# الجرائم الإلكترونية: المخاطر الجديدة على الأمن العالمي

## *القرار الذي اعتمد بتوافق الآراء* من قبل الجمعية العامة الـ146 للاتحاد البرلماني الدولي*
## *(المنامة، 15 آذار/مارس 2023)*

إن الجمعية العامة الـ146 للاتحاد البرلماني الدولي،

*إذ تدين* جميع أشكال الجرائم الإلكترونية، *وإذ تعيد تأكيد* ضرورة مكافحة هذه الأعمال من خلال التعاون الدولي

*وإذ تؤكد من جديد* إطار الأمم المتحدة الحالي لسلوك الدول المسؤول في استخدام تكنولوجيا المعلومات والاتصالات وضرورة تنفيذ هذا الإطار،

*وإذ تعترف* بضرورة بناء الثقة والتفاهم المتبادل بين البلدان للتصدي للاستخدام الخبيث لتكنولوجيا المعلومات والاتصالات من جانب الجهات الفاعلة الحكومية وغير الحكومية الذين لا يعرفون قيوداً ولا حدوداً،

*وإذ تلاحظ* تزايد استخدام تكنولوجيا المعلومات والاتصالات والاعتماد عليها على الصعيد العالمي،

*وإذ تدرك* الزيادة في أنشطة الجرائم الإلكترونية بسبب زيادة الرقمنة التي سرّعت وتيرتها جائحة كوفيد-19،

*وإذ تلاحظ* مسؤولية البرلمانات عن بناء إطار تنظيمي يحمي المواطنين في الفضاء الإلكتروني بهياكل أساسية وموارد جديدة، بالطريقة نفسها التي تحملها في العالم المادي،

* أعرب وفد الهند عن تحفظه على الفقرة 25 من المنطوق.

أعرب وفد روسيا الاتحادية عن تحفظه على الفقرة 11 من الديباجة، والفقرة 1 من المنطوق.

*وإذ تشير* إلى قرار الجمعية العامة للأمم المتحدة 72/31 المؤرخ 10 كانون الأول/ديسمبر 1976 بشأن *اتفاقية حظر استخدام تقنيات التغيير في البيئة لأغراض عسكرية أو لأية أغراض عدائية أخرى*، والقراران 63/55 المؤرخ 4 كانون الأول/ديسمبر 2000 و121/56 المؤرخ 19 كانون الأول/ديسمبر 2001 *بشأن مكافحة إساءة استخدام تكنولوجيا المعلومات لأغراض إجرامية*، والقرار 239/57 المؤرخ 31 كانون الثاني/يناير 2003 بشأن *إنشاء ثقافة عالمية للأمن السيبراني*،

*وإذ تشير أيضاً إلى* القرارات السنوية للجمعية العامة للأمم المتحدة بشأن *التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، ولا سيما القرار* 28/69 المؤرخ 2 كانون الأول/ديسمبر 2014، والقرار 266/73 المؤرخ 22 كانون الأول/ديسمبر 2018، الذي بموجبه أنشئ فريق الخبراء الحكوميين التابع للأمم المتحدة المعني بالنهوض بسلوك الدول المسؤول في سياق الأمن الدولي، والقرار 240/75 المؤرخ 31 كانون الأول/ديسمبر 2020 الذي بموجبه أنشئ الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات واستخدامها 2021-2025، *وإذ تشدد* على المعايير الطوعية وغير الملزمة المتعلقة بسلوك الدول المسؤول في استخدام تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي، التي وضعها فريق الخبراء الحكوميين وأيدها قرار الجمعية العامة للأمم المتحدة 237/70 المؤرخ 23 كانون الأول/ديسمبر 2015 الذي يدعو الدول الأعضاء في الأمم المتحدة إلى الاسترشاد بهذه المعايير، وكذلك، من خلال قرار الجمعية العامة للأمم المتحدة 37/77 المؤرخ 7 كانون الأول/ديسمبر 2022، وضع برنامج عمل للأمم المتحدة لمناقشة التهديدات القائمة والمحتملة ودعم قدرات الدول وجهودها لتنفيذ الالتزامات والنهوض بها،

*وإذ تستذكر أيضاً اتفاقية* الأمم المتحدة *لمكافحة الجريمة المنظمة عبر الوطنية* المؤرخة 15 تشرين الثاني/نوفمبر 2000، واتفاقية الأمم المتحدة *لمكافحة الفساد* المؤرخة 31 تشرين الأول/أكتوبر 2003،

