**الجمعية العالمية لتقييس الاتصالات**

نيودلهي، 24-15 أكتوبر 2024

القـرار 50 – الأمن السيبراني

تمهيـد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات. وقطاع تقييس الاتصالات (ITU‑T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار رقم 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

© ITU 2024

جميع الحقوق محفوظة. لا يجوز استنساخ أي جزء من هذه المنشورة بأي وسيلة كانت إلا بإذن خطي مسبق من الاتحاد الدولي للاتصالات.

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 تعزيز دور الاتحاد في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات (ICT)؛

*ب)* القرار 174 (المراجَع في بوسان، 2014) 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 (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 وتقييم الجهود المبذولة على الصعيد الوطني لحماية البنية التحتية الحرجة للمعلومات؛

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

*ط)* القرار 19/76 للجمعية العامة للأمم المتحدة، بشأن التطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي ‏والنهوض بسلوك الدول المسؤول في استخدام تكنولوجيا المعلومات والاتصالات‎؛

*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 نيودلهي، 2024) لهذه الجمعية، بشأن مكافحة الرسائل الاقتحامية والتصدي لها؛

*م )* القرار 58 (المراجَع في نيودلهي، 2024) لهذه الجمعية، بشأن تشجيع إنشاء وتعزيز الأفرقة الوطنية للاستجابة في حالات الحوادث الحاسوبية، خاصة للبلدان 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 الاتصالات/تكنولوجيا المعلومات والاتصالات؛

*و )* أن الخسائر الكبيرة والمتزايدة التي يتحملها مستعملو الاتصالات/تكنولوجيا المعلومات والاتصالات بسبب المشكلة المتنامية للأمن السيبراني تثير 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 جميع الاتصالات/تكنولوجيات المعلومات والاتصالات؛

*ي)* أن ضمان سلامة وأمن الاتصالات/تكنولوجيا المعلومات والاتصالات الناشئة أمر حيوي لضمان أمن الفضاء السيبراني، ما يجعل وضع معايير أمنية لها أمراً أساسياً؛

*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 بقطاع تقييس الاتصالات (ITU‑T)، ولجنة الدراسات 2 بقطاع تنمية الاتصالات (ITU‑D)، وفي إطار خطة عمل كيغالي التي اعتمدها المؤتمر العالمي لتنمية الاتصالات (كيغالي، 2022)؛

*م )* أن قطاع تقييس الاتصالات للاتحاد عليه أن يؤدي دوراً في إطار ولايته واختصاصاته فيما يتعلق بالفقرة *ك)* من "*وإذ تضع في اعتبارها*" في هذا القرار،

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؛

*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 الاتحادات والكيانات المعنية بوضع المعايير مجموعة هامة من المواد المنشورة والأعمال الجارية التي لها صلة مباشرة بهذا الموضوع والتي ينبغي مراعاتها؛

*د )* أهمية اعتبار الأمن في استخدام الاتصالات/تكنولوجيا المعلومات والاتصالات عمليةً مستمرة ومتكررة تُدمج في المنتجات منذ البداية وتستمر طوال مراحل عمرها التشغيلي؛

*هـ )* أن النهج المتكرر القائم على المخاطر الذي يضم توليفة من العوامل التكنولوجية والعملياتية والبشرية هو نهج أساسي لتعزيز الأمن والقدرة على الصمود في استخدام الاتصالات/تكنولوجيا المعلومات والاتصالات - من خلال تمكين تطوير ممارسات الأمن السيبراني وتطبيقها حسب الحاجة من أجل معالجة التهديدات ومواطن الضعف المتطورة باستمرار - مع 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 قطاع تقييس الاتصالات بالاتحاد الحالية؛

*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: إتاحة وتعزيز النفاذ الشامل إلى اتصالات/تكنولوجيا معلومات واتصالات ميسورة التكلفة وعالية الجودة وآمنة)، التي بموجبها سيركز الاتحاد على تحقيق بنية تحتية وخدمات وتطبيقات للاتصالات/تكنولوجيا المعلومات والاتصالات يمكن للجميع النفاذ إليها بتكلفة ميسورة وتتسم بجودة عالية وقابلة للتشغيل البيني وآمنة؛

*ج)* بأن المعايير عنصر من العناصر الأساسية للركيزة 2 (التدابير التقنية والإجرائية) للبرنامج العالمي للأمن السيبراني (GCA) الصادر عن الاتحاد والذي يعزز التعاون الدولي الرامي إلى اقتراح استراتيجيات للتوصل إلى حلول تعزز الثقة والأمن في استخدام الاتصالات/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 الاتصالات/تكنولوجيا المعلومات والاتصالات،

