146TH IPU ASSEMBLY
المنامة، البحرين
MANAMA, BAHRAIN
11-15 MARCH 2023 - ١٠-١١ مارس ٢٠٢٣

الجمعية العامة الـ 146 للاتحاد البرلماني الدولي

المنامة (11 – 15 آذار/مارس 2023)

1889
Inter-Parliamentary Union
For democracy. For everyone.

اللجنة الدائمة
للسلم والأمن الدوليين

C-I/146/Dr-am
6 آذار/مارس 2023

الهجمات والجرائم الإلكترونية:
المخاطر الجديدة على الأمن العالمي

تعديلات على مشروع القرار مقدمة ضمن المهل القانونية من قبل الأرجنتين، وبلجيكا، وكندا، وجمهورية التشيك، وجمهورية مصر العربية، وفنلندا، وفرنسا، ألمانيا، والهند، والجمهورية الإسلامية الإيرانية، واليابان، وليتوانيا، ونيكاراغوا، وباكستان، والفلبين، وجمهورية كوريا، ورومانيا، وروسيا الاتحادية، وسنغافورة، وجنوب إفريقيا، وجنوب السودان، وتايلاند، وتركيا، وأوكرانيا، وفيتنام

الديباجة

الفقرة 1 من الديباجة

تعدّل لتصبح كالتالي:

1 *(1) إذ تدين* جميع أشكال **استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية** ~~الجرائم~~ والهجمات الإلكترونية، *وإذ تعيد تأكيد* ضرورة مكافحة هذه الأعمال من خلال التعاون الدولي ووضع أطر ~~قانونية~~ **دولية** فعالة **ملزمة قانوناً مصممة وفقاً للسمات الفريدة لتكنولوجيا المعلومات والاتصالات،**

(الجمهورية الإسلامية الإيرانية)

تعدّل لتصبح كالتالي:

2 *(1) إذ تدين* جميع أشكال ~~الجرائم~~ **إساءة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية** والهجمات الإلكترونية، *وإذ تعيد تأكيد* ضرورة مكافحة هذه الأعمال من خلال التعاون الدولي ووضع أطر قانونية فعالة،

(باكستان)

تعدّل لتصبح كالتالي:

3 *(1) إذ تدين* جميع **أشكال استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية، المشار إليها في ما يلي بـ**"الجرائم الإلكترونية"، **والهجمات الحاسوبية، المشار إليها في ما يلي بـ** "الهجمات الإلكترونية"، *وإذ تعيد تأكيد* ضرورة مكافحة هذه الأعمال من خلال التعاون الدولي ووضع أطر قانونية فعالة،

(روسيا الاتحادية)

تعدّل لتصبح كالتالي:

4 (1) *إذ تدين* جميع أشكال الجرائم ~~والهجمات~~ الإلكترونية، *وإذ تعيد تأكيد* ضرورة مكافحة هذه الأعمال من خلال التعاون الدولي ووضع أطر قانونية فعالة،

(جمهورية التشيك، السويد)

تعدّل لتصبح كالتالي:

5 (1) إذ تدين جميع أشكال الجرائم ~~والهجمات~~ **والحوادث** الإلكترونية، *وإذ تعيد تأكيد* ضرورة مكافحة هذه الأعمال من خلال التعاون الدولي ووضع أطر قانونية فعالة،

(الهند)

تعدّل لتصبح كالتالي:

6 (1) *إذ تدين* جميع أشكال الجرائم والهجمات الإلكترونية **الخبيثة**، *وإذ تعيد تأكيد* ضرورة مكافحة هذه ~~**الأعمال**~~ **الجرائم** من خلال التعاون الدولي ووضع أطر قانونية فعالة،

(بلجيكا)

تعدّل لتصبح كالتالي:

7 (1) *إذ تدين* جميع أشكال الجرائم والهجمات الإلكترونية، ~~*وإذ تعيد تأكيد ضرورة مكافحة هذه الأعمال من خلال التعاون الدولي ووضع أطر قانونية فعالة*~~ **مع جميع الجرائم المروعة المرتبطة بها،**

(جنوب السودان)

تعدّل لتصبح كالتالي:

8 (1) *إذ تدين* جميع أشكال الجرائم والهجمات الإلكترونية، *وإذ تعيد تأكيد* ضرورة مكافحة هذه الأعمال من خلال التعاون الدولي ~~ووضع أطر قانونية فعالة~~،

(ألمانيا)

تعدّل لتصبح كالتالي:

9 (1) *إذ تدين* جميع أشكال الجرائم والهجمات الإلكترونية، *وإذ تعيد تأكيد* ضرورة مكافحة هذه الأعمال من خلال التعاون الدولي ~~ووضع أطر~~ **نقاشات** قانونية فعالة،

(اليابان)

تعدّل لتصبح كالتالي:

10 (1) *إذ تدين* جميع أشكال الجرائم والهجمات الإلكترونية، *وإذ تعيد تأكيد* ضرورة مكافحة هذه الأعمال من خلال التعاون الدولي **والتنسيق بين الجهات المعنية داخل البلدان وفي ما بينها على السواء، بما في ذلك تبادل المعلومات عن مخاطر الجرائم الإلكترونية**، ووضع أطر قانونية فعالة،

(جنوب إفريقيا)

تعدّل لتصبح كالتالي:

11 (1) *إذ تدين* جميع أشكال الجرائم والهجمات الإلكترونية، *وإذ تعيد تأكيد* ضرورة مكافحة هذه الأعمال من خلال التعاون الدولي **وتطبيق** أطر قانونية فعّالة **أو** وضعها **عند الضرورة**

(سويسرا)

تعدّل لتصبح كالتالي:

12 *(1) إذ تدين* جميع أشكال الجرائم والهجمات الإلكترونية، *وإذ تعيد تأكيد* ضرورة مكافحة هذه الأعمال من خلال التعاون الدولي ووضع أطر قانونية فعالة **تعكس النظام الدولي القائم على القواعد،**

(كندا)

الفقرة 1 جديدة من الديباجة مكررة

13 **(مكررة) *إذ تسلّم* بأن الجرائم والهجمات الإلكترونية ظاهرتان متميزتان لكن مترابطتين ذات طابع إجرامي في العصر الرقمي، وترتبطان بنطاقات مختلفة من الاستخدامات الخبيثة لتكنولوجيا المعلومات والاتصالات،**

(الأرجنتين)

14 **(مكررة) *إذ تؤكد من جديد* إطار الأمم المتحدة الحالي لسلوك الدول المسؤول في استخدام تكنولوجيا المعلومات والاتصالات وضرورة تنفيذ هذا الإطار،**

(ألمانيا)

15 **(مكررة) *إذ تؤكد* ضرورة مكافحة هذه الأعمال من خلال التعاون الوطني والإقليمي والدولي ووضع أطر قانونية فعالة،**

(جنوب السودان)

الفقرة 2 من الديباجة

تعدّل لتصبح كالتالي:

16 *(2) وإذ تعترف* بضرورة بناء الثقة بين البلدان ~~للتصدي لمرتكبي الجرائم الإلكترونية الذين لا يعرفون قيوداً ولا حدوداً~~ **للتصدي للمخاطر التي تهدد الأمن الإلكتروني،**

(الهند)

تعدّل لتصبح كالتالي:

17 *(2) وإذ تعترف* بضرورة بناء الثقة بين البلدان للتصدي ~~لمرتكبي الجرائم الإلكترونية~~ **للاستخدام الخبيث لتكنولوجيا المعلومات والاتصالات من جانب الجهات الفاعلة الحكومية وغير الحكومية** الذين لا يعرفون قيوداً ولا حدوداً،

(ألمانيا)

تعدّل لتصبح كالتالي:

18 *(2) وإذ تعترف* بضرورة بناء الثقة بين البلدان للتصدي لمرتكبي الجرائم الإلكترونية **والجهات الفاعلة الخبيثة** الذين لا يعرفون قيوداً ولا حدوداً،

(الجمهورية الإسلامية الإيرانية)

تعدّل لتصبح كالتالي:

19 *(2) وإذ تعترف* بضرورة بناء الثقة **والتفاهم المتبادل** بين البلدان للتصدي لمرتكبي الجرائم الإلكترونية الذين لا يعرفون قيوداً ولا حدوداً،

(تايلاند)

الفقرة 3 من الديباجة

20 تعدّل لتصبح كالتالي:

(3) وإذ تلاحظ تزايد **استخدام تكنولوجيا المعلومات والاتصالات** والاعتماد عليها **على الصعيد**

العالمي، ~~الفضاء الإلكتروني بين الأفراد والمؤسسات والدول~~،

(ألمانيا)

تعدّل لتصبح كالتالي:

21 *(3) وإذ تلاحظ* تزايد الاعتماد على **بيئة تكنولوجيا المعلومات والاتصالات** ~~الفضاء الإلكتروني~~ بين الأفراد والمؤسسات والدول،

(الجمهورية الإسلامية الإيرانية)

تعدّل لتصبح كالتالي:

22 *(3) وإذ تلاحظ* تزايد الاعتماد على **الفضاء الذي تستخدم فيه تكنولوجيا المعلومات والاتصالات، المشار إليه في ما يلي بـ** "الفضاء الإلكتروني"، بين الأفراد والمؤسسات والدول،

(روسيا الاتحادية)

الفقرة 4 من الديباجة

تعدّل لتصبح كالتالي:

23 *(4) وإذ تدرك* الزيادة في **استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية** ~~الجرائم~~ و~~الهجمات الإلكترونية~~ **وتهديدات تكنولوجيا المعلومات والاتصالات** بسبب زيادة الرقمنة، ولا سيما الرقمنة القسرية التي فرضتها جائحة كوفيد-19،

(الجمهورية الإسلامية الإيرانية)

تعدّل لتصبح كالتالي:

24 *(4) وإذ تدرك* الزيادة في ~~الجرائم~~ **إساءة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية** والهجمات الإلكترونية بسبب زيادة الرقمنة، ولا سيما الرقمنة القسرية التي فرضتها جائحة كوفيد-19،

(باكستان)

تعدّل لتصبح كالتالي:

25 *(4) وإذ تدرك* الزيادة في الجرائم ~~والهجمات~~ الإلكترونية بسبب زيادة الرقمنة، ~~ولا سيما الرقمنة القسرية التي فرضتها~~ **في خلال** جائحة كوفيد-19 **وما بعدها،**

(جمهورية التشيك)

تعدّل لتصبح كالتالي:

26 *(4) وإذ تدرك* الزيادة في الجرائم ~~والهجمات~~ الإلكترونية **وتطبيقها المتزايد في عمليات الحرب الإلكترونية، مثل برامج الفدية المزيفة التي يتم الاستفادة منها في الهجمات الإلكترونية المدمرة على الهياكل الأساسية المدنية الحيوية،** بسبب زيادة الرقمنة، ولا سيما الرقمنة القسرية التي فرضتها جائحة كوفيد-19،

(السويد)

تعدّل لتصبح كالتالي:

27 *(4) وإذ تدرك* الزيادة في الجرائم و~~الهجمات~~ **والحوادث** الإلكترونية بسبب زيادة الرقمنة، ولا سيما ~~الرقمنة القسرية التي فرضتها~~ **منذ ظهور** جائحة كوفيد-19،

(الهند)

تعدّل لتصبح كالتالي:

28 *(4) وإذ تدرك* الزيادة في **أنشطة** الجرائم والهجمات الإلكترونية بسبب زيادة الرقمنة~~، ولا سيما الرقمنة القسرية التي فرضتها~~ **سرّعت وتيرتها** جائحة كوفيد-19،

(ألمانيا)

تعدّل لتصبح كالتالي:

29 *(4) وإذ تدرك* الزيادة في الجرائم والهجمات الإلكترونية **الخبيثة** بسبب زيادة الرقمنة، ولا سيما الرقمنة القسرية التي فرضتها جائحة كوفيد-19،

(بلجيكا)

تعدّل لتصبح كالتالي:

30 *(4) وإذ تدرك* الزيادة في الجرائم والهجمات الإلكترونية بسبب زيادة الرقمنة، ولا سيما الرقمنة ~~القسرية~~ التي فرضتها جائحة كوفيد-19،

(ليتوانيا)

تعدّل لتصبح كالتالي:

31 *(4) وإذ تدرك* الزيادة في الجرائم والهجمات الإلكترونية **على الهياكل الأساسية الحيوية للدول والمؤسسات التي تدعم الخدمات الأساسية للناس، وكذلك على رفاه الأفراد،** بسبب زيادة الرقمنة، ولا سيما الرقمنة القسرية التي فرضتها جائحة كوفيد-19،

(جنوب إفريقيا)

الفقرة 4 جديدة من الديباجة مكررة

32 ***(4 مكررة) وإذ تدرك*** **أيضاً التحديات التي تواجهها الدول في مكافحة الهجمات والجرائم الإلكترونية، *وإذ تشدد* على ضرورة تعزيز أنشطة المساعدة التقنية وبناء القدرات، بناء على الطلب، لتعزيز قدرة السلطات الوطنية على التصدي للهجمات والجرائم الإلكترونية،**

(جنوب إفريقيا)

الفقرة 5 من الديباجة:

تعدّل لتصبح كالتالي:

33 *(5) وإذ تلاحظ* مسؤولية البرلمانات عن حماية المواطنين في ~~الفضاء الإلكتروني~~ **بيئة تكنولوجيا المعلومات والاتصالات** بهياكل أساسية وموارد جديدة، بالطريقة نفسها التي تحملها في العالم المادي،

(الجمهورية الإسلامية الإيرانية)

تعدّل لتصبح كالتالي:

34 *(5) وإذ تلاحظ* مسؤولية البرلمانات عن حماية المواطنين في الفضاء الإلكتروني ~~بهياكل أساسية وموارد جديدة~~، بالطريقة نفسها التي تحملها في العالم المادي،

(الهند)

تعدّل لتصبح كالتالي:

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

(الأرجنتين)

تعدّل لتصبح كالتالي:

(5) وإذ تلاحظ مسؤولية البرلمانات عن ~~حماية~~ **ضمان حماية** مواطنيها في الفضاء الإلكتروني بهياكل أساسية وموارد جديدة، بالطريقة نفسها التي تحملها في العالم المادي،

36 *(تايلاند)*

تعدّل لتصبح كالتالي:

37 *(5) وإذ تلاحظ* ~~مسؤولية~~ **دور** البرلمانات ~~عن~~ **في** حماية المواطنين في الفضاء الإلكتروني بهياكل أساسية وموارد جديدة، بالطريقة نفسها التي تحملها في العالم المادي،

(ليتوانيا)

تعدّل لتصبح كالتالي:

38 *(5) وإذ تلاحظ* مسؤولية البرلمانات عن حماية المواطنين في الفضاء الإلكتروني بهياكل أساسية وموارد جديدة، بالطريقة نفسها التي تحملها في العالم المادي، **حيث لا ترد بعد في بلدانها؛**

(نيكاراغوا)

الفقرة 5 جديدة من الديباجة مكررة

39 **(5 مكررة) *وإذ تسلم* بأنه، في ضوء وتيرة التطورات التكنولوجية العالمية، يجب بالمثل وضع سياسات وأطر قانونية جديدة على نحو سريع وشامل،**

(الفلبين)

40 **(5 مكررة) *وإذ تؤكد من جديد* أن الأمم المتحدة تؤدي دوراً رائداً في تيسير الحوار بشأن استخدام الدول لتكنولوجيا المعلومات والاتصالات، عملاً بقرار الجمعية العامة للأمم المتحدة رقم 76/19،**

(روسيا الاتحادية)

41 **(5 مكررة) *وإذ تشدد* على الاعتماد على منصات التكنولوجيا الرقمية وهيكلها الأساسي، إلى جانب مخاطر الهجمات الإلكترونية، عندما تنشر الحكومات تطبيقات الخدمة العامة على الإنترنت،**

(فيتنام)

الفقرة 5 جديدة من الديباجة مكررة ثانياً

(5 مكررة ثانياً) *وإذ تدعم* الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات واستخدامها 2021–2025، *وإذ تعترف* بولايته عملاً بقرار الجمعية العامة للأمم المتحدة 75/240، 42

(روسيا الاتحادية)

(5 مكررة ثانياً) *وإذ تؤكد* الرأي القائل بأن حماية حقوق الإنسان في عالم الفضاء الإلكتروني مشابهة للحالة الحقيقية، بما يتماشى مع الالتزامات الدولية للدول الأعضاء في الأمم المتحدة، 43

(فيتنام)

الفقرة 6 من الديباجة:

تعدّل لتصبح كالتالي:

(6) 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 و 121/56 المؤرخ 19 كانون الأول/ديسمبر 2001 *بشأن مكافحة إساءة استخدام تكنولوجيا المعلومات لأغراض إجرامية*، ~~القرار 239/57 المؤرخ 31 كانون الثاني/يناير 2003 بشأن إنشاء ثقافة عالمية للأمن السيبراني، والقرار~~ **والقرارات** 28/69 المؤرخ 2 كانون الأول/ديسمبر 2014، **237/70 المؤرخ 5 كانون الأول/ديسمبر 2018، 28/71 المؤرخ 5 كانون الأول/ديسمبر 2016، 27/73 المؤرخ 5 كانون الأول/ديسمبر 2018، 29/74 المؤرخ 12 كانون الأول/ديسمبر 2019، 240/75 المؤرخ 31 كانون الأول/ديسمبر 2020، 36/77 المؤرخ 7 كانون الأول/ديسمبر 2022** بشأن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، **والقرار 19/76 المؤرخ 6 كانون الأول/ديسمبر 2021 بشأن *التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، والنهوض بسلوك الدول المسؤول في استخدام تكنولوجيا المعلومات والاتصالات*،** 44

(روسيا الاتحادية)

تعدّل لتصبح كالتالي:

(6) 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 و 121/56 المؤرخ 19 كانون الأول/ديسمبر 2001 بشأن مكافحة إساءة استخدام تكنولوجيا المعلومات لأغراض إجرامية، القرار 239/57 المؤرخ 31 كانون الثاني/يناير 2003 بشأن إنشاء ثقافة عالمية للأمن السيبراني، والقرار ~~28/69 المؤرخ 2 كانون الأول/ديسمبر 2014 بشأن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي~~، **19/76 المؤرخ 6 كانون الأول/ديسمبر 2021 بشأن *التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، والنهوض بسلوك الدولة المسؤول في استخدام تكنولوجيا المعلومات والاتصالات*، والقرار 36/77 المؤرخ 7 كانون الأول/ديسمبر 2022 بشأن *التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي*، والقرار 37/77 المؤرخ 7 كانون الأول/ديسمبر 2022 بشأن *برنامج العمل للنهوض بسلوك الدولة المسؤول في استخدام تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي*،**

45

(جمهورية مصر العربية)

تعدّل لتصبح كالتالي:

(6) 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 و 121/56 المؤرخ 19 كانون الأول/ديسمبر 2001 بشأن مكافحة إساءة استخدام تكنولوجيا المعلومات لأغراض إجرامية، القرار 239/57 المؤرخ 31 كانون الثاني/يناير 2003 بشأن إنشاء ثقافة عالمية للأمن السيبراني، و~~القرار~~ **القرارات** 28/69 المؤرخ 2 كانون الأول/ديسمبر 2014، **27/73 المؤرخ 5 كانون الأول/ديسمبر 2018، 240/75 المؤرخ 31 كانون الأول/ديسمبر 2020،**

46

36/77 المؤرخ 7 كانون الأول/ديسمبر 2022 بشأن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي،

(الجمهورية الإسلامية الإيرانية)

تعدّل لتصبح كالتالي:

(6) 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 و 121/56 المؤرخ 19 كانون الأول/ديسمبر 2001 بشأن مكافحة إساءة استخدام تكنولوجيا المعلومات لأغراض إجرامية، القرار 239/57 المؤرخ 31 كانون الثاني/يناير 2003 بشأن إنشاء ثقافة عالمية للأمن السيبراني، والقرار 28/69 المؤرخ 2 كانون الأول/ديسمبر 2014 بشأن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، **فضلاً عن التقارير النهائية الصادرة بتوافق الآراء في العام 2021 عن فريق الأمم المتحدة العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وعن فريق الخبراء الحكوميين التابع للأمم المتحدة المعني بالنهوض بسلوك الدول المسؤول في سياق الأمن الدولي،**

47

(ألمانيا)

تعدّل لتصبح كالتالي:

(6) 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 و 121/56 المؤرخ 19 كانون الأول/ديسمبر 2001 بشأن مكافحة إساءة استخدام تكنولوجيا المعلومات لأغراض إجرامية، القرار 239/57 المؤرخ 31 كانون الثاني/يناير 2003 بشأن إنشاء ثقافة عالمية للأمن السيبراني، والقرار 28/69 المؤرخ 2 كانون الأول/ديسمبر 2014 بشأن التطورات في ميدان

48

المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، **والقرار 266/73 المؤرخ 22 كانون الأول/ديسمبر 2018 بشأن *الارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي*،**

(تايلاند)

الفقرة 6 جديدة من الديباجة مكررة

(6 مكررة) ***وإذ تشير أيضاً إلى قرار الجمعية العامة للأمم المتحدة 237/70 المؤرخ 23 كانون الأول/ديسمبر 2015 بشأن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، الذي أيد المعايير الطوعية وغير الملزمة المتعلقة بسلوك الدول المسؤول في استخدام تكنولوجيا المعلومات والاتصالات التي وضعها فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، ودعت الدول الأعضاء إلى الاسترشاد بهذه المعايير،***

