|  |  |
| --- | --- |
| **مؤتمر المندوبين المفوضين (PP-22)بوخارست، 26 سبتمبر - 14 أكتوبر 2022** |  |
|  |  |
|  |  |
| الجلسة العامة | **الإضافة 35للوثيقة 76-A** |
|  | **1 سبتمبر 2022** |
|  | **الأصل: بالإنكليزية** |
|  |  |
| الدول الأعضاء في لجنة البلدان الأمريكية للاتصالات (CITEL) |
| المقترح الأمريكي المشترك 35 – مقترح لتعديل القرار 130 بشأن |
| تعزيز دور الاتحاد في مجال بناء الثقة والأمنفي استخدام تكنولوجيا المعلومات والاتصالات |
|  |

MOD IAP/76A35/1

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 76/189 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 76/19 للجمعية العامة للأمم المتحدة، بشأن التطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي، والنهوض بسلوك الدولة المسؤول في استخدام تكنولوجيا المعلومات والاتصالات؛

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

*ز)* القـرار 70 (المراجَع في دبي، 2018) لمؤتمر المندوبين المفوضين، بشأن تعميم منظور المساواة بين الجنسين في الاتحاد وترويج المساواة بين الجنسين وتمكين المرأة من خلال الاتصالات/تكنولوجيا المعلومات والاتصالات؛

*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 بوخارست، 2022) لهذا المؤتمر، بشأن حماية مستعملي/مستهلكي خدمات الاتصالات؛

*ل)* بالقرار 45 (المراجَع في كيغالي، 2022) 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 بوخارست، 2022) لهذا المؤتمر، بشأن دور الاتحاد في تنفيذ نتائج القمة العالمية لمجتمع المعلومات وفي الاستعراض الشامل للجمعية العامة للأمم المتحدة لتنفيذها؛

*ن)* بالقرار 50 (المراجَع في جنيف، 2022) للجمعية العالمية لتقييس الاتصالات (WTSA)، بشأن الأمن السيبراني؛

*س)* القرار 58 (المراجَع في جنيف، 2022) للجمعية العالمية لتقييس الاتصالات، بشأن تشجيع إنشاء أفرقة وطنية للتصدي للحوادث الحاسوبية لا سيما في البلدان النامية[[1]](#footnote-1)1؛

*ع)* بالقرار 67 (المراجَع في كيغالي، 2022) للمؤتمر العالمي لتنمية الاتصالات، بشأن دور قطاع تنمية الاتصالات للاتحاد الدولي للاتصالات (ITU-D) في حماية الأطفال على الخط؛

*ف)* بالقرار 69 (المراجَع في كيغالي، 2022) للمؤتمر العالمي لتنمية الاتصالات، بشأن تسهيل إنشاء أفرقة استجابة وطنية للحوادث الحاسوبية، خاصة في البلدان النامية، والتعاون فيما بينها؛

*ص)* 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)* أن التهديدات ومواطن الضعف التي تعاني منها البنية التحتية والشبكات والتكنولوجيات والتطبيقات المتعلقة بها والأجهزة لا تزال تثير تحديات أمنية متزايدة عبر الحدود الوطنية تواجهها جميع البلدان؛

*د )* أن المجلس وافق، خلال دورته لعام 2022، على المبادئ التوجيهية لقيام الاتحاد باستخدام البرنامج العالمي للأمن السيبراني في عمله؛ البرنامج العالمي للأمن السيبراني (GCA)، الذي يشجع التعاون الدولي الهادف إلى اقتراح استراتيجيات لإيجاد حلول من أجل تعزيز الثقة والأمن في استخدام الاتصالات/تكنولوجيا المعلومات والاتصالات؛

*هـ )* أن حماية هذه البنية التحتية والتصدي لهذه التحديات والتهديدات يتطلبان إجراءات وطنية وإقليمية ودولية منسقة من أجل منع وقوع أي حادث مرتبط بأمن الحواسيب 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؛