وإذ تقر كذلك

 *أ )* بأن هناك نطاقاً وتنوعاً متزايدين في الهجمات السيبرانية مثل التدليس والاحتيال والمسح/التدخل، وعمليات رفض الخدمة الموزعة، وتغيير واجهة الويب والنفاذ غير المخول به، باتت من الهجمات الناشئة والمتطورة ولها عواقب وخيمة؛

*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 ومنح حقوق النفاذ المناسبة لمنع الهجمات؛

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

*و )* بأن الأمن السيبراني يمثل عنصراً أساسياً في بناء الثقة والأمن في استعمال الاتصالات/تكنولوجيا المعلومات والاتصالات؛

*ز )* بتزايد النفاذ واسع النطاق إلى الاتصالات/تكنولوجيات المعلومات والاتصالات على الصعيد العالمي، ولا سيما الإنترنت واستخدام الأفراد القاصرين لهذه التكنولوجيات،

وإذ تلاحظ

 *أ )* جدية النشاط والاهتمام لوضع معايير للأمن وتوصيات قطاع تقييس الاتصالات بشأن الاتصالات/تكنولوجيا المعلومات والاتصالات في لجنة الدراسات 17 بقطاع 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)* أنهبالإضافة إلى التهديدات السيبرانية الأخرى، فإن جوانب الأمن السيبراني المتعلقة بحماية البيانات المعلومات المحدِّدة للهوية الشخصية (PII)، قد برزت كقضية كبرى بالنسبة للدول الأعضاء؛

*د )* 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 الاتصالات/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 الاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الوطني والإقليمي والدولي؛

2 أن تواصل لجان دراسات قطاع تقييس الاتصالات تقييم التوصيات القائمة والتوصيات الناشئة، وفقاً لولاية كل منها المحدَّدة في القرار 2 (المراجَع في نيودلهي، 2024) لهذه الجمعية، وإحالة القضايا الأمنية إلى لجنة الدراسات 17 بقطاع تقييس الاتصالات للنظر فيها، فيما يتعلق بسلامة التصميم والتشغيل واحتمالات قيام أطراف خبيثة باستغلالها وتأخذ بعين الاعتبار خدمات وتكنولوجيات الاتصالات/تكنولوجيا المعلومات والاتصالات الجديدة والناشئة التي ينبغي أن تدعمها البنية التحتية العالمية للاتصالات/تكنولوجيا المعلومات والاتصالات؛

3 أن يواصل قطاع تقييس الاتصالات، في إطار ولايته واختصاصاته، إذكاء الوعي العالمي بالأمن في مجال الاتصالات/تكنولوجيا المعلومات والاتصالات، من خلال وضع توصيات وتقارير تقنية من قطاع تقييس الاتصالات التي تدعم إجراءات الأمن السيبراني والسياسات التقنية وأطر المعايير حول أهمية حماية الاتصالات/تكنولوجيا المعلومات والاتصالات من التهديدات السيبرانية والأنشطة السيبرانية الخبيثة، لتعزيز تطوير القدرات الأمنية لموظفي المنظمات، ومواصلة تعزيز التعاون بين المنظمات الدولية والإقليمية الملائمة من أجل تعزيز تبادل المعلومات التقنية في مجال أمن الاتصالات/تكنولوجيا المعلومات والاتصالات، بهدف مزدوج يتمثل في إدارة مخاطر الأمن السيبراني وحماية الاتصالات/تكنولوجيا المعلومات والاتصالات؛

4 أن يأخذ قطاع تقييس الاتصالات في الاعتبار احتياجات المستخدمين والمطورين عند تطوير المخرجات التي يمكن استخدامها لتعزيز الأمن السيبراني للتكنولوجيات الناشئة المتعلقة بالاتصالات/تكنولوجيا المعلومات والاتصالات؛

5 أن يأخذ قطاع تقييس الاتصالات، عند القيام بعمله، بعين الاعتبار أهمية بناء القدرات لتسهيل اعتماد المعايير لدعم الأمن السيبراني، وخاصة بالنسبة للدول النامية، ولكن ليس على سبيل الحصر؛

6 أن ينسق قطاع تقييس الاتصالات مع قطاع تنمية الاتصالات وأن يتعاون معه في هذا الصدد، في سياق المسألة 3/2 لقطاع تنمية الاتصالات (تأمين شبكات المعلومات والاتصالات: الممارسات الفضلى من أجل بناء ثقافة الأمن السيبراني) وفي سياق أعمال مكتب تنمية الاتصالات (BDT) المتعلقة بتطوير القدرات؛

7 أن تواكب لجان دراسات قطاع تقييس الاتصالات ذات الصلة تطور الخدمات والتكنولوجيات الجديدة والناشئة فيما يتعلق بالاتصالات/تكنولوجيا المعلومات والاتصالات، وفقاً لاختصاصاتها، من أجل إبلاغ لجنة الدراسات 17 بقطاع تقييس الاتصالات بالمجالات التي قد تستلزم وضع توصيات وإضافات وتقارير تقنية جديدة من قطاع تقييس الاتصالات لمعالجة التحديات المتعلقة بالأمن السيبراني وجوانبه المتصلة بحماية البيانات والمعلومات المحدِّدة للهوية الشخصية؛

