مجلس الأمن

السنة التاسعة والسبعون

مؤقت

الجلسة 9662

الخميس، 20 حزيران/يونيه 2024، الساعة 15/00

نيويورك

الرئيس	السيد هيونوو تشو	(جمهورية كوريا)
الأعضاء:	الاتحاد الروسي	السيد ديرغاتشيف
	إكوادور	السيد دوران مدينة
	الجزائر	السيد الوافي
	سلوفينيا	السيد بوركيليتش
	سويسرا	السيد ستريت
	سيراليون	السيد شينكس
	الصين	السيد وانغ جن جيانغ
	غيانا	السيدة بارماناند
	فرنسا	السيد سترينانو
	مالطة	السيد سيسكالدي
	المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية	السيدة بيدج
	موزامبيق	السيد إراتشاندي غوفيا
	الولايات المتحدة الأمريكية	السيدة وو
	اليابان	السيد سوزوكي

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)

يتضمن هذا المحضر نص الخطب والبيانات الملقاة بالعربية وترجمة الخطب والبيانات الملقاة باللغات الأخرى. وسيطبع النص النهائي في الوثائق الرسمية لمجلس الأمن. وينبغي ألا تُقدم التصويبات إلا للنص باللغات الأصلية. وينبغي إدخالها على نسخة من المحضر وإرسالها بتوقيع أحد أعضاء الوفد المعني إلى: Chief of the Verbatim Reporting Service, Room AB-0928 (verbatimrecords@un.org). وسيعاد إصدار المحاضر المصوَّبة إلكترونيا في نظام الوثائق الرسمية للأمم المتحدة (http://documents.un.org).

استُؤنِفت الجلسة الساعة 15/05.

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

أعطي الكلمة الآن لممثل كوبا.

السيد غالا لوبيز (كوبا) (*تكلم بالإسبانية*): من الأهمية بمكان الحفاظ على استخدام تكنولوجيا المعلومات والاتصالات للأغراض السلمية حصرا لتعزيز أواصر التعاون فيما بين الشعوب والنهوض بها.

وتؤكد كوبا معارضتها الشديدة لعسكرة الفضاء الإلكتروني وترفض بشدة أي استخدام لتكنولوجيا المعلومات والاتصالات كأدوات للتهديد باستخدام القوة أو استخدامها أو في أفعال تهدف إلى التدخل في الشؤون الداخلية للدول. ولا تنطبق المادة 51 من ميثاق الأمم المتحدة في سياق الفضاء الإلكتروني ولا يمكن الاحتجاج بها في هذا الإطار. لذلك من المثير للقلق أن تعمد بعض الدول إلى إدراج استخدام الأسلحة الإلكترونية وإمكانية شن هجمات في الفضاء الإكتروني في استراتيجيات أمنها القومي بدعوى ردع الخصوم.

ويتعين اتخاذ جميع التدابير اللازمة للحيلولة دون إساءة استخدام تكنولوجيات المعلومات والاتصالات والمنصات الإعلامية، بما في ذلك شبكات التواصل الاجتماعي والبث الإذاعي والإلكتروني، كأدوات للترويج لخطاب الكراهية، والتحريض على العنف، والتخريب، وزعزعة الاستقرار، ونشر الأخبار الكاذبة وتشويه واقع الدول لمآرب تخريبية وبهدف التدخل في شؤونها، في انتهاك للقانون الدولي. كما أن الاستخدام السري وغير القانوني لأنظمة تكنولوجيات المعلومات والاتصالات التابعة للدول من قبل الأفراد والمنظمات والدول لتنفيذ هجمات إلكترونية ضد بلدان ثالثة أمر مرفوض.

وتدعو كوبا إلى التفاوض، في إطار الأمم المتحدة، بشأن صك دولي ملزم قانونا واعتماده في أقرب وقت ممكن لسد الثغرات القانونية الكبيرة في مجال أمن الفضاء الإلكتروني والتصدي بفعالية للتحديات والتهديدات المتزايدة في هذا المجال، بما في ذلك من خلال التعاون الدولي. وهناك حاجة إلى تجاوز الفجوة التكنولوجية الهائلة وتذليل العقبات التي تواجه البلدان النامية من أجل الاستثمار في أمن بنيتها التحتية في مجال تكنولوجيا المعلومات والاتصالات والتي تقيد قدرات تلك البلدان على التصدي للمخاطر المحدقة.

إن الفريق العامل المفتوح باب العضوية المعني بأمن واستخدام تكنولوجيات المعلومات والاتصالات المكلف بتفويض من اللجنة الأولى للجمعية العامة هو المنبر الأمثل لعمليات تبادل الآراء والتوصل إلى إجماع بشأن التهديدات والتحديات التي نواجهها كدول وتتضمن الاستخدام الخبيث لتكنولوجيات المعلومات والاتصالات. والفريق منتدى جامع وديمقراطي ونزيه يتيح لكل الدول الأعضاء المساهمة بالتساوي في إيجاد حلول قائمة على التوافق في هذا المجال.

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

السيدة سلمان (البحرين): بداية، يطيب لي أن أرحب بترؤس معالي السيد شو تايول وزير خارجية جمهورية كورية جلسة المناقشة المفتوحة اليوم، وأن أتقدم بالشكر إلى الوفد الدائم لجمهورية كوريا لدى الأمم المتحدة على عقد هذه الجلسة حول موضوع يكتسي أهمية متزايدة في ظل التطورات الهائلة في الفضاء السيبراني. كما أود أن أتوجه بالشكر إلى معالي السيد أنطونيو غوتيريش الأمين العام للأمم المتحدة وباقي مقدمي الإحاطات على ما تفضلوا به من بيانات قيمة.

إن المخاطر المتصاعدة التي تشكلها الأنشطة الخبيثة في الفضاء السيبراني، مثل هجمات برامج انتزاع الفدية وسرقة العملات المشفرة وسرقة المعلومات والأصول الحساسة لا تؤدي فقط إلى تعريض سلامة البنية التحتية الحيوية للخطر، بل وتؤدي أيضا إلى تفاقم التحديات القائمة التي تواجه الاستقرار العالمي؛ حيث تعمل هذه الأنشطة كمضاعفات قوية للتهديدات مما يؤدي إلى تضخيم المخاوف الأمنية التقليدية ونشوء نقاط ضعف جديدة؛ علاوة على أن الطبيعة المترابطة للأنظمة الرقمية تعني أن الحوادث السيبرانية يمكن أن تتصاعد بسرعة إلى أزمات دولية، مما يقوض الثقة والاستقرار بين الدول.

ومن هذا المنطلق، تشير مملكة البحرين إلى أهمية اتباع نهج متعدد الأوجه يتضمن الاستفادة من الأدوات والمنصات والأطر والاستراتيجيات الحالية والمبتكرة للتخفيف من المخاطر المرتبطة بالتهديدات السيبرانية، إلى جانب إشراك جميع أصحاب المصلحة، بالنظر إلى أن الأدوات والتقنيات السيبرانية لم تعد مجالا ً حصريا ً للحكومات. كما تؤكد مملكة البحرين أهمية بناء القدرات وتبادل التكنولوجيات والمعرفة والممارسات الفضلى لتعزيز قدرات الدول على منع الحوادث السيبرانية والاستجابة لها.

وفي هذا السياق دعمت مملكة البحرين المبادرات المختلفة الصادرة عن الجمعية العامة للأمم المتحدة حول تعزيز التعاون في مجال الحفاظ على الأمن السيبراني، والتي تضم أفرقة الخبراء الحكوميين والفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها، وبرنامج العمل للارتقاء بسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي.

وعلى الصعيد الوطني، تولي مملكة البحرين اهتماما كبيرا بأمن الفضاء السيبراني، وتستند في ذلك على منظومة واضحة لحوكمة أمن الفضاء الإلكتروني معززة باستراتيجية وطنية شاملة، حيث تم تأسيس المركز الوطني للأمن السيبراني؛ سعيا إلى توفير فضاء إلكتروني آمن في مملكة البحرين، عن طريق وضع معايير الحوكمة الفعالة وتوفير وسائل الدفاع والمراقبة والاستجابة للهجمات الإلكترونية، فضلا عن نشر الوعي بين الأفراد والمؤسسات.

وتمتد الاستراتيجية الوطنية للأمن السيبراني لتعزيز الشراكات الإقليمية والدولية. حيث تم تحديد خمس ركائز أساسية في هذه الإستراتيجية. وتعد كل ركيزة مكونا ً أساسيا ً وضروريا لتحقيق رؤية مملكة البحرين في مجال الأمن السيبراني. وتشكل في مجملها إطار عمل شاملا ومتماسكا للحفاظ على فضاء سيبراني آمن وموثوق. وتتمثل هذه الركائز في؛ أولا، حماية سيبرانية قوية ومرنة؛ ثانيا، الحوكمة والمعايير الفعالة للأمن السيبراني؛ ثالثاً، بناء مجتمع واع بالأمن السيبراني؛ رابعا، تعزيز الحماية من خلال الشراكات والتعاون؛ وخامساً، تطوير الكوادر الوطنية.

وختاما، تتطلع مملكة البحرين إلى المزيد من الحوارات المثمرة حول الأمن السيبراني في إطار الأمم المتحدة، لا سيما مجلس الأمن نظرا للطبيعة المتسارعة للتهديدات الناشئة عن التطورات المتصلة بتكنولوجيا المعلومات والاتصالات..

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

السيد تشزيرسكي (بولندا) (*تكلم بالإنكليزية*): إن الانتشار العالمي للتكنولوجيات الرقمية، بما في ذلك تطوير وتنفيذ الحكومة الإلكترونية والإدارة الإلكترونية لموارد البنية التحتية الحيوية، يؤدي إلى تزايد الاعتماد على الفضاء الإلكتروني. ويشكل تحديات خطيرة لأمن الدول وسيادتها. ونشهد يوميا عدداً متزايداً من الأنشطة الخبيثة في الفضاء الإلكتروني تنفذها جهات من غير الدول وجهات حكومية على السواء تستهدف استقرار وأمن البلدان والمجتمعات.

لقد اعتمدت بولندا موقفاً وطنياً بشأن تطبيق القانون الدولي في الفضاء الإلكتروني كتدبير أساسي لضمان السلم والأمن الدوليين. وفي هذا الصدد، هناك نقطتان في غاية الأهمية بالنسبة لبلدي. النقطة الأولى هي أنه في ظل ظروف معينة، قد تشكل الأفعال في الفضاء الإلكتروني انتهاكًا لحظر استخدام القوة. والنقطة الثانية هي أن الهجوم الإلكتروني قد يُعتبر هجوماً مسلحاً. وبالنسبة لنا، ينطبق الحق في الدفاع عن النفس في الفضاء الإلكتروني.

ومن التحديات التي نواجهها في كثير من الأحيان إسناد المسؤولية عن الهجمات الإلكترونية. وبغض النظر عن ذلك، لن نتوانى عن متابعة جهودنا لضمان تقديم الدول المسؤولة ومجرمي الإنترنت إلى العدالة. من المهم أن ندرك أن بعض الدول، عوضًا عن مكافحة مجرمي الإنترنت العاملين من أراضيها، تتولى دعمهم وحمايتهم لتحقيق مآرب سياسية أو اقتصادية. وهي بذلك تقوض استقرار وأمن الآخرين. وتسعى إلى طمس الحدود الفاصلة بين الأطراف التي تدعمها الدول والعناصر ذات النوايا الإجرامية وتسبب التباسا لدى الكيانات المستهدفة عندما تحاول الدفاع عن نفسها ومحاسبة الجناة.

وفي الوقت نفسه، هناك فئة كبيرة من الدول التي تمتلك الإرادة السياسية لتنفيذ القانون الدولي والمعايير الطوعية، بيد أنها قد تعاني من نقص في الإمكانيات الضرورية لتحقيق ذلك. من الأهمية بمكان لمصلحتنا المشتركة أن نعمل معها بشكل وثيق لمساعدتها وتوفير بناء قدرات مدروسة وموجهة بدقة. ولن يحدث ذلك بين عشية وضحاها. لذلك، نحن بحاجة إلى منصة دائمة لمثل هذا التعاون في إطار الأمم المتحدة. وفي ذلك السياق، وتماشيًا مع البيان الذي تم الإدلاء به نيابة عن الاتحاد الأوروبي، تؤيد بولندا بقوة وضع برنامج العمل. ونشجع جميع أعضاء الأمم المتحدة على دعمه والمساهمة بفعالية في تفعيله.

إن الهجمات الإلكترونية والأنشطة الخبيثة تسعى إلى تقويض السلم والأمن الدوليين. لذلك، ندعو مجلس الأمن إلى تكثيف الجهود لوقف الأنشطة الخبيثة في الفضاء الإلكتروني ومنع ارتكابها. كما نود أن ندعو إحدى الدول الأعضاء في المجلس – أي الاتحاد الروسي – إلى احترام القانون الدولي ووقف عدوانها غير القانوني على أوكرانيا لا على الأرض فحسب بل في الفضاء الإلكتروني وضد دول الجوار.

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

السيد فيرواتا (رومانيا) (*تكلم بالإنكليزية*): أود أن أشكر جمهورية كوريا على تنظيم مناقشة بشأن هذا الموضوع المهم.

وأود أن أدلي ببعض النقاط إضافة إلى البيان الذي أدلي به نيابة عن الاتحاد الأوروبي.

إن التهديدات في الفضاء الإلكتروني مستمرة ومعقدة ومدمرة وأصبحت أكثر تواتراً. ويساور رومانيا القلق إزاء عدد الأنشطة الإلكترونية الخبيثة التي تستهدف المؤسسات الحكومية والعمليات الديمقراطية. وهذا تهديد خطير – فالعمليات السيبرانية، التي غالبًا ما تقترن بالمعلومات المضللة، قد تقوض نزاهة العمليات الديمقراطية وتنال من مرونة مجتمعاتنا الكلية.

نحن قلقون أيضًا من الهجمات الإلكتروني على البنية التحتية الحيوية والخدمات الأساسية، مع ما قد يترتب على ذلك من آثار تخريبية ومدمرة. ونحن ندين بشدة الأنشطة السيبرانية الخبيثة التي تهدف إلى تقويض مؤسساتنا الديمقراطية وأمننا القومي ومجتمعنا الحر. إن السلوك غير المسؤول في الفضاء الإلكتروني يسفر عن مخاطر تهدد السلم والأمن الدوليين ولا يمكن التهاون في ذلك. ويحق لمجلس الأمن معالجة تلك المسائل والتشجيع على تعزيز المساءلة.

إن القانون الدولي ينطبق في الفضاء الإلكتروني. وفي الفضاء الإلكتروني، يقع على عاتق الدول نفس الالتزام بالتصرف بطريقة مسؤولة، بما يتماشى مع القانون الدولي، بما في ذلك ميثاق الأمم المتحدة، ونحن نشجع مجلس الأمن على إدانة السلوكيات الضارة في الفضاء الإلكتروني. إن استخدام الدول لأي تكنولوجيات المعلومات والاتصالات، بطريقة لا تتفق مع القانون الدولي والتزاماتها بموجب إطار الأمم المتحدة لسلوك الدول المسؤول في استخدام تكنولوجيا المعلومات والاتصالات يقوض السلم والأمن الدوليين.

وتعزيز دور مجلس الأمن في التصدي للتهديدات الإلكترونية بطريقة مكملة لعمليات الأمم المتحدة الأخرى المتعلقة بتكنولوجيا المعلومات والاتصالات يأتي في الوقت المناسب وهو أمر بالغ الأهمية لصون السلم والأمن الدوليين في الفضاء الإلكتروني. وتؤكد هذه المناقشة المفتوحة والاجتماعان السابقان المعقودان بصيغة آريا في أيار/مايو 2023 ونيسان/أبريل 2024 على المساهمة المهمة التي يمكن أن يقدمها مجلس الأمن.

وتركز رومانيا بشكل كبير على الحاجة إلى تعزيز المرونة في الفضاء الإلكتروني. نحن بحاجة إلى تعزيز حماية البنية التحتية الوطنية الحيوية، حيث تحاول الجهات الفاعلة الخبيثة بقوة تعطيل عمل مجتمعاتنا. لا نزال ملتزمين بالمبادرة الدولية لمكافحة برمجيات انتزاع الفدية ونتطلع إلى تعزيزها في إطار استجابة دولية منسقة لهذه المجموعة من التهديدات. وعلاوة على ذلك، تستدعي طبيعة الفضاء السيبراني نفسها إجراء مناقشة استشرافية بشأن قدرة تكنولوجيات الذكاء الاصطناعي على زيادة حجم الهجمات السيبرانية وتعقيدها وقدرتها في الوقت نفسه على منع الهجمات السيبرانية ومواجهتها بسرعة أكبر بل والتخفيف من آثارها.

ختاماً، ندعو جميع الدول إلى احترام التزاماتها وتعهداتها الدولية بالامتثال للقانون الدولي والتصرف ضمن الإطار المتفق عليه لسلوك الدول المسؤول في الفضاء الإلكتروني. ويجب أن نبقى أوفياء بالفعل لقيمنا ومبادئنا الأساسية وأن نتصرف بطريقة مسؤولة.

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

السيد بريتهوفر (النمسا) (*تكلم بالإنكليزية*): تود النمسا أن تشكر جمهورية كوريا على عقد هذه المناقشة المفتوحة التي جاءت في الوقت المناسب.

تؤيد النمسا البيان الذي أُدلي به باسم الاتحاد الأوروبي. وأود أن أضيف النقاط التالية بصفتنا الوطنية.

للإجابة على أسئلتكم الإرشادية حول دور مجلس الأمن، سيدي الرئيس، نعتقد أن الخوض في هذا النقاش باستخدام اللغة المشتركة التي نتفق عليها جميعاً، أي القانون الدولي، يوفر وضوحاً مفاهيمياً. لقد اتفقت جميع الدول الأعضاء بتوافق الآراء على أن القانون الدولي، ولا سيما ميثاق الأمم المتحدة، ينطبق بالكامل على الأنشطة السيبرانية. والميثاق واضح: فهو يسند إلى مجلس الأمن مهمة التصدي للأخطار التي تهدد السلام والأمن الدوليين. ومن الضروري أن يواصل مجلس الأمن التصدي للأخطار المعاصرة التي تهدد السلام والأمن الدوليين من أجل الاضطلاع بولايته. ومن المهم بالقدر نفسه تسليط الضوء على دور مجلس الأمن في التسوية السلمية للمنازعات على النحو المنصوص عليه في الفصل السادس من الميثاق. ولا تتم الأنشطة السيبرانية في فضاء سيبراني افتراضي منفصل، بل في العالم الحقيقي. ولذلك، لا تشكل الأنشطة السيبرانية مجالاً جديداً يتطلب قواعدا جديدة أو تطبيقاً مختلفاً للقانون الدولي. فالمجلس في نهاية المطاف يتطرق إلى سلوك الدول. ومن المنطقي ألا يحجم المجلس عن معالجة أحد أشكال سلوك الدول – الأنشطة السيبرانية – كلما كان ذلك متصلا بولايته. وفيما يتعلق بالعقوبات على سبيل المثال، فإن جميع الأنشطة، بما في ذلك الأنشطة السيبرانية، التي تهدف إلى خرق العقوبات الملزمة التي قررها المجلس تستحق اهتمامه. وفي هذا الصدد، يكتسي إدراج الأمن السيبراني في ملفات مجلس الأمن أهمية بالغة.

وتلتزم النمسا بسيادة القانون في السياق السيبراني وخارجه على حد سواء وقد نشرت مؤخراً ورقة موقفها بشأن الأنشطة السيبرانية والقانون الدولي. وترحب النمسا بمناقشة اليوم التي تشدد على الدور الهام لمجلس الأمن في الوفاء بولايته التي حددها ميثاق الأمم المتحدة لمواجهة الأخطار التي تهدد السلام والأمن الدوليين.

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

السيد عمروف (كازاخستان) (*تكلم بالإنكليزية*): أود أن أعرب عن امتناننا لجمهورية كوريا على تنظيم جلسة اليوم الهامة جدا.

إن وتيرة الرقمنة أسرع من أي ابتكار آخر في تاريخ البشرية. ففي غضون عقدين، أحدثت التكنولوجيات الرقمية تحولاً في المجتمعات وأثرت على ما يقرب من 50 في المائة من السكان في البلدان النامية. ويمكن أن يؤدي استخدام التكنولوجيا لتحسين الاتصال والوصول إلى الخدمات المالية والتجارية والحكومية إلى الحد بشكل كبير من عدم المساواة بين السكان. ويستخدم قطاع الرعاية الصحية التكنولوجيات المتقدمة التي تعتمد على الذكاء الاصطناعي لإنقاذ الأرواح وتشخيص الأمراض وزيادة متوسط العمر المتوقع. كما أن توفر بيئات التعلم الافتراضية والتعلم عن بُعد في مجال التعليم يمكّن الطلاب من المشاركة في برامج لم يكن الوصول إليها في السابق ممكنا.

وفي الوقت نفسه، تستخدم العديد من الجهات من غير الدول، بما في ذلك الجماعات الإجرامية والإرهابيون، تكنولوجيا المعلومات والاتصالات لسرقة الهوية والاحتيال وشن هجمات إلكترونية. وتُستخدم أيضا لزرع الفتنة ونشر المعلومات المغلوطة التي يمكنها أن تزعزع استقرار الدول وتقوض الثقة بين البلدان. وقد تؤدي الأعمال الخبيثة في الفضاء السيبراني إلى تعطيل البنية التحتية الحيوية مثل الطاقة والنقل والاتصالات، وبالتالي يمكنها أن تكون بمثابة عامل مضاعف للخطر في النزاعات القائمة، مما يستدعي تدخل مجلس الأمن. وهو ما يؤكد الاتجاه السائد بأن التهديدات السيبرانية أصبحت تحديًا جيوسياسيًا.

وفي هذا الصدد، تدعم كازاخستان اتباع نهج عالمي ومسؤول في استخدام تكنولوجيا المعلومات والاتصالات والذكاء الاصطناعي من

خلال وضع معايير مقبولة عموماً لاستخدامها. ويشارك الخبراء من بلدنا مشاركة فعالة في العمل الذي يقوم به الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها واللجنة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية. وندعم دليل جهات الاتصال الحكومية الدولية العالمي الذي أُطلق في شهر أيار/مايو. وعلى غرار العديد من الدول الأعضاء، تعكف كازاخستان حالياً على تعيين جهات اتصال دبلوماسية وتقنية للدليل.

أخيراً، أود أن أؤكد على أهمية تجنب تسييس المسألة والسعي بدلاً من ذلك إلى إيجاد أرضية مشتركة في ظل ظروف عدم الاستقرار الجيوسياسي. ويمكن أن يضطلع مجلس الأمن بدور رئيسي في تنسيق الجهود الدولية وتنفيذ تدابير محددة لمواجهة التهديدات السيبرانية، بما في ذلك عن طريق دعم مبادرات بناء قدرات الدول، وخاصة في المناطق النامية، وتعزيز قدرتها على منع محاولات خرق نظام المعلوماتية والتصدي لها وإشراك الجهات من غير الدول، بما في ذلك شركات التكنولوجيا ومنظمات المجتمع المدني، وتعزيز الجهود الجماعية ضد المخاطر السيبرانية وبالطبع إذكاء الوعي بمسائل الأمن السيبراني وتنظيم استعراضات منتظمة لمشهد التهديدات السيبرانية المتغير.

