

القرار 45 (المراجع في باكو، 2025)

آليات لتعزيز التعاون في مجال الأمن السيبراني، بما في ذلك مكافحة الرسائل الاحتمالية والتصدي لها

إن المؤتمر العالمي لتنمية الاتصالات (باكو، 2025)،

إذ يذكّر

(أ) بالقرار 130 (المراجع في بوخارست، 2022) لمؤتمر المندوبين المفوضين، بشأن تعزيز دور الاتحاد في مجال بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات؛

(ب) بالقرار 174 (المراجع في بوسان، 2014) لمؤتمر المندوبين المفوضين، بشأن دور الاتحاد الدولي للاتصالات في قضايا السياسة العامة الدولية المتعلقة بمخاطر الاستعمال غير القانوني لتكنولوجيا المعلومات والاتصالات؛

(ج) بالقرار 179 (المراجع في بوخارست، 2022) لمؤتمر المندوبين المفوضين، بشأن دور الاتحاد الدولي للاتصالات في حماية الأطفال على الإنترنت؛

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

(هـ) بالقرار 50 (المراجع في نيودلهي، 2024) للجمعية العالمية لتقييس الاتصالات (WTSA)، بشأن الأمن السيبراني؛

(و) بالقرار 52 (المراجع في نيودلهي، 2024) للجمعية العالمية لتقييس الاتصالات، بشأن مكافحة الرسائل الاحتمالية والتصدي لها؛

(ز) بالقرار 58 (المراجع في نيودلهي، 2024) للجمعية العالمية لتقييس الاتصالات، بشأن تشجيع إنشاء وتعزيز الأفرقة الوطنية للاستجابة في حالات للحوادث الحاسوبية، خاصة للبلدان النامية¹؛

(ح) بالقرار 69 (المراجع في باكو، 2025) لهذا المؤتمر، بشأن تيسير إنشاء أفرقة استجابة للحوادث الحاسوبية، خاصة في البلدان النامية، والتعاون فيما بينها؛

(ط) بالقرار 67 (المراجع في باكو، 2025) لهذا المؤتمر، بشأن دور قطاع تنمية الاتصالات (ITU-D) في حماية الأطفال على الإنترنت؛

¹ تشمل أقل البلدان نمواً والدول الجزرية الصغيرة النامية والبلدان النامية غير الساحلية والبلدان التي تمر اقتصاداتها بمرحلة انتقالية.

(ي) بالقرار 214 (بوخارست، 2022) لمؤتمر المندوبين المفوضين، بشأن تكنولوجيا الذكاء الاصطناعي والاتصالات/تكنولوجيا المعلومات والاتصالات، الذي يحدد النطاق الذي يمكن من خلاله لمدير مكتب تنمية الاتصالات (BDT) دعم عمل قطاع تنمية الاتصالات في التعامل مع التحديات والفرص التي يجلبها الذكاء الاصطناعي كتكنولوجيا جديدة وناشئة، من حيث تطبيقه على الأمن السيبراني ومكافحة الرسائل الاحتمالية؛

(ك) بالآراء ذات الصلة للمنتدى العالمي السادس لسياسات الاتصالات/تكنولوجيا المعلومات والاتصالات لعام 2021 التي تقع ضمن ولاية قطاع تنمية الاتصالات؛

(ل) بالمبادئ والمقاصد والأهداف النبيلة المتجسدة في ميثاق الأمم المتحدة وفي الإعلان العالمي لحقوق الإنسان؛

(م) بأن الاتحاد هو جهة التيسير الرئيسية لخط العمل جيم5 الوارد في برنامج عمل تونس بشأن مجتمع المعلومات (بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات) للقمّة العالمية لمجتمع المعلومات (WSIS)؛

(ن) بالأحكام المتصلة بالأمن السيبراني في التزام تونس وفي برنامج عمل تونس للقمّة العالمية لمجتمع المعلومات؛

(س) بالأولويات المواضيعية المنصوص عليها في الخطة الاستراتيجية للاتحاد المعمول بها؛

(ع) بإعلان مبادئ جنيف للقمّة العالمية لمجتمع المعلومات (WSIS)، الذي تنص الفقرة 37 منه على: "أن الرسائل الاحتمالية تمثل مشكلة هامة ومتزايدة للمستعملين والشبكات ولإنترنت برمتها، وينبغي تناول مسألة الرسائل الاحتمالية والأمن السيبراني على المستويات الوطنية والدولية الملائمة"؛

(ف) بمسألة الدراسة 3/2 لدى قطاع تنمية الاتصالات بشأن "تأمين شبكات المعلومات والاتصالات: الممارسات الفضلى من أجل تطوير ثقافة الأمن السيبراني"؛

