مجلس الأمن

السنة التاسعة والسبعون

مؤقت

الجلسة 9779

الجمعة، 8 تشرين الثاني/نوفمبر 2024، الساعة 10/00

نيويورك

الرئيس	السيد كاريوكي	(المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية)
الأعضاء:	الاتحاد الروسي	السيد نيبنزيا
	إكوادور	السيد مونتالفو سوسا
	الجزائر	السيد كودري
	جمهورية كوريا	السيد هوانغ
	سلوفينيا	السيدة بلوكار دروبيتش
	سويسرا	السيد هاوري
	سيراليون	السيد كانو
	الصين	السيد غنغ شوانغ
	غيانا	السيدة بيرسود
	فرنسا	السيد دارماديكاري
	مالطة	السيد كاميليري
	موزامبيق	السيد أفونسو
	الولايات المتحدة الأمريكية	السيدة نويبرغر
	اليابان	السيد ميكاناغي

جدول الأعمال

الأخطار التي تهدد السلام والأمن الدوليين

افتتحت الجلسة الساعة 10/05.

إقرار جدول الأعمال

أقر جدول الأعمال.

الأخطار التي تهدد السلام والأمن الدوليين

الرئيس (*تكلم بالإنكليزية*): وفقا للمادة 39 من النظام الداخلي المؤقت للمجلس، أدعو مقدمي الإحاطتين التالي اسماهما إلى المشاركة في هذه الجلسة: الدكتور تيدروس أدهانوم غيبريسوس، المدير العام لمنظمة الصحة العالمية؛ والسيد إدواردو كونرادو، رئيس مؤسسة أسينشن.

وفقا للمادة 39 من النظام الداخلي المؤقت للمجلس، أدعو كذلك سعادة السيد ستافروس لامبرينيديس، رئيس وفد الاتحاد الأوروبي لدى الأمم المتحدة، إلى المشاركة في هذه الجلسة.

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

أعطي الكلمة للدكتور غيبريسوس.

الدكتور غيبريسوس (*تكلم بالإنكليزية*): أشكر فرنسا واليابان ومالطة وجمهورية كوريا وسلوفينيا والمملكة المتحدة والولايات المتحدة على عقد مناقشة اليوم وعلى الفرصة لإحاطة المجلس علما بشأن هذه المسألة المتزايدة أهميتها والمثيرة للقلق.

في آذار/مارس من عام 2020، تعرّض المستشفى الجامعي في مدينة برنو بالجمهورية التشيكية لهجوم إلكتروني من خلال برمجيات انتزاع الفدية اضطره إلى تعطيل شبكته على الإنترنت ونقل مرضاه إلى المنشآت الطبية المجاورة وإرجاء كافة العمليات المقررة سلفاً واضطر إلى اللجوء إلى النظام الورقي التقليدي في إدارة أعماله. وقد تزامن هذا الهجوم مع دخول البلد في حالة الطوارئ جراء تفشي الجائحة. في أيار/مايو 2021، اخترقت مجموعة "كونتي" لبرمجيات انتزاع الفدية موقع الهيئة التنفيذية للخدمات الصحية في أيرلندا. نشأ الهجوم من خلال رسالة احتيالية للتصيد الإلكتروني تضمنت ملفا مرفقا لجداول البيانات أدى فتحه إلى تحميل برمجيات خبيثة. امتد انتشار البرمجيات الخبيثة عبر الشبكة الإلكترونية للهيئة التنفيذية للخدمات الصحية على مدار شهرين، مما أسفر عن تشفير ما يقارب 80 في المائة من البيانات، الأمر الذي أدى إلى تعذر الوصول إلى منصة التصوير التشخيصي عبر الأشعة على المستوى المحلي، وتوقف خدمات العلاج الإشعاعي في خمسة مراكز طبية رئيسية. وترتب على ذلك أن اضطر ما يزيد على نصف مستشفيات الحالات الحرجة إلى تأجيل المواعيد المقررة لمرضى العيادات الخارجية، وكذلك الفحوص والإجراءات السريرية الاختيارية، في حين لجأت الكوادر الطبية إلى استخدام النظام الورقي التقليدي للحفاظ على تقديم الحد الأدنى من الخدمات الطبية الأساسية.

ومن الأهمية بمكان أن نوضح في البداية أن هجمات برمجيات انتزاع الفدية وسائر الهجمات الإلكترونية التي تطال المستشفيات والمرافق الصحية الأخرى لا تنحصر في كونها مجرد مسائل تتصل بالأمن وسرية المعلومات؛ بل إنها قد تشكل مسألة حياة أو موت. وفي أهون الأحوال، تسفر تلك الهجمات عن توقف الخدمات وتكبد خسائر مادية. أما في أسوأ تجلياتها، فإنها تنال من ثقة المجتمع في النظم الصحية التي يعول عليها السكان، بل قد تفضي إلى إلحاق الضرر بالمرضى وتعريض حياتهم للخطر.

وتتضافر عوامل عدة في جعل المرافق الصحية هدفاً مستساغاً لهجمات برمجيات انتزاع الفدية، وتتمثل هذه العوامل في التحول الرقمي للأنظمة الصحية، والقيمة الكبيرة للبيانات الطبية، إلى جانب تزايد الأعباء على النظام الصحي وشح الموارد. وتستهدف هذه الهجمات البنية التحتية الرقمية للمرافق الصحية وتعطيل عملها أو إيقافها تماما عن أداء مهامها. ويشترط الجناة، لإعادة إمكانية الوصول إلى الأنظمة، دفع مبلغ مالي أو فدية.

تعمل مجموعات الجريمة الإلكترونية وفق منطق مفاده أنه كلما زادت حدة التهديدات التي يمكنهم توجيهها لسلامة المرضى وخصوصية معلوماتهم ولانتظام الخدمات، تسنى لهم المطالبة بمبالغ فدية أعلى. وإذا لم تدفع المرافق الصحية الفدية، لن تقتصر العواقب ببساطة على النواحي المالية والتشغيلية فحسب؛ فمن المحتمل أن يعرضوا المرضى للخطر. وفي سبيل إعادة تشغيل النظام واستعادة البيانات بسرعة، كثيراً ما تُبدي المرافق الصحية استعداداً لدفع مبالغ فدية طائلة، على الرغم

من غياب أي ضمانات بفك شفرة البيانات أو بعدم معاودة المهاجمين للكرة مرة أخرى.

وقد أظهرت الدراسات الاستقصائية أن الهجمات على قطاع الرعاية الصحية قد ازدادت من حيث النطاق والتواتر. وذلك بسبب النجاح الذي حققه قراصنة الإنترنت في مهاجمة المستشفيات والمرافق الصحية. في دراسة استقصائية عالمية أُجريت في عام 2021، صرح ما يزيد على ثلث المشاركين في الدراسة بتعرضهم لهجوم واحد على الأقل من هجمات برمجيات الفدية الخبيثة خلال العام المنصرم، فيما أقر ثلث هؤلاء باضطرارهم لدفع الفدية المطلوبة. بيد أنه، وحتى في حالات دفع الفدية، تعذر على 31 في المائة من المشاركين استعادة الوصول إلى بياناتهم المشفرة.

وفي حين استهدفت هجمات برمجيات الفدية المستشفيات وسائر مرافق تقديم الخدمات الصحية بشكل رئيسي، فإن سلسلة الإمدادات الطبية الحيوية بنطاقها الأوسع لم تسلم هي الأخرى من هذه الهجمات خلال فترة استشراء الجائحة. فكشف الباحثون المختصون في الأمن الإلكتروني عن مواطن ضعف في ما لا يقل عن 17 شركة طبية حيوية تعمل في مجال تصنيع لقاحات مرض فيروس كورونا وتطوير العلاجات الدوائية. كما وردت تقارير عن هجمات أخرى طالت الجهات المطورة لبرمجيات التجارب السريرية والمختبرات وشركات صناعة الأدوية.

يقدم تقرير الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021 2025 (انظر A/79/214) العديد من التوصيات بشأن التدابير التي يمكن للدول الأعضاء اتخاذها لتعزيز أمن الفضاء الإلكتروني من خلال القواعد والمعايير والمبادئ المتعلقة بسلوك الدول المسؤول والقانون الدولي وتدابير بناء الثقة وبناء القدرات والحوار المؤسسي. وتعمل منظمة الصحة العالمية وشركاؤنا على تنفيذ العديد من تلك التوصيات إذ تنطبق على الصحة.

وعقدت منظمة الصحة العالمية اجتماعًا للخبراء في جنيف، في كانون الأول/ديسمبر من العام الماضي، لوضع استراتيجيات ونُهج للتصدي لتهديدات الأمن السيبراني، لا سيما في البيئات محدودة الموارد. وقد حددوا العديد من التحديات الرئيسية، بما في ذلك – في جملة أمور – عدم إيصال المعلومات بشأن خطر برمجيات انتزاع الفدية وقيمة الاستثمار في الأمن السيبراني بوضوح إلى صانعي القرار؛ وغياب وجود إطار إداري واضح للأمن السيبراني؛ وبنية تحتية معقدة يصعب جعلها أكثر أمانًا؛ وفجوة كبيرة بين الطلب العالمي على مهارات وخبراء الأمن السيبراني والعرض العالمي.

ولسد تلك الثغرات، تعمل منظمة الصحة العالمية ووكالات الأمم المتحدة الأخرى بنشاط على دعم الدول الأعضاء بالمساعدة التقنية والقواعد والمعايير والتوجيهات لتعزيز قدرة البنية التحتية الصحية على الصمود في مواجهة الجرائم السيبرانية، بما في ذلك برمجيات انتزاع الفدية. وفي كانون الثاني/يناير، نشرت المنظمة تقريرين بالتعاون مع الإنتربول ومكتب الأمم المتحدة المعني بالمخدرات والجريمة وشركاء آخرين عن سبل تعزيز الأمن السيبراني ومكافحة المعلومات المضللة. وتعمل منظمة الصحة العالمية كذلك على وضع إرشادات بشأن تنفيذ الأمن السيبراني وحماية خصوصية التدخلات الصحية الرقمية والاستثمار فيها، ومن المقرر أن تنشر العام المقبل.

إن الأمن السيبراني مسؤولية الحكومة بأكملها، ولكن تظل سلطات القطاع الصحي والجهات الممولة وأصحاب المنتجات مسؤولين عن أمن نظم المعلومات المستخدمة في مجال الصحة. وهناك العديد من التدابير التي يمكن للدول الأعضاء اتخاذها لتعزيز أمنها السيبراني، أو مستوى استعدادها للتصدي للهجمات السيبرانية. وذلك يعني الاستثمار في التكنولوجيا وضمان أن تتضمن ميزانيات مشاريع الصحة الرقمية تكاليف ضوابط الأمن السيبراني الأساسية. ويجب على المؤسسات تجنب البرامج غير المدعومة، التي تكون أكثر عرضة للهجمات. وعلى وجه الخصوص، يكتسي الاستثمار في أنظمة تحديد الهجمات في وقت مبكر أهمية كبيرة، إذ أن معظم الهجمات لا تُكتشف إلا بعد أشهر من حدوثها، عندما يكون الضرر قد وقع أصلا.

ولكن على الرغم من أهمية تقنيات تحديد وحماية واكتشاف واستجابة واستعادة البيانات والاستجابة والتعافي من المخاطر، فإنها

غير كافية – خاصةً مع تزايد استخدام الذكاء الاصطناعي. فيجب أن تتغير طريقة تفكيرنا بشكل جذري لإدراك أنه لا يمكننا الاعتماد على أنظمة تكنولوجيا المعلومات وحدها لحمايتنا من الهجمات السيبرانية. لذلك، فإن تعزيز الأمن السيبراني يعني كذلك الاستثمار في الموارد البشرية. فالبشر هم من يرتكب هجمات برمجيات انتزاع الفدية، والبشر هم من يستطيعون إيقافها. وتدريب الموظفين على تحديد الهجمات الإلكترونية والاستجابة لها والتدرب على خطط الاستجابة للحوادث أمر بالغ الأهمية. والبشر هم الحلقة الأضعف والأقوى في ذات الوقت في الأمن السيبراني.

وذلك أمر لا يمكن لأي دولة أن تفعله بمفردها. وكما أن الفيروسات لا تحترم الحدود، كذلك الهجمات الإلكترونية لا تحترم الحدود. ولذلك فإن التعاون الدولي أمر ضروري. وللعديد من التدابير التي نتخذها لمواجهة التهديدات الأخرى نفس الأهمية هنا، سواء التعاون في التحقيقات المشتركة وإنفاذ القانون أو مشاركة المعلومات الاستخباراتية أو إنشاء شبكات إقليمية. وتستضيف منظمة الصحة العالمية منصتين عالميتين جديدتين للحوار الدولي: المبادرة العالمية للصحة الرقمية والمبادرة العالمية بشأن الذكاء الاصطناعي من أجل الصحة – وهي منصة ثلاثية مع الاتحاد الدولي للاتصالات والمنظمة العالمية للملكية الفكرية.

أتوجه بالشكر مرة أخرى إلى مجلس الأمن على لفت الانتباه إلى هذه المسألة الهامة جدا. وكما يعلم أعضاء المجلس، فإن ولايته بموجب ميثاق الأمم المتحدة هي صون السلم والأمن الدوليين. وتشكل الجرائم الإلكترونية، بما في ذلك برمجيات انتزاع الفدية، تهديدًا خطيراً للأمن الدولي. وكما استخدم الأعضاء تلك الولاية لاتخاذ قرارات ومقررات بشأن مسائل الأمن المادي، فإننا نطلب منهم النظر في استخدام نفس الولاية لتعزيز الأمن السيبراني العالمي والمساءلة. وتلتزم منظمة الصحة العالمية بدعم جميع الدول الأعضاء لتعظيم قوة التكنولوجيات الرقمية من أجل الصحة وتقليل مخاطرها إلى الحد الأدنى.

الرئيس (*تكلم بالإنكليزية*): أشكر الدكتور غيبريسوس على إحاطته.

أعطي الكلمة الآن للسيد كونرادو.

السيد كونرادو (*تكلم بالإنكليزية*): أشكركم، السيد الرئيس، على دعوتي للمشاركة في جلسة اليوم. اسمي إدواردو كونرادو وأنا رئيس أسينشن، ثالث أكبر منظومة للرعاية الصحية في الولايات المتحدة.

إن أسينشن منظومة صحية كاثوليكية غير ربحية. ولدينا حوالي 330 000 شخص – بما في ذلك حوالي 33 000 من مقدمي الخدمات المنتسبين – يعملون في مستشفياتنا البالغ عددها 120 مستشفى، و 2 000 موقع للرعاية الإسعافية و 75 مركزاً للجراحة الإسعافية، وهي منتشرة في 17 ولاية ومقاطعة كولومبيا. ونقدم كل عام الرعاية لأكثر من 6 ملايين فرد، مع أكثر من 3 ملايين زيارة لغرفة الطوارئ، ونجري ما يقرب من 600 000 عملية جراحية. وتقوم أسينشن بتوليد ما يقرب من 1 من كل 50 من الأطفال الذين يولدون في الولايات المتحدة كل عام – ولتحديد ذلك كمياً، يتراوح عدد الأطفال الذين يولدون سنوياً بين 72 000 و 78 000. وتتمثل مهمتنا في خدمة الجميع باهتمام خاص وتوفير الرعاية الشاملة والرحيمة للفئات الفقيرة والضعيفة في الولايات المتحدة.

وكما يعلم الأعضاء، فإن قطاع الرعاية الصحية معرض بشكل خاص للهجمات الإلكترونية وهجمات برمجيات انتزاع الفدية بسبب حجمه واعتماده على التكنولوجيا والبيانات الحساسة التي نؤمنها ونحتفظ بها. وقعت أسنشن ضحية، في 8 أيار/مايو، لهجوم برمجيات انتزاع الفدية. وقد شفر الهجوم الآلاف من أنظمتنا الحاسوبية وشكل تحدياً كبيراً لقدرتنا على خدمة مرضانا ومجتمعاتنا. وكنتيجة مباشرة لتشفير أنظمتنا، لم نتمكن من الوصول إلى سجلاتنا الصحية الإلكترونية. كما إن العديد من أنظمة التكنولوجيا الأخرى لم تكن متوفرة لنا، بما في ذلك تلك التي يستخدمها المرضى للتواصل مع أطبائهم وتنزيل بياناتهم. كما أدى هجوم برمجيات انتزاع الفدية إلى زيادة صعوبة الوصول إلى الأنظمة المختلفة المستخدمة في طلب وإجراء بعض الفحوص التشخيصية الهامة – مثل الفحوص المختبرية والتصوير بالرنين المغناطيسي والتصوير المقطعي الحاسوبي والأشعة السينية – وصرف الأدوية لمرضانا.

