلاسي+)، ومبادرة الاتحاد الأوروبي السيبرانية المباشرة، ومبادرة الأمن المعزز في آسيا وبالتضامن معها.

ومن أجل التأكيد على إطار منع نشوب النزاعات والتعاون والاستقرار في الفضاء الإلكتروني، سيواصل الاتحاد الأوروبي تعزيز السلوك المسؤول في الفضاء الإلكتروني. وفي ضوء ذلك، يلتزم الاتحاد الأوروبي ودوله الأعضاء بتسوية المنازعات الدولية بالوسائل السلمية أيضا عندما تنشأ مثل هذه المنازعات في الفضاء الإلكتروني.

ولذلك، فإن إطار الاستجابة الدبلوماسية المشتركة للاتحاد الأوروبي هو جزء من نهج الاتحاد الأوروبي إزاء الدبلوماسية السيبرانية، التي تسهم في منع نشوب النزاعات، والتخفيف من تهديدات الأمن السيبراني، وتحقيق استقرار أكبر في العلاقات الدولية. ومن أجل تعزيز فضاء إلكتروني مفتوح وحر ومستقر وآمن وحمايته، سيواصل الاتحاد الأوروبي استخدام مجموعة أدواته الخاصة بالدبلوماسية السيبرانية، والتعاون مع الشركاء الدوليين لتحقيق هذه الغاية.

ومنذ البداية، ونظرا للطابع المعقد للفضاء الإلكتروني، فمن الأهمية بمكان أن تتصدى الدول والمجتمع المتعدد أصحاب المصلحة للتحديات التي يجلبها الفضاء الإلكتروني، وأن تحسِّن التعاون فيما بينها وتعزز قدراتها. وتقع على عاتقنا أيضا مسؤولية أساسية لتمكين جميع أصحاب المصلحة من تحمل مسؤوليتهم عن النهوض بفضاء إلكتروني مفتوح وحر وآمن ومستقر، يقوم على حقوق الإنسان والحريات الأساسية والديمقراطية وسيادة القانون، ودعم جهودهم. ويأخذ نهج الاتحاد الأوروبي إزاء الدبلوماسية السيبرانية في الاعتبار أيضا أهمية المنظورات الجنسانية في الحد من "الفجوة الرقمية بين الجنسين" وتعزيز المشاركة الفعالة والهادفة للمرأة في عمليات صنع القرار المتصلة باستخدام تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي.

ومن أجل تعزيز التعاون، نرى أن للأمم المتحدة دورا مركزيا في دفع تنفيذ الإنجازات حتى الآن. ولتشجيع إجراء مناقشة فعالة متعددة الأطراف بين أصحاب المصلحة المتعددين من أجل تعزيز السلام والأمن في الفضاء الإلكتروني، هناك حاجة واضحة إلى المضي قدما بإطار الأمم المتحدة لسلوك الدول المسؤول في الفضاء الإلكتروني. ويقترح الاتحاد الأوروبي، إلى جانب 53 دولة عضوا، وضع برنامج عمل لتعزيز سلوك الدول المسؤول في الفضاء الإلكتروني.

واستنادا إلى التشريعات القائمة التي أقرتها الجمعية العامة، يوفر برنامج العمل منبرا دائما للتعاون وتبادل أفضل الممارسات داخل الأمم المتحدة. ويتيح برنامج العمل الفرصة لتعزيز برامج بناء القدرات المصممة خصيصا لتلبية الاحتياجات التي تحددها الدول المستفيدة. ويوفر أيضا آلية مؤسسية داخل الأمم المتحدة لتحسين التعاون مع أصحاب المصلحة الآخرين من قبيل القطاع الخاص والأوساط الأكاديمية والمجتمع المدني بشأن مسؤوليات كل منها في الحفاظ على بيئة مفتوحة وحرة وآمنة ومستقرة ومتاحة وسلمية لتكنولوجيا المعلومات والاتصالات.

ونظرا للطابع الدائم والعملي المنحى لهذا المنتدى، نعتقد أن اقتراح برنامج العمل قد حان أوانه ويستحق مزيدا من البحث من جانب المجتمع الدولي. وهو يشكل أساسا متينا وعملي المنحى لمواصلة العمل بشأن إطار منع نشوب النزاعات والتعاون والاستقرار في الفضاء الإلكتروني وضمان قدرة الدول على جني ثمار فضاء إلكتروني عالمي مفتوح ومستقر وآمن.

المرفق الحادي والثلاثون

بيان البعثة الدائمة لجورجيا لدى الأمم المتحدة

أود أن أعرب عن امتناني لرئاسة إستونيا لعقدها مناقشة اليوم الرفيعة المستوى بشأن هذه المسألة الهامة، وأن أشكر المتكلمين الموقرين.

وتلتزم جورجيا منذ فترة طويلة بتوفير فضاء إلكتروني يتحلى بالمسؤولية والأخلاق، بما في ذلك الأمن السيبراني وقدرة النظم السيبرانية على الصمود، من أجل تمكين الأطر الشاملة اللازمة لبيئة رقمية آمنة وموثوقة ويمكن الاطمئنان إليها لصالح الأمة بأسرها. وفي العقد الماضي، أنشأنا القاعدة القانونية الضرورية للمعلومات والأمن السيبراني وحددنا مواضيع حاسمة لنظم المعلومات؛ واعتمدنا ونفذنا استراتيجيتين للأمن السيبراني مع خطط عمل ذات صلة؛ وعملية الاعتماد جارية بالنسبة للاستراتيجية الوطنية الثالثة للأمن السيبراني.

ومع ذلك، وكما نعلم جميعا، يجلب الفضاء الإلكتروني أنواعا جديدة من التهديدات الأمنية إلى جانب الفرص الاقتصادية والاجتماعية الكبرى، والابتكار والتنمية. وفي السنوات الأخيرة شهدنا استخدام الفضاء الإلكتروني ليس لأغراض الإرهاب والاحتيال والجريمة فحسب، بل كأداة قوية للحرب الهجينة والتدخل في الشؤون الداخلية للدول أيضا.

وللأسف، أصبحت الحرب الهجينة أيضا أداة قوية في يد بعض الدول لتعزيز مصالحها الوطنية، وبما أن هذه الهيئة على علم جيد، فإن جورجيا لديها تجربة طويلة ومؤلمة في التعامل مع التهديدات الهجينة المنبثقة عن أحد أعضائها الدائمين. ولا يزال الاتحاد الروسي يشن حربا هجينة ضد جورجيا منذ أوائل التسعينات من القرن الماضي، ولم يتوقف قط عن محاولة تقويض سيادة بلدنا وسلامته الإقليمية وتطلعاته الأوروبية والأوروبية الأطلسية.

وقائمة الحوادث واسعة النطاق. ففي آب/أغسطس 2008، شهدنا خلال العدوان العسكري الروسي الواسع النطاق على جورجيا أول سابقة لهجوم سيبراني واسع النطاق تم تنفيذه بالتوازي مع العدوان المستمر. وفي عام 2019، شُنّ هجوم سيبراني واسع النطاق على المواقع الشبكية والخواديم وغيرها من نظم التشغيل التابعة لإدارة رئيس جورجيا، والمحاكم، والمجالس البلدية، وهيئات الدولة، ومنظمات القطاع الخاص، ووسائل الإعلام. وأسفر التحقيق الذي أجرته السلطات الجورجية، بالتعاون مع شركائنا، عن أن هذا الهجوم السيبراني قد خططت له ونفذته الشعبة الرئيسية في هيئة الأركان العامة للقوات المسلحة في الاتحاد الروسي.

وللأسف، حتى عندما يخوض المجتمع الدولي معركة ضد جائحة مرض فيروس كورونا (كوفيد-19)، لا يزال الاتحاد الروسي يحاول تحقيق مكاسب سياسية من خلال تكثيف الحرب الدعائية ضد واحدة من أنجح المؤسسات في جورجيا في مكافحة انتشار فيروس كورونا، أي مركز ريتشارد لوغار لأبحاث الصحة العامة. وتمثل اتهامات روسيا نموذجا للمعلومات المضللة والحملة الدعائية ضد هذا المختبر الفريد الذي أنشئ لتحديد فاشيات مثل الجائحة والتصدي لها.

واليوم نشهد جميعا تطبيقا قويا لمجموعة أدوات هجينة من جانب روسيا ليس فقط في منطقتنا، ولكن على نطاق عالمي أيضا. وأبرز الأدوات في مجموعة الأدوات الهجينة الروسية هي الوجود العسكري،

والعمليات الإعلامية، والهجمات السيبرانية، ودعم الجماعات السياسية التي تعمل بالوكالة، والتدخل في الشؤون الداخلية والنفوذ الاقتصادي.

وفي الختام، يجب أن نؤكد أن الهجمات السيبرانية والحرب الهجينة ضد الدول ذات السيادة تمثل انتهاكات خطيرة للقانون الدولي وقواعده ومبادئه وتقوض السلام والأمن الدوليين. وبينما نؤكد من جديد التزامنا بمواصلة تعزيز الأمن السيبراني على الصعيدين الوطني والدولي، فإننا ندعو المجتمع الدولي أيضا إلى زيادة اهتمامه بالأنشطة الخبيثة لتكنولوجيا المعلومات والاتصالات التي يقوم بها الاتحاد الروسي في جورجيا وغيرها.

المرفق الثاني والثلاثون

بيان البعثة الدائمة لألمانيا لدى الأمم المتحدة

قبل عام ونصف، ضربت جائحة مرض فيروس كورونا (كوفيد-19) العالم وجعلتنا ندرك، على نحو مفاجئ، مدى تشكيل التكنولوجيات الرقمية لحياتنا اليومية وقدرتنا الاقتصادية على الصمود. وفي الوقت نفسه، فقد كشفت بلا رحمة عن نقاط ضعفنا. ويمكن أن تشكل الهجمات السيبرانية، بما في ذلك تلك التي تشن ضد الهياكل الأساسية الحيوية، تهديدا للسلام والأمن الدوليين، ولا تزال ألمانيا مقتنعة بأنها موضوع مهم بالنسبة لمجلس الأمن.

ويتعرض السلام والأمن الدوليان لضغوط من جوانب مختلفة: أولا وقبل كل شيء، تقوض الأنشطة الجنائية السيبرانية موثوقية ومصداقية التكنولوجيات التي أصبحت الآن حاسمة بالنسبة لعمل اقتصاداتنا وحكوماتنا ومجتمعاتنا الحديثة ككل. وعلى سبيل المثال لا الحصر، كانت هناك زيادة حادة في الهجمات لقطع الخدمات والتصيد السيبراني وانتشار البرامجيات الخبيثة منذ تفشّي جائحة كوفيد-19. كما أن الهجمات على الهياكل الأساسية الحيوية في أوروبا وأمريكا الشمالية والهجمات السيبرانية المستخدمة كوسيلة للابتزاز آخذة في الازدياد أيضا.

ثانيا، إن الأنشطة السيبرانية الخبيثة التي ترعاها الدولة بغرض التجسس والتخريب والتضليل وزعزعة الاستقرار أو الكسب المالي تضر بالثقة الدولية وآليات التعاون الخاصة بتخفيف حدة النزاعات، وبالتالي تهدد الأمن في جميع أنحاء العالم.

ثالثا، يتعرض المجتمع المدني ككل والمدافعون عن حقوق الإنسان بشكل خاص لضغوط متزايدة في الفضاء الإلكتروني. فمساحة حرية التعبير والشفافية والاتصال الحقيقي، التي صممت شبكة الإنترنت لتوفيرها، آخذة في التقلص.

ومن أجل التصدي لهذه التهديدات المتزايدة، لا بد من اتباع نهج متعدد الركائز: وتتمثل احدى الركائز في تعزيز قدرتنا على الصمود على الصعيدين الوطني والدولي. ويشمل ذلك تحسين الهياكل الأساسية التقنية، والقدرات السياسية والقانونية، فضلا عن زيادة التعاون الدولي.

وتتمثل الركيزة الثانية في زيادة تعزيز وتحديد فهمنا المشترك لسلوك الدول المسؤول في الفضاء الإلكتروني ووضع خطوط حمراء يجب عدم تجاوزها. ولذلك، يجب أن ندافع عن المكتسبات القائمة التي حققها الفريق العامل المفتوح العضوية ومجموعة الخبراء الحكوميين، وأن نزيد من دفع تطوير معايير السلوك المسؤول للدول.

ويتمثل موقف ألمانيا في أن القانون الدولي، بما في ذلك ميثاق الأمم المتحدة والقانون الدولي الإنساني، ينطبق على شبكة الإنترنت وخارجها. وينبغي للدول أن تمتنع تماما عن دعم نشاط تكنولوجيا المعلومات والاتصالات الذي يتعارض مع التزاماتها بموجب القانون الدولي، وليس أقله في ضوء إمكانية إيجاد توترات وتصعيدها بين الدول. ويجب ألا يلحق نشاط تكنولوجيا المعلومات والاتصالات ضررا متعمدا بالهياكل الأساسية الحيوية أو أن يعوق بشكل آخر استخدام الهياكل الأساسية الحيوية وتشغيلها. وعلى وجه الخصوص، لا ينبغي أن تقوض أي جهة فاعلة التوافر العام للنواة العامة للإنترنت أو سلامتها، وهو أمر حيوي بالنسبة لاستقرار الفضاء الإلكتروني. وندعو جميع الدول إلى التقيد الصارم بالتزاماتها المتعلقة ببذل

العناية الواجبة واتخاذ إجراءات سريعة ضد الجهات الفاعلة التي تقوم بأنشطة سيبرانية خبيثة انطلاقا من أراضيها – وفقا للقانون الدولي.

ومن أجل تحفيز المناقشات الجارية بشأن القانون الدولي في الفضاء الإلكتروني، نشرت ألمانيا وثيقة سياسات بشأن تطبيق القانون الدولي في الفضاء الإلكتروني، ونشجع الآخرين على أن يحذوا حذوها.

بيد أن الاتفاق على تشريعات مشتركة لا يكفي. ومن المهم بنفس القدر أن يكون هناك رد حازم على السلوك غير المقبول. ويمكن النظر في صكوك مختلفة، تتراوح بين الحوار والتبادل والإعلانات السياسية من جانب الدول أو مجموعات الدول التي تكشف السلوك غير المسؤول وتندد به، أو تفرض جزاءات على الأشخاص والكيانات المعنية. وقد وضعنا، بالتعاون مع شركائنا في الاتحاد الأوروبي، نظاما للجزاءات متعلقا بالفضاء الإلكتروني يسمح لنا بالرد على الهجمات السيبرانية بطريقة حازمة وفعالة ومستهدفة وفي اتساق تام مع القانون الدولي. وقد استخدمنا هذه الأداة في الماضي ولن نتردد في استخدامها مرة أخرى إذا تعرض أمننا للخطر. وبالإضافة إلى ذلك، يمكن لثقافة إسناد المسؤولية أن تعزز الإطار المعياري وتدعم المساءلة في الفضاء الإلكتروني.

إن التبادل المستمر مع المجتمع المدني والقطاع الخاص والأوساط الأكاديمية أمر ضروري لزيادة قدرتنا على الصمود في الفضاء الإلكتروني، وعلى النهوض بقضية حوكمة الإنترنت. ويتعين تسخير الخبرة الوفيرة التي توجد خارج السلطات العامة من خلال هذه الجهود، وإدراجها فيها، بهدف صون السلام والأمن الدوليين في مجال الفضاء الإلكتروني.

المرفق الثالث والثلاثون

بيان البعثة الدائمة لليونان لدى الأمم المتحدة

تسهم التكنولوجيات الرقمية إسهاما عميقا في التحول الحالي للاقتصادات والمجتمعات، مما يتيح فرصا كبيرة للنمو الاقتصادي، فضلا عن التنمية المستدامة والشاملة للجميع. وقد أصبح الفضاء الإلكتروني، على وجه الخصوص، إحدى الدعامات الأساسية لمجتمعاتنا. وفي الوقت نفسه، أصبح تصاعد السلوك الخبيث في الفضاء الإلكتروني، بما في ذلك إساءة استعمال تكنولوجيات المعلومات والاتصالات من جانب الجهات الفاعلة من الدول وغير الدول لأغراض خبيثة، مصدرا لمخاطر وتحديات جديدة. ويهدد هذا السلوك النمو الاقتصادي ويمكن أن يؤدي إلى آثار مزعزعة للاستقرار ومتتالية مع زيادة مخاطر نشوب النزاعات.

ولذلك، فإننا نؤيد بقوة الإطار الاستراتيجي لمنع نشوب النزاعات والتعاون والاستقرار في الفضاء الإلكتروني، الذي أقرته الجمعية العامة، ونشدد على ضرورة تركيز جهودنا الجماعية على تطوير المهارات والقدرات اللازمة للتصدي على نحو ملائم للتهديدات السيبرانية. وتبرز الأزمة الصحية العالمية الراهنة الحاجة إلى قدرة النظم السيبرانية على الصمود على الصعيد العالمي، حيث لاحظنا التهديدات السيبرانية والأنشطة السيبرانية الخبيثة التي تستهدف قطاع الرعاية الصحية.

وتحد القدرة على الصمود في الفضاء الإلكتروني على الصعيد العالمي من قدرة الجناة المحتملين على إساءة استخدام تكنولوجيا المعلومات والاتصالات، وتعزز قدرة الدول على التصدي بفعالية للحوادث السيبرانية والتعافي من آثارها. وفي إطار جهودنا الأخيرة في تعزيز القدرة على الصمود على الصعيد العالمي ووضع تدابير تعاونية عملية، نحن حاليا بصدد تنظيم حلقة دراسية إقليمية بشأن الأمن الإلكتروني، مع مشاركين من غرب البلقان.

ومن خلال مشاركتنا النشطة في المنظمات الدولية من قبيل الأمم المتحدة ومنظمة حلف شمال الأطلسي ومنظمة الأمن والتعاون في أوروبا، نسعى إلى التعاون وتبادل الخبرات وأفضل الممارسات، والمساهمة إلى أقصى حد ممكن في تطوير الوسائل المناسبة للتصدي للتهديدات السيبرانية. وعلاوة على ذلك، فإننا، بصفتنا عضوا في الاتحاد الأوروبي، ننفذ إطارا استراتيجيا شاملا للجميع ومتعدد الأوجه لمنع نشوب النزاعات والاستقرار في الفضاء الإلكتروني. ويمثل الأمن السيبراني داخل الاتحاد الأوروبي جهدا منسقا وجماعيا بين الدول الأعضاء مما يشكل سابقة فريدة وقيّمة للتعاون المتعدد الأطراف.

ونحن ملتزمون التزاما كبيرا بفضاء إلكتروني عالمي وسلمي وآمن ومفتوح ومستقل يحكمه القانون الدولي، حيث تُطبق حقوق الإنسان والحريات الأساسية وسيادة القانون تطبيقا كاملا. وما فتئنا نشارك خبراتنا بنشاط في تنفيذ المعايير، وتدابير بناء الثقة، وبناء القدرات على الصعيدين الثنائي والمتعدد الأطراف في كل المنتديات الإقليمية والدولية التي نشارك فيها. ونحن ملتزمون التزاما قويا بالمشاركة بنشاط في مزيد من المناقشات في الأمم المتحدة بشأن مسائل الأمن السيبراني، ونؤكد من جديد استعدادنا للمشاركة بإيجابية في مسعى إلى إحراز تقدم بناء.

المرفق الرابع والثلاثون

بيان البعثة الدائمة لغواتيمالا لدى الأمم المتحدة

تود غواتيمالا أن تعرب عن امتنانها للوفد الإستوني بوصفه رئيسا لمجلس الأمن لعقد هذه المناقشة المفتوحة بشأن مسألة ذات أهمية قصوى، دون أدنى شك، بالنسبة للدول من أجل معالجتها. ولقد أصبح الفضاء الإلكتروني مجالا مركزيا لا غنى عنه بالنسبة للنشاط العالمي، كما أن حمايته من خلال سلوك الدول المسؤول أمر بالغ الأهمية لضمان صون السلام والأمن الدوليين. ونحن واثقون من أن هذا النوع من الاجتماعات يوفر فرصة ممتازة لبلداننا من أجل تبادل الآراء والممارسات الجيدة بشأن مختلف مستويات تنفيذ موضوع متزايد الأهمية.

ويواجه العالم حاليا العديد من التحديات الأمنية التي تتفاقم بسبب ظهور تهديدات جديدة، مثل قضايا الأمن السيبراني. وإذا نظرنا إلى الهجمات السيبرانية السابقة، وكذلك زيادتها خلال أوقات جائحة مرض فيروس كورونا (كوفيد-19)، فإن الحاجة واضحة إلى معالجة هذا الموضوع، خاصة إذا وضعنا في الاعتبار أنه يمكن أن يؤثر على القطاعات الأكثر ضعفا في مجتمعنا.

وتنشأ التهديدات والهجمات السيبرانية وتتطور نتيجة لمختلف الأنشطة التي يتم تطويرها من خلال الترابط بين الوسائط الرقمية، والتي تمثل تعقيدا في الظروف التي تتطلب مشاركة وتعاون جميع قطاعات بلداننا، من أجل تطوير الأطر التقنية والقانونية التي تعزز الأمن السيبراني على الصعيدين المحلي والعالمي.

وكما هو الحال في جميع البلدان، فإن الزيادة في استخدام تكنولوجيا المعلومات والاتصالات أصبحت منتشرة على نطاق واسع في جميع قطاعات مجتمعنا. وهذا السيناريو الجديد ييسر تطورا غير مسبوق لتبادل المعلومات والاتصالات، ولكنه ينطوي في الوقت نفسه على مخاطر وتهديدات جديدة يمكن أن تؤثر على أمن سكاننا.

وبالنظر إلى ذلك، يود وفدي أن يعرب عن قلقه إزاء هذه التكنولوجيات الجديدة، لا سيما بالنظر إلى الطابع المدني والمزدوج الاستخدام للفضاء الإلكتروني والشبكات الرقمية، التي يمكن أن تستخدمها الجماعات الإجرامية والإرهابية. ومن المقلق للغاية قيام عدد من الدول حاليا باستحداث قدرات في مجال تكنولوجيات المعلومات والاتصالات للأغراض العسكرية، والتزايد المستمر حاليا في احتمال استخدام هذه التكنولوجيات في النزاعات المقبلة بين الدول.

وتدرك غواتيمالا أن الطبيعة المترابطة والمعقدة للفضاء الإلكتروني تتطلب قيام الحكومات والقطاع الخاص والمجتمع المدني والأوساط الأكاديمية ببذل جهود مشتركة لمواجهة تحديات الأمن السيبراني بطريقة شاملة ومتوازنة. وتقع على عاتق جميع هذه القطاعات مسؤولية الحفاظ على فضاء إلكتروني مفتوح وحر وآمن ومستقر.

ولهذا السبب، يشجع بلدي تدابير بناء الثقة والشفافية، ويدعم أنشطة بناء القدرات وتبادل المعلومات ونشر أفضل الممارسات، على الصعيد دون الإقليمي والإقليمي والدولي على السواء.

ويشدد وفد بلدي على أن تطبيق القانون الدولي على سلوك الدول في الفضاء الإلكتروني، والمعايير الطوعية غير الملزمة لسلوك الدول المنطبقة في وقت السلم، وتنفيذ تدابير بناء الثقة، لا تزال حاسمة. وعلاوة على ذلك، وبعد أن شهد بلدي الفجوات القائمة بين البلدان في مجالي الأمن الإلكتروني

والدفاع، فإنه يولي اهتماما خاصا لجهود بناء القدرات من أجل إيجاد ساحة أكثر إنصافا تساعد على صون السلام والأمن الدوليين.

وتعتقد غواتيمالا أن المنظمات الإقليمية تؤدي دورا لا غنى عنه في صنع السلام على أرض الواقع. وهناك إمكانات كبيرة لتعزيز وجودها في الفضاء الإلكتروني، إقليميا وعالميا، من أجل النهوض بطريقة مبتكرة بخطة السلام المستدام. وركزت المنظمات الإقليمية ودون الإقليمية على تحسين أمن الدول، مما حقق خطوات كبيرة في تنفيذ تدابير عملية لبناء الثقة في مختلف المناطق لتحسين استقرار الفضاء الإلكتروني. ولا شك أنه بدون مساهمات هذه المنظمات، ستكون الجهود المبذولة لمنع نشوب النزاعات وتحقيق الاستقرار أقل.

ولدى غواتيمالا حاليا استراتيجية وطنية للأمن السيبراني هدفها الرئيسي تعزيز قدرات البلد، وتهيئة البيئة والظروف اللازمة لضمان مشاركة الناس في الفضاء الإلكتروني وتطوير حقوقهم في هذا الشأن وممارستها. وبالإضافة إلى ذلك، لديها مركز للتصدي للحوادث السيبرانية، يوفر خدمات تدقيق الأمن الإلكتروني، ومسح نقاط الضعف، وتصنيف التنبيهات. وقد تحقق كل منهما بمرافقة منظمة الدول الأمريكية.

وبالإضافة إلى ذلك، فإن غواتيمالا بصدد وضع قانون بشأن الجرائم السيبرانية، يحدد بوضوح خطوط العمل وأنواع الجريمة باستخدام تكنولوجيا المعلومات والاتصالات ومن خلالها من أجل تعزيز بناء القدرات من خلال التعاون الدولي، وتفضيل الإجراءات القانونية الواجبة من خلال وجود بروتوكولات محددة جيدا لسلسلة الاحتجاز ومعالجة الأدلة الرقمية. ومن الضروري أيضا الإشارة إلى أن بلدي يشرفه أن يكون بلدا مراقبا لاتفاقية بودابست، التي تسعى إلى التصدي للجرائم الحاسوبية والجرائم المرتكبة على شبكة الإنترنت من خلال تنسيق القوانين السارية بين البلدان، وتحسين أساليب التحقيق، وزيادة التعاون فيما بين الأمم.

ويرى وفد بلدي ضرورة مواصلة إجراء التحولات والتعديلات في القوانين التي تحكم كل بلد بطريقة منسقة، وتصميم نظم تسمح باكتشاف الجرائم المحتملة والتحقيق فيها وملاحقة مرتكبيها قضائيا في إطار يحمي حقوق الأفراد ويقلل في الوقت نفسه من خطر استخدام شبكات الحواسيب لانتهاك سرية المعلومات وسلامتها وتوافرها. ونأمل أن تسهم مناقشتنا اليوم مساهمة إيجابية، وأن تكمل عملية وضع المعايير السيبرانية، التي تجري في الجمعية العامة، ولا سيما من خلال الأعمال المجدية لفريق الخبراء الحكوميين والفريق العامل المفتوح العضوية للفترة 2021-2025.

وفي الختام، نذكر جميع الدول بوجوب استخدام تكنولوجيا المعلومات والاتصالات بطريقة سلمية وللصالح العام للبشرية ولتعزيز التنمية المستدامة لجميع البلدان، أياً كان مستواها من التطور العلمي والتكنولوجي.

المرفق الخامس والثلاثون

بيان القائم بأعمال إندونيسيا لدى الأمم المتحدة، محمد كورنيادي كوبا

أود أن أشكر إستونيا على الدعوة إلى عقد هذا الاجتماع. وأود أيضا أن أشكر مقدمة الإحاطة على إحاطتها القيّمة.

ومع تزايد اعتماد الناس على الاتصال الرقمي، أصبحت تكنولوجيا المعلومات والاتصالات جزءا لا يتجزأ من حياتنا اليومية.

وعلاوة على ذلك، وفرت تكنولوجيا المعلومات والاتصالات، أثناء جائحة مرض فيروس كورونا (كوفيد-19)، شريان حياة للقطاعين العام والخاص في تقديم الخدمات الأساسية للسكان.

وفي هذا الصدد، من الأهمية بمكان التأكيد على أن الأنشطة السيبرانية الخبيثة التي تقوم بها الجهات الفاعلة من الدول وغير الدول، ولا سيما تلك التي تستهدف الهياكل الأساسية الحيوية، يمكن أن تقوض الاستقرار الوطني وكذلك السلام والأمن الدوليين.

وفي هذا السياق، تود إندونيسيا أن تؤكد على ما يلي.

أولا، أسبقية سيادة القانون في توجيه سلوكنا فيما يتعلق باستخدام تكنولوجيا المعلومات والاتصالات، فضلا عن آثارها على السلام والأمن الدوليين.

وتوفر مبادئ القانون الدولي وميثاق الأمم المتحدة القواعد القانونية الأساسية التي توجه الدول بشأن استخدامها لتكنولوجيا المعلومات والاتصالات، بما في ذلك في التصدي لأي هجمات خبيثة.

ويجب أن تسترشد جميع الدول بنفس المجموعة من القواعد والقوانين. ولا ينبغي استثناء أحد.

وعلاوة على ذلك، تؤيد إندونيسيا معايير السلوك المسؤول للدول المبينة في قرار الجمعية العامة 237/70.

وفي الوقت الذي نواصل فيه تلبية الحاجة المتزايدة إلى تحديد وتطوير إطار قانوني دولي بشأن هذه المسألة، ينبغي أن توجه جهودنا أيضا نحو معالجة الثغرات بين البلدان والمناطق.

وإلى جانب الثغرات التقنية، لا بد من تعزيز أطر السياسات الوطنية فضلا عن تنفيذ القانون الدولي القائم والمعايير الطوعية وغير الملزمة في الفضاء الإلكتروني.

وثانيا، دور النهج الثنائية والإقليمية والمتعددة الأطراف في تعزيز الثقة في الفضاء الإلكتروني.

وتعزز التدابير التعاونية على الصعيد الثنائي والإقليمي والمتعدد الأطراف بعضها بعضا في النهوض بالتفاهم وتعزيز الاستقرار في الفضاء الإلكتروني، ولا سيما في مجال القدرات وبناء الثقة.