*وإذ تشدد على* أهمية الاتفاقيات الإقليمية المتعلقة بالجريمة الإلكترونية والجريمة المنظمة عبر الوطنية، وتبادل المعلومات والمساعدة الإدارية، بما في ذلك *اتفاقية مجلس أوروبا بشأن الجرائم الإلكترونية* المؤرخة 23 تشرين الثاني/نوفمبر 2001، *وبروتوكولها الإضافي بشأن تجريم الأفعال المرتبطة بالتمييز العنصري وكراهية الأجانب التي ترتكب عبر أنظمة الكمبيوتر*، المؤرخة 28 كانون الثاني/يناير 2003، *واتفاقية التعاون في ضمان أمن المعلومات الدولية بين الدول الأعضاء في منظمة شنغهاي للتعاون*، المؤرخة 16 حزيران/يونيو 2009،

*والاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات* المؤرخة 21 كانون الأول/ديسمبر 2010، *والقانون النموذجي* لبرلمان أمريكا اللاتينية ومنطقة البحر الكاريبي *بشأن جرائم الفضاء الإلكتروني* الصادر في تشرين الثاني/نوفمبر 2013 وتحديثاته، *والقانون النموذجي* لبرلمان أمريكا اللاتينية ومنطقة البحر الكاريبي *بشأن المنع الاجتماعي للعنف والجريمة الصادر في تشرين الثاني/نوفمبر 2015*، *والقانون النموذجي* لبرلمان أمريكا اللاتينية ومنطقة البحر الكاريبي *بشأن جرائم الحاسوب* الصادر في شباط/فبراير 2021، *والقانون النموذجي* لبرلمان أمريكا اللاتينية ومنطقة البحر الكاريبي *لمكافحة الاتجار غير المشروع والجريمة عبر الوطنية* الصادر في شباط/فبراير 2021، *واتفاقية التعاون بين الدول الأعضاء في رابطة الدول المستقلة الكومنولث في مجال ضمان أمن* المعلومات المؤرخة 20 تشرين الثاني/نوفمبر 2013، *واتفاقية التعاون بين الدول الأعضاء في رابطة الدول المستقلة الكومنولث في مكافحة الجرائم في ميدان تكنولوجيا المعلومات* المؤرخة 28 أيلول/سبتمبر 2018، *واتفاقية* الاتحاد الإفريقي *بشأن الأمن الإلكتروني وحماية البيانات الشخصية* المؤرخة 27 حزيران/يونيو 2014،

*وإذ تشدد أيضاً* على أن *اتفاقية* مجلس أوروبا *المتعلقة بجرائم الفضاء الإلكتروني* التي يفتح باب الانضمام إليها أمام أي بلد، قد أصبحت صكاً ذا أهمية عالمية مع وجود دول أطراف من جميع مناطق العالم والتأثير فيها،

*وإذ تشير* إلى عمل الاتحاد البرلماني الدولي بشأن مختلف المخاطر الجديدة التي تواجهها مجتمعاتنا التي تتزايد رقمنتها، بما في ذلك قراري الاتحاد البرلماني الدولي: *الحرب الإلكترونية: تهديد خطير للسلم والأمن العالمي* (اعتمد في الجمعية العامة الـ 132، هانوي، 1 نيسان/أبريل 2015)، *والتشريعات في جميع أنحاء العالم لمكافحة الاستغلال والاعتداء الجنسيين للأطفال عبر الإنترنت* (اعتمد في الجمعية العامة الـ 143، مدريد، 30 تشرين الثاني/نوفمبر 2021)، الذي يشير أيضاً إلى *اتفاقية* مجلس أوروبا *بشأن حماية الأطفال من الاستغلال الجنسي والاعتداء الجنسي* ("اتفاقية لانزاروت")، المؤرخة 25 تشرين الأول/أكتوبر 2007،

*وإذ تثني* على عمل الأمم المتحدة بشأن النهوض بسلوك الدول المسؤول في الفضاء الإلكتروني،

*وإذ تشيد* بالجهود التي تبذلها الأمم المتحدة لسن اتفاقية دولية بشأن الجرائم الإلكترونية، من خلال قرار الجمعية العامة 247/74 المؤرخ 27 كانون الأول/ديسمبر 2019، *وإذ ترحب* بإنشاء لجنة مخصصة مكلفة بصياغة هذه الاتفاقية،

*وإذ ترحب* بمشاركة الاتحاد البرلماني الدولي في عملية التشاور بين الجهات المعنية المتعددة التابعة لتلك اللجنة المخصصة من أجل ضمان الاستماع إلى صوت البرلمانات،

*وإذ تلاحظ* الحاجة إلى اتباع نهج عالمي إزاء مسألة الجرائم الإلكترونية وعواقبها الخطيرة على المواطنين، فضلاً عن الحاجة لحماية السلام والأمن والاستقرار الاقتصادي على الصعيد العالمي مع التمسك بالمبادئ الأساسية لحقوق الإنسان بما في ذلك حرية التعبير،

*وإذ تعترف* بالحاجة الملحة إلى أن يتخذ المشرعون والحكومات وجميع الجهات المعنية خطوات وطنية أكثر استباقية لمكافحة الجرائم الإلكترونية، نظراً لكثافتها المتجددة وطابعها السريع التطور،