(ص) بتقرير رئيس فريق الخبراء رفيع المستوى (HLEG) المعني بالبرنامج العالمي للأمن السيبراني (GCA) والذي شكله الأمين العام للاتحاد عملاً بمتطلبات خط العمل جيم5 للقمّة العالمية لمجتمع المعلومات بشأن بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات، ووفقاً للقرار 140 (المراجع في بوخارست، 2018) لمؤتمر المندوبين المفوضين، بشأن دور الاتحاد بوصفه الجهة المسهلة الرئيسية لخط العمل جيم5 والقرار 58 (المراجع في نيودلهي، 2024) للجمعية العالمية لتقييس الاتصالات، بشأن تشجيع إنشاء وتعزيز الأفرقة الوطنية للاستجابة في حالات الحوادث الحاسوبية، خاصة للبلدان النامية؛

ق) بأن المجلس وافق، خلال دورته في عام 2022، على المبادئ التوجيهية بشأن استخدام الاتحاد للبرنامج العالمي للأمن السيبراني في عمله؛

ر) بأن الاتحاد الدولي للاتصالات ومكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC) وقعا مذكرة تفاهم (MoU) بهدف تعزيز الأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

ش) بالتعاهد الرقمي العالمي المعتمد كالملحق 1 بالقرار 79/1 للجمعية العامة للأمم المتحدة (UNGA)، الذي يحدد الأهداف والمبادئ والالتزامات والإجراءات المتعلقة بالتحول الرقمي²،

وإذ يضع في اعتباره

أ) دور الاتصالات/تكنولوجيات المعلومات والاتصالات كأداة فعّالة في تعزيز السلام والتنمية الاقتصادية والأمن والاستقرار والديمقراطية والتلاحم الاجتماعي والإدارة الرشيدة وحكم القانون، وضرورة مواجهة التحديات المتصاعدة والتهديدات الناجمة عن الاستخدامات الضارة لهذه التكنولوجيات بما في ذلك للأغراض الإجرامية والإرهابية، وفي الوقت ذاته احترام حقوق الإنسان (انظر أيضاً الفقرة 15 من التزام تونس)؛

ب) ضرورة بناء الثقة والأمن في استعمال الاتصالات/تكنولوجيات المعلومات والاتصالات بتعزيز إطار الثقة (الفقرة 39 من برنامج عمل تونس)، وضرورة قيام الحكومات، بالتعاون مع غيرها من أصحاب المصلحة في إطار دور كل منها، بوضع التشريعات الضرورية لتحقيق في الجرائم السيبرانية وملاحقة مرتكبيها على الأصعدة الوطنية والتعاون على الأصعدة الإقليمية والدولية مع مراعاة الأطر القائمة؛

ج) أن من شأن وجود حاسوب كمومي ذي صلة بالتجفير أن يشكل تهديداً لبعض أساليب التجفير المستخدمة في شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات؛

د) أن القرار 64/211 للجمعية العامة للأمم المتحدة (UNGA) يدعو الدول الأعضاء، عندما ترى ذلك ملائماً، إلى استعمال الأداة الطوعية للتقييم الذاتي الملحقة بالقرار، من أجل الجهود الوطنية؛

² مع الإحاطة علماً بأن بعض البلدان لم تصادق على التعاهد الرقمي العالمي (GDC).

هـ) أن الدول الأعضاء عليها وضع برامج وطنية للأمن السيبراني تتركز حول خطة وطنية وشراكات بين القطاعين العام والخاص وأساس قانوني سليم وقدرات لإدارة الحوادث ومراقبتها والإنذار بوقوعها والاستجابة لها والاستعادة بعد وقوعها وثقافة وعي، مسترشدة بالعديد من الموارد التي استحدثها و/أو وفرها الاتحاد والأعضاء فيه وشركاؤه، متى وُجدت رغبة في ذلك أو حسب الانطباق؛

و) أن اتباع نهج تكراري قائم على تقييم المخاطر في الأمن السيبراني يمكن من إرساء ممارسات الأمن السيبراني وتطبيقها حسب الحاجة من أجل التصدي للتهديدات ومواطن الضعف المتطورة باستمرار، وأن الأمن السيبراني عملية متواصلة وتكرارية ويجب أن تُدمج في عمليات تطوير ونشر التكنولوجيات وتطبيقاتها من البداية وأن تستمر طوال دورة حياتها؛

ز) أن الخسائر الهائلة والمتزايدة التي يتكبدها مستعملو أنظمة الاتصالات/تكنولوجيا المعلومات والاتصالات نتيجة تفاقم مشكلة حوادث الأمن السيبراني بما في ذلك المتصلة منها بإساءة استعمال الاتصالات/تكنولوجيا المعلومات والاتصالات لأغراض خبيثة على صعيد العالم، كل ذلك يهدد جميع البلدان المتقدمة والنامية في العالم دون استثناء؛

ح) الأسباب الموجبة لاعتماد القرار 37 (المراجع في باكو، 2025) لهذا المؤتمر، بشأن سد الفجوة الرقمية، فيما يخص أهمية قيام أصحاب المصلحة بتنفيذه على المستوى الدولي وخطوط العمل المشار إليها في الفقرة 108 من برنامج عمل تونس، ومنها بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات؛

