|  |  |
| --- | --- |
| الجمعية العالمية لتقييس الاتصالات (WTSA-20)جنيف، 1- 9 مارس 2022 |  |
|  |  |
|  |  |
| الجلسة العامة | الإضافة 30للوثيقة 39-A |
|  | 19 أكتوبر 2021 |
|  | الأصل: بالإنكليزية |
|  |
| الدول الأعضاء في لجنة البلدان الأمريكية للاتصالات (CITEL) |
| تعديل مقترح للقرار 50 |
|  |
|  |
| **ملخص:** | تقترح لجنة البلدان الأمريكية للاتصالات تعديل القرار 50 للجمعية العالمية لتقييس الاتصالات. |

مقدمة

تقدم هذه المساهمة مقترحاً بتعديل القرار 50 للجمعية العالمية لتقييس الاتصالات. ويتضمن النص المعدّل المقترح فقرة جديدة في قسم "*وإذ تضع في اعتبارها*" وتغييرات في قسم " *تقرر*" فيما يتعلق بالحاجة إلى مواءمة الاستراتيجيات والنُهُج التنظيمية المتعلقة بالأمن في تكنولوجيا المعلومات والاتصالات من أجل إذكاء الوعي العالمي وتيسير التنسيق.

المقترح

تعديل القرار 50 للجمعية العالمية لتقييس الاتصالات على النحو المبين.

MOD IAP/39A30/1

القـرار 50 (المراجَع في جنيف، 2022)

الأمن السيبراني

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

إن الجمعية العالمية لتقييس الاتصالات (جنيف، 2022)،

إذ تشير إلى

 *أ )* القرار 130 (المراجَع في دبي، 2018) 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 دبي، 2018) 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 70/125 للجمعية العامة للأمم المتحدة، بشأن الوثيقة الختامية للاجتماع رفيع المستوى للجمعية العامة بشأن الاستعراض الشامل لتنفيذ نواتج القمة العالمية لمجتمع المعلومات (WSIS)؛

 *ط)* القرار 45 (المراجَع في دبي، 2014) الصادر عن المؤتمر العالمي لتنمية الاتصالات (WTDC)، بشأن آليات لتعزيز التعاون في مجال الأمن السيبراني، بما في ذلك مكافحة الرسائل الاقتحامية والتصدي لها؛

 *ي)* القرار 52 (المراجَع في جنيف، 2022) لهذه الجمعية، بشأن مكافحة الرسائل الاقتحامية والتصدي لها؛

 *ك)* القرار 58 (المراجَع في دبي، 2012)، بشأن تشجيع إنشاء أفرقة وطنية للتصدي للحوادث الحاسوبية لا سيما في البلدان النامية[[1]](#footnote-1)1؛

*ل)* 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)؛

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

وإذ تضع في اعتبارها

 *أ )* الأهمية الحاسمة للبنية التحتية للاتصالات/تكنولوجيا المعلومات والاتصالات وتطبيقاتها 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 الضرر الجسيم الذي قد ينجم عن عدم كفاية أمن تكنولوجيات المعلومات والاتصالات يثير قلق جميع البلدان المتقدمة والنامية في العالم بدون استثناء؛

*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؛

 *ﻫ)* 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 أمن جميع الاتصالات/تكنولوجيات 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 والاستجابة لها والتعافي منها؛

*ح)* أنه لحماية البيئة العالمية للاتصالات/تكنولوجيا المعلومات والاتصالات، ينبغي لأعضاء الاتحاد النظر في مجموعة من المتطلبات الدنيا على الصعيد الوطني، من أجل التعايش على الصعيد الدولي، والإجراءات التي تم وضعها من خلال توصيات ودراسات قطاع تقييس الاتصالات وكذلك منظمات وضع المعايير الأخرى المعترف بها؛

*ط)* 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 بيونس آيرس التي اعتمدها المؤتمر العالمي لتنمية الاتصالات (بوينس آيرس، 2017)؛