*و )* 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؛

*ز )* الحاجة إلى إحراز تقدم مستمر في التكنولوجيات الحديثة لدعم القدرة على الاكتشاف المبكر للأحداث أو الحوادث التي تؤثر على أمن الحواسيب 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 أرجحية وأثر هذه الحوادث وتخفيف المخاطر والتهديدات المتنامية التي تتعرض لها هذه المنصات؛

*ح)* 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؛

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

*ي)* أن واقع معايير الأمن السيبراني بطبيعته يعبر عن طبيعة تعدد أصحاب المصلحة في الأمن السيبراني ويتطلب مراعاة الاتحاد الدولي للاتصالات للعمليات التي يقودها الخبراء والتعاون بين الاتحاد والمنظمات الوطنية والإقليمية والعالمية والقطاعية الأخرى؛

*ي مكرراً)* أن هذا المشهد يمكن أن يكون معقداً ويمكن للاتحاد أن يؤدي دوراً هاماً في إذكاء الوعي بين الأعضاء بالعمل ذي الصلة في المنظمات الأخرى وبالعمليات والمبادرات الرامية إلى تعزيز الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات؛

*ي مكرراً ثانياً)* أن الاتحاد يمكنه أن يؤدي دوراً هاماً في إذكاء الوعي بين المنظمات الأخرى المعنية والعمليات والمبادرات المعنية بالتحديات الخاصة التي تواجهها البلدان النامية في بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات؛

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

*ك مكرراً)* أن الحاجة تدعو لمحترفي الأمن السيبراني وللتأكد من أن برامج التدريب متاحة وفعالة لتوظيف الأشخاص ذوي المهارات والخبرات المناسبة؛

*ك مكرراً ثانياً)* أنه على الرغم من التقدم المحرز في بعض المجالات، يواجه العديد من البلدان تحديات في تطوير مؤهلات ومسارات مهنية فعالة، وهذا يشكل عائقاً كبيراً أمام تعزيز الثقة والأمن في تكنولوجيا المعلومات والاتصالات؛

*ل)* 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؛

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

*ن)* أن بعض الشركات الصغيرة والمتوسطة تواجه تحديات إضافية في تنفيذ ممارسات الأمن السيبراني؛

*ن مكرراً)* الحاجة إلى زيادة الوعي وتعزيز الخطوات الأساسية بين عامة الناس التي تبين أفضل الممارسات لحماية أنفسهم من مخاطر الأمن السيبراني، بما في ذلك في المجتمعات النائية والريفية والمحرومة والفئات الضعيفة،

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؛

*ب مكرراً)* بأن الاتصالات/تكنولوجيا المعلومات والاتصالات تمكّن من تنمية المجتمع المدني وتسهم في تحقيق مستويات أعلى من المنافع الاجتماعية والإدماج الاجتماعي، وتوفر قنوات جديدة بين المواطنين والشركات والحكومات لتبادل المعارف وتعزيزها، فضلاً عن المشاركة في اتخاذ القرارات التي تؤثر على حياتهم وعملهم؛

*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 2022 قد اعتمد خطة عمل كيغالي وأولوياته لقطاع تنمية الاتصالات، ولا سيما أولوية قطاع تنمية الاتصالات بشأن الاتصالات/تكنولوجيا المعلومات والاتصالات الشاملة والآمنة من أجل التنمية المستدامة بهدف تقديم الدعم للدول الأعضاء لتحقيق الاتصالات/تكنولوجيا المعلومات والاتصالات الآمنة التنمية الرقمية للجميع؛ والمؤتمر العالمي لتنمية الاتصالات لعام 2022 اعتمد القرار 45 (المراجَع في كيغالي، 2022)، بشأن آليات تعزيز التعاون في مجال الأمن السيبراني بما في ذلك مواجهة ومكافحة الرسائل الاقتحامية، والمؤتمر العالمي لتنمية الاتصالات لعام 2022 اعتمد القرار 69 (المراجَع في كيغالي، 2022) الخاص بتسهيل إنشاء أفرقة استجابة وطنية للحوادث الحاسوبية، خاصة في البلدان النامية، والتعاون فيما بينها؛

