|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | الجمعية العالمية لتقييس الاتصالات (WTSA-24)  نيودلهي، 24-15 أكتوبر 2024 | | | |  |
|  | | | |  | |
|  | | | |  | |
| الجلسة العامة | | | | الإضافة 15 للوثيقة 39-A‬‬‬‬‬‬‬ | |
|  | | | | 13 سبتمبر 2024 | |
|  | | | | الأصل: بالإنكليزية | |
|  | | | | | |
| الدول الأعضاء في لجنة البلدان الأمريكية للاتصالات (CITEL) | | | | | |
| تعديلات مقترحة على القرار 50 | | | | | |
|  | | | | | |
|  | | | | | |
| **ملخص:** | | تقترح لجنة البلدان الأمريكية للاتصالات (‏CITEL‏) إدخال تعديلات على القرار 50 للجمعية العالمية لتقييس ‏الاتصالات (‏WTSA‏) لضمان توافقه مع التعديلات المدخلة في القرار 130 لمؤتمر المندوبين المفوضين لعام 2022 ‏‏(‏PP-22‎‏) والقرار 45 للمؤتمر العالمي لتنمية الاتصالات لعام 2022 (‏WTDC-22‎‏). والهدف من هذا الجهد مواءمة ‏القرارات وتنسيقها لتعزيز نهج يركز على الأمن، حيث يُدمج الأمن بسلاسة في تصميم المنتجات منذ البداية ويُدعم ‏باستمرار طوال فترة وجودها. وعلاوة على ذلك، يُقترح إدخال مجموعة من التعديلات الصياغية لزيادة الوضوح ‏بشكل عام.‏ | | | |
| **للاتصال:** | | Maria Celeste Fuenmayor لجنة البلدان الأمريكية للاتصالات (CITEL) | البريد الإلكتروني: [mfuenmayor@oas.org](mailto:mfuenmayor@oas.org) | | |

MOD IAP/39A15/1

القرار 50 (المراجَع في نيودلهي، 2024)

الأمن السيبراني

(فلوريانوبوليس، 2004؛ جوهانسبرغ، 2008؛ دبي، 2012؛ الحمامات، 2016؛ جنيف، 2022؛ نيودلهي، 2024)

إن الجمعية العالمية لتقييس الاتصالات (نيودلهي، 2024)،

إذ تشير إلى

*أ )* القرار 130 (المراجَع في بوخارست، 2022) لمؤتمر المندوبين المفوضين، بشأن دور الاتحاد في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات (ICT)؛

*ب)* القرار 174 (المراجَع في بوخارست، 2022) لمؤتمر المندوبين المفوضين، بشأن دور الاتحاد الدولي للاتصالات في قضايا السياسة العامة الدولية المتعلقة بمخاطر الاستعمال غير القانوني لتكنولوجيا المعلومات والاتصالات؛

*ج)* القرار 179 (المراجَع في بوخارست، 2022) لمؤتمر المندوبين المفوضين، بشأن دور الاتحاد الدولي للاتصالات في حماية الأطفال على الإنترنت؛

*د )* القرار 181 (غوادالاخارا، 2010) لمؤتمر المندوبين المفوضين، بشأن التعاريف والمصطلحات المتعلقة ببناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات؛

*ﻫ )* القرارين 55/63 و56/121 الصادرين عن الجمعية العامة للأمم المتحدة (UNGA)، اللذين يضعان الإطار القانوني بشأن مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية؛

*و )* القرار 57/239 الصادر عن الجمعية العامة للأمم المتحدة، بشأن إرساء ثقافة عالمية للأمن السيبراني؛

*ز )* القرار 64/211 الصادر عن الجمعية العامة للأمم المتحدة، بشأن إرساء ثقافة عالمية للأمن السيبراني وحماية البنية التحتية الأساسية للمعلومات؛

*ح)* القراران 211/77 و167/68 الصادران عن الجمعية العامة للأمم المتحدة بشأن الحق في الخصوصية في العصر الرقمي؛