وما فتئت تدابير بناء الثقة التي تتخذها رابطة أمم جنوب شرق آسيا، من خلال إنشاء جهات اتصال وتبادل المعلومات والتحاور وتبادل أفضل الممارسات بانتظام، تسهم في تحقيق الاستقرار السيبراني في منطقة جنوب شرق آسيا وخارجها، ولا سيما من خلال المنتدى الإقليمي للرابطة.

وعلاوة على ذلك، تؤكد إندونيسيا على ميزة الشراكة المجدية مع الكيانات الأخرى المتعددة أصحاب المصلحة لمساعدة الدول على تطبيق إطار السلوك المسؤول في استخدامها لتكنولوجيا المعلومات والاتصالات.

وفي هذا الصدد، نؤكد على ضرورة مشاركة البلدان المتقدمة لتكنولوجيات المعلومات والاتصالات مع البلدان النامية. وكما هو الحال مع جميع المشاكل العالمية الأخرى، فإن ضمان أن يكون لدى الآخرين الأدوات والقدرات المناسبة للتصدي لهذا الخطر، سيسهم في الاستقرار العام في مجال تكنولوجيا المعلومات والاتصالات.

وثالثا، دور الأمم المتحدة في قيادة جهد منسق في التصدي للنزاعات التي قد تنشأ عن حوادث تكنولوجيا المعلومات والاتصالات.

إن مناقشة اليوم هي أول مناقشة رسمية مكرسة للمجلس بشأن أثر تكنولوجيات المعلومات والاتصالات على صون السلام والأمن الدوليين.

وهي تمثل خطوة هامة إلى الأمام بشأن هذه المسألة في الأمم المتحدة.

وفي المستقبل، يحتاج المجلس إلى توقع تزايد التهديدات في الفضاء الإلكتروني، فضلا عن احتمال وقوع حوادث كبيرة في بيئة تكنولوجيا المعلومات والاتصالات يمكن أن تؤدي إلى نشوب حرب كبرى.

ونشدد على أهمية ضمان أن تظل إجراءات الأمم المتحدة منسقة ومتآزرة. وينبغي للمجلس أن يواصل الاستجابة للسلام والأمن الدوليين، فضلا عن الآثار الإنسانية المترتبة على التطورات في مجال تكنولوجيا المعلومات والاتصالات.

وفي الوقت نفسه، يجب أن يسترشد المجلس بالمعايير والقواعد التي تتداولها الجمعية العامة وتبلورها.

واسمحوا لي أن أختتم كلمتي بالتأكيد مجددا على التزام إندونيسيا بدفع جهودنا المشتركة نحو الاستجابة على النحو المناسب للتحديات المتزايدة باستمرار في مواجهة صون السلام والأمن فيما يتصل باستخدام تكنولوجيا المعلومات والاتصالات.

المرفق السادس والثلاثون

بيان اللجنة الدولية للصليب الأحمر

تعرب اللجنة الدولية للصليب الأحمر عن الامتنان لإتاحة الفرصة لها للمساهمة في هذه المناقشة المفتوحة لمجلس الأمن حول "صون السلام والأمن الدوليين في الفضاء الإلكتروني".

وعلى مدى العقدين الماضيين، أصبحت العمليات السيبرانية العدائية شاغلا متزايد الأهمية لصون السلام والأمن الدوليين. ومع رقمنة المجتمعات، يتم أيضا رقمنة القدرات العسكرية للدول والجهات الفاعلة الأخرى. واليوم، يدرك المجتمع الدولي قيام "عدد من الدول باستحداث قدرات في مجال تكنولوجيات المعلومات والاتصالات لأغراض عسكرية" و "تزايد احتمال استخدام تكنولوجيات المعلومات والاتصالات في النزاعات المقبلة بين الدول"[(10)].

وفي ضوء هذا الواقع، تود اللجنة الدولية للصليب الأحمر أن تذكّر بالضرر المحتمل الذي يمكن أن يسببه استخدام التكنولوجيا السيبرانية للبشر، وبعد ذلك تعرض كيف يمكن للدول أن تخفف من هذه العواقب الإنسانية السلبية من خلال العمل على الصعيدين الدولي والوطني.

ومن المعروف جيدا اليوم أن العمليات السيبرانية ضد الهياكل الأساسية المدنية الحيوية قد تسببت في ضرر اقتصادي كبير، وألحقت اضطرابات بالمجتمعات، وأشعلت توترات بين الدول. وفي التقرير النهائي للفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، أقرت جميع الدول بأن العمليات السيبرانية ضد الهياكل الأساسية الحيوية تنطوي على "عواقب إنسانية مدمرة محتملة"[(11)]. وفي حين لا تستطيع اللجنة الدولية للصليب الأحمر تأكيد أي عمليات سيبرانية تسفر عن خسائر بشرية، فإننا نشعر بالقلق إزاء الآثار المدمرة للعمليات السيبرانية، مثل انقطاع إمدادات الكهرباء أو شبكات المياه أو الخدمات الطبية[(12)]. وتشكل هذه الأنواع من العمليات مخاطر حادة على البشر في جميع الأوقات. غير أن تجربتنا تبين أن تعطيل الهياكل الأساسية المدنية الحيوية له عواقب وخيمة بشكل خاص في المجتمعات التي أضعفها النزاع المسلح بالفعل.

والعواقب الإنسانية الخطيرة *ليست* حتمية. ويجب على الدول أن تتخذ خطوات حاسمة لضمان امتثال استخدامها للعمليات السيبرانية أثناء النزاع المسلح للقواعد القائمة للقانون الدولي. وترى اللجنة الدولية للصليب الأحمر أن هذا يتطلب اتخاذ إجراءات على الصعيدين الدولي والوطني.

وعلى الصعيد الدولي، أكدت الدول أن القانون الدولي ينطبق في بيئة تكنولوجيا المعلومات والاتصالات. ويشمل ذلك، أولا وقبل كل شيء، التزامات الدول بموجب ميثاق الأمم المتحدة، ولا سيما حظر استخدام القوة والالتزام بتسوية المنازعات الدولية بالوسائل السلمية. وفي الآونة الأخيرة، لاحظ فريق الخبراء الحكوميين أيضا أن 'القانون الدولي الإنساني لا ينطبق إلا في حالات النزاع المسلح'. وأشار الفريق إلى 'المبادئ القانونية الدولية الراسخة، بما في ذلك، حيثما ينطبق، مبادئ الإنسانية والضرورة والتناسب والتمييز التي لوحظت في تقرير عام 2015'، وأقر 'بالحاجة إلى مزيد من الدراسة بشأن كيفية تطبيق هذه المبادئ

(10) الفريق العامل المفتوح العضوية، التقرير النهائي، 2021، الفقرة 16؛ وفريق الخبراء الحكوميين، التقرير النهائي، 2021، الفقرة 7.

(11) الفريق العامل المفتوح العضوية، التقرير النهائي، 2021، الفقرة 18.

(12) متاح في الرابط: www.icrc.org/en/document/potential-human-cost-cyber-operations.

على اســـتخدام الدول لتكنولوجيا المعلومات والاتصـــالات، ومتى تنطبق، وأكد أن التذكير بهذه المبادئ لا يضـفي الشرعية على النزاع أو يشـجعه بأي حال من الأحوال‘[13]. وتؤيد اللجنة الدولية للصـليب الأحمر هذا الرأي تأييدا تاما: فالأنشـطة السـيبرانية في أثناء النزاع المسـلح لا تحدث في ’فراغ قانوني‘ أو ’منطقة رمادية‘، فهي تخضع للمبادئ والقواعد الراسخة للقانون الدولي الإنساني.

ولضـــمان فهم القانون الدولي الإنســـاني وتطبيقه بفعالية، ترحب اللجنة الدولية للصـــليب الأحمر بإجراء مزيد من الدراسة حول كيفية تطبيق هذا المجال من القانون، ومتى ينطبق. ولتجنب العواقب الإنسانية السـلبية واضـطراب المجتمعات، نطلب إلى الدول أن تفسـر قواعد ومبادئ القانون الدولي الإنسـاني وتطبقها بطريقة تأخذ في الاعتبار الخصـــائص المحددة لبيئة تكنولوجيا المعلومات والاتصـــالات. وتتطلب المســائل الأسـاسـية المتعلقة بحماية الحياة المدنية مزيدا من الدراسـة وتحديد موقعها بوضـوح من جانب الدول. فعلى ســـبيل المثال، ينبغي أن تكون الأولوية للدول، في عالم يتزايد فيه اســـتخدام البيانات، أن توافق على أن البيانات المدنية تتمتع بالحماية من الهجمات، تماما كما الحال مع الملفات الورقية المدنية. وعلاوة على ذلك، ينبغي للدول أن تؤكد أن العمليات السـيبرانية، التي تلحق الضـرر بالأعيان المدنية عن طريق تعطيل وظائفها، تخضع لجميع قواعد القانون الدولي الإنساني المتعلقة بتسيير الأعمال العدائية[14].

وفي حين أن مواصلة الدراسة والاتفاق بشأن كيفية أن القانون الدولي يحد من العمليات السيبرانية أثناء النزاعات المســـلحة أمر مهم، فإن هذه القواعد لن تصـــبح فعالة إلا من خلال التنفيذ على الصـــعيد الوطني. ومن خلال المناقشات التي دارت مع المتعهدين العسكريين والخبراء، حددت اللجنة الدولية للصليب الأحمر عددا من الخطوات الرئيسـية بشـأن كيفية تجنب الدول للضـرر الذي يلحق بالمدنيين جراء العمليات العسكرية أثناء النزاع المسلح، وضرورة قيامها بذلك[15]. واليوم، نود أن نؤكد على أربع خطوات منها:

- أولا، كل دولة مسـؤولة عن جميع أجهزتها المشـاركة في العمليات السـيبرانية وغيرها من الجهات الفاعلة التي تعمل بناء على تعليمات تلك الدولة، أو تحت إدارتها أو سـيطرتها. ويجب على الدول أن تكفل احترام جميع هذه الجهات الفاعلة للقانون الدولي الإنساني.
- ثانيا، ينبغي للدول أن تضـع عمليات داخلية واضـحة لضـمان امتثال وسـائل أو أسـاليب الحرب المتصلة بالفضاء الإلكتروني للإطار القانوني المنطبق إذا ما استخدمت.
- ثالثا، على الدول الالتزام باتخاذ جميع الاحتياطات الممكنة لتجنب الضـــرر العرضـــي الذي يلحق بالمدنيين عند تنفيذ الهجمات، أو على الأقل التقليل منه إلى أدنى حد، بما في ذلك من خلال وسائل وأساليب الحرب المتعلقة بالفضاء الإلكتروني. وفي بيئة تكنولوجيا المعلومات والاتصالات، قد يشـــمل ذلك تنفيذ تدابير تقنية من قبيل "ســـياج الأنظمة" أو "الســـياج الجغرافي" أو "مفاتيح الإيقاف"[16].

(13) فريق الخبراء الحكوميين، التقرير النهائي، 2021، الفقرة 71 (و).

(14) انظر أيضا: اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، ورقة موقف، 2019.

(15) ICRC, Avoiding Civilian Harm from Military Cyber Operations During Armed Conflicts, 2021.

(16) يعني "سياج الأنظمة" منع البرامج الضارة من تنفيذ نفسها ما لم يكن هناك تطابق دقيق مع النظام المستهدف، و "السياج الجغرافي" يعني الحد من البرامج الضـــارة لتعمل فقط في نطاق بروتوكول الانترنت المحدد، وتعني "مفاتيح الإيقاف" طريقة لتعطيل البرامج الضارة بعد وقت معين أو عند تنشيطها عن بعد.

- رابعا، يتعين على الدول أيضـا أن تتخذ تدابير لحماية السـكان المدنيين من الأخطار الناجمة عن العمليات السيبرانية العسكرية. وقد يتعين تنفيذ بعض هذه التدابير بالفعل في وقت السلم.

وفي الختام، تثني اللجنة الدولية للصـليب الأحمر على الدول الأعضـاء لسـعيها من أجل تعزيز الحوار الدولي والاتفاق على التكلفة البشـرية المحتملة للعمليات السـيبرانية وتدابير منع الضـرر البشـري والتخفيف من حدته. وفي رأينا أن القانون الدولي الإنسـاني يجب أن يكون جزءا من هذه المناقشـات، وتظل اللجنة الدولية للصليب الأحمر جاهزة لتقديم خبرتها إليها.

المرفق السابع والثلاثون

بيان من المدير التنفيذي لأجهزة الشرطة في المنظمة الدولية للشرطة الجنائية (الإنتربول)

مقدمة

تمثل الجريمة السيبرانية تحدياً عالمياً في هذا العصر الرقمي. ويتجاوز تأثيرها بكثير ما يتم الإبلاغ عنه أو كشفه، مما يؤثر على الحياة اليومية لأكثر من 4,5 بلايين شخص على شبكة الإنترنت. وقد أدى الاعتماد المتزايد مؤخرا على البيئة الرقمية إلى إتاحة المزيد من فرص القيام بأعمال إجرامية في الفضاء الإلكتروني. وتشكل الجريمة السيبرانية اليوم، بتحويل أهدافها نحو الحكومات والشركات والبنى التحتية الرئيسية وحتى المستشفيات، تحديا هائلا للأمن في جميع أنحاء العالم. ونظرا لتنامي الجريمة السيبرانية السريع من حيث الحجم والشدة على السواء، تولي المنظمة الدولية للشرطة الجنائية (الإنتربول) الأولوية لمكافحتها.

ويدرك الإنتربول، بوصفه منظمة حكومية دولية محايدة، أهمية القانون الدولي والمعايير وتدابير بناء الثقة وجهود بناء القدرات لصون السلام والأمن في الفضاء الإلكتروني. وفي ضوء هدف هذه المناقشة المفتوحة المتمثل في فهم المخاطر المتزايدة الناجمة عن الأنشطة الخبيثة في الفضاء الإلكتروني على نحو أفضل، يقدم الإنتربول هذا البيان الخطي إلى مجلس الأمن لتأييد التزامه بتحقيق فضاء إلكتروني سلمي وآمن. ويعرض هذا البيان أحدث اتجاهات الجرائم السيبرانية وتأثيرها، فضلا عن الآليات والحلول العالمية للإنتربول المتاحة لبلدانه الأعضاء الـ 194 لمواجهة هذه التحديات الملحة.

التهديدات السيبرانية الحالية والناشئة

حلل الإنتربول خلال العام الماضي مجموعة واسعة من التهديدات السيبرانية. وأكد تقييمه الأخير أن جائحة مرض فيروس كورونا (كوفيد-19) فتحت آفاقا جديدة لمجرمي الفضاء السيبراني لتنفيذ مختلف أشكال الإجرام عبر الإنترنت بغض النظر عن المنطقة. وتشمل التهديدات البارزة الابتزاز القائم على برمجيات انتزاع الفدية، واختراق عناوين البريد الإلكتروني للعمل، وعمليات جمع البيانات غير القانونية، ونشر المعلومات المضللة، وعودة ظهور أنواع قديمة من البرمجيات الخبيثة، المعاد توجيهها للاستفادة من الجائحة العالمية.

وتشمل الاتجاهات المحددة أيضا تحول الأهداف إلى الشركات الكبرى والحكومات والبنى التحتية الحيوية[17]. ويستغل المجرمون والمحتالون في الفضاء السيبراني الاحتياجات الاجتماعية وعوامل القلق الجوهرية. وما فتئ الإنتربول يتلقى منذ آذار/مارس 2020 عددا من الطلبات من بلدانه الأعضاء للتصدي لهجمات برمجيات انتزاع الفدية الموجهة ضد المستشفيات والمؤسسات الأخرى التي تقف في الخطوط

(17) الإنتربول، تقرير تقييم تبعات كوفيد-19 على الجريمة السيبرية، يمكن تنزيله من الرابط https://www.interpol.int/ar/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf.

الأمامية لمكافحة فيروس كورونا[18]. وقد تمكن المجرمون، من خلال مهاجمة هذه البنى التحتية الحيوية التي تؤدي دورا حاسما في الاستجابة للفاشية، من تعظيم الأضرار والمكاسب المالية.

وفي حين أن هجمات برمجيات انتزاع الفدية ليست جديدة، فهي تمثل الشكل الأسرع نموا من الجرائم السيبرانية. وتوفر برمجيات انتزاع الفدية نموذجا تجاريا مغريا ومربحا للغاية لمجرمي الفضاء السيبراني، الذين يضاعفون الابتزاز ويستخدمون نموذج تقديم هذه البرمجيات كخدمة. ولقد شهدنا أيضاً نمطا لم تكن هذه الهجمات فيه محدودة جغرافيا، مما يشير إلى أن المجرمين يوسعون نطاق تركيزهم لاستهداف أي مؤسسة حول العالم. فعلى سبيل المثال، استُخدمت في آسيا نفس سلالة برمجيات انتزاع الفدية التي أدت إلى إغلاق مستشفى في أوروبا أيضاً.

وبالإضافة إلى ذلك، شهدنا عمليات احتيال معقدة تصيب ضحايا في أوروبا، وتُوَجَّه فيها العائدات وصولاً إلى غرب أفريقيا وجنوب شرق آسيا في غضون ساعات. وتتواصل أيضاً الخروقات الهائلة للبيانات مسببةً خسائر مالية كبيرة للشركات في جميع أنحاء العالم. وفي الوقت نفسه، يختبئ مجرمو الفضاء السيبراني في الشبكة الخفية التي تضمن الوصول الخفي وغير القابل للتعقب. وهذا يزيد من أهمية وجدوى نشرات الإنتربول[19]، ولا سيما النشرة البنفسجية، التي تعد أداة تتبادل البلدان الأعضاء من خلالها المعلومات عن أساليب عمل هذه المخططات الاحتيالية. والهدف من ذلك هو نشر هذه المعلومات الحيوية لتسبق الهجوم التالي.

وعلاوة على ذلك، يشكل التقارب بين الجرائم السيبرانية والجرائم المالية تحديا معقدا. ويتضمن هذا النوع من الجرائم مراحل متعددة بدءاً من الهجوم السيبراني إلى استغلال البيانات، ثم غسل الأموال لتمويه أثرها، وصولاً إلى صرفها في نهاية المطاف. واستخدام العملة المشفرة في هذه العملية يعيق أيضاً جهود التصدي لهذه الجرائم بفعالية وفي الوقت المناسب. ونظرا لتعقد الأمر، يلزم وضع نموذج تشغيل مشترك يجمع بين قدرات مختلف الوحدات المتخصصة في مجال إنفاذ القانون لتحسين مكافحة عمليات الاحتيال وغسل الأموال التي تسهّل شبكة الإنترنت ارتكابها. ولتقديم كامل مجموعة الدعم التشغيلي والتحليلي في هذا الصدد، أطلق الإنتربول فرقة العمل المعنية بالجريمة المالية العالمية التابعة للإنتربول في نهاية عام 2020.

الآلية العالمية للتخفيف من التهديدات السيبرانية

يمثل التعاون الشرطي الدولي أمراً حيوياً في الواقع، وذلك للحفاظ على سلامة وأمن العالم الشديد الترابط. وكما هو معترف به في الدراسة الشاملة لمكتب الأمم المتحدة المعني بالمخدرات والجريمة بشأن الجرائم السيبرانية، فإن الإنتربول يؤدي دورا فريدا في تيسير التعاون فيما بين دوائر الشرطة[20]. ودعما للبلدان الأعضاء الـ 194 فيه، يُعهَد إليه بمهمة تيسير التعاون عبر الحدود في مجال إنفاذ القانون، حسب الاقتضاء، ودعم المنظمات الحكومية والمنظمات الحكومية الدولية والسلطات والدوائر التي تتمثل مهمتها في

(18) https://www.interpol.int/ar/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware.

(19) https://www.interpol.int/ar/How-we-work/Notices/About-Notices.

(20) دراسة مكتب الأمم المتحدة المعني بالمخدرات والجريمة الشاملة عن الجريمة السيبرانية، الصفحة 195 (من النص الإنكليزي).

منع الجريمة أو مكافحتها، وذلك في حدود القوانين القائمة في مختلف البلدان وبما يتماشى مع الإعلان العالمي لحقوق الإنسان.

ونظرا لحياد الإنتربول وتواجده على الصعيد العالمي، فهو في وضع فريد يمكنه من قيادة وتنسيق الاستجابة العالمية لأجهزة إنفاذ القانون للجرائم السيبرانية. ويتيح ذلك أيضاً لأجهزة إنفاذ القانون في جميع أنحاء العالم تبادل المعلومات عن الجرائم السيبرانية وعن الجهات الفاعلة المهدِّدة، ويوفر مجموعة واسعة من الخبرات والتوجيه التقني والدعم التشغيلي. واستنادا إلى هذا الدور الفريد، يدعو الإنتربول إلى التعاون الدولي للشرطة في مختلف العمليات السياساتية للأمم المتحدة، مثل فريق خبراء الأمم المتحدة المعني بإجراء دراسة شاملة عن مشكلة الجريمة السيبرانية[21] والفريق العامل المفتوح العضوية التابع للأمم المتحدة المعني بأمن تكنولوجيا المعلومات والاتصالات، ويؤكد على أهميته.

ومن أجل الارتقاء بالشراكة إلى مستوى أعلى، تم بالإجماع اعتماد الاستعراض نصف السنوي الثاني لقرار الجمعية العامة بشأن التعاون بين الأمم المتحدة والإنتربول في 23 تشرين الثاني/نوفمبر 2020[22]. ومثل ذلك إنجازا هاماً لأنه أدخل لغة جديدة بشأن مجالات التعاون الرئيسية، بما في ذلك الجريمة السيبرانية، مما يوفر شرعية أكبر لمواصلة التعاون بين المنظمتين في هذا المجال.

وفي عصر الرقمنة هذا، لم تعد الحلول الوطنية، وحتى الحلول الإقليمية، كافية. وللمساعدة في تحقيق السلام والأمن الدوليين في الفضاء الإلكتروني، فإن الإنتربول قادر على أن يعمل كآلية عالمية لمكافحة الجرائم السيبرانية بفعالية وتزويد بلدانه الأعضاء بمجموعة متنوعة من الخدمات والأدوات، بما في ذلك:

- منظومة عالمية للاتصالات الشرطية المأمونة تدعى I/24-7 لتبادل المعلومات العاجلة للشرطة بشكل آمن وفي الوقت الحقيقي؛
- 19 قاعدة بيانات[23] ونشرات[24] لها دور أساسي في إرسال التنبيهات إلى المجتمع الدولي ودعم التحقيقات عبر الوطنية؛
- برنامج الإنتربول العالمي للجرائم السيبرانية الذي يوفر القدرات الشرطية في منع الجرائم السيبرانية وكشفها والتحقيق فيها ووقفها، بغية الحد من الأثر العالمي للجرائم السيبرانية وحماية المجتمعات من أجل عالم أكثر أمانا؛
- فريق خبراء الإنتربول العالمي لمكافحة الجريمة السيبرية والأفرقة العاملة الإقليمية مع رؤساء الوحدات المعنية بمكافحة الجريمة السيبرية لمناقشة القضايا الملحة المتعلقة بالجرائم السيبرانية ووضع خطط تنفيذية واستراتيجية؛

(21) https://www.unodc.org/documents/Cybercrime/IEG_cyber_comments/INTERPOL.pdf و https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2021/Statements/Item-3/INTERPOL_item_3.pdf

(22) قرار الجمعية العامة 10/75 بشأن التعاون بين الأمم المتحدة والمنظمة الدولية للشرطة الجنائية (الإنتربول).

(23) https://www.interpol.int/ar/How-we-work/Databases/Our-19-databases.

(24) https://www.interpol.int/ar/How-we-work/Notices/About-Notices.

- منصات الاتصالات مثل منصة تبادل المعارف المتصلة بالجريمة السيبرية لتبادل المعلومات بشكل آمن ضمن الأوساط الأوسع نطاقاً لإنفاذ القانون ومنصة التعاون لمكافحة الجريمة السيبرية – العمليات للمناقشات المغلقة المتعلقة بالعمليات؛
- المنصة المتعددة الاختصاصات لمكافحة الجريمة السيبرية لجمع البيانات عن الجرائم السيبرانية وإجراء تحليلات متعمقة بشأنها؛
- نقطة الاتصال التابعة للإنتربول المعنية بالجرائم السيبرانية على مدار الساعة طوال الأسبوع لربط وحدات الجرائم السيبرانية من مختلف البلدان في الوقت الحقيقي من أجل التعاون في مجال إنفاذ القانون؛
- إطار عمل لفريق الإنتربول للاستجابة العالمية للحوادث السيبرانية من أجل تنسيق الاستجابات العالمية في مجال إنفاذ القانون للحوادث السيبرانية الكبرى؛
- فرقة عمل الإنتربول المعنية بالجريمة المالية العالمية من أجل الحد من حجم الجريمة المالية وتأثيرها على نطاق العالم من خلال تعزيز التعاون الدولي والابتكار، مع التركيز على مخططات الاحتيال السيبراني وغسل الأموال.

النهج المتعدد أصحاب المصلحة

تتميز التحقيقات المتعلقة بالجرائم السيبرانية بعدد من التحديات التي لا تحدث في الحيز المادي. وبالنسبة لإنفاذ القانون، من الصعب إدراك وقوع هجوم مباشرةً، وحتى في تلك الحالة تكون معدلات الإبلاغ منخفضة. ويتطلب التحقيق في الجرائم السيبرانية أيضاً مهارات وتكنولوجيات محددة، وهي غير متاحة عالميا. والجريمة السيبرانية، العالمية بطبيعتها، غالباً ما تضر بالاستجابة الفعالة بسبب تزامن وجود الأدلة والمشتبه بهم في عدة ولايات قضائية.

وللتغلب على هذه التحديات، وضع الإنتربول الشراكة في صميم جهوده للتصدي للجرائم السيبرانية. وقد أقرت البلدان الأعضاء، في الدورة الثامنة والثمانين للجمعية العامة للإنتربول التي عقدت في عام 2019، إطارا قانونيا بعنوان "Gateway" يمكن الإنتربول من تبادل المعلومات مع شركات القطاع الخاص[25]. واستند هذا القرار إلى ضرورة أن تعمل أجهزة إنفاذ القانون عن كثب مع القطاع الخاص حيث تكمن غالبية البيانات والخبرات فيما يتعلق بالجريمة السيبرانية.

ويوجد حاليا لدى برنامج الإنتربول العالمي للجريمة السيبرانية 12 شريكا من القطاع الخاص بموجب هذا الإطار، يتبادلون أحدث المعلومات والخبرات في مجال الجرائم السيبرانية، فضلا عن تقديم المساعدة التقنية لوكالات إنفاذ القانون. والوصول إلى البيانات – من القطاعين العام والخاص على حد سواء – يتيح للإنتربول تقديم الدعم التشغيلي والتوجيه التقني المخصصَين للبلدان الأعضاء.

وعلاوة على ذلك، فإن التعاون مع مختلف الجهات الفاعلة في البيئة الإيكولوجية العالمية للأمن السيبراني أمر بالغ الأهمية لأن مجموعات البيانات المتنوعة يمكن أن تساعد في تشكيل سياسات فعالة واستجابات تنفيذية للجرائم السيبرانية. وهذا يساعد أيضا على حشد حكمتنا لنكون مرنين ورشيقين، لا سيما

(25) https://www.interpol.int/ar/News-and-Events/News/2019/INTERPOL-s-General-Assembly-sets-roadmap-for-global-policing.

في أوقات عدم اليقين. وفي نهاية العام الماضي، قدم الإنتربول الدعم للشرطة النيجيرية، بالاشتراك مع شريكه من القطاع الخاص، في اعتقال أعضاء من مجموعة إجرامية منظمة مسؤولة عن شنّ حملات التصيّد الاحتيالي وعمليات الاحتيال لاختراق البريد الإلكتروني للعمل التي تؤثر على الحكومات وشركات القطاع الخاص في أكثر من 150 بلدا[26].

ويركز الإنتربول أيضاً بشكل خاص على الوقاية. وللوقاية من الجرائم السيبرانية، يعمل الإنتربول بشكل وثيق مع شركائه من القطاعين العام والخاص لتشجيع الوقاية السيبرية الجيدة من خلال تنظيم سلسلة من حملات التوعية العالمية. وتدعم هذه الجهود أيضا مؤسسات إنفاذ القانون في التغلب على العديد من التحديات في التصدي للجريمة السيبرانية من خلال زيادة الوعي العام بالجريمة نفسها، وسبل الحماية منها، وما يجب القيام به عند وقوعها.

خاتمة

بما أن الصلة بين الجهات الفاعلة الإجرامية والبنى التحتية والضحايا تتجاوز الحدود والولايات القضائية الوطنية، فإن أجهزة إنفاذ القانون المحلية لا تتمتع دائماً بالقدرات أو الطاقة اللازمة للتصدي لهذه العناصر الانتقالية في التصدي للجريمة السيبرانية. وينبغي للبلدان الأعضاء أن تضع في اعتبارها أن الثغرات في القدرات أو الطاقة السيبرانية لأجهزة إنفاذ القانون في جميع المناطق لا تزال تشكل عامل تمكين رئيسي للشبكات الإجرامية في توزيع هياكلها الأساسية وأنشطتها حيثما يكون مستوى الخطر أدنى.

وللتخفيف من هذه التهديدات والمخاطر المتغيرة باستمرار فيما يتعلق بالفضاء الإلكتروني، ينبغي للبلدان الأعضاء أن تستفيد من التعاون على مستوى الشرطة وأن تزيد من استخدامه إلى أقصى حد لتكون الاستجابة فعالة ومناسبة التوقيت. ومع تواجد محلي للإنتربول في كل بلد، فهو قادر على ربط النقاط؛ وتحديد وتعطيل الجهات الإجرامية الفاعلة في الفضاء الإلكتروني، جنبا إلى جنب مع بلداننا الأعضاء وشركائنا.