ط) نتائج العديد من أنشطة الاتحاد المتعلقة بالأمن السيبراني، وخاصة، على سبيل المثال لا الحصر، الأنشطة التي ينسقها مكتب تنمية الاتصالات، من أجل إنجاز ولاية الاتحاد بوصفه الميسر في تنفيذ خط العمل جيم5؛

ي) أن مجموعة واسعة من المنظمات من جميع قطاعات المجتمع تعمل بالتعاون فيما بينها من أجل تعزيز الأمن السيبراني لخدمات وتكنولوجيا الاتصالات/تكنولوجيا المعلومات والاتصالات، وبناء الثقة فيها؛

ك) أن جميع أصحاب المصلحة المعنيين يمكنهم الاضطلاع بدور قيّم في إذكاء الوعي بقضايا الأمن السيبراني، ولا سيما بين النساء والأطفال والأشخاص ذوي الإعاقة والأشخاص ذوي الاحتياجات المحددة والأشخاص ذوي الإعاقات المتصلة بالعمر؛

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

(م) أن العديد من الدول الأعضاء تواجه أوجه نقص كبيرة في مهارات القوى العاملة لديها في مجال الأمن السيبراني، وأن هذا النقص في المهنيين المتمرسين في مجال الأمن السيبراني يشكل عائقاً أساسياً أمام الأمن السيبراني، وأن من المهم تشجيع المزيد من الأشخاص على اختيار مسار وظيفي في مجال الأمن السيبراني؛

(ن) أن تنمية المهارات البشرية وبناء القدرات من العوامل الأساسية لتعزيز الأمن السيبراني بما يشمل الحاجة إلى إذكاء الوعي وتعزيز التدابير الأمنية الأساسية المتعلقة بالسلامة السيبرانية، التي ينبغي أن يتخذها الجميع، بما في ذلك النساء والأطفال والأشخاص ذوو الإعاقة والأشخاص ذوو الاحتياجات المحددة والأشخاص ذوو الإعاقات المتصلة بالعمر، لحماية أنفسهم من مخاطر الأمن السيبراني؛

(س) أن المنظمات الوطنية والإقليمية والدولية الأخرى ذات الصلة توفر للدول الأعضاء وفقاً لدور كل منها مختلف المعلومات والمواد والممارسات الفضلى والموارد المالية، حسب الاقتضاء؛

(ع) أن البرنامج العالمي للأمن السيبراني (GCA) يشجع التعاون الدولي الهادف إلى اقتراح استراتيجيات لإيجاد حلول من أجل تعزيز الثقة والأمن في استخدام الاتصالات/تكنولوجيا المعلومات والاتصالات؛

(ف) أن الأمن السيبراني والصمود السيبراني قد أصبحا عنصريين أساسيين على الأصعدة الوطنية والإقليمية والدولية من أجل تحقيق التنمية الرقمية المستدامة، وأن قطاع تنمية الاتصالات في إطار ولايته يمكن أن يواصل المساهمة في بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات في هذه الجهود،

وإذ يدرك

(أ) التحديات التي تواجهها الدول، ولا سيما البلدان النامية، في بناء الثقة والأمن في استخدام الاتصالات/تكنولوجيا المعلومات والاتصالات؛

(ب) أن التدابير المتخذة لضمان استقرار وأمن شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات، والحماية من التهديدات السيبرانية/الجريمة السيبرانية والرسائل الاقتحامية، يجب أن تحمي وتحتزم الأحكام المتعلقة بالخصوصية وحرية التعبير المتجسدة في الأجزاء ذات الصلة من الإعلان العالمي لحقوق الإنسان (انظر أيضاً الفقرة 42 من برنامج عمل تونس) والعهد الدولي الخاص بالحقوق المدنية والسياسية؛

(ج) أن القرار 75/176 للجمعية العامة للأمم المتحدة، بشأن الحق في الخصوصية في العصر الرقمي، يؤكد، من بين عدة أمور، أن "الحقوق نفسها التي يتمتع بها الأشخاص خارج الإنترنت يجب أن تحظى بالحماية أيضاً على الإنترنت، بما في ذلك الحق في الخصوصية، مع إيلاء اهتمام خاص لحماية الأطفال"؛

