|  |  |  |  |
| --- | --- | --- | --- |
| itu_logo | **الجمعية العالمية لتقييس الاتصالات (WTSA-16)**  **الحمامات، 25 أكتوبر - 3 نوفمبر 2016** | | CCITT/ITU-T 60th Anniversary logo |
|  |  | |  |
|  | |  | |
| الجلسة العامة | | الإضافة 19 للوثيقة 46-A | |
|  | | 22 سبتمبر 2016 | |
|  | | الأصل: بالإنكليزية | |
|  | | | |
| الدول الأعضاء في لجنة البلدان الأمريكية للاتصالات (CITEL) | | | |
| اقتراح لتعديل القرار 50 للجمعية العال‍مية لتقييس الاتصالات لعام 2012 - الأمن السيبراني | | | |
|  | | | |
|  | | | |

|  |  |
| --- | --- |
| تقترح هذه المساهمة إدخال تعديلات صياغية على القرار 50 (المراجَع في دبي، 2012) لتحديث النص وفقاً للقرار 130 (المراجَع في بوسان، 2014) والقرار 45 (المراجَع في دبي، 2014). وستساعد هذه التعديلات على ضمان أن يعكس القرار الوضع العالمي الراهن في مجال بناء الثقة والأمن في استخدام تكنولوجيات المعلومات والاتصالات وأن تكون مساهمة قطاع تقييس الاتصالات في هذا الموضوع متماشية مع الأهداف والأولويات التي اتفق عليها الأعضاء. | **ملخص**: |

مقدمة

تشكل تكنولوجيات المعلومات والاتصالات (ICT) جزءاً لا يتجزأ من التنمية الاقتصادية والاجتماعية. والأمن عنصر أساسي لتشغيل هذه التكنولوجيات واستخدامها ويقتضي أن يكون جميع الأشخاص المعنيين على وعي بالأمور الأمنية وأن يتخذوا إجراءات تلائم دورهم. وبما أن استخدام تكنولوجيا المعلومات والاتصالات آخذ في النمو، فإن الأمن السيبراني لا يزال يشكل أولوية بين أعضاء الاتحاد. وخلال السنوات الأربع الماضية، واصلت لجنة الدراسات 17 لقطاع تقييس الاتصالات عملها في هذا المجال، شأنها شأن العديد من المنظمات والاتحادات الأخرى لوضع المعايير على الصعيد الوطني والإقليمي والدولي. وإضافةً إلى ذلك، وافق مؤتمر المندوبين المفوضين للاتحاد لعام 2014 والمؤتمر العالمي لتنمية الاتصالات لعام 2014 على الأهداف والأولويات في مجال بناء الثقة والأمن في استخدام تكنولوجيات المعلومات والاتصالات التي يُنتظر أن يساهم فيها قطاع تقييس الاتصالات. ومن ثم، ترى لجنة البلدان الأمريكية للاتصالات أن من المهم تحديث القرار 50 لضمان تماشيه مع هذه التطورات.

وقد أضحى الأمن السيبراني محل اهتمام للخبراء، ومنهم الاتحاد الدولي للاتصالات والمستخدمون والدول بوجه خاص.

ومنذ انعقاد آخر جمعية حتى اليوم لم تكتسب قضايا الأمن السيبراني طابع الاستمرارية فحسب، بل زادت أهميتها أيضاً من حيث استلزام انتباه ومشاركة قطاع تكنولوجيات المعلومات والاتصالات. ولهذا السبب، يُحتفظ بهذا القرار وأحكامه نظراً إلى أهميته كعنصر أساسي فيما يتعلق بالتقييس وكصك بارز للاتحاد وأعضائه.

وتقدم جمهورية الأرجنتين هذا المقترح للتعديل، إذ ترى أنه يتعين الإبقاء على أحكام القرار، وتقترح في المقابل تحديثها لإدراج العناصر الجديدة المتعلقة بالأمن السيبراني الناجمة عن الاتجاهات في بعض المجالات الناشئة وخاصةً عن التهديدات الجديدة. ونقترح كذلك إدراج العناصر المستمدة من المؤتمر العالمي الأخير لتنمية الاتصالات لعام 2014 (WTDC‑14) الذي وافق على مساهمة قطاع تنمية الاتصالات في الخطة الاستراتيجية للاتحاد للفترة 2019‑2016 بتأييد خمسة أهداف من بينها الهدف 3 - تعزيز الثقة والأمن في استخدام الاتصالات/تكنولوجيا المعلومات والاتصالات وكذلك تعزيز نشر تطبيقات وخدمات تكنولوجيا المعلومات والاتصالات؛ والنتيجة 1.3 للهدف المذكور: تحسين الثقة والأمن في استخدام تكنولوجيات المعلومات والاتصالات والخدمات، ويتمثل الإطار التنفيذي للهدف والنتيجة المذكورين في برنامج الأمن السيبراني.