وبمجرد ما اكتشفنا هجوم برمجيات انتزاع الفدية، بدأت فرقنا للرعاية الصحية إجراءات تقليل الانقطاع وضمان سلامة المرضى، وهي خطوات محددة مسبقاً تتبعها جميع مؤسسات الرعاية الصحية أثناء تعطل النظام أو الشبكة. وتضمنت إحدى تلك الخطوات التحول إلى السجلات الورقية أثناء تعطل سجلاتنا الإلكترونية. وكما يمكن للأعضاء أن يتخيلوا، فقد وضع ذلك عبئاً هائلاً على القوى العاملة والأطباء المتفانين. وأود أن أرسم صورة لما بدا عليه الأمر بالنسبة لموظفينا خلال تلك الفترة.

لم يتمكن الممرضون بين عشية وضحاها من البحث بسرعة عن سجلات المرضى من أجهزتهم الحاسوبية. واضطروا إلى تمشيط النسخ الاحتياطية الورقية للعثور على التواريخ الطبية للمرضى أو الأدوية التي يتناولونها. ولم تتمكن فرق التصوير من إرسال أحدث صور الأشعة بسرعة إلى الجراحين المنتظرين في غرف العمليات. وبالفعل، كان علينا الاعتماد على عدائين لإيصال النسخ المطبوعة من عمليات المسح الضوئي إلى أيدي فرقنا الجراحية. وإذ كنا نحاول استقدام المزيد من الموظفين لتخفيف العبء عن ممرضينا، واجهتنا بعض العوائق لأن نظامنا لخدمات التجهيز كان متوقفًا أيضًا. وبسبب الهجوم الخبيث، تحولت فرق رعايتنا الصحية ومرضانا من استخدام جميع التقنيات المذهلة التي يستخدمونها كل يوم إلى العمل من الورق والفاكس والتوصيل باليد. باختصار، عاد نظام رعايتنا الصحية الحديث القهقرى.

خلال الهجوم، اضطرت العديد من مستشفياتنا أيضًا إلى تحويل مسار الخدمات الطبية الطارئة إلى مستشفيات أخرى، ما يعني أن سيارات الإسعاف وُجِّهت إلى غرف الطوارئ في مستشفيات أخرى بدلاً من مستشفيات أسينشن. يمكن أن تتفاوت آثار التحويل، ولكن يمكن أن يؤدي ذلك إلى تأخر الخدمات بسبب زيادة أوقات الانتقال واحتمال حدوث نتائج سيئة للمرضى. كما يمكن لذلك أن يحدث أيضًا تأثيراً مضاعفًا حيث تكون المستشفيات المستقبلة مثقلة بالأعباء وتضطر أيضًا إلى تحويل المرضى. وبالإضافة إلى تحويل سيارات الإسعاف بدافع الحذر، أوقفت بعض الإجراءات والفحوص والمواعيد الاختيارية غير الطارئة مؤقتًا بينما كنا نعمل على إعادة تشغيل أنظمتنا الإلكترونية.

فالرعاية الصحية الحديثة تعتمد على العديد من الحلول الرقمية من أطراف ثالثة. وقد وجدنا أن مهمة إعادة تشغيل تلك النظم على شبكة الإنترنت وإقناع كل مورد خدمات من مئات الموردين بإعادة الاتصال بأسينشن كانت ضخمة. واستغرق الأمر حتى 14 حزيران/يونيه، أي بعد 37 يوماً من هجوم برمجيات انتزاع الفدية، لكي نتمكن من استعادة الاتصالات والوصول إلى جميع سجلاتنا الصحية الإلكترونية وإعادة آخر مستشفياتنا إلى العمل على شبكة الإنترنت.

واليوم نواصل التعامل مع تداعيات ذلك الهجوم. فبعد عودة نظمنا الصحية الإلكترونية للعمل مرة أخرى، نضطلع بعملية طويلة لرقمنة البيانات من جميع سجلات المرضى الورقية التي أُنشئت وجُمعت على مدار 37 يوماً من تعطل نظمنا. ولتوضيح الأمر، فإن كمية الورق التي أُنتجت في تلك الفترة، إذا ما كُدست فوق بعضها البعض، سيتجاوز ارتفاعها 1,5 كيلومتر. ومن المحتمل أن يستغرقنا الأمر حتى نهاية هذه السنة التقويمية – أي ستة أشهر كاملة بعد إعادة تشغيل نظمنا – حتى نتمكن من رقمنة تلك السجلات الورقية.

وفي حين أنني ركزت في المقام الأول على تأثير هجمات برمجيات انتزاع الفدية على نظمنا وخدماتنا، أود أن أؤكد على التأثير البشري الهائل لمثل هذه الهجمات. لقد ارتقى مقدمو الخدمات والموظفون لدينا إلى مستوى التحديات الهائلة الناجمة عن القيود التكنولوجية وتعطل سير العمل لمساعدة المرضى في توفير الرعاية الآمنة والفعالة التي يحتاجونها. وقد فعلوا ذلك بينما كانوا يتحملون العمل لساعات أطول والمزيد من الإجهاد، وفي بعض الحالات، المزيد من الإنهاك المهني. وبالإضافة إلى ذلك، عندما كان يُحَوَّل المرضى إلى مرافق أخرى للرعاية الصحية، أو يتوجهون إليها طلباً للعلاج، كان على مقدمي الخدمات والموظفين في تلك المرافق الأخرى أيضاً تحمل عبء إضافي بسبب زيادة عدد المرضى وولوج أسينشن المحدود إلى السجلات الطبية وزيادة الإجهاد. إننا نقدر العمل الذي قام به مقدمو الخدمات، وأود أن أشكرهم على استعدادهم للقيام بذلك وما يترتب عليه من جهود.

إن مؤسستنا ليست سوى واحدة من العديد من كيانات الرعاية الصحية التي يستهدفها مرتكبو الجرائم السيبرانية كل يوم. وخلافاً للعديد

من مؤسسات الرعاية الصحية الأصغر حجماً التي قد لا تمتلك الكثير من الموارد مثل أسينشن، فقد كنا محظوظين لأننا تمكنا بسرعة من إشراك خبراء أمن سيبراني داخليين وخارجيين ومستشارين قانونيين للتحقيق في المشكلة واحتوائها وتأمين نظمنا. وقد عملنا بشكل وثيق أيضاً مع مكتب التحقيقات الاتحادي ووكالة الأمن السيبراني وأمن البنية التحتية في الاستجابة للهجوم. ومع ذلك، كان الأثر المالي لهجوم برمجيات انتزاع الفدية في أيار/مايو 2024 هائلاً بالنسبة لنا؛ فقد أنفقت أسينشن حوالي 130 مليون دولار على استجابتها للهجوم وخسرت 900 مليون دولار من إيرادات التشغيل حتى نهاية السنة المالية الحالية.

إن أسينشن ليست الوحيدة التي تعاني من تأثير مالي كبير جراء الهجمات السيبرانية. فالتقديرات الأخيرة تشير إلى أن التكاليف التراكمية لوقت التعطل وجهود التعافي والخسائر في الإيرادات لمؤسسات الرعاية الصحية في الولايات المتحدة تجاوزت 70 بليون دولار منذ عام 2019، وبلغت حوالي 15 بليون دولار حتى تشرين الأول/أكتوبر من هذا العام وحده. وما فتئت هجمات برمجيات انتزاع الفدية على نظم الرعاية الصحية تتزايد، حيث أُبلغ عن 386 هجوماً سيبرانياً على نظم الرعاية الصحية حتى اليوم في عام 2024 في الولايات المتحدة، وفقاً لوزارة الصحة والخدمات الإنسانية الأمريكية، وتقوم فرق التكنولوجيا والأمن السيبراني الرائعة لدينا داخل أسينشن بوقف محاولات الهجوم على نظمنا بشكل شبه يومي.

إن هجمات برمجيات انتزاع الفدية على قطاع الرعاية الصحية هي أكثر من مجرد تهديدات سيبرانية، إذ يمكن أن تشكل خطراً مباشراً ومنهجياً على الصحة العامة والأمن على الصعيد العالمي. ولا يقود هذه الهجمات أفراد مارقون، بل مرتكبو جرائم سيبرانية محترفون ممن يتمتعون بمهارات عالية وموارد جيدة. وهناك حاجة إلى التنسيق والتعاون الدوليين لمكافحة هجمات برمجيات انتزاع الفدية وحماية أنظمة الرعاية الصحية في جميع أنحاء العالم.

ونقدر اهتمام مجلس الأمن بحماية أنظمتنا للرعاية الصحية، وحماية مرضانا ومجتمعاتنا في نهاية المطاف. أشكر أعضاء المجلس على وقتهم هذا الصباح.

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

وأعطي الكلمة الآن لأعضاء المجلس الراغبين في الإدلاء ببيانات.

السيدة نويبرغر (الولايات المتحدة الأمريكية) (*تكلمت بالإنكليزية*): اسمي آن نويبرغر، ومنذ عام 2021 كان لي شرف تنسيق سياسة الأمن القومي للولايات المتحدة فيما يتعلق بالتكنولوجيات السيبرانية والناشئة. ويشرفني أن أمثل الرئيس بايدن اليوم للتحدث عن تهديد برمجيات انتزاع الفدية.

أود أن أشكر المملكة المتحدة على تكريس جزء من رئاستها لمجلس الأمن لجلسة اليوم وعلى قيادتها المستمرة في تعزيز السلوك المسؤول للدول في الفضاء السيبراني. وأشكر أيضاً الدكتور تيدروس غيبريسوس، المدير العام لمنظمة الصحة العالمية، وإدواردو كونرادو، رئيس مؤسسة أسينشن للرعاية الصحية، على انضمامهما إلينا. وننوه بخبراتهما ورؤاهما التي وردت في إحاطتيهما.

أود اليوم أن أتحدث إلى المجلس عن ثلاثة مواضيع: أولاً، طبيعة التهديد الذي تشكله هجمات برمجيات انتزاع الفدية، خاصةً على نظم الرعاية الصحية؛ ثانياً، ما تقوم به الولايات المتحدة للتصدي لهذا التهديد، سواء على الصعيد العالمي أو في الداخل؛ وأخيراً، الدور الحاسم الذي يمكن، بل ويجب، أن تؤديه كل دولة في مواجهة هذا التحدي.

الواقع أن هجمات برمجيات انتزاع الفدية على المستشفيات ونظم الرعاية الصحية تشكل تهديداً خطيراً للسلام والأمن الدوليين. فهي تعرض الأرواح للخطر. وتزعزع استقرار المجتمعات. وبالتالي فإن لمجلس الأمن دوراً يقوم به في مواجهة هذا التهديد للسلام وفي تحفيز البلدان على العمل. منذ بضعة أشهر فقط، في المناقشة المفتوحة الرفيعة المستوى التي عقدها المجلس بشأن التهديدات المتطورة في الفضاء السيبراني، والتي دعت إليها جمهورية كوريا، دعانا الأمين العام أنطونيو غوتيريش إلى التفكير في الفوائد الهائلة التي تجلبها

التكنولوجيات الرقمية لمجتمعاتنا (انظر S/PV.9662). ولكن كما حذّر الأمين العام، فإن الاتصال نفسه الذي يجمعنا يعرّض أيضاً البلدان في جميع أنحاء العالم لتهديدات سيبرانية كبيرة. فبرمجيات انتزاع الفدية هي واحدة من أكثر هذه التهديدات انتشاراً وضرراً. وحكومة الولايات المتحدة على علم بأكثر من 500 1 حادثة مرتبطة ببرمجيات انتزاع الفدية في عام 2023 وحده، أدت إلى دفع أكثر من 1,1 بليون دولار كفدية. وهذه زيادة كبيرة عن عام 2022، حيث كانت مدفوعات برمجيات انتزاع الفدية تزيد قليلا عن نصف هذا المبلغ. وبالفعل، فإن المدفوعات في عام 2023 تزيد بمقدار عشرة أضعاف عن عام 2018، وبمقدار 100 مرة عن عام 2014.

والولايات المتحدة ليست وحدها. ففي تموز/يوليه 2023، تعرّض ميناء ناغويا، وهو ميناء الشحن التجاري في اليابان، لهجوم من برمجيات انتزاع الفدية من قبل مجموعة LockBit، مما أجبر الميناء على التوقف عن التعامل مع جزء كبير من حاويات الشحن الواردة. وفي العام نفسه، أدى هجوم برمجيات انتزاع الفدية على شراكة في علم الأمراض في المملكة المتحدة إلى تعرض إمدادات الدم على الصعيد الوطني لخطر كبير. وتعرضت خدمة المختبرات الصحية الوطنية في جنوب أفريقيا لهجوم برمجيات انتزاع الفدية مما أثّر على نشر نتائج المختبرات، وأعاق الجهود الوطنية للاستجابة لتفشي جدري القردة.

ووفقاً للتحليل الذي أجرته دوائر الاستخبارات الأمريكية في حزيران/يونيه 2024، فإن 51 في المائة من هجمات برمجيات انتزاع الفدية على الصعيد العالمي في النصف الأول من هذا العام كانت ضد ضحايا في الولايات المتحدة. وتتوزع نسبة 49 في المائة المتبقية على جميع أنحاء العالم. إنها حقاً تهديد عالمي. وقطاع الرعاية الصحية وخدمات الطوارئ أحد القطاعات الأربعة الأكثر استهدافاً من هجمات برمجيات انتزاع الفدية، حيث تعرض لما لا يقل عن 191 حادثة في جميع أنحاء العالم في النصف الأول من هذا العام وحده. وفي الولايات المتحدة، أبلغ مكتب التحقيقات الاتحادي عن 249 تقريراً عن حوادث هجمات برمجيات انتزاع الفدية ضد قطاع الرعاية الصحية العام الماضي.

ماذا يعني هجوم برمجيات انتزاع الفدية بالنسبة لمستشفى؟ كما سمعنا للتو من الإحاطة، فإن ذلك يعني تحويل مسار سيارات الإسعاف وحالات تأخير أخرى في الرعاية الصحية الطارئة، وإلغاء عمليات جراحية، وتأخيرات للعلاجات الطبية المهمة، وانتهاك سجلات الرعاية الصحية الحساسة للغاية. وعندما تستهدف هجمات برمجيات انتزاع الفدية بنوك الدم، يمكنها أن تمنع الوصول إلى الإمدادات المنقذة للحياة. ويمكن أن يؤدي استهداف برمجيات انتزاع الفدية لتلك المرافق إلى حدوث حالات تعطل كبيرة تعرّض رعاية المرضى والوصول إلى الأدوية للخطر، وتزيد من مدة إقامة المرضى، وتجبر على نقل المرضى إلى مرافق أخرى، وتهدد الأرواح. وأود أن أؤكد من جديد على الجملة الأخيرة. لقد قدّر خبراء الصحة أن هجمات برمجيات انتزاع الفدية مسؤولة عن وفاة عشرات المرضى من مستخدمي برنامج مديكير للرعاية الصحية في الولايات المتحدة بين عامي 2016 و 2021. وتؤكد البيانات الأحدث أن معدلات الوفيات في المستشفيات تزداد عندما يتعطل مستشفى بسبب الهجمات السيبرانية.

ما الذي نفعله حيال انتشار هذه الجريمة الخطيرة؟ ننطلق من فرضية أن القوة في العدد. فلسنا وحدنا من يواجه هذا التهديد، ولسنا وحدنا من يرغب في التمسك بالأعراف الدولية التي تحظر هذا السلوك بجميع جوانبه. كان إيماننا بأن عملنا الجماعي أكثر قيمة من مجموع أعمالنا منفردين هو ما ألهمنا في عام 2021 لإطلاق المبادرة الدولية لمكافحة برمجيات انتزاع الفدية التي تضم 68 عضواً، والتي تضم عدداً من الدول الموجودة حول الطاولة معي هنا اليوم. تركز هذه المبادرة على تعطيل هجمات برمجيات انتزاع الفدية وتعزيز أمن البنية التحتية الحيوية وزيادة إمكانيات شركائنا وقدراتهم في الاستجابة للحوادث عند عملهم معاً.

كما نستخدم قدراتنا في مجال إنفاذ القانون لتعطيل موجات الجريمة هذه. ومن أجل جعل هجمات برمجيات انتزاع الفدية أقل جاذبية، فإننا نعمل بشكل وثيق مع شركات التأمين الإلكتروني والقطاع الخاص لتقليل مدفوعات برمجيات انتزاع الفدية وتحسين الإبلاغ عن

الحوادث. وقد تعهدنا أيضاً – إلى جانب 40 دولة أخرى – بعدم السماح لحكوماتنا أو أي من وكالاتها بدفع فدية لتلك البرمجيات.