*ط)* القرار 76/19 الصادر عن الجمعية العامة للأمم المتحدة، بشأن التطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي؛

*ي)* القرار 70/125 للجمعية العامة للأمم المتحدة، بشأن الوثيقة الختامية للاجتماع رفيع المستوى للجمعية العامة بشأن الاستعراض الشامل لتنفيذ نواتج القمة العالمية لمجتمع المعلومات (WSIS)؛

*ك)* القرار 45 (المراجَع في كيغالي، 2022) الصادر عن المؤتمر العالمي لتنمية الاتصالات (WTDC)، بشأن آليات لتعزيز التعاون في مجال الأمن السيبراني، بما في ذلك مكافحة الرسائل الاقتحامية والتصدي لها؛

*ل)* القرار 52 (المراجَع في الحمامات، 2016) للجمعية العالمية لتقييس الاتصالات، بشأن مكافحة الرسائل الاقتحامية والتصدي لها؛

*م )* القرار 58 (المراجَع في جنيف، 2022) لهذه الجمعية، بشأن تشجيع إنشاء أفرقة وطنية للتصدي للحوادث الحاسوبية لا سيما في البلدان النامية[[1]](#footnote-1)1؛

*ن)* أن الاتحاد ميسر رئيسي لخط العمل جيم5 من برنامج عمل تونس لمجتمع المعلومات للقمة العالمية لمجتمع المعلومات (بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات)؛

*س)* الأحكام ذات الصلة بالأمن السيبراني في نواتج القمة العالمية لمجتمع المعلومات،

وإذ تضع في اعتبارها

*أ )* الأهمية الحاسمة للبنية التحتية للاتصالات/تكنولوجيا المعلومات والاتصالات وتطبيقها في النشاط الاجتماعي والاقتصادي بجميع أشكاله تقريباً؛

*ب)* أن الشبكة الهاتفية العمومية التبديلية (PSTN) الموروثة تنطوي على مستوى من الخصائص الأمنية المتأصلة بسبب هيكلها الهرمي وأنظمة الإدارة المدمجة فيها؛

*ج)* أن الفصل بين عناصر المستعمل وعناصر الشبكة يقل في شبكات بروتوكول الإنترنت (IP) في حالة عدم اتخاذ الحيطة الكافية في تصميم الأمن وإدارته؛

*د )* أن تقارب الشبكات الموروثة وشبكات بروتوكول الإنترنت يؤدي بالتالي إلى زيادة التعرض لإمكانية التدخل إذا لم تُتخذ الحيطة الكافية في تصميم الأمن وإدارته في هذه الشبكات؛

*ﻫ )* أن الأمن السيبراني قضية شاملة وأن عالم الأمن السيبراني معقد ومشتت إلى حدٍ كبير ويضم الكثير من أصحاب المصلحة المختلفين على المستوى الوطني والإقليمي والعالمي بمسؤوليات تتمثل في تحديد ودراسة ومواجهة القضايا المتعلقة ببناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات؛

*و )* أن تزايد التهديدات والهجمات السيبرانية قد تتسبب في خسائر كبيرة ومتزايدة لمستعملي الاتصالات/تكنولوجيا المعلومات والاتصالات، مما أثار قلق جميع البلدان المتقدمة والنامية في العالم بدون استثناء؛

*ز )* أن البنى التحتية للاتصالات/تكنولوجيا المعلومات والاتصالات موصولة بينياً على المستوى العالمي مما يعني، *من بين جملة أمور*، أن عدم كفاية أمن البنية التحتية في بلد ما يمكن أن يتسبب في مواطن ضعف ومخاطر أكبر في بلدان أُخرى، وبالتالي، فإن التعاون مهم؛

*ح)* أن عدد وأشكال التهديدات والهجمات السيبرانية يتزايد كما يتزايد الاعتماد على الإنترنت والشبكات الأُخرى الضرورية للنفاذ إلى الخدمات والمعلومات؛