ومن بين العناصر والمجالات الناشئة الجديدة، يمكننا الإشارة إلى القيمة المتزايدة التي يوليها المستعملون و/أو الأجهزة للمهاجمين نظراً لتنامي مستوى التوصيل البيني المادي وتبادل المعلومات، ما أدى إلى ظهور استعمالات جديدة من قبيل العمليات المصرفية الإلكترونية والإقرارات الموثقة وتطبيقات الهواتف الذكية بشكل أساسي.

وعلى نحو مماثل، أدى التقدم والتطور اللذان تشهدهما إنترنت الأشياء حالياً إلى توقعات واسعة النطاق من حيث الأجهزة والأنشطة، وفي الوقت نفسه من حيث التهديدات.

المقترح

تقترح لجنة البلدان الأمريكية للاتصالات مراجعة القرار 50 (المراجَع في دبي، 2012) لتحديث النص وفقاً للقرار 130 (المراجَع في بوسان، 2014) والقرار 45 (المراجَع في دبي، 2014)، وكي يعبر عن الوضع العالمي الراهن في مجال بناء الثقة والأمن في استخدام تكنولوجيات المعلومات والاتصالات.

MOD IAP/46A19/1

القـرار 50 (المراجَع في الحمامات، 2016)

الأمن السيبراني

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

إن الجمعية العالمية لتقييس الاتصالات (الحمامات، 2016)،

إذ تشير إلى

*أ )* القرار 130 (المراجَع في بوسان، 2014) لمؤتمر المندوبين المفوضين، بشأن 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 بوسان، 2014) 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 45 (المراجَع في دبي، 2012) الصادر عن المؤتمر العالمي لتنمية الاتصالات (WTDC)؛

*ي)* القرار 52 (المراجَع في دبي، 2012) لهذه الجمعية، بشأن مكافحة الرسائل الاقتحامية والتصدي لها؛

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

وإذ تضع في اعتبارها

*أ )* الأهمية الحاسمة للبنية التحتية لتكنولوجيا المعلومات والاتصالات 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 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 )* وقوع حوادث سيبرانية ناجمة عن هجمات سيبرانية، مثل التدخلات الخبيثة أو تدخلات الباحثين عن المغامرة باستخدام البرمجيات الضارة (مثل الديدان والفيروسات) الموزعة بطرق مختلفة مثل التوزيع عبر الإنترنت والحواسيب المصابة بالبرمجيات الروبوتية؛ وأن عدد وأساليب التهديدات والهجمات السيبرانية يتزايد كما يزيد الاعتماد على الإنترنت وغيرها من الشبكات الأساسية للنفاذ إلى الخدمات والمعلومات؛

*و )* 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 لتحديد حوادث الأمن السيبراني والتأهب لها والتصدي لها والتعافي منها؛

*ز )* أن قطاع تقييس الاتصالات عليه أن يؤدي دوراً في إطار ولايته واختصاصاته فيما يتعلق بالفقرة *و)* 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؛

*ج)* أن لقطاع تقييس الاتصالات واللجنة التقنية الأولى (JTC 1) المشتركة بين المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC) وكذلك العديد من الاتحادات وكيانات وضع المعايير مثل اتحاد شبكة الويب العالمية (W3C) ومنظمة النهوض بمعايير المعلومات المنسقة (OASIS) وفريق مهام هندسة الإنترنت ومعهد مهندسي الكهرباء والإلكترونيات وغير ذلك، مجموعة هامة من المواد المنشورة والأعمال الجارية التي لها صلة مباشرة بهذا الموضوع والتي ينبغي مراعاتها،

وإذ تقر

*أ )* بالنواتج ذات الصلة للقمة العالمية لمجتمع المعلومات (WSIS) التي حددت الاتحاد الدولي للاتصالات بصفته منسقاً ومسهلاً لخط العمل جيم5 (بناء الثقة والأمن في استعمال تكنولوجيات المعلومات والاتصالات)؛

*ب)* بأحكام الفقرة *يقرر* من القرار 130 (المراجَع في بوسان، 2014) لمؤتمر المندوبين المفوضين القاضية بتعزيز دور الاتحاد في بناء الثقة والأمن في استعمال تكنولوجيات المعلومات والاتصالات، والتكليف الداعي إلى تكثيف العمل بأولوية عالية ضمن لجان الدراسات التابعة لقطاع تقييس الاتصالات بالاتحاد؛

