مجلس الأمن

السنة التاسعة والسبعون

مؤقت

الجلسة 9662

الخميس، 20 حزيران/يونيه 2024، الساعة 10/00

نيويورك

الرئيس	السيد تشو تاي – يول/السيد هوانغ	(جمهورية كوريا)
الأعضاء:	الاتحاد الروسي	السيد نبينزيا
	إكوادور	السيد دي لا غاسكا
	الجزائر	السيد بن جامع
	سلوفينيا	السيد جبوغار
	سويسرا	السيدة شاندا
	سيراليون	السيد كانو
	الصين	السيد فو كونغ
	غيانا	السيد بيرسود
	فرنسا	السيد دو ريفيير
	مالطة	السيدة فرازير
	المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية	السيدة باربرا وودورد
	موزامبيق	السيد أفونسو
	الولايات المتحدة الأمريكية	السيدة توماس – غرينفيلد
	اليابان	السيد يامازاكي

جدول الأعمال

صون السلام والأمن الدوليين

التصدي للتهديدات المتطورة في الفضاء السيبراني

رسالة مؤرخة 7 حزيران/يونيه 2024 موجهة إلى رئيس مجلس الأمن من الممثل الدائم لجمهورية كوريا لدى الأمم المتحدة (S/2024/446)

افتُتِحت الجلسة الساعة 10/00.

إقرار جدول الأعمال

أقر جدول الأعمال.

صون السلام والأمن الدوليين

التصدي للتهديدات المتطورة في الفضاء السيبراني

رسالة مؤرخة 7 حزيران/يونيه 2024 موجهة إلى رئيس مجلس الأمن من الممثل الدائم لجمهورية كوريا لدى الأمم المتحدة (S/2024/446)

الرئيس (*تكلم بالإنكليزية*): أود أن أرحب ترحيباً حاراً بالأمين العام وبالوزراء وغيرهم من الممثلين الرفيعي المستوى الحاضرين في القاعة اليوم. ويؤكد حضورهم اليوم أهمية الموضوع قيد المناقشة.

وفقا للمادة 37 من النظام الداخلي المؤقت للمجلس، أدعو إلى المشاركة في هذه الجلسة ممثلي الأرجنتين، إسبانيا، أستراليا، إستونيا، إسرائيل، ألبانيا، ألمانيا، الإمارات العربية المتحدة، إندونيسيا، أوروغواي، أوكرانيا، جمهورية إيران الإسلامية، إيطاليا، باكستان، البحرين، البرازيل، البرتغال، بلجيكا، بلغاريا، بنغلاديش، بنما، بولندا، تركيا، تشيكيا، جورجيا، رومانيا، السلفادور، سنغافورة، شيلي، غامبيا، غانا، غواتيمالا، الفلبين، فييت نام، كازاخستان، كرواتيا، كمبوديا، كوبا، كوستاريكا، كيريباس، لاتفيا، ليختنشتاين، مصر، المغرب، النرويج المملكة العربية السعودية، النمسا، نيبال، الهند، واليونان.

وفقا للمادة 39 من النظام الداخلي المؤقت للمجلس، أدعو مقدمي الإحاطتين التالي اسماهما للمشاركة في هذه الجلسة: السيد ستيفان دوغين، الرئيس التنفيذي لمعهد السلام الإلكتروني؛ والسيدة نينا إيفياني – أجوفو، أستاذة القانون والتكنولوجيا بجامعة ليدز بيكيت.

ووفقا للمادة 39 من النظام الداخلي المؤقت للمجلس، أدعو أيضا التالي أسماؤهم إلى المشاركة في هذه الجلسة: سعادة السيدة هيدا سامسون، القائمة بالأعمال بالنيابة لوفد الاتحاد الأوروبي لدى الأمم المتحدة؛ والسيدة روراييما آنا أندرياني، الممثلة الخاصة للإنتربول لدى الأمم المتحدة؛ والسيدة لاتيتيا كورتوا، المراقبة الدائمة ورئيسة وفد اللجنة الدولية للصليب الأحمر لدى الأمم المتحدة.

يبدأ مجلس الأمن الآن نظره في البند المدرج في جدول أعماله.

أود أن أسترعي انتباه أعضاء المجلس إلى الوثيقة S/2024/446، التي تتضمن نص رسالة مؤرخة 7 حزيران/يونيه 2024 موجهة إلى رئيس مجلس الأمن من الممثل الدائم لجمهورية كوريا لدى الأمم المتحدة، يحيل بها ورقة مفاهيمية بشأن البند قيد النظر.

أعطي الكلمة الآن للأمين العام، معالي السيد أنطونيو غوتيريش.

الأمين العام (*تكلم بالإنكليزية*): أشكر جمهورية كوريا على عقد هذه المناقشة الرفيعة المستوى بشأن مسألة تؤثر علينا جميعاً – السلام والأمن في الفضاء الإلكتروني.

تحدث تطورات في التكنولوجيا الرقمية بسرعة فائقة – بدءًا من تكنولوجيا المعلومات والاتصالات والحوسبة السحابية إلى تقنية سلسلة الكتل وشبكات الجيل الخامس والتقنيات الكمية وغيرها. يُحدث التقدم الرقمي ثورة في الاقتصادات والمجتمعات. إنه يجمع بين الناس؛ ويعمل على إيصال المعلومات والأخبار والمعرفة والتعليم بنقرة على الشاشة أو بنقرة على الفأرة؛ ويوفر للمواطنين إمكانية الوصول إلى الخدمات والمؤسسات الحكومية؛ ويعزز الاقتصادات والتجارة والشمول المالي.

ولكن جودة الاتصال السلس والفوري التي توفر المزايا الهائلة للفضاء الإلكتروني يمكن أن تجعل الناس والمؤسسات والبلدان بأكملها عرضة للخطر الشديد. كما أن مخاطر استخدام التكنولوجيا الرقمية كسلاح تتزايد عاماً بعد عام. لقد فتح الفضاء الإلكتروني الأبواب على مصراعيها. يمكن لأي شخص الدخول، وكثيرون يفعلون. تتزايد الأنشطة الخبيثة في الفضاء الإلكتروني على يد الجهات الفاعلة من الدول ومن غير الدول والمجرمين.

حوادث الأمن السيبراني الخطيرة شائعة بشكل مقلق. من اختراق منظومات الخدمات العامة الأساسية مثل الرعاية الصحية والخدمات المصرفية والاتصالات السلكية واللاسلكية؛ إلى الأنشطة غير المشروعة

التي لا تتوقف، بما في ذلك ما تمارسه المنظمات الإجرامية ومن يُطلق عليهم اسم مرتزقة الإنترنت؛ إلى فيالق تجار الكراهية الذين يملأون طريق المعلومات الفائق السرعة بمثيرات الخوف والانقسام؛ إلى الاستخدام المتزايد للفضاء الإلكتروني كسلاح آخر في النزاعات المسلحة الجارية – إذ يدخل من يسمى بنشطاء القرصنة المدنيين في النزاع، وفي حالات كثيرة، يطمسون الخط الفاصل بين المقاتلين والمدنيين. كما أن الدمج المتزايد للأدوات الرقمية مع منظومات الأسلحة، بما في ذلك الأنظمة ذاتية التشغيل، يمثل أوجه ضعف جديدة.

وفي الوقت نفسه، أصبحت إساءة استخدام التكنولوجيا الرقمية أكثر تعقيدا وقدرة على التخفي. تنتشر البرمجيات الخبيثة، وبرمجيات محو الذاكرة وفيروسات حصان طروادة. إن العمليات السيبرانية التي يتيحها الذكاء الاصطناعي (AI) تضاعف من التهديد، ويمكن للحوسبة الكمية أن تسبب انهيار منظومات بأكملها بقدرتها على اختراق التشفير. وتستغل الثغرات البرمجية، بل إن قدرات الاختراق السيبراني تُباع عبر الإنترنت. ويستهدف القراصنة بنشاط سلاسل التوريد الخاصة بالشركات، مع ما يترتب على ذلك من آثار خطيرة ومُدمرة ومتتالية. تُعد برمجيات انتزاع الفدية الخبيثة أحد الأمثلة الخطيرة – وهي تهديد كبير للمؤسسات العامة والخاصة والبنية التحتية الحيوية التي يعتمد عليها الناس. ووفقًا لبعض التقديرات، بلغ إجمالي مدفوعات برمجيات انتزاع الفدية 1,1 بليون دولار في عام 2023.

ولكن ما هو أهم من التكاليف المالية هو ما يترتب على ذلك من تكلفة لسلامنا وأمننا واستقرارنا المشترك – سواء داخل الدول أو فيما بينها. فالأنشطة الخبيثة التي تقوض المؤسسات العامة والعمليات الانتخابية وسلامة الإنترنت تؤدي إلى تآكل الثقة وتؤجج التوترات، بل وتزرع بذور العنف والنزاع.

توفر التكنولوجيا الرقمية فرصة رائعة لتهيئة مستقبل أكثر عدلاً ومساواة واستدامة وسلاماً للجميع. لكن الإنجازات يجب أن تكون موجهة نحو الخير. تضع الخطة الجديدة للسلام المنع في صميم جميع جهود السلام. وتدعو إلى وضع أطر عمل قوية تتماشى مع القانون الدولي وحقوق الإنسان وميثاق الأمم المتحدة، وإلى تركيز جهود جميع الدول على منع امتداد النزاعات وتصعيدها داخل الفضاء الإلكتروني ومن خلاله. وكما هو مبين في الرؤية الجديدة لسيادة القانون، يجب أن تكون سيادة القانون موجودة في المجال الرقمي مثلما هي موجودة في العالم المادي.

وأرحب أيضا بالتزام الجمعية العامة بالعمل في هذا المجال. ويشمل ذلك الفريق العامل المكرس المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها. وتستند الدول إلى الإطار المعياري المعتمد عالميًا لسلوك الدول المسؤول في الفضاء السيبراني، وتنظر بنشاط في إمكانية تطبيق القانون الدولي على أنشطة الدول في هذا المجال. وتحت رعاية الجمعية العامة، تعمل الدول الأعضاء على التوصل إلى توافق في الآراء بشأن معاهدة جديدة لمكافحة الجريمة السيبرانية في الأشهر المقبلة، والتي ينبغي أن تعمق التعاون مع حماية حقوق الإنسان على الإنترنت. ولكن نظراً للصلات الواضحة والمتنامية بين الفضاء الإلكتروني والسلام والأمن العالميين، يمكن للمجلس أيضاً أن يلعب دوراً رئيسياً من خلال دمج الاعتبارات السيبرانية في مسارات عمله وقراراته الحالية.

هذه هي المرة الثانية فقط التي يعقد فيها مجلس الأمن جلسة رسمية بشأن هذه المسألة. غير أن الكثير من المسائل التي ينظر فيها حول هذه الطاولة تتأثر بالفضاء الإلكتروني وترتبط به، بما في ذلك حماية المدنيين في النزاعات المسلحة وعمليات السلام ومكافحة الإرهاب والعمليات الإنسانية. وإدماج هذه المسألة في مداولات المجلس سيكون وسيلة مفيدة لإرساء الأساس لاستجابات أكثر فعالية لهذه المسألة الهامة.

(تكلم بالفرنسية)

من أجل ضمان السلام والأمن في العالم المادي، نحتاج إلى نهج جديدة للسلام والأمن في العالم الرقمي. سيكون مؤتمر قمة المستقبل في أيلول/سبتمبر فرصة حيوية لتعزيز التعاون في مواجهة التحديات العالمية الحرجة وتنشيط النظام المتعدد الأطراف. ويمثل الميثاق الذي

سينبثق عن مؤتمر القمة فرصة فريدة لدعم الحفاظ على السلام والأمن الدوليين في الفضاء الإلكتروني. ويهدف الفصل الثاني من الميثاق، من بين الأولويات الأخرى، إلى إعادة تأكيد التوافق العالمي على حماية البنية التحتية الحيوية من الممارسات الرقمية الضارة وإيجاد مساءلة معززة للتكنولوجيا القائمة على البيانات، بما في ذلك الذكاء الاصطناعي. وفي الوقت نفسه، تعكف هيئتي الاستشارية رفيعة المستوى المعنية بالذكاء الاصطناعي على استكمال تقريرها النهائي عن كيفية إدارة الذكاء الاصطناعي من أجل البشرية، مع معالجة مخاطره وأوجه عدم اليقين التي تكتنفه. وأتطلع إلى العمل مع المجلس والجمعية العامة وجميع الدول الأعضاء لضمان استخدام التكنولوجيا على النحو الملائم: للعمل من أجل تقدم وأمن جميع الناس والكوكب الذي نتشاركه.

الرئيس (*تكلم بالإنكليزية*): أشكر الأمين العام على إحاطته.

أعطي الكلمة الآن للسيد دوغين.

السيد دوغين (*تكلم بالإنكليزية*): يشرفني أن أخاطب مجلس الأمن اليوم بشأن مسألة ذات أهمية حاسمة: كيفية التصدي للتهديدات المتطورة في الفضاء الإلكتروني. وبصفتي الرئيس التنفيذي لمعهد سيبرسبيس (CyberPeace)، وهو منظمة غير حكومية مستقلة ومحايدة تتخذ من سويسرا مقرا لها، أتكلم من واقع خبرتي، حيث يقدم المعهد الأمن السيبراني المجاني للفئات الأكثر عرضة للخطر، وهي المنظمات غير الربحية، ويراقب الجهات الفاعلة في مجال التهديدات ويوفر الكشف عن التهديدات وتحليلها ويدعو إلى احترام القوانين والأعراف في الفضاء السيبراني.

وإذ نحلل تطور التهديد، أود أن أتناول الأثر التراكمي للاضطرابات الخطيرة التي طرأت على مشهد التهديد والتي تؤثر مجتمعةً تأثيراً مباشراً على صون السلم والأمن الدوليين. سأتطرق إلى مواضيع مختلفة: انتشار الجهات الفاعلة في مجال التهديدات، وكيف أنها تزيد من استهداف البنية التحتية الحيوية؛ وتحوّر التهديد اليوم، لا سيما مع تقارب الهجمات السيبرانية والتضليل الإعلامي واستخدام الهجمات السيبرانية للالتفاف على الجزاءات الدولية؛ وتطور التهديد غداً، مع الخطر الفريد الذي يشكله الذكاء الاصطناعي على الأمن السيبراني. وينتج عن تلك التطورات تحديات فريدة من نوعها للسلم والأمن الدوليين، لا سيما من خلال إعاقة عملية الإسناد، أي عملية تحديد مرتكب أو مصدر الهجوم أو العملية السيبرانية.

سأبدأ بانتشار الجهات الفاعلة المهدِّدة. فمنذ غزو الاتحاد الروسي لأوكرانيا في عام 2022، وثّق معهد سيبرسبيس انتشار الجهات الفاعلة في مجال التهديد التي تقف إلى جانب كلا الطرفين المتحاربين. ولم تعد الحرب حكراً على الدول وحدها. فمجموعة من الجهات الفاعلة من غير الدول – الجماعات الإجرامية، وجماعات القرصنة ذات الدوافع الجيوسياسية وغيرهم من المدنيين – تشارك في الهجمات والعمليات السيبرانية في سياق النزاعات المسلحة. وهي تسعى إلى تحقيق أربعة أهداف: تدمير البنية التحتية وتعطيل الأداء الطبيعي للخدمات الأساسية ومزامنة المعلومات المضللة والهجمات السيبرانية وسرقة البيانات واستخدامها سلاحا من خلال التسلل والتجسس. وفي ذلك السياق قمنا نحن، معهد سيبرسبيس، بتتبع أكثر من 3 000 حملة هجوم إلكتروني من قبل 127 جهة تهديد، أثرت على 56 دولة واستهدفت 24 قطاعًا من قطاعات البنية التحتية الحيوية. وقد تجاوز الضرر الناجم عن تلك الهجمات السيبرانية حدود الدول المتحاربة، حيث أن ما يقرب من 70 في المائة من جميع الهجمات السيبرانية أثرت على منظمات في دول غير متحاربة. وتلك المقاييس متاحة مجاناً على منصتنا للهجمات السيبرانية في زمن النزاعات. يطرح ذلك الانتشار الواسع للهجمات مسألة وقف التصعيد في سياق وقف محتمل للأعمال العدائية. كيف يمكن إجبار هؤلاء الـ 127 مهددًا على وقف أنشطتهم الخبيثة أو السيطرة عليها في تلك الظروف؟

إن لذلك الانتشار تأثير مباشر على أمن البنية التحتية الحيوية. وأود أن أعطي مثالين. في شباط/فبراير 2022، استهدف هجوم إلكتروني باستخدام برمجية خبيثة ماسحة تسمى AcidRain، الوصول إلى الإنترنت عبر الأقمار الصناعية في أوكرانيا. وكان التأثير محسوسًا خارج حدود أوكرانيا. وقد أثّر ذلك على عمل توربينات الرياح

في جميع أنحاء أوروبا، حيث فقدت إحدى شركات الطاقة الألمانية الكبرى إمكانية الوصول إلى المراقبة عن بُعد لأكثر من 800 5 من تلك التوربينات، كما تأثر آلاف المشتركين في خدمات الإنترنت عبر الأقمار الصناعية في ألمانيا وفرنسا والمجر واليونان وإيطاليا وبولندا. ولا تقتصر تلك الآثار على أوقات النزاعات المسلحة فقط. فخلال جائحة مرض فيروس كورونا (كوفيد-19)، رصد معهد سيبرسبيس 500 هجوم إلكتروني ضد مرافق الرعاية الصحية على مدار عامين من جائحة كوفيد-19. وخمسمائة هجوم إلكتروني ليس حتى قمة جبل الجليد – إنها تمثل مكعب ثلج على قمة جبل الجليد. وقد أدت تلك الهجمات الـ 500 وحدها إلى تعطيل الرعاية الصحية في 43 دولة وأدت إلى سرقة بيانات 20 مليون مريض وتسببت في تعطيل تراكمي في الوصول إلى الرعاية الصحية لمدة خمس سنوات. وذلك يعني تراكم خمس سنوات من إعادة توجيه سيارات الإسعاف وإلغاء المواعيد ومعاناة المرضى من تقليل فرص الحصول على الرعاية الصحية.

لكن هناك جانب آخر للتهديد المتطور وهو استخدام الهجمات السيبرانية للتهرب من الجزاءات الدولية وتمويل الأنشطة غير القانونية. وكمثال على ذلك، قامت العديد من الجهات الفاعلة في المجتمع المدني ومنظمات الأمن السيبراني والدول بتحليل أنشطة جماعتين إجراميتين مزعومتين هما جماعة كيمسوكي وجماعة لازاروس، نُسبت تكتيكاتهما وأدواتهما وعملياتهما ونواياهما إلى جمهورية كوريا الشعبية الديمقراطية. تقوم تلكما الجماعتان الإجراميتان بتنسيق الهجمات الإلكترونية العالمية من جميع الأنواع: على سلسلة التوريد وبرامج الفدية وعلى تبادل العملات الرقمية والمؤسسات المالية. وبالإضافة إلى الضرر المباشر أو الأساسي المهم لتلك الهجمات، فهي وسيلة للالتفاف على الجزاءات الدولية. ووفقًا للتقديرات الأخيرة، ربحت مجموعة لازاروس وكيمسوكي أكثر من 3 بلايين دولار من تلك الهجمات. ويؤدي ذلك التصعيد إلى إحداث ضرر كبير. وتسبب هجوم WannaCry الذي وقع في أيار/مايو 2017، والذي أثر على أكثر من ربع مليون جهاز كمبيوتر في أقل من 24 ساعة في أكثر من 150 دولة، في حدوث اضطراب كبير وكان له تأثير واسع النطاق في قطاعات الرعاية الصحية والمالية والنقل.

ولكي نختم بشأن تطور التهديدات، من المهم استشراف المخاطر الجديدة، مثل تهديد الحوسبة الكمية لعلم الترميز، كما ذكرنا سابقًا، والتهديد الذي يشكله الذكاء الاصطناعي التوليدي للنماذج الإجرامية. فمنذ ظهور الذكاء الاصطناعي التوليدي والنماذج اللغوية الكبيرة، استخدم الذكاء الاصطناعي من قبل الجهات الخبيثة لمجرد زيادة قدراتها. ويُستخدم الذكاء الاصطناعي اليوم لتوسيع نطاق العمليات الحالية فيما يسمى بسلسلة القتل السيبرانية، وهي العملية القياسية التي يجب أن يمر بها أي مهاجم من أجل شن هجوم إلكتروني. يؤدي استخدام الذكاء الاصطناعي إلى توفير الوقت في التعرف على الأهداف، وجعل عمليات البحث عن الثغرات تلقائية، وزيادة القدرة الإنتاجية للتصيد الإلكتروني، على سبيل المثال. وذلك ليس سوى الخطوة الأولى فقط، حيث تقوم المجموعات بالفعل بتجربة استخدام الذكاء الاصطناعي التوليدي لجعل أجزاء مختلفة من الهجوم الإلكتروني آلية تلقائية. وذلك يشكل خطراً غير مقبول. وتنطوي الاختبارات الناجحة على خطر الوصول إلى مستوى عالٍ من التلقائية الآلية عبر سلسلة القتل السيبرانية بحيث يمكن لفاعل خبيث أن يشن هجوماً إلكترونياً ذاتي التشغيل عن قصد أو عن غير قصد.

ونظراً لتلاقي العديد من الاضطرابات المتراكمة – انتشار التهديدات وطريقة العمل الجديدة المحددة لمهاجمة البنية التحتية الحيوية أو التحايل على الجزاءات وما سيحدث بسبب تكنولوجيا الذكاء الاصطناعي الجديدة، من الصعب الاستجابة باستراتيجية متماسكة. ومع ذلك، يمكن اتخاذ عدة خطوات، وسأختتم بهذا.

بإمكاننا إنفاذ القوانين وتطبيق الضوابط والجزاءات، لا سيما عن طريق التوثيق الصريح للانتهاكات واتباع نهج استباقي لمنع استغلال الفضاء الإلكتروني في أنشطة خبيثة، بما في ذلك سوء استخدام تكنولوجيا الذكاء الاصطناعي أو الحوسبة الكمية.

ومن الأهمية بمكان الكشف عن مرتكبي الانتهاكات وإنفاذ الجزاءات واتخاذ التدابير المجدية والوافية. فلا مجال لتخفيف حدة التوتر من دون تحديد الجهات المسؤولة، حيث يعتبر ذلك عنصراً

أساسيًا في توجيه عملية اتخاذ القرارات بشأن التدابير التي يجب اتخاذها وأساليب الحماية المطلوبة. ومن شأن تحديد الجهات المسؤولة أن يحقق تأثيراً رادعًا، إذ أن مساءلة مقترفي الانتهاكات قد تمكّن من اتخاذ إجراءات قانونية ودبلوماسية وتعزز صياغة السياسات.

ختاما، من الضروري التمكن من تقدير الأضرار الناجمة عن الهجمات الإلكترونية تقديرا وافيا وقابلا للقياس الكمي. ويعكف معهد السلام الإلكتروني على صياغة منهجية من هذا النوع لقياس الأضرار الناجمة عن الهجمات الإلكترونية نظرا لأنها حتى الآن، غالبا ما توصف من منظور الخسائر المالية أو التشغيلية، مع أن الأذى الذي يلحق بالسكان والتركيبات الاجتماعية لا يقل أهمية.

هذه الجوانب بالغة الأهمية لصون السلم والأمن الدوليين.

الرئيس (*تكلم بالإنكليزية*): أشكر السيد دوغين على إحاطته.

أعطي الكلمة الآن للسيدة إيفياني – أجوفو.

السيدة إيفياني – أجوفو (*تكلمت بالإنكليزية*): إنه لشرف لي أن أُدعى لمخاطبة هذا المنتدى بشأن صون السلم والأمن الدوليين والتصدي للتحديات المتنامية في الفضاء الإلكتروني، وبالأخص من خلال تقديم منظور إقليمي واستعراض الحالة في أفريقيا.

عند التطرق إلى السلام والأمن في الفضاء الإلكتروني، يجب الأخذ بعين الاعتبار قياس الأمن الإلكتروني وفقًا للحقائق والمنظورات الإقليمية القائمة. وعلينا أن نقر بأن التحقيق الفعال للأمن السيبراني غالبًا ما يصطدم بواقع الدول النامية، لا سيما تلك الواقعة في المنطقة الأفريقية والتي لا تزال متأخرة في مجال سد الفجوة الرقمية وتعاني من قصور في القدرات والمهارات والبنية التحتية اللازمة لكفالة السلام والأمن بفاعلية وفق المستويات المتوقعة. لذلك، وبينما نقر بالقواسم المشتركة في مجال الأمن الإلكتروني، علينا أيضاً إدراك التباينات والتحديات فيما بين المناطق، والنظر إلى المخاطر الإلكترونية في سياق الواقع الخاص بكل بلد ومنطقة.