(د) ضرورة اتخاذ الإجراءات المناسبة والتدابير الوقائية، حسبما يحددها القانون، ضد إساءة استعمال الاتصالات/تكنولوجيا المعلومات والاتصالات كما ذكرت في إطار "الأبعاد الأخلاقية لمجتمع المعلومات" في إعلان مبادئ وخطة عمل جنيف (الفقرة 43 من برنامج عمل تونس) للقمة العالمية لمجتمع المعلومات، وضرورة مكافحة الإرهاب بجميع أشكاله ومظاهره على شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات وفي الوقت ذاته احترام حقوق الإنسان والوفاء بالواجبات الأخرى التي يفرضها القانون الدولي، على النحو المحدد في الفقرة 81 من منطوق قرار الجمعية العامة للأمم المتحدة 60/1 بشأن نتائج القمة العالمية لعام 2005 وأهمية أمن واستمرار واستقرار الإنترنت، وضرورة حماية الإنترنت وغيرها من شبكات تكنولوجيا المعلومات والاتصالات من التهديدات ومواطن الضعف (الفقرة 45 من برنامج عمل تونس)، مع ضمان احترام الخصوصية وحماية المعلومات والبيانات الشخصية، سواء من خلال اعتماد التشريعات أو من خلال تنفيذ أطر تعاونية أو اتباع الشركات التجارية والمستعملين للممارسات الفضلى والتدابير التنظيمية الذاتية والتدابير التقنية (الفقرة 46 من برنامج عمل تونس)؛

(هـ) ضرورة التصدي الفعال للتحديات والتهديدات الناتجة عن استخدام الاتصالات/تكنولوجيات المعلومات والاتصالات مثل استخدامها لأغراض لا تتفق مع أهداف حفظ الاستقرار والأمن الدوليين ويمكن أن تؤثر على سلامة البنية التحتية داخل الدول، والعمل بشكل تعاوني على منع إساءة استخدام موارد وتكنولوجيا المعلومات، وفي الوقت ذاته احترام حقوق الإنسان؛

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

(ز) رغبة جميع الأطراف المعنية والتزامها ببناء مجتمع معلومات جامع وذي توجه تنموي ويضع البشر في صميم اهتمامه، يقوم على أساس أغراض ومبادئ ميثاق الأمم المتحدة والقانون الدولي والتعددية والاحترام الكامل للإعلان العالمي لحقوق الإنسان والالتزام به، حتى يتسنى للناس في كل مكان إنشاء المعلومات والمعارف والنفاذ إليها واستعمالها وتبادلها على نحو آمن، كي يحققوا إمكاناتهم بالكامل ويبلغوا الأهداف والمقاصد الإنمائية المتفق عليها دولياً، بما في ذلك أهداف التنمية المستدامة (SDG)؛

(ح) أحكام الفقرات 4 و5 و55 من إعلان مبادئ جنيف، وأن حرية التعبير وحرية تدفق المعلومات والمعارف والأفكار تعود بالنفع على التنمية؛

(ط) أن مرحلة تونس للقمة العالمية لمجتمع المعلومات مثلت فرصة فريدة لإذكاء الوعي بما تجلبه تكنولوجيا المعلومات والاتصالات من فوائد للإنسانية وبما يمكنها إحداثه من تحول في الأنشطة البشرية والتفاعل بين البشر وفي حياتهم وبذلك تسهم في زيادة الثقة في المستقبل، شريطة استعمال الاتصالات/تكنولوجيات المعلومات والاتصالات استعمالاً آمناً، وعلى النحو الذي يبيّنه تنفيذ نواتج القمة العالمية لمجتمع المعلومات؛

(ي) أن الرسائل الاقتحامية تمثل مشكلة عالمية ذات خصائص مختلفة في المناطق المختلفة، وأن النهج التعاوني لأصحاب المصلحة المتعددين ضروري لمكافحتها؛

(ك) أن التلاعب بكيفية عرض معلومات طالب النداء عند استلام نداء من قبل المستخدم يمثل قضية هامة فيما يتعلق بالرسائل الاقتحامية الصوتية، التي يمكن أن تنشأ عن مواطن ضعف في الأمن السيبراني وقد تتطلب تطبيق التدابير المناسبة واستمرار التعاون الدولي بين جميع أصحاب المصلحة؛

(ل) الحاجة إلى التصدي على نحو فعال للمشكلة الهامة التي يطرحها البريد الاقتحامي، كما تدعو إلى ذلك الفقرة 41 من برنامج عمل تونس؛ علاوة على التهديدات السيبرانية وحوادث الأمن السيبراني؛

(م) أن لا غنى عن آليات شاملة لمكافحة الرسائل الاقتحامية لحماية مستخدمي الاتصالات/تكنولوجيا المعلومات والاتصالات، لا سيما في البلدان النامية،

وإذ يلاحظ

(ن) الحاجة إلى التنسيق الفعال داخل قطاع تنمية الاتصالات؛

(ب) العمل المستمر بشأن الجوانب المختلفة لأمن الاتصالات/تكنولوجيا المعلومات والاتصالات الذي تضطلع به لجنة الدراسات 17 (الأمن) بقطاع تقييس الاتصالات بالاتحاد (ITU-T) وغيرها من المنظمات المعنية بوضع المعايير على جوانب مختلفة لأمن الاتصالات/تكنولوجيا المعلومات والاتصالات؛

(ج) أن الرسائل الاقتحامية تمثل مشكلة هامة وما زالت تشكل تهديداً للمستعملين والشبكات ولإنترنت جميعاً وأنه ينبغي تناول مسألة الأمن السيبراني على المستويات الوطنية والإقليمية والدولية؛