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 الاتصالات/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 الاتصالات/تكنولوجيا المعلومات والاتصالات؛

13 أن تعتبر المرونة السيبرانية لشبكات وأنظمة الاتصالات/تكنولوجيا المعلومات والاتصالات أولوية في تطوير البنية التحتية لشبكات الاتصالات/تكنولوجيا المعلومات والاتصالات وتطبيقاتها،

تُكلّف لجنة الدراسات 17 بقطاع تقييس الاتصالات بالاتحاد

1 بتشجيع الدراسات المتعلقة بالأمن السيبراني بما في ذلك جوانبه المتصلة بحماية البيانات والمعلومات المحددة للهوية وأمن الخدمات والتكنولوجيات الجديدة والناشئة فيما يتعلق بالاتصالات/تكنولوجيا المعلومات والاتصالات للتصدي لمواطن الضعف فيما يتعلق باستخدام البنية التحتية العالمية للاتصالات/تكنولوجيا المعلومات والاتصالات، من خلال إعداد توصيات وإضافات وتقارير تقنية من قطاع تقييس الاتصالات، حسب الاقتضاء؛

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 السيبراني وجوانبه المتصلة بحماية البيانات والمعلومات المحددة للهوية الشخصية، والخلاصة الوافية بشأن الأمن والتي ينبغي أن تتضمن قائمة بتوصيات قطاع تقييس الاتصالات والمصطلحات والتعريفات، وإحاطة الأفرقة ذات الصلة في قطاع الاتصالات الراديوية وقطاع تنمية الاتصالات بالاتحاد علماً بها، باعتبار ذلك مهمة لجنة دراسات قطاع تقييس الاتصالات الرئيسية والمعنية بالأمن؛

3 بريادة أنشطة التقييس المشتركة المتعلقة بالثقة والأمن بين جميع لجان الدراسات في الاتحاد وغيره من المنظمات المعنية بوضع المعايير، حسب الاقتضاء؛

4 بالتعاون الوثيق مع جميع لجان دراسات قطاع تقييس الاتصالات الأخرى لوضع خطة عمل لتقييم توصيات قطاع تقييس الاتصالات القائمة وقيد الإعداد والجديدة لمعالجة التهديدات الأمنية ومواطن الضعف الأمني المتطورة باستمرار وتشجيع قدرة شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات على الصمود في وجه الهجمات السيبرانية، وأن تواصل تزويد الفريق الاستشاري لتقييس الاتصالات (TSAG) بانتظام بتقارير بشأن أمن الاتصالات/تكنولوجيا المعلومات والاتصالات؛

5 بمواصلة تحديد مجموعة عامة/مشتركة من القدرات الأمنية في كل مرحلة من مراحل دورة حياة التطوير، من قبيل المتطلبات والتصميم والتنفيذ والتحقيق والإصدار والصيانة، لمنتجات أنظمة المعلومات/الشبكات/التطبيقات، بما في ذلك تطوير القدرات الأمنية لموظفي المنظمات، بحيث يمكن تحقيق الأمن من خلال التصميم (القدرات والميزات الأمنية المتوافرة منذ التصميم) للأنظمة/الشبكات/التطبيقات من البداية؛

6 بمواصلة تصميم إطار أو أكثر من الأطر الأمنية أو المعماريات المرجعية التي تتضمن عناصر وظيفية أمنية، بما في ذلك النظر في قابلية التشغيل البيني للأمان بين أنواع مختلفة من الأنظمة، والتي يمكن اعتبارها أساساً لتصميم المعمارية الأمنية لمختلف الأنظمة/الشبكات/التطبيقات من أجل تحسين جودة توصيات قطاع تقييس الاتصالات المتعلقة بالأمن، وتوفير مراجع التصميم الأمني للتطبيقات المحتملة في البنية التحتية العالمية للاتصالات/تكنولوجيا المعلومات والاتصالات؛

7 بمواصلة دعم التحليل الأمني التعاوني والأدوات من أجل إدارة الحوادث، سعياً إلى دعم عمل أفرقة الاستجابة للحوادث الحاسوبية (CIRT)، لا سيما في البلدان النامية؛

8 بالنظر في تلبية المتطلبات، عند صياغتها، ووضع المعايير التقنية لدعم الجهود الرامية إلى تعزيز الأمن السيبراني للقاصرين؛