*وإذ تسلم* أيضاً بأن جميع الإجراءات المتخذة في هذا الميدان تحتاج إلى احترام حقوق الإنسان والحقوق الأساسية في صميمها،

*وإذ تلاحظ* تفاوت التطور في قدرة البلدان على تطبيق تكنولوجيا المعلومات والاتصالات وقدرتها على حماية الهياكل الأساسية لتكنولوجيا المعلومات والاتصالات، *وإذ تشدد* على الحاجة إلى زيادة المساعدة والتعاون التقنيين، ولا سيما للبلدان النامية،

*وإذ تلاحظ أيضاً أن* على الدول أن تتصرف وفقاً لالتزاماتها بموجب القانون الدولي لحقوق الإنسان، بما في ذلك على سبيل المثال لا الحصر *العهد الدولي الخاص بالحقوق المدنية والسياسية*، *واتفاقية حقوق الطفل*، *واتفاقية مناهضة التعذيب وغيره من ضروب المعاملة أو العقوبة القاسية أو اللاإنسانية أو المهينة*، *واتفاقية القضاء على جميع أشكال التمييز ضد المرأة*، والبروتوكولات الإضافية وغيرها من صكوك حقوق الإنسان الدولية ذات الصلة،

*وإذ تعترف* بالحاجة إلى اتخاذ إجراءات برلمانية دولية مشتركة لزيادة الوعي وتنفيذ القواعد الطوعية وغير الملزمة في ما يتعلق بسلوك الدولة المسؤول في استخدام تكنولوجيا المعلومات والاتصالات،

*وإذ تلاحظ* أن الجرائم الإلكترونية قد تشكل تهديداً خطيراً للعمليات الديمقراطية، وبخاصة التدخل في الانتخابات من خلال انتهاكات الأمن الإلكتروني أو حسابات مزيفة على وسائل التواصل الاجتماعي،

*وإذ تقر* بأن النساء والشباب والأطفال وكبار السن والأشخاص ذوي الإعاقة والمجتمعات العرقية معرضين بشكل خاص للجرائم الإلكترونية،

*وإذ تسلم أيضاً* بالحاجة إلى بذل جهود لتعزيز المساواة بين الرجال والنساء وتمكين النساء والفتيات بجميع تنوعهن، بما في ذلك من خلال تعميم مراعاة المنظور الجندري، ووضع السياسات والبرامج والتشريعات وتنفيذها وتطبيقها في هذا الميدان،

*وإذ تلاحظ* طبيعة التهديدات والمخاطر الناجمة عن الجرائم الإلكترونية التي تهدد السلم والأمن الدوليين، والتطورات الهائلة في الفضاء الإلكتروني، التي نجم عنها ازدياد تعقيد الأساليب التي يستخدمها مرتكبو الجرائم الإلكترونية،

*وإذ تلاحظ أيضاً* أن الجرائم الإلكترونية تتضمن على سبيل المثال لا الحصر الهجمات على أنظمة الكمبيوتر، وانتهاكات الخصوصية، وإنشاء البرامج الخبيثة ونشرها، وتسهل أيضاً الهجمات بشكل متزايد على الهياكل الأساسية المدنية، فضلاً عن الأعمال الأخرى التي يمكن أن تحدث خارج الإنترنت، وتيسرها أنظمة الكمبيوتر، بما في ذلك الاحتيال عبر الإنترنت، وتجارة المخدرات، وغسل الأموال، وجرائم الكراهية، والاتجار بالبشر، والعنف القائم على الجندر الذي تيسره التكنولوجيا مثل التحرش الجنسي، والتهديدات، والمطاردة، والتنمر، والخطاب المتحيز ضد المرأة، والاستغلال الجنسي للنساء والأطفال عبر الإنترنت – وجميعها تؤثر سلباً على الأمن العالمي، والاستقرار الاقتصادي،

*وإذ تضع في اعتبارها* أن معظم القوانين الوطنية قد سُنت قبل نشوء الجرائم الإلكترونية، ومن ثم فهي لا تتصدى دائماً لهذه التهديدات على النحو المناسب،

1. *تشجع* البرلمانات على النظر في اتخاذ الخطوات اللازمة لبلدانها للانضمام، إذا لم تكن قد فعلت ذلك بعد، إلى الصكوك الدولية القائمة التي تتناول استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية، بما في ذلك اتفاقية مجلس أوروبا بشأن الجرائم الإلكترونية، وهي أكثر المعاهدات المتعددة الأطراف شمولاً بشأن الجرائم الإلكترونية السارية والمفتوحة للانضمام إليها من قبل جميع الدول؛