(د) أن التعاون والعمل المشترك ما بين الدول الأعضاء وأعضاء القطاع وأصحاب المصلحة ذوي الصلة يسهم في بناء ثقافة للأمن السيبراني وفي الحفاظ عليها؛

(هـ) العمل المتواصل المضطلع به في القطاع الخاص والأوساط الأكاديمية والمجتمع التقني وفي إطار جميع أصحاب المصلحة الآخرين ذوي الصلة لتعزيز الأمن السيبراني لقطاع الاتصالات/تكنولوجيا المعلومات والاتصالات؛

(و) أن البلدان قد تواجه تحديات وفرصاً جديدة كبيرة فيما يتعلق بالأمن السيبراني ومكافحة الرسائل الاقتحامية، مع استمرار تطور خدمات وتكنولوجيا الاتصالات/تكنولوجيا المعلومات والاتصالات الجديدة والناشئة؛

(ز) أن جوانب الأمن السيبراني المتعلقة بحماية البيانات والمعلومات المحددة لهوية الشخص (PII) تمثل قضية هامة؛

(ح) أن الحاجة تدعو إلى تعزيز نمو وتطوير قوى عاملة متنوعة وماهرة في مجال الأمن السيبراني، قادرة على معالجة وتخفيف المخاطر السيبرانية، وتعزيز على أهمية المؤهلات والمسارات المهنية الفعالة،

يقرر

1 مواصلة اعتبار الأمن السيبراني في صدارة أنشطة الاتحاد ذات الأولوية، مع مراعاة خدمات وتكنولوجيا الاتصالات/تكنولوجيا المعلومات والاتصالات الجديدة والناشئة، والاستمرار، في إطار مجالات اختصاصاته الرئيسية، بدراسة مسألة بناء الثقة والأمن في استعمال الاتصالات/تكنولوجيا المعلومات والاتصالات من خلال إذكاء الوعي وتبادل الممارسات الفضلى، وتقديم المساعدة في تنفيذ التدابير التقنية وتطوير الأدوات ومواد التدريب المناسبة لتعزيز ثقافة الأمن السيبراني؛

2 مواصلة تعزيز العمل والتعاون وتبادل المعلومات مع جميع المنظمات الدولية والإقليمية ذات الصلة فيما يتعلق بالمبادرات المتصلة بالأمن السيبراني بما في ذلك الصمود السيبراني في مجالات اختصاصاتها، مع مراعاة احتياجات مساعدة البلدان النامية؛

3 دعوة منظمات التمويل الوطنية والدولية إلى إيلاء مزيد من الاهتمام لمنح دعم مالي كبير، بوسائل منها الترتيبات الائتمانية التفضيلية، للبرامج الوطنية المتعلقة بالمهارات التقنية في مجال الأمن السيبراني وتوفير التدريب للبلدان النامية التي تفتقر إلى المهارات التقنية اللازمة في مجال الأمن السيبراني، مع إعطاء الأولوية للشباب والنساء والأشخاص ذوي الإعاقة؛

4 مواصلة تعزيز الشراكات الرامية إلى بناء القدرات في مجال الأمن السيبراني، بما يمكّن قطاع تنمية الاتصالات من العمل مع المعنيين الآخرين من أصحاب المصلحة والمنظمات، الذين لديهم الخبرة والمعرفة في هذا المجال؛

5 مواصلة دمج الاعتبارات المتعلقة بالأمن السيبراني في جميع مبادرات ومشاريع التنمية الرقمية التي ينفذها قطاع تنمية الاتصالات،

يكلف مدير مكتب تنمية الاتصالات

1 بتشجيع ثقافة يُنظر فيها إلى الأمن كعملية مستمرة ومتكررة تُدمج في المنتجات منذ البداية وتستمر طوال فترة عمرها ويتسنى للمستعملين النفاذ إليها وفهمها؛

2 بمواصلة تنظيم اجتماعات للدول الأعضاء وأعضاء القطاع وأصحاب المصلحة المعنيين الآخرين بالتعاون مع المنظمات ذات الصلة، حسب الاقتضاء، لمناقشة أساليب ووسائل تعزيز الأمن السيبراني، بما في ذلك مكافحة الرسائل الاحتمالية والتصدي لها، مع مراعاة مساهمات الأعضاء وبالتعاون مع مدير مكتب تقييس الاتصالات (TSB)؛

3 بمواصلة إجراء دراسات عن تعزيز الأمن السيبراني والصمود السيبراني في البلدان النامية على المستويين الإقليمي والدولي، بالتعاون مع المنظمات ذات الصلة وأصحاب المصلحة المعنيين، على أساس تحديد واضح لاحتياجاتها، لا سيما تلك المتعلقة باستخدام الاتصالات/تكنولوجيا المعلومات والاتصالات، بما في ذلك مكافحة الرسائل الاحتمالية والتصدي لها، وخدمات وتكنولوجيا الاتصالات/تكنولوجيا المعلومات والاتصالات الجديدة والناشئة وكذلك حماية الأطفال على الإنترنت والشباب وجميع الأشخاص الضعفاء، وجوانب الأمن السيبراني المتعلقة بحماية البيانات والمعلومات المحددة لهوية الشخص (PII)؛

