|  |  |  |
| --- | --- | --- |
|  | الجمعية العالمية لتقييس الاتصالات (WTSA-24)نيودلهي، 24-15 أكتوبر 2024 |  |
|  |  |
|  |  |
| الجلسة العامة | ‏الإضافة 10‏للوثيقة ‎37-A‏ |
|  | 22 سبتمبر 2024 |
|  | الأصل: بالإنكليزية |
|  |
| إدارات أعضاء جماعة آسيا والمحيط الهادئ للاتصالات |
| تعديل يُقترح إدخاله على القرار 50 |
|  |
|  |

|  |  |
| --- | --- |
| **ملخص:** | تتضمن هذه الوثيقة مقترح تعديل القرار 50 للجمعية العالمية لتقييس الاتصالات (WTSA) بشأن "الأمن السيبراني". |
| **للاتصال:** | السيد Masanori Kondoالأمين العاملجماعة آسيا والمحيط الهادئ للاتصالات | البريد الإلكتروني: aptwtsa@apt.int |

مقدمة

إن أهمية الأمن للبنية التحتية الحالية للاتصالات/تكنولوجيا المعلومات والاتصالات (ICT) آخذة في التزايد أكثر فأكثر. ولقطاع تقييس الاتصالات بالاتحاد (ITU-T) دور في إعداد توصيات تقنية بالغة الأهمية بشأن دعم بناء الاطمئنان والثقة والأمن فيما يتعلق باستخدام تكنولوجيا المعلومات والاتصالات. وتوفير الأمن من قبل تكنولوجيا المعلومات والاتصالات وضمان الأمن لها مجالان دراسيان رئيسيان على السواء.

وينبغي إيلاء اعتبار لعنصر الأمن في جميع مراحل دورة حياة النظام/الشبكة/التطبيق، وإلا استشرَت فيها مواطن ضعف يلزمها الكثير من الأعمال التصحيحية.

وبالنظر إلى إسهام أنشطة تقييس الأمن في منع الأضرار الناجمة عن الأنشطة السيبرانية الضارة، فينبغي مواصلة الأعمال المتعلقة بموضوع الأمن. إضافةً إلى ذلك، ينبغي للجان الدارسات بقطاع تقييس الاتصالات، خاصة لجنة الدراسات 17، بحث التكنولوجيات الأمنية الناشئة التي سبق تحديدها كأمن الذكاء الاصطناعي (AI)، وأمن الميتافيرس، والأمن القائم على نهج انعدام الثقة، وأمن سلاسل إمداد البرمجيات، وغيرها من التكنولوجيات.

والهدف الرئيسي من هذا التعديل توضيح وتعزيز دور لجنة الدراسات 17 بوصفها لجنة الدراسات الرئيسية المعنية بموضوع الأمن.

المقترح

استناداً إلى الخلفية المقدمة أعلاه، تقترح الإدارات الأعضاء في جماعة آسيا والمحيط الهادئ (APT) على الجمعية العالمية لتقييس الاتصالات عام 2024 (WATSA-24) النظر في مراجعة القرار 50 الصادر عنها بشأن "الأمن السيبراني".

MOD APT/37A10/1

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 تعزيز 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 68/167 الصادر عن الجمعية العامة للأمم المتحدة، بشأن الحق في الخصوصية في العصر الرقمي، الذي يؤكد جملة مسائل من بينها أن "الحقوق نفسها التي يتمتع بها الأشخاص خارج الإنترنت يجب أن تحظى بالحماية أيضاً على الإنترنت، بما في ذلك الحق في الخصوصية"؛

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

*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 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؛

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

*م )* 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؛

*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 الاطمئنان والثقة والأمن في استعمال 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 إنترنت الأشياء (IoT) والمدن والمجتمعات الذكية (SC&C) بما في ذلك الجوانب الأمنية للتكنولوجيات الجديدة والناشئة؛

*ي)* 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؛

*ك)* العمل المضطلَع به والجاري في الاتحاد، بما فيه عمل لجنة الدراسات 17 لقطاع تقييس الاتصالات، ولجنة الدراسات 2 لقطاع تنمية الاتصالات، وبما في ذلك التقرير النهائي للمسألة 22/1-1 للجنة الدراسات 1 لقطاع تنمية الاتصالات، وفي إطار خطة عمل دبي التي اعتمدها المؤتمر العالمي لتنمية الاتصالات (دبي، 2014)؛

*ل)* 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 تتعلق بالأمن السيبراني؛

*ب)* أن التوصية ITU‑T X.805 تقدم إطاراً منهجياً لتحديد نقاط الضعف الخاصة بالأمن وأن التوصية ITU‑T X.509 تقدم إطاريْ المفاتيح العمومية وشهادة النعوت، 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 التوصية ITU‑T X.1060 تقدم إلى المنظمات إطاراً لبناء وإدارة مركز للدفاع السيبراني (CDC) يُفعِّل القدرة الأمنية للمنظمة، ولتقييم مدى فعالية هذا المركز في تنفيذ الخدمات الأمنية ومعالجة ما تواجهه المنظمة من مخاطر أمنية سيبرانية؛