الرئيس (*تكلم بالإنكليزية*): أعطي الكلمة الآن لممثل جمهورية إيران الإسلامية.

السيد إيرواني (جمهورية إيران الإسلامية) (*تكلم بالإنكليزية*): أشكركم، سيدي الرئيس، على عقد هذه المناقشة المفتوحة.

يتطلب التصدي للتهديدات المتطورة في بيئة تكنولوجيا المعلومات والاتصالات نهجا متعدد الأوجه يشمل استراتيجيات تكنولوجية وقانونية وتعاونية.

ولطالما كانت إيران الهدف الأساسي والضحية الرئيسية للعديد من الهجمات السيبرانية التي تستهدف بنيتها التحتية وتعطل بشكل كبير تقديم الخدمات العامة وممارسة الوظائف الحكومية. ومن الأمثلة الواضحة على ذلك الهجمات التي شُنت بواسطة فيروس ستاكسنت وفيروس دوكو على المنشآت النووية السلمية في إيران، بالإضافة إلى الهجمات السيبرانية على البنية التحتية الصناعية الحيوية مثل صناعات الصلب والصناعات البتروكيميائية ومحطات الوقود. وسلطت تلك الأنشطة الخبيثة الضوء على إمكانية استخدام بيئات تكنولوجيا المعلومات والاتصالات سلاحا لإلحاق الضرر بالبنى التحتية للدول.

ونظراً للطبيعة المعقدة لحوكمة تكنولوجيا المعلومات والاتصالات، أود أن أسلط الضوء على النقاط التالية:

أولاً، تقع على عاتق فرادى الدول المسؤولية الرئيسية عن الحفاظ على أمن تكنولوجيا المعلومات والاتصالات وسلامتها وموثوقيتها. ويجب تعزيز وضمان الدور البارز والمشاركة الفعالة للدول في إدارة بيئة تكنولوجيا المعلومات والاتصالات على الصعيد العالمي، ولا سيما في مجال السياسات وصنع القرار. وينبغي تطوير حوكمة تكنولوجيا المعلومات والاتصالات بطريقة لا تؤثر سلباً على حقوق الدول في تحديد تنميتها وحوكمتها وتشريعاتها المتعلقة ببيئة تكنولوجيا المعلومات والاتصالات. ويجب أن تتصرف الدول بمسؤولية ووفقا للمبادئ الأساسية للقانون الدولي، ولا سيما مقاصد الأمم المتحدة ومبادئها.

ثانياً، لا يزال غياب معايير ملزمة قانوناً على الصعيد العالمي لتكنولوجيا المعلومات والاتصالات يشكل تحدياً. وغالباً ما يتخلف القانون الدولي الحالي عن الوتيرة السريعة للتغير التكنولوجي، مما يُحدث ثغرات تستغلها الجهات الفاعلة الخبيثة. وبالتالي، من الضروري وضع معايير دولية ملزمة قانوناً تتطرق إلى السمات المحددة لبيئة تكنولوجيا المعلومات والاتصالات وإنفاذها.

ثالثًا، يجب أن تمتنع الدول عن استخدام التقدم في مجال تكنولوجيا المعلومات والاتصالات كأدوات لاتخاذ تدابير قسرية اقتصادية أو سياسية أو غيرها، بما في ذلك تدابير فرض القيود أو الحظر التي تُتَّخَذ ضد دول أخرى. ويجب أن تمنع أيضًا وتتجنب إساءة استخدام سلاسل الإمداد المتعلقة بتكنولوجيا المعلومات والاتصالات الخاضعة لسيطرتها وولايتها القضائية، مع ضمان أن سلاسل الإمداد تلك لا تُنشئ ثغرات تعرّض سيادة الدول الأخرى وحماية بياناتها للخطر.

ويجب أن تكفل الدول اتخاذ التدابير المناسبة إزاء شركات ومنصات تكنولوجيا المعلومات والاتصالات التي تتجاوز آثارها حدودها الإقليمية ضمن ولايتها القضائية ومساءلتها عن سلوكها في مجال تكنولوجيا المعلومات والاتصالات، ولا سيما إذا كانت تنتهك السيادة الوطنية أو الأمن أو النظام العام للدول الأخرى.

رابعاً، نعتقد اعتقاداً راسخاً بأن بيئة تكنولوجيا المعلومات والاتصالات يجب أن تستخدم حصرياً للأغراض السلمية. ولتحقيق هذه الغاية، يجب أن تواصل الأمم المتحدة دورها المحوري من خلال الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات وأمن استخدامها من أجل وضع التزامات ملزمة قانوناً لمنع استخدام تكنولوجيا المعلومات والاتصالات للأغراض الخبيثة والحفاظ على هذا المجال للأغراض السلمية حصراً.

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

السيد أكرم (باكستان) (*تكلم بالإنكليزية*): نشكر وفد جمهورية كوريا على عقد هذه المناقشة الهامة بشأن التصدي للتهديدات الآخذة في التطور في الفضاء السيبراني. كما أود أن أشكر الأمين العام ومقدمي الإحاطات الآخرين على ملاحظاتهم الثاقبة.

تساهم تكنولوجيات وتطبيقات تكنولوجيا المعلومات والاتصالات بشكل كبير في التنمية الاجتماعية والاقتصادية. لكن هذه التقنيات وسعت أيضًا من نطاق النزاعات. وقد برزت الحرب السيبرانية باعتبارها مجالا جديدا ومهما من مجالات الحروب بما يشمل حرب المعلومات والهجمات السيبرانية الفعلية التي تشنها جهات فاعلة من الدول وغير الدول. وتدرك باكستان خطورة مشهد التهديد السيبراني المتطور وتأثيره على السلام والأمن الدوليين. كما أننا ندرك الحاجة الملحة للتصدي للأنشطة الخبيثة الأخرى في الفضاء السيبراني، بما في ذلك برمجيات انتزاع الفدية وسرقة المعلومات الحساسة.

وتقع العديد من الدول، بما في ذلك باكستان، ضحية لاستخدام المعلومات المضللة. وقد كشفت منظمة EU DisinfoLab، وهي منظمة مقرها في بروكسل، في تقريريها لعامي 2019 و 2020، عن القيام بأنشطة دعائية وتضليلية معادية لباكستان وحرب سيبرانية ضد باكستان. وقدم تقرير عام 2019 دليلًا على 15 عامًا من العمليات الكبيرة ضد باكستان، التي شملت أكثر من 10 منظمات غير حكومية مزعومة معتمدة احتياليًا لدى مجلس حقوق الإنسان، وأكثر من 750 وسيلة إعلامية مزيفة و 550 موقعًا إلكترونيًا مزيفًا وصلت إلى حد إحياء الموتى. وكانت هذه حملة ممنهجة تقودها دول ما لنشر المعلومات المضللة وإساءة استخدام الأمم المتحدة، وكذلك المؤسسات الأوروبية، بهدف الإساءة إلى باكستان. ويتطلب الأمر إيلاء اهتمام عالمي للتقرير الذي يكشف حملة المعلومات المضللة تلك، الصادر عن منظمة EU DisinfoLab. ويجب أن نطور طرائق لمنع مثل هذا الاستخدام غير القانوني والصارخ للأدوات السيبرانية للترويج لروايات وأهداف الدول المعادية.

وفي كانون الأول/ديسمبر 2021، اتخذت الجمعية العامة بتوافق الآراء القرار 227/76 الذي قدمته باكستان بعنوان "مكافحة التضليل الإعلامي من أجل تعزيز وحماية حقوق الإنسان والحريات الأساسية". وأكد القرار مسؤولية الدول عن التصدي لنشر المعلومات المضللة التي تقوض تعزيز السلام والتعاون بين الدول. إن باكستان، باعتبارها ضحية للدعاية المعادية المستمرة عبر الفضاء الإلكتروني وغيرها من أشكال الدعاية، لا تزال ملتزمة بمكافحة فيروس التضليل الإعلامي. وسنعزز العمل على ذلك من خلال التعاون الدولي، بما في ذلك في مجلس الأمن.

وبينما ننوه بالدور الهام الذي يضطلع به مجلس الأمن في التصدي للأخطار السيبرانية المحددة التي تهدد السلام والأمن الدوليين، فإننا نعتقد أن الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات وأمن استخدامها هو الأقدر على تعزيز التعاون الدولي والاستجابات القائمة على توافق الآراء للتحديات التي تطرحها التطورات السريعة في تكنولوجيا المعلومات والاتصالات، والفرص التي تتيحها هذه التطورات.

ويحث ميثاق الأمم المتحدة بشكل لا لبس فيه على التقيد العالمي بمبادئ السيادة والسلامة الإقليمية وعدم استخدام القوة وعدم التدخل في

الشؤون الداخلية للدول. ويجب أن تكون هذه المبادئ بمثابة إطار عمل إرشادي لإدارة الفضاء السيبراني.

ومع ذلك، فإن مجرد التأكيد على أن القانون الدولي ينطبق على الفضاء السيبراني ليس كافياً. وتشاطر باكستان الرأي القائل بأن من الضروري وضع صك دولي ملزم قانوناً مصمم خصيصاً للسمات الفريدة لتكنولوجيا المعلومات والاتصالات من أجل توفير إطار تنظيمي وآلية حوكمة ضرورية لجعل الفضاء السيبراني مستقرا وآمنا. وينبغي أن يعالج هذا الإطار القانوني والمؤسسي شواغل ومصالح جميع الأطراف وأن يجري التفاوض بشأنه داخل الأمم المتحدة بمشاركة جميع الدول على قدم المساواة.

ويمكن أن تسهم التدابير المناسبة لبناء الثقة، مثل التبادل الطوعي للمعلومات وأفضل الممارسات، في زيادة الشفافية والقدرة على التنبؤ في الفضاء السيبراني وتقليل احتمالات سوء الفهم وبالتالي تقليل مخاطر النزاع. وكان إطلاق دليل جهات الاتصال العالمية لأمن تكنولوجيا المعلومات والاتصالات الشهر الماضي خطوة مهمة لتعزيز الثقة والتعاون بين الدول في مجال أمن تكنولوجيا المعلومات والاتصالات. ويجب علينا البناء على مثل هذه الآليات والتعاون من أجل ترسيخ الأمن السيبراني المعزز وضمان الاستفادة الكاملة من قدرات تكنولوجيا المعلومات والاتصالات في التنمية الاقتصادية والاجتماعية.

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

السيدة غونزاليس (أوروغواي) (*تكلمت بالإسبانية*): نرحب بمشاركة الأمين العام هذا الصباح، وكذلك بمساهمات الرئيس التنفيذي لمعهد السلام السيبراني وأستاذة القانون والتكنولوجيا في جامعة ليدز بيكيت ونائب رئيس فريق خبراء الأمن السيبراني التابع للاتحاد الأفريقي.

ونعتبر أن عقد هذه المناقشة المفتوحة من جانب الرئاسة الحالية للمجلس، جمهورية كوريا، قد جاء في الوقت المناسب تماما. ويسلط هذا النقاش الضوء على هذه المسألة ويثري الحوار والنقاش حول قضية محورية في جدول أعمال السلام والأمن الدوليين ووثيقة الصلة بالعديد من المسائل الأخرى التي تقع ضمن اختصاص المنظمة.

وتؤيد أوروغواي هذا النوع من المبادرات وغيرها من أنواع المبادرات التي تسعى إلى توليد إجراءات إيجابية في مواجهة الأثر المدمر للاستخدام الخبيث لتكنولوجيا المعلومات والاتصالات على السلام والأمن والاستقرار في العالم.

ما من منطقة أو بلد في مأمن من هذا الخطر الذي لا يعرف حدودًا. فقد تعرضت معظم الدول الأعضاء لهجوم من هذا النوع، مما جعل الفضاء السيبراني مكانًا غير آمن، وزاد من تفاقم الآفات التي تعاني منها مجتمعاتنا، مثل الإرهاب والاتجار بالمخدرات والاتجار بالبشر والهجمات على البنية التحتية الحيوية، على سبيل المثال لا الحصر.

وقد استمعنا بعناية إلى الأمين العام هذا الصباح، ونتفق معه على أن مخاطر التكنولوجيا الرقمية المسلحة آخذة في التزايد. كما ندين استخدام الذكاء الاصطناعي كعامل مضاعف للخطر في الفضاء السيبراني، وكذلك الاستخدام المماثل لتقنيات الحوسبة الكمية، التي تعزز القدرة على إلحاق الضرر.

وتشجع أوروغواي الاستخدام الحر والمفتوح والآمن للفضاء السيبراني بما يسمح بتطوير الجوانب الإيجابية للتكنولوجيات واستخدام الإنترنت – وهو نهج إيجابي يمكّننا من تحقيق أهداف التنمية المستدامة، وتعزيز التجارة الدولية ومواصلة تحقيق أوجه التقدم العلمي والطبي التي تحسن رفاه شعوبنا.

ولتحقيق هذه الغاية، يجب أن تكون لدينا أدوات ملموسة وأطر تنظيمية آمنة توفر هذا الأمن. ولكن، في الواقع، ليست جميع البلدان والمناطق في نفس الوضع الذي يمكنها من الاستجابة أو حماية نفسها من هذه التهديدات السيبرانية بسبب تفاوت مستويات تطورها في تقنيات الأمن السيبراني.

وفي هذا السياق، نشعر بالقلق إزاء عدم إحراز تقدم كبير في بناء القدرات والتعاون الدولي. وتحتاج البلدان النامية، أكثر من أي وقت مضى، إلى نقل التكنولوجيا والمعارف والممارسات الجيدة والمعدات اللازمة كي تواجه بكفاءة التحديات الناشئة عن الاستخدام الضار لتكنولوجيا المعلومات والاتصالات.

وفي السياق السلبي الذي نشأ في الفضاء الإلكتروني، تؤدي الأمم المتحدة دوراً أساسياً في تحقيق السلام والأمن الدوليين، وهو شرط مسبق لأي نوع من الازدهار.

وفي هذا السياق، نسلط الضوء على الدور الذي تضطلع به الجمعية العامة من خلال اللجنة الأولى. ونقدر ونؤيد عمل الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات وأمن استخدامها، كما قدرنا وأيدنا عمل فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي في الماضي. فقد أرسى عملهما، الذي تمخض عن توصيات ومعايير موحدة بشأن سلوك الدول المسؤول، أساساً مشتركاً يُستند إليه للتفاهم ويشكل المنتدى الرئيسي للمناقشة والحوار. وتقع على عاتق الدول أيضا مسؤولية تطبيق هذه المعايير والأسس التي قد تبلورت.

ونظرا لتقدم التكنولوجيات، يجب أن تتعزز فعالية المؤسسات أيضا. ويجب أن تتطور وتحسن إطارها المؤسسي وحوكمتها عن طريق آلية دائمة تتيح لها مواجهة التحديات التي تفرضها هذه التطورات المستجدة باستمرار. ويجب تجنب الازدواجية والقيام في نهاية المطاف بوضع قواعد إلزامية لجميع الدول. ولا يُستثنى الفضاء الإلكتروني من تطبيق القانون الدولي واللوائح الدولية، مما يوفر لنا اليقين القانوني.

ونغتنم هذه الفرصة للإشارة إلى أهمية الدورة المقبلة للجنة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، المعروفة أيضا بالاتفاقية المتعلقة بالجريمة الإلكترونية. ونأمل أن تُعتمد هذه الاتفاقية في أقرب وقت ممكن، وأن تقوم الدول بوضع معايير وطنية وفقاً لها. ونعتقد أن هذه خطوة إيجابية يمكن أن تتخذها المنظمة في هذا الصدد.

أخيراً، أود أن أؤكد من جديد على أهمية تعزيز المناعة السيبرانية وبناء القدرات، الذي يشكل قاسماً مشتركاً لمعظم كيانات المنظمة، تؤدي المنظمات الإقليمية دوراً رئيسياً فيه. ونولي تقديراً وقيمة للدعم الذي تقدمه مختلف البلدان التي لديها برامج تعاون وتعزز تدريب الأخصائيين التقنيين والمهنيين القادرين على مواجهة التحديات المتعلقة بالفضاء الإلكتروني، ونحثها على الاستمرار في هذا الطريق، مما سيفضي بلا شك إلى بيئة إلكترونية أكثر فائدة للجميع – نظام قائم على التعاون الدولي، بدلاً من المواجهة أو تسييس هذه المسائل.

وكما في المجالات الأخرى، فإن التآزر بين مجلس الأمن والجمعية العامة في التصدي للتهديدات السيبرانية يكتسي أهمية بالغة. فمن الضروري عقد جلسات إحاطة ومناقشات دورية، مثل هذه، لوضع إجراءات فعالة رامية إلى مكافحة إساءة استخدام التكنولوجيات في مجال الأمن الدولي بأكمله، بما في ذلك في النزاعات، وبالتالي تعزيز حماية المدنيين في الجوانب المرتبطة بالفضاء الإلكتروني.

وأشكركم، سيدي الرئيس، على إدراج هذا البند في جدول أعمال اليوم.

السيدة جانينا (ألبانيا) (*تكلمت بالإنكليزية*): في عالم اليوم الذي يتسم بالرقمنة، يتجلى الأمن السيبراني كمسألة ذات أهمية لدى جميع الدول الأعضاء. ونود أن نشكر الرئاسة الكورية على عقد هذه المناقشة المهمة في مجلس الأمن، كما نشكر مقدمي الإحاطتين على إسهاماتهما المفيدة.

لقد واجه كثير منا شكلاً من أشكال الهجمات الإلكترونية. ورأينا أن هذه الأنشطة الخبيثة لا تؤثر على الحياة اليومية لمواطنينا فحسب، بل تؤثر بشكل أوسع على المجتمع الدولي ككل وتهدد السلام والأمن الدوليين تهديداً مباشراً. ويترتب عن تزايد عدد الهجمات السيبرانية أثر كبير في خفض إجمالي الناتج المحلي للبلدان في مختلف المناطق، حيث تعتبر البلدان النامية أكثر البلدان عرضة للهجمات السيبرانية.

ولما كانت التهديدات السيبرانية تزداد تعقيداً وتنوعاً، يجب أن تتسم استجاباتنا بالمرونة. وعلينا أن نتزود بالأدوات اللازمة لوضع هذه الاستجابات والتخفيف من التهديدات السيبرانية التي نواجهها، فردياً وجماعياً، بتيسير التعاون الدولي وتبادل المعلومات. وتعرضت ألبانيا، قبل عامين، لهجوم إلكتروني مكثف غير مسبوق شنتها مجموعات متعددة من القراصنة مرتبطة بجمهورية إيران الإسلامية، بهدف واضح

هو تدمير البنية التحتية الحكومية وشل الخدمات العامة وإثارة الفوضى وانعدام الأمن في البلد. وما زلنا هدفاً لهجمات إلكترونية المتطورة.

وفي هذا السياق، تستثمر ألبانيا في مناعتها السيبرانية على المستوى الوطني، مع إيلاء اهتمام كبير للنُهج الإقليمية والدولية للأمن السيبراني. ولا تزال منطقتنا، غرب البلقان، تواجه عدداً متزايداً من التهديدات السيبرانية التي لا تزال تتطور. ونعمل على بناء القدرات السيبرانية في المنطقة من خلال برامج في مجالات الأمن السيبراني والجريمة السيبرانية والدبلوماسية السيبرانية. وسيسعى مؤتمر القمة الإقليمي المعني بالأمن السيبراني، الذي سيعقد في تموز/يوليه في بلدي، ألبانيا، إلى تعزيز المناعة السيبرانية في غرب البلقان.

ونعتقد اعتقادا قوياً أنه يمكن وينبغي بذل مزيد من الجهود على الصعيد الدولي.

وفي هذا السياق، أود أن أشدد على ثلاثة عناصر.

أولاً، يمكن لمجلس الأمن، بصفته الجهاز الرئيسي المعني بصون السلام والأمن الدوليين، أن يعزز عمله في هذا المجال. فهذه منصة قيمة لمناقشة التهديدات السيبرانية وسبل التصدي لها. ويجب أن تكون المناقشات شاملة ومفتوحة لمختلف الجهات الفاعلة. وفي هذا الصدد، نجد قيمة مضافة في التعاون بين الحكومات والقطاع الخاص على تعزيز الدفاع ضد التهديدات السيبرانية.

ثانياً، يجب أن تتعزز عملية المساءلة تجاه الجهات الفاعلة الحكومية وغير الحكومية التي تتعرض لسوء المعاملة في جهودنا المشتركة من أجل فضاء إلكتروني آمن. ويقترن ذلك باحترام المعايير الدولية للسلوك المسؤول في الفضاء الإلكتروني.

ثالثاً، يتعين تعزيز بناء القدرات. ففي حين أن البلدان المتقدمة النمو تتمتع بوضع السيبراني قوي، تفتقر العديد من البلدان النامية إلى الموارد والخبرات اللازمة لمواجهة التهديدات السيبرانية. وقد يؤدي ذلك إلى تعرض البنية التحتية الحيوية لخطر شديد، وإلى الهجمات السيبرانية، والتجسس الإلكتروني وغير ذلك من الأنشطة المدمرة.

في الختام، أود أن أكرر مرة أخرى أنه لا يمكن تحقيق أمن الفضاء الإلكتروني إلا بتضافر الجهود على المستوى العالمي، وهذه الجلسة خطوة في الاتجاه الصحيح.

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

السيد سيكيريس (اليونان) (*تكلم بالإنكليزية*): أولاً وقبل كل شيء، أود أن أشكر جمهورية كوريا على تنظيم هذه المناقشة الرفيعة المستوى البالغة الأهمية، وأود أن أشكر مقدمي الإحاطتين على ملاحظاتهما المثيرة للاهتمام.

وتؤيد اليونان تأييدا تاما البيان الذي أدلى به ممثل وفد الاتحاد الأوروبي وتود أن تبدي الملاحظات التالية بصفتها الوطنية.

لقد كان التطور الرقمي في عصرنا هذا حافزاً للتقدم البشري، حيث أدى إلى تحويل مجتمعاتنا واقتصاداتنا وتوسيع فرص التعاون. كما تتيح التكنولوجيات الناشئة للبشرية فرصاً كبيرة للنمو الاقتصادي، وللتنمية المستدامة والشاملة للجميع، مما يؤثر على جميع الركائز الثلاث لعمل المنظمة وهي: السلام والأمن، وحقوق الإنسان، والتنمية المستدامة.

ونظراً لأن اقتصاداتنا وديمقراطياتنا ومجتمعاتنا تعتمد أكثر من أي وقت مضى على شبكات وأنظمة معلومات آمنة وموثوقة ومترابطة بشكل متزايد، فقد أصبح الأمن السيبراني ضرورياً لبناء فضاء إلكتروني عالمي مفتوح وحر ومستقر وآمن.

وفي الوقت نفسه، أصبح الاستغلال الخبيث لهذه التكنولوجيات مصدرا لمخاطر وتحديات جديدة. وازدادت السلوكيات الخبيثة في الفضاء الإلكتروني في السنوات الأخيرة، بما في ذلك الزيادة الحادة والمستمرة في الهجمات الإلكترونية التي تستهدف البنية التحتية الحيوية وسلاسل الإمداد والملكية الفكرية، إضافة إلى زيادة الهجمات الرامية إلى انتزاع الفدية ضد الحكومات والمنظمات والشركات والمواطنين.