ومن الواضح أنه لا يمكن مكافحة الجريمة السيبرانية بفعالية إلا من خلال استجابة منسقة – والأهم من ذلك سريعة – على الصعيد العالمي. ونحن بحاجة إلى حماية النظم وإعداد قياداتنا وتبادل الحلول وتشجيع الاستجابة الصحيحة. وعلى وجه الخصوص، يجب أن تكون أجهزة إنفاذ القانون شريكا موثوقا وفعالا، لأن تبادل البيانات أمر أساسي – بما في ذلك بين قوات الشرطة الوطنية والقطاع الخاص والخبراء العالميين مثل الإنتربول. وزيادة الثقة داخل الأوساط العالمية لأجهزة إنفاذ القانون التي تتخذ موقف "التجرؤ على التبادل" أمر بالغ الأهمية في إطار الهدف المشترك المتمثل في مكافحة الجريمة السيبرانية.

وفي الوقت الذي يخضع فيه المجتمع الدولي لضغوط استثنائية، فإن ضمان أمننا المشترك يقتضي أن نتحرك باتجاه المزيد من التعاون والإدماج. وهذا ما يمثله الإنتربول: المساعدة في التعاون الدولي في مجال إنفاذ القانون من أجل عالم أكثر أمنا. وبما أننا نتشاطر الاقتناع بأن الأمن والعدالة أساسيان لتحقيق فضاء إلكتروني سلمي ومستدام، فإن الإنتربول يعمل إلى جانب الأمم المتحدة من خلال تيسير التعاون الدولي في مجال إنفاذ القانون. ومن أجل إنجاح هذا المسعى، سيواصل الإنتربول دعم بلدانه الأعضاء في مكافحة الجريمة السيبرانية.

(26) https://www.interpol.int/ar/News-and-Events/News/2020/Three-arrested-as-INTERPOL-Group-IB-and-the-Nigeria-Police-Force-disrupt-prolific-cybercrime-group.

المرفق الثامن والثلاثون

بيان الممثل الدائم لجمهورية إيران الإسلامية لدى الأمم المتحدة، مجيد تخت روانجي

يوفر الفضاء الإلكتروني فرصا ذهبية للبشرية لتطوير وتعزيز جميع مناحي حياتها بشكل مستمر. ولذلك، يجب ألا يتم فقط تعزيز عامل التمكين المتميز هذا في جميع أنحاء العالم، وخاصة في البلدان النامية، بل يجب أيضا حمايته من جميع التهديدات.

ويمكن أيضا استخدام الفضاء الإلكتروني لارتكاب أعمال عدوانية أو انتهاكات للسلام أو "التهديد باستعمال القوة أو استعمالها" أو "التدخل في الشؤون التي تكون من صميم السلطان الداخلي لدولة ما" أو لانتهاك سيادة الدول أو للتدخل في شؤون دول أخرى. ويجب أيضا منع هذه الأعمال بفعالية.

وكمبدأ توجيهي، يجب أن تحكم مبادئ وقواعد القانون الدولي "المنطبقة" القائمة، دون سوء تفسير أو تفسير تعسفي بالطبع، حقوق الدول وواجباتها وسلوكها فيما يتعلق بالفضاء الإلكتروني.

ومع ذلك، عندما لا يكون هناك توافق في الآراء بشأن انطباق القانون الدولي، أو حتى عندما يُفتقر للمعايير الدولية المتعلقة بالفضاء الإلكتروني، يجب على المجتمع الدولي أن يعمل من أجل وضع المعايير المطلوبة.

وتحقيقا لهذه الغاية، ونظرا لأن الميثاق يكلف الجمعية العامة بـ "التطوير التدريجي للقانون الدولي وتدوينه"، يجب على الجمعية العامة أن تواصل جهودها المستمرة في وضع وتدوين المبادئ والقواعد الدولية اللازمة للفضاء الإلكتروني، بما في ذلك في شكل صك دولي ملزم قانونا.

وبالتوازي مع هذه الجهود، يجب على الدول أن تبذل كل جهد ممكن للتشجيع على توسيع نطاق استخدام الفضاء الإلكتروني إلى أقصى حد ممكن من أجل تنميتها، وأن تتصرف لدى قيامها بذلك بمسؤولية ووفقا للقانون الدولي المنطبق، ولا سيما مقاصد الأمم المتحدة ومبادئها.

وتقع المسؤولية الرئيسية عن الحفاظ على فضاء إلكتروني منيع وآمن وموثوق به على عاتق فرادى الدول. ولذلك، ونظرا للوضع الراهن والمعقد لإدارة الفضاء الإلكتروني، يجب تعزيز وضمان الدور البارز والمشاركة الجادة للدول في إدارة بيئة الفضاء الإلكتروني على الصعيد العالمي، ولا سيما في مجال السياسات وصنع القرار.

وفي الوقت نفسه، يجب تطوير إدارة الفضاء الإلكتروني المتوخاة بطريقة لا تؤثر سلبا على حقوق الدول في اختياراتها المتعلقة بالتنمية والإدارة والتشريع فيما يتعلق ببيئة الفضاء الإلكتروني.

ويجب احترام كامل حق الدول في "الوصول الحر إلى المعلومات وفي تطوير نظامها الإعلامي ووسائط إعلامها الجماهيري تطويرا تاما دون تدخل، وفي استخدام وسائط إعلامها الجماهيري في تعزيز مصالحها وأمانيها السياسية والاجتماعية والاقتصادية والثقافية" وكذلك "حق الدول وواجبها، داخل إطار حقوقها الدستورية، في مكافحة نشر الأنباء الكاذبة أو المشوهة"، الذي جددت تأكيده الجمعية العامة أيضا في "إعلان عدم جواز التدخل بجميع أنواعه في الشؤون الداخلية للدول" لعام 1981.

ويجب على الدول، لدى اضطلاعها بمسؤولياتها عن الحفاظ على فضاء إلكتروني منيع وآمن وموثوق به، أن تعتمد نهجا تعاونيا بدلا من نهج المواجهة.

وكما أكدت الجمعية العامة في "إعلان عدم جواز التدخل في الشـــؤون الداخلية للدول، وحماية استقلالها وسيادتها" لعام 1965، "ليس لأية دولة حق التدخل، بصورة مباشرة أو غير مباشرة ولأي سبب كان، في الشؤون الداخلية أو الخارجية لأية دولة أخرى". ولذلك، يجب على جميع الدول أن تمنع وتمتنع عن القيام بهذه الأعمال، في جملة أمور، ضد العناصر السياسية والاقتصادية والثقافية أو البنى التحتية الحيوية للدول المرتبطة بالفضاء الإلكتروني، بما في ذلك من خلال الطرق والوسائل المرتبطة بالفضاء الإلكتروني.

وعلاوة على ذلك، فإن الجمعية، من خلال "إعلان عدم جواز التدخل بجميع أنواعه في الشـــؤون الداخلية للدول" لعام 1981، أعادت تأكيد واجب الدولة "في ضمان عدم استخدام إقليمها على أي نحو فيه انتهاك لسيادة دولة أخرى ولاستقلالها السياسي وسلامتها الإقليمية ووحدتها الوطنية أو زعزعة لاستقرارها السياسي والاقتصادي والاجتماعي"؛ و "الامتناع عن أي إجراء أو أية محاولة بأي شكل من الأشكال أو بأي حجة كانت بهدف زعزعة أو تقويض استقرار دولة أخرى أو أي من مؤسساتها"، وكذلك "الامتناع عن القيام بأي حملة تشهيرية أو قذف أو دعاية عدائية بغرض التدخل بأي شكل في الشؤون الداخلية لدول أخرى". ويجب على الدول أيضا أن تراعي هذه القواعد فيما يتعلق بالفضاء الإلكتروني.

ووفقا لأحد المبادئ التي أعادت تأكيدها الجمعية العامة في "إعلان مبادئ القانون الدولي المتعلقة بالعلاقات الودية والتعاون بين الدول وفقاً لميثاق الأمم المتحدة" لعام 1970، يجب على الدول ألا تســـتخدم أي "نوع من التدابير لإجبار دولة أخرى على التبعية لها في ممارسة حقوقها السيادية وللحصول منها على أية مزايا". وبناء عليه، لا يجوز للدول أن تستخدم أوجه التقدم في مجال الفضاء الإلكتروني كأدوات لاتخاذ تدابير اقتصادية أو سياسية أو أي نوع آخر من التدابير القسرية، بما فيها من خلال تدابير فرض القيود أو العرقلة ضد دول أخرى.

وبالمثل، يجب على الدول أن تمتنع عن التهديد باستعمال القوة أو استعمالها داخل بيئة الفضاء الإلكتروني أو عبرها. ويجب عليها أن تمتنع أيضاً عن إساءة استخدام سلاسل الإمداد الخاصة بالفضاء الإلكتروني التي تُنشأ تحت رقابتها وولايتها من أجل إحداث، أو المساعدة في إيجاد، نقاط ضعف في المنتجات والخدمات والصيانة بما ينتهك سيادة دول أخرى وحماية البيانات فيها، وينبغي لها أن تمنع حدوث ذلك.

ويجب على الدول أيضا أن تمارس الرقابة الواجبة على الشركات والمنصات المتصلة بالفضاء الإلكتروني والخاضعة لولايتها القضائية، وأن تتخذ التدابير المناسبة لجعلها مسؤولة عن سلوكها في بيئة تكنولوجيا المعلومات والاتصالات، بما في ذلك انتهاك السيادة الوطنية للدول الأخرى وأمنها ونظامها العام. وعلى أي حال، فإن الدول مسؤولة عن أفعالها غير المشروعة دوليا داخل الفضاء الإلكتروني أو عبره.

وعلاوة على ذلك، يجب تسوية جميع المنازعات الدولية المتصلة بالفضاء الإلكتروني بالوسائل السلمية حصرا، وعلى أساس "تساوي الدول في السيادة وفقا لمبدأ حرية الاختيار بين الوسائل" كما جاء في "إعلان مانيلا بشأن تسوية المنازعات الدولية بالوسائل السلمية" لعام 1970.

ومن الجدير بالذكر في هذا الســـياق أننا شـــهدنا خلال الســـنوات الأخيرة اتجاها مثيرا للقلق من الاتهامات المنهجية من جانب بعض الدول ضـد دول أخرى بشـن هجمات سـيبرانية أو أنشـطة مماثلة في الفضاء الإلكتروني. ونظرا للتحديات القائمة المرتبطة بإسناد المسؤولية في بيئة الفضاء الإلكتروني، فضلا عن عدم وجود مجموعة من المعايير الموضـــوعة دوليا والمتفق عليها بشـــأن ما يعتبر دليلا حقيقيا وموثوقا وكافيا لإثبات المسؤولية، يجب اعتبار هذه الاتهامات ذات دوافع سياسية فحسب.

وبصورة عامة، يجب أن يُستخدم الفضاء الإلكتروني وما يتصل به من وسائل وتقنيات وتكنولوجيات حصرا للأغراض السلمية، وتحقيقا لهذه الغاية، يجب على الدول أن تتصرف بشكل تعاوني ومسؤول بما يتفق تماما مع القانون الدولي المعمول به.

وأخيرا، نتشاطر الآراء بأنه يجب مواصلة النظر في المسائل المتصلة بالفضاء الإلكتروني في الجمعية العامة. وجمهورية إيران الإسلامية من جانبها، باعتبارها إحدى ضحايا الهجمات السيبرانية، من خلال الدودة الحاسوبية الخبيثة ستاكسنت (Stuxnet) – التي يُعتقد أن الولايات المتحدة والنظام الإسرائيلي قد صنعاها معا للإضرار بالمنشآت النووية الإيرانية السلمية – تقف على أهبة الاستعداد للمساهمة في جهود الجمعية في وضع المبادئ والقواعد اللازمة للفضاء الإلكتروني.

المرفق التاسع والثلاثون

بيان البعثة الدائمة لإيطاليا لدى الأمم المتحدة

تثني إيطاليا على إستونيا لتوجيهها انتباه مجلس الأمن إلى مسألة الأمن السيبراني، ويسرها أن تشارك في المناقشة المفتوحة اليوم.

ونقدر أيضا دعم وتفاني الممثلة السامية لشؤون نزع السلاح، السيدة ناكاميتسو، واستعدادها لتقديم إحاطة إلى مجلس الأمن في الوقت الذي يساور القلق فيه الدول الأعضاء إزاء تزايد عدد حوادث الأمن السيبراني.

وتؤيد إيطاليا بيان الاتحاد الأوروبي وتود أن تضيف الملاحظات التالية بصفتها الوطنية.

ما كان لتوقيت هذه المناقشة أن يكون أكثر ملاءمة. فقد اعترفت الجمعية العامة بالعمل الذي اضطلعت به اللجنة الأولى في السنتين الماضيتين فيما يتعلق بالتطورات في ميدان تكنولوجيات المعلومات والاتصالات بشأن الأمن الدولي والنهوض بالسلوك المسؤول للدول في الفضاء الإلكتروني. ويمثل التقريران اللذان اعتمدهما الفريق العامل المفتوح العضوية وفريق الخبراء الحكوميين خلال هذا الفصل إنجازين هامين ينبغي أن يسهما في بناء الثقة بين الدول الأعضاء. كما سلطا الضوء على مجال كان يعتبر لسنوات عديدة مجالا تقنيا محضا.

ووتيرة الرقمنة تتسارع على الصعيد العالمي، وإلى جانب الفوائد المرتبطة بهذا التطور، يظهر التحدي المتمثل في الحفاظ على الفضاء الإلكتروني كمجال عالمي ومفتوح ومستقر. والتزايد الذي شهدته الأشهر الأخيرة في الحوادث، التي تستهدف في بعض الأحيان البنى التحتية الحيوية وتفرض تكاليف باهظة على اقتصادات العالم، أمر مؤسف. وقد قدمت بعض الهجمات لمحة عن الخسائر في الأرواح البشرية التي يمكن أن تتسبب بها هذه الأعمال، ولا سيما أثناء الجائحة. ويتزايد وضوح الإمكانيات التدميرية لإساءة استخدام التكنولوجيات الجديدة، وكذلك الحاجة إلى إبقائها تحت السيطرة. وتعتقد إيطاليا أن الأمم المتحدة هي الأقدر على النهوض بهذه المهمة وتعزيز السلام والاستقرار في الفضاء الإلكتروني.

وتود إيطاليا أن تكرر بيان الاتحاد الأوروبي فيما يتعلق بانطباق القانون الدولي في الفضاء الإلكتروني، بما في ذلك القانون الدولي الإنساني والقانون الدولي لحقوق الإنسان، وأهمية التقيد بمعايير السلوك المسؤول للدول، وفائدة تدابير بناء الثقة كوسيلة عملية لمنع نشوب النزاعات. ونود أيضا أن نسلط الضوء على الدور الهام الذي يمكن للمنظمات الإقليمية أن تؤديه في مجال الأمن السيبراني. وبصفتنا من المؤيدين بشدة لتعددية الأطراف، فإننا نشجع الحوار بين الأمم المتحدة والمنظمات الإقليمية، ونرحب في هذا الصدد بالمناقشات التي جرت مؤخرا بين الأمين العام للأمم المتحدة والمجلس الأوروبي، بوصفها فرصة قيمة لتبادل الآراء بشأن التحديات التي نواجهها. ونقدر أيضا جهود الرئاسة السويدية لمنظمة الأمن والتعاون في أوروبا، التي تبرز الصلات بين حقوق الإنسان والمسائل الجنسانية والأمن السيبراني.

وفي عالم يزداد ترابطاً، تتزايد أهمية الحوار لتعزيز التفاهمات المشتركة وزيادة فرص التعاون. وبهذه الروح، نؤيد حوار الاتحاد الأوروبي مع الأمم المتحدة ومع المنظمات الإقليمية، ولا سيما الاتحاد الأفريقي، والمنتدى الإقليمي لرابطة أمم جنوب شرق آسيا، ومكتب المستشار الخاص.

ومن خلال المنظمات الإقليمية، يمكن للدول الأعضاء أن تزيد اتصالاتها الثنائية إلى أقصى حد، وأن تتشاطر أفضل الممارسات والدروس المستفادة، مما يضمن عدم تباين النهج الإقليمية. وينبغي تكريس المزيد من الجهود لآليات التسوية السلمية للمنازعات، فضلا عن المبادرات الرامية إلى تطوير الدبلوماسية والوساطة المتعلقتان بمسائل الفضاء الإلكتروني.

ونعتقد أن المجال السيبراني ينبغي أن يظل مفتوحا وحرا وآمنا ومستقرا، كوسيلة للدول لتنفيذ سياسات تمكن المجتمعات من الازدهار وضمان التنمية المستدامة للجميع، مما يسهم في تحقيق أهداف التنمية المستدامة. ولا يمكن التقليل من أهمية بناء القدرات، لأنها تضمن تجانس قدرة الدول على الصمود، وترفع الوعي وتحفز تنمية القدرات. ولا يزال هناك الكثير مما ينبغي عمله في هذا القطاع، ونحن نعتقد أن برنامج العمل للارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني، الذي نروج له مع 52 دولة عضوا أخرى، يمكن أن يمثل منبرا ذا أولوية لتنسيق هذا المسعى وتشجيعه. وقد أعلنا بالفعل عن استعدادنا لمواصلة تبادل الآراء بشأن هذه المبادرة في سياق مناقشات اللجنة الأولى، ونود أن نكرر تأكيد عزمنا اليوم. ويمكن لبرنامج العمل أن يكون أيضا بمثابة المنتدى الذي يتشكل فيه النهج المتعدد أصحاب المصلحة وتقام فيه الشراكات بين القطاعين العام والخاص.

وقد شكلت الجائحة نكسة هائلة خلال عامي 2020 و 2021. وينبغي لجهودنا المشتركة أن تركز على إعادة إطلاق التنمية المستدامة، والمجال السيبراني عنصر أساسي لذلك. وتعمل إيطاليا على تحقيق هذا الهدف بصفتها عضوا في مجموعة الدول السبع، وهي تروج لهذه الرؤية في سياق رئاستها الحالية لمجموعة العشرين. وتمثل مناقشة اليوم خطوة حيوية باتجاه رفع الوعي وضمان حدوث التطورات المرتبطة بالرقمنة في مجال سيبراني آمن ومستقر، مع الحيلولة دون تقويض أي جهد.

وتجري هذه المناقشة في الوقت الذي يجتمع فيه وزراء خارجية مجموعة العشرين في ماتيرا لمناقشة مسائل التعافي والتنمية المستدامة، بهدف عدم ترك أحد خلف الركب. ويحدونا الأمل في أن تعزز هذه الجهود بعضها بعضا وأن يواصل مجلس الأمن التركيز على المسائل السيبرانية، ورصد التقدم المحرز، والاستعداد لدعوة الدول غير الممتثلة إلى الوفاء بالتزاماتها. ونأمل أن تكون هذه الحالات قليلة جدا مع تلاقي الدول الأعضاء حول ضرورة تكريس الوقت والجهد اللازمين لوضع برنامج إيجابي للأمن السيبراني يعزز الثقة والشفافية والشمولية.

المرفق الأربعون

بيان السفير المعني بشؤون الأمم المتحدة والسياسات السيبرانية في وزارة خارجية اليابان، أكاهوري تاكيشي

تود اليابان أن تعرب عن خالص تقديرها لكايا كالاس، رئيسة وزراء جمهورية إستونيا، لتنظيم هذه المناقشة المفتوحة بشأن الأمن السيبراني. وتشكر اليابان إستونيا على اعترافها في مذكرتها المفاهيمية بالمناقشة المفتوحة حول التحديات المعاصرة المعقدة التي تواجه السلام والأمن الدوليين، التي نظمت عام 2017 تحت رئاسة اليابان.

وترحب اليابان باعتماد تقرير الفريق العامل المفتوح العضوية في آذار/مارس وتقرير فريق الخبراء الحكوميين السادس في أيار/مايو، بتوافق الآراء.

وتكمن القيمة الأكبر لتقرير الفريق العامل المفتوح العضوية في اعتماده بتوافق الآراء في عملية تمكنت فيها جميع الدول الأعضاء من المشاركة الكاملة. وأكدت الدول الأعضاء على انطباق التشريعات بشكل مباشر، بما في ذلك القانون الدولي، ولا سيما ميثاق الأمم المتحدة برمته، على الفضاء الإلكتروني.

ولتقرير فريق الخبراء الحكوميين قيمة إضافية. فبالنسبة لكل من القواعد الـ 11 المدرجة في تقرير فريق الخبراء الحكوميين لعام 2015، يقدم التقرير الجديد إرشادات وأمثلة عن التنفيذ. وتأمل اليابان أن يزيد هذا المضمون من تعزيز التعاون بين الدول في النهوض بالسلوك المسؤول للدول. وبالإضافة إلى ذلك، أصبح من الواضح الآن أن الأفعال غير المشروعة دوليا التي تعزى إلى دولة ما تستتبع مسؤولية الدولة. وانطباق القانون الدولي الإنساني منصوص عليه بشكل واضح. وأشار الفريق مرة أخرى إلى الحق الأصيل للدول في اتخاذ التدابير المعترف بها في الميثاق.

ونحن نتطلع إلى تعميق المناقشات الملموسة بشأن تطبيق القانون الدولي في الفضاء الإلكتروني في مختلف المنابر في المستقبل. وتأمل اليابان أن تسهم ورقة الموقف، التي قدمتها في إطار خلاصة فريق الخبراء الحكوميين للمواقف الوطنية، في هذه المناقشات. وأود هنا أن أشاطركم أهم النقاط الأساسية في موقف اليابان.

ترى اليابان أنه يجب ألا تنتهك دولة ما سيادة دولة أخرى عن طريق العمليات السيبرانية. وعلاوة على ذلك، يجب ألا تتدخل دولة ما في المسائل الداخلة في نطاق الولاية القضائية المحلية لدولة أخرى عن طريق العمليات السيبرانية. وتنطوي الأفعال غير المشروعة دوليا التي ترتكبها دولة ما في الفضاء الإلكتروني على مسؤولية الدول.

وعلى الدول التزام ببذل العناية الواجبة فيما يتعلق بالعمليات السيبرانية بموجب القانون الدولي. وترتبط القاعدتان 13 (ج) و (و) والجملة الثانية من الفقرة 71 (ز) من تقرير فريق الخبراء الحكوميين لعام 2021 بهذا الالتزام. وفيما يتعلق بالحادث الأخير الذي أصاب خط الأنابيب "كولونيال"، أشار رئيس الولايات المتحدة إلى أن هناك جهوداً تبذل باتجاه وضع "نوع من المعايير الدولية يقضي بأن تتحرك الحكومات التي تعلم بحصول أنشطة إجرامية انطلاقاً من أراضيها لوقف تلك المشاريع الإجرامية". ونحن نسلم بصعوبة إسناد مسؤولية العمليات السيبرانية إلى دولة ما. وقد يوفر التزام العناية الواجبة أسبابًا للاحتجاج بمسؤولية الدولة التي نشأت من أراضيها عملية سيبرانية غير منسوبة إلى أي دولة.

ويجب تسوية أي نزاع دولي ينطوي على عمليات سيبرانية بالوسائل السلمية عملا بالمادة 2 (3) من ميثاق الأمم المتحدة. ولضمان التسوية السلمية للمنازعات، ينبغي استخدام سلطات مجلس الأمن استنادا إلى الفصلين السادس والسابع من ميثاق الأمم المتحدة ووظائف أجهزة الأمم المتحدة الأخرى في المنازعات الناشئة عن العمليات السيبرانية. ولليابان تحفظات على فكرة إنشاء آلية دولية جديدة للإسناد.

وترى اليابان أنه عندما تشكل عملية سيبرانية هجوما مسلحا بموجب المادة 51 من ميثاق الأمم المتحدة، يجوز للدول أن تمارس الحق الأصيل في الدفاع عن النفس الفردي أو الجماعي المعترف به بموجب نفس المادة.

وينطبق القانون الدولي الإنساني على العمليات السيبرانية. ويسهم هذا التأكيد في تنظيم أساليب ووسائل الحرب. والحجة القائلة بأن التأكيد سيؤدي إلى عسكرة الفضاء الإلكتروني لا أساس لها من الصحة.

وينطبق القانون الدولي لحقوق الإنسان أيضاً على العمليات السيبرانية. ويتمتع الأفراد، فيما يتعلق بالعمليات السيبرانية، بنفس حقوق الإنسان التي يتمتعون بها بخلاف ذلك.

وفيما يتصل بالعلاقة بين القانون الدولي والقواعد الطوعية، من الضروري، من أجل تثبيت استقرار الفضاء الإلكتروني، أن يعمل القانون الدولي والقواعد الدولية معا لمنع الأفعال غير المشروعة دوليا باستخدام تكنولوجيا المعلومات والاتصالات وتعزيز السلوك المسؤول للدول في الفضاء الإلكتروني. وكما ورد بوضوح في تقرير الفريق العامل المفتوح العضوية، فإن القواعد لا تحل محل التزامات الدول بموجب القانون الدولي أو تغيرها.

وتأمل اليابان أن يقوم عدد كبير من الدول الأعضاء بنشر مواقفها الوطنية طوعا بشأن كيفية تطبيق القانون الدولي.

وتعتقد اليابان أن الوقت قد حان لإيلاء الأولوية لتنفيذ القواعد والالتزامات الطوعية المتفق عليها بموجب القانون الدولي، إلى جانب تدابير بناء الثقة وتدابير بناء القدرات.

وفي سياق التنفيذ، تود اليابان أن تدعو الحكومات إلى أن تعلن بشكل استباقي عن تقييمها القانوني عند حدوث عملية سيبرانية خبيثة، بما في ذلك، في جملة أمور، عما إذا كانت تشكل انتهاكا للقانون الدولي. وستعزز هذه الممارسة الفهم المشترك بشأن كيفية انطباق القانون الدولي على العمليات السيبرانية. وسيكون لتطبيق القانون الدولي من قبل المحاكم والهيئات القضائية الدولية والمحلية على الحوادث السيبرانية تأثير مماثل. وتأمل اليابان أن يردع تراكم هذه الممارسة الأنشطة الخبيثة في الفضاء الإلكتروني.

وتؤيد اليابان بقوة برنامج العمل. ونعتقد أن برنامج العمل سيكون بمثابة آلية فعالة لتأمين ورصد تنفيذ المعايير المتفق عليها، والالتزامات بموجب القانون الدولي، وتدابير بناء الثقة وبناء القدرات. ونحن نتطلع إلى تعميق المناقشات بشأن برنامج العمل. وسنواصل أيضا المشاركة بشكل استباقي في الفريق العامل الجديد المفتوح العضوية.

واليابان ملتزمة بحماية فضاء إلكتروني حر ومنصف وآمن، وستواصل الإسهام بنشاط في المناقشات والجهود الرامية إلى تعزيز سيادة القانون في الفضاء الإلكتروني، بما في ذلك في الأمم المتحدة.

المرفق الحادي والأربعون

بيان الممثل الدائم لكازاخستان لدى الأمم المتحدة، ماغزان إلياسوف

نود أن نعرب عن امتناننا للرئاسة الإستونية لتنظيم وإجراء المناقشة المعنونة "صون السلام والأمن الدوليين: الأمن السيبراني".

وفي ظروف تسودها التهديدات على الصعيد العالمي، فإن ضمان الأمن يتطلب التنسيق في إطار المجتمع الدولي وتسوية الجوانب العديدة ذات الطابع السياسي والاقتصادي. وفي هذا السياق، تجدر الإشارة إلى ظهور عنصر جديد ومعقد في الوقت نفسه في العالم، وهو الأمن السيبراني.

وينبغي أن يكون واضحا أن لتكنولوجيات المعلومات والاتصالات إمكانات هائلة لتنمية الدول. وهي في الوقت نفسه تتيح فرصا جديدة للجناة وقد تسهم في زيادة مستويات الجريمة وتعقيدها، والخطر المحتمل لإساءة استخدام التكنولوجيات الناشئة، بما في ذلك الذكاء الاصطناعي. وفي هذا الصدد، ينبغي أن يكون منع وقمع استخدام تكنولوجيات المعلومات والاتصالات لأغراض إجرامية بمثابة أولوية لعمل الدول في المرحلة الراهنة.

ونحن نرحب في هذا الصدد بإنشاء لجنة خبراء حكومية دولية مخصصة مفتوحة العضوية، تُمثَّل فيها جميع المناطق، لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، مع المراعاة الكاملة للصكوك الدولية القائمة وللجهود المبذولة على كل من الصعيد الوطني والإقليمي والدولي لمكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، على النحو المتوخى في القرار 247/74 الذي اتخذته الجمعية العامة في 27 كانون الأول/ديسمبر 2019.

ونعتقد أن عمل الأمم المتحدة في هذا المجال سيتأثر على نحو أكبر بالتقرير الموضوعي النهائي للفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي الذي اعتُمد في آذار/مارس 2021، وبتوافق الآراء المعبَّر عنه في القرار 240/75 الذي أُنشئ بموجبه فريق عاملا مفتوح العضوية معني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025، وكذلك بالتقرير المعتمد بتوافق الآراء من جانب فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي في أيار/مايو 2021.

وينبغي 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 بهذا المجال.

وفي هذا الصدد، نرحب بعملية التفاوض بشأن الأمن السيبراني في الأمم المتحدة وتفهم المشاركين والدول الأعضاء أن جميع القرارات بشأن جدول الأعمال المحدد هذا يجب أن تتخذ بتوافق الآراء.

