|  |  |  |
| --- | --- | --- |
| itu_logo | **الجمعية العالمية لتقييس الاتصالات (WTSA-16)****الحمامات، 25 أكتوبر - 3 نوفمبر 2016** | CCITT/ITU-T 60th Anniversary logo |
|  |  |  |
|  |  |
| الجلسة العامة | الإضافة 21للوثيقة 43-A |
|  | 9 أكتوبر 2016 |
|  | الأصل: بالإنكليزية |
|  |
| إدارات الدول العربية |
| مقترح لتعديل القرار 50 - الأمن السيبراني |
|  |

|  |  |
| --- | --- |
| تقترح إدارات الدول العربية تعديل القرار 50 على النحو المبين في هذه الوثيقة. | **ملخص:** |

MOD ARB/43A21/1

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 (المراجَع في بوسان، 2014) 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، 2014) 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 دبي، 2012) لهذه الجمعية، بشأن تشجيع إنشاء أفرقة وطنية للتصدي للحوادث الحاسوبية لا سيما في البلدان النامية[[1]](#footnote-1)؛

*ل)* أن الاتحاد هو جهة التيسير الرئيسية لخط العمل جيم5 الوارد في برنامج عمل تونس بشأن مجتمع المعلومات (بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات)؛

*م )* الأحكام المتصلة بالأمن السيبراني في التزام تونس وفي برنامج عمل تونس؛

*ن)* أن الاتحاد الدولي للاتصالات ومكتب الأمم المتحدة المعني بالمخدرات والجريمة وقّعا مذكرة تفاهم (MoU) بهدف تعزيز الأمن في استخدام تكنولوجيا المعلومات والاتصالات،

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 )* أن الخسائر الهائلة والمتزايدة التي يتكبدها مستعملو أنظمة الاتصالات/تكنولوجيا المعلومات والاتصالات نتيجة تفاقم مشكلة الأمن السيبراني وأعمال التخريب المتعمدة على صعيد العالم، تهدد جميع البلدان المتقدمة والنامية في العالم دون استثناء؛

*و )* أن واقع التوصيل ما بين البنى التحتية الحيوية للاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد العالمي يعني، من جملة أمور، أن ضعف أمن البنية التحتية في بلدٍ ما قد يؤدي إلى مزيد من مواطن الضعف والمخاطر في البلدان الأخرى؛

*ز )* 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؛

*ﺡ)* 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 للحماية من الحوادث الضارة وأشكالها المختلفة؛

*ﻁ)* أن قطاع تقييس الاتصالات عليه أن يؤدي دوراً في إطار ولايته واختصاصاته فيما يتعلق بالفقرة *إذ تضع في اعتبارها* *و )*،

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 بين المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC) 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)* بالبرنامج 2 بشأن الأمن السيبراني وتطبيقات تكنولوجيا المعلومات والاتصالات والقضايا المتصلة بالشبكات القائمة على بروتوكول الإنترنت الذي اعتمده المؤتمر العالمي لتنمية الاتصالات (WTDC) (المراجَع في دبي، 2014) والذي يشمل الأمن السيبراني بوصفه أحد الأنشطة ذات الأولوية والأنشطة ذات الصلة التي ينبغي لمكتب تنمية الاتصالات (BDT) تنفيذها، وأن المسألة 22/1 لقطاع تنمية الاتصالات تتناول قضية تأمين شبكات المعلومات والاتصالات عن طريق تحديد أفضل الممارسات الهادفة إلى تطوير ثقافةٍ للأمن السيبراني، واعتماد القرار 45 (المراجَع في دبي، 2014)، بشأن آليات تعزيز التعاون في مجال الأمن السيبراني، بما في ذلك مكافحة الرسائل الاقتحامية والتصدي لها؛

*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؛

*ه )* بضرورة اتخاذ الإجراءات المناسبة والتدابير الوقائية على المستوى الدولي ضد إساءة استعمال الفضاء السيبراني بما في ذلك شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات، وضرورة مكافحة الإرهاب بجميع أشكاله ومظاهره في الفضاء السيبراني بما في ذلك شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات، وأهمية أمن شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات واستمرارها واستقرارها، وضرورة حماية هذه الشبكات من التهديدات ومواطن الضعف (الفقرة 45 من برنامج عمل تونس)، مع ضمان احترام الخصوصية وحماية المعلومات والبيانات الشخصية؛