وعلاوة على ذلك، فإن الأمر الأكثر إثارة للقلق هو أن الهجمات السيبرانية أصبحت جزءًا لا يتجزأ من العمليات أثناء النزاعات المسلحة.

وأعربت اليونان عن قلقها البالغ إزاء هذه الأنشطة التي تقوض السلام والأمن الدوليين ويمكن أن تؤدي إلى زعزعة الاستقرار وإلى آثار متتالية، مع زيادة مخاطر نشوب النزاعات.

بيد أن الفضاء الإلكتروني ليس مجالاً يسود فيه قانون الغاب. فضمن ما يُعرف بإطار سلوك الدول المسؤول في الفضاء الإلكتروني، اتفقت جميع الدول على أن القانون الدولي القائم، لا سيما ميثاق الأمم المتحدة، هو القانون المنطبق والأساسي للحفاظ على السلام والاستقرار. ويجب التمسك بالقانون الدولي وتطبيقه في هذا المجال بنفس الطريقة التي ينطبق بها على جميع مجالات العلاقات الدولية الأخرى.

وبما أن مجلس الأمن يتحمل المسؤولية الرئيسية عن صون السلام والأمن الدوليين، فإننا نأمل أن يؤدي في المستقبل دوراً أكثر نشاطاً في المسائل التي تنطوي على تهديدات ناشئة ومعاصرة. ويمكن أن يشمل هذا الدور بذل جهود لتعزيز إطار سلوك الدول المسؤول المذكور أعلاه والرد على الأنشطة السيبرانية التي لا تتفق مع أهداف صون السلام والاستقرار والأمن الدولي.

وباعتبارنا بلدا يؤيد بقوة أولوية القانون الدولي والتسوية السلمية للنزاعات، نؤكد من جديد تطلعنا إلى فضاء إلكتروني سلمي وآمن، ونلتزم تماما بإجراء مزيد من المناقشات بشأن هذا الموضوع المهم للغاية، بما في ذلك خلال فترة ولايتنا كعضو غير دائم في مجلس الأمن للفترة 2025-2026.

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

السيد غوميث هيرناندیث (إسبانيا) (*تكلم بالإسبانية*): أرحب بعقد هذه المناقشة المفتوحة. إن إسبانيا، باعتبارها بلدا يدافع بقوة عن صون السلم والأمن الدوليين ويساهم فيه بنشاط، تؤكد من جديد التزامها بمكافحة التهديدات السيبرانية وتشجيع سلوك الدول المسؤول في الفضاء الإلكتروني عن طريق التعاون الإقليمي والدولي في إطار السلوك المسؤول للدول الأعضاء في الأمم المتحدة.

ولئن كانت طبيعة التهديدات المتغيرة بسرعة تجبرنا على تكييف النهج والأدوات اللازمة للتصدي لها بطريقة مشتركة ومتكاملة، يبقى مفتاح الصمود السيبراني العالمي والوطني هو تطبيق المزيد والأفضل من الأدوات السيبرانية التي تضمن حماية البنية التحتية الحيوية في جميع أنحاء العالم.

وبعض الاتجاهات الأكثر إثارة للقلق هي انتشار عمليات القرصنة على البيانات، خاصةً ضد البنية التحتية الحيوية؛ والتلاعب بالمعلومات والإدراك من خلال التقنيات الرقمية؛ وشن هجمات على سلاسل التوريد الدولية تستغل نقاط ضعف مختلفة وتؤدي إلى خسائر اقتصادية.

لقد تطور مفهوم النزاع ذاته مع ظهور الاستراتيجيات الهجينة والمناطق الرمادية والحرب غير المتكافئة. ولم تعد الفوارق الحادة بين الحرب والسلام، في بعض الحالات، قاطعة. إن الاستخدام الخبيث لتكنولوجيا المعلومات والاتصالات أصبح الآن جزءًا لا يتجزأ من المشهد المعقد والمتغير للأدوات المستخدمة لتحقيق ميزة في النزاعات. وهناك حاجة ملحة لتبني منظور أوسع من أجل معالجة النزاعات المعاصرة بطريقة شاملة.

ولذلك، ينبغي أن تستند أي آلية أو التزام دولي محتمل يتعلق بتكنولوجيا المعلومات والاتصالات إلى اتفاقات توافقية بشأن إطار السلوك المسؤول للدول فيما يتعلق بتكنولوجيا المعلومات والاتصالات، وأن يتم التوصل إليه من خلال عملية مفتوحة وشاملة وشفافة.

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

السيد فينهاس (البرتغال) (*تكلم بالإنكليزية*): أشيد بجمهورية كوريا على مناقشة اليوم وأؤيد البيان الذي أدلى به ممثل الاتحاد الأوروبي في وقت سابق اليوم.

يجب أن يكون مجلس الأمن قادراً، بصفته الضامن للسلم والأمن الدوليين، على التصدي للتهديدات الحالية والناشئة والمستقبلية. فحقيقة أننا نناقش مسألة التهديدات في الفضاء الإلكتروني تُظهر أن المجلس قادر على التكيف في مواجهة التحديات الجديدة عندما يُطلب منه ذلك.

وقد أثبتت الأنشطة والعمليات السيبرانية العدوانية أنها أخطر التحديات التي تواجه الازدهار الذي يبشر به التحول الرقمي. وأثبتت

أيضًا أنها تشكل تحديًا خطيراً لنزاهة مؤسساتنا والثقة التي يضعها مواطنونا فيها. والأمر الأكثر إثارة للقلق هو أنه لا يمكن الاستهانة بتأثير الأمن السيبراني على العالم المادي.

فقد أدت القدرات الهجومية المتزايدة للجهات الفاعلة السيبرانية العدوانية إلى تزايد تكاليف منع هجماتهم والتعافي منها. وأدى دور الجماعات الإجرامية السيبرانية، على وجه الخصوص، إلى زيادة تعقيد مشهد التهديدات السيبرانية. وقد انضمت البرتغال، في أعقاب الهجمات التخريبية لمجموعات برمجيات الفدية الخبيثة المزعومة في عام 2022، إلى المبادرة الدولية لمكافحة برمجيات الفدية الخبيثة. وتجدر الإشارة إلى أن برمجيات الفدية الخبيثة تُستخدم أيضًا بشكل متزايد من قبل الجهات الفاعلة التي ترعاها الدول كغطاء لتحقيق أهداف استراتيجية.

وقد برز الذكاء الاصطناعي كعامل كبير في تسوية القدرات عبر العديد من الجهات الفاعلة في مجال التهديدات، موفرا للمشغلين غير المتمرسين درجة جديدة من الإمكانيات ومن المحتمل أن يزيد من نطاق الهجمات. وفي مواجهة ذلك المشهد من التهديدات، نحن على ثقة من أن اتفاقية الأمم المتحدة المستقبلية لمكافحة الجريمة السيبرانية ستوضع في صيغتها النهائية قريبًا وستكون قادرة على تعزيز التعاون الدولي في مجال إنفاذ القانون. وسييسر ذلك التعاون في مكافحة الجرائم السيبرانية – التي ترتكبها الجهات الفاعلة التي ترعاها الدول – بدوره تنفيذ إطار الأمم المتحدة للقوانين والمعايير وتدابير بناء الثقة من أجل سلوك الدول المسؤول في الفضاء السيبراني.

وكذلك يضطلع بناء القدرات بدور أساسي، وتعتزم البرتغال إطلاق برنامج سنوي لبناء القدرات الرقمية للبلدان النامية، بالشراكة مع جامعة الأمم المتحدة. ومن المتوقع أيضًا أن تسهم الآلية المؤسسية الدائمة أو برنامج العمل المستقبلي الدائم الذي سينفذ اعتباراً من عام 2026 فصاعدًا في سد الفجوة الرقمية.

ويضطلع المجلس بدور تكميلي هام، مع الحفاظ على دور الفريق العامل المفتوح باب العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات واستخدامها بوصفه المنبر الرئيسي لتعميق فهمنا للتهديدات والمعايير والقوانين، وكذلك لتعزيز بناء القدرات وبناء الثقة فيما بين الدول.

أولا، يمكن لمجلس الأمن أن يعيد التأكيد على مجموعة معايير السلوك المسؤول للدول المتفق عليها بتوافق الآراء في الفريق العامل المفتوح باب العضوية، وذلك على سبيل المثال بإصدار بيان رئاسي بذلك المعنى. وسيوفر ذلك الإجراء وحده اعترافاً هاماً بالآثار التي يمكن أن تحدثها التهديدات السيبرانية على السلم والأمن الدوليين.

ثانيًا وأخيراً، يمكن لمجلس الأمن أيضًا أن يحاول إدماج الشواغل المتعلقة بتكنولوجيا المعلومات والاتصالات في ولاياته ذات الصلة، حيثما كان ذلك مناسبًا. فبناء مرونة البنية التحتية الحيوية ضد النشاط السيبراني المعادي يمكن أن يسهم، في سياقات معينة، بشكل حاسم في زيادة الاستقرار على المدى الطويل.

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

السيدة غونزاليس لوبيس (السلفادور) (*تكلمت بالإسبانية*): أشكر جمهورية كوريا على عقد هذه المناقشة الهامة بشأن التهديدات المتطورة التي نواجهها في الفضاء السيبراني.

وكما أشار وفد بلدي في مناسبات أخرى، فإن التهديدات المرتبطة باستخدام تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي لا تزال تتطور من حيث الحجم والشدة. ويمكن لتلك التهديدات، المرتبطة بسوء استخدام التقنيات الناشئة، مثل الذكاء الاصطناعي أو الحوسبة الكمية، أن تولد نواقل هجوم جديدة، تؤدي إلى استغلال نقاط الضعف في أنظمة تكنولوجيا المعلومات والاتصالات. ونظراً لتزايد ترابط البنية التحتية الرقمية في جميع مجالات الحوكمة – الاجتماعية والاقتصادية والسياسية – يمكن أن نشهد آثاراً متتالية يصعب التنبؤ بها.

ويمكن أن تكون للأنشطة الخبيثة في مجال تكنولوجيا المعلومات والاتصالات آثار مدمرة تتجاوز حدود السلم والأمن الدوليين. وبالمثل، يمكنها أن تتسبب في إلحاق ضرر مباشر بالمدنيين، لا سيما عندما

تُنفذ هذه الهجمات ضد البنية التحتية الحيوية الضرورية لعمل المجتمع، مثل أنظمة الصحة العامة أو الخدمات الأساسية مثل إمدادات المياه والطاقة وأنظمة النقل، أو عندما تعطل أو تعيق عمل الإنترنت وتوافره.

ويعتقد بلدي أن هذه الهيئة، أي مجلس الأمن، ينبغي أن تتصدى بشكل أكثر منهجية واستباقية للمخاطر السيبرانية على السلم والأمن كجزء من ولايته ومسؤوليته في صون السلم والأمن الدوليين. ويمكن أن يتم ذلك من خلال مناقشات محددة، مع نتائج ملموسة تتعلق بحماية البنية التحتية الحيوية والبنية التحتية الحيوية المعلوماتية؛ والكشف عن حوادث الأمن السيبراني والاستجابة لها والتعافي منها؛ ورؤية شاملة لبناء القدرات في مجال الأمن السيبراني، من بين مسائل أخرى.

وبالإضافة إلى ذلك، يمكن النظر في إمكانية إدراج بند في جدول الأعمال الموضوعي للمجلس لمعالجة التهديدات التي يتعرض لها السلام والأمن الناشئة عن المجال الرقمي، بما في ذلك تكنولوجيا المعلومات والاتصالات وغيرها من التكنولوجيات الناشئة، مثل الذكاء الاصطناعي، لاستكمال الجهود المبذولة في إطار الجمعية العامة والهيئات الفرعية الأخرى.

ومن المهم أيضاً الإشارة إلى ضرورة مواصلة معالجة تأثير التقنيات الرقمية على حماية المدنيين والأعيان المدنية في النزاعات المسلحة، بما في ذلك تطبيق مبادئ القانون الدولي الإنساني في المجال الرقمي واحترامها احتراما كاملا. ونعتقد أن زيادة وتأثير المعلومات المضللة وانتشار المعلومات المغلوطة وخطاب الكراهية من خلال المنصات الرقمية مسائل تستحق اهتمام مجلس الأمن أيضًا.

وحرصاً على الوقت، سيكون البيان الكامل متاحاً من خلال الأمانة العامة.

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

السيدة ستويفا (بلغاريا) (*تكلمت بالإنكليزية*): تؤيد بلغاريا البيان الذي أدلي به باسم الاتحاد الأوروبي. وأود أن أسلط الضوء على بعض النقاط بصفتي الوطنية.

نشيد بجمهورية كوريا على تنظيم المناقشة الرفيعة المستوى اليوم وعلى توجيه انتباه مجلس الأمن إلى هذا الموضوع المهم. وأود أيضا أن أشكر مقدمي الإحاطتين على عرضيهما الثاقبين والزاخرين بالمعلومات.

إن مسألة التهديدات المتطورة في الفضاء الإلكتروني تزداد أهمية بالنسبة لأمن مجتمعاتنا واستقرارها. واليوم يتزايد استغلال الفضاء الإلكتروني من أجل تحقيق أغراض سياسية وأيديولوجية، وتعوق زيادة الاستقطاب على الصعيد الدولي فعالية تعددية الأطراف.

وكما أوضح مقدما الإحاطتين، فإن بعض أكبر المخاطر التي نواجهها من الاستخدام الفضاء الإلكتروني في الأغراض الخبيثة هي حملات التضليل المزودة بالإمكانات التي تحاول استغلال مواطن ضعف المجتمع، وتقويض العمليات والمؤسسات الديمقراطية، وإثارة انعدام الثقة، وإضعاف المجتمعات في نهاية المطاف. وإضافة إلى ذلك، يشكل الاستهداف الخبيث للبنية التحتية الحيوية والخدمات الأساسية تهديدا عالميا كبيرا. وكل هذه الأنشطة تقوض الأمن والاستقرار الدوليين والفوائد التي يجلبها الفضاء الإلكتروني للتنمية الاقتصادية والاجتماعية والسياسية.

وفي حين يظل الأمن الوطني، بما في ذلك الأمن السيبراني، من اختصاص الحكومة الوطنية، فإن إمكانية تأثير الحوادث السيبرانية عبر الحدود تدل على ضرورة بذل جهود مشتركة. ولهذا السبب، من المهم تعزيز التعاون في المسائل السيبرانية على المستوى الدولي. ورغم أن النقاش الفعال المتعدد الأطراف بشأن الأمن الدولي في الفضاء الإلكتروني يتدهور بشكل عام بسبب التوترات الجيوسياسية، من الواضح أنه لا بد أن يتخذ مجلس الأمن موقفاً أكثر استباقية بشأن هذه المسألة.

وترى بلغاريا أن الأمن والاستقرار الدوليين يترتهنان بفضاء إلكتروني عالمي مفتوح وحر ومستقر وآمن، يُحترم فيه القانون الدولي، لا سيما ميثاق الأمم المتحدة، ويُتقيد فيه بالمعايير والقواعد والمبادئ الطوعية غير الملزمة لسلوك الدول المسؤول. وتحقيقاً لهذه الغاية،

لا بد من التعاون على الصعيد الدولي. ولهذا السبب من الأهمية بمكان أن نعزز دور مجلس الأمن في التصدي للتهديدات السيبرانية. فالمشاركة الاستباقية للمجلس بشأن الأمن السيبراني، التي تتماشى مع مسؤوليته الأساسية في صون السلام والأمن الدوليين، تجعله في وضع جيد يتيح له التصدي للأنشطة السيبرانية الضارة.

وطابع الترابط الذي يتسم به الفضاء الإلكتروني يتطلب من جميع أصحاب المصلحة تبادل المعلومات بشأنه وتحمل مسؤولياتهم المحددة فيما يتعلق به من أجل الحفاظ على فضاء إلكتروني عالمي ومفتوح ومستقر وآمن. وبالتالي، من الأهمية بمكان اتباع نهج متعدد من حيث أصحاب المصلحة لمواجهة التهديدات المتطورة في الفضاء الإلكتروني على النحو الواجب. وينبغي أن تسعى الدول والمؤسسات الدولية، بما في ذلك مجلس الأمن، إلى تعزيز التبادل الدائم والمنظم مع جميع أصحاب المصلحة، بما في ذلك القطاع الخاص والأوساط الأكاديمية والمجتمع المدني. وهذا هو السبيل أيضاً لتعزيز الوقاية والتأهب والقدرة على الصمود والاستجابة في الفضاء الإلكتروني والنهوض بها.

أخيراً، تجدر الإشارة إلى أن مستوى المناعة السيبرانية والقدرة على اكتشاف الأنشطة السيبرانية الخبيثة والتصدي لها يتفاوتان تفاوتا كبيرا بين البلدان من حيث القدرة والنضج. لهذا السبب، من الضروري تحسين المستوى العام للأمن السيبراني من خلال بناء القدرات ووضع معايير مشتركة للأمن السيبراني، لا سيما للبنية التحتية الحيوية، ولتطوير تكنولوجيات جديدة وتطبيقها.

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

السيدة أندرياني (*تكلمت بالإنكليزية*): يشرفني أن أخاطب مجلس الأمن اليوم بشأن مسألة بالغة الأهمية وهي إساءة استخدام التكنولوجيات الحديثة وتزايد التهديدات للفضاء الإلكتروني.

إن الجريمة الإلكترونية عامل مضاعف للخطر، حيث تتيح أشكالاً أخرى من الإجرام وتزيد من تفاقم الصدمات العالمية وتقوض التنمية المستدامة والسلام والأمن.

وتؤيد الإنتربول هذه المناقشة المفتوحة وستطرح ثلاث نقاط فيما يتعلق بتعزيز البنية الأمنية العالمية ضد التهديدات السيبرانية التي تشكلها الجهات الفاعلة الإجرامية من غير الدول.

أولاً، يجب أن نعزز إدراكنا لواقع التهديدات السيبرانية الحديثة، الذي لا يزال حتى يومنا هذا مجزأً بين المناطق والقطاعات. وفي هذا الصدد، وضعت الإنتربول بوابة نموذجية لتيسير الوصول إلى بيانات هذا القطاع استكمالاً لتبادل المعلومات بين البلدان الأعضاء. وعلى منصتنا I-24/7، نربط بين 196 من الدول الأعضاء، مما يتيح تبادل معلومات الشرطة بشكل آمن على مستوى العالم. وإضافة إلى ذلك، نوفر منصات مصممة خصيصاً لمكافحة الجرائم الإلكترونية من لأغراض تبادل أفضل الممارسات والتحليل. وعلاوة على ذلك، تيسر قائمة جهات الاتصال على مدار الساعة طوال أيام الأسبوع والأفرقة العاملة الإقليمية سرعة الاستجابة في الحالات العاجلة وبناء الثقة بين الأجهزة. وبالعمل معا والاستفادة من الآليات القائمة والراسخة لتبادل المعلومات، يمكننا أن نخطو خطوات كبيرة في حماية الفضاء الإلكتروني وضمان الأمن العالمي.

ثانياً، يجب أن نسد الثغرات في القدرات. فلا تزال هناك أوجه تفاوت كبيرة في المناعة السيبرانية. وتقدم الإنتربول الدعم للدول الأعضاء في التغلب على الفجوة الرقمية بتقديم المساعدة التقنية وبناء القدرات. ونسعى إلى تزويد أجهزة إنفاذ القانون بالمعرفة والمهارات اللازمة لمواجهة التحديات السيبرانية الحالية.

ثالثاً، يجب علينا تحقيق أقصى قدر من التآزر عن طريق الحوار المؤسسي المنتظم والآليات المتعددة الأطراف. ولنتذكر أن المفتاح هو التعاون وليس الازدواجية. ولهذا السبب، تشارك الإنتربول بنشاط في مختلف العمليات المتصلة بالفضاء الإلكتروني في إطار الأمم المتحدة وخارجها، بما في ذلك الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها، واللجنة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية.

إن التهديدات السيبرانية لا تعرف حدوداً، وتدابيرنا الدفاعية ينبغي ألا تعرف حدوداً. ولا تزال الإنتربول ملتزمة بضمان عالم سيبراني أكثر أماناً للجميع من خلال التعاون والابتكار والتفاني.

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

السيد راغوتاهالي (الهند): (*تكلم بالإنكليزية*): أهنئ جمهورية كوريا على توليها رئاسة مجلس الأمن لشهر حزيران/يونيه. وأرحب بهذه المبادرة لعقد مناقشة مفتوحة بشأن "التصدي للتهديدات المتطورة في الفضاء الإلكتروني". وأود أيضا أن أشكر الأمين العام وممثلي المجتمع المدني على أفكارهما الثاقبة.

إن عالم اليوم هو عالم العصر الرقمي. فقد تجاوز التحول الرقمي جميع الحدود الجغرافية والسياسية والاقتصادية التقليدية. وبفعل التقدم السريع واعتماد التكنولوجيات الجديدة والناشئة، مثل الذكاء الاصطناعي، أصبحت حياتنا متشابكة بشكل متزايد مع العالم الرقمي. وفي هذا العالم المترابط، من الاتصالات الشخصية إلى البنية التحتية الحيوية، أصبح الاعتماد على الفضاء الإلكتروني اعتماداً شديداً.

كما أن التحول الرقمي يعرضنا لعدد لا يحصى من التهديدات السيبرانية. ويزداد تواتر وتعقيد الهجمات الإلكترونية ضد البنية التحتية الحيوية، ونظم المعلومات والنظم المالية، والشبكات الحكومية. وعمليات السطو على العملات المشفَّرة، واختطاف البيانات، والتزييف التزييف المحكَم، والتضليل والتحريض، صارتً شائعة الآن. وعلاوة على ذلك، تجدر الإشارة أيضا إلى قدرة الذكاء الاصطناعي على توسيع نطاق للهجمات السيبرانية وزيادة حجمها.

وتتعرض للخطر سلامة وأمن منتجات تكنولوجيا المعلومات والاتصالات، التي تشكل عناصر الفضاء الإلكتروني. وترتكب هذه الأفعال جهات فاعلة ترعاها الدول وجهات فاعلة من غير الدول، إضافة إلى شبكات الجريمة العابرة للحدود الوطنية. وهذه الأعمال الشائنة تقوض الثقة في سلاسل الإمداد العالمية لتكنولوجيا المعلومات والاتصالات، وتعرض الأمن للخطر ويمكن أن تؤدي إلى بؤر توتر بين الدول. ووفقا لتقديرات البنك الدولي، من الممكن أن تكون الهجمات الإلكترونية قد كبدت العالم خسائر تقدر بحوالي 5,2 تريليونات دولار في الفترة من 2019 إلى 2023.

كما يجد الإرهابيون طرقا جديدة عبر الفضاء الإلكتروني لارتكاب أعمال العنف؛ ودفع الشباب إلى التطرف؛ والقيام بالتجنيد؛ وإجراء أنشطة التدريب وجمع الموارد المالية. وأصبحت الأساليب الجديدة المتمثلة في الأصول الافتراضية والعملات المشفرة هي القاعدة في المعاملات المالية لدى الإرهابيين. ويستغل الإرهاب قنوات جديدة وأساليب تمويل جديدة من العالم السيبراني، مما يجعل منها مسألة بالغة الأهمية بالنسبة لأمن كل دولة وازدهارها. وتتعرض الهند للإرهاب منذ عدة عقود، وهي تدرك الطابع الخطير لتحدي الإرهاب الإلكتروني.