4 بالنظر في نتائج الرقم القياسي العالمي للأمن السيبراني (GCI) لتوجيه مبادرات مكتب تنمية الاتصالات في مجال الأمن السيبراني، ولا سيما مراعاة الفجوات المحددة من خلال عملية الرقم القياسي العالمي للأمن السيبراني؛

5 بالحفاظ على كيفية عرض نتائج الرقم القياسي العالمي للأمن السيبراني في مستويات بدلاً من ترتيبها فردياً من أجل التعبير بدقة أكبر عن تطور الأمن السيبراني في الدول الأعضاء؛

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

7 بدعم مبادرات الدول الأعضاء، خاصةً في البلدان النامية، فيما يتعلق بآليات تعزيز التعاون في مجال الأمن السيبراني، بما في ذلك مكافحة الرسائل الاحتمالية والتصدي لها؛

8 بأن يدعم الدول الأعضاء في تحديد التدابير الأمنية الأساسية للسلامة السيبرانية التي ينبغي للجميع اتخاذها لحماية أنفسهم من المخاطر السيبرانية والرسائل الاحتمالية، ويشجع أعضاء الاتحاد وأصحاب المصلحة الآخرين على ترويج هذه التدابير للجمهور ويدعمهم في القيام بذلك؛

9 بأن يساعد الدول الأعضاء، لا سيما البلدان النامية، من خلال تقديم الإرشادات والممارسات الفضلى للتعامل مع التحديات والفرص المتصلة بالأمن السيبراني ومكافحة الرسائل الاحتمالية التي تسببها خدمات وتكنولوجيا الاتصالات/تكنولوجيا المعلومات والاتصالات الجديدة والناشئة؛

10 بالمساعدة على إذكاء الوعي والفهم بالحاجة إلى الإعداد للانتقال الوطني إلى التجفير ما بعد الحوسبة الكمومية في شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات، في إطار اختصاصات الاتحاد وخبراته، وتشجيع الأعضاء على تبادل الممارسات الجيدة والتجارب الوطنية في هذا الصدد؛

11 بأن يعمم على البلدان النامية معلومات بشأن المبادئ التوجيهية والتوصيات والتقارير التقنية والممارسات الفضلى المتعلقة بالأمن السيبراني، التي تضعها لجان الدراسات بقطاع تقييس الاتصالات بالاتحاد (ITU-T)، ولا سيما لجنة الدراسات 17 بوصفها اللجنة الرئيسية المعنية بالأمن، بالتعاون مع مدير مكتب تقييس الاتصالات؛

12 بالمساعدة في نشر التوصيات التقنية لقطاع تقييس الاتصالات وموارد المعلومات ذات الصلة التي وضعتها منظمات أخرى والتي يمكن أن تساعد البلدان النامية في تحديد وتنفيذ التدابير التي يمكن أن تمنع الرسائل الاقتحامية الصوتية الناجمة عن مواطن ضعف الأمن السيبراني وتكتشف وتخفف من حدتها، وتشجع التعاون الدولي بين جميع أصحاب المصلحة؛

13 بأن يساعد البلدان النامية على تحسين استعدادها لضمان مستوى عالٍ وفعال للأمن السيبراني، بما في ذلك الصمود السيبراني، للبنى التحتية الحيوية للاتصالات/تكنولوجيا المعلومات والاتصالات الخاصة بها، بما في ذلك من خلال عقد حلقات دراسية وورش عمل ودورات تدريبية لتعزيز السلامة السيبرانية، وأحداث أخرى في إطار ركائز البرنامج العالمي للأمن السيبراني، بشأن التدابير التنظيمية والتقنية وتدابير بناء القدرات، بالتعاون مع مدير مكتب تقييس الاتصالات، حسب الاقتضاء؛

14 بأن يساعد الدول الأعضاء في وضع إطار ملائم بين البلدان النامية يسمح بسرعة التصدي للحوادث الكبيرة بما في ذلك تعزيز تبادل المعلومات الطوعي بين الإدارات المهتمة، وأن يقترح خطة عمل لتعزيز حمايتها وتعزيز الصمود السيبراني، مع مراعاة الآليات والشراكات، حسب الاقتضاء؛

15 بجمع وتبادل المعلومات من الدول الأعضاء فيما يتعلق باللوائح التنظيمية والسياسات والنهج الأخرى التي تضعها و/أو تنفذها الهيئات التنظيمية الوطنية للاتصالات والمنظمات الأخرى من أصحاب المصلحة من أجل بناء الثقة والأمن في الاتصالات/تكنولوجيات المعلومات والاتصالات، وذلك بالاقتراح مع العمل المضطلع به في إطار مسألة الدراسة 3/2 للجنة الدراسات 2 بقطاع تنمية الاتصالات؛