*ج)* بأن المؤتمر العالمي لتنمية الاتصالات لعام 2014 وافق على المساهمة في الخطة الاستراتيجية للاتحاد للفترة 2016-2019 بتأييد خمسة أهداف من بينها الهدف 3 – *تعزيز الثقة والأمن في استخدام الاتصالات/تكنولوجيا المعلومات والاتصالات وكذلك تعزيز نشر تطبيقات وخدمات تكنولوجيا المعلومات والاتصالات؛* والنتيجة 3. 1للهدف المذكور: *تحسين الثقة والأمن في استخدام تكنولوجيات المعلومات والاتصالات والخدمات*، ويتمثل الإطار التنفيذي للهدف والنتيجة المذكورين في برنامج الأمن السيبراني وفي المسألة 3/2 لقطاع تنمية الاتصالات (ITU-D)؛

*د )* بالبرنامج العالمي للأمن السيبراني الصادر عن الاتحاد الذي يعزز التعاون الدولي الرامي إلى اقتراح استراتيجيات للتوصل إلى حلول تعزز الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات،

وإذ تقر كذلك

*أ )* بأن موجِّهات الهجمات السيبرانية مثل التدليس والاحتيال والمسح/التدخل، وعمليات رفض الخدمة الموزعة، وتغيير واجهة الويب والنفاذ غير المخول به إلخ.، لها 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 (مثل الهجمات باستخدام عناوين بروتوكول الإنترنت المزورة)؛

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

*ﻫ )* بأنه وفقاً للقرار 181 (غوادالاخارا، 2010) لمؤتمر المندوبين المفوضين، من المعترف به أنه من الضروري دراسة مسألة المصطلحات المتصلة ببناء الثقة والأمن في استخدام تكنولوجيات المعلومات والاتصالات، وأن هذه المجموعة الأساسية يجب أن تتضمن مسائل هامة أخرى بالإضافة إلى الأمن السيبراني وأن تعريف الأمن السيبراني قد يحتاج إلى التعديل من وقت إلى آخر لإبراز التغيرات في مجال السياسة العامة؛

*و )* بأن القرار 181 (غوادالاخارا، 2010) لمؤتمر المندوبين المفوضين ينص على مراعاة تعريف الأمن السيبراني المعتمد في التوصية ITU‑T X.1205 لاستعماله في أنشطة الاتحاد المتعلقة ببناء الثقة والأمن في استعمال تكنولوجيات المعلومات والاتصالات؛

*ز )* بأن لجنة الدراسات 17 لقطاع تقييس الاتصالات مسؤولة عن إعداد التوصيات الأساسية بشأن أمن الاتصالات وتكنولوجيا المعلومات والاتصالات وفقاً لما يقره القرار 181 (غوادالاخارا، 2010) لمؤتمر المندوبين المفوضين،

وإذ تلاحظ

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

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

*ج)* أن من شأن التنسيق والتعاون بين المنظمات العاملة على قضايا الأمن تعزيز التقدم والمساهمة في بناء ثقافة الأمن السيبراني والحفاظ عليها؛

*د )* الجهود الكبيرة التي يبذلها ويتعاون على بذلها كلٌّ من الحكومات والقطاع الخاص والمجتمع المدني والأوساط التقنية والهيئات الأكاديمية من أجل بناء الثقة والأمن في استعمال تكنولوجيات المعلومات والاتصالات،

تقـرر

1 أن تواصل جميع لجان دراسات قطاع تقييس الاتصالات تقييم التوصيات القائمة والتوصيات الجديدة الناشئة، وخاصة توصيات بروتوكولات التشوير والاتصالات، وأن ينصبّ هذا التقييم على سلامة تصميمها واحتمالات قيام أطراف خبيثة باستغلالها من أجل التدخل المدمر فيما يتعلق بنشرها في البنية التحتية العالمية للمعلومات والاتصالات، وأن تعد توصيات جديدة فيما يتعلق بقضايا الأمن المستجدة وتأخذ بعين الاعتبار الخدمات والتطبيقات الجديدة التي ينبغي أن تدعمها البنية التحتية العالمية للاتصالات/تكنولوجيا المعلومات والاتصالات (مثل الحوسبة السحابية والشبكات الذكية وأنظمة النقل الذكية التي تقوم على شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات)؛

2 أن يواصل قطاع تقييس الاتصالات، في إطار عمله ونفوذه، نشر الوعي بالحاجة إلى تمتين أنظمة المعلومات والاتصالات والدفاع عنها من التهديدات والهجمات السيبرانية، ويواصل تعزيز التعاون بين المنظمات الدولية والإقليمية الملائمة من أجل تعزيز تبادل المعلومات التقنية في ميدان أمن شبكات المعلومات والاتصالات؛

3 أن يعمل قطاع تقييس الاتصالات بتعاون وثيق مع قطاع تنمية الاتصالات، لا سيما في سياق المسألة 3/2؛