باتت جوانب السلام والأمن في الفضاء الإلكتروني موضوعًا محوريًا في خطط عمل كثير من المناطق. فعلى سبيل الإيضاح، شهد نوفمبر/تشرين الثاني 2022 أول مرة يتطرق فيها مجلس السلم والأمن التابع للاتحاد الأفريقي مسألة السلام والأمن في الفضاء الإلكتروني من منظور تنظيمها وفقا لأحكام القانون الدولي. عقب ذلك، اعتمد الاتحاد الأفريقي الأمن الإلكتروني برنامجا رائدا في خطة الاتحاد الأفريقي لعام 2063 وموضوعا شاملا في استراتيجية الاتحاد الأفريقي للتحول الرقمي في أفريقيا للفترة 2020–2030. والأهم من ذلك إن اتفاقية الاتحاد الأفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، التي توفر إطارا تنظيميا موحدا للتخفيف من التهديدات الإلكترونية وحماية البنى التحتية لتكنولوجيا المعلومات والاتصالات، دخلت حيز التنفيذ في حزيران/يونيه 2023. في كانون الثاني/يناير من هذا العام، اعتمد الاتحاد الأفريقي أيضاً موقفا أفريقيا موحدا بشأن تطبيق القانون الدولي على استخدامات تكنولوجيا المعلومات والاتصالات في الفضاء الإلكتروني. وأود التنويه بأن الموقف الأفريقي هو السبّاق في كونه أول وثيقة بشأن تطبيق القانون الدولي في الفضاء الإلكتروني تتضمن جزءا لمسألة بناء القدرات. كما تنفرد أفريقيا بأسبقيتها في صياغة موقف مشترك إقليميا.

كما ينبغي لنا الإقرار بوجود تحديات شتى بشأن كيفية صون المناطق للسلام والأمن والاستقرار في الفضاء الإلكتروني. فمنذ العام الماضي، على سبيل المثال، شهدنا هجمات إلكترونية على مقر مفوضية الاتحاد الأفريقي أدت إلى تعطيل عمل أنظمة البريد الإلكتروني. وكشفت هيئة الاتصالات في كينيا أن البلد تعرض، خلال عام 2023 وحده، لـ 860 مليون من الهجمات الإلكترونية، بما في ذلك هجمات معقدة استهدفت البنية التحتية للمعلومات الحيوية في البلد. وفي شهر تموز/يوليه 2023 وحده، واجهت كينيا هجوما إلكترونيا كبيرا استهدف منصة المواطن الإلكترونية eCitizen ذات الأهمية القصوى، مما أدى إلى تعطيل الوصول إلى أكثر من 000 5 خدمة مقدمة من مختلف الجهات الحكومية بما فيها الوزارات والحكومات المحلية والوكالات. وأعلنت مجموعة تطلق على نفسها "السودان المجهول" مسؤوليتها عن عمليات القرصنة الإلكترونية تلك في كينيا وأجزاء أخرى من أفريقيا. ومنذ عدة أشهر، اضطرت حكومة ملاوي إلى تعليق إصدار جوازات السفر نتيجة

هجوم إلكتروني اخترق الشبكات الحاسوبية لمصلحة الهجرة، مما اعتبر انتهاكا جسيما للأمن الوطني.

ويثير ذلك قضايا مهمة، بما فيها الحدود المبهمة لمسؤولية جهات من الدول وجهات من غير الدول وديناميكيات مفاقمة هذه المخاطر الإلكترونية الناشئة لصدوع في النزاعات القائمة بالفعل. ونرى كيف تزداد أنشطة الجماعات الإرهابية والمتطرفة المنظمة تمكينا بسبب النزاعات في مناطق مثل أفريقيا. ونرى أن الأنشطة الإجرامية في الفضاء الإلكتروني لا تفاقم التهديدات والتحديات القائمة للسلم والأمن الدوليين في المنطقة فحسب، بل نرى أيضا كيفية انتهاك الدول حقوق الإنسان الدولية بحجة الأمن الإلكتروني عبر حجب خدمات الإنترنت، لا سيما أثناء النزاعات المسلحة. وتلك الإجراءات لا تنتهك حق المواطنين في التواصل وحرية الإعلام فحسب، بل حالت أيضا دون العمل الإنساني الفعال أثناء النزاعات في أماكن مثل أفريقيا، وبالطبع في أماكن أخرى. ونلمس أيضا كيف يتم استخدام المعلومات المضللة والمعلومات المغلوطة بشكل متزايد كأدوات لتقويض السلام والأمن في أجزاء من المنطقة. ويتفاقم الأمر بسبب استخدام الذكاء الاصطناعي في مثل هذه الظروف.

إلا أننا نعتقد أن مجلس الأمن قادر على إحداث تغيير هائل من أجل تعزيز السلام والأمن في الفضاء الإلكتروني، لا سيما من منظور إقليمي. والواقع أن مصادر أوجه التفاوت القائمة تستدعي تفاعلات معقدة من أجل تكليف مجلس الأمن بولاية بشأن السلام والأمن في الفضاء الإلكتروني. وتُعد هذه التباينات في البنية التحتية للأمن الإلكتروني والقدرات الرقمية تحدياً رئيسياً إضافة إلى النزاعات السياسية المستمرة في مناطق مثل أفريقيا. كما يبدو أن هناك قصورا في إدراك الالتزامات المتعلقة بمبدأ عدم التدخل والعناية الواجبة وتسوية المنازعات بالطرق السلمية في سياق الفضاء الإلكتروني.

إذ يحدد مجلس الأمن ولايته لصون السلام والأمن في الفضاء الإلكتروني، يغدو من المهم بالتالي النظر في تدابير التعاونية يمكن الاستفادة منها لمواجهة التهديدات القائمة وبناء القدرات. ومن الضروري إنشاء وتعزيز القدرات على المستويات الإقليمية. إلا أنه يجدر بنا الإشارة إلى أن هذه المسألة تتجاوز مجرد القدرات القانونية والتكنولوجية والتشغيلية، وتمتد لتشمل أيضًا الحقائق المجتمعية والاقتصادية والسياسية. ونظراً لتفاوت مستويات النضج في مجال الأمن الإلكتروني والسياقات المحلية، يلزم بناء القدرات الإقليمية الاستراتيجية. ويجب مراعاة الحقائق المحددة للمناطق المتنوعة لأن الثغرات في القدرات قد لا تكون بالضرورة هي نفسها عبر مختلف المناطق. من الضروري التعامل مع محاولات تطوير بناء القدرات في الفضاء الإلكتروني ونقلها عبر المناطق بشكل هادف، كما يجب أن تكون محددة استراتيجياً على أساس آليات مساءلة محددة.

في مناطق مثل أفريقيا، تشمل المجالات ذات الأولوية التي تستدعي بناء القدرات للتصدي للتهديدات الإلكترونية، الحوكمة وصنع السياسات والأدوات التقنية والبنية التحتية، فضلاً عن الأبحاث. هناك حاجة إلى تنمية القدرات لحماية البنية التحتية الحيوية. ومن المهم التأكد من إنشاء فرق الاستجابة لحوادث أمن الفضاء الإلكتروني على المستويات الإقليمية حيث لم يتم إنشاؤها بعد، والتكليف بتشكيل نقاط اتصال إقليمية على مدار الساعة طوال أيام الأسبوع. كما أنه من المهم أيضاً تطوير وتنفيذ آليات للتعاون الإقليمي والدولي بين تلك الأفرقة.

ولترسيخ الثقة والأمن في الميدان الإلكتروني، من الضروري الاهتمام بتطبيق قواعد الأمم المتحدة للسلوك المسؤول للدول في الفضاء السيبراني في جميع المناطق. وقد طُرحت العديد من الأسئلة حول الطابع الطوعي للمعايير والحاجة إلى وجود نهج أكثر عرضة للمساءلة لصون السلام والأمن في الفضاء الإلكتروني، على سبيل المثال، وجود مبادئ توجيهية واضحة ومحددة بشأن استخدام القوة والهجمات المسلحة والدفاع عن النفس في الفضاء الإلكتروني. مرة أخرى، إن إنشاء منتديات لتطوير تدابير بناء الثقة ودعمها سيقللان من انعدام الثقة بين الدول الأعضاء ويساهم في التسوية السلمية للنزاعات في المجال الإلكتروني.

ومن المهم أيضاً أن يقوم مجلس الأمن بتطوير آليات لفهم مشهد التهديد الإلكتروني في مختلف المناطق. وسيمكن ذلك من اتخاذ

قرارات مستنيرة بشأن تنظيم الأمن والاستقرار. وقد ينطوي ذلك أيضًا على إنشاء فريق عمل معني بالسلام والأمن في الفضاء الإلكتروني – للنظر أولا في التوصيات المتعلقة بالنزاعات وتعزيز السلام والاستقرار في الفضاء الإلكتروني. كما أن إنشاء مراكز إقليمية فعالة لأمن الفضاء الإلكتروني من أجل تعزيز التعاون وتبادل المعلومات عبر الحدود سيساعد على تحقيق تلك الأهداف. كما يجدر الاهتمام بتعزيز القدرات اللازمة لتطوير وتنفيذ استراتيجيات شاملة للأمن الإلكتروني على المستويين الإقليمي والوطني إلى جانب ترسيخ ثقافة الريادة في مجال أمن الفضاء الإلكتروني.

وتضطلع المنظمات الإقليمية بدور رئيسي في صياغة السياسات والعمل مع الدول في مناطقها لتحقيق نتائج من اجل تعزيز السلام والأمن. ولذلك، يجب أن يشمل الآن التعاون القائم بين الأمم المتحدة والمنظمات الإقليمية ودون الإقليمية على صون السلام والأمن الدوليين خطة بشأن أمن الفضاء الإلكتروني. وأخيراً، ينبغي لمجلس الأمن أن يدعم منصة تتيح إجراء حوار فعال يهدف إلى تشجيع كل منطقة على وضع إطار للسلام والأمن في الفضاء الإلكتروني.

وأختتم بياني بالتأكيد على أهمية أن يسعى مجلس الأمن إلى اعتماد خطة متعددة الأطراف تؤكد بصورة قاطعة أبعاد السلام والأمن لسيادة القانون في الفضاء الإلكتروني. كما يستوجب ذلك وضع مبادئ توجيهية ومعايير دقيقة محددة لتنظيم الفضاء الإلكتروني تكفل مساءلة جميع المناطق والحكومات عن السلام والاستقرار. كلما ازداد ارتباطنا ببعضنا وتعمق تأثرنا بالتكنولوجيات الإحلالية، مثل الذكاء الاصطناعي، نصبح أيضاً أكثر عرضة للخطر. لذلك، من الأهمية بمكان تعزيز قدرتنا البشرية والمؤسسية على تأمين الفضاء الإلكتروني من خلال بناء الثقة في استخدام تكنولوجيا الفضاء الإلكتروني.

الرئيس (*تكلم بالإنكليزية*): سأدلي الآن ببيان بصفتي وزير خارجية جمهورية كوريا.

أود أن أبدأ بتوجيه الشكر مرة أخرى إلى الأمين العام غوتيريش على حضوره وعلى إحاطته اليوم. وأود أيضًا أن أشكر السيد ستيفان دوغين، من معهد السلام الإلكتروني والأستاذة نينا إيفياني – أجوفو بجامعة ليدز بيكيت على مشاركتنا رؤاهما وخبراتهما. كما أعرب عن تقديري العميق لجميع ممثلي الدول الأعضاء على مشاركتهم في هذه المناقشة المفتوحة رفيعة المستوى.

إن جلسة اليوم تصادف المرة الثانية فحسب في تاريخ الأمم المتحدة التي يعقد فيها مجلس الأمن اجتماعا رسميا لبحث مخاطر الفضاء الإلكتروني التي تهدد السلم والأمن الدوليين. وقد عقد المجلس أول مناقشة مفتوحة على الإطلاق بشأن هذا الموضوع قبل ثلاث سنوات في حزيران/يونيه 2021 (انظر S/2021/621). من المؤكد أن تم تحقيق إنجازات مهمة خارج مجلس الأمن. لقد أحرزت الكيانات التي أنشأتها الجمعية العامة تقدما في وضع المعايير المتعلقة بسلوك الدول المسؤول في الفضاء الإلكتروني. كما عقد عدد من الجلسات وفق صيغة آريا بشأن أمن الفضاء الإلكتروني، كانت آخرها الجلسة التي اشتركت جمهورية كوريا في استضافتها مع الولايات المتحدة واليابان في أبريل/نيسان.

وقد أظهر الأمين العام أيضًا قيادة قوية، حيث دعا إلى اتخاذ تدابير للحد من المخاطر المتصلة بالفضاء الإلكتروني وإنشاء الهيئة الاستشارية الرفيعة المستوى المعنية بالذكاء الاصطناعي التي تشارك فيها كوريا. لكن التطورات التي حدثت منذ انعقاد الجلسة الأولى لمجلس الأمن قبل ثلاث سنوات تؤكد بشدة ضرورة أن يبادر المجلس، الآن أكثر من أي وقت مضى، بتكثيف جهوده في مواجهة التهديدات الناشئة عن الفضاء الإلكتروني. يشهد العالم – إضافة إلى عدد لا يحصى من الهجمات الإلكترونية عبر الحدود – اندلاع نزاعات مسلحة كبرى لم يقتصر شن الهجمات فيها على ساحة المعركة التقليدية فحسب، بل أصاب الفضاء الإلكتروني أيضًا.

ويشهد العالم أيضًا كيف تمكن الطفرات الهائلة في تكنولوجيا الذكاء الاصطناعي الجهات الخبيثة من تعزيز قدرتها لإثارة المزيد من الفوضى والإرباك في الفضاء الإلكتروني. لقد أدرك العالم أن الأنشطة الإلكترونية الخبيثة قادرة على إحداث تداعيات واقعية من

خلال تقويض الثقة في نزاهة الانتخابات السياسية وأمن البنية التحتية الحيوية ونسيج السلام والأمن. وفي واقع الأمر، بلغ الأمر بإحدى الدول الأعضاء حد الإعلان عن حالة الطوارئ بعد تعرضها لهجمات برمجيات انتزاع الفدية قادمة من بلد آخر.

إن الوسائل الإلكترونية بطابعها مزدوجة الاستخدام في الأساس: حيث يستطيع أي شخص لديه نوايا خبيثة استحداث تهديدات جديدة أو إثارتها ويفاقم من التهديدات القائمة أو يسرع من وتيرتها. وكما أشار ذات مرة آلفين توفلر، عالم شهير في مجال دراسات المستقبل: "إن قوانا التكنولوجية تتزايد، ولكن التأثيرات الجانبية الضارة واحتمالات الخطر تتصاعد".

تدرك جمهورية كوريا جيدًا التهديدات التي تشكلها الأنشطة الإلكترونية الخبيثة وتأثيرها على الأمن، نظراً لأن تطوير أسلحة الدمار الشامل التي تهدد كوريا يمول إلى حد كبير من هذه الأنشطة. ويشير أحدث تقرير لفريق الخبراء التابع للجنة المنشأة عملا بالقرار 1718 (2006) (S/2024/215) إلى أن 40 في المائة من برامج أسلحة الدمار الشامل لجمهورية كوريا الشعبية الديمقراطية تموَّل بوسائل إلكترونية غير مشروعة. كان الفريق يحقق في حوالي 60 هجومًا إلكترونيًا يُشتبه أن تكون جمهورية كوريا الشعبية الديمقراطية قد شنّته على شركات مرتبطة بالعملات المشفَّرة بين عامي 2017 و 2023. وللأسف، لم يعد للفريق الآن وجود لأسباب واضحة نعرفها جميعاً.

من خلال الوسائل الرقمية، تتهرب جمهورية كوريا الشعبية الديمقراطية بشكل منهجي من الجزاءات ذاتها التي اعتمدها المجلس وتتحدى النظام الدولي لعدم الانتشار الذي هو جزء لا يتجزأ من أعمال المجلس. مع ازدياد الترابط بين السلام والأمن في العالم المادي والرقمي، ينبغي لمجلس الأمن ألا يتجنب مواجهة الحقيقة ويدفن رأسه في الرمال. فعلى أقل تقدير، يجب أن يواكب المجلس الاتجاهات خارج المجلس ويعزز مشاركته في الاستجابة للتهديدات الحقيقية والراهنة من الفضاء الإلكتروني. كما يتعاون مجلس الأمن والجمعية العامة في تآزر عندما يتعلق الأمر بالمناقشات بشأن الأسلحة الصغيرة والإرهاب وعدم الانتشار، يمكن لمجلس الأمن والجمعية العامة بالمثل أن يتعاونا في الاضطلاع بأدوار تكميلية في مجال الأمن الإلكتروني.

وفي حين أنه لا يوجد حتى الآن أي نهج موثوق به للمضي قدما، تود جمهورية كوريا أن تطرح الاقتراحات الثلاثة التالية لينظر فيها مجلس الأمن.

أولاً، يحتاج المجلس إلى تشخيص واضح للوضع الحالي. ولتحقيق هذه الغاية، يمكن لمجلس الأمن أن يطلب تقريراً يقدم على أساس منتظم للنظر في كيفية تقاطع التهديدات الإلكترونية مع ولاية المجلس وكيفية تأثير التهديدات الإلكترونية المتطورة على السلم والأمن الدوليين.

ثانيًا، يجب أن تشمل الطريقة التالية المجموعة الكاملة من الملفات المدرجة على جدول أعمال المجلس. يمكن تعميم الأمن الإلكتروني في جدول أعمال المجلس على غرار المسائل الشاملة الأخرى، مثل الخطة المتعلقة بالمرأة والسلام والأمن، وكذلك الخطة المتعلقة بالشباب والخطة المتعلقة بتغير المناخ. وكما أشار العديد من الدول الأعضاء في اجتماع صيغة آريا في نيسان/أبريل، هناك صلة مباشرة بين الاستخدام الخبيث لتكنولوجيا المعلومات والاتصالات ومختلف المسائل التي تدخل في اختصاص مجلس الأمن، بما في ذلك الجزاءات وعدم الانتشار والإرهاب. وفي هذا السياق، يمكن للمجلس أن يعتبر الأمن الإلكتروني عنصراً رئيسياً يتقاطع مع ملفاته أو قضاياه الإقليمية والمواضيعية.

ثالثًا، في الأجلين المتوسط والطويل، يجب أن يتمكن مجلس الأمن من التوصل إلى علاج مناسب للتحدي. ويمكن للمجلس عقد جلسات بشأن الأنشطة الإلكترونية الخبيثة التي تنتهك القانون الدولي وتضر بالسلم والأمن الدوليين. علاوة على ذلك، يمكن للمجلس أن يحث جميع الجهات الفاعلة ذات الصلة على استخدام تكنولوجيا الفضاء الإلكتروني بطريقة مسؤولة ومتابعة المساءلة من خلال الأدوات المتاحة للمجلس. وغني عن القول أنه ينبغي لمجلس الأمن وضع برنامج عمل بشأن الأمن الإلكتروني بطريقة تكمل المناقشات الجارية في الجمعية العامة.

ولمجلس الأمن باع طويل في وضع جدول أعماله بما يتماشى مع ظهور تحديات أمنية جديدة. لم يتصور واضعو ميثاق الأمم المتحدة أن يصبح تغير المناخ وانتهاكات حقوق الإنسان والجائحة من المسائل التي تقع ضمن اختصاص مجلس الأمن. ويجب على مجلس الأمن أن يتصدى للأمن الإلكتروني بشكل مباشر إذا ما أراد أن يظل مجديا وأن يتحلى بالحصافة في التصدي لأحد أكثر التحديات الأمنية إلحاحًا في عصرنا. وآمل مخلصًا أن ينجم عن المناقشة المفتوحة المعقودة اليوم زخما لتحقيق ذلك.

قبل أن أختتم بياني، أود أن أضيف نقطة أخيرة. إن طابع الفضاء الإلكتروني الذي لا حدود له يعرض جميع الدول – سواء كانت متطورة رقميا أو هشة إلكترونيًا – لأضرار الأنشطة الإلكترونية الخبيثة. ولا يمكن أن يصبح الأمن الدولي في الفضاء الإلكتروني قويا إلا بقدر قوة أضعف حلقاته. وبالتالي، فإن الترابط بين العمل الإنساني والتنمية والسلام ليس أقل واقعية في عالم الإنترنت. إن وجود فضاء إلكتروني خالٍ من الأنشطة الإلكترونية الضارة سيسهل التطور الرقمي ويطلق العنان للفرص الرقمية التي تساهم في نهاية المطاف في تحقيق أهداف التنمية المستدامة. كما أن وجود فضاء إلكتروني مفتوح وآمن يسهل الوصول إليه وسلمي يمكن من خلاله ردع التهديدات الإلكترونية بشكل فعال سيحمي الحرية وحقوق الإنسان على الإنترنت.

أستأنف مهامي بصفتي رئيسا للمجلس.

أعطي الكلمة الآن لسعادة السيدة ليندا توماس – غرينفيلد، الممثلة الدائمة للولايات المتحدة وإحدى الأعضاء في إدارة الرئيس بايدن.

السيدة توماس – غرينفيلد (الولايات المتحدة الأمريكية) (*تكلمت بالإنكليزية*): أود أن أبدأ بشكر جمهورية كوريا على جمعنا مرة أخرى لمناقشة هذه المسألة البالغة الأهمية المتعلقة بالسلام والأمن. وأود أن أرحب بكم هنا في مجلس الأمن، سيدي الرئيس، وأن أعرب لكم عن تقديري الكبير. لقد تشرفت بلقائكم في سيول خلال زيارتي لها قبل بضعة أشهر، وإنه لأمر رائع أن تحضروا هنا. وأشكر الأمين العام ومقدمي الإحاطات على إحاطاتهم وأرحب بالوزراء الآخرين الذين شرفونا بحضورهم اليوم.

منذ جلستنا السابقة في نيسان/أبريل، لا نزال نرى أنه من الضروري تعزيز الأمن الفضاء الإلكتروني، وبالتالي مناقشة هذه المسألة في المجلس. فالأمن السيبراني يمكن أنظمتنا الأساسية من أداء مهامها – اقتصاداتنا ومؤسساتنا الديمقراطية، بل الأمم المتحدة نفسها. وتلتزم الولايات المتحدة بالعمل مع جميع الجهات الفاعلة المسؤولة لحماية فوائد الفضاء الإلكتروني وبناء التضامن في مجال التكنولوجيا الرقمية والاستفادة من التكنولوجيا لتحقيق أهداف التنمية المستدامة. غير أن الكثير من الجهات الفاعلة من الدول وغير الدول قد اتخذت المسار المعاكس. واستغلت التوصيلية الرقمية في جميع أنحاء العالم لابتزاز الضحايا من أجل الربح، وسرقة الأموال والأفكار من الحكومات والكيانات الخاصة، واستهداف الصحفيين والمدافعين عن حقوق الإنسان، والاستعداد المسبق لما قد ينشب من نزاعات في المستقبل وتهديد بنيتنا التحتية الحيوية، بما في ذلك هنا في الأمم المتحدة.

ويجب علينا كمجلس أن نعمل معاً للتصدي للتهديدات السيبرانية التي تشكلها الجهات الفاعلة من غير الدول والتابعة لها، وتعزيز معايير السلوك المسؤول للدول، ومساءلة الدول عن السلوك غير المسؤول في الفضاء الإلكتروني ودعم الضحايا المتضررين من هذا السلوك، وتعطيل شبكات المجرمين الذين يقفون وراء الهجمات الإلكترونية الخطيرة في جميع أنحاء العالم. ويوجد بالفعل إطار عمل للقيام بذلك. ويوضح إطار سلوك الدول المسؤول في الفضاء الإلكتروني، الذي اعتُمد مراراً وبتوافق الآراء، أن القانون الدولي ينطبق على الفضاء الإلكتروني، وأنه يُتوقع من الدول أن تتمسك بالمعايير الطوعية لسلوك الدول في وقت السلم. ومن بين هذه المعايير توقع أن تقوم الدول بالتحقيق في الأنشطة السيبرانية الخبيثة المنطلقة من أراضيها وتستهدف البنية التحتية الحيوية لدولة أخرى، والتخفيف من آثارها. ولكن من أيدوا هذا الإطار اختاروا تجاهل – أو الأسوأ من ذلك، تمكين – الجهات الفاعلة الشريرة.

لقد سُلط الضوء على ذلك في الاجتماع الذي عقد بصيغة آريا في نيسان/أبريل بشأن الأمن السيبراني، الذي يشمل العمليات السيبرانية الخبيثة التي تقوم بها جمهورية كوريا الشعبية الديمقراطية

والتي تستخدمها لتمويل برامجها لأسلحة الدمار الشامل والقذائف التسيارية. ويشمل ذلك النشاط السيبراني الروسي في أوكرانيا وألمانيا وتشيكيا وليتوانيا وبولندا وسلوفاكيا والسويد، حيث استهدفت مديرية الاستخبارات الرئيسية التابعة للأركان العامة الروسية، من بين أنشطة أخرى، الأحزاب السياسية والمؤسسات الديمقراطية. وليس ذلك فحسب، بل كانت الحكومة الروسية أيضا بمثابة ملاذ آمن للجهات الفاعلة في مجال برمجيات انتزاع الفدية، التي سببت في السنوات الأخيرة خسائر تقدر ببلايين الدولارات وألحقت أضرارا كبيرة بالمستشفيات وغيرها من مرافق البنية التحتية الحيوية.

