

Distr.: General
22 January 2024
Arabic
Original: English

الجمعية العامة



الفريق العامل المفتوح العضوية المعني بأمن
تكنولوجيات المعلومات والاتصالات وأمن
استخدامها للفترة 2021-2025

الدورة الموضوعية السابعة
نيويورك، 4-8 آذار/مارس 2024

عملية مسح لاستعراض واقع برامج ومبادرات بناء القدرات داخل الأمم المتحدة
وخارجها وعلى الصعيدين العالمي والإقليمي

ورقة أعدتها الأمانة العامة

أولا - مقدمة

1 - في الفقرة 46 من "التقرير المرحلي عن مناقشات الفريق العامل بشأن البند 5 من جدول الأعمال" الوارد في مرفق الوثيقة المعنونة "التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي" (A/78/265) طُلب إلى الأمانة العامة للأمم المتحدة إجراء "عملية مسح" بالتشاور مع الكيانات ذات الصلة، من أجل إجراء مسح لمخزون برامج ومبادرات بناء القدرات داخل الأمم المتحدة وخارجها وعلى الصعيدين العالمي والإقليمي، بما في ذلك عن طريق التماس آراء الدول الأعضاء. وطُلب أيضا إلى الأمانة العامة أن تعد تقريرا يتضمن نتائج "عملية المسح" المذكورة، وأن تقدم التقرير إلى الدورة السابعة للفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025، التي ستعقد في الفترة من 4 إلى 8 آذار/مارس 2024 لدعم جهود الدول الرامية إلى تقييم الجهود المبذولة حاليا لبناء القدرات وتشجيع إقامة المزيد من التآزر والتنسيق بين هذه الجهود. ويُقدّم هذا التقرير تلبيةً لذلك الطلب.

2 - وفي 2 تشرين الأول/أكتوبر 2023، عمم مكتب شؤون نزع السلاح مذكرة شفوية على جميع البعثات الدائمة لدى الأمم المتحدة يوجه فيها انتباهها إلى الفقرة 46 من التقرير المشار إليه أعلاه، وتدعوها إلى إبداء رأيها في واقع برامج ومبادرات بناء القدرات في مجال تكنولوجيات المعلومات والاتصالات، داخل



الأمم المتحدة وخارجها وعلى الصعيدين العالمي والإقليمي. وحُدد يوم 10 تشرين الثاني/نوفمبر 2023 موعداً نهائياً لتلقي الردود، ومُدد هذا الموعد لاحقاً إلى يوم 16 تشرين الثاني/نوفمبر. وحتى 22 كانون الثاني/يناير 2024، قدمت الدول التالية آراء خطية: الاتحاد الروسي وأستراليا وإستونيا وألمانيا وأوروغواي وإيران (جمهورية - الإسلامية) والبرازيل والبرتغال وبلجيكا وبوركينا فاسو وتركيا وتشيكيا وجمهورية كوريا وسلوفاكيا وسلوفينيا وسنغافورة وسويسرا وشيلي وفرنسا وقطر وكمبوديا وكوبا وكولومبيا ولبنان والمكسيك والمملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية والهند وهولندا (مملكة -) والولايات المتحدة الأمريكية.

3 - وطلب مكتب شؤون نزع السلاح كذلك آراء كيانات منظومة الأمم المتحدة ذات الصلة من خلال رسائل مؤرخة 2 تشرين الأول/أكتوبر 2023. وحتى 22 كانون الثاني/يناير 2024، قدمت كيانات الأمم المتحدة التالية آراء خطية: الاتحاد الدولي للاتصالات، والمديرية التنفيذية للجنة الأمم المتحدة لمكافحة الإرهاب، وبرنامج الأمم المتحدة الإنمائي، ومعهد الأمم المتحدة لبحوث نزع السلاح، ومعهد الأمم المتحدة الأقاليمي لأبحاث الجريمة والعدالة، ومكتب مكافحة الإرهاب، ومكتب تكنولوجيا المعلومات والاتصالات، ومكتب الشؤون القانونية، ومكتب الأمم المتحدة المعني بالمخدرات والجريمة.

4 - كما وجهت دعوة لتقديم مدخلات إلى الكيانات غير الحكومية صاحبة المصلحة المعنية بالأمر عن طريق البريد الإلكتروني في 2 تشرين الأول/أكتوبر 2023. واعتباراً من 22 كانون الثاني/يناير 2024، قدمت الكيانات صاحبة المصلحة التالية آراء مكتوبة: جمعية الاتصالات التقدمية، ومركز حوكمة الاتصالات بكلية القانون الوطنية في دلهي، ومؤسسة الدبلوماسية، والمنتدى العالمي للخبرة السيبرانية، وغرفة التجارة الدولية، ومركز امتياز الأمن القومي بكلية س. راجاراتنام للدراسات الدولية، وحلول الحاسوب الآمن، والعين الثالثة القانونية، والكتابة التجريبية. وقدم الاتحاد الأوروبي أيضاً آراء. ووردت أيضاً التقارير الخطية المشتركة التالية: تقرير مشترك من الأرجنتين وإكوادور وأوروغواي وباراغواي والبرازيل والجمهورية الدومينيكية والسلفادور وشيلي وغواتيمالا وكوستاريكا وكولومبيا، وتقرير مشترك من الوكالة الوطنية التشيكية للأمن السيبراني والمعلومات، ولجنة الصليب الأحمر الدولية، ومركز الامتياز التعاوني للدفاع السيبراني التابع لمنظمة حلف شمال الأطلسي (الناتو)، وجامعة إكستر، والكلية الحربية البحرية الأمريكية وجامعة ووهان.

5 - وجميع الآراء الخطية الواردة، بما في ذلك الآراء الواردة بعد الموعد النهائي الرسمي الممدد، متاحة على الموقع الشبكي للفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025⁽¹⁾. وتُشجع الدول على الاطلاع على التقارير الخطية الكاملة المقدمة من الدول الأعضاء وكيانات منظومة الأمم المتحدة والكيانات صاحبة المصلحة غير الحكومية، لأن هذا التقرير لا يمثل جرداً شاملاً لجميع الأنشطة المفصلة فيه.

6 - ويستند هذا التقرير أساساً إلى المدخلات الواردة من الدول الأعضاء وكيانات الأمم المتحدة والكيانات غير الحكومية المذكورة أعلاه دون المساس بمواقف كل منها. وتقدم معلومات إضافية متاحة في مصادر مفتوحة بهدف تقديم صورة متوازنة وتوضيحية عن برامج ومبادرات بناء القدرات القائمة داخل الأمم المتحدة وخارجها وعلى الصعيدين العالمي والإقليمي.

7 - وتعرض أمثلة على برامج ومبادرات بناء القدرات، تبرز أولاً الجهود المبذولة على الصعيدين الإقليمي ودون الإقليمي، تليها معلومات مصنفة تصنيفاً عاماً حسب الموضوع. ولا تمثل هذه الأوصاف جرداً

(1) متاحة في الموقع <https://meetings.unoda.org/meeting/57871/documents>.

شاملا لجميع مبادرات وبرامج بناء القدرات، بل تسعى إلى تقديم صورة عامة عن الأنشطة بطريقة توضيحية. وليس للأنشطة سلم أولويات أو تراتب ضمني.

8 - وينتهي هذا التقرير بملاحظات واستنتاجات من الأمانة العامة بغية دعم الدول في المضي قدما بمبادرات أكثر فعالية واستدامة وكفاءة لبناء القدرات على الصعيد العالمي والإقليمي ودون الإقليمي.

ثانياً - استعراض عام لمناقشات الدول واستنتاجاتها بشأن بناء القدرات على الصعيد المتعدد الأطراف

9 - في ضوء الواقع المتغير للتهديدات الناشئة عن استخدام الدول لتكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي، تواصل الدول التشديد على الحاجة الملحة إلى تعزيز قدرة جميع الدول على احترام وتنفيذ الإطار التراكمي والمتطور للسلوك المسؤول للدول في استخدام تكنولوجيات المعلومات والاتصالات على النحو الذي أكدته التقرير المرحلي السنوي الثاني للفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025 (A/78/265).

10 - وسلطت الدول الضوء على ضرورة إشاعة فهم أفضل لاحتياجات الدول النامية بهدف تضيق الفجوة الرقمية من خلال بذل جهود مصممة خصيصا لبناء القدرات. وقد شددت الدول على الحاجة الملحة إلى بناء القدرات والممارسات الجيدة في طائفة من المجالات الدبلوماسية والقانونية والسياساتية والتشريعية والتنظيمية، بالإضافة إلى المهارات التقنية وبناء المؤسسات والآليات التعاونية. وشددت الدول بشتى الوسائل على أهمية التعاون بين بلدان الجنوب والتعاون الثلاثي ودون الإقليمي والإقليمي، كتكملة للتعاون بين الشمال والجنوب. وأشارت دول أيضا إلى أهمية نهج تدريب المدربين من خلال تنظيم تدريب متخصص ووضوح مناهج دراسية مصممة خصيصا لهذا التدريب والتصديق المهني، مما سييسر نقل المعارف والمهارات اللازمة إلى النظراء المعنيين.

11 - وفي إطار الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025، تواصل الدول تقديم مقترحات ملموسة وعملية المنحى بشأن جهود بناء القدرات، بما في ذلك، في جملة أمور، مقترح بإنشاء بوابة للتعاون العالمي في مجال الأمن السيبراني، ومقترح لتشجيع المزيد من التبادل التقني بشأن التهديدات التي تتعرض لها تكنولوجيات المعلومات والاتصالات لتبين وكشف الأنشطة الكيدية وتيسير الاستجابات المستنيرة لها، ومقترح لإجراء مناقشات بشأن تعزيز المشاركة الهادفة والشراكات مع أصحاب المصلحة غير الحكوميين في مجال بناء القدرات، بما في ذلك لأغراض التدريب والبحث.

12 - واعترف بالفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025 نفسه كمنبر لمواصلة تبادل الآراء والأفكار المتعلقة بجهود بناء القدرات، بما في ذلك أفضل السبل للاستفادة من المبادرات القائمة من أجل دعم الدول في تطوير القوة المؤسسية اللازمة لتنفيذ إطار السلوك المسؤول للدول.

13 - وواصلت الدول تشجيع تعميم مبادئ بناء القدرات فيما يتعلق باستخدام الدول لتكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي الواردة في المرفق جيم للوثيقة A/78/265 والتي وردت تفاصيلها لأول مرة في التقرير النهائي للفريق العامل المفتوح العضوية المعني بالتطورات في ميدان

المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي⁽²⁾. وبتأييدها هذه المبادئ، خلصت الدول إلى أن بناء القدرات ينبغي أن يكون عملية مستدامة، تشمل أنشطة محددة قائمة على النتائج، وأن يكون لها أيضا هدف واضح، وأن تكون قائمة على الأدلة، ومحايده سياسيا، وشفافة، وخاضعة للمساءلة، وبدون شروط. علاوة على ذلك، اتفقت الدول على أن بناء القدرات ينبغي أن يجري بناء على الاحترام الكامل لمبدأ سيادة الدول، وأن يكون مدفوعا بالطلب، وأن يتوافق مع الاحتياجات والأولويات المحددة وطنيا، وأن يحترم حقوق الإنسان والحريات الأساسية. وأوصى الفريق العامل المفتوح باب العضوية، في تقريره المرحلي الثاني (A/78/265)، بأن تضع الدول قوائم مرجعية طوعية وأدوات أخرى وتتبادلها لتعميم تنفيذ مبادئ بناء القدرات المتفق عليها.