*ط)* أن بإمكان المعايير دعم جوانب أمن إنترنت الأشياء (IoT) والمدن والمجتمعات الذكية (SC&C)، ‏وغيرها من خدمات وتكنولوجيات الاتصالات وتكنولوجيا المعلومات والاتصالات الناشئة؛

*ي)* ‏أن الحد من المخاطر التي يسببها الإنسان عنصر أساسي في الأمن السيبراني؛

*ك)* أنه بغية حماية البنى التحتية العالمية للاتصالات/تكنولوجيا المعلومات والاتصالات من تهديدات وتحديات تطور مجال الأمن السيبراني، هناك حاجة إلى إجراءات وطنية وإقليمية ودولية منسقة لمنع حوادث الأمن السيبراني والتأهب والتصدي لها والتعافي منها؛

*ل)* العمل المضطلَع به والجاري في الاتحاد، بما فيه عمل لجنة الدراسات 17 لقطاع تقييس الاتصالات، ولجنة الدراسات 2 لقطاع تنمية الاتصالات، وفي إطار خطة عمل كيغالي التي اعتمدها المؤتمر العالمي الأخير لتنمية الاتصالات (كيغالي، 2022)؛

*م)* أن قطاع تقييس الاتصالات للاتحاد عليه أن يؤدي دوراً في إطار ولايته واختصاصاته فيما يتعلق بالفقرة *ي)* من *"إذ تضع في اعتبارها"*،

وإذ تضع في اعتبارها كذلك

*أ )* أن التوصية ITU‑T X.1205 تقدم تعريفاً ووصفاً للتكنولوجيات ومبادئ لحماية الشبكات؛

*ب)* أن التوصية ITU‑T X.805 تقدم إطاراً منهجياً لتحديد نقاط الضعف الخاصة بالأمن وأن التوصية ITU‑T X.1500 تقدم نموذج تبادل معلومات الأمن السيبراني (CYBEX) وتناقش التقنيات التي يمكن استخدامها لتسهيل تبادل معلومات الأمن السيبراني وأن التوصية ITU-T X.509 تقدم الأطر العامة لشهادات المفاتيح العمومية والنعوت؛

*ج)* أن لقطاع تقييس الاتصالات واللجنة التقنية الأولى المشتركة (JTC 1) بين المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC) إضافةً إلى العديد من اتحادات وكيانات وضع المعايير مثل اتحاد شبكة الويب العالمية (W3C) ومنظمة النهوض بمعايير المعلومات المهيكلة (OASIS) وفريق مهام هندسة الإنترنت (IETF) ورابطة المعايير معهد مهندسي الكهرباء والإلكترونيات (IEEE-SA)، وجهات أُخرى، مجموعة هامة من المواد المنشورة والأعمال الجارية التي لها صلة مباشرة بهذا الموضوع والتي ينبغي مراعاتها؛

*د )* أهمية تعزيز ثقافة يُنظر فيها إلى الأمن على أنه عملية مستمرة ومتكررة، مدمجة في المنتجات منذ البداية ومستمرة طيلة دورة حياتها،

وإذ تقر

*أ )* بالفقرة من منطوق القرار 130 (المراجَع في بوخارست، 2022) التي تكلف مدير مكتب تقييس الاتصالات بتكثيف العمل ضمن لجان الدراسات الحالية لقطاع تقييس الاتصالات بالاتحاد؛

ب) بأن مؤتمر المندوبين المفوضين في القرار 71 (المراجَع في بوخارست، 2022) اعتمد الخطة الاستراتيجية للفترة 2027-2024، بما في ذلك الغاية الاستراتيجية 1 (التوصيلية الشاملة: تمكين وتعزيز النفاذ الشامل إلى اتصالات/تكنولوجيا معلومات واتصالات ميسورة التكلفة وعالية الجودة وآمنة)، التي بموجبها سيركز الاتحاد على تحقيق البنية التحتية للاتصالات/تكنولوجيا المعلومات والاتصالات وخدماتها وتطبيقاتها التي يسهل النفاذ إليها وبأسعار معقولة وعالية الجودة وقابلة للتشغيل البيني وآمنة؛