المرفق الثاني والأربعون

بيان البعثة الدائمة للاتفيا لدى الأمم المتحدة

لقد أتاحت التطورات في تكنولوجيات المعلومات والاتصالات للدول والمجتمعات عددا لا يحصى من الفوائد في مجالات الاقتصاد والخدمات والتعليم والاتصال. وإلى جانب الآثار الإيجابية إلى حد كبير لتطبيق تكنولوجيا المعلومات والاتصالات، تشعر لاتفيا بقلق متزايد إزاء الآثار المترتبة على الاستخدام الخبيث والمعرقل لتكنولوجيا المعلومات والاتصالات، مع ما يترتب على ذلك من آثار على السلام والأمن والاستقرار وحقوق الإنسان على الصعيد الدولي.

وفي أغلب الأحيان تعاني الدول من هذه الجرائم، بما فيها تلك التي تمس بالمؤسسات الديمقراطية والبنى التحتية الحيوية. ومما يثير الجزع أكثر أن الأنشطة السيبرانية الخبيثة تستغل جائحة مرض كورونا مستهدفة نظم الرعاية الطبية الضرورية للحفاظ على الصحة البشرية، وبحوث اللقاحات، فضلا عن حيز المعلومات.

وقد أكدت المشاركة الواسعة والمناقشة التي جرت في اجتماع مجلس الأمن التابع للأمم المتحدة المعقود بصيغة آريا في العام الماضي على الأهمية المتزايدة للأمن السيبراني بالنسبة لجدول أعمال السلام والاستقرار الدوليين. ولذلك، فإن الوقت مناسب وملائم لإدراج مسألة الأمن السيبراني في جدول الأعمال الرسمي لمجلس الأمن. وتؤيد لاتفيا تأييدا كاملا جهود إستونيا للتفكير على النحو الواجب في التخفيف من حدة أثر السلوك غير المسؤول في الفضاء الإلكتروني على السلام والأمن الدوليين.

ويجب أن تظل الأمم المتحدة طرفاً عالميا هاما لتعزيز السلام والأمن والاستقرار، بما في ذلك في الفضاء الإلكتروني. وقد أرسى العمل الفعال الذي قام به فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي والفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي على مدى السنوات الماضية، أسساً متينة لمناقشة اليوم.

ويمثل التقريران النهائيان اللذان يستندان إلى توافق الآراء لفريق الخبراء الحكوميين والفريق العامل المفتوح العضوية منطلقين مرحب بهما لمواصلة العمل بغية التوصل إلى تفاهم مشترك بشأن طائفة واسعة من المسائل.

وفي هذا الصدد، فإن برنامج العمل المتعلق بالاستخدام المسؤول لتكنولوجيا المعلومات والاتصالات من جانب الدول في سياق الأمن الدولي هو نتيجة قيّمة لتقريري فريق الخبراء الحكوميين والفريق العامل المفتوح العضوية. وينبغي أن يكون برنامج العمل المتصل بالمسائل السيبرانية بمثابة أساس متين، والأهم من ذلك عملي المنحى، من أجل مواصلة العمل بغية إحراز تقدم ملموس في تنفيذ معايير السلوك المسؤول.

وفي هذا السياق، تود لاتفيا أن تؤكد على الطابع المتعدد أصحاب المصلحة للفضاء الإلكتروني، الذي يتطلب مشاركة مجموعة من الجهات غير الحكومية من القطاع الخاص والمجتمع المدني والأوساط الأكاديمية في المناقشات. وبالنظر إلى ما لهذه الجهات من مصالح هامة في النظام الإيكولوجي لتكنولوجيا المعلومات والاتصالات، فإنها يمكن أن تسهم إسهاما كبيرا بطرق مختلفة عديدة، من خلال تشاطر وجهات نظرها ومعارفها وخبراتها.

وينبغي للدول أن تواصل العمل بفعالية وأن تكون على أهبة الاستعداد لإجراء مناقشات متعمقة في إطار عمليات الأمم المتحدة المقبلة للارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي. وبينما يتعين علينا جميعا أن نعمل بلا كلل لتعزيز حماية وأمن تكنولوجيا المعلومات والاتصالات الخاصة بنا، ينبغي للدول ألا تسمح لجهات أخرى حكومية أو غير حكومية باستخدام تكنولوجيا المعلومات والاتصالات داخل أراضيها لارتكاب أفعال غير مشروعة دوليا. وندعو جميع الدول إلى الامتناع عن القيام بأنشطة لا تتفق مع القانون الدولي، بما في ذلك ميثاق الأمم المتحدة، أو تمكينها أو التسامح معها، لتجنب عرقلة الأمن المرتبط باستخدام تكنولوجيا المعلومات والاتصالات. ويجب أن تكون المسؤولية وبناء الثقة والقدرة على التنبؤ بمثابة عناصر رئيسية للتعاون الدولي في مجال الأمن السيبراني.

ولمنع حالات سوء الفهم والتصورات الخاطئة من جهة، ولإرساء ممارسة التواصل بشأن حوادث تكنولوجيا المعلومات والاتصالات من جهة أخرى، يجب أن ننشئ قنوات اتصال مفتوحة بين الدول الأعضاء. ويمكن لإنشاء شبكة لجهات الاتصال على الصعيدين السياساتي والتقني في الأمم المتحدة أن يقدم مساهمة مجدية في إقامة اتصالات أكثر فعالية على الصعيد العالمي. وقد أثبتت شبكة جهات الاتصال فعاليتها بالفعل على الصعيد الإقليمي في منظمة الأمن والتعاون في أوروبا.

وأخيرا، تود لاتفيا أن تشيد بجميع الدول الأعضاء لإثبات التزامها بالتعاون والعمل معا من أجل التوصل إلى توافق في الآراء بشأن التقريرين الصادرين في إطار عمليتي فريق الخبراء الحكوميين والفريق العامل المفتوح العضوية. فهذا هو السبيل الصحيح، وهو يمثل فرصة ممتازة لزيادة تعزيز التعاون الدولي من أجل فضاء إلكتروني عالمي ومفتوح ومستقر وسلمي وآمن تطبق فيه حقوق الإنسان والحريات الأساسية وسيادة القانون تطبيقا كاملا.

المرفق الثالث والأربعون

بيان القائم بالأعمال بالنيابة ونائب الممثل الدائم لليختنشتاين لدى الأمم المتحدة، غيورغ شبارير

لقد مثلت العمليات السيبرانية عامل توازن في الحروب الحديثة من خلال توفير سبل جديدة للعمليات الهجومية والدفاعية على حد سواء لجميع الجهات الفاعلة، بما فيها تلك التي تملك موارد أقل. ونتيجة لذلك، ازدادت وتيرة العمليات السيبرانية وشدتها في السنوات الأخيرة، مهددةً السلام والأمن الدوليين. ومن المثير للقلق أن هذه الهجمات تنطوي على إمكانية التسبب بمعاناة خطيرة للسكان المدنيين، بما يشمل إيقاع خسائر في الأرواح وتعطيل الخدمات الأساسية. وفي هذا السياق، نشير إلى أن الدول تتفق بشكل متزايد على أن القانون الدولي، وتحديداً ميثاق الأمم المتحدة برمته وقواعد القانون الدولي العرفي المستمدة من مبادئ الميثاق، فضلاً عن نظام روما الأساسي للمحكمة الجنائية الدولية والقانون الدولي الإنساني، تنطبق على الفضاء الإلكتروني.

وقد قام الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي بإضفاء طابع مؤسسي على المناقشات المتعلقة بالسلام والأمن الدوليين في سياق الشؤون السيبرانية داخل الأمم المتحدة. وعلاوة على ذلك، فإن التقرير النهائي الذي أصدره فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي (فريق الخبراء الحكوميين) يؤكد من جديد على انطباق القانون الدولي في الفضاء الإلكتروني وعلى ضرورة تطبيقه. وتحيط ليختنشتاين علما بالمساهمات المجمعة للفريق العامل المفتوح العضوية وفريق الخبراء الحكوميين في تعزيز المناقشة بشأن كيفية انطباق القانون الدولي، ولا سيما ميثاق الأمم المتحدة، على الفضاء الإلكتروني.

ويمثل حظر استعمال القوة أحد الإنجازات التاريخية لميثاق الأمم المتحدة. ويُحظَر استعمال القوة إلا إذا أذن به مجلس الأمن بموجب الفصل السابع أو في حال الدفاع عن النفس بموجب المادة 51 من الميثاق. غير أن الاحتجاج بالمادة 51 يتزايد كأساس قانوني لاستعمال القوة دون مبررات قانونية ضرورية. وهناك خطر كبير من امتداد هذا الاتجاه إلى الفضاء الإلكتروني مع تطور التكنولوجيات الجديدة وقدرات الدول. وينبغي أن نضمن عدم تيسير الفضاء الإلكتروني لعمليات الدفاع عن النفس غير المبررة. ونذكر بأن الاحتجاج بالمادة 51 يتطلب بشكل استباقي دليلا على قرب وقوع هجوم مسلح، ويتطلب دائما إثبات الضرورة وتناسب التدابير المتخذة في الرد.

ويتوقع ميثاق الأمم المتحدة من مجلس الأمن الاضطلاع بدور إنفاذي فيما يتعلق بأخطر الانتهاكات للقواعد ذات الصلة بموجب القانون الدولي التي ترقى إلى مستوى الأعمال العدوانية. وبالإضافة إلى الأدوات الواردة في الميثاق، فإن أمام المجلس الآن أيضا خيار تحميل المسؤولية الجنائية الفردية لمرتكبي جريمة العدوان عن طريق إحالة الحالات ذات الصلة إلى المحكمة الجنائية الدولية. وفي هذا السياق، تعتقد ليختنشتاين أن وجود فهم واضح لكيفية تطبيق نظام روما الأساسي على العمليات السيبرانية سيساعد في توجيه عمل المجلس.

وفي محاولة لتوضيح تطبيق نظام روما الأساسي على العمليات السيبرانية، أنشأت ليختنشتاين، إلى جانب عشر دول أطراف أخرى في المحكمة الجنائية الدولية، مجلسا للمستشارين لاستكشاف دور

المحكمة في وضع ضوابط للحرب السيبرانية. وقد اجتمع مجلس المستشارين، المؤلف من 16 محاميا دوليا بارزا، ثلاث مرات خلال العامين 2019 و 2020 لمناقشة مدى انطباق الأحكام الأساسية في نظام روما الأساسي على العمليات السيبرانية. ومن المقرر تقديم تقرير نهائي هذا العام. ونأمل أن يسهم ذلك في الفهم المشترك للمساءلة في سياق العمليات السيبرانية فضلا عن ردع هذه الجرائم في المقام الأول.

وتؤكد ليختنشتاين على الحاجة إلى إطار قانوني متين لتنظيم الفضاء الإلكتروني من أجل السلام والأمن الدوليين. ويسرنا أن نسهم في الجهود العالمية لمكافحة العمليات السيبرانية الخبيثة من خلال تقريرنا المقبل الذي يركز على نظام روما الأساسي، وسنواصل السعي من أجل السلام والأمن الدوليين بالتزامنا الثابت بالقانون الدولي.

المرفق الرابع والأربعون

بيان البعثة الدائمة لمالطة لدى الأمم المتحدة

تعرب مالطة عن شكرها لإستونيا لتنظيم هذه المناقشة في الوقت المناسب بشأن مسألة نعتقد أنها ينبغي أن تحتل الصدارة في جدول أعمال مجلس الأمن. وعلى الرغم من التلميح إلى مسائل الأمن السيبراني في عدد من مناقشات مجلس الأمن، نعتقد أنه ينبغي إيلاؤها مزيدا من الأهمية، بالنظر إلى أنها تمثل أحد أهم التحديات المتغيرة باستمرار التي تواجه السلام والأمن الدوليين.

وتؤيد مالطة البيان الذي أدلى به الاتحاد الأوروبي، وتود إلقاء الضوء على بضع نقاط بصفتها الوطنية. لقد صاحب التطور في الفضاء الإلكتروني عدد من الفرص للدول الأعضاء والمواطنين في جميع أنحاء العالم، وأدى إلى زيادة الرخاء والقدرة على الاتصال والنمو الاقتصادي. غير أن المجال السيبراني فتح الباب أيضا أمام الأنشطة الخبيثة الرامية إلى تعطيل واستغلال مواطن الضعف في المجتمعات وشن هجمات يمكن أن يكون لها تأثير كبير على الدول الأعضاء ومواطنيها، من حيث البيانات الحساسة والبنى التحتية الحيوية على سبيل المثال. وفي الواقع أننا كلما تحولنا نحو العالم الافتراضي والمترابط، كلما أصبحنا أكثر عرضة لهذا النوع من الأنشطة الخبيثة.

وتعتقد مالطة أن للأمم المتحدة دور مركزي تؤديه في تنظيم سلوك الدول في الفضاء الإلكتروني، وتحديداً بسبب المجموعة الواسعة من نصوص القانون الدولي الموجودة بالفعل. ومما يشجعنا جداً أيضا النتائج التي حققها فريق الخبراء الحكوميين والفريق العامل المفتوح العضوية التابع للأمم المتحدة اللذان اعتمدا تقريرين بتوافق الآراء بشأن أمور منها الارتقاء بسلوك الدول في الفضاء الإلكتروني. ونحن بحاجة لأن تستمر هذه العمليات في إمداد منظومة الأمم المتحدة، والتوسع في تطبيق القانون الدولي في الفضاء الإلكتروني، وأهمية تدابير بناء الثقة وتقديم المزيد من الإرشادات والقواعد. ونحن نقدر مشاركة الدول الأعضاء ومساهمتها في هذه العمليات، ونحث على المضي قدما بهذه المناقشات ومواكبة التطورات السريعة في هذا المجال.

ولقد شهدنا التأثير المدمر الذي قد تتكبده البيانات والبنى التحتية الحساسة نتيجة للهجمات السيبرانية. ومن الأهمية بمكان أن يتم تحديد القواعد والأنظمة المتعلقة بسلوك الدول في المجال السيبراني بشكل مفصل. وسيؤدي ذلك إلى زيادة القدرة على التنبؤ وتفادي أي سوء تقدير عند تقييم التهديدات السيبرانية. وأثر الاستخدام الخبيث للفضاء الإلكتروني مستدام إلى حد يقتضي أيضاً تعاوناً دولياً لتجنب نشوء أي نزاعات محتملة.

وتدابير بناء الثقة بين الدول من خلال تطبيق الممارسات الجيدة والقواعد الراسخة عنصر حيوي من أجل المضي قدما. ومن شأن ذلك أن يقلل احتمال وقوع حالات سوء فهم، ويمكِّن من إجراء تقييمات للسلوك الخبيث على نحو أفضل.

ويجب على المجتمع الدولي أيضا أن يتواصل مع عدد وافر من الجهات الفاعلة الأخرى في هذا الملف، بما في ذلك المجتمع المدني والقطاع الخاص، لضمان تكافؤ الفرص ووضع مجموعة عادلة من القواعد. ويجب أن يعترف جميع المستخدمين المحتملين للفضاء الإلكتروني بالدور الذي يقومون به في زيادة القدرة على الصمود في وجه التهديدات السيبرانية ومنع الاستخدام الخبيث للأدوات المتاحة لنا.

وتعتقد مالطة أن لمجلس الأمن دور هام يضـــطلع به عندما يتعلق الأمر بالتكنولوجيات الجديدة التي يمكن أن يكون لها تأثير على الســلام والأمن الدوليين. ويجب على مجلس الأمن أن يكفل احترام جميع الجهات الفاعلة المعنية في الفضــاء الإلكتروني للقانون الدولي والقواعد والمبادئ التوجيهية المعمول بها بغية تجنب احتمال نشــوء النزاعات نتيجة للهجمات الســيبرانية. ونحث المجلس على إبقاء هذه المســألة قيد نظره وكفالة أن نعزز معاً التفاهم والثقة المتبادلة.

المرفق الخامس والأربعون

بيان البعثة الدائمة للمغرب لدى الأمم المتحدة

[الأصل: بالفرنسية]

تتوجه المملكة المغربية بالشكر أولا لإستونيا، لقيامها بتنظيم هذه المناقشة المفتوحة الأولى لمجلس الأمن المكرسة لبحث المسألة الهامة والمناسبة التوقيت المتمثلة في صون السلام والأمن الدوليين في الفضاء الإلكتروني. ويرحب المغرب بالبيان الشامل الذي أدلت به السيدة كايا كالاس، رئيسة وزراء جمهورية إستونيا، فضلا عن القيادة الممتازة لإستونيا في القضايا السيبرانية وأمن الفضاء الإلكتروني.

ويتوجه المغرب بالشكر أيضاً إلى الممثلة السامية لشؤون نزع السلاح، السيدة إيزومي ناكاميتسو، على إحاطتها الإعلامية الزاخرة بالمعلومات بشأن التحديات الراهنة التي تواجه صون السلام والأمن الدوليين في الفضاء الإلكتروني.

والمملكة المغربية، بوصفها من البلدان النامية التي تتمتع بمستوى عال من إمكانية الاتصال الإلكتروني، أولت اهتماما خاصا في وقت مبكر جدا لتطوير تكنولوجيا المعلومات والاتصالات وأصولها بوصفها محركات للتنمية المستدامة. ومع ذلك، وعلى الرغم من وجود إجماع على المنافع والفوائد التي يجلبها تقدم تكنولوجيا المعلومات والاتصالات لرفاه البشرية في الحياة اليومية، فقد بدأ الوعي العالمي يتطور بشأن التهديدات التي يمكن أن تنبثق عنه، بدءا من مجرد تداول الأخبار الزائفة، إلى التهديدات الحقيقية للسلام والأمن، على الصعيدين الوطني والدولي على السواء.

وفي الوقت الذي نتحدث فيه عن الشروط المفترضة لإنترنت الأشياء أو الثورة الرقمية أو الحرب السيبرانية، ظلت قدرتنا على مكافحة التهديدات السيبرانية، مع ذلك، أقل من المستوى المرتفع لاعتمادنا على هذه الأدوات التي لا غنى عنها. وعلاوة على ذلك، من المهم ملاحظة أن السياق الحالي الذي يتميز بجائحة مرض فيروس كورونا (كوفيد-19)، لم يدفعنا فقط باتجاه عصر علم التحكم الآلي، بل عرَّضنا في الوقت نفسه لمستوى هائل لا رجعة فيه من الهشاشة تجاه الهجمات والتهديدات السيبرانية، بما فيها تلك التي تستهدف البنى التحتية الحيوية.

وهذه العمليات الخبيثة، التي تتجاوز تهديد سيادة الدول، تنطوي على إمكانية مؤسفة لزيادة خطر نشوب نزاعات في الفضاء الإلكتروني، والتسبب أيضا في أضرار بشرية ومادية كبيرة. ومن المرجح أن يؤدي ذلك إلى تقويض صرح السلام والأمن الدوليين وأن تمثل الهجمات السيبرانية في هذا السياق تهديداً ناشئاً رئيسياً.

وكما أكد الأمين العام، عند إطلاق برنامجه لنزع السلاح في عام 2018، "نحن نعيش في فترة خطرة".

والواقع أن المخاطر المحتملة والحقيقية المرتبطة بالتهديدات في الفضاء الإلكتروني تشكل تحديا للمجتمع الدولي والدول الأعضاء في الأمم المتحدة اليوم أكثر من أي وقت مضى. ولا يمكننا ضمان استمرار الفضاء الإلكتروني كمحرك للسلام والأمن والاستقرار والتنمية إلا إذا عملنا جماعات وفرادى لمنع الاستخدام الخبيث لتكنولوجيا المعلومات والاتصالات.

وفي هذا الصدد، يعتقد المغرب أن الحاجة إلى تأمين الفضاء الإلكتروني وحمايته تظل مسؤولية مشتركة بين الدول، القادة الأوائل. ولهذا السبب، قام المغرب منذ البداية، وفقا للتوجيهات الملكية السامية، باتخاذ إجراءات هامة على المستويات التشريعية والتنظيمية والوقائية، بما في ذلك:

- تحديد استراتيجية للأمن السيبراني، تدور حول أربعة محاور استراتيجية: تقييم المخاطر التي تؤثر على نظم المعلومات داخل الإدارات والهيئات العامة والبنى التحتية ذات الأهمية الحيوية؛ وحماية هذه النظم الإعلامية والدفاع عنها؛ وتعزيز أسس الأمن (الإطار القانوني، والتوعية، والتدريب والبحث والتطوير)؛ وتعزيز وتنمية التعاون الوطني والإقليمي والدولي؛

- إصدار القانون رقم 05-20 المتعلق بالأمن السيبراني في 25 تموز/يوليه 2020، الذي يهدف إلى وضع إطار قانوني يوصي الكيانات بمجموعة دنيا من القواعد والتدابير الأمنية، من أجل ضمان موثوقية ومرونة نظم المعلومات الخاصة بها. كما يهدف إلى تطوير الثقة الرقمية، ورقمنة الاقتصاد، وبشكل أعم، ضمان استمرارية الأنشطة الاقتصادية والمجتمعية في المغرب من أجل تعزيز تطوير نظام إيكولوجي وطني للأمن السيبراني؛

- إنشاء عدة منظمات خلال هذا العقد تهدف إلى ضمان إدارة الدولة للأمن السيبراني، مثل اللجنة الاستراتيجية لأمن نظم المعلومات في عام 2011، والمديرية العامة لأمن نظم المعلومات، والوكالة الوطنية لتنظيم الاتصالات السلكية واللاسلكية، واللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي، والمركز المغربي للأبحاث المتعددة التقنيات والابتكار الذي يضطلع بالحملة الوطنية لمكافحة الجريمة الإلكترونية.

وعشية هذه المناقشة العامة، وافق المغرب أيضا، في 28 حزيران/يونيه 2021، على مشروع مرسوم يتعلق بالأمن السيبراني يحدد القواعد المنطبقة على أمن نظم المعلومات، وكذلك على اتفاقية الاتحاد الأفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات الشخصية.

ومع ذلك، ونظرا للطابع العالمي للتهديدات السيبرانية، يجب أن تكون التدابير الهامة المتفق عليها دوليا قادرة على استكمال اللوائح المعمول بها على الصعيد الوطني. ولهذا السبب صادق المغرب على اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية، المعروفة أيضا باتفاقية بودابست، وانضم في عام 2018 إلى نداء باريس من أجل الثقة والأمن في الفضاء الإلكتروني. وفي إطار الأمم المتحدة، يشارك المغرب في الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وفريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي، والفريق العامل الجديد المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025، وفي وضع برنامج العمل في المستقبل للارتقاء بالسلوك المسؤول للدول في الفضاء الإلكتروني. والمغرب أيضا عضو في مجموعة أصدقاء الحوكمة الإلكترونية والأمن السيبراني، التي تشارك إستونيا في رئاستها، بشكل ممتاز، جنباً إلى جنب مع سنغافورة.

وفي الختام، تؤكد المملكة المغربية أن للدول مسؤولية مشتركة في إثبات إرادة مشتركة وحازمة لحماية الفضاء الإلكتروني، ويرجع ذلك أساسا إلى أن الجوانب الوقائية والأمنية للفضاء الإلكتروني هي نتيجة طبيعية لاستخدام تكنولوجيا المعلومات والاتصالات.

وعلى وجه الخصوص، فإن مجلس الأمن مدعو إلى الاضطلاع بدور رئيسي، لا سيما عندما يشكل وقوع الهجمات السيبرانية تهديدا مباشرا للسلام والأمن الدوليين، وللاضطلاع بدور ريادي في مجال الوقاية.

ويكرر المغرب شكره العميق لإستونيا على تنظيمها هذه المناقشة المفتوحة والضرورية والمناسبة من حيث التوقيت، لأننا بحاجة إلى مزيد من الوعي والمناقشات بشأن مسألة صون السلام والأمن الدوليين في الفضاء الإلكتروني، ولإدراج هذه المسألة في جدول أعمال مجلس الأمن.

المرفق السادس والأربعون

بيان الممثلة الدائمة لهولندا لدى الأمم المتحدة، يوكا براندت

تود مملكة هولندا أن تشكر إستونيا ورئيسة الوزراء كالاس على تنظيم هذه المناقشة المفتوحة بشأن صون السلام والأمن الدوليين في الفضاء الإلكتروني.

ولقد أتى الاجتماع في الوقت المناسب – حيث نشهد ارتفاعا حادا في الهجمات السيبرانية، من قبل الجهات الحكومية وغير الحكومية على السواء. ويمكن أن تؤدي هذه النشاطات السيبرانية الخبيثة إلى احتمال حدوث عرقلة واسعة النطاق في مجتمعاتنا، من خلال موارد محدودة نسبيا. وتنجم عنها زعزعة للعلاقات الدولية.

ولذلك، فقد حان الوقت للتعاون في تأمين فضاء إلكتروني مفتوح وحر وآمن من خلال الارتقاء بالسلوك المسؤول للدول، وإدانة السلوك غير المسؤول وتحميل مرتكبيه عواقبه.

ومع الاعتراف بوجود العديد من الجوانب الأخرى الهامة لهذه المسألة، فإن هولندا ستقتصر على تناول ثلاثة عناصر محددة تظل حتمية لزيادة الاستقرار في الفضاء الإلكتروني، وهي:

- الامتثال للتشريعات
- إسناد المسؤولية
- بناء القدرات

الامتثال للتشريعات

على مر السنين، أظهرت العمليات السيبرانية ضد البنى التحتية الحيوية والمدنية أنها تشكل تهديدا حقيقيا ومؤكداً. وقد تصاعد الأمر خلال العام الماضي حيث شهدنا تطور الهجمات السيبرانية من حيث النطاق والحجم والشدة والتعقيد. وقد ازداد تحويلنا كمجتمعات لجميع مناحي حياتنا تقريبا إلى عالم رقمي، ويجب أن ندرك أن شبكة الإنترنت هي التي تسهل هذه الروابط في جميع أنحاء العالم. ولذلك فلا غرابة في أن تظهر الآثار الضارة للعمليات السيبرانية الخبيثة ضد البنى التحتية الحيوية أو الحكومات أو المجتمعات على الفور وعلى نطاق واسع. وهي تشكل خطرا كبيرا على الأمن والاستقرار الدوليين، وعلى التنمية الاقتصادية والاجتماعية، وكذلك على سلامة الأفراد ورفاههم.

ومع توافق الآراء الذي تم التوصل إليه مؤخرا بشأن تقريري الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي، وفريق الخبراء الحكوميين التابع للأمم المتحدة المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني (فريق الخبراء الحكوميين)، أصبح لدى الدول الآن إطار للسلوك المسؤول للدول في الفضاء الإلكتروني. ويسمح ذلك للدول بفهم انطباق القانون الدولي والقواعد الطوعية غير الملزمة الـ 11 المتفق عليها على نحو أفضل. وتشير هولندا إلى أن القانون الدولي القائم، وبخاصة ميثاق الأمم المتحدة، ينطبق على الفضاء الإلكتروني وهو بالغ الأهمية فيما يتعلق بصون السلام والاستقرار، والارتقاء بفضاء إلكتروني حر ومفتوح وآمن، بما في ذلك احترام حقوق الإنسان والحريات الأساسية في الفضاء الإلكتروني.

وتتفق الدول على أن العمليات السيبرانية الخبيثة ضد البنى التحتية والهياكل الأساسية للمعلومات التي تدعم الخدمات الأساسية للبنى التحتية العمومية أمر محظور، حسب تأكيد فريق الخبراء الحكوميين في القاعدة 13 (و). ومن حق كل دولة أن تحدد البنى التحتية التي تعتبرها حيوية، وهي تشمل: المرافق الطبية، والخدمات المالية، والطاقة، والمياه، والنقل، والمرافق الصحية. وتركز هولندا باستمرار على ثلاث من البنى التحتية (غير الحصرية):

1 - البنية التحتية التقنية الضرورية للتوافر العام لشبكة الإنترنت أو سلامتها؛

والبنية التحتية التقنية الضرورية للانتخابات؛

وقطاع الرعاية الصحية.

وفي هذا السياق، نشجع الدول على أن تحدد وتشاطر علنا ما تعتبره بنية تحتية حيوية عن طريق إصدار بيانات إعلانية وطنية، تفصل فيها مواقف الدول الأعضاء بشأن التقيد بإطار السلوك المسؤول للدول. وهذه هي الطريقة الوحيدة التي يمكننا بها زيادة الشفافية، وتطوير التفاهم المشترك، وإيجاد القدرة على التنبؤ، وبناء الثقة. ويلزم مواصلة الجهود الرامية إلى تنفيذ الإطار المتفق عليه للحد من خطر التصعيد، فضلا عن تقيد جميع الدول بالتشريعات.

إسناد المسؤولية

يبدو أننا جميعا متفقون على القواعد والمعايير في الفضاء الإلكتروني. ومع ذلك، ما زلنا نشهد زيادة في التهديدات السيبرانية. وتشعر هولندا بالفزع إزاء استغلال جائحة مرض فيروس كورونا (كوفيد-19) للقيام بعمليات سيبرانية خبيثة ضد البنى التحتية الحيوية؛ والقطاع الصحي والبنى التحتية التقنية الضرورية للتوافر العام لشبكة الإنترنت أو سلامتها، وكذلك البنية التحتية التقنية للانتخابات.

ولنكن واضحين - سنعمل معا على أساس طوعي لمساءلة الدول عندما تتصرف على نحو مخالف لهذا الإطار، بما في ذلك باتخاذ تدابير تكون شفافة ومتسقة مع القانون الدولي. ويجب أن تكون هناك عواقب للسلوك السيئ في الفضاء الإلكتروني.