14 - وواصلت الدول، من خلال مناقشات الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025، التوعية بالأبعاد الجنسانية للأمن في استخدام تكنولوجيا المعلومات والاتصالات وتشجيع بناء القدرات المراعية للاعتبارات الجنسانية على مستوى السياسات وكذلك في اختيار مشاريع بناء القدرات ووضعها موضع التنفيذ. وشجعت الدول الجهود الرامية إلى تعزيز جهود بناء القدرات المراعية للمنظور الجنساني، بما في ذلك من خلال إدماج منظور جنساني في السياسات الوطنية المتعلقة بتكنولوجيا المعلومات والاتصالات ومبادرات بناء القدرات، فضلا عن وضع قوائم مرجعية أو استبيانات لتحديد الاحتياجات والثغرات في هذا المجال.

15 - وارتأت الدول أن الأمم المتحدة يمكن أن تؤدي دورا أساسيا في تنسيق جهود بناء القدرات عن طريق تقييم احتياجات الدول، وتحديد الثغرات من خلال الأدوات والدراسات الاستقصائية، وتيسير وصول الدول إلى برامج بناء القدرات، بما في ذلك من خلال "عملية المسح" الحالية.

ثالثا - التعاون الإقليمي ودون الإقليمي والأقاليمي

16 - ما برحت الدول تؤكد من جديد أن المنظمات الإقليمية ودون الإقليمية تؤدي دورا هاما في دعم تنفيذ إطار السلوك المسؤول للدول في استخدام تكنولوجيا المعلومات والاتصالات، بما في ذلك من خلال دعم مبادرات بناء القدرات ذات الصلة. وأعربت دول عن أفكار مختلفة بشأن الجهود التي يمكن بذلها على الصعيد الإقليمي ودون الإقليمي والأقاليمي، بما في ذلك حلقات العمل والدورات التدريبية وتبادل الآراء بشأن أفضل الممارسات والدروس المستفادة. وشجعت دول أيضا على دعم برامج بناء القدرات، بما في ذلك بالتعاون مع المنظمات الإقليمية ودون الإقليمية عند الاقتضاء⁽³⁾.

17 - وفيما يتعلق بالتعاون عبر الأقاليم، فإن المنتدى العالمي للخبرات السيبرانية هو مجتمع لأصحاب المصلحة المتعددين يضم أكثر من 200 عضو وشريك، بما في ذلك دول من جميع المناطق، والمنظمات الدولية والإقليمية، وجهات فاعلة من القطاع الخاص والمجتمع المدني والأوساط الأكاديمية. وبوابة سيبييل

(2) A/75/816، المرفق الأول، الفقرة 56.

(3) A/78/265، المرفق، الفقرة 51.

(Cybil) مبادرة رائدة للمنتدى العالمي للخبرات السيبرانية، وهي مستودع على الإنترنت لمشاريع بناء القدرات السيبرانية الدولية وتستضيف البوابة مكتبة موارد لأصحاب المصلحة المهتمين⁽⁴⁾.

18 - وفي تشرين الثاني/نوفمبر 2023، استضاف المنتدى العالمي للخبرات السيبرانية المؤتمر العالمي الافتتاحي لبناء القدرات السيبرانية بالتعاون مع غانا والمنتدى الاقتصادي العالمي والبنك الدولي ومعهد السلام السيبراني. وعُقدت خلال المؤتمر جلسات مواضيعية وإقليمية عميقة. وأصدر المؤتمر وثيقة ختامية، هي نداء أكر من أجل التنمية المرنة في الفضاء السيبراني، وتتألف من مجموعة من الإجراءات الطوعية غير الملزمة لتحديد الاتجاهات التي تهدف إلى: (أ) تعزيز دور المرونة السيبرانية كعامل تمكيني للتنمية المستدامة؛ (ب) والنهوض ببناء قدرات سيبرانية مدفوعة بالطلب وفعالة ومستدامة؛ (ج) وإقامة شراكات أقوى وتنسيق أفضل؛ (د) وتحرير الموارد المالية وطرائق التنفيذ⁽⁵⁾. وأعلن كجزء من المؤتمر أن المؤتمر العالمي المقبل بشأن بناء القدرات السيبرانية سيعقد في جنيف في أيار/مايو 2025، بهدف البناء على التقدم المحرز في غانا.

19 - ومن أجل تعزيز التعاون بين الأقاليم، يستضيف التحالف الرقمي بين الاتحاد الأوروبي وأمريكا اللاتينية ومنطقة البحر الكاريبي حوارات بشأن اللوائح التنظيمية والأمن السيبراني، من بين أنشطة أخرى بشأن المسائل الرقمية والفضائية. ويهدف التحالف إلى دعم التحول الرقمي والابتكار من خلال رؤية محورها الإنسان للاقتصادات والمجتمعات الرقمية. ومن أجل تحقيق هذه الأهداف، تشمل أنشطة التحالف إقامة حوار ثنائي إقليمي بشأن السياسات الرقمية، وتوسيع برنامج بناء وصلة أوروبا وأمريكا اللاتينية (البرنامج الثاني)، وتنفيذ استراتيجية كوبرنيكوس الإقليمية لتعزيز المرونة الرقمية من خلال دعم القدرة على إدارة البيانات المكانية والاستخدام الاستراتيجي، وإنشاء مسرع رقمي إقليمي بين الاتحاد الأوروبي وأمريكا اللاتينية ومنطقة البحر الكاريبي لتعزيز روح المبادرة والابتكار.

20 - ويهدف مشروع جارٍ عنوانه "تعزيز التعاون الأمني في آسيا ومعها" بدعم من الاتحاد الأوروبي وتمويل من ألمانيا فرنسا، إلى زيادة التقارب في سياسات وممارسات الاتحاد الأوروبي والبلدان الشريكة، وزيادة الوعي ودعم الحوارات الأمنية العملية⁽⁶⁾. ويضطلع المشروع بأنشطة في أربعة مجالات مواضيعية: مكافحة الإرهاب ومنع التطرف العنيف، والأمن السيبراني، والأمن البحري، وإدارة الأزمات. والدول المشاركة حاليا هي إندونيسيا وجمهورية كوريا وسنغافورة وفيت نام والهند واليابان.

21 - وفي منطقة أوروبا الوسطى والشرقية، أطلقت بلدان الجبل الأسود وسلوفينيا وفرنسا مركز القدرات السيبرانية لغرب البلقان في أيار/مايو 2023⁽⁷⁾. ويهدف المركز إلى دعم ستة بلدان ومناطق مشاركة في تعزيز قدراتها السيبرانية المؤسسية والعملية. وتشمل الأنشطة دورات تدريبية، ووضع مناهج دراسية سيبرانية، وتبادل المعلومات وأفضل الممارسات لدعم الممارسين في دول غرب البلقان في مجال اتقاء التهديدات السيبرانية والتأهب والتصدي لها. وفي عام 2023، قدم المركز دورات تدريبية عن النظافة السيبرانية للإدارات العامة، وبرنامجا توجيهيا للنساء في مجال صنع السياسات السيبرانية والمفاوضات

(4) انظر <https://cybilportal.org/about-cybil>.

(5) متاح في الموقع <https://gc3b.org/news/read-the-full-accra-call-for-cyber-resilient-development>.

(6) انظر https://www.eas.europa.eu/sites/default/files/factsheet_eu_asia_security_july_2019.pdf.

(7) انظر <https://cybilportal.org/projects/western-balkans-cyber-capacity-centre-wb3c>.

الدولية، ودورات في الجرائم السيبرانية للسلطات القضائية وقوات الشرطة، ودورة لكبار مسؤولي أمن المعلومات في البنى التحتية الحيوية. وفي وقت كتابة هذا التقرير، من المقرر عقد 12 دورة تدريبية أخرى في عام 2024. وبالمثل، يهدف مشروع للاتحاد الأوروبي تشارك في قيادته إستونيا وتشيكيا إلى دعم بناء القدرات في مجال الأمن السيبراني في غرب البلقان من خلال تطوير: (أ) حوكمة الأمن السيبراني والتوعية به؛ (ب) وتعزيز الأطر القانونية والقواعد السيبرانية والامتثال للقانون الدولي؛ (ج) وإدارة المخاطر والأزمات؛ (د) والقدرات العملية، بما في ذلك عن طريق تعزيز فريق الاستجابة لحوادث أمن الحواسيب. ونفذ مشروع آخر للاتحاد الأوروبي بعنوان "الاستجابة السريعة للأمن السيبراني من أجل ألبانيا والجبل الأسود ومقدونيا الشمالية" لدعم قدرتها على الصمود في مواجهة الحوادث السيبرانية.

22 - وتقدم إدارة التهديدات عبر الوطنية التابعة لمنظمة الأمن والتعاون في أوروبا أنشطة لتعزيز قدرات الدول المشاركة على التصدي للتهديدات المتصلة بالأمن في مجال تكنولوجيا المعلومات والاتصالات. وتشمل مجموعة الأنشطة تمارين لتعزيز الاستجابات الوطنية الملائمة للحوادث التي تمس البنية التحتية الحيوية، وحلقات عمل بشأن مكافحة استخدام الإنترنت لأغراض إرهابية، والتدريب على التحقيق في جرائم الفضاء الحاسوبي ومقاضاة مرتكبيها⁽⁸⁾. وفي عام 2023، أقامت الإدارة دورة تدريبية في فيينا بشأن الدبلوماسية السيبرانية الدولية، وركزت الدورة على بناء القدرات الوطنية للمشاركة في المداولات الدولية بشأن السياسات السيبرانية. وبصفتها الجهة المنفذة للمقاييس الوطنية لخطورة الحوادث السيبرانية والتدابير ذات الصلة لحماية البنى التحتية الحيوية، تدعم منظمة الأمن والتعاون في أوروبا تطوير إجراءات الاتصال وإدارة الأزمات وأساليب تصنيف الحوادث بين بلدان أوروبا وآسيا الوسطى وبلدان أخرى. وبالإضافة إلى ذلك، تعمل منظمة الأمن والتعاون في أوروبا كمنتدى متعدد الأطراف للعديد من المناقشات المتعلقة بالتعاون السيبراني وبناء القدرات.

23 - ويعقد الاتحاد الروسي حلقات دراسية سنوية وحلقات عمل على الإنترنت مع المنتدى الإقليمي لرابطة أمم جنوب شرق آسيا بشأن المصطلحات المستخدمة في مجال أمن تكنولوجيا المعلومات والاتصالات واستخدامها، ومكافحة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية، والتطوير المستدام والأمن للإنترنت والاستدلال الرقمي الجنائي. والاتحاد الروسي استضاف أيضا دورات تدريبية بشأن التحقيق في جرائم الاختلاس المتصلة بتكنولوجيا المعلومات والاتصالات في المؤتمر المعني بالتفاعل وتدابير بناء الثقة في آسيا.