*ﻫ )* بأن إعلان كيغالي الذي اعتمده المؤتمر العالمي لتنمية الاتصالات لعام 2022 ينص على أن: " في العصر الرقمي لا غنى عن توصيلية النطاق العريض الشاملة للجميع والآمنة وميسورة التكلفة والتي تتيح الفرص لتحفيز الإنتاجية والكفاءة، والقضاء على الفقر، وتحسين سبل العيش، وضمان أن تصبح التنمية المستدامة واقعاً ملموساً للجميع. وتبقى مواصلة بناء الاطمئنان والثقة والأمن في استخدام الاتصالات/تكنولوجيا المعلومات والاتصالات بالغة الأهمية."؛

*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-22) القرار 58 (المراجَع في جنيف، 2022)، بشأن تشجيع إنشاء أفرقة استجابة وطنية في حالات الحوادث الحاسوبية، خاصة للبلدان النامية، كما اعتمد المؤتمر العالمي لتنمية الاتصالات لعام 2022 القرار 69 (المراجَع في كيغالي، 2022)، 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 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؛

*ي)* بالنتائج ذات الصلة للجمعية العالمية لتقييس الاتصالات لعام 2022، وبالأخص:

 ’1‘ القرار 50 (المراجَع في جنيف، 2022)، بشأن الأمن السيبراني؛

 ’2‘ القرار 52 (المراجَع في جنيف، 2022)، بشأن مكافحة الرسائل الاقتحامية والتصدي لها؛

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

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

*ل مكرراً)* بأن العديد من الدول الأعضاء تواجه نقصاً كبيراً في المهارات في القوى العاملة لديها في مجال الأمن السيبراني، وأن هذا النقص في المهنيين المتمرسين في مجال الأمن السيبراني يشكل عائقاً أساسياً أمام بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات؛

*ل مكرراً ثانياً)* بأن العديد من الدول الأعضاء تواجه اختلالاً كبيراً في التوازن بين الجنسين في القوى العاملة لديها في مجال الأمن السيبراني، وهذا يزيد من صعوبة معالجة نقص المهارات؛

*ل مكرراً ثالثاً)* بأن من المهم تشجيع المزيد من الناس، ولا سيما النساء والفتيات، على اختيار مسار وظيفي في مجال الأمن السيبراني من أجل معالجة نقص المهارات؛

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

*ن)* 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؛

*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 (المراجَع في جنيف، 2022) و52 (المراجَع في الحمامات، 2016)، والقرارين 45 (المراجَع في كيغالي، 2022) و69 (المراجَع في كيغالي، 2022)؛

*ج)* أن للاتحاد دوراً أساسياً ينبغي أن يضطلع به، وعندما يتطلبه أعضاؤه، يكون أحد الخيارات العديدة المتاحة لبناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

*د)* أن الاتحاد يساعد أيضاً البلدان النامية في بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات ويدعم إنشاء أفرقة الاستجابة للحوادث الحاسوبية، بالتنسيق بين جميع المنظمات ذات الصلة؛

*هـ )* 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؛

*و )* 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؛

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

يقرر

1 أن يستمر في إيلاء هذا العمل أولوية عالية داخل الاتحاد، بأخذ خدمات وتكنولوجيات الاتصالات/تكنولوجيا المعلومات والاتصالات الجديدة والناشئة بعين الاعتبار 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 يواصل العمل، مولياً أولوية عالية طبقاً لاختصاصاته ومجالات خبراته، 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 2022؛

4 تشجيع ثقافة يُنظر فيها إلى الأمن كعملية مستمرة ومتكررة تُدمج وفق التصميم في المنتجات منذ البداية وعبر مرحلة التصنيع وتستمر طوال فترة عمرها ويتسنى للمستعملين النفاذ إليها وفهمها؛

4مكرراً تعزيز الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات بطريقة تتيح تنمية المجتمع المدني وتدعم تحقيق مستويات أعلى من المنافع الاجتماعية والاندماج الاجتماعي؛

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؛

5مكرراً الانخراط بنشاط مع البلدان النامية بشأن التحديات الخاصة التي تثيرها في بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات، وحيثما توجد تعهدات متعددة، تنسيق جهودها ودمجها 12؛