من جانبنا،أعلنت الولايات المتحدة والمملكة المتحدة، في شباط/فبراير الماضي، عن عمليات لتعطيل مجموعة برمجيات انتزاع الفدية LockBit، التي استهدفت 2 000 ضحية وطالبت بفدية قدرها مئات الملايين من الدولارات، دُفع منها أكثر من 120 مليون دولار. وكشفنا في الأشهر الأخيرة عن لائحة التهم الموجهة إلى المواطنين الروسيين أرتور سونغاتوف وإيفان كوندراتييف، المعروف أيضا باسم باسترلورد، بنشر برمجية LockBit ضد العديد من الضحايا في جميع أنحاء الولايات المتحدة وعلى الصعيد الدولي. ويأتي ذلك إضافة إلى الجهود المبذولة في إطار المبادرة الدولية لمكافحة برمجيات انتزاع الفدية، التي اتخذناها في عام 2021، وهي الآن أكبر شراكة إلكترونية في العالم. ونحن، فرادى الدول، وعن طريق هذه الشراكة وفي المحافل المتعددة الأطراف، بما في ذلك الأمم المتحدة، ندعو جميع الدول إلى القيام بدورها في تنفيذ الإطار وتعزيز السلام والاستقرار في الفضاء الإلكتروني. وندعو المجلس إلى ضمان أن يكون الأمن السيبراني أولوية شاملة تراعى في كل جانب من جوانب ولايتنا. وسواء كان الأمر يتعلق بالنظر في كيفية تعزيز عمليات حفظ السلام للنظافة الإلكترونية الجيدة بغية الحد من المخاطر أو تحسين فهم الكيفية التي يمكن بها أن يعزز الأمن السيبراني جهود عدم الانتشار، يجب على المجلس أن يواصل النظر إلى التحديات من منظور الأمن السيبراني.

إن بمقدورنا حماية بنيتنا التحتية البالغة الأهمية وجميع من يعتمدون عليها. وب إمكاننا حماية فوائد الفضاء الإلكتروني للجميع. إ فلنؤكد ذاً من جديد انطباق القانون الدولي على السلوك فيما بين الدول، مسترشدين بإطار سلوك الدول المسؤول في الفضاء الإلكتروني. ولنعزز الالتزام بالمعايير الطوعية لسلوك الدول المسؤول في وقت السلم ونساعد على الحد من مخاطر النزاعات الناشئة عن حوادث الفضاء الإلكتروني. ولنتمسك بالنظام الدولي القائم على القواعد ولنكفل أن يؤثر العالم الرقمي على العالم المادي للأفضل.

أشكركم مرة أخرى، السيد الرئيس، على جمعنا بشأن هذا الموضوع.

السيد بيرسود (غيانا) (*تكلم بالإنكليزية*): أشكر معالي السيد تشو تاي يول، وزير الخارجية، ورئاسة جمهورية كوريا على تنظيم المناقشة المفتوحة اليوم بشأن التصدي للتهديدات المتطورة في الفضاء الإلكتروني. وأشكر أيضا الأمين العام ومقدمي الإحاطات على إسهاماتهم الثاقبة في المناقشة.

لقد أوجدت التطورات التكنولوجية السريعة عالما ينطوي على إمكانات غير محدودة، بفوائد اقتصادية واجتماعية وجيوسياسية كبيرة. إلا أن التكنولوجيات الرقمية، نظرا لازدياد تطورها واستخدامها من جانب جهات فاعلة خبيثة، تشكل مخاطر غير مسبوقة تهدد الأمن البشري والأمن القومي على حد سواء. كما أثبت الاستخدام الخبيث للتكنولوجيات الرقمية إمكانية تعطيل المؤسسات والتسبب في تحديات تنظيمية وسياسية تتعلق بالحوكمة. وعلاوة على ذلك، فإن الطبيعة العابرة للحدود الوطنية للتهديدات السيبرانية جعلت مفهومي الأمن الوطني والدفاع التقليديين متقادمين.

ويمكن أن يكون لتهديدات الأمن السيبراني التي نتعرض لها الآن تأثير خطير على صحة مواطنينا وسلامتهم وأمنهم وسير الخدمات الأساسية. وبينما يزداد تطور التهديدات المعاصرة للأمن السيبراني وتعدد أوجهها، التي تشمل التجسس الإلكتروني الذي ترعاه الدول، والتدخل في العمليات الديمقراطية، وانتهاكات حقوق الإنسان، والهجمات على البنية التحتية الحيوية، ونشر المعلومات المغلوطة والمعلومات المضللة وخطاب الكراهية، يجب أن تتطور استجابتنا تطورا.

وفي هذا الصدد، أقترح النظر في ثلاثة مجالات.

أولاً، يجب أن تكون هناك آليات للمساءلة والرقابة للحماية من الهجمات الإلكترونية. وفي هذا الصدد، نشير إلى المناقشات الأخيرة بشأن ما إذا كانت الهجمات الإلكترونية التي تستهدف البنية التحتية الحيوية، مثل المرافق الطبية أو محطات توليد الطاقة، والتي تترتب عنها عواقب وخيمة على حياة الناس، ترقى إلى جرائم حرب و/أو جرائم ضد الإنسانية و/أو إبادة جماعية و/أو جريمة عدوان. ويجب دراسة ذلك الأمر بدقة وإدراجه في إطار قانوني عالمي يجب أن يكفل أيضا تطوير الأدوات والتكنولوجيات الرقمية واستخدامها مع المراعاة الواجبة للاعتبارات الأخلاقية واحترام حقوق الإنسان. وفي هذا الصدد، تدرك غيانا أهمية اختتام أعمال اللجنة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، والحاجة إلى اتفاقية يتم التصديق عليها على نطاق واسع.

ثانياً، يجب أن نعطي الأولوية للتعاون والتآزر والشراكات لبناء القدرات والمرونة في مجال الأمن السيبراني والتحقيق في الجرائم الإلكترونية ومقاضاة مرتكبيها في جميع البلدان والمناطق. وفيما يتعلق بالشراكات، يجب أن نستثمر في بناء الثقة وتحسين التعاون الإقليمي والدولي لتعزيز تبادل المعارف والمعلومات ونقل التكنولوجيا. ويجب أن نسعى أيضا إلى تطوير قابلية التشغيل البيني بين نُظمنا الوطنية والإقليمية والدولية التي تعالج تعقب تهديدات الأمن السيبراني ورصدها. ولتحقيق الفعالية، يجب وضع إطار عمل عالمي يسمح للدول وأصحاب المصلحة المعنيين بتبادل المعلومات الاستخباراتية عن التهديدات الحديثة التي تواجه الأمن السيبراني. ولئن كانت المناقشات الجارية داخل الأمم المتحدة والآليات الإقليمية تسهم على نحو إيجابي في هذا المسعى، بما في ذلك في إطار خارطة الطريق من أجل التعاون الرقمي وخطة تسريع التحول الرقمي لأهداف التنمية المستدامة، فإن هناك الكثير من العمل الذي ينبغي إنجازه. ويجب أن نستفيد أيضا من الفرص المتاحة في المجال السيبراني لاتباع نهج يشمل المجتمع بأسره لمواجهة التهديدات السيبرانية وتعزيز الأمن السيبراني.

ويمكن أن تساعد التكنولوجيات الجديدة مثل أنظمة الذكاء الاصطناعي في تحديد هذه التهديدات والتخفيف من حدتها. وفي هذا الصدد، يجب أن تضاعف الحكومات جهودها للتعاون مع شركات التكنولوجيا والقطاع الخاص لإعداد أدوات وسياسات أمنية أقوى ولتعزيز تبادل المعلومات في تحليل المعلومات الاستخباراتية المتعلقة بالتهديدات. وعلاوة على ذلك، تفتقر العديد من البلدان النامية مثل غيانا إلى الموارد والخبرات اللازمة لمكافحة التهديدات السيبرانية وبناء القدرة على الصمود. ويجب أن يُعتبر بناء القدرات التقنية في تلك البلدان استثمارا في أمننا الجماعي من شأنه أن يعمل على إزالة أوجه عدم المساواة والاختلالات القائمة في قدرات الأمن السيبراني. وبالنظر إلى ذلك، يمكننا بوصفنا مجتمعا عالميا أن نستكشف إمكانية إنشاء صندوق عالمي موجه للتدريب وبناء القدرات، فضلاً عن تطوير البرمجيات والأجهزة. وعلاوة على ذلك، تدعو غيانا البلدان المتقدمة النمو التي تملك قدرات تكنولوجية متطورة إلى تقديم المساعدة التقنية والتمويل لتعزيز البنية التحتية للأمن السيبراني وقدرات الاستجابة في البلدان النامية. وينبغي عدم ادخار أي جهد لضمان عدم احتكار أي بلد أو كيان للأدوات والقدرات التكنولوجية، مما قد يزيد من تفاقم مواطن الضعف في البلدان النامية، من خلال مثلا فرض قوانين وأنظمة يتجاوز أثرها الحدود الإقليمية.

ثالثًا، يجب أن يشارك مجلس الأمن في الحوار المتعلق بالأمن السيبراني بغض النظر عن العمليات الجارية في محافل الأمم المتحدة الأخرى، نظراً للتهديد الذي يشكله النشاط السيبراني الخبيث في صون السلام والأمن الدوليين. لذلك، يجب أن يكثف المجلس مناقشته لهذه المسألة من خلال الاستفادة من الاجتماعات المعقودة بصيغة آريا والمناقشات المفتوحة، بما في ذلك النقاش الحالي، لزيادة الوعي بالتهديدات الناشئة التي تشكلها التكنولوجيات الجديدة والاستكشاف الجماعي للتدابير الفعالة التي يمكن نشرها ضد الاستخدام الضار لهذه التكنولوجيات.

في الختام، تشكل تهديدات الأمن السيبراني تحديات هائلة ولكنها لا تستعصي على الحل. ويمكننا بناء عالم رقمي قادر على الصمود وآمن يعزز الثقة والابتكار والازدهار للجميع من خلال جهودنا وإرادتنا الجماعية وعملنا المتضافر. فلنغتنم الفرصة، ليس لمجرد التصدي

للتهديدات الماثلة أمامنا، بل لنشكل على نحو فاعل مستقبلًا لا يُترك فيه أحد خلف الركب. وتقف غيانا على أهبة الاستعداد للعمل مع جميع الدول الأعضاء لتحقيق هذا المسعى.

السيد نبينزيا (الاتحاد الروسي) (*تكلم بالروسية*): يسرنا أن نراكم، سيدي الرئيس، تترأسون مجلس الأمن. ونشكر الأمين العام على إحاطته. كما استمعنا باهتمام لمقدمي الإحاطات.

كانت روسيا حاضرة في بداية المناقشات حول مسائل أمن المعلومات على الصعيد الدولي في الأمم المتحدة. وفي عام 1998، أي قبل 26 عامًا، طرحنا الموضوع لأول مرة في الجمعية العامة من خلال تقديم أول قرار (قرار الجمعية العامة 70/53) بشأن هذا الموضوع بالتحديد. وقد أصبح اتخاذ القرارات المتعلقة بهذا الموضوع منذئذ حدثاً سنوياً تؤيده الأغلبية الساحقة من الدول الأعضاء.

وبمبادرة منا، أُنشئ فريق الخبراء الحكوميين التابع للأمم المتحدة لمناقشة المسائل الأمنية في استخدام تكنولوجيا المعلومات والاتصالات. وتطور في وقت لاحق إلى صيغة شاملة ليصبح الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات واستخدامها، وهو منبر فريد وموحد للتفاوض تحت رعاية الأمم المتحدة لمناقشة جميع المسائل المتعلقة بأمن المعلومات على الصعيد الدولي.

وأثبت الفريق العامل المفتوح العضوية طوال فترة عمله فعاليته وأهميته. وترتبت عنه نتائج عملية منها إطلاق دليل لجهات الاتصال في مايو/أيار – بمبادرة من روسيا – من أجل تبادل المعلومات حول الهجمات أو الحوادث الحاسوبية. ويجري حالياً استعراض تفصيلي للتهديدات القائمة والمحتملة في مجال أمن المعلومات على الصعيد الدولي. وتُتخذ خطوات ملموسة لبناء القدرات الرقمية للدول. وفي العام الماضي، جرى الاتفاق على مبادئ عالمية للمساعدة في هذا المجال.

ونعتقد أن جهود المجتمع الدولي ينبغي أن تتركز على مواصلة تعزيز التعاون بين الدول في إطار الفريق العامل المفتوح العضوية من أجل تحقيق نتائج ملموسة وعملية لضمان أمن المعلومات على الصعيد الدولي. ونعتقد أنه من الأهمية بمكان تعزيز النتائج التي حققها الفريق العامل المفتوح العضوية والاستفادة منها، سواء في إطار ولايته الحالية أو في إطار صيغة تفاوضية مقبلة. وقدمت روسيا بالفعل رؤيتها لآلية دائمة شاملة في هذا المجال. ونرى أن الحكمة تقتضي الحفاظ على مكاسبنا المشتركة من خلال إنشاء فريق عامل دائم مفتوح العضوية له صلاحية صنع القرار بعد عام 2025.

وتُظهر الحقائق المذكورة أعلاه بوضوح أن الأمم المتحدة تملك سجلا طويلا من العمل المتسق والتدريجي في مجال أمن المعلومات على الصعيد الدولي. ولذلك، فإن الحاجة إلى إشراك مجلس الأمن تثير تساؤلات جدية. فلهذا الموضوع خصوصياته وينبغي مناقشته في المحافل المتخصصة التي تتوفر فيها الخبرات المناسبة. ومن الأهمية بمكان أن تظل المناقشات مهنية وبناءة مع تجنب التسييس. ويؤدي تكرار الجهود التي يبذلها المجتمع الدولي ونشر الموضوع في مختلف محافل الأمم المتحدة إلى نتائج عكسية وقد يضيع كل النتائج التي تحققت على مدى عقود تحت رعاية الجمعية العامة.

ومما يكتسي القدر نفسه من الأهمية أن تكون مناقشات الفريق العامل المفتوح العضوية شاملة. ويمكن أن يشارك جميع أعضاء الأمم المتحدة دون استثناء وعلى قدم المساواة بما أن القرارات تُتخذ بتوافق الآراء. وقد تُستبعد تلقائياً جميع الدول غير الأعضاء في المجلس من عملية صنع القرار عند إحالة الموضوع إلى مجلس الأمن. وينبغي لأولئك الذين أيدوا اليوم دعوة الرئاسة لإدراج أمن المعلومات على الصعيد الدولي في جدول أعمال مجلس الأمن أن يضعوا ذلك في الاعتبار.

أخيراً، يجب أن تراعي أية مناقشة للمخاطر المحتملة الخصائص التكنولوجية للفضاء السيبراني. وعلى عكس العالم المادي، من الصعب للغاية تحديد التهديدات في الفضاء السيبراني ومن الأصعب تحديد مصدر الهجوم أو ما يسمى بالإسناد. وغالباً ما يستغرق إدراك وقوع الهجوم وقتاً طويلاً من خلال الأدلة الظرفية. ولذلك، لم نتوصل بعد حتى إلى فهم أولي لحالات الاستخدام الخبيث لتكنولوجيا المعلومات والاتصالات التي يمكن اعتبارها بكل ثقة تهديدات مباشرة للسلام

والأمن الدوليين. وفي غياب حل لمشكلة الإسناد ونهج موحد للجوانب المعقدة الأخرى لتلك المشكلة المتعددة الأوجه والمحددة، بما في ذلك الجوانب القانونية، فإن أي مناقشة في مجلس الأمن يمكن أن تتحول إلى تبادل آخر للادعاءات الواهية وتُعمّق الانقسام في المجتمع الدولي. وهو ما قد يقوض سلطة المجلس ولن يساعد بأي حال من الأحوال على وضع حلول بناءة.

إن جميع الدول التي تكلمت أو التي ستتكلم اليوم مشاركةٌ في الفريق العامل المفتوح العضوية، والمسائل المقترحة للمناقشة مماثلة لتلك المسائل التي ناقشها الفريق. وعُقدت مائدة مستديرة على المستوى الوزاري بشأن بناء القدرات في مجال أمن المعلومات على الصعيد الدولي في شهر أيار/مايو وستُعقد الدورة الثامنة للفريق العامل المفتوح العضوية في شهر تموز/يوليه. والواقع أن النقاش حول هذا الموضوع قد بدأ بالفعل، ويمكن للجميع الاطلاع على تطوراته ونتائجه.

وعليه، فإننا لا نؤيد الدعوة إلى زيادة وعي المجتمع الدولي بالمسائل المتعلقة بأمن المعلومات على الصعيد الدولي من خلال عقد جلسات منتظمة لمجلس الأمن. وتتوخى ولاية مجلس الأمن الاستجابة السريعة للأخطار التي تهدد السلام والأمن الدوليين، بدلاً من تبادل فلسفي للآراء حول مواضيع مشتركة في المجال العام. فهناك محافل وصيغ أخرى لذلك.

ومما يثير بالغ القلق أيضا محاولات الزملاء الغربيين إثارة مزاعم حول أنشطة خبيثة باستخدام تكنولوجيا المعلومات والاتصالات ومن ثم استخدامها كوسيلة ضغط على الدول "غير المرغوب فيها". والأنكى من ذلك أنهم لا يقدمون أي دليل مقنع يدعم كلامهم.

وقد استُخدم فريق الخبراء المعني بجمهورية كوريا الشعبية الديمقراطية التابع للجنة مجلس الأمن المنشأة عملا بالقرار 1718 (2006) مرارا وتكرارا أداةً في تلك اللعبة التي تنم عن انعدام الضمير. وبناءً على معلومة صادرة عن دولة محددة من الدول الأعضاء، تواصل الفريق مع الجانب الروسي بشأن هجمات حاسوبية منسوبة إلى بيونغ يانغ. وعندما طلبنا الحصول على البيانات الدقيقة اللازمة للتحقيق في الحوادث المزعومة، أجابنا الخبراء بأنهم لم يتلقوا أي معلومات إضافية من "مصادرهم". ولكن عدم التوفر على أي تفاصيل لا يمنع زملاءنا الغربيين من اتهام البلدان التي لا توافق على أفعالهم بارتكاب كل "الذنوب السيبرانية" دون أساس. وعادة ما توصف هذه الاتهامات بأنها "مرجحة جدا"، وهو التعبير المفضل للبلدان الغربية. وهذه الادعاءات التي لا أساس لها من الصحة غير مقبولة. ويتطلب إسناد المسؤولية اتباع نهج احترافي وأدلة فنية شاملة.

ونرفض رفضًا قاطعًا أي تكهنات تزعم أن روسيا تشجع الأعمال الخبيثة على الإنترنت. وما فتئنا ندعو منذ ربع قرن إلى منع عسكرة الفضاء الإلكتروني وبدأنا في اقتراح خطوات ملموسة في هذا المجال قبل وقت طويل من اعتراف البلدان الغربية بوجود هذا الخطر.

إن أولوية بلدنا هي وضع صكوك عالمية ملزمة قانونًا بشأن الأمن السيبراني، مما سيساهم في منع النزاعات بين الدول في هذا المجال. وتحقيقًا لهذه الغاية، قدمت روسيا إلى الجمعية العامة في عام 2023 نموذجًا أوليًا لمعاهدة دولية متخصصة. لقد كان تصورا لاتفاقية للأمم المتحدة معنية بضمان أمن المعلومات على الصعيد الدولي. ولن يتيح اعتماد هذا الاتفاق العالمي إمكانية تحديد حقوق البلدان والتزاماتها المتعلقة بأنشطتها في مجال تكنولوجيا المعلومات والاتصالات بشكل قانوني فحسب، بل سينظم أيضاً مسألة الإسناد السياسي للهجمات الحاسوبية في العلاقات الدولية. وقد يساعد أيضًا على ضمان الامتثال الكامل لمبدأ المساواة في السيادة بين الدول في الفضاء الرقمي الذي تتجاهله علنًا في الوقت الحاضر العديد من البلدان المتقدمة تكنولوجيًا. وندعو جميع الدول الأعضاء إلى الانخراط في مناقشة موضوعية انطلاقا من اقتراحنا في الجمعية العامة.

وترفض البلدان الغربية للأسف، وعلى رأسها الولايات المتحدة، هذه الفكرة لأنها تحاول الحفاظ لنفسها على أكبر قدر ممكن من حرية التصرف. ويصبح ذلك واضحًا بوجه خاص في ضوء اعتراف مسؤولين أمريكيين رفيعي المستوى بتنفيذ هجمات خبيثة ضد روسيا باستخدام تكنولوجيا المعلومات والاتصالات. ويتجلى ذلك أيضًا في ما تنص عليه عقيدتا واشنطن وحلف الناتو من نُهج "هجومية" أو عدوانية في الواقع.

وتحدث مقدمو الإحاطات اليوم والوفود التي أخذت الكلمة في وقت سابق عن الهجمات السيبرانية. ولكنهم نسوا أن يذكروا أن هناك حرب معلومات مضللة غير مسبوقة تُشن ضد روسيا. وتنسق كل ذلك النشاط الخبيث منظمات توجد مقراتها في لندن من بريطانيا العظمى، وهي "جمعية العلاقات العامة والاتصالات" و "شبكة العلاقات العامة"، بالإضافة إلى "جيش تكنولوجيا المعلومات الأوكراني" الذي يعمل بلا كلل في مجال التضليل الإعلامي. وتُنشر أطنان من المعلومات المضللة والأكاذيب عن روسيا والعملية العسكرية الروسية الخاصة من خلال جهود هذه الموارد المعلوماتية.

ويساورنا القلق أيضا إزاء محاولات تمييع النقاش العالمي حول مكافحة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية. ومن الأمثلة الواضحة على ذلك "مبادرة مكافحة برمجيات انتزاع الفدية". وتقوض هذه "الأندية الحصرية"، التي لا تخفي بوجه خاص أهدافها المسيّسة، جهود الدول الأعضاء الرامية إلى وضع آليات عالمية لمكافحة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية، ولا سيما من خلال لجنة الأمم المتحدة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية.

ويعمل الاتحاد الروسي منذ أكثر من 26 عامًا على تعزيز جدول أعمال بنّاء في مجال أمن المعلومات على الصعيد الدولي ويقدم مساهمته الخاصة في الحفاظ على السلام والاستقرار في العالم الحقيقي والافتراضي على السواء. وسنواصل الدعوة إلى تهيئة بيئة سلمية وآمنة لتكنولوجيا المعلومات والاتصالات على نطاق عالمي.

الرئيس (*تكلم بالإنكليزية*): أود تذكير جميع المتكلمين بألا تزيد مدة بياناتهم على ثلاث دقائق حتى يتسنى للمجلس إنجاز عمله بسرعة. الأضواء الوامضة المثبتة على أطواق الميكروفونات ستنبه المتكلمين إلى إنهاء ملاحظاتهم بعد ثلاث دقائق.

السيد أفونسو (موزامبيق) (*تكلم بالإنكليزية*): تود موزامبيق أن تعرب عن امتنانها لكم، سيدي الرئيس، ولجمهورية كوريا، على الاختيار المناسب لهذا الموضوع الهام بوصفه الحدث المميز لرئاستها لمجلس الأمن لشهر حزيران/يونيه. ونعرب عن امتناننا العميق للأمين العام على نهجه الثاقب للغاية في تناول هذا الموضوع، وهو نهج يتماشى على نحو جيد ومناسب مع ميثاق الأمم المتحدة. لقد تابعنا باهتمام كبير الآراء المهمة التي قدمها السيد ستيفان دوجين، رئيس معهد السلام السيبراني، والبروفيسورة نينا إفاني أجوفو، أستاذة القانون والتكنولوجيا.

ونرحب بالوزراء والشخصيات الرفيعة المستوى الحاضرين في القاعة اليوم.

تشهد جميع البيانات التي أُدلي بها حتى الآن على أن الحدود الفاصلة بين الفضاء السيبراني والعالم المادي تستمر في التلاشي بسرعة. ونتيجة لذلك، انتقلت تقريبا جميع جوانب حياتنا المعاصرة إلى التكنولوجيا الرقمية التي تعتمد عليها. لذلك، فإن ما يدعم ضرورة مشاركة المجلس هو أن العديد من البلدان، كبيرة كانت أم صغيرة، تنظر بجدية إلى الفضاء السيبراني الذي لا حدود له على أنه مجال نزاع محتمل، إلى جانب المجال البري والبحري والجوي والفضاء.

وفي الواقع، يمكننا أن نعتبر أن نقطة الانطلاق حُددت في عام 2013 حينما وافقت الجمعية العامة على أن القانون الدولي، بما في ذلك ميثاق الأمم المتحدة، ينطبق على الفضاء السيبراني. ولكن الحوار الدبلوماسي العالمي المتعلق بقواعد الاشتباك في الفضاء السيبراني شهد حتى الآن تقدما بطيئا. وفي هذا الصدد، لم تسفر بعدُ المناقشات التي جرت تحت رعاية الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات واستخدامها عن أي نتائج.