24 - وأنشأ الاتحاد الدولي للاتصالات، بالتعاون مع الشراكة الدولية المتعددة الأطراف ضد التهديدات السيبرانية، المركز الإقليمي للأمن السيبراني لعمان والاتحاد الدولي للاتصالات، بدعم من عُمان⁽⁹⁾. ويهدف المركز إلى تحسين الطاقات والقدرات والجاهزية والمهارات والمعارف في مجالات الأمن السيبراني وحماية البنية التحتية الحيوية وبناء القدرات في المنطقة العربية، ومقره في مبنى فريق التصدي للطوارئ الحاسوبية في عُمان.

(8) انظر <https://www.osce.org/secretariat/cyber-ict-security>.

(9) انظر <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Global-Partners/oman-itu-arab-regional-cybersecurity-centre.spx>.

25 - وتدعم لجنة البلدان الأمريكية لمكافحة الإرهاب التابعة لمنظمة الدول الأمريكية، من خلال برنامجها للأمن الحاسوبي، الدول الأعضاء في بناء القدرات التقنية والسياسية والدبلوماسية لمنع الحوادث السيبرانية وتحديدها والتصدي لها والتعافي منها، وتعزيز سلوك الدول المسؤول في الفضاء السيبراني⁽¹⁰⁾. ومن بين الأنشطة الأخرى، يساعد البرنامج في وضع استراتيجيات وطنية للأمن السيبراني وإنشاء أفرقة وطنية للاستجابة لحوادث الأمن الحاسوبي. كما يقدم المساعدة والتدريب ومجموعات أدوات وأدلة لواضعي السياسات وقطاع الصناعة والمجتمع المدني، ويدير شبكة نصف الكرة الغربي لأفرقة الاستجابة لحوادث الأمن الحاسوبي في الأمريكتين، التي تتبادل المعلومات عن التهديدات والاستخبارات فيما بين 29 فريقاً من أفرقة الاستجابة لحوادث الأمن الحاسوبي من 20 دولة عضواً في منظمة الدول الأمريكية. ويدعم البرنامج أيضاً زيادة تعميم المنظورات الجنسانية في صنع سياسات الأمن السيبراني وتمثيلها في العمليات المتعددة الأطراف.

26 - وانعقد في البرازيل المنتدى الأيبيري الأمريكي للدفاع السيبراني في تشرين الأول/أكتوبر 2023⁽¹¹⁾. وشارك في المنتدى نحو 13 دولة بهدف تعميق التكامل والتعاون الإقليميين لمنع التهديدات السيبرانية وتحديدها والتصدي لها. وشملت الأنشطة تمارين وتدريبات محاكاة، بما في ذلك تمرين (Cyber Guardian 5.0) وتطوير منصة لتبادل المعلومات عن البرامجيات الخبيثة.

رابعاً - استعراض عام توضيحي غير شامل لمبادرات بناء القدرات حسب مجال التركيز المواضيعي

القانون الدولي

27 - اعترفت الدول بالحاجة الخاصة إلى مبادرات بناء القدرات في مجال القانون الدولي في سياق أمن تكنولوجيا المعلومات والاتصالات. وشددت الدول على الحاجة الملحة إلى مواصلة جهود بناء القدرات هذه، بما في ذلك بهدف ضمان أن تكون جميع الدول قادرة على المشاركة على قدم المساواة في وضع تفاهات مشتركة بشأن كيفية تطبيق القانون الدولي في استخدام تكنولوجيا المعلومات والاتصالات. وشملت هذه الجهود حلقات عمل ودورات تدريبية وتبادل للآراء بشأن أفضل الممارسات على الصعيد الدولي والأقليمي والإقليمي ودون الإقليمي. ولاحظت الدول أيضاً قيمة توفير بناء القدرات بغية إعداد ورقات موقف وطنية بشأن انطباق القانون الدولي على استخدام الدول لتكنولوجيا المعلومات والاتصالات.

28 - وتشمل الموارد المتاحة عالمياً على الإنترنت بشأن بناء القدرات في مجال القانون الدولي مجموعة أدوات القانون السيبراني، التي وضعها اتحاد من الوكالة الوطنية للأمن السيبراني والمعلومات في تشيكيا، واللجنة الدولية للصليب الأحمر، ومركز الامتياز التعاوني للدفاع السيبراني التابع لمنظمة حلف شمال الأطلسي، وجامعة إكستر، والكلية الحربية البحرية للولايات المتحدة، وجامعة ووهان⁽¹²⁾. ومجموعة الأدوات متاحة مجاناً للاختصاصيين الحكوميين والقانونيين وتتألف حالياً مما يلي: (أ) 28 سيناريو تستكشف إمكانية

(10) انظر <https://www.oas.org/ext/en/security/prog-cyber>.

(11) انظر <https://dialogo-americas.com/articles/brazil-leads-ibero-american-cyber-defense-forum>.

(12) انظر https://cyberlaw.ccdcoe.org/wiki/Main_Page.

تطبيق القانون الدولي على العمليات السيبرانية؛ (ب) ومعلومات عن المواقف الوطنية بشأن تطبيق القانون الدولي على استخدامات تكنولوجيا المعلومات والاتصالات، بما في ذلك ما يتعلق بالسيادة أو عدم التدخل أو ما يشكل هجوما بموجب القانون الدولي الإنساني؛ (ج) وأكثر من 50 صفحة حوادث سيبرانية تقدم معلومات عن الهجمات الأخيرة أو النزاعات المسلحة الجارية.

29 - وفي عام 2020، أطلق معهد أكسفورد للأخلاقيات والقانون والنزاع المسلح بالشراكة مع مايكروسوفت عملية أكسفورد بشأن الحماية التي يوفرها القانون الدولي في الفضاء السيبراني⁽¹³⁾. وفي وقت كتابة هذا التقرير، تمخضت عملية أكسفورد عن إصدار خمسة "بيانات أكسفوردية بشأن الحماية التي يوفرها القانون الدولي"، وهي ثمرة تعاون بين الخبراء القانونيين الدوليين على مستوى العالم لتحديد وتوضيح قواعد القانون الدولي المطبقة على العمليات السيبرانية في مجموعة من السياقات، بما في ذلك ما يتعلق بحماية قطاع الرعاية الصحية، وحماية أبحاث اللقاحات، والحماية من التدخل في الانتخابات، وتنظيم عمليات وأنشطة المعلومات وعمليات برمجيات انتزاع الفدية.

30 - وفيما يتعلق بانطباق القانون الدولي الإنساني على الفضاء السيبراني، توفر اللجنة الدولية للصليب الأحمر موارد لوضعي السياسات، بما في ذلك الأوراق البحثية وحلقات العمل والندوات وإنشاء وفد للجنة الدولية للصليب الأحمر معنية بالفضاء السيبراني مقرها في لوكسمبورغ وتحظى بدعمها. ومن الأمثلة على الأنشطة الأخيرة إطلاق برنامج عمل إنساني بالتعاون مع مركز جامعة كامبريدج للبحوث في الفنون والعلوم الاجتماعية والإنسانية، واستضافة اجتماع دولي للخبراء بشأن القانون الدولي الإنساني، وتزايد مشاركة المدنيين في العمليات السيبرانية وغيرها من العمليات الرقمية أثناء النزاعات المسلحة مع أكاديمية جنيف للقانون الدولي الإنساني وحقوق الإنسان، عقد يومي 28 و 29 أيلول/سبتمبر 2023 في جنيف، ومائدة مستديرة بشأن الحرب السيبرانية بالشراكة مع جمعية أبحاث القانون الدولي، عقدت في 17 أيار/مايو 2023 في إسلام أباد.

31 - ونسقت أستراليا وسنغافورة وهولندا (مملكة -)، بالاشتراك مع المنظمة الدولية للقانون السيبراني، تنظيم دورة تدريبية دولية في مجال القانون السيبراني للدول الأعضاء في رابطة أمم جنوب شرق آسيا ومنظمة الأمن والتعاون في أوروبا بشأن القانون الدولي للعمليات السيبرانية.

32 - وتقوم الوكالة اليابانية للتعاون الدولي، من خلال تدريب على بناء القدرات في مجال القانون الدولي ووضع السياسات من أجل تعزيز التدابير الرامية إلى ضمان الأمن السيبراني، بتزويد المسؤولين من الوكالات الحكومية والأفرقة الوطنية للاستجابة للطوارئ الحاسوبية من البلدان النامية بالمعارف والمهارات في مجال القانون الدولي والسياسات الدولية التي يحتاجون إليها لوضع وتنفيذ سياسات الأمن السيبراني بفعالية.

33 - وأجرت الدول أيضا مشاورات مختلفة لإفساح المجال للحوار بشأن انطباق القانون الدولي. فعلى سبيل المثال، استضافت منظمة الدول الأمريكية، بالتعاون مع اللجنة القانونية للبلدان الأمريكية ولجنة الصليب الأحمر الدولية، مشاورات بشأن القانون الدولي المنطبق على الفضاء السيبراني⁽¹⁴⁾. وبالإضافة إلى ذلك، استضافت المكسيك، بالتعاون مع معهد القانون والابتكار والتكنولوجيا في جامعة تمبل في بنسلفانيا ومع شركة مايكروسوفت، ثلاث حلقات عمل افتراضية بشأن تطبيق القانون الدولي على الفضاء السيبراني،

(13) انظر <https://www.elac.ox.ac.uk/the-oxford-process>

(14) انظر https://www.oas.org/en/sla/dil/International_Law_Applicable_to_Cyberspace_2022.asp

وتعزيز قواعد ومعايير من أجل السلوك السلمي، وسد الفجوات الرقمية. وأنتج المشروع خلاصة وافية لأصحاب المصلحة المتعددين للممارسات الجيدة وتوصيات بشأن تطبيق القانون الدولي على الفضاء السيبراني، وقد أُطلقت في الدورة الموضوعية السادسة للفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات واستخدامها، في كانون الأول/ديسمبر 2023.

34 - وعقدت منظمة الأمن والتعاون في أوروبا دورات تنفيذية بشأن القانون الدولي للعمليات السيبرانية، بما في ذلك دورة عقدت في الفترة من 13 إلى 17 شباط/فبراير 2023 في سكوبي، بالتعاون مع مملكة هولندا وبدعم إضافي من إيطاليا وجمهورية كوريا وسلوفاكيا وسويسرا والمملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية، والمنظمة الدولية للقانون السيبراني.