2. *وتطلب من* البرلمانات أن تحرص من أن التشريعات بشأن الجرائم الإلكترونية محدثة وذات صلة، وفقاً للقانون الدولي، بما فيه صكوك حقوق الإنسان الدولية، من أجل تخصيص الموارد الضرورية لهذه الغاية، وإشراك جميع الجهات المعنية، بما فيها القطاع الخاص، والأوساط الأكاديمية، والمجتمع المدني، والمجتمع التقني، بالنظر إلى الزيادة المستمرة في حجم هذه الأعمال ونطاقها وسرعتها وتعقدها وتواترها وآثارها على الأمن الوطني، والسلم والأمن الدوليين، والاستقرار الاقتصادي العالمي، وأن تدرج كذلك في هذه

التشريعات الولاية القضائية خارج الإقليم لتمكين مقاضاة الأفعال الإجرامية، بصرف النظر عن مكان ارتكاب هذه الأعمال وما إذا كانت تشكل جرائم في الولاية القضائية الأجنبية المعنية؛

3. *وتحث* البرلمانات على ضمان إدراج تقييمات الأثر على حقوق الإنسان في جميع العمليات التشريعية المتعلقة بالجرائم الإلكترونية؛

4. *وتدعو* البرلمانات إلى تعزيز قدرة ضباط إنفاذ القانون، بما في ذلك سلطات التحقيق والمدعون العامون والقضاة، في مجال الجرائم الإلكترونية، وتجهيزهم للتحقيق الفعال والملاحقة القضائية والفصل في قضايا الجرائم الإلكترونية؛

5. *وتشجع* البرلمانات على الاستفادة الكاملة من وظيفتها الرقابية لضمان أن تكون لدى الحكومات الأدوات اللازمة، بما في ذلك الموارد والقدرات الملائمة، لمكافحة الزيادة السريعة في الجرائم الإلكترونية والتصدي لها ولحماية الأمن الإلكترون، للمواطنين وهويتهم وخصوصيتهم وبياناتهم، مع صون حقوق الإنسان والحريات؛

6. *وتوصي بشدة* بأن تضمن البرلمانات أن الإطار التشريعي بشأن حماية الهياكل الأساسية الوطنية، بما فيها الهياكل الأساسية التي تدعم الإنترنت، محدثة، أو أنها تضع أطراً مماثلة عند الاقتضاء؛

7. *وتشجع* البرلمانات على الترويج لفضاء إلكتروني مفتوح ومجاني وآمن من خلال دعوة حكوماتها إلى الالتزام بقواعد الأمم المتحدة المتعلقة بسلوك الدول المسؤول في الفضاء الإلكتروني من أجل وقف الجريمة الإلكترونية، وكذلك، مرتكبي الجرائم الإلكترونية والجهات الفاعلة الخبيثة، للاستجابة في الوقت الحقيقي إن أمكن، وفقاً لسيادة القانون والاحترام الكامل للقانون الدولي لحقوق الإنسان والحريات الأساسية، لتأمين سلسلة التوريد للشركات في بلدانها، والتقديم بشكل طوعي تقارير عن مواطن الضعف المحتملة أمام أطراف ثالثة لمساعدتها في منع وقوع حوادث في المستقبل، وعلى وجه الخصوص دعم وحماية جميع فرق الاستجابة للحوادث الإلكترونية داخل حدودها وخارجها؛

8. *وتشجع أيضاً* البرلمانات على صياغة تشريعات مراعية للمنظور الجندري، تعزز خدمات الأمن الإلكتروني الشاملة التي تعطي الأولوية للوقاية (التوعية ومراجعة الحسابات والتدريب)، والكشف عن الحوادث (24 ساعة في اليوم، 7 أيام في الأسبوع)، والتصدي الفوري والفعال للتهديدات الإلكترونية، من خلال نهج يركز على الضحايا؛

9. *وتوصي* بأن تعزز البرلمانات إقامة المؤسسات والهيئات ذات الصلة – مثل المراكز الوطنية لأمن الفضاء الإلكتروني، وفرق الاستجابة للطوارئ الحاسوبية، وفرق التصدي للحوادث الأمنية الحاسوبية، ومراكز العمليات الأمنية – حيثما لا ترد هذه المؤسسات والهيئات في بلدانها؛

10. *وتوصي أيضاً* بأن تضمن جميع البرلمانات أن تتوافر لهذه المؤسسات والهيئات موارد كافية من الموازنة وموظفون متخصصون، بمن فيهم النساء، للسماح باستجابة مرنة وفعالة للجرائم الإلكترونية، وحماية الهياكل الأساسية الحيوية والمؤسسات العامة والشركات والمواطنين من دون انتهاك الخصوصية، مع الأخذ في الاعتبار أن الرقمنة المتزايدة للخدمات والمرافق العامة يمكن أن تنطوي على تعرض كبير للمخاطر الرقمية؛

11. *وتحث* البرلمانات على تعزيز التنسيق الدولي بين هذه المؤسسات والهيئات من أجل الرصد المستمر للتهديدات الإلكترونية ومنعها وكشفها والتحقيق فيها والتصدي لها؛

