|  |  |  |  |
| --- | --- | --- | --- |
|  | الجمعية العالمية لتقييس الاتصالات (WTSA-24)  نيودلهي، 24-15 أكتوبر 2024 | |  |
|  | |  | |
|  | |  | |
| الجلسة العامة | | الإضافة 5 للوثيقة 38-A | |
|  | | 16 سبتمبر 2024 | |
|  | | الأصل: بالإنكليزية | |
|  | | | |
| الدول الأعضاء في المؤتمر الأوروبي لإدارات البريد والاتصالات (CEPT) | | | |
| تعديلات يُقترح إدخالها على القرار 50 | | | |
|  | | | |
|  | | | |

|  |  |  |
| --- | --- | --- |
| **ملخص:** | يقترح المؤتمر الأوروبي لإدارات البريد والاتصالات إدخال تعديلات على هذا القرار لتشجيع العمل المشترك وتجنب الازدواجية مع منظمات وضع المعايير الأخرى، وللحد من فرصة أن يصبح القرار قديم العهد خلال دورة الدراسة المقبلة، ولمواصلة تعزيز دور لجنة الدراسات 17 بوصفها لجنة الدراسات الرائدة لقطاع تقييس الاتصالات في مجال قضايا الأمن، ولزيادة العمل مع منظمات الاتصالات الإقليمية، من جملة تغييرات أخرى. كما يقترح تغييراً لتوضيح أنه ينبغي النظر في الأمن طوال دورة حياة النظام/الشبكة/التطبيق بأكملها. | |
| **للاتصال:** | Annie Norfolk Beadle وزارة العلوم والابتكار والتكنولوجيا المملكة المتحدة | البريد الإلكتروني: [Annie.NorfolkBeadle@dsit.gov.uk](mailto:Annie.NorfolkBeadle@dsit.gov.uk) |

MOD ECP/38A5/1

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 دبي، 2018) 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 الخط؛

*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، 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 58/199 الصادر عن الجمعية العامة للأمم المتحدة، بشأن إرساء ثقافة عالمية للأمن السيبراني وحماية البنية التحتية الأساسية للمعلومات؛

*ح)* القرار 41/65 الصادر عن الجمعية العامة للأمم المتحدة، بشأن المبادئ المتعلقة باستشعار الأرض عن بُعد من الفضاء الخارجي؛

*ط)* 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)؛

*ي)* 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؛

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

*ل)* 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؛

*م )* 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)؛

*ن)* 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 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؛

*ج)* أن عواقب عدم اتخاذ تدابير كافية بشأن الأمن السيبراني يمكن أن تؤثر على جميع البلدان؛

*د )* 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؛

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

*و )* أن بإمكان المعايير دعم جوانب كل الاتصالات/تكنولوجيا المعلومات والاتصالات؛

*ز )* 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؛

*ح)* 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 لتنمية الاتصالات (كيغالي، 2022)؛

*ط)* 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 النُهُج القائمة على المبادئ وعلى المخاطر وتبادل المعلومات والتحليل المنهجي لنقاط الضعف يمكن أن تحسن كثيراً أمن التكنولوجيات الحالية والناشئة؛

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

*ج)* أهمية اعتبار الأمن في استخدام تكنولوجيات المعلومات والاتصالات عمليةً مستمرة ومتكررة تُدمج في المنتجات منذ بداية استخدامها وتستمر طوال فترة عمرها؛

*د )* أن نهجاً متكرراً قائماً على المخاطر يضم توليفة من النُهج القائمة على التكنولوجيا والعمليات والبشر هو أساسي لتعزيز الأمن والقدرة على الصمود في استخدام تكنولوجيات المعلومات والاتصالات - من خلال التمكين من استحداث ممارسات الأمن السيبراني وتطبيقها حسب الحاجة من أجل معالجة التهديدات ومواطن الضعف المتطورة باستمرار - بموازاة دعم الابتكار والاتصالات/تكنولوجيا المعلومات والاتصالات الناشئة،

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، "البنية التحتية والخدمات الشاملة والآمنة للاتصالات/تكنولوجيا المعلومات والاتصالات"، باعتبارها أحد الأولويات المواضيعية الخمس للاتحاد، وتسليط الضوء على "تحسين قدرات أعضاء الاتحاد على نشر بنى تحتية شاملة وآمنة وصامدة للاتصالات/تكنولوجيا المعلومات والاتصالات من أجل التصدي للحوادث المتصلة بالأمن السيبراني، وبناء الثقة والأمن في استخدام الاتصالات/تكنولوجيا المعلومات والاتصالات، واعتماد ممارسات إدارة المخاطر" بوصفه نتيجة رئيسية؛

*ج)* بالبرنامج 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 زيادة نطاق وتنوع الهجمات السيبرانية باتت من الهجمات الناشئة والمتطورة ولها عواقب كبيرة؛

*ب)* بأن مجموعة من النواقل يمكن أن 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،

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، وتسليط الضوء على أي شواغل أمنية للجنة الدراسات 17؛

3 أن يواصل قطاع تقييس الاتصالات، في إطار ولايته واختصاصاته، نشر الوعي بالحاجة إلى تقوية أنظمة المعلومات والاتصالات وتحصينها 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 يراعيَ قطاع تقييس الاتصالات تماماً أهمية بناء القدرات لتسهيل اعتماد المعايير لدعم الأمن السيبراني، لا سيما بالنسبة للبلدان النامية، ولكن ليس على سبيل الحصر؛