السياسة، بما في ذلك وضع استراتيجيات وطنية

35 - وافق الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025 في المرفق باء لتقريره المرحلي السنوي الثاني الوارد في الوثيقة A/78/265 على قائمة أولية بالتدابير الطوعية لبناء الثقة على الصعيد العالمي. وأحد تلك التدابير يشجع الدول على أن تواصل، على أساس طوعي، تبادل الورقات المفاهيمية والاستراتيجيات والسياسات والبرامج الوطنية. وعلاوة على ذلك، اعترفت الدول بأهمية امتلاك القدرة اللازمة لوضع السياسات والتشريعات والاستراتيجيات اللازمة لتهيئة بيئة آمنة لتكنولوجيات المعلومات والاتصالات. وفي هذا السياق، بُذلت جهود شتى لبناء القدرات لدعم الدول في صياغة سياساتها الوطنية، ووضع الاستراتيجيات، وإنشاء المؤسسات والهياكل اللازمة المشفوعة بالكفاءة ذات الصلة في مسائل تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي.

36 - وعلى الصعيد العالمي، يستضيف معهد الأمم المتحدة لبحوث نزع السلاح مؤتمرا سنويا عن الاستقرار السيبراني تجري فيه مناقشات بشأن تعزيز فضاء سيبراني آمن ومستقر والقواعد والقانون الدولي وبشأن دعم الحوار المتعدد الأطراف بخصوص قضايا الأمن السيبراني. وألقى علماء في مؤتمرات سابقة إحاطات مواضيعية لدعم بلورة وجهات النظر الوطنية للدول، بما في ذلك بشأن المسائل القانونية المتعلقة بالتسوية السلمية للمنازعات فيما يتعلق باستخدام الدول لتكنولوجيات المعلومات والاتصالات، فضلا عن المسائل السياسية والتقنية المتعلقة بحماية البنية التحتية الحيوية والخدمات الحيوية في كل القطاعات. وركزت مؤتمرات سابقة أيضا على العمليات الحكومية الدولية ذات الصلة تحت رعاية الأمم المتحدة. وسيعقد مؤتمر الاستقرار السيبراني القادم في 29 شباط/فبراير و 1 آذار/مارس 2024 في نيويورك.

37 - واعترفت الدول أيضا بقيمة بوابة السياسة السيبرانية لمعهد الأمم المتحدة لبحوث نزع السلاح، التي تمثل شكلا مفيدا للدول لكي تشارك طوعا في تدابير الشفافية عن طريق تبادل المعلومات والسياسات والتشريعات وغيرها من الممارسات الجيدة ذات الصلة⁽¹⁵⁾. وحتى كانون الأول/ديسمبر 2023، تم تحميل 528 1 وثيقة إلى قاعدة بيانات بوابة السياسة السيبرانية، وثمة وثائق متاحة بـ 55 لغة ومعلومات منشورة عن 897 مشروعا لبناء القدرات. وكان هناك ما يقرب من 23 ألف زيارة للبوابة في عام 2023.

38 - وفي كانون الأول/ديسمبر 2023، ضمت بوابة السياسة السيبرانية ما يقرب من 900 مشروع لبناء القدرات من بوابة سيبييل Cybil التابعة للمنتدى العالمي للخبرات السيبرانية. ويشمل تبادل البيانات تفاصيل

(15) انظر <https://cyberpolicyportal.org>.

عن المشروع مثل عنوان المشروع، ومعلومات عن المستفيدين والممولين وتاريخي بدء المشروع وانتهائه، وهي متاحة باللغات الرسمية الست للأمم المتحدة. وتبرز المبادرة أمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها من خلال تحسين الوعي بالموارد القائمة، وتيسير التعاون بين أصحاب المصلحة، والتشجيع على زيادة الشفافية في جهود بناء القدرات السيبرانية.

39 - ويقدم الاتحاد الدولي للاتصالات، بالشراكة مع البنك الدولي ومؤتمر الأمم المتحدة للتجارة والتنمية (الأونكتاد) ومنظمة الكومنولث للاتصالات، الدعم السياساتي في مجال إنشاء إطار وطني فعال للأمن السيبراني. وتحقيقاً لهذه الغاية، فإن الطبعة الثانية من دليل وضع استراتيجيات وطنية للأمن السيبراني، الذي نشره الاتحاد الدولي للاتصالات في عام 2021⁽¹⁶⁾، تقدم لوائح السياسات استعراضاً عاماً لعملية وضع الاستراتيجية تراعي الوضع الخاص لبلدانهم وقيمها الثقافية والمجتمعية. وبالإضافة إلى ذلك، يقدم الاتحاد دورة تدريبية بواسطة الإنترنت لإعداد واضعي السياسات الوطنيين وممارسي الأمن السيبراني من القطاعين العام والخاص من خلال أربع وحدات للتعلم الإلكتروني وتمارين محاكاة بواسطة الإنترنت استناداً إلى الدليل⁽¹⁷⁾. ويتوفر أيضاً على الإنترنت مستودع محدث لاستراتيجيات الأمن السيبراني الوطنية يحتوي على سياسات وخطط عمل وطنية وعناصر أخرى ذات صلة بالأمن السيبراني⁽¹⁸⁾.

40 - ويعقد برنامج الزمالات الحاسوبية المشترك بين الأمم المتحدة وسنغافورة مرتين في السنة في دورة مدتها ستة أيام لمسؤولين حكوميين مرشحين من أجل بناء القدرات والشبكات المتعلقة بالسياسات والاستراتيجيات والعمليات الوطنية للأمن السيبراني والرقمي. وبعد الجلسات الثلاث الأولى للبرنامج، من المقرر عقد جلستين أخريين في عام 2024. ولدى البرنامج شبكة خريجين تضم أكثر من 70 زميلاً يمثلون 62 دولة عضواً.

41 - ومولت مملكة هولندا سلسلة حوارات السياسة السيبرانية العالمية مع مؤسسة أبحاث الرصد الأمريكية. وعلى مدى عامين، دعم المشروع وضع استراتيجيات وطنية للأمن السيبراني واستضاف حوارات إقليمية بشأن السياسات السيبرانية في جنوب شرق آسيا، وغرب البلقان، والشرق الأوسط وشمال أفريقيا، والجنوب الأفريقي، وأمريكا اللاتينية ومنطقة البحر الكاريبي. ويهدف المشروع أيضاً إلى تعزيز التحول الرقمي للأمن والشراكات بين القطاعين العام والخاص، وتحديد الاحتياجات والثغرات في مجال بناء القدرات ودعم التطوير المستمر لمعايير سلوك الدول في الفضاء السيبراني.

42 - وكجزء من مركز التكنولوجيا الرقمية من أجل التنمية، تعاون الاتحاد الأوروبي وألمانيا ومؤسسة خبراء فرنسا والمؤسسة الدولية والأيبيرية الأمريكية للإدارة والسياسات العامة ومبادرة القرن الأفريقي لتقديم مبادرة للحكومة الرقمية والأمن السيبراني في منطقة القرن الأفريقي⁽¹⁹⁾. ويهدف المشروع إلى مساعدة الدول المشاركة (جيبوتي والصومال وكينيا) على تعزيز الخدمات التي يقدمها القطاع العام من خلال قنوات رقمية

(16) انظر <https://ncsguide.org/the-guide>.

(17) انظر <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx>.

(18) انظر <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx>.

(19) انظر https://www.fiiapp.org/en/proyectos_fiiapp/d4d-initiative-for-digital-governance-and-cybersecurity-idgc-for-the-horn-of-africa-initiative.

آمنة. ويشمل المشروع حوارات وتبادل المعلومات من خلال لجنة تقنية إقليمية، فضلا عن استعراضات لخرائط الطريق ومشاريع الرقمنة الجارية في كل دولة.

43 - وعلى الصعيد الثنائي، دخلت فرنسا والسنغال في شراكة في المدرسة الوطنية للأمن السيبراني ذات التوجه الإقليمي التي تتخذ من داكار مقرا لها، والتي توفر، ضمن أنشطة أخرى، التدريب وتعزز التعاون وتزيد الوعي بالأمن السيبراني بين الدول الأفريقية⁽²⁰⁾. ومما يوضح أيضا العديد من البرامج الثنائية الحالية، أن البرتغال تدعم برامج التعاون الاستراتيجي الجارية في شراكات مع أنغولا وتيمور - ليشتي وسان تومي وبرينسيبي وغينيا - بيساو وكابو فيردي وموزامبيق، مما يعزز الهياكل القانونية والإدارية لمنع الجرائم السيبرانية والإرهاب السيبراني والحوادث السيبرانية وتحديدها والتصدي لها.

44 - وفي آسيا، يقدم المركز العالمي للأمن السيبراني من أجل التنمية، الذي يوجد مقره في جمهورية كوريا، المساعدة إلى الدول بناء على طلبها لبناء الخبرة السيبرانية والمرونة السيبرانية في القطاع العام. ويمكن تقديم حلقات دراسية بشأن صياغة استراتيجيات وأطر وطنية للأمن السيبراني، وإنشاء وتشغيل أفرقة وطنية للاستجابة للطوارئ الحاسوبية، والكشف عن الحوادث السيبرانية وتحليلها والاستجابة لها، وتبادل المعلومات عن الاتجاهات والتهديدات السيبرانية⁽²¹⁾. واستُضيفت مؤخرا حلقات دراسية في جمهورية لاو الديمقراطية الشعبية وصربيا وكوستاريكا بشأن وضع استراتيجيات للأمن السيبراني، والتعامل مع الحوادث، والسلامة السيبرانية والمرونة، ومواضيع أخرى.

45 - وكجزء من برنامجها في مجال التكنولوجيات السيبرانية والتكنولوجيات الحيوية، تدعم وزارة الخارجية والتجارة في أستراليا مفوض السلامة الإلكترونية لتطوير موارد السلامة العالمية على الإنترنت والعمل مع حكومات في آسيا والمحيط الهادئ لتطوير مناهج وطنية لحماية المواطنين على الإنترنت⁽²²⁾. وبالشراكة مع الصناعات والأوساط الأكاديمية والمجتمع المدني ووكالات الحكومة الأسترالية وغيرها من الجهات المانحة ذات التفكير المماثل، يدعم البرنامج أكثر من 25 بلدا في جميع أنحاء جنوب شرق آسيا والمحيط الهادئ لتعزيز وحماية مصالحها الجماعية في الفضاء السيبراني.

46 - وفي الأمريكتين، شاركت كندا والمكسيك والولايات المتحدة الأمريكية، في إطار مؤتمر قمة قادة أمريكا الشمالية، في اجتماع مائدة مستديرة بشأن أمن الفضاء السيبراني لتعزيز التعاون بين الدول المشاركة في وضع وتنفيذ سياسات بشأن أمن الفضاء السيبراني، عُقد في كانون الثاني/يناير 2023. وفي الفترة من 8 إلى 14 تشرين الأول/أكتوبر 2023، شاركت كولومبيا وتشيكيا في عقد مناقشات حول التداخل بين الأمن السيبراني والنكاء الاصطناعي، مع التركيز على التشريعات والسياسات والاستراتيجيات الوطنية.

47 - وتدعم مبادرة الدبلوماسية السيبرانية للاتحاد الأوروبي (Cyber Direct) مجموعة واسعة من الدعم السياساتي والبحث والتوعية وبناء القدرات في مجال الدبلوماسية السيبرانية، بما في ذلك من خلال الحفاظ على مجموعة أدوات الدبلوماسية السيبرانية واستضافة حوار سنوي بشأن الدبلوماسية السيبرانية الأوروبية⁽²³⁾.