وبالإضافة إلى الحد من مدفوعات الفدية، فإننا نعمل مع كيانات القطاعين العام والخاص لوقف التدفق غير المشروع للمدفوعات المبتزّة من خلال برمجيات انتزاع الفدية التي تتم بالعملات المشفَّرة والتي يتم غسلها من خلال مزودي خدمات الأصول الافتراضية. وبالنظر إلى المستقبل، تعمل وكالة التنمية الدولية التابعة للولايات المتحدة على إنشاء صندوق لبناء قدرات الأمن السيبراني على المدى الطويل ضد هجمات برمجيات انتزاع الفدية ومساعدة البلدان على التصدي لهجمات برمجيات انتزاع الفدية والتعافي من هذه الهجمات.

ولكن لا أحد منا يفعل ما يكفي. وستستمر هجمات برمجيات انتزاع الفدية، وسيزدهر الجناة طالما يستمر دفع الفدية، وطالما يستطيع المجرمون تجنب القبض عليهم، خاصةً عن طريق الفرار عبر الحدود.

وهذا يقودني إلى موضوعي الثالث والأخير – ما الذي يمكن وينبغي لكل بلد أن يفعله لإنهاء هذه الحلقة من الإيذاء والنهب والإفلات من العقاب؟ ولماذا ينبغي لمجلس الأمن، بولايته الفريدة من نوعها، أن يدعم الجهود المبذولة للتصدي لهذا التهديد الآخذ في التطور للسلام والأمن؟

إن هجمات برمجيات انتزاع الفدية جذابة لمجرمي الإنترنت بسبب المدفوعات الفردية الكبيرة لكل فدية. فبالنسبة لمجموعة مثل "بلاك كات" التي تلقت أكثر من 420 مليون دولار من مدفوعات الفدية منذ عام 2019، فإن هذا نشاط تجاري مزدهر. وفي الواقع، في العام الماضي، كانت مجموعتا "بلاك كات" و "لوك بيت" ضالعتين في أكثر من 30 في المائة من هجمات برمجيات انتزاع الفدية المدعى حدوثها في مجال الرعاية الصحية في جميع أنحاء العالم. وفي عام 2024، ومن بين هجمات أخرى، أعلنت مجموعة "لوك بيت" مسؤوليتها عن هجوم إلكتروني على أكبر مستشفى في كرواتيا ونشرت بيانات سرية عن المرضى مسروقة من نظام مستشفى فرنسي.

أولاً، يجب على كل دولة أن تتصرف وفقاً لإطار سلوك الدول المسؤول في الفضاء الإلكتروني الذي أقرته الجمعية العامة مراراً وتكراراً وبتوافق الآراء. فمن خلال تأكيدنا على هذا الإطار، نكون قد قطعنا بالفعل التزامات للتصدي للأنشطة السيبرانية الخبيثة المنطلقة من أراضينا. وبموجب هذا الإطار، ينبغي للدول ألا تسمح عن علم باستخدام أراضيها لارتكاب أفعال غير مشروعة دولياً باستخدام تكنولوجيا المعلومات والاتصالات، وينبغي أن تستجيب للطلبات المناسبة للتخفيف من ضرر النشاط الخبيث لتكنولوجيا المعلومات والاتصالات المنطلق من أراضيها الذي يستهدف البنية التحتية الحيوية لدولة أخرى.

لذلك، عندما تستهدف جهات برمجيات انتزاع الفدية في إحدى الدول البنية التحتية الحيوية مثل المستشفيات في دولة أخرى، يتعين على الدولة الأولى اتخاذ إجراءات للتحقيق في هذا النشاط والتخفيف من حدته بما يتماشى مع معايير الإطار، خاصة عندما يُطلب منها ذلك. بيد أن بعض الدول – وأبرزها روسيا – مستمرة في السماح لجهات برمجيات انتزاع الفدية بالعمل من أراضيها دون عقاب، حتى بعد أن طُلب منها كبح جماحها. إن مطور ومدير عصابة القرصنة الإلكترونية "لوك بيت" هو المواطن الروسي ديمتري خوروشيف الذي اتهمته وزارة العدل لدينا بارتكاب جرائم اختراق حاسوبي.

وتقييمنا أن مجرمي الإنترنت المرتبطين بالجهات الأكثر تأثيراً لبرمجيات انتزاع الفدية مرتبطون بروسيا، مثل تلك التي ارتكبت الهجوم على مؤسسة أسينشن للرعاية الصحية، استناداً إلى جنسية الأعضاء وموقعهم الجغرافي وولائهم المزعوم أو ارتباطهم بجهات روسية فاعلة معروفة في فضاء الإنترنت. وبعض الجهات التي تغسل الأموال لكبار الجهات الفاعلة في مجال برمجيات انتزاع الفدية هذه تتخذ من روسيا مقراً لها وتستخدم المصارف الروسية أو منصات تداول العملات المشفرة لغسل مكاسبها غير المشروعة.

وفي عام 2021، التقى الرئيس بايدن بالرئيس بوتين وطلب منه كبح جماح هجمات برمجيات انتزاع الفدية على أهداف تابعة للولايات المتحدة. وقد أوضح الرئيس بايدن في ذلك الاجتماع أنه عندما تأتي عملية هجوم لبرمجيات انتزاع الفدية من الأراضي الروسية، حتى وإن

لم تكن برعاية الدولة، فإن الولايات المتحدة تتوقع من الحكومة الروسية أن تتصرف. وبدلاً من أن تتقيد روسيا بالتزاماتها في الأمم المتحدة، فإنها تواصل إيواء هؤلاء المجرمين. وتناشد الولايات المتحدة الدول عدم اتباع ممارسات روسيا في حماية مجرمي الإنترنت الدوليين، وتكرر طلبنا إلى الدول باتباع إطار سلوك الدول المسؤول في الفضاء الإلكتروني كمسألة تتعلق بصون السلام والأمن الدوليين.

إننا نصدر اليوم دعوة إلى العمل – ينبغي للبلدان التي تتعرض لهجوم ببرمجيات انتزاع الفدية ضد أحد المستشفيات أن تبلغ بلد المنشأ بالهجوم وتطلب منه اتخاذ إجراءات تتماشى مع التزامات الأمم المتحدة فيما يتعلق بسلوك الدول المسؤول في الفضاء الإلكتروني.

في الختام، يمكننا أن نقضي على هذه الآفة بشكل جماعي إذا عملنا معاً، والتزمنا بمبادئنا المشتركة، ورفضنا دفع الأموال للعصابات الإجرامية، وساعدنا بعضنا البعض في القبض على مجرمي الإنترنت الذين يعتقدون أن بإمكانهم التملّص من نظامنا. وأشكر الأعضاء على اهتمامهم وأتطلع إلى استمرار وتوسيع نطاق التعاون في الأيام والأشهر المقبلة.

السيد دارماديكاري (فرنسا) (*تكلم بالفرنسية*): أود أن أبدأ بشكر المدير العام لمنظمة الصحة العالمية، الدكتور تيدروس غيبريسوس، والسيد إدواردو كونرادو، على إحاطتيهما اللتين أبرزتا بوضوح المسائل التي هي على المحك في جلسة مجلس الأمن اليوم.

في حزيران/يونيه الماضي، وبمبادرة من رئاسة كوريا الجنوبية، عقد مجلس الأمن مناقشة مفتوحة حول تطور التهديدات السيبرانية (انظر S/PV.9662). وشددت العديد من الدول على التأثير المتزايد على السلام والأمن الدوليين الناتج عن إساءة استخدام تكنولوجيا المعلومات والاتصالات. ومن بين أخطر التهديدات هجمات برمجيات انتزاع الفدية. تستمر تهديدات برمجيات انتزاع الفدية في النمو والتفاقم. وقد شهدنا عام 2023 في فرنسا زيادة بنسبة 30 في المائة في هذه الأنواع من الهجمات عن العام السابق. ويُعزى هذا النمو إلى وصول الشفرة المصدرية وأدوات الاختراق الإلكتروني إلى الأسواق، مما يتيح للعديد من الجهات الإجرامية تنفيذ هجمات سيبرانية.

تؤثر هجمات برمجيات انتزاع الفدية، التي تحركها دوافع مالية، على الأفراد والشركات وعلى تشغيل الخدمات العامة الأساسية ذاتها، وبالتالي على استقرار الدول. واستهدفت حوالي 10 في المائة من هجمات برمجيات انتزاع الفدية التي حددتها السلطات الفرنسية في عام 2023 مؤسسات الرعاية الصحية، مع ما يترتب على ذلك من عواقب وخيمة على تقديم الرعاية الصحية الحيوية. واستهدفت العديد من الهجمات الشركات العاملة في القطاعات الاستراتيجية والمؤسسات البحثية ومؤسسات التعليم العالي والإدارات العامة.

وكما نعلم، يمكن أن تساعد هجمات برمجيات انتزاع الفدية في تمويل انتشار أسلحة الدمار الشامل. وقد أشار أحدث تقرير لفريق الخبراء التابع للجنة مجلس الأمن المنشأة عملاً بالقرار 1718 (2006) (انظر S/2024/215) إلى أن 40 في المائة من برامج كوريا الشمالية النووية والتسيارية غير المشروعة تم تمويلها من أنشطة إجرامية سيبرانية.

ولمواجهة هذه التهديدات، علينا أولاً أن نؤكد التزامنا بالمعايير التي تضمن أمن واستقرار الفضاء السيبراني. وكما أكدت الجمعية العامة في عدد من المناسبات، فإن القانون الدولي، بما في ذلك ميثاق الأمم المتحدة، ينطبق على الفضاء السيبراني. وقد حددت الدول، بتوافق الآراء، سلسلة من معايير السلوك المسؤول للدول في الفضاء السيبراني من أجل تحسين الوقاية من الحوادث السيبرانية وإدارتها. يحث هذا الإطار المعياري الدول على اتخاذ كل التدابير المعقولة لمنع استخدام أراضيها من جانب الجهات السيبرانية الخبيثة لارتكاب أفعال غير مشروعة دولياً. وفي الجمعية العامة، ستواصل فرنسا دعم العمل الهادف إلى تعزيز هذا الإطار المعياري، وتعزيز الفهم المشترك له ودعم الدول في تنفيذه. وستشارك فرنسا بنشاط في العام المقبل في المناقشات التي ستتناول إنشاء آلية برنامج عمل دائم لتحقيق تلك الأهداف.

وتدعم فرنسا المبادرة الدولية لمكافحة برمجيات انتزاع الفدية، التي أطلقتها الولايات المتحدة في عام 2021، وتشارك في هذه المبادرة. وتعزز المبادرة تبادل أفضل الممارسات من أجل صياغة استجابة جماعية للتهديد الذي تشكله برمجيات انتزاع الفدية لمجتمعاتنا وديمقراطياتنا.

وكما شدد عدد من الدول خلال المناقشة المفتوحة التي عُقدت تحت رئاسة كوريا الجنوبية في حزيران/يونيه (انظر S/PV.9662)، يجب على مجلس الأمن، في إطار ولايته، أن يعزز أيضا قبضته على تهديدات الأمن السيبراني. وبعقد جلسات مثل جلسة اليوم، يتمكن المجلس من مواكبة تغير مشهد التهديدات السيبرانية. وفرنسا على استعداد للعمل في سبيل تحسين فهم المخاطر التي تمثلها التحديات السيبرانية في الهيئات الفرعية للمجلس، لا سيما فيما يتعلق بالتحايل على نظم الجزاءات.

السيد ميكاناغي (اليابان) (*تكلم بالإنكليزية*): في البداية، أشكركم، سيدي، على عقد هذه الجلسة بناء على طلب سبعة من أعضاء مجلس الأمن، بما في ذلك اليابان. وأشكر أيضا مقدمي الإحاطتين على أفكارهما الثاقبة.

من الجدير بالملاحظة أن مجلس الأمن يواصل التصدي للتهديدات التي تشكلها الهجمات الإلكترونية في أعقاب الجلسة المعقودة بصيغة آريا والمناقشة المفتوحة التي عُقدت في نيسان/أبريل وحزيران/يونيه (انظر S/PV.9662)، على التوالي. ونشهد اليوم تزايد مخاطر الهجمات الإلكترونية بوسائل أكثر تطورا من أي وقت مضى. وهناك اتجاه تصاعدي للهجمات الإلكترونية التي تستهدف البنية التحتية الحيوية، بما في ذلك الهجمات ببرمجيات انتزاع الفدية ضد مرافق الرعاية الصحية. وأشار تقرير صادر عن فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي (انظر A/76/135) في عام 2021 إلى أن أوجه الاستخدام المعقدة والمتطورة لتكنولوجيا المعلومات والاتصالات تقوض الثقة، وقد تكون تصعيدية ويمكن أن تهدد السلام والأمن الدوليين. ويشير التقرير أيضا إلى مخاطر وعواقب الأنشطة الخبيثة التي تُستخدم فيها تكنولوجيا المعلومات والاتصالات أثناء جائحة فيروس كورونا. وتواصل اليابان التعاون مع جامعة أكسفورد في دراسة الجوانب القانونية لهذه المسائل من خلال عملية أكسفورد بشأن الحمايات التي يوفرها القانون الدولي في الفضاء السيبراني وتقرير نُشر في العام الماضي عن العمليات السيبرانية ضد قطاع الرعاية الصحية. وتشكل مواطن الضعف في تكنولوجيا المعلومات والاتصالات عامل خطورة للعالم بأسره. ولا يمكن لأي بلد أن يتعامل مع التهديد بمفرده وعلينا أن نعمل معا على سبيل الاستعجال.

وتشكل برمجيات انتزاع الفدية واحدا من أكبر التهديدات السيبرانية التي تسبب الأعطال والتي تقوض عمليات البنية التحتية الحيوية في المجتمع، بما في ذلك المستشفيات ومحطات توليد الطاقة. وبالنظر إلى الآثار والتداعيات العامة، من المؤكد أن برمجيات انتزاع الفدية يمكن أن تشكل أخطارا مباشرة تهدد السلام والأمن الدوليين. وواجهت بعض المستشفيات اليابانية أيضا عوائق كبيرة في رعاية المرضى في حالات الطوارئ والعمليات الجراحية المقررة بسبب هجمات برمجيات انتزاع الفدية. ومن الأهمية بمكان منع شن هجوم ببرمجيات انتزاع الفدية، وفي حالة وقوع هجوم، تقليل الاضطراب الاجتماعي والاقتصادي الناتج عنه إلى أدنى حد ممكن. ولهذه الأغراض، تقدر اليابان تبادل المعلومات والتعاون الوثيق بين سلطات الدول الأعضاء، بما في ذلك وكالات إنفاذ القانون التي تعمل على التوعية بالأهداف المحتملة لهجمات برمجيات انتزاع الفدية؛ وتعزيز القدرة على الصمود في مواجهة تهديدات الأمن السيبراني؛ وبناء القدرات. ومن هذا المنطلق، لا يزال من الضروري تطوير القدرة الجماعية على الصمود لمنع مختلف الجهات الفاعلة من استغلال أي أوجه ضعف إزاء هجمات برمجيات انتزاع الفدية. وتقدر اليابان وتثمن مبادرة مكافحة برمجيات انتزاع الفدية التي تقودها الولايات المتحدة وتتشاطر التزامها الراسخ بالعمل معا على مستوى السياسات والعمليات لمواجهة تهديدات برمجيات انتزاع الفدية. ومن الضروري أيضا تعزيز برامج بناء القدرات لتعزيز الأمن السيبراني من أجل ضمان سلامة البنية التحتية السيبرانية وقدرتها على الصمود. وتحقيقا لهذه الغاية، تقدم اليابان الدعم في بناء قدرات بلدان المحيطين الهندي والهادئ وستواصل القيام بذلك بالتعاون مع البلدان التي تشاطرها الرأي والمنظمات الدولية ودوائر الصناعة والأوساط الأكاديمية.

وتؤكد اليابان أهمية سيادة القانون في الفضاء الإلكتروني. وفي إطار الأمم المتحدة، نشارك في مناقشات ملموسة بشأن تطبيق القانون الدولي القائم وتنفيذ المعايير والقواعد والمبادئ المتفق عليها لسلوك الدول المسؤول. وفي حين أننا اتفقنا على أن القانون الدولي الحالي

ينطبق على العمليات السيبرانية، اكتشفنا أيضا أنه لا يوجد اتفاق بشأن المسائل الرئيسية، بما في ذلك انتهاكات السيادة وتطبيق مبدأ بذل العناية الواجبة. ومن أجل صون السلام والأمن مع الاعتماد على تدفق البيانات عبر الحدود عبر الإنترنت، يجب أن نسعى إلى تحقيق توازن مناسب بين التدفق الحر للبيانات والسيادة الإقليمية، في أقرب وقت ممكن. ونرى أن عدم الاتفاق الراهن بشأن هذه المسائل ليس في صالح صون السلام والأمن الدوليين. وبالتالي، علينا أن نضاعف جهودنا في البحث عن أرضية مشتركة بشأن تطبيق القانون الدولي القائم. ولتحقيق هذه الغاية، يمكن لمجلس الأمن أن يؤدي دورا في هذا الصدد أيضا. وقد يكون من الصعب على المجلس تحديد وجود خطر يهدد السلام والأمن الدوليين استنادا إلى محاولة واحدة لخرق نظام المعلوماتية، ولكن بالنظر إلى الاتجاه المثير للقلق المتمثل في زيادة العمليات السيبرانية الخبيثة مثل هجمات برمجيات انتزاع الفدية على قطاع الرعاية الصحية، قد يكون مجلس الأمن قادرا على تحديد أن بعض اتجاهات العمليات السيبرانية الخبيثة تشكل خطرا يهدد السلام والأمن الدوليين.