*ي)* 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.509 تقدم أطر شهادات المفاتيح العمومية والنعوت 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 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 ومعهد مهندسي الكهرباء والإلكترونيات، ضمن جهات أُخرى، مجموعة هامة من المواد المنشورة والأعمال الجارية التي لها صلة مباشرة بهذا الموضوع والتي ينبغي مراعاتها؛

*د )* أهمية اعتبار الأمن في استخدام تكنولوجيات المعلومات والاتصالات كعملية مستمرة ومتكررة تُدمج في المنتجات والخدمات الرقمية منذ تصميمها وتستمر طوال فترة عمرها، مع المراعاة الواجبة للمخاطر المرتبطة بالانتهاكات الأمنية، بما في ذلك العمل الجاري بشأن المعمارية المرجعية الأمنية لإدارة خدمات الحكومة الإلكترونية وإدارة الأعمال الإلكترونية والتجارة الإلكترونية وخدمات المجتمع الإلكتروني الأخرى، طيلة دورة حياتها،

وإذ تقر

*أ )* بالفقرة من منطوق القرار 130 (المراجَع في بوسان، 2014) التي تكلف مدير مكتب تقييس الاتصالات بتكثيف العمل ضمن لجان الدراسات الحالية لقطاع تقييس الاتصالات بالاتحاد؛

*ب)* بأن مؤتمر المندوبين المفوضين في القرار 71 (دبي، 2018) اعتمد الخطة الاستراتيجية للفترة 2023‑2020، بما في ذلك الغاية الاستراتيجية 3 بشأن *الاستدامة: إدارة المخاطر والتحديات والفرص الناشئة الناجمة عن النمو السريع للاتصالات/تكنولوجيا المعلومات والاتصالات*، وبموجبها سيركز الاتحاد على تعزيز جودة وموثوقية واستدامة وصمود الشبكات والأنظمة وكذلك *بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات*؛

*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 النطاق والتنوع المتزايدين للهجمات السيبرانية مثل التدليس والاحتيال والمسح/التدخل، وعمليات رفض الخدمة الموزعة، وتغيير واجهة الويب والنفاذ غير المخول به إلخ.، باتت من الهجمات الناشئة 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؛

*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؛

*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،

تقـرر

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 (على سبيل المثال لا الحصر الحوسبة السحابية والأمن القائم على التكنولوجيا الكمومية وإنترنت الأشياء 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 بالحاجة إلى تقوية أنظمة المعلومات والاتصالات وتحصينها من التهديدات والهجمات السيبرانية، ومواصلة تعزيز التعاون بين المنظمات الدولية والإقليمية الملائمة من أجل تعزيز تبادل المعلومات التقنية في ميدان أمن شبكات المعلومات والاتصالات؛

4 أن يعمل قطاع تقييس الاتصالات على إذكاء الوعي العالمي وتسليط الضوء على الاستراتيجيات والنُهُج الوطنية فيما يتعلق بأمن تكنولوجيات المعلومات والاتصالات من خلال وضع توصيات وتقارير تقنية؛

5 أن يقوم قطاع تقييس الاتصالات بالتنسيق والتعاون الوثيق 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 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؛

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

8 أن تضع لجنة الدراسات 17 بالتعاون الوثيق مع جميع لجان الدراسات الأُخرى التابعة لقطاع تقييس الاتصالات 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؛

9 أن تواصل لجان الدراسات التابعة لقطاع تقييس الاتصالات إقامة الاتصال مع المنظمات المعنية بوضع المعايير (SDO) وغيرها من الهيئات النشطة في هذا المجال؛

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

تكلف 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، 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؛

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 أصحاب المصلحة المعنيين وذلك كسبيل من سبل تبادل المعلومات 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، 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 فيما يخص مساعدة الدول الأعضاء على وضع إطار ملائم بين البلدان النامية يسمح بالتصدي للحوادث الكبيرة والتصدي لها بسرعة، 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،

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 دبي، 2018) 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.

ـــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــ

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