ويتطور مشهد التهديدات السيبرانية ونطاقها بسرعة، مع التقدم السريع للذكاء الاصطناعي والتهديدات الكبيرة التي تشكل تحديات جديدة للسلام والأمن والاستقرار على الصعيدين الوطني والدولي. ومع ازدياد التهديدات السيبرانية، لا يكاد يمر يوم دون الإبلاغ عن هجوم ببرمجيات انتزاع الفدية ضد كيانات عامة أو خاصة أو انتشار التزييف العميق القائم على الذكاء الاصطناعي الذي يبدو حقيقيا للغاية أو

محاولة منع الخدمة عن أجزاء أو خدمات بلد ما الأساسية كالقطاع المالي والرعاية الصحية وشبكات الكهرباء والحوكمة الإلكترونية وغيرها من الهياكل الأساسية الحيوية. وبما أن الأدوات المعدة لجعل الحياة العصرية ممكنة يُساء استعمالها وتُوظَّف سلاحا، برزت الجريمة السيبرانية لتكون أحد أهم العوامل المضاعفة للخطر بتقويضها ثقة الجمهور في المؤسسات وزيادتها التوترات السياسية والاجتماعية.

ومما يزيد من هذه التحديات، اشتداد المنافسة الجيوسياسية التي أصبحت قوة دافعة في مجال الأمن السيبراني. ويسعى الخصوم جاهدين للحصول على القدرات السيبرانية العسكرية والاستخباراتية، مما يؤدي إلى سباق تسلح إلكتروني وسط تزايد تبادل الاتهام والانتقام والتصعيد. وبما أن تشابك الأمن السيبراني مع الجغرافيا السياسية آخذ في التزايد، لا تزال آفاق التقدم نحو اتفاق دولي بشأن معايير أفضل للأمن السيبراني تتعثر، بل تتراجع. وهذا الجمود أو عدم إحراز التقدم بشأن مسألة في غاية الأهمية للبشرية قد يقوض أمننا الجماعي.

ونظراً لسرعة تطور واقع التهديدات وعدم وجود قواعد متفق عليها للتصدي لها، ينبغي لمجلس الأمن أن يتفق على القيام، على سبيل الاستعجال، بعدة أدوار وإجراءات محددة من بينها ما يلي.

أولاً، ينبغي أن يضع معايير وأطر عمل دولية للسلوك المسؤول للدول والكيانات الخاصة في الفضاء الإلكتروني، على أساس التعاون العالمي.

ثانياً، انطلاقاً من روح تعزيز أمننا الجماعي، يمكن للمجلس أن يدعم مبادرات بناء القدرات لتعزيز قدرات الدول الأعضاء في مجال الدفاع السيبراني، لا سيما الدول ذات الموارد المحدودة.

ثالثاً، يمكن للمجلس أن يشجع على تقديم إحاطات للتوعية بالحالة وتسهيل تبادل المعلومات الاستخباراتية المتعلقة بالتهديدات وأفضل الممارسات بين الدول لتحسين قدرتنا المشتركة على الصمود في مواجهة تهديدات الأمن السيبراني.

رابعاً، يجب أن ترتبط التهديدات السيبرانية ارتباطاً جوهرياً ببنود أخرى على جدول أعمال مجلس الأمن، مثل مكافحة الإرهاب، والتدخل في الانتخابات، وحماية البنية التحتية الحيوية، والحفاظ على عمليات السلام والعمل الإنساني.

ونعتقد أن من الضروري استكمال النقاش بشأن الأمن السيبراني وتوسيع نطاقه. فالمسائل المتعلقة بسرقة الأفكار والبيانات والملكية الفكرية وحقوق الإنسان والخصوصية، وكذلك معايير تصميم السلع الاستهلاكية الحيوية والمرافق العامة، تستحق نفس القدر من الاهتمام. ومن الضروري، بالنسبة لبلدان مثل موزامبيق، أن تُسمع أصوات بلدان الجنوب ووجهات نظرها في النقاش العالمي حول الأمن السيبراني. ومن الأهمية بمكان وجود مجموعة متنوعة من الآراء على الطاولة وتجنب اتباع نهج واحد إزاء جميع الحالات لإحراز التقدم العالمي نحو إطار حوكمة أكثر عدلاً وقدرة على الصمود. وبتشجيع مناقشات مثل المناقشة التي نجريها الآن تحت رئاسة جمهورية كوريا، يمكن للمجلس أن يؤدي دوراً محورياً في صون السلام والأمن الدوليين في العصر الرقمي. وتلتزم موزامبيق بمواصلة المشاركة في هذا العمل.

السيد كانو (سيراليون) (*تكلم بالإنكليزية*): أشكركم، سيدي الرئيس، على عقد هذه المناقشة المفتوحة المهمة. وأشكر معالي السيد أنطونيو غوتيريش، الأمين العام للأمم المتحدة، على إحاطته الثاقبة. كما نشكر السيد ستيفان دوغين والسيدة نينا إيفياني – أجوفو على أفكارهما. ونرحب بمشاركة الوزراء الرفيعي المستوى في هذه الجلسة.

تعرب سيراليون عن تقديرها للفرصة التي أتيحت لها للتكلم عن المسألة البالغة الأهمية، وهي التصدي للتهديدات المتطورة في الفضاء الإلكتروني، مع الاعتراف بالفوائد الهائلة والتحديات المترابطة التي تمثلها تكنولوجيا المعلومات والاتصالات بالنسبة للسلام والأمن الدوليين. وندرك أيضا التحدي الإنمائي الأساسي المتمثل في معالجة الفجوة الرقمية العالمية وخطر تعميق هذه الفجوة بفعل انتشار الذكاء الاصطناعي، وخاصة الذكاء الاصطناعي التوليدي.

ستتكلم سيراليون في هذا البيان عن الأسئلة الإرشادية على وجه التحديد. فالاتجاهات الرئيسية الناشئة والمتطورة للأنشطة الخبيثة في الفضاء الإلكتروني التي تشكل تحديات للسلام والأمن الدوليين تشمل انتشار البرمجيات الخبيثة، وبرمجيات انتزاع الفدية ونماذج برمجيات

انتزاع الفدية كخدمة، وعمليات السطو على العملات المشفَّرة. وتشكل هذه الأنشطة خطراً كبيراً على السكان المدنيين ولها آثار مدمرة على الأمن القومي والاستقرار العام في بلداننا، مما يشكل مخاطر كبيرة تهدد السلام الدولي.

ويساورنا قلق بالغ إزاء تطور الأساليب المستخدمة في الفضاء الإلكتروني، التي لا تغذي الأنشطة الإرهابية فحسب، بل تعرض للخطر سلامة النظم المالية والخدمات الحيوية. ونشدد على أن الاستخدام المتزايد لنماذج برمجيات انتزاع الفدية كخدمة وسرقة العملات المشفَّرة لدعم الأنشطة الشائنة يسلط الضوء على الحاجة الملحة إلى تعزيز التعاون وبناء القدرات لمكافحة هذه التهديدات بفعالية. والتصعيد الأخير في وتيرة ونطاق هجمات برمجيات انتزاع الفدية التي تستهدف البنية التحتية الحيوية والخدمات العامة الأساسية يدل على التأثير الشديد للتهديدات السيبرانية على السلامة العامة والاستقرار السياسي ويتطلب توخي اليقظة باستمرار. وتشعر سيراليون بقلق بالغ إزاء الآثار المترتبة عن التهديدات السيبرانية، بما في ذلك استخدام الجرائم السيبرانية لتمويل الأنشطة غير المشروعة والتهرب من الجزاءات الدولية. وهذه العناصر كلها تؤكد على الحاجة الملحة إلى تعزيز التعاون الدولي وجهود بناء القدرات لمكافحة هذه التهديدات بفعالية. وندعو إلى زيادة التعاون بين الدول الأعضاء لتعزيز قدرة مجلس الأمن على التصدي بفعالية للأنشطة الخبيثة في الفضاء الإلكتروني، لا سيما الأنشطة التي تهدد البنية التحتية الحيوية والعمليات الإنسانية وحماية المدنيين. ومن الضروري اتباع نهج كلي لصون السلام والأمن في العصر الرقمي.

ونرى صادقين أن استخدام تكنولوجيا المعلومات والاتصالات في الأنشطة الخبيثة عامل مضاعف للخطر عندما يؤدي إلى تفاقم النزاعات والتحديات القائمة. والانتشار المتزايد للأنشطة السيبرانية الخبيثة التي تستهدف البنية التحتية الحيوية، بما في ذلك المستشفيات وغيرها من نظم الرعاية الصحية، والخدمات المالية، وقطاع الطاقة، والسواتل، والنقل وغير ذلك من أنظمة الطوارئ، يؤكد الحاجة الملحة إلى اتخاذ إجراءات متضافرة على صعيد العالم لحماية شبكاتنا وأنظمتنا الرقمية وأهمية مشاركة مجلس الأمن في معالجة هذه المسائل وإدارة النزاعات التي تنطوي على عناصر سيبرانية وتسويتها.

وكما سمعنا، يمكن استخدام الذكاء الاصطناعي، رغم فوائده الهائلة، كسلاح لزيادة حجم الهجمات الإلكترونية وسرعتها وتعقيدها. فبإمكان المنظومات الذاتية التشغيل شن هجمات مستمرة وقابلة للتكييف، والتعلم من بيئتها لاستغلال مواطن الضعف بفعالية أكبر. ويمكن أن تستهدف هذه الهجمات التي تعتمد على الذكاء الاصطناعي البنية التحتية الحيوية والنظم المالية وحتى خصوصية الأفراد، مما يؤدي إلى أوجه التعطيل والإضرار على نطاق واسع. بيد أننا ندرك أيضاً أن الاستفادة من الذكاء الاصطناعي في مجال الدفاع السيبراني يمكن أن تساعدنا على استباق التهديدات الناشئة. ف بالذكاء الاصطناعي يمكن الاستعانة به لتحسين رصد التهديدات وزمن الاستجابة وإدارة الحوادث. وبالاستثمار في التكنولوجيات الدفاعية القائمة على الذكاء الاصطناعي، يمكننا بناء بنية تحتية إلكترونية أقدر على الصمود. وبالاستثمار في بناء القدرات ونقل التكنولوجيا، يمكننا أن نعزز مستوى قدرات الدول النامية. وترى سيراليون أن مجلس الأمن يمكن أن يضطلع بدور محوري في التصدي للطبيعة المتطورة للتهديدات السيبرانية وتعزيز السلم والأمن الدوليين من خلال المشاركة الشاملة مع لجان الجمعية العامة والوكالات والهيئات المتخصصة ذات الصلة.

على مدى العقد الماضي، أصبح مجلس الأمن يبقي قيد نظره على نحو متزايد آثار الفضاء السيبراني على السلام والأمن الدوليين. منذ عام 2016، عقد أعضاء المجلس العديد من الاجتماعات بصيغة آريا تناولت الدول خلالها الأمن السيبراني، مع الصلات المختلفة بمواضيع مثل حماية البنية التحتية الحيوية، وحماية المدنيين والمعلومات المضللة وخطاب الكراهية في الفضاء السيبراني.

لذلك، تثني سيراليون على إستونيا لعقدها أول مناقشة مفتوحة رفيعة المستوى حول هذا الموضوع خلال فترة رئاستها في حزيران/يونيه 2021. وفي ضوء تركيز مجلس الأمن المتزايد على الأمن السيبراني، فإننا نؤيد اقتراح عقد جلسات إحاطة منتظمة لتقييم مشهد التهديدات السيبرانية المتغير، مع دمج رؤى مختلف أصحاب المصلحة من أجل ضمان فهم شامل للتحديات الناشئة واستباقها. ونؤكد على ضرورة

التنسيق والتعاون والمشاركة بشكل فعال من قبل المجلس إذا أردنا مكافحة التهديدات السيبرانية بشكل شامل.

ونشدد على أن مشاركة مجلس الأمن يمكن أن تتم بطريقة مكملة لعمليات الأمم المتحدة الأخرى الجارية بشأن تكنولوجيا المعلومات والاتصالات، بما في ذلك المناقشات ذات الصلة بشأن معايير سلوك الدول المسؤول في استخدام تكنولوجيا المعلومات والاتصالات وإطار الأمم المتحدة لسلوك الدول المسؤول في استخدام تكنولوجيا المعلومات والاتصالات، الذي اعتمد بتوافق الآراء، تحت رعاية الجمعية العامة.

ومن شأن وضع تقييمات واستراتيجيات حول مشهد التهديدات السيبرانية المتغير من خلال دمج رؤى شاملة من منظومة الأمم المتحدة والقطاع الخاص والمجتمع المدني والأوساط الأكاديمية أن يضمن بقاء مجلس الأمن على اطلاع دائم بالتطورات الجديدة وآثارها على السلم والأمن الدوليين.

وإدراكا للروابط بين التهديدات السيبرانية والبنود الأخرى المدرجة على جدول أعمال مجلس الأمن، ينبغي للدول الأعضاء أن تستكشف سبل تعميم الشواغل المتعلقة بالفضاء الإلكتروني وتكنولوجيا المعلومات والاتصالات بفعالية في مجموعة الأعمال الحالية للمجلس. وتقترح سيراليون تعميم الشواغل المتعلقة بالفضاء الإلكتروني في مناقشات المجلس بشأن مختلف الملفات المواضيعية، بما في ذلك بعثات حفظ السلام، والجزاءات التي يفرضها المجلس وجهود عدم الانتشار ومكافحة الإرهاب.

إن تعزيز القدرات الوطنية في مجال الأمن السيبراني وتعزيز التعاون الدولي هما عنصران حيويان في هذا النهج، ويمكن أيضاً إدماجهما في كل مسار من مسارات هذه الجهود. ومن خلال دمج الاعتبارات المتعلقة بالمواضيع المتصلة بالفضاء الإلكتروني في عمله، يمكن للمجلس أن يتصدى بشكل أفضل للتحديات المعقدة التي تشكلها التهديدات السيبرانية بطريقة شاملة وكلية.

ومن جانبنا، أدى إنشاء المركز الوطني لتنسيق الاستجابة لحوادث أمن الحاسوب في سيراليون إلى إضفاء الطابع المركزي على ولاية التصدي لجميع قضايا الأمن السيبراني، بما في ذلك الاستجابة لحوادث الأمن السيبراني في سيراليون.

وقد حقق المركز منذ إنشائه إنجازات كبيرة في قدرة الأمن السيبراني في البلد على الصمود من خلال نهج متعدد الأوجه لبناء القدرات والتعاون. وتشمل الأنشطة الهامة مبادرات بناء القدرات التي تركز على الأمن السيبراني والجريمة الإلكترونية. وقد اضطلع المركز بدور محوري في رفع مستوى الوعي وتوفير برامج تدريبية لمختلف أصحاب المصلحة، والتعاون مع الشركاء الإقليميين وشركاء التنمية لإجراء تدريبات متخصصة للسلطة القضائية ووكالات إنفاذ القانون بشأن الجرائم الإلكترونية والأدلة الإلكترونية، ونقل المعرفة وتبادل أفضل الممارسات في مجال الأمن السيبراني والتحقيقات في الجرائم الإلكترونية. يعزز هذا التعاون القدرة الجماعية على مكافحة التهديدات السيبرانية على صعيد العالم بفعالية من خلال تعزيز القدرات الوطنية.

أولاً – وللأسف – أود أن أختتم بالإشارة إلى التهديدات السيبرانية الصفيقة المتزايدة الموجهة إلى مؤسساتنا المتعددة الأطراف والدولية والقضائية. وفي هذا الصدد، تدين سيراليون بشكل قاطع الهجمات الموجهة ضد المحكمة الجنائية الدولية. ووصفت المحكمة أحد هذه الهجمات بأنه "هجوم محدد الأهداف ومعقد بهدف التجسس، وبالتالي يمكن تفسيره على أنه محاولة خطيرة لتقويض ولاية المحكمة". وتؤكد سيراليون مجدداً، بصفتها دولة طرفاً، التزامها بدعم المبادئ والقيم المكرسة في نظام روما الأساسي والدفاع عنها والحفاظ على سلامتها من أي تدخل وضغط ضد المحكمة ومسؤوليها والمتعاونين معها.

ثانيا، أود أن أؤكد من جديد التزام سيراليون بتعزيز الأمن السيبراني باعتباره جانبا أساسيا من جوانب السلم والأمن الدوليين والعمل بشكل تعاوني داخل مجلس الأمن والمجتمع الدولي الأوسع نطاقا للتصدي للتهديدات المعقدة والمتغيرة في الفضاء السيبراني التي تشكلها الأنشطة الخبيثة.

السيد بن جامع (الجزائر) (*تكلم بالإنكليزية*): أشكركم، سيدي الرئيس، على تنظيم هذه المناقشة المفتوحة المهمة حول المخاطر

المتزايدة للتهديدات السيبرانية على الأمن العالمي. كما أشكر الأمين العام ومقدمي الإحاطتين على عروضهم بشأن الزيادة المقلقة في الأنشطة السيبرانية الضارة.

تُعرِّض هجمات برمجيات انتزاع الفدية الخبيثة على البنية التحتية الحيوية وسرقة الأصول والبيانات الرقمية السلامة العامة والاستقرار السياسي للخطر. إن مشاركة الجهات الفاعلة الحكومية وغير الحكومية على حد سواء تجعل الوضع أكثر تعقيدًا وخطورة. إن انتشار المعلومات المضللة على منصات الإنترنت يؤجج الانقسام والكراهية والتعصب، وفي نهاية المطاف الإرهاب، حيث تتدخل المعلومات الكاذبة في شؤون الدول، مما يعرقل التعاون، وفي نهاية المطاف، يهدد السلام والأمن في العالم.

إن التكنولوجيات الجديدة، بما في ذلك الذكاء الاصطناعي، تجعل التهديدات السيبرانية أسوأ وتزيد صعوبة التعامل معها. لذلك نحن بحاجة إلى التصدي لهذه التحديات على الصعيد العالمي وبشكل عاجل. وبالنظر إلى هذه الحقائق، أريد أن أؤكد على عدة نقاط رئيسية.

أولاً، يجب أن تنطبق مبادئ ميثاق الأمم المتحدة بالمثل على الفضاء الإلكتروني. ويجب استخدام تكنولوجيا المعلومات والاتصالات وفقاً لتلك المبادئ.

ثانياً، نحن نسعى جاهدين لضمان وجود فضاء إلكتروني مفتوح وآمن، وهو أمر ضروري لتحقيق الأهداف الإنمائية العالمية لخطة التنمية المستدامة لعام 2030. ولهذا السبب، نحن بحاجة إلى إطار عمل ملزم قانونًا يتم إنشاؤه في الأمم المتحدة.

ثالثاً، يجب علينا مساعدة البلدان النامية على بناء قدرات وقائية ضد التهديدات السيبرانية وسد الفجوة الرقمية. إن بناء قدراتها أمر ضروري لتأمين الفضاء السيبراني لجميع الدول، وينبغي أن يكون أولوية قصوى.

رابعًا، يجب على المجتمع الدولي العمل معًا لمكافحة انتشار المعلومات الكاذبة على الإنترنت. الحكومات أطراف معنية، وعلى الأطراف المعنية أن تتعاون وفقاً للقانون الدولي. التعاون الدولي أمر أساسي في سعينا لمكافحة التهديدات السيبرانية المتغيرة باستمرار بفعالية.

خامساً، نحن بحاجة إلى تعزيز الإطار القانوني لمنع الجرائم الإلكترونية والمعاقبة عليها. وفي هذا الصدد، أود أن أسلط الضوء على أن بلدي يضطلع بدور نشط في الجهود الدولية لمكافحة الاستخدام الضار للتكنولوجيا في الأنشطة الإجرامية. ويتجلى ذلك بشكل خاص في قيادة الجزائر للجنة الأمم المتحدة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية. ونأمل أن تحقق تلك اللجنة نتائج ناجحة في دورتها القادمة هذا الصيف.

وفي الختام، تدعم الجزائر بقوة دور الأمم المتحدة في التعامل مع المسائل المتعلقة باستخدام تكنولوجيا المعلومات والاتصالات التي تؤثر على السلم والأمن الدوليين. إن الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات واستخدامها والجمعية العامة منبران أساسيان للمناقشة الشاملة للتهديدات السيبرانية. وهما يضمنان مشاركة جميع الأعضاء في تشكيل الاستجابة العالمية لتحديات الأمن السيبراني، ونؤكد التزامنا بدعم عملهما القيّم.

السيد زبوغار (سلوفينيا) (*تكلم بالإنكليزية*): أتقدم بالشكر لجمهورية كوريا على تنظيم مناقشة اليوم. وأشكر الأمين العام على إحاطته، كما أشكر مقدمي إحاطاتينا اليوم على أفكارهما وتوصياتهما.

أود أن أتناول نقطتين وثيقتي الصلة بموضوع مناقشة اليوم.

أولاً، فيما يتعلق بالتهديدات المتطورة في الفضاء السيبراني، نرى أن الفهم الدقيق لمشهد التهديدات السيبرانية المتطور باستمرار، لا سيما في سياق النمو السريع للتكنولوجيات الناشئة، مثل الذكاء الاصطناعي، أمر بالغ الأهمية لمناقشة التدابير التعاونية التي يمكن للمجتمع الدولي اتخاذها رداً على الأنشطة السيبرانية الضارة. وفي ذلك الصدد، نثني على العمل الجاري الذي يقوم به الفريق العامل المخصص المفتوح باب العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات واستخدامها الذي أنشأته الجمعية العامة، ولكننا ندرك كذلك الإمكانية التكميلية لتعزيز نظر المجلس في هذا الموضوع، على سبيل المثال من خلال تناول النتائج التي توصل إليها تقرير الأمين العام عن التهديدات السيبرانية (A/77/92). ويمكن للأنشطة السيبرانية

الخبيثة – مثل هجمات الفدية والهجمات التي تستهدف البنية التحتية المدنية الحيوية، لا سيما عندما تكون عابرة للحدود بطبيعتها – أن تشكل تحديات جديدة وتفاقم التهديدات القائمة للسلم والأمن الدوليين.

وذلك يقودني إلى نقطتي الثانية، وهي التصدي للتهديدات المتطورة في الفضاء الإلكتروني. تقع على المجلس المسؤولية الرئيسية عن صون السلم والأمن الدوليين. وينبغي للمجلس أن يقوم بدور حاسم، من أجل الاضطلاع بمسؤوليته وفقاً لولايته، في تهدئة التوترات وتعزيز المساءلة عندما تهدد الأنشطة السيبرانية الخبيثة السلم والأمن الدوليين. ومن وجهة نظرنا، فإن الأنشطة التي تدعم الإرهاب أو انتشار أسلحة الدمار الشامل أو التي تؤدي إلى تفاقم النزاعات القائمة أو تستهدف البنية التحتية المدنية الحيوية تشكل ذلك التهديد، وبالتالي تستدعي رد المجلس. وعلى نفس المنوال، ينبغي للمجلس أن يتصدى للأنشطة السيبرانية الخبيثة، مثل حملات التضليل الإعلامي، التي تحرض على العنف ضد السكان المدنيين أو تتسبب في معاناة إنسانية أو تعطل عمل المنظمات الإنسانية وعمليات حفظ السلام وبناء السلام.

في عصر يتسم بتنامي رقمنة النزاعات، من الأهمية بمكان التأكيد على انطباق القانون الدولي، بما في ذلك القانون الدولي الإنساني والقانون الدولي لحقوق الإنسان، الذي يجب احترامه.

وأود أن أختتم كلمتي بالتأكيد للمجلس على التزامنا بالتعاون مع أعضاء المجلس وأعضاء الأمم المتحدة على نطاق أوسع في مواصلة المناقشات بشأن التهديدات السيبرانية للسلم والأمن الدوليين. كما إننا لا نزال ثابتين في التزامنا بتنفيذ التدابير الرامية إلى التخفيف من تلك المخاطر، بما في ذلك تنفيذ المعايير الحالية لسلوك الدولة المسؤول في الفضاء الإلكتروني.

السيدة فرايزر (مالطة) (*تكلمت بالإنكليزية*): أبدأ بشكر جمهورية كوريا على تنظيم هذه المناقشة المفتوحة بشأن هذه المسألة البالغة الأهمية والموضوعية. كما أشكر الأمين العام ومقدمي الإحاطتين على ملاحظاتهم المتبصرة.

تمثل الأنشطة السيبرانية الخبيثة تحديات متعددة الأوجه يمكن أن تكون لها آثار خطيرة على صون السلم والأمن الدوليين. وتتراوح تلك الهجمات بين هجمات الفدية الخبيثة على المؤسسات الحكومية والبنية التحتية الحيوية والخدمات العامة الأساسية إلى الوصول غير المصرح به إلى البيانات المخزنة إلكترونيًا واستخدامها.

إننا نشعر بالقلق إزاء الأنشطة السيبرانية الخبيثة التي تستهدف المؤسسات الحكومية والعمليات الديمقراطية، وغالباً ما يكون الهدف المباشر منها تقويض الاستقرار والأمن وتقويض الثقة في نتائج الانتخابات الديمقراطية. إن الاعتماد المتزايد على التقنيات الرقمية من قبل المدافعات عن حقوق الإنسان والناشطات الأخريات يزيد من خطر تعرضهن للمضايقات والاعتداءات عبر الإنترنت. وعلاوة على ذلك، تُقَيَّد حقوق الإنسان والحريات الأساسية، بما في ذلك حرية التعبير والتجمع، بشكل متزايد من خلال المراقبة الصارمة وإغلاق الإنترنت واختناق عرض النطاق الترددي. وفي نفس الوقت، غالبًا ما تُستغل المنصات الرقمية لنشر المعلومات المضللة والمغلوطة وخطاب الكراهية، بما في ذلك المحتوى الكاره للنساء والمثليين والزارع لنزعة التطرف.