وبينما نواصل عملنا، تتطلع اليابان إلى الإسهام في الدورات القادمة للفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها. وتعتقد اليابان أن برنامج العمل للارتقاء بسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي ينبغي أن يكون بمثابة منبر دائم في المستقبل لضمان الانتقال السلس من الفريق العامل بعد عام 2025. أخيرا، ستواصل اليابان بذل الجهود لمكافحة التهديدات السيبرانية والسعي إلى تحقيق الحرية والعدالة والأمن في الفضاء الإلكتروني.

السيد كاميليري (مالطة) (*تكلم بالإنكليزية*): نشكر الدكتور غيبريسوس والسيد كونرادو على ملاحظاتهما الثاقبة.

إن تطور الأساليب المستخدمة في برمجيات انتزاع الفدية يمثل تصعيدا شديدا في مشهد تهديدات الأمن السيبراني. فقد أصبحت هذه الهجمات أكثرا ضررا، مما يزيد من صعوبة استعادة القدرة على العمل دون الرضوخ لمطالب الجهات ذات النوايا الخبيثة. ولهذا السبب، انضمت مالطة إلى الدعوة إلى عقد هذه الجلسة. واعتبرت منظمة الصحة العالمية برمجيات انتزاع الفدية الخطر الرقمي الرئيسي الذي يهدد الرعاية الصحية ويزداد الوضع سوءا بسبب التحول الرقمي الناجم عن مرض فيروس كورونا. ولا تقتصر الهجمات على تهديد سبل الحصول على الخدمات الطبية الأساسية فحسب، بل تنتهك أيضا حق الفرد الأساسي في الخصوصية وتهدد رفاه المواطنين وأمنهم عموما وحقوقهم الإنسانية الأساسية.

ويسلط التقرير المرحلي السنوي الصادر في تموز/يوليه عن الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها الضوء على القلق المتزايد لدى الدول بشأن برمجيات انتزاع الفدية، مشيرا إلى زيادة تواتر الهجمات وخطورتها. وأدى ظهور برمجيات انتزاع الفدية باعتبارها خدمة إلى توسيع نطاق الجهات الفاعلة ذات النوايا الخبيثة الضالعة في الأمر. ويؤكد التقرير ضرورة اتباع نهج شامل لمواجهة تهديد برمجيات انتزاع الفدية، يشمل استهداف التمويل غير المشروع لهذه الأنشطة. وخلال المناقشة رفيعة المستوى التي أجراها مجلس الأمن بشأن التهديدات السيبرانية أثناء رئاسة جمهورية كوريا في حزيران/يونيه (انظر S/PV.9662)، أقرت عدة وفود بقدرة برمجيات انتزاع الفدية على زعزعة استقرار الحكومات وتعطيل الخدمات العامة الأساسية. وأكدت أيضا تزايد حدة هجمات هذه البرمجيات والهجمات الإلكترونية التي ترعاها الدول والتي تستهدف البنية التحتية الحيوية.

كما ورد التأكيد على هذه الشواغل في التقرير النهائي لفريق الخبراء التابع للجنة المنشأة عملاً بالقرار 1874 (2009) (انظر S/2024/215)، الذي أشار إلى أن التحقيقات جارية في 58 واقعة يشتبها بأنها هجمات إلكترونية خلال الفترة بين عامي 2017 و 2023، بقيمة حوالي 3 بلايين دولار. وتفيد التقارير بأن هذه الهجمات تساعد جمهورية كوريا الشعبية الديمقراطية في التحايل على الجزاءات ومواصلة تطوير أسلحة دمار شامل. وتدرك مالطة الطابع السريع التطور للتهديدات المستندة إلى التكنولوجيا وتؤكد ضرورة وضع تدابير شاملة لمواجهتها. ومن الضروري أن تكفل الدول الأعضاء

تزويد القوة العاملة في مجال تكنولوجيا المعلومات، لا سيما في مجال الرعاية الصحية، بأحدث المهارات في مجال الأمن السيبراني. وإضافة إلى ذلك، من الأهمية بمكان التوعية على المستوى التنفيذي بإمكانية أن تكون الهجمات السيبرانية بمثابة حالة طوارئ صحية عامة.

ومن الضروري الاستثمار في رأس المال البشري وإعداد عمليات قوية للاستجابة للحوادث وتدريب الموظفين السريريين للحفاظ على جودة الخدمة أثناء الهجمات الإلكترونية. ومن المهم أيضا إرساء سبل تواصل قوية داخل كيانات الرعاية الصحية من أجل تنسيق الاستجابات، وربما عبر الحدود. فللجهود الوطنية وحدها أثر محدود. ويجب استكمالها أيضا بالتعاون الدولي لضمان الالتزام بالقانون الدولي. وتشكل هجمات برمجيات انتزاع الفدية عبر الحدود مخاطر متزايدة على الصحة العامة، مع ما يترتب عليها من آثار تتجاوز كثيرا مجرد الأعطال التقنية. وأدى توفر هذه البرمجيات عبر الإنترنت إلى تقليل الحواجز أمام الهجمات، بما في ذلك هجمات جماعات الجريمة المنظمة العابرة للحدود الوطنية، مما يسهل على الجهات الفاعلة ذات النوايا الخبيثة تنفيذ عملياتها على مستوى العالم.

ويتعين تعميم مراعاة المنظور الجنساني في تنفيذ المعايير السيبرانية ومراعاة الاعتبارات الجنسانية في بناء القدرات. ويكتسي انخراط المرأة ومشاركتها في صنع القرار في المجال السيبراني أهمية بالغة، خاصة في سياقات النزاع وما بعد النزاع. ومن الضروري ضمان مراعاة المنظور الجنساني في استراتيجياتنا للأمن السيبراني لإيجاد حلول شاملة وفعالة.

في الختام، نتطلع إلى مواصلة مناقشاتنا حول الأمن السيبراني ونثني على الجهود المبذولة لإبراز الدور البالغ الأهمية لمجلس الأمن. ونؤكد مجددا دعمنا لبرنامج العمل الذي تسترشد به الأمم المتحدة. ونعتقد أن الإطار المتفق عليه لسلوك الدول المسؤول في الفضاء السيبراني ضروري للوفاء بمسؤولياتنا المشتركة والتوفيق بين مصالحنا المشتركة.

السيد هوانغ (جمهورية كوريا) (*تكلم بالإنكليزية*): أعرب عن امتناني للمدير العام لمنظمة الصحة العالمية وللسيد كونرادو على آرائهما القيّمة.

ترحب جمهورية كوريا بعقد جلسة اليوم حسنة التوقيت بشأن برمجيات انتزاع الفدية التي تشكل أحد أبرز أنواع الهجمات السيبرانية. وما يحفزنا هو الزخم المستمر في مناقشات الأمن السيبراني في مجلس الأمن هذا العام، استنادا إلى الاجتماع المعقود بصيغة آريا في شهر نيسان/أبريل والمناقشة المفتوحة التي عُقدت في حزيران/يونيه (انظر S/PV.9662) وشكلت الحدث المميز لرئاسة جمهورية كوريا لمجلس الأمن. وأكدت العديد من البلدان خلال هذين الاجتماعين أن برمجيات انتزاع الفدية، إلى جانب أنواع أخرى من التهديدات السيبرانية، تبرز بوصفها تحديا خطيرا للسلام والأمن الدوليين. وما فتئت العديد من البلدان تؤكد ضرورة أن يتصدى مجلس الأمن للتهديدات السيبرانية وفقا لمسؤوليته الرئيسية التي أناطه بها ميثاق الأمم المتحدة. وفي هذا الصدد، أود التركيز على النقاط التالية:

أولا، تشكل الأنشطة السيبرانية الخبيثة، بما في ذلك هجمات برمجيات انتزاع الفدية، عوامل مضاعفة للخطر وتفضي إلى تفاقم التحديات القائمة وتضخيم النزاعات. فهي تعطل الخدمات الاجتماعية أو العامة الأساسية، مما قد يؤدي إلى عدم الاستقرار الاجتماعي وتقويض الأمن القومي. ففي أوكرانيا، تسبب عدد من الهجمات السيبرانية التي استهدفت البنية التحتية الحيوية، مثل شبكات الكهرباء ونُظم الاتصالات السلكية واللاسلكية، في انقطاع التيار الكهربائي على نطاق واسع وتعطل الشبكات. إنها لا تتسبب في معاناة إنسانية فحسب، بل تزيد أيضا من تصعيد الحرب.

ثانيا، تقوض الهجمات السيبرانية على نحو خطير نظم الجزاءات التي يفرضها مجلس الأمن. فعلى سبيل المثال، يشير التقرير السنوي لفريق الخبراء التابع للجنة المنشأة عملا بالقرار 1718 (2006) (انظر S/2024/215) إلى أن جمهورية كوريا الشعبية الديمقراطية تجني نحو 50 في المائة من إيراداتها من العملات الأجنبية من خلال الأنشطة السيبرانية الخبيثة. وهذا يؤكد بوضوح كيف أصبحت الهجمات السيبرانية أداة أساسية للالتفاف على جزاءات مجلس الأمن وإبطالها. وعلاوة على ذلك، تستفيد الجماعات المسلحة الخاضعة للجزاءات من

الأنشطة السيبرانية غير القانونية لجمع الأموال وإخفاء الأصول والاتجار بالأسلحة، مما يعقد إنفاذ عمليات تجميد الأصول وحظر الأسلحة.

ثالثا، ترتبط هذه الإيرادات غير المشروعة بانتشار أسلحة الدمار الشامل، وهو ما يقع ضمن الاختصاص المباشر لمجلس الأمن. وبالفعل، تمول جمهورية كوريا الشعبية الديمقراطية 40 في المائة من برامجها غير القانونية المتعلقة بتطوير أسلحة الدمار الشامل والقذائف من خلال الأنشطة السيبرانية الخبيثة على غرار ما أشار إليه أحدث تقرير لفريق الخبراء. وأطلقت جمهورية كوريا الشعبية الديمقراطية الأسبوع الماضي سلسلة من القذائف التسيارية، بما في ذلك نوع جديد من القذائف التسيارية العابرة للقارات. وغني عن القول إن العاملين في مجال تكنولوجيا المعلومات من كوريا الشمالية ضالعون أيضًا في جرائم خطيرة مثل سرقة الملكية الفكرية من العديد من شركات الدفاع العالمية بهدف تطوير قدرات البلد في مجال أسلحة الدمار الشامل.

ونعتقد أن هناك حاجة ماسة إلى تعزيز دور مجلس الأمن وتقوية التعاون الدولي من أجل التعامل مع التهديدات الوشيكة التي تشكلها الهجمات السيبرانية، بما في ذلك برمجيات انتزاع الفدية. أما على مستوى مجلس الأمن، فينبغي أن ننظر في طلب تقارير منتظمة من الأمين العام عن التهديدات السيبرانية المتطورة لإدراج الأمن السيبراني في جدول أعمال المجلس وعقد جلسات منتظمة لمجلس الأمن كما نفعل بشأن بنود جدول الأعمال الأخرى. ويمكننا اتخاذ إجراءات في الأجل المتوسط إلى الطويل لتحقيق المساءلة في مجلس الأمن في إطار التصدي للأنشطة السيبرانية التي تنتهك القانون الدولي وتضر بالسلام والأمن الدوليين.

وفيما يتعلق بالحاجة إلى التعاون الدولي، نود أن نشدد على الطابع العالمي للتهديدات السيبرانية الذي يتضح من الحوادث الأخيرة التي وقعت خلال السنوات القليلة المنصرمة في كوستاريكا وترينيداد وتوباغو حيث أدت هجمات برمجيات انتزاع الفدية إلى الإعلان عن حالات طوارئ وطنية.

ولا تزال جمهورية كوريا تتعرض أيضا للهجمات السيبرانية. ووقع مؤخرا في هذا الأسبوع هجوم لحجب الخدمة الموزَّع، مستهدفا وزارة الدفاع الوطني. وأعلنت حكومة بلدي قبيل ساعات عن زيادة وتيرة الهجمات السيبرانية التي تشنها مجموعات القرصنة الموالية لروسيا بعد نشر كوريا الشمالية قوات في روسيا.

ونظرا لطابع الفضاء السيبراني العابر للحدود الوطنية، فإن أمننا السيبراني لا يكون قويا إلا بقدر قوة أضعف حلقاته. ولذلك، يكتسي التعاون الدولي وبناء القدرات على الصعيد الدولي، ولا سيما مع البلدان النامية، أهمية بالغة في التصدي للتهديدات السيبرانية. وتحقيقا لهذه الغاية، تشارك حكومة بلدي حاليا في مبادرة مكافحة برمجيات انتزاع الفدية التي تقودها الولايات المتحدة الأمريكية والتي تهدف إلى تعزيز الوعي العالمي وبناء القدرة الجماعية على الصمود في مواجهة برمجيات انتزاع الفدية.

وتعتقد جمهورية كوريا اعتقادا راسخا أنه ينبغي لمجلس الأمن، حفاظا على أهميته، أن يولي مزيدا من الاهتمام للتهديدات الناجمة عن التكنولوجيات الناشئة مثل الذكاء السيبراني والذكاء الاصطناعي. وبالإضافة إلى جهودنا المستمرة، مثل اعتماد مشروع قرار الجمعية العامة بشأن الذكاء الاصطناعي في المجال العسكري في اللجنة الأولى هذا الأسبوع (A/C.1/79/L.77) وقمة تسخير الذكاء الاصطناعي المسؤول في المجال العسكري لعام 2024 المعقودة في سول، ستواصل جمهورية كوريا الاضطلاع بدورها في مجلس الأمن.

السيدة بلوكار دروبيتش (سلوفينيا) (*تكلمت بالإنكليزية*): أود أن أشكر المدير العام غيبريسوس والسيد كونرادو على إسهاماتهما القيّمة في إحاطة اليوم.

إن سلوفينيا عضوٌ في مبادرة مكافحة برمجيات انتزاع الفدية. وبهذه الصفة، نود أولا أن نلفت انتباه المجلس إلى أحدث تقرير مرحلي سنوي صادر عن الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021–2015 (انظر A/79/214). وفي التقرير، أعربت الدول الأعضاء في الأمم المتحدة عن قلقها إزاء تزايد حجم وشدة هجمات برمجيات انتزاع الفدية التي تعطل الخدمات الأساسية، بما في ذلك قطاع الرعاية

الصحية، وهو أمر خطير ومقلق جدا. وسلطت الدول الأعضاء أيضا الضوء على أن هذه الهجمات يمكن أن تؤثر على السلام والأمن الدوليين وأنها تتطلب استجابة شاملة.

ولا يزال موقفنا من المناقشات المتعلقة بالفضاء السيبراني في المجلس يسترشد بمسؤولية المجلس الأساسية المتمثلة في صون السلام والأمن الدوليين. ونظرا للطابع الفريد جدا للفضاء السيبراني، فإن المشكلة دولية ونادرا ما تنحصر في الحدود الوطنية. ومن ثم، يتعلق الأمر بمشكلة لا يمكن حلها إلا بدرجة عالية من التعاون الدولي. وللوفاء بهذه المسؤولية، يجب أن يشارك المجلس بفاعلية في التصدي للتهديدات التي تشكلها هجمات برمجيات انتزاع الفدية، بما في ذلك على المستشفيات وغيرها من مرافق الرعاية الصحية وخدماتها.

وفي أعقاب جائحة مرض فيروس كورونا والتحول الرقمي السريع لمؤسسات الرعاية الصحية على الصعيد العالمي، تزايد استهداف هجمات برمجيات انتزاع الفدية لتلك الكيانات. وتُحفَّز الجهات الفاعلة الحكومية وغير الحكومية لاستغلال نظم تكنولوجيا المعلومات البالغة الأهمية في مجال الرعاية الصحية أو لتقويض سرية البيانات الشخصية والبيانات المتعلقة بالصحة. وفي العديد من الحالات، تُؤوي الحكومات جهات من غير الدول أو حتى تيسر عملها. وتشكل هجمات برمجيات انتزاع الفدية على المرافق والمؤسسات الصحية تهديدًا مباشراً للصحة العامة والسلامة والأمن.