12. *وتدعو* البرلمانات إلى تشجيع حكوماتها على توفير تدريب محدد في مجال الأمن الإلكتروني من أجل المساعدة في زيادة عدد المتخصصين في الأمن الإلكتروني وتعزيز أدائهم؛

13. *وتؤكد من جديد* أن توافر بيئة مفتوحة وآمنة ومستقرة ويسهل الوصول إليها وسلمية لتكنولوجيا المعلومات والاتصالات أمر ضروري للجميع ويتطلب تعاوناً فعالاً بين الدول للحد من المخاطر التي يتعرض لها السلام والأمن الدوليان، *وتدعو* المجتمع الدولي إلى تعزيز الاحترام الكامل لحقوق الإنسان والحريات الأساسية؛

14. *وتطلب من* البرلمانات أن تشجع الاستثمار في البحث والتطوير، وأن تدرج في تصميم كل مشروع اعتمادات خاصة بالأمن الإلكتروني، مع تخصيص اعتمادات مناسبة في الموازنة، من أجل التنبؤ بالتهديدات الإلكترونية الناشئة المحتملة والحماية منها؛

15. *وتشجع* البرلمانات على إقامة شراكات مع دوائر الصناعة والأوساط الأكاديمية وجميع الجهات المعنية الأخرى، بما في ذلك المجتمع المدني، مع حكوماتهما كميسرين رئيسيين، من أجل تعزيز نظام قوي وتعاوني للأمن الإلكتروني يحترم مبادئ حقوق الإنسان والالتزامات الدولية لحقوق الإنسان احتراماً كاملاً؛

16. *وتطلب* من البرلمانات والبرلمانيين أن يشاركوا بنشاط في الترويج لفهم وطني مشترك ومستكمل لطبيعة الجرائم الإلكترونية على نحو ما يعانيه المواطنون والمنظمات والمؤسسات؛

17. *وتحث* البرلمانات على المساعدة في تعزيز "ثقافة حقيقية للأمن الإلكتروني" من خلال وضع مناهج تعليمية تركز على تدريب الأجيال المقبلة، ابتداء من الطفولة فصاعداً، على محو الأمية الرقمية والدراية التكنولوجية، تغطي كلا من الفرص الكبيرة المتاحة والمخاطر الجسيمة التي تشكلها التكنولوجيا؛

18. *وتوصي* بأن توسع البرلمانات نطاق الحماية المتاحة للنساء والشباب والأطفال وكبار السن والأشخاص ذوي الإعاقة والمجتمعات العرقية، وغيرهم من الفئات الضعيفة في الفضاء الإلكتروني، مع مراعاة احترام حقوق الإنسان ومنع العنف القائم على الجندر عند وضع السياسات التعليمية المتعلقة باستخدام وسائل التواصل الاجتماعي؛

19. *وتحث* البرلمانات على اتخاذ الإجراءات اللازمة لحماية اللحظات الحاسمة في الديمقراطية، ولا سيما الفترات التي يمارس فيها المواطنون حقهم في التصويت، من أجل تجنب الهجمات والتدخلات التي تسعى إلى التأثير في حرية تشكيل الرأي العام أو تغييره أو انتهاكه أثناء العملية الانتخابية؛

20. *وتطلب من* المجتمع الدولي أن يتخذ إجراءات لحماية الديمقراطية من خلال ضمان توفير حماية خاصة لجميع البرلمانات في جميع أنحاء العالم، بوصفها مؤسسات تمثل إرادة الشعب، من خلال إدراجها في قوائم الهياكل الأساسية المدنية، والخدمات الأساسية؛

21. *وتشدد* على الحاجة إلى زيادة تعزيز التعاون والمساعدة الدوليين في مجال أمن تكنولوجيا المعلومات والاتصالات وبناء القدرات، كوسيلة لسد الفجوات الرقمية وتعزيز الاستجابة للتهديدات الإلكترونية على الصعيد العالمي؛

22. *وتطلب من* البرلمانات أن تعمق فهمها للطابع المعقد وطبيعة الجرائم الإلكترونية سريعة التطور من خلال تمكين التبادل المفتوح للمعرفة والخبرة والتجربة وعقد ندوات وورشات عمل ومؤتمرات متخصصة بشأن هذا الموضوع؛

23. *وتدعو* الأمانة العامة للاتحاد البرلماني الدولي إلى القيام، بالشراكة مع المنظمات الأخرى ذات الصلة، بتعزيز هذه الرؤية الجديدة لأمن الفضاء الإلكتروني من خلال دعم البرلمانات في مساعيها لبناء القدرات؛

24. *وتوصي* بأن يقوم الاتحاد البرلماني الدولي، بوصفه المنظمة العالمية للبرلمانات، الاضطلاع بدور قيادي في منع الجرائم الإلكترونية ومكافحتها وفي تحفيز المرونة الإلكترونية من خلال المشاركة في جميع المحافل الدولية ذات الصلة، بما في ذلك تلك التي تقودها الأمم المتحدة، بغية ضمان سماع صوت البرلمانات؛