9 بإيلاء اعتبار للتغيرات المستمرة في الاتصالات/تكنولوجيات المعلومات والاتصالات والانتظام في استعراض توصيات قطاع تقييس الاتصالات القائمة المتعلقة بأمن الشبكات ومراجعتها لتكييفها مع المتطلبات الأمنية الجديدة ولكي تتصدى للتهديدات الجديدة لأمن الشبكات؛

10 بتقديم الممارسات الفضلى لتقييم الأمن السيبراني وتحسينه، بما في ذلك جوانب حماية البيانات والمعلومات المحدِّدة للهوية الشخصية، في البنية التحتية الآخذة في التطور للاتصالات/تكنولوجيا المعلومات والاتصالات؛

11 بإجراء تقييم لتأثير الاتصالات/تكنولوجيا المعلومات والاتصالات الجديدة والناشئة، من منظور الأمن السيبراني، وتحديد الثغرات والتوصية باستراتيجيات للتبني والاستخدام الآمن،

تكلف مدير مكتب تقييس الاتصالات

1 بأن يواصل، استناداً إلى قاعدة المعلومات المرتبطة "بخارطة الطريق الخاصة بمعايير الأمن للاتصالات/تكنولوجيات المعلومات والاتصالات"وجهود قطاع تنمية الاتصالات بشأن الأمن السيبراني، 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 الاتصالات/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 الاتصالات/تكنولوجيا المعلومات والاتصالات"؛

4 بمواصلة الاعتراف بالدور الذي تؤديه المنظمات الأُخرى ذات الخبرات والتجارب في مجال الأمن السيبراني، بما يشمل جملة أمور منها جوانب الأمن السيبراني لحماية معايير البيانات والمعلومات المحدِّدة للهوية الشخصية (PII) والتنسيق مع هذه المنظمات حسب الاقتضاء؛

5 بمواصلة تنفيذ ومتابعة أنشطة القمة العالمية لمجتمع المعلومات (WSIS) ذات الصلة بشأن بناء الثقة والأمن في استعمال الاتصالات/تكنولوجيا المعلومات والاتصالات، بالتعاون مع قطاعي الاتحاد الآخرين وبالتعاون مع المنظمات الأخرى وكل أصحاب المصلحة المعنيين وذلك كسبيل من سبل تبادل المعلومات والممارسات الفضلى 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 توصيات قطاع تقييس الاتصالات وربما الأدوات الأخرى التي يمكن للدول الأعضاء، لا سيما البلدان النامية، أن تستخدمها لاستباق الاستجابات السريعة في حال وقوع حوادث كبرى، وأن يساعد هذه الهيئات على أن تقترح خطط عمل تستعمل إطاراً ملائماً، حسب الاقتضاء وبناءً على الطلب، لتعزيز حمايتها، مع مراعاة الآليات والشراكات؛

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

9 بتعميم المعلومات على جميع أصحاب المصلحة وزيادة فهم أصحاب المصلحة بالأمن السيبراني من خلال تنظيم برامج تدريبية ومنتديات وورش عمل وحلقات دراسية، إلخ. حسب الاقتضاء، بشأن توصيات قطاع تقييس الاتصالات والمبادئ التوجيهية لتنفيذها تستهدف واضعي السياسات والمنظمين والمشغلين 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 والخبرة إلى جمهور أوسع بفعالية أكبر؛

11 بأن ينظر، متى أمكن، في إذكاء الوعي عن طريق عقد ورش عمل بالتزامن مع اجتماعات الأفرقة الإقليمية التابعة لكل من لجان الدراسات بقطاع تقييس الاتصالات، أو تنظيم أحداث إلى جانب هذه الاجتماعات بالتنسيق والتعاون مع مدير مكتب تنمية الاتصالات (BDT) ومكاتب الاتحاد الإقليمية، عند الاقتضاء،

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 الاتصالات/تكنولوجيا المعلومات والاتصالات، للتخفيف من المخاطر ومعالجة التهديدات؛

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 الاتصالات/تكنولوجيا المعلومات والاتصالات؛

4 استخدام توصيات قطاع تقييس الاتصالات وتقاريره التقنية وإضافاتها ذات الصلة؛

5 مواصلة المساهمة في عمل لجنة الدراسات 17 بقطاع تقييس الاتصالات بشأن نُهج إدارة المخاطر الأمنية السيبرانية والدفاع السيبراني، في نطاق ولاية الاتحاد؛

6 مواصلة دعم المبادرات الرامية إلى تشجيع المشاركة الفعالة للمرأة في الأنشطة المتعلقة بالأمن السيبراني والأدوار القيادية في قطاع تقييس الاتصالات (ITU-T)؛

7 اعتماد ودعم تنفيذ تدابير الأمن السيبراني لتكنولوجيات الاتصالات/تكنولوجيا المعلومات والاتصالات الجديدة والناشئة ضمن ولاياتها القضائية، مما يشجع بيئة آمنة ومرنة لجميع المستعملين.

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