6 أن ينسق ويتعاون قطاع تقييس الاتصالات مع قطاع تنمية الاتصالات في هذا الصدد، في إطار سياق المسألة 3/2 لقطاع تنمية الاتصالات (تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني) وفي إطار سياق أعمال بناء القدرات التي يضطلع بها مكتب تنمية الاتصالات؛

7 أن تواكب لجان دراسات قطاع تقييس الاتصالات ذات الصلة تطور تكنولوجيات جديدة وناشئة، وفقاً لاختصاصاتها، من أجل تنبيه لجنة الدراسات 17 إلى مجالات قد تتطلب توصيات وإضافات وتقارير تقنية جديدة لمعالجة التحديات المتعلقة بالأمن؛

8 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؛

9 أنه ينبغي تعزيز العمليات العالمية المتسقة والتي تسمح بالتشغيل البيني، بغية تبادل المعلومات المتعلقة بالتصدي للحوادث؛

10 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؛

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

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

13 أن لجنة الدراسات 17 تواصل دعم التحليل الأمني التعاوني والأدوات من أجل إدارة الحوادث، سعياً إلى دعم عمل أفرقة الاستجابة للحوادث الحاسوبية (CIRTs)، لا سيما في البلدان النامية؛

14 أن تعتبر قدرة شبكات وأنظمة تكنولوجيا المعلومات والاتصالات على الصمود أولوية في تطوير الشبكات والبنى التحتية،

تُكلّف لجنة الدراسات 17

1 بتشجيع الدراسات المتعلقة بالأمن السيبراني بما في ذلك أمن الخدمات الجديدة والتطبيقات الناشئة 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 المعنية بالأمن؛

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

4 بوضع خطة عمل للعمل المشترك مع منظمات وضع المعايير الأخرى، مع أهداف قابلة للقياس يمكن رصدها خلال دورة الدراسة المقبلة، وتقديم تقرير عن أداء خطة العمل هذه إلى الفريق الاستشاري لتقييس الاتصالات على أساس سنوي على الأقل؛

5 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؛

6 بوضع نهج مشترك إزاء عملية تحليل الثغرات اللازمة لبنود العمل الجديدة، والعمل مع المنظمات الأخرى المعنية بوضع المعايير الأخرى (مثل المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC) واتحاد شبكة الويب العالمية (W3C) ومنظمة النهوض بمعايير المعلومات المهيكلة (OASIS) وفريق مهام هندسة الإنترنت (IETF) ومعهد مهندسي الكهرباء والإلكترونيات (IEEE) والمعهد الأوروبي لمعايير الاتصالات (ETSI)) وكذلك الشركاء في النظام الإيكولوجي الأمني ذوي معارف وخبرات محددة في توفير الأمن للشبكات/التطبيقات والخدمات، وتقديم ذلك إلى الفريق الاستشاري لتقييس الاتصالات للموافقة عليه ونشره على الموقع الإلكتروني للاتحاد؛

7 بتحديد مجموعة عامة/مشتركة من القدرات الأمنية لكل مرحلة من مراحل دورة حياة أنظمة المعلومات/الشبكات/التطبيقات، بحيث يمكن نتيجة لذلك تحقيق أمن للأنظمة/الشبكات/التطبيقات/البيانات من البداية والاستمرار خلال دورات حياة النظام/الشبكة/التطبيق؛

8 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،

تُكلّف مدير مكتب تقييس الاتصالات

1 بمواصلة المساهمة في أعمال الاتحاد الجارية في مجال تحديد مواقع الأعمال ووضع العلامات عليها ودعم الجهود الرامية إلى إشراك هيئات وضع المعايير الأخرى في هذه العملية- من أجل تزويد البلدان بمزيد من المعلومات عن أعمال وضع المعايير في هذا المجال الهام؛

2 بالمساهمة في التقارير السنوية لمجلس الاتحاد بشأن بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات، على النحو المحدد في القرار 130 (المراجَع في دبي، 2018)؛

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 المنظمات الأخرى وكل 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 الإشراف على إعداد التوصيات وربما الأدوات الأخرى التي يمكن للدول الأعضاء، لا سيما البلدان النامية، أن تستخدمها لاستباق الاستجابات السريعة في حال وقوع حوادث كبيرة، وأن تساعد هذه الهيئات على أن تعد خطط عمل لتعزيز حمايتها، مع مراعاة الآليات والشراكات حسب الاقتضاء؛

8 بأن يدعم الأنشطة التي تضطلع بها لجنة الدراسات 17 ذات الصلة فيما يتعلق بتعزيز وبناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات، وبأن ينسق هذا العمل مع أعمال لجنتي دراسات قطاع تنمية الاتصالات ومع أنشطة البرامج ذات الصلة؛

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 بالعمل مع منظمات الاتصالات الإقليمية لتقديم المعرفة والأدوات والخبرة إلى جمهور أوسع بفعالية أكبر،

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

1 العمل معاً بشكلٍ وثيق لتعزيز التعاون والدعم الإقليميين والدوليين، 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.

ــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــ

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