25. *وتشجع على* إنشاء مجموعة عمل معنية بالجرائم الإلكترونية، تابعة للمجلس الحاكم للاتحاد البرلماني الدولي، وتتمثل مهمتها المحددة في الامتثال للولايات والأهداف المحددة في هذا القرار، التي يجب أن تشمل صلاحياتها دعم عملية تعزيز اتفاقية دولية بشأن الجرائم الإلكترونية في إطار الأمم المتحدة، وتعزيز قدرات البرلمانات الأعضاء في الاتحاد البرلماني الدولي من حيث سن القوانين والرقابة وإعداد الموازنة؛

26. *وتوصي* بأن يعمل الاتحاد البرلماني الدولي على زيادة الوعي بين البرلمانات بشأن تحقيق أهداف التنمية المستدامة من خلال، قبل كل شيء، التزاماتها العالمية بالأمن الرقمي؛

Inter-Parliamentary Union
For democracy. For everyone.

146TH IPU ASSEMBLY
المنامة، البحرين
MANAMA, BAHRAIN
11-15 MARCH 2023 - ١١-١٥ مارس ٢٠٢٣

# 146th IPU Assembly
## Manama (11–15 March 2023)

## Cybercrimes: The new risks to global security

***Resolution adopted by consensus[*] by the 146th IPU Assembly***
***(Manama, 15 March 2023)***

The 146th Assembly of the Inter-Parliamentary Union,

*Condemning* all forms of cybercrime and *reaffirming* the need to combat such acts through international cooperation,

*Reaffirming* the existing United Nations framework for responsible State behaviour in the use of information and communications technologies (ICTs) and the need to implement this framework,

*Recognizing* the need to build trust and mutual understanding between countries in response to the malicious use of ICTs by State as well as non-State actors, who recognize neither boundaries nor borders,

*Observing* the growing use of and dependence on ICTs worldwide,

*Cognizant of* the increase in cybercrime activities due to increasing digitalization, accelerated by the COVID-19 pandemic,

*Noting* the responsibility of parliaments to build a regulatory framework that protects citizens in cyberspace with new infrastructure and resources, in the same way as in the physical world,

*Recalling* United Nations General Assembly resolution 31/72 of 10 December 1976 on the *Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques*, resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on *Combating the criminal misuse of information technologies*, and resolution 57/239 of 31 January 2003 on the *Creation of a global culture of cybersecurity*,

*Recalling also* the annual resolutions of the United Nations General Assembly on *Developments in the field of information and telecommunications in the context of international security*, and in particular resolution 69/28 of 2 December 2014, resolution 73/266 of 22 December 2018 establishing the Group of Governmental Experts on advancing responsible State behaviour in the context of international security, and resolution 75/240 of 31 December 2020 establishing the Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025, and *highlighting* the voluntary and non-binding norms of responsible State behaviour in the use of ICTs in the context of international security, developed by the Group of Governmental Experts and endorsed by United Nations General Assembly resolution 70/237 of 23 December 2015, which calls on United Nations Member States to be guided by these norms, as well as the establishment, through United Nations General Assembly resolution 77/37 of 7 December 2022, of a United Nations programme of action to discuss existing and potential threats and to support States' capacities and efforts to implement and advance commitments,

[*] The delegation of India expressed reservations on operative paragraph 25.
The delegation of the Russian Federation expressed reservations on preambular paragraph 11 and operative paragraph 1

*Recalling further* the United Nations *Convention against Transnational Organized Crime* of 15 November 2000 and the United Nations *Convention against Corruption* of 31 October 2003,

*Stressing* the importance of regional conventions on cybercrime, transnational organized crime, exchange of information and administrative assistance, including the Council of Europe *Convention on Cybercrime* of 23 November 2001 and its *Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* of 28 January 2003, the *Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization* of 16 June 2009, the *Arab Convention on Combating Information Technology Offences* of 21 December 2010, the Latin American and Caribbean Parliament (Parlatino) *Model Law on Cybercrime* of November 2013 and its updates, the Parlatino *Model Law on Social Prevention of Violence and Crime* of November 2015, the Parlatino *Model Law on Computer Crimes* of February 2021, and the Parlatino *Model Law on Combating Illicit Trade and Transnational Crime* of February 2021, the *Agreement on Cooperation among the Member States of the Commonwealth of Independent States in the Field of Ensuring Information Security* of 20 November 2013, the *Agreement on Cooperation among the Member States of the Commonwealth of Independent States in the Fight Against Crimes in the Field of Information Technology* of 28 September 2018, and the African Union *Convention on Cyber Security and Personal Data Protection* of 27 June 2014,