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 إعداد تقارير إحصائية تبين أثر نشر التكنولوجيات الناشئة على الأمن السيبراني وإدراج تلك النتائج في أنشطة الاتحاد في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

11 تعزيز 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 تيسير ودفع عجلة إنشاء بيئات تكنولوجيا المعلومات والاتصالات على أساس مبادئ الثقة والأمن بما يعود بالنفع على البلدان النامية؛

13 استخدام إطار البرنامج العالمي للأمن السيبراني للاتحاد لمواصلة توجيه عمل الاتحاد بشأن الجهود الرامية إلى بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات، مع مراعاة المبادئ التوجيهية التي وافق عليها المجلس لاستخدام الاتحاد للبرنامج العالمي للأمن السيبراني،

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 كيغالي، 2022)، 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 كيغالي، 2022) 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؛

9 بالنظر في نتائج الرقم القياسي العالمي للأمن السيبراني (GCI) لتوجيه مبادرات الاتحاد في مجال الأمن السيبراني، ولا سيما مراعاة الفجوات المحددة من خلال عملية الرقم القياسي العالمي للأمن السيبراني،

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 (المراجَع في جنيف، 2022) و52 (المراجعَ في الحمامات، 2016) و58 (المراجَع في جنيف، 2022) 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، من:

• القرار 50 (المراجَع في جنيف، 2022)، بشأن الأمن السيبراني؛

• القرار 52 (المراجَع في جنيف، 2022)، 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، بالاستفادة من خبرات عمليات وضع المعايير لأصحاب المصلحة المتعددين التي يقودها الخبراء، ومن نتائجها؛

4 بدعم عمل مسألة الدراسة 3/2 لقطاع تنمية الاتصالات؛

5 التعاون مع مدير مكتب تنمية الاتصالات في توزيع المعلومات على البلدان النامية بشأن المبادئ التوجيهية والتوصيات والتقارير التقنية والممارسات الفضلى المتعلقة ببناء الثقة والأمن في استخدام تكنولوجيات المعلومات والاتصالات، والتي تعدها لجان الدراسات التابعة لقطاع تقييس الاتصالات (ITU-T)،

يكلف مدير مكتب تنمية الاتصالات

1 بأن يقوم، بما يتفق مع نتائج المؤتمر العالمي لتنمية الاتصالات لعام 2022 وعملاً بالقرارات 45 (المراجَع في كيغالي، 2022) و69 (المراجَع في بوينس آيرس، 2017) و80 (المراجَع في بوينس آيرس، 2017)، لدعم المشاريع الإقليمية والعالمية بشأن الأمن السيبراني وتشجيع جميع البلدان على المشاركة في هذه الأنشطة؛

2 بدعم ومساعدة الدول الأعضاء في الاتحاد، لا سيما البلدان النامية، في جهودها لبناء القدرات بما يتسق مع تشريعاتها الوطنية للحماية؛

2مكرراً بمواصلة برامج التطوير الناجحة لدى الاتحاد التي تضع تدابير تقنية وإجرائية لتأمين الاتصالات/تكنولوجيا المعلومات والاتصالات، مثل تطوير استراتيجيات الأمن السيبراني وأفرقة الاستجابة للحوادث الحاسوبية، لمنع التهديدات السيبرانية وتحديدها ومعالجتها والتعافي منها؛

2 مكرراً ثانياً بتوجيه الدول الأعضاء في الاتحاد، بناءً على طلبها، إلى الموارد التي طورتها المنظمات الدولية الأخرى لمكافحة الجريمة السيبرانية، ولا سيما مكتب الأمم المتحدة المعني بالمخدرات والجريمة ومنظمة الإنتربول؛

3 بتقديم الدعم المالي والإداري اللازم لهذه المشاريع في حدود الموارد الحالية، بما في ذلك تلك المتعلقة باستمرارية عملية الرقم القياسي العالمي للأمن السيبراني (GCI)، 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 المعلومات ذات الصلة بتهديدات الأمن السيبراني، وأفضل 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 الأعضاء في تنمية المهارات البشرية وبناء القدرات لتعزيز الأمن السيبراني؛