ويجب أن تكون جهودنا الجماعية لتعزيز الاستقرار في هذا المجال متجذرة في حقوق الإنسان، سواء على الإنترنت أو خارجه. ويجب أن تكون السياسات السيبرانية مراعية للنزاعات ومراعية للعمر ومراعية للنوع الاجتماعي من أجل اكتشاف ومنع الآثار الضارة لتهديدات الأمن الرقمي، مثل العنف الجنساني الذي تيسره التكنولوجيا. إن قيادة المرأة ومشاركتها مشاركة كاملة وعلى قدم المساواة والآمنة والهادفة في صنع القرار السيبراني أمر بالغ الأهمية، خاصة في سياقات النزاع وما بعد النزاع.

ونؤكد من جديد أن القانون الدولي، ولا سيما ميثاق الأمم المتحدة، ينطبق على الأنشطة في الفضاء الإلكتروني، كما أقرت الجمعية العامة. وفي السياق نفسه، يوفر إطار سلوك الدولة المسؤول في الفضاء الإلكتروني مبادئ توجيهية متفق عليها للدول الأعضاء. وينبغي أن تتمسك جميع الدول الأعضاء بهذا الإطار، ونحن نؤيد وضع برنامج عمل لضمان استمرار الحوار وإضفاء الطابع المؤسسي عليه. وبالإضافة إلى ذلك، ندعو جميع الدول إلى توخي الحرص

واتخاذ التدابير المناسبة بما يتماشى مع معايير إطار السلوك المسؤول للدول في الفضاء الإلكتروني، والامتناع عن المشاركة في الأنشطة السيبرانية الخبيثة التي تنطلق من أراضيها أو المساعدة عليها.

وتستغل الجهات السيبرانية الخبيثة التي ترعاها الدول برامج الفدية والسرقة الرقمية لتوليد إيرادات غير مشروعة. وتشمل تلك هجمات على البنية التحتية الحيوية والمؤسسات المالية وشركات العملات الرقمية. والهجمات والجرائم الإلكترونية لا تعرف الحدود، ولا توجد دولة محصنة ضدها. وتُقدِّر التقارير أن الأنشطة السيبرانية الخبيثة التي ارتكبها قراصنة برعاية جمهورية كوريا الشعبية الديمقراطية في عام 2023 وحده، قد حققت ما يعادل بليون دولار. ويستخدم النظام تلك العائدات لتمويل برنامجه غير القانوني لأسلحة الدمار الشامل، الذي يهدد السلام والأمن في شبه الجزيرة وخارجها. وقد تم توثيق تلك الأنشطة توثيقا جيدا في تقارير فريق الخبراء التابع للجنة المنشأة عملا بالقرار 1718 (2006)، الذي يقوم بدور قيم في التحقيق في تلك الجرائم.

وفي الختام، يمكن لمجلس الأمن أن يضطلع بدور مهم في معالجة مسألة الأمن السيبراني. ويمكن لجهوده أن تكون مكملة لجهود المنتديات الأخرى المعنية بالأمن السيبراني القائمة في الجمعية العامة، بما في ذلك فريقه العامل المفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات واستخدامها. ويمكن للمجلس أن يكون بمثابة منصة قوية لتعزيز المبادئ المتفق عليها وتعزيز المزيد من المناقشات. وينبغي له أن يروّج لفضاء إلكتروني مفتوح وآمن وسهل الوصول إليه وسلمي. وسنواصل دعم انخراطه المتجدد بشأن ذلك الموضوع.

السيد يامازاكي (اليابان) (*تكلم بالإنكليزية*): أعرب عن خالص امتناني لكم، سيدي الرئيس، على دوركم القيادي في عقد هذه المناقشة المفتوحة الهامة والمناسبة التوقيت، وللأمين العام ومقدمي الإحاطات على أفكارهم القيمة.

في البداية، تود اليابان أن تعرب عن التزامها بتعزيز فضاء سيبراني حر وعادل وآمن. لقد شهدنا في السنوات الأخيرة اتجاهاً خطيرا يتمثل في الزيادة النوعية والكمية في العمليات السيبرانية المستخدمة لأغراض خبيثة، بما في ذلك هجمات برمجيات انتزاع الفدية، والإضرار بالبنية التحتية الحيوية، والتدخل في الانتخابات الديمقراطية، وسرقة البيانات الحساسة. كما يشكل الارتفاع المثير للقلق في سرقة العملات الرقمية تهديدًا واضحًا وقائمًا للسلام والأمن الدوليين، إذ من المحتمل استخدام ذلك في تمويل برامج الأسلحة غير المشروعة. وعلى وجه الخصوص، من المعروف جيدا أن كوريا الشمالية تمول برامجها لأسلحة الدمار الشامل والقذائف التسيارية من خلال عمليات سيبرانية خبيثة، ويجب على المجتمع الدولي أن يتصدى على وجه السرعة لهذه التهديدات، كما أفاد بذلك فريق الخبراء التابع للجنة المنشأة عملا بالقرار 1718 (2006). وعلاوة على ذلك، فإن انتشار أدوات الاختراق السيبراني التجارية، مثل برامج التجسس الحاسوبي، يثير مخاوف عميقة بشأن تأثيرها على الأمن القومي وحقوق الإنسان والسلام والأمن الدوليين. ولم تكن المخاطر أعلى مما هي عليه الآن.

ولمواجهة هذه التحديات المثيرة للقلق وضمان وجود فضاء سيبراني حر وعادل وآمن، ينبغي علينا دعم سيادة القانون في الفضاء السيبراني من خلال المضي قدماً في مناقشات ملموسة حول تطبيق القانون الدولي القائم وتنفيذ المعايير والقواعد والمبادئ المتفق عليها لسلوك الدول المسؤول. كما يجب أن نولي أهمية كبيرة لتبادل المعلومات حول التهديدات المحتملة القائمة، وتبادل أفضل الممارسات وتعزيز جهود بناء القدرات. ويجب أن نهدف من خلال الحوارات على جميع المستويات إلى تعزيز الثقة والحد من التهديدات، والأهم من ذلك الحد من سوء التقدير. وفي إطار الأمم المتحدة، ستواصل اليابان مشاركتها البناءة في الفريق العامل الحالي المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها. وتعتقد اليابان أيضا أن برنامج العمل للنهوض بسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي، باعتباره إطارا عملي المنحى، ينبغي أن يكون بمثابة منبر دائم في المستقبل لدعم تنفيذ المعايير والقواعد والمبادئ المتفق عليها لسلوك الدول المسؤول.

وفي الوقت نفسه، توافق اليابان تماما على أن مجلس الأمن، الذي يتحمل المسؤولية الرئيسية عن صون السلام والأمن، يجب أن يكون له دور مكمل أكبر في مجال الأمن السيبراني. ويجب على المجلس أن

يراقب عن كثب الحوادث السيبرانية الخطيرة ذات العواقب الوخيمة على السلام والأمن الدوليين، بما في ذلك تلك التي تستهدف البنية التحتية الحيوية. وستكون جلسات الإحاطة المنتظمة التي يعقدها المجلس مفيدة للغاية لتتبع مشهد التهديدات الآخذة في التطور في مجال أمن تكنولوجيا المعلومات والاتصالات. وبالإضافة إلى ذلك، يجب أن يتصدى المجلس للتهديدات السيبرانية المتزايدة التي يتعرض لها النظام العالمي للحد من الأسلحة وعدم الانتشار، بما في ذلك مخاطر الانتشار التي يحتمل أن تشكلها الجهات الفاعلة من غير الدول.

وفي الختام، تؤكد اليابان من جديد التزامها الثابت بحماية الفضاء السيبراني الحر والعادل والآمن. ويجب أن يظل مجلس الأمن في حالة تأهب قصوى فيما يتعلق بالمخاطر الأمنية الناشئة المرتبطة بتكنولوجيا المعلومات والاتصالات. ونتطلع إلى مزيد من المناقشات حول الخطوات التالية للمجلس لمعالجة هذا الموضوع الهام بفعالية استناداً إلى مناقشة اليوم التي جرت بمبادرة منكم، سيدي الرئيس.

السيدة باربارا وودوارد (المملكة المتحدة) (*تكلمت بالإنكليزية*): أشكر السيد تشو تاي يول، وزير خارجية جمهورية كوريا، على عقد هذه المناقشة وعلى عرضه على مجلس الأمن بعض الأفكار الواضحة بشأن كيفية المضي قدما بعملنا في هذا المجال. كما أشكر الأمين العام ومقدمي الإحاطات لنا اليوم على توضيحهم لكيفية تأثير التهديدات السيبرانية على السلام والأمن الدوليين.

سأتطرق إلى ثلاثة اتجاهات تعتبرها المملكة المتحدة اتجاهات مهمة.

أولاً، كما سمعنا، يمكن لبرمجيات انتزاع الفدية أن تشل وظائف الحكومة والخدمات العامة الحيوية. ويوجد ذلك ظروفًا لعدم الاستقرار عندما يحدث على نطاق واسع أو لفترات طويلة، مما قد يؤثر على السلام والأمن، كما يعلم المجلس. ويمكن لأي دولة أن تكون ضحية لبرمجيات انتزاع الفدية. ولهذا السبب هناك حاجة إلى استجابة دولية لتضييق الخناق على المنظومة التي تسهل ذلك، ولتمكين جميع الدول من زيادة قدراتها على الصمود والاستجابة. وتؤدي المملكة المتحدة دوراً رائدًا إلى جانب سنغافورة كرئيسين مشاركين لركيزة السياسات الخاصة بمبادرة مكافحة برمجيات انتزاع الفدية. ونحث الآخرين على الانضمام إلى المبادرة.

ثانياً، بتزايد استخدام أنظمة الذكاء الاصطناعي في مجتمعاتنا، نحتاج إلى فهم الكيفية التي ستتغير بها التهديدات السيبرانية، مع تحديد الفرص المتاحة لاستخدام الذكاء الاصطناعي في دعم أهدافنا في مجال الأمن السيبراني. ويمكن للجهات الفاعلة الخبيثة وغير المسؤولة استغلال نقاط الضعف في أنظمة الذكاء الاصطناعي للحث على سلوك معين أو التلاعب في عملية اتخاذ القرار. ومن أجل الحفاظ على السلام الدولي، يجب أن تكون أنظمة الذكاء الاصطناعي آمنة من حيث التصميم. ولهذا السبب عقدت المملكة المتحدة أول مناقشة للمجلس بشأن الذكاء الاصطناعي في العام الماضي أثناء رئاستنا للمجلس (انظر S/PV.9381)، ولهذا السبب نشرنا مبادئ توجيهية لتطوير نظام آمن للذكاء الاصطناعي إلى جانب الولايات المتحدة ومجموعة أقاليمية تضم 18 دولة.

ثالثاً، إن الجهات الفاعلة الخبيثة وغير المسؤولة قادرة أيضاً على الاستفادة من السوق الآخذ في الاتساع لقدرات الاختراق السيبراني المتقدمة، مما يؤدي إلى مشهد خطير يصعب علينا جميعا التنبؤ بعواقبه. وتدعو المملكة المتحدة وفرنسا الشركاء الدوليين للانضمام إلينا في عملية بال مول المتعددة أصحاب المصلحة بينما ننظر في النهج المتبعة تجاه هذا الشاغل المشترك.

وفي هذا السياق، يجب أن نستمر في زيادة الوعي بالتهديدات السيبرانية. فعلى سبيل المثال، نشعر بقلق بالغ إزاء استخدام جمهورية كوريا الشعبية الديمقراطية للأنشطة السيبرانية الخبيثة للحصول على العملات الرقمية لتمويل برنامجها غير القانوني للأسلحة. ولهذا السبب يجب علينا مضاعفة جهودنا لضمان التنفيذ الفعال لنظام الجزاءات المفروضة على جمهورية كوريا الشعبية الديمقراطية.

وأخيراً، تزيد التهديدات السيبرانية أيضاً من مخاطر المعلومات المضللة. ومن الواضح أن هذا تحدٍ كبير لعملنا. ومن المدهش أن تتهم روسيا المملكة المتحدة بإدارة حرب بالمعلومات المضللة في حين أن آلة المعلومات المضللة لديها قد انكشفت بشكل واضح وجلي للغاية،

بما في ذلك هنا في الأمم المتحدة. فإننا لم نكن الوفد الذي جاء إلى هذه القاعة وإلى الإنترنت بمؤامرة استخدام الخفافيش والبط كأسلحة.

وستشكل التهديدات السيبرانية عدداً متزايداً من المخاطر التي تهدد السلام والأمن الدوليين، ويتعين على الحكومات أن تتطور من أجل التصدي لها بفعالية. وفي إطار ذلك، تظل المملكة المتحدة ملتزمة بدعم إطار عمل الأمم المتحدة لسلوك الدول المسؤول والعمل مع الآخرين من خلال بناء القدرات وتمكين الشراكات بين القطاعين العام والخاص.

السيدة شاندا (سويسرا) (*تكلمت بالفرنسية*): أشكر جمهورية كوريا على تنظيم هذه المناقشة الهامة بشأن التهديدات التي يتعرض لها الأمن السيبراني. كما أشكر الأمين العام للأمم المتحدة، والبروفيسور نينا إفاني – أجوفو والسيد ستيفان دوغين، الرئيس التنفيذي لمعهد السلام الإلكتروني في جنيف، على إحاطاتهم.

تشهد سويسرا تطورين حاسمين في الفضاء الإلكتروني يثيران قلقنا. فمن ناحية، تؤدي الرقمنة المتزايدة للنزاعات واستخدام العمليات السيبرانية في النزاعات المسلحة إلى تغيير طبيعة تلك النزاعات. ومن ناحية أخرى، فإن تزايد كثافة هجمات برمجيات انتزاع الفدية والهجمات السيبرانية التي ترعاها الدول ضد البنية التحتية الحيوية تشكل مصدر قلق كبير لسويسرا. إن استخدام برمجيات انتزاع الفدية لابتزاز العملات والعملات الرقمية أو استهداف البنية التحتية الحيوية قد يشل الهياكل الرئيسية في مجتمعاتنا. وتؤثر هذه الأنشطة أيضًا على قدرة المجتمع الدولي على تحقيق أهداف التنمية المستدامة، وذلك بسبب زيادة ضعف البلدان النامية. ويمكن أن تشكل هذه الأنشطة تهديداً للسلام والأمن الدوليين، وبالتالي فهي تقع ضمن ولاية المجلس.

وتتساءل المذكرة المفاهيمية التي اقترحتها جمهورية كوريا عن الدور الذي يمكن أن يؤديه المجلس في التصدي للتهديدات الناشئة عن الأنشطة الخبيثة في الفضاء السيبراني. وأود أن أوضح بعض الخيارات في هذا الصدد.

أولاً، يجب على المجلس أن يطلع بانتظام على التطورات والتهديدات الحالية للأمن السيبراني. ونظراً للآثار المتعددة الأبعاد والنطاق الجغرافي للمشكلة، سيكون من المناسب أن يعقد المجلس جلسة إحاطة منتظمة. ويمكن أن تشمل الإحاطة عروضاً يقدمها ممثلو كيانات الأمم المتحدة والقطاع الخاص والمجتمع المدني والأوساط الأكاديمية، فضلاً عن الكيانات المعنية الأخرى. فهذه التوعية ستمكّن المجلس من اتخاذ قرارات مستنيرة تماماً، لا سيما بشأن مسائل جغرافية محددة وفي سياق عمليات حفظ السلام.

ثانياً، ينبغي للمجلس إعادة التأكيد على بعض المبادئ الراسخة. إننا نولي أهمية خاصة لانطباق القانون الدولي على الفضاء السيبراني، ولا سيما انطباق القانون الدولي الإنساني على الأنشطة التي تجري في الفضاء السيبراني في سياق النزاع المسلح. كما ينبغي للمجلس أن يشدد على أهمية مسؤولية الدول وبذل العناية الواجبة والاعتراف بالمعايير الـ 11 لسلوك الدول المسؤول في الفضاء السيبراني. وتشكّل هذه العناصر، التي تكملها تدابير بناء الثقة وبناء القدرات، إطاراً لسلوك الدول المسؤول في استخدام تكنولوجيا المعلومات والاتصالات، وهو إطار اعتمدته جميع الدول الأعضاء بتوافق الآراء. وندعم قيام المجلس بإصدار ناتج يؤكد هذا الإطار وبالتالي يساهم في إعادة بناء الثقة.

وأخيراً، يجب أن تكون أنشطة المجلس مكملة لأنشطة الهيئات الأخرى. فليس من اختصاص المجلس وضع قواعد للسلوك أو الاتفاقات. وإنما هذا من اختصاص الجمعية العامة وعمليات الخبراء التي كلفتها الجمعية بذلك. وينبغي أن يركز المجلس اهتمامه على تطوير فهمه للمخاطر والتخفيف من حدتها، بما في ذلك في حالات محددة.

ويتيح الاستخدام المسؤول للفضاء السيبراني فرصاً هائلة لمواجهة تحديات الغد، على الرغم من المخاطر المعترف بها. ويشجعنا الأمين العام في خطته الجديدة للسلام على إيجاد طرق جديدة لحماية أنفسنا من هذه التهديدات الجديدة. وبينما توفر لنا المفاوضات المتعلقة بالميثاق من أجل المستقبل فرصة لتطوير تفاهم مشترك في هذا الصدد، فإن للمجلس أيضًا دوراً رئيسيًا يؤديه في هذا الصدد. وتؤكد مناقشة اليوم هذا الأمر.

السيد فو كونغ (الصين) (*تكلم بالصينية*): أشكركم، سيدي الرئيس، على ترؤسكم جلسة اليوم. وأشكر الأمين العام غوتيريش على الإحاطة وأشكر الخبيرين على العرضين اللذين قدماهما.

وفي الوقت الحاضر، نعيش عصرا رقميا غير مسبوق، إذ تتقدم ثورة تكنولوجيا المعلومات بشكل متسارع، وتزدهر الاقتصادات الرقمية والاقتصادات الإلكترونية، ويشهد المجتمع الدولي اندماجًا متسارعًا في مجتمع ذي مستقبل مشترك يتشاطر السراء والضراء. وفي الوقت نفسه، فإن المخاطر والتحديات في الفضاء السيبراني تزداد خطورة أكثر من أي وقت مضى. وتستمر الهجمات السيبرانية والتجسس السيبراني والجرائم السيبرانية وهجمات المعلومات المضللة بلا هوادة. وقد أصبح الإرهاب السيبراني خطراً عالمياً عاماً. والفضاء السيبراني آخذ على نحو متزايد في العسكرة والتخندق والانقياد بالأيديولوجيات، وتستمر الفجوة الرقمية بين البلدان والمناطق في الاتساع.

في الفضاء السيبراني تتمتع جميع البلدان بفرص مشتركة ومصالح مشتركة، إلا أنها تواجه أيضاً تحديات مشتركة وتتحمل مسؤوليات مشتركة. ويجب على المجتمع الدولي تعميق التبادلات وتعزيز الثقة المتبادلة والعمل معًا وبشكل مشترك على تعزيز الحوكمة ووضع القواعد الدولية بشأن الفضاء السيبراني. وتود الصين أن تقترح ما يلي:

أولاً، نحن بحاجة إلى بناء فضاء سيبراني أكثر سلاماً وأماناً. فالفضاء السيبراني يتكامل بعمق مع العالم المادي ويشكل ركيزة مهمة لتطور المجتمع البشري. ويجب ألا يصبح ساحة معركة جديدة. وهناك دولة معينة تصنف الفضاء السيبراني كمجال للعمليات العسكرية، وتطور قدرات عسكرية سيبرانية هجومية، وتبني تحالفات سيبرانية عسكرية، وتدفع باتجاه تعريف قواعد الاشتباك في الفضاء السيبراني. وهذا لن يؤدي إلا إلى تقويض الثقة المتبادلة بين الدول، وتصعيد مخاطر الاحتكاك والصراع في الفضاء السيبراني وتهديد السلام والأمن الدوليين. وينبغي على جميع الأطراف أن تتخلى عن لعبة المحصلة الصفرية وعقلية الحرب الباردة، وأن تعزز رؤية قائمة على الأمن المشترك والشامل والتعاوني والمستدام، وأن تتمسك بحزم بالطبيعة السلمية للفضاء السيبراني، وأن تمنع عسكرة الفضاء السيبراني وحدوث سباق تسلح فيه بشكل فعال، وأن تتصدي للتهديدات التي يتعرض لها الأمن السيبراني من خلال الحوار والتعاون، وأن يظل كل طرف ملتزما بتحقيق أمنه من خلال تحقيق الأمن المشترك.

ثانياً، نحن بحاجة إلى بناء فضاء سيبراني أكثر نفعاً وازدهاراً على الصعيد العالمي. فقد أصبحت الاقتصادات الرقمية والاقتصادات الإلكترونية بالفعل محركات رئيسية للنمو الاقتصادي العالمي. وينبغي لجميع البلدان اعتماد سياسات أكثر نشاطاً وانفتاحاً وتنسيقاً وشمولاً، وتعزيز تطبيق تكنولوجيا المعلومات والاتصالات وتعميمها للجمهور، وضمان انفتاح واستقرار وأمن السلسلة الصناعية لتكنولوجيا المعلومات والاتصالات حتى يتسنى لعدد أكبر من البلدان والشعوب التمتع بمزايا الإنترنت. وينبغي للبلدان المتقدمة النمو مساعدة البلدان النامية على تعزيز التنمية الرقمية والذكية والقائمة على الإنترنت وتعزيز قدرة البلدان النامية على الوقاية من المخاطر والاستجابة لحالات الطوارئ، وضمان الوصول العادل إلى الموارد الرئيسية مثل تكنولوجيات البنية التحتية السيبرانية والقدرة الحاسوبية من أجل تقليص الفجوة الرقمية وتنفيذ أهداف التنمية المستدامة لخطة التنمية المستدامة لعام 2030. إن ممارسة تشكيل التكتلات على أسس أيديولوجية، والمبالغة في مفهوم الأمن القومي، وإقامة ستار حديدي رقمي، والسعي إلى الهيمنة والمزايا التكنولوجية، بل والتدخل السافر في التنمية الاقتصادية والتكنولوجية للبلدان الأخرى وقمعها، لن يؤدي إلا إلى عرقلة جهود المجتمع الدولي لتعزيز حوكمة الفضاء السيبراني.

ثالثًا، نحن بحاجة إلى بناء فضاء سيبراني أكثر إنصافًا وتنظيمًا. إن وضع قواعد دولية بشأن الفضاء السيبراني مقبولة للجميع أمر أساسي لدعم السلام والاستقرار الدائمين في الفضاء السيبراني. وينبغي لجميع الأطراف الالتزام بجدية بمقاصد ومبادئ ميثاق الأمم المتحدة، ولا سيما المبادئ من قبيل المساواة في السيادة، وعدم التدخل في الشؤون الداخلية، وعدم استخدام القوة أو التهديد باستخدامها، والتسوية السلمية للمنازعات، والامتثال لإطار سلوك الدول المسؤول في الفضاء السيبراني وتنفيذه. وفي الوقت نفسه، ينبغي لجميع الأطراف أن تتمسك دائمًا بدور الأمم المتحدة باعتبارها القناة الرئيسية وأن تترجم، على أساس المشاركة المتساوية والواسعة النطاق، توافق الآراء الدولي القائم منذ فترة طويلة إلى قواعد سلوك ملزمة قانونًا في الفضاء السيبراني. ويمكن للحلول البناءة التي اقترحتها الصين، مثل المبادرة العالمية

لحوكمة الذكاء الاصطناعي والمبادرة العالمية لأمن البيانات، أن تكون بمثابة مخططات لوضع القواعد المستقبلية بشأن الفضاء السيبراني.

رابعاً، نحن بحاجة إلى بناء فضاء سيبراني أكثر مساواة وشمولا.

التنوع هو السمة الأساسية للعالم وحافز للتقدم البشري. وتربط شبكة الإنترنت بين جميع البلدان والشعوب والحضارات بطرق غير مسبوقة، ومن الطبيعي أن تصبح الإنترنت منصة مهمة للبشرية جمعاء لعرض الثقافات المتنوعة والنهوض بتطور الحضارات وتوارثها. ويجب علينا الاستفادة بشكل كامل من تكنولوجيا المعلومات والاتصالات، وزيادة تبادل الآراء عبر الإنترنت في الحوار، وتشجيع التفاهم والمودة بين شعوب جميع البلدان، وتعزيز التسامح والتعايش بين مختلف الحضارات، وترويج القيم المشتركة للبشرية بشكل أفضل. ويجب أن نكون متيقظين إزاء ممارسة عدد قليل من الدول المتمثلة في فرض قيمها الخاصة باعتبارها قيما عالمية، بل والتدخل في الشؤون الداخلية للدول الأخرى وتعطيل تنميتها واستقرارها. ويجب أن نعارض بحزم استخدام الفضاء الإلكتروني لنشر التطرف والإرهاب والتضليل وخطاب الكراهية.