*Stressing also* that the Council of Europe *Convention on Cybercrime*, which is open for accession by any country, has become an instrument of global significance, with States Parties from, and impact in, all regions of the world,

*Recalling* the IPU's work on the various new risks faced by our increasingly digitized societies, including the IPU resolutions *Cyber warfare: A serious threat to peace and global security* (adopted at the 132nd Assembly, Hanoi, 1 April 2015), and *Legislation worldwide to combat online child sexual exploitation and abuse* (adopted at the 143rd Assembly, Madrid, 30 November 2021), which also recalls the Council of Europe *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse* (the "Lanzarote Convention") of 25 October 2007,

*Commending* the work of the United Nations on advancing responsible State behaviour in cyberspace,

*Commending also* the efforts of the United Nations to enact, through General Assembly resolution 74/247 of 27 December 2019, an international cybercrime convention, and *welcoming* the creation of an ad hoc committee charged with drafting this convention,

*Welcoming* the participation of the IPU in the multi-stakeholder consultation process of that ad hoc committee in order to ensure that the voice of parliaments is heard,

*Noting* the need for a global approach to the issue of cybercrime and its serious consequences for citizens, as well as the need to protect global peace, security and economic stability while upholding the basic tenets of human rights including freedom of speech,

*Recognizing* the urgent need for legislators, governments and all stakeholders to take more proactive national steps to combat cybercrime, given its renewed intensity and rapidly evolving nature,

*Recognizing also* that all actions in this field need to have respect for human rights and fundamental rights at their centre,

*Noting* the uneven development in countries' ICT application capacity and ability to protect ICT infrastructure, and *emphasizing* the need for increased technical assistance and collaboration, especially for developing countries,

*Noting also* that States shall act in accordance with their obligations under international human rights law, including but not limited to the *International Covenant on Civil and Political Rights*, the *Convention on the Rights of the Child*, the *Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*, the *Convention on the Elimination of All Forms of Discrimination against Women*, and additional protocols and other relevant international human rights instruments,

*Recognizing* the need for common, international parliamentary action to advance awareness and implementation of voluntary and non-binding norms regarding responsible State behaviour in the use of ICTs,

*Noting* that cybercrime may constitute a serious threat to democratic processes, especially interference in elections through cybersecurity breaches or false social media accounts,

*Acknowledging* that women, young people, children, elderly people, people with disabilities, and racialized communities are particularly vulnerable to cybercrimes,

*Acknowledging also* the need for efforts to promote gender equality and the empowerment of women and girls in all their diversity, including through gender mainstreaming, in the development, implementation and application of policies, programmes and legislation in this field,

*Noting* the nature of the threats and risks of transnational cybercrime to international peace and security, and the tremendous developments in cyberspace, as a result of which the methods used by cybercriminals are becoming increasingly sophisticated,

*Noting also* that cybercrime includes but is not limited to attacks on computer systems, breaches of privacy, the creation and deployment of malware, and, increasingly, the facilitation of attacks on critical civilian infrastructure, as well as other acts that can occur offline and be facilitated by computer systems, including online fraud, drug trade, money-laundering, hate crimes, human trafficking, and technology-facilitated gender-based violence such as sexual harassment, threats, stalking, bullying, sexist hate speech, and the sexual exploitation of women and children via the internet – all of which negatively affect global security and economic stability,

*Considering* that most national laws were enacted before cybercrime arose and therefore do not always adequately address these threats,

1. *Encourages* parliaments to consider taking the necessary steps for their country to accede, if it has not yet done so, to existing international instruments that address the use of ICTs for criminal purposes, including the Council of Europe *Convention on Cybercrime*, which is the most comprehensive multilateral cybercrime treaty in force and is open for accession by all States;

2. *Calls upon* parliaments to make sure their legislation on cybercrime is up to date and relevant, in accordance with international law, including international human rights instruments, to allocate the necessary resources to this end and to engage all stakeholders, including the private sector, academia, civil society and the technical community, considering the ongoing increase in the scale, scope, speed, complexity and frequency of such acts and their implications for national security, international peace and security, and global economic stability, as well as to include in such legislation extraterritorial jurisdiction to enable the prosecution of criminal acts, irrespective of where those acts were committed and whether they constitute offences in the foreign jurisdiction in question;

3. *Urges* parliaments to ensure that human rights impact assessments are embedded in all legislative processes on cybercrime;

4. *Calls upon* parliaments to enhance the capacity of law enforcement officers, including investigative authorities, prosecutors and judges, in the field of cybercrime, and to equip them to effectively investigate, prosecute and adjudicate cases of cybercrime offences;

5. *Encourages* parliaments to make full use of their oversight function to ensure that governments have the tools, including appropriate resources and capacity, to prevent and combat the rapid increase in cybercrimes and to protect the cybersecurity, identity, privacy and data of citizens while safeguarding human rights and freedoms;