*و )* بدور الاتحاد في حماية الأطفال وفي تعزيز تنميتهم، وضرورة تعزيز العمل من أجل حماية الأطفال والشباب من الاستغلال والدفاع عن حقوقهم في سياق الاتصالات/تكنولوجيا المعلومات والاتصالات، مع التأكيد أن تحقيق المصلحة القصوى للأطفال اعتبار أساسي؛

*ز )* بأهمية جعل "الأمن كجزء أساسي من التصميم" النهج التلقائي عند وضع المعايير؛

*ح)* بأن التوصية ITU‑T X.1255 لتي تستند إلى معمارية الأشياء الرقمية (DOA)، توفر إطاراً لاكتشاف معلومات إدارة الهوية؛

*ط)* بأن نظام "Handle" الذي هو أحد مكونات معمارية الأشياء الرقمية، يوفر خدمة معرّف هوية آمنة تشمل آلية ضمنية لحماية سلامة الخدمة وسرية البيانات وتوفر وظائف الإدارة القائمة بذاتها وأن التحكم في التغييرات يتم باستخدام البنية التحتية للمفاتيح العمومية (PKI) القائمة بذاتها أيضاً في النظام،

وإذ تقر كذلك

 *أ )* بأن الهجمات 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 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/تكنولوجيا 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 تكنولوجيا 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 تكنولوجيا 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، لجنة الدراسات الرائدة المعنية بالأمن، وغيرها من هيئات التقييس، بما فيها مجموعة التعاون لوضع معايير عالمية؛

*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 )* أن لجنة الدراسات 17 لقطاع تقييس الاتصالات تقوم بدراسة إمكانية إنشاء مركز وطني لأمن الشبكات العمومية القائمة على بروتوكول الإنترنت لفائدة البلدان النامية، وفقاً لما يقره القرار 130 (المراجَع في بوسان، 2014) لمؤتمر المندوبين المفوضين، وأن بعض الأعمال قد أنجزت في هذا المجال بما في ذلك سلسلة التوصيات ITU‑T X.800 - ITU‑T X.849 وإضافاتها،

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 البينة 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 الدفاع عن أنظمة المعلومات والاتصالات ضد مخاطر الهجمات السيبرانية ومواصلة 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 22/1؛

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 الهجمات 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 وفريق العمل المعني بالاتصالات والمعلومات التابع لرابطة التعاون الاقتصادي لآسيا والمحيط الهادئ، وفريق مهام هندسة الإنترنت وسلطة الترقيم للأشياء الرقمية (DONA)؛

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؛

11 أن تواصل لجنة الدراسات 3 عملها بشأن وضع التوصيات والورقات التقنية والمنشورات الأخرى المتصلة بالقضايا السياساتية والتنظيمية والاقتصادية وآثارها مع مراعاة التكنولوجيات الناشئة بما في ذلك البيانات الضخمة والحوسبة السحابية وإنترنت الأشياء (IoT)؛

12 جعل "الأمن كجزء أساسي من التصميم" النهج المفترض عند وضع معايير قطاع تقييس الاتصالات،

تكلف مدير مكتب تقييس الاتصالات

1 بأن يقوم، 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، بإعداد جرد للمبادرات والأنشطة الوطنية والإقليمية والدولية الرامية، بهدف 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، 2014) للمؤتمر العالمي لتنمية الاتصالات؛

3 بمواصلة التعاون مع برنامج الأمن السيبراني العالمي للأمين العام ومع الشراكة الدولية متعددة الأطراف لمكافحة التهديدات السيبرانية (الاتحاد الدولي للاتصالات – إمباكت)، ومشروع FIRST وغيرها من المشاريع العالمية والإقليمية الأخرى، 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؛

4 بالعمل بشكل تعاوني مع مديري المكتبين الآخرين تماشياً مع القرار 130 (المراجَع في بوسان، 2014) لدعم الأمين العام في إعداد وثيقة تتعلق بمذكرة تفاهم محتملة (وفقاً للقرار 45 (المراجَع في دبي، 2014) للمؤتمر العالمي لتنمية الاتصالات) بين الدول الأعضاء المهتمة لتعزيز الأمن السيبراني ومكافحة التهديدات السيبرانية من أجل حماية البلدان النامية وأي بلد يهتم بالانضمام إلى هذه المذكرة المحتملة،

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)