*ج)* بأن المعايير عنصر أساسي في الركيزة 2 – التدابير التقنية والإجرائية للبرنامج العالمي للأمن السيبراني (GCA) الصادر عن الاتحاد الذي يعزز التعاون الدولي الرامي إلى اقتراح استراتيجيات للتوصل إلى حلول تعزز الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات، مع مراعاة الجوانب الأمنية في جميع مراحل عملية وضع المعايير؛

*د )* بالتحديات التي تواجهها الدول، خاصةً في البلدان النامية، في بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات،

وإذ تقر كذلك

*أ )* بأن مجموعة متنوعة من الهجمات السيبرانية مثل التدليس والاحتيال والمسح/التدخل، وعمليات رفض الخدمة الموزعة، وتغيير واجهة الويب والنفاذ غير المخول به قد ظهرت ولها عواقب وخيمة؛

*ب)* بأن روبوتات الشبكة (برامج التسلل) تستخدم في توزيع البرمجيات الروبوتية الضارة وشن هجمات سيبرانية؛

*ج)* بأن من الصعب أحياناً تحديد مصادر الهجمات؛

*د )* بأن التهديدات الحرجة للأمن السيبراني في البرمجيات والمعدات قد تتطلب إدارة نقاط الضعف في الوقت المناسب وتحديث المعدات والبرمجيات في الوقت المناسب؛

*ﻫ )* بأن تأمين البيانات عنصر رئيسي للأمن السيبراني علماً بأن البيانات تمثل الهدف المنشود في كثير من الأحيان؛

*و )* بأن الأمن السيبراني يمثل أحد العناصر اللازمة لبناء الثقة والأمن في استعمال الاتصالات/تكنولوجيا المعلومات والاتصالات؛

*ز )* بأن ظهور تطبيقات وتقنيات جديدة تعتمد على الذكاء الاصطناعي يمكن أن يؤثر تأثيراً كبيراً على الأمن السيبراني، مما يؤدي إلى ظهور تهديدات جديدة واستراتيجيات دفاعية جديدة*.*،

وإذ تلاحظ

*أ )* جدية النشاط والاهتمام لوضع معايير للأمن وتوصيات بشأن الاتصالات/تكنولوجيا المعلومات والاتصالات في لجنة الدراسات 17 لقطاع تقييس الاتصالات، لجنة الدراسات الرائدة المعنية بالأمن وإدارة الهوية، وغيرها من هيئات التقييس، بما فيها مجموعة التعاون العالمي بشأن المعايير (GSC)؛

*ب)* ضرورة مواءمة الاستراتيجيات والمبادرات الوطنية والإقليمية والدولية إلى أقصى حد ممكن من أجل تلافي الازدواجية وتحقيق الاستعمال الأمثل للموارد؛

*ج)* الجهود الكبيرة والتعاونية التي تبذلها الحكومات والقطاع الخاص والمجتمع المدني والأوساط التقنية والأكاديمية، كل في نطاق دوره ومسؤولياته، من أجل بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات،

تقرر

1 مواصلة إيلاء أولوية عالية لهذا العمل داخل قطاع تقييس الاتصالات طبقاً لاختصاصاته وخبراته، بما في ذلك تعزيز الفهم المشترك بين الحكومات وأصحاب المصلحة الآخرين بشأن بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات على الصعيد الوطني والإقليمي والدولي؛