*د )* 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) وتحالف الهوية السريعة على الإنترنت (FIDO) وفريق مهام هندسة الإنترنت (IETF) ومعهد مهندسي الكهرباء والإلكترونيات (IEEE)، وجِهات أُخرى، مجموعة هامة من المواد المنشورة والأعمال الجارية التي لها صلة مباشرة بهذا الموضوع والتي ينبغي مراعاتها؛

*هـ )* أهمية العمل الجاري بشأن المعمارية المرجعية الأمنية لإدارة بيانات الأعمال التجارية الإلكترونية طيلة دورة حياتها،

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، بما في ذلك الغاية الاستراتيجية 1 (التوصيلية الشاملة: إتاحة وتعزيز النفاذ الشامل إلى اتصالات/تكنولوجيا معلومات واتصالات ميسورة التكلفة وعالية ومأمونة)، التي ينبغي أن يحقق الاتحاد في إطارها بنية تحتية وخدمات وتطبيقات للاتصالات/تكنولوجيا المعلومات والاتصالات (ICT) يمكن للجميع النفاذ إليها بتكلفة ميسورة وتتسم بعلو الجودة والقابلية للتشغيل البيني والمأمونية؛

*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، وبأحكام القرار 44 (المراجَع في جنيف، 2022) للجمعية العالمية لتقييس الاتصالات، بشأن سد الفجوة التقييسية بين البلدان النامية والبلدان المتقدمة؛

*هـ )* بالتحديات التي تواجهها الدول الأعضاء، لا سيما الدول النامية، في بناء بنى تحتية وتطبيقات موثوقة ومأمونة للاتصالات/تكنولوجيا المعلومات والاتصالات فيما يتعلق بالجوانب التقنية والتشغيلية لحماية البيانات وحماية المعلومات المحدِّدة للهوية الشخصية (PII)،

وإذ تقر كذلك

 *أ )* بأن الهجمات السيبرانية مثل التدليس والرسائل الاقتحامية والاحتيال والمسح/التدخل، وعمليات رفض الخدمة الموزعة، والتهديد المتقدم المستعصي، وتغيير واجهة الويب، والنفاذ غير المخول به، والبرمجيات الضارة، وتسميم البيانات، وهجمة انتحال الشخصية، 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؛

*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 على النحو الملائم لمنع الهجمات الموجهة إلى الأجهزة الطرفية؛

*ﻫ )* بأن هجمات برمجيات طلب الفدية ما زالت تتنامى؛

*و )* بأن تطبيق التكنولوجيات الجديدة في ظل دوام تطور البنية التحتية العالمية للاتصالات/تكنولوجيا المعلومات والاتصالات يطرح تحديات جديدة ويستلزم زيادة المتطلبات المتعلقة بأمن الاتصالات/تكنولوجيا المعلومات والاتصالات وبالجوانب التقنية والتشغيلية لحماية البيانات وحماية المعلومات المحدِّدة للهوية الشخصية (PII)، الأمر الذي قد يؤثر على المعمارية الأمنية للشبكة؛

*ز )* بتقدم التكنولوجيات في مجال إدارة التهديدات الأمنية السيبرانية وحماية الاتصالات/تكنولوجيا المعلومات والاتصالات؛

*ح)* بالحاجة إلى تطوير القدرات الأمنية بما يشمل تنمية قدرات العاملين فيما يتعلق بإدارة المخاطر الأمنية والتكنولوجيات الأمنية؛

*ط)* بأن تأمين البنية التحتية لكل من البيانات والبيانات الضخمة مكوِّن رئيسي في الأمن السيبراني ذلك أنه عادةً ما تكون البيانات هدف الهجمات السيبرانية، بينما اتساع تطبيق تكنولوجيا البيانات الضخمة يجعل هذا الهدف شديد الانتشار في سلوكيات الشبكات الحالية؛

*ي)* بأن الأمن السيبراني عنصر رئيسي لبناء الاطمئنان والثقة والأمن في استعمال الاتصالات/تكنولوجيا المعلومات والاتصالات؛

*ك)* بأن الأمن يحتل مكانة مهمة في جميع مراحل دورات حياة الأنظمة والشبكات والتطبيقات والبيانات؛

*ل)* بأن المعمارية والإطار الأمنيين مهمان كما يمكن أن يعتبرا أساس تصميم المعمارية الأمنية في مختلف الأنظمة والشبكات والتطبيقات والبيانات،