إن الصين شاهدة على تطور الإنترنت ومستفيدة منه. وتضم اليوم ما يقرب من 1,1 بليون مستخدم للإنترنت. وأقمنا أكبر بنية تحتية إلكترونية في العالم وأكثرها تقدماً من الناحية التكنولوجية، ووضعنا نظاماً سليماً من السياسات لإدارة الفضاء الإلكتروني. وما فتئت الصين تعمل بنشاط، خلال السنوات الأخيرة، على زيادة تواصلها فيما يتعلق بالسياسات وتبادل الخبرات مع بلدان الجنوب في العالم؛ وتعزيز التعاون العملي على بناء القدرات في مجالات مثل البنية التحتية والتكنولوجيا وإنفاذ القانون والاستجابة لحالات الطوارئ؛ والمشاركة بنشاط في عمليات الأمن السيبراني ضمن أطر عمل منها الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات وأمن استخدامها؛ ومجموعة العشرين؛ ومنتدى التعاون الاقتصادي لآسيا والمحيط الهادئ؛ مجموعة البرازيل وروسيا والهند والصين وجنوب أفريقيا؛ ومنظمة شنغهاي للتعاون والمنتدى الإقليمي لرابطة دول جنوب شرق آسيا، من بين منظمات أخرى؛ وتقديم مساهمات مهمة لتعزيز الحوكمة العالمية للفضاء الإلكتروني.

تتسارع ثورة المعلومات باعتبارها اتجاه العصر. وينطوي الفضاء الإلكتروني على آمال غير محدودة في مستقبل مشرق للبشرية. والصين على استعداد للعمل مع المجتمع الدولي لبناء فضاء إلكتروني أكثر سلاماً وأمناً وانفتاحاً وتعاوناً وتنظيماً والتكاتف لبناء مجتمع ذي مستقبل مشترك في الفضاء الإلكتروني.

السيد دي لا غاسكا (إكوادور) (*تكلم بالإسبانية*): أود أن أرحب بحضور السيد تشو تاي يول، وزير خارجية جمهورية كوريا. وأشكر أيضا الأمين العام أنطونيو غوتيريش على المعلومات التي قدمها ومقدمي الإحاطتين، السيد ستيفان دوغين والسيدة نينا إيفياني – أجوفو، على إحاطتيهما.

في عالم يزداد ترابطاً وتكافلاً، يشكل الأمن السيبراني تحدياً عالمياً يتطلب من المجتمع الدولي بأسره التنسيق والتعاون لمواجهته.

واستخدام تكنولوجيا المعلومات والاتصالات في الأغراض الخبيثة عامل يضاعف الأخطار التي تهدد السلام والأمن، بما في ذلك في المجالات التالية.

أولاً، يمكن أن يؤثر هذا الاستخدام على البنية التحتية الحيوية، مثل النظم الصحية والخدمات المالية وشبكات الطاقة، الضرورية لسير شؤون المجتمعات.

ثانياً، يمكن أن ينشر المعلومات المضللة وخطاب الكراهية، مما يزيد من استقطاب المجتمعات ويؤجج النزاع.

ثالثاً، يمكن أن يدعم الأنشطة الإرهابية وتمويل الأنشطة غير المشروعة التي تقوم بها الجهات الفاعلة الحكومية وغير الحكومية.

وفي ضوء هذه التحديات، يجب على مجلس الأمن ألا يتخلف عن الركب فيما يتعلق بتطور التهديدات السيبرانية، حيث إن هذه التهديدات مترابطة مع العديد من البنود المدرجة في جدول أعمال المجلس، بما في ذلك عدم الانتشار ومكافحة الإرهاب. وفي هذا الصدد، ينبغي لمجلس الأمن أن ينظر في إمكانية إدراج عناصر متعلقة بالأمن السيبراني في وثائقه، وفقاً لاحتياجات كل ملف. ومن

أمثلة ذلك تعزيز الاتصالات الاستراتيجية في عمليات السلام والبعثات السياسية الخاصة.

وتتطلب تهيئة فضاء إلكتروني آمن ومفتوح وسلمي وضع معايير للسلوك المسؤول في استخدام تكنولوجيا المعلومات والاتصالات. وإضافة إلى ذلك، يجب أن يقترن تطوير القانون الدولي في هذا المجال ببناء القدرات، خاصة في البلدان التي تشهد حالات نزاع، لأنها أكثر البلدان عرضة لإساءة استخدام تكنولوجيا المعلومات والاتصالات. ويحرز الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها تقدما في هذا المجال. ويمكن الاسترشاد بناتج عملها في عمل المجلس.

وأختتم بياني مذكراً بضرورة الحفاظ على الاستخدام المسؤول للفضاء الإلكتروني وتعزيزه من أجل ضمان استقراره وأمنه وبالتالي الحد من المخاطر الكبيرة التي يشكلها بالنسبة للدول.

السيد دو ريفيير (فرنسا) (*تكلم بالفرنسية*): أشكر الأمين العام والسيد دوغين والسيدة إيفياني – أجوفو على إحاطاتهم، وأشكركم، سيدي الرئيس، على عقد هذه المناقشة.

إن تطور تكنولوجيا المعلومات والاتصالات يساهم في التقدم وتحقيق أهداف التنمية المستدامة. لكنه يطرح أيضا تحديات كبيرة لأمننا الجماعي. ففي المجتمعات التي تعتمد اعتماداً كبيراً على هذه التكنولوجيات، تزداد الأنشطة السيبرانية الخبيثة تواتراً وخطورة وتطوراً. وهي قادرة على استغلال عديد من مواطن الضعف واستخدام وسائل متزايدة التنوع، أصبحت الآن في متناول جهات فاعلة متعددة. وتنتشر أدوات وخدمات الاقتحام بشكل لا يمكن السيطرة عليه في الأسواق، ويساهم استخدامها غير المسؤول في زيادة التهديدات السيبرانية.

ويمكن أن تشكل الهجمات السيبرانية، في حد ذاتها، أخطارا على السلام والأمن الدوليين عن طريق تأثيرها على البنية التحتية الحيوية، وبفعل مخاطر استفحالها. وبالتالي، يمكن أن تؤثر هجمات برمجيات انتزاع الفدية، التي زادت بنسبة 30 في المائة عام 2023، وفقا لما أفادت به السلطات الفرنسية، على قطاعات أساسية مثل قطاع الطاقة، وأن تزعزع استقرار الاقتصادات، بل تعطل سير عمل المؤسسات الحكومية. وتُنفذ الهجمات السيبرانية الآن في سياق النزاع المسلح، كما رأينا في الهجمات التي شنتها روسيا على شبكة سواتل فياسات في الساعات الأولى من غزوها غير المشروع لأوكرانيا.

ويمكن أيضا أن تغذي الأنشطة السيبرانية الخبيثة تهديدات أخرى للسلام والأمن الدوليين، بما في ذلك الانتشار. ويشير أحدث تقرير لفريق الخبراء التابع للجنة المنشأة عملا بالقرار 1718 (2006) (S/2024/215) إلى أن برامج نظام كوريا الشمالية لأسلحة الدمار الشامل غير المشروعة تم تمويلها بنسبة تصل إلى 40 في المائة بوسائل إلكترونية غير مشروعة، مثل برمجيات انتزاع الفدية أو سرقة العملات المشفَّرة.

لكن تتوفر للأمم المتحدة ومجلس الأمن، تنفيذاً للولاية المنوطة به، وسائل كفيلة بتنفيذ تدابير منسقة لمواجهة هذه التهديدات. أولاً، ينبغي أن نتذكر أن الفضاء الإلكتروني ليس مجالاً غير خاضع للرقابة أو بلا معايير، بل ينطبق عليه تماما القانون الدولي الحالي، بما في ذلك ميثاق الأمم المتحدة والقانون الدولي الإنساني والقانون الدولي لحقوق الإنسان. وقد حُددت معايير سلوك الدول المسؤول بتوافق الآراء من أجل تشجيع التعاون، وتعزيز منع نشوب النزاعات وزيادة الاستقرار في الفضاء الإلكتروني.

وتؤيد فرنسا عمل اللجنة الأولى للجمعية العامة لمواصلة تطوير هذا الإطار المعياري. ودعماً لتنفيذ هذا الإطار، اقترحت فرنسا هيكلاً لآلية برنامج عمل طموح للفضاء الإلكتروني في المستقبل. وعلى مجلس الأمن أن يتخذ احترام الإطار المعياري لسلوك الدول المسؤول محوراً لعمله بشأن التهديدات السيبرانية وأن يشجع الدول على الوفاء بالتزاماتها بالمساهمة في تحقيق أمن الفضاء السيبراني واستقراره.

وإلى جانب ذلك، يجب على مجلس الأمن أن يواصل جهوده لإدماج المسائل السيبرانية في مختلف أبعاد ولايته. ومن الضروري أن يتلقى المجلس إحاطات منتظمة من الخبراء بشأن تطور التهديدات السيبرانية وآثارها على السلام والأمن الدوليين. وتشكل مناقشة اليوم مثالاً على ذلك.

ويجب على المجلس أيضا أن يواصل الاهتمام باستخدام الوسائل الإلكترونية للتحايل على نظم الجزاءات. وفي هذا الصدد، ينبغي مواصلة الاهتمام على وجه خاص بالأنشطة السيبرانية الخبيثة التي يقوم بها النظام الكوري الشمالي لتمويل برامجه المتعلقة بأسلحة الدمار الشامل. وستواصل فرنسا العمل بنشاط لضمان استمرار المجلس، على الرغم من عدم تمديد ولاية فريق الخبراء التابع للجنة القرار 1718، في رصد انتهاكات قراراته في هذا المجال بيقظة.

الرئيس (*تكلم بالإنكليزية*): أعطي الكلمة الآن لمعالي السيد مامادو تانغارا، ووزير الخارجية والتعاون الدولي وشؤون المغتربين في غامبيا.

السيد تانغارا (غامبيا) (*تكلم بالإنكليزية*): أولا وقبل كل شيء، أود أن أشكر مقدمي الإحاطات على ملاحظاتهم المستنيرة وأن أهنئ جمهورية كوريا على تنظيم هذه المناقشة.

إننا نقف اليوم عند مفترق طرق. فقد نسج العصر الرقمي شبكة من التواصل والفرص والتقدم. ولكن عتمة متزايدة تتسلل بين خيوط هذا النسيج وتهدد السلام والأمن الدوليين. فالتهديد المتزايد باستمرار للجريمة الإلكترونية لا يقتصر على المكاسب المالية أو البيانات المسروقة. وتشكل الموجة الجديدة من التهديدات السيبرانية تحديا مباشرا للسلام والأمن الدوليين وتتطلب اهتمامنا العاجل. وفي هذا الصدد، نشكر جمهورية كوريا على لفت انتباهنا إلى مشاركة مبتكرة أخرى لمجلس الأمن بهدف تبادل الأفكار الموضوعية بشأن بند جدول الأعمال المعنون "صون السلام والأمن الدوليين: التصدي للتهديدات المتطورة في الفضاء السيبراني". ولا يمكن لمجلس الأمن، بوصفه الهيئة المكلفة بصون السلام والأمن الدوليين، أن يبقى صامتا ونشيد بجهوده المستمرة في دق ناقوس الخطر بشأن هذه المسألة الهامة والمشتركة. إننا بحاجة إلى نهج شامل يتصدى لهذا التهديد المتزايد.

وفي هذا الصدد، أود أن أقترح النقاط الثلاث التالية لدعم جهودنا المشتركة في الحد من المخاطر السيبرانية التي تهدد السلام والأمن الدوليين.

أولاً، يجب أن يصبح مجلس الأمن نصيراً للمعايير النموذجية لسلوك الدول المسؤول في الفضاء السيبراني ويمكننا تحقيق ذلك من خلال بذل جهود التوعية على نحو منتظم لتعزيز المناقشات ذات الصلة بالأمن السيبراني بهدف توسيع نطاق عمل المنتديات الإلكترونية للجمعية العامة والتعاون مع الدول الأعضاء لترجمة تلك المعايير إلى أفعال وتعزيز بناء القدرات وتبادل المعلومات لمنع الأنشطة الخبيثة.

ثانياً، يمكن أن يعزز مجلس الأمن المساءلة عن التهديدات الأمنية المتعلقة بالفضاء السيبراني من خلال الدعوة إلى تحسين القدرات السيبرانية للدول الأعضاء بغية تحديد الجهات الفاعلة الخبيثة وبناء جبهة موحدة لمكافحة الإفلات من العقاب.

ثالثاً، يمكن أن يستفيد مجلس الأمن من خبرات كيانات الأمم المتحدة مثل مكتب شؤون نزع السلاح ومكتب مكافحة الإرهاب من أجل التصدي على نحو مناسب لخطر تقويض ديمومة السلام والأمن والديمقراطية على الصعيد الدولي. ويمكن أن يؤدي التعاون مع تلك الكيانات أيضًا إلى التنسيق لتجنب الازدواجية وضمان اتباع نهج شامل ملائم للغرض المنشود.

ولن تؤدي هذه الإجراءات، التي تُتخذ في إطار ولاية المجلس، إلى تعزيز السلام والأمن الدوليين فحسب، بل ستعزز أيضاً الجهود القائمة من خلال النهوض بالوعي وتعزيز المساءلة والتشجيع على التعاون الفعال بين الدول والمؤسسات الدولية المعنية. وعليه، فإن بمقدور مجلس الأمن أن يضطلع بدور رائد في بناء فضاء سيبراني أكثر أمناً واستقراراً للجميع.

ويجب أن نرتقي بمستوى المناقشة وندرج بانتظام التهديدات السيبرانية في مداولاتنا المتعلقة بالنزاعات الإقليمية والمسائل الموضوعية. وهو ما يوسع من نطاق عمل منتديات الجمعية العامة المخصصة للمعايير السيبرانية. ويجب أن نشجع أيضا الدول الأعضاء على تحويل تلك المعايير إلى إجراءات ملموسة. ويشمل ذلك بناء القدرات في مجال الدفاع السيبراني وتعزيز تبادل المعلومات وردع الأنشطة الخبيثة.

في الختام، أود أن أشيد مرة أخرى بجمهورية كوريا على هذه المبادرة الجديرة بالثناء التي تتيح للدول الأعضاء فرصة المشاركة في هذه المناقشة الهامة جدا والموضوعية بشأن مسألة ذات اهتمام مشترك. ويضطلع مجلس الأمن بدور محوري في تقديم الدعم الحاسم الذي تشتد الحاجة إليه للتخفيف من حدة المخاطر السيبرانية التي تهدد السلام والأمن الدوليين وإنهائها.

الرئيس (*تكلم بالإنكليزية*): أعطي الكلمة الآن لممثل ألمانيا.

السيد ليندنر (ألمانيا) (*تكلم بالإنكليزية*): تشكر ألمانيا جمهورية كوريا على دورها القيادي في لفت انتباه مجلس الأمن إلى مسائل الأمن السيبراني. كما أود أن أشكر الأمين العام ومقدمي الإحاطات على إسهاماتهم المتبصرة.

يتعرض المجتمع الدولي لعدد متزايد من الحوادث السيبرانية الخبيثة التي ترعاها دول أو جهات خاصة. وتؤثر هذه الحوادث تأثيرا خطيرا على صون السلام والأمن الدوليين. وأظهرت الهجمات الشرسة التي يشنها مرتكبو الجرائم السيبرانية، بما في ذلك الهجمات ببرمجيات انتزاع الفدية، أن هذه الهجمات قد تهدد استقرار مؤسسات الدولة. فقد أثرت على مجتمعات بأكملها.

ونشهد في الآونة الأخيرة ظهور مجموعات القراصنة في مسرح النزاعات الدولية بحيث تهاجم أهدافًا رئيسية في الهياكل الأساسية الحيوية. وقد أدى ذلك إلى إضعاف الثقة في تقديم الخدمات العامة ونشر الخوف بين المدنيين. وأدى التعاون المتزايد لعدد من الجهات الفاعلة الحكومية مع شركات تكنولوجيا المعلومات الخاصة ومجموعات القراصنة ومجرمي الإنترنت إلى تفاقم المخاطر القائمة. وأصبحت هذه الاتجاهات كلها عوامل مضاعفة للخطر، نظراً إلى أن المجال السيبراني يوسع نطاق ساحات القتال التقليدية لتشمل المجال المدني.

وفي ضوء هذا التهديد الآخذ في التطور على نحو كبير، تقترح ألمانيا المجالات الأربعة التالية التي ينبغي أن ينشط فيها مجلس الأمن:

أولاً، نرى أن مجلس الأمن يضطلع بدور مهم في تقييم التهديد، سواء وفقاً للمادة 34 من ميثاق الأمم المتحدة التي تمنح مجلس الأمن سلطة التحقيق في أي حالة قد تؤدي إلى احتكاك دولي أو تؤدي إلى نشوب نزاع أو بشكل أعم من حيث ضرورة أن ينظر المجلس ويحلل بصورة أعمق المخاطر التي تهدد السلام والأمن الدوليين الناجمة عن الهجمات السيبرانية.

ثانياً، يؤدي مجلس الأمن دورا مهما في تسوية المنازعات، استناداً إلى قابلية تطبيق ميثاق الأمم المتحدة على الفضاء السيبراني تطبيقا كاملا.

ثالثاً، نرى أن مجلس الأمن قادر على أداء دور قوي في بناء الثقة ووضع المعايير. وسيساعد المجلس في وضع إطار متطور ينظم السلوك المسؤول للدول في الفضاء السيبراني من خلال إدراج النزاعات السيبرانية الدولية في جدول أعماله أو التحقيق في حالات النزاع السيبراني أو تيسير التسوية السلمية لهذه الحالات. ويجب أن يستند ذلك إلى القانون الدولي وأن يُستكمل بمعايير الأمم المتحدة الطوعية وتدابير بناء الثقة.

أخيراً، ترحب ألمانيا بالجهود التي يبذلها مجلس الأمن لإدراج تهديدات الأمن السيبراني في جدول أعماله. وينبغي أن يشمل ذلك حماية الأمم المتحدة من الهجمات السيبرانية الخبيثة، ولا سيما وجودها في الميدان مثل عمليات حفظ السلام.

في الختام، أود أن أؤكد أن ألمانيا ستواصل المساهمة في النقاش الدولي حول هذه المسألة الهامة. وأطلقنا في العام الماضي، على سبيل المثال لا الحصر، حوارا عالميا بخصوص الفضاء السيبراني في حالات النزاع. ويسعى بوجه خاص إلى التصدي للمخاطر المتزايدة التي يتعرض لها المدنيون جراء استخدام الأدوات السيبرانية في النزاعات الدولية والتوعية واقتراح حلول للتخفيف من حدة المخاطر. وسيُعقد الحوار التالي هنا في نيويورك في البيت الألماني في 8 تموز/يوليه بالتعاون مع اليابان والسنغال واللجنة الدولية للصليب الأحمر.

الرئيس (*تكلم بالإنكليزية*): أعطي الكلمة الآن لممثل الإمارات العربية المتحدة.

السيد شرف (الإمارات العربية المتحدة) (*تكلم بالإنكليزية*): أشكر معالي السيد تشو تاي يول، وزير الخارجية، على ترؤسه هذه المناقشة

المفتوحة وأثني على قيادة جمهورية كوريا لمجلس الأمن هذا الشهر. كما أشكر الأمين العام وغيره من مقدمي الإحاطات على إسهاماتهم المتبصرة.

كما سمعنا اليوم، تشهد التهديدات التي يتعرض لها الفضاء السيبراني تطورا سريعا. وتُستخدم الأدوات والتقنيات السيبرانية الخبيثة، مثل برمجيات انتزاع الفدية والتصيد الإلكتروني والهجمات لقطع الخدمة، لاستهداف شبكات الحكومة والقطاع الخاص، مما يهدد الهياكل الأساسية الحيوية والسلامة العامة. وهو أمر مثير للقلق بالنظر إلى أن دولنا تشهد تحولات رقمية، بما في ذلك الإمارات العربية المتحدة، مما يجعلنا أكثر اعتماداً على النظم الإلكترونية الآمنة. كما أن المؤسسات التعليمية معرضة أيضاً للخطر، بما أن الجهات الفاعلة الخبيثة تستهدف البنية التحتية الرقمية لقطاع التعليم وأصول المعلومات القيمة. وعلاوة على ذلك، يمثل الاستخدام الخبيث لتكنولوجيا المعلومات والاتصالات، بما في ذلك تقنيات الذكاء الاصطناعي الناشئة على سبيل المثال لا الحصر، عاملا مضاعفا للخطر في النزاعات القائمة.

وأنشأت الإمارات العربية المتحدة، باعتبارها مركزاً عالمياً للتكنولوجيا والابتكار، مجلس الأمن السيبراني في عام 2020. ويهدف المجلس إلى تحقيق تحول رقمي أكثر أمانًا وتحسين الأمن السيبراني لجميع القطاعات المستهدفة في البلد. ونلتزم ببناء القدرات وتبادل المعلومات مع شركائنا، بالإضافة إلى تعزيز التصميم المسؤول للتكنولوجيا واستخدام الذكاء الاصطناعي من أجل تحقيق المنفعة لمكافحة انتشار وتضخيم خطاب الكراهية والمعلومات المغلوطة والمضللة. وتماشيًا مع هذا الالتزام، استضفنا مع ألبانيا اجتماعًا بصيغة آريا في كانون الأول/ديسمبر 2023 من أجل التطرق لتلك التحديات.

وأخذا لما سبق في الاعتبار، أود أن أطرح أربع نقاط للنظر فيها.

أولاً، يجب أن يوجه القانون الدولي استخدام تكنولوجيا الفضاء الإلكتروني. ويجب احترام ميثاق الأمم المتحدة وسيادة الدول وعدم التدخل في شؤونها الداخلية ومسؤولية الدول وقوانين النزاعات المسلحة، بما في ذلك معايير الأمم المتحدة لسلوك الدول المسؤول في الفضاء السيبراني. وتتطلب معالجة الثغرات المعيارية تحقيق تقارب مستمر بشأن كيفية الامتثال للقانون الدولي في المجال السيبراني والحفاظ عليه.

ثانياً، تؤيد الإمارات العربية المتحدة إدراج الشواغل السيبرانية في أعمال المجلس المتعلقة بالسلام والأمن الدوليين. ويمكن أن يشمل ذلك الإشارة إلى الشواغل والاتجاهات والتطورات المتعلقة بالفضاء السيبراني في الإحاطات والبيانات والمسائل ذات الأولوية على نحو أكثر انتظاماً، وكذلك فيما يتعلق بالملفات الخاصة ببلدان بعينها وغيرها من الملفات المواضيعية. وعلى سبيل المثال، ينص القرار 2341 (2017) على ضرورة حماية الهياكل الأساسية الحيوية من الهجمات الإرهابية، بما في ذلك الأمن السيبراني، مع تأكيد الحاجة إلى التصدي بصورة أفضل للطائفة الواسعة من التهديدات السيبرانية التي ترافق الرقمنة والفضاء السيبراني.

ثالثاً، ينبغي أن ينظر المجلس في عقد جلسة إحاطة سنوية حول التهديدات التكنولوجية الناشئة وآثارها على السلام والأمن الدوليين. وعلاوة على ذلك، فإن نشر الأمين العام لتقرير سنوي عن الأمن السيبراني كفيل بتقديم تقييم شامل للمشهد العالمي المتعلق بالتهديدات السيبرانية وتوصيات لتعزيز التعاون الدولي. وينبغي أن يتضمن التقرير أيضا تحليلاً جنسانيًا للاستجابة على نحو أفضل للتهديدات التي تستهدف النساء والفتيات في الفضاء السيبراني.

رابعاً، إن تعزيز الشراكات القوية بين القطاعين العام والخاص أمر بالغ الأهمية للاستفادة من الخبرات والموارد لمواجهة التهديدات السيبرانية بفعالية. وتلتزم الإمارات العربية المتحدة بالتعاون مع القطاع الخاص لاستحداث أدوات قوية للأمن السيبراني وبناء قدرات وطنية ودولية، إلى جانب دعم القطاع الخاص في ضمان وضع حلول على نحو آمن ومسؤول.

إن تسخير تكنولوجيات الفضاء الإلكتروني أمر بالغ الأهمية لمستقبلنا، ولكن من الضروري توخي الحذر من مخاطرها. ويشكل التعاون وبناء القدرات على الصعيد الدولي أمران حيويان ليتمكن الأمن العالمي من الصمود. وستواصل الإمارات العربية المتحدة تعزيز

السلوك المسؤول في الفضاء الإلكتروني وضمان أن يعكس تطلعاتنا الجماعية إلى السلام والأمن.

الرئيس (*تكلم بالإنكليزية*): أعطي الكلمة الآن لممثلة لاتفيا.

السيدة ملباردي (لاتفيا) (*تكلمت بالإنكليزية*): تود لاتفيا أن تعرب عن امتنانها لجمهورية كوريا على تنظيم هذه المناقشة المفتوحة الرفيعة المستوى لمجلس الأمن. كما نود أن نشكر الأمين العام ومقدمي الإحاطات من معهد السلام السيبراني وجامعة ليدز بيكيت على عروضهم الثاقبة.