6. *Strongly recommends* that parliaments ensure that their national legislative frameworks on the protection of critical national infrastructure, including the infrastructure that supports the internet, are up to date, or that they establish such frameworks where necessary;

7. *Encourages* parliaments to promote an open, free and secure cyberspace by calling on their governments to abide by the United Nations norms of responsible State behaviour in cyberspace, to cooperate in fighting cybercrime as well as cybercriminals and malicious actors, to respond to requests for assistance and capacity-building, if possible in real time, in accordance with the rule of law and fully respecting international human rights law and fundamental freedoms, to secure the supply chain of companies in their countries, to report voluntarily on potential vulnerabilities to third parties to assist them in preventing future incidents, and in particular to support and protect all cyber incident response teams within and beyond their borders;

8. *Also encourages* parliaments to draft gender-responsive legislation promoting cross-cutting cybersecurity services that prioritize prevention (awareness-raising, auditing and training), incident detection (24 hours a day, 7 days a week), and an instant and efficient response to cyber threats, through a victim-centric approach

9. *Recommends* that parliaments promote the establishment of relevant institutions and bodies – such as national cybersecurity centres, computer emergency response teams, computer security incident response teams and security operations centres – where these do not already exist in their country;

10. *Also recommends* that all parliaments ensure that such institutions and bodies have adequate budgetary resources and specialized personnel, including women cybersecurity experts, to allow for an agile, timely and effective response to cybercrime and to protect critical civilian infrastructure, public institutions, companies and citizens without breaching privacy, while taking into account that the increasing digitalization of public services and utilities could imply major exposure to digital risks;

11. *Urges* parliaments to promote international coordination between such institutions and bodies in order to monitor, prevent, detect, investigate and respond to cyber threats;

12. *Invites* parliaments to encourage their governments to provide specific cybersecurity training in order to help increase the number of cybersecurity professionals and to strengthen their performance;

13. *Reaffirms* that an open, secure, stable, accessible and peaceful ICT environment is essential for all and requires effective cooperation among States to reduce risks to international peace and security, and *calls upon* the international community to promote full respect for human rights and fundamental freedoms;

14. *Calls upon* parliaments to encourage investment in research and development, incorporating into the design of each project specific cybersecurity provisions, with appropriate budget allocation, in order to anticipate and protect against possible emerging cyber threats;

15. *Encourages* parliaments to partner with industry, academia and all other stakeholders, including civil society, with their respective governments as key facilitators, in order to foster a strong and collaborative cybersecurity ecosystem that fully respects human rights principles and international human rights obligations;

16. *Calls upon* parliaments and parliamentarians to actively engage in promoting a shared, up-to-date national understanding of the nature of cybercrime as experienced by citizens, organizations and institutions;

17. *Urges* parliaments to help foster a true “culture of cybersecurity” by developing educational curricula focused on training future generations, from childhood onwards, in digital literacy and technological know-how, covering both the great opportunities presented and the serious risks posed by technology;

18. *Recommends* that parliaments broaden protections for women, young people, children, elderly people, people with disabilities, and racialized communities in cyberspace, taking respect for human rights and the prevention of gender-based violence into account in the development of educational policies on the use of social media;

19. *Urges* parliaments to take the necessary action to protect critical moments in democracy, and especially those periods when citizens exercise their right to vote, in order to avoid attacks and interferences that seek to influence, change or violate the free formation of public opinion during the electoral process;

20. *Calls upon* the international community to take action to protect democracy by ensuring that all parliaments worldwide, as institutions representing the will of the people, are afforded special protection through their inclusion in lists of critical civilian infrastructure and essential services;

21. *Stresses* the need to further enhance international cooperation and assistance in the area of ICT security and capacity-building, as a means to bridge digital divides and strengthen the response to cyber threats globally;

22. *Calls upon* parliaments to deepen their understanding of the complex and rapidly evolving nature of cybercrime by enabling the open sharing of knowledge, experience and expertise, and by holding specialized seminars, workshops and conferences on this subject;

23. *Invites* the IPU Secretariat, in partnership with other relevant organizations, to promote this new vision of cybersecurity by supporting parliaments in their capacity-building endeavours;

24. *Recommends* that the IPU, as the global organization of parliaments, play a leading role in preventing and combating cybercrime, and in stimulating cyber-resilience, by participating in all relevant international forums, including those led by the United Nations, with a view to ensuring that the voice of parliaments is heard;

25. *Promotes* the creation of a working group on cybercrime, subsidiary to the Governing Council of the IPU, whose specific mission shall be to comply with the mandates and objectives established in this resolution, and whose powers shall include both supporting the process for the promotion of an international convention on cybercrime within the framework of the United Nations, and strengthening the capacities of IPU Member Parliaments in terms of law-making, oversight and budgeting;

26. *Recommends* that the IPU raise awareness among parliaments on achieving the Sustainable Development Goals through, above all else, their universal commitments to digital security.