2 أن تواصل جميع لجان دراسات قطاع تقييس الاتصالات تقييم التوصيات القائمة والتوصيات الجديدة الناشئة، وأن ينصبّ هذا التقييم على سلامة تصميمها واحتمالات قيام أطراف خبيثة باستغلالها وتأخذ بعين الاعتبار الخدمات والتطبيقات الجديدة التي ينبغي أن تدعمها البنية التحتية العالمية للاتصالات/تكنولوجيا المعلومات والاتصالات (بما في ذلك، على سبيل المثال لا الحصر، الحوسبة السحابية والشبكات الذكية وأنظمة النقل الذكية التي تقوم على شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات)، وفقاً لاختصاصاتها المنصوص عليها في القرار 2 (المراجَع في جنيف، 2022) لهذه الجمعية؛

3 أن يواصل قطاع تقييس الاتصالات، في إطار ولايته واختصاصاته، نشر الوعي بأهمية تعزيز أنظمة المعلومات والاتصالات وحمايتها من التهديدات والهجمات السيبرانية والأنشطة السيبرانية الخبيثة، ومواصلة تعزيز التعاون بين المنظمات الدولية والإقليمية الملائمة من أجل تعزيز تبادل المعلومات التقنية في مجال أمن شبكات المعلومات والاتصالات؛

4 أن يعمل قطاع تقييس الاتصالات على إذكاء الوعي العالمي فيما يتعلق بأمن تكنولوجيات المعلومات والاتصالات من خلال وضع توصيات وتقارير تقنية تدعم إجراءات الأمن السيبراني والسياسات التقنية وأطر المعايير؛

5 أن يعمل قطاع تقييس الاتصالات مع قطاع تنمية الاتصالات، لا سيما في سياق المسألة 3/2 لقطاع تنمية الاتصالات (تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني)؛

6 أن تواكب لجان دراسات قطاع تقييس الاتصالات ذات الصلة تطور تكنولوجيات وخدمات الاتصالات/تكنولوجيا المعلومات والاتصالات الجديدة والناشئة، وفقاً لاختصاصاتها، من أجل وضع توصيات وإضافات وتقارير تقنية تساعد على التغلب على التحديات المتعلقة بالأمن؛

7 أن يواصل قطاع تقييس الاتصالات العمل على وضع وتحسين المصطلحات والتعاريف المتصلة ببناء الثقة والأمن في استخدام الاتصالات/تكنولوجيا المعلومات والاتصالات، بما فيها مصطلح الأمن السيبراني؛

8 أنه ينبغي تعزيز العمليات المتسقة والتي تسمح بالتشغيل البيني، بغية تبادل المعلومات المتعلقة بالتصدي للحوادث على المستويات الوطنية والإقليمية والدولية‎؛

9 أن تواصل لجان دراسات قطاع تقييس الاتصالات التنسيق مع المنظمات المعنية بوضع المعايير وغيرها من الهيئات النشطة في هذا المجال وتشجيع مشاركة الخبراء في أنشطة الاتحاد في مجال بناء الثقة والأمن في استخدام تكنولوجيات المعلومات والاتصالات؛

10 أن تراعى الجوانب الأمنية في عملية وضع المعايير في قطاع تقييس الاتصالات بأكملها؛

11 أنه ينبغي تطوير شبكات وخدمات للاتصالات/تكنولوجيا المعلومات والاتصالات تتسم بالأمن والموثوقية والقدرة على الصمود، وصيانتها لتعزيز الثقة في استخدام تكنولوجيا المعلومات والاتصالات؛

12 أن تعتبر المرونة السيبرانية لشبكات وأنظمة تكنولوجيا المعلومات والاتصالات أولوية في تطوير الشبكات والبنى التحتية،

تُكلّف لجنة الدراسات 17

1 بتشجيع الدراسات المتعلقة بالأمن السيبراني بما في ذلك أمن خدمات وتكنولوجيات الاتصالات/تكنولوجيا المعلومات والاتصالات الجديدة والناشئة التي ستدعمها البنية التحتية العالمية للاتصالات/تكنولوجيا المعلومات والاتصالات؛