بناء القدرات

إن القدرة على الصمود ضد المخاطر الرقمية أساسية لإدارة المخاطر السيبرانية والتخفيف من تأثيرها. غير أن تباين مستويات القدرات في مجال الأمن السيبراني بين مختلف الدول يزيد من هشاشة عالمنا المترابط. ولذلك، تقضي مصلحتنا المشتركة بأن نبذل جهودا هادفة لبناء القدرات من أجل ضمان أن تتمكن جميع الدول المسؤولة من تنفيذ هذا الإطار وحماية شبكاتها بشكل أفضل من النشاط السيبراني المعطِّل أو المدمِّر أو المزعزِع للاستقرار. وعلاوة على ذلك، يتطلب بناء القدرات السيبرانية الفعال التعاون بين الجهات الفاعلة الحكومية وغير الحكومية على السواء. وفي ضوء ذلك، أنشأت هولندا المنتدى العالمي للخبرات السيبرانية، الذي نضج ليصبح منصة قوية مشتركة بين القطاعين العام والخاص لبناء القدرات، تعمل على تسخير وتجميع أكثر من 700 من جهود بناء القدرات السيبرانية القائمة التي تقدم المساعدة في بناء القدرة على الصمود تقنياً، وتساعد في صياغة التشريعات التي تضمن السلامة والأمن واحترام حقوق الإنسان.

ونحن نشيد بإستونيا لإرسائها الأساس للمناقشات المتعلقة بالمسائل السيبرانية في مجلس الأمن في المستقبل، ونرحب بالمناقشة الرسمية الأولى اليوم بشأن الأمن السيبراني.

المرفق السابع والأربعون

بيان البعثة الدائمة لنيوزيلندا لدى الأمم المتحدة

تود نيوزيلندا أن تشير إلى تقديرها لإستونيا لطرحها المسألة الهامة المتمثلة في صون السلام والأمن الدوليين في الفضاء الإلكتروني على جدول أعمال مجلس الأمن.

وتمثل التهديدات السيبرانية قضية ملحة وواسعة الانتشار بالنسبة لجميع الدول الأعضاء. وهي تشكل مخاطر كبيرة على ازدهار نيوزيلندا وأمنها، وكذلك على السلام والأمن الدوليين.

ويجب أن نعمل معا لبناء بيئة مستقرة وآمنة على الإنترنت لكي نتمتع جميعا بفوائد الاتصال الرقمي، الذي يعد أحد العوامل التمكينية الهامة للتنمية الاقتصادية والاجتماعية والثقافية.

ونحن نقدر هذه الفرصة لعرض وجهات نظر نيوزيلندا بشأن الجهود الدولية الرامية إلى صون السلام والأمن في الفضاء الإلكتروني. وتحقيقا لهذا الغرض، نؤكد من جديد الأهمية الحاسمة للإطار المتفق عليه للسلوك المسؤول للدول على الإنترنت:

- يجب أن نتقيد بالتزاماتنا بموجب القانون الدولي القائم، الذي اتفقنا جميعا على أنه ينطبق على شبكة الإنترنت كما ينطبق خارجها؛
- يجب أن ننفذ معايير السلوك المسؤول للدول على الإنترنت، الذي أيده كل منا من خلال قرار الجمعية العامة 237/70؛
- يجب أن نضمن اعتماد تدابير بناء الثقة واستخدامها على نطاق واسع؛
- يجب أن نضاعف جهودنا لبناء القدرات لضمان أن نكون جميعا قادرين على الصمود في وجه التهديدات السيبرانية.

ويوفر هذا الإطار ما نحتاج إليه لتشجيع السلوك المسؤول على الإنترنت، ولكن يجب تطبيقه لكي يكون فعالا. وعلينا أن نواصل تنفيذ هذا الإطار بطرق عملية ومجدية وملموسة. ونيوزيلندا ملتزمة بمواصلة العمل معكم جميعا لتحقيق هذه الغاية.

القانون الدولي

إن نيوزيلندا، بوصفها دولة صغيرة، داعم ثابت للنظام الدولي القائم على القواعد. ويصدق هذا بصفة خاصة فيما يتعلق بالتهديدات العابرة للحدود. وعزلتنا الجغرافية لا تحمينا من التهديدات السيبرانية.

وضمان أن يعزز هذا النظام بيئة مفتوحة وآمنة ومستقرة ومتاحة وسلمية على الإنترنت، وأن يشجع السلوك المسؤول للدول في الفضاء الإلكتروني، من الأولويات الرئيسية بالنسبة لنيوزيلندا.

والتوصل إلى توافق في الآراء بشأن كيفية تطبيق القانون الدولي على الإنترنت على وجه التحديد هو بمثابة إسهام حاسم باتجاه صون السلام والاستقرار. ونحن جميعا متفقون على أن القانون الدولي ينطبق على شبكة الإنترنت كما ينطبق خارجها. ويشمل القانون الدولي المنطبق ما يلي: ميثاق الأمم المتحدة؛ وقانون مسؤولية الدول؛ والقانون الدولي الإنساني؛ والقانون الدولي لحقوق الإنسان.

ولكننا نعترف بأنه لا تزال هناك بعض الاختلافات بشأن هذه المسائل. ولدعم فهم *كيفية* انطباق القانون الدولي على الإنترنت، أصدرت نيوزيلندا في كانون الأول/ديسمبر 2020 بيانا بموقفها الوطني. ونشجع الدول الأعضاء الأخرى على عرض وجهات نظرها الوطنية من أجل تطوير وتعزيز فهمنا المشترك لهذه المسائل.

معايير السلوك المسؤول للدول

إن نيوزيلندا ملتزمة بمنع الأنشطة السيبرانية الخبيثة وبالكشف عنها وردعها والتصدي لها، وبالتمسك بمعايير السلوك المسؤول للدول على النحو الذي أقره تقرير الفريق العامل المفتوح العضوية التابع للأمم المتحدة لعام 2021. وتمثل المعايير التي التزمنا بها جميعا عنصراً أساسياً للاستقرار والأمن في الفضاء الإلكتروني. ويتعين علينا أن نواصل تحمل المسؤولية – وأن نسائل الآخرين – عن الالتزامات التي قطعناها.

ويجب علينا، في جملة أمور، أن نعزز التعاون بين الدول، وأن نحمي البنى التحتية الحيوية، وأن نحافظ على سلاسل الإمداد العالمية، وأن نقدم المساعدة عند الاقتضاء، وأن نحترم حقوق الإنسان والخصوصية، وأن نمنع الاستخدام الخبيث للتكنولوجيات الرقمية في الأقاليم الوطنية للدول.

ولا نزال نواصل التأمل في الطريقة التي أكدت بها جائحة مرض فيروس كورونا (كوفيد-19) على أهمية سلامة وأمن الفضاء الإلكتروني. وقد رأينا تقارير على الصعيد الدولي عن مجموعة من مختلف الأنشطة الخبيثة على الإنترنت، من الجهات الحكومية وغير الحكومية على السواء. وقد استهدفت هذه الأنشطة، في جملة أمور، البنية التحتية الحيوية للرعاية الصحية؛ والعاملين في مجال الاستجابة؛ وعامة الناس. وهذا أمر غير مقبول ويبرز أن التهديدات في الفضاء الإلكتروني تعرض حياة الناس للخطر. ولقد أدانت نيوزيلندا علنا، إلى جانب عدد من الدول الأخرى، النشاط السيبراني الخبيث الذي يقوض جهود الاستجابة لهذه الجائحة.

تدابير بناء الثقة

إننا لا نزال ملتزمين بتحقيق نتائج بناءة وعملية وملموسة لتحسين الأمن السيبراني على الصعيدين الدولي والإقليمي. وتوفر تدابير بناء الثقة سبيلا هاما لتحقيق ذلك الهدف، ونحن نرحب بالمبادرات العملية التي تدعم التفاهم المتبادل والشفافية والقدرة على التنبؤ والاستقرار في الفضاء الإلكتروني.

وبالنسبة لنيوزيلندا، يشكل المنتدى الإقليمي لرابطة أمم جنوب شرق آسيا منتدى رئيسيا للمناقشات الإقليمية بشأن الأمن السيبراني. ونحن نقدر التعاون القائم مع الأعضاء في ذلك المنتدى ونتطلع إلى مواصلة العمل معكم جميعا في السنوات المقبلة. وترحب نيوزيلندا بفرصة تبادل الدروس المستفادة داخل المناطق وفيما بينها لتحسين الشفافية والتفاهم والثقة فيما بين الشركاء الإقليميين في الفضاء الإلكتروني.

بناء القدرات

تود نيوزيلندا تقديم المساعدة في ضمان أن تتمكن جميع الدول من الحد من المخاطر المرتبطة بزيادة الاتصال، مع الاستمرار في الاستفادة من هذه الزيادة في الوقت نفسه. ويشمل ذلك دعم أن يكون فهم إطار السلوك المسؤول للدول في الفضاء الإلكتروني والالتزام به أوسع وأعمق.

ولتحقيق ذلك، نحتاج إلى ضمان أن تتوفر لنا جميعا الأدوات والقدرات اللازمة للمشاركة بصورة مجدية في المناقشات الجارية ومجالات النقاش، وتنفيذ المبادرات المحلية والإقليمية التي تدعم الاستقرار على الصعيد الدولي.

ولا تزال نيوزيلندا ملتزمة ببناء القدرات الإقليمية في مجال الأمن السيبراني، مع التركيز بوجه خاص على العمل مع جيراننا في منطقة المحيط الهادئ وجنوب شرق آسيا. ولا نزال نقدم المبادرات في إطار برنامج نيوزيلندا لدعم الأمن السيبراني إلى منطقة المحيط الهادئ الذي تبلغ تكلفته 10 ملايين دولار نيوزيلندي، ولدعم مركز التميز في مجال الأمن السيبراني المشترك بين رابطة أمم جنوب شرق آسيا وسنغافورة.

خاتمة

أمامنا الكثير من العمل، ولكننا لن نبدأ من الصفر. ونحن نرحب مرة أخرى بنتائج عمليتي فريق الخبراء الحكوميين التابع للأمم المتحدة والفريق العامل المفتوح العضوية. وتشكل هاتان العمليتان، والتقريران الناتجان عنهما، إنجازين هامين متكاملين يعزز بعضهما بعضاً. ويجب أن نواصل البناء على هذا الأساس الذي أوجدته اتفاقات توافق الآراء هذه وغيرها من الاتفاقات التي أقرتها الجمعية العامة.

ومن المهم أن تشمل تلك المناقشات طائفة متنوعة من الآراء، بما في ذلك آراء الدول الصغيرة، وآراء أصحاب المصلحة غير الحكوميين. وقد أثلج صدرنا اتساع نطاق الاهتمام بالأمن السيبراني من جانب الدول الأعضاء – فالسلام والأمن في الفضاء الإلكتروني يؤثران علينا جميعا – ومن المشجع أن نرى هذه المجموعة الكبيرة من الدول تشارك بصدق في الجهود الرامية إلى التصدي لهذه التحديات. ونيوزيلندا على استعداد للمشاركة معكم جميعا في هذا التحدي.

المرفق الثامن والأربعون

بيان الممثل الدائم لباكستان لدى الأمم المتحدة

أود أن أعرب عن عميق تقديري وخالص شكري للبعثة الدائمة لجمهورية إستونيا لعقد هذه المناقشة المفتوحة الهامة والحسنة التوقيت لمجلس الأمن بشأن موضوع "صون السلام والأمن الدوليين في الفضاء الإلكتروني".

وتتيح تكنولوجيات المعلومات والاتصالات فرصا هائلة، وتتزايد أهميتها بالنسبة للمجتمع الدولي. وفي الوقت نفسه، فإن تعقد المسائل الملازمة لاستخدام تكنولوجيا المعلومات والاتصالات يشكل مخاطر جسيمة على السلام والأمن الدوليين.

والاستخدام العدائي للتكنولوجيات السيبرانية يقترب بسرعة من المرحلة التي يمكن أن يشكل فيها خرقا للسلام أو تهديدا للسلام والأمن الدوليين.

ويمكن أن يؤدي سوء استخدام تكنولوجيا المعلومات والاتصالات واستخدامها غير المنظم إلى آثار خطيرة على السلام والأمن الدوليين في حالة شن هجوم سيبراني على البنية التحتية الحيوية. والحوادث الأخيرة للهجمات السيبرانية المشتبه فيها تعطي مثالا على ذلك.

وثمة حاجة للتصدي لتنامي آفاق الأمن السيبراني بشكل عاجل كجزء من جهود الأمم المتحدة الأوسع نطاقا لمنع نشوب النزاعات.

وفي هذا الصدد، كان لاعتماد تقرير بتوافق الآراء للفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي في آذار/مارس من هذا العام أهمية تاريخية في دعم الجهود العالمية الرامية إلى تحقيق الهدف المشترك المتمثل في تهيئة بيئة آمنة ومأمونة ومستقرة وسلمية لتكنولوجيا المعلومات والاتصالات.

وهو يمثل أيضاً تأكيداً قوياً لقدرة المجتمع الدولي على التكاتف للتصدي للتحديات العالمية الرئيسية في أحلك الظروف، مثل الجائحة.

وفي حين أننا نتفهم أن التقرير لم يعالج شواغل جميع الدول الأعضاء، نرى أنه من المهم توطيد التقدم الذي أُحرز حتى الآن والحفاظ على الزخم لمواصلة هذه العملية الشاملة والشفافة.

وظلت باكستان تشارك بشكل إيجابي وبناء في عمل الفريق العامل المفتوح العضوية، وهي ترحب بإنشاء الفريق العامل الجديد المفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات وأمن استخدامها للفترة (2021-2025)، عملا بقرار الجمعية العامة 240/75.

وهو (أي الفريق العامل الجديد المفتوح العضوية) يوفر منتديات مفيدة للغاية لتحقيق تقدم مجدٍ، بالاستفادة من التوصيات السابقة من أجل تعزيز معايير السلوك المسؤول في الفضاء الإلكتروني وتحقيق تعاون دولي هادف للحد من التهديدات التي تشكلها الاستخدامات الخبيثة لتكنولوجيا المعلومات والاتصالات على الأمن الدولي.

ويتفق فريق الخبراء الحكوميين لعام 2015 والتقرير الأخير للفريق العامل المفتوح العضوية على مجموعة من النتائج الهامة التي ساهمت في التوصل إلى توافق واسع في الآراء بين الدول الأعضاء على

أن القانون الدولي، ولا سيما ميثاق الأمم المتحدة، قابل للتطبيق وضروري للحفاظ على السلام والاستقرار في بيئة تكنولوجيا المعلومات والاتصالات.

وميثاق الأمم المتحدة لا لبس فيه في تأييده القاطع لمبادئ السيادة والسلامة الإقليمية وعدم التدخل في الشؤون الداخلية للدول الأخرى. وينبغي الاسترشاد بهذه المبادئ في سياق استكشافنا لتعقيدات الحوكمة السيبرانية.

وفي الوقت نفسه، فإن مدى ونطاق وطبيعة انطباق القانون الدولي وتفسيره في سلوك الدول واستخدامها لتكنولوجيا المعلومات والاتصالات أمور تتطلب دراسة متأنية.

ومجرد التأكيد على انطباق القانون الدولي القائم على الفضاء الإلكتروني ليس كافيا للتصدي للتحديات القانونية المتعددة الأوجه الناشئة عن تكنولوجيا المعلومات والاتصالات. وينبغي تكييفه وفقا للسمة الفريدة للمجال السيبراني.

وتدرك باكستان أهمية وضع صك دولي ملزم قانونا، مصمم خصيصا للسمات الفريدة لتكنولوجيا المعلومات والاتصالات، من أجل توفير مسار تنظيمي يسعى إلى تحقيق الاستقرار والسلامة في الفضاء الإلكتروني. وينبغي أن يعالج هذا الإطار القانوني شواغل جميع الدول ومصالحها، وأن يستند إلى توافق الآراء، وأن يجري إعداده داخل الأمم المتحدة بمشاركة جميع الدول على قدم المساواة.

ويمكن للمعايير الطوعية غير الملزمة لاستخدام الدول المسؤول لتكنولوجيا المعلومات والاتصالات أن تسهم في الحد من المخاطر التي تهدد السلام والأمن الدوليين. ولكن نظرا للتهديدات غير المسبوقة في بيئة تكنولوجيا المعلومات والاتصالات والوتيرة السريعة للتطورات التكنولوجية، ثمة حاجة إلى تعزيز الجهود الدولية لوضع معايير ملزمة يمكن أن تساعد في صون السلام والاستقرار وتعزيز بيئة مفتوحة وآمنة ومستقرة ومتاحة وسلمية لتكنولوجيا المعلومات والاتصالات.

وينبغي أن نضمن عدم إساءة استخدام الفضاء الإلكتروني لإدامة حملات التضليل التي ترعاها الدول، والتحريض على العنف، وخطاب الكراهية، وغير ذلك من أشكال التعصب ذات الصلة، بما في ذلك كراهية الإسلام.

وللأمم المتحدة دور محوري في تعزيز الحوار والتعاون الدولي فيما بين الدول الأعضاء للتوصل إلى تفاهم مشترك بشأن الجوانب الرئيسية، بما في ذلك بشأن تطبيق القانون الدولي والقواعد والمعايير والمبادئ الدولية للسلوك المسؤول للدول، وتعزيز تدابير بناء الثقة والشفافية، ودعم بناء القدرات وتعميم أفضل الممارسات.

وبعدد سكان يتجاوز 200 مليون نسمة، ومشهد رقمي مزدهر يتسم بعدد متزايد من مستخدمي الإنترنت، تعلق باكستان أهمية كبيرة على الاستفادة من التكنولوجيات الرقمية لتمكين التنمية الاجتماعية والاقتصادية، وتيسير الحوكمة لتصبح أكثر فعالية وكفاءة، وتقديم الخدمات العامة.

وباكستان ملتزمة بتعزيز التعاون الدولي في مجال تكنولوجيا المعلومات والاتصالات والأمن السيبراني كوسيلة لسد الفجوة الرقمية. وتتساوى جميع البلدان في أنها من أصحاب المصلحة في وضع قواعد تحكم الاقتصاد الرقمي وأمن الفضاء الإلكتروني وتكنولوجيا المعلومات والاتصالات.

المرفق التاسع والأربعون

بيان البعثة الدائمة لبيرو لدى الأمم المتحدة

[الأصل: بالإسبانية]

إن بيرو تعرب عن ترحيبها بمبادرة الرئاسة الإستونية لعقد هذه المناقشة المفتوحة الرفيعة المستوى لمجلس الأمن بشأن مسألة ذات أهمية متزايدة وأساسية لصون السلام والأمن الدوليين. ونعرب أيضا عن ترحيبنا بالإحاطات التي قدمها المتكلمون الآخرون.

وإننا ندرك أهمية استخدام تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي، وتطورها السريع، وما يتولد عنها من فوائد. وقد أبرزت الأزمة الصحية الناجمة عن جائحة مرض فيروس كورونا (كوفيد-19) اعتمادنا عليها، والحاجة الملحة إلى الحد من الفجوة الرقمية، وأهمية حماية البنى التحتية الحيوية.

وعلى المنوال نفسه، ندرك أيضا المخاطر التي يمكن أن تنشأ عن استخدام تكنولوجيات المعلومات والاتصالات لأغراض خبيثة، مما يزيد من خطر نشوب نزاعات في الفضاء الإلكتروني. ويتسبب استخدامها لأغراض خبيثة من قِبل جماعات إرهابية ومنظمات إجرامية وجماعات مسلحة وغيرها من العناصر، في خطر جسيم ونظمي يهدد السلام والأمن الدوليين.

وبما أن التهديدات لا تنشأ عن التكنولوجيات في حد ذاتها، بل عن الطريقة التي تُستخدم بها، فيجب أن نعمق فهمنا لاستخدامها على النحو السليم، وكيفية تجنب الاستخدامات الخبيثة المتعمدة، من خلال تعزيز فضاء سيبراني مفتوح وحر ومستقر وآمن.

ولتلك الغاية، نقرّ بأولوية ميثاق الأمم المتحدة كأساس راسخ للأمن، ونؤيد تطبيق القانون الدولي والقانون الدولي الإنساني، في الفضاء الإلكتروني. وعلاوة على ذلك، نعتقد أن المسألة ذات الأهمية الأساسية هي وضع معايير دولية في هذا المجال من خلال إنشاء التزامات ملزمة قانونا.

ونقدر الجهود الملحوظة التي بذلتها الأمم المتحدة والتقدم الملحوظ المحرز في صياغة عناصر لتعزيز تطبيق القانون الدولي وتنفيذ معايير للسلوك المسؤول للدول في الفضاء الإلكتروني في سياق الأمن الدولي. ونشيد بالتقارير الموضوعية التي اعتمدها كل من الفريق العامل المفتوح العضوية وفريق الخبراء الحكوميين، ونأمل أن نتمكن، من خلال تنسيق سير العمليتين، من اعتماد بيان واحد متماسك ومسار عمل واحد بشأن الأمن السيبراني.

وإضافة إلى الجهود الدولية، نعتقد أن الإجراءات الإقليمية والوطنية ضرورية، ولا سيما في تعزيز تدابير بناء الثقة، وبناء القدرات، وتبادل المعلومات، وتقاسم الممارسات الفضلى لضمان الأمن السيبراني. وأما البلدان ذات التطور التكنولوجي المتدني، فيبدو لنا من الضروري أن تنشئ تفاهمات واتفاقات تتجنب تحويل الفضاء الإلكتروني إلى معترك للنزاعات بسبب الآثار المحتملة الناجمة عن عدم قدرتها على تجنب ذلك.

ومع مراعاة الطابع المترابط والمعقد للفضاء السيبراني، والابتكارات المستمرة في مجال تكنولوجيا المعلومات والاتصالات، وتزايد إدماج التكنولوجيات الناشئة، فإننا نؤيد مشاركة القطاع الخاص، ولا سيما صناعة المعلومات والمجتمع المدني والأوساط الأكاديمية، في مواجهة تلك التحديات. ونحن على اقتناع بأن مساهماتها ستستمر في إثراء المداولات المتعددة الأطراف بشأن هذه المسألة.

ونختتم بالتشـــديد على ضـــرورة قيام المجتمع الدولي ككل بتنســـيق العمل، واتخاذ إجراءات جديدة لدراسة التهديدات القائمة، وتدابير التعاون الممكنة للتصدي لها. وسيكون لدور مجلس الأمن في منع نشوب النزاعات وتعزيز السلام والأمن أهمية أساسية لضمان فضاء سيبراني مفتوح وسلمي وآمن وفيه منافع، ويعزز التنمية المستدامة ورفاه الشعوب.

المرفق الخمسون

بيان البعثة الدائمة لبولندا لدى الأمم المتحدة

إن أول مناقشـــة مفتوحة على الإطلاق في مجلس الأمن حول الأمن الســـيبراني هي معلم هام في تصورنا للتحديات المعاصرة التي تهدد السلام والأمن الدوليين.

ونعرب عن شكرنا للرئاسة الإستونية ونشيد بها لتمكيننا من معالجة مسائل الأمن السيبراني في هذا الوقت المناسب تماما.

وفي عام 2019، وخلال فترة عضـــويتنا، لفتت بولندا انتباه مجلس الأمن إلى مشـــاكل الحوادث السيبرانية في الشرق الأوسط.

وقد حان الوقت الآن لتوعية المجتمع الدولي ككل بالأنشـــطة الخبيثة المتزايدة باطّراد في الفضـــاء الإلكتروني. فعلى مدى عقدين من الزمن، وبالتوازي مع التطور غير المسبوق للتكنولوجيات الرقمية، ما فتئنا نشهد في جميع أنحاء العالم عددا متزايدا باستمرار من الهجمات والحوادث السيبرانية المتطورة. وتشهد بولندا حاليا هذه الزيادة يوميا.

وهي بالفعل ذات طابع متباين. فبعضـــها له خلفية إجرامية بحتة، والبعض الآخر مدفوع بأهداف اقتصادية، وفي الأعم الأغلب، لها أهداف سياسية. ومع ذلك، يوجد قاسم مشترك واحد لهذه الأنشطة، وهو أنها كلها غير قانونية. والأنشطة السيبرانية الخبيثة لا يمكن تبريرها ولا الدفاع عنها، بأي حال من الأحوال.

وكما أشرتم بحق، سيدتي الرئيسة، في مذكرتكم المفاهيمية: "يوفر القانون الدولي القائم، ولا سيما ميثاق الأمم المتحدة، إرشادات كافية للدول بشأن الاضطلاع بالأنشطة الإلكترونية". وإنها لمهمة عظيمة للمجتمع الدولي أن يعمل على إيجاد نموذج مقبول عموما للأنشطة في الفضاء الإلكتروني.

وتؤيد بولندا بقوة إنجازات فريق الخبراء الحكوميين، وقد شاركت بهمة في عمل الفريق العامل المفتوح العضوية، الذي أعاد التأكيد، في تقريره، على ضرورة تطبيق القانون الدولي في الفضاء الإلكتروني. ونأمل أن يسهم الفريق العامل المفتوح العضوية الثاني في تحسين الفهم المشترك لأهمية الاستخدام السلمي للفضاء الإلكتروني. ونحن نولي أهمية كبيرة أيضا لعمل اللجنة المخصصة في إطار اللجنة الثالثة للجمعية العامة.

وبصـــرف النظر عن التقييم المشـــترك للحالة، فما هو أكثر أهمية هو العمل المشـــترك والمنســـق بإحكام. ولذلك، فإن بولندا تؤيد المشاركة الواسعة النطاق للجهات المتعددة صاحبة المصلحة والمنظمات غير الحكومية والقطاعات الخاصة والأوساط الأكاديمية في المناقشة الدولية بشأن الأمن السيبراني.

ولدينا إيمان راسخ أيضا بضرورة الاضطلاع بالعمل الحاسم داخل المناطق. ومن خلال مشاركة المنظمات الإقليمية وفرادى الدول وممثلي المجتمع المدني، يمكننا تطوير أدوات مفيدة لبناء القدرات أو تدابير لبناء الثقة.

وابتغاء تحفيز الجهود الدولية، على الصـــعيدين العالمي والإقليمي، فإننا بحاجة إلى تجميع مواردنا وطاقاتنا الدبلوماسية. وهذا هو ما يجعلنا نؤيد ونعزز بقوة إنشاء برنامج العمل بوصفه شكلا نهائيا للتعاون الدولي بشأن أنشطة الفضاء الإلكتروني.

وبهذه المناقشـــة المفتوحة، نأمل أن يحتل الأمن الســـيبراني مكانه الدائم في جدول أعمال مجلس الأمن. فالتكاليف السياسية والاقتصادية للأنشطة الخبيثة في الفضاء الإلكتروني هي أبهظ من أن تتغاضى عنها هذه الهيئة الهامة التابعة للأمم المتحدة.

ونرجو أن تكونوا على ثقة من أن بولندا لن تدخر وســـعا للمســـاهمة في جميع العمليات العالمية والإقليمية، مما سـيؤدي إلى تعزيز النظام السـيبراني القائم على التقيد بالقانون الدولي والمعايير المتفق عليها بصورة مشتركة.

المرفق الحادي والخمسون

بيان البعثة الدائمة لدولة قطر لدى الأمم المتحدة

[الأصل: بالعربية]

أود أن أهنئ إستونيا على رئاستها الناجحة لمجلس الأمن هذا الشهر، وأشكركم على عقد هذه الجلسة لتسليط الضوء مرة أخرى على مسألة تهم جميع الدول الأعضاء. واسمحوا لي أيضًا أن أتقدم بالشكر للسيدة إيزومي ناكاميتسو، الممثلة السامية للأمم المتحدة لشؤون نزع السلاح، على إحاطتها والعمل الذي يقوم به مكتب شؤون نزع السلاح لمنح الأمن السيبراني المكانة التي تنبغي له في جدول أعمال الأمم المتحدة لنزع السلاح.

وفي كل يوم نشهد التأثير التحويلي لعالمٍ يعتمد بشكل كبير على الفضاء الإلكتروني، لكن التقنيات الرقمية والترابط العالمي يسهلان أيضا إساءة استخدام الفضاء السيبراني، وهو أمر مثير للقلق خاصةً بالنظر إلى اعتماد البنى التحتية والخدمات العامة الحيوية على المجال الرقمي. وتشكل إساءة استخدام الفضاء الإلكتروني وتكنولوجيا المعلومات والاتصالات من قبل الجهات الفاعلة الحكومية وغير الحكومية تهديدا للأمن القومي وتؤثر على السلم والأمن الإقليميين والدوليين والعلاقات الدولية. وعلاوة على ذلك، تستغل الجماعات الإرهابية التقنيات الرقمية الناشئة لزيادة قدرتها على ارتكاب جرائمها.

ومن الواضح أنه ما من بلد في منأى عن تهديد إساءة استخدام الفضاء الإلكتروني، وبالتالي فمن الضروري اتخاذ إجراءات جماعية لمواجهة هذا التحدي العالمي. ولحسن الحظ، فإن الفضاء الإلكتروني نفسه يمكن أن يوفر أداة ممتازة لتنسيق الجهود الدولية الرامية لمواجهة هذا التحدي. كما رأينا خلال العام الماضي، كانت المنصات الرقمية وسيلة لا غنى عنها لاستمرارية أعمال هيئات الأمم المتحدة وغيرها من منتديات التعاون الدولي.

وهناك حاجة لتقييم التهديدات المحتملة وتأثير القرصنة الإلكترونية وإساءة استخدام الفضاء الإلكتروني على السلم والأمن، ولبذل جهود جماعية لتعزيز البيئة الأمنية الإقليمية والدولية في مواجهة تلك التهديدات ولتعزيز الاستخدام السلمي للفضاء الإلكتروني والتقنيات الرقمية المتقدمة ذات الصلة.