49

(كندا)

الفقرة 7 من الديباجة:

تعدّل لتصبح كالتالي:

(7) *وإذ تشدد على* أهمية الاتفاقيات الإقليمية المتعلقة ~~بالجريمة الإلكترونية والجريمة المنظمة عبر الوطنية~~، **واستخدام تكنولوجيات المعلومات والاتصالات لأغراض إجرامية، وبشأن** 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، المؤرخ 16 حزيران/يونيو 2009، *والاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات* المؤرخة 21 كانون الأول/ديسمبر 2010،

50

(الجمهورية الاسلامية الإيرانية)

تعدّل لتصبح كالتالي:

(7) وإذ تشدد على أهمية الاتفاقيات الإقليمية المتعلقة ~~بالجريمة الإلكترونية~~ **بإساءة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية،** 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، المؤرخ 16 حزيران/يونيو 2009، *والاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات* المؤرخة 21 كانون الأول/ديسمبر 2010،

51

(باكستان)

تعدّل لتصبح كالتالي:

(7) *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، المؤرخ 16 حزيران/يونيو 2009، *والاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات* المؤرخة 21 كانون الأول/ديسمبر 2010،~~

52

(الهند)

تعدّل لتصبح كالتالي:

(7) ~~*وإذ تشدد على*~~ ~~أهمية~~ ***وإذ تحيط علماً ب***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

53

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، المؤرخ 16 حزيران/يونيو 2009، *والاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات* المؤرخة 21 كانون الأول/ديسمبر 2010،

(سنغافورة)

تعدّل لتصبح كالتالي:

(7) وإذ تشدد على أهمية الاتفاقيات الإقليمية **والدولية القائمة** المتعلقة بالجريمة الإلكترونية والجريمة المنظمة عبر الوطنية، وتبادل المعلومات والمساعدة الإدارية، بما في ذلك **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،** واتفاقية 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، المؤرخ 16 حزيران/يونيو 2009، *والاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات* المؤرخة 21 كانون الأول/ديسمبر 2010،

54

(بلجيكا)

تعدّل لتصبح كالتالي:

(7) 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، المؤرخ 16 حزيران/يونيو 2009، *والاتفاقية العربية لمكافحة جرائم*

55

تكنولوجيا المعلومات المؤرخة 21 كانون الأول/ديسمبر 2010، **بالإضافة إلى القانون النموذجي لبرلمان أمريكا اللاتينية ومنطقة البحر الكاريبي بشأن جرائم الفضاء الإلكتروني الصادر في تشرين الثاني/نوفمبر 2013 وتحديثاته، والقانون النموذجي بشأن *المنع الاجتماعي للعنف والجريمة الصادر في تشرين الثاني/نوفمبر 2015*، والقانون النموذجي بشأن جرائم الحاسوب الصادر في شباط/فبراير 2021، والقانون النموذجي لمكافحة الاتجار غير المشروع والجريمة عبر الوطنية* الصادر في شباط/فبراير 2021،**

(الأرجنتين)

تعدّل لتصبح كالتالي:

(7) 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، المؤرخ 16 حزيران/يونيو 2009، *والاتفاقية العربية لمكافحة جرائم* **56**
تكنولوجيا المعلومات المؤرخة 21 كانون الأول/ديسمبر 2010، ***واتفاقية التعاون بين الدول الأعضاء في رابطة الدول المستقلة في مجال ضمان أمن المعلومات المؤرخة 20 تشرين الثاني/نوفمبر 2013، واتفاقية التعاون بين الدول الأعضاء في رابطة الدول المستقلة في مكافحة الجرائم في ميدان تكنولوجيا المعلومات المؤرخة 28 أيلول/سبتمبر 2018،***

(روسيا الاتحادية)

تعدّل لتصبح كالتالي:

(7) وإذ تشدد على أهمية الاتفاقيات الإقليمية المتعلقة بالجريمة الإلكترونية والجريمة المنظمة عبر **57**
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، المؤرخ 16 حزيران/يونيو 2009، *والاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات* المؤرخة 21 كانون الأول/ديسمبر 2010، **واتفاقية الاتحاد الإفريقي *بشأن الأمن الإلكتروني وحماية البيانات الشخصية* المؤرخة 27 حزيران/يونيو 2014،**

(جنوب إفريقيا)

الفقرة 7 جديدة من الديباجة مكررة

(7 مكررة) *وإذ تشدد أيضاً* على أن اتفاقية مجلس أوروبا *المتعلقة بجرائم الفضاء الإلكتروني* المؤرخة 23 تشرين الثاني/نوفمبر 2001 (اتفاقية بودابست")، التي يفتح باب الانضمام إليها أمام أي بلد، قد أصبحت صكاً ذا أهمية عالمية مع وجود دول أطراف من جميع مناطق العالم والتأثير فيها، 58

(رومانيا)

الفقرة 8 من الديباجة:

تعدّل لتصبح كالتالي:

(8) وإذ تشير إلى عمل الاتحاد البرلماني الدولي بشأن مختلف المخاطر الجديدة التي تواجهها مجتمعاتنا التي تتزايد رقمنتها، بما في ذلك قرارَي الاتحاد البرلماني الدولي: *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،~~ 59

(الهند)

تعدّل لتصبح كالتالي:

(8) وإذ تشير إلى عمل الاتحاد البرلماني الدولي بشأن مختلف المخاطر الجديدة التي تواجهها مجتمعاتنا التي تتزايد رقمنتها، بما في ذلك قرارَي الاتحاد البرلماني الدولي: *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، ***بالإضافة إلى القانون النموذجي لبرلمان أمريكا اللاتينية ومنطقة البحر الكاريبي بشأن الحماية من العنف المدرسي الصادر في تشرين الثاني/نوفمبر 2015، والقانون النموذجي بشأن ضمان منع الاعتداء الجنسي على الأطفال والمراهقين ورعايتهم ومعاقبتهم الصادر في تشرين الثاني/نوفمبر 2015، والقانون النموذجي ضد الإغواء حزيران/يونيو 2019،***

(الأرجنتين)

60

الفقرة 8 جديدة من الديباجة مكررة

(8 مكررة) وإذ *تشير* إلى مبادئ الأمن الإلكتروني المتفق عليها في *تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي* المؤرخ 22 تموز/يوليو 2015 (A/70/174) المقدم إلى الجمعية العامة للأمم المتحدة،

61

(فيتنام)

الفقرة 9 من الديباجة:

تحذف الفقرة.

62

(بلجيكا، كندا، سويسرا)

تعدّل لتصبح كالتالي:

~~*(9) وإذ تعرب عن قلقها إزاء عدم ورود صكوك قانونية عالمية لقمع الجرائم والهجمات الإلكترونية،*~~

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

(ألمانيا)

تعدّل لتصبح كالتالي:

(9) وإذ تعرب عن قلقها إزاء عدم ورود صكوك قانونية عالمية لقمع ~~الجرائم والهجمات الإلكترونية~~

64 ***استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية وتهديدات تكنولوجيا المعلومات والاتصالات،***

(الجمهورية الإسلامية الإيرانية)

تعدّل لتصبح كالتالي:

(9) وإذ تعرب عن قلقها إزاء عدم ورود صكوك قانونية عالمية لقمع ~~الجرائم~~، **إساءة استخدام تكنولوجيا**

65 **المعلومات والاتصالات لأغراض إجرامية** والهجمات الإلكترونية

(الباكستان)

تعدّل لتصبح كالتالي:

(9) وإذ تعرب عن قلقها إزاء ~~عدم ورود صكوك قانونية عالمية~~ **بطء وتيرة التصديق على الأدوات القانونية القائمة** لقمع الجرائم ~~والهجمات~~ الإلكترونية، **مثل اتفاقية مجلس أوروبا بشأن جرائم الفضاء**

66 **الإلكتروني المؤرخة 23 تشرين الثاني/نوفمبر 2001 وبروتوكولاها الإضافيان،**

(السويد)

تعدّل لتصبح كالتالي:

(9) وإذ تعرب عن قلقها إزاء عدم ورود صكوك قانونية عالمية لقمع الجرائم ~~والهجمات~~ الإلكترونية، 67

(اليابان)

تعدّل لتصبح كالتالي: 68

(9) وإذ تعرب عن قلقها إزاء عدم ورود صكوك قانونية عالمية ~~لقمع~~ **منع ومكافحة** الجرائم ~~والهجمات~~ **والحوادث** الإلكترونية،

(الهند)

تعدّل لتصبح كالتالي:

(9) وإذ تعرب عن قلقها إزاء عدم ورود صكوك قانونية عالمية لقمع الجرائم والهجمات الإلكترونية، **وكذلك لمنع أعمال الحرب الإلكترونية،** **69**

(الأرجنتين)

تعدّل لتصبح كالتالي:

(9) وإذ تعرب عن قلقها إزاء عدم ورود **استراتيجية و**صكوك قانونية عالمية لقمع الجرائم والهجمات الإلكترونية، **70**

(الفلبين)

الفقرة 10 من الديباجة:

تحذف الفقرة. **71**

(كندا)

تعدّل لتصبح كالتالي:

(10) وإذ تشيد بالجهود التي تبذلها الأمم المتحدة لسن اتفاقية دولية ~~شاملة~~ بشأن **الجرائم الإلكترونية** ~~مكافحة استخدام تكنولوجيات المعلومات والاتصالات في الأغراض الإجرامية~~، من خلال قرار الجمعية العامة 247/74 المؤرخ 27 كانون الأول/ديسمبر 2019، *وإذ ترحب* بإنشاء لجنة مخصصة مكلفة بصياغة هذه الاتفاقية، **72**

(السويد)

73 تعدّل لتصبح كالتالي:

(10) وإذ تشيد بالجهود التي تبذلها الأمم المتحدة لسن اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات في الأغراض الإجرامية، من خلال قرار الجمعية العامة 247/74 المؤرخ 27 كانون الأول/ديسمبر 2019، *وإذ ترحب* بإنشاء لجنة مخصصة مكلفة ~~بصياغة~~ **إعداد** هذه الاتفاقية،

(سنغافورة)

الفقرة 10 جديدة من الديباجة مكررة

(10 مكررة) وإذ تثني **أيضاً على جهود الأمم المتحدة الرامية إلى القيام، من خلال قرارات الجمعية العامة للأمم المتحدة 27/73 المؤرخ 5 كانون الأول/ديسمبر 2018 و240/75 المؤرخ 31 كانون الأول/ديسمبر 2020 و36/77 المؤرخ 7 كانون الأول/ديسمبر 2022،**

74 **بعقد اجتماع لفريق عامل مفتوح العضوية، بشأن أمن تكنولوجيا المعلومات والاتصالات واستخدامها، بغية جعل عملية مفاوضات الأمم المتحدة بشأن الأمن في استخدام تكنولوجيا المعلومات والاتصالات أكثر ديمقراطية وشمولية وشفافية،**

(الجمهورية الإسلامية الإيرانية)

الفقرة 11 من الديباجة:

تعدّل لتصبح كالتالي:

(11) *وإذ ترحب* بمشاركة الاتحاد البرلماني الدولي في **أي** عملية ~~التشاور~~ بين الجهات المعنية المتعددة

75 ~~التابعة لتلك اللجنة المخصصة~~ **التي تذكي الوعي بالمعايير الطوعية وغير الملزمة وتنفيذها في ما يتعلق بسلوك الدولة المسؤول في استخدام تكنولوجيا المعلومات والاتصالات**، من أجل ضمان الاستماع إلى صوت البرلمانات،

(كندا)

تعدّل لتصبح كالتالي:

(11) وإذ ترحب بمشاركة الاتحاد البرلماني الدولي في عملية التشاور بين الجهات المعنية المتعددة التابعة لتلك اللجنة المخصصة، **وكذلك في الفريق العامل مفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات واستخدامها،** من أجل ضمان الاستماع إلى صوت البرلمانات، 76

(الجمهورية الإسلامية الإيرانية)

تعدّل لتصبح كالتالي:

(11) وإذ ترحب بمشاركة الاتحاد البرلماني الدولي في عملية التشاور بين الجهات المعنية المتعددة التابعة لتلك اللجنة المخصصة من أجل ضمان الاستماع إلى صوت البرلمانات، **بعد التشاور مع الدول الأطراف،** 77

(نيكاراغوا)

تعدّل لتصبح كالتالي:

(11) وإذ ترحب بمشاركة الاتحاد البرلماني الدولي في عملية التشاور بين الجهات المعنية المتعددة التابعة لتلك اللجنة المخصصة من أجل ضمان الاستماع إلى صوت البرلمانات، **في محاولة لمكافحة الجرائم والهجمات الإلكترونية،** 78

(تايلاند)

الفقرة 11 جديدة من الديباجة مكررة

(11 مكررة) *وإذ تدعم* الفريق العامل المفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات واستخدامها للفترة 2021–2025 المنشأ عملاً بقرار الجمعية العامة للأمم المتحدة 240/75، *وإذ تشجعه* على مراعاة نتائج تقارير أفرقة الخبراء الحكوميين للأعوام 2010 و2013 و2015 و2021 وتقرير الفريق العامل مفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وإضافة إلى الجهود التي تبذلها هذه التطورات، 79

(جمهورية مصر العربية)

الفقرة 11 جديدة من الديباجة مكررة ثانياً

(11 مكررة ثانياً) ***وإذ ترحب*** **بالاقتراح الذي أقرته الجمعية العامة للأمم المتحدة في قرارها 37/77 المؤرخ 7 كانون الأول/ديسمبر 2022، بوضع برنامج عمل للأمم المتحدة للنهوض بالسلوك المسؤول للدول في استخدام تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي، كبرنامج دائم وآلية شاملة وعملية المنحى لمناقشة التهديدات القائمة والمحتملة؛ ودعم قدرات الدول وجهودها الرامية إلى تنفيذ الالتزامات والاسترشاد بالإطار والنهوض بها؛ وتعزيز المشاركة والتعاون مع أصحاب المصلحة المعنيين؛ والمراجعة الدورية للتقدم المحرز في تنفيذ برنامج العمل فضلاً عن عمل البرنامج في المستقبل،**

80

(جمهورية مصر العربية)

الفقرة 12 من الديباجة:

81

تحذف الفقرة.

(كندا)

تعدّل لتصبح كالتالي:

(12) وإذ تلاحظ الحاجة إلى اتباع نهج شامل وعالمي إزاء ~~مسألة الجرائم والهجمات الإلكترونية، بما في ذلك من خلال وضع إطار قانوني دولي للتصدي للجرائم والهجمات الإلكترونية وعواقبها الخطيرة على المواطنين~~ **والاستخدام الخبيث لتكنولوجيا المعلومات والاتصالات** لحماية السلام والأمن والاستقرار ~~الاقتصادي~~ على الصعيد العالمي،

82

(ألمانيا)

تعدّل لتصبح كالتالي:

(12) وإذ تلاحظ الحاجة إلى اتباع نهج ~~شامل و~~عالمي إزاء مسألة الجرائم ~~والهجمات~~ الإلكترونية، ~~بما في ذلك من خلال وضع إطار قانوني دولي للتصدي للجرائم والهجمات الإلكترونية~~ وعواقبها

84

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**،

(السويد)

تعدّل لتصبح كالتالي:

(12) وإذ تلاحظ الحاجة إلى اتباع نهج شامل وعالمي إزاء ~~مسألة الجرائم والهجمات الإلكترونية، بما في ذلك من خلال وضع إطار قانوني دولي~~ التصدي للجرائم والهجمات الإلكترونية وعواقبها الخطيرة على المواطنين وحماية السلام والأمن والاستقرار الاقتصادي على الصعيد العالمي، **84**

(سويسرا)

تعدّل لتصبح كالتالي:

(12) وإذ تلاحظ الحاجة إلى اتباع نهج شامل وعالمي إزاء مسألة ~~الجرائم والهجمات الإلكترونية~~ **استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية وتهديدات تكنولوجيا المعلومات والاتصالات**، بما في ذلك من خلال وضع ~~إطار قانوني دولي~~ **أطر ملزمة قانوناً مصممة خصيصاً للسمات الفريدة لتكنولوجيا المعلومات والاتصالات** للتصدي ~~للجرائم والهجمات الإلكترونية~~ **لاستخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية وتهديدات تكنولوجيا المعلومات والاتصالات** وعواقبها الخطيرة على المواطنين وحماية السلام والأمن والاستقرار الاقتصادي على الصعيد العالمي، **85**

(الجمهورية الإسلامية الإيرانية)

تعدّل لتصبح كالتالي:

(12) وإذ تلاحظ الحاجة إلى اتباع نهج شامل وعالمي إزاء مسألة ~~الجرائم~~ **إساءة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية** والهجمات الإلكترونية، بما في ذلك من خلال وضع إطار قانوني دولي للتصدي ~~للجرائم~~ **إساءة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية** والهجمات الإلكترونية وعواقبها الخطيرة على المواطنين وحماية السلام والأمن والاستقرار الاقتصادي على الصعيد العالمي، **86**

(باكستان)

تعدّل لتصبح كالتالي:

(12) وإذ تلاحظ الحاجة إلى اتباع نهج شامل وعالمي إزاء مسألة الجرائم ~~والهجمات~~ الإلكترونية، بما
87 في ذلك من خلال وضع إطار قانوني دولي للتصدي للجرائم ~~والهجمات~~ الإلكترونية وعواقبها الخطيرة على المواطنين وحماية السلام والأمن والاستقرار الاقتصادي على الصعيد العالمي،

(اليابان)

تعدّل لتصبح كالتالي:

(12) وإذ تلاحظ الحاجة إلى اتباع نهج شامل وعالمي إزاء مسألة الجرائم ~~والهجمات~~ **والحوادث**
88 الإلكترونية، بما في ذلك من خلال وضع إطار قانوني دولي للتصدي للجرائم والهجمات الإلكترونية وعواقبها الخطيرة على المواطنين وحماية السلام والأمن والاستقرار الاقتصادي على الصعيد العالمي،

(الهند)

تعدّل لتصبح كالتالي:

(12) وإذ تلاحظ الحاجة إلى اتباع نهج شامل وعالمي إزاء مسألة الجرائم والهجمات الإلكترونية، بما
89 في ذلك من خلال وضع إطار قانوني دولي للتصدي للجرائم والهجمات الإلكترونية وعواقبها الخطيرة على المواطنين **والهياكل الأساسية** وحماية السلام والأمن والاستقرار الاقتصادي على الصعيد العالمي،

(ليتوانيا)

الفقرة 12 جديدة من الديباجة مكررة

(12 مكررة) *وإذ تلاحظ* أيضاً أن المجتمع الدولي بحاجة إلى اتباع نهج شامل إزاء التهديدات في
مجال أمن تكنولوجيا المعلومات والاتصالات لا يعالج البعد التكنولوجي للتهديدات في هذا
90 **المجال فحسب، بل أيضاً بعدها السياسي والأيديولوجي، الذي يشمل، في جملة أمور، استخدام تكنولوجيات المعلومات والاتصالات للتدخل في الشؤون الداخلية للدول الأخرى وتقويض استقرارها السياسي والاقتصادي والاجتماعي،**

(الجمهورية الإسلامية الإيرانية)

(12 مكررة) ***وإذ ترحب*** **بالجهود الجارية لتكييف وتطبيق النظم القانونية الدولية القائمة لتنظيم الفضاء الإلكتروني، بما في ذلك وضع *دليل تالين بشأن القانون الدولي المنطبق على الحروب الإلكترونية*،**

91

(أوكرانيا)

الفقرة 13 من الديباجة:

تعدّل لتصبح كالتالي:

(13) *وإذ تعترف* بالحاجة الملحة إلى أن يتخذ المشرعون والحكومات خطوات وطنية أكثر استباقية لمكافحة ~~الجرائم~~ **استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية** ~~والهجمات الإلكترونية~~ ***وتهديدات تكنولوجيا المعلومات والاتصالات***، نظراً لكثافتها المتجددة وطابعها السريع التطور،

92

(الجمهورية الإسلامية الإيرانية)

تعدّل لتصبح كالتالي:

(13) *وإذ تعترف* بالحاجة الملحة إلى أن يتخذ المشرعون والحكومات خطوات وطنية أكثر استباقية لمكافحة الجرائم ~~والهجمات~~ الإلكترونية، نظراً لكثافتها المتجددة وطابعها السريع التطور،

93

(جمهورية التشيك، السويد)

تعدّل لتصبح كالتالي:

(13) *وإذ تعترف* بالحاجة الملحة إلى أن يتخذ المشرعون والحكومات خطوات وطنية أكثر استباقية لمكافحة الجرائم ~~والهجمات~~ **الحوادث** الإلكترونية، نظراً لكثافتها **لشدتها** المتجددة وطابعها السريع التطور،

94

(الهند)

تعدّل لتصبح كالتالي:

95

(13) *وإذ تعترف* بالحاجة الملحة إلى أن يتخذ المشرعون والحكومات خطوات وطنية أكثر استباقية

لمكافحة ~~الجرائم~~ **إساءة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية** والهجمات الإلكترونية، نظراً لكثافتها المتجددة وطابعها السريع التطور،

(باكستان)

تعدّل لتصبح كالتالي:

(13) *وإذ تعترف* بالحاجة الملحة إلى أن يتخذ المشرعون والحكومات **وجميع الجهات المعنية** خطوات وطنية أكثر استباقية لمكافحة الجرائم والهجمات الإلكترونية، نظراً لكثافتها المتجددة وطابعها السريع التطور، **96**