وبسبب هذه الهجمات، تتعطل بصورة مستمرة خدمات التصوير التشخيصي وعلم الأمراض وأقسام الطوارئ وخدمات الإسعاف ورعاية مرضى السرطان. وهذه ليست جريمة بلا ضحايا؛ بل إن هناك أرواحا بشرية معرضة للخطر. ولا شك في أن هناك آثارا مالية أيضا لهذه الهجمات حيث تشير التقديرات إلى أن هجوما باستخدام برمجيات انتزاع الفدية على نظام الرعاية الصحية لإحدى الدول الأعضاء قد كلف حوالي 100 مليون دولار. ويمكن استخدام هذه الأموال في تمويل جرائم أخرى وربما حتى في تمويل الإرهاب.

ونظراً للتطور السريع للذكاء الاصطناعي الذي أدى إلى زيادة وتيرة تنفيذ هجمات برمجيات انتزاع الفدية وسمح للجهات الفاعلة الحكومية وغير الحكومية على حد سواء بتنفيذ تلك الهجمات دون الحاجة إلى مهارات تكنولوجية عالية، فإن هناك حاجة إلى استجابة حاسمة من المجتمع الدولي لمنعها والتخفيف من آثارها. يمثل بناء القدرات، وتحديداً على الصعيد الفني، أساساً راسخاً لتعزيز الصمود الإلكتروني. وفي هذا السياق، شاركت سلوفينيا في تأسيس المركز الإقليمي للقدرات السيبرانية لغرب البلقان وبرنامجه لتأهيل المدربين، الذي يُنفّذ بكفاءة تدريبات إقليمية في منطقة غرب البلقان منذ عام ونصف.

ولما كانت أغلب هجمات طلب الفدية تتسم بطابعها العابر للحدود، فإنه يتوجب على المجلس أن يؤدي دوراً حاسماً في نزع فتيل التوترات وتعزيز المساءلة، ولا سيما حين تعرّض مثل هذه الهجمات الأمن والحياة للخطر. ونعتقد أيضاً أنه بإمكان المجلس دراسة إمكانية إدراج مجرمي الإنترنت في قوائم الجزاءات.

دعوني أختم بالتأكيد لزملائي في المجلس على التزامنا الذي لا يتزعزع بالعمل معهم ومع عموم أعضاء الأمم المتحدة لمواصلة المناقشات بشأن برمجيات انتزاع الفدية، والتي تشكل هاجساً مشتركاً فيما يخص السلم والأمن الدوليين. كما نظل راسخين في التزامنا بمواصلة تنفيذ التدابير الرامية إلى التخفيف من حدة تلك المخاطر، بما في ذلك تنفيذ المعايير الحالية لسلوك الدولة المسؤول في الفضاء الإلكتروني.

السيد نيبنزيا (الاتحاد الروسي) (*تكلم بالروسية*): نود أن نشكر الدكتور تيدروس غيبريسوس، المدير العام لمنظمة الصحة العالمية، على إحاطته. واستمعنا بإمعان إلى السيد إدواردو كونرادو، رئيس مؤسسة أسينشن غير الربحية للخدمات الصحية.

يدرك جميع أعضاء المجتمع الدولي تماماً مدى الاهتمام الذي يوليه الاتحاد الروسي لمسائل الأمن المتعلقة باستخدام تكنولوجيات المعلومات والاتصالات. كان بلدنا، منذ ما يربو على ربع قرن، السبّاق في بدء المناقشات بشأن هذه المسألة داخل الأمم المتحدة. كانت روسيا صاحبة فكرة إنشاء منصات تفاوضية متخصصة داخل الأمم المتحدة، بما فيها الفريق العامل المفتوح العضوية الحالي والناجح المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021–

2025. كما بادرنا بأعمال اللجنة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، حيث اتفق بنجاح على مشروع وثيقة في آب/أغسطس (انظر A/AC.291/22/Rev.2).

توجد آليات مواضيعية شاملة متعددة لمناقشة المسائل المتصلة بأمن المعلومات، تشمل طيفاً واسعاً من التهديدات الراهنة والمحتملة في ذلك المجال. لذلك، لم يتضح لنا بعد ما الذي استوجب الحاجة إلى توسيع دائرة المناقشة لتشمل مجلس الأمن. ولم نسمع اليوم إجابة محددة على هذا السؤال. وعلاوةً على ذلك، وحيث إن جلسة اليوم قد طُلب عقدها خلال مهلة زمنية وجيزة جداً، لم نتمكن من استيعاب ما الذي يشكل تهديداً آنياً وملموساً للسلم والأمن الدوليين من خلال بيانات الدول التي بادرت بطلب عقدها. وهذه تحديداً هي الحالات التي ينبغي لمجلس الأمن أن يعطيها الأولوية استنادا إلى ولايته.

ونظراً لتركيز جلسة اليوم على مسألة برمجيات انتزاع الفدية، نود الإشارة إلى أن مشروع اتفاقية الأمم المتحدة لمكافحة الجرائم الإلكترونية، الذي أشرت إليه، مُصمم لمكافحة هذا النوع من البرمجيات الخبيثة بالتوازي مع أنواع أخرى من الجرائم المتعلقة بتكنولوجيا المعلومات والاتصالات والتي لا تقل خطورة على الأمن العام والشخصي. ونحن نحث جميع زملائنا على التركيز على تيسير سرعة دخول تلك المعاهدة الدولية العملية المهمة حيز النفاذ. وفضلاً عن ذلك، وفي ظل التوسع المستمر في نطاق تهديدات الجريمة الإلكترونية، يتعين علينا أن ننظر من الآن في مواصلة تطوير الاتفاقية عبر اعتماد بروتوكولات إضافية لها.

فيما يتعلق بضمان حماية البنية التحتية الحيوية، بما في ذلك مرافق الرعاية الصحية، من الاستخدامات الضارة لتكنولوجيا المعلومات والاتصالات، فإن روسيا على دراية تامة بهذه المخاطر. يواجه بلدنا باستمرار هجمات إلكترونية على مرافق الرعاية الصحية. ومنذ بداية عام 2022، شهدنا مراراً حوادث مختلفة في طابعها ونطاقها – امتدت من سرقة البيانات الشخصية للمرضى وتعطيل أجهزة تصوير مقطعي حاسوبي، إلى قرصنة المواقع الإلكترونية لمستشفيات الأطفال، مما أدى إلى توقفها عن العمل. وتتحمل المجموعات الأوكرانية في العديد من الحالات المسؤولية عن هذه الهجمات – وخاصة جيش تكنولوجيا المعلومات الأوكراني الذي يحظى بدعم الناتو.

ونود أن نذكّر بأن التفاهم التوافقي بشأن ضرورة ضمان أمن المرافق التي تقدم خدمات حيوية للسكان قد تأكد مراراً في إطار عمل فريق الخبراء الحكوميين والأفرقة العاملة المفتوحة العضوية الحالية المعنية بأمن تكنولوجيا المعلومات والاتصالات على الصعيد الدولي. كما طورت المعايير ذات الصلة هناك. نحن مقتنعون بأن المساهمة الأكبر في تعزيز أمن البنية الأساسية الحيوية ستتحقق من خلال تقنين الترتيبات المعنية، والتي تتسم في الوقت الراهن بطابعها الطوعي وغير الملزم.

وتحقيقاً لهذه الغاية، نحبذ الإسراع في وضع صك قانوني دولي يغطي جميع جوانب ضمان الأمن في استخدام تكنولوجيا المعلومات والاتصالات. وستكون المنصة الأنسب للجهود في هذا المجال آلية تفاوض دائمة تحت رعاية الأمم المتحدة، يتم إنشاؤها عند انتهاء ولاية الفريق العامل المفتوح العضوية الحالي في عام 2025. وفي الواقع، اعتمدت اللجنة الأولى للجمعية العامة بتوافق الآراء، قبل يومين فقط، مشروع قرار قدمته سنغافورة يكرس ذلك الاتفاق (A/C.1/79/L.13).

وعودة إلى تحفظاتنا بشأن القيمة التي ستضيفها جلسة اليوم، نعتقد أنه من المهم تذكر أن نظر مجلس الأمن في مسائل الاستخدام الضار لتكنولوجيات المعلومات والاتصالات، وخاصة ما يتعلق بوقائع محددة، يعقده الطابع الخاص للفضاء الإلكتروني. نتحدث بداية عن خاصية إخفاء الهوية فيه، مما يجعل من المستحيل تقريبًا تحديد مصدر النشاط الخبيث بشكل موثوق. وفي ضوء ذلك، فإن أية محاولات للجوء إلى ما يسمى بالإسناد القائم على دوافع سياسية هي محاولات غير بناءة بشكل كبير بل وخطيرة – إذ أنها تخفي في الواقع رغبة مبتذلة في الاحتفاظ بحق توجيه اتهامات لا أساس لها ومسيسة ضد الدول المناوئة، بالطبع دون تقديم أي دليل على الإطلاق.

وللأسف، لم تكن جلسة اليوم استثناءً من هذه القاعدة. ومجدداً، قررت الولايات المتحدة استخدام منصة مجلس الأمن للترويج لسرديتها المنفصلة تماماً عن الواقع. لقد أصبحت التكهنات حول ما يسمى بقراصنة روس والتلميحات عن دعم بلدنا المزعوم للأنشطة الخبيثة في مجال استخدام تكنولوجيات المعلومات والاتصالات باتت منذ وقت طويل وكأنها مزحة، لا يسعُ أي شخص عاقل إلا الضحك عند سماعها.

بيد أن واشنطن تصر على اللجوء إلى ذلك الخطاب، مخاطبة على ما يبدو جمهورها المحلي بالدرجة الأولى. فحتى خلال الانتخابات الرئاسية الأمريكية التي جرت يوم الثلاثاء، طرحت نظرية التدخل الروسي المثير للجدل بشكل متكرر أمام عامة الناس، رغم أن وكالة الأمن الإلكتروني وأمن البنية التحتية الأمريكية نفسها أكدت عدم وجود أي محاولات للتأثير على النتائج على نحو ضار. ومع ذلك، تستمر الولايات المتحدة وحلفاؤها في استخدام الخطاب ذاته بشأن تهديد إلكتروني وهمي من خصومهم السياسيين. لقد أوضحنا مراراً افتقار هذه التلميحات لأي أساس في إطار المنتديات ذات الصلة.

ونود أن نشير إلى أنه في إطار المناقشة التي جرت تحت رعاية الجمعية العامة، اتخذت تدابير عملية لتعزيز التعاون غير المسيّس بين الدول الأعضاء في الأمم المتحدة في مجال أمن المعلومات، بما في ذلك ما يتعلق بالتصدي للهجمات الإلكترونية. وأشير بالدرجة الأولى إلى الدليل العالمي لنقاط الاتصال الحكومية الدولية أطلق في أيار/مايو بمبادرة من الاتحاد الروسي. وتهدف هذه الآلية إلى منع وقوع حوادث خطيرة في الفضاء الإلكتروني وحلها، فضلاً عن الحد من التوترات في حالات الأزمات. وفي حال وقوع حوادث خطيرة للاستخدام الخبيث لتكنولوجيا المعلومات والاتصالات، بإمكان أي دولة استخدام تلك الأداة. ومن اللافت للنظر أننا لم نتلق أي طلبات عبر السجل من تلك البلدان التي تتهم روسيا بتعصب شديد بتنفيذ هجمات إلكترونية. وهذا يبرهن مجدداً على أن الولايات المتحدة وحلفاءها لا يمتلكون أي أدلة فنية يدعم استنتاجاتها.

وفي الوقت ذاته، لا تتوانى واشنطن نفسها عن الإقرار بوقائع عملياتها الخاصة المنفذة ضد روسيا باستخدام تكنولوجيات المعلومات والاتصالات، إضافة إلى تنامي قدراتها الهجومية في ذلك المجال. علاوة على ذلك، تمارس أجهزة الاستخبارات الأمريكية على نطاق واسع ما يسمى بعمليات التضليل. وهي تفعل ذلك حتى ضد أقرب حلفائها، الذين يبدون نشاطاً كبيراً في دعمهم للولايات المتحدة في الترويج لسياساتها العدوانية.

وبالنظر إلى الاعتبارات المذكورة، نعتقد أنه من الصعب اعتبار جلسة اليوم استخداماً رشيداً لوقت المجلس وموارده. ولا يتعدى نقاشنا كونه تكراراً مملاً للمواقف الوطنية المعروفة وازدواجية في العمل الذي يجري تحت رعاية الجمعية العامة. وإذا كان زملاؤنا الغربيون يرغبون في مناقشة أمن مرافق الرعاية الصحية، ألا يعتقدون أن ما يجب أن نبدأ به ليس التهديدات المنطلقة من الفضاء الإلكتروني، بل ضرورة أن يتفق مجلس الأمن على خطوات ملموسة لوقف الهجمات الإسرائيلية المروعة والعبثية على المستشفيات في قطاع غزة، التي تقتل الآلاف من الأشخاص؟ وإلى أن يحدث ذلك في العالم الحقيقي، يبدو أن تحويل انتباه المجلس إلى العالم الافتراضي سيؤدي إلى نتائج عكسية بل ويدعو حتى إلى السخرية.

وندعو جميع الدول ذات العقلية البناءة إلى مواصلة مشاركتها الفعالة في المناقشة العالمية بشأن الأمن الدولي لتكنولوجيا المعلومات والاتصالات. ويظل بلدنا ملتزماً التزاماً قوياً بمواصلة الحوار مع المجتمع الدولي بأسره بهدف إنشاء فضاء إلكتروني سلمي وآمن، بما في ذلك من خلال وضع اتفاقات ملزمة قانوناً في ذلك المجال في إطار آليات شاملة متخصصة تحت رعاية الجمعية العامة. ونأمل أن يمكّننا هذا التعاون من الاستجابة بفعالية وبشكل جماعي لأي تهديدات في ذلك المجال.

السيد غنغ شوانغ (الصين) (*تكلم بالصينية*): أشكر الدكتور تيدروس أدهانوم غيبريسوس، المدير العام لمنظمة الصحة العالمية، والسيد إدواردو كونرادو على إحاطتيهما.

إننا نعيش في عصر إلكتروني سريع التغير. ففي الوقت الذي نستفيد فيه تماماً من فرص التنمية التي يوفرها الفضاء الإلكتروني، نواجه كذلك تحديات معقدة ومتنوعة في مجال الأمن السيبراني. وقد أصبحت الهجمات السيبرانية والجرائم الإلكترونية والإرهاب السيبراني

خطراً عالمياً متزايداً، وبرمجيات انتزاع الفدية من أبرز المشاكل في ذلك الصدد. إن مشكلة برمجيات انتزاع الفدية متخصصة وتقنية للغاية. وهي في الأساس جريمة إلكترونية. ولا تؤيد الصين الدفع المتسرع من قبل أعضاء مجلس الأمن المعنيين لمناقشة هذه المسألة في المجلس، وتأمل أن تتمكن جميع الأطراف من إجراء مناقشات أكثر تخصصاً وعملية وتعمقاً في منابر أخرى أكثر ملاءمة.

لقد أورد مقدما الإحاطتين وبعض الأعضاء لتوهم أمثلة على هجمات برمجيات انتزاع الفدية في بياناتهم. وتدعم الصين جهود المجتمع الدولي لتحليل ومعالجة الأبعاد المتعددة لتلك المشكلة، مثل مصادر برمجيات انتزاع الفدية ومسارات انتشارها وقنوات تحقيق الدخل منها. ونعتقد أنه ينبغي للدول تكثيف تبادل المعلومات والتعاون التقني في مجال إنفاذ القانون والتعاون القضائي في جهد مشترك للاستجابة.

إن برمجيات انتزاع الفدية ما هي إلا واحدة من التحديات العديدة التي تواجه الأمن السيبراني. فهناك أنواع أخرى من الهجمات السيبرانية، مثل التصيد الإلكتروني واختراق الأنظمة السحابية وسرقة البيانات الشخصية وهجمات الحرمان من الخدمة الموزعة التي تتزايد بسرعة أيضاً، إذ صارت أساليب عمل الجرائم السيبرانية أكثر تنوعاً ومنهجية. وتدعم الصين تعزيز حوكمة الأمن السيبراني والحفاظ على السلام والاستقرار الدائمين في الفضاء السيبراني. ولتحقيق تلك الغاية، ندعو جميع الأطراف إلى بذل الجهود في المجالات التالية.