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 تقييم جانب إمكانية التشغيل البيني والجوانب الأمنية للبنية التحتية للشبكة المتطورة، والابتكار السريع في مجال تطوير البنية التحتية للشبكة المفتوحة؛

*ج)* أنه قد نشأت، بالإضافة إلى التهديدات السيبرانية، جوانب تقنية وتشغيلية لحماية البيانات وكذلك المعلومات المحدِّدة للهوية الشخصية (PII) تمثل مشكلة كبيرة للدول الأعضاء؛

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

*هـ )* الجهود الكبيرة والتعاونية التي تبذلها الحكومات والقطاع الخاص والمجتمع المدني والأوساط التقنية والأكاديمية، كل في نطاق دوره ومسؤولياته، من أجل بناء الاطمئنان والثقة 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، وفقاً لولاية كل منها المحدَّدة في القرار 2 (المراجَع في جنيف، 2022) لهذه الجمعية، مع مراعاة المسائل الأمنية في جميع مراحل كامل عملية تطوير معايير القطاع، وأن ينصبّ هذا التقييم على سلامة تصميمها وعملها، 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 (بما في ذلك، على سبيل المثال لا الحصر، الحوسبة السحابية والشبكات الذكية وأنظمة النقل الذكية التي تقوم على شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات)؛

3 أن يواصل قطاع تقييس الاتصالات، في إطار ولايته واختصاصاته، نشر الوعي عالمياً فيما يتعلق بأمن تكنولوجيا المعلومات والاتصالات بالحاجة إلى تقوية أنظمة المعلومات والاتصالات وتحصينها من التهديدات والهجمات السيبرانية والأنشطة السيبرانية الخبيثة، وزيادة تنمية قدرات العاملين فيما يخص الأمن، ومواصلة تعزيز التعاون بين المنظمات الدولية والإقليمية الملائمة من أجل تعزيز تبادل المعلومات التقنية في مجال أمن شبكات المعلومات والاتصالات، وذلك بإعداد توصيات، وتقارير تقنية، تدعم الإجراءات الأمنية السيبرانية والسياسات والأطر التقنية في مجال الأمن السيبراني؛

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 والأطر التقنية في مجال الأمن السيبراني، بهدف تحسين إدارة مخاطر الأمن السيبراني وحماية شبكات المعلومات والاتصالات؛

5 أن يعمل قطاع تقييس الاتصالات 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 تواكب لجان دراسات قطاع تقييس الاتصالات ذات الصلة تطور التكنولوجيات الجديدة والناشئة، وفقاً لاختصاصاتها، من أجل توجيه انتباه لجنة الدراسات 17 إلى المجالات التي تتطلب وضع توصيات وإضافات وتقارير تقنية جديدة لمواجهة التحديات المتعلقة بالأمن والجوانب التقنية والتشغيلية لحماية البيانات وكذلك المعلومات المحدِّدة للهوية الشخصية (PII)؛

7 أن يواصل قطاع تقييس الاتصالات العمل على وضع وتحسين المصطلحات والتعاريف المتصلة ببناء الاطمئنان والثقة (بسبل منها حماية البيانات وحماية المعلومات المحدِّدة للهوية الشخصية (PII)) والأمن في استخدام الاتصالات/تكنولوجيا المعلومات والاتصالات، بما فيها مصطلح الأمن السيبراني؛

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

9 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؛

10 أنه ينبغي تطوير شبكات وخدمات للاتصالات/تكنولوجيا المعلومات والاتصالات تتسم بالأمن والموثوقية والقدرة على الصمود، وصيانتها لتعزيز الاطمئنان والثقة في استخدام الاتصالات/تكنولوجيا المعلومات والاتصالات؛

11 أن لجنة الدراسات 17 بحاجة إلى وضع أطر تعاونية للتحليل الأمني السيبراني وإدارة الحوادث؛

12 أن تُعتبر قدرة شبكات وأنظمة تكنولوجيا المعلومات والاتصالات على الصمود أولوية في تطوير البنى التحتية لشبكات الاتصالات/تكنولوجيا المعلومات والاتصالات، وتطبيقاتها،

تُكلّف لجنة الدراسات 17

1 بتشجيع الدراسات المتعلقة بالأمن السيبراني بما في ذلك أمن البيانات وكذلك المعلومات المحدِّدة للهوية الشخصية وجوانبهما التقنية والتشغيلية في الخدمات والتكنولوجيات الجديدة والناشئة للتصدي لمواطن الضعف فيما يتعلق باستخدام البنية التحتية العالمية للاتصالات/تكنولوجيا المعلومات والاتصالات، وذلك بإعداد توصيات، وإضافات، وتقارير تقنية، 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 بالجوانب الأمنية والتقنية والتشغيلية لحماية البيانات وحماية المعلومات المحدِّدة للهوية الشخصية، وخلاصة وافية عن الأمن ينبغي أن تشمل قائمة التوصيات والمصطلحات والتعاريف وإطلاع الأفرقة المعنية في قطاع الاتصالات الراديوية وقطاع تنمية الاتصالات بالاتحاد عليها، باعتبار ذلك مهمة لجنة الدراسات الرئيسية المعنية بالأمن؛