(20) انظر <https://www.diplomatie.gouv.fr/en/country-files/senegal/news/article/regionally-oriented-national-school-for-cyber-security-opens-in-dakar-senegal>

(21) انظر <https://www.kisa.or.kr/EN/201>

(22) انظر <https://www.internationalcybertech.gov.au/cyber-tech-cooperation-program>

(23) انظر <https://eucyberdirect.eu>

ومن بين العديد من البرامج والمبادرات الأخرى، تستضيف مبادرة Cyber Direct برنامج زمالة للخبراء السيبرانيين أو الرقميين المبتدئين والمتوسطين من البلدان الشريكة، وهي الدول غير الأعضاء في الاتحاد الأوروبي من مجموعة دول أوروبا الشرقية أو مجموعة الدول الأفريقية أو مجموعة دول أمريكا اللاتينية ومنطقة البحر الكاريبي أو مجموعة دول آسيا والمحيط الهادئ⁽²⁴⁾. وفي المنطقة أيضاً، يقوم تحالف بين إستونيا وألمانيا وفنلندا ولكسمبرغ، بقيادة هيئة نظم المعلومات في إستونيا، بإدارة وتنفيذ مبادرة الاتحاد الأوروبي (CyberNet)، 2019-2025⁽²⁵⁾، والتي بنت مجتمعاً يضم أكثر من 300 خبير سيبراني في أكثر من 40 مجالاً من مجالات الكفاءة لدعم تنمية القدرات السيبرانية.

48 - ويدير مركز جنيف لحكومة قطاع الأمن برنامجاً لإدارة الأمن السيبراني يدعم الجهات الفاعلة الحكومية بقوانين وسياسات الأمن السيبراني بغية تعزيز أطر المساءلة وبناء القدرات⁽²⁶⁾. وأنشأ مشروع حديث شبكة لبحوث الأمن السيبراني في غرب البلقان يجري، من بين أنشطة أخرى، بحثاً في مجال الأمن السيبراني وحقوق الإنسان، واحتياجات الأمن السيبراني للفئات الضعيفة، ونوع الجنس، كل في سياقها الوطني. وبالمثل، يقدم مركز جنيف للسياسات الأمنية دورات تدريبية وحلقات عمل في مجال الأمن السيبراني⁽²⁷⁾. وتدعم مؤسسة الدبلوماسية، ومقرها أيضاً في جنيف، تنمية القدرات في مجال حوكمة الإنترنت والسياسة الرقمية من خلال توفير دورات وحلقات عمل وتمارين محاكاة بواسطة الإنترنت في الأمن السيبراني والبيانات والذكاء الاصطناعي وغيرها من القضايا الناشئة ومن خلال تعزيز وتطوير الأدوات الرقمية للحكومة وصنع السياسات الجامعة والمؤثرة⁽²⁸⁾.

49 - ويهدف مشروع "الفضاء السيبراني للجميع" (Cyberspace4All)، الذي تدعمه مملكة هولندا، إلى تعزيز الشمولية والوعي من خلال خلق لغة ومراجع مشتركة بشأن الحوكمة السيبرانية الدولية، وزيادة الوعي بالتطورات الرئيسية المتعلقة بقضايا الإنترنت في الأمم المتحدة والمساعدة في التأثير على سياسات الدولة بشأن المعايير السيبرانية. وفي مرحلته الأولى، أنتج المشروع عدداً من مجلة السياسة السيبرانية، وأشرطة فيديو قصيرة عن بناء القدرات السيبرانية، ومدونة صوتية رقمية عنوانها "من يحكم الفضاء السيبراني؟". وتهدف المرحلة الثانية، التي يشترك في تنفيذها معهد تشاتم هاوس (المعهد الملكي للشؤون الدولية)، إلى تقديم توصيات بشأن معايير الأمم المتحدة ومبادئها المتعلقة ببناء القدرات والسلوك المسؤول للدول في الفضاء السيبراني وذكاء الوعي بها ودعم تنفيذها.

50 - كما تم توفير بناء القدرات في مجال الدبلوماسية السيبرانية من خلال قنوات مختلفة. فعلى سبيل المثال، نُظمت مدرسة تالين الصيفية للدبلوماسية السيبرانية كجزء من برنامج التعددية والرقمنة، بالتعاون مع وزارة خارجية إستونيا وأكاديمية الحوكمة الإلكترونية والمركز الإستوني للتنمية الدولية. وهدفها الرئيسي هو توفير التدريب للدبلوماسيين العاملين في صنع السياسة الخارجية السيبرانية، وكذلك للمسؤولين الحكوميين الآخرين المهتمين بالقضايا السيبرانية المعقدة. وبالمثل، يوفر برنامج الأمن السيبراني للجنة البلدان الأمريكية

(24) انظر <https://eucyberdirect.eu/news/eu-cd-fellowship>

(25) انظر <https://eucyberdirect.eu>

(26) انظر <https://www.dcaf.ch/cybersecurity-governance>

(27) انظر <https://www.gcsp.ch>

(28) انظر <https://www.diplomacy.edu>

لمكافحة الإرهاب التابعة لمنظمة الدول الأمريكية برنامجاً تدريبياً في مجال الدبلوماسية السيبرانية لدعم المسؤولين العاملين في هذا المجال. ومن جانب الأمانة العامة للأمم المتحدة، سَتُحدَّثُ دورة الدبلوماسية السيبرانية على الإنترنت المتاحة حالياً على لوحة التثقيف في مجال نزع السلاح في عام 2024⁽²⁹⁾.

فرق الاستجابة للطوارئ الحاسوبية، والتدريب التقني وغير ذلك من أشكال الدعم ذات الصلة

51 - ما برحت الدول تدعو إلى اتباع نهج ملموس وعملي المنحى لبناء القدرات. وخلصت الدول إلى أن هذه التدابير الملموسة يمكن أن تشمل تقديم الدعم لأفرقة الاستجابة للطوارئ الحاسوبية أو أفرقة الاستجابة لحوادث الأمن الحاسوبي ووضع تدريب متخصص ومناهج دراسية متخصصة بما في ذلك برامج تدريب المدربين والتصديق المهني. وأعربت الدول أيضاً عن قلقها من أن الافتقار إلى الوعي بالتهديدات القائمة والمحتملة والافتقار إلى قدرات كافية للكشف عن الأنشطة الخبيثة التي تستخدم تكنولوجيات المعلومات والاتصالات ودرء خطرها أو التصدي لها قد يجعلها أكثر عرضة للأذى.

52 - وُسلط الضوء أيضاً على أهمية التدريب التقني للعاملين في ميدان تكنولوجيات المعلومات والاتصالات، بما في ذلك في مجالات أمن المعلومات، وأساليب الكشف عن الهجمات على شبكات الحاسوب والتصدي لها في نظم المعلومات المفتوحة، وتكتيكات وتقنيات وإجراءات حماية المعلومات من الوصول غير المأذون به إليها، وجمع البيانات من مصادر مفتوحة، وتقنيات التحقيق في الجرائم المرتبطة بتكنولوجيات المعلومات والاتصالات في مجال السلام والأمن الدوليين والتعاون الدولي في هذا الميدان، والتحليل الجنائي الحاسوبية، والتصدي لاستخدام تكنولوجيات المعلومات والاتصالات والخدمات البريدية الدولية في الاتجار بالمخدرات وسرقة الأموال، وتبين المعاملات غير القانونية مع الأصول الرقمية والتحقيق فيها، بما في ذلك العملات المشفرة، واستخدامها لتمويل الإرهاب.

53 - وعلى الصعيد العالمي، يقدم الاتحاد الدولي للاتصالات مساعدة مستمرة إلى الدول لإنشاء أفرقة وطنية للاستجابة للطوارئ الحاسوبية⁽³⁰⁾. ومن الأمثلة الحديثة على ذلك عمليات إطلاق هذه الأفرقة، بتيسير من الاتحاد، في أوغندا وبربادوس وبوركينا فاسو وترينيداد وتوباغو وجامايكا والجزر الأسود وجزر البهاما وجمهورية تنزانيا المتحدة وزامبيا وغامبيا وغانا وقبرص وقيرغيزستان وكوت ديفوار وكينيا ولبنان وملاوي. وفي كل حالة، تعمل هذه الأفرقة كهيئة تنسيق مركزية لتبين التهديدات السيبرانية وإدارتها والاستجابة لها.

54 - ويحتفظ منتدى أفرقة الاستجابة للحوادث والأمن بشبكة تضم أكثر من 700 فريق مشارك للاستجابة للطوارئ الحاسوبية بغية دعم التعاون للاستجابة بشكل استباقي وتفاعلي لحوادث الأمن السيبراني. ومن بين الأنشطة الأخرى، يتبادل المنتدى أفضل الممارسات فيما بين أعضائه ويشجع على تنظيم ندوات تقنية، ودروس، ومنتشورات، وخدمات على شبكة الإنترنت، ومجموعات ذات مصالح خاصة، ومؤتمر سنوي للاستجابة للحوادث⁽³¹⁾.

55 - ودشن أمين وزارة الإلكترونيات وتكنولوجيا المعلومات في الهند، ألكيش كومار شارما، تمريناً وتدريباً لمجموعة العشرين للأمن السيبراني لأكثر من 400 مشارك محلي ودولي كجزء من رئاسة الهند

(29) انظر <https://cyberdiplomacy.disarmamenteducation.org/home>

(30) انظر <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx>

(31) انظر <https://www.first.org>

لمجموعة العشرين. وعقد فريق الاستجابة للطوارئ الحاسوبية الهندي تمرين وتدريبات الأمن السيبراني في شكل هجين. وشارك مشاركون دوليون من نحو 12 بلدا على الإنترنت. وحضر مشاركون محليون من قطاعات مثل المالية والتعليم والاتصالات السلكية واللاسلكية والموانئ والشحن والطاقة وتكنولوجيات المعلومات والاتصالات شخصيا وافتراسيا.

56 - ومن خلال فترة رئاستها الحالية للكونولث، اضطلعت المملكة المتحدة بمجموعة من أنشطة بناء القدرات في إطار اختصاص برنامج الكونولث للأمن السيبراني دعما لأهداف إعلان الكونولث السيبراني لعام 2018⁽³²⁾. وقدم البرنامج الدعم إلى الدول الأعضاء في الكونولث لإجراء تقييمات ذاتية وطنية للقدرات في مجال أمن الفضاء السيبراني، وقدم المساعدة التقنية والتدريب والمشورة بشأن تهديدات الأمن السيبراني والجرائم السيبرانية. ومن خلال المشروع، عُقد أكثر من 140 فعالية في 32 دولة، واستفاد أكثر من 6 آلاف شخص من التدريب.