(تايلاند)

تعدّل لتصبح كالتالي:

(13) *وإذ تعترف* بالحاجة الملحة إلى أن يتخذ المشرعون والحكومات خطوات وطنية أكثر استباقية لمكافحة الجرائم والهجمات الإلكترونية، نظراً لكثافتها المتجددة وطابعها السريع التطور، **فضلاً عن احترام حقوق الإنسان والحريات الأساسية وسيادة القانون احتراماً كاملاً والتزاماتهم بموجب القانون الدولي لحقوق الإنسان،** **97**

(كندا)

تعدّل لتصبح كالتالي:

(13) *وإذ تعترف* بالحاجة الملحة إلى أن يتخذ المشرعون والحكومات خطوات وطنية أكثر استباقية لمكافحة الجرائم والهجمات الإلكترونية، نظراً لكثافتها المتجددة وطابعها السريع التطور، **وبشكل متساو لتعزيز حماية حرية التعبير والحقوق الأساسية الأخرى،** **98**

(جنوب إفريقيا)

الفقرة 13 جديدة من الديباجة مكررة

(13 مكررة) *وإذ تسلم* بأن جميع الإجراءات المتخذة في هذا الميدان تحتاج إلى احترام حقوق الإنسان والحقوق الأساسية في صميمها، **99**

(السويد)

(13 مكررة) وإذ تلاحظ تفاوت التطور في قدرة البلدان على تطبيق تكنولوجيا المعلومات وقدرتها على حماية الهياكل الأساسية لتكنولوجيا المعلومات، *وإذ تشدد* على الحاجة إلى زيادة المساعدة والتعاون التقنيين، ولا سيما للبلدان النامية، 100

(فيتنام)

الفقرة 13 جديدة من الديباجة مكررة ثانياً

(13 مكررة ثانياً) *وإذ تلاحظ 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، 101

(السويد)

الفقرة 14 من الديباجة:

تحذف الفقرة. 102

(الهند)

تعدّل لتصبح كالتالي:

(14) *وإذ تعترف أيضاً* بالحاجة إلى اتخاذ إجراءات برلمانية دولية مشتركة ~~لتوفير درع وقائي للمواطنين والحكومات والدول، وجميعهم جهات معنية في هذه المهمة.~~ **وزيادة الوعي وتنفيذ القواعد الطوعية وغير الملزمة في ما يتعلق بسلوك الدولة المسؤول في استخدام تكنولوجيا المعلومات والاتصالات،** 103

(كندا)

تعدّل لتصبح كالتالي:

(14) *وإذ تعترف أيضاً* بالحاجة إلى اتخاذ إجراءات برلمانية **إقليمية و**دولية مشتركة لتوفير درع وقائي للمواطنين والحكومات والدول، وجميعهم جهات معنية في هذه المهمة **فضلاً عن التنسيق التشريعي اللازم على المستوى دون الوطني،** 104

(الأرجنتين)

الفقرة 14 جديدة من الديباجة مكررة

(14 مكررة) *وإذ تلاحظ* أن الجرائم الإلكترونية قد تشكل تهديداً خطيراً للعمليات الديمقراطية، ولا سيما التدخل في الانتخابات من خلال انتهاكات الأمن الإلكتروني أو حسابات مزيفة على وسائل التواصل الاجتماعي، 105

(فنلندا)

(14 مكررة) *وإذ تشير* إلى الآثار الضارة للتدابير القسرية المتخذة من جانب واحد وغيرها من القيود المفروضة خلال جائحة كوفيد-19، التي اعترف بها على نطاق واسع، بما في ذلك في تقارير الأمم المتحدة، 106

(الجمهورية الإسلامية الإيرانية)

الفقرة 14 جديدة من الديباجة مكررة ثانياً

(14 مكررة ثانياً) *وإذ تحث* البرلمانات على دعوة حكوماتها إلى الامتناع عن إصدار أو تطبيق أي تدابير قسرية من جانب واحد (تدابير مالية أو اقتصادية أو تجارية من جانب واحد) تعيق أو تؤثر سلباً في قدرة الدول على منع الجرائم الإلكترونية ومكافحتها أو على التعاون والمساعدة في ما بينها في هذا الصدد، 107

(الجمهورية الإسلامية الإيرانية)

الفقرة 15 من الديباجة:

تعدّل لتصبح كالتالي:

(15) *وإذ تقر* بأن النساء ~~والشباب والأطفال هم الأكثر ضعفاً ويعانون من أكبر الاعتداءات على الإنترنت، وهم يتأثرون شخصياً واجتماعياً وثقافياً واقتصادياً بمرتكبي الجرائم الإلكترونية~~ **والفتيات وكبار السن والأطفال، من بين آخرين، هم الأكثر عرضة لخطر التعرض للتهديدات في الفضاء الإلكتروني،** 108

(ألمانيا)

تعدّل لتصبح كالتالي:

(15) وإذ تقر بأن النساء والشباب **والمسنين والأشخاص ذوي الاحتياجات الخاصة** والأطفال هم ~~الأكثر~~ **ضعفاء بشكل خاص** ويعانون من أكبر **عدد من** الاعتداءات على الإنترنت،~~وهم يتأثرون شخصياً واجتماعياً وثقافياً واقتصادياً بمرتكبي الجرائم الإلكترونية.~~ 109

(بلجيكا)

تعدّل لتصبح كالتالي:

(15) وإذ تقر بأن النساء ~~والشباب~~ والأطفال **وكذلك كبار السن** هم الأكثر ضعفاً ويعانون من أكبر الاعتداءات على الإنترنت، وهم يتأثرون شخصياً واجتماعياً وثقافياً واقتصادياً ~~بمرتكبي~~ **بالجرائم** الإلكترونية، 110

(جمهورية التشيك)

تعدّل لتصبح كالتالي:

(15) وإذ تقر بأن النساء والشباب والأطفال هم الأكثر ضعفاً ويعانون من أكبر الاعتداءات ~~على الإنترنت~~ **في الفضاء الإلكتروني،** وهم يتأثرون شخصياً واجتماعياً وثقافياً واقتصادياً بمرتكبي الجرائم الإلكترونية، 111

(ليتوانيا)

تعدّل لتصبح كالتالي:

(15) وإذ تقر بأن النساء والشباب والأطفال هم الأكثر ضعفاً ويعانون من أكبر الاعتداءات على الإنترنت، وهم يتأثرون شخصياً واجتماعياً وثقافياً واقتصادياً بمرتكبي الجرائم الإلكترونية، **مع *التأكيد* على الحاجة إلى زيادة التعاون مع القطاع الخاص ومقدمي الخدمات من أجل حماية المتضررين،**

(تايلاند)

112

تعدّل لتصبح كالتالي:

(15) وإذ تقر بأن النساء والشباب والأطفال **والمجتمعات التي تعاني من التمييز العنصري** هم الأكثر ضعفاً ويعانون من أكبر الاعتداءات على الإنترنت، وهم يتأثرون شخصياً واجتماعياً وثقافياً واقتصادياً بمرتكبي الجرائم الإلكترونية،

(كندا)

113

تعدّل لتصبح كالتالي:

(15) وإذ تقر بأن النساء والشباب والأطفال **والأشخاص ذوي الإعاقة** هم الأكثر ضعفاً ويعانون من أكبر الاعتداءات على الإنترنت، وهم يتأثرون شخصياً واجتماعياً وثقافياً واقتصادياً بمرتكبي الجرائم الإلكترونية،

(فنلندا)

114

تعدّل لتصبح كالتالي:

(15) وإذ تقر بأن النساء والشباب والأطفال **وكبار السن** هم الأكثر ضعفاً ويعانون من أكبر الاعتداءات على الإنترنت، وهم يتأثرون شخصياً واجتماعياً وثقافياً واقتصادياً بمرتكبي الجرائم الإلكترونية،

(فيتنام)

115

تعدّل لتصبح كالتالي:

(15) وإذ تقر بأن النساء والشباب والأطفال **وكبار السن** هم الأكثر ضعفاً ويعانون من أكبر الاعتداءات على الإنترنت، وهم يتأثرون شخصياً واجتماعياً وثقافياً واقتصادياً بمرتكبي الجرائم الإلكترونية،

(تركيا)

116

الفقرة 15 جديدة من الديباجة مكررة

117 **(15 مكررة)** ***وإذ تضع في اعتبارها*** **أن البحوث تبين أنه في أوقات كوفيد-19، أصبح عدد أكبر من النساء والفتيات ضحايا للعنف على الإنترنت من خلال التهديدات البدنية والتحرش الجنسي والمطاردة، من بين أمور أخرى،**

(الفلبين)

118 **(15 مكررة)** ***وإذ تسلم*** **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،**

(السويد)

الفقرة 16 من الديباجة:

تعدّل لتصبح كالتالي:

119 (16) *وإذ تلاحظ* طبيعة التهديدات والمخاطر الناجمة عن ~~الجرائم الإلكترونية~~ **استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية** عبر الوطنية و~~الهجمات الإلكترونية~~ **تهديدات تكنولوجيا المعلومات والاتصالات** التي تهدد السلم والأمن الدوليين، والتطورات الهائلة في ~~الفضاء الإلكتروني~~ **بيئة تكنولوجيا المعلومات والاتصالات**، التي نجم عنها ازدياد تعقيد الأساليب التي يستخدمها مرتكبو الجرائم الإلكترونية **والجهات الفاعلة الخبيثة**،

(الجمهورية الإسلامية الإيرانية)

تعدّل لتصبح كالتالي:

120 *(16) وإذ تلاحظ* طبيعة التهديدات والمخاطر الناجمة عن ~~الجرائم الإلكترونية~~ **استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية** عبر الوطنية والهجمات الإلكترونية التي تهدد السلم والأمن الدوليين، والتطورات الهائلة في الفضاء الإلكتروني، التي نجم عنها ازدياد تعقيد الأساليب التي يستخدمها مرتكبو الجرائم الإلكترونية،

(باكستان)

تعدّل لتصبح كالتالي:

(16) وإذ تلاحظ طبيعة التهديدات والمخاطر الناجمة عن الجرائم الإلكترونية عبر الوطنية ~~والهجمات الإلكترونية~~ التي تهدد السلم والأمن الدوليين، والتطورات الهائلة في الفضاء الإلكتروني، التي نجم عنها ازدياد تعقيد الأساليب التي يستخدمها مرتكبو الجرائم الإلكترونية، 121

(السويد)

تعدّل لتصبح كالتالي:

(16) وإذ تلاحظ طبيعة التهديدات والمخاطر الناجمة عن الجرائم الإلكترونية عبر الوطنية ~~والهجمات الإلكترونية~~ **الحوادث الإلكترونية** التي تهدد السلم والأمن الدوليين، والتطورات الهائلة في الفضاء الإلكتروني، التي نجم عنها ازدياد تعقيد الأساليب التي يستخدمها مرتكبو الجرائم الإلكترونية، 122

(الهند)

تعدّل لتصبح كالتالي:

(16) وإذ تلاحظ طبيعة التهديدات والمخاطر الناجمة عن الجرائم الإلكترونية عبر الوطنية والهجمات الإلكترونية **الخبيثة** التي تهدد السلم والأمن الدوليين، والتطورات الهائلة في الفضاء الإلكتروني، التي نجم عنها ازدياد تعقيد الأساليب التي يستخدمها مرتكبو الجرائم الإلكترونية، 123

(بلجيكا)

الفقرة 16 جديدة من الديباجة مكررة

(16 مكررة) *وإذ تعرب عن القلق* إزاء الاستخدام العشوائي للهجمات الإلكترونية ضد أهداف الهياكل الأساسية المدنية، التي تلحق أضراراً غير متناسبة وغير ضرورية بمرافق توليد الطاقة وتوزيعها والمستشفيات ونظم المصارف وغيرها من الهياكل الأساسية الوطنية الحيوية، 124

(أوكرانيا)

الفقرة 17 من الديباجة:

تعدّل لتصبح كالتالي:

(17) وإذ تلاحظ أيضاً أن الجرائم ~~والهجمات~~ الإلكترونية لا ~~تشملان~~ **تشمل** الهجمات على ~~تكنولوجيات المعلومات والاتصالات~~ **أنظمة الحاسوب** فحسب، وانتهاكات الخصوصية، وإنشاء البرامج الخبيثة ونشرها، ولكن أيضاً ~~الهجمات~~ **تسهل الهجمات الإلكترونية بشكل متزايد** على الهياكل الأساسية ~~الوطنية~~ **المدنية**، فضلاً عن الأعمال الأخرى التي يمكن أن تحدث خارج الإنترنت، وتيسرها ~~تكنولوجيات المعلومات والاتصالات~~ **أنظمة الحاسوب**، بما في ذلك الاحتيال عبر الإنترنت، وشراء المخدرات، وغسل الأموال، وجرائم الكراهية، ~~والدعاية، والتلقين المتطرف،~~ والاستغلال الجنسي للنساء والأطفال عبر الإنترنت – وجميعها تؤثر سلباً على الأمن العالمي، والاستقرار الاقتصادي،

125

(السويد)

تعدّل لتصبح كالتالي:

(17) وإذ تلاحظ أيضاً أن الجرائم والهجمات الإلكترونية لا تشملان الهجمات على تكنولوجيات المعلومات والاتصالات فحسب، وانتهاكات الخصوصية، وإنشاء البرامج الخبيثة ونشرها، ولكن أيضاً الهجمات على الهياكل الأساسية الحيوية، ~~فضلاً عن الأعمال الأخرى التي يمكن أن تحدث خارج الإنترنت، وتيسرها تكنولوجيات المعلومات والاتصالات، بما في ذلك الاحتيال عبر الإنترنت، وشراء المخدرات، وغسل الأموال، وجرائم الكراهية، والدعاية، والتلقين المتطرف، والاستغلال الجنسي للنساء والأطفال عبر الإنترنت – وجميعها تؤثر سلباً على الأمن العالمي، والاستقرار الاقتصادي،~~ **مع الاعتراف أيضاً بالحاجة إلى التعاون الدولي بشأن الجرائم الخطيرة الأخرى التي يمكن تيسيرها بواسطة تكنولوجيا المعلومات والاتصالات،**

126

(ألمانيا)

127 تعدّل لتصبح كالتالي:

(17) وإذ تلاحظ أيضاً أن ~~الجرائم~~ **استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية** ~~والهجمات الإلكترونية~~ **وتهديدات تكنولوجيا المعلومات والاتصالات** لا تشملان الهجمات على تكنولوجيات المعلومات والاتصالات فحسب، وانتهاكات الخصوصية، **وحملات التضليل، و بناء الصور الملفقة، وكره الأجانب، والتدخل في الشؤون الداخلية للدول،** وإنشاء البرامج الخبيثة ونشرها، ولكن أيضاً الهجمات على الهياكل الأساسية الحيوية، فضلاً عن الأعمال الأخرى التي يمكن أن تحدث خارج الإنترنت، وتيسرها تكنولوجيات المعلومات والاتصالات، بما في ذلك الاحتيال عبر الإنترنت، وشراء المخدرات، وغسل الأموال، وجرائم الكراهية، والدعاية، والتلقين المتطرف، والاستغلال الجنسي للنساء والأطفال عبر الإنترنت – وجميعها تؤثر سلباً على الأمن العالمي، **فضلاً عن** الاستقرار الاقتصادي **والثقافي،**

(الجمهورية الإسلامية الإيرانية)

تعدّل لتصبح كالتالي:

(17) وإذ تلاحظ أيضاً أن الجرائم ~~والهجمات~~ **والحوادث** الإلكترونية لا تشملان الهجمات على تكنولوجيات المعلومات والاتصالات فحسب، وانتهاكات الخصوصية، وإنشاء البرامج الخبيثة ونشرها، ولكن أيضاً الهجمات على الهياكل الأساسية الحيوية، فضلاً عن الأعمال الأخرى التي
128 يمكن أن تحدث خارج الإنترنت، وتيسرها تكنولوجيات المعلومات والاتصالات، بما في ذلك الاحتيال عبر الإنترنت، وشراء المخدرات، وغسل الأموال، وجرائم الكراهية، والدعاية، والتلقين المتطرف، والاستغلال الجنسي للنساء والأطفال عبر الإنترنت – وجميعها تؤثر سلباً على الأمن العالمي، والاستقرار الاقتصادي،

(الهند)

تعدّل لتصبح كالتالي:

(17) وإذ تلاحظ أيضاً أن ~~الجرائم~~ **إساءة استخدام تكنولوجيا المعلومات والاتصالات لأغراض**
129 **إجرامية** والهجمات الإلكترونية لا تشملان الهجمات على تكنولوجيات المعلومات والاتصالات

فحسب، وانتهاكات الخصوصية، وإنشاء البرامج الخبيثة ونشرها، ولكن أيضاً الهجمات على الهياكل الأساسية الحيوية، فضلاً عن الأعمال الأخرى التي يمكن أن تحدث خارج الإنترنت، وتيسرها تكنولوجيات المعلومات والاتصالات، بما في ذلك الاحتيال عبر الإنترنت، وشراء المخدرات، وغسل الأموال، وجرائم الكراهية، والدعاية، والتلقين المتطرف، والاستغلال الجنسي للنساء والأطفال عبر الإنترنت – وجميعها تؤثر سلباً على الأمن العالمي، والاستقرار الاقتصادي،

(باكستان)

تعدّل لتصبح كالتالي:

(17) وإذ تلاحظ أيضاً أن الجرائم والهجمات الإلكترونية لا تشملان الهجمات ~~على تكنولوجيات المعلومات والاتصالات~~ **أنظمة الحاسوب** فحسب، وانتهاكات الخصوصية، وإنشاء البرامج الخبيثة ونشرها، ولكن أيضاً الهجمات على الهياكل الأساسية الحيوية، فضلاً عن الأعمال الأخرى التي يمكن أن تحدث خارج الإنترنت، ~~وتيسرها تكنولوجيات المعلومات والاتصالات~~ **ولكنها تحدث الآن في الفضاء الإلكتروني بتيسير من أنظمة الحاسوب**، بما في ذلك الاحتيال عبر الإنترنت، وشراء المخدرات، وغسل الأموال، وجرائم الكراهية، والدعاية، والتلقين المتطرف، والاستغلال الجنسي للنساء والأطفال عبر الإنترنت – وجميعها تؤثر سلباً على الأمن العالمي، والاستقرار الاقتصادي،

130

(سنغافورة)

تعدّل لتصبح كالتالي:

(17) وإذ تلاحظ أيضاً أن الجرائم والهجمات الإلكترونية ~~لا تشملان~~ **تتضمن على سبيل المثال لا الحصر** الهجمات على تكنولوجيات المعلومات والاتصالات ~~فحسب~~، وانتهاكات الخصوصية، وإنشاء البرامج الخبيثة ونشرها، ~~ولكن أيضاً~~ **والهجمات** على الهياكل الأساسية الحيوية، فضلاً عن الأعمال الأخرى التي يمكن أن تحدث خارج الإنترنت، وتيسرها تكنولوجيات المعلومات والاتصالات، بما في ذلك الاحتيال عبر الإنترنت، وشراء المخدرات، وغسل الأموال، وجرائم الكراهية، والدعاية، والتلقين المتطرف، والاستغلال الجنسي للنساء والأطفال عبر الإنترنت – وجميعها تؤثر سلباً على الأمن العالمي، والاستقرار الاقتصادي،

131

(كندا)

تعدّل لتصبح كالتالي:

(17) وإذ تلاحظ أيضاً أن الجرائم والهجمات الإلكترونية لا تشملان الهجمات على تكنولوجيات المعلومات والاتصالات فحسب، وانتهاكات الخصوصية، وإنشاء البرامج الخبيثة ونشرها، ولكن أيضاً الهجمات على الهياكل الأساسية الحيوية، فضلاً عن الأعمال الأخرى التي يمكن أن تحدث خارج الإنترنت، وتيسرها تكنولوجيات المعلومات والاتصالات، بما في ذلك الاحتيال عبر الإنترنت، وشراء المخدرات، وغسل الأموال، ~~وجرائم الكراهية، والدعاية، والتلقين المتطرف،~~ والاستغلال الجنسي للنساء والأطفال عبر الإنترنت – وجميعها تؤثر سلباً على الأمن العالمي، والاستقرار الاقتصادي،

132

(بلجيكا)

تعدّل لتصبح كالتالي:

(17) وإذ تلاحظ أيضاً أن الجرائم والهجمات الإلكترونية لا تشملان الهجمات على تكنولوجيات المعلومات والاتصالات فحسب، وانتهاكات الخصوصية، وإنشاء البرامج الخبيثة ونشرها، ولكن أيضاً الهجمات على الهياكل الأساسية الحيوية، فضلاً عن الأعمال الأخرى التي يمكن أن تحدث خارج الإنترنت، وتيسرها تكنولوجيات المعلومات والاتصالات، بما في ذلك الاحتيال عبر الإنترنت، وشراء المخدرات، وغسل الأموال، وجرائم الكراهية، والدعاية، والتلقين المتطرف، **والتسلط والمطاردة عبر الإنترنت، والاتجار بالأشخاص،** والاستغلال الجنسي للنساء والأطفال عبر الإنترنت – وجميعها تؤثر سلباً على الأمن العالمي، والاستقرار الاقتصادي،

133

(جنوب إفريقيا)

تعدّل لتصبح كالتالي:

(17) وإذ تلاحظ أيضاً أن الجرائم والهجمات الإلكترونية لا تشملان الهجمات على تكنولوجيات المعلومات والاتصالات فحسب، وانتهاكات الخصوصية، وإنشاء البرامج الخبيثة ونشرها، ولكن أيضاً الهجمات على الهياكل الأساسية الحيوية، فضلاً عن الأعمال الأخرى التي يمكن أن تحدث

134

خارج الإنترنت، وتيسرها تكنولوجيات المعلومات والاتصالات، بما في ذلك الاحتيال عبر الإنترنت، وشراء المخدرات، وغسل الأموال، **والاتجار بالأشخاص**، وجرائم الكراهية، والدعاية، والتلقين المتطرف، والاستغلال الجنسي للنساء والأطفال عبر الإنترنت – وجميعها تؤثر سلباً على الأمن العالمي، والاستقرار الاقتصادي،

(رومانيا)

تعدّل لتصبح كالتالي:

(17) وإذ تلاحظ أيضاً أن الجرائم والهجمات الإلكترونية لا تشملان الهجمات على تكنولوجيات المعلومات والاتصالات فحسب، وانتهاكات الخصوصية، وإنشاء البرامج الخبيثة ونشرها، ولكن أيضاً الهجمات على الهياكل الأساسية الحيوية، فضلاً عن الأعمال الأخرى التي يمكن أن تحدث
135 خارج الإنترنت، وتيسرها تكنولوجيات المعلومات والاتصالات، بما في ذلك الاحتيال عبر الإنترنت، وشراء المخدرات، وغسل الأموال، وجرائم الكراهية، والدعاية، والتلقين المتطرف، والاستغلال الجنسي للنساء والأطفال **بشكل خاص** عبر الإنترنت – وجميعها تؤثر سلباً على الأمن العالمي، والاستقرار الاقتصادي،

(ليتوانيا)

الفقرة 17 جديدة من الديباجة مكررة

(17 مكررة) *وإذ تسلم* بقيمة تبادل الخبرات مع مختلف تعاريف الجرائم والهجمات الإلكترونية
136 **من أجل بناء أساس أوسع نطاقاً لوضع تدابير لبناء الثقة،**

(كندا)

(17 مكررة) *وإذ تسلم* بأن انعدام مسؤولية مقدمي الخدمات والمنابر عبر الوطنية يشكل أيضاً تهديداً خطيراً في ميدان تكنولوجيا المعلومات والاتصالات، الأمر الذي يحتاج إلى أن يعالجه
137 **المجتمع الدولي،**

(الجمهورية الإسلامية الإيرانية)

الفقرة من 18 من الديباجة

138 تحذف الفقرة.