وفي هذا الصدد، لا بد من إيلاء الاعتبار الواجب لانطباق القانون الدولي على استخدام الدول لتكنولوجيا المعلومات والاتصالات وتعزيز السلوك المسؤول المتعلق بالفضاء الإلكتروني للدول في سياق الأمن الدولي.

وفي الوقت نفسه، يجب الحفاظ على التدفق الحر للمعلومات واحترام حقوق الإنسان والحريات الأساسية في بيئة رقمية مفتوحة وآمنة ويمكن للجميع الوصول إليها.

وبالإضافة إلى الأُطر الدولية، تعتبر الاستراتيجيات الوطنية مهمة لتوجيه العمل والتنسيق بين أصحاب المصلحة المعنيين، بمن فيهم القطاع الخاص الذي يعتبر دوره محوريًا فيما يتعلق بالتكنولوجيا الرقمية.

وتولي دولة قطر أولوية لحماية أمن المعلومات والبنية التحتية للمعلومات، ولهذا الغرض تتخذ تدابير شاملة وطوّرت قدراتها في هذا الصدد، حيث تعمل على تعزيز التعاون الدولي وبناء القدرات.

إن مسألة أمن المعلومات والأمن السيبراني مطروحة على جدول أعمال الأمم المتحدة منذ سنوات عدة، لكن التطورات المتسارعة في هذا المجال تتطلب إجراءات تواكبها. ولذلك نرحب بالاهتمام الذي أولاه لهذه المسألة الأمينُ العام للأمم المتحدة الذي جعل تعزيز بيئة سلمية لتكنولوجيا المعلومات والاتصالات من أولوياته الرئيسية. كما يسعدنا أن نرى التوصل مجددا إلى توافق الآراء في فريق الخبراء الحكوميين. كما نتطلع إلى الدورة القادمة للفريق العامل المفتوح العضوية من أجل الإسهام في توسيع نطاق التوافق الدولي في هذا الصدد.

وأخيرًا، أود أن أؤكد مجددا أن دولة قطر ستواصل السعي الدؤوب على مختلف المستويات للمساهمة في الجهود العالمية لتعزيز السلام والأمن والاستقرار في الفضاء السيبراني.

المرفق الثاني والخمسون

بيان الممثل الدائم لجمهورية كوريا لدى الأمم المتحدة، تشو هيون

أود أولا أن أشكركم على عقد مناقشة اليوم المفتوحة التي جاءت في حينها حول "صون السلام والأمن الدوليين في الفضاء الإلكتروني". كما أعرب عن تقديري للممثلة السامية لشؤون نزع السلاح، السيدة ناكاميتسو، على الإحاطة المتعمقة التي قدمتها.

وعلى مدى العقدين الماضيين، شهد الجنس البشري تقدما تكنولوجيا في مجال التكنولوجيا الرقمية لم يسبق له مثيل. ومنذ ذلك الحين، فإن مفهوم الفضاء الإلكتروني، الذي لم يكن له من وجود في وقت ما سوى في الخيال العلمي، أصبح واقعا يوميا بالنسبة لنا جميعا؛ حيث يجري دمج الفضاء الافتراضي والمادي المحيطين بنا في نظام بيئي واحد. وبقدر ما حقق لنا هذا التقدم من فوائد اقتصادية واجتماعية غير مسبوقة، أصبحنا أيضا أكثر عرضة، من أي وقت مضى، للأنشطة السيبرانية الخبيثة. وعلى مدى العام الماضي، في خضم الجائحة العالمية، أصبحت حياتنا أكثر عرضة للتهديدات السيبرانية نظرا لتزايد عدد الأشخاص المتصلين بالإنترنت. وفي الوقت نفسه، يتزايد القلق إزاء تزايد عدد الهجمات السيبرانية على البنى التحتية الحيوية، بما في ذلك البنى التحتية والمرافق الطبية في جميع أنحاء العالم.

وعليه، فأود أن أبرز النقاط الأربع التالية ذات الأهمية البالغة لوفد بلدي.

أولا، إن جمهورية كوريا تؤيد الدور المحوري للأمم المتحدة في المناقشات الجارية بصدد كيفية التصدي للتحديات المطروحة وتشجيع السلوك المسؤول للدول في الفضاء الإلكتروني. وفي هذا الصدد، يرحّب وفد بلدي بقيام فريق الأمم المتحدة العامل المفتوح العضوية، في وقت سابق من هذا العام، باعتماد تقرير بتوافق الآراء عن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، فضلا عن التقرير الرابع لفريق الخبراء الحكوميين، الذي اعتُمد بتوافق الآراء في الشهر الماضي. وهذه الإنجازات تعكس التقدم المحرز في الإطار التراكمي والمتطور للسلوك المسؤول للدول في استخدامها لتكنولوجيا المعلومات والاتصالات، وقد تعزز، من خلال هذه العمليات، فهم المجتمع الدولي ككل في هذا المجال الحيوي.

وعلى نحو ما اتفقت جميع الدول الأعضاء بتوافق الآراء في التقرير السابق للفريق العامل المفتوح العضوية، فإن القانون الدولي ينطبق على استخدام الدول لتكنولوجيا المعلومات والاتصالات، وينبغي للدول أن تسترشد بإطار السلوك المسؤول للدول في استخدامها لتكنولوجيا المعلومات والاتصالات، على النحو المبين في تقارير فريق الخبراء الحكوميين. ويجب أن يُطبّق، على قدم المساواة، إيلاء الأولوية للقانون الدولي والنظام القائم على القواعد على الفضاء الإلكتروني، من أجل ضمان السلام والأمن.

ثانيا، إن وفد بلدي يقدر تقديرا عاليا التقرير الذي صدر مؤخرا بتوافق آراء فريق الخبراء الحكوميين، والذي يقدم مستوى إضافيا من الفهم بشأن قواعد السلوك المسؤول للدول، وتدابير بناء الثقة، وبناء القدرات، وكيفية انطباق القانون الدولي على استخدام الدول لتكنولوجيا المعلومات والاتصالات. وأعاد التقرير التأكيد على انطباق القانون الدولي، بما في ذلك ميثاق الأمم المتحدة، ولا سيما القانون الدولي الإنساني في حالات النزاع المسلح. كما نؤيد بقوة توصية فريق الخبراء الحكوميين بأن تسعى الدول الأطراف في أي نزاعات دولية، بما في ذلك النزاعات المتعلقة باستخدام تكنولوجيا المعلومات والاتصالات، أولا وقبل كل شيء إلى إيجاد حل بالوسائل السلمية، على النحو المبين في المادة 33 من ميثاق الأمم المتحدة.

وعلى وجه التحديد، يسرُّ وفد بلدي أن يرى التقرير يعرض مزيدا من التفاصيل عن القاعدة التي تدعو الدول إلى عدم السماح، عن علم، باستخدام أراضيها لارتكاب أفعال غير مشروعة دوليا باستخدام تكنولوجيا المعلومات والاتصالات. ويشير مبدأ "بذل العناية الواجبة" هذا، الذي اقترحته جمهورية كوريا والذي ورد لأول مرة في تقرير فريق الخبراء الحكوميين لعام 2015، إلى أنه ينبغي لكل دولة أن تتخذ خطوات مناسبة ومعقولة لمعالجة الوضع إذا كانت على علم بعمل غير مشروع دوليا أو إذا أخطرت به.

ثالثا، يجب علينا أن نرتقيَ بجهودنا نحو بناء الثقة وتعزيز التفاهم العام. وما برحت جمهورية كوريا، بوصفها دولة عضوا مسؤولة في الأمم المتحدة ودولة رائدة في القطاع الرقمي والتكنولوجي، تشارك وتساهم بنشاط في مختلف المحافل الإقليمية والمتعددة الأطراف. ففي الأسبوع الماضي وحدَه، وفي 22 حزيران/يونيه، استضافت جمهورية كوريا بنجاح، وبالتعاون الوثيق مع منظمة الأمن والتعاون في أوروبا، "المؤتمر الأقاليمي الثالث المعني بالأمن السيبراني/أمن تكنولوجيا المعلومات والاتصالات" لمناقشة الاتجاهات الراهنة في مجال الأمن السيبراني وتعزيز التعاون في مجال الأمن السيبراني بين المنظمات الإقليمية. واستضفنا أيضا الدورة التاسعة عشرة للمؤتمر المشترك بين جمهورية كوريا والأمم المتحدة بشأن قضايا نزع السلاح وعدم الانتشار، مع التركيز على تطوير التكنولوجيات الناشئة وتأثيرها، في عام 2020، وسنشترك في رئاسة اجتماع المنتدى الإقليمي لرابطة أمم جنوب شرق آسيا الذي يُعقد فيما بين الدورات بشأن أمن تكنولوجيا المعلومات والاتصالات للفترة 2021–2023. وعلاوة على ذلك، ستطلق جمهورية كوريا، في تشرين الثاني/نوفمبر المقبل، منتدى دوليا لزيادة تنشيط المناقشات من أجل التصدي للتهديدات الأمنية الناشئة، بما في ذلك الهجمات السيبرانية، واستخدام التكنولوجيات الناشئة لأغراض خبيثة في سياق السلام والأمن الدوليين. وبموجب مبادئ الشمولية للجميع والشفافية والانفتاح، سيوفر المنتدى منبرا دوليا مضيافا، متاحا لمختلف الجهات صاحبة المصلحة.

رابعا، إننا لا نبالغ مهما أكّدنا أن الأمن السيبراني يتطلب نهجا متعدد الجهات صاحبة المصلحة، حيث إن البعد الأمني الدولي للفضاء الإلكتروني يشمل مجالات وتخصصات متعددة. وبينما تبقى الحكومات هي المحور، فلا نتمكن من أن نكون فعالين حقا إلا عندما نشرك الجهات صاحبة المصلحة الرئيسية الأخرى مثل القطاع الخاص، والأوساط الأكاديمية، والمجتمع المدني، والأوساط التقنية، في هذه العملية. وينبغي أن نضع في اعتبارنا أيضا أن التعاون مع الجهات الأخرى صاحبة المصلحة يمكن أن يسهم إسهاما كبيرا في تعزيز التفاهمات المشتركة، وتنفيذ إطار السلوك المسؤول في الفضاء الإلكتروني.

وفي الختام، أود أن أغتنم هذه الفرصة لأؤكد من جديد التزام جمهورية كوريا بالعمل مع الأمم المتحدة ومع جميع الدول الأعضاء من أجل تعزيز وتشجيع فضاء إلكتروني مفتوح وآمن ومستقر وميسّر وسلمي.

المرفق الثالث والخمسون

بيان البعثة الدائمة لرومانيا لدى الأمم المتحدة

1 - إننا نشيد بإستونيا لمبادرتها بتنظيم أول مناقشة مفتوحة بشأن الأمن السيبراني كمسألة رسمية محددة مدرجة في جدول أعمال مجلس الأمن. وإن ذلك مبادرة جاءت في وقتها لزيادة تعزيز النظام الدولي القائم على القواعد، وكذلك تعزيز التعاون المتعدد الأطراف فيما بيننا بشأن موضوع في غاية الأهمية، وهو صون السلام والأمن الدوليين.

2 - وإن مناقشة اليوم تعزز التقدم الملحوظ الذي أحرزته الدول الأعضاء في آخر تقريرين اعتمدا بتوافق الآراء في إطار فريق الخبراء الحكوميين والفريق العامل المفتوح العضوية في توطيد الإطار المعياري للسلوك المسؤول للدول في الفضاء الإلكتروني - القائم على أساس القانون الدولي الحالي والمعايير والتدابير القائمة لبناء الثقة وبناء القدرات.

3 - وفي ظل بيئة أمنية دولية دائمة التغير، فإن تكنولوجيا المعلومات والاتصالات السلكية واللاسلكية تقدم مزايا بارزة، وتطرح، في الوقت نفسه أيضا، بعض أبرز التهديدات وأكثرها حدة في الوقت الحاضر. وهذه التهديدات تنشأ من جهات فاعلة من الدول ومن غير الدول، على حد سواء، وتستهدف مجموعة متنوعة من القطاعات الرئيسية، مثل قطاعات الطاقة والنقل والمالية والصحة، التي تعتمد على البنى التحتية الأساسية المادية والرقمية على السواء لتوفير الخدمات محليا أو إقليميا أو عالميا. ويمكن أيضا أن يساء استخدام التكنولوجيات الرقمية في محاولة لإضعاف مؤسساتنا الديمقراطية، وتقويض ثقة الجمهور في المبادئ الديمقراطية. وإضافة إلى ذلك، يمكن استخدامها لاستغلال مواطن ضعف بنيوية لأغراض جيوسياسية. وجائحة مرض فيروس كورونا (كوفيد-19) هي مثال صارخ حديث على التأثير المدمر للعمليات السيبرانية التي تهدف إلى الإضرار بالمعلومات الاستراتيجية حول أبحاث اللقاحات وتوزيعها، أو تغيير تلك المعلومات.

4 - وفي ظل هذه البيئة، فإننا لا نبالغ مهما قلنا في تقدير قيمة التعاون المتعدد الأطراف بين دول ذات حس بالمسؤولية، ولا نغالي في قيمة تعزيز الشراكات بين الإدارة العامة والقطاع الخاص والمجتمع المدني والأوساط الأكاديمية. وعلينا أن نعمل معا على تبادل معلومات موثوقة ودقيقة وحسنة التوقيت وجديرة بالثقة عن التهديدات وسبل التصدّي الموثوقة، وأن ننسق جهودنا ونعزز الآليات الوقائية ذات الصلة على الصعد العالمي والإقليمي والوطني. والأهم من ذلك هو أننا بحاجة إلى تركيز جهودنا من أجل تطوير قدرة مجتمعاتنا على الصمود في وجه تأثير التهديدات التي تتعرض لها بنيتنا التحتية الحيوية - سواء أكانت مادية أو رقمية أو مؤسسية.

5 - ومع مراعاة ذلك، فمن الجدير بالإشارة أن رومانيا، في إطار رئاستها الحالية لمجتمع الديمقراطيات، تعمل بهمة على تعزيز الصلة بين التكنولوجيا والعمليات الديمقراطية، معتبرة ذلك إحدى أولوياتها الرئيسية؛ وترحب رومانيا، بصفتها البلد المضيف للمركز الأوروبي للأمن المعلوماتي للكفاءة الصناعية والتكنولوجية والبحثية، المُنشأ حديثا في بوخارست، باستثمارات الشراكة المخطط لها ذات الإدارة المشتركة بين الدول الأعضاء في الاتحاد الأوروبي والقطاع الصناعي، وتشجعها بنشاط؛ وستعمل رومانيا، كونها الجهة البادئة والمستضيفة للمركز الأوروبي الأطلسي للقدرة على الصمود، المنشأ حديثا، على توليد الأفكار والاستراتيجيات الجديدة اللازمة لتكيف المجتمعات من أجل مواجهة التحديات الجديدة التي تواجه السلام والأمن والاستقرار الديمقراطي.

6 - وتعمل رومانيا، بوصفها دولة عضوا في الاتحاد الأوروبي، على تعزيز وتنفيذ الأبعاد الرئيسية لاستراتيجية الاتحاد الأوروبي الجديدة للأمن السيبراني للعقد الرقمي، ولا سيما مجموعة أدوات الدبلوماسية السيبرانية، بما في ذلك أدوات الردع السيبراني والاتصالات الاستراتيجية للاتحاد الأوروبي ضد الأنشطة السيبرانية الخبيثة. وتؤدي مجموعة أدوات الدبلوماسية السيبرانية للاتحاد الأوروبي دورا مهما في منع الحوادث السيبرانية التي تؤثر على أمن الاتحاد الأوروبي والدول الأعضاء، وردع تلك الحوادث والرد عليها.

7 - وتتعامل رومانيا مع الأمن السيبراني باعتباره بعدا رئيسيا من أبعاد الأمن الوطني، باذلة في ذلك جهودا لضمان وضع إطار قانوني وطني سليم وتكييفه من أجل تيسير التعاون وتبادل المعلومات بكفاءة فيما بين السلطات المختصة، والوفاء بالتزاماتها الدولية. وينطوي السلوك المسؤول للدول على التزامات إيجابية رئيسية، هي: وضع تشريعات واستراتيجيات ومؤسسات وطنية حديثة وفعالة فيما يتعلق بالفضاء الإلكتروني، وتعزيز تعاون دولي جوهري والمشاركة فيه، والأهم من ذلك هو الشفافية، والتمسك بالمعايير المتفق عليها، وتعزيز المبادئ الديمقراطية، والاحترام الكامل لكرامة الإنسان.

8 - وأمن الفضاء الإلكتروني بالنسبة لرومانيا هو في صدارة أولوياتها السياسية والدبلوماسية، التي تسعى إلى تحقيقها من خلال تعزيز السلوك المسؤول للدول وتوطيد الآليات الوقائية والمعيارية على المستوى العالمي والإقليمي والوطني. ونحن ملتزمون بدعم فضاء إلكتروني عالمي مفتوح وآمن ومأمون، تطبَّق فيه حقوق الإنسان والحريات الأساسية وسيادة القانون تطبيقا تاما. ونرى أيضا أنه لا يمكن تصور بيئة مفتوحة وآمنة ومستقرة وميسَّرة وسلمية على الإنترنت خارجَ نظام دولي قائم على القواعد، يقوم أساسا على القانون الدولي.

9 - وشاركت رومانيا بنشاط في عمليتي الأمم المتحدة الراميتين إلى توطيد إطار الأمن السيبراني (الفريق الحكومي الدولي والفريق العامل المفتوح العضوية)، اللتين اختتمتا بنجاح من خلال الاتفاق على توصيات هامة لمنع النزاعات في الفضاء الإلكتروني (من تعزيز التفاهم بشأن تطبيق القانون الدولي في الفضاء الإلكتروني، إلى المعايير الطوعية غير الملزمة للسلوك المسؤول للدول، وكذلك إلى مقترحات لإجراء حوار مؤسسي في المستقبل).

10 - وفي المستقبل، ترى رومانيا أن وضع برنامج عمل للأمم المتحدة للارتقاء بالسلوك المسؤول للدول في الفضاء الإلكتروني يعزز اعتماد تدابير عملية ملموسة لبناء القدرات وبناء الثقة، وكذلك تيسير الوصول إلى مصادر التمويل، بطريقة منفتحة وشاملة للجميع وشفافة ودائمة، مما يساعد جميع الدول الأعضاء في جهودها الرامية إلى منع نشوب النزاعات، وتطوير تصورات مشتركة للتهديدات، وزيادة قدرتها على الصمود في وجه التهديدات السيبرانية.

11 - وفي جميع عمليات الأمم المتحدة المقبلة، ستعمل رومانيا بنشاط على تعزيز موقفها بأن القانون الدولي ينطبق على الفضاء الإلكتروني. ونحن على اقتناع راسخ بأنه لا يوجد ما يدعو إلى اعتبار أن القانون الدولي القائم لا يمكن أن يحكم على النحو المناسب العلاقات فيما بين الدول التي تتم في الفضاء الإلكتروني أو من خلال الفضاء الإلكتروني. وذلك يشمل القانون الدولي الإنساني في سياق العمليات السيبرانية التي تنفذ في إطار نزاع مسلح (سواء أكان دوليا أو غير دولي). وفي مثل هذه الظروف، يجب أن يتم تخطيط العمليات السيبرانية وتنفيذها وفقا للمبادئ التي تحكم سير الأعمال العدائية، أي التمييز والتناسب والضرورة والحيطة.

12 - بيد أن زيادة الحوار وتبادل الآراء فيما بين الدول يمكن أن تساعد في توضيح بعض الظروف المعينة لانطباق القانون الدولي على الفضاء الإلكتروني. ومن هذا المنطلق، نشير إلى أن وجهة النظر الأولية لرومانيا بشأن هذا الموضوع قد صدرت لغرض المساهمة في عمل فريق الخبراء الحكوميين عملا بقرار الجمعية العامة 266/73.

المرفق الرابع والخمسون

بيان البعثة الدائمة للسنغال لدى الأمم المتحدة

[الأصل: بالفرنسية]

أولا، أود أن أشكر السيدة كايا كلاس، رئيسة وزراء جمهورية إستونيا، على ترؤسها هذه المناقشة العامة الافتراضية الرفيعة المستوى الهامة بشأن الأمن السيبراني، وهو موضوع ذو أهمية متزايدة داخل منظومة الأمم المتحدة، نظرا لتزايد التهديدات الأمنية المصادفة في الفضاء الإلكتروني. وأود أيضا أن أشكر الممثلة السامية لشؤون نزع السلاح، السيدة إيزومي ناكاميتسو، التي تابع وفد بلدي إحاطتها باهتمام كبير.

إن الحقيقة واضحة، وهي أن انتشار الأعمال الخبيثة في الفضاء الإلكتروني هو تهديد حقيقي للسلام والأمن الدوليين، وهو ما يستدعي تصرفا من جانب مجلس الأمن. وإن المناقشة التي تجمعنا اليوم تدل على أن المجلس يدرك هذا التهديد، وأنه يضطلع بقسطه من الجهود المستمرة والدؤوبة التي تبذلها الجمعية العامة بشأن الأمن السيبراني منذ أكثر من عقد من الزمن.

ومن هذا المنطلق، فإن المداولات المختلفة التي أجرتها الأفرقة الأربعة للخبراء الحكوميين والفريق العامل المفتوح العضوية، على التوالي، بشأن السلوك المسؤول للدول في الفضاء الإلكتروني، وأوجه التقدم في مجال المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، هي مداولات إيجابية، وهي إشارة لا لبس فيها إلى إرادة الدول في التوصل إلى توافق في الآراء بشأن طرائق تنظيم الفضاء الإلكتروني.

واعترافا بانطباق عدة مبادئ وقواعد للقانون الدولي القائم، وإعلان مسؤولية الدول عن أعمال غير مشروعة دوليا قد ترتكبها في الفضاء الإلكتروني، فإن الاستنتاجات التي خلص إليها تقريرا الفريق العامل المفتوح العضوية، وآخر فريق من الخبراء الحكوميين في آذار/مارس وأيار/مايو 2021، هي إسهام إضافي في فهم ممارسة القانون الدولي في الفضاء الإلكتروني.

وعلاوة على ذلك، فإن السنغال، شأنها شأن عدة بلدان، تعتقد أن تدابير بناء الثقة والشفافية ضرورية لتعزيز السلوك المسؤول للدول في الفضاء الإلكتروني، وبالتالي ينبغي تعزيزها.

وفي الواقع، يمكن للدول، من خلال تبادل المعلومات بانتظام عن أنشطتها السيبرانية، أن تساعد على تلافي الأخطاء في الإدراك وسوء الفهم، وعلى منع وإدارة الأزمات الناشئة عن استخدام الفضاء الإلكتروني، وعند الاقتضاء، إرساء أساس لتعاون مثمر في المسائل الرقمية.

ومع ذلك، وبسبب التغيرات الهائلة في هذا القطاع ونشوء تهديدات سيبرانية جديدة، فإن السنغال تعتقد أن قواعد القانون الدولي الوضعي وتدابير بناء الثقة والشفافية لن تكون كافية في حد ذاتها لتنظيم الفضاء الإلكتروني على النحو المناسب. وينبغي أن تُستكمل بصك قانوني دولي ملزم.

ومن ثم، يصبح من الضروري اتباع نهج عام يجمع بين تدابير طوعية لبناء الثقة والشفافية وبين اتفاقية دولية ملزمة، لا من أجل وضع قواعد الفضاء الإلكتروني فحسب، ولكن أيضا لمراعاة مواقف جميع الدول الأعضاء ومصالحها. ومن أجل هذا النهج، ينبغي أن تتجه مداولات الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025.

وحكومة السنغال، من جانبها، ملتزمة التزاما راسخا بتقديم مساهمة إيجابية في العمل في هذا المشروع، الذي لا يزال إحدى أولوياتها منذ اعتماد الاستراتيجية الوطنية للأمن السيبراني في تشرين الثاني/نوفمبر 2017. وهذه الوثيقة، المشتملة على رؤية إنشاء فضاء إلكتروني في السنغال في عام 2022 جدير بالثقة وآمن ومرن للجميع، تتضمن تقييما للسياق الاستراتيجي للأمن السيبراني في السنغال، مع أخذ التهديدات الحالية والمستقبلية في الاعتبار. وهي تحدد خمسة أهداف استراتيجية، هي: تعزيز الإطار القانوني والمؤسسي للأمن السيبراني؛ وحماية البنية التحتية الحيوية للمعلومات ونظم المعلومات الخاصة بالدولة؛ وتعزيز ثقافة الأمن السيبراني؛ وبناء القدرات والمعرفة التقنية في مجال الأمن السيبراني في جميع القطاعات؛ والمشاركة في الجهود المبذولة في مجال الأمن السيبراني على الصعيدين الإقليمي والدولي.

ووفقا للهدف الأخير، كانت السنغال أول بلد يصبح طرفا في اتفاقية الاتحاد الأفريقي المتعلقة بأمن الفضاء الإلكتروني وحماية البيانات الشخصية (اتفاقية مالابو). وانضمت أيضا إلى اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية (اتفاقية بودابست)، واتفاقية مجلس أوروبا رقم 108 لحماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية (STE n°108)، فضلا عن البروتوكول الإضافي للاتفاقية المتعلق بسلطات الرقابة وتدفق البيانات عبر الحدود (STE n°181). وإضافة إلى ذلك، اعتمدت توجيه المجموعة الاقتصادية لدول غرب أفريقيا الصادر في 19 آب/أغسطس 2011 بشأن مكافحة الجريمة السيبرانية، وأيدت نداء باريس من أجل الثقة والأمن في الفضاء الإلكتروني الصادر في 12 تشرين الثاني/نوفمبر 2018، ونداء كرايستشيرش في 15 أيار/مايو 2019 للقضاء على الإرهاب والمحتوى الذي يتضمن تطرفا عنيفا على الإنترنت.

وعلى الصعيد المحلي، وضع البلد إطارا قانونيا لتنظيم القطاع الرقمي واستخدام التكنولوجيا الرقمية. وإضافة إلى القانون رقم 2008-08 المؤرخ 25 كانون الثاني/يناير 2008 بشأن المعاملات الإلكترونية، بإمكاننا أن نذكر القانون التوجيهي رقم 2008-10 المؤرخ 25 كانون الثاني/يناير 2008 بشأن مجتمع المعلومات، والقانونين رقم 2008-11 و 2008-12 المؤرخين 25 كانون الثاني/يناير 2008 بشأن الجرائم السيبرانية وحماية البيانات الشخصية، والقانون رقم 2018-28 المؤرخ 28 تشرين الثاني/نوفمبر 2018 بشأن مدونة للاتصالات الإلكترونية. وعلى نفس المنوال، نُقح قانون الإجراءات الجنائية من أجل مراعاة الإجراءات في مجال الجرائم المرتكبة باستخدام تكنولوجيات المعلومات والاتصالات.

وفي الوقت نفسه، تعزز الهيكل المؤسسي بإنشاء دائرة تقنية مركزية لأمن نظم المعلومات، والشعبة الخاصة لمكافحة الجرائم السيبرانية، ولجنة حماية البيانات. وقريبا سيزداد إثراء هذا الهيكل من خلال إنشاء لجنة استشارية وطنية للأمن السيبراني ووكالة وطنية للأمن السيبراني، من أجل تنفيذ الاستراتيجية الوطنية للأمن السيبراني لعام 2022.

ويطرح بناء القدرات المتعلقة بالفضاء الإلكتروني تحديا آخر، ولا سيما بالنسبة للبلدان النامية. وهكذا فقد بذلت السنغال جهودا متعددة لتوفير التدريب في مجال أمن المعلومات. ولدى البلد حاليا العديد من المؤسسات التدريبية في هذا المجال، أبرزها المدرسة الوطنية للأمن السيبراني الإقليمي، في داكار، التي افتتحت في تشرين الثاني/نوفمبر 2018، والمعهد المهني لأمن المعلومات، الذي أنشئ في تشرين الأول/أكتوبر 2015.

وينبغي ألا يعوق الأمن السـيبراني فرص الابتكار والتطوير التي تتيحها تكنولوجيات المعلومات والاتصالات الجديدة، وألاّ يستخدم لغرض الحد من تطوير تلك التكنولوجيات.

وكوسـيلة لمنع الاسـتخدام الخبيث للفضـاء الإلكتروني ومكافحته، ينبغي أن يكون لمبادرات الأمن السيبراني الهدف النهائي وهو تعزيز بيئة رقمية ميسّرة، وآمنة، وسلمية ومزدهرة، ولا تترك أحدا خلف الركب، وفقا للغاية 9-ج من الهدف 9 من خطة عام 2030.

ومع أخذ هذا الطموح في الاعتبار، وضـعت حكومة السـنغال اسـتراتيجية السـنغال الرقمية للفترة 2016-2025، وفقا لخطة السـنغال الناشـئة. وهذه الوثيقة، التي تجسـد طموح السـنغال في الحفاظ على مكانتها كبلد رائد في أفريقيا للابتكار الرقمي، تركز على شعار "الرقمية للجميع ولجميع الاستخدامات بحلول عام 2025 في السنغال، في ظل قطاع خاص دينامي ومبتكر في نظام بيئي فعال".

المرفق الخامس والخمسون

بيان الممثل الدائم لسنغافورة لدى الأمم المتحدة، برهان غفور

أشكركم على عقد هذه الجلسة الهامة، وهي المرة الأولى التي يتناول فيها مجلس الأمن مسألة الأمن السيبراني بصفة رسمية.