3 بتعزيز أنشطة التقييس المشتركة المتعلقة بالاطمئنان والثقة والأمن بين جميع لجان الدراسات والأفرقة المتخصصة في الاتحاد وغيره من المنظمات المعنية بوضع المعايير، بما في ذلك نشاط التنسيق المشترك بشأن حماية الأطفال على الخط وتحليل الفجوات المتصل به؛

4 بالتعاون الوثيق مع جميع لجان الدراسات الأخرى التابعة لقطاع تقييس الاتصالات، ووضع خطة عمل لتقييم توصيات قطاع تقييس الاتصالات القائمة وقيد الإعداد والجديدة بهدف بحث مسألة الأمن والتهديدات ومواطن الضعف ، دائمة التطور، لضمان مرونة شبكات تكنولوجيا المعلومات والاتصالات إزاء الهجمات الأمنية السيبرانية، وبأن تواصل تزويد الفريق الاستشاري لتقييس الاتصالات (TSAG) بانتظام بتقارير بشأن أمن الاتصالات/تكنولوجيا المعلومات والاتصالات؛

5 بمواصلة تحديد مجموعة عامة/مشتركة من القدرات الأمنية لكل مرحلة من مراحل دورة حياة أنظمة المعلومات/الشبكات/التطبيقات، بما في ذلك تنمية قدرات العاملين فيما يخص الأمن بحيث يمكن نتيجة لذلك تحقيق أمن مدمج (القدرات والميزات الأمنية متوفرة منذ التصميم) للأنظمة/الشبكات/التطبيقات/البيانات من البداية؛

6 بأن تواصل تصميم إطار أمني واحد أو معمارية أمنية مرجعية واحدة، أو أكثر، يتضمنان عناصر وظيفية أمنية بما يشمل النظر في تحقيق التعاون الأمني فيما بين مختلف أنماط الأنظمة، ويمكن اعتبارهما أساساً لتصميم المعمارية الأمنية لمختلف الأنظمة/الشبكات/التطبيقات من أجل تحسين جودة التوصيات المتعلقة بالأمن، وأن تقدم مراجع للتصاميم الأمنية لما يُحتمل ظهوره من تطبيقات للتكنولوجيات الناشئة فيما يتعلق بالبنية التحتية العالمية للاتصالات/تكنولوجيا المعلومات والاتصالات؛

7 بإيلاء اعتبار للتغيرات المستمرة في تكنولوجيات وقطاع أعمال تكنولوجيا المعلومات والاتصالات والانتظام في استعراض التوصيات المتعلقة بأمن الشبكات ومراجعة التوصيات القائمة لتكييفها مع المتطلبات الأمنية الجديدة ولكي تتصدى للتهديدات الجديدة لأمن الشبكات؛

8 بتقديم أفضل الممارسات في مجال تقييم وتحسين أمن البيانات وأمن المعلومات المحدِّدة للهوية الشخصية والجوانب التقنية والتشغيلية لحمايتهما في البنية التحتية المتطورة للاتصالات/تكنولوجيا المعلومات والاتصالات،

تُكلّف مدير مكتب تقييس الاتصالات

1 بأن يواصل، استناداً إلى قاعدة المعلومات المرتبطة "بخارطة الطريق الخاصة بمعايير أمن الاتصالات/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 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 معايير الأمن ومعايير حماية البيانات وحماية المعلومات المحدِّدة للهوية الشخصية، 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 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 مساعدة الدول الأعضاء على وضع إطار ملائم بين البلدان النامية يسمح بالتصدي بسرعة للحوادث الكبيرة، 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 الاطمئنان والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

9 بتعميم المعلومات على جميع أصحاب المصلحة وزيادة فهم أصحاب المصلحة لموضوع الأمن 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 وأصحاب المصلحة الآخرين، خاصة من البلدان النامية؛

10 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،

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 بوخارست، 2022) لمؤتمر المندوبين المفوضين، بهدف تعزيز الثقة والأمن في استخدام الاتصالات/تكنولوجيا المعلومات والاتصالات، للتخفيف من المخاطر والتصدي للتهديدات؛

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 الاطمئنان والثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

4 استخدام التوصيات، والتقارير التقنية، والإضافات، المتصلة بالموضوع الصادرة عن قطاع تقييس الاتصالات؛

5 مواصلة المساهمة في عمل لجنة الدراسات 17 بشأن نُهج إدارة كل من المخاطر الأمنية السيبرانية والدفاع السيبراني.

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