57 - ويقدم مركز الامتياز المشترك بين رابطة أمم جنوب شرق آسيا وسنغافورة للأمن السيبراني الدعم للدول الأعضاء في رابطة أمم جنوب شرق آسيا لتعزيز بناء القدرات السيبرانية في المنطقة، من خلال توفير البحوث والتدريب والدعم التقني المتصل بأفرقة الاستجابة للطوارئ الحاسوبية، وتبادل المعلومات عن التهديدات السيبرانية من مصادر مفتوحة، والهجمات وأفضل الممارسات، ومن خلال التدريبات والتمارين⁽³³⁾. ومنذ إنشائه، قدم مركز الامتياز أكثر من 50 برنامجا حضرها أكثر من 1 600 من كبار المسؤولين في الدول المشاركة. وابتداء من عام 2024، ستكون برامج مركز الامتياز متاحة للدول خارج منطقة رابطة أمم جنوب شرق آسيا. ومن أجل دعم التنسيق والتعاون المنتظمين، يجتمع الفريق العامل المعني بالأمن السيبراني التابع لاجتماع وزراء دفاع رابطة أمم جنوب شرق آسيا بانتظام منذ عام 2016 كمنبر لبناء الثقة ووضع المعايير بين الدول الأعضاء في رابطة أمم جنوب شرق آسيا.

58 - ويهدف برنامج القدرات السيبرانية لرابطة أمم جنوب شرق آسيا إلى بناء القدرات في الدول الأعضاء في رابطة أمم جنوب شرق آسيا، من خلال تعزيز المرونة والاستجابات الإقليمية للتهديدات⁽³⁴⁾. وتشمل الأنشطة حلقات العمل والحلقات الدراسية وأسبوع سنغافورة الدولي السنوي للأمن السيبراني وحلقة عمل مشتركة بين الولايات المتحدة الأمريكية وسنغافورة بشأن الأمن السيبراني والمؤتمر الوزاري لرابطة أمم جنوب شرق آسيا المعني بالأمن السيبراني. وفي أسبوع سنغافورة السيبراني الدولي الثامن للإنترنت في عام 2023، أُطلق برنامج سنغافورة للقيادة السيبرانية والخريجين. ويوفر البرنامج المفتوح للمرشحين من جميع الدول دورات تأسيسية وتنفيذية ومتقدمة للمسؤولين من أجل تعميق خبراتهم في مفاهيم وعمليات الدبلوماسية السيبرانية والقانون الدولي والمعايير في الفضاء السيبراني والاعتبارات العملية والتقنية للسياسة السيبرانية

(32) انظر https://assets.publishing.service.gov.uk/media/60538ad98fa8f55d38ea34c3/UK_Commonwealth_Cyber_Security_Programme_six_case_studies.pdf

(33) انظر <https://www.csa.gov.sg/News-Events/Press-Releases/2021/asean-singapore-cybersecurity-centre-of-excellence>

(34) انظر [https://www.csa.gov.sg/docs/default-source/csa/documents/sicw-2016/factsheet_accp_final.pdf?sfvrsn=a45aecbb_0#:~:text=Cyber%20Capacity%20Programme-,The%20ASEAN%20Cyber%20Capacity%20Programme%20\(ACCP\)%20aims%20to%20build%20cyber,secure%20and%20resilient%20ASEAN%20cyberspace](https://www.csa.gov.sg/docs/default-source/csa/documents/sicw-2016/factsheet_accp_final.pdf?sfvrsn=a45aecbb_0#:~:text=Cyber%20Capacity%20Programme-,The%20ASEAN%20Cyber%20Capacity%20Programme%20(ACCP)%20aims%20to%20build%20cyber,secure%20and%20resilient%20ASEAN%20cyberspace)

الدولية. وبالإضافة إلى ذلك، من المتوخى عقد "زمالة خريجي القادة السيبرانيين" لربط المشاركين السابقين في أنشطة بناء القدرات التي يستضيفها مركز التميز للأمن السيبراني من أجل عقد سلسلة من الاجتماعات المغلقة لبحث الاتجاهات والخطاب الدولي بشأن الأمن السيبراني، فضلا عن تبادل أفضل الممارسات في مجالات تشمل تنمية القوى العاملة والمهارات، والأطر القانونية، والسلوك السيبراني المسؤول.

59 - واستضافت جمهورية كوريا تحالف الأمن السيبراني من أجل التقدم المتبادل منذ إنطلاقه في عام 2016. ويركز التحالف على تعزيز التعاون وبناء القدرات بين الدول المشاركة⁽³⁵⁾. وفي وقت كتابة هذا التقرير، انضمت إلى التحالف 67 منظمة من 49 بلدا.

60 - وفي عام 2023، أطلقت وكالة الإنترنت والأمن الكورية مشروع الدرع السيبراني لرابطة أمم جنوب شرق آسيا، بالتعاون مع جامعة كانجون الوطنية وجامعة جانجنيونج ونجو وجامعة بروناي للتكنولوجيا. ويهدف المشروع إلى تعزيز التعاون بين الدول الأعضاء في رابطة أمم جنوب شرق آسيا بشأن الأمن السيبراني، وتفعيل منهج للأمن السيبراني على الإنترنت في المنطقة، وإنتاج بحوث عن خطط التصديق على الأمن السيبراني، واستضافة ماراتونات لخبراء البرمجة لرابطة أمم جنوب شرق آسيا، وإيفاد بعثات طلابية بشأن الأمن السيبراني⁽³⁶⁾.

61 - وفي الفترة الممتدة من 2017 إلى 2019، نفذ الاتحاد مشروعاً لدعم الدول الجزرية الصغيرة في المحيط الهادئ في إنشاء أطر وطنية ودون إقليمية وإقليمية للأمن السيبراني وتعزيز المهارات في هذه المجالات. وكان البرنامج يهدف إلى تقييم مدى الاستعداد لإنشاء أفرقة وطنية للاستجابة للطوارئ الحاسوبية في بابوا غينيا الجديدة وتونغا وساموا وفانواتو ووضع خطط تنفيذ لهذه الأفرقة. ومن خلال المشروع، استضاف الاتحاد حلقات عمل تدريبية لتعزيز الوعي والمهارات، تبادل فيها أكثر من 200 مشارك وأكثر من 70 منظمة الخبرات في مجال الاستجابة للحوادث وحماية البنى التحتية الحيوية للمعلومات. وقيست نتائج عملية التقييم في وقت لاحق بالمؤشرات الواردة في نموذج نضج قدرات الأمن السيبراني للدول الذي طوره المركز العالمي لقدرات الأمن السيبراني التابع لكلية أكسفورد مارتين بجامعة أكسفورد⁽³⁷⁾.

62 - وكجزء من برنامج التعاون في المجال السيبراني والتكنولوجيا الحرجة في أستراليا، فإن الشبكة العملياتية للأمن السيبراني في المحيط الهادئ⁽³⁸⁾ هي شبكة عملياتية للأمن السيبراني مؤلفة من خبراء عمليين إقليميين في الأمن السيبراني في منطقة المحيط الهادئ. وتحقق الشبكة بسجل نقاط اتصال خاصة بالأمن السيبراني العملياتية وتمكن الأعضاء من تبادل معلومات عن التهديدات التي تواجه الأمن السيبراني، وتوفر فرصاً للخبراء التقنيين لتبادل الأدوات والتقنيات والأفكار، وهي عامل تمكين للتعاون والتآزر، لا سيما عندما يؤثر حادث مأسّ بالأمن السيبراني على المنطقة.

63 - واضطلع أيضاً بأنشطة ثنائية مختلفة تركز على القدرات التقنية. فعلى سبيل المثال، يقدم برنامج بناء القدرات في مجال الأمن السيبراني في منطقة المحيط الهادئ في نيوزيلندا دعماً ثنائياً للدول الجزرية في المحيط الهادئ في وضع استراتيجيات وطنية للأمن السيبراني، وبناء قدرات أفرقة الاستجابة للطوارئ

(35) انظر <https://www.cybersec-alliance.org/camp/index.do>

(36) انظر <https://www.kangwon.ac.kr/english/contents.do?key=2356>

(37) انظر <https://gcscc.ox.ac.uk/the-cmm>

(38) انظر <https://pacson.org>

الحاسوبية، والتوعية، وصياغة تشريعات بشأن الأمن السيبراني والجرائم السيبرانية بما يتفق مع المعايير الدولية، والتحقيق والمقاضاة بما يتفق مع هذه التشريعات. وتشمل المؤتمرات الأخيرة في المنطقة الندوة الدولية بشأن الاستجابة للجرائم السيبرانية، التي عقدت في جمهورية كوريا في الفترة من 13 إلى 15 أيلول/سبتمبر 2023، ومؤتمر المحيط الهادئ لبناء القدرات والتعاون في المجال السيبراني، الذي عقد في فيجي في الفترة من 2 إلى 4 تشرين الأول/أكتوبر 2023.

64 - ومن خلال برنامج التعاون في المجال السيبراني والتكنولوجيا الحيوية، تدعم أستراليا الشركاء في منطقة المحيط الهادئ وجنوب شرق آسيا في تعزيز المرونة التقنية والحكومية في مواجهة التهديدات السيبرانية⁽³⁹⁾. وأسس برنامج التعاون في عام 2016، ووسّع في عام 2021 ليشمل التعاون في مجال التكنولوجيا الحيوية. واعتباراً من تشرين الثاني/نوفمبر 2023، دعم البرنامج 126 مشروعاً في 21 دولة من دول المنطقة. وتشمل المشاريع أنشطة لتعزيز قدرات الأمن السيبراني، والاستفادة من التكنولوجيا لدعم النمو الاقتصادي والتنمية، والدعوة إلى حماية حقوق الإنسان والديمقراطية على الإنترنت، ومنع الجريمة السيبرانية ومقاضاة مرتكبيها، ودعم تنفيذ الإطار المعياري الذي أقرته الأمم المتحدة بشأن سلوك الدول المسؤول عند استخدام تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي. وقد تم تصميم مشروع "دورة الأعرار السيبرانية" (Cyber Bootcamp)، الذي دُشن في آب/أغسطس 2019 كجزء من برنامج التعاون، بغية بناء الخبرات العملية للمسؤولين الحكوميين في جميع أنحاء جنوب شرق آسيا وتدريبهم على اكتساب المهارات اللازمة لمواجهة التحديات واغتنام الفرص المشتركة.

65 - ويقدم مركز الكفاءة السيبرانية لأمريكا اللاتينية ومنطقة البحر الكاريبي الذي أنشئ في عام 2022، بدعم من الاتحاد الأوروبي ومقره في الجمهورية الدومينيكية، التدريب وبناء القدرات في معالجة الأمن السيبراني والجريمة السيبرانية لدول أمريكا اللاتينية ومنطقة البحر الكاريبي. وتشمل الأنشطة توفير المواد والدورات التدريبية، والتوعية والدعم لوضع السياسات بشأن الأمن السيبراني الوطني والتحول الرقمي وبشأن المشاورات الوطنية والإقليمية بشأن قضايا الأمن السيبراني. وبُنذلت أيضاً جهود ثنائية لدعم إنشاء أفرقة وطنية للاستجابة للطوارئ الحاسوبية، بما في ذلك مشروع قامت به وكالة التعاون البرازيلية لدعم إنشاء مركز للاستجابة لحوادث الأمن السيبراني في سورينام.