وهو موضوع يأتي في أوانه. فقد أفادت السرعة المتزايدة للرقمنة الناجمة عن جائحة مرض فيروس كورونا (كوفيد-19) حياتنا بطرق جديدة. وكشفت لنا أيضا نقاط ضعف جديدة. وقد أصبحت التهديدات السيبرانية والأنشطة السيبرانية الخبيثة أكثر تواترا وأشد تعقيدا منذرة بعواقب أشد. وفي عام 2020، قدرت تكاليف الأنشطة السيبرانية الخبيثة بنحو تريليون دولار. والموجة الأخيرة من هذه الأنشطة هي تذكير صارخ بأن على المجتمع الدولي أن يواصل الاحتراز من هذه التهديدات العالمية والعابرة للحدود وأن يكون مستعدا لمواجهتها. وأود أن أسلّط الضوء على خمس نقاط في هذا الصدد.

أولا، يجب أن ندرك أن الفضاء الإلكتروني هو في الأساس مسألة تتعلق بإدارة المشاعات العالمية. وسنغافورة، وهي الدولة الصغيرة، تؤيد دائما نظاما متعدد الأطراف قائما على القواعد مركوزا في احترام القانون الدولي. ونهجنا لا يختلف فيما يتعلق بالفضاء الإلكتروني. وللحفاظ على فضاء إلكتروني آمن وموثوق به ومفتوح وقابل للتشغيل البيني، يجب أن نعتمد نهجا عالميا يستند إلى قواعد ومعايير عالمية وإلى التزام بالقانون الدولي. وسيكون القيام بذلك محفوفا بصعوبات، في ظل مشهد عالمي متقلب ومنقسم ناجم عن توترات جيوسياسية متنامية. ومع ذلك، فليس لدينا خيار سوى الاستمرار في الدعوة إلى تطبيق القانون الدولي والمعايير الدولية ودعمها من أجل تشجيع السلوك المسؤول للدول في الفضاء الإلكتروني. ونحن بحاجة إلى مضاعفة التضافر الدولي من أجل المزيد من القدرة على الصمود في وجه التهديدات السيبرانية والاستقرار السيبراني.

إن سنغافورة ملتزمة بدور الأمم المتحدة، باعتبارها المنتدى العالمي الوحيد الشامل للجميع والمتعدد الأطراف، في وضع القواعد التي تحكم الفضاء الإلكتروني. ونشعر بالتفاؤل إزاء المناقشات الواعية بشأن الأمن السيبراني في الأمم المتحدة. فمنذ إدراج أمن تكنولوجيا المعلومات والاتصالات لأول مرة في جدول أعمال الأمم المتحدة في عام 1998، قامت ستة أفرقة من الخبراء الحكوميين بدراسة التهديدات التي تطرحها إساءة استخدام تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي، وكيفية التصدي لهذه التهديدات. وقد اتفقت أربعة من هذه الأفرقة على تقارير موضوعية، بما في ذلك آخر فريق انتهى لتوه من عمله.

وقد عرضت مناقشات الأمن السيبراني على عموم الأعضاء للمرة الأولى في دورة الجمعية العامة الثالثة والسبعين. وتم ذلك من خلال إنشاء الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي. ونشعر بالتفاؤل إزاء النجاح مؤخرا في اعتماد التقرير الصادر بتوافق الآراء لفريق الأمم المتحدة العامل المفتوح العضوية. والتقرير يسهم في فهمنا المشترك بشأن العديد من المسائل، ويحدد المجالات التي تحتاج إلى مزيد من المناقشات.

وشاركت سنغافورة بنشاط في كل من الفريق العامل المفتوح العضوية ومؤخرا في فريق الخبراء الحكوميين. كما تتشرف سنغافورة بأن تُنتخب رئيسة للفريق الجديد العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025. وسنغافورة، بصفتها رئيسة هذه الهيئة، ملتزمة التزاما قويا بمواصلة المناقشات المفتوحة والشاملة للجميع والشفافة بشأن الأمن السيبراني في

الأمم المتحدة. ويحدونا الأمل في أن يسهم عمل الفريق العامل المفتوح العضوية الجديد في إيجاد نظام متعدد الأطراف قائم على القواعد في الفضاء الإلكتروني، وأن يمنح جميع الدول، كبيرها وصغيرها، الثقة والقدرة على التنبؤ والاستقرار، وهي أمور ضرورية للتقدم الاقتصادي، وخلق فرص العمل، واعتماد التكنولوجيا. ونحن نتطلع إلى العمل عن كثب مع جميع الدول الأعضاء في هذا الصدد.

ثانيا، إن جميع الدول معرضة للنشاط السيبراني الخبيث الذي يتزايد من حيث النطاق والتعقيد. ولكن الدول الصغيرة معرضة للخطر بوجه خاص، ولا سيما البلدان النامية وأقل البلدان نموا. وإذا كنا جادين بشأن نهج عالمي إزاء الأمن السيبراني، فيجب أن نواصل التركيز بقوة على بناء قدرات البلدان التي تحتاج إلى المساعدة. وهذا مجال يمكن للأمم المتحدة أن تساعد فيه في تنسيق الجهود. واشتركت سنغافورة مع مكتب الأمم المتحدة لشؤون نزع السلاح في إعداد دورة تدريبية عبر الإنترنت مفتوحة لجميع الدول الأعضاء من أجل تشجيع فهم أكبر لاستخدام تكنولوجيا المعلومات والاتصالات والآثار المترتبة عليها بالنسبة للأمن الدولي. وما زلنا على التزامنا بالعمل مع الأمم المتحدة ودعمها لتقديم المزيد من برامج بناء القدرات.

ثالثا، تعتقد سنغافورة أنه لا يزال الكثير مما ينبغي عمله لتعزيز زيادة الوعي بالمعايير الطوعية وغير الملزمة للسلوك المسؤول للدول في استخدام تكنولوجيا المعلومات والاتصالات، البالغ عددها 11 معيارا، وتنفيذها. ونحن نؤيد تبادل أفضل الممارسات والخبرات بشأن تنفيذ هذه المعايير. وذلك سيساعد على تعيين التحديات التي ينبغي أن نعالجها والثغرات التي قد تستدعي وضع معايير إضافية. وتؤيد سنغافورة القيام بمزيد من العمل للتوسع في القواعد القائمة. فعلى سبيل المثال، يمكن أن يتسبب النشاط السيبراني الخبيث ضد أي بنية تحتية حيوية للمعلومات عبر الحدود، مثل النظم السحابية والمصرفية، في تعطيل واسع النطاق للخدمات الأساسية في دول متعددة، بما في ذلك الخدمات المتعلقة بالتجارة والنقل والاتصالات على الصعيد الدولي. فينبغي للدول أن تنظر في كيفية تحسين التعاون عبر الحدود مع الجهات المعنية المالكة والمشغلة للبنى التحتية من أجل تعزيز التدابير الأمنية لتكنولوجيا المعلومات والاتصالات المخصصة لهذه البنى التحتية.

وبهذا أنتقل إلى نقطتي الرابعة بشأن زيادة المشاركة مع الجهات الأخرى صاحبة المصلحة، ولا سيما القطاع الخاص. وبما أن القطاع الخاص يمتلك جزءا كبيرا من البنية التحتية الحيوية للمعلومات، فعلى المجتمع الدولي أن يجد سبلا للتعاون الوثيق مع القطاع الخاص بهدف منع تأثير هذه الاضطرابات وتخفيف حدتها. وتؤيد سنغافورة اتباع نهج تعاوني بين القطاعين العام والخاص لتبادل الممارسات الفضلى من أجل دعم إطار قوي للأمن السيبراني.

خامسا، إن سنغافورة تعتقد أن المنظمات الإقليمية تضطلع بقسط أساسي من دعم مناقشات الأمم المتحدة والمساعدة في تنفيذ القواعد والمعايير التي وضعت في الأمم المتحدة. وقد كان الأمن السيبراني من الأولويات في إطار رئاسة سنغافورة لرابطة أمم جنوب شرق آسيا، في عام 2018. ففي ذلك العام، أصبحت الرابطة أول منظمة إقليمية تنضم من حيث المبدأ إلى اعتماد المعايير الطوعية وغير الملزمة البالغ عددها 11 قاعدة للسلوك المسؤول للدول في استخدام تكنولوجيا المعلومات والاتصالات. وتقوم الرابطة الآن بوضع خطة عمل لتنفيذ هذه المعايير. وفي إطار الرابطة، دأبت سنغافورة أيضا على دعم برامج بناء القدرات. وقد تأسس مركز التميز المشترك بين الرابطة وسنغافورة المعني بالأمن السيبراني، في عام 2019، كمركز متعدد التخصصات لبناء القدرات في مجالات من قبيل تدابير بناء الثقة والسياسات والاستراتيجيات والتشريعات والعمليات. ونحن نتطلع إلى العمل مع الدول الأعضاء لتعزيز جهودنا الجماعية لبناء القدرات السيبرانية.

واســـمحوا لي أن أختتم بالقول إن البنية التحتية الرقمية الآمنة والمأمونة يجب أن تدعم طموحاتنا للاقتصـاد الرقمي. ومن المهم، أكثر من أي وقت مضـى، أن تتصـدى الدول الأعضـاء معا لتحدي الأمن السـيبراني، بطريقة مسـتدامة وشـاملة ومنسـقة. وسـنغافورة على اسـتعداد للعمل مع جميع البلدان على إقامة شراكات وتعاون من أجل إنشاء فضاء إلكتروني آمن وموثوق به ومفتوح وقابل للتشغيل البيني.

المرفق السادس والخمسون

بيان الممثل الدائم لسلوفاكيا لدى الأمم المتحدة، ميشال ملينار

إن سلوفاكيا تؤيد البيان الذي أدلى به الاتحاد الأوروبي. ونود تقديم بعض الملاحظات الإضافية بصفتنا الوطنية.

أود أن أشكر الرئيسة على تنظيم هذه المناقشة التي جاءت في حينها، والتي توفر فرصة للتداول في المخاطر المتزايدة الناجمة عن الأنشطة الخبيثة في الفضاء الإلكتروني وتأثيرها على السلام والأمن الدوليين، وكذلك تناول الجهود العالمية الرامية إلى تعزيز السلام والاستقرار في الفضاء الإلكتروني.

لقد جعلت أزمة مرض فيروس كورونا (كوفيد-19) الحاجة إلى تعزيز أمن واستقرار الفضاء الإلكتروني قضية من قضايا الساعة الأكثر إلحاحاً. فقد أظهرت الأزمة أن القدرات الرقمية أصبحت عاملا حاسما في توفير الخدمات الأساسية، وكذلك استمرار الحوكمة الفعالة. وقد يؤدي تعطيل عمل البنية التحتية الحيوية إلى عواقب وخيمة. والأنشطة السيبرانية الخبيثة التي تستهدف القطاعات والخدمات الحيوية لها آثار مزعزعة للاستقرار، ومن ثم قد تهدد السلام والأمن الدوليين.

وبما أن التهديدات السيبرانية هي، إلى حد بعيد، تهديدات عابرة للأوطان بطابعها، فمن المهم الحفاظ على التعاون الدولي والحوار بين الدول، وبين الدول وغيرها من الجهات المعنية المتعددة. فمن خلال مسؤوليتنا المشتركة والجهود المشتركة للحكومات والقطاع الخاص والمجتمع المدني، يمكننا أن ندعم بفعالية صون السلام والأمن الدوليين في الفضاء الإلكتروني وحماية حقوق الإنسان.

وتضطلع الأمم المتحدة بدور هام في قيادة المناقشات الدولية لزيادة الوعي بالتحديات السيبرانية الماثلة أمام السلام والأمن الدوليين، ولإحراز تقدم في الارتقاء بالسلوك المسؤول للدول في الفضاء الإلكتروني.

وتؤيد سلوفاكيا بقوة تعددية الأطراف التي تساعد على إدارة التحديات الحالية والمستقبلية في الفضاء الإلكتروني والتصدي لها. ونحن على اقتناع بأن الاستقرار في الفضاء الإلكتروني يجب أن يستند إلى القانون الدولي القائم، بما في ذلك ميثاق الأمم المتحدة برمته، وإلى القانون الدولي الإنساني، والقانون الدولي لحقوق الإنسان. وتؤيد سلوفاكيا تأييدا كاملا انطباق القانون الدولي القائم على سلوك الدول في الفضاء الإلكتروني، على النحو المعترف به في ثلاثة تقارير لأفرقة الخبراء الحكوميين أُعدت بتوافق الآراء، وأقرتها الجمعية العامة في أعوام 2010 و 2013 و 2015. وسنبذل قصارى جهدنا من أجل إجراء مناقشات شفافة وبناءة، حتى نتمكن من الاستفادة المتبادلة من خبرة كل منا وممارساته وخبراته الجيدة.

وسلوفاكيا أيضا من المشاركين في رعاية برنامج العمل للارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في إطار الفريق العامل المفتوح العضوية. ونحن نؤمن بحوار مؤسسي شامل وبنّاء يركز على النتائج والانتظام والنهج القائم على توافق الآراء. وفي رأينا أن اقتراح برنامج العمل يوفر منطلقات لهذا الحوار على نطاق جميع أعضاء الأمم المتحدة.

وعندما يتعلق الأمر بتدابير بناء الثقة وبناء القدرات في الفضاء الإلكتروني، فإن سلوفاكيا ترى أن هذين الإجراءين هما أهم تدبيرين من أجل الحفاظ على الاستقرار في الفضاء الإلكتروني. فالمنظمات الإقليمية، مثل منظمة الأمن والتعاون في أوروبا، على سبيل المثال، هي حاليا أدوات مفيدة جدا في منع نشوب النزاعات،

وتعزيز التعاون بين الدول. ويساعد التواصل والتفاعل المنتظمان بين الدول في الفضاء الإلكتروني على تجنب النزاع وإزالة التوترات المتزايدة المحتملة، وفي الوقت نفسه، فإنهما يخلقان منبرا للحوار.

والقانون الدولي هو أحد الأركان الأساسية للاستقرار وإمكانية التنبؤ في العلاقات بين الدول. وسلوفاكيا تقف بقوة إلى جانب أولئك الذين يؤكدون من جديد أن القانون الدولي القائم – ولا سيما ميثاق الأمم المتحدة برمته والقانون الدولي الإنساني والقانون الدولي لحقوق الإنسان – ينطبق بالفعل على أعمال الدول في الفضاء الإلكتروني. ويحدد ميثاق الأمم المتحدة قواعد ومبادئ القانون الدولي ذات الأهمية الخاصة لصون السلام والاستقرار. ولا شك في أن حقوق الإنسان تنطبق داخل شبكة الإنترنت مثلما تنطبق خارجها، ويجب على الدول احترام تلك الحقوق والدفاع عنها.

شكرا لكم، السيدة الرئيسة.

المرفق السابع والخمسون

بيان البعثة الدائمة لسلوفينيا لدى الأمم المتحدة

تعرب سلوفينيا عن ترحيبها بأول مناقشة مفتوحة لمجلس الأمن، مكرسة لمسألة مواضيعية محددة تتعلق بالأمن السيبراني. وتأتي معالجة الأمن السيبراني في حينها، وهي مفيدة لجميع الدول الأعضاء. وإن إجراء مناقشة مفتوحة في مجلس الأمن حول هذا الموضوع يسهم في جهود التوعية في إطار السلام والأمن الدوليين. وفي هذا الصدد، ترحب سلوفينيا بالتقارير الأخيرة التي اعتمدها بتوافق الآراء كل من الفريقُ العامل المفتوح العضوية المعني بالتطورات في ميدان تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي (الفريق العامل المفتوح العضوية) وفريق الخبراء الحكوميين للأمم المتحدة المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني.

وتؤيد سلوفينيا بيان الاتحاد الأوروبي، ونحن نود أن نقدم بعض الملاحظات الإضافية بصفتنا الوطنية.

إننا نعيش في عالم مترابط وسريع التغير. ويسهم الفضاء الإلكتروني العالمي المفتوح والحر والمستقر والآمن في تحقيق فوائد اقتصادية واجتماعية. بيد أنه توجد أيضا أنشطة سيبرانية خبيثة. ويمكن أن تؤثر إساءة استخدام الفضاء الإلكتروني على القطاعات الاقتصادية الحيوية، وتقديم الخدمات الأساسية للجمهور، مثل الرعاية الصحية والطاقة، وغيرها من البنى التحتية الأساسية. ويمكن أن تؤدي الأغراض الخبيثة في استخدام تكنولوجيا المعلومات والاتصالات من جانب جهات من الدول أو من غير الدول إلى تقويض الثقة بين الحكومات، مما يترتب عليه آثار سلبية تؤدي إلى زعزعة السلام والأمن الدوليين.

وللتخفيف من حدة التهديدات القائمة والناشئة، تؤمن سلوفينيا إيمانا راسخا بأن الفضاء الإلكتروني ينبغي أن يحكم في ظل احترام كامل للقانون الدولي القائم، ولا سيما ميثاق الأمم المتحدة برمته، والقانون الدولي الإنساني وحقوق الإنسان، فضلا عن تنفيذ المعايير والقواعد المتعلقة بالسلوك المسؤول للدول. ولهذه الغاية، ينبغي أن يكون هدفنا الأول هو تعزيز تطبيق القانون الدولي القائم، وتركيز جهودنا الجماعية على النهوض بتنفيذ القواعد القائمة للسلوك المسؤول للدول، بما في ذلك الملاحقة الجنائية للكيانات الخاصة العاملة من ولاية قضائية قُطرية.

وتواكب معايير السلوك المسؤول للدول سياسة بناء الثقة وتدابير بناء القدرات. وهذا هو المجال الذي يمكننا فيه إحداث تغيير حقيقي. وتؤيد سلوفينيا بقوة – من ضمن دول أعضاء يبلغ عددها 53 دولة عضوا – مقترح إنشاء برنامج عمل للارتقاء بالسلوك المسؤول للدول في الفضاء الإلكتروني. وسيعتمد برنامج العمل على النصوص التشريعية الحالية للجمعية العامة. وسيوفر برنامج العمل فرصة لتعزيز برامج بناء القدرات، كما سيوفر آلية مؤسسية داخل الأمم المتحدة للتعاون وتبادل أفضل الممارسات والتعاون مع الجهات الأخرى صاحبة المصلحة.

وعلاوة على ذلك، ستواصل سلوفينيا، في تنفيذها لمعايير السلوك المسؤول للدول، تعزيز ودعم صدارة المنظور الجنساني في الحد من "الفجوة الرقمية بين الجنسين" ومشاركة المرأة مشاركة كاملة وفعالة وذات مغزى في عمليات صنع القرار المتصلة باستخدام تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي.

وستعمل سلوفينيا، بصفتها شاغلة منصب الرئاسة المقبلة لمجلس الاتحاد الأوروبي ابتداء من 1 تموز/يوليه 2021، على تعزيز التعاون في مجال الأمن السيبراني، وتعميم المسائل السيبرانية بين الاتحاد الأوروبي ومنطقة غرب البلقان. وإن تقريب غرب البلقان من النظام البيئي السيبراني الأوروبي هو عنصر مهم في بناء بيئة موثوقة وآمنة من أجل التنمية الرقمية، وتحسين الاتصال، وتحسين فرص النفاذ إلى الاقتصاد والمجتمع الرقميين. كما أنه إسهام في الاستقرار العالمي في الفضاء الإلكتروني.

ولهذه الغاية، تعتزم سلوفينيا تنظيم مؤتمر القمة غير الرسمي للاتحاد الأوروبي وغرب البلقان في أوائل تشرين الأول/أكتوبر 2021. وستنظم سلوفينيا أيضا مؤتمرا للأمن السيبراني – وهو الحدث الذي سيقام بشأن غرب البلقان بالتعاون مع معهد الدراسات الأمنية بالاتحاد الأوروبي. وإضافة إلى ذلك، سنسهم في استعراض التعاون مع دول غرب البلقان، وفي إحراز تقدم في هذا الشأن، في مجال منع الاعتداء والاستغلال الجنسيين للأطفال، والتحقيق فيهما.

وستعمل سلوفينيا أيضا، حين ستشغل منصب الرئاسة القادمة لمجلس الاتحاد الأوروبي، على تعضيد الجهود التنظيمية الأوروبية الرامية إلى تعزيز القدرة على الصمود في وجه التهديدات السيبرانية، وإدارة الأزمات السيبرانية، مع استعراض التوجيه المتعلق بأمن الشبكات ونظم المعلومات، الذي يحدد التدابير الرامية إلى تحقيق مستوى مشترك عال من الأمن السيبراني في جميع أنحاء الاتحاد، وكذلك الجهود الرامية إلى تعزيز تنفيذ مجموعة أدوات الدبلوماسية السيبرانية للاتحاد الأوروبي كوسيلة للمساهمة في منع نشوب النزاعات، والتخفيف من تهديدات الأمن السيبراني، وزيادة الاستقرار في العلاقات الدولية. وسنسعى جاهدين إلى زيادة التعاون الدولي، والحد من خطر التصورات الخاطئة والتصعيد والنزاع.

وأود أن أختتم بياني بالتأكيد مجددا على أن مجلس الأمن يضطلع بدور محوري في دعم الجهود المبذولة في مجال الأمن السيبراني، وهي جهود ذات أهمية حاسمة في صون السلام والأمن الدوليين. وبتنظيمكم هذه المناقشة المفتوحة، فقد شجعتم بالفعل وبقوة على تهيئة بيئة تفضي إلى تعزيز التعاون وبناء الثقة فيما يتصل بتكنولوجيا المعلومات والاتصالات والترويج لفضاء إلكتروني مفتوح وحر ومستقر وآمن عالميا.

المرفق الثامن والخمسون

بيان البعثة الدائمة لجنوب أفريقيا لدى الأمم المتحدة

إن جنوب أفريقيا قد لاحظت باهتمام عقد هذه المناقشـــة المفتوحة لمجلس الأمن من أجل النظر، لأول مرة، في مسألة مواضيعية مخصصة، في صون السلام والأمن الدوليين في الفضاء الإلكتروني. كما نشكر الممثلة السامية لشؤون نزع السلاح، السيدة ناكاميتسو، على الإحاطة التي قدمتها.

ولاحظنا كذلك الأسئلة التوجيهية المقدمة للمناقشة اليوم، والتي سنسعى إلى الرد عليها في بياننا.

بادئ ذي بدء، تود جنوب أفريقيا أن تؤكد أن مسـألة السـلام والأمن في الفضـاء الإلكتروني هي مسألة واسعة الانتشار ومعقدة، وهي تتطلب المشاركة الكاملة من جميع الدول الأعضاء في الأمم المتحدة. ولهذا السبب، نعتقد أن المكان المناسب لمعالجة هذه المسألة هو في إطار مداولات اللجنة الأولى للجمعية العامة، التي ما فتئت تشارك بالفعل في هذه المسألة.

وفي هذا الصدد، شاركت الدول الأعضاء من خلال عمل عدد من أفرقة الخبراء الحكوميين، ركز آخرها على الارتقاء بالسلوك المسؤول للدول في الفضاء الإلكتروني، وأصدر تقريره بتوافق الآراء في نهاية أيار/مايو 2021 تحت القيادة المقتدرة للسفير غيليرمي دي أغيار باتريوتا من البرازيل.

وعلاوة على ذلك، شـاركت جميع الدول الأعضـاء مشـاركة واسـعة في الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، اعتبارا من عام 2019، والذي اعتمد تقريره بتوافق الآراء في نهاية آذار/مارس 2021؛ والفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021–2025، الذي سيوجه أعماله السفير برهان غفور، الممثل الدائم لجمهورية سنغافورة، بصفته رئيسا له.

وبذلك، يكون أعضاء الأمم المتحدة قد قطعوا شوطا طويلا في مناقشة التهديدات الناشئة للسلام والأمن الدوليين في الفضـاء الإلكتروني؛ وأطر القانون الدولي التي تحكم هذا الجانب من السـلام والأمن الدوليين؛ والمعايير والقواعد والمبادئ التي توجه الدول الأعضـاء؛ والتدابير اللازمة لبناء الثقة؛ ومتطلبات بناء القدرات؛ وكذلك سبل مواصلة الحوار في هذا الصدد.

واسمحوا لي أن أطرح النقاط الموجزة التالية في هذا السياق.

إن جنوب أفريقيا تعتقد أن تعدد التهديدات الناشـئة يسـتلزم مشـاركة جميع الجهات الفاعلة ذات الصـلة، بما في ذلك المجتمع المدني والقطاع الخاص. وذلك سـيكون ضـروريا لفهم طبيعة هذه التهديدات وللتعاون عبر المجتمع بأسـره لمواجهة التهديدات التي تطرحها الجهات الفاعلة من الدول وغير الدول في الفضاء الإلكتروني، والتصدي لها على نحو كاف.

وتود جنوب أفريقيا أن تؤكد على ضـرورة سـد الفجوات الرقمية والجنسـانية، وكذلك تحويل الفجوة الرقمية إلى فرص رقمية، وهو ما سـيكون عاملا أسـاسـيا في بناء القدرة على الصـمود، وفي الوقت نفسـه، تعزيز التنمية. بيد أن التعقيد المتنامي للحوادث الضـارة في مجال تكنولوجيا المعلومات والاتصـالات هو مصدر قلق للبلدان النامية مثل جنوب أفريقيا.

ولا تزال جنوب أفريقيا تشـــعر بالقلق إزاء التهديد المتزايد للهجمات الســـيبرانية على البنية التحتية الحيوية والبنية التحتية الحيوية للمعلومات. وبينما نعتقد أنه ينبغي لنا مواجهة هذه التهديدات من خلال زيادة التعاون ووضع آليات لأفضل الممارسات، فإن هذه الجهود ينبغي أن تدعم الأولويات والجهود الوطنية لتحديد هذه البنية التحتية وتعيينها. ونحن ندرك أيضـــا أنه، على الرغم من التعرض للتهديدات، فإن الفرص الاقتصـــادية والاجتماعية الإيجابية التي يمكن أن تســـتمد من تكنولوجيا المعلومات والاتصـــالات ينبغي ألا تطغى عليها الاستخدامات الخبيثة لهذه التكنولوجيات. ولذلك، فإن التكنولوجيات نفسها ليست هي ما تثير القلق، بل إساءة استخدام هذه التكنولوجيات.

وبغية تنظيم استخدام الفضاء الإلكتروني، وخاصة الأخطار التي تهدد السلام والأمن الدوليين، فإن جنوب أفريقيا تؤيد انطباق القانون الدولي عليه، وتحديدا ميثاق الأمم المتحدة برمته.

وبالنظر إلى العمل الهام الذي أنجز بالفعل، نعتقد أنه ينبغي لنا أن نركز على تنفيذ المعايير والقواعد والمبادئ القائمة. ومن المبادئ الأســاســية المشــتركة بين البلدان النامية أنه يجب علينا أيضــا أن نعترف بأننا جميعا في مواقف متفاوتة من المخاطر، بالنظر إلى اختلاف قدرات الدول على الاحتراز من التهديدات التي تطرحها الأعمال الخبيثة في الفضـــاء الإلكتروني. ولذلك، فإن وفد بلدي يود أن يؤكد على الحاجة إلى برامج لبناء القدرات من الدول والجهات الأخرى صــاحبة المصــلحة، على حد ســواء، لمســاعدة البلدان على مكافحة التهديدات المزعزعة للاســتقرار من قِبَل الجهات الفاعلة الخبيثة في المجال الســيبراني. وتعتقد جنوب أفريقيا أن بناء القدرات أمر بالغ الأهمية في تحقيق المساواة بين الدول من أجل تحسين الأمن السيبراني العالمي، لأن هذا تحد عالمي حقا يتطلب حلولا عالمية.

وأخيرا، إن جنوب أفريقيا لا تزال على التزامها بمواصـــلة المشـــاركة في معالجة هذه المســـائل، ولا ســيما في ســياق الفريق العامل المفتوح العضــوية المعني بأمن تكنولوجيا المعلومات والاتصــالات وأمن استخدامها، الذي سيبدأ عمله الموضوعي في كانون الأول/ديسمبر. وسيكون ذلك بمنزلة مسار واحد شامل للجميع من أجل مناقشــة الكيفية التي يمكننا بها جميعا التصــدي للأخطار الناشــئة والمعقدة والمعممة التي تهدد السلام والأمن الدوليين في الفضاء الإلكتروني.

المرفق التاسع والخمسون

بيان البعثة الدائمة لسويسرا لدى الأمم المتحدة

[الأصل: بالفرنسية]

أود أن أشكر إستونيا على تنظيم هذه المناقشة المفتوحة، كما أشكر الممثلة السامية على الإحاطة التي قدمتها. لقد أصبح الفضاء الإلكتروني جزءا لا يتجزأ من مجتمعاتنا، وهو يخلق فرصا عظيمة للتنمية الاجتماعية والاقتصادية. وفي الوقت نفسه، فإن العمليات السيبرانية الخبيثة تهدد بخلق عدم الاستقرار، وقد أصبحت خطرا يتهدد السلام والأمن الدوليين. ويساورنا القلق من أن الفضاء الإلكتروني يستخدم حاليا لعرض القوة، وقد أصبح يتزايد تجزؤا وزعزعةً.

إن الفضاء الإلكتروني المفتوح والآمن والمستقر والميسّر والسلمي فيه فائدة للجميع. وتضطلع الأمم المتحدة بدور بالغ الأهمية في هذا المسعى. وترحب سويسرا باعتماد تقريري فريق الخبراء الحكوميين والفريق العامل المفتوح العضوية بتوافق الآراء. ويمثل هذان التقريران خطوتين أساسيتين صوب السلوك المسؤول للدول في الفضاء الإلكتروني.

ولتعزيز السلام والاستقرار في الفضاء الإلكتروني، أود أن أبرز بعض النقاط.