(اليابان)

تعدّل لتصبح كالتالي:

(18) *وإذ تضع في اعتبارها* أن معظم القوانين الوطنية قد سُنت قبل ~~وقت طويل من~~ نشوء الجرائم ~~والهجمات~~ الإلكترونية، ومن ثم فهي لا تتصدى دائماً لهذه التهديدات على النحو المناسب،

139 *(جمهورية التشيك)*

تعدّل لتصبح كالتالي:

(18) *وإذ تضع في اعتبارها* أن معظم القوانين الوطنية قد سُنت قبل وقت طويل من نشوء الجرائم ~~والهجمات~~ الإلكترونية، ومن ثم فهي لا تتصدى دائماً لهذه التهديدات على النحو المناسب،

140 *(السويد)*

تعدّل لتصبح كالتالي:

(18) *وإذ تضع في اعتبارها* أن معظم القوانين الوطنية قد سُنت قبل وقت طويل من نشوء ~~الجرائم~~ ~~والهجمات الإلكترونية~~ **استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية وتهديدات تكنولوجيا المعلومات والاتصالات** ومن ثم فهي لا تتصدى دائماً لهذه التهديدات على النحو المناسب،

141 *(الجمهورية الإسلامية الإيرانية)*

تعدّل لتصبح كالتالي:

(18) *وإذ تضع في اعتبارها* أن معظم القوانين الوطنية قد سُنت قبل وقت طويل من نشوء ~~الجرائم~~ **إساءة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية** والهجمات الإلكترونية، ومن ثم فهي لا تتصدى دائماً لهذه التهديدات على النحو المناسب،

142 *(باكستان)*

تعدّل لتصبح كالتالي:

(18) *وإذ تضع في اعتبارها* أن معظم القوانين الوطنية قد سُنت قبل وقت طويل من ~~نشوء~~ **انتشار** الجرائم والهجمات الإلكترونية، ومن ثم فهي لا تتصدى دائماً لهذه التهديدات على النحو المناسب،

143 *(تايلاند)*

تعدّل لتصبح كالتالي:

144

(18) *وإذ تضع في اعتبارها* أن معظم القوانين الوطنية قد سُنت قبل وقت طويل من نشوء الجرائم والهجمات **الخبيثة** الإلكترونية، ومن ثم فهي لا تتصدى دائماً لهذه التهديدات على النحو المناسب،

(بلجيكا)

الفقرة 18 جديدة من الديباجة مكررة

(18 مكررة) *وإذ تؤكد* الحاجة إلى تعزيز الجهود لسد الفجوة الرقمية بتيسير نقل تكنولوجيا المعلومات وبناء القدرات إلى البلدان النامية في مجالات استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية وأمن تكنولوجيا المعلومات والاتصالات،

145

(فيتنام)

منطوق مشروع القرار

146

الفقرة 1 من منطوق مشروع القرار

تحذف الفقرة.

(بلجيكا، كندا، اليابان، سويسرا)

147

تعدّل لتصبح كالتالي:

1. *تطلب* من المجتمع الدولي أن **يعدل** ويعتمد، عبر الأمم المتحدة، ~~تعاريف عالمية مشتركة~~ **تعريفاً عالمياً مشتركاً** للجرائم ~~والهجمات~~ الإلكترونية ~~تشمل كل تنوع لهذه الأفعال، والأفعال التي يمكن أن تيسرها؛~~

(السويد)

148

تعدّل لتصبح كالتالي:

1. *تطلب* من المجتمع الدولي أن يعتمد، عبر الأمم المتحدة، تعاريف عالمية مشتركة للجرائم والهجمات الإلكترونية ~~تشمل كل تنوع لهذه الأفعال، والأفعال التي يمكن أن تيسرها،~~

(ألمانيا، جمهورية كوريا، سنغافورة)

تعدّل لتصبح كالتالي:

149

1. *تطلب* من المجتمع الدولي أن يعتمد، عبر الأمم المتحدة، ~~تعاريف عالمية مشتركة~~ **تعريفاً عالمياً مشتركاً** للجرائم ~~والهجمات~~ الإلكترونية ~~تشمل~~ **يشمل** كل تنوع ~~لهذه الأفعال~~ **لهذا الفعل**، والأفعال التي يمكن أن تيسرها، **بما في ذلك التمييز الواضح بين الجريمة الإلكترونية والحرب الإلكترونية، وبين الأمن الإلكتروني والدفاع الإلكتروني؛**

(الأرجنتين)

تعدّل لتصبح كالتالي:

1. *تطلب* من المجتمع الدولي أن يعتمد، عبر الأمم المتحدة، ~~تعاريف عالمية مشتركة~~ **تعريفاً عالمياً مشتركاً**

150 للجرائم ~~والهجمات~~ الإلكترونية ~~تشمل~~ **يشمل** كل تنوع لهذه الأفعال، والأفعال التي يمكن أن تيسرها،

(جمهورية التشيك)

تعدّل لتصبح كالتالي:

151 1. *تطلب* من المجتمع الدولي أن يعتمد، عبر الأمم المتحدة، ~~تعاريف عالمية مشتركة للجرائم والهجمات الإلكترونية~~ **مصطلحات عالمية في مجال أمن تكنولوجيا المعلومات والاتصالات** تشمل كل تنوع لهذه الأفعال، والأفعال التي يمكن أن تيسرها،

(الجمهورية الإسلامية الإيرانية)

تعدّل لتصبح كالتالي:

1. *تطلب* من المجتمع الدولي أن يعتمد، عبر الأمم المتحدة، تعاريف عالمية مشتركة للجرائم ~~والهجمات الإلكترونية~~

152 **التي ترتكب من خلال استخدام تكنولوجيا المعلومات والاتصالات، والحوادث الإلكترونية التي** تشمل كل تنوع لهذه الأفعال، والأفعال التي يمكن أن تيسرها،

(الهند)

تعدّل لتصبح كالتالي:

153 1. *تطلب* من المجتمع الدولي أن يعتمد، عبر الأمم المتحدة، تعاريف عالمية مشتركة ~~للجرائم والهجمات الإلكترونية~~ **لإساءة استخدام تكنولوجيا المعلومات والاتصالات والحوادث الإلكترونية التي** تشمل كل تنوع لهذه الأفعال، والأفعال التي يمكن أن تيسرها،

(باكستان)

تعدّل لتصبح كالتالي:

154 1. *تطلب* من المجتمع الدولي أن يعتمد، عبر الأمم المتحدة، تعاريف عالمية مشتركة للجرائم والهجمات الإلكترونية تشمل كل تنوع لهذه الأفعال، والأفعال التي يمكن أن تيسرها، **مع الأخذ في الاعتبار واقع كل دولة؛**

(نيكاراغوا)

الفقرة 2 من منطوق مشروع القرار

155 تحذف الفقرة.

(بلجيكا، كندا)

تعدّل لتصبح كالتالي:

156 2. *وتشجع* البرلمانات على دعوة حكوماتها إلى دعم جهود الأمم المتحدة الرامية إلى سن اتفاقية ~~جديدة~~ **دولية شاملة** بشأن ~~الجرائم الإلكترونية~~ **مكافحة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية** من خلال المشاركة بنشاط في صياغتها؛

(الهند، روسيا الاتحادية)

تعدّل لتصبح كالتالي:

2. *وتشجع* البرلمانات على دعوة حكوماتها إلى دعم جهود الأمم المتحدة الرامية إلى سن اتفاقية جديدة بشأن ~~الجرائم الإلكترونية~~ **استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية** من خلال المشاركة بنشاط في

157 صياغتها؛

(الجمهورية الإسلامية الإيرانية)

تعدّل لتصبح كالتالي:

2. *وتشجع* البرلمانات على دعوة حكوماتها إلى دعم جهود الأمم المتحدة الرامية إلى سن اتفاقية جديدة بشأن

158 ~~الجرائم الإلكترونية~~ **إساءة استخدام تكنولوجيا المعلومات والاتصالات** من خلال المشاركة بنشاط في صياغتها؛

(باكستان)

الفقرة 2 مكررة جديدة من منطوق مشروع القرار

2 مكررة. *وتشجع* البرلمانات على دعوة حكوماتها إلى دعم جهود فريق الأمم المتحدة العامل مفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات واستخدامها من خلال المشاركة بنشاط في دوراته؛ 159

(الجمهورية الإسلامية الإيرانية)

الفقرة 3 من منطوق مشروع القرار 160

تحذف الفقرة.

(بلجيكا، كندا)

تعدّل لتصبح كالتالي:

3. وتحث البرلمانات وحكوماتها على أن تدرج في الاتفاقية ~~تعاريف شاملة للجرائم والهجمات الإلكترونية، إلى جانب~~ آليات تدعم التعاون الدولي لمكافحة الجرائم ~~والهجمات~~ الإلكترونية **مع توفير ضمانات كافية؛** 161

(السويد)

تعدّل لتصبح كالتالي: 162

3. وتحث البرلمانات وحكوماتها على أن تدرج في الاتفاقية ~~تعاريف شاملة للجرائم والهجمات الإلكترونية، إلى جانب~~ آليات تدعم التعاون الدولي لمكافحة الجرائم ~~والهجمات~~ الإلكترونية؛

(اليابان)

تعدّل لتصبح كالتالي:

3. وتحث البرلمانات وحكوماتها على أن تدرج في الاتفاقية ~~تعاريف شاملة للجرائم والهجمات الإلكترونية، إلى جانب~~ آليات تدعم التعاون الدولي لمكافحة الجرائم والهجمات الإلكترونية؛ 163

(ليتوانيا، جمهورية كوريا)

تعدّل لتصبح كالتالي:

3. وتحث البرلمانات وحكوماتها على أن تدرج في الاتفاقية ~~تعاريف~~ **قائمة** شاملة ~~للجرائم والهجمات الإلكترونية~~ **للجرائم الإلكترونية المحددة بوضوح**، إلى جانب آليات تدعم التعاون الدولي لمكافحة الجرائم والهجمات الإلكترونية؛ 164

(سويسرا)

تعدّل لتصبح كالتالي:

3. وتحث البرلمانات وحكوماتها على أن تدرج في الاتفاقية ~~تعاريف~~ **تعريف** شاملة ~~ة~~ للجرائم ~~والهجمات~~ الإلكترونية، إلى جانب آليات تدعم التعاون الدولي لمكافحة ~~الجرائم والهجمات الإلكترونية~~ **مثل هذه الجرائم، من دون الإخلال بتطبيق التشريعات الوطنية الحالية بشأن الأمن الإلكتروني وحماية البيانات الشخصية**؛ 165

(الأرجنتين)

تعدّل لتصبح كالتالي:

3. وتحث البرلمانات وحكوماتها على أن تدرج في الاتفاقية تعاريف شاملة للجرائم ~~والهجمات~~ الإلكترونية، إلى جانب آليات تدعم التعاون الدولي لمكافحة الجرائم ~~والهجمات~~ الإلكترونية؛ 166

(ألمانيا)

تعدّل لتصبح كالتالي:

3. وتحث البرلمانات وحكوماتها على أن تدرج في الاتفاقية ~~تعاريف شاملة للجرائم والهجمات الإلكترونية~~ **وكذلك نتائج فريق الأمم المتحدة العامل مفتوح العضوية المعني بأمن تكنولوجيا المعلومات والاتصالات، والمصطلحات العالمية في مجال أمن تكنولوجيا المعلومات والاتصالات**، إلى جانب آليات تدعم التعاون الدولي ~~لمكافحة الجرائم والهجمات الإلكترونية~~ **لمكافحة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية وتهديدات تكنولوجيا المعلومات والاتصالات**؛ 167

(الجمهورية الإسلامية الإيرانية)

تعدّل لتصبح كالتالي:

168 3. *وتحث* البرلمانات وحكوماتها على أن تدرج في الاتفاقية تعاريف شاملة ~~للجرائم والهجمات الإلكترونية~~ **للجرائم المرتكبة باستخدام تكنولوجيا المعلومات والاتصالات، والحوادث الإلكترونية**، إلى جانب آليات تدعم التعاون الدولي لمكافحة الجرائم ~~والهجمات الإلكترونية~~ **والحوادث الإلكترونية**؛

(الهند)

تعدّل لتصبح كالتالي:

169 3. *وتحث* البرلمانات وحكوماتها على أن تدرج في الاتفاقية تعاريف شاملة ~~للجرائم~~ **لإساءة استخدام تكنولوجيا المعلومات والاتصالات لأغراض** إجرامية ~~و~~ **ل**لهجمات الإلكترونية، إلى جانب آليات تدعم التعاون الدولي لمكافحة ~~الجرائم~~ **إساءة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية** والهجمات الإلكترونية؛

(باكستان)

تعدّل لتصبح كالتالي:

170 3. *وتحث* البرلمانات وحكوماتها على أن تدرج في الاتفاقية تعاريف شاملة للجرائم والهجمات الإلكترونية **بما في ذلك الجرائم الجنائية ذات الصلة، والضمانات المطلوبة لحماية حقوق الإنسان والحريات الأساسية**، إلى جانب آليات تدعم التعاون الدولي **والمساعدة التقنية** لمكافحة الجرائم والهجمات الإلكترونية **ومنع حدوثها**؛

(جنوب إفريقيا)

تعدّل لتصبح كالتالي:

171 3. *وتحث* البرلمانات وحكوماتها على أن تدرج في الاتفاقية تعاريف شاملة للجرائم والهجمات الإلكترونية، إلى جانب آليات تدعم التعاون الدولي **المتعدد الجهات المعنية، وكذلك، مبادئها للتنفيذ والتقييم**، لمكافحة الجرائم والهجمات الإلكترونية **بشكل فعال**؛

(تايلاند)

الفقرة 3 مكررة جديدة من منطوق مشروع القرار

172 **3 مكررة. *كما تحث* البرلمانات وحكوماتها على ضمان أن الاتفاقية الجديدة تكمل الصكوك الدولية والإقليمية القائمة بشأن الجرائم الإلكترونية والجريمة المنظمة العابرة للحدود الوطنية، فضلاً عن الصكوك الأخرى ذات الصلة، ولا سيما تلك المتعلقة بحماية حقوق الإنسان؛**

(رومانيا)

173 **3 مكررة. *كما تحث* البرلمانات وحكوماتها على التأكيد على أهمية أن تتضمن الاتفاقية الجديدة حماية قوية لحقوق الإنسان والحريات الأساسية؛**

(السويد)

الفقرة 4 من منطوق مشروع القرار

174 تحذف الفقرة.

(بلجيكا، كندا)

تعدّل لتصبح كالتالي:

175 4. *وتدعو* البرلمانات وحكوماتها إلى استخدام هذه الاتفاقية، بمجرد اعتمادها، كوسيلة لتعزيز التشريعات الوطنية وزيادة التعاون الدولي لمكافحة الجرائم ~~والهجمات~~ الإلكترونية؛

(الأرجنتين، جمهورية التشيك، ألمانيا، السويد)

176 4. *وتدعو* البرلمانات وحكوماتها إلى استخدام هذه الاتفاقية، بمجرد اعتمادها، كوسيلة لتعزيز التشريعات الوطنية وزيادة التعاون الدولي لمكافحة ~~الجرائم والهجمات الإلكترونية~~ **استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية وتهديدات تكنولوجيا المعلومات والاتصالات؛**

(الجمهورية الإسلامية الإيرانية)

تعدّل لتصبح كالتالي:

177 4. *وتدعو* البرلمانات وحكوماتها إلى استخدام هذه الاتفاقية، بمجرد اعتمادها، كوسيلة لتعزيز التشريعات الوطنية وزيادة التعاون الدولي لمكافحة ~~الجرائم~~ **إساءة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية** والهجمات الإلكترونية؛

(باكستان)

تعدّل لتصبح كالتالي:

178 4. *وتدعو* البرلمانات وحكوماتها إلى استخدام هذه الاتفاقية، بمجرد اعتمادها، كوسيلة ~~لتعزيز~~ **لتحديث** التشريعات الوطنية وزيادة التعاون الدولي لمكافحة الجرائم والهجمات الإلكترونية؛

(اليابان)

تعدّل لتصبح كالتالي:

179 4. *وتدعو* البرلمانات وحكوماتها إلى استخدام هذه الاتفاقية، بمجرد اعتمادها **ومتى أصبحت سارية،** كوسيلة لتعزيز التشريعات الوطنية وزيادة التعاون الدولي لمكافحة الجرائم والهجمات الإلكترونية؛

(فيتنام)

تعدّل لتصبح كالتالي:

180 4. *وتدعو* البرلمانات وحكوماتها إلى استخدام ~~هذه~~ الاتفاقية **المذكورة في الفقرتين 2 و3 من المنطوق الواردتين أعلاه،** بمجرد اعتمادها، كوسيلة لتعزيز التشريعات الوطنية وزيادة التعاون الدولي لمكافحة الجرائم والهجمات الإلكترونية؛

(جنوب السودان)

الفقرة 4 مكررة جديدة من منطوق مشروع القرار

181 **4 مكررة.** ***وتشجع*** **البرلمانات على أن تأخذ في الاعتبار بالكامل الإمكانات التخريبية والتدميرية للهجمات الإلكترونية من خلال معالجة مسألة حماية الهياكل الأساسية الوطنية الأساسية، بما في ذلك على سبيل المثال لا الحصر الكهرباء والمياه والغاز والاتصالات ومحطات الطاقة النووية والنقل والتمويل والإمدادات الغذائية؛**

(الأرجنتين)

4 مكررة. ***وتشجع*** **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*** **المؤرخة 23 تشرين الثاني/نوفمبر 2001 ("اتفاقية بودابست") ، وهي أكثر المعاهدات المتعددة الأطراف شمولاً بشأن الجرائم الإلكترونية السارية والمفتوحة للانضمام إليها من قبل جميع الدول؛** 182

(رومانيا)

الفقرة 5 من منطوق مشروع القرار

تعدّل لتصبح كالتالي:

5. *وتطلب من* البرلمانات أن ~~تسن~~ **تحرص من أن** تشريعات ~~جديدة~~ بشأن الجرائم ~~والهجمات~~ الإلكترونية **محدثة وذات صلة،** بالنظر إلى الزيادة المستمرة في حجم هذه الأعمال وتواترها وآثارها على السلم والأمن الدوليين، والاستقرار الاقتصادي العالمي؛ 183

(السويد)

تعدّل لتصبح كالتالي:

5. *وتطلب من* البرلمانات أن تسن، **عند الاقتضاء،** تشريعات جديدة بشأن الجرائم ~~والهجمات~~ الإلكترونية، بالنظر إلى الزيادة المستمرة في حجم هذه الأعمال وتواترها وآثارها على السلم والأمن الدوليين، والاستقرار الاقتصادي العالمي؛ 184

(جمهورية التشيك)

تعدّل لتصبح كالتالي:

5. *وتطلب من* البرلمانات أن تسن تشريعات جديدة بشأن ~~الجرائم والهجمات الإلكترونية~~ **استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية وتهديدات تكنولوجيا المعلومات والاتصالات،** بالنظر إلى الزيادة المستمرة في حجم هذه الأعمال وتواترها وآثارها على السلم والأمن الدوليين، والاستقرار الاقتصادي العالمي؛ 185