16 بتشجيع جميع أصحاب المصلحة المعنيين على المشاركة و/أو المساهمة في أنشطة مراكز التدريب التابعة لأكاديمية الاتحاد الدولي للاتصالات من أجل التدريب والتثقيف والتوعية بقضايا الأمن السيبراني، في إطار البرنامج العالمي للأمن السيبراني (GCA)؛

17 بأن يساعد الدول الأعضاء عن طريق تعزيز إفادتها بأحدث المعلومات المتعلقة بقضايا الأمن السيبراني والممارسات الفضلى، لتتخذ فيها الدول الأعضاء؛

18 بتقديم تقرير عن نتائج تنفيذ هذا القرار إلى المؤتمر العالمي المقبل لتنمية الاتصالات؛

19 بمواصلة التشاور مع الأعضاء بشأن تحسين عملية الرقم القياسي العالمي للأمن السيبراني، بما في ذلك مناقشة المنهجية والمؤشرات والهيكل والترجيح والأسئلة، بالاستعانة بفريق الخبراء حسب الاقتضاء، مع مراعاة الآثار المالية؛

20 بمواصلة دعم شبكة المرأة (NoW) بقطاع تنمية الاتصالات وغيرها من المبادرات الرامية إلى تشجيع المشاركة الفعالة للمرأة في الأنشطة المتعلقة بالأمن السيبراني والأدوار القيادية في قطاع تنمية الاتصالات؛

21 بالاحتفاظ بمستودع للممارسات الفضلى بشأن التدابير التي تسهل على الأشخاص، ولا سيما النساء والفتيات، اختيار مسار وظيفي في مجال الأمن السيبراني وتشجيعهم على ذلك؛ وتطوير هذا المستودع وتعزيزه،

يدعو الأمين العام بالتنسيق مع مديري مكتب الاتصالات الراديوية ومكتب تقييم الاتصالات ومكتب تنمية الاتصالات إلى

1 تقديم تقرير بشأن مذكرات التفاهم الموقعة بين البلدان، علاوةً على أشكال التعاون القائمة، مع تقديم تحليل لأوضاعها ونطاقها وتطبيقات آليات التعاون هذه لتعزيز الأمن السيبراني ومكافحة التهديدات السيبرانية، بغية تمكين الدول الأعضاء من تحديد مدى الاحتياج إلى مزيدٍ من مذكرات التفاهم أو الآليات؛

2 دعم مشاريع الأمن السيبراني الإقليمية والعالمية ودعوة جميع البلدان إلى المشاركة في هذه الأنشطة وعلى الأخص البلدان النامية؛

3 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، والحاجة إلى تجنب ازدواج العمل بين المنظمات وبين المكاتب أو الأمانة العامة،

يطلب إلى الأمين العام

أن يتقدم بتقرير عن نتائج هذه الأنشطة إلى اجتماعات المجلس اللاحقة وإلى مؤتمرات المندوبين المفوضين، حسب الاقتضاء،

يدعو الدول الأعضاء وأعضاء القطاع والمنتسبين والهيئات الأكاديمية إلى

- 1 أن توفر الدعم اللازم وأن تعمل بشكل فعال في تنفيذ هذا القرار؛
- 2 أن تواصل الشراكة مع قطاع تنمية الاتصالات لتوفير الموارد اللازمة لتنفيذ المبادرات التي تهدف إلى دعم البلدان النامية، مع إيلاء اهتمام خاص لأقل البلدان نمواً والبلدان النامية غير الساحلية والدول الجزرية الصغيرة النامية، في تنمية قدراتها في مجال الأمن السيبراني، عبر مشروع الأمن السيبراني من أجل المصلحة العامة مثلاً؛
- 3 أن تعترف بالأمن السيبراني، بما في ذلك الجوانب ذات الصلة بتأثير خدمات وتكنولوجيات الاتصالات/تكنولوجيات المعلومات والاتصالات الجديدة والناشئة، والتصدي للبريد الاقتحامي ومكافحته، كمسألتين لهما أولوية عالية وأن تتخذ الإجراءات الملائمة وأن تسهم في بناء الثقة والأمن في استخدام الاتصالات/تكنولوجيات المعلومات والاتصالات على الصعد الوطنية والإقليمية والدولية؛
- 4 أن تشجع مقدمي الخدمات على حماية أنفسهم من مخاطر الأمن السيبراني المحددة، و تقليل تعرضها لهذه المخاطر، والاجتهاد في ضمان استمرار الخدمات المقدمة وتقديم إخطارات بشأن بانتهاكات الأمن السيبراني وفقاً للقوانين الوطنية؛
- 5 أن تعزز المبادرات التي تشجع المزيد من الأشخاص، وخاصة النساء والفتيات، على دخول مهنة الأمن السيبراني، بما في ذلك من خلال تطوير برامج التعليم والتدريب ذات الصلة؛
- 6 أن تساهم في الحلول المبتكرة التي تعالج تهديدات الأمن السيبراني ومكافحة الرسائل الاقتحامية، وتبادل المعلومات حولها؛
- 7 أن تتعاون بشكل وثيق للمساعدة في مواجهة التحديات والاستفادة من الفرص الناشئة عن التكنولوجيات الجديدة والناشئة فيما يتعلق بالأمن السيبراني لخدمات وتكنولوجيات الاتصالات/تكنولوجيا المعلومات والاتصالات، ومكافحة الرسائل الاقتحامية، بما في ذلك من خلال الجهود الوطنية والإقليمية والدولية، حسب الاقتضاء؛
- 8 أن تتعاون فيما بينها على المستوى الوطني بغية تعزيز الحلول الرامية إلى حماية الأمن السيبراني للشبكات وقدرتها على الصمود؛
- 9 أن تحيط الاتحاد علماً بأطر التعاون القائمة فيما بين الأعضاء ومع سائر الكيانات والوكالات، إقليمية كانت أو دولية، على الصعيد الثنائي الأطراف؛