لقد زاد استخدام التكنولوجيا الرقمية والاعتماد عليها زيادة كبيرة منذ إدراج مسائل الأمن السيبراني لأول مرة في جدول أعمال الأمم المتحدة قبل أكثر من 20 عاماً. وأصبح المجال السيبراني اليوم النسيج الجامع بين التنمية الاقتصادية والاجتماعية على الصعيد العالمي. ولطالما ارتبط توسع الفضاء السيبراني أيضاً بتزايد المخاطر والتحديات على الرغم من توفيره فرصا هائلة للتقدم. وواجهنا في السنوات الأخيرة العديد من الاتجاهات السلبية فيما يتعلق بالسلام والأمن الدوليين. وتتزايد عدد الحالات التي استُهدفت فيها البنية التحتية الحيوية، بما في ذلك البنية التحتية الحيوية للمعلومات، في هجمات سيبرانية تنذر بعواقب كارثية في العالم الواقعي. وعلاوة على ذلك، نلاحظ أن الهجمات السيبرانية أصبحت جزءًا لا يتجزأ من العدوان الروسي الشامل على أوكرانيا.

وغالباً ما تتقاطع التهديدات السيبرانية مع أعمال عدائية أخرى مثل انتشار المعلومات المضللة والمغلوطة والاستخدام الخبيث للذكاء الاصطناعي والتقنيات الناشئة الأخرى. وتنتشر الجرائم الإلكترونية أيضًا حيث وصلت المدفوعات المتصلة ببرمجيات انتزاع الفدية إلى مستوى قياسي في عام 2023. وتؤثر هذه التطورات على السلام والأمن العالميين. ويجب أن ينسق المجتمع الدولي استجابته ويضطلع مجلس الأمن بدور يتماشى مع ولايته.

لذلك، تعتقد لاتفيا أن تهديدات الفضاء السيبراني وتحدياته تستحق مناقشتها بانتظام في المجلس. ويمكن أن تسترشد هذه المناقشات بتقرير دوري يقدمه الأمين العام. وقد تيسر زيادة اهتمام المجلس بالأمن السيبراني أيضا إدراج الجوانب المتعلقة بالفضاء السيبراني في ولايات مواضيعية أخرى مثل حفظ السلام والمرأة والسلام والأمن. وينبغي أن ينظر المجلس أيضا في تعزيز قدرته على الاستجابة للهجمات السيبرانية واسعة النطاق التي يُحتمل أن تكون لها تداعيات أمنية على الصعيد الدولي.

ومن البديهي أن تعزيز دورالمجلس في معالجة مسائل الأمن السيبراني لا يمكن أن يتحقق بين عشية وضحاها. إنه مسعى متدرج وتؤدي الجلسات مثل جلسة اليوم دوراً حاسمًا في تيسير هذه العملية. ومن الواضح أيضا أن أعمال المجلس لا ينبغي أن تحل محل ما أُنجز بالفعل في محافل الأمم المتحدة الأخرى في إطار الجمعية العامة. بل على العكس تماماً، ينبغي أن يعزز المجلس التفاهمات المتفق عليها في تلك المحافل، ولا سيما إمكانية تطبيق القانون الدولي في مجمله على الفضاء السيبراني. كما أن هناك المزيد من العمل الذي يتعين القيام به بشكل جماعي بشأن تنفيذ إطار سلوك الدول المسؤول في الفضاء السيبراني. وإذ نتوقع إنشاء آلية دائمة للأمم المتحدة لمعالجة الأمن السيبراني، معروفة باسم برنامج العمل للنهوض بسلوك الدول المسؤول في استخدام تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي، فإننا نرى إمكانية إيجاد أوجه تآزر جديدة بين المجلس والجمعية العامة في هذا المجال.

في الختام، أود أن أؤكد على التزام لاتفيا بمواصلة دعم الجهود المبذولة في إطار الأمم المتحدة للتصدي للتهديدات والتحديات المتزايدة في مجال الأمن السيبراني. ولطالما انخرطنا بهمة في المناقشات المتعلقة بهذا الموضوع في لجان الجمعية العامة وسنواصل أيضًا الدعوة إلى اضطلاع المجلس بدور أكبر.

الرئيس (*تكلم بالإنكليزية*): أعطي الكلمة الآن لممثلة مصر.

السيدة رزق (مصر) (*تكلم بالإنكليزية*): تولي مصر أهمية كبيرة لجوانب تكنولوجيا المعلومات والاتصالات المتعلقة بالأمن الدولي وتدعو الأمم المتحدة بقوة إلى الاضطلاع بدور مركزي ورائد في تعزيز وتطوير القواعد والمبادئ المنظمة لاستخدام الدول لتكنولوجيا المعلومات والاتصالات من خلال عملية شاملة ومنصفة بمشاركة جميع الدول.

ويعكف عدد من الدول على تطوير القدرات في مجال تكنولوجيا المعلومات والاتصالات في سياق إمكانية استخدامها في أغراض خبيثة ولأغراض عسكرية هجومية. لقد أصبح استخدام تكنولوجيا المعلومات والاتصالات في النزاعات بين الدول مستقبلا حقيقة واقعة، كما أن خطر شن هجمات ضارة باستخدام هذه التكنولوجيا على البنية التحتية الحيوية حقيقي وجاد على حد سواء. ويخلّف هذا السباق الجديد نحو التسلح تداعيات بعيدة المدى على السلام والأمن والاستقرار على الصعيد الدولي، ولا سيما مع استمرار تراجع الحدود الفاصلة بين الأسلحة التقليدية وغير التقليدية.

وعلاوة على ذلك، ينقل الإرهابيون والمجرمون التقنيات ذات الصلة التي طورتها الدول وينسخونها ويعيدون إنتاجها. ويشكل استخدام المنظمات الإرهابية والإجرامية الخبيث لتكنولوجيا المعلومات والاتصالات خطرا كبيرا على السلام والأمن الدوليين، ولا سيما في ضوء التحديات المتعلقة بالإسناد. وبموجب القانون الدولي وميثاق الأمم المتحدة، ينبغي أن تمتنع جميع الدول الأعضاء عن القيام بأي عمل يلحق الضرر باستخدام وتشغيل الهياكل الأساسية الحيوية للدول الأخرى أو يعوق ذلك بأي شكل آخر، سواء عن علم أو قصد، أو يفضي إلى التدخل في شؤونها الداخلية. ولا شك في أن جوانب تكنولوجيا المعلومات والاتصالات المتعلقة بالأمن الدولي أضحت على درجة من الأهمية والاستراتيجية تستدعي وضع قواعد ملزمة واضحة لها على الصعيد الدولي. إن إجراء عملية شاملة للجميع في إطار منظومة الأمم المتحدة هو أفضل السبل وأكثرها فعالية لوضع ترتيبات منصفة وشاملة وفعالة في هذا المجال.

وقد اتخذت الأمم المتحدة بالفعل بعض الخطوات نحو وضع إطار معياري يكمل مبادئ القانون الدولي. وباعتماد تقريرين مرحليين سنويين بتوافق الآراء للفريق العامل المفتوح باب العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات وأمن استخدامها، المنشأ عملاً بقرار الجمعية العامة 240/75، وتقارير أخرى بتوافق الآراء لعمليات الأمم المتحدة ذات الصلة، تكون الأمم المتحدة قد وضعت بالفعل العناصر الأولية لإطار عمل لمنع نشوب النزاعات وتحقيق الاستقرار في الفضاء السيبراني.

ودعت الجمعية العامة الدول الأعضاء إلى الاسترشاد في استخدامها لتكنولوجيا المعلومات والاتصالات بالإطار التراكمي والمتطور لسلوك الدول المسؤول الوارد في التقارير المتتالية لأفرقة الخبراء الحكوميين التابعة للجنة الأولى. لكن تنفيذ هذه المعايير لا يزال محدودا للغاية في أفضل الأحوال، نظراً لطبيعتها الطوعية وعدم وجود أي آلية للمتابعة.

ومع الإقرار بالتقدم المحرز في الفريق العامل المفتوح باب العضوية المنشأ عملا بقرار الجمعية العامة 240/75 بشأن مختلف جوانب ولايته، فمن المهم أن يرسي الفريق الأساس لإنشاء آلية في المستقبل، تحت رعاية الأمم المتحدة، تكون عملية المنحى وذات مسار واحد وقائمة على توافق الآراء وشاملة للجميع. وينبغي أن تستند هذه الآلية إلى النتائج المتفق عليها للعمليات المتصلة بالأمم المتحدة وأن تركز على تنفيذ النتائج المتفق عليها، بما في ذلك إطار سلوك الدول المسؤول، ومواصلة تطوير هذا الإطار وتعزيز التعاون الدولي مع البلدان النامية وتقديم المساعدة لها.

إن العمليات الشاملة للجميع داخل الأمم المتحدة، تحت رعاية الجمعية العامة في المقام الأول، هي الطريقة الأكثر فعالية لوضع ترتيبات منصفة وشاملة وفعالة في هذا المجال. ويشجع مجلس الأمن من جانبه على مراعاة الفرص التي تتيحها التكنولوجيات الناشئة عند النظر في مواضيع من قبيل حفظ السلام ومكافحة الإرهاب. ومع ذلك، ينبغي ألا يُستخدم المجلس باعتباره هيئة تشريعية تحاول وضع المعايير والقواعد نيابة عن الدول الأعضاء في الأمم المتحدة في المسائل التي تتطلب بالضرورة عمليات شاملة للجميع وشفافة.

ويمكن للتوصيات التي أقرتها الجمعية العامة بتوافق الآراء أن تشكل أساساً لقواعد ملزمة سياسياً أو قانونياً، خاصة وأنها مستمدة من مبادئ القانون الدولي وميثاق الأمم المتحدة. وإذ نعتقد أن القانون الدولي ومبادئ ميثاق الأمم المتحدة تنطبق بالفعل على جميع المجالات، بما

في ذلك الفضاء السيبراني، فإننا نرى أيضاً أن هناك حاجة ملحة لتحديد التزامات معينة تجعل سلوك الدول في الفضاء السيبراني متوافقاً مع القانون الدولي وأهداف ومبادئ ميثاق الأمم المتحدة.

وفي عالم يزداد ترابطاً، فإن أي نظام دولي للأمن السيبراني لن يكون قوياً إلا بقدر قوة أضعف حلقاته. ولحسن الحظ، هناك إجماع على ضرورة تكثيف جهود بناء القدرات وتعزيزها لمنع الهجمات المحتملة ضد البنية التحتية الحيوية وتطوير القدرات والمهارات التقنية اللازمة في البلدان النامية. وينبغي أن تقود الأمم المتحدة جهداً منسقاً يهدف إلى تقديم المساعدة اللازمة للبلدان النامية.

وفي الختام، تتيح تكنولوجيا المعلومات والاتصالات فرصاً وتنطوي على تحديات كبيرة، ونؤكد على أن هناك حاجة ملحة لتحديد وتطوير قواعد لسلوك الدول المسؤول من أجل زيادة الاستقرار والأمن في البيئة العالمية لتكنولوجيا المعلومات والاتصالات ومنع تحول الفضاء السيبراني إلى ساحة أخرى للنزاعات ولحدوث سباق للتسلح.

الرئيس (*تكلم بالإنكليزية*): أود تذكير جميع المتكلمين بألا تزيد مدة بياناتهم على ثلاث دقائق حتى يتسنى للمجلس إنجاز عمله بسرعة. الأضواء الوامضة المثبتة على أطواق الميكروفونات ستنبه المتكلمين إلى إنهاء ملاحظاتهم بعد ثلاث دقائق.

أعطي الكلمة الآن لممثلة أوكرانيا.

السيدة هايوفيشين (أوكرانيا) (*تكلمت بالإنكليزية*): نشكر رئاسة جمهورية كوريا لمجلس الأمن على عقد هذه المناقشة المفتوحة الرفيعة المستوى. كما نعرب عن تقديرنا للأمين العام ومقدمي الإحاطات الآخرين على ملاحظاتهم.

تؤيد أوكرانيا البيان الذي سيُلقى باسم الاتحاد الأوروبي وتود أن تبدي بعض الملاحظات بصفتها الوطنية.

نعتقد بقوة أن مجلس الأمن يؤدي دوراً هاماً في التصدي للأخطار التي تهدد السلام والأمن الدوليين، بما في ذلك في الفضاء السيبراني. ويستمر مشهد التهديد السيبراني في التطور وقد أصبح أكثر صعوبة من أي وقت مضى. وتشكِّل برمجيات انتزاع الفدية خطراً متزايداً وكبيراً على الحكومات والشركات والأفراد. وبالإضافة إلى ذلك، فإننا نشهد زيادة في عدد العمليات السيبرانية الخبيثة التي تستهدف البنية التحتية الحيوية والبنية التحتية المعلوماتية الحيوية، بما في ذلك قطاع الطاقة والخدمات العامة والعمليات الانتخابية. وتواصل بعض الجهات الحكومية الفاعلة تقويض النظام الدولي القائم على القواعد وإطار سلوك الدول المسؤول في الفضاء السيبراني من خلال القيام بأنشطة سيبرانية خبيثة.

وفي هذا الصدد، تعمل جمهورية كوريا الشعبية الديمقراطية في أنشطة التجسس السيبراني وسرقة العملات المشفرة، بهدف مواصلة تطوير برامجها النووية وبرامج أسلحة الدمار الشامل لديها، في انتهاك لقرارات مجلس الأمن ذات الصلة. وفي الآونة الأخيرة، شنت مجموعة التجسس السيبراني الروسية APT28 هجمات سيبرانية ضد عدد من الدول الأعضاء في الاتحاد الأوروبي.

وتواجه أوكرانيا عدوان روسيا، بما في ذلك في الفضاء السيبراني. وقد ازدادت الهجمات السيبرانية الروسية تعقيدًا منذ بداية الحرب واستهدفت الوكالات الحكومية والأمنية والشركات والمؤسسات المالية. ويشن مجرمو الإنترنت في موسكو هجمات استراق الهوية الرقمية والتجسس السيبراني والهجمات ضد البنية التحتية الحيوية، بالإضافة إلى نشر المعلومات المضللة والدعاية.

ومن أجل منع التهديدات السيبرانية ومكافحتها والتخفيف من حدتها بشكل فعال، تتعاون أوكرانيا بنشاط مع الشركاء الدوليين لتطوير بناء القدرات السيبرانية الفعالة، وهو أمر أساسي لممارسة الحق في الدفاع عن النفس في الفضاء السيبراني. وبالإضافة إلى ذلك، بدأت أوكرانيا أيضًا في التحقيق في الهجمات السيبرانية ومقاضاة مرتكبيها باعتبارها جرائم حرب.

ويجب أن تتقيد الدول بالتزاماتها وتعهداتها الدولية، بما في ذلك في سياق أمن استخدام تكنولوجيا المعلومات والاتصالات. وكما أكدنا من جديد هنا في الأمم المتحدة، فإن القانون الدولي، بما في ذلك ميثاق الأمم المتحدة، ينطبق على المجال السيبراني. ولذلك، يجب محاسبة

جميع الجهات الفاعلة الحكومية التي تتصرف بطريقة تتعارض مع الإطار المتفق عليه.

وختامًا، نشجع الدول الأعضاء في الأمم المتحدة على مواصلة العمل معًا على تعزيز وتنفيذ الإطار المعياري لسلوك الدول المسؤول، وزيادة الوعي وتبادل أفضل الممارسات في الاستجابة للتهديدات القائمة والناشئة في المجال السيبراني.

الرئيس (*تكلم بالإنكليزية*): أعطي الكلمة الآن لممثل إستونيا.

السيد تامسار (إستونيا) (*تكلم بالإنكليزية*): نرحب بتبادل الآراء اليوم ونشكر مقدمي الإحاطة، والأمين العام على وجه الخصوص، على أفكارهم القيمة للغاية.

وتؤيد إستونيا البيان الذي سيدلي به ممثل الاتحاد الأوروبي. اسمحوا لي أن أدلي ببعض الملاحظات بصفتي الوطنية.

لا يمكننا تجاهل التطور والضرر المتزايدين من جراء الحوادث السيبرانية الخبيثة التي تنفذها الجهات الفاعلة من الدول وغير الدول على حد سواء. وبالنظر إلى الأهداف الرفيعة المستوى، مثل البنية التحتية الحيوية والمؤسسات المالية والعمليات الديمقراطية؛ والطبيعة العابرة للحدود للحوادث وزيادة القدرات، فإن الهجمات السيبرانية قادرة على إحداث المزيد من ال أضرار. ولذلك، من الواضح أن الأمن السيبراني جزء من التحديات الأمنية الوطنية والدولية على حد سواء، وأولويتنا المشتركة هي منع هذه التهديدات والتخفيف من حدتها.

وقد أبرز العدوان الروسي على أوكرانيا كيف تتشابك العمليات السيبرانية مع أعمال الحرب الحركية. وقد شهدنا كيف تستهدف روسيا البنية التحتية الحيوية الأوكرانية، في انتهاك للقانون الدولي الإنساني. وقد أكدت تصرفات روسيا على ضرورة التركيز على نهج شامل للدفاع الوطني والأمن الداخلي. ومن أجل تعزيز استعداد أوكرانيا للهجمات السيبرانية ومقاومتها لها، تدعم إستونيا أوكرانيا بنشاط في المجال السيبراني على المستوى الثنائي، وكذلك من خلال آلية تالين وتحالف تكنولوجيا المعلومات.

كما أننا نشعر بقلق عميق إزاء آخر الأنباء الواردة من بيونغ يانغ، والتي تشير إلى أن التعاون العسكري لجمهورية كوريا الشعبية الديمقراطية مع روسيا قد تعزز بشكل أكبر، في انتهاك صارخ لقرارات مجلس الأمن ذات الصلة. وتدين إستونيا بشدة الأنشطة السيبرانية الخبيثة المستمرة التي ترتكبها جمهورية كوريا الشعبية الديمقراطية، والتي تهدف إلى تغذية برنامج الأسلحة للبلد، وزعزعة الأمن الإقليمي وتهديد السلام العالمي.

ويقوم إطار الأمم المتحدة لسلوك الدول المسؤول في الفضاء السيبراني على أساس القانون الدولي القائم. وينطبق القانون الدولي – ولا سيما ميثاق الأمم المتحدة، وقانون مسؤولية الدولة، والقانون الدولي لحقوق الإنسان، والقانون الدولي الإنساني – بشكل كامل على العمليات السيبرانية. إننا بحاجة إلى العمل معاً لدعم القانون الدولي وضمان الالتزام به أيضاً في الفضاء السيبراني. ومن أجل دعم تنفيذ إطار سلوك الدول المسؤول في الفضاء السيبراني، تؤيد إستونيا إنشاء برنامج عمل شامل وعملي المنحى كهيكل دائم واحد بعد اختتام أعمال الفريق العامل الحالي المفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات وأمن استخدامها في عام 2025.

لا يمكن اعتبار بيئة تكنولوجيا المعلومات والاتصالات المفتوحة والآمنة والمستقرة والمتاحة والسلمية أمراً مسلما به وهي غير منفصلة عن العالم المادي. ففي حين أن العدوان الروسي على أوكرانيا أظهر الطبيعة المتكاملة للهجمات الإلكترونية والحرب النشطة، فإننا نعتقد أن هذا نمط سيتم استخدامه أيضًا في النزاعات المستقبلية. وبالتالي، فإن لمجلس الأمن دور كبير في العمل كمنتدى لتبادل المعلومات حول التهديدات السيبرانية الحالية والمستقبلية، فضلاً عن زيادة الوعي بالآثار الاستراتيجية للأمن السيبراني، وهو ما سبق أن أكدت عليه إستونيا خلال فترة عضويتها في مجلس الأمن.

في الختام، ولهذا السبب تشيد إستونيا بجمهورية كوريا لعقدها المناقشة الحالية في القاعة، حيث مكانها المستحق. ستكون المناقشات المفتوحة حول الأمن السيبراني كهذه المناقشات ضرورية لدعم تعزيز

القدرة على الصمود في المجال السيبراني على الصعد المحلية والإقليمية والعالمية من خلال المساهمة في منع نشوب النزاعات في المجال السيبراني والتخفيف من حدتها.

الرئيس (*تكلم بالإنكليزية*): أعطي الكلمة الآن لممثل تشيكيا.

السيد كولهانيك (تشيكيا) (*تكلم بالإنكليزية*): أود أولا أن أشكر جمهورية كوريا على تنظيم هذه المناقشة المفتوحة البالغة الأهمية. نرحب بمناقشة اليوم حول دور مجلس الأمن في مجال الأمن السيبراني، لا سيما فيما يتعلق بتنفيذ الإطار المتفق عليه لسلوك الدول المسؤول في الفضاء السيبراني.

وغني عن القول إننا نتشاطر العديد من الشواغل والتحذيرات التي تم الإعراب عنها هنا اليوم. نحن قلقون بشكل خاص من الهجمات على البنية التحتية الحيوية، والتجسس الإلكتروني، وهجمات برمجيات انتزاع الفدية ضد المؤسسات العامة والخاصة على حد سواء، بما في ذلك قطاع الرعاية الصحية، وسرقات العملات المشفرة والجهود المبذولة لتحقيق اختراق الأنظمة الصناعية الحيوية، ليس من أجل التجسس وسرقة حقوق الملكية الفكرية فحسب، ولكن أيضًا بهدف التمكن من السيطرة عليها بطريقة عدائية علنية. إن الاستخدام المتزايد لتكنولوجيا المعلومات والاتصالات في النزاعات المسلحة وآثارها الضارة على المدنيين أمر مثير للقلق. إن هذه الأعمال غير المسؤولة تعرض السلم والأمن الدوليين للخطر، وهما ما تقع المسؤولية عنهما على عاتق مجلس الأمن. وبالمثل، يستخدم الفضاء الإلكتروني بشكل متزايد لنشر المعلومات المضللة، ومفاقمة النزاعات الاجتماعية القائمة، بل والتحريض على الأعمال الإرهابية. وينبغي للمجلس، إلى جانب منتديات الأمم المتحدة ذات الصلة وغيرها من المنظمات الدولية التي تتناول جدول أعمال الفضاء الإلكتروني، أن يكثف جهوده لإيجاد سبل فعالة للتصدي لتلك الأنشطة الخبيثة الأقل وضوحاً في الفضاء الإلكتروني. كما ينبغي له أن يعمل على زيادة الوعي بالحجم الحقيقي لتلك التهديدات وتيسير الأنشطة التي تعزز قدرة أكبر على الصمود.

في أيار/مايو، أدانت تشيكيا علنًا، بالتنسيق مع ألمانيا ودول أخرى، أنشطة الجهة الفاعلة التي تسيطر عليها الدولة الروسية APT28، التي كانت تقوم بحملة تجسس سيبراني طويلة الأمد في البلدان الأوروبية وتستهدف مؤسسات الحكومة التشيكية. هذه الأنشطة تنتهك معايير الأمم المتحدة لسلوك الدول المسؤول في الفضاء الإلكتروني. سنواصل التصدي لهذه الأنشطة بقوة، بالتعاون مع شركائنا ووفقاً لالتزاماتنا الدولية.

تؤيد تشيكيا تأييدًا تامًا نظامًا دوليًا قائمًا على القانون الدولي يعزز بيئة مفتوحة وآمنة ومستقرة ويمكن الوصول إليها وسلمية لتكنولوجيا المعلومات والاتصالات. ونكرر دعمنا لإنشاء آلية دائمة أحادية المسار وشمولية وعملية المنحى تحت رعاية الأمم المتحدة ولاختتام أعمال الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها في عام 2025. ونعتقد أن برنامج عمل للارتقاء بسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي يمكن أن يكون بمثابة آلية من هذا القبيل.

أخيراً، أود أن أؤكد مجددًا أن بلدي لا يزال ملتزمًا بأن يكون مشاركًا نشطًا في ما يجب أن يكون شراكة عالمية حقيقية للتصدي لتهديدات الأمن السيبراني اليوم وغدًا. في الواقع، سيتطلب الأمر اتباع نهج قائم على تكاتف الجميع. ونحن منخرطون بالفعل في مناقشات مفصلة مع عدد من البلدان في أفريقيا ومنطقة المحيطين الهندي والهادئ وأمريكا اللاتينية لتحديد مشهد التهديدات المتغير وتعزيز استجابتنا المشتركة. على سبيل المثال، نظمت تشيكيا في نهاية نيسان/أبريل حلقة دراسية في بوغوتا حول التحديات الحالية في مجال الأنشطة الإجرامية في الفضاء الإلكتروني. كنا ممتنين لحضور خبراء من إكوادور، بنما، الجمهورية الدومينيكية، السلفادور، غواتيمالا، كوستاريكا، كولومبيا، وهندوراس ومشاركتنا رؤاهم القيمة.

أشكركم مرة أخرى، سيدي الرئيس، على إتاحة الفرصة لي لتشاطر وجهات نظر بلدي حول هذا الموضوع المهم.

الرئيس (*تكلم بالإنكليزية*): أعطي الكلمة الآن للسيدة سامسون.

السيدة سامسون (*تكلمت بالإنكليزية*): يشرفني أن أتكلم باسم الاتحاد الأوروبي ودوله الأعضاء. تؤيد هذا البيان البلدان المرشحة

للانضمام وهي مقدونيا الشمالية والجبل الأسود وألبانيا وأوكرانيا وجمهورية مولدوفا والبوسنة والهرسك وجورجيا وكذلك أندورا.