(الجمهورية الإسلامية الإيرانية)

تعدّل لتصبح كالتالي:

5. *وتطلب من* البرلمانات أن تسن تشريعات جديدة بشأن الجرائم ~~والهجمات~~ الإلكترونية **والأمن الإلكتروني**، بالنظر إلى الزيادة المستمرة في حجم ~~هذه الأعمال~~ **الجرائم الإلكترونية والهجمات الإلكترونية الخبيثة** وتواترها وآثارها على السلم والأمن الدوليين، والاستقرار الاقتصادي العالمي؛ **186**

(بلجيكا)

تعدّل لتصبح كالتالي:

5. *وتطلب من* البرلمانات أن تسن تشريعات جديدة بشأن ~~الجرائم~~ **إساءة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية** والهجمات الإلكترونية، بالنظر إلى الزيادة المستمرة في حجم هذه الأعمال وتواترها وآثارها على السلم والأمن الدوليين، والاستقرار الاقتصادي العالمي؛ **187**

(باكستان)

تعدّل لتصبح كالتالي:

5. *وتطلب من* البرلمانات أن **تحدّث** ~~تسن~~ تشريعات **وطنية** ~~جديدة~~ بشأن الجرائم والهجمات الإلكترونية، بالنظر إلى الزيادة المستمرة في حجم هذه الأعمال وتواترها وآثارها على السلم والأمن الدوليين، والاستقرار الاقتصادي العالمي؛ **188**

(اليابان)

تعدّل لتصبح كالتالي:

5. *وتطلب من* البرلمانات ~~أن تسن تشريعات~~ **التي لم تسن بعد قانوناً جديداً** بشأن الجرائم والهجمات الإلكترونية **أن تقوم بذلك**، بالنظر إلى الزيادة المستمرة في ~~حجم هذه~~ **ارتكاب** أعمال **غير مشروعة** وتواترها وآثارها **المنطوية على مخاطر كبيرة** على السلم والأمن الدوليين، والاستقرار الاقتصادي العالمي؛ **189**

(نيكاراغوا)

تعدّل لتصبح كالتالي:

5. *وتطلب من* البرلمانات أن تسن تشريعات جديدة بشأن الجرائم والهجمات الإلكترونية **وفقاً للقانون الدولي، بما فيه صكوك حقوق الإنسان الدولية**، بالنظر إلى الزيادة المستمرة في حجم هذه الأعمال وتواترها وآثارها على السلم والأمن الدوليين، والاستقرار الاقتصادي العالمي، **وأن تدرج 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؛** **190**

(جنوب إفريقيا)

تعدّل لتصبح كالتالي:

5. *وتطلب من* البرلمانات أن تسن تشريعات جديدة بشأن الجرائم والهجمات الإلكترونية، **من خلال إشراك جميع الجهات المعنية، بما فيها القطاع الخاص، والأوساط الأكاديمية، والمجتمع المدني، والمجتمع التقني،** بالنظر إلى الزيادة المستمرة في حجم هذه الأعمال وتواترها وآثارها على **الأمن الوطني،** والسلم والأمن الدوليين، والاستقرار الاقتصادي العالمي؛ **191**

(رومانيا)

تعدّل لتصبح كالتالي:

5. *وتطلب من* البرلمانات أن تسن تشريعات جديدة **أو تستعرض قوانين** بشأن الجرائم والهجمات الإلكترونية، بالنظر إلى الزيادة المستمرة في حجم هذه الأعمال وتواترها وآثارها على السلم والأمن الدوليين، والاستقرار الاقتصادي العالمي؛ **192**

(فيتنام)

تعدّل لتصبح كالتالي:

5. *وتطلب من* البرلمانات أن تسن تشريعات جديدة بشأن الجرائم والهجمات الإلكترونية، **وتخصص الموارد الضرورية لهذه الغاية،** بالنظر إلى الزيادة المستمرة في حجم هذه الأعمال وتواترها وآثارها على السلم والأمن الدوليين، والاستقرار الاقتصادي العالمي؛ **193**

(فرنسا)

تعدّل لتصبح كالتالي:

5. *وتطلب من* البرلمانات أن تسن تشريعات جديدة بشأن الجرائم والهجمات الإلكترونية بالنظر إلى الزيادة المستمرة في حجم هذه الأعمال **ونطاقها وسرعتها وتعقدها** وتواترها وآثارها على السلم والأمن الدوليين، والاستقرار الاقتصادي العالمي؛ **194**

(الهند)

الفقرة 5 مكررة جديدة من منطوق مشروع القرار

195 **5 مكررة.** ***وتدعو*** **المجتمع الدولي إلى عدم استخدام تكنولوجيا المعلومات والاتصالات وشبكات المعلومات والاتصالات للتدخل في الشؤون الداخلية للدول الأخرى أو بهدف تقويض استقرارها السياسي والاقتصادي والاجتماعي؛**

(الجمهورية الإسلامية الإيرانية)

196 **5 مكررة.** ***وتحث*** **البرلمانات على ضمان إدراج تقييمات الأثر على حقوق الإنسان في جميع العمليات التشريعية المتعلقة بالجرائم والهجمات الإلكترونية؛**

(رومانيا)

197 **5 مكررة.** ***وتدعو*** **البرلمانات أيضاً إلى تعزيز قدرة ضباط إنفاذ القانون، بما في ذلك سلطات التحقيق والمدعون العامون والقضاة، في مجال الهجمات والجرائم الإلكترونية، وتجهيزهم للتحقيق الفعال والملاحقة القضائية والفصل في قضايا الهجمات والجرائم الإلكترونية؛**

(جنوب إفريقيا)

198 **5 مكررة.** ***وتحث*** **البرلمانات والحكومات على وضع واعتماد إطار قانوني عالمي للحرب الإلكترونية، يتضمن مفهومي التمييز والتناسب، لمنع الهجمات الإلكترونية ضد الهياكل الأساسية المدنية الأساسية؛**

(أوكرانيا)

الفقرة 6 من منطوق مشروع القرار

199 تعدّل لتصبح كالتالي:

6. *وتشجع* البرلمانات على الاستفادة الكاملة من وظيفتها الرقابية لضمان أن تكون لدى الحكومات الأدوات اللازمة للسيطرة على الزيادة السريعة في ~~الجرائم والهجمات الإلكترونية~~ **الجرائم الإلكترونية** ولحماية ~~الأمن الرقمي~~ **الأمن الإلكتروني** للمواطنين وهويتهم وخصوصيتهم وبياناتهم، ولا سيما أشدهم ضعفاً؛

(جمهورية التشيك)

تعدّل لتصبح كالتالي:

6. *وتشجع* البرلمانات على الاستفادة الكاملة من وظيفتها الرقابية لضمان أن تكون لدى الحكومات الأدوات اللازمة ~~للسيطرة على~~ **لمنع ومكافحة** الزيادة السريعة في الجرائم ~~والهجمات~~ الإلكترونية ولحماية الأمن الرقمي للمواطنين وهويتهم وخصوصيتهم وبياناتهم، ولا سيما أشدهم ضعفاً؛ **200**

(بلجيكا)

تعدّل لتصبح كالتالي:

6. *وتشجع* البرلمانات على الاستفادة الكاملة من وظيفتها الرقابية لضمان أن تكون لدى الحكومات الأدوات اللازمة للسيطرة على الزيادة السريعة في الجرائم ~~والهجمات~~ الإلكترونية ولحماية الأمن الرقمي للمواطنين وهويتهم وخصوصيتهم وبياناتهم، ولا سيما أشدهم ضعفاً، **مع صون حقوق الإنسان والحريات؛** **201**

(السويد)

تعدّل لتصبح كالتالي:

6. *وتشجع* البرلمانات على الاستفادة الكاملة من وظيفتها الرقابية لضمان أن تكون لدى الحكومات الأدوات اللازمة للسيطرة على الزيادة السريعة في ~~الجرائم والهجمات الإلكترونية~~ **استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية وتهديدات تكنولوجيا المعلومات والاتصالات** ولحماية الأمن الرقمي للمواطنين وهويتهم وخصوصيتهم وبياناتهم، ولا سيما أشدهم ضعفاً؛ **202**

(الجمهورية الإسلامية الإيرانية)

تعدّل لتصبح كالتالي:

6. *وتشجع* البرلمانات على الاستفادة الكاملة من وظيفتها الرقابية لضمان أن تكون لدى الحكومات الأدوات اللازمة للسيطرة على الزيادة السريعة في ~~الجرائم~~ **إساءة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية** والهجمات الإلكترونية ولحماية الأمن الرقمي للمواطنين وهويتهم وخصوصيتهم وبياناتهم، ولا سيما أشدهم ضعفاً؛ **203**

(باكستان)

تعدّل لتصبح كالتالي:

204 6. *وتشجع* البرلمانات على الاستفادة الكاملة من وظيفتها ~~الرقابية~~ لضمان أن تكون لدى الحكومات الأدوات اللازمة ~~للسيطرة على~~ **بوجه** الزيادة السريعة في الجرائم والهجمات الإلكترونية ولحماية الأمن الرقمي للمواطنين وهويتهم وخصوصيتهم وبياناتهم، ولا سيما أشدهم ضعفاً؛

(اليابان)

تعدّل لتصبح كالتالي:

205 6. *وتشجع* البرلمانات على الاستفادة الكاملة من وظيفتها الرقابية لضمان أن تكون لدى الحكومات الأدوات اللازمة للسيطرة على الزيادة السريعة في الجرائم والهجمات الإلكترونية ولحماية الأمن الرقمي للمواطنين وهويتهم وخصوصيتهم وبياناتهم~~، ولا سيما أشدهم ضعفاً~~؛

(الهند)

تعدّل لتصبح كالتالي:

206 6. *وتشجع* البرلمانات على الاستفادة الكاملة من وظيفتها الرقابية لضمان أن تكون لدى الحكومات الأدوات اللازمة، **بما في ذلك الموارد والقدرات الملائمة،** للسيطرة على الزيادة السريعة في الجرائم والهجمات الإلكترونية ولحماية الأمن الرقمي للمواطنين وهويتهم وخصوصيتهم وبياناتهم، ولا سيما أشدهم ضعفاً؛

(جنوب إفريقيا)

تعدّل لتصبح كالتالي:

207 6. *وتشجع* البرلمانات على الاستفادة الكاملة من وظيفتها الرقابية لضمان أن تكون لدى الحكومات الأدوات اللازمة للسيطرة على الزيادة السريعة في الجرائم والهجمات الإلكترونية ولحماية **حقوق الإنسان في الفضاء الإلكتروني بما في ذلك** الأمن الرقمي للمواطنين وهويتهم وخصوصيتهم وبياناتهم، ولا سيما أشدهم ضعفاً؛

(الأرجنتين)

208

الفقرة 6 مكررة جديدة من منطوق مشروع القرار

6 مكررة. *وتدعو* برلمانات وحكومات البلدان المتقدمة إلى مساعدة البلدان النامية في جهودها لتعزيز بناء القدرات في مجال أمن تكنولوجيا المعلومات والاتصالات وسد الفجوة الرقمية؛

(الجمهورية الإسلامية الإيرانية)

209

الفقرة 6 مكررة ثانياً جديدة من منطوق مشروع القرار

6 مكررة ثانياً. *كما تدعو* البرلمانات وحكوماتها إلى الامتناع عن اعتماد أي تدابير قسرية من جانب واحد تقيد أو تمنع الوصول الشامل إلى فوائد تكنولوجيا المعلومات والاتصالات؛

(الجمهورية الإسلامية الإيرانية)

210

الفقرة 7 من منطوق مشروع القرار

تعدّل لتصبح كالتالي:

7. *وتوصي بشدة* بأن **تضمن البرلمانات أن الإطار التشريعي بشأن حماية الهياكل الأساسية الوطنية الأساسية، بما فيها الهياكل الأساسية التي تدعم الإنترنت، محدثة، وأنها تستعرض أو** تضع أطراً تشريعية ~~ترمي إلى حماية الهياكل الأساسية الحيوية التي تدعم الإنترنت، ولا سيما الكابلات البحرية والشبكات الفضائية وخدمات الإنترنت الأساسية، فضلاً عن مراكز البيانات العامة والخاصة الكبيرة التي توفر الخدمات السحابية، التي ينبغي لها بدورها أن تتبادل المعلومات عن الحوادث الإلكترونية، في الوقت الحقيقي، عبر الهيئات الوطنية وفوق الوطنية ذات الصلة~~ **عند الاقتضاء؛**

(سويسرا)

211

تعدّل لتصبح كالتالي:

7. *وتوصي بشدة* بأن تضع البرلمانات أطراً تشريعية ترمي إلى حماية الهياكل الأساسية **المدنية الحيوية** ~~التي تدعم الإنترنت، ولا سيما الكابلات البحرية والشبكات الفضائية وخدمات الإنترنت الأساسية، فضلاً عن مراكز البيانات العامة والخاصة الكبيرة التي توفر الخدمات السحابية،~~ التي ينبغي لها بدورها أن تتبادل المعلومات عن الحوادث الإلكترونية، في الوقت الحقيقي، عبر الهيئات الوطنية وفوق الوطنية ذات الصلة؛

(السويد)

تعدّل لتصبح كالتالي:

7. *وتوصي بشدة* بأن تضع البرلمانات أطراً تشريعية ترمي إلى حماية الهياكل الأساسية الحيوية التي تدعم الإنترنت، ولا سيما الكابلات البحرية والشبكات الفضائية وخدمات الإنترنت الأساسية، **212** ~~فضلاً عن مراكز البيانات العامة والخاصة الكبيرة التي توفر الخدمات السحابية، التي ينبغي لها بدورها أن تتبادل المعلومات عن الحوادث الإلكترونية، في الوقت الحقيقي، عبر الهيئات الوطنية وفوق الوطنية ذات الصلة~~ **وإلى تيسير التعاون مع القطاع الخاص؛**

(ألمانيا)

تعدّل لتصبح كالتالي:

7. *وتوصي بشدة* بأن تضع البرلمانات أطراً تشريعية ~~ترمي إلى حماية~~ **لموفري خدمة الإنترنت، من أجل حماية** الهياكل الأساسية الحيوية التي تدعم الإنترنت، ولا سيما الكابلات البحرية والشبكات الفضائية **213** وخدمات الإنترنت الأساسية، فضلاً عن مراكز البيانات العامة والخاصة الكبيرة التي توفر الخدمات السحابية، التي ينبغي لها بدورها أن تتبادل المعلومات عن الحوادث الإلكترونية، في الوقت الحقيقي، عبر الهيئات الوطنية وفوق الوطنية ذات الصلة؛

(نيكاراغوا)

تعدّل لتصبح كالتالي:

7. *وتوصي بشدة* بأن تضع البرلمانات أطراً تشريعية ترمي إلى حماية الهياكل الأساسية الحيوية التي تدعم الإنترنت، ولا سيما الكابلات البحرية والشبكات الفضائية وخدمات الإنترنت الأساسية، فضلاً عن مراكز البيانات العامة والخاصة الكبيرة التي توفر الخدمات السحابية، التي ينبغي لها بدورها أن تتبادل المعلومات **214** عن الحوادث الإلكترونية، في الوقت الحقيقي، عبر الهيئات الوطنية ~~وفوق الوطنية~~ **الدولية** ذات الصلة؛

(الهند)

تعدّل لتصبح كالتالي:

7. *وتوصي بشدة* بأن تضع البرلمانات أطراً تشريعية ترمي إلى حماية الهياكل الأساسية الحيوية التي تدعم الإنترنت، ولا سيما الكابلات البحرية والشبكات الفضائية وخدمات الإنترنت الأساسية، فضلاً عن مراكز **215** البيانات العامة والخاصة الكبيرة التي توفر الخدمات السحابية، التي ينبغي لها بدورها أن تتبادل المعلومات عن الحوادث الإلكترونية، ~~في الوقت الحقيقي،~~ عبر الهيئات الوطنية وفوق الوطنية ذات الصلة؛

(بلجيكا)

تعدّل لتصبح كالتالي:

7. *وتوصي بشدة* بأن تضع البرلمانات أطراً تشريعية ترمي إلى حماية الهياكل الأساسية الحيوية التي تدعم ~~الإنترنت~~ **الفضاء الإلكتروني**، ولا سيما الكابلات البحرية والشبكات الفضائية وخدمات الإنترنت الأساسية، فضلاً عن مراكز البيانات العامة والخاصة الكبيرة التي توفر الخدمات السحابية، التي ينبغي لها بدورها أن تتبادل المعلومات عن الحوادث الإلكترونية، في الوقت الحقيقي، عبر الهيئات الوطنية وفوق الوطنية ذات الصلة؛ 216

(ليتوانيا)

تعدّل لتصبح كالتالي:

7. *وتوصي بشدة* بأن تضع البرلمانات أطراً تشريعية ترمي إلى حماية الهياكل الأساسية الحيوية التي تدعم الإنترنت **من الهجمات الإلكترونية**، ولا سيما الكابلات البحرية والشبكات الفضائية وخدمات الإنترنت الأساسية، فضلاً عن مراكز البيانات العامة والخاصة الكبيرة التي توفر الخدمات السحابية، التي ينبغي لها بدورها أن تتبادل المعلومات عن الحوادث الإلكترونية، في الوقت الحقيقي، عبر الهيئات الوطنية وفوق الوطنية ذات الصلة؛ 217

(الأرجنتين)

الفقرة 7 مكررة جديدة من منطوق مشروع القرار

7 مكررة. *وتوصي* أيضاً بأن تؤدي جميع الدول الدور نفسه في الحوكمة الدولية للإنترنت وتحملها مسؤولية متساوية من خلال إنشاء آلية دولية متعددة الأطراف وشفافة وديمقراطية لحوكمة الإنترنت؛ 218

(الجمهورية الإسلامية الإيرانية)

الفقرة 8 من منطوق مشروع القرار

تعدّل لتصبح كالتالي:

8. *وتشجع* البرلمانات على الترويج ~~لفضاء إلكتروني~~ **لبيئة تكنولوجيا المعلومات والاتصالات** آمنة من خلال دعوة حكوماتها إلى التعاون في وقف ~~الجريمة الإلكترونية~~ **استخدام تكنولوجيا المعلومات** 219

والاتصالات لأغراض إجرامية، وكذلك، مرتكبي الجرائم الإلكترونية **والجهات الفاعلة الخبيثة،** للاستجابة لطلبات المساعدة **وبناء القدرات،** في الوقت الحقيقي إن أمكن، 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؛

(الجمهورية الإسلامية الإيرانية)

تعدّل لتصبح كالتالي:

8. *وتشجع* البرلمانات على الترويج لفضاء إلكتروني آمن من خلال دعوة حكوماتها إلى التعاون في وقف ~~الجريمة الإلكترونية~~ **إساءة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية** ومرتكبي الجرائم الإلكترونية، للاستجابة لطلبات المساعدة، في الوقت الحقيقي إن أمكن، لتأمين سلسلة التوريد للشركات في بلدانها، وتقديم 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؛ **220**

(باكستان)

تعدّل لتصبح كالتالي:

8. ~~وتشجع~~ **وتحث** البرلمانات على الترويج لفضاء إلكتروني آمن من خلال دعوة حكوماتها إلى التعاون في وقف الجريمة الإلكترونية ومرتكبي الجرائم الإلكترونية، للاستجابة لطلبات المساعدة، في الوقت الحقيقي إن أمكن، لتأمين سلسلة ~~التوريد للشركات في بلدانها~~ **مع مقدمي الخدمات في كل بلد،** وتقديم 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؛ **221**

(نيكارغوا)

تعدّل لتصبح كالتالي:

8. *وتشجع* البرلمانات على الترويج لفضاء إلكتروني **مفتوح ومجاني** وآمن من خلال دعوة حكوماتها إلى التعاون في ~~وقف~~ **مكافحة** الجريمة الإلكترونية ومرتكبي الجرائم الإلكترونية، للاستجابة لطلبات **222**

المساعدة، في الوقت الحقيقي إن أمكن، لتأمين سلسلة التوريد للشركات في بلدانها، وتقديم 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؛

(جمهورية التشيك)

تعدّل لتصبح كالتالي:

223 8. *وتشجع* البرلمانات على الترويج لفضاء إلكتروني آمن من خلال دعوة حكوماتها إلى **الالتزام بقواعد الأمم المتحدة المتعلقة بسلوك الدول المسؤول في الفضاء الإلكتروني و**التعاون في وقف الجريمة الإلكترونية ومرتكبي الجرائم الإلكترونية، للاستجابة لطلبات المساعدة، في الوقت الحقيقي إن أمكن، لتأمين سلسلة التوريد للشركات في بلدانها، وتقديم 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؛

(كندا)

تعدّل لتصبح كالتالي:

224 8. *وتشجع* البرلمانات على الترويج لفضاء إلكتروني آمن من خلال دعوة حكوماتها إلى التعاون في ~~وقف~~ **منع** الجريمة الإلكترونية **ومكافحتها** ~~ومرتكبي الجرائم الإلكترونية~~، للاستجابة لطلبات المساعدة، في الوقت الحقيقي إن أمكن، لتأمين سلسلة التوريد للشركات في بلدانها، وتقديم 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؛

(ليتوانيا)

تعدّل لتصبح كالتالي:

225 8. *وتشجع* البرلمانات على الترويج لفضاء إلكتروني آمن من خلال دعوة حكوماتها إلى التعاون في ~~وقف~~ **التخفيف من حدة آثار الجرائم والهجمات الإلكترونية** ~~الجريمة الإلكترونية ومرتكبي~~ الجرائم الإلكترونية، للاستجابة لطلبات المساعدة، في الوقت الحقيقي إن أمكن، لتأمين سلسلة التوريد للشركات في بلدانها، وتقديم 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؛

(الأرجنتين)

تعدّل لتصبح كالتالي:

8. *وتشجع* البرلمانات على الترويج لفضاء إلكتروني آمن من خلال دعوة حكوماتها إلى التعاون في وقف الجريمة الإلكترونية ومرتكبي الجرائم الإلكترونية، للاستجابة لطلبات المساعدة **وتبادل المعلومات بشأن الحوادث الإلكترونية ومرتكبي الجريمة الإلكترونية**، في الوقت الحقيقي إن أمكن، لتأمين سلسلة التوريد للشركات في بلدانها، وتقديم 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؛ **226**

(أوكرانيا)

تعدّل لتصبح كالتالي:

8. *وتشجع* البرلمانات على الترويج لفضاء إلكتروني آمن من خلال دعوة حكوماتها إلى التعاون في وقف الجريمة الإلكترونية ومرتكبي الجرائم الإلكترونية، للاستجابة لطلبات المساعدة، في الوقت الحقيقي إن أمكن، **وفقاً لسيادة القانون والاحترام الكامل للقانون الدولي لحقوق الإنسان والحريات الأساسية**، لتأمين سلسلة التوريد للشركات في بلدانها، وتقديم 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؛ **227**

(ألمانيا)

تعدّل لتصبح كالتالي:

8. *وتشجع* البرلمانات على الترويج لفضاء إلكتروني آمن من خلال دعوة حكوماتها إلى التعاون في وقف الجريمة الإلكترونية ومرتكبي الجرائم الإلكترونية، للاستجابة لطلبات المساعدة، في الوقت الحقيقي إن أمكن، لتأمين سلسلة التوريد للشركات في بلدانها، وتقديم تقارير عن مواطن الضعف المحتملة ~~أمام أطراف ثالثة~~ ~~ولمساعدتها~~ **والمساعدة** في منع وقوع حوادث في المستقبل، وعلى وجه الخصوص دعم وحماية جميع فرق الاستجابة للحوادث الإلكترونية داخل حدودها وخارجها؛ **228**

(الهند)

الفقرة 9 من منطوق مشروع القرار

تعدّل لتصبح كالتالي:

229 9. *وتشجع أيضاً* البرلمانات على صياغة تشريعات 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 لتهديدات ~~الإلكترونية~~ **تكنولوجيا المعلومات والاتصالات؛**

(الجمهورية الإسلامية الإيرانية)

تعدّل لتصبح كالتالي:

230 9. *وتشجع أيضاً* البرلمانات على صياغة تشريعات 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**، حيث لم ترد بعد في بلدانها؛**

(نيكاراغوا)

تعدّل لتصبح كالتالي:

9. *وتشجع أيضاً* البرلمانات على صياغة تشريعات تعزز الخدمات ~~الأمن الإلكتروني~~ الشاملة **للأمن في استخدام تكنولوجيا المعلومات والاتصالات، المشار إليها في ما بعد بـ"الأمن الإلكتروني"**، التي تعطي 231 الأولوية للوقاية (التوعية ومراجعة الحسابات والتدريب)، والكشف عن الحوادث (24 ساعة في اليوم، 7 أيام في الأسبوع)، والتصدي الفوري والفعال **للتهديدات على الأمن في استخدام تكنولوجيا المعلومات والاتصالات، المشار إليها في ما بعد بـ** "التهديدات الإلكترونية"؛

(روسيا الاتحادية)

الفقرة 10 من منطوق مشروع القرار

تعدّل لتصبح كالتالي:

10. *وتوصي* بأن ~~تنشئ~~ **تعزز** البرلمانات **إقامة** المؤسسات والهيئات ذات الصلة – مثل المراكز الوطنية لأمن الفضاء الإلكتروني، وفرق الاستجابة للطوارئ الحاسوبية، وفرق التصدي للحوادث الأمنية الحاسوبية، 232 ومراكز العمليات الأمنية – حيثما لا ترد هذه المؤسسات والهيئات في بلدانها؛

(رومانيا)

تعدّل لتصبح كالتالي:

10. *وتوصي* بأن **تقدم** البرلمانات **المشورة إلى حكوماتها من أجل** إنشاء المؤسسات والهيئات **لمنع الجرائم والهجمات الإلكترونية** 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؛ **233**

(تايلاند)

الفقرة 11 من منطوق مشروع القرار

تعدّل لتصبح كالتالي:

11. *وتوصي أيضاً* بأن تضمن ~~جميع~~ البرلمانات أن تتوافر لهذه المؤسسات والهيئات موارد كافية من الموازنة وموظفون متخصصون للسماح باستجابة مرنة وفعالة للهجمات الإلكترونية، وحماية الهياكل الأساسية الحيوية والمؤسسات العامة والشركات والمواطنين؛ **234**

(جمهورية كوريا)

تعدّل لتصبح كالتالي:

11. *وتوصي أيضاً* بأن تضمن جميع البرلمانات أن تتوافر لهذه المؤسسات والهيئات موارد كافية من الموازنة وموظفون متخصصون، **خضعوا لتدريب حول مبادئ حقوق الإنسان وممارساتها،** للسماح باستجابة مرنة وفعالة للهجمات الإلكترونية، وحماية الهياكل الأساسية الحيوية والمؤسسات العامة والشركات والمواطنين؛ **235**

(كندا)

تعدّل لتصبح كالتالي:

11. *وتوصي أيضاً* بأن تضمن جميع البرلمانات أن تتوافر لهذه المؤسسات والهيئات موارد كافية من الموازنة وموظفون متخصصون للسماح **بمنع وكشف** واستجابة مرنة وفعالة للهجمات الإلكترونية، ~~وحماية~~ **لا سيما حماية** الهياكل الأساسية الحيوية **والضعيفة (مثل أنظمة إدارة الحركة الجوية وشبكات الطاقة الكهربائية)** والمؤسسات العامة **(مثل المستشفيات والخدمات الصحية)** والشركات والمواطنين؛ **236**

(الفلبين)

تعدّل لتصبح كالتالي:

237 11. *وتوصي أيضاً* بأن تضمن جميع البرلمانات أن تتوافر لهذه المؤسسات والهيئات موارد كافية من الموازنة وموظفون متخصصون للسماح باستجابة مرنة وفعالة **للجرائم** والهجمات الإلكترونية، وحماية الهياكل الأساسية الحيوية والمؤسسات العامة والشركات والمواطنين؛

(بلجيكا)

تعدّل لتصبح كالتالي:

11. *وتوصي أيضاً* بأن تضمن جميع البرلمانات أن تتوافر لهذه المؤسسات والهيئات موارد كافية من الموازنة

238 وموظفون متخصصون للسماح باستجابة مرنة وفعالة ~~للهجمات الإلكترونية~~ **لتهديدات تكنولوجيا المعلومات والاتصالات**، وحماية الهياكل الأساسية الحيوية والمؤسسات العامة والشركات والمواطنين؛

(الجمهورية الإسلامية الإيرانية)

تعدّل لتصبح كالتالي:

11. *وتوصي أيضاً* بأن تضمن جميع البرلمانات أن تتوافر لهذه المؤسسات والهيئات موارد كافية من الموازنة وموظفون متخصصون للسماح باستجابة مرنة **وبالوقت المناسب** وفعالة للهجمات الإلكترونية، وحماية

239 الهياكل الأساسية الحيوية والمؤسسات العامة والشركات والمواطنين، **من دون انتهاك الخصوصية؛**

(تايلاند)

تعدّل لتصبح كالتالي:

11. *وتوصي أيضاً* بأن تضمن جميع البرلمانات أن تتوافر لهذه المؤسسات والهيئات موارد كافية من الموازنة وموظفون متخصصون للسماح باستجابة مرنة وفعالة للهجمات الإلكترونية، وحماية الهياكل الأساسية

240 **المدنية** الأساسية والمؤسسات العامة والشركات والمواطنين؛

(السويد)

تعدّل لتصبح كالتالي:

11. *وتوصي أيضاً* بأن تضمن جميع البرلمانات أن تتوافر لهذه المؤسسات والهيئات موارد كافية من الموازنة وموظفون متخصصون للسماح باستجابة مرنة وفعالة للهجمات الإلكترونية، وحماية الهياكل الأساسية الحيوية والمؤسسات

241 العامة والشركات والمواطنين، **مع الأخذ في الاعتبار أن الرقمنة المتزايدة للخدمات والمرافق العامة يمكن أن تنطوي على تعرض كبير للمخاطر الرقمية؛**

(الأرجنتين)

الفقرة 11 مكررة جديدة من منطوق مشروع القرار

11 مكررة. *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؛ 242

(تايلاند)

الفقرة 12 من منطوق مشروع القرار

243 تحذف الفقرة.

(بلجيكا، كندا، جمهورية مصر العربية، اليابان، روسيا الاتحادية)

تعدل لتصبح كالتالي:

244 12. *وتحث* البرلمانات على تعزيز التنسيق الدولي بين هذه المؤسسات والهيئات ~~وإنشاء مركز عالمي للعمليات الأمنية، تحت رعاية الأمم المتحدة،~~ من أجل الرصد المستمر للتهديدات الإلكترونية ومنعها وكشفها والتحقيق فيها والتصدي لها؛

(سويسرا)

تعدل لتصبح كالتالي:

245 12. *وتحث* البرلمانات على تعزيز التنسيق الدولي بين هذه المؤسسات والهيئات ~~وإنشاء مركز عالمي للعمليات الأمنية، تحت رعاية الأمم المتحدة،~~ من أجل الرصد المستمر للتهديدات الإلكترونية ومنعها وكشفها والتحقيق فيها والتصدي لها؛

(ألمانيا)

تعدل لتصبح كالتالي:

246 12. *وتحث* البرلمانات على تعزيز التنسيق الدولي بين هذه المؤسسات والهيئات وإنشاء مركز عالمي ~~للعمليات الأمنية~~ **للأمن الإلكتروني**، تحت رعاية الأمم المتحدة، من أجل الرصد المستمر للتهديدات الإلكترونية ومنعها وكشفها والتحقيق فيها والتصدي لها؛

(فرنسا)

تعدل لتصبح كالتالي:

247 12. *وتحث* البرلمانات على تعزيز التنسيق الدولي بين هذه المؤسسات والهيئات وإنشاء مركز عالمي للعمليات الأمنية، تحت رعاية الأمم المتحدة، من أجل الرصد المستمر للتهديدات الإلكترونية **العالمية** ~~منعها~~ وكشفها والتحقيق فيها والتصدي لها **بالتعاون مع فرق الدول الأعضاء للاستجابة إلى الحوادث الإلكترونية الوطنية من أجل دعم منع هذه التهديدات؛**

(تركيا)

تعدل لتصبح كالتالي:

12. *وتحث* البرلمانات على تعزيز التنسيق الدولي بين هذه المؤسسات والهيئات وإنشاء مركز عالمي للعمليات الأمنية، تحت رعاية الأمم المتحدة، من أجل الرصد المستمر لتهديدات ~~الإلكترونية~~ **تكنولوجيا الاتصالات والمعلومات** ومنعها وكشفها والتحقيق فيها والتصدي لها؛ 248

(الجمهورية الإسلامية الإيرانية)

تعدل لتصبح كالتالي:

12. *وتحث* البرلمانات على تعزيز التنسيق الدولي بين هذه المؤسسات والهيئات وإنشاء مركز عالمي للعمليات الأمنية، تحت رعاية الأمم المتحدة، من أجل الرصد المستمر للتهديدات الإلكترونية ومنعها وكشفها والتحقيق فيها والتصدي لها، **مع تحديد نطاق ولايته بوضوح في ما يتعلق بهيئات الأمم المتحدة الأخرى ذات الصلة، مثل مجلس الرؤساء التنفيذيين في الأمم المتحدة، من خلال اللجنة الرفيعة المستوى المعنية بالبرامج وإطار عمل الأمم المتحدة بشأن الأمن الإلكتروني والجريمة الإلكترونية؛** 249

(السويد)

الفقرة 12 مكررة جديدة من منطوق مشروع القرار

12 مكررة. ***وتدعو*** **الحكومات والمجتمع الدولي إلى التعاون بشأن سبل كشف الجهات الفاعلة والكيانات التي تقف وراء هذه الهجمات الإلكترونية وجعلها مسؤولة عن أفعالها من خلال رفع الدعاوى الجنائية وفرض العقوبات السارية؛** 250

(الفلبين)

الفقرة 13 من منطوق مشروع القرار

تحذف الفقرة. 251

(بلجيكا، كندا، جمهورية مصر العربية، ألمانيا، روسيا الاتحادية، سويسرا)

تعدل لتصبح كالتالي:

13. *وتوصي* بأن ~~يدعم هذا الكيان~~ يتم **توفير المساعدة التقنية وبناء القدرات إلى** جميع الدول، ولا سيما الدول التي لديها موارد أقل، في تطوير قدرات العمل والاستجابة، وفي تبادل المعلومات والمعارف والبحوث تحسباً

252 للتحديات المستقبلية المتصلة ~~بالتكنولوجيا، مثل الحوسبة الكمومية، والجيل الخامس (5G)، وميتفارس (metaverse)، والذكاء الاصطناعي~~ **بالتقنيات**، ~~وفي إثارة ناقوس الخطر~~ **والتنبيه في أي ظرف من الظروف، إلى** انتهاك الإعلان العالمي لحقوق الإنسان ~~في أي ظرف من الظروف~~

(جمهورية التشيك)

تعدل لتصبح كالتالي:

13. *وتوصي* بأن يدعم هذا الكيان ~~جميع~~ الدول، ولا سيما الدول التي لديها موارد أقل، في تطوير قدرات العمل والاستجابة، وفي تبادل المعلومات والمعارف والبحوث تحسباً للتحديات المستقبلية المتصلة بالتكنولوجيا، مثل الحوسبة الكمومية، والجيل الخامس (5G)، وميتفارس (metaverse)، والذكاء 253 الاصطناعي، وفي إثارة ناقوس الخطر في حال انتهاك الإعلان العالمي لحقوق الإنسان في أي ظرف من الظروف؛

(جمهورية كوريا)

تعدل لتصبح كالتالي:

13. *وتوصي* بأن يدعم هذا الكيان جميع الدول، ولا سيما الدول ~~التي لديها موارد أقل~~ **النامية**، في تطوير قدرات العمل والاستجابة، وفي تبادل المعلومات والمعارف والبحوث تحسباً للتحديات 254 المستقبلية المتصلة بالتكنولوجيا، مثل الحوسبة الكمومية، والجيل الخامس (5G)، وميتفارس (metaverse)، والذكاء الاصطناعي، وفي إثارة ناقوس الخطر في حال انتهاك الإعلان العالمي لحقوق الإنسان في أي ظرف من الظروف؛

(الجمهورية الإسلامية الإيرانية)

تعدل لتصبح كالتالي:

13. *وتوصي* بأن يدعم هذا الكيان جميع الدول، ولا سيما الدول التي لديها موارد أقل، في تطوير قدرات 255 العمل والاستجابة، وفي تبادل المعلومات والمعارف والبحوث تحسباً للتحديات المستقبلية المتصلة بالتكنولوجيا، مثل الحوسبة الكمومية، والجيل الخامس (5G)، وميتفارس (metaverse)، والذكاء الاصطناعي، ~~وفي إثارة ناقوس الخطر في حال انتهاك الإعلان العالمي لحقوق الإنسان في أي ظرف من الظروف؛~~

(الهند)

تعدل لتصبح كالتالي:

13. *وتوصي* بأن يدعم هذا الكيان جميع الدول، ولا سيما الدول التي لديها موارد أقل، في تطوير قدرات العمل والاستجابة، وفي تبادل المعلومات والمعارف والبحوث تحسباً للتحديات المستقبلية المتصلة بالتكنولوجيا، مثل الحوسبة الكمومية، والجيل الخامس (5G)، وميتفارس (metaverse)، والذكاء الاصطناعي، وفي ~~إثارة ناقوس الخطر في حال انتهاك الإعلان العالمي لحقوق الإنسان في أي ظرف من الظروف~~ **زيادة قدرتها على الصمود في وجه التهديدات الإلكترونية؛**

256

(فرنسا)

تعدل لتصبح كالتالي:

13. *وتوصي* بأن يدعم هذا الكيان جميع الدول، ولا سيما الدول التي لديها موارد أقل، في تطوير قدرات العمل والاستجابة، وفي تبادل المعلومات والمعارف والبحوث تحسباً للتحديات المستقبلية المتصلة بالتكنولوجيا، مثل الحوسبة الكمومية، والجيل الخامس (5G)، وميتفارس (metaverse)، والذكاء الاصطناعي، وفي إثارة ناقوس الخطر في حال ~~انتهاك الإعلان العالمي لحقوق الإنسان في أي ظرف من الظروف~~ **تنجم انتهاكات حقوق الإنسان المعترف بها عالمياً عن التطورات في منطقة مسؤوليتها؛**

257

(أوكرانيا)

تعدل لتصبح كالتالي:

13. *وتوصي* بأن يدعم هذا الكيان جميع الدول، ولا سيما الدول التي لديها موارد أقل، في تطوير قدرات العمل والاستجابة، وفي تبادل المعلومات والمعارف والبحوث تحسباً للتحديات المستقبلية المتصلة بالتكنولوجيا، مثل الحوسبة الكمومية، والجيل الخامس (5G)، وميتفارس (metaverse)، والذكاء الاصطناعي، وفي إثارة ناقوس الخطر في حال انتهاك الإعلان العالمي لحقوق الإنسان **أو صكوك أخرى لحقوق الإنسان** في أي ظرف من الظروف؛

258

(السويد)

الفقرة 13 مكررة جديدة من منطوق مشروع القرار

259 **13 مكررة.** ***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؛**

(ألمانيا)

الفقرة 14 من منطوق مشروع القرار

260 تحذف الفقرة.

(الهند)

تعدل لتصبح كالتالي:

14. *وتطلب من* البرلمانات أن تشجع الاستثمار في البحث والتطوير، وأن تدرج في تصميم كل مشروع اعتمادات خاصة ~~بالأمن الإلكتروني~~ **بأمن تكنولوجيا المعلومات والاتصالات،** مع تخصيص اعتمادات 261 مناسبة في الموازنة، من أجل التنبؤ بتهديدات ~~الحاسوبية~~ **تكنولوجيا المعلومات والاتصالات** الناشئة المحتملة والحماية منها؛

(الجمهورية الإسلامية الإيرانية)

الفقرة 15 من منطوق مشروع القرار

262 تحذف الفقرة.

(الهند)

تعدل لتصبح كالتالي:

15. *وتشجع* البرلمانات على إقامة شراكات مع دوائر الصناعة والأوساط الأكاديمية وجميع الجهات المعنية 263 الأخرى، بما في ذلك المجتمع المدني، من أجل تعزيز نظام قوي وتعاوني ~~للأمن الإلكتروني~~ **لأمن تكنولوجيا المعلومات والاتصالات؛**

(الجمهورية الإسلامية الإيرانية)

تعدل لتصبح كالتالي:

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؛ **264**

(تايلاند)

تعدل لتصبح كالتالي:

15. *وتشجع* البرلمانات على إقامة شراكات مع دوائر الصناعة والأوساط الأكاديمية وجميع الجهات المعنية الأخرى، بما في ذلك المجتمع المدني، من أجل تعزيز نظام قوي وتعاوني للأمن الإلكتروني **يحترم مبادئ حقوق الإنسان والالتزامات الدولية لحقوق الإنسان احتراماً كاملاً**؛ **265**

(كندا)

تعدل لتصبح كالتالي:

15. *وتشجع* البرلمانات على إقامة شراكات مع دوائر الصناعة والأوساط الأكاديمية وجميع الجهات المعنية الأخرى، بما في ذلك المجتمع المدني، من أجل تعزيز نظام قوي وتعاوني للأمن الإلكتروني **من دون المساس بإنشاء الأنظمة التي تضمن قيام مزودي خدمة الإنترنت والتطبيقات بتسليم المعلومات على وجه السرعة عن الآثار والإشارات التي تطلبها المحاكم القضائية في مختلف البلدان، إلى الحد الذي قد تشكل فيه هذه المعلومات دليلاً رقمياً للتحقيق في الجرائم الإلكترونية على المستوى المحلي بغض النظر عن مقرها الإقليمي أو قواعد الخصوصية في البلد الذي يتم فيه تخزين هذه المعلومات**؛ **266**

(الأرجنتين)

الفقرة 16 من منطوق مشروع القرار

تحذف الفقرة. **267**

(بلجيكا، كندا)

تعدل لتصبح كالتالي:

16. *وتشجع أيضاً* البرلمانات على تطوير ~~مجالات تشريعية~~ **الثقة بحيث** يمكن فيها للبرلمانات والحكومات والشركات والأوساط الأكاديمية والمجتمع المدني أن تتعاون في الوقت الحقيقي من أجل الدفاع عن المصالح العامة لجميع الدول؛ **268**

(الهند)

16. *وتشجع أيضاً* البرلمانات على تطوير مجالات تشريعية يمكن فيها للبرلمانات والحكومات والشركات والأوساط الأكاديمية والمجتمع المدني أن تتعاون في الوقت الحقيقي، **وفقاً لسيادة القانون والاحترام الكامل للقانون الدولي لحقوق الإنسان والحريات الأساسية،** من أجل الدفاع عن المصالح العامة لجميع الدول؛ **269**

(ألمانيا)

الفقرة 16 مكررة جديدة من منطوق مشروع القرار **270**

16 مكررة. *وتدعو* البرلمانات وحكوماتها إلى معالجة نقص مسؤولية مقدمي الخدمات والمنصات عبر الوطنية، الأمر الذي يشكل تهديداً خطيراً في بيئة تكنولوجيا المعلومات والاتصالات؛

(الجمهورية الإسلامية الإيرانية)

الفقرة 17 من منطوق مشروع القرار

تعدل لتصبح كالتالي: **271**

17. *وتطلب* من البرلمانات والبرلمانيين أن يشاركوا بنشاط في الترويج لفهم وطني مشترك ومستكمل لطبيعة ~~الجرائم والهجمات الإلكترونية~~ **استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية وتهديدات تكنولوجيا المعلومات والاتصالات** على نحو ما يعانيه المواطنون والمنظمات والمؤسسات؛

(الجمهورية الإسلامية الإيرانية)

تعدل لتصبح كالتالي:

272 17. *وتطلب* من البرلمانات والبرلمانيين أن يشاركوا بنشاط في الترويج لفهم وطني مشترك ومستكمل لطبيعة ~~الجرائم~~ **إساءة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية** والهجمات الإلكترونية على نحو ما يعانيه المواطنون والمنظمات والمؤسسات؛

(باكستان)

تعدل لتصبح كالتالي:

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

(بلجيكا، جمهورية التشيك، السويد)

تعدل لتصبح كالتالي:

274 17. *وتطلب* من البرلمانات والبرلمانيين أن يشاركوا بنشاط في الترويج لفهم وطني مشترك ومستكمل لطبيعة الجرائم والهجمات الإلكترونية على نحو ما يعانيه المواطنون والمنظمات والمؤسسات، **حيث لا ترد بعد في بلدانهم؛**

(نيكاراغوا)

الفقرة 18 من منطوق مشروع القرار

275 تحذف الفقرة.