وفي هذا السياق، أود أن أسلط الضوء على أربع نقاط.

إن التهديدات في الفضاء الإلكتروني لا تهدد الأمن الوطني فحسب، بل قد تقوض نسيج الاستقرار والتعاون العالميين. ولا يمكن لأي دولة أو منظمة أن تكافح التهديدات السيبرانية بمفردها، فالكفاح يتطلب جبهة موحدة.

هناك حاجة متزايدة إلى وضع صكوك دولية للتصدي للتهديدات الناجمة عن الفضاء الإلكتروني. القانون الدولي الحالي غير مهيأ بشكل مناسب لدعم الرد على الهجمات في الفضاء الإلكتروني. يجب التعامل مع الهجمات في الفضاء الإلكتروني ضد البنية التحتية الحيوية وأنظمة المعلومات والأنظمة المالية والشبكات الحكومية على أنها هجمات إرهابية. وينبغي النظر في إمكانية تطبيق معاهدات مكافحة الإرهاب الحالية على مجال الفضاء الإلكتروني. ينبغي على المجتمع الدولي ضمان توحيد قوانين مكافحة جرائم الإرهاب. إن التعاون على الصعيد العالمي في هذا المجال سيساعد على مواءمة معايير أمن الفضاء الإلكتروني وأفضل الممارسات واللوائح التنظيمية.

إن الهند تشارك في العمليات والمشاورات المتعلقة بالفضاء الإلكتروني الصادر بها ولايات من الأمم المتحدة والتي تدعم المشاركة الحكومية الدولية العالمية والشاملة للجميع والشفافة بهدف تحقيق فضاء إلكتروني آمن ومأمون. نحن نعتقد أن التعاون بين أصحاب المصلحة

المتعددين ضروري للإحاطة علما بالتهديدات الناشئة في الفضاء الإلكتروني وفهمها.

في الختام، تعد الهند من بين الدول الرائدة في العالم في مجال تطوير التكنولوجيا الرقمية والربط الإلكتروني والقدرة على الصمود في الفضاء الإلكتروني. وتلتزم الهند ببيئة فضاء إلكتروني مفتوح وآمن ومجاني وسهل الوصول إليه ومستقر. وستواصل الهند العمل مع المجتمع العالمي للتصدي للتهديدات في الفضاء الإلكتروني وضمان استمرار الثورة الرقمية في إفادة البشرية من دون المساس برفاهها واستقرارها الجماعي.

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

السيد ماو (كمبوديا) (*تكلم بالإنكليزية*): في البداية، أود أن أعرب عن تقديري لكم، سيدي الرئيس، على عقد المناقشة المفتوحة الرفيعة المستوى اليوم، التي تتيح للدول الأعضاء تبادل وجهات نظرها بشأن الفضاء الإلكتروني، حيث أصبحت التهديدات في الفضاء الإلكتروني مصدر قلق متزايد لكل بلد. كما أشكر معالي السيد أنطونيو غوتيريش ومقدمي الإحاطتين والمتكلمين على ملاحظاتهم الثاقبة.

لا يمكن إنكار أن عالمنا الآن يعتمد بشكل كبير على التكنولوجيات الرقمية. لقد أتاح التقدم السريع لتكنولوجيا المعلومات والاتصالات إمكانيات هائلة، ولكنه يعرضنا أيضاً لمخاطر جديدة ومتغيرة تهدد السلم والأمن الدوليين. لقد أظهرت زيادة الهجمات في الفضاء الإلكتروني مؤخرا أن أنظمة تكنولوجيا المعلومات والاتصالات أصبحت أكثر عرضة للخطر من أي وقت مضى.

وفي هذا الصدد، تلتزم كمبوديا بتعزيز بيئة رقمية آمنة للجميع. نحن نستفيد من منتدى رابطة أمم جنوب شرق آسيا لتيسير برامج بناء القدرات وتعزيز تبادل أفضل الممارسات. ونؤمن إيماناً راسخاً بقوة التعاون الدولي ونحث المجتمع الدولي على تقديم المساعدة التقنية وتبادل المعرفة لتعزيز أمن الفضاء الإلكتروني، لا سيما في البلدان النامية.

على المستوى الوطني، اتخذت كمبوديا إجراءات حاسمة من خلال إنشاء لجنة الأمن الرقمي في وقت سابق من هذا العام. تقود هذه اللجنة، التي تتألف من الوزارات المعنية، جهودنا في مجال أمن الفضاء الإلكتروني، ومنع ارتكاب الجرائم فيه، وقدرات الدفاع عنه، ودبلوماسية الفضاء الإلكتروني. يتيح لنا هذا النهج المنسق تقييم احتياجاتنا ومعالجة الثغرات في المهارات وتنفيذ استراتيجيات فعالة لحماية بنيتنا التحتية الرقمية.

تقدر كمبوديا أهمية بناء القدرات في مجال امن الفضاء الإلكتروني. في الشهر الماضي، شارك وزير البريد والاتصالات السلكية واللاسلكية لدينا مشاركة فعالة في المائدة المستديرة العالمية حول بناء القدرات في مجال أمن تكنولوجيا المعلومات والاتصالات. ونثني على الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها، الذي ترأسه سنغافورة، لجهوده الدؤوبة في تعزيز الحوار والتعاون الدوليين بشأن هذه المسألة الحاسمة الأهمية.

وعلاوة على ذلك، تدعو كمبوديا إلى وضع أطر قانونية وقواعد دولية قوية تعزز السلوك المسؤول في الفضاء الإلكتروني، وتدعم السيادة الوطنية وتمنع الأعمال الخبيثة. إن التعاون بين الحكومات والشركات والمجتمع المدني أمر حيوي لتبادل المعلومات وتطوير حلول مبتكرة. كما نعطي الأولوية لمبادرات التثقيف والتوعية لتمكين مواطنينا بالمعرفة والمهارات اللازمة للتنقل في العالم الرقمي بأمان.

في الختام، تلتزم كمبوديا بالعمل مع جميع الدول لبناء مستقبل رقمي آمن وقادر على الصمود. ونؤكد من جديد التزامنا بالتعاون والتآزر سعياً لتحقيق مستقبل أقوى وأكثر أماناً وقدرة على الصمود في مجال الفضاء الإلكتروني للجميع. يؤمن وفد بلدي بأننا نستطيع معًا تهيئة فضاء إلكتروني يعزز الابتكار والنمو الاقتصادي ورفاه جميع مواطنينا.

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

السيد فرانسا دانيزي (البرازيل) (*تكلم بالإنكليزية*): أشكر جمهورية كوريا على عقد هذه الجلسة.

كما ذكرنا خلال اجتماع بصيغة آريا في نيسان/أبريل، نظمته جمهورية كوريا، فإن البرازيل تشارك العديد من الوفود الأخرى القلق

بشأن تطور مشهد التهديدات التي يتعرض لها أمن الفضاء الإلكتروني. ونحن متفقون أيضًا على الحاجة إلى حلول متعددة الأطراف يمكنها تحسين القدرة على الصمود في الفضاء الإلكتروني للجميع.

غير أننا ما زلنا مقتنعين بأن أفضل طريقة لتحقيق هذا الهدف هي أن تكون مناقشاتنا شاملة للجميع من دون تكرار عمل جار. وبينما نقدر الجهود الصادقة التي تبذلها جمهورية كوريا سعيا لإيجاد صيغ أوسع للمناقشات في مجلس الأمن، سواء من خلال صيغة آريا أو من خلال هذه المناقشة المفتوحة، فإننا نعتقد أن المحفل المناسب لهذه المناقشات لا يزال الجمعية العامة.

لقد شهدنا هذا العام حدود قدرات المجلس على وضع قواعد لمجالات جديدة عندما فشل مرتين في اعتماد مشروع قرار بشأن وضع أسلحة في الفضاء الخارجي (انظر S/PV.9616 و S/PV.9630). وفي كلتا المناسبتين، أعربت الوفود عن شواغلها بشأن طرح قضايا معقدة على المجلس من الأفضل أن يعالجها جميع الأعضاء في الأمم المتحدة. هذه الشواغل وجيهة وتنطبق في هذه الحالة أيضا.

يضطلع الفريق العامل المفتوح العضوية الحالي المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها بمهمة مناقشة هذا الموضوع تحديدا وحقق نتائج في تحديد التهديدات التي يتعرض لها الفضاء الإلكتروني. وقد سلط الضوء على تهديدات برمجيات انتزاع الفدية والعملات المشفرة، بالإضافة إلى وسائل الهجوم الأخرى، بما في ذلك على البنية التحتية الحيوية. وقد ناقش الآثار غير المباشرة للهجمات في الفضاء الإلكتروني وناقش كيفية حماية وتمييز الأنظمة ذات الأهمية الإنسانية الخاصة. وأوضح انطباق القانون الدولي والقانون الدولي الإنساني على الفضاء الإلكتروني. وهو يناقش حالياً تدابير ملموسة لتنفيذ إطار سلوك الدول المسؤول في الفضاء الإلكتروني. هذه إنجازات مهمة توضح جدوى وأهمية عقد هذه المناقشات في المنتدى المناسب.

وهذا لا يعني أن المجلس ليس له دور يضطلع به. واتساقاً مع صلاحياته ومهامه بموجب ميثاق الأمم المتحدة، يجوز لهذا الجهاز أن يستجيب لحوادث اختراق محددة وملموسة في الفضاء الإلكتروني تشكل تهديداً للسلم والأمن الدوليين.

في عصر توقف فيه تقريبا إحراز تقدم في مجال نزع السلاح، يبرز مجال أمن الفضاء الإلكتروني كنتيجة للتقدم الكبير الذي تحقق في الجمعية العامة. لنعمل من أجل الحفاظ على هذا الزخم.

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

السيدة رودريغيز مانسيا (غواتيمالا) (*تكلمت بالإسبانية*): تود غواتيمالا أن تشكر جمهورية كوريا، بصفتها رئيسة مجلس الأمن، على عقد هذه المناقشة المفتوحة المهمة.

يدرك وفد بلدي أن الفضاء الإلكتروني أصبح مجالاً محورياً ولا غنى عنه للنشاط على الصعيد العالمي، وبسبب طبيعته المدنية وذات الاستخدام المزدوج، فقد استخدمته الجماعات الإجرامية والإرهابية في أكثر من مناسبة. وقد أدى ذلك إلى زيادة استغلال البنية التحتية الحيوية وشن هجمات إلكترونية عليها، حيث تتأثر شبكات نقل الكهرباء وأنظمة النقل والمستشفيات والمدارس وغيرها، مما يؤثر تأثيرا مدمرا على حياة الناس والاقتصاد. لقد فتحت الشبكات المترابطة عالميا ورقمنة الاقتصاد العالمي مجالًا يمكن أن تشكل فيه انتهاكات أمن الفضاء الإلكتروني تهديدات اقتصادية وأمنية دولية كبيرة.

يمكن للأنشطة الخبيثة في الفضاء الإلكتروني أن تكون عاملا مضاعفا للنزاعات بعدة طرق. ويمكنها أن تزيد من حدة التوترات بين الدول من خلال تمكين شن هجمات سرية مع إمكانية الإنكار المعقول، وتعقيد عملية الإسناد وتعزيز عدم الثقة. بالإضافة إلى ذلك، يمكن للجهات الفاعلة الحكومية وغير الحكومية استخدام الفضاء السيبراني للدعاية والتضليل والتجسس، وبث الانقسامات الداخلية وتأجيج النزاعات الداخلية والعابرة للحدود الوطنية.

وعلاوة على ذلك، لا يمكن إنكار أن الذكاء الاصطناعي يمثل فرصة مهمة للغاية للمساهمة في تقدم البشرية، بدءًا من منع الأزمات ومعالجتها، إلى تنفيذ خدمات الرعاية الصحية والتعليم، وتوسيع نطاق

عمل الحكومات والمجتمع المدني والأمم المتحدة في جميع المجالات. لكن الاستخدام الخبيث للذكاء الاصطناعي يمكن أن يؤدي إلى تقويض الثقة في المؤسسات وإضعاف التماسك الاجتماعي وتهديد الديمقراطية. وفي ضوء ما سبق ذكره، يرى وفد بلدي ضرورة تعزيز الجهود المبذولة حاليا، أولا، من أجل الوقاية، وثانيا، لمواجهة التهديدات القائمة والمحتملة.

وقد جرى بالفعل اتخاذ بعض الخطوات لإدماج مسائل الأمن السيبراني في برامج عمل هذه المنظمة. ومع ذلك، فمن الضروري تعزيز الجهود الرامية إلى إضافة هذه المسائل بفعالية إلى جدول أعمال مجلس الأمن من خلال اتخاذ إجراءات قوية. ومن الأمثلة على هذه الإجراءات إنشاء آلية لفرض جزاءات لتنظيم السلوك في الفضاء السيبراني؛ وزيادة المساعدة المقدمة إلى الدول لتعزيز قدراتها في مجال الأمن السيبراني، ومواصلة العمل مع القطاع الخاص والمجتمع المدني لوضع استراتيجيات قوية للرقابة على تكنولوجيا المعلومات والاتصالات.

ويجب أن يؤدي مجلس الأمن دورا قياديا أكبر في مكافحة التهديدات السيبرانية التي تقوض السلام والأمن الدوليين.

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

السيد كريديلكا (بلجيكا) (*تكلم بالإنكليزية*): في البداية، أتوجه بجزيل الشكر إلى جمهورية كوريا على تنظيم هذه الجلسة.

يشرفني أن أدلي بهذا البيان باسم البلدان الأعضاء في اتحاد بنلوكس – لكسمبرغ ومملكة هولندا وبلدي بلجيكا. وتؤيد بلدان اتحاد بنلوكس البيان الذي أدلي به باسم الاتحاد الأوروبي. ونود أن نؤكد على أربع نقاط إضافية.

أولاً، فيما يتعلق بالتهديدات، كما ذكرنا سابقًا في المجلس، لا تزال بلدان اتحاد بنلوكس تشعر بقلق عميق إزاء التهديد المتزايد والآخذ في التطور للأنشطة السيبرانية الخبيثة. ويستمر هذا التهديد في الارتفاع من حيث الحجم، وقد يتفاقم بسبب التقنيات الناشئة، بما في ذلك تقنيات الذكاء الاصطناعي والتقدم في الحوسبة الكمية. وأحد الاتجاهات المثيرة للقلق التي نلاحظها هو زيادة هجمات برمجيات انتزاع الفدية، واستخدام برمجيات انتزاع الفدية كخدمة والتهديدات السيبرانية الخبيثة، التي تستهدف البنية التحتية الحيوية، بما في ذلك قطاعي الصحة والتعليم، والعمليات الانتخابية. وتشكل آثار هذه الحوادث وخطر امتداد آثارها تهديدًا للسلام والأمن الدوليين.

وهذا يقودني إلى نقطتي الثانية. في إطار اللجنة الأولى للجمعية العامة، اعتمدنا جميعاً بتوافق الآراء إطار الأمم المتحدة لسلوك الدول المسؤول في الفضاء السيبراني. ويؤكد الإطار أن القانون الدولي، ولا سيما ميثاق الأمم المتحدة، ينطبق على الفضاء السيبراني. ويبقى تنفيذ الإطار أمراً أساسياً للتصدي للتهديدات القائمة والمحتملة المتعلقة بتكنولوجيا المعلومات والاتصالات على الأمن الدولي. وفي هذا الصدد، تؤيد بلدان اتحاد بنلوكس إنشاء برنامج عمل الأمم المتحدة للارتقاء بسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي. وتشمل عمليات الأمم المتحدة الأخرى ذات الصلة وضع اتفاقية للأمم المتحدة لمكافحة الجريمة السيبرانية.

بالإضافة إلى ذلك – وهذه هي نقطتي الثالثة – فبموجب الفصل السادس من ميثاق الأمم المتحدة، فإن لمجلس الأمن دورا واضحا في التسوية السلمية للمنازعات، بما في ذلك في المجال السيبراني، وذلك بدعوة الأطراف إلى تسوية أي نزاع من المحتمل أن يعرض صون السلام والأمن الدوليين للخطر. ونحن في بلدان اتحاد بنلوكس نرى أن للمجلس دوراً مهمًا في تعزيز المجال السيبراني المفتوح والحر والآمن. ولذلك فإننا نرحب باهتمام المجلس المتزايد بالأمن السيبراني، كما يشهد على ذلك ارتفاع عدد الجلسات التي عُقدت بشأن المسائل المتعلقة بالفضاء الإلكتروني منذ عام 2016. وتُظهر النزاعات الجارية أن المتعلقة بالفضاء الإلكتروني جزء لا يتجزأ من الأخطار الأوسع نطاقاً التي تهدد السلام والأمن الدوليين. ولذلك، فإن بلدان اتحاد بنلوكس تؤيد أيضاً اقتراحاتكم، سيدي الرئيس، بشأن تعميم المسائل السيبرانية في العمل الحالي للمجلس.

وأخيراً – وهذه هي نقطتي الرابعة – تدعو بلدان اتحاد بنلوكس إلى إيلاء مزيد من الاهتمام بضحايا العمليات السيبرانية. وفي حين أن

الأنشطة السيبرانية الخبيثة غالباً ما يُنظر إليها من منظور المنافسة الجيوسياسية، فإن لها آثارا مدمرة على الناس، مما يحد بشدة من حقوق الإنسان. لذلك، ومن أجل الحفاظ على رفاه الإنسان وكرامته في صدارة مناقشاتنا، فإننا ندعو إلى اتباع نهج يركز على الضحايا.

وينبغي ألا ننسى مخاطر الحماية الكبيرة التي يشكلها التحول الرقمي، بما في ذلك في الفضاء السيبراني، على الأشخاص المتضررين من الأزمات الإنسانية. ونرى أن اللجنة الدولية للصليب الأحمر، بسبل من بينها مركزها السيبراني العالمي، ومقره في لكسمبرغ، هي في طليعة الجهات التي تتصدى لبعض هذه التحديات، على سبيل المثال، من خلال تطوير واختبار أدوات جديدة لتقديم الخدمات الرقمية للسكان المتضررين بطريقة محايدة ونزيهة ومستقلة.

ونحن في بلدان اتحاد بنلوكس نشكركم، سيدي الرئيس، مرة أخرى على تنظيم هذه المناقشة، ونشيد بجهودكم لزيادة الوعي ومعالجة أهمية التهديدات السيبرانية.

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

السيد لوفولد (النرويج) (*تكلم بالإنكليزية*): يسرني أن أتكلم باسم بلدان الشمال الأوروبي: آيسلندا، والدانمرك، والسويد، وفنلندا وبلدي، النرويج.

أود أن أبدأ بشكر جمهورية كوريا على مبادرتها بتنظيم هذه الجلسة التي جاءت في الوقت المناسب. وهذه هي المرة الثانية فقط التي يتناول فيها المجلس رسمياً موضوع الأمن السيبراني المهم.

إن التطورات في مجال التهديدات السيبرانية لا تزال مثيرة للقلق منذ أن ناقش المجلس هذه المسألة لأول مرة تحت رئاسة إستونيا في عام 2021 (انظر S/2021/621).

وأود أن أسلط الضوء بسرعة على ثلاثة أنواع من التهديدات.

أولاً، استمر التهديد الناجم عن الأعمال السيبرانية التي ترعاها الدول، وعلى الخصوص في سياق الحرب العدوانية غير القانونية التي تشنها روسيا على أوكرانيا. ولقد استُخدمت قدرات روسيا السيبرانية كسلاح في أوكرانيا في محاولة لتقويض الثقة في السلطات وتدمير البنية التحتية الحيوية. ولا نزال نولي أهمية للدفاع السيبراني في أوكرانيا، وكذلك لحماية مجتمعاتنا من الجهات الفاعلة الخبيثة. وفي هذا السياق، نود أن نؤكد مرة أخرى على أن القانون الدولي ينطبق أيضاً في الفضاء السيبراني.

ثانياً، ي تزايد تمييع الخطوط الفاصلة بين الجهات الفاعلة التي ترعاها الدولة والجهات الفاعلة من غير الدول والجهات الإجرامية. وتشمل المخاوف الرئيسية تزايد عدد هجمات برمجيات انتزاع الفدية وإمكانية وصول الأدوات والتقنيات السيبرانية المتقدمة إلى مجموعة أوسع من الجهات الفاعلة من الدول ومن غير الدول على حد سواء.

أخيراً، وبما يرتبط بكل هذه التهديدات، هناك مصدر قلق خاص يتمثل في تزايد استهداف الجهات الخبيثة للقطاعات الحيوية والبنية التحتية الحيوية.

ومن أجل التصدي لهذه التهديدات، تود بلدان الشمال الأوروبي أن تسلط الضوء بشكل خاص على أهمية مشاركة أصحاب المصلحة المتعددين في مجال الأمن السيبراني. ويجب أن نسعى جاهدين لتعزيز التنسيق بين الحكومات وجميع أصحاب المصلحة المعنيين، بما في ذلك المجتمع المدني والأوساط الأكاديمية والقطاع الخاص. ويؤدي القطاع الخاص دوراً أساسياً في الفضاء السيبراني بفضل قدرته على الوصول إلى المعلومات، حيث تؤدي شركات التكنولوجيا والأمن السيبراني دوراً رئيسياً في التنبؤ بالتهديدات والاستجابة لها. ومن المهم الاستفادة بشكل أفضل من معارف أصحاب المصلحة المعنيين وقدراتهم لدعم فضاء سيبراني حر ومفتوح وسلمي وآمن.

وفي ضوء تطور مشهد التهديدات، ترى دول الشمال الأوروبي فائدة متزايدة في مناقشة مجلس الأمن للأمن السيبراني بشكل أكثر انتظاماً. ويمكن أن تساعد المناقشات في مجلس الأمن حول التهديدات السيبرانية الحالية والناشئة خلال المناقشات المواضيعية والمناقشات الخاصة بكل بلد على حدة في زيادة الوعي بالتهديدات وتبادل الدروس المستفادة وصياغة الاستجابات المناسبة.

كما يكمل عمل المجلس المناقشات التي تجري في المنتديات الأخرى. ومع أخذ ذلك في الاعتبار، وفي الختام، أود أن أؤكد من جديد دعم بلدان الشمال الأوروبي لإنشاء برنامج عمل بشأن الأمن السيبراني كآلية دائمة وشاملة للجميع وعملية المنحى للنهوض بسلوك الدول المسؤول في هذا المجال.

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

السيد سيمونوفيتش (كرواتيا) (*تكلم بالإنكليزية*): أشكركم، سيدي الرئيس، على تنظيم هذه المناقشة المفتوحة حسنة التوقيت، وأشكر مقدمي الإحاطتين على إسهاماتهما.

تؤيد كرواتيا البيان الذي أدلت به ممثلة الاتحاد الأوروبي، وأود أن أدلي ببعض الملاحظات بصفتي الوطنية.

نحن نواجه عدداً متزايداً من التهديدات المعقدة في الفضاء الإلكتروني. وتشمل هذه التهديدات هجمات برمجيات انتزاع الفدية التي تستهدف البنية التحتية الحيوية، والحملات المستمرة والتدخل الأجنبي في العمليات الديمقراطية، على سبيل المثال لا الحصر. ولكل من هذه الأنشطة القدرة على زعزعة استقرار الحكومات بشكل خاص، والسلام والأمن بشكل عام.