أولا، إن القانون الدولي ينطبق على الفضاء الإلكتروني. وإن احترام القانون الدولي شرط أساسي لمنع نشوب النزاعات وصون السلام والأمن الدوليين. وينطبق الالتزام بتسوية النزاعات بالوسائل السلمية أيضا على أنشطة الدول في الفضاء الإلكتروني. وعلاوة على ذلك، فإن القانون الدولي الإنساني ينطبق عندما يكون النزاع المسلح، سواء أكان دوليا أم غير دولي، قائما بحكم الواقع. وترحب سويسرا بأن آخر تقرير لفريق الخبراء الحكوميين يذكر ذلك بوضوح. وهذا معلم هام. فالقانون الدولي الإنساني ومبادئه الأساسية تضع قيودا هامة على تنفيذ العمليات في الفضاء الإلكتروني في سياق النزاع المسلح.

ثانيا، إن سويسرا تشعر بالقلق إزاء الأثر الإنساني للعمليات السيبرانية الخبيثة، الآخذة في الازدياد منذ انتشار الجائحة، وهي تتعلق في معظم الحالات بالبنية التحتية الطبية. وتشدد سويسرا على أن هذه البنية التحتية مشمولة بالحماية، كما يتضح من المناقشة المفتوحة التي جرت في نيسان/أبريل. وتوفر تقارير فريق الخبراء الحكوميين إطارا لحماية البنية التحتية الحيوية من الأنشطة السيبرانية الخبيثة. وإضافة إلى ذلك، يجب حماية البيانات التي تُجمع لأغراض إنسانية. ونشجع الدول أيضا على الامتثال للمعايير الطوعية للسلوك المسؤول في الفضاء الإلكتروني، وللتوجيهات الإضافية لفريق الخبراء الحكوميين من أجل تنفيذها، بهدف تجنب إلحاق الضرر بالبنية التحتية الحيوية، وتخفيف الآثار الإنسانية، وضمان حماية المدنيين.

ثالثا، إن تدابير بناء الثقة مهمة لمنع إشاعة مناخ من انعدام الثقة في الفضاء الإلكتروني. وعلى الصعيد الإقليمي، تلتزم سويسرا بتعزيز دور منظمة الأمن والتعاون في أوروبا في تعزيز الاستقرار السيبراني. وهي تقوم حاليا، وبالاشتراك مع ألمانيا، بوضع اقتراح لتنفيذ تدبير لبناء الثقة ينص على إجراء مشاورات في سياق أي حادث سيبراني خطير. وسويسرا ملتزمة أيضا بالشفافية وبناء القدرات. ويقدم المركز الوطني للأمن السيبراني لدينا الدعم التقني للدول الأخرى في حالة وقوع حادث، وهو يتبادل البيانات والمعلومات المتعلقة بالتهديدات المحتملة. وينبغي لمجلس الأمن ومؤسسات الأمم المتحدة أن تأخذ في الاعتبار المبادرات الإقليمية، وتدابير بناء الثقة التي أثبتت جدواها في تعزيز السلام والاستقرار في الفضاء الإلكتروني.

وأخيرا، تؤدي منظمات المجتمع المدني والأوساط الأكاديمية والأوساط التقنية والقطاع الخاص دورا هاما في دعم استقرار الفضاء الإلكتروني على الصعيد الدولي، ولا سيما فيما يتعلق باحترام حقوق الإنسان والحريات الأساسية على شبكة الإنترنت وخارجها. وتعمل سويسرا، بوصفها عضوا في التحالف من أجل الحرية على شبكة الإنترنت، مع أكثر من 30 حكومة، ومع شبكة من الجهات صاحبة المصلحة، على تعزيز حرية التعبير على شبكة الإنترنت. ونحن نشجع مجلس الأمن والدول الأعضاء على إشراك مختلف الجهات الفاعلة في تنفيذ إطار السلوك المسؤول للدول في الفضاء الإلكتروني.

والتعاون المتعدد الأطراف والالتزام بالقانون الدولي، بما في ذلك القانون الدولي لحقوق الإنسان والقانون الدولي الإنساني، هما أمران أساسيان للسلام والأمن في الفضاء الإلكتروني. وسويسرا تشجع على مواصلة العمل بشأن هذه المواضيع، بما في ذلك العمل في الفريق العامل المفتوح العضوية الجديد، وبرنامج العمل المقبل من أجل الارتقاء بالسلوك المسؤول للدول في الفضاء الإلكتروني. وسويسرا، بوصفها مرشحة لمجلس الأمن، تتطلع إلى مواصلة حوار بنّاء ومتعدد الأطراف، وذلك بالاستناد إلى الإنجازات القائمة.

المرفق الستون

بيان البعثة الدائمة لتايلند لدى الأمم المتحدة

إن تايلند تقدر جهود إستونيا في تنظيم المناقشة المفتوحة الرفيعة المستوى لمجلس الأمن بعنوان "صون السلام والأمن الدوليين في الفضاء الإلكتروني" في هذا المنعطف المهم والحَسن التوقيت. ونشيد أيضا بقيادة إستونيا، حيث إنها كانت سباقة إلى عقد جلسة رسمية للمجلس بشأن الأمن السيبراني. ونأمل أن يظل تأمين الفضاء الإلكتروني وتكنولوجيا المعلومات والاتصالات، ومنع إساءة استخدامهما، على رأس جدول أعمال المجلس، وفي الوقت نفسه، مواصلة الترحيب بمشاركة عموم الدول الأعضاء في الأمم المتحدة في هذه المناقشات الهامة.

إن تايلند ترى أن الفضاء الإلكتروني قد أفاد البشرية، كما اتضح خلال الجائحة، من خلال إبقاء السكان على اتصال بالخدمات الاجتماعية الأساسية، والأهم من ذلك، على تواصل بعضهم ببعض، وكذلك المساهمة في تحقيق خطة التنمية المستدامة لعام 2030. ومع ذلك، فإن استخدام الدول والجهات الفاعلة من غير الدول لتكنولوجيا المعلومات والاتصالات، بما في ذلك الإرهابيون، لأغراض خبيثة مثل الهجمات على البنية التحتية المدنية الحيوية، يؤدي لا إلى تقويض السلام والأمن الدوليين فحسب، بل يؤثر أيضا على سلامة شعوبنا. ولذلك، تقع على عاتق الدول مسؤولية معالجة هذه المسائل، تمشيا مع القوانين والقواعد الدولية ذات الصلة.

وتعتقد تايلند أن بإمكان الأمم المتحدة أن تضطلع بدور هام في دعم الجهود الرامية إلى إنشاء فضاء إلكتروني مستقر وآمن. والواقع أن أمن الفضاء الإلكتروني مدرج في جدول أعمال الدول الأعضاء منذ أكثر من عقدين من الزمن. وكانت أبرز النجاحات هي الاعتماد التاريخي الذي تم مؤخرا، بتوافق الآراء، لتقرير الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي (2019-2021)، ولتقرير فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي (2019-2021).

وترحب تايلند بالفريق العامل المفتوح العضوية الجديد المعني بأمن تكنولوجيات المعلومات والاتصالات واستخدامها للفترة 2021-2025. وإننا على ثقة من أن الدول، في ظل القيادة المقتدرة لسعادة للسيد برهان غفور، الممثل الدائم لسنغافورة ورئيس الفريق العامل المفتوح العضوية، ستشارك في مناقشات مثمرة، بما في ذلك مناقشات بشأن تعزيز الثقة والتعاون والشفافية فيما بين الدول، ومواصلة وضع معايير بشأن السلوك المسؤول للدول في الفضاء الإلكتروني.

وفي الفريق العامل المفتوح العضوية الجديد، تأمل تايلند أن تُسوى أو توضح المسائل التالية: مواصلة وضع توجيهات وتوصيات بشأن كيفية تفعيل معايير السلوك المسؤول للدول؛ والتوصل إلى فهم مشترك بشأن كيفية تطبيق القانون الدولي في الفضاء الإلكتروني، وهل يعاني ذلك من ثغرات أم لا؛ ووضع تدابير مستدامة لبناء الثقة تكون قائمة على الطلب، واعتماد "حوار مؤسسي منتظم".

وتحيط تايلند علما أيضا بالجهود الطيبة التي تبذلها الهيئات الحكومية الدولية الأخرى والقطاع الخاص ومنظمات المجتمع المدني، والعمليات التي أسهمت في مسعانا الجماعي نحو إنشاء فضاء إلكتروني آمن ومأمون. وتؤيد تايلند النهج القائم على تعدد الجهات صاحبة المصلحة في عملنا لضمان المشاركة المجدية للجهات صاحبة المصلحة والجهات الشريكة المعنية في المجتمع، بما في ذلك مشاركة النساء والشباب.

ولهذه الغاية، تؤيد تايلند تقوية الأسس المعيارية بتعزيز التنفيذ العملي لمعايير متفق عليها، وسد الثغرات القائمة واحتياجات القدرات، وضمان إبقاء القنوات المتعددة الأطراف والثنائية القائمة مفتوحة لمواصلة الحوار. ويجب على جميع الدول أن تواصل العمل معا على صون رؤيتنا المشتركة لبيئة حاوية لفضاء إلكتروني وتكنولوجيات المعلومات والاتصالات تكون مفتوحة ومأمونة وميسّرة وسلمية للجميع.

المرفق الحادي والستون

بيان البعثة الدائمة لتركيا لدى الأمم المتحدة

أود أن أشكر إستونيا على تنظيم هذه المناقشة المفتوحة، التي تركز على موضوع حاسم، ولا سيما في ظل الظروف الراهنة الناجمة عن الجائحة. كما أشكر السيدة ناكاميتسو، الممثلة السامية لشؤون نزع السلاح، على الإحاطة التي قدمتها.

إن استخدام تكنولوجيات المعلومات والاتصالات يؤثر على الاقتصاد والتنمية في جميع أنحاء العالم. وقد أبرزت الجائحة مدى اعتمادنا الشديد على التكنولوجيات الرقمية. ومن المؤكد أن ضمان وصول حر ومفتوح وآمن إلى تكنولوجيا المعلومات والاتصالات هو أمر بالغ الأهمية.

وتشعر تركيا بالقلق إزاء تزايد أعداد الهجمات الإلكترونية. ومن بين التهديدات الحالية التي تعرض للخطر أيضا السلام والأمن الدوليين هي الأنشطة السيبرانية الخبيثة التي تستهدف البنية التحتية الحيوية، والإرهاب، والتجسس الرقمي، والاحتيال، وإساءة معاملة الأطفال واستغلالهم على الإنترنت، وإساءة استخدام البيانات الشخصية.

وبسبب التطورات التكنولوجية، أصبح تنفيذ الهجمات السيبرانية أسهل، في حين أن الآثار السلبية والتكاليف التي يتحملها الضحايا آخذة في الازدياد بسرعة. كما أن الهجمات السيبرانية تصبح "موجهة نحو أهداف" بشكل أكبر. وتتزايد التكاليف السنوية للهجمات السيبرانية زيادة تصاعدية. ويتطلب صدّ هذه الهجمات أساليب وأدوات جديدة وحديثة.

وتعرب تركيا عن الترحيب بالتقارير الصادرة بتوافق الآراء للفريق العامل المفتوح العضوية المعني بالتطورات في ميدان تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي، ومؤخرا، فريق الخبراء الحكوميين التابع للأمم المتحدة المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني. وهذه التقارير هي مساهمات قيّمة في الإنجازات الحالية بشأن الأمن السيبراني تحت مظلة الأمم المتحدة. ومن المهم بنفس القدر أن يكون كل من تقريري الفريق العامل المفتوح العضوية وفريق الخبراء الحكوميين متوافقين ومتكاملين من أجل زيادة الاستقرار والقدرة على الصمود والتعاون الدولي في الفضاء الإلكتروني. ونأمل أن نرى المزيد من التماسك في هذه المساعي مستقبلا.

إن تركيا، وفي ظل تسارع عملية الرقمنة فيها، تركز على اتخاذ التدابير اللازمة من أجل تحسين أمنها السيبراني الوطني. إذ يجري، حاليا، تنفيذ الاستراتيجية وخطة العمل الوطنية للأمن السيبراني، التي تغطي الفترة 2020-2023. والأهداف الاستراتيجية الرئيسية لخطة العمل هذه هي حماية البنية التحتية الحيوية وزيادة القدرة على الصمود، وبناء القدرات، وإقامة شبكة عضوية للأمن السيبراني، وأمن تكنولوجيات الجيل الجديد (مثل إنترنت الأشياء، والجيل الخامس، والحوسبة السحابية، وما إلى ذلك)، ومكافحة الجريمة السيبرانية، وتطوير وتعزيز التكنولوجيات المحلية والوطنية، وإدماج الأمن السيبراني في الأمن الوطني، وتحسين التعاون الدولي.

وإضافة إلى ذلك، يضطلع الفريق الوطني لمواجهة الطوارئ الإلكترونية في تركيا بدور حيوي في تنفيذ وتنسيق التدابير الوقائية الرامية إلى مكافحة التهديدات السيبرانية.

وتُستكمل جهودنا ببرامج تدريبية وكذلك بتدريبات وطنية ودولية في مجال الأمن السيبراني. وتقدم الهيئة التركية لتكنولوجيا المعلومات والاتصالات دورات تدريبية عامة عبر الإنترنت حول الأمن السيبراني ومجالات أخرى ذات صلة. وقد تدرّب ما يربو على 000 5 شخص في مجالات مختلفة من الأمن السيبراني في السنوات الأربع الماضية.

و "يوم الإنترنت الأكثر أمانا"، الذي ينظم سنويا، هو من بين أنشطة التوعية التي تقوم بها الهيئة التركية لتكنولوجيا المعلومات والاتصالات بهدف زيادة الوعي بالاستخدام الواعي والآمن للإنترنت. وإضافة إلى ذلك، تتخذ تركيا خطوات لمواجهة المخاطر الأمنية الرقمية المتزايدة على الأمن السيبراني، وقد اتخذت تدابير بالتعاون مع الجهات المعنية صاحبة المصلحة من أجل ضمان استمرارية تصريف الأعمال، وإمكانية الوصول، وحماية المستهلكين أثناء الجائحة.

واتخذنا أيضا خطوات لتعزيز إطارنا التشريعي الوطني.

ونظرا للطابع العابر للحدود للمخاطر السيبرانية، فإن لزيادة التعاون الدولي أهمية بالغة. ومن هذا المنطلق، تشارك تركيا في تبادل المعلومات الاستخباراتية المتعلقة بالتهديدات السيبرانية، وتساهم في سياسات واستراتيجيات التعاون ضمن المنظمات الإقليمية والدولية، بما في ذلك منظمة الأمن والتعاون في أوروبا، ومجموعة العشرين، ومنظمة التعاون والتنمية في الميدان الاقتصادي. وتشارك تركيا أيضا في التدريبات الدولية، بما في ذلك التدريبات ضمن نطاق الاتحاد الدولي للاتصالات السلكية واللاسلكية ومنظمة حلف شمال الأطلسي.

وللأمم المتحدة دور مركزي في تحقيق تعاون أشد فعالية يتسم بطابع استراتيجي أكبر في استخدام الدول لتكنولوجيا المعلومات والاتصالات. وتؤيد تركيا انطباق القانون الدولي في الفضاء الإلكتروني. وقد حان الوقت للاستفادة من العمل السابق الذي اضطُلع به داخل منظومة الأمم المتحدة وإيجاد طرق مجدية لتفعيل القواعد والمعايير والمبادئ والتوصيات المتعلقة بالسلوك المسؤول للدول في الفضاء الإلكتروني.

ومن المجالات ذات الأولوية في عملنا المستقبلي بلورة فهم مشترك بشأن كيفية تطبيق القانون الدولي في الفضاء الإلكتروني. وهذا أمر ضروري بالفعل للحد من حالات سوء الفهم، ولتعزيز المساءلة في الفضاء الإلكتروني.

وثمة حاجة أيضا إلى إنشاء قنوات اتصال فيما بين الدول الأعضاء في حالات الطوارئ ولتبادل المعلومات والموارد من خلال تلك القنوات. وذلك يسهم إسهاما كبيرا في بناء الثقة، وتسريع جهودنا في مجال بناء القدرات.

وإضافة إلى ذلك، فإننا بحاجة أيضا إلى استعراض وتعزيز الصكوك الدولية القائمة، على وجه السرعة، من أجل تعزيز التعاون ضمن إطار التكنولوجيات الجديدة، مثل الحوسبة السحابية، وإنترنت الأشياء، والجيل الخامس، والذكاء الاصطناعي.

ويمكن أن يكون إجراء مسح للنهج التنظيمية الوطنية الرامية إلى ضمان أمن التكنولوجيات الجديدة، وإعداد مدونة لقواعد السلوك، كي تسترشد بها الأطر الوطنية وتعمل على ضوئها، أدوات مفيدة في هذا الصدد. ونحن بحاجة أيضا إلى وضع فهم مشترك وتعاريف مشتركة للتهديدات.

وفي ســـياق بناء القدرات، نعتقد أن الأمم المتحدة والمنظمات الإقليمية يمكنها تعزيز برامج التبادل لخبراء الأمن السـيبراني، وإنشـاء منصـات تدريب مشـتركة. ويجب تشـجيع التدريبات الدولية من أجل تعزيز القدرات الوطنية على التأهب للحوادث السيبرانية وقدرات التصدي.

وبما أن الفضـاء الإلكتروني مجال لا يعترف بالحدود، وأن الأمن السـيبراني قضـية متعددة الجهات صـاحبة المصـلحة، فلا بد للسلطات الوطنية من العمل مع الجهات المسـتخدِمة والقطاع الخاص والمنظمات غير الحكومية والجهات النظيرة الدولية على مكافحة التهديدات السـيبرانية. وينبغي للجهات الموردة والجهات المقدمة للخدمات وشـركات الأمن، على الصـعيد العالمي، أن تتعاون أيضـا بمزيد من الفعالية مع الحكومات والمنظمات الدولية من أجل المساهمة في الأمن السيبراني العالمي.

وتركيا ملتزمة بمواصلة مشاركتها وحوارها من أجل تعزيز الأمن السيبراني الإقليمي والعالمي.

المرفق الثاني والستون

بيان البعثة الدائمة لأوكرانيا لدى مجلس الأمن

إننا نعرب عن شكرنا لإستونيا على المبادرة بعقد هذه الجلسة الهامة لمجلس الأمن، وكذلك السيدة ناكاميتسو، الممثلة السامية لشؤون نزع السلاح، على الإحاطة التي قدمتها.

لقد أدى التطور السريع لتكنولوجيا المعلومات والاتصالات تدريجيا إلى "إعادة تنسيق" فضاء الإنترنت: ففي الوقت الحاضر، لم تعد الإنترنت منصة مريحة للتواصل فحسب، ولكنها أيضا سلاح حقيقي، يصبح أكثر خطورة في أيدي قراصنة الحواسيب والمجرمين وبعض الجهات الفاعلة من الدول ووكلائها.

وللأسف، فعلى الرغم من القواعد القانونية والآليات المؤسسية القائمة لمكافحة الجرائم السيبرانية على المستويات الوطني والإقليمي والدولي، فإن مزايا العالم الرقمي الحديث كثيرا ما يساء استخدامها، حيث إن الهجمات السيبرانية في تزايد، بعد أن أصبحت طريقة جديدة للحرب الهجينة.

لقد غدت السياسة الدولية، باطّراد، عرضة للتهديدات السيبرانية. فعلى مدى السنوات القليلة الماضية، أصبح عدد من الدول في العالم أهدافا مربحة للهجمات السيبرانية.

وأوكرانيا هي الدولة التي أصبحت فيها الهجمات السيبرانية، منذ عام 2014، أحد العناصر الرئيسية في المحاولة الخارجية لتقويض سيادتنا. ففي الفترة بين عامي 2014 و 2021، واجهت أوكرانيا عددا غير مسبوق من العمليات السيبرانية ضد أهداف حيوية في بنيتنا التحتية الحيوية. ومعظم تلك الهجمات نفذتها مجموعات من قراصنة الحواسيب يجري التحكم فيها من داخل الاتحاد الروسي.

والعمليات السيبرانية ضد مرافق البنية التحتية الحيوية الرئيسية، وقطاعات الطاقة والنقل والنفط والغاز، هي تحديات وتهديدات للسلام والأمن الدوليين. وفي الآونة الأخيرة، كان خط الأنابيب "كولونيال" هدفا لهجوم سيبراني أثر تأثيرا خطيرا على المعدات المحوسبة التي تدير خط الأنابيب، مما أدى إلى عواقب وخيمة.

وفي أوقات جائحة مرض فيروس كورونا (كوفيد-19)، يتجلى التأثير المدمر للعمليات السيبرانية الخبيثة. وبعض الجهات الفاعلة، سواء من الدول أو من غير الدول، تستغل الأزمة العالمية استغلالا سيئا لشنّ عمليات سيبرانية، منها عمليات استهدفت القطاع الصحي، وهو أمر يسبب قلقا ملحا للمجتمع الدولي.

بل إن الأمر لا يقتصر على البنية التحتية الحيوية، فقد أصبحت السياسة الدولية، باطّراد، عرضة للاستخدام الخبيث لقدرات تكنولوجيا المعلومات والاتصالات التي ما فتئت تزداد تعقيدا وتطورا، وهو ما أكدته حالات تدخل في الحملات الانتخابية الرئيسية ونُبذ المرشحين ارتكبها قراصنة حواسيب محسوبين على الكرملين، وتصدرت العناوين الرئيسية لنشرات الأخبار.

ولذلك، أصبح الاستقرار السيبراني عنصرا حاسما في ضمان السلام والأمن على نطاق أوسع، يتطلب تقيدا صارما بالقانون الدولي، الذي أعيد التأكيد على تطبيقه في الفضاء الإلكتروني مؤخرا في تقريري الفريق العامل المفتوح العضوية وفريق الخبراء الحكوميين، والتنفيذ المناسب للمعايير والقواعد والمبادئ المتعلقة بالسلوك المسؤول، وكذلك تعزيز التعاون الدولي للحفاظ على فضاء إلكتروني حر ومفتوح ومستقر وآمن.

ونؤكد على ضرورة إيلاء اهتمام خاص لوضع معايير موحدة من أجل مكافحة التهديدات السيبرانية، وتبادل الممارسات الفضلى، وبناء الثقة المتبادلة في مجال الأمن السيبراني، ومنع استخدام

الفضاء الإلكتروني لأغراض سياسية وإرهابية وعسكرية، وكذلك تقديم مساعدة مالية وتقنية لتعزيز القدرات الوطنية على التعامل مع التهديدات السيبرانية، والتخفيف من المخاطر، وتعزيز القدرة على الصمود.

ولغاية اليوم، فإن العمليات السيبرانية ضد البنية التحتية الحيوية والوكالات الحكومية، وكذلك حملات التضليل الإعلامي، التي قد تحرّض على الإرهاب، هي طريقة شائعة الاستخدام للتدخل في الشؤون الداخلية للدول ذات السيادة، بما في ذلك أوكرانيا.

ولا شك في أن روسيا تستخدم تكنولوجيات متطورة لتحقيق مآربها السياسية والجيوسياسية الخاصة بها، أي من خلال تأجيج النزاعات في الدول المجاورة وإذكائها، وشن حروب معلوماتية عدوانية.

ونحن نشجع بقوة المجتمع الدولي على النظر بدقة في مسألة المساءلة في الحالات التي تحدَّد فيها هوية دولة معينة أو جهات فاعلة معينة من الدول تقف وراء الإعداد للاستخدام الخبيث المستهدف لتكنولوجيات المعلومات والاتصالات، أو نشر أكاذيب لأغراض عدائية، أو ممارسة ذلك فعليا.

ففي نهاية الأمر، فإن الجهود الدولية المبذولة في هذا المجال تذهب هكذا سدى، ما لم تكن توجد آليات موثوقة للكشف عن الأفراد والدول المعنية، المسؤولة عن تنسيق وتمويل الأنشطة غير المشروعة في الفضاء الإلكتروني العالمي، ومعاقبتها وتقديمها للمحاكمة.

المرفق الثالث والستون

بيان البعثة الدائمة لدولة الإمارات العربية المتحدة لدى الأمم المتحدة

إن جائحة مرض فيروس كورونا (كوفيد-19) قد سلطت الضوء على مدى اعتماد العالم على تكنولوجيات المعلومات والاتصالات، حيث إنها تؤدي دورا جوهريا في إبقائنا على اطلاع بالأمور، وعلى اتصال ببعضنا البعض، حتى وإن كنا نظل متباعدين بدنيا.

وعلى مدى الأشهر الثمانية عشر الماضية، شهدنا اتجاها متزايدا في العمليات السيبرانية الخبيثة التي تستهدف المرافق الطبية، بما في ذلك المنظمات المكرسة للبحث وتطوير اللقاحات لمكافحة كوفيد-19. ونحن نعيش في منطقة مضطربة، والشرق الأوسط ليس بمنأى عن الخطر الذي يطرحه النشاط السيبراني الخبيث – فهو غالبا ما يكون هدفا لعمليات سيبرانية وعمليات تجسس كبرى. ففي السنوات القليلة الماضية، شهدت منطقتنا حوادث خطيرة أثرت على قطاع الاتصالات السلكية واللاسلكية، والقطاع المصرفي، والقطاع العام. واستهدفت أيضا منشآت النفط والغاز الطبيعي، مما تسبب في أضرار بمئات الملايين. ومثل هذا النشاط السيبراني الخبيث الموجه إلى البنية التحتية الحيوية في المنطقة لديه القدرة على إشعال نزاع في بيئة متوترة أصلا، ويؤدي إلى أخطار تهدد السلام والأمن الدوليين.

وتلتزم دولة الإمارات العربية المتحدة بإنشاء البنية التحتية والآليات اللازمة لتعزيز قدراتها في مجال الأمن السيبراني، سواء بغرض حماية نفسها من التهديدات السيبرانية، والعمل بشكل أفضل مع الآخرين لمواجهة التحديات المشتركة. وفي تشرين الثاني/نوفمبر 2020، أنشأنا مجلس الأمن السيبراني بالإمارات العربية المتحدة، الذي سيعمل على تطوير استراتيجية وطنية شاملة للأمن السيبراني وخطة وطنية للاستجابة للحوادث السيبرانية. ونحن نستضيف أكبر مؤتمرات الأمن السيبراني والتحول الرقمي بما في ذلك جيتكس (GITEX) وجيسيك (GISEC) وسيبرتيك (Cybertech)، لبناء القدرات المحلية، كما طورنا منصة للشراكة بين القطاعين العام والخاص من أجل تسهيل تبادل المعلومات. ونحن نتعاون أيضا مع الدول والمنظمات الدولية وكيانات القطاع الخاص لتبادل المعلومات على مستوى السياسات والمستوى الفني. فعلى سبيل المثال، تساهم الإمارات العربية المتحدة في عمل المنظمات الإقليمية، مثل المنصة المشتركة الجديدة لتحليل البرمجيات الخبيثة التابعة لمجلس التعاون الخليجي، وهي عضو نشط في فريق الاستجابة للطوارئ الحاسوبية بمنظمة التعاون الإسلامي. وتدابير بناء الثقة هذه، التي تتسم بالطابع التعاوني والشفافية، هي بعض الطرق التي تقوم من خلالها الإمارات العربية المتحدة بقسطها من الحد من المخاطر السيبرانية التي تتهدد السلام والأمن الدوليين.

وترحب الإمارات العربية المتحدة بالتوصيات الواردة في تقريري كل من الفريق العامل المفتوح العضوية المعني بتكنولوجيات المعلومات والاتصالات، وفريق الخبراء الحكوميين. فهي تؤكد أهمية دعم الجهود الرامية إلى تعزيز تنفيذ المعايير الطوعية للسلوك المسؤول للدول في الفضاء الإلكتروني، وكذلك الحاجة إلى بلورة تفاهمات عامة بشأن انطباق القانون الدولي على النشاط على شبكة الإنترنت. غير أنه ما يزال يتعين القيام بالمزيد لتشجيع ودعم الدول في تنفيذ التوصيات، وكذلك لتوفير مزيد من التوجيه في بيئة تمور بالمتغيرات. ويوفر برنامج العمل للسلوك المسؤول للدول في الفضاء الإلكتروني خريطة طريق مثالية للعمل المستقبلي، وسيساهم في التصدي للمخاطر السيبرانية التي تهدد السلام والأمن الدوليين.

وسيظل التقليل إلى أدنى حد من المخاطر السيبرانية على السلام والأمن الدوليين أحد التحديات الماثلة في ذلك الصدد. وتقترح الإمارات العربية المتحدة توصيتين يمكنهما المساعدة في هذه المهمة.

أولا، توفير التدريب وبناء القدرات اللازمة على المستويات الثنائي والإقليمي والدولي، بسبل منها برامج التدريب ووضع الإرشادات للمساعدة على تنفيذ معايير السلوك المسؤول للدول. ومثل هذه الإجراءات يمكن أن تكون بمثابة تدابير لبناء الثقة، والرد على انعدام الثقة وسوء الفهم بين الدول في الفضاء الإلكتروني الذي يمكن أن يشكل خطرا على السلام والأمن الدوليين.

ثانيا، ينبغي للدول مواصلة تبادل وجهات نظرها وتقييماتها مع الأمين العام، وعبر المشاركة النشطة في المنتديات الدولية ذات الصلة بالفضاء الإلكتروني، وعبر أطر التنسيقات الإقليمية. ويمكن لتبادل الممارسات الفضلى وتبادل الخبرات أن يساعد الدول على مواكبة المعايير المتطورة وأن تصبح جهات فاعلة مسؤولة في الفضاء الإلكتروني.

وتتحمل جميع الدول مسؤولية تعزيز السلام والأمن الدوليين، سواء على شبكة الإنترنت أو خارجها. وإن التقيد بمعايير السلوك المسؤول للدول، بالاقتران مع احترام الالتزامات الواجبة بمقتضى القانون الدولي، هو أفضل نقطة للانطلاق.