(الهند)

تعدل لتصبح كالتالي:

18. *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 ~~الاستخدام~~ 276 ~~الصحيح~~ **محو الأمية الرقمية والدراية** ~~للأجهزة~~ التكنولوجية، تغطي كلا من الفرص الكبيرة التي تتيحها والمخاطر الجسيمة التي تشكلها؛

(تايلاند)

الفقرة 18 مكررة جديدة من منطوق مشروع القرار

277 **18 مكررة. *وتحث* البرلمانات أيضاً، في جميع أنشطتها المتعلقة بمكافحة الجرائم الإلكترونية والحوادث الإلكترونية الخبيثة، على تعزيز الالتزامات بموجب القانون الدولي لحقوق الإنسان**

والاحترام الكامل لحقوق الإنسان والحريات الأساسية وسيادة القانون؛

(كندا)

الفقرة 19 من منطوق مشروع القرار

تحذف الفقرة.

278

(الجمهورية الإسلامية الإيرانية)

تعدل لتصبح كالتالي:

19. *وتوصي* بأن توسع البرلمانات نطاق الحماية المتاحة ~~للنساء والشباب وغيرهم من~~ للفئات الضعيفة **لا سيما الأطفال، وكبار السن،** في الفضاء الإلكتروني، مع مراعاة احترام حقوق الإنسان ومنع العنف القائم على الجندر عند وضع السياسات التعليمية المتعلقة باستخدام وسائل التواصل الاجتماعي؛ **279**

(ألمانيا)

تعدل لتصبح كالتالي:

280

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

(جمهورية التشيك)

تعدل لتصبح كالتالي:

19. *وتوصي* بأن توسع البرلمانات نطاق الحماية المتاحة للنساء والشباب **وكبار السن والأطفال** 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؛ **281**

(فيتنام)

تعدل لتصبح كالتالي:

19. *وتوصي* بأن توسع البرلمانات نطاق الحماية المتاحة للنساء **والأطفال** والشباب 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؛ **282**

(رومانيا)

تعدل لتصبح كالتالي:

19. *وتوصي* بأن توسع البرلمانات نطاق الحماية المتاحة للنساء والشباب **وكبار السن** 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؛ **283**

(تركيا)

تعدل لتصبح كالتالي:

19. *وتوصي* بأن توسع البرلمانات نطاق الحماية المتاحة للنساء والشباب **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؛ **284**

(كندا)

تعدل لتصبح كالتالي:

19. *وتوصي* بأن توسع البرلمانات نطاق الحماية المتاحة للنساء والشباب **والأشخاص ذوي الإعاقة** 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؛ **285**

(فنلندا)

الفقرة 19 مكررة جديدة من منطوق مشروع القرار

19 مكررة. ***وتدعو*** **البرلمانات إلى عقد تعاون بين الجهات المعنية المتعددة بين الحكومة والقطاع الخاص من أجل إضفاء الطابع المؤسسي على التكنولوجيا كأداة لزيادة الوعي بشأن التحرش 286 الجنسي ومكافحة العنف الإلكتروني ضد النساء والأطفال؛**

(الفلبين)

الفقرة 20 من منطوق مشروع القرار

287

تحذف الفقرة.

(الهند)

تعدل لتصبح كالتالي:

20. *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~~ **288** ~~التي تسعى إلى التأثير في حرية تشكيل الرأي العام أو تغييره أو انتهاكه أثناء العملية الانتخابية~~ **لمنع التدخل في الشؤون الداخلية للدولة من خلال استخدام تكنولوجيا المعلومات والاتصالات؛**

(روسيا الاتحادية)

الفقرة 21 من منطوق مشروع القرار

289

تحذف الفقرة.

(الجمهورية الإسلامية الإيرانية)

تعدل لتصبح كالتالي:

21. *وتطلب من* المجتمع الدولي أن يتخذ إجراءات لحماية ~~الديمقراطية~~ **نظم تكنولوجيا المعلومات والاتصالات للسلطات الحكومية** من خلال ضمان توفير حماية خاصة لجميع البرلمانات في جميع أنحاء العالم، بوصفها **290** مؤسسات تمثل إرادة الشعب، من خلال إدراجها في قوائم الهياكل الأساسية الوطنية الأساسية، والخدمات الأساسية؛

(روسيا الاتحادية)

تعدل لتصبح كالتالي:

21. *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 ~~الوطنية~~ **المدنية** الأساسية، والخدمات الأساسية؛ **291**

(السويد)

الفقرة 21 مكررة جديدة من منطوق مشروع القرار **292**

21 مكررة. *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؛

(رومانيا)

الفقرة 22 من منطوق مشروع القرار

تعدل لتصبح كالتالي: **293**

22. *وتطلب من* البرلمانات أن تعمق فهمها للطابع المعقد والسريع ~~للجرائم والهجمات الإلكترونية~~ **لاستخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية وتهديدات تكنولوجيا المعلومات والاتصالات** من خلال عقد ندوات وورشات عمل ومؤتمرات متخصصة بشأن هذا الموضوع؛

(الجمهورية الإسلامية الإيرانية)

22. *وتطلب من* البرلمانات أن تعمق فهمها للطابع المعقد والسريع للجرائم ~~والهجمات~~ **والحوادث** الإلكترونية من خلال عقد ندوات وورشات عمل ومؤتمرات متخصصة بشأن هذا الموضوع؛ **294**

(الهند)

22. *وتطلب من* البرلمانات أن تعمق فهمها للطابع المعقد والسريع ~~للجرائم~~ **لإساءة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية** والهجمات الإلكترونية من خلال عقد ندوات وورشات عمل ومؤتمرات متخصصة بشأن هذا الموضوع؛ **295**

(باكستان)

296 22. *وتطلب من* البرلمانات أن تعمق فهمها للطابع المعقد ~~والسريع~~ **وسريع التطور** للجرائم ~~والهجمات~~ الإلكترونية من خلال عقد ندوات وورشات عمل ومؤتمرات متخصصة بشأن هذا الموضوع؛

(السويد)

297 22. *وتطلب من* البرلمانات أن تعمق فهمها للطابع المعقد والسريع للجرائم والهجمات الإلكترونية من خلال **تمكين التبادل المفتوح للمعرفة والخبرة والتجربة عبر** عقد ندوات وورشات عمل ومؤتمرات متخصصة بشأن هذا الموضوع؛

(جنوب إفريقيا)

298 22. *وتطلب من* البرلمانات أن تعمق فهمها للطابع المعقد والسريع للجرائم والهجمات الإلكترونية من خلال عقد ندوات وورشات عمل ومؤتمرات متخصصة بشأن هذا الموضوع **حيث لا ترد بعد في بلدانهم؛**

(نيكاراغوا)

299 الفقرة 23 من منطوق مشروع القرار

تحذف الفقرة.

(روسيا الاتحادية)

تعدل لتصبح كالتالي:

300 23. *وتدعو* ~~الأمانة العامة~~ الاتحاد 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؛

(بلجيكا)

تعدل لتصبح كالتالي:

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

(الجمهورية الإسلامية الإيرانية)

تعدل لتصبح كالتالي:

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 **وتحديد هدفها الاستراتيجي في تشجيع البرلمانات على إنشاء مراكز استخبارات للأمن الإلكتروني داخلية لمشاركة وتبادل معلوماتها وذكائها وخبراتها وأفضل ممارساتها، بهدف توسيع المعرفة المشتركة بالأمن الإلكتروني؛**

302

(تايلاند)

303

الفقرة 24 من منطوق مشروع القرار

تعدل لتصبح كالتالي:

24. *وتوصي* بأن يقوم الاتحاد البرلماني الدولي~~، بوصفه المنظمة العالمية للبرلمانات، الاضطلاع بدور قيادي في حوكمة الإنترنت على الصعيد الدولي والمرونة الإلكترونية من خلال المشاركة في جميع المحافل الدولية ذات الصلة، بما في ذلك تلك التي تقودها الأمم المتحدة، بغية ضمان سماع صوت البرلمانات، من أجل توقع أي تهديد إلكتروني لأمن الناس أو سبل عيشهم أو أسلوب حياتهم والاستعداد له ومقاومته والاستجابة له والتعافي منه~~ **بالمساهمة في إضفاء طابع دولي على إدارة الإنترنت، والمشاركة المتساوية لجميع الدول في هذه العملية، والحفاظ على الحق السيادي للدول في تنظيم الجزء الوطني من شبكة الإنترنت العالمية.**

(روسيا الاتحادية)

تعدل لتصبح كالتالي:

24. *وتوصي* بأن يقوم الاتحاد البرلماني الدولي، بوصفه المنظمة العالمية للبرلمانات، الاضطلاع بدور قيادي في ~~حوكمة الإنترنت على الصعيد الدولي~~ **منع الجرائم الإلكترونية ومكافحتها وتحفيز** المرونة الإلكترونية من خلال المشاركة في جميع المحافل الدولية ذات الصلة، بما في ذلك تلك التي تقودها الأمم المتحدة، بغية ضمان سماع صوت البرلمانات، من أجل توقع أي تهديد إلكتروني لأمن الناس أو سبل عيشهم **أو حقوق الإنسان** أو أسلوب حياتهم والاستعداد له ومقاومته والاستجابة له والتعافي منه.

304

(بلجيكا)

تعدل لتصبح كالتالي:

24. *وتوصي* بأن يقوم الاتحاد البرلماني الدولي، بوصفه المنظمة العالمية للبرلمانات، الاضطلاع بدور قيادي في حوكمة الإنترنت على الصعيد الدولي والمرونة الإلكترونية من خلال ~~المشاركة في جميع~~ **تعزيز الشراكات مع** المحافل الدولية ذات الصلة، بما في ذلك تلك التي تقودها الأمم المتحدة، بغية ضمان سماع صوت البرلمانات، من أجل توقع أي تهديد إلكتروني لأمن الناس أو سبل عيشهم أو أسلوب حياتهم والاستعداد له ومقاومته والاستجابة له والتعافي منه.

305

(جمهورية كوريا)

تعدل لتصبح كالتالي:

24. *وتوصي* بأن يقوم الاتحاد البرلماني الدولي، بوصفه المنظمة العالمية للبرلمانات، الاضطلاع بدور قيادي في حوكمة الإنترنت على الصعيد الدولي والمرونة الإلكترونية من خلال المشاركة في جميع المحافل الدولية ذات الصلة، بما في ذلك تلك التي تقودها الأمم المتحدة، ~~بغية ضمان سماع صوت البرلمانات، من أجل توقع أي تهديد إلكتروني لأمن الناس أو سبل عيشهم أو أسلوب حياتهم والاستعداد له ومقاومته والاستجابة له والتعافي منه.~~

306

(فرنسا)

تعدل لتصبح كالتالي:

24. *وتوصي* بأن يقوم الاتحاد البرلماني الدولي، بوصفه المنظمة العالمية للبرلمانات، الاضطلاع بدور قيادي في حوكمة الإنترنت على الصعيد الدولي والمرونة الإلكترونية من خلال المشاركة في جميع المحافل الدولية ذات الصلة، بما في ذلك تلك التي تقودها الأمم المتحدة، بغية ضمان سماع صوت البرلمانات، من أجل توقع أي تهديد ~~إلكتروني~~ **من تكنولوجيا المعلومات والاتصالات** لأمن الناس أو سبل عيشهم أو أسلوب حياتهم والاستعداد له ومقاومته والاستجابة له والتعافي منه.

307

(الجمهورية الإسلامية الإيرانية)

تعدل لتصبح كالتالي:

24. *وتوصي* بأن يقوم الاتحاد البرلماني الدولي، بوصفه المنظمة العالمية للبرلمانات، الاضطلاع بدور قيادي في حوكمة الإنترنت على الصعيد الدولي والمرونة الإلكترونية من خلال المشاركة في جميع

المحافل الدولية ذات الصلة، بما في ذلك تلك التي تقودها الأمم المتحدة، بغية ضمان سماع صوت البرلمانات، من أجل توقع أي تهديد إلكتروني لأمن الناس أو سبل عيشهم أو أسلوب حياتهم والاستعداد له ومقاومته والاستجابة له والتعافي منه، **بعد التشاور مع الدول الأطراف.** 308

(نيكاراغوا)

الفقرة 24 مكررة جديدة من منطوق مشروع القرار

24 مكررة. ***وتشجع على*** **إنشاء مجموعة عمل معنية بالهجمات والجرائم الإلكترونية، تحت إشراف مجلس 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 الوطنية الأعضاء في الاتحاد البرلماني الدولي من حيث سن القوانين والرقابة وإعداد الموازنة؛** 309

(الأرجنتين)

24 مكررة. ***وتوصي*** **أيضاً بأن يعمل الاتحاد البرلماني الدولي على زيادة الوعي بين البرلمانات بشأن تحقيق أهداف التنمية المستدامة من خلال، قبل كل شيء، التزاماتها العالمية بالأمن الرقمي؛** 310

(تايلاند)

الفقرة 24 مكررة ثانياً جديدة من منطوق مشروع القرار

24 مكررة ثانياً. ***وتحث*** **المنظمات الدولية على مناقشة اتفاقية بشأن أعمال الحرب الإلكترونية في إطار الحفاظ على السلم والأمن الدوليين.** 311

(الأرجنتين)

العنوان

تعديل العنوان على النحو التالي:

~~الهجمات والجرائم الإلكترونية~~ **الجرائم الإلكترونية:** المخاطر الجديدة على الأمن العالمي 312

(جمهورية التشيك)

313 تعديل العنوان على النحو التالي:

~~الهجمات والجرائم الإلكترونية~~ **الجرائم والحوادث الإلكترونية**: المخاطر الجديدة على الأمن العالمي

(الهند)

تعديل العنوان على النحو التالي:

314 ~~الهجمات والجرائم الإلكترونية~~ **تهديدات تكنولوجيا المعلومات والاتصالات واستخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية**: المخاطر الجديدة على الأمن العالمي

(الجمهورية الإسلامية الإيرانية)

تعديل العنوان على النحو التالي:

315 الهجمات والجرائم الإلكترونية: المخاطر ~~الجديدة~~ **المتزايدة** على الأمن العالمي

(ليتوانيا)

تعديل العنوان على النحو التالي:

316 الهجمات ~~والجرائم~~ الإلكترونية **وإساءة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية**: المخاطر الجديدة على الأمن العالمي

(باكستان)

317 تعديل العنوان على النحو التالي:

~~الهجمات~~ والجرائم الإلكترونية: المخاطر ~~الجديدة~~ **المتطورة** على الأمن العالمي

(السويد)

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)

Standing Committee on
Peace and International Security

C-I/146/DR-am
6 March 2023

Cyberattacks and cybercrimes: The new risks to global security

<u>Amendments to the draft resolution</u> submitted within the statutory deadline by Argentina, Belgium, Canada, Czech Republic, Egypt, Finland, France, Germany, India, Iran (Islamic Republic of), Japan, Lithuania, Nicaragua, Pakistan, Philippines, Republic of Korea, Romania, Russian Federation, Singapore, South Africa, South Sudan, Sweden, Switzerland, Thailand, Türkiye, Ukraine and Viet Nam

PREAMBULAR

<u>Preambular paragraph 1</u>

Amend to read as follows:

(1) *Condemning* all forms of ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** and cyberattacks**,** and *reaffirming* the need to combat such acts through international cooperation and the development of effective**,** ~~legal~~ **international, legally binding** frameworks **tailored to the unique attributes of information and communications technologies (ICTs)**, **1**

(Islamic Republic of Iran)

Amend to read as follows:

(1) *Condemning* all forms of ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks and *reaffirming* the need to combat such acts through international cooperation and the development of effective legal frameworks, **2**

(Pakistan)

E

#IPU146

Amend to read as follows:

(1) *Condemning* all forms of **the use of information and communications technologies for criminal purposes, hereinafter referred to as "**cybercrime**",** and **computer attacks, hereinafter referred to as "**cyberattacks**",** and *reaffirming* the need to combat such acts through international cooperation and the development of effective legal frameworks, **3**

(Russian Federation)

Amend to read as follows:

(1) *Condemning* all forms of cybercrime ~~and cyberattacks~~ and *reaffirming* the need to combat such acts through international cooperation and the development of effective legal frameworks, **4**

(Czech Republic, Sweden)

Amend to read as follows:

(1) *Condemning* all forms of cybercrime and ~~cyberattacks~~ **cyber incidents** and *reaffirming* the need to combat such acts through international cooperation and the development of effective legal frameworks, **5**

(India)

Amend to read as follows:

(1) *Condemning* all forms of cybercrime and **malicious** cyberattacks and *reaffirming* the need to combat such ~~acts~~ **crimes** through international cooperation and the development of effective legal frameworks, **6**

(Belgium)

Amend to read as follows:

(1) *Condemning* all forms of cybercrime and cyberattacks ~~and *reaffirming* the need to combat such acts through international cooperation and the development of effective legal frameworks~~ **together with all heinous crimes associated with them**, **7**

(South Sudan)

Amend to read as follows:

(1) *Condemning* all forms of cybercrime and cyberattacks and *reaffirming* the need to combat such acts through international cooperation ~~and the development of effective legal frameworks~~, **8**

(Germany)

Amend to read as follows:

(1) *Condemning* all forms of cybercrime and cyberattacks and *reaffirming* the need to combat such acts through international cooperation and ~~the development of~~ effective legal ~~frameworks~~ **discussions**, **9**

(Japan)

Amend to read as follows:

(1) *Condemning* all forms of cybercrime and cyberattacks and *reaffirming* the need to combat such acts through international cooperation **and coordination among stakeholders both within and between countries**, **including the sharing of information on cybercrime threats,** and the development of effective legal frameworks, **10**

(South Africa)

Amend to read as follows:

(1) *Condemning* all forms of cybercrime and cyberattacks and *reaffirming* the need to combat such acts through international cooperation and the **application or, where necessary,** development of effective legal frameworks, **11**

(Switzerland)

Amend to read as follows:

(1) *Condemning* all forms of cybercrime and cyberattacks and *reaffirming* the need to combat such acts through international cooperation and the development of effective legal frameworks **that reflect the rules-based international system**, **12**

(Canada)

New preambular paragraph 1bis

(1bis) *Acknowledging* that cybercrime and cyberattacks are distinct yet interrelated phenomena of a criminal nature in the digital era, associated with different scopes of malicious uses of information and communications technologies, **13**

(Argentina)

(1bis) *Reaffirming* the existing United Nations framework for responsible State behaviour in the use of ICTs and the need to implement this framework, **14**

(Germany)

(1bis) *Affirming* the need to combat such acts through national, regional and international cooperation and the development of effective legal frameworks, **15**

(South Sudan)

Preambular paragraph 2

Amend to read as follows:

(2) *Recognizing* the need to build trust between countries ~~in response to cybercriminals, who recognize neither boundaries nor borders~~ **to address risks to cybersecurity**, **16**

(India)

Amend to read as follows:

(2) *Recognizing* the need to build trust between countries in response to ~~cybercriminals~~ **the malicious use of ICTs by State as well as non-State actors**, who recognize neither boundaries nor borders, **17**

(Germany)

Amend to read as follows:

(2) *Recognizing* the need to build trust between countries in response to cybercriminals **and malicious actors**, who recognize neither boundaries nor borders, **18**

(Islamic Republic of Iran)

Amend to read as follows:

(2) *Recognizing* the need to build trust **and mutual understanding** between countries in response to cybercriminals, who recognize neither boundaries nor borders, **19**

(Thailand)