2 بدعم مدير مكتب تقييس الاتصالات في تحديث "خارطة الطريق الخاصة بمعايير الأمن لتكنولوجيا المعلومات والاتصالات" التي ينبغي أن تشمل بنود عمل ترمي إلى المضي قدماً بأعمال التقييس المتعلقة بالأمن، وإحاطة الأفرقة ذات الصلة في قطاع الاتصالات الراديوية وقطاع تنمية الاتصالات بالاتحاد علماً بها، باعتبار ذلك مهمة لجنة الدراسات الرئيسية بقطاع تقييس الاتصالات المعنية بالأمن؛

3 بتعزيز أنشطة التقييس المشتركة المتعلقة بالأمن بين جميع لجان الدراسات والأفرقة المتخصصة في الاتحاد وغيره من المنظمات المعنية بوضع المعايير؛

4 بالتعاون الوثيق مع جميع لجان الدراسات الأخرى التابعة لقطاع تقييس الاتصالات لوضع خطة عمل لتقييم توصيات قطاع تقييس الاتصالات القائمة وقيد الإعداد والجديدة المتعلقة بالتصدي لمواطن الضعف الأمني وأن تواصل تزويد الفريق الاستشاري لتقييس الاتصالات (TSAG) بانتظام بتقارير بشأن أمن الاتصالات/تكنولوجيا المعلومات والاتصالات؛

5 بتحديد مجموعة عامة/مشتركة من القدرات الأمنية من خلال كل مرحلة من مراحل دورة تطوير (المتطلبات والتصميم والتنفيذ والتحقق والإصدار والصيانة) منتجات خدمات أنظمة المعلومات/الشبكات/التطبيقات، بحيث يمكن دمج القدرات والميزات الأمنية في جميع مراحل دورة حيات المنتج من البداية؛

6 بتصميم إطار أو أطر أمنية مشتركة تتضمن عناصر وظيفية أمنية يمكن اعتبارها أساساً لتصميم المعمارية الأمنية لمختلف الأنظمة/الشبكات/التطبيقات من أجل تحسين جودة التوصيات المتعلقة بالأمن؛

7 بوضع أطر تعاونية للتحليل الأمني وإدارة الحوادث؛

8 ‏بمواصلة النظر في المخاطر التي يسببها الإنسان في مجال الأمن السيبراني،

تُكلّف مدير مكتب تقييس الاتصالات

1 بأن يواصل، استناداً إلى قاعدة المعلومات المرتبطة "بخارطة الطريق الخاصة بمعايير الأمن لتكنولوجيات المعلومات والاتصالات"وجهود قطاع تنمية الاتصالات بشأن الأمن السيبراني والخلاصة الوافية للأمن، وبمساعدة المنظمات الأُخرى ذات الصلة، تحديث قائمة المبادرات والأنشطة الوطنية والإقليمية والدولية، بهدف تعزيز إلى أقصى حد ممكن، المواءمة العالمية للاستراتيجيات والنهج في هذه المجالات ذات الأهمية البالغة، بما في ذلك وضع نهُج مشتركة في مجال الأمن السيبراني؛

2 بالمساهمة في التقارير السنوية لمجلس الاتحاد بشأن بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات، على النحو المحدد في القرار 130 (المراجَع في بوخارست، 2022)؛

3 بأن يقدم تقريراً سنوياً إلى مجلس الاتحاد بشأن "خارطة طريق معايير أمن تكنولوجيا المعلومات والاتصالات"؛

4 بمواصلة الاعتراف بالدور الذي تؤديه المنظمات الأُخرى ذات الخبرات والتجارب في مجال معايير الأمن والتنسيق مع هذه المنظمات حسب الاقتضاء؛