66 - وفي الفترة الممتدة من 2016 إلى 2019، قدم البرنامج العالمي لبناء القدرات في مجال الأمن السيبراني الذي يموله مرفق الشراكة بين كوريا الجنوبية والبنك الدولي مساعدة تقنية وطنية وإقليمية لمجموعة أقاليمية مؤلفة من ست دول⁽⁴⁰⁾. وخضعت كل دولة مشاركة لتقييم يستند إلى نموذج نضج قدرات الأمن السيبراني للدول، وقدمت على أساسه تقارير تحليلية ودورات تدريبية وحلقات عمل ومساعدة تقنية. ويهدف المشروع إلى مساعدة الدول المشاركة على تعزيز البيئة الوطنية للأمن السيبراني، بمشاركة واضعي السياسات في مجال الأمن السيبراني وأصحاب المصلحة المعنيين. وقاست تقييمات الأثر فعالية التدخلات.

(39) انظر <https://www.internationalcybertech.gov.au/our-work/capacity-building>

(40) انظر <https://www.worldbank.org/en/news/feature/2020/06/01/kwpgfscp>

مجالات إضافية لبناء القدرات

67 - تتواصل جهود بناء القدرات في المجالات المتداخلة والمواضيعية الأخرى، بما في ذلك التركيز على فئات محددة مثل النساء والشباب والأكاديميين وقطاع الصناعة. وتشمل مجالات التركيز الأخرى توعية عامة الناس، والوصول الرقمي ومحو الأمية، ومكافحة الجريمة السيبرانية.

نوع الجنس ومشاركة المرأة

68 - أطلقت في عام 2020 مبادرة زمالة المرأة في الأمن الدولي والفضاء السيبراني، وهي مبادرة مشتركة بين أستراليا وكندا وهولندا (مملكة -) ونيوزيلندا والمملكة المتحدة والولايات المتحدة⁽⁴¹⁾. وتدعم المبادرة حضور الدبلوماسيات دورات العمليات الحكومية الدولية ذات الصلة تحت رعاية الأمم المتحدة، بما في ذلك الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها، وتستضيف التدريب على مهارات التفاوض وحلقات العمل. ويدعم البرنامج، في نسخته الثانية، 35 دبلوماسية يمثلن بلدانا من مختلف أنحاء رابطة أمم جنوب شرق آسيا ومنطقة آسيا والمحيط الهادئ وأمريكا الجنوبية والكومنولث للمشاركة في اجتماعات الفريق العامل المفتوح العضوية. ويتلقى الزملاء أيضا تدريباً من معهد الأمم المتحدة للتدريب والبحث بشأن المفاوضات المتعددة الأطراف، ويشاركون في تمهيد للقضايا ذات الصلة بالأمن الدولي في الفضاء السيبراني، ويتلقون التوجيه من الزملاء الأقدم العاملين في هذه القضايا في الأمم المتحدة في نيويورك.

69 - ويدير الاتحاد الدولي للاتصالات حالياً برنامجاً بعنوان "مساراتها السيبرانية" يعزز التمثيل المتساوي والكامل والهادف للمرأة في مجال الأمن السيبراني⁽⁴²⁾. ويدعم البرنامج المشاركين في بناء المهارات للانخراط في صنع سياسات الأمن السيبراني الوطنية والدولية، وتعزيز الوعي والحد من الحواجز التي تحول دون مشاركة المرأة في هذا المجال وزيادة مشاركة المرأة وتمثيلها في القوة العاملة في مجال الأمن السيبراني. وفي جنوب شرق آسيا، نفذ الاتحاد مشروعاً لتعزيز وضع معايير وأطر عمل في التكنولوجيات الحيوية التي تدعم مشاركة المرأة واندماجها وتمكينها. ويدعم المشروع عملية صنع السياسات والمعايير وأطر العمل والمبادرات للتخفيف من حدة التحيزات وبناء الثقة والشمول. ونُشر المشروع في البداية في إندونيسيا وتايلند والفلبين وماليزيا، بهدف التوسع ليشمل دولاً أخرى في المنطقة.

70 - ويقدم الاتحاد الدولي للاتصالات أيضاً برنامجاً إرشادياً للمرأة في المجال السيبراني. وأطلقت النسخة الأولى من البرنامج في عام 2021 في اليوم الدولي للمرأة وشارك في تنظيمه الاتحاد الدولي للاتصالات ومنتهى أفرقة الاستجابة للحوادث والأمن ومتساوون: الشراكة العالمية من أجل المساواة بين الجنسين في العصر الرقمي (المعروفة أيضاً باسم المتساوون). ومنذ إنشائه، تم تدريب وتوجيه ما يقرب من 300 امرأة في 73 بلداً من خلال البرنامج.

(41) انظر <https://eucyberdirect.eu/good-cyber-story/women-and-international-security-in-cyberspace-fellowship>.

(42) انظر <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Women-in-Cyber/HerCyberTracks/Her-CyberTracks.aspx>.

انخراط الشباب والتوعية

- 71 - من أجل نشر الوعي وإشراك وبناء قدرات الشباب المهتمين بأمن تكنولوجيات المعلومات والاتصالات، استضاف فريق الاستجابة للطوارئ الحاسوبية لتركيا مسابقة الأمن السيبراني بواسطة الإنترنت على مدار 24 ساعة، والتي يشار إليها باسم "النجم السيبراني" (Cyber Star). وتنافس أكثر من 20 ألف مشارك في مسابقة عام 2019، في فرق وبشكل فردي. كما يدير فريق الاستجابة للطوارئ الحاسوبية برنامجا سيبرانيا يشار إليه باسم "FETİH" لمواصلة تطوير مهارات المتدربين الذين يهدفون إلى دخول هذا الميدان.
- 72 - وأشار بعض الدول إلى الجهود المبذولة على الصعيد الوطني لنشر الوعي بأهمية الممارسات الجيدة في مجال أمن الفضاء السيبراني. فعلى سبيل المثال، خلال شهر تشرين الأول/أكتوبر، يروج الحرس الوطني المكسيكي للأنشطة كجزء من أسبوع الأمن السيبراني الوطني، الذي يهدف إلى الجمع بين ممثلي جميع القطاعات المعنية لتبادل الممارسات والخبرات الجيدة بشأن حماية البنية التحتية الحيوية، وأمن المواطنين في الفضاء السيبراني، والاقتصاد الرقمي، والخصوصية، وتنسيق الأطر التشريعية الوطنية.

الانخراط مع قطاع الصناعة والقطاع الخاص

- 73 - أكدت الدول على اختلافها قيمة الشراكات بين القطاعين العام والخاص والانخراط مع الشركاء في قطاع الصناعة من أجل بناء القدرة على المنعة السيبرانية. وأشارت الدول إلى جهودها الرامية إلى إجراء مشاورات مع المنظمات الرئيسية من القطاعين العام والخاص لتقييم المستوى العام للأمن السيبراني الوطني. وفي تشرين الأول/أكتوبر 2023، استضاف مؤتمر كوبان للأمن السيبراني ممثلين عن مؤسسات التعليم العالي وسلطات الدولة والبلدية ورؤساء مؤسسات ومرافق البنية التحتية في الاتحاد الروسي وأعضاء المجتمع الدولي لمناقشة التحديات والمهام والاتجاهات. كما استضاف الحدث مسابقة تركز على الشباب عنوانها "KubanCTF-2023"⁽⁴³⁾.

- 74 - ووضعت شركة غوغل خارطة طريق للأمن السيبراني لكي تنتظر فيها الدول، معتمدة على الدروس المستفادة وأفضل الممارسات في بناء حلول سحابية وأمنية عالمية للحكومات وفرادى المستخدمين. والهدف من خارطة الطريق هو دعم الدول في وضع استراتيجيات وطنية للأمن السيبراني من أجل حماية البنية التحتية الحيوية والمواطنين والازدهار الاقتصادي⁽⁴⁴⁾.

موارد ودراسات مستقاة من المؤسسات الأكاديمية

- 75 - يُنتج برنامج لاهاي للأمن السيبراني الدولي أبحاثا حول التطورات الرقمية والمعايير السيبرانية، ويستضيف مؤتمرا أكاديميا سنويا ويعد ملخصا للبحوث والمناقشات الأكاديمية⁽⁴⁵⁾. وتناولت منشوراته الأخيرة مواضيع مثل انخراط أصحاب المصلحة المتعددين في عمليات وضع معايير الأمن السيبراني والسلوك المسؤول في الفضاء السيبراني.

(43) انظر <https://kubsc.ru/en#events>.

(44) انظر https://safety.google/intl/en_uk.

(45) انظر <https://www.thehagueprogram.nl>.

76 - ويحدد نموذج نضج قدرات الأمن السيبراني للدول خمسة أبعاد لنضج الأمن السيبراني والخطوات اللازمة للوصول إليها. ونُشر النموذج أكثر من 130 مرة في أكثر من 90 دولة منذ عام 2015، بتيسير من المركز العالمي لقدرات الأمن السيبراني بالتعاون مع المنظمات الدولية والمنظمات الإقليمية وغيرها من المنظمات الشريكة. وسيقوم المركز العالمي لقدرات الأمن السيبراني في المستقبل بتطوير مقياس إضافي كجزء من النموذج لقياس قدرات الذكاء الاصطناعي من أجل دعم الدول في التكيف مع الذكاء الاصطناعي واستخدامه بشكل آمن ومستدام.

التمية الرقمية والوصول والإلمام الرقمي

77 - ينفذ برنامج الأمم المتحدة الإنمائي مجموعة متنوعة من المبادرات لدعم بناء البنية التحتية الرقمية أو تعزيز الإلمام بالتكنولوجيا الرقمية أو تنفيذ حلول الحوكمة الإلكترونية⁽⁴⁶⁾. وقدم البرنامج الإنمائي تقييم الاستعداد الرقمي بهدف تحديد التدخلات الرقمية وتحديد أولوياتها كجزء من رحلة التحول الرقمي للبلد. ويسلط التقييم الضوء على السياق الرقمي الراهن لبلد ما - انطلاقاً من سياق قد يفتقر إلى الأسس الرقمية الأساسية أو تكون ناقصة، وانتهاء بحالة بلد يكون فيه السياق الرقمي ركيزة أساسية للنمو والتنمية الوطنيين (يشار إليها بمراحل الاستعداد الرقمي).

78 - ويسعى برنامج الوصول الرقمي لحكومة المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية إلى حفز وصول رقمي يكون أكثر شمولاً وميسور التكلفة ومأموناً وأمناً للمجتمعات المحلية في إندونيسيا والبرازيل وجنوب أفريقيا وكينيا ونيجيريا⁽⁴⁷⁾.

79 - وتدعم مبادرة الحكومة الرقمية والأمن السيبراني في بلدان القرن الأفريقي حكومات جيبوتي والصومال وكينيا في تعزيز الحوكمة الإلكترونية وتطوير الخدمات الإلكترونية التي تركز على الإنسان. وفي تموز/يوليه 2023، بالشراكة مع مبادرة "أفريقيا الذكية" (Smart Africa) من خلال أكاديمية أفريقيا الذكية الرقمية، نظمت بوركينا فاسو دورات تدريبية على التصديق في مجال الحوسبة السحابية والأمن السيبراني.