10 أن تساهم في العمل في إطار مسألة دراسة الأمن السيبراني ذات الصلة بقطاع تنمية الاتصالات وفي مبادرات قطاع تنمية الاتصالات الأخرى المتعلقة بالأمن السيبراني؛

11 أن تشجع تطوير البرامج التدريبية وتعزيز وعي المستخدم بالمخاطر السيبرانية، مستهدفةً النساء والأطفال والأشخاص ذوي الإعاقة وذوي الاحتياجات المحددة والأشخاص ذوي الإعاقات المرتبطة بالعمر على وجه الخصوص، مع بيان الخطوات التي يمكن أن يتخذوها من أجل حماية أنفسهم من مثل هذه المخاطر؛

12 أن تشجع تطوير الأدوات والمواد اللازمة لتعزيز الأمن السيبراني والصمود السيبراني للشركات الصغيرة والمتوسطة (SME)؛

13 أن تشارك في تحسين عملية الرقم القياسي العالمي للأمن السيبراني (GCI)، بما في ذلك المناقشة المتعلقة بالمنهجية والهيكل والوزن الترجيحي والأسئلة، مستعينةً بفريق خبراء الرقم القياسي العالمي للأمن السيبراني؛

14 أن تساهم في المناقشات وتبادل المعلومات وبناء القدرات والدراسات بشأن التحديات والفرص المتعلقة بالأمن السيبراني ومكافحة الرسائل الاحتمالية مع تطور تكنولوجيات الذكاء الاصطناعي واستخدامها في الاتصالات/تكنولوجيات المعلومات والاتصالات لتحسين كفاءتها وقدراتها؛

15 أن تستفيد من أكاديمية الاتحاد لبناء القدرات والتدريب على خدمات وتكنولوجيات الاتصالات/تكنولوجيا المعلومات والاتصالات الجديدة والناشئة ومواضيع الأمن السيبراني ذات الصلة،

يدعو الدول الأعضاء إلى

1 استقصاء وتحليل ممارسات استخدام الاتصالات/تكنولوجيات المعلومات والاتصالات الجديدة والناشئة للتصدي للرسائل الاحتمالية؛

2 تشجيع جميع أصحاب المصلحة المعنيين على المساعدة في إذكاء وعي الجمهور بالمخاطر السيبرانية، وخاصةً في صفوف النساء والأطفال والأشخاص ذوي الإعاقة وذوي الاحتياجات المحددة والأشخاص ذوي الإعاقات المرتبطة بالعمر؛

3 المشاركة بنشاط في عمل قطاع تنمية الاتصالات بشأن الأمن السيبراني ومكافحة انتشار الرسائل الاحتمالية والتصدي لها، بتقديم دورات تدريبية وأنشطة ورش عمل تقنية للهيئات التنظيمية ومشغلي الاتصالات؛

4 وضع إطاراً مناسباً يسمح بالاستجابة السريعة لحوادث الأمن السيبراني الحرجة وأن تقترح خطة عمل لمنع مثل هذه الحوادث والتخفيف من أثارها والتعافي منها؛

- 5 وضع استراتيجيات وتوفير إمكانيات على المستوى الوطني لضمان حماية البنى التحتية الحيوية الوطنية، بما في ذلك تعزيز متانة البنى التحتية للاتصالات/تكنولوجيا المعلومات والاتصالات؛
- 6 اتخاذ خطوات نحو تطوير قدراتها الوطنية في مجال الأمن السيبراني مع مراعاة ركائز الرقم القياسي العالمي للأمن السيبراني (GCI)، حسب الاقتضاء؛
- 7 تعزيز تبادل المعلومات بشأن الأمن السيبراني على الصعد الوطنية والإقليمية والدولية؛
- 8 المساهمة في مستودع الاتحاد للممارسات الفضلى بشأن التدابير التي تسهل على الأشخاص، ولا سيما النساء والفتيات، اختيار مسار وظيفي في مجال الأمن السيبراني وتشجيعهم المزيد منهم على ذلك.