8مكرراً بدعم الأعضاء لمعالجة النقص في مهارات الأمن السيبراني من خلال تشجيع الناس على الانخراط في المهن المتعلقة بالأمن السيبراني وتيسير توظيف النساء والرجال في مجال الأمن السيبراني؛

9 بدعم الأعضاء في أنشطة تقييم المخاطر المتعلقة بالأمن السيبراني؛

10 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 2022 والمؤتمر العالمي لتنمية الاتصالات لعام 2022، فيما يتعلق بأولوية قطاع تنمية الاتصالات بشأن خطة عمل كيغالي، 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 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؛

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

4مكرراً النظر في التحديات والاحتياجات المحددة في مجال الأمن السيبراني التي تواجهها الشركات الصغيرة والمتوسطة (SME)، وإدراج هذه الجوانب الخاصة في أنشطة الاتحاد لبناء الطمأنينة، والثقة، والأمن في استخدام مراكز التدريب على الإنترنت (ITC)؛

5 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؛

5مكرراً دعم الدول الأعضاء في تحديد الخطوات الأساسية التي ينبغي للجميع اتخاذها لحماية أنفسهم من المخاطر السيبرانية، وتشجيع ودعم أعضاء الاتحاد وغيرهم من أصحاب المصلحة للترويج لهذه الخطوات لدى الجمهور؛

6 تحديد وتوثيق وتعزيز 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؛

7 دعم الاستراتيجية والتنظيم والتوعية والتعاون والتقييم وتنمية المهارات؛

8 تقديم الدعم التقني والمالي اللازم في حدود الموارد المتاحة في الميزانية؛

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

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

11 دعم البلدان النامية ومساعدتها في تشجيع وتسهيل تنفيذ توصيات قطاع تقييس الاتصالات المتعلقة بالأمن،

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 مواصلة حشد خبرة الاتحاد الدولي للاتصالات في مجال التنمية بهدف تعزيز الأمن السيبراني الوطني والإقليمي والدولي لدعم أهداف التنمية المستدامة، والعمل مع الهيئات/الوكالات الأخرى ذات الصلة داخل الأمم المتحدة والهيئات الدولية الأخرى ذات الصلة، مع مراعاة الولايات ومجالات الخبرة المحددة للوكالات المختلفة، مع مراعاة الحاجة إلى تجنب ازدواج العمل بين المنظمات وبين المكاتب أو الأمانة العامة،

3 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 كيغالي، 2022) 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 الوطنية 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؛

7مكرراً إلى تحديد الخطوات الأساسية التي ينبغي لعامة الناس اتخاذها لحماية أنفسهم من المخاطر السيبرانية وتشجيع ودعم أعضاء الاتحاد وأصحاب المصلحة الآخرين لتعزيزها،

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 المستخدمين بشأن المخاطر في الفضاء السيبراني، خاصة للفئات والمجتمعات الضعيفة، والخطوات التي يمكن أن يتخذوها من أجل حماية أنفسهم؛

5 إلى إطلاع عامة الناس على نتائج تبادل المعلومات بين الدول الأعضاء والمنظمات المختصة والمتخصصين لتعزيز وتقوية المعرفة بشأن الأمن السيبراني؛

6 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 الاتصالات/تكنولوجيا المعلومات والاتصالات؛

6 مكرراً إلى تعزيز المبادرات الرامية إلى تشجيع المزيد من الناس على ممارسة مهنة الأمن السيبراني وتزويدهم بفرص التدريب؛

6 مكرراً ثانياً إلى تقديم الدعم بحيث تتمكن النساء والفتيات من القيام بدراسات والعمل في مجال الأمن السيبراني؛

7 إلى التعاون حسب الاقتضاء للتغلب على المشاكل التي تضعف الثقة والأمن في استخدام الاتصالات/تكنولوجيا المعلومات والاتصالات ومنعها وكذلك تحسين الحلول لحماية الأمن السيبراني وقدرة الشبكات على الصمود؛

8 إلى المساهمة في تحسين عملية الرقم القياسي العالمي للأمن السيبراني (GCI)، بما في ذلك مناقشة المنهجية والهيكل ومقاييس الترجيح والأسئلة.

ــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــ

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