80 - وتهدف مبادرة الاتحاد الدولي للاتصالات "Cyber4Good" إلى تيسير الوصول إلى الخدمات والأدوات الرقمية في أقل البلدان نمواً، بمشاركة الجهات الفاعلة في القطاع الخاص وبدعم من جمهورية كوريا⁽⁴⁸⁾. وإحدى النتائج التي سيتمخض عنها المشروع هي إنشاء صندوق للاتحاد الدولي للاتصالات لتنمية الأمن السيبراني، الذي سيعمل وفقاً لنموذج حوكمة وتحت إشراف مجلس استشاري. ويدعم برنامج المرونة السيبرانية من أجل التنمية التابع للاتحاد الأوروبي الجهات الفاعلة العامة والخاصة في تعزيز الأمن السيبراني والمرونة على نطاق عالمي⁽⁴⁹⁾.

(46) انظر <https://www.undp.org/digital>

(47) انظر <https://www.oecd.org/development-cooperation-learning/practices/leaving-no-one-behind-in-a-digital-world-the-united-kingdom-s-digital-access-programme-e8b15982>

(48) انظر www.itu.int/net4/ITU-D/CDS/projects/display.asp?ProjectNo=2GLO21119

(49) انظر <https://cyber4dev.eu>

81 - وتساند شراكة التنمية الرقمية للبنك الدولي التحول الرقمي الجامع في أكثر من 80 بلدا على مستوى العالم⁽⁵⁰⁾. ويدعم الصندوق الاستئماني المتعدد المانحين للأمن السيبراني، الذي افتتح في عام 2021 بدعم من إستونيا وألمانيا وهولندا (مملكة -) واليابان، برنامج التنمية الرقمية من خلال البحث ودعم البرنامج وتقييم المخاطر والتخفيف من حدتها في البنية التحتية الحيوية والقطاعات المعرضة لدرجة عالية من المخاطر. وبالتعاون مع الاتحاد الأفريقي، تدعم مبادرة الاقتصاد الرقمي لأفريقيا للبنك الدولي تنفيذ استراتيجية التحول الرقمي للاتحاد الأفريقي، 2020-2030. وتستند الاستراتيجية إلى ركائز أساسية مثل البنية التحتية الرقمية، والخدمات، والمهارات، والبيئة السياسية والتنظيمية المواتية، والابتكار وروح المبادرة، وتعتبر الأمن السيبراني والخصوصية وحماية البيانات الشخصية موضوعا متداخل الجوانب. وهي تحدد مقترحات مفصلة لبناء القدرات في مجال التنمية الرقمية والوصول والإمام الرقمي، بما في ذلك تعزيز بناء القدرات البشرية والمؤسسية من خلال حملات التوعية العامة والتدريب المهني والبحث والتطوير وأفرقة الاستجابة للطوارئ الحاسوبية⁽⁵¹⁾.

مكافحة الجرائم السيبرانية

82 - أنشئ البرنامج العالمي بشأن الجريمة السيبرانية في مكتب الأمم المتحدة المعني بالمخدرات والجريمة في عام 2013. وترد الولاية في قرار الجمعية العامة 230/65 وفي قرار لجنة منع الجريمة والعدالة الجنائية 7/22 و 8/22. ويعمل البرنامج العالمي على أساس تلك القرارات، بينما تجدر الإشارة إلى أن الجمعية العامة تتفاوض حاليا على معاهدة. ويتناول البرنامج الجوانب المترابطة لمكافحة الجريمة السيبرانية: المنع والكشف والتحقيق والمقاضاة وإصدار الأحكام أو البت فيها.

83 - وتقود المنظمة الدولية للشرطة الجنائية (الإنتربول) حاليا، من خلال مركزها للاندماج السيبراني الذي يضم أصحاب مصلحة متعددين، عملية تطوير وتقديم المساعدة التقنية الخاصة بإنفاذ القانون وبناء القدرات في مجال تكنولوجيات المعلومات والاتصالات ومسائل الجريمة السيبرانية. ويساعد مركز الدمج السيبراني البلدان الأعضاء على تبين التهديدات السيبرانية، ووضع استراتيجيات للوقاية والتعطيل، وتنسيق استجابتها لهذه التهديدات.

مكافحة استخدام تكنولوجيات المعلومات والاتصالات لأغراض إرهابية

84 - يساعد البرنامج العالمي لمكافحة الإرهاب بشأن الأمن السيبراني والتكنولوجيات الجديدة الدول الأعضاء والمنظمات الدولية والإقليمية على وضع وتنفيذ استجابات فعالة للتحديات الناشئة والفرص التي تتيحها تكنولوجيات المعلومات والاتصالات في مجال مكافحة الإرهاب. ويهدف البرنامج إلى تطوير المعارف ونشر الوعي، فضلا عن تعزيز المهارات والقدرات اللازمة لتنفيذ الاستجابات السياسية، وحماية البنية التحتية الحيوية من النشاط الإرهابي الذي يشمل تكنولوجيات المعلومات والاتصالات، وتعزيز قدرات العدالة الجنائية. وتم تدريب أكثر من 4 آلاف مسؤول من 150 دولة عضوا من خلال البرنامج، فضلا عن عقد أكثر من 60 حلقة عمل لبناء القدرات، ونشر 12 منتجا معرفيا كجزء من البرنامج. وكجزء من البرنامج،

(50) انظر <https://www.digitaldevelopmentpartnership.org>.

(51) انظر www.worldbank.org/en/programs/all-africa-digital-transformation.

قدمت أيضا المساعدة لبناء القدرات في مجال الأمن السيبراني في شكل تدريبات سيبرانية لمكافحة الإرهاب وتمارين محاكاة.

خامسا - ملاحظات الأمانة العامة واستنتاجاتها

85 - لا يزال بناء القدرات في مجال تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي بحق من بين الأولويات العليا للدول. ويشكل بناء القدرات إلى حد كبير الدعائم التي تقوم عليها الجهود المبذولة في جميع المسائل ذات الصلة التي يعالجها الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات وأمن استخدامها للفترة 2021-2025، أي التصدي للتهديدات القائمة والناشئة وبحث مدى انطباق القانون الدولي على استخدام الدول لهذه التكنولوجيات وتعزيز تدابير بناء الثقة. وشددت دول عديدة أيضا على أهمية تناول مسألة بناء القدرات في أي حوار مؤسسي منتظم يعقد في المستقبل تحت رعاية الأمم المتحدة بشأن أمن تكنولوجيا المعلومات والاتصالات. وفي هذا الصدد، ينبغي أن يظل بناء القدرات دعامة أساسية ومتداخلة الجوانب لجميع المناقشات ذات الصلة التي تجريها الدول في الأمم المتحدة بشأن أمن تكنولوجيا المعلومات والاتصالات. وسيطلب إحراز تقدم في جميع المجالات ذات الصلة، بدءا بالقواعد ومرورا بالقانون الدولي وتدابير بناء الثقة، موارد مكرسة لتنفيذ تدابير موازية لبناء القدرات.

86 - وشدد الأمين العام على الأهمية الحيوية للاستثمار في الإلمام بالتكنولوجيا الرقمية والبنية التحتية الرقمية بغية سد الفجوة الرقمية (A/75/982). وبالمثل، واصلت الدول التأكيد على أن فوائد التكنولوجيا الرقمية لا يتمتع بها الجميع على قدم المساواة، ولذلك شددت على ضرورة إيلاء الاهتمام الواجب للفجوة الرقمية المتنامية في سياق التعجيل بتنفيذ أهداف التنمية المستدامة، مع احترام الاحتياجات والأولويات الوطنية للدول. ولذلك، من الضروري أن يخدم بناء القدرات في مجال تكنولوجيا المعلومات والاتصالات بفعالية احتياجات وأولويات جميع الدول، لا سيما البلدان النامية، بغية سد الفجوة الرقمية، بما في ذلك الفجوة الرقمية بين الجنسين. وينبغي أيضا أن تكون جهود بناء القدرات عاملا تمكينا للتنمية المستدامة.

87 - وليس معروفا تمام المعرفة حتى الآن ما أثر التقدم السريع في العلم والتكنولوجيا على السلم والأمن الدوليين. ومن المتوقع أن يكون للفرص والمخاطر الناجمة عن التطور السريع للتكنولوجيا الناشئة، بما في ذلك الذكاء الاصطناعي وتكنولوجيا الكم، آثار عميقة على احتياجات الدول وأولوياتها في مجال بناء القدرات على المستويين التقني والسياساتي. فمن ناحية، لا بد من زيادة القدرات من أجل استخدام قدرات تكنولوجيا المعلومات والاتصالات، مثل تعزيز الكشف عن التهديدات وتحليلها، والاستجابة الآلية للحوادث، وتعزيز الكشف عن البرامج الضارة وأدوات كشف الغش ومنعه. ومن ناحية أخرى، تعتبر جهود بناء القدرات عاملا بالغ الأهمية بالنسبة للدول لكي يكون لديها المعارف والمهارات اللازمة لمواجهة لتحديات مثل أنشطة تكنولوجيا المعلومات والاتصالات الخبيثة المدعومة بالذكاء الاصطناعي، والتحيز والتمييز المتأصلين في أنظمة الذكاء الاصطناعي، ومسائل الشفافية. ويمكن أن تركز المبادرات الملموسة لبناء القدرات على بناء المعارف والخبرة بشأن آثار هذه التكنولوجيات الناشئة، ووضع استراتيجيات وطنية بشأن التصميم المسؤول للتكنولوجيا الناشئة وتطويرها واستخدامها، وآليات التعاون الدولي لتعزيز المنعة السيبرانية من خلال نقل المعرفة وأفضل الممارسات والدروس المستفادة.

88 - ولا يزال احتمال الازدواجية يمثل تحدياً مستمراً يواجه جهود بناء القدرات الفعالة والمستدامة. وفي هذا السياق، تجدر الإشارة إلى أنه في القرار 630 لمجلس الاتحاد الدولي للاتصالات، المتخذ في آب/أغسطس 2023، كلف الاتحاد بإعداد مورد للدول الأعضاء يتضمن، في جملة أمور، معلومات عن برامج بناء القدرات التي ينفذها، فضلاً عن البرامج الأخرى ذات الصلة⁽⁵²⁾. ويُطلب تحديث المورد لمراعاة التحديات والتطورات الجديدة. وكانت الدول تتأثر بانتظام مسألة تسخير أوجه التآزر والاستفادة من المبادرات القائمة في هذا الصدد. وفي ضوء الطابع العالمي للفريق العامل المفتوح باب العضوية المعني بأمن تكنولوجيات المعلومات والاتصالات وأمن استخدامها، تشجع الدول على استخدام العملية الحكومية الدولية المكرسة لمواصلة توضيح كيف يسعنا تبادلي الازدواجية بغية التوفيق بين الاحتياجات والموارد على أفضل وجه ممكن.

(52) متاح في الموقع <https://www.itu.int/md/S23-CL-C-0124/en>.