أولاً، يجب علينا أن نتمسك بحزم بالطبيعة السلمية للفضاء الإلكتروني. ويجب علينا أن نعارض الممارسات الخاطئة مثل تعريف الفضاء السيبراني كمجال للعمليات العسكرية ووضع قواعد الاشتباك في الفضاء السيبراني وبناء تحالفات عسكرية سيبرانية وإدراج البنية التحتية الحيوية للدول الأخرى كأهداف للهجمات السيبرانية. ونرفض عسكرة الفضاء السيبراني وسباق التسلح فيه بهدف الحد بشكل أساسي من تطوير وانتشار التقنيات السيبرانية الهجومية، بما في ذلك برمجيات انتزاع الفدية.

ثانياً، يجب علينا أن نتمسك بدور الأمم المتحدة كقناة رئيسية. فعلى أساس المشاركة الواسعة وعلى قدم المساواة، ينبغي لنا صياغة قواعد دولية بشأن الفضاء الإلكتروني تكون مقبولة بشكل عام لجميع الأطراف والتخلي عن الدوائر الصغيرة المرسومة على أسس أيديولوجية وبناء نظام حوكمة عالمي متعدد الأطراف وشفاف وديمقراطي وحماية الأمن السيبراني لجميع البلدان بشكل مشترك.

ثالثًا، يجب علينا أن نلتزم بالتعاون الثنائي والمتعدد الأطراف لمكافحة الجريمة الإلكترونية والإرهاب الإلكتروني. وينبغي لنا أن نكافح على نحو شامل جميع سلاسل الأعمال غير المشروعة في ذلك الصدد، وأن نزيد من تحسين آليات إنفاذ القانون والمساعدة القضائية في جميع البلدان. وفي ذلك الصدد، ترحب الصين بالاتفاق الذي توصلت إليه الأمم المتحدة في آب/أغسطس لاعتماد اتفاقية مكافحة الجرائم الإلكترونية.

رابعاً، يجب علينا أن نزيد من المساعدة للبلدان النامية لبناء القدرات اللازمة للحفاظ على الأمن السيبراني. ويجب علينا أن نشارك بنشاط في التعاون الدولي في مجالات مثل تنمية المواهب والابتكار التكنولوجي والإنذار المبكر والوقاية والاستجابة لحالات الطوارئ؛ ودعم الحلقات الضعيفة في الأمن السيبراني العالمي؛ وألا نترك أحدا يتخلف عن الركب؛ وألا نسمح لأي جزء من الفضاء الإلكتروني بأن يصبح فضاءً خارجا عن القانون.

إن الفضاء الإلكتروني يؤثر على السلام والأمن ومعيشة الناس ورفاههم. وتقف الصين على أهبة الاستعداد للعمل مع المجتمع الدولي لاستكشاف الاستجابات المشتركة لتهديدات وتحديات الأمن السيبراني وبذل جهود دؤوبة لدعم الازدهار والاستقرار في الفضاء السيبراني العالمي وبناء مجتمع ذي مستقبل مشترك في الفضاء السيبراني.

السيد أفونسو (موزامبيق) (*تكلم بالإنكليزية*): تشيد موزامبيق برئاسة المملكة المتحدة على توجيه انتباه مجلس الأمن إلى هذا الموضوع الهام حسن التوقيت. ونحن ممتنون لمقدمي إحاطتي اليوم، وهما الدكتور تيدروس أدهانوم غيبريسوس، المدير العام لمنظمة الصحة العالمية، والسيد إدواردو كونرادو، رئيس أسينشن، على إحاطتيهما الهامتين والمتبصرتين.

برزت برمجيات انتزاع الفدية كأداة مفضلة لمجرمي الإنترنت والشبكات الإرهابية. إنه نشاط إجرامي له عواقب وخيمة بشكل خاص على البلدان التي تفتقر إلى موارد الأمن السيبراني المتقدمة. وكما سمعنا من مقدمي الإحاطتين، فإن قطاع الرعاية الصحية معرض بشكل خاص لتلك الهجمات، خاصة في البلدان النامية، حيث يتزايد الاعتماد على الأنظمة الرقمية للخدمات الأساسية مثل السجلات الصحية الإلكترونية والتشخيص ولكن غالباً ما يكون ذلك من دون اتخاذ التدابير الأمنية اللازمة. وفي بلداننا، يمكن أن تكون اضطرابات كالتي سمعنا عنها اليوم كارثية، لا تهدد سلامة المرضى فحسب، بل تهدد حياة البشر كذلك. والتأثير على الدول التي لديها موارد أقل لتستجيب أكبر أضعافاً مضاعفة. وفي البلدان النامية، تمثل برمجيات انتزاع الفدية خطراً واضحًا وقائمًا على أمننا الوطني وعلى استقرار الخدمات العامة الأساسية والمرونة الاقتصادية وثقة الجمهور في الحوكمة. علاوة على ذلك، تؤدي الهجمات العابرة للحدود إلى تفاقم التوترات الجيوسياسية، معرضة البلدان النامية للخطر. ويمكن أن تتسبب تلك الهجمات في أضرار جانبية في النزاعات السيبرانية الأوسع نطاقاً.

وتعمل التقنيات الناشئة مثل الذكاء الاصطناعي والحوسبة الكمية على تضخيم ذلك التهديد. وهي تزيد من حدة الصعوبات على الدول ذات القدرات المحدودة على الحصول على قدرات الدفاع السيبراني المتقدمة، وتدفع العالم نحو سباق تسلح رقمي. وفي ذلك الصدد، تواجه الدول النامية مثل موزمبيق نقاط ضعف خاصة. ويرجع ذلك إلى محدودية البنية التحتية للأمن السيبراني، والأطر التنظيمية المتخلفة وضعف إمكانية الحصول على التدريب الأمني الرقمي عالي الجودة. وعندما تتسبب هجمات برمجيات انتزاع الفدية في تعطيل قطاعات حيوية مثل الرعاية الصحية، يتطلب التعافي موارد مالية كبيرة لتدخل الخبراء وتحديثات النظام، وفي بعض الأحيان دفع الفدية. وبالنسبة للبلدان التي تعاني بالفعل من ميزانيات مقيدة، تمثل هذه المطالب تحدياً شبه مستحيل.

لهذه الأسباب، نعتقد أن التصدي لبرمجيات انتزاع الفدية في البلدان النامية يتطلب استراتيجية شاملة ومصممة خصيصاً لها. ويجب أن يركز هذا النهج على الوقاية في المقام الأول. ويجب أن يشمل أيضاً التأهب والاستجابة، بما في ذلك تدريب موظفي تكنولوجيا المعلومات وتحديث الأنظمة القديمة ووضع سياسات تنظيمية صارمة وإنشاء الشراكات. ومن الضروري اتخاذ تدابير وقائية – مثل التحديثات المنتظمة للبرامج، وتجزئة الشبكة، وهندسة الثقة الصفرية، وتدريب الموظفين على الوعي بالتصيد الإلكتروني – ولكنها غالباً ما تتطلب دعماً لبناء القدرات.

وإذ تدرك موزامبيق الأثر السلبي لبرمجيات انتزاع الفدية على اقتصادات البلدان، فهي تعمل على وضع إطار تنظيمي لمعالجة هذه المشكلة والجرائم السيبرانية بشكل عام. وكجزء من تلك الإجراءات، يمكننا تسليط الضوء على صياغة قانون الجرائم السيبرانية، وعلى قانون لحماية البيانات وقانون للأمن السيبراني. وبالإضافة إلى الجوانب التشريعية، تعمل موزامبيق على تنفيذ آليات لتعزيز الأمن السيبراني والقدرة على الصمود، مع التركيز على التوعية والتدريب على مختلف المستويات.

وعلى الصعيد العالمي، ندعو إلى التركيز على وضع معايير موحدة للأمن السيبراني وتعزيز إنفاذها. ويجب ألا تصبح أي دولة ملاذاً آمناً لمرتكبي الجرائم السيبرانية. والأهم من ذلك أننا نعتبر أن هناك حاجة ماسة إلى إطار قانوني عالمي قوي ينبغي أن يتماشى تماماً مع مقاصد ومبادئ ميثاق الأمم المتحدة.

ونأمل أن يمثل حوار اليوم خطوة نحو تعزيز التعاون الدولي والعمل الدبلوماسي لردع التهديدات السيبرانية والتصدي لها. وتعزيز تلك الجهود أمر بالغ الأهمية لحماية السلام والأمن العالميين وضمان عدم تخلف أي دولة عن الركب وحماية جميع الدول في هذا العصر الرقمي. وكما هو الحال في الحالات الأخرى التي تشكل تهديداً للسلام والأمن الدوليين، يجب علينا أيضاً أن نوحد جهودنا لجعل الفضاء السيبراني آمناً وقادراً على الصمود.

السيد هاوري (سويسرا) (*تكلم بالفرنسية*): أود أن أشكر السيد تيدروس غيبريسوس، المدير العام لمنظمة الصحة العالمية، والسيد كونرادو على إسهاماتهما المفصلة.

ترحب سويسرا بتركيز مجلس الأمن المتجدد على مسألة الأمن السيبراني المهمة. فالتهديدات في الفضاء السيبراني، لا سيما تلك الصادرة عن جهات حكومية أو التي تتغاضى عنها الدول، يمكن أن تهدد السلام والأمن الدوليين، على النحو المعترف به في ميثاق المستقبل (قرار الجمعية العامة 1/79).

ولا يمكن إنكار الفرص العديدة التي تتيحها التطورات في مجال تكنولوجيا المعلومات والاتصالات. كما أن من المعروف جيداً تنوع الأخطار والجهات الحكومية وغير الحكومية التي تستغل نقاط ضعف النظم لتنفيذ هجمات سيبرانية خبيثة. ومن بين هذه الهجمات، تُعد هجمات برمجيات انتزاع الفدية التي تستهدف أنظمة الرعاية الصحية اتجاهاً مقلقاً للغاية ما فتئ يتزايد على مستوى العالم منذ عام 2020.

وتتيح رقمنة أنظمة الرعاية الصحية إحراز تقدم كبير لصالح السكان، لكن بنيتها التحتية السيبرانية تزداد تعقيداً، وتزداد بالتالي تكلفة تأمينها. وتزيد ضرورة استمرار التشغيل في جميع الأوقات من الضغط على مقدمي الرعاية الصحية أنفسهم، وكذلك على الهيئات العامة. وبالتالي فإن هذه الهجمات هي طريقة غادرة بشكل خاص لاستهداف البنية التحتية الحيوية لأي دولة ولسيادتها.

وتثير التقارير الأخيرة عن التعاون بين مجموعة ترعاها جمهورية كوريا الشعبية الديمقراطية وشبكة "بلاي" لبرمجيات انتزاع الفدية مخاوف أمنية خطيرة، حيث يمكن أن يؤدي ذلك إلى زيادة انتشار الهجمات وزيادة ضررها على نطاق العالم.

وأود أن أسلط الضوء على ثلاثة جوانب.

أولاً، نؤكد مجدداً أن القانون الدولي، بما في ذلك ميثاق الأمم المتحدة والاتفاقيات الدولية المتعلقة بحقوق الإنسان والقانون الدولي الإنساني، في حالة النزاع المسلح، ينطبق أيضاً ويجب احترامه في الفضاء السيبراني.

وعلى وجه التحديد، فإن مبدأ العناية الواجبة، الذي تطور على مدى فترة طويلة من الزمن، والذي يشكل من وجهة نظر سويسرا جزءاً من القانون الدولي العرفي، يدعو جميع الدول لئلا تسمح عن علم باستخدام أراضيها لارتكاب أفعال تتعارض مع حقوق الدول الأخرى. وهذا ينطبق على العالم المادي وعلى الفضاء السيبراني على السواء. والدول مدعوة إلى بذل العناية الواجبة لمنع الجماعات الإجرامية من استخدام بنيتها التحتية لتكنولوجيا المعلومات والاتصالات، وللتعاون على الصعيدين الوطني والدولي لعرقلة أنشطة هذه الجماعات. كما أن إطار سلوك الدول المسؤول في الفضاء السيبراني، الذي اعتُمد بتوافق الآراء، يعترف بهذا المبدأ. وتتطلب هذه المعايير أيضاً من الدول عدم إجراء أو دعم العمليات السيبرانية ضد البنى التحتية الحيوية، مثل الخدمات الصحية، عن علم.

ثانياً، من المهم قمع الجماعات الإجرامية الناشطة في الفضاء السيبراني. وقد كان لإجراءات الشرطة الأخيرة تأثير كبير على تلك الجماعات، ولكن قمعها وحده لن يقضي على هذه الظاهرة. فيجب أن تتخذ الدول الإجراءات والتدابير المناسبة لمنع الهجمات على بنيتها التحتية الحيوية. ونولي أهمية خاصة لتعزيز أمن قطاع الرعاية الصحية وقدرته على الصمود في مجال الأمن السيبراني.

ثالثاً، في هذا السياق العابر للحدود في معظم الأحيان، لا يمكننا أن ننجح إن لم نعمل معاً. ويجب تشجيع التعاون الدولي وبناء القدرات بين جميع الدول لزيادة أمن النظام الإيكولوجي السيبراني العالمي وقدرته على الصمود. وتُعد المبادرة الدولية لمكافحة برمجيات انتزاع الفدية، وسويسرا عضو فيها، منتدىً مهماً في هذا الصدد. ويجب على الدول أيضاً أن تمتثل على نحو أكمل لالتزاماتها الدولية فيما يتعلق بطلبات المساعدة القانونية المتبادلة، بحيث يمكن اتخاذ الإجراءات الجنائية أينما حُددت هوية الجاني.

وعلى الصعيد المتعدد الأطراف، أود أن أشدد على أهمية الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي. وسيكون من المهم أن يتمكن الفريق في العام المقبل من التوصية بإنشاء آلية واحدة داخل الجمعية العامة لمواصلة عمله، بالبناء على الإنجازات التي تحققت في السنوات الأخيرة.

وقد كان موضوع المؤتمر الدولي الرابع والثلاثين للصليب الأحمر والهلال الأحمر "اجتياز حالة عدم اليقين وتعزيز الإنسانية". وأكد أحد القرارات المعتمدة في إطار هذا الموضوع على أهمية القانون الدولي الإنساني في حماية السكان المدنيين والممتلكات المدنية في سياق النزاع المسلح في العالم الرقمي.

ولمجلس الأمن أيضاً دور ليؤديه. فعليه أن يعزز احترام القانون الدولي وتنفيذ إطار السلوك المسؤول للدول في الفضاء السيبراني حتى يتسنى لشعوبنا الاستفادة من الفرص الهائلة التي يتيحها الفضاء السيبراني، لا سيما في مجال الصحة.

السيد كودري (الجزائر): في البداية، أود أن أشكر الدكتور تيدروس غيبريسوس على إحاطته القيمة. كما استمعت بعناية إلى السيد كونرادو.

إن تزايد هجمات برمجيات الفدية ضد المرافق الطبية يتفاقم بسبب الظهور السريع والتطور الهائل لبرامج القرصنة الإلكترونية والذكاء الاصطناعي. كما تتضاعف المخاطر بسبب غياب المعايير التنظيمية الدولية في هذا المجال.

إن التتويج الناجح مؤخرا لاتفاقية الأمم المتحدة لمكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، والذي تشرفت الجزائر بقيادة مفاوضاته يظهر ما يمكننا تحقيقه من خلال التعاون المتعدد للأطراف الحقيقي، لما يكون في إطاره الصحيح.

أود الإشارة بداية إلى مبدأين رئيسيين في بالغ الأهمية.

أولا النهج الحالي للأمن السيبراني بما في ذلك الأمن السيبراني للرعاية الصحية لا يزال يديم تكريس عدم المساواة العالمية ويفاقم نقاط الضعف تجاه التهديدات المعززة بالذكاء الاصطناعي.

ثانيا، يجب أن تنبثق الحلول من مسارات متعددة الأطراف شاملة وتحترم سيادة جميع الدول والمساواة في السيادة بينها.

بناء على ما سبق، أضحى من الواجب مواجهة خمسة تحديات أساسية.

أولا، تحدي الهيمنة التكنولوجية، حيث تحتكر الدول المتقدمة والشركات الخاصة وحتى الأفراد قدرات الأمن السيبراني وتقنيات الذكاء الاصطناعي، تاركة نظم الرعاية الصحية في الدول النامية عرضة للخطر.

ثانيا، تحدي العمل الأحادي، حيث إن الهيمنة على الفضاء الإلكتروني وتطوير الذكاء الاصطناعي من خلال الحواجز التكنولوجية تقوض التعاون الدولي.

ثالثا، تحدي التفاوت في الموارد، حيث تكافح الدول النامية لحماية بنيتها التحتية للرعاية الصحية، بسبب محدودية الوصول إلى التكنولوجيا والخبرات.