أشكركم، سيدي الرئيس، على تنظيم هذه المناقشة المفتوحة رفيعة المستوى. يرحب الاتحاد الأوروبي بمناقشة اليوم لتبادل وجهات النظر حول مشهد التهديدات المتغيرة في الفضاء الإلكتروني وآثارها على صون السلم والأمن الدوليين.

وقد اشتملت البيانات التي ألقيت للتو على مجموعة واسعة من التهديدات الناشئة والمتغيرة، بدءاً من هجمات الحرمان من الخدمة منخفضة التأثير إلى العمليات الواسعة النطاق في الفضاء الإلكتروني والهجمات على البنية التحتية الحيوية. ونضيف إلى تلك الشواغل التأثير المحتمل عبر الحدود الذي يمكن أن ينشأ عن النشاط الخبيث في الفضاء الإلكتروني. كما نشير إلى عدم وضوح الخطوط الفاصلة بين الأنشطة الإجرامية والهجمات التي ترعاها الدول باستخدام مجرمي الإنترنت المأجورين، مما يجعل مهمة الإسناد الصعبة أصلاً أكثر صعوبة. علينا الالتزام بشكل مشترك بتعزيز مجموعة أدواتنا من أجل القدرة الجماعية على الصمود، ونرحب بتشاطر الوفود الأخرى لرؤاها وتجاربها.

يشعر الاتحاد الأوروبي ودوله الأعضاء بالقلق إزاء عدد الأنشطة الخبيثة في الفضاء الإلكتروني التي تستهدف المؤسسات الحكومية، والعمليات الديمقراطية ومدى تطورها ونطاقها. في الشهر الماضي، شاركت ألمانيا تقييمها بأن مجموعة التجسس الإلكتروني APT28 المرتبطة بروسيا قد اخترقت حسابات البريد الإلكتروني للحزب الاشتراكي الديمقراطي الألماني. لقد استهدفت من قبل نفس جهة التهديد المؤسسات والوكالات والكيانات الحكومية في الدول الأعضاء في الاتحاد الأوروبي، بما في ذلك في تشيكيا وبولندا وليتوانيا وسلوفاكيا والسويد. يجب أن تتوقف هذه الأنشطة الخبيثة.

إن معايير الأمم المتحدة لسلوك الدول المسؤول في الفضاء الإلكتروني توفر التوجيه في هذا الصدد. الالتزامات الرئيسية واضحة ومباشرة: ينطبق القانون الدولي في الفضاء الإلكتروني؛ يتوقع من الدول التقيد بالقواعد الطوعية لسلوك الدول؛ يجب على الدول منع إساءة استخدام الإنترنت على أراضيها؛ هناك حاجة إلى تدابير عملية لبناء الثقة للمساعدة في الحد من مخاطر التصعيد والنزاع الناجمة عن حوادث اختراق نظم الفضاء الإلكتروني. بالنسبة للاتحاد الأوروبي، فإن التركيز على تطوير وتنفيذ الإطار المتفق عليه لسلوك الدول المسؤول في الفضاء الإلكتروني أمر بالغ الأهمية إذا أردنا الوفاء بمسؤوليتنا المشتركة بما يتماشى مع مصلحتنا المشتركة وحماية جميع الدول من مخاطر النشاط الضار في الفضاء الإلكتروني. ويمكن للدول إحراز تقدم ملموس من خلال توضيح انطباق القانون الدولي القائم ومناقشة تطبيق معايير السلوك المسؤول القائمة والالتزام بها. ولكي يكون الإطار المتفق عليه لسلوك الدول المسؤول فعالاً، يجب أن نتقيد به معاً. وهذا يعزز أهمية إنشاء آلية دائمة وشمولية وعملية المنحى تحت رعاية الأمم المتحدة. ولذلك فإننا نؤيد وضع برنامج عمل للارتقاء بسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي، ونأمل أن نتفق على طرائق العمل هذا الصيف.

ونحن نتطلع إلى مواصلة النهوض بالمناقشات حول هذا الموضوع المهم، ونرحب بجهود من هذا القبيل تهدف إلى تسليط الضوء على الدور المهم لمجلس الأمن في الوفاء بولايته كما حددها ميثاق الأمم المتحدة المتمثلة في التصدي للتهديدات التي يتعرض لها السلم والأمن الدوليين من خلال تسليط الضوء على التهديدات الدولية الفريدة والمحددة الناشئة في مجال الفضاء السيبراني. ونود أيضا أن نواصل استكشاف الكيفية التي يمكن بها لعمل المجلس في المستقبل أن يكمل بفعالية عمليات الأمم المتحدة الأخرى ذات الصلة في هذا الصدد.

الرئيس (*تكلم بالإنكليزية*): أعطي الكلمة الآن لممثل الفلبين.

السيد لاغداميو (الفلبين) (*تكلم بالإنكليزية*): تغتنم الفلبين هذه الفرصة لتعيد التأكيد على الأهمية الحاسمة للتصدي لتهديدات تكنولوجيا المعلومات والاتصالات التي تواجه الأمن الدولي. إن التقدم السريع للتقنيات الرقمية يفرض تحديات جديدة تتطلب إجراءات فورية ومتضافرة. وفي ذلك الصدد، نود أن نسلط الضوء على ثلاث نقاط رئيسية: الاتجاهات في تهديدات تكنولوجيا المعلومات والاتصالات وتأثير التهديدات السيبرانية على السلم والأمن الدوليين والهجمات السيبرانية كمضاعف للتهديدات.

أولاً، فيما يتعلق بالاتجاهات السائدة في تهديدات تكنولوجيا المعلومات والاتصالات، فإن ظهور المكالمات الآلية المدعومة بالذكاء الاصطناعي التي تُستخدم في الاحتيال وانتشار عمليات التزييف العميق والمعلومات المغلوطة وهجمات برامج الفدية الخبيثة تمثل مخاطر كبيرة وتحديات معقدة. فالاستراتيجيات الشاملة ضرورية لمواجهة تلك التهديدات المتطورة. ويشكل الاستخدام الخبيث للذكاء الاصطناعي في الفضاء الإلكتروني مخاطر جسيمة. فيجب علينا إيلاء الأولوية لتقييم تلك التهديدات لوضع سياسات قوية للأمن السيبراني وضمان النشر الآمن لتقنيات الذكاء الاصطناعي.

ثانياً، فيما يتعلق بتأثير التهديدات السيبرانية على الأمن والسلم الوطنيين، فقد اختبرت الفلبين بشكل مباشر التأثير المدمر للهجمات السيبرانية على الأمن القومي والثقة العامة. وتسلط الحوادث الأخيرة، مثل تشويه المواقع الإلكترونية الحكومية وخروقات البيانات التي استهدفت مؤسسات حيوية وسرقة المعلومات الشخصية على نطاق واسع، الضوء على الحاجة الملحة لتعزيز تدابير الأمن السيبراني. ويمكن للهجمات الإلكترونية أن تعطل الخدمات الأساسية، وتقوض الثقة في المؤسسات، وتتسبب في عواقب اجتماعية واقتصادية بعيدة المدى. كما يساورنا قلق بالغ إزاء أنشطة تكنولوجيا المعلومات والاتصالات الخبيثة التي تهدف إلى التدخل في الشؤون الداخلية للدول. إننا نشهد زيادة في الاستخدام الخبيث للحملات الإعلامية الخفية التي تتيحها تكنولوجيا المعلومات والاتصالات للتأثير على العمليات والأنظمة والاستقرار العام للدول الأخرى. فتلك الاستخدامات تقوض الثقة، ومن المحتمل أن تكون تصعيدية ويمكن أن تهدد السلم والأمن الدوليين. ومن الاعتبارات الأخرى المثيرة للقلق توافر تلك القدرات المتطورة في مجال تكنولوجيا المعلومات والاتصالات للجهات الفاعلة من غير الدول وقدرتها على استخدام تلك التكنولوجيات بشكل خبيث لتحقيق مكاسب تجارية والتهرب من المسؤولية.

ثالثاً، فيما يتعلق بالأثر المضاعف للتهديدات الناجمة عن الهجمات السيبرانية، فإن الأنشطة الإجرامية في الفضاء السيبراني تفاقم التحديات القائمة التي تواجه السلم والأمن الدوليين. وقد شهدت الفلبين كيف يمكن للهجمات السيبرانية أن تكون بمثابة مضاعفات تهديد كبيرة، ما يعقد جهود الحفاظ على السلام والاستقرار. إن طبيعة الفضاء الإلكتروني العابرة للحدود الوطنية تعني أنه لا توجد دولة محصنة، وأن أمننا الجماعي لا يكون قوياً إلا بقدر قوة أضعف حلقاته. ونظراً للمخاطر الجسيمة التي تشكلها التهديدات السيبرانية، تشدد الفلبين على الدور المحوري لمجلس الأمن في التصدي لتلك التهديدات. وعلى الرغم من أن المناقشات الجارية في الفريق العامل المفتوح باب العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات واستخدامها ذات قيمة، من الضروري كذلك أن يواصل مجلس الأمن مشاركته في تشكيل البرنامج العالمي للأمن السيبراني.

وفي ذلك الصدد، تؤيد الفلبين اتخاذ المجلس التدابير الجماعية التالية لمواجهة التهديدات السيبرانية، على النحو الذي أثير خلال اجتماع صيغة آريا بشأن الأمن السيبراني الذي عقد في نيسان/أبريل: أولاً، تعزيز الإطار المعياري المتفق عليه للسلوك المسؤول للدول في الفضاء السيبراني؛ ثانياً، عقد اجتماع سنوي لمناقشة واستعراض مشهد تهديدات تكنولوجيا المعلومات والاتصالات واستعراضها، وفي ذلك الصدد، الطلب من الأمين العام إعداد تقرير سنوي عن الاتجاهات السائدة لإثراء مناقشات الدول الأعضاء؛ وثالثاً، الريادة في جمع المعلومات أو دراسة تهديدات أو حوادث محددة لتوجيه الدول الأعضاء والرجوع إليها.

وتعيد الفلبين تأكيد التزامها بتعزيز المرونة السيبرانية وتعزيز السلوك المسؤول في الفضاء السيبراني. وندعو إلى مواصلة التعاون وجهود بناء القدرات وآليات الدعم، بما في ذلك إنشاء صندوق استئماني منتظم لمساعدة البلدان النامية في التصدي للتهديدات السيبرانية. إننا نعتمد على الشراكات وعمليات نقل التكنولوجيا لمساعدتنا في تضييق الفجوة الرقمية وتعزيز دفاعاتنا الإلكترونية.

الرئيس (*تكلم بالإنكليزية*): أعطي الكلمة الآن لممثل إندونيسيا.

السيد ناصر (إندونيسيا) (*تكلم بالإنكليزية*): تشكر إندونيسيا جمهورية كوريا على عقد هذه الجلسة الهامة. كما نشكر الأمين العام ومقدمي الإحاطتين على عروضهم.

أصبحت التهديدات في الفضاء الإلكتروني خطراً حقيقياً وقائماً يتهدد السلام والأمن الوطنيين والدوليين. إننا نتعرض بشكل متزايد

لتهديدات جديدة من التقنيات الجديدة وسريعة التطور. ولا يمكن للمجتمع الدولي تعزيز القدرة على الصمود في الفضاء الإلكتروني والتخفيف من تلك المخاطر بفعالية إلا من خلال استجابة منسقة وأطر قانونية قوية.

وفي ذلك السياق، أود أن أسلط الضوء على النقاط التالية.

أولاً، يجب علينا إيلاء الأولوية للتخفيف من التكلفة البشرية للهجمات السيبرانية التي تستهدف البنية التحتية الحيوية. ويجب علينا أن نكفل أن يحمى الفضاء السيبراني كمجال خالٍ من النزاعات وليس كساحة للنزاع. ولئن كانت التطورات في مجال الذكاء الاصطناعي – بما في ذلك الذكاء الاصطناعي التوليدي والتعلم الآلي – يمكن أن تفيد الجنس البشري، فإنها يمكن أن تكون مدمرة أيضًا وتسهل الهجمات السيبرانية، مع تأثير سلبي كبير على سكان العالم. ولذلك من الضروري حماية البنية التحتية الحيوية في إطار جهودنا الرامية إلى منع وقوع ضرر كبير من قبل الجهات السيبرانية الخبيثة والدول غير المسؤولة.

ثانياً، من الضروري تحقيق التآزر والاتساق داخل منظومة الأمم المتحدة في مجالات الأمن السيبراني وتكنولوجيا المعلومات والاتصالات والسلام والأمن الدوليين. ولئن كانت لدى مجلس الأمن ولاية هامة للحفاظ على السلم والأمن الدوليين، فإن لدى هيئات الأمم المتحدة الأخرى ولايات لا تقل أهمية للعمل على مسائل الأمن الرقمي وأمن تكنولوجيا المعلومات والاتصالات والأمن السيبراني. ومن المهم أن يضع مجلس الأمن معايير وآليات تساعده على تعزيز التعاون والتآزر، الأمر الذي يؤدي إلى فهم أفضل للمخاطر التي تشكلها التهديدات السيبرانية على السلم والأمن الدوليين. ومن ثم، تعيد إندونيسيا تأكيد التزامها بعمل الفريق العامل المفتوح باب العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات واستخدامها والعمليات الأخرى التي يجري الاضطلاع بها في هذا المجال، بما في ذلك عملية مؤتمر قمة المستقبل.

ثالثاً، يجب علينا تعزيز الأمن السيبراني العالمي من خلال تعزيز التعاون الإقليمي. إن التعاون مع المنظمات الإقليمية ضروري، حيث أنها تضطلع بدور هام في الإسهام في نهج قوي وشامل للأمن السيبراني. وفي منطقتنا، اضطلعت رابطة دول جنوب شرق آسيا بدور فعال في إنشاء أطر ومبادرات، بما في ذلك من خلال المنتدى الإقليمي لرابطة دول جنوب شرق آسيا، لتعزيز القدرة الإقليمية على مواجهة التهديدات السيبرانية. إن الاستفادة من تلك الخبرات من المنظمات الإقليمية يمكن أن توفر بالفعل رؤى قيمة وتعزز الجهود الدولية الأكثر شمولية.

وأخيراً، يجب علينا سد الفجوة التكنولوجية لتحسين المنعة السيبرانية. وتشكل فجوة القدرات في مجال الأمن السيبراني تحدياً خطيراً للبلدان النامية، ما يجعلها عرضة للتهديدات المتصاعدة ويقوض استقرارها. إن التدابير التعاونية على جميع المستويات، بما في ذلك مع أصحاب المصلحة المعنيين في القطاع الخاص، ضرورية لتعزيز الاستقرار في الفضاء الإلكتروني، لا سيما من خلال بناء القدرات والمساعدة التقنية ونقل التكنولوجيا. ولن نتمكن من إنشاء فضاء إلكتروني آمن يعزز السلام والاستقرار العالميين إلا بتوحيد الجهود.

الرئيس (*تكلم بالإنكليزية*): أعطي الكلمة الآن لممثل سنغافورة.

السيد سيه (سنغافورة) (*تكلم بالإنكليزية*): نشكر جمهورية كوريا على عقد اجتماع اليوم بشأن هذه المسألة الهامة.

منذ المناقشة المفتوحة الأولى لمجلس الأمن بشأن الأمن السيبراني، التي جرت في حزيران/يونيه 2021 (انظر S/2021/621)، استمر مشهد التهديدات السيبرانية في التطور بوتيرة مقلقة. وعلى تلك الخلفية، فإن التعاون الدولي في الأمم المتحدة أمر حيوي ولا غنى عنه لمكافحة الطبيعة العالمية والعابرة للحدود للتهديدات السيبرانية. وفي ذلك الصدد، من الضروري أن تعمل الجمعية العامة ومجلس الأمن معا على تعزيز الالتزام بالإطار المعياري لسلوك الدول المسؤول، القائم على تطبيق القانون الدولي واحترام مبادئ ميثاق الأمم المتحدة. وظلت سنغافورة دائمًا، باعتبارها دولة صغيرة، تدعم نظامًا متعدد الأطراف قائمًا على سيادة القانون. ولا يختلف نهجنا عن ذلك عندما يتعلق الأمر بالأمن السيبراني، وهو أمر ذو أهمية حيوية للعديد من الدول الصغيرة والنامية. وتؤمن سنغافورة إيماناً راسخاً بأهمية الأمم المتحدة

كمنبر رئيسي لمناقشة وضع وتنفيذ قواعد ومعايير ومبادئ سلوك الدول المسؤول التي تحكم الفضاء الإلكتروني.

وتشرفت سنغافورة بتوليها رئاسة الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها منذ عام 2021. ويستند الفريق العامل المفتوح العضوية في عمله إلى أكثر من عقدين من العمل في الأمم المتحدة، الأمر الذي أفضى إلى إنشاء إطار ذي طابع تراكمي ومتطور لسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات صدقت عليه كافة الدول الأعضاء. ومن المشجع أن نلاحظ أن الفريق العامل المفتوح العضوية أحرز تقدماً جيداً على مدى السنوات الثلاث الماضية في زيادة تعزيز الإطار المعياري لسلوك الدول المسؤول في الفضاء الإلكتروني.

كما شكل الفريق العامل المفتوح العضوية في حد ذاته تدبيرا قيما لبناء الثقة. وبالإضافة إلى التفاهمات المشتركة التي تم التوصل إليها في التقريرين المرحليين السنويين للفريق العامل المفتوح العضوية اللذين تم الاتفاق عليهما بتوافق الآراء في تموز/يوليو 2022 (انظر A/77/275) وتموز/يوليو 2023 (انظر A/78/265) على التوالي، قاد الفريق العامل المفتوح العضوية عملية وضع وتفعيل مبادرات ملموسة عملية المنحى لها دور مهم في تعزيز السلم والأمن الدوليين في الفضاء الإلكتروني، وعلى الأخص في شكل الدليل العالمي لجهات الاتصال، الذي تم إطلاقه رسمياً في 9 أيار/مايو. وفي شهر أيار/مايو أيضاً، عقد الفريق العامل المفتوح العضوية اجتماعاً ناجحاً وموضوعياً على المستوى الوزاري بشأن بناء القدرات في مجال أمن تكنولوجيا المعلومات والاتصالات. والرسالة الرئيسية المنبثقة من ذلك الاجتماع كانت الحاجة الماسة إلى بناء القدرات لمساعدة العديد من البلدان الصغيرة والنامية على تحقيق القدرة على الصمود في الفضاء الإلكتروني. وعلى نفس القدر من الأهمية، كان هناك اعتراف واسع النطاق بأن بناء القدرات يمكن أن يشكل وسيلة مهمة لبناء الثقة بين الدول.

لقد سألتم، السيد الرئيس، في أسئلتكم التوجيهية، عن كيفية ترابط التهديدات في مجال الفضاء الإلكتروني مع البنود الأخرى المدرجة على جدول أعمال مجلس الأمن والدور المحدد الذي يمكن أن يضطلع به مجلس الأمن في التصدي لتحديات السلام والأمن الدوليين الناشئة من الفضاء الإلكتروني. وبالنظر إلى العمل الجاري في الجمعية العامة، من المهم أن يتجنب مجلس الأمن تكرار العمل الذي يجري بالفعل في عمليات أخرى. ومع ذلك، يجب أن ندرك في الوقت نفسه أن مجلس الأمن لديه ولاية واضحة لمناقشة المسائل المتعلقة بصون السلم والأمن الدوليين. ولا يمكننا أن نستبعد إمكانية أن تتسبب محاولة خرق نظام المعلوماتية في الفضاء الإلكتروني في سوء تفاهم بين الدول وتؤدي إلى تصعيد بل وربما إلى نشوب نزاع، وبالتالي تشكل واقعة تتعلق بالسلم والأمن الدوليين. لذلك لا يمكننا استبعاد دور لمجلس الأمن كجزء من مسؤوليته التي أناطها به الميثاق عن صون السلم والأمن الدوليين.

وعليه ينبغي للمجلس أن يتبنى نظرة شمولية لما يشكل تهديدات للسلم والأمن الدوليين وأن يعمل مع إدراك أن التهديدات في الفضاء الإلكتروني يمكن أن تكون لها عواقب مادية وحقيقية. وفي ذلك الصدد، نحن منفتحون على فكرة استمرار مجلس الأمن في عقد مناقشات مفتوحة مثل مناقشة اليوم كسبيل لتبادل المعلومات وتعزيز التفاهم بين الدول الأعضاء. ويمكن للمناقشات المنعقدة في المجلس أن تساعد في إثراء عمل الجمعية العامة، بما في ذلك في مجالات بناء القدرات وبناء الثقة، وأن تساعد كذلك في تعزيز إطار سلوك الدول المسؤول، بما في ذلك النظر في أفضل السبل لتطبيق القواعد والمعايير والمبادئ على التهديدات القائمة والمحتملة في الفضاء الإلكتروني.

وأود أن أختتم بالتأكيد على الحاجة إلى مزيد من التعاون الدولي من أجل تعزيز قدرتنا الجماعية على الصمود في الفضاء الإلكتروني. إن تعزيز تعاون أكبر بين مجلس الأمن والجمعية العامة بشأن مسائل السلم والأمن الدوليين والعمل معاً بطريقة مستمرة وكلية ومتآزرة سيمكن المجتمع الدولي من صون السلم والأمن الدوليين في مجال الفضاء الإلكتروني بشكل أفضل. وسنغافورة على استعداد للعمل مع جميع الدول الأعضاء لتحقيق هذا الهدف.

الرئيس (*تكلم بالإنكليزية*): أعطي الكلمة الآن لممثلة كوستاريكا.

السيدة تشان فالفيردي (كوستاريكا) (*تكلمت بالإسبانية*): أشكر جمهورية كوريا على عقد هذه المناقشة المفتوحة.

قبل عامين، وقعت كوستاريكا ضحية لهجمات برمجيات انتزاع الفدية على نطاق واسع. وما زلنا نعاني من التأثير الناجم عن الاضطرابات التي لحقت بنظام الرعاية الصحية وقطاع الضمان الاجتماعي والقطاع المالي وغيرها من القطاعات الحيوية.

وفي هذا الصدد، تود كوستاريكا أن تدلي اليوم بثلاث نقاط.

أولاً، تؤمن كوستاريكا إيماناً راسخاً بضرورة توسيع نطاق الخطة المتعلقة بحماية المدنيين لتشمل الأنشطة في الفضاء الإلكتروني التي تؤثر على السكان المدنيين أثناء النزاعات المسلحة. ويجب على الدول أن تنضم إلى الإجماع المتزايد بأن البيانات المدنية تتمتع بالحماية نفسها بموجب القانون الدولي الإنساني شأنها شأن جميع الأعيان المدنية الأخرى، وأن عمليات الاختراق في الفضاء الإلكتروني التي تعطل أو تعرقل تشغيل الأنظمة المدنية محظورة بموجب القانون الدولي الإنساني. كما يجب على الدول الامتناع عن الزج بالمدنيين في الأنشطة العسكرية في الفضاء الإلكتروني، لأن ذلك قد يعرضهم للخطر.

ثانياً، تعتقد كوستاريكا أن الوقت قد حان لتحديث الخطة المتعلقة بالمرأة والسلام والأمن لمعالجة السلامة الرقمية للنساء. وتدعو كوستاريكا أعضاء مجلس الأمن إلى النظر في اعتماد مشروع قرار جديد ينص على تدابير لحماية النساء والفتيات من العنف والإيذاء والاستغلال على الإنترنت، لا سيما في حالات النزاع وما بعد النزاع. كما يجب أيضاً دمج اعتبارات السلامة الرقمية بشكل منهجي في جميع الولايات والأهداف والمبادرات الجديدة المتعلقة بتلك الخطة.

ثالثاً، جميع الدول، سواء كانت أعضاء في المجلس أم لا، مسؤولة عن تعزيز سيادة القانون الدولي في الفضاء الإلكتروني. وتفخر كوستاريكا بأنها عضو في مجموعة متنامية من الدول التي أعلنت مواقف وطنية بشأن تطبيق القانون الدولي في الفضاء الإلكتروني. وتستند أوراق الموقف هذه إلى التوافق العالمي في الآراء على أن القانون الدولي، بما في ذلك القانون الدولي الإنساني والقانون الدولي لحقوق الإنسان، ينطبق على استخدام الدول لتكنولوجيا المعلومات والاتصالات وضروري لصون السلام والاستقرار. ونحن نشجع الدول الأخرى على وضع أوراق مواقف من هذا القبيل، ونشيد بمصادر بناء القدرات القانونية القائمة، مثل مجموعة أدوات قانون الفضاء الإلكتروني، التي يمكن أن تسترشد بها الجهود في هذا المجال.

ومع زيادة تعرض مجتمعاتنا للتهديدات في المجال الرقمي وفي الفضاء الإلكتروني، تحث كوستاريكا المجلس على إدراج هذه الشواغل في أعماله والقيام بذلك بطريقة تعزز احترام القانون الدولي في أوقات السلم والنزاع المسلح على حد سواء.

الرئيس (*تكلم بالإنكليزية*): لا يزال هناك عدد من المتكلمين في قائمتي لهذه الجلسة. أعتزم، بموافقة أعضاء المجلس، تعليق الجلسة حتى الساعة 15/00.

عُلقت الجلسة الساعة 13/10.