ففي مناطق النزاع، يمكن أن تفاقم العمليات في الفضاء الإلكتروني من آثار الحرب التقليدية، خاصة عند استهداف البنية التحتية الحيوية، مما يؤدي إلى تصعيد الأعمال العدائية والمزيد من الأضرار المدنية. وفي هذا الصدد، نشيد باللجنة الدولية للصليب الأحمر على عملها في تسليط الضوء على أن الفضاء الإلكتروني ليس مجالاً لا يسود فيه القانون، ونؤكد أن القانون الدولي الإنساني ينطبق على حد سواء في المجالين المادي والإلكتروني.

ولهذا السبب ينبغي لمجلس الأمن أن ينظر في زيادة تطوير فهمه لهذه المسألة بالغة التعقيد، ليس من خلال التبادل المنتظم للآراء مع أصحاب المصلحة المتعددين في مجال أمن الفضاء الإلكتروني فحسب، ولكن أيضًا في مجال بناء السلام، وكذلك في جهود منع نشوب النزاعات والوساطة. ويمكن تحقيق ذلك من خلال عقد جلسات إحاطة منتظمة وتقديم تقارير دورية عن التهديدات في الفضاء الإلكتروني، بما يضمن إطلاع المجلس والدول الأعضاء على آخر التطورات والاتجاهات.

وعلاوة على ذلك، فإن دور مجلس الأمن في التصدي للتهديدات في الفضاء الإلكتروني يمكن أن يتطور بطريقة تكميلية ومتعاضدة، إلى جانب العمل الحالي لهيئات الأمم المتحدة الأخرى والمبادرات المتعددة الأطراف. ويشمل ذلك عمل الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات واستخدامها والأطر الأخرى ذات الصلة والمستقبلية، بما يضمن اتباع نهج منسق وشامل على نطاق المنظومة. ويمكن للمجلس أيضًا أن يستكشف مساهمته في تخفيف حدة التوترات من خلال تعزيز الحوار وتدابير بناء الثقة بين الدول، مما يقلل من خطر تصاعد النزاعات في الفضاء الإلكتروني إلى مواجهات مسلحة.

ويمكن للمجلس أن يضطلع بدور مهم في منظومة الأمم المتحدة الحالية لأمن الفضاء الإلكتروني وأن يحافظ بشكل أفضل على السلم والأمن الدوليين في العصر الرقمي، من خلال اتخاذ خطوات استباقية لفهم التهديدات في الفضاء الإلكتروني والتخفيف من حدتها، وتعزيز التعاون الدولي وإدماج الاعتبارات المتعلقة بالفضاء الإلكتروني في ولايته الأوسع.

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

السيدة نارفايز أوهيدا (شيلي) (*تكلمت بالإسبانية*): إننا نقدر فرصة المشاركة في هذه المناقشة المفتوحة. نحيط علماً بالعروض والمساهمات التي استمعنا إليها اليوم من المتكلمين. ونغتنم هذه الفرصة لتهنئة جمهورية كوريا على رئاستها لمجلس الأمن هذا الشهر.

كما ذكرنا في مناسبات سابقة، تعتقد شيلي أن الهجمات في الفضاء الإلكتروني والأنشطة الخبيثة فيه تشكل تهديداً للسلم والأمن الدوليين ويمكن أن تؤثر على الدول بطرق مختلفة رهنا، بشكل جزئي، بمستويات الرقمنة والقدرات والأمن والبنية التحتية والتنمية فيها. وعلى وجه الخصوص، نسلط الضوء على أن هذه التهديدات يمكن أيضا أن تؤثر بشكل متباين على مختلف الفئات والكيانات، لا سيما النساء والفتيات والفتيان والمراهقين.

وفيما يتعلق بالاتجاهات الناشئة والمتطورة في الأنشطة الخبيثة في الفضاء الإلكتروني، نلاحظ استخدام الذكاء الاصطناعي والتعلم الآلي، والجمع بين مختلف تكتيكات وسائل الهجوم، والهجمات على سلاسل الإمداد د التي تعرض للخطر سلامة المنتجات والخدمات، والهجمات على أجهزة إنترنت الأشياء، وغيرها.

كما نلاحظ الخطر الذي تشكله البرمجيات الخبيثة مثل برمجيات انتزاع الفدية وبرمجيات محو البيانات وبرمجيات أحصنة طروادة، إلى جانب تقنيات مثل برمجيات التصيد الإلكتروني وهجمات الحرمان من خدمة الإنترنت بعرقلة تدفق المعلومات. وفي حال وقوع هذه الوسائل في أيدي جهات خبيثة، يمكن لهذه التهديدات أن تلحق أضرارا جسيمة بأداء البلدان لمهامها وتؤثر على اقتصاداتها ورفاه شعوبها.

لذلك نعتقد أنه من الضروري تعزيز العمل المشترك والتعاون فيما بين الدول. ويشمل ذلك تبادل الخبرات والدروس المستفادة، وتنفيذ المعايير القائمة لسلوك الدول المسؤول في الفضاء الإلكتروني، وتطبيق القانون الدولي والقانون الدولي الإنساني، وتدابير بناء الثقة وبناء القدرات، وكلها أمور تساعد على الحد من انعدام الثقة فيما بين الدول وتسهم في تحقيق الاستقرار في الفضاء الإلكتروني. وتشجع شيلي على ما سبق ذكره، وتشير إلى أن جميع المداولات والمناقشات ذات الصلة يجب أن تشمل جميع الأطراف المعنية، مثل المجتمع المدني والأوساط الأكاديمية والقطاع الخاص والمجتمع التقني، من بين الجهات الفاعلة الأخرى ذات الصلة.

ونشدد على أهمية تعزيز دور مجلس الأمن في التصدي للتهديدات في الفضاء الإلكتروني ونعتقد أنه يمكن أن يسهم بشكل كبير في إيجاد فضاء إلكتروني آمن ومفتوح وسلمي لصالح جميع الدول. تولي شيلي أهمية كبيرة لهذه المسألة تحديداً، حيث تستغل الجهات الفاعلة الخبيثة نقاط ضعف البلدان التي تفتقر إلى الأدوات والتدريب اللازمين للتعامل مع مثل هذه التهديدات.

ومن هذا المنطلق، يمكن للمجلس أن يكون أداة قيمة لتوليد أحياز للحوار والتعاون فيما يتعلق ببناء القدرات والمساعدة التقنية، وهو ما يمكن أن يفيد البلدان التي هي في أمس الحاجة إليها. وندعو إلى أن يتصدى هذا الجهاز للتحدي المتمثل في المشهد المتغير لتهديدات الفضاء الإلكتروني، إلى جانب التعاون الدولي، وهو ما نعتقد أنه يجب أن يكون محل إجماع.

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

السيد ثابا (نيبال) (*تكلم بالإنكليزية*): بداية، أود أن أشكر رئاسة جمهورية كوريا على عقد هذه المناقشة المفتوحة. كما أود أن أشيد بمقدمي الإحاطتين على مساهماتهما الثاقبة والقيّمة.

لقد أحدثت التطورات السريعة في تكنولوجيا المعلومات والاتصالات والذكاء الاصطناعي ثورة في حياتنا، مما أتاح فرصًا غير مسبوقة لتسريع وتيرة التنمية الاجتماعية والاقتصادية. ما فتئ اعتمادنا على التكنولوجيا يتزايد باستمرار. لكن سوء استخدامها ولد تهديدات جديدة وخطيرة. ونشعر بالقلق إزاء تصاعد حالات هجمات انتزاع الفدية وجرائم الفضاء الإلكتروني وانتشار المعلومات المغلوطة والكراهية في جميع أنحاء العالم.

لا توجد بنية تحتية أو نظام بمنأى عن الهجمات عبر الفضاء الإلكتروني – سواء كانت بنية تحتية مدنية، مثل المؤسسات المالية أو المستشفيات أو أنظمة النقل أو المياه أو إمدادات الطاقة، أو نظام القيادة والتحكم العسكري للأسلحة النووية أو منظومات الأسلحة الذاتية التشغيل. وهذا يشكل تحديات للسلم والأمن والاستقرار والتنمية على الصعيد الدولي.

كما أننا في نيبال نواجه تحديات هائلة جراء هذا الخطر، حيث تتعرض المؤسسات المصرفية والمواقع الإلكترونية الحكومية والخوادم في نيبال لهجمات إلكترونية وهجمات انتزاع الفدية من وقت لآخر.

وفي هذا السياق، أود أن أسلط الضوء على بعض النقاط.

أولاً، نحن بحاجة إلى تطبيق مجموعة قوية من القواعد المستندة إلى المعايير المقبولة للقوانين الدولية، بما في ذلك ميثاق الأمم المتحدة، مع ضمان انفتاح الفضاء الإلكتروني واستقراره وأمنه. ينبغي أن نطور فهماً مشتركاً لتطبيق القواعد ونعزز تدابير بناء الثقة في

الفضاء الإلكتروني، وكذلك في تعزيز سلوك الدول المسؤول في الفضاء الإلكتروني.

ثانياً، يجب أن نعقد جلسات إحاطة ونجري تقييمات منتظمة تتضمن رؤى من الشركات التي تقودها التكنولوجيا والقطاع الخاص والمجتمع المدني والأوساط الأكاديمية، لتبادل معارفها وأفضل الممارسات حول الكيفية التي يمكننا بها أن نبقى مستعدين لمواجهة التهديدات المتغيرة في الفضاء الإلكتروني.

ثالثاً، إن دولاً مثل نيبال أكثر عرضة لهذه التهديدات الناشئة. إن الافتقار إلى الأطر القانونية والتنظيمية الملائمة ومحدودية القدرات البشرية والموارد المالية من بين التحديات التي نواجهها في الاستعداد لمنع تلك التهديدات والتصدي لها. ولذلك، يشكل الدعم والمساعدة المستمرين على الصعيد الدولي أمرين حاسمين لتعزيز قدرات بلدان مثل نيبال لتمكينها من منع الهجمات السيبرانية والتصدي لها. وينبغي أن ننهوض بالشراكات بين أصحاب المصلحة المتعددين من أجل سد الثغرات القائمة على مستوى المؤسسات والمهارات والقدرات والتكنولوجيا والموارد.

رابعاً، ينبغي أن نعزز الأمن السيبراني من خلال التنمية الشاملة والازدهار للجميع من خلال سد الفجوات الرقمية بين الدول.

ختاما، فإن التهديدات السيبرانية التي نواجهها تهديدات كبيرة. ويمكننا ضمان فضاء سيبراني آمن ومفتوح وسلمي للجميع من خلال اتخاذ إجراءات استباقية شاملة ومنسقة. وإذ نمضي قدماً في تنفيذ خطتنا الرامية إلى تحقيق مستقبل رقمي مستدام للجميع، يجب أن نبني معا مجتمعا عالميا مرنا قادرا على الصمود في مواجهة تهديدات العصر الرقمي والتغلب عليها.

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

السيد مغيث (بنغلاديش) (*تكلم بالإنكليزية*): أشكر جمهورية كوريا، الرئاسة الحالية لمجلس الأمن، على عقد هذه المناقشة المفتوحة المهمة. وأشكر أيضا مقدمي الإحاطات على عروضهم المستنيرة.

أصبحت التهديدات السيبرانية في المشهد الرقمي المتغير منتشرة ووشيكة في كثير من الأحيان، مما يؤدي إلى تعطيل الهياكل المالية والديمقراطية والاجتماعية والثقافية والأمنية العالمية. ويشدد تقرير المخاطر العالمية لعام 2024 على أن التهديدات السيبرانية أحد أخطر التحديات في عصرنا الحالي ويقدّر أن التكاليف المحتملة للجرائم السيبرانية ستبلغ 24 تريليون دولار بحلول عام 2027. ويتطلب منا هذا الرقم الصاعق اتخاذ إجراءات فورية وعاجلة. ولكن بغض النظر عن التكلفة من الناحية الاقتصادية، لا يمكن الاستهانة بالتأثير المروع للجريمة السيبرانية على الأفراد والمجتمعات.

للإجابة على أسئلة الرئيس التوجيهية، أود أن أسلط الضوء على عدة نقاط.

أولاً، يتعرض السلام والاستقرار العالميان لمخاطر كبيرة بسبب انتشار التهديدات السيبرانية، بما في ذلك الهجمات ببرمجيات انتزاع الفدية والتجسس الإلكتروني وحملات نشر المعلومات المغلوطة والمضللة من خلال التزييف العميق وغيرها من الوسائل. وتستهدف هذه التهديدات البنية التحتية الحيوية وتقوض العمليات الديمقراطية والوئام المجتمعي من خلال نشر كراهية الأجانب والتعصب والقوالب النمطية. بالإضافة إلى ذلك، أدى التقدم في مجال الذكاء الاصطناعي والحوسبة الكمية إلى توسيع نطاق التهديدات السيبرانية وزيادة تعقيدها. وباعتماد البلايين من الناس على المنصات الرقمية في أنشطتهم اليومية، أضحى التصدي لهذه التهديدات أكثر إلحاحا من أي وقت مضى.

ثانيًا، نعتقد اعتقادا راسخًا بأننا لن نكون أقوياء في مواجهة هذه التهديدات الخطيرة إلا بقدر قوة أضعف حلقاتنا. وبالتالي، لا غنى اليوم عن تعزيز التعاون والتنسيق الدوليين. ولا بد من تعزيز تدابير الأمن السيبراني وتشجيع آليات تبادل المعلومات والاستثمار في مبادرات بناء القدرات من أجل تعزيز القدرة على الصمود في مواجهة التهديدات السيبرانية. وفي هذا الصدد، نؤكد على أهمية احترام مبدأ المساواة في السيادة والقانون الدولي في المجال الرقمي. ويجب علينا إيجاد طرق لتحقيق التوازن بين حرية التعبير والحاجة إلى مكافحة النشر الضار للمعلومات المغلوطة.

ثالثاً، نشيد في هذا المشهد السيبراني السريع التطور بالفريق العامل المفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات وأمن استخدامها على تيسير النقاش والتعاون الدوليين الضروريين. وتظل الجمعية العامة، التي تجسد الإرادة العالمية للمجتمع الدولي وتطلعاته، المنصة الرئيسية لهذه المناقشات الهامة، مما يتيح لجميع الدول المشاركة بفعالية في تشكيل مستقبلنا السيبراني الجماعي. ونأمل أيضًا أن يؤدي الاتفاق الرقمي العالمي الذي يجري إعداده دوراً حاسمًا في معالجة هذه المسألة وندعو إلى اتباع نهج تعاوني بين الجمعية العامة ومجلس الأمن من أجل التنفيذ الفعال للاتفاق.

أخيراً، فيما يتعلق بمسألة ما إذا كان التصدي للتهديدات المتطورة في الفضاء السيبراني يندرج ضمن اختصاص المجلس، وبما أنه ليس جزءاً من المفهوم التقليدي للأمن، نعتقد أن الأمن السيبراني يستحق أقصى درجات الاهتمام من الأمم المتحدة نظراً للتهديدات الناشئة التي تشكلها هذه المسألة على السلام والأمن. وينبغي إجراء حوارات مفتوحة وشفافة لتحديد المنصة المناسبة لمعالجة هذه المسألة الحاسمة، بدلاً من أن تصبح مجالاً آخر للاختلاف والاستقطاب.

وفي الوقت نفسه، نعتقد أن المجلس قد يؤدي دورا حيويا في تعزيز تدابير بناء الثقة، بما في ذلك من خلال تبادل المعلومات والآراء على نحو فعال. ويجب أن نعمل معا لوضع قواعد ومعايير ولوائح تعزز بيئة رقمية آمنة ومأمونة وغير تمييزية ومستقرة للجميع، سواء كان ذلك تحت رعاية المجلس أو في أي محفل مناسب آخر في الأمم المتحدة بما في ذلك الفريق العامل المفتوح العضوية. وتؤكد بنغلاديش من جديد التزامها بالتعاون مع المجتمع العالمي للتصدي لتهديدات الأمن السيبراني العالمي المتغيرة.

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

السيد دانغ (فييت نام) (*تكلم بالإنكليزية*): ما فتئت التهديدات في الفضاء السيبراني تتطور من حيث الحجم والتعقيد على حد سواء، مما يشكل تحديات كبيرة للسلام والأمن الدوليين. وتشمل تلك التهديدات الأنشطة السيبرانية الخبيثة، بما في ذلك التجسس والهجمات التي تستهدف البنية التحتية الحيوية واختراق البيانات، والمعلومات المغلوطة والمضللة والحرب النفسية السيبرانية. ويمكن أن تشكل هذه الأنشطة خطرا كبيرا على الأمن القومي وتتسبب في أضرار اقتصادية بالغة وتقوض ثقة الجمهور في المؤسسات.

لا يوجد بلد محصن ضد هذه التهديدات. ولا شك أن البلدان النامية، على وجه الخصوص، التي تفتقر في الغالب إلى قدرات قوية في مجال الأمن السيبراني، الأكثر عرضة للخطر وتُستخدم أحيانا كحقل تجارب للحرب السيبرانية التي تشنها الدول القومية وللجرائم السيبرانية التي ترتكبها جهات من غير الدول.

وعلى الصعيد العالمي، قد تؤدي الهجمات السيبرانية إلى نشوب نزاعات وتفاقم التوترات الجغرافية السياسية نظراً إلى طابع الفضاء السيبراني المتخطي للحدود وتحديات الإسناد. وبالتالي، تتطلب معالجة هذه المسألة المعقدة اتباع نهج متعدد الأوجه تؤدي فيه الأمم المتحدة دوراً مهمًا.

أولاً، من الضروري أن تلتزم الدول بالمعايير والقواعد القائمة للقانون الدولي المنطبق التي تشكل دليلاً شاملاً لسلوك الدول في الفضاء السيبراني، وتنفذها.

وفي الوقت نفسه، ينبغي أن نواصل تعزيز الإطار الدولي الذي ينظم الأنشطة السيبرانية لزيادة تعزيز السلام والأمن والتعاون بين البلدان في المجال الرقمي، ولا سيما من خلال الالتزام بالعمليات الجارية المتعلقة بهذا المجال، بما في ذلك الاتفاق الرقمي العالمي واتفاقية مكافحة الجريمة السيبرانية.

ثانياً، يعد بناء القدرات أمراً أساسياً للحفاظ على فضاء سيبراني مفتوح وآمن ومستقر وسلمي وقادر على الصمود، خاصة بالنسبة لتلك الدول التي تملك قدرات سيبرانية محدودة، من أجل منع آثار الأنشطة السيبرانية الخبيثة والاستعداد لها والاستجابة لها بفعالية. ومن الأهمية بمكان أن يتشاطر جميع الدول هدفا مشتركا يتمثل في تعزيز القدرات وتضييق الفجوة التنموية في مجال تكنولوجيا المعلومات والاتصالات بين البلدان والمناطق.

ثالثاً، ينبغي أن يولي المجلس، بالنظر إلى ولايته، مزيداً من الاهتمام لهذه المسألة وأن يعالج الروابط القائمة بين التهديدات السيبرانية والمسائل الرئيسية الأخرى المدرجة في جدول أعماله مثل منع نشوب النزاعات ومكافحة الإرهاب وحماية البنية التحتية الحيوية. ومن الضروري أيضاً أن يعمل المجلس على تعزيز التعاون مع هيئات الأمم المتحدة الأخرى والمنظمات الإقليمية والقطاع الخاص من أجل بلورة استجابة موحدة وشاملة للتهديدات السيبرانية.

واتبعت حكومة فييت نام نهجاً شاملاً على مستوى المجتمع من أجل التصدي للتهديدات السيبرانية بسن قانون الأمن السيبراني في عام 2018. وتكرر فييت نام دعمها للجهود العالمية المتضافرة الرامية إلى وضع أطر وآليات قوية تهدف إلى احترام مبادئ السيادة وعدم التدخل والسلوك المسؤول في الفضاء السيبراني. ويمكننا أن نتصدى بفعالية للتحديات التي تقترن بالتكنولوجيات المتطورة من خلال الحوار والتعاون البنّاءين، مع الحفاظ على سلامة الفضاء السيبراني العالمي ومنظومة المعلومات.

السيدة أوبونغ – نتيري (غانا) (*تكلمت بالإنكليزية*): أبدأ بشكركم، سيدي الرئيس، على تنظيم مناقشة اليوم المفتوحة بشأن هذا الموضوع الهام. ونعرب عن امتناننا أيضًا لمقدمي الإحاطات على آرائهم الثاقبة.

وبينما تؤمن غانا بمدى التأثير المهيمن لثورة تكنولوجيا المعلومات والاتصالات، فإنها تظل مدركة تمامًا للمخاطر التي تشكلها تلك الثورة أيضًا على السلام والأمن الدوليين. وبالقرب من وطننا، في القارة الأفريقية، شهدنا تأثيرات وآثار النمو المتسارع لتكنولوجيا المعلومات والاتصالات، التي تفضي إلى تعديلات على مجموعة متنوعة من التحديات والتهديدات للأمن الوطني. وسواء كان الأمر يتعلق باستراق الهوية الرقمية وسرقة الهوية، أو تجنيد الإرهابيين لأتباعهم أو تجارة الأسلحة الصغيرة والذخيرة على الشبكة الخفية، فإن المخاطر الأمنية من العالم الرقمي لا تهدأ. ولم تسلم الشركات الخاصة والبنية التحتية العامة الحيوية من المخاطر، مما يشكل مخاطر جسيمة على السلام والاستقرار في بعض الحالات. وحتى في مجال الحكم الديمقراطي، فإن التأثير الإيجابي لتكنولوجيا المعلومات والاتصالات في تمكين المواطنين الأفارقة من النهوض بالقضايا السياسية التي يختارونها في إطار حرية تكوين الجمعيات والتجمع، قد تعرض لصعوبات ضخمة من جراء سوء استخدام هذه التكنولوجيا في نشر الأخبار الكاذبة والمعلومات المضللة والمعلومات المغلوطة، وهو ما يشكل خطراً كبيراً على الوحدة الوطنية والتماسك الوطني.

وفي حين أنه يجب بناء قدرات دفاعية سيبرانية قوية للتصدي لهذه الاتجاهات المتزايدة، التي تقلل من وثقته الجمهور في الحكومة، فإننا ننبه إلى الحاجة إلى استجابة مدروسة لتجنب التجاوزات الحكومية والإجراءات التي تنتقص من حقوق وحرية المواطنين، والتي يمكن أن تصبح بمفردها مصدراً للسخط وعدم الاستقرار. وبالفعل، وإدراكًا للتحدي الذي يواجه إفريقيا، اتخذ قادة قارتنا العديد من التدابير لتعزيز دفاعاتها السيبرانية. فخلال الدورة العادية السابعة والثلاثين لجمعية رؤساء دول وحكومات الاتحاد الأفريقي، التي عُقدت هذا العام، احتل الأمن السيبراني مركز الصدارة، حيث اتُخذت قرارات رئيسية لتعزيز جدول أعمال الاستراتيجية الأفريقية للتحول الرقمي. وبالإضافة إلى الدفع نحو الإسراع في وضع استراتيجية قارية للأمن السيبراني، اتفق القادة الأفارقة على موقف مشترك بشأن تطبيق القانون الدولي في الفضاء السيبراني. ونتفق على أنه لا يزال هناك الكثير مما يجب القيام به لإنشاء فضاء سيبراني جدير بالثقة وقادر على التصدي للتهديدات الآخذة في التطور باستمرار. ويجب علينا بذل كل جهد ممكن لسد الفجوة الرقمية من خلال بناء القدرات والمساعدة التقنية.