رابعا، تحدي عدم اليقين بشأن الذكاء الاصطناعي، حيث يمكن إساءة استخدام أدوات الذكاء الاصطناعي رغم ما تقدمه من إمكانات هائلة للتنمية والدفاع والأمن لتعزيز تطور وحجم الهجمات، بما في ذلك ضد المرافق الصحية عوض حمايتها.

خامسا، تحدي تداخل التهديدات، حيث لا تشكل هجمات برمجيات الفدية المخاطر الوحيدة على البيانات الشخصية. فالمتاجرة الغامضة والمعقدة للبيانات تمثل تهديدا مماثلا للبيانات الشخصية والحق في حماية خصوصية الأفراد.

هذه الأنماط من الهيمنة وعدم الشمول والتفاوت وعدم اليقين والفوضى بشأن الذكاء الاصطناعي تعتبر مترابطة ومتداخلة.

في هذا السياق، نود التأكيد على ثلاثة تدابير ملموسة.

أولا إنشاء آليات دولية لنقل التكنولوجيا وبناء القدرات، لضمان الوصول الشامل والعادل إلى حلول الأمن السيبراني للمرافق المدنية.

ثانيا تطوير بروتوكولات موحدة، لكن قابلة للتكيف، للأمن السيبراني تناسب الدول في مراحل التنمية المختلفة مع الإقرار بأن الحلول الأحادية المقاس غير فعالة.

ثالثا، إيجاد وتوفير حلول أمنية ميسورة التكلفة مصممة خصيصا لتلبية احتياجات نظم الرعاية الصحية في الدول النامية. كما يجب

على المجتمع الدولي أن يعطي الأولوية لوضع الأخلاقيات كأولوية في تطوير الذكاء الاصطناعي.

علاوة على ذلك، يجب أن نلتزم بالسلامة والقابلية للتحكم. حيث إن هناك العديد من أوجه عدم اليقين في تطوير وتطبيق التقنيات المتعلقة بالذكاء الاصطناعي؛ لذا، فالسلامة هي الخط الأحمر الذي يجب عدم تجاوزه. كما يحتاج المجتمع الدولي إلى تعزيز الوعي بالمخاطر وإنشاء آليات فعالة للإنذار والاستجابة للمخاطر، وضمان عدم حدوث مخاطر خارجة عن السيطرة البشرية.

ونود أن نؤكد أنه يجب أن تكون انشغالات دول الجنوب محورية لا هامشية في أطر الأمن السيبراني والذكاء الاصطناعي الدولية. ولا يتعلق الأمر بالعدالة فحسب؛ بل بالفعالية أيضا. حيث غالبا ما تواجه الدول النامية تحديات فريدة في مجال الأمن السيبراني في نظمها الصحية مما يتطلب حلولا مخصصة لا معايير مفروضة.

في الختام، يتطلب المضي قدما في هذا المجال إجراءات فورية من جهة وطويلة الأجل من جهة أخرى، من خلال عمليات متعددة الأطراف شاملة، كما أبرز نجاح الاتفاقية المتعلقة بالجريمة السيبرانية ما يمكننا تحقيقه عندما نعمل معا وعلى قدم المساواة.

ينبغي أن يتجه العالم نحو مزيد من المساواة التكنولوجية والقدرات المشتركة ومزيد من التعاون المتعدد الأطراف والحد من العمل الأحادي وتقليل الحلول المفروضة ومزيد من النهج الشاملة، ونحو تطوير للذكاء الاصطناعي يخدم البشرية بدلا من تعريضها للخطر.

إن سلامة نظمنا الصحية ليست امتيازا للدول الغنية. إنه حق أساسي يجب حمايته وتوفيره لجميع الشعوب في جميع الدول. علينا أن نعمل معا لضمان ألا يصبح التقدم التكنولوجي في مجال الأمن السيبراني للرعاية الصحية والذكاء الاصطناعي عاملا إضافيا في توسيع هوة عدم المساواة على الصعيد العالمي.

السيد كانو (سيراليون) (*تكلم بالإنكليزية*): أشكر الدكتور تيدروس غيبريسوس، المدير العام لمنظمة الصحة العالمية، على إحاطته المفيدة، والسيد إدواردو كونرادو، رئيس منظمة أسينشن، على المعلومات التي قدمها.

ما فتئت سيراليون تعطي الأولوية للتصدي للتهديدات الجديدة والناشئة للسلام والأمن الدوليين خلال فترة عضويتها في مجلس الأمن. لذلك نرحب بهذه الفرصة لتناول هذه القضية المهمة المتعلقة بالتهديد المتزايد لهجمات برمجيات انتزاع الفدية ضد المستشفيات ومرافق وخدمات الرعاية الصحية، والتي تنطوي على إمكانية تقويض الحق الأساسي في الصحة وتهدد مكافحة أزمات الصحة العامة على مستوى العالم.

وتدرك سيراليون أن الهجمات السيبرانية، بما في ذلك هجمات برمجيات انتزاع الفدية، تشكل تحديًا متزايدا للسلام والأمن الدوليين، لا سيما عندما تستهدف بنية تحتية حيوية، مثل نظم الرعاية الصحية. ولا تسبب هذه الهجمات اضطرابا واسع النطاق فحسب، بل وتعرض حياة الناس للخطر، وتؤثر على الفئات الأضعف، لا سيما في مناطق النزاعات، وفي الأماكن التي تعاني من نقص الموارد، وأثناء حالات الطوارئ الصحية، مثل الجائحات.

وسواء كان الهدف منها تحقيق مكاسب مالية و/أو إحداث اضطراب اجتماعي وسياسي، فإن الهجمات السيبرانية على نظم الرعاية الصحية، وخاصةً برمجيات انتزاع الفدية، ذات طابع انتهازي في استغلال اعتمادنا على التدخلات الصحية الرقمية، بما في ذلك نظم التطبيب عن بُعد المتصلة بالإنترنت، ونظم الصحة الإلكترونية، ومنصات التواصل الافتراضية، ولوحات المتابعة الإدارية للنظم الصحية، خاصةً منذ جائحة فيروس كورونا، التي أدت إلى زيادة الطلب على نظم الرعاية الصحية. كما أنها تعيق زيادة فرص الوصول إلى الرعاية الصحية والنظم الصحية. ورغم أن الاعتماد على نظم الرعاية الصحية المتصلة بالإنترنت والقائمة على الحاسوب يزيد كثيرا من كفاءة إدارة الرعاية الصحية وفعاليتها، فإنه يزيد أيضا من التعرض للهجمات الإلكترونية على أيدي التنظيمات الإجرامية. فهذه التنظيمات تستغل هذه المرافق وتستفيد منها، وهي مرافق تقدم خدمات منقذة للحياة ولكنها تخزن أيضا كميات كبيرة من البيانات الحساسة والشخصية.

وبينما تزايدت إعلانات المسؤولية عن هجمات برمجيات انتزاع الفدية في جميع أنحاء العالم في جميع القطاعات، تشير تقارير منظمة الصحة العالمية والإنتربول وأجهزة المخابرات في بعض الدول الأعضاء

إلى أن الهجمات على قطاع الرعاية الصحية خبيثة بصفة خاصة. وقد أُبلغ عن عدة هجمات إلكترونية ضد قطاع الرعاية الصحية في النصف الأول من عام 2024. ويشير "تقرير الإنتربول عن تقييم التهديدات السيبرية في أفريقيا لعام 2024" إلى أن ما يقرب من نصف البلدان الأفريقية التي شملها الاستطلاع أبلغت عن هجمات ببرمجيات انتزاع الفدية ضد بنيتها التحتية الحيوية، بما في ذلك المستشفيات. ويُضاف إلى ذلك تقارير عدة بلدان في السنوات الأخيرة عن تعرضها لهجمات على بنيتها التحتية للرعاية الصحية، أدت إلى فقدان بيانات المرضى وتعطيل الخدمات الصحية الأساسية، بل إلى حدوث وفيات. وليست هذه الهجمات ذات طابع إجرامي فحسب، بل إنها تمثل أيضا خطرا واضحا وقائما يهدد الصحة العامة ويرتبط ذلك ارتباطا وثيقا بالسلام والأمن الدوليين.

وتمشيا مع جهود الاتحاد الأفريقي والجهود الإقليمية، تؤيد سيراليون بقوة ضرورة اتباع نهج دولي منسق لمكافحة الجريمة الإلكترونية وتعزيز قدرة نظمنا الصحية على الصمود. وتشدد اتفاقية الاتحاد الأفريقي لعام 2020 بشأن الأمن السيبراني وحماية البيانات الشخصية على ضرورة التعاون وبناء القدرات وتبادل المعارف بين الدول الأعضاء لمنع التهديدات السيبرانية والتصدي لها. وتلتزم سيراليون بتحقيق الاتساق مع هذا الإطار والعمل مع الاتحاد الأفريقي وعموم المجتمع الدولي لتعزيز قدرات الدول الأفريقية في مجال الأمن السيبراني.

ويجب أيضا أن نعترف بأهمية التعاون المتعدد الأطراف في مواجهة هذه التحديات. وعلى الأمم المتحدة، عن طريق هيئاتها المختلفة، بما في ذلك مكتب مكافحة الإرهاب والاتحاد الدولي للاتصالات، أن تضطلع بدور أساسي في توفير منبر للتعاون وتيسير المساعدة التقنية وتعزيز وضع معايير دولية لسلوك الدول المسؤول في الفضاء الإلكتروني. ويجب النظر إلى الدعوة الأخيرة في التعاهد الرقمي العالمي (انظر قرار الجمعية العامة 1/79) لضمان مستقبل رقمي آمن ومستدام وشامل للجميع باعتبارها فرصة بالغة الأهمية لتعزيز التعاون العالمي في مجال الأمن السيبراني. وتؤيد سيراليون المبادئ المنصوص عليها في التعاهد التي تشمل ضمان إمكانية الوصول إلى بنية تحتية رقمية آمنة وقادرة على الصمود وحماية الخدمات الحيوية وتشجيع الاستخدام المسؤول للتكنولوجيا من جانب جميع الجهات الفاعلة، بما فيها الجهات الخاصة وغير الحكومية، التي غالبا ما تؤدي دورا في هذه الهجمات.

وإذ نلاحظ تزايد مستويات الهجمات ببرمجيات انتزاع الفدية على عمليات الرعاية الصحية ومرافقها في جميع أنحاء العالم، نسلط الضوء على ثلاث نقاط رئيسية.

أولا، تدرك سيراليون، كما سبقت الإشارة، أن هجمات برمجيات انتزاع الفدية على المستشفيات وعمليات الرعاية الصحية الأخرى تشكل تهديدا للأمن الوطني والسلام والأمن والتنمية على الصعيد الدولي. فالحصول على الرعاية الصحية الجيدة حاجة أساسية للناس في جميع أنحاء العالم وتعرض الهجمات السيبرانية التي تعطل تقديم هذه الخدمات الصحة العامة للخطر، مما يعرض حياة الملايين من الناس وسبل عيشهم للخطر وقد يؤدي إلى تفاقم انعدام الأمن والنزاع. وترد روايات مروعة عن الفوضى التي سببتها هجمات برمجيات انتزاع الفدية في جميع أنحاء العالم في الماضي القريب، وقد سمعنا رواية السيد كونرادو.

وفي عالم أصبحت فيه معظم مرافق الرعاية الصحية من المستوى الثالث مرقمنة جزئيا أو كليا، يشكل فقدان هذه النظم تحديا كبيرا لتوفير رعاية فعالة للمرضى. وتزداد الآثار على الصحة والأمن العالميين عندما نأخذ في الاعتبار الهجمات على المؤسسات الصحية العالمية ومراكز البحوث الطبية التي تدعم خدمات الرعاية الصحية لنسبة كبيرة من سكان العالم والتي تجري بحوثا طبية باستخدام التكسينات البيولوجية أو العوامل المعدية والتي يمكن أن تستغلها المنظمات الإرهابية والإجرامية بسهولة.

ثانيا، إن الطابع العابر للحدود للهجمات السيبرانية، بما في ذلك هجمات برمجيات انتزاع الفدية، التي يظل مرتكبوها في الغالب مجهولي الاسم والهوية ولا يعرفون حدودا والذين ينتشر ضحاياها عبر الحدود الجغرافية، يتطلب التعاون والتنسيق على الصعيد الدولي. وعلى الصعيد الإقليمي، ندعو بإلحاح إلى دعم تنفيذ مبادرات الاتحاد الأفريقي في مجال الأمن السيبراني مع تعزيز نهج إقليمي لضمان حماية البنية التحتية الصحية في القارة من التهديدات الرقمية.

وبما أن مجرمي الفضاء الإلكتروني أصبحوا أكثر تنظيما وأصبحوا يستخدمون برمجيات خبيثة أكثر تطورا ويشنون هجمات محددة الأهداف على نحو أدق، مثل الهجمات على الأجهزة الطبية بدلا من الشبكات والنظم الطبية، فمن الضروري أن تجمع جهودنا لمكافحة هذا التهديد بين تدابير مناسبة وقابلة للتطبيق في المجالين التشريعي والاستخباراتي وفي مجال إنفاذ القانون. ويجب أن تكون الإجراءات القوية المتخذة على الصعيد الوطني مدعومة بمعاهدات وقوانين ولوائح عالمية لا تكتفي بوضع معايير للسلوك، بل يجب أن تكون مدعومة بعواقب حقيقية على المخالفين، وبالتالي ضمان التعامل مع تهديدات الأمن السيبراني التي تستهدف المستشفيات ومرافق الرعاية الصحية كمسألة خطيرة تتعلق بالسلام والأمن الدوليين، مع التركيز على العمل الجماعي والمساءلة والردع.

وتظل سيراليون، بصفتها عضوا في المبادرة الدولية لمكافحة برمجيات انتزاع الفدية، ملتزمة بتعزيز نظمنا الوطنية للتصدي للجريمة الإلكترونية من خلال تشريعات مثل قانون الأمن السيبراني والجريمة الذي أصدرناه في عام 2021. وباعتبارنا إحدى الدول الموقعة على اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية، نرحب بموافقة اللجنة المخصصة التي أنشأتها الجمعية العامة في آب/أغسطس الماضي على اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية التي أفاد مكتب الأمم المتحدة المعني بالمخدرات والجريمة، بأنها

”خطوة تاريخية باعتبارها أول معاهدة متعددة الأطراف لمكافحة الجريمة منذ أكثر من 20 عاما وأول اتفاقية للأمم المتحدة لمكافحة الجريمة السيبرانية في وقت تتزايد فيه التهديدات في الفضاء الإلكتروني بسرعة“.

ثالثا وأخيرا، ما فتئ مجلس الأمن في السنوات الأخيرة يؤدي دورا فعالا في دعم الدول والمؤسسات في وضع تدابير للتصدي لهذا التهديد، بما في ذلك تسليط الضوء عليه وزيادة قاعدة معارف المجتمع العالمي لاتخاذ قرارات مستنيرة. ومن الأهمية بمكان تبادل المعلومات بشأن التهديدات ومرتكبيها، إلى جانب وضع تدابير أمنية وقائية واستخدامها، بما في ذلك بالتعاون مع القطاع الخاص، حسب الاقتضاء، للدفاع عن الصحة والسلامة العامتين. ومن المهم أيضا أن يكفل المجلس الالتزام بالقواعد والمعايير والمبادئ الراسخة التي تنظم الاستخدام المسؤول للفضاء الإلكتروني.

ونظرا لوجود فجوات كبيرة بين البلدان في تسخير القدرات المالية واللوجستية والبشرية اللازمة للتصدي للهجمات الإلكترونية كما ينبغي، يجب أن تشمل الآليات التعاونية العالمية والإقليمية تعزيز التعاون في مجال بناء القدرات، بما في ذلك تبادل التكنولوجيا والخبرات، لا سيما بالنسبة للبلدان الصغيرة والنامية، من أجل تعميق فهمها لهذه التهديدات وتنفيذ تدابير لمواجهتها.

في الختام، تعتقد سيراليون اعتقادا راسخا أن استجابة المجلس بصورة قوية وموحدة للتهديد الذي تشكله الهجمات ببرمجيات انتزاع الفدية على المستشفيات وعمليات الرعاية الصحية ومرافقها ذات أهمية أساسية في إرساء فضاء إلكتروني يسوده السلام والأمن. ونؤكد من جديد دعمنا للمبادرات المتخذة في هذا الصدد، وذلك في إطار المعايير والمبادئ الراسخة لسلوك الدول المسؤول وحقوق الإنسان والمبادئ الأساسية لميثاق الأمم المتحدة.

السيدة بيرسود (غيانا) (*تكلمت بالإنكليزية*): أشكر المدير العام لمنظمة الصحة العالمية غيبريسوس والسيد كونرادو على إحاطتيهما.