5 بمواصلة تنفيذ ومتابعة أنشطة القمة العالمية لمجتمع المعلومات (WSIS) ذات الصلة بشأن بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات، بالتعاون مع قطاعي الاتحاد الآخرين وبالتعاون مع أصحاب المصلحة المعنيين وذلك كسبيل من سبل تبادل المعلومات وأفضل الممارسات على الصعيد العالمي بشأن المبادرات الوطنية والإقليمية والدولية غير التمييزية المتعلقة بالأمن السيبراني؛

6 بالتعاون مع برنامج الأمن السيبراني العالمي (GCA) للأمين العام وغيره من المشاريع العالمية والإقليمية الأُخرى، حسب الاقتضاء، في تعزيز بناء القدرات وإقامة علاقات وشراكات مع المنظمات والمبادرات الإقليمية والدولية المختلفة المتصلة بالأمن السيبراني، حسب الاقتضاء، ودعوة جميع الدول الأعضاء وخاصة البلدان النامية إلى المشاركة في هذه الأنشطة، وكفالة التنسيق والتعاون مع هذه الأنشطة المختلفة؛

7 بأن يدعم مدير مكتب تنمية الاتصالات (BDT) فيما يخص مساعدة الدول الأعضاء على وضع إطار ملائم بين البلدان النامية يسمح بالتصدي بسرعة للحوادث الكبيرة، وأن يقترح خطة عمل لتعزيز حمايتها، مع مراعاة الآليات والشراكات حسب الاقتضاء؛

8 بأن يدعم الأنشطة التي تضطلع بها لجان دراسات قطاع تقييس الاتصالات ذات الصلة فيما يتعلق بتعزيز وبناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

9 بتعميم المعلومات على جميع أصحاب المصلحة ذوي الصلة بالأمن السيبراني من خلال تنظيم برامج تدريبية ومنتديات وورش عمل وحلقات دراسية، إلخ. لواضعي السياسات والمنظمين وأصحاب المصلحة الآخرين، خاصة من البلدان النامية، لإذكاء الوعي وتحديد الاحتياجات بالتعاون مع مدير مكتب تنمية الاتصالات؛

10 بمواصلة دعم المبادرات الرامية إلى تشجيع المشاركة الفعالة للمرأة في الأنشطة المتعلقة بالأمن السيبراني والأدوار القيادية في قطاع تقييس الاتصالات (ITU-T)، بما في ذلك شبكة المرأة (NoW) في قطاع تقييس الاتصالات،

تدعو الدول الأعضاء وأعضاء القطاع والمنتسبين والهيئات الأكاديمية، حسب الاقتضاء إلى

1 العمل معاً بشكلٍ وثيق لتعزيز التعاون الإقليمي والدولي، مع مراعاة القرار 130 (المراجَع في بوخارست، 2022) لمؤتمر المندوبين المفوضين، بهدف تعزيز الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات، للتخفيف من المخاطر والتهديدات؛

2 التعاون والمشاركة بفعالية في تنفيذ هذا القرار والإجراءات المرتبطة به؛

3 المشاركة في أنشطة لجان دراسات قطاع تقييس الاتصالات ذات الصلة من أجل وضع معايير ومبادئ توجيهية للأمن السيبراني، بهدف بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

4 استخدام توصيات قطاع تقييس الاتصالات وإضافاتها ذات الصلة؛

5 مواصلة المساهمة في عمل لجنة الدراسات 17 بشأن نُهج إدارة المخاطر السيبرانية؛

6 بمواصلة المشاركة في المبادرات الرامية إلى تشجيع المشاركة الفعالة للمرأة في الأنشطة المتعلقة بالأمن السيبراني والأدوار القيادية في قطاع تقييس الاتصالات (ITU-T)، بما في ذلك شبكة المرأة في قطاع تقييس الاتصالات (ITU-T).

ــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــ

1. 1 تشمل أقل البلدان نمواً والدول الجزرية الصغيرة النامية والبلدان النامية غير الساحلية والبلدان التي تمر اقتصاداتها بمرحلة انتقالية. [↑](#footnote-ref-1)