وفي معرض الرد على السؤال المتعلق بالدور الذي يمكن أن يضطلع به مجلس الأمن في التصدي للأخطار التي تهدد السلام والأمن الدوليين في الفضاء السيبراني، تود غانا أن تثير النقاط الإضافية الثلاث التالية.

أولاً، من أجل الاستفادة الكاملة من الإمكانات الهائلة التي يتيحها الفضاء السيبراني لتحقيق النمو والازدهار، يجب أن يكون هناك عمل عالمي متضافر لمعالجة المخاطر الناشئة ولجعل الفضاء السيبراني

موثوقا وآمنا ومرنا لصالح الجميع. وهذا ما يؤكد أهمية التقارير التي صدرت بتوافق الآراء عن الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات وأمن استخدامها، وفريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي، والتي لا تترك لنا مجالاً للشك في أن القانون الدولي وميثاق الأمم المتحدة قابلان للتطبيق وضروريان لصون السلام والأمن والاستقرار في بيئة تكنولوجيا المعلومات والاتصالات.

ثانياً، إن المناقشة المفتوحة التي جرت اليوم، وهي إحدى المناقشات القليلة في الآونة الأخيرة حول هذا الموضوع، خطوة مهمة أخرى في الاعتراف بالأخطار المتزايدة التي تشكلها الجهات الفاعلة الخبيثة في الفضاء السيبراني على السلام والاستقرار العالميين. وينبغي أن تهدف أعمال المجلس إلى أن تكون مكملة لدور الجمعية العامة في وضع وتعزيز معايير السلوك المسؤول في الفضاء السيبراني. كما يمكن أن تنظر أيضاً في تشجيع وضع إطار عمل ملزم قانوناً للمجال الرقمي لتنظيم أي تصرفات من جانب كيانات حكومية أو غير حكومية تهدد السلام والأمن الدوليين. ويمكن لإطار من هذا القبيل أن يستفيد من خبرات أصحاب المصلحة الرئيسيين في مجال تكنولوجيا المعلومات والاتصالات من أجل تنسيق الجهود الدولية في الاستجابة للجرائم السيبرانية وإسناد وتحديد المسؤولية عنها لضمان المساءلة. ويمكن أن يكون إنشاء هيئة فرعية مخصصة لهذه المسألة نقطة انطلاق في هذا الصدد.

ثالثًا، ونظراً للتقدم السريع لتكنولوجيا المعلومات والاتصالات، وتحديدًا الذكاء الاصطناعي، والمخاطر المحتملة لإساءة استخدامها، يمكن للمجلس أن ينظر في إدراج بند محدد في جدول الأعمال يركز على الأمن السيبراني قبل دمجه في نهاية المطاف في مختلف جداول الأعمال المواضيعية والجغرافية. ومن شأن مثل هذا النهج أن يتيح للمجلس متسعاً من الوقت للتداول بشأن الآثار المترتبة على هذه المسألة واستيعابها بشكل كامل، مما يتيح له وضع استراتيجيات شاملة لحماية السلام والأمن العالميين من التهديدات السيبرانية.

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

السيدة كونسبسيون هاراميّو (بنما) (*تكلمت بالإسبانية*): في العصر الرقمي، تتزايد التهديدات الناجمة عن الأنشطة السيبرانية الخبيثة. وتدرك بنما أهمية بناء هيكل عالمي للأمن السيبراني لمكافحة تلك التهديدات السيبرانية الآخذة في التطور بفعالية. ويمكن لمجلس الأمن، من بين جهات فاعلة أخرى وفي سياق ولايته، أن يؤدي دوراً حاسماً في التصدي لتلك التحديات وفي تعزيز التعاون الدولي لحماية بيئتنا الرقمية المشتركة. وتقع على عاتق المجلس المسؤولية الرئيسية عن صون السلام والأمن الدوليين، وهذه المسؤولية حاسمة بنفس القدر في مجال الفضاء السيبراني. ومن خلال المشاركة الاستباقية في جهود الأمن السيبراني والبقاء على اطلاع على التهديدات الناشئة، يمكن للمجلس أن يساهم بشكل كبير في جعل الفضاء السيبراني آمنا وسلميا لجميع الدول. ومن الضروري أن نستكشف سبل تحسين قدرة المجلس على الاستجابة للأنشطة السيبرانية الخبيثة، التي يمكن أن تؤثر على البنية التحتية الحيوية والمدنيين والجهود الإنسانية.

وعند استكشاف المشهد المعقد لتلك التهديدات السيبرانية، من الضروري النظر في المناقشات الجارية بشأن وضع اتفاقية دولية شاملة لمكافحة الاستخدام الإجرامي لتكنولوجيا المعلومات والاتصالات، يكون دورها مكملا لاتفاقية مجلس أوروبا بشأن الجريمة الإلكترونية. وفي حين أن تلك الاتفاقية وبروتوكولاتها مفيدة في تيسير التعاون الدولي في مكافحة الجريمة السيبرانية، فإن الطبيعة المتطورة للتهديدات السيبرانية تستدعي تكييف وتعزيز أطرنا القانونية. ومن خلال تحديث تلك الأطر وتحسينها، يمكننا مواجهة التحديات الجديدة في الفضاء السيبراني بشكل أفضل وضمان بنية عالمية أكثر مرونة للأمن السيبراني.

وبالنظر إلى الطبيعة العابرة للحدود الوطنية للتهديدات السيبرانية الخبيثة، من الضروري أن يعمل مجلس الأمن بالتعاون مع الدول الأعضاء والمنظمات الدولية وأصحاب المصلحة الآخرين لمواجهة تلك التحديات المتعددة الأوجه. ومن خلال تعزيز التعاون ومشاركة أفضل الممارسات وتعزيز سلوك الدول المسؤول في الفضاء السيبراني، يمكننا

بشكل جماعي التخفيف من المخاطر ونقاط الضعف المرتبطة بتلك التهديدات. وتعتقد بنما أنه يمكن تعزيز هذه الجهود في بعض لجان المجلس، مثل اللجنة المنشأة عملا بالقرار 1540 (2004). وبصفة عامة، يمكن لمجلس الأمن أن يضطلع بأدوار وإجراءات محددة للتصدي لتحديات السلام والأمن الدوليين الناشئة عن الفضاء السيبراني، بما في ذلك وضع تقييمات واستراتيجيات بشأن التهديدات السيبرانية وإدماج الأمن السيبراني في مناقشاته بشأن مسائل محددة. وتترابط التهديدات السيبرانية مع مسائل أخرى مدرجة على جدول أعمال مجلس الأمن، بما في ذلك حماية المدنيين، والسلام والأمن في النزاعات المسلحة، ومحاربة الإرهاب ومكافحته، وموضوع المرأة والسلام والأمن. وينبغي أن تراعي التقييمات والاستراتيجيات المنظور الجنساني ومشاركة المرأة في صنع السياسات، مع مراعاة تفاوت ما تتعرض له من أوجه للخطر.

ومن أجل إدماج الشواغل المتعلقة بالفضاء السيبراني بفعالية في عمله، يمكن للمجلس أن يستكشف سبلا لتعزيز المنعة السيبرانية وتعزيز التعاون الدولي والتصدي للتهديدات السيبرانية بشكل كلي. ومن خلال تعزيز التنسيق والتعاون وتحسين قدرات الأمن السيبراني، يمكننا بناء بيئة رقمية أكثر أماناً ومرونة لصالح جميع الدول. وتدعو بنما مجلس الأمن إلى اتخاذ إجراءات حاسمة في هذا الصدد، وإلى أن نعمل معاً لضمان أن يكون الفضاء السيبراني أكثر أمناً وسلاماً للأجيال الحالية والمقبلة.

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

السيد جوفانوفيتش (إيطاليا) (*تكلم بالإنكليزية*): أود أن أعرب عن امتناني لكم، سيدي الرئيس، على عقد هذه المناقشة المفتوحة في وقتها المناسب. ففي الوقت الذي نعيش فيه عصراً يتسم بالتقدم التكنولوجي السريع، فإن الحاجة إلى نهج قوي وموحد للأمن السيبراني قد صارت أكثر إلحاحًا من أي وقت مضى.

وتؤيد إيطاليا البيان الذي أُدلي به باسم الاتحاد الأوروبي وتود أن تضيف بعض الاعتبارات بصفتها الوطنية.

تشعر إيطاليا بالقلق إزاء تزايد عدد الأنشطة السيبرانية الخبيثة وتطوير قدرات تكنولوجيا المعلومات والاتصالات لأغراض عسكرية. ونحن ملتزمون بقوة بتعزيز التعاون بين جميع الدول الأعضاء في مجال التقنيات الرقمية الجديدة. وتسعى رئاسة إيطاليا لمجموعة الدول السبع إلى البناء على جهود المجتمع الدولي في النهوض بفضاء سيبراني مفتوح وقابل للتشغيل البيني وآمن ومأمون ومرن ويحترم حقوق الإنسان، تحكمه مبادئ وقواعد القانون الدولي. وتدعو إيطاليا إلى احترام ميثاق الأمم المتحدة والمعايير الدولية القائمة من أجل الحفاظ على السلام والاستقرار وتعزيز أمننا المشترك.

ويتمتع مجلس الأمن، نظراً لمسؤوليته الأساسية في الحفاظ على السلام والأمن الدوليين، بوضع فريد يمكنه من التصدي لتهديدات الأمن السيبراني لصالح جميع الدول. والواقع أن مشاركة المجلس ينبغي أن تكمل عمليات الأمم المتحدة الأخرى الجارية، مثل برنامج العمل المقترح للارتقاء بسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي. وتهدف المقترحات التي طُرحت في جلسات سابقة لمجلس الأمن إلى تحسين المبادرات الجماعية الرامية إلى التصدي للآثار الأمنية المترتبة عن استخدام تكنولوجيا المعلومات والاتصالات في العالم. وأحد هذه المقترحات هو النظر في شواغل الأمن السيبراني ذات الصلة في حالات وطنية معينة أو في مسائل مواضيعية أخرى أوسع نطاقاً، مثل بعثات حفظ السلام وبناء السلام، وعدم الانتشار ومكافحة الإرهاب.

وعلاوة على ذلك، ينبغي أن نعزز قدرة الأمم المتحدة على التصدي أوجه الاستخدام الخبيثة لتكنولوجيا المعلومات والاتصالات التي تعرض السلام والأمن الدوليين للخطر. ويكتسي ذلك أهمية خاصة عندما يتعلق الأمر بحماية المدنيين والبنية التحتية الحيوية والعمليات الإنسانية. وبينما نمضي قدما، يجب أن ننظر في الاتجاهات الرئيسية للأنشطة الخبيثة، التي تضاعف أثرها أحيانا التكنولوجيات الجديدة، مثل الذكاء الاصطناعي، وفي إمكانية مضاعفتها للتهديدات في النزاعات القائمة، وما هي الإجراءات المحددة التي يمكن أن يتوخاها مجلس الأمن والأمم المتحدة ككل لمواجهة التحديات المتزايدة التي أمامنا.

وندرك جميعاً التأثير غير المتناسب الذي يمكن أن تؤثره الأنشطة السيبرانية الخبيثة على الشرائح الضعيفة من سكاننا. فنحن جميعاً

معرضون لخطر الهجمات الإلكترونية التي تستهدف البنية التحتية الحيوية، مثل الرعاية الصحية أو الطاقة، أو المواطنين العاديين والشركات. ومن الضروري بناء القدرات لمنع مرتكبي الهجمات الإلكترونية من جني المكافآت على سلوكهم غير المشروع. وفي هذا الصدد، ستستضيف إيطاليا مؤتمراً وطنياً في 2 تموز/يوليه بشأن تعزيز منظومة الكيانات العامة والخاصة المكلفة بأنشطة بناء القدرات السيبرانية في جميع أنحاء العالم. وسيساعد ذلك في تيسير تنفيذ المشاريع في المستقبل بنهج شامل ومتعدد أصحاب المصلحة.

وتأكيداً لالتزام إيطاليا بنجاح هذا النهج، أود أن أؤكد من جديد استعدادنا للعمل مع جميع الدول الأعضاء على تطوير وتعزيز المهارات والعمليات والموارد اللازمة للتكيف مع الفضاء الإلكتروني السريع التطور ولضمان مستقبل أكثر أمناً لجميع الدول في نهاية المطاف.

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

السيد كالمار (إسرائيل) (*تكلم بالإنكليزية*): تود إسرائيل أن تنضم إلى الآخرين في تهنئة جمهورية كوريا على تنظيم ورئاسة هذه المناقشة المهمة التي جاءت في وقت مناسب جدا بشأن تهديدات الأمن السيبراني، وأن تضيف بعض الملاحظات بشأن التهديدات القائمة والمتطورة في الفضاء الإلكتروني من وجهة نظرنا.

لا تزال إسرائيل تواجه موجة غير مسبوقة من الاعتداءات الإلكترونية. ولا يكتفي خصومنا بالحرب التقليدية والإرهاب، بل يسعون إلى استغلال المجال الرقمي لتقويض أمننا وإثارة الفتنة بين سكاننا وتمزيق أسلوب حياتنا. وأصبحت الهجمات الإلكترونية واقعاً يومياً بالنسبة لإسرائيل. وتواجه بنيتنا التحتية الحيوية، سواء منها الحكومية أو المالية أو المجتمعية، هجمات لا هوادة فيها من الجهات الفاعلة الحكومية وغير الحكومية على حد سواء. وترمي هذه الهجمات إلى تعريض سلامة مواطنينا ورفاهيتهم للخطر، وتهدد استقرارنا الاقتصادي وتتحدى مؤسساتنا الديمقراطية. والتهديدات التي نواجهها في الفضاء الإلكتروني تهديدات حقيقية ومتفشية، وتتطلب منا اليقظة والعمل الجماعي.

وعلى غرار العديد من الدول، تدرك إسرائيل الآثار العميقة المترتبة عن التهديدات السيبرانية. لقد علمتنا تجربتنا أن هذه التهديدات ليست نظرية. ففي يوم السبت الموافق 7 تشرين الأول/أكتوبر 2023، اخترق آلاف من إرهابيي حماس حدود إسرائيل الجنوبية وقاموا بذبح 1 200 من النساء والرجال والشيوخ والأطفال والرضع الأبرياء وحرقهم واغتصابهم وتشويههم. وإضافة إلى ذلك، أصيب آلاف آخرون بجروح، واختطف الإرهابيون أكثر من 240 مواطناً بريئاً واحتجزوهم كرهائن. ومنذ 7 تشرين الأول/أكتوبر 2023، تتعرض إسرائيل أيضا لهجمات إلكترونية مستمرة وواسعة النطاق. وقد دبرت إيران هذه الهجمات بدعم ومشاركة نشطة من وكلائها، حزب الله وحماس وغيرهما من الجماعات الإرهابية، التي شنت هجمات إلكترونية واسعة النطاق استهدفت أكثر بنيتنا التحتية أهمية وحساسية، مثل إمدادات المياه والبنية التحتية للطاقة والمستشفيات. ويجب إدانة إيران لانتهاكها السافر لمعايير سلوك الدول المسؤول في الفضاء الإلكتروني وخرق المعايير الإنسانية والأخلاقية الأساسية. وإضافة إلى الهجمات الإلكترونية، نتعرض لحملة تأثير إيرانية واسعة النطاق تهدف إلى ترويع المواطنين الإسرائيليين والإساءة إلى مجتمعنا الحر والديمقراطي، والتسبب في مزيد من المعاناة لضحايا الهجوم الوحشي الذي شنته حماس وعائلاتهم. ويستخدم المهاجمون الفضاء الإلكتروني كأداة ومنطلقا لأنشطتهم الإرهابية، محاولين الإضرار بأسس المجتمع الإسرائيلي.

وتواجه الجاليات الإسرائيلية واليهودية في جميع أنحاء العالم موجة عالمية من التحريض وخطاب الكراهية ومعاداة السامية، يعززها بشكل كبير السلوك الزائف المنسَّق على وسائل التواصل الاجتماعي. ونلاحظ الجهود المتطورة التي تبذلها بعض شركات التكنولوجيا الكبرى ومنصاتها على وسائل التواصل الاجتماعي للتخفيف من حدة الكراهية والعنف، بيد أنه لا يزال يتعين بذل جهود أكبر بكثير. وندعو جميع منصات التواصل الاجتماعي إلى توخي مزيد من المسؤولية في هذا الصدد. فلا ينبغي السماح لخطاب الكراهية من أي نوع كان، والدعوات إلى التدمير والدعوات التي تنطوي على إبادة شعب من الشعوب بأن يتردد صداها في جميع أنحاء العالم.

واستخدام حماس للفضاء الإلكتروني يجمع بين مجموعة كبيرة من الاستراتيجيات والأهداف، كما قيل في الاجتماع الأخير الذي عقده في لاهاي يوم 15 أيار/مايو التحالف الدولي لمكافحة تحريض حماس وتمويلها، الذي أنشأه الرئيس الفرنسي ماكرون في أعقاب هجوم 7 تشرين الأول/أكتوبر 2023. ويستخدم عناصر حماس منصات مختلفة على الإنترنت للدفع إلى التطرف وتلقين العقيدة والتحريض على العنف ونشر الكراهية والتضليل وجمع الأموال، وكل ذلك يرمي إلى تحقيق الهدف الذي أعلنته المنظمة، وهو تدمير دولة إسرائيل عن طريق العنف والجهاد. ورسائل حماس في الفضاء الإلكتروني، التي تتضمن استخداما متطورا للصور والرموز من أجل التغلب على أنظمة رصد اللغة بالذكاء الاصطناعي، تتيح للجماعات والأفراد التماهي مع رؤية حماس القائمة على العنف للعالم ونقل هذه الأفكار من الفضاء الإلكتروني إلى أرض الواقع. ويتجلى انتقال هذه الأفكار من خلال الزيادات الكبيرة في التبرعات والأموال التي تبلغ عشرات الملايين من دولارات الولايات المتحدة والتي توجَّه إلى حسابات حماس، وحشد المتظاهرين في المظاهرات المفعمة بالكراهية، وهجمات الطعن التي تحفزها خطابات حماس المعادية لإسرائيل والمعادية للسامية المنشورة على الإنترنت. ولم يتصد المجتمع الدولي للإرهاب السيبراني في حد ذاته حتى الآن. فلدى الإرهابيين في الفضاء الإلكتروني دوافع متميزة ولا يتأثرون بالأعراف الدولية. ولا يزال العالم اليوم يفتقر إلى الوسائل المناسبة للتعامل مع الإرهاب الإلكتروني.

وعلى جميع الدول المحبة للسلام أن تنظر في معالجة هذه الفجوة عاجلاً وليس آجلاً. فما يبدأ في الشرق الأوسط نادراً ما يبقى في منطقتنا وحدها. وما من دولة، في هذا العالم المترابط، بمنأى عن هذا التهديد. والموجة الأخيرة من الحوادث السيبرانية في جميع أنحاء العالم – بدءاً من الهجمات ببرمجيات انتزاع الفدية التي تشل البنية التحتية الحيوية إلى حملات التضليل التي تقوض ثقة الجمهور – تؤكد إلحاح مسؤوليتنا المشتركة. وهذه التهديدات لا تعرض تقدمنا التكنولوجي للخطر ولا تؤثر على اقتصاداتنا فحسب، بل تهدد أيضا المقومات الأساسية لمؤسساتنا الديمقراطية والاستقرار العالمي. وتشدد إسرائيل على أهمية التعاون الدولي. إذ لا يمكن لأي دولة أن تواجه هذه التهديدات بمفردها. فيجب علينا تعزيز شراكاتنا، وتحسين آليات تبادل المعلومات ومطالبة كل دولة بتنفيذ معايير وقواعد السلوك المسؤول في الفضاء الإلكتروني. وذلك أمر ضروري لتهيئة بيئة رقمية آمنة ومستقرة يمكن أن يزدهر فيها الابتكار دون خوف من الاستغلال. وعلى المجتمع الدولي أن يتحد في إدانة العدوان السيبراني وأن يكفل أن يتحمل من يسعون إلى تقويض أمننا الجماعي بالوسائل السيبرانية عواقب ذلك.

في الختام، لنغتنم هذه الفرصة ونؤكد من جديد التزامنا بالحفاظ على سلامة الفضاء الإلكتروني وأمنه. ويمكننا معاً، عن طريق الحوار والتعاون والعمل الحاسم، التخفيف من التهديدات التي نواجهها وتسخير الإمكانات التحويلية التي تنطوي عليها التكنولوجيات الرقمية لصالح البشرية جمعاء.

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

السيد هلال (المغرب) (*تكلم بالفرنسية*): أولاً، أود أن أهنئكم، سيدي الرئيس، على عقد هذه المناقشة المفتوحة في مجلس الأمن بشأن موضوع يكتسي أهمية حيوية في هذه الأوقات الصعبة التي يواجهها عالمنا حاليا وبالنظر إلى الطابع المتغير والمعقد للتهديدات الكامنة في الفضاء الإلكتروني. وأرحب بمشاركة وزير خارجية جمهورية كوريا، السيد تشو تاي يول، والأمين العام، السيد أنطونيو غوتيريش، ومقدمي الإحاطتين اللذين أود أن أشكرهما على إحاطتيهما الشاملتين.

يفخر المغرب بمشاركته، إلى جانب 62 بلدا آخر، في رعاية البيان المشترك بشأن استخدام تكنولوجيا المعلومات والاتصالات في سياق السلام والأمن الدوليين.

وما فتئ المغرب يدعو باستمرار إلى تعزيز التعاون بين الدول الأعضاء في مجال الفضاء السيبراني ويؤكد دعمه للمبادرات المتخذة تحت رعاية الأمم المتحدة والرامية إلى إقامة فضاء سيبراني آمن ومأمون ومرن، باعتباره مجالا مشتركا ينبغي أن يحافظ دائما على طبيعته السلمية والمزدهرة وأن يستفيد بشكل كامل من الفرص التي يتيحها الاستخدام المسؤول لتكنولوجيا المعلومات والاتصالات.

وفي مواجهة ذلك السياق الجيوسياسي المعقد والذي لا يمكن التنبؤ به، فإن المجتمع الدولي مدعو إلى إرساء أسس تحول رقمي عالمي ومستدام وسلمي، وهو ما سيتحدد من خلال جهودنا الجماعية لتعزيز الثقة المتبادلة والشفافية وتبادل أفضل الممارسات وبناء القدرات والمساعدة التقنية – بناء على طلب الدول الأطراف ووفق احتياجاتها وتقليص الفجوة المتسعة بين البلدان المتقدمة والنامية في مجال تكنولوجيا المعلومات والاتصالات، ولا سيما احترام السيادة الوطنية والسلامة الإقليمية للدول الأعضاء.

وظلت المملكة المغربية على الدوام، تحت قيادة جلالة الملك محمد السادس، من أشد المدافعين عن الاستخدام المسؤول لتكنولوجيا المعلومات والاتصالات والثقة الرقمية والرقمنة، وذلك بفضل استراتيجيتها الوطنية الجديدة للأمن السيبراني 2030، والتي تهدف إلى تعزيز الإنجازات التي تحققت منذ عام 2012، عندما اعتمدت الاستراتيجية الوطنية للأمن السيبراني، بهدف دعم التحول الرقمي بشكل أفضل، باعتباره رافعة أساسية للتنمية الاجتماعية والاقتصادية.

وكذلك يرتكز النهج المغربي في مجال الأمن السيبراني على التعاون الدولي، بما في ذلك مع الدول العربية والأفريقية الشقيقة والصديقة، بهدف الاستفادة المثلى من المزايا والفرص التي يمثلها هذا المجال الحيوي في إطار التعاون فيما بين دول الجنوب والتعاون الثلاثي.

وتعمل الأمم المتحدة على إنشاء آليات ومنصات متعددة مخصصة لاستعراض التهديدات السيبرانية والرقمية. ويرى المغرب أنه ينبغي لمجلس الأمن أن ينخرط بشكل أكثر تفاعلا ونشاطا في ذلك المجال الحساس، من أجل الوفاء بولايته، ولا سيما في مجال صون السلم والأمن الدوليين في المجال السيبراني، نظرا لطبيعة التهديدات السيبرانية التي لا تعرف حدودا.

ونعتقد أنه ينبغي لمجلس الأمن أن ينظر في إجراء مناقشات أكثر تعمقاً بشأن تعريف التهديدات السيبرانية التي تشكل خطراً مباشراً ومستمراً على السلم والأمن الدوليين وتحديد أولوياتها، بما في ذلك التركيز على ما يلي: أولاً، ينبغي للمجلس أن يركز على المعايير الرئيسية التي تحدد أن التهديد قد وصل إلى مستوى "الإنذار" الذي يسمح بفحصه من قبل مجلس الأمن. ثانياً، يجب عليه أن يتناول التدابير الواجب اتخاذها لمنع تصاعد التهديدات السيبرانية. ثالثاً، ينبغي أن يعقد مجلس الأمن مناقشة سنوية لمجلس الأمن تحدد التهديدات الناشئة في الفضاء الإلكتروني. ورابعا، ينبغي له أن يركز على زيادة مشاركة المرأة والشباب والقطاع الخاص والمجتمع المدني والأكاديميين ليتمكن من مواكبة التهديدات الناشئة في مجال تكنولوجيا المعلومات والاتصالات وتأثيرها على السلم والأمن الدوليين.

ويشدد المغرب على أن إجراء المزيد من المناقشات داخل مجلس الأمن بشأن التهديدات السيبرانية يتيح للمجلس فرصة للاضطلاع بدوره الريادي في وضع استجابات عملية المنحى والتخفيف من التهديدات السيبرانية الجماعية التي تواجهها الدول الأعضاء بشكل يومي.

وفي الختام، نعتقد أن الوقت قد حان للحفاظ على الزخم الذي تولد على مدى العقد الماضي داخل الأمم المتحدة، من أجل الحفاظ على التزامنا الجماعي والبنّاء بفضاء إلكتروني آمن ومأمون وقادر على الصمود. إن الأمن السيبراني والجريمة السيبرانية لا يوجدان بمعزل عن بعضهما البعض، بل لهما عواقب واسعة النطاق تؤثر بشكل غير متناسب على المجتمع الدولي بأسره.

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

السيد ويناويسر (ليختنشتاين) (*تكلم بالإنكليزية*): نشكر جمهورية كوريا على مواصلة العملية التي بدأتها إستونيا بجعل مجلس الأمن ينخرط في الأمن السيبراني (انظر S/2021/621). فانخراط مجلس الأمن في هذا الموضوع يساعد على ضمان أن تتصدى سيادة القانون بفعالية للتحديات التكنولوجية الحديثة، بما في ذلك التهديدات المتطورة في الفضاء الإلكتروني، وهو أمر جوهري في ولاية المجلس.

ولا يوفر ظهور التقنيات السيبرانية الجديدة في عالم اليوم المترابط فرصاً غير مسبوقة للتعاون الدولي فحسب، بل يمثل كذلك مخاطر العمليات السيبرانية الخبيثة بآثار كارثية محتملة. ويتطلب منا التطور المتصاعد للهجمات الإلكترونية وتواترها، بما في ذلك العدوان الروسي

على أوكرانيا، أن نكون واضحين بشأن كيفية تطبيق القانون الدولي على الفضاء السيبراني.

فأولاً وقبل كل شيء، نذكّر بالإجماع الواسع على أن القانون الدولي ينطبق على الفضاء الإلكتروني، بما في ذلك القانون الدولي الإنساني والقانون الدولي لحقوق الإنسان والقانون الجنائي الدولي وبالطبع ميثاق الأمم المتحدة. وقد أكدت اللجنة الدولية للصليب الأحمر أن القانون الدولي الإنساني يمتد ليشمل العمليات السيبرانية أثناء النزاعات المسلحة، مؤكدة على ضرورة الالتزام بالمعايير القانونية في المجال الرقمي أيضاً. وعلاوة على ذلك، ومع تزايد استخدام العديد من العمليات السيبرانية لتمكين الجرائم الدولية، بما في ذلك جرائم الحرب والجرائم ضد الإنسانية، هناك حاجة ماسة لفهم الآثار المترتبة عليها بموجب نظام روما الأساسي للمحكمة الجنائية الدولية. وقد أكدت التقييمات ذات الصلة أن المحكمة يمكنها بالفعل التحقيق في الهجمات الإلكترونية ذات الصلة ومقاضاة مرتكبيها. وذلك أمر منطقي تماما: فالقانون الدولي الإنساني ينطبق على العمليات السيبرانية، وبالتالي فإن انتهاكات القانون الدولي الإنساني التي تستوفي عتبة الخطورة التي حددتها المحكمة الجنائية الدولية قابلة للملاحقة القضائية. وقد أصدر مجلس المستشارين، الذي عقدته ليختنشتاين في عامي 2020 و 2021، تقريراً يوضح كيفية تطبيق كل جريمة من الجرائم الأساسية الأربع الواردة في نظام روما الأساسي – جريمة العدوان وجرائم الحرب والجرائم ضد الإنسانية والإبادة الجماعية – في سياق العمليات السيبرانية.

فالملاحقة القضائية للجرائم الممكّنة عبر الإنترنت في المحكمة الجنائية الدولية أمر أساسي للتصدي بفعالية للتهديدات السيبرانية المتطورة. واستناداً إلى تقرير مجلس المستشارين، أطلق المدعي العام للمحكمة الجنائية الدولية مؤخراً عملية تشاور بين أصحاب المصلحة المتعددين بالتعاون مع شركة مايكروسوفت لوضع سياسة للمحكمة الجنائية الدولية لمعالجة الجرائم التي ترتكب عبر الإنترنت. وسيساعد ذلك ممارسي القانون الدولي على اكتساب فهم أعمق للتعقيدات المرتبطة بمقاضاة الجرائم السيبرانية. وعلاوة على ذلك، فإن تعزيز الحوار بين المحكمة والأمم المتحدة والحكومات والقطاع الخاص والمجتمع المدني سيعزز تطوير السياسات الهامة في السياق السيبراني وسيدعم في نهاية المطاف دور المحكمة كعنصر رئيسي في هيكلية السلم والأمن الدوليين.

وأخيراً، فإن لمجلس الأمن دور حاسم في ضمان المساءلة عن الهجمات الإلكترونية من خلال سلطته في تقديم إحالات إلى المحكمة الجنائية الدولية وإرسال الحالات ذات الصلة إلى المحكمة للتحقيق فيها. فالعلاقة بين المحكمة ومجلس الأمن ضرورية لضمان ألا تكون الطبيعة المتغيرة لأدوات الحرب وتطوراتها أسرع من العدالة.

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

السيد تشيتن (تركيا) (*تكلم بالإنكليزية*): نشكركم، السيد الرئيس، على تنظيم هذه المناقشة المفتوحة بشأن التهديدات المتطورة في الفضاء الإلكتروني.

لقد أصبحت تكنولوجيا المعلومات والاتصالات جزءًا لا غنى عنه في المجتمع والاقتصاد، حيث تؤثر على كل جانب من جوانب الحياة.

واليوم، تضطلع قدرات الدول في تطوير واستخدام التكنولوجيا بدور مهم في تطورها ونموها. وفي الوقت الذي توفر لنا فيه التطورات التكنولوجية العديد من الفرص، فإن التهديدات السيبرانية تتطور وتصبح أكثر تعقيداً. وغالبًا ما تهدد الثغرات الأمنية في أنظمة تكنولوجيا المعلومات والاتصالات الاقتصاد والنظام العام والأمن القومي. ومن بين التهديدات التي تشكل أيضاً خطراً على السلم والأمن الدوليين الإرهاب والتجسس الرقمي والاحتيال وإيذاء الأطفال عبر الإنترنت واستغلال البيانات الشخصية وإساءة استخدامها عبر تكنولوجيا المعلومات والاتصالات.

ويساورنا قلق بالغ من تزايد عدد الهجمات الإلكترونية. وتشير الدراسات إلى أنه في عام 2023 كان هناك أكثر من 317 مليون برمجية خبيثة وأكثر من 6 بلايين محاولة برمجيات خبيثة في جميع أنحاء العالم. وبسبب التطورات التكنولوجية، أصبح تنفيذ الهجمات السيبرانية أسهل، في حين أن الآثار السلبية والأعباء التي تقع على

الضحايا تتزايد بسرعة. وتتطلب مكافحة تلك الهجمات والتصدي للتهديدات أساليب وأدوات حديثة، سواء من الناحية العملية أو القانونية.

ونظراً لطبيعة التهديدات السيبرانية العابرة للحدود، فإن زيادة التعاون الدولي وبناء القدرات في هذا المجال أمر بالغ الأهمية. وانطلاقا من ذلك، تشارك تركيا في تبادل المعلومات الاستخباراتية المتعلقة بالتهديدات السيبرانية وتسهم في السياسات واستراتيجيات التعاون داخل المنظمات الإقليمية والدولية.

وفي سياق القانون الدولي، فإن تركيا طرف في اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية. ونشارك بنشاط أيضا في الجهود المبذولة في إطار الأمم المتحدة، لا سيما عن طريق اللجنة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية. ونرى أن الجرائم المتصلة بالإرهاب، عندما تُرتكب بواسطة تكنولوجيا المعلومات والاتصالات، ينبغي تنظيمها بموجب اتفاقية في المستقبل.

وهناك أيضا مسألة انطباق القانون الدولي على الفضاء الإلكتروني. وتركيا هي إحدى الدول المشاركة في رعاية برنامج العمل للارتقاء بسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي، وتؤيد بقوة قراري الجمعية العامة 37/77 و 16/78.

وبما أن الفضاء الإلكتروني مجال لا حدود له، وبما أن الأمن السيبراني مسألة تهم أصحاب مصلحة متعددين، فإن التعاون الدولي يكتسي أهمية قصوى. ويجب أن تتعاون الجهات المقدمة للخدمات وشركات الأمن بمزيد من الفعالية مع الحكومات والمنظمات الدولية من أجل المساهمة في الأمن السيبراني العالمي. ونرحب بتركيز مجلس الأمن على استخدام الفضاء الإلكتروني لمواجهة التهديدات المتزايدة، ونلتزم بمواصلة مشاركتنا وحوارنا في هذا الصدد.

الرئيس (*تكلم بالإنكليزية*): أعطي الكلمة الآن لممثل المملكة العربية السعودية.

السيد الواصل (المملكة العربية السعودية): شكرا، سيدي الرئيس، بداية أود أن أهنئ سعادة السفير جونكوك هوانغ، مندوب جمهورية كوريا، على تولي رئاسة المجلس، متمنيا كل التوفيق والنجاح لبعثة جمهورية كوريا لفترة رئاستهم. ولا يفوتني تقديم الشكر إلى معالي الأمين العام أنطونيو غوتيريش، والسيد ستيفان دوغين، الرئيس التنفيذي لمعهد السلام الإلكتروني، وأستاذة القانون والتكنولوجيا، السيدة نينا إيفياني – أجوفو على إحاطاتهم القيمة وما يقومون به من جهود حثيثة ومتميزة ونوعية في مجال التصدي لمخاطر الأمن السيبراني والتهديدات المتزايدة في الفضاء السيبراني. لقد بذلوا جهوداً دؤوبة واستثنائية وكبيرة لمواجهة الأخطار التي تواجه الأمن السيبراني والتهديدات السيبرانية المتزايدة.

سيدي الرئيس، السيدات والسادة، لقد باتت الحاجة إلى وجود فضاء سيبراني آمن وموثوق يمكن النمو والازدهار أكثر إلحاحا من أي وقت مضى. وهذا يؤكد على أهمية وضع تعزيز الأمن السيبراني ضمن الأولويات للدول، لا سيما وأن تعزيز الأمن السيبراني أمر ضروري لحماية المصالح الحيوية للدول وأمنها الوطني. وتؤمن المملكة بأن تعزيز التعاون الدولي في هذا المجال وتضافر الجهود الدولية للحد من المخاطر السيبرانية يعد أمرا حيويا وضروريا. وقد حان الوقت للمجتمع الدولي أن يتبع نهجاً جاداً وعملياً يسهم في توحيد الجهود الدولية لمكافحة تهديدات الفضاء السيبراني من خلال لجانها الأممية المعنية وهيئاتها المتخصصة.

السيد الرئيس، لقد شهد مجال الأمن السيبراني في المملكة تطوراً قوياً ومتسارعاً، حيث ابتدأت أعمال تأسيس هذا القطاع استنادا إلى رؤية المملكة 2030 وممكناتها ومستهدفاتها. فقد بدأت المملكة رحلة التحول بتطوير النموذج السعودي في الأمن السيبراني يرتكز على المركزية في الحوكمة واللامركزية في التشغيل والذي يقع تحت مسؤولية الجهات الوطنية.

وفي هذا الشأن، فقد تم في عام 2017 تأسيس الهيئة الوطنية للأمن السيبراني لتكون الجهة المختصة بالأمن السيبراني في المملكة

والمرجع الوطني في جميع شؤونه. ويتميز النموذج المعتمد في المملكة بالشمولية في تناول مجالات الأمن السيبراني سواء التشريعية أو الأمنية أو الاقتصادية والتنموية. ولقد أثمرت جهود المملكة في مجال الأمن السيبراني في تحقيق إنجازات عالمية، ومن أبرزها حصول المملكة على المرتبة الثانية عالميا والمركز الأول على مستوى الوطن العربي والشرق الأوسط وقارة آسيا وذلك في المؤشر العالمي للأمن السيبراني الذي تصدره وكالة الأمم المتحدة المتخصصة في تكنولوجيا المعلومات والاتصالات كما حققت المملكة المرتبة الثانية عالميا لعامين على التوالي، 2022 و 2023 بمؤشر الأمن السيبراني وذلك ضمن تقرير الكتاب السنوي للتنافسية العالمية الصادر عن مركز التنافسية العالمي التابع للمعهد الدولي للتنمية الإدارية. وفي هذا العام 2024، تكرست ريادة المملكة في قطاع الأمن السيبراني دوليا حيث حققت المرتبة الأولى عالميا في الكتاب السنوي للتنافسية العالمية.

السيد الرئيس، إيمانا من المملكة بتعزيز التعاون الدولي في مجال الأمن السيبراني، أطلقت المملكة المنتدى الدولي للأمن السيبراني، الذي يعد منصة عالمية تجمع متخذي القرار حول العالم لمناقشة القضايا الاستراتيجية المتصلة بالأمن السيبراني. وقد شهد المنتدى خلال نسخته التي عقدت العام الماضي مشاركة أكثر من 120 دولة. كما أنشأت المملكة مؤسسة المنتدى الدولي للأمن السيبراني، لتكون منظمة مقرها مدينة الرياض، بهدف المساهمة في تعزيز الأمن السيبراني على المستوى الدولي، وتعزيز التعاون الدولي والتنمية الاقتصادية والاجتماعية في هذا المجال، ومواءمة الجهود الدولية ذات الصلة بالأمن السيبراني ودعمها بما يخدم رخاء وازدهار الإنسان حول العالم.

وتساهم المملكة العربية السعودية في بناء القدرات لعدد من الدول والمنظمات الدولية. وشاركت في التمارين السيبرانية التي تعقدها المملكة أكثر من 40 دولة ومنظمة. كما تحرص المملكة على توحيد الجهود الإقليمية للتعاون في تعزيز الأمن السيبراني الإقليمي. وقد أسفرت تلك الجهود عن إنشاء لجنة وزارية متخصصة في الأمن السيبراني، تحت مظلة مجلس التعاون لدول الخليج العربية، وذلك بناء على مقترح من المملكة. كما تم، بناءً على مقترح من المملكة، إنشاء مجلس وزراء الأمن السيبراني العرب تحت مظلة جامعة الدول العربية. وأقر قادة الدول العربية في اجتماع القمة الأخير أن يكون مقر مجلس وزراء الأمن السيبراني وأمانته العامة ومكتبه التنفيذي في مدينة الرياض بالمملكة العربية السعودية.

السيد الرئيس، السيدات والسادة، ختاماً، فإن تعزيز الأمن السيبراني هو مسؤولية الجميع، وتتطلب منا جميعاً التعاون والشراكة للوصول نحو فضاء سيبراني آمن وموثوق يمكن النمو والازدهار لجميع شعوب العالم.

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

السيد ماينيرو (الأرجنتين) (*تكلم بالإسبانية*): نود أن نشكر جمهورية كوريا على استكمال هذه المناقشة المفتوحة الرفيعة المستوى بشأن الأمن السيبراني، وهي مسألة ذات أهمية كبيرة لدى الأرجنتين.

وترى الأرجنتين أن التهديدات الرئيسية التي يجب علينا مواجهتها لا علاقة لها بالتطورات الجيوسياسية على الصعيد العالمي. ويصدق ذلك بصفة خاصة نظرا للطبيعة العالمية للفضاء الإلكتروني والطبيعة العابرة للحدود الوطنية للأحداث الإلكترونية. وفي هذا الصدد، نود أن نسلط الضوء على أن تحديد التهديدات المحتملة أو الموجودة والتدابير التي يجب أن تتخذها الدول لمنعها والتخفيف من حدتها، إضافة إلى جهود التعاون وبناء القدرات، يجب ألا تنتهك القانون الدولي، بما في ذلك القانون الدولي لحقوق الإنسان والقانون الدولي الإنساني. وينبغي ألا تمس بالمبادئ المنصوص عليها في ميثاق الأمم المتحدة، مثل السلامة الإقليمية للدول وسيادتها، وعدم التدخل في شؤونها الداخلية والتسوية السلمية للمنازعات.

ونعتقد أنه يجب ألا يكون دور مجلس الأمن وجهوده في مجال أمن الفضاء الإلكتروني تكرارا لعمل آخر، بل يجب أن يكونا مكملين للجهود التي يبذلها منذ أمد بعيد فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، الذي أنشئ في عام 2004، والجهود الحالية للفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات

والاتصالات وأمن استخدامها، الذي سينظر في تموز/يوليه في مشروع التقرير المرحلي السنوي الثالث، لاعتماده.

وفيما يتعلق باقتراح عقد جلسات إحاطة منتظمة لتقييم الواقع المتطور للتهديدات السيبرانية فيما يخص الولاية الحالية للمجلس وجدول أعماله الحالي، نعتقد أن من الأساسي التفكير في إمكانية دعوة ممثلين عن مكتب شؤون نزع السلاح، بصفته أمانة الفريق العامل المفتوح العضوية، وكذلك رئيس الفريق العامل وممثلين عن القطاع الأكاديمي والمجتمع المدني والقطاع الخاص لحضور جلسات الإحاطة المذكورة.

وعلى وجه الخصوص، فيما يتعلق بالتهديدات الجديدة في الفضاء الإلكتروني، نعتقد أن مجلس الأمن سيستفيد من تلقي تقارير أو عروض من ممثلي القطاع الخاص، نظراً لأنهم في معظم الحالات هم مالكو ومشغلو البنية التحتية الحيوية. كما أنهم يتمتعون بقدرات وموارد أكبر لاستكشاف عمل البرمجيات الخبيثة، مما يسمح لهم بتحديث قوائم التهديدات باستمرار مع مرور الوقت.

ونرحب أيضاً بحقيقة أن الرئاسة في المذكرة المفاهيمية (S/2024/446، المرفق) تعترف بأن بناء القدرات عنصر لا غنى عنه. نحن نعتقد أن بناء القدرات أمر بالغ الأهمية لسد الفجوة في أمن الفضاء الإلكتروني – وهي فجوة لا تميز وتؤثر على جميع الدول على قدم المساواة، بغض النظر عن مستوى تنميتها. فالدول التي لديها قدرات أقل في مجال أمن الفضاء الإلكتروني غالباً ما يكون لديها نقاط ضعف يمكن للجهات الفاعلة الخبيثة استغلالها. ونظراً لطبيعة الفضاء الإلكتروني المتأصلة من حيث قابلية التشغيل البيني، فإن الثغرات في أي مكان في الفضاء الإلكتروني العالمي يمكن أن يكون لها تداعيات كبيرة وواسعة النطاق. لذلك فإن التعاون في بناء القدرات أمر ضروري. ولن نتمكن من ضمان وجود فضاء إلكتروني قادر على الصمود ومفتوح وآمن ومستقر ويسهل الوصول إليه وسلمي وحر وقابل للتشغيل المتبادل للجميع إلا من خلال التعاون الدولي القوي والمستدام في مجال بناء القدرات.

وفي هذا الصدد، نحن نرى أن بناء القدرات مرتبط بطبيعته بتنفيذ إطار سلوك الدول المسؤول في الفضاء الإلكتروني. يجب أن يُستكمل تنفيذ معايير وقواعد ومبادئ السلوك المسؤول في الفضاء الإلكتروني بتعزيز الابتكار والمساعدة التقنية لبناء القدرات ونقل التكنولوجيا من أجل القدرة على الصمود في الفضاء الإلكتروني، وفقاً للقانون الدولي القائم ومع مراعاة احتياجات البلدان النامية. ولن يسهم ذلك في تحقيق الرفاهية والتنمية الاقتصادية لبلداننا فحسب، بل سيسهم أيضا بصورة متساوية في تنفيذ واعتماد إطار تراكمي ومتطور للسلوك المسؤول في استخدام تكنولوجيا المعلومات والاتصالات، وبالتالي في تحقيق السلام والأمن الدوليين.

وتشعر الأرجنتين بالقلق بشكل خاص إزاء تزايد تواتر العمليات باستخدام البرمجيات الخبيثة وبرامج انتزاع الفدية والتصيد الإلكتروني وآثارها على البنية التحتية الحيوية. لقد زادت مجموعة أوجه الضعف في تلك البنية التحتية الحيوية بشكل كبير، وهو ما يمثل مصدر قلق مشترك للدول والقطاع الخاص والمجتمع المدني. وفي هذا الصدد، نسلط الضوء على أهمية التعاون بين أصحاب المصلحة المتعددين لمواصلة تحليل التهديدات القائمة والمحتملة للفضاء الإلكتروني وتعزيز الإجراءات على المستوى العالمي، مثل تبادل الخبرات. وفي الوقت نفسه، نلاحظ باهتمام كبير الفرص التي تتيحها تكنولوجيا المعلومات والاتصالات وغيرها من التكنولوجيات الناشئة لتنمية مجتمعاتنا. نحن ندرك أن التقنيات الناشئة محايدة وأن المشكلة تكمن في تحكمنا بها واستخدامنا لها. وفي هذا الصدد، ندرك الحاجة إلى إيجاد توازن عادل بين الأطر التنظيمية التي يجري وضعها بشأن نقل تكنولوجيا المعلومات والاتصالات وحق جميع الدول في الوصول إلى التكنولوجيات الناشئة من أجل رفاهها ونموها الاجتماعي والاقتصادي، وكذلك المساهمة في قدرة الفضاء الإلكتروني على الصمود لصالح الجميع.

وفي الختام، يمكن لمجلس الأمن أن يؤدي دوراً حاسماً في مجال أمن الفضاء الإلكتروني من خلال البناء على العمل الذي يقوم به الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيا المعلومات

والاتصالات وأمن استخدامها وغيره من المنتديات ذات الصلة. من الضروري التأكد من أن إجراءات المجلس تتماشى مع اللوائح والتوصيات المعمول بها بالفعل. ومن شأن التنسيق المتعدد الأطراف تيسير التعاون بين الدول والمنظمات الدولية، مما يعزز نهجاً موحداً لأمن الفضاء الإلكتروني.

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

السيد إيناشفيلي (جورجيا) (*تكلم بالإنكليزية*): تؤيد جورجيا البيان الذي أُدلي به باسم الاتحاد الأوروبي وتود أن تضيف بعض الملاحظات بصفتها الوطنية.

بادئ ذي بدء، نشكر رئاسة جمهورية كوريا على عقد المناقشة المفتوحة اليوم. كما نود أن نعرب عن تقديرنا لمقدمي الاحاطتين على عرضيهما المتبصرين اللذين قدماهما في وقت سابق اليوم.

توفر التطورات الأخيرة في الفضاء الإلكتروني فرصاً كبيرة للابتكار والتقدم الاقتصادي والتنمية. إنه ينطوي على إمكانية تعزيز قدرة الدول الأعضاء على تحسين حماية المجتمعات المفتوحة والمسالمة. ومع ذلك، فقد يشكل أيضًا تهديدات محتملة إذا أسيء استخدامه. تتغير التهديدات لأمن الفضاء الإلكتروني باستمرار مع تقدم التكنولوجيا، بما في ذلك البرمجيات الخبيثة والتصيد الإلكتروني وخرق البيانات وما إلى ذلك. وفي مواجهة الأزمات المترابطة عالمياً، يظل دور مجلس الأمن حاسماً في التصدي للتهديدات التي يتعرض لها السلم والأمن الدوليين وتقليلها إلى أدنى حد، بما في ذلك تلك من الفضاء الإلكتروني.

شهد المجتمع الدولي في السنوات الأخيرة كيف يمكن لبعض الجهات الفاعلة من الدول وغير الدول أن تهدد النظام الدولي القائم على القواعد من خلال الجمع بين أساليب الحرب التقليدية والوسائل غير التقليدية المطورة حديثاً. وقد استخدم البعض تكتيكات الفضاء الإلكتروني لاكتساب مزايا استراتيجية، مثل تعطيل شبكات الاتصالات، واستهداف البنية التحتية الحيوية، وتعريض الأنظمة العسكرية للخطر.

ومن هذا المنطلق، تظل جورجيا ملتزمة بتعزيز سلوك الدولة المسؤول في الفضاء الإلكتروني. يتماشى موقفنا في مجال أمن الفضاء الإلكتروني مع الإطار المعياري الذي وضعه فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي والفريق العامل المفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات وأمن استخدامها.

على مدى السنوات القليلة الماضية، شهدنا مساهمات أكبر في السلام والأمن بفضل مشاركة المرأة. لقد مهدت مشاركة المرأة المتزايدة في مجال أمن الفضاء الإلكتروني الطريق أمام منظورات أكثر شمولاً وتنوعاً. مع ذلك، وعلى الرغم من الجهود التي تبذلها الحكومة الجورجية لضمان السلوك المسؤول في الفضاء الإلكتروني، فإننا نشهد استخدام روسيا العدواني لمجموعة أدوات هجينة ضد سيادة جورجيا. كانت جورجيا هي الحالة الأولى التي أصبح فيها بلد ما هدفًا للعديد من الهجمات في الفضاء الإلكتروني إلى جانب الاشتباك العسكري التقليدي، وذلك خلال العدوان العسكري الروسي الشامل في عام 2008.

لذلك نعتبر بناء القدرات عنصراً لا غنى عنه في التعاون المتعدد الأطراف. فإلى جانب تعزيز القدرات الوطنية في مجال أمن الفضاء الإلكتروني، سيعزز التعاون الدولي الأكثر كفاءة للتصدي للتهديدات المعقدة في الفضاء الإلكتروني، والتي غالباً ما تتجاوز الحدود الوطنية وتتطلب استجابة منسقة. ونظرا للتوزيع غير المتكافئ لقدرات تكنولوجيا المعلومات والاتصالات، نعتقد أن الأمم المتحدة يمكن أن تدعم بشكل أفضل الجهود الوطنية لوضع إطار معياري ومساعدة الدول الأعضاء في بناء القدرات لتقليص الفجوة القائمة.

وفي الختام، نؤكد من جديد التزامنا بتعزيز أمن الفضاء الإلكتروني على الصعيدين الوطني والدولي، مع التأكيد على الطبيعة الشاملة للتهديدات في الفضاء الإلكتروني وضرورة التصدي لها بفعالية من خلال العمل الجماعي.

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

السيد لارسن (أستراليا) (*تكلم بالإنكليزية*): أشكر جمهورية كوريا على جمعنا معا لمناقشة هذا الموضوع الهام.

يسعدني أن أتحدث باسم كندا ونيوزيلندا وأستراليا.

تقوض التهديدات في الفضاء الإلكتروني الفرص التحويلية للتقنيات الرقمية. وهي تتزايد من حيث النطاق والتعقيد وتطرح تحديات محددة عند استخدامها فيما يتعلق بالنزاعات المسلحة. نحن جميعاً كمواطنين ومستهلكين نعتمد على هذه الخدمات كل يوم، مما يعني أن حوادث الاختراق في الفضاء الإلكتروني التي تنطوي على اختراق بنية تحتية حيوية يمكن أن يكون لها آثار مدمرة ومتتالية على المجتمع. فهي بمثابة تهديد مضاعف للمخاطر القائمة ويمكن أن تهدد، على أبسط المستويات الأساسية والرئيسية، الأداء الفعال للحكومة والثقة العامة فيها.

لقد شهدنا في جميع أنحاء العالم حوادث اختراق كبيرة في الفضاء الإلكتروني أدّت إلى تدمير البنية التحتية الحيوية وتعطيل الخدمات الأساسية والعمليات الحكومية. لقد خبرنا ذلك في بلداننا بشكل مباشر. في أستراليا، أدت واقعة اختراق ببرمجيات انتزاع الفدية استهدفت قطاع الرعاية الصحية إلى كشف المعلومات الشخصية لملايين الأفراد. وفي كندا، أصابت واقعة اختراق ببرمجيات انتزاع الفدية أنظمة مقدمي الرعاية الصحية على مستوى مقاطعة بالشل، مما تسبب في تأخيرات خطيرة وعرّض المعلومات الحساسة المتعلقة بآلاف الموظفين والمرضى للخطر. في نيوزيلندا، تجاوزت نسبة أنشطة الفضاء الإلكتروني ذات الدوافع المالية الأنشطة التي ترعاها الدولة لأول مرة.

وفي حالات النزاع المسلح المستمرة، رأينا مشغلي الإنترنت العسكريين ينشرون برمجيات خبيثة مدمرة ضد شبكات الحكومة والقطاع الخاص ويهددون البنية التحتية المدنية الحيوية والكيانات المدنية المشاركة في الاستجابة للأزمات، بما في ذلك خدمات الطوارئ وشبكات الطاقة والنقل والاتصالات. وكذلك نرى صلة واضحة بين استخدام أدوات الفدية لارتكاب الجرائم المالية – بما في ذلك سرقة العملات الرقمية لتمويل البرامج النووية وبرامج أسلحة الدمار الشامل بشكل مباشر – وتقويض جهودنا الرامية إلى تحقيق الاستقرار العالمي ونزع السلاح. ولمجلس الأمن دور حاسم في منع ذلك. إننا نرحب بالفرص التي تتيحها مناقشات كهذه لمناقشة التهديدات السيبرانية، التي تساعد على تعميم تلك المسائل في مناقشات مجلس الأمن وترفع من شأنها وتجلب خبرات مجتمع أصحاب المصلحة المتعددين، بما في ذلك منظمات المجتمع المدني.

وقد أرسلنا بشكل جماعي رسالة لا لبس فيها بأن جميع أنشطة الدول في الفضاء الإلكتروني لها حدود وتخضع لالتزامات، تماماً كما هو الحال في المجال المادي. وقد اتفق جميع أعضاء الأمم المتحدة بتوافق الآراء على أن القانون الدولي القائم – ولا سيما ميثاق الأمم المتحدة في مجمله – ينطبق في الفضاء الإلكتروني. فيجب على الدول أن تكون قاطعة في التزامها بالتصرف وفقاً للقانون الدولي والتوقعات التي حددتها القواعد غير الملزمة المتفق عليها.

في الختام، لدينا طلبان رئيسيان.

أولاً، نطلب من مجلس الأمن التأكيد على الإطار المتفق عليه لسلوك الدول المسؤول في الفضاء الإلكتروني الذي يدعم السلام والاستقرار ويعزز وجود فضاء إلكتروني مفتوح وآمن ومستقر ومتوفر وسلمي. ويتطلب تحقيق تلك الأهداف الرئيسية تنفيذ الالتزامات ذات الصلة والتقيد بها، مدعومة ببناء القدرات المنسقة لدعم جميع الدول في زيادة قدرتها على الاستجابة للتحديات المطروحة.

ثانياً، ندعو مجلس الأمن إلى التأكيد على أن القانون الدولي الإنساني ينطبق على الفضاء الإلكتروني في حالات النزاع المسلح. فتلك التأكيدات تعزز التزاماتنا الجماعية بحماية البنية التحتية الحيوية وتعزيز القانون الدولي، ولا سيما ميثاق الأمم المتحدة.

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

السيدة كورتوا (*تكلمت بالإنكليزية*): تشاطر اللجنة الدولية للصليب الأحمر جمهورية كوريا قلقها بشأن الكلفة البشرية المحتملة للعمليات السيبرانية أثناء النزاعات المسلحة.

فاللجنة الدولية للصليب الأحمر تعمل على حماية ومساعدة الأشخاص المتضررين من أكثر من 120 نزاعاً مسلحاً في جميع أنحاء العالم. وفي عدد متزايد من تلك النزاعات، تتسبب العمليات السيبرانية في مخاطر إضافية على أمن الناس ورفاههم. وهناك ثلاثة اتجاهات تثير قلقا بالغا.

أولاً، عطلت العمليات السيبرانية توفير الخدمات الأساسية للسكان المدنيين – مثل الكهرباء والمياه والرعاية الطبية. وتعرّض تلك العمليات السيبرانية للخطر الأشخاص الذين يعانون أصلاً من الدمار وانعدام الأمن الناجم عن النزاعات المسلحة، وغالباً ما تتم في تجاهل للقانون الدولي الإنساني.

ثانياً، يساورنا قلق بالغ إزاء التورط المتزايد للجهات الفاعلة المدنية – أفراد ومجموعات قراصنة وشركات تكنولوجيا – في العمليات السيبرانية المتعلقة بالنزاعات المسلحة. وكلما قرب المدنيون والأعيان المدنية من الأعمال العدائية، كلما زاد خطر تعرضهم للأذى.

ثالثاً، تواجه اللجنة الدولية للصليب الأحمر والحركة الدولية للصليب الأحمر والهلال الأحمر الأوسع نطاقاً – كمنظمات إنسانية – تهديداً متزايداً من العمليات السيبرانية، بما في ذلك اختراق البيانات والعمليات المعلوماتية الضارة. وإذا تعطلت عمليات الإغاثة التي نقوم بها أو قوضت الثقة في عملياتنا وعملنا، فإن قدرتنا على مساعدة الناس وحمايتهم ستضعف.

وتقع على أعضاء مجلس الأمن المسؤولية الرئيسية عن صون السلم والأمن الدوليين ولهم دور رئيسي في حماية السكان المدنيين أثناء النزاعات المسلحة. ولطالما كان مجلس الأمن واضحًا: الحروب لها حدود. فلم يترك المجلس مجالاً للشك في أن المتحاربين يجب ألا يستهدفوا المدنيين أو الأعيان المدنية، وأنه يجب احترام وحماية المرافق الطبية وعمليات الإغاثة الإنسانية والعاملين في مجال الإغاثة الإنسانية. وبالتالي، فإن اللجنة الدولية للصليب الأحمر تحث مجلس الأمن على تعميم مراعاة الكلفة البشرية المحتملة للعمليات السيبرانية في عمله وعلى التمسك بشكل منهجي بالحدود القائمة منذ أمد بعيد التي يفرضها القانون الدولي الإنساني على جميع وسائل وأساليب الحرب – القديمة والجديدة، السيبرانية والحركية.

وقد كان القرار 2730 (2024) الذي اتخذ مؤخراً والذي يعرب صراحةً عن القلق إزاء أنشطة تكنولوجيا المعلومات والاتصالات الخبيثة التي تستهدف المنظمات الإنسانية ويدين التضليل الإعلامي والتحريض على العنف ضد العاملين في مجال تقديم المساعدة الإنسانية، خطوة أولى مهمة في ذلك الاتجاه. في عالمنا الرقمي اليوم، ينبغي لمجلس الأمن ألا يتجاهل التهديدات التي تشكلها أنشطة تكنولوجيا المعلومات والاتصالات على السكان المدنيين أثناء النزاعات المسلحة.

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

السيد تيتو (كيريباس) (*تكلم بالإنكليزية*): تقدر كيريباس الفرصة التي أتيحت لها لتشاطر أفكارها بشأن استخدام تكنولوجيا المعلومات والاتصالات في سياق السلم والأمن الدوليين. إننا نشكر الأمين العام ومقدمي الإحاطتين من المنظمات غير الحكومية والأوساط الأكاديمية على تبادل وجهات نظرهم.

في وقت سابق من هذا الأسبوع، أيدت كيريباس البيان المشترك الذي أصدرته جمهورية كوريا حول هذا الموضوع. ونشيد بجمهورية كوريا على قيادتها في هذه المسألة، ونود أن ننوه بحضور وزير خارجية جمهورية كوريا، السيد تشو تاي يول، الذي يترأس هذه الجلسة. أشكركم، السيد الرئيس، على تسليطكم الضوء على دور مجلس الأمن في ضمان استخدام تكنولوجيا المعلومات والاتصالات بشكل مسؤول لتعزيز السلم والأمن العالميين وليس لأغراض تعرض السلم والأمن الدوليين للخطر، خاصة في هذا الوقت الذي تتزايد فيه الحروب الإقليمية والنزاعات العنيفة.

إننا نتقاسم نفس المخاوف بشأن استخدام الأنشطة السيبرانية الخبيثة ضد البنية التحتية المدنية وتأثيرها على حياة البشر ورفاههم، لا سيما فيما يتعلق بالأفراد الأكثر تهميشاً وضعفاً في مجتمعاتنا. ونود أن نعرب عن قلقنا البالغ إزاء العمليات السيبرانية التي تستهدف البنية التحتية المدنية الحيوية، مثل المياه والكهرباء. فتلك الأعيان محمية بموجب القانون الدولي الإنساني. وبالإضافة إلى ذلك، بموجب القانون الدولي الإنساني، يجب احترام وحماية المرافق الطبية. وفي أوقات النزاع المسلح، يجب أيضاً احترام عمليات الإغاثة الإنسانية وحمايتها.

وعندما يعبر أصحاب المصلحة عن آرائهم حول العمليات السيبرانية الضارة في حالات النزاع المسلح ويدعون إلى تطبيق القانون

الدولي الإنساني ومناقشته، فإنهم يفعلون ذلك من منطلق حرصهم الصادق على سلامة شعوبهم. ولنتخيل عالمًا لا تنطبق فيه هذه الحماية على العمليات السيبرانية، ولنسأل أنفسنا ما إذا كان هذا العالم هو العالم الذي نريد أن نعيش فيه ونسميه وطنًا. بالنسبة لنا، الإجابة هي لا، خاصة في المحيط الهادئ حيث نتمتع بالكثير من السلام والانسجام مع الطبيعة ومع أنفسنا.

فيجب علينا أن نتمسك بتطبيق القانون الدولي الإنساني على المجال السيبراني. ونتيجة لذلك، نعتقد اعتقاداً راسخاً بأنه ينبغي للمجتمع الدولي، ولا سيما مجلس الأمن، الاستماع إلى أصحاب المصلحة والجهات الفاعلة من المنظمات غير الحكومية والأوساط الأكاديمية الذين يعربون عن قلقهم إزاء الأنشطة الخبيثة لمجرمي الإنترنت. فيجب علينا أن نكون مستعدين لدعم وتطبيق مبادئ القانون الدولي الإنساني. ولذلك، فإننا نحث مجلس الأمن بقوة على تعميم الشواغل الإنسانية للعمليات السيبرانية والتمسك بالحدود المفروضة على جميع وسائل الحرب، بما في ذلك العمليات السيبرانية بموجب القانون الدولي الإنساني. فلا يمكننا المخاطرة بتآكل القانون الدولي الإنساني في المجال السيبراني الناشئ لتكنولوجيا المعلومات والاتصالات.

وأود أن أختتم كلمتي بالتذكير بالبيان الذي ألقاه رئيس الولايات المتحدة الأسبق هاري ترومان قبل 79 عاما للترحيب بميثاق الأمم المتحدة الذي أطلق حديثا.

”لن تصبح الوثيقة واقعًا إنسانيًا حيًا إلا إذا فهمنا ماهية الميثاق وما يمكن أن يعنيه لسلام العالم“.

فلنحترم جميعا ميثاق الأمم المتحدة في مجمله وندعو جميع شركات التكنولوجيا العالمية، ومعظمها خارج سيطرة الحكومات، التي تتحكم في جميع تكنولوجيات المعلومات والاتصالات إلى ضمان استخدام تلك التكنولوجيات بشكل مسؤول لتعزيز الاحترام الكامل للميثاق والنهوض بالهدف النبيل للميثاق لبناء عالم أكثر سلاما وازدهارا وإنسانية ومحبة للجميع.

الرئيس (*تكلم بالإنكليزية*): طلب ممثل جمهورية إيران الإسلامية الكلمة للإدلاء ببيان آخر.

السيد أحمدي (جمهورية إيران الإسلامية) (*تكلم بالإنكليزية*): أدرك أن جلسة اليوم كانت طويلة، ولا أنوي أن آخذ الكثير من وقت أعضاء المجلس. غير أنني طلبت الكلمة للإدلاء ببيان آخر حيث أساء ممثلا ألبانيا والنظام الإسرائيلي استخدام القاعة لتوجيه ادعاءات لا أساس لها من الصحة ضد إيران، متهمين بلدي زوراً بدعم هجمات في الفضاء الإلكتروني.

نحن نرفض ونستنكر بشكل قاطع هذه الادعاءات التي لا أساس لها من الصحة. وفيما يتعلق بالإشارة غير المبررة إلى إيران في بيان ممثل ألبانيا، فقد قمنا بالرد على هذا الادعاء الكاذب ورفضناه في رسالتنا إلى مجلس الأمن المؤرخة 10 أيلول/سبتمبر 2022 (S/2022/685). نحن نعتقد أن حكومة ألبانيا قد ضُلِّلت بمعلومات مغلوطة من المنظمة الإرهابية، أي منظمة مجاهدي خلق، ونسبت زوراً الهجوم الإلكتروني إلى إيران.

إن منظمة مجاهدي خلق، ومقرها ألبانيا حاليًا، قامت بالفعل بتنفيذ العديد من الهجمات الإرهابية في الفضاء الإلكتروني ضد البنية التحتية الحيوية في إيران، بمساعدة ودعم بعض الدول، بما في ذلك النظام الإسرائيلي. وقد تسببت هذه المنظمة الإرهابية في استشهاد العديد من المسؤولين والمدنيين الإيرانيين من خلال التفجيرات الإرهابية والاغتيالات، ومنذ عام 1981، أزهقت أرواح ما يقرب من 17 000 مواطن إيراني.

وعلى الرغم من هذه الحقيقة، فقد قدمت حكومة جمهورية إيران الإسلامية، بحسن نية، عرضاً إلى حكومة ألبانيا للتعاون والمشاركة البناءة من أجل توضيح الاتهام الذي لا أساس له من الصحة الموجه إلى إيران. وللأسف، لم يتم الرد على طلبنا.

وفيما يتعلق بالادعاءات التي لا أساس لها من الصحة التي أطلقها النظام الإسرائيلي، فإننا نرفضها بشكل قاطع. من المثير للسخرية أن يقوم ممثل نظام مشهور بأنشطته الخبيثة والإجرامية والإرهابية في الفضاء الإلكتروني والفضاء الحقيقي على حد سواء، باتهام الآخرين بالأفعال ذاتها التي ارتكبها النظام الإسرائيلي مراراً وتكراراً.

تشن إسرائيل، نظام الاحتلال، منذ أكثر من تسعة أشهر، حرب إبادة جماعية وعدواناً عسكرياً على الشعب الفلسطيني الأعزل، وهي ضالعة في أعمال وحشية وإرهابية في المنطقة، في انتهاك صارخ لجميع القواعد والمبادئ والأعراف القانونية الدولية، بما في ذلك القانون الدولي الإنساني والقانون الدولي لحقوق الإنسان. ويستخدم النظام بلا خجل كل وسيلة ممكنة لإبادة السكان الضعفاء، بما في ذلك استخدام التجويع كأسلوب من أساليب الحرب، والاستهداف العشوائي للمدنيين، بمن فيهم النساء والأطفال، والاعتداء المتعمد على البنية التحتية المدنية الحيوية وعرقلة وصول المساعدات والخدمات الإنسانية الأساسية للمدنيين، في انتهاك مباشر لقرارات مجلس الأمن ذات الصلة.

بالإضافة إلى ذلك، لهذا النظام الإرهابي تاريخ طويل وأسود من الهجمات الإلكترونية ضد البنية التحتية الحيوية للدول ذات السيادة. وكما ورد في بيان إيران الذي ألقي في وقت سابق في القاعة، فإن هجومي "ستوكسنت" و "دوكو" على المنشآت النووية السلمية الإيرانية مثالان واضحان على الأنشطة الإجرامية والهجمات الإلكترونية الإسرائيلية ضد البنية التحتية الحيوية. وقد اعترف النظام صراحةً بهذه الأعمال الإجرامية وأثبت تورطه في العمليات الإلكترونية الخبيثة.

ومع تاريخه الحافل بالانتهاكات الفظيعة للمبادئ الأساسية للقانون الدولي، فإن النظام الإسرائيلي ليس في وضع يسمح له باتهام الآخرين أو إلقاء المحاضرات عليهم بشأن مراعاة تلك المبادئ. يجب ألا يفلت النظام من العقاب، ويجب على مجلس الأمن أن يحاسبه على جميع الجرائم الدولية التي ارتكبها ولا يزال يرتكبها.

رُفعت الجلسة الساعة 17/55.