Preambular paragraph 3

Amend to read as follows:

(3) *Observing* the growing **use of and** dependence on ~~cyberspace among individuals, institutions and States~~ **ICTs worldwide**, **20**

(Germany)

Amend to read as follows:

(3) *Observing* the growing dependence on ~~cyberspace~~ **the ICT environment** among individuals, institutions and States, **21**

(Islamic Republic of Iran)

Amend to read as follows:

(3) *Observing* the growing dependence on **the space in which information and communications technologies are used, hereinafter referred to as "**cyberspace**",** among individuals, institutions and States, **22**

(Russian Federation)

Preambular paragraph 4

Amend to read as follows:

(4) *Cognizant of* the increase in ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** and ~~cyberattacks~~ **ICT threat** due to increasing digitalization, especially the forced digitalization imposed by the COVID-19 pandemic, **23**

(Islamic Republic of Iran)

Amend to read as follows:

(4) *Cognizant of* the increase in ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks due to increasing digitalization, especially the forced digitalization imposed by the COVID-19 pandemic, **24**

(Pakistan)

Amend to read as follows:

(4) *Cognizant of* the increase in cybercrime ~~and cyberattacks~~ due to increasing digitalization~~, especially the forced digitalization imposed by~~ **during and following** the COVID-19 pandemic, **25**

(Czech Republic)

Amend to read as follows:

(4) *Cognizant of* the increase in cybercrime and ~~cyberattacks~~ **its increasing application in cyberwarfare operations, such as decoy ransomware leveraged for destructive cyberattacks on critical civilian infrastructure,** due to increasing digitalization, especially the forced digitalization imposed by the COVID-19 pandemic, **26**

(Sweden)

Amend to read as follows:

(4) *Cognizant of* the increase in cybercrime and ~~cyberattacks~~ **cyber incidents** due to increasing digitalization, especially ~~the forced digitalization imposed by~~ **since the onset of** the COVID-19 pandemic, **27**

(India)

Amend to read as follows:

(4) *Cognizant of* the increase in cybercrime **activities** and cyberattacks due to increasing digitalization, ~~especially the forced digitalization imposed~~ **accelerated** by the COVID-19 pandemic, **28**

(Germany)

Amend to read as follows:

(4) *Cognizant of* the increase in cybercrime and **malicious** cyberattacks due to increasing digitalization, especially the ~~forced~~ digitalization imposed by the COVID-19 pandemic, **29**

(Belgium)

Amend to read as follows:

(4) *Cognizant of* the increase in cybercrime and cyberattacks due to increasing digitalization, especially the ~~forced~~ digitalization imposed by the COVID-19 pandemic, **30**

(Lithuania)

Amend to read as follows:

(4) *Cognizant of* the increase in cybercrime and cyberattacks **on the critical infrastructure of States and of enterprises supporting essential services to the public, as well as on the well-being of individuals,** due to increasing digitalization, especially the forced digitalization imposed by the COVID-19 pandemic, **31**

(South Africa)

New preambular paragraph 4bis

(4bis) *Also cognizant* of the challenges faced by States in combating cyberattacks and cybercrime, and *emphasizing* the need to reinforce technical assistance and capacity-building activities, upon request, to strengthen the ability of national authorities to deal with cyberattacks and cybercrime, **32**

(South Africa)

Preambular paragraph 5

Amend to read as follows:

(5) *Noting* the responsibility of parliaments to protect citizens in ~~cyberspace~~ **the ICT environment** with new infrastructure and resources, in the same way as in the physical world, **33**

(Islamic Republic of Iran)

Amend to read as follows:

(5) *Noting* the responsibility of parliaments to protect citizens in cyberspace ~~with new infrastructure and resources,~~ in the same way as in the physical world, **34**

(India)

Amend to read as follows:

(5) *Noting* the responsibility of parliaments to ~~protect~~ **build a regulatory framework that protects** citizens in cyberspace with new infrastructure and resources, in the same way as in the physical world, **35**

(Argentina)

Amend to read as follows:

(5) *Noting* the responsibility of parliaments to ~~protect~~ **ensure the protection of their** citizens in cyberspace with new infrastructure and resources, in the same way as in the physical world, **36**

(Thailand)

Amend to read as follows:

(5) *Noting* the ~~responsibility~~ **role** of parliaments to protect citizens in cyberspace with new infrastructure and resources, in the same way as in the physical world, **37**

(Lithuania)

Amend to read as follows:

(5) *Noting* the responsibility of parliaments to protect citizens in cyberspace with new infrastructure and resources, in the same way as in the physical world, **where they do not yet exist in their country**, **38**

(Nicaragua)

New preambular paragraph 5bis

(5bis) *Recognizing* that, in light of the pace of global technological developments, new policy and legal frameworks must likewise be swiftly and comprehensively developed, **39**

(Philippines)

(5bis) *Reaffirming* that the United Nations has a leading role in facilitating dialogue on the use of information and communications technologies by States, pursuant to United Nations General Assembly resolution 76/19, **40**

(Russian Federation)

(5bis) *Emphasizing* the dependence on digital technology platforms and infrastructure, along with the risk of cyberattacks, when governments deploy online public service applications, **41**

(Viet Nam)

New preambular paragraph 5ter

(5ter) *Supporting* the Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025, and *recognizing* its mandate pursuant to United Nations General Assembly resolution 75/240, **42**

(Russian Federation)

(5ter) *Affirming* the view that the protection of human rights in the cyber world is similar to in the real one, in line with the international commitments of United Nations Member States, **43**

(Viet Nam)

Preambular paragraph 6

Amend to read as follows:

(6) *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*, ~~resolution 57/239 of 31 January 2003 on the *Creation of a global culture of cybersecurity*, and resolution~~ **resolutions** 69/28 of 2 December 2014**, 70/237 of 23 December 2015, 71/28 of 5 December 2016, 73/27 of 5 December 2018, 74/29 of 12 December 2019, 75/240 of 31 December 2020 and 77/36 of 7 December 2022** on *Developments in the field of information and telecommunications in the context of international security*, **and resolution 76/19 of 6 December 2021 *on Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies,** **44**

(Russian Federation)

Amend to read as follows:

(6) *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*, resolution 57/239 of 31 January 2003 on the *Creation of a global culture of cybersecurity*, ~~and~~ resolution ~~69/28 of 2 December 2014 on *Developments in the field of information and telecommunications in the context of international security*~~ **76/19 of 6 December 2021 on *Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies*, resolution 77/36 of 7 December 2022 on *Developments in the field of information and telecommunications in the context of international security*, and resolution 77/37 of 7 December 2022 on a *Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security***, **45**

(Egypt)

Amend to read as follows:

(6) *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*, resolution 57/239 of 31 January 2003 on the *Creation of a global culture of cybersecurity*, and ~~resolution~~ **resolutions** 69/28 of 2 December 2014, **73/27 of 5 December 2018, 75/240 of 31 December 2020 and 77/36 of 7 December 2022** on *Developments in the field of information and telecommunications in the context of international security*, **46**

(Islamic Republic of Iran)

Amend to read as follows:

(6) *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*, resolution 57/239 of 31 January 2003 on the *Creation of a global culture of cybersecurity*, and resolution 69/28 of 2 December 2014 on *Developments in the field of information and telecommunications in the context of international security**,*** **as well as the consensus final reports of 2021 of the United Nations Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, and of the United Nations Group of Governmental Experts on advancing responsible State behaviour in the context of international security**, **47**

(Germany)

Amend to read as follows:

(6) *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*, resolution 57/239 of 31 January 2003 on the *Creation of a global culture of cybersecurity*, ~~and~~ resolution 69/28 of 2 December 2014 on *Developments in the field of information and telecommunications in the context of international security*, **and resolution 73/266 of 22 December 2018 on *Advancing responsible State behaviour in cyberspace in the context of international security***, **48**

(Thailand)

New preambular paragraph 6bis

(6bis) *Also recalling* United Nations General Assembly resolution 70/237 of 23 December 2015, also on *Developments in the field of information and telecommunications in the context of international security*, which endorsed the voluntary and non-binding norms regarding responsible State behaviour in the use of information and communications technologies developed by the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, and called on Member States to be guided by these norms, **49**

(Canada)

Preambular paragraph 7

Amend to read as follows:

(7) *Stressing* the importance of regional conventions on ~~cybercrime, transnational organized crime~~ **the use of information and communications technologies for criminal purposes, and on the** 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, and the *Arab Convention on Combating Information Technology Offences* of 21 December 2010, **50**

(Islamic Republic of Iran)

Amend to read as follows:

(7) *Stressing* the importance of regional conventions on ~~cybercrime~~ **misuse of ICT for criminal purposes**, 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, and the *Arab Convention on Combating Information Technology Offences* of 21 December 2010, **51**

(Pakistan)

Amend to read as follows:

(7) *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, and the *Arab Convention on Combating Information Technology Offences* of 21 December 2010,~~ **52**

(India)

Amend to read as follows:

(7) ~~*Stressing* the importance~~ ***Taking note*** 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, and the *Arab Convention on Combating Information Technology Offences* of 21 December 2010, **53**

(Singapore)

Amend to read as follows:

(7) *Stressing* the importance of **existing international and** regional conventions on cybercrime, transnational organized crime, exchange of information and administrative assistance, including **the United Nations *Convention against Transnational Organized Crime* of 15 November 2000, the United Nations *Convention against Corruption* of 31 October 2003,** 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, and the *Arab Convention on Combating Information Technology Offences* of 21 December 2010, **54**

(Belgium)

Amend to read as follows:

(7) *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, and the *Arab Convention on Combating Information Technology Offences* of 21 December 2010, **as well as the Latin American and Caribbean Parliament (Parlatino) *Model Law on Cybercrime* of November 2013 and its updates, the *Model Law on Social Prevention of Violence and Crime* of November 2015, the *Model Law on Computer Crimes* of February 2021, and the *Model Law on Combating Illicit Trade and Transnational Crime* of February 2021,** **55**

(Argentina)

Amend to read as follows:

(7) *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, ~~and~~ the *Arab Convention on Combating Information Technology Offences* of 21 December 2010, **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, and 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,** **56**

(Russian Federation)

Amend to read as follows:

(7) *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, ~~and~~ the *Arab Convention on Combating Information Technology Offences* of 21 December 2010 **and the African Union *Convention on Cyber Security and Personal Data Protection* of 27 June 2014**, **57**

(South Africa)

New preambular paragraph 7bis

(7bis) *Also stressing* that the Council of Europe *Convention on Cybercrime* of 23 November 2001 (the "Budapest Convention"), 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, **58**

(Romania)

Preambular paragraph 8

Amend to read as follows:

(8) *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,~~ **59**

(India)

Amend to read as follows:

(8) *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, **as well as the Latin American and Caribbean Parliament (Parlatino) *Model Law on Protection against School Violence* of November 2015, the *Model Law on guaranteeing the prevention, care and punishment of sexual abuse against children and adolescents* of November 2015, and the *Model Law against Grooming* of June 2019,** **60**

(Argentina)

New preambular paragraph 8bis

(8bis) *Noting* the principles of cybersecurity that were agreed upon in the *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* of 22 July 2015 (A/70/174) to the United Nations General Assembly, **61**

(Viet Nam)

Preambular paragraph 9

Delete the paragraph. **62**

(Belgium, Canada, Switzerland)

Amend to read as follows:

(9) ~~*Expressing concern* about the lack of universal legal instruments for the suppression of cybercrime and cyberattacks~~ ***Commending*** **the work of the United Nations on advancing responsible State behaviour in cyberspace**, **63**

(Germany)

Amend to read as follows:

(9) *Expressing concern* about the lack of universal legal instruments for the suppression of ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** and ~~cyberattacks~~ **ICT threats**, **64**

(Islamic Republic of Iran)

Amend to read as follows:

(9) *Expressing concern* about the lack of universal legal instruments for the suppression of ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks, **65**

(Pakistan)

Amend to read as follows:

(9) *Expressing concern* about ~~the lack of universal legal instruments~~ **the slow pace of ratification of existing legal tools** for the suppression of cybercrime ~~and cyberattacks~~**, such as the Council of Europe *Convention on Cybercrime* of 23 November 2001 and its Additional Protocols**, **66**

(Sweden)

Amend to read as follows:

(9) *Expressing concern* about the lack of universal legal instruments for the suppression of cybercrime ~~and cyberattacks~~, **67**

(Japan)

Amend to read as follows:

(9) *Expressing concern* about the lack of universal legal instruments for ~~the suppression of~~ **preventing and combating** cybercrime and ~~cyberattacks~~ **cyber incidents**, **68**

(India)

Amend to read as follows:

(9) *Expressing concern* about the lack of universal legal instruments for the suppression of cybercrime and cyberattacks, **as well as for the prevention of acts of cyberwar**, **69**

(Argentina)

Amend to read as follows:

(9) *Expressing concern* about the lack of **a** universal **strategy and** legal instruments for the suppression of cybercrime and cyberattacks, **70**

(Philippines)

Preambular paragraph 10

Delete the paragraph. **71**

(Canada)

Amend to read as follows:

(10) *Commending* the efforts of the United Nations to enact, through General Assembly resolution 74/247 of 27 December 2019, ~~a comprehensive~~ **an** international **cybercrime** convention ~~on countering the use of information and communications technologies for criminal purposes~~, and welcoming the creation of an ad hoc committee charged with drafting this convention, **72**

(Sweden)

Amend to read as follows:

(10) *Commending* the efforts of the United Nations to enact, through General Assembly resolution 74/247 of 27 December 2019, a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, and welcoming the creation of an ad hoc committee charged with ~~drafting~~ **elaborating** this convention, **73**

(Singapore)

New preambular paragraph 10bis

(10bis) *Commending* also the efforts of the United Nations to convene, through United Nations General Assembly resolutions 73/27 of 5 December 2018, 75/240 of 31 December 2020 and 77/36 of 7 December 2022, an Open-ended Working Group (OEWG) on security of and in the use of information and communications technologies (ICTs), with a view to making the United Nations negotiation process on security in the use of ICTs more democratic, inclusive and transparent, **74**

(Islamic Republic of Iran)

Preambular paragraph 11

Amend to read as follows:

(11) *Welcoming* the participation of the IPU in ~~the~~ **any** multi-stakeholder consultation ~~process of that ad hoc committee~~ **that advances awareness and implementation of voluntary and non-binding norms regarding responsible State behaviour in the use of information and communications technologies,** in order to ensure that the voice of parliaments is heard, **75**

(Canada)

Amend to read as follows:

(11) *Welcoming* the participation of the IPU in the multi-stakeholder consultation process of that ad hoc committee**, as well as in the OEWG on security of and in the use of ICTs,** in order to ensure that the voice of parliaments is heard, **76**

(Islamic Republic of Iran)

Amend to read as follows:

(11) *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, **after consultation with the States Parties,** **77**

(Nicaragua)

Amend to read as follows:

(11) *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 **in an effort to fight against cybercrime and cyberattacks**, **78**

(Thailand)

New preambular paragraph 11bis

(11bis) *Supporting* the Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025 established pursuant to United Nations General Assembly resolution 75/240, and further *encouraging* it to take into account the outcomes of the 2010, 2013, 2015 and 2021 reports of the Groups of Governmental Experts and the 2021 report of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, and to add to the efforts undertaken by them, **79**

(Egypt)

New Preambular paragraph 11ter

(11ter) *Welcoming* the proposal, endorsed by the United Nations General Assembly in its resolution 77/37 of 7 December 2022, to establish a United Nations programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security, as a permanent, inclusive, action-oriented mechanism to discuss existing and potential threats; to support States' capacities and efforts to implement and advance commitments to be guided by the framework; to promote engagement and cooperation with relevant stakeholders; and to periodically review the progress made in the implementation of the programme of action as well as the programme's future work, **80**

(Egypt)

Preambular paragraph 12

Delete the paragraph. **81**

(Canada)

Amend to read as follows:

(12) *Noting* the need for a comprehensive and global approach to ~~the issue of cybercrime and cyberattacks, including through the development of an international legal framework to address cybercrime and cyberattacks and their serious consequences for citizens and~~ **the malicious use of ICTs** to protect global peace, security and ~~economic~~ stability, **82**

(Germany)

Amend to read as follows:

(12) *Noting* the need for a ~~comprehensive and~~ global approach to the issue of cybercrime ~~and cyberattacks, including through the development of an international legal framework to address cybercrime and cyberattacks~~ and ~~their~~ **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**, **83**

(Sweden)

Amend to read as follows:

(12) *Noting* the need for a comprehensive and global approach ~~to the issue of cybercrime and cyberattacks, including through the development of an international legal framework~~ to address cybercrime and cyberattacks and their serious consequences for citizens and to protect global peace, security and economic stability, **84**

(Switzerland)

Amend to read as follows:

(12) *Noting* the need for a comprehensive and global approach to the issue of ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** and ~~cyberattacks~~ **ICT threats**, including through the development of ~~an~~ international**,** ~~legal framework~~ **legally binding frameworks tailored to the unique attributes of ICTs** to address ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** and ~~cyberattacks~~ **ICT threats** and their serious consequences for citizens and to protect global peace, security and economic stability, **85**

(Islamic Republic of Iran)

Amend to read as follows:

(12) *Noting* the need for a comprehensive and global approach to the issue of ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks, including through the development of an international legal framework to address ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks and their serious consequences for citizens and to protect global peace, security and economic stability, **86**

(Pakistan)

Amend to read as follows:

(12) *Noting* the need for a comprehensive and global approach to the issue of cybercrime ~~and cyberattacks~~, including through the development of an international legal framework to address cybercrime ~~and cyberattacks~~ and their serious consequences for citizens and to protect global peace, security and economic stability, **87**

(Japan)

Amend to read as follows:

(12) *Noting* the need for a comprehensive and global approach to the issue of cybercrime and ~~cyberattacks~~ **cyber incidents**, including through the development of an international legal framework to address cybercrime and cyberattacks and their serious consequences for citizens and to protect global peace, security and economic stability, **88**

(India)

Amend to read as follows:

(12) *Noting* the need for a comprehensive and global approach to the issue of cybercrime and cyberattacks, including through the development of an international legal framework to address cybercrime and cyberattacks and their serious consequences for citizens **and infrastructure,** and to protect global peace, security and economic stability, **89**

(Lithuania)

New preambular paragraph 12bis

(12bis) *Noting* also that international community needs to take a comprehensive approach to threats in the sphere of ICT security that addresses not only the technological dimension of threats in this area, but also their political and ideological dimension, which includes, inter alia, the use of ICTs to interfere in the internal affairs of other States and to undermine their political, economic and social stability, **90**

(Islamic Republic of Iran)

(12bis) *Welcoming* the ongoing efforts to adapt and apply existing international legal regimes to the regulation of cyberspace, including the development of the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, **91**

(Ukraine)

Preambular paragraph 13

Amend to read as follows:

(13) *Recognizing* the urgent need for legislators and governments to take more proactive national steps to combat ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** and ~~cyberattacks~~ **ICT threats**, given their renewed intensity and rapidly evolving nature, **92**

(Islamic Republic of Iran)

Amend to read as follows:

(13) *Recognizing* the urgent need for legislators and governments to take more proactive national steps to combat cybercrime ~~and cyberattacks~~, given ~~their~~ **its** renewed intensity and rapidly evolving nature, **93**

(Czech Republic, Sweden)

Amend to read as follows:

(13) *Recognizing* the urgent need for legislators and governments to take more proactive national steps to combat cybercrime and ~~cyberattacks~~ **cyber incidents**, given their renewed ~~intensity~~ **severity** and rapidly evolving nature, **94**

(India)

Amend to read as follows:

(13) *Recognizing* the urgent need for legislators and governments to take more proactive national steps to combat ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks, given their renewed intensity and rapidly evolving nature, **95**

(Pakistan)

Amend to read as follows:

(13) *Recognizing* the urgent need for legislators ~~and~~**,** governments **and all stakeholders** to take more proactive national steps to combat cybercrime and cyberattacks, given their renewed intensity and rapidly evolving nature, **96**

(Thailand)

Amend to read as follows:

(13) *Recognizing* the urgent need for legislators and governments to take more proactive national steps to combat cybercrime and cyberattacks, given their renewed intensity and rapidly evolving nature, **while fully respecting human rights, fundamental freedoms and the rule of law, as well as their obligations under international human rights law,** **97**

(Canada)

Amend to read as follows:

(13) *Recognizing* the urgent need for legislators and governments to take more proactive national steps to combat cybercrime and cyberattacks, given their renewed intensity and rapidly evolving nature, **and equally to reinforce protections for freedom of expression and other fundamental rights**, **98**

(South Africa)

New preambular paragraph 13bis

(13bis) *Recognizing* that all actions in this field need to have respect for human rights and fundamental rights at their centre, **99**

(Sweden)

(13bis) *Noting* the uneven development in countries' IT application capacity and ability to protect IT infrastructure, and *emphasizing* the need for increased technical assistance and collaboration, especially for developing countries, **100**

(Viet Nam)

New preambular paragraph 13ter

(13ter) *Noting* 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, **101**

(Sweden)

Preambular paragraph 14

Delete the paragraph. **102**

(India)

Amend to read as follows:

(14) *Recognizing also* the need for common, international parliamentary action to ~~provide a protective shield for citizens, governments and States, which are all stakeholders in this task,~~ **advance awareness and implementation of voluntary and non-binding norms regarding responsible State behaviour in the use of information and communications technologies,** **103**

(Canada)

Amend to read as follows:

(14) *Recognizing also* the need for common, **regional and** