|  |  |
| --- | --- |
| **مؤتمر المندوبين المفوضين (PP-22) بوخارست، 26 سبتمبر - 14 أكتوبر 2022** |  |
|  |  |
|  |  |
| الجلسة العامة | **الإضافة 5 للوثيقة 68-A** |
|  | **18 أغسطس 2022** |
|  | **الأصل: بالروسية** |
|  |  |
| الدول الأعضاء في الاتحاد أعضاء الكومنولث الإقليمي في مجال الاتصالات (RCC) | |
| مُقترحات لمراجعة القرار 130 | |
| تعزيز دور الاتحاد في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات | |
|  | |

|  |
| --- |
| **ملخص**  يقدم العمل الجاري الاتحاد الدولي للاتصالات لتعريف الرقم القياسي العالمي للأمن السيبراني (GCI) للدول الأعضاء مساهمة كبيرةً في حماية مصالح مستخدمي شبكات وأنظمة وسائط الإعلام والاتصالات في جميع أنحاء العالم. وفي الوقت نفسه، يبدو أن البلدان النامية تواجه صعوبات معينة في تفسير نتائج الرقم القياسي العالمي للأمن السيبراني (GCI) وفي اتخاذ قرارات بشأن زيادة تحسين الرقم القياسي العالمي للأمن السيبراني (GCI) على أساس البيانات المتاحة.  ولذلك سيكون من المناسب توسيع نطاق أنشطة الاتحاد من أجل تعزيز حسابات الرقم القياسي العالمي للأمن السيبراني (GCI) والاضطلاع بمجموعة واسعة من الأنشطة لتسهيل تنفيذ التوصيات العملية الصادرة عن خبراء الاتحاد.  وفي المقابل، سيتيح تنظيم إبداء تعليقات تقييمية منتظمة على هذا الموضوع للاتحاد تقييم نجاح أنشطته وتمهيد السبيل لزيادة تحسين منهجيات حساب الرقم القياسي العالمي للأمن السيبراني (GCI).  ويُقترح أيضاً تغيير عبارة "أمن الحواسيب" لتصبح "الأمن السيبراني" في نص هذا القرار.  وعبارة "أمن الحواسيب" ليست في الوقت الراهن تعريفاً حصرياً وهي تشمل كل مجالات تكنولوجيات المعلومات والاتصالات (مجموعات المخدّمات، والشبكات من أجل إنترنت الأشياء، والمنصات السحابية، وغير ذلك).  وأحد جوانب الاستخدام الآمن لتكنولوجيا المعلومات والاتصالات هو استخدام التوقيعات الرقمية. وتختلف آليات الثقة الحالية المتعلقة باستخدام التواقيع الإلكترونية اختلافاً كبيراً من بلد إلى آخر. فعلى سبيل المثال، يمكن تفويض أوراق اعتماد أحد أصحاب المشاريع، في بعض البلدان، من خلال شهادة أُصدرت لصاحب المشروع باعتباره كياناً للأعمال التجارية، وفي بلدان أخرى باعتباره فرداً، في حين تستلزم مجموعة ثالثة من البلدان شهادة تفويض (شهادة نعت) إضافةً إلى التوقيع الإلكتروني للفرد. ومن شأن الاختلافات الكبيرة بين البلدان في طرق بناء الثقة على أساس البنية التحتية للمفاتيح العمومية أن تنشئ صعوبات كبيرة في مزاولة الأعمال التجارية.  ويتمثل أحد الحلول الممكنة في الاحتفاظ بسجل عام للسلطات المعتمدة لإصدار الشهادات، وإتاحة المعلومات ذات الصلة. ومن شأن الاحتفاظ بسجل عام عن السلطات المعتمدة لإصدار الشهادات بمعلومات عن مجالات نشاطها، وخوارزميات التجفير والمعرفات التي تستخدمها، وأنواع الشهادات التي تصدرها أن يساعد كثيراً في تبسيط التفاعلات بين كيانات الأعمال التجارية في مختلف البلدان.  وبناءً على ما تقدم، يقترح أعضاء الكومنولث الإقليمي في مجال الاتصالات (RCC) إدخال بعض التعديلات على القرار 130.  **الإجراء المطلوب**  يُدعى مؤتمر المندوبين المفوضين إلى النظر في هذا المقترح وإجراء التغييرات اللازمة في القرار 130 لمؤتمر المندوبين المفوضين "تعزيز دور الاتحاد في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات".  \_\_\_\_\_\_\_\_\_  **المراجع**  *-* |

MOD RCC/68A5/1

القـرار 130 (المراجَع في بوخارست، 2022)

تعزيز دور الاتحاد في مجال بناء الثقة والأمن  
في استخدام تكنولوجيا المعلومات والاتصالات

إن مؤتمر المندوبين المفوضين للاتحاد الدولي للاتصالات (بوخارست، 2022)،

إذ يذكِّر

*أ )* بالقرار 68/198 للجمعية العامة للأمم المتحدة، بشأن تسخير تكنولوجيات المعلومات والاتصالات (ICT) لأغراض التنمية؛

*ب)* بالقرار 71/199 للجمعية العامة للأمم المتحدة، بشأن الحق في الخصوصية في العصر الرقمي؛

*ج)* بالقرار 68/243 للجمعية العامة للأمم المتحدة، بشأن التطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي؛

*د )* بالقرار 57/239 للجمعية العامة للأمم المتحدة، بشأن إنشاء ثقافة أمنية عالمية للفضاء الحاسوبي؛

*ﻫ )* بالقرار 64/211 للجمعية العامة للأمم المتحدة، بشأن إرساء ثقافة عالمية تكفل أمن الفضاء الإلكتروني وتقييم الجهود الوطنية الرامية إلى حماية الهياكل الأساسية الحيوية للمعلومات؛

*و )* ببيان الحدث الرفيع المستوى للقمة العالمية لمجتمع المعلومات (WSIS+10) بشأن تنفيذ نتائج القمة العالمية لمجتمع المعلومات بعد مضي عشر سنوات ورؤية الحدث WSIS+10 للقمة لما بعد عام 2015، اللذين تم اعتمادهما في هذا الحدث الذي تولى الاتحاد تنسيقه (جنيف، 2014) على أساس عملية المنصة التحضيرية لأصحاب المصلحة المتعددين (MPP) مع وكالات الأمم المتحدة الأخرى والجامع لكل أصحاب المصلحة في القمة العالمية لمجتمع المعلومات وأقرهما مؤتمر المندوبين المفوضين (بوسان، 2014) واللذين تم تقديمهما للاستعراض الشامل للجمعية العامة للأمم المتحدة؛

*ز )* بالقرار 70/125 للجمعية العامة للأمم المتحدة، بشأن الوثيقة الختامية للاجتماع الرفيع المستوى للجمعية العامة بشأن الاستعراض العام لتنفيذ نتائج القمة العالمية لمجتمع المعلومات؛

*ح)* بالقرار 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؛

*ط)* بالقرار 179 (المراجَع في دبي، 2018) لهذا المؤتمر، بشأن دور الاتحاد في حماية الأطفال على الخط؛

*ي)* بالقرار 181 (المراجَع في غوادالاخارا، 2010) لمؤتمر المندوبين المفوضين، بشأن التعاريف والمصطلحات المتعلقة ببناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات؛

*ك)* بالقرار 196 (المراجَع في دبي، 2018) لهذا المؤتمر، بشأن حماية مستعملي/مستهلكي خدمات الاتصالات؛

*ل)* بالقرار 45 (المراجَع في دبي، 2014) للمؤتمر العالمي لتنمية الاتصالات (WTDC)، بشأن آليات تعزيز التعاون في مجال الأمن السيبراني، بما في ذلك مواجهة ومكافحة الرسائل الاقتحامية؛

*م )* بالقرار 140 (المراجَع في دبي، 2018) لهذا المؤتمر، بشأن دور الاتحاد في تنفيذ نتائج القمة العالمية لمجتمع المعلومات وفي الاستعراض الشامل للجمعية العامة للأمم المتحدة لتنفيذها؛

*ن)* بالقرار 58 (المراجَع في دبي، 2012) للجمعية العالمية لتقييس الاتصالات، بشأن تشجيع إنشاء أفرقة وطنية للتصدي للحوادث الحاسوبية لا سيما في البلدان النامية[[1]](#footnote-1)1؛

*س)* بالقرار 67 (المراجَع في بوينس آيرس، 2017) للمؤتمر العالمي لتنمية الاتصالات، بشأن دور قطاع تنمية الاتصالات للاتحاد الدولي للاتصالات (ITU-D) في حماية الأطفال على الخط؛

*ع)* بالقرار 69 (المراجَع في بوينس آيرس، 2017) للمؤتمر العالمي لتنمية الاتصالات، بشأن إنشاء أفرقة استجابة وطنية للحوادث الحاسوبية (CIRT)، خاصة في البلدان النامية، والتعاون فيما بينها؛

*ف)* بأن القرار 1305 الذي اعتمده مجلس الاتحاد في دورته لعام 2009 حدّد مسائل الأمن والسلامة والاستدامة والمتانة بالنسبة إلى الإنترنت كمسائل تتعلق بالسياسات العامة التي تندرج في إطار عمل الاتحاد الدولي للاتصالات،

وإذ يضع في اعتباره

*أ )* أن الحدث الرفيع المستوى WSIS+10 الذي نسقه الاتحاد أكد من جديد أهمية بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات، على النحو المشار إليه في الفقرات ذات الصلة من الوثائق الختامية للحدث WSIS+10 (جنيف، 2014)؛

*ب)* الأهمية البالغة للبنية التحتية للمعلومات والاتصالات وتطبيقاتها بالنسبة إلى جميع أشكال النشاط الاجتماعي والاقتصادي تقريباً؛

*ج)* الأحكام المتصلة بالأمن السيبراني في التزام تونس وبرنامج عمل تونس والوثيقة الختامية للاجتماع رفيع المستوى للجمعية العامة للأمم المتحدة بشأن الاستعراض العام لتنفيذ نتائج القمة العالمية لمجتمع المعلومات؛

*د )* أن تهديدات جديدة من مختلف المصادر تظهر مع تطبيق وتنمية تكنولوجيا المعلومات والاتصالات وأن هذه التهديدات تؤثر على الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات من جانب جميع الدول الأعضاء وأعضاء القطاعات وأصحاب المصلحة الآخرين، بمن فيهم جميع مستعملي تكنولوجيا المعلومات والاتصالات، إلى جانب أثرها في الحفاظ على السلام وفي التنمية الاقتصادية والاجتماعية لجميع الدول الأعضاء، وأن التهديدات ومواطن الضعف التي تعاني منها البنية التحتية والشبكات والأجهزة لا تزال تثير تحديات أمنية متزايدة عبر الحدود الوطنية تواجهها جميع البلدان، وخاصة البلدان النامية، ويلاحظ في الوقت نفسه في هذا السياق تعزيز دور الاتحاد الدولي للاتصالات في بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات وضرورة مواصلة تعزيز التعاون الدولي وبناء القدرات وتطوير وتكييف الآليات الوطنية والإقليمية والدولية الملائمة الموجودة حالياً (مثل الاتفاقات، وأفضل الممارسات، ومذكرات التفاهم، وما إلى ذلك)؛

*ﻫ )* أنه تمت دعوة الأمين العام للاتحاد لدعم مشاريع عالمية وإقليمية أخرى للأمن السيبراني، حسب الاقتضاء، كما أن جميع البلدان، خاصة البلدان النامية، وجهت إليها الدعوة للمشاركة في أنشطتها ذات الصلة بالاتحاد الدولي للاتصالات؛

*و )* البرنامج العالمي للأمن السيبراني (GCA) للاتحاد الدولي للاتصالات، الذي يشجع التعاون الدولي الهادف إلى اقتراح استراتيجيات لإيجاد حلول من أجل تعزيز الثقة والأمن في استخدام الاتصالات/تكنولوجيا المعلومات والاتصالات؛

*ز )* أن حماية هذه البنية التحتية والتصدي لهذه التحديات والتهديدات يتطلبان إجراءات وطنية وإقليمية ودولية منسقة من أجل منع وقوع أي حادث مرتبط بالأمن السيبراني والاستعداد له والاستجابة له والتغلب عليه من جانب السلطات الحكومية على الأصعدة الوطنية (بما في ذلك إنشاء أفرقة وطنية للاستجابة للحوادث الحاسوبية) ودون الوطنية، ومن جانب القطاع الخاص والمواطنين والمستعملين، كما يتطلبان التعاون والتنسيق على الصعيدين الدولي والإقليمي، وأن على الاتحاد الاضطلاع بدور ريادي في هذا المجال، في إطار اختصاصاته وكفاءاته؛

*ح)* أن النهج التكراري والقائم على المخاطر للأمن السيبراني يمكّن من تطوير وتطبيق ممارسات الأمن السيبراني بطريقة حسب الحاجة من أجل التصدي للتهديدات ومواطن الضعف المتغيرة باستمرار، وأن الأمن هو عملية متواصلة ومتكررة يجب أن تكون في صلب تطور ونشر التكنولوجيات وتطبيقاتها من البداية وأن تستمر طوال دورة حياتها؛

*ط)* الحاجة إلى إحراز تقدم مستمر في التكنولوجيات الحديثة لدعم القدرة على الاكتشاف المبكر للأحداث أو الحوادث التي تؤثر على الأمن السيبراني ومعالجتها بشكل منسّق وفي الوقت المناسب، أو الحوادث المتعلقة بأمن الشبكات الحاسوبية والتي من شأنها تقويض توفر البنى التحتية الحرجة وسلامتها وسريتها في الدول الأعضاء في الاتحاد والحاجة إلى استراتيجيات تتيح الحد من أثر هذه الحوادث وتخفيف المخاطر والتهديدات المتنامية التي تتعرض لها هذه المنصات؛

*ي)* أن القرار 70/125 للجمعية العامة للأمم المتحدة، الوثيقة الختامية للاجتماع الرفيع المستوى للجمعية العامة بشأن الاستعراض العام لتنفيذ نتائج القمة العالمية لمجتمع المعلومات (WSIS)، يقر بالتحديات التي تواجهها البلدان، خاصةً البلدان النامية، في بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات وينادي بالتركيز مجدداً على بناء القدرات والتعليم وتبادل المعارف والممارسات التنظيمية إضافةً إلى تعزيز التعاون بين أصحاب المصلحة المتعددين على جميع المستويات وزيادة الوعي بين مستعملي تكنولوجيا المعلومات والاتصالات، خاصةً بين الفئات الأكثر فقراً والأشد ضعفاً؛

*ك)* أن عدد التهديدات السيبرانية والهجمات السيبرانية يتزايد، ويزداد أيضاً الاعتماد على الإنترنت وغيرها من الشبكات الأساسية لأغراض النفاذ إلى الخدمات والمعلومات؛

*ل)* أن قطاع تقييس الاتصالات بالاتحاد (ITU-T) اعتمد نحو 300 معيار فيما يتعلق ببناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

*م )* التقرير النهائي للمسألة ITU‑D 3/2 (تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني) التي يقوم بدراستها قطاع تنمية الاتصالات بالاتحاد (ITU‑D)؛

*ن)* أن واقع معايير الأمن السيبراني بطبيعته يتطلب التعاون بين الاتحاد الدولي للاتصالات والمنظمات الوطنية والإقليمية والعالمية والقطاعية الأخرى؛

*س)* أن العديد من البلدان النامية تضع أو تنفذ استراتيجيات وطنية للأمن السيبراني؛

*ع)* أن الأمن السيبراني أصبح مسألة في غاية الأهمية على الصعيد الدولي وبالتالي، فإن دور ومشاركة الأمم المتحدة ووكالاتها المتخصصة ذات الصلة، من قبيل الاتحاد الدولي للاتصالات، في بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات، يتسمان بالأهمية؛

*ف)* الأدوار والمسؤوليات المختلفة لجميع أصحاب المصلحة في ضمان الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

*ص)* أن بعض الشركات الصغيرة والمتوسطة تواجه تحديات إضافية في تنفيذ ممارسات الأمن السيبراني،

وإقراراً منه

*أ )* بأن الأمن السيبراني عنصر أساسي لتأمين البنى التحتية للاتصالات/تكنولوجيا المعلومات والاتصالات، كما أنه ركيزة أساسية بالنسبة إلى التنمية الاجتماعية والاقتصادية؛

*ب)* بأن تطوير تكنولوجيا المعلومات والاتصالات كان ولا يزال عاملاً حاسماً في نمو الاقتصاد العالمي، بما في ذلك الاقتصاد الرقمي وتنميته على أساس من الأمن والثقة؛

*ج)* بأن القمة العالمية لمجتمع المعلومات أكدت على أهمية بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات والأهمية الكبرى لأعمال التنفيذ من جانب أصحاب المصلحة المتعددين على الصعيد الدولي، وأنها وضعت خط العمل جيم5 (بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات) وحددت دور الاتحاد في برنامج عمل تونس بشأن مجتمع المعلومات ليقوم بمهمة تنسيق/تيسير تنفيذ هذا الخط وأقرت باضطلاع الاتحاد بهذه المهمة في السنوات الأخيرة، من خلال البرنامج العالمي للأمن السيبراني على سبيل المثال؛

*د )* بأن المؤتمر العالمي لتنمية الاتصالات لعام 2017 قد اعتمد خطة عمل بوينس آيرس والهدف 2 الوارد فيها ولا سيما الناتج 2.2 بشأن بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات، حيث يعيِّن الأمن السيبراني نشاطاً ذا أولوية لدى مكتب تنمية الاتصالات (BDT) ويحدد مجالات العمل الرئيسية التي يتعيَّن على المكتب الاضطلاع بها؛ والمؤتمر العالمي لتنمية الاتصالات اعتمد القرار 45 (المراجَع في دبي، 2014)، بشأن آليات تعزيز التعاون في مجال الأمن السيبراني بما في ذلك مواجهة ومكافحة الرسائل الاقتحامية، الذي دعا الأمين العام إلى استرعاء اهتمام مؤتمر المندوبين المفوضين التالي بهذا القرار لينظر فيه ويتخذ ما يلزم من إجراءات بشأنه، وأن يقدم تقريراً عن نتائج مجالات العمل الرئيسية هذه إلى المجلس وإلى مؤتمر المندوبين المفوضين في عام 2018 حسب الاقتضاء؛ والقرار 69 (المراجَع في بوينس آيرس، 2017) الخاص بتسهيل إنشاء أفرقة استجابة وطنية للحوادث الحاسوبية، خاصة في البلدان النامية، والتعاون فيما بينها؛

*ﻫ )* بأن إعلان بوينس آيرس الذي اعتمده المؤتمر العالمي لتنمية الاتصالات لعام 2017 ينص على أن: "بناء الثقة والاطمئنان والأمن في استعمال الاتصالات/تكنولوجيا المعلومات والاتصالات فضلاً عن حماية البيانات الشخصية من الأولويات التي تستدعي تعاوناً وتنسيقاً دوليين بين الحكومات والمنظمات ذات الصلة وشركات القطاع الخاص والكيانات المعنية في مجال بناء القدرات وتبادل أفضل الممارسات من أجل وضع السياسات العامة ذات الصلة والتدابير القانونية والتنظيمية والتقنية التي تتناول حماية البيانات الشخصية، من بين عدة أمور، وأنه ينبغي لأصحاب المصلحة العمل معاً لضمان موثوقية وأمن شبكات وخدمات تكنولوجيا المعلومات والاتصالات"؛

*و )* بأنه لدعم تشكيل أفرقة الاستجابة الوطنية للحوادث الحاسوبية في الدول الأعضاء التي تفتقر إلى هذه الأفرقة على الرغم من الحاجة إليها، اعتمدت الجمعية العالمية لتقييس الاتصالات لعام 2016 (WTSA-16) القرار 58 (المراجَع في دبي، 2012)، بشأن تشجيع إنشاء أفرقة استجابة وطنية في حالات الحوادث الحاسوبية، خاصة للبلدان النامية، كما اعتمد المؤتمر العالمي لتنمية الاتصالات لعام 2017 القرار 69 (المراجَع في بوينس آيرس، 2017)، بشأن تسهيل إنشاء أفرقة استجابة وطنية للحوادث الحاسوبية، بما في ذلك أفرقة استجابة للحوادث الحاسوبية تكون مسؤولة عن التعاون بين الحكومات، خاصة في البلدان النامية، والتعاون فيما بينها وأهمية التنسيق بين جميع المنظمات ذات الصلة؛

*ز )* بالفقرة 15 من التزام تونس التي تنص على ما يلي: "مع الاعتراف بمبادئ النفاذ الشامل وغير التمييزي إلى تكنولوجيا المعلومات والاتصالات لجميع البلدان وبضرورة مراعاة مستوى التنمية الاجتماعية والاقتصادية لكل بلد واحترام نواحي مجتمع المعلومات ذات التوجه التنموي، فإننا نؤكد على أن تكنولوجيا المعلومات والاتصالات هي أداة فعالة في تعزيز السلام والأمن والاستقرار والديمقراطية والتلاحم الاجتماعي والإدارة الرشيدة وحكم القانون، على المستويات الوطنية والإقليمية والدولية. ويمكن الاستفادة من تكنولوجيا المعلومات والاتصالات في تعزيز النمو الاقتصادي ونمو المؤسسات. وندرك أن النهوض بالبنية التحتية وبناء القدرات البشرية وأمن المعلومات وأمن الشبكات كلها أمور حيوية في تحقيق هذه الغايات. ونعترف كذلك بضرورة المواجهة الفعالة للتحديات والتهديدات الناتجة عن استخدام تكنولوجيا المعلومات والاتصالات لأغراض لا تتفق مع أهداف حفظ الاستقرار والأمن الدوليين وبأنها يمكن أن تؤثر تأثيراً سيئاً على تكامل البنية التحتية في داخل الدول، مما يؤثر على أمن تلك الدول. لذلك من الضروري أن نعمل على منع إساءة استخدام موارد المعلومات وتكنولوجيا المعلومات لأغراض إجرامية وإرهابية، وذلك مع احترام حقوق الإنسان"، وأن التحديات الناجمة عن سوء استعمال موارد تكنولوجيا المعلومات والاتصالات استمرت في الازدياد منذ انعقاد القمة العالمية لمجتمع المعلومات؛

*ح)* بأن الحدث الرفيع المستوى (WSIS+10) الذي نسقه الاتحاد قد عيّن تحديات عديدة أمام تنفيذ خطوط عمل القمة العالمية لمجتمع المعلومات لا يزال يتعين التصدي لها ومواجهتها بعد عام 2015؛

*ط)* بأن الدول الأعضاء، ولا سيما البلدان النامية، قد تحتاج، لدى وضع تدابير قانونية مناسبة وعملية بشأن الحماية من التهديدات السيبرانية على المستويات الوطنية والإقليمية والدولية، إلى مساعدة من الاتحاد في وضع تدابير تقنية وإجرائية، الهدف منها ضمان أمن البنى التحتية الوطنية لتكنولوجيا المعلومات والاتصالات، وذلك بناءً على طلب هذه الدول الأعضاء، مع ملاحظة أن هناك عدداً من المبادرات الوطنية والدولية التي قد تدعم هذه البلدان لإعداد مثل هذه التدابير القانونية؛

*ي)* بالرأي 4 (لشبونة، 2009) للمنتدى العالمي لسياسات الاتصالات/تكنولوجيا المعلومات والاتصالات، بشأن الاستراتيجيات التعاونية لبناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

*ك)* بالنتائج ذات الصلة للجمعية العالمية لتقييس الاتصالات لعام 2016، وبالأخص:

’1‘ القرار 50 (المراجَع في الحمامات، 2016)، بشأن الأمن السيبراني؛

’2‘ القرار 52 (المراجَع في الحمامات، 2016)، بشأن مكافحة الرسائل الاقتحامية والتصدي لها؛

*ل)* بأن الشبكات الآمنة والموثوقة من شأنها بناء الثقة والتشجيع على تبادل واستخدام المعلومات والبيانات؛

*م )* بأن تنمية المهارات البشرية وبناء القدرات يشكلان عنصرين رئيسيين في تعزيز حماية شبكات المعلومات؛

*ن)* بأن الدول الأعضاء تبذل جهوداً لتحسين البيئات المؤسسية؛

*س)* بأن عمليات تقييم المخاطر وتحليلها توفر فهماً أفضل لمخاطر الأمن السيبراني التي تواجهها المنظمات وكيفية تخفيف أثرها،

وإذ يدرك

*أ )* أن الاتحاد الدولي للاتصالات والمنظمات الدولية الأخرى تقوم، من خلال مجموعة منوعة من الأنشطة، بفحص المسائل المتصلة ببناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات، بما في ذلك الاستقرار وتدابير مكافحة الرسائل الاقتحامية والبرمجيات الضارة وما إلى ذلك، إلى جانب حماية البيانات الشخصية والخصوصية؛

*ب)* أن لجنة الدراسات 17 لقطاع تقييس الاتصالات ولجنتي الدراسات 1 و2 لقطاع تنمية الاتصالات ولجان الدراسات الأخرى ذات الصلة في الاتحاد تواصل العمل في موضوع الوسائل التقنية لتحقيق أمن شبكات المعلومات والاتصالات، وفقاً للقرارين 50 و52 (المراجَعين في الحمامات، 2016)، والقرارين 45 (المراجَع في دبي، 2014) و69 (المراجَع في بوينس آيرس، 2017)؛

*ج)* أن للاتحاد دوراً أساسياً ينبغي أن يضطلع به في بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

*د )* أن لجنة الدراسات 2 لقطاع تنمية الاتصالات مستمرة في إجراء الدراسات المنادى بها في المسألة 3/2 لقطاع تنمية الاتصالات (تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني)، والتي تم إبرازها في القرار 64/211 للجمعية العامة للأمم المتحدة؛

*هـ )* أن الاتحاد يساعد أيضاً البلدان النامية في بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات ويدعم إنشاء أفرقة الاستجابة للحوادث الحاسوبية، بما في ذلك أفرقة استجابة للحوادث الحاسوبية تكون مسؤولة عن التعاون بين الحكومات، وأهمية التنسيق بين جميع المنظمات ذات الصلة؛

*و )* أن القرار 1336 الذي اعتمده مجلس الاتحاد في دورته لعام 2011، أنشأ فريق العمل التابع للمجلس والمعني بقضايا السياسة العامة الدولية المتعلقة بالإنترنت (CWG-Internet)، واختصاصاته هي تحديد ودراسة وتطوير المسائل ذات الصلة بقضايا السياسة العامة الدولية المتعلقة بالإنترنت، بما في ذلك تلك القضايا المحددة في القرار 1305 الذي اعتمده المجلس في دورته لعام 2009، مثل أمن وسلامة واستمرارية واستدامة ومتانة الإنترنت؛

*ز )* أن المؤتمر العالمي لتنمية الاتصالات لعام 2017 اعتمد القرار 80 (المراجَع في بوينس آيرس، 2017) بشأن وضع أطر إعلامية موثوقة في البلدان النامية وتعزيزها من أجل تسهيل وتشجيع عمليات التبادل الإلكترونية للمعلومات الاقتصادية بين الشركاء الاقتصاديين؛

*ح)* المادة 6 بشأن أمن الشبكات وحصانتها والمادة 7 من لوائح الاتصالات الدولية بشأن الاتصالات الإلكترونية غير المرغوبة المرسلة بالجملة اللتين اعتمدهما المؤتمر العالمي للاتصالات الدولية (دبي، 2012)،

وإذ يلاحظ

*أ )* أن الاتحاد، بصفته منظمة دولية حكومية يشارك فيها القطاع الخاص، يحتل مركزاً يسمح له بأن يقوم بدور هام، مشتركاً مع المنظمات والهيئات الدولية الأخرى، في التصدي للتهديدات ومواطن الضعف التي تؤثر على بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

*ب)* الفقرتين 35 و36 من إعلان مبادئ جنيف والفقرة 39 من برنامج عمل تونس بشأن بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

*ج)* أنه رغم عدم وجود تعاريف متفق عليها عالمياً للرسائل الاقتحامية وغير ذلك من العبارات في هذا المجال، فقد وصفت لجنة الدراسات 2 لقطاع تقييس الاتصالات، في اجتماعها في يونيو 2006، الرسائل الاقتحامية بأنها عبارة تُستعمل عموماً لتصف الرسائل الإلكترونية غير المرغوبة التي تصل بحجم كبير في البريد الإلكتروني أو نظام رسائل الهاتف المحمول SMS)، (MMS، وغايتها تسويق منتجات أو خدمات تجارية؛

*د )* مبادرة الاتحاد المتعلقة بالتعاون مع منتدى أفرقة الأمن والاستجابة للحوادث (FIRST)،

وإذ يأخذ في الاعتبار

الأعمال المنوطة بالاتحاد بموجب القرارات 50 و52 (المراجَعين في الحمامات، 2016) و58 (المراجَع في دبي، 2012)؛ و45 (المراجَع في دبي، 2014) و69 (المراجَع في بوينس آيرس، 2017)؛ والهدف 2 لخطة عمل بوينس آيرس؛ ومسائل الدراسة ذات الصلة لقطاع تقييس الاتصالات بشأن الجوانب التقنية المتعلقة بأمن شبكات المعلومات والاتصالات؛ والمسألة 3/2 لقطاع تنمية الاتصالات،

يقرر

1 أن يستمر في إيلاء هذا العمل أولوية عالية داخل الاتحاد 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 يعطي أولوية عالية للعمل الجاري في الاتحاد والموصوف في فقرة *"إذ* *يأخذ في الاعتبار"* أعلاه، طبقاً لاختصاصاته ومجالات خبراته، وأن يواصل العمل عن كثب، حسب الاقتضاء، مع الهيئات/الوكالات الأخرى ذات الصلة التابعة للأمم المتحدة والهيئات الدولية الأخرى ذات الصلة، مع مراعاة الولايات المحددة ومجالات الخبرة لمختلف الوكالات مع التنبه إلى الحاجة إلى تفادي ازدواج الأعمال بين المنظمات وبين المكاتب أو الأمانة العامة؛

3 أن يركز الاتحاد موارده وبرامجه على مجالات الأمن السيبراني الوطنية والإقليمية والدولية التي تندرج ضمن اختصاصاته وخبراته الأساسية، وتحديداً الجوانب التقنية والتنموية، مع استبعاد المجالات المتعلقة بتطبيق الدول الأعضاء لمبادئ قانونية أو سياساتية تتعلق بالدفاع والأمن الوطنيين والمحتوى والجريمة السيبرانية والتي تشملها الحقوق السيادية لهذه الدول، بيد أن ذلك لا يستثني الاتحاد من الاضطلاع بولايته المتعلقة بوضع توصيات تقنية معدة للحد من أوجه الضعف في البنية التحتية لتكنولوجيا المعلومات والاتصالات، كما لا يستثني ذلك الاتحاد من توفير المساعدة المتفق عليها في المؤتمر العالمي لتنمية الاتصالات لعام 2017 بما في ذلك في إطار الهدف 2 والأنشطة ذات الصلة بالمسألة 3/2؛

4 تشجيع ثقافة يُنظر فيها إلى الأمن كعملية مستمرة ومتكررة تُدمج في المنتجات منذ بداية استخدامها وتستمر طوال فترة عمرها ويتسنى للمستعملين النفاذ إليها وفهمها؛

5 تعزيز زيادة وعي أعضاء الاتحاد بالأنشطة المضطلع بها في الاتحاد والكيانات الأخرى ذات الصلة المشاركة في تعزيز الأمن السيبراني، بما في ذلك أنشطة بناء القدرات فضلاً عن زيادة الوعي بين هذه الكيانات بالتحديات الخاصة التي تواجهها البلدان النامية، في بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

6 المساهمة في مواصلة تعزيز الثقة وإطار الأمن، بما يتسق مع دور الاتحاد بوصفه جهة التيسير الرئيسية لخط العمل جيم5 للقمة العالمية لمجتمع المعلومات، مع مراعاة القرار 140 (المراجَع في دبي، 2018) لهذا المؤتمر؛

7 الاستمرار، استناداً إلى قاعدة المعلومات المرتبطة "بخارطة الطريق الخاصة بمعايير أمن تكنولوجيا المعلومات والاتصالات"وجهود قطاع تنمية الاتصالات بشأن الأمن السيبراني، وبمساعدة المنظمات الأُخرى ذات الصلة، في تحديث قائمة المبادرات والأنشطة الوطنية والإقليمية والدولية لتشجيع وضع نهج مشتركة في مجال الأمن السيبراني؛

8 إعداد دراسات حالة عن الترتيبات المؤسسية المتعلقة بالأمن السيبراني بالتعاون مع الأعضاء ومع المنظمات ذات الصلة؛

9 النظر في التحديات الخاصة بالأمن السيبراني التي تواجهها الشركات الصغيرة والمتوسطة وإدراج هذه الاعتبارات في أنشطة الاتحاد في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

10 مراعاة أثر نشر التكنولوجيات الناشئة على الأمن السيبراني وإدراج تلك الاعتبارات في أنشطة الاتحاد في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

11 دعم تطوير البنية التحتية التي يرتكز عليها التحول الرقمي الجاري للاقتصاد العالمي من خلال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات، خاصةً في التصدي للتهديدات الحالية والمستقبلية، وذلك في إطار ولاية الاتحاد؛

12 استخدام إطار البرنامج العالمي للأمن السيبراني للاتحاد لمواصلة توجيه عمل الاتحاد بشأن الجهود الرامية إلى بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات،

يكلف الأمين العام ومديري المكاتب

1بمواصلة استعراض:

’1‘ العمل المنجز حتى الآن في القطاعات الثلاثة للاتحاد وفي إطار البرنامج العالمي للأمن السيبراني للاتحاد والمنظمات الأخرى المعنية ومبادرات التصدي للتهديدات القائمة والمقبلة وتعزيز الحماية منها، من أجل بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

’2‘ التقدم المحرز في تنفيذ هذا القرار، مع مواصلة الاتحاد دوره كجهة التنسيق/التيسير الرئيسية لخط العمل جيم5 للقمة العالمية، وذلك بمساعدة الأفرقة الاستشارية وبما يتماشى مع دستور الاتحاد واتفاقيته؛

’3‘ نتائج العمل المنجز حتى الآن في دعم البلدان النامية خصوصاً، في مجال بناء القدرات والمهارات المتعلقة بالأمن السيبراني للتأكد من أن الاتحاد يركز موارده بشكل فعّال للتصدي لتحديات التنمية؛

2 بتقديم تقرير إلى المجلس، بما يتفق والقرار 45 (المراجَع في دبي، 2014)، بشأن الأنشطة الجارية في الاتحاد والمنظمات والكيانات الأخرى ذات الصلة لتعزيز التعاون والعمل المشترك، على الصعيدين الإقليمي والعالمي، وتعزيز بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات للدول الأعضاء، ولا سيما البلدان النامية، مع مراعاة أي معلومات تقدمها الدول الأعضاء، بما في ذلك معلومات عن الحالات التي تقع ضمن ولايتها ويمكن أن تؤثر على هذا التعاون؛

3 بتقديم تقرير عن مذكرات التفاهم (MoU) بين البلدان المعنية، بما يتفق والقرار 45 (المراجَع في دبي، 2014) علاوةً على أشكال التعاون القائمة، مع تقديم تحليل عن حالتها ونطاقها وتطبيقات آليات التعاون هذه لتعزيز الأمن السيبراني ومكافحة التهديدات السيبرانية، بغية تمكين الدول الأعضاء من تحديد مدى الاحتياج إلى مزيدٍ من المذكرات أو الآليات؛

4 بإذكاء الوعي بشأن الأنشطة المضطلع بها داخل الاتحاد والكيانات الأخرى ذات الصلة المشاركة في تعزيز الأمن السيبراني، بما في ذلك أنشطة بناء القدرات، والتحديات الخاصة التي تواجهها البلدان النامية، في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات بما يتماشى مع الفقرة 5 من *"يقرر"*؛

5بتسهيل النفاذ إلى الأدوات والموارد المطلوبة، في حدود الميزانية المتاحة، لتعزيز الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات لصالح جميع الدول الأعضاء، وذلك تماشياً مع أحكام القمة العالمية بشأن النفاذ الشامل وغير التمييزي إلى تكنولوجيا المعلومات والاتصالات أمام جميع البلدان؛

6 بمواصلة تبادل المعارف والمعلومات عن المبادرات الوطنية والإقليمية والدولية المتصلة بالأمن السيبراني الحالية والمستقبلية في أنحاء العالم عن طريق الصفحة الإلكترونية للأمن السيبراني للاتحاد وتشجيع جميع أصحاب المصلحة على المساهمة في هذه الأنشطة، مع مراعاة البوابات الإلكترونية القائمة؛

7 بتقديم تقرير سنوي إلى المجلس عن هذه الأنشطة وعرض مقترحات حسب الاقتضاء؛

8 بمواصلة تعزيز التنسيق بين لجان الدراسات والبرامج المعنية،

يكلف مدير مكتب تقييس الاتصالات

1 بتكثيف الأعمال في لجان دراسات القطاع القائمة حالياً بغية:

’1‘ التصدي للتهديدات ومواطن الضعف القائمة والمقبلة التي تؤثر على جهود بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات، مع مراعاة الخدمات الجديدة والتطبيقات الناشئة القائمة على شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات، من خلال إعداد تقارير أو توصيات حسب الاقتضاء، بهدف تنفيذ قرارات الجمعية العالمية لتقييس الاتصالات، لا سيما القرارات 50 و52 (المراجعَين في الحمامات، 2016) و58 (المراجَع في دبي، 2012) التي تتيح البدء بالعمل قبل الموافقة على المسألة؛

’2‘ التماس الطرق لتعزيز تبادل المعلومات التقنية في هذه المجالات، وتعزيز اعتماد البروتوكولات والمعايير التي تزيد من تعزيز الأمن وتشجع التعاون الدولي بين الهيئات ذات الصلة؛

’3‘ تسهيل المشاريع المنبثقة عن نتائج الجمعية العالمية لتقييس الاتصالات، لا سيما:

• القرار 50 (المراجَع في الحمامات، 2016)، بشأن الأمن السيبراني؛

• القرار 52 (المراجَع في دبي، 2012)، بشأن التصدي للرسائل الاقتحامية ومكافحتها؛

2 بالنظر داخل قطاع تقييس الاتصالات في تشجيع ثقافة ينظر فيها إلى الأمن كعملية مستمرة ومتكررة وتقديم مقترحات إلى المجلس حسب الاقتضاء؛

3 بمواصلة التعاون مع المنظمات المعنية بغية تبادل أفضل الممارسات ونشر المعلومات من خلال ورش عمل ودورات تدريبية مشتركة وأفرقة أنشطة تنسيق مشتركة ومن خلال مساهمات خطية من المنظمات ذات الصلة بناءً على دعوات توجه إليها، على سبيل المثال،

يكلف مدير مكتب تنمية الاتصالات

1 بأن يقوم، بما يتفق مع نتائج المؤتمر العالمي لتنمية الاتصالات لعام 2017 وعملاً بالقرارات 45 (المراجَع في دبي، 2014) و69 (المراجَع في بوينس آيرس، 2017) و80 (المراجَع في بوينس آيرس، 2017) والهدف 2 من خطة عمل بوينس آيرس، لدعم المشاريع الإقليمية والعالمية بشأن الأمن السيبراني وتشجيع جميع البلدان على المشاركة في هذه الأنشطة؛

2 بدعم الدول الأعضاء في الاتحاد، بناءً على طلبها، في جهودها الرامية إلى بناء القدرات من خلال تسهيل نفاذ الدول الأعضاء إلى الموارد التي طورتها المنظمات الدولية الأخرى ذات الصلة التي تعمل في مجال التشريعات الوطنية لمكافحة الجرائم السيبرانية؛ ودعم جهود الدول الأعضاء في الاتحاد على الصعيدين الوطني والإقليمي لبناء القدرات اللازمة للحماية من التهديدات والجرائم السيبرانية وذلك بالتعاون فيما بينها بما يتفق مع التشريعات الوطنية للدول الأعضاء المشار إليها أعلاه، ومساعدة الدول الأعضاء، لا سيما البلدان النامية، في وضع تدابير قانونية مناسبة وقابلة للتطبيق تتصل بالحماية من التهديدات السيبرانية على المستويات الوطنية والإقليمية والدولية، وإرساء التدابير التقنية والإجرائية التي تهدف إلى تأمين البنى التحتية الوطنية لتكنولوجيا المعلومات والاتصالات مع الأخذ بعين الاعتبار عمل لجان الدراسات ذات الصلة في قطاع تقييس الاتصالات، وعمل المنظمات الأخرى ذات الصلة حسب الاقتضاء؛ وإنشاء الهياكل التنظيمية مثل أفرقة الاستجابة للحوادث الحاسوبية، لتحديد التهديدات السيبرانية وإدارتها والتعامل معها، ووضع آليات التعاون على المستويين الإقليمي والدولي؛

3 بتقديم الدعم المالي والإداري اللازم لهذه المشاريع في حدود الموارد الحالية، والتماس موارد إضافية (نقدية وعينية) لتنفيذ هذه المشاريع من خلال اتفاقات الشراكة؛

4 بتأمين تنسيق عمل هذه المشاريع في سياق مجمل الأنشطة التي يقوم بها الاتحاد بناء على دوره كجهة تنسيق/تسهيل في خط العمل جيم5 للقمة العالمية لمجتمع المعلومات، والتخلص من أي ازدواجية في العمل فيما يتعلق بهذا الموضوع الهام مع أنشطة الأمانة العامة وقطاع تقييس الاتصالات؛

5 بتنسيق عمل هذه المشاريع مع أعمال لجان دراسات قطاع تنمية الاتصالات بشأن هذا الموضوع، ومع أنشطة البرامج ذات الصلة ومع الأمانة العامة؛

6 بمواصلة التعاون مع المنظمات ذات الصلة بغية تبادل أفضل الممارسات ونشر المعلومات من خلال ورش عمل ودورات تدريبية مشتركة على سبيل المثال؛

7 بدعم أعمال لجنة الدراسات 17 ولجان الدراسات الأخرى لقطاع تقييس الاتصالات من خلال تعزيز وتسهيل الدول الأعضاء في الاتحاد وأعضاء القطاعات، خاصةً من البلدان النامية، تنفيذ التوصيات الموافق عليها لقطاع تقييس الاتصالات المتعلقة بالأمن؛

8 بدعم الدول الأعضاء في الاتحاد في وضع استراتيجياتها الوطنية و/أو الإقليمية للأمن السيبراني، من أجل بناء القدرات الوطنية للتصدي للتهديدات السيبرانية والحماية منها ضمن مبادئ التعاون الدولي بما يتفق والهدف 2 لخطة عمل بوينس آيرس للمؤتمر العالمي لتنمية الاتصالات؛

9 بدعم الأعضاء في تنمية المهارات البشرية وبناء القدرات لتعزيز الأمن السيبراني؛

10 بدعم الأعضاء في أنشطة تقييم المخاطر المتعلقة بالأمن السيبراني؛

11 بتقديم تقرير سنوي إلى المجلس عن هذه الأنشطة وعرض مقترحات حسب الاقتضاء،

يكلف كذلك مدير مكتب تقييس الاتصالات ومدير مكتب تنمية الاتصالات بأن يقوم كل منهما في نطاق مسؤولياته بما يلي

1 تنفيذ القرارات ذات الصلة الصادرة عن الجمعية العالمية لتقييس الاتصالات لعام 2016 والمؤتمر العالمي لتنمية الاتصالات لعام 2017، بما في ذلك الناتج 2.2 من الهدف 2 من خطة عمل بوينس آيرس، مع تركيز خاص على احتياجات البلدان النامية عند قيامها بجهود من أجل تحسين الأمن السيبراني وبناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

2 تحديد وتعزيز توافر المعلومات بشأن بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات بما في ذلك البنية التحتية لتكنولوجيا المعلومات والاتصالات من أجل الدول الأعضاء وأعضاء القطاعات والمنظمات ذات الصلة؛

3 مواصلة تحديد أفضل الممارسات المتعلقة بالمسألة 3/2 بما في ذلك تأسيس أفرقة الاستجابة للحوادث الحاسوبية واستعراض الدليل المرجعي للدول الأعضاء دون تكرار العمل الجاري في المسألة 3/2 لقطاع تنمية الاتصالات، من أجل المساهمة في هذه المسألة؛

4 التعاون مع المنظمات ذات الصلة وسائر الخبراء الدوليين والوطنيين، حسب الاقتضاء، من أجل تحديد أفضل الممارسات في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات، بما في ذلك إنشاء أفرقة الاستجابة للحوادث الحاسوبية؛

5 اتخاذ الإجراءات الكفيلة بدراسة مسائل جديدة في لجان الدراسات ضمن القطاعات المعنية بإرساء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

6 تحديد وتوثيق الخطوات العملية اللازمة لدعم البلدان النامية في بناء القدرات والمهارات في مجال الأمن السيبراني، مع مراعاة التحديات المحددة التي تواجهها؛

7 مراعاة التحديات التي يواجهها جميع أصحاب المصلحة، خاصةً في البلدان النامية، من أجل بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات وتحديد الخطوات التي يمكن أن تساعد في التصدي لها؛

8 تعزيز إتاحة المعلومات عن السلطات الوطنية لإصدار الشهادات ومجالات نشاطها، والخوارزميات والمعرفات التي تستخدمها، للدول الأعضاء وأعضاء القطاعات والمنظمات ذات الصلة؛

9 تحديد وتوثيق الخطوات العملية اللازمة لتعزيز الأمن في استخدام تكنولوجيا المعلومات والاتصالات على الصعيد الدولي، بما في ذلك مفهوم أن ينظر إلى الأمن كعملية مستمرة ومتكررة، استناداً إلى الممارسات والمبادئ التوجيهية والتوصيات المقبولة على نطاق واسع، التي يمكن أن تقرر الدول الأعضاء وأصحاب المصلحة الآخرون تطبيقها لتحسين قدرتها على مكافحة التهديدات السيبرانية والهجمات السيبرانية، بما في ذلك نهج دينامي وتكراري قائم على المخاطر ينعكس فيه الطابع المتطور للتهديدات ومواطن الضعف، وتعزيز التعاون الدولي في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات، ومع مراعاة البرنامج العالمي للأمن السيبراني (GCA) وفي حدود الموارد المالية المتاحة؛

10 دعم الاستراتيجية والتنظيم والتوعية والتعاون والتقييم وتنمية المهارات؛

11 تقديم الدعم التقني والمالي اللازم في حدود الموارد المتاحة في الميزانية وفقاً للقرار 58 (المراجَع في دبي، 2012) للجمعية العالمية لتقييس الاتصالات؛

12 تشجيع مشاركة الخبراء في أنشطة الاتحاد في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

13 تعبئة الموارد المناسبة من خارج الميزانية العادية للاتحاد من أجل تنفيذ هذا القرار، لمساعدة البلدان النامية؛

14 دعم البلدان النامية ومساعدتها في تشجيع وتسهيل تنفيذ توصيات قطاع تقييس الاتصالات المتعلقة بالأمن؛

15 مساعدة الدول الأعضاء على تقييم وتكييف الأطر التشريعية والتنظيمية، بالاستفادة بشكل أفضل من التقرير الصادر عن الاتحاد بشأن الرقم القياسي العالمي للأمن السيبراني (CGI)؛

16 تنظيم "ملاحظات تقييمية" سنوية مع الإدارات المصرح لها من الدول الأعضاء لتحليل وتحسين عملية حساب الرقم القياسي العالمي للأمن السيبراني (CGI)،

يكلف الأمين العام

وفقاً لمبادرته في هذا الشأن:

1 بتقديم تقرير إلى المجلس، مع مراعاة أنشطة القطاعات الثلاثة عن تنفيذ وفعالية خطة العمل لتعزيز دور الاتحاد في بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

2 بالتعاون مع المنظمات الدولية ذات الصلة بما في ذلك من خلال اعتماد مذكرات التفاهم التي تخضع لموافقة المجلس في هذا الصدد، وفقاً للقرار 100 (مينيابوليس، 1998) لمؤتمر المندوبين المفوضين،

يطلب من مجلس الاتحاد

أن يدرج تقرير الأمين العام في الوثائق المرسلة إلى الدول الأعضاء وفقاً للرقم 81 من الاتفاقية.

يدعو الدول الأعضاء

1 إلى النظر في الانضمام إلى المبادرات الدولية والإقليمية المختصة المناسبة التي تعزز الأطر التشريعية الوطنية ذات الصلة بأمن شبكات المعلومات والاتصالات؛

2 إلى التعاون بشكل وثيق على تعزيز التعاون الإقليمي والدولي، مع الأخذ في الاعتبار القرار 45 (المراجَع في دبي، 2014) بهدف تعزيز الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات، من أجل تخفيف المخاطر والتهديدات؛

3 إلى دعم مبادرات الاتحاد بشأن الأمن السيبراني، بما في ذلك الرقم القياسي العالمي للأمن السيبراني (GCI)، من أجل تشجيع الاستراتيجيات الحكومية وتبادل المعلومات عن الجهود المبذولة عبر الصناعات والقطاعات؛

4 إلى إبلاغ الأمين العام عن الأنشطة ذات الصلة المتعلقة بهذا القرار فيما يتعلق بالثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

5 إلى الاستفادة من موارد المبادرات الوطنية والإقليمية والدولية المتعلقة بالأمن السيبراني حول العالم ومن الدعم الذي تقدمه وأفضل ممارساتها، وذلك عن طريق الصفحة الإلكترونية للأمن السيبراني للاتحاد؛

6 إلى التعاون مع المنظمات ذات الصلة، عن طريق تبادل أفضل الممارسات في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات بما في ذلك إنشاء وتنفيذ أفرقة وطنية للاستجابة للحوادث الحاسوبية؛

7 إلى مواصلة إذكاء الوعي من خلال نشر أفضل الممارسات والسياسات التي تم تنفيذها من أجل زيادة القدرة على وضع سياسات ملائمة لحماية المستخدمين وتعزيز الثقة في استخدام الاتصالات/تكنولوجيا المعلومات والاتصالات،

يدعو الدول الأعضاء وأعضاء القطاعات والمنتسبين إليها

1 إلى تقديم مساهمات بشأن هذا الموضوع إلى لجان الدراسات ذات الصلة في الاتحاد والمساهمة في أي أنشطة أخرى يتولى الاتحاد مسؤوليتها؛

2 إلى المساهمة في بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات على الأصعدة الوطنية والإقليمية والدولية وذلك بالاضطلاع بأنشطة على النحو الموضح في الوثائق الختامية للقمة في القمة العالمية لمجتمع المعلومات، وبيان الحدث الرفيع المستوى (WSIS+10) بشأن تنفيذ نتائج القمة العالمية لمجتمع المعلومات ورؤية الحدث (WSIS-10) للقمة العالمية بعد 2015، والوثيقة الختامية للاجتماع الرفيع المستوى للجمعية العامة بشأن الاستعراض العام لتنفيذ نتائج القمة العالمية لمجتمع المعلومات، والمساهمة في إعداد تلك الأنشطة وتنفيذها؛

3 إلى زيادة الوعي بين أصحاب المصلحة كافة، بما في ذلك المنظمات وفرادى المستعملين بأهمية تعزيز الأمن السيبراني، بما في ذلك تنفيذ تدابير الحماية الأساسية؛

4 إلى تشجيع تطوير البرامج التعليمية والتدريبية لتعزيز وعي المستخدم بشأن المخاطر في الفضاء السيبراني والخطوات التي يمكن أن يتخذها المستخدمون من أجل حماية أنفسهم؛

5 إلى إدراج نهج دينامي وتكراري قائم على المخاطر للتصدي للتهديدات ومواطن الضعف الآخذة في التطور، وتعزيز ثقافة ينظر فيها إلى الأمن على أنه عملية مستمرة ومتكررة يجب أن يشملها تطوير ونشر التكنولوجيات وتطبيقاتها منذ البداية ويجب الاستمرار فيها على مدى دورة حياتها، في إطار جهودها الرامية إلى بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

6 إلى التعاون حسب الاقتضاء للتغلب على المشاكل التي تضعف الثقة والأمن في استخدام الاتصالات/تكنولوجيا المعلومات والاتصالات ومنعها.

ــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــ

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