تكشف الإحصاءات الأخيرة عن زيادات مذهلة في تواتر هجمات برمجيات انتزاع الفدية وحجمها في جميع أنحاء العالم. وللهجمات على البنية التحتية الحيوية، لا سيما المستشفيات ومرافق الرعاية الصحية، تداعيات خطيرة على الصحة العامة والأمن الوطني. وتتزايد مخاطر هذه الهجمات بتزايد استخدام التحول الرقمي في المزيد من النظم الصحية على صعيد العالم لتعزيز جودة الرعاية السريرية وكفاءة خدماتها من حيث التكلفة.

وفي ظل ازدياد إمكانية الحصول على برمجيات انتزاع الفدية واتساع نطاق الجهات الفاعلة المهدِّدة في جميع أنحاء العالم، نشهد زيادة في حجم الهجمات بهذه البرمجيات ضد المؤسسات الطبية، مما يؤثر سلبا على عملياتها وتقديم خدمات الرعاية الصحية، إضافة إلى ما يترتب عليها من سرقة البيانات السرية. وإلى جانب تعطيل تقديم

الخدمات الصحية والآثار المالية المترتبة على تعطلها، تؤدي الهجمات ببرمجيات انتزاع الفدية في بعض الحالات إلى خسائر في الأرواح عندما تتسبب في عرقلة تقديم العلاج الطبي العاجل.

وبالنظر إلى آثارها المدمرة المحتملة على استقرار نظم الرعاية الصحية الوطنية، يجب إعطاء الأولوية لإنشاء أطر متينة لمواجهة هذه الهجمات. ويجب على الدول أن تتصرف بشكل أكثر إلحاحا لاعتماد نهج استباقي وكلي لمواجهة هذه الهجمات، مع الاعتراف بأنها تتجاوز الحدود وأنه ما من بلد في مأمن منها. وفي هذا السياق، أسلط الضوء على النقاط التالية.

أولاً، يجب على الدول أن تستثمر في مبادرات بناء القدرات وأن تضع خطط استجابة للحوادث. إن العديد من البلدان النامية يفتقر إلى الموارد والخبرات اللازمة لحماية نفسه من التهديدات السيبرانية، مثل هجمات برمجيات انتزاع الفدية، ومكافحتها. ولذلك، فإن بناء القدرات في تلك البلدان أمر حاسم. وينبغي أن يشمل ذلك المساعدة التقنية والدعم التمويلي والتدريب لتعزيز قدرة الدول المعرضة للخطر على الاستجابة، بسبل منها وضع خطط استجابة للحوادث للتعامل بفعالية مع تلك الهجمات.

ثانياً، نظراً لتزايد حجم هجمات برمجيات انتزاع الفدية وعواقبها، تؤكد غيانا على ضرورة تعزيز التعاون بين الدول وفيما بينها من خلال تبادل المعارف بشأن أفضل الممارسات والتحديات، وتبادل المعلومات ونقل التكنولوجيا. وفي هذا الصدد، من الأهمية بمكان إنشاء نظام دولي لتبادل المعلومات يوفر المعلومات للبلدان حول كيفية تعزيز بنيتها التحتية الصحية الحيوية وحمايتها من التعرض لهجمات برمجيات انتزاع الفدية، بحيث يمكن اكتشافها والتصدي لها في الوقت المناسب. وبالإضافة إلى ذلك، يجب وضع إطار عمل عالمي يتيح هذا النوع من تبادل المعلومات الاستخباراتية فيما بين الدول وأصحاب المصلحة المعنيين بشأن التهديدات السيبرانية المحتملة.

ثالثاً، يجب محاسبة مرتكبي هجمات برمجيات انتزاع الفدية. ويجب إعطاء الأولوية للتعاون والشراكات للتحقيق في الجرائم السيبرانية وملاحقة مرتكبيها قضائياً، بما في ذلك هجمات برمجيات انتزاع الفدية في جميع البلدان والمناطق. ويجب أن يشمل ذلك تفكيك شبكات برمجيات انتزاع الفدية ومراقبة المعاملات التي يُشتبه في أنها مدفوعات لهذه البرمجيات. وتسهم اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية التي اعتُمدت مؤخراً في هذا الجهد من خلال توفير أطر تنظيمية وتعاونية للتصدي لهذه الجرائم. وبالإضافة إلى ذلك، تدرك غيانا أن القانون الدولي ينطبق على الفضاء السيبراني.

ويجب التعامل مع المستشفيات ومرافق الرعاية الصحية وخدماتها على أنها مقدسة، ويجب بذل كل الجهود الممكنة لحمايتها من هجمات برمجيات انتزاع الفدية. وعلى المجتمع الدولي توحيد الجهود لمنع جميع أشكال الهجمات السيبرانية على البنى التحتية الوطنية الحيوية. ولا تزال غيانا ملتزمة بالمبادرات العالمية التي تسعى إلى زيادة الوعي بهذا التهديد والتصدي له وضمان عدم تقويضه للسلام والأمن الدوليين.

السيد مونتالفو سوسا (إكوادور) (*تكلم بالإسبانية*): أود أن أشكر المدير العام لمنظمة الصحة العالمية، الدكتور تيدروس أدهانوم غيبريسوس، على إحاطته الهامة. ويود وفد بلدي أن يشكر أيضاً السيد إدواردو كونرادو، وقد استمعنا بعناية شديدة لإحاطته.

إن هجمات برمجيات انتزاع الفدية ضد القطاع الصحي لا تعرض سلامة النظم الصحية للخطر فحسب، بل تهدد حياة البشر أيضاً. وتؤثر تلك الهجمات على الصحة العامة، بتعطيل الخدمات الحيوية والحد من الوصول إلى الخدمات الطبية الأساسية، وتشكل بالتالي تهديداً للسلام والأمن الدوليين. ويبرز التقرير المرحلي السنوي الثالث للفريق العامل المفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات وأمن استخدامها، المؤرخ تموز/يوليه 2024، قلق الدول المتزايد إزاء وتيرة ونطاق وشدة هذه الهجمات، التي تتزايد. وكما ذكر وفد بلدي خلال المناقشة المفتوحة التي عقدت في حزيران/يونيه الماضي بمبادرة من جمهورية كوريا (انظر S/PV.9662)، يجب على مجلس الأمن ألا يتخلف عن الركب فيما يتعلق بتطور التهديدات السيبرانية.

وكما قلنا في عدة مناسبات، تعتبر إكوادور أن الوقاية هي حجر الزاوية في بناء السلام. وفي هذا السياق، ينبغي لمجلس الأمن أن يدرج

بين نواتجه بناء القدرات في مجال تسخير التكنولوجيا، واستراتيجيات مكافحة الاستخدام الخبيث لها، بما يكمل الجهود العالمية.

فإذا لم تكن دولة عضو واحدة آمنة، لن تكون أي دولة عضو أخرى آمنة. فالتهديدات التي نواجهها اليوم بطبيعتها عابرة للحدود إلى حد كبير، والطريقة الوحيدة لمواجهتها، سواء في المجال المادي أو في الفضاء السيبراني، هي من خلال التعاون الدولي. إن الأمن السيبراني تحدٍ عالمي يتطلب استجابة شاملة ومنسقة وتعاونية من المجتمع الدولي بأسره. ولذلك، يؤيد وفدي أي آلية تشجع على زيادة التعاون الدولي للحد من أوجه عدم التماثل في القدرة على تنفيذ قواعد السلوك المسؤول للدول، وكذلك اعتماد تدابير تعزز قدرة الدول على حماية بنيتها التحتية الحيوية. ويتعين تعزيز المعايير الحالية لمراعاة التطورات التكنولوجية السريعة.

وتؤكد إكوادور من جديد التزامها بفضاء سيبراني آمن ومفتوح وسلمي، يمكن للتكنولوجيا فيه أن تشكل أداة للتنمية. ويقع على عاتق جميع الدول التزام بتعزيز التعددية من أجل بناء بيئة رقمية تحترم كرامة الإنسان، من خلال تعزيز السلام والأمن الدوليين. وينطبق القانون الدولي والقانون الدولي الإنساني على الفضاء السيبراني.

وأختتم بالتذكير بضرورة الحفاظ على الاستخدام المسؤول لتكنولوجيا المعلومات والاتصالات وتعزيزه باعتباره أمراً أساسياً لكفالة الاستقرار والأمن في الفضاء السيبراني.

الرئيس (*تكلم بالإنكليزية*): أدلي الآن ببيان بصفتي ممثل المملكة المتحدة.

أود أن أشكر الدكتور غيبريسوس والسيد كونرادو على الإحاطتين اللتين قدماهما إلينا اليوم.

في وقت سابق من هذا العام في الفريق العامل المفتوح باب العضوية التابع للجمعية العامة المعني بأمن تكنولوجيا المعلومات والاتصالات وأمن استخدامها، أقرت جميع الدول بأن هجمات برمجيات انتزاع الفدية قد يكون لها تأثير على السلام والأمن الدوليين. وقد دأبت الجهات الفاعلة في مجال برمجيات انتزاع الفدية على مهاجمة البنى التحتية الوطنية الحيوية والحكومات المحلية والمستشفيات لتحقيق مكاسب مالية شخصية. وتوجد معظم الجماعات في ولايات قضائية تسمح لها بالعمل بدون عقاب. وندعو تلك الدول إلى بذل المزيد من الجهود للتصدي للجماعات الإجرامية الموجودة في أراضيها أو التي تستخدمها.

والمملكة المتحدة، كما هو الحال بالنسبة للكثيرين هنا اليوم، لا تزال ضحية لحوادث برمجيات انتزاع الفدية. فقد تأثرت خدماتنا الصحية الوطنية بسلالة برنامج انتزاع الفدية "واناكراي" في عام 2017، والذي بلغت تكلفة التعافي منه 118 مليون دولار. وكان من الممكن إنفاق هذه الأموال على إنقاذ الأرواح. وهذا العام، تأثر أحد الموردين المهمين لمستشفيات لندن بواقعة اختراق ببرمجيات انتزاع الفدية أدت إلى تأجيل أكثر من 000 10 موعد طبي وأكثر من 700 1 إجراء طبي. ويتكرر هذا التعطل في جميع قطاعاتنا الحيوية. ولهذا السبب تعتبر المملكة المتحدة برمجيات انتزاع الفدية أحد أهم التهديدات السيبرانية للأمن القومي. وتعمل المملكة المتحدة، بهدف مكافحتها، على كسر نموذج عمل برمجيات انتزاع الفدية وتثني الضحايا عن الدفع للمجرمين. وقد أصدرت المملكة المتحدة، إلى جانب شركاء دوليين، 36 عقوبة ضد جهات فاعلة متورطة في هذه الأنواع من الأنشطة. غير أننا نحتاج إلى استجابة عالمية لهذا التهديد العالمي.

أولاً، نحث الآخرين على الانضمام إلى حكومة المملكة المتحدة في عدم دفع الفدية. ففي تشرين الأول/أكتوبر، وقّعت المملكة المتحدة و 49 عضواً آخر من أعضاء المبادرة الدولية لمكافحة برمجيات انتزاع الفدية على بيان عام يُلزم الحكومات بعدم دفع الفدية.

ثانياً، سيكون التنسيق أفضل وسائلنا الدفاعية. ففي الآونة الأخيرة، قادت أجهزة إنفاذ القانون في المملكة المتحدة تحالفاً من وكالات إنفاذ القانون العالمية لتعطيل مجموعة "لوك بيت" لبرمجيات انتزاع الفدية، وهي أكثر مجموعات هذه البرمجيات انتشاراً في عام 2024.

ثالثاً، يجب أن نزيد من قدرتنا على الصمود في وجه تلك الهجمات من خلال تبادل المعلومات لإلقاء الضوء على التهديدات وبناء فهمنا الجماعي. وسنواصل التعاون مع الشركاء الدوليين ومع

هذا القطاع لمكافحة برمجيات انتزاع الفدية وتفكيك منظومة مرتكبي الجرائم السيبرانية.

أستأنف مهامي بصفتي رئيس المجلس.

أعطي الكلمة الآن للسيد لامبرينيديس.

السيد لامبرينيديس (*تكلم بالإنكليزية*): يشرفني أن أتكلم بالنيابة عن الاتحاد الأوروبي والدول الأعضاء فيه. وتؤيد هذا البيان البلدان المرشحة للانضمام إلى الاتحاد وهي مقدونيا الشمالية والجبل الأسود وصربيا وألبانيا وأوكرانيا وجمهورية مولدوفا والبوسنة والهرسك وجورجيا.

عندما تصاب المستشفيات والمختبرات وخدمات الطوارئ بالشلل بسبب برمجيات انتزاع الفدية، فإن تأثير ذلك يتجاوز حدود الدولة، مما يعرّض حياة المرضى للخطر ويزعزع استقرار نظم الرعاية الصحية ويقوض الثقة في الخدمات العامة الأساسية. وتنفذ برمجيات انتزاع الفدية هجوماً كل 11 ثانية ويُتوقع أن يتصاعد هذا المعدل إلى هجوم كل ثانيتين بحلول عام 2031. ويتطلب الطابع العالمي لبرمجيات انتزاع الفدية وتأثيرها المحتمل على السلام والأمن الدوليين أن نستجيب جماعياً وبحسم لمنع الضرر في المستقبل.

ويتخذ الاتحاد الأوروبي إجراءات قوية لحماية البنية التحتية الحيوية والخدمات الأساسية، بما في ذلك الرعاية الصحية، في سبيل الوقاية من هذا التهديد. ونعمل على تعزيز دفاعاتنا وزيادة استجاباتنا وتقوية شراكاتنا الدولية للتصدي للكم المتزايد من برمجيات انتزاع الفدية. ويحدد الأمر التوجيهي للاتحاد الأوروبي المتعلق بأمن الشبكات والمعلومات الذي اعتُمد في كانون الأول/ديسمبر 2022 متطلبات إدارة مخاطر الأمن السيبراني والإبلاغ عن الحوادث للقطاعات الحيوية في جميع أنحاء الاتحاد الأوروبي ويعترف بالصحة باعتبارها "قطاعًا شديد الحساسية". وهو ما يكفل متطلبات الأمن السيبراني للمرافق الصحية. تهدف هذه الإجراءات إلى حماية الرعاية الصحية وتأمين البيانات الطبية الحساسة وضمان استمرار عمل الخدمات الأساسية على الرغم من الهجمات السيبرانية. وبعبارة أخرى، ندرك أن برمجيات انتزاع الفدية تمثل تهديدًا خطيراً ونؤكد مجددًا على الطابع الملح لهذه المسألة على جدول الأعمال السياسي للاتحاد الأوروبي.

لقد كثفنا أيضاً، بالإضافة إلى الوقاية، استجابتنا للأنشطة السيبرانية الخبيثة، وخاصة هجمات برمجيات انتزاع الفدية. وفي شهر حزيران/يونيه، فرض الاتحاد الأوروبي تدابير تقييدية على الأفراد المرتبطين بحملات برمجيات انتزاع الفدية. بالإضافة إلى ذلك، أطلق مركز الاتحاد الأوروبي لمكافحة الجريمة السيبرانية في شباط/فبراير، بالتعاون مع شركاء دوليين، عملية لتفكيك مجموعة "لوك بيت" لبرمجيات انتزاع الفدية التي تشكل أحد أكثر مشغلي برمجيات انتزاع الفدية انتشاراً على الصعيد العالمي. ونتخذ إجراءات باستخدام جميع الأدوات المتاحة لنا ضد أولئك الذين يتعمدون تعطيل الخدمات الحيوية. وندعو بقوة أيضاً جميع الدول، تمشياً مع إطار الأمم المتحدة لسلوك الدول المسؤول في الفضاء السيبراني، إلى عدم السماح باستخدام أراضيها لهذه الأنشطة الخبيثة والاستجابة للطلبات المناسبة للتخفيف من حدة هذه الأنشطة.

أخيراً، سنواصل تعزيز الشراكات للتصدي لتهديدات برمجيات انتزاع الفدية من خلال مبادرات الاتحاد الأوروبي لبناء القدرات مثل دعم تطوير استراتيجيات الأمن السيبراني الوطنية وتحسين إدارة الأزمات. إن إنشاء آلية دائمة للأمم المتحدة – برنامج عمل الأمم المتحدة السيبراني – سيسمح لنا بتعزيز قدرتنا الجماعية على مواجهة التهديدات التي تتعرض لها مجتمعاتنا واقتصاداتنا مثل برمجيات انتزاع الفدية. والاتحاد الأوروبي مستعد لمواصلة العمل مع المجتمع العالمي وكذلك القطاع الخاص لحماية البنية التحتية الحيوية، وخاصة الرعاية الصحية، من التهديدات السيبرانية. ويمكننا معاً، من خلال نهج عالمي موحد ومنسق، أن نكافح بفعالية التهديد المتصاعد لبرمجيات انتزاع الفدية.

رُفعت الجلسة الساعة 12/05.