4 أنه لدى تقييم الشبكات والبروتوكولات فيما يتعلق بمواطن الضعف المتعلقة بالأمن وتسهيل تبادل معلومات الأمن السيبراني؛ ينبغي مراعاة وتطبيق توصيات قطاع تقييس الاتصالات، بما فيها توصيات السلسلة ITU‑T X وإضافاتها ومنها التوصيات ITU‑T X.805 وITU‑T X.1205 وITU‑T X.1500، ومعايير المنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية وغيرها من النواتج الأخرى ذات الصلة الصادرة عن المنظمات الأخرى، حسب الاقتضاء؛

5 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؛

6 دعوة الأطراف المعنية إلى العمل معاً من أجل وضع معايير ومبادئ توجيهية للحماية من التهديدات والهجمات السيبرانية ولتسهيل اقتفاء أثر مصدر الهجمات؛

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

8 أن تواصل جميع لجان الدراسات التابعة لقطاع تقييس الاتصالات عملها لتزويد الفريق الاستشاري لتقييس الاتصالات (TSAG) بانتظام بتقارير بشأن أمن الاتصالات/تكنولوجيا المعلومات والاتصالات فيما يتعلق بالتقدم المحرز في تقييم التوصيات القائمة والتوصيات الجديدة الناشئة؛

9 أن تواصل لجان الدراسات التابعة لقطاع تقييس الاتصالات إقامة الاتصال مع المنظمات المعنية بوضع المعايير (SDO) وغيرها من الهيئات النشطة في هذا المجال، مثل اللجنة التقنية الأولى المشتركة بين المنظمة الدولية للتوحيد القياسي واللجنة الكهرتقنية الدولية، ومنظمة التعاون والتنمية في الميدان الاقتصادي (OECD) وفريق العمل المعني بالاتصالات والمعلومات التابع لرابطة التعاون الاقتصادي لآسيا والمحيط الهادئ (APEC‑TEL) وفريق مهام هندسة الإنترنت (IETF)؛

10 أن تواصل لجنة الدراسات 17 عملها بشأن المسائل المثارة في القرار 130 (المراجَع في بوسان، 2014) لمؤتمر المندوبين المفوضين، وبشأن توصيات السلسلة ITU-T X لقطاع تقييس الاتصالات بما فيها الإضافات حسب الاقتضاء،

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 الأخرى ذات الصلة، الاحتفاظ بقائمة محدثة للمبادرات والأنشطة الوطنية والإقليمية والدولية الرامية إلى تعزيز المواءمة العالمية للاستراتيجيات والنهج إلى أقصى الحدود الممكنة في هذه المجالات ذات الأهمية البالغة؛

2 بأن يقدم تقريراً سنوياً إلى مجلس الاتحاد، على النحو المحدد في القرار 130 (المراجَع في بوسان، 2014) لمؤتمر المندوبين المفوضين، بشأن التقدم المحرز في الإجراءات المبينة أعلاه؛

3 بمواصلة الاعتراف بالدور الذي تؤديه المنظمات الأخرى ذات الخبرات والتجارب في مجال معايير الأمن والتنسيق مع هذه المنظمات حسب الاقتضاء،

تكلف مدير مكتب تقييس الاتصالات كذلك

1 بمواصلة متابعة أنشطة القمة العالمية لمجتمع المعلومات (WSIS) بشأن بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات، بالتعاون مع أصحاب المصلحة المعنيين وذلك كسبيل من سبل تبادل المعلومات على الصعيد العالمي بشأن المبادرات الوطنية والإقليمية والدولية وغير التمييزية المتعلقة بالأمن السيبراني؛

2 بالتعاون مع مكتب تنمية الاتصالات، فيما يتعلق بأي بند يخص الأمن السيبراني وفقاً للقرار 45 (المراجَع في دبي، 2012) للمؤتمر العالمي لتنمية الاتصالات؛

3 بدعم المشاريع الإقليمية والعالمية المتعلقة بالأمن السيبراني من قبيل المنتدى العالمي لفرق الاستجابة للطوارئ وأمن المعلومات (FIRST) ومنظمة الدول الأمريكية (OAS) وفريق الاستجابة للطوارئ الحاسوبية لمنطقة آسيا والمحيط الهادئ (APCERT) وفريق الاستجابة للحوادث الحاسوبية لمنطقة أمريكا اللاتينية والكاريبي (LAC-CSIRT) وغير ذلك، ودعوة جميع البلدان، ولا سيما البلدان النامية، إلى المشاركة في هذه الأنشطة، مع أخذ القرار 45 (المراجَع في دبي، 2012) في الاعتبار،

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

إلى التعاون والمشاركة بفعالية في تنفيذ هذا القرار والإجراءات المرتبطة به.

\_\_\_\_\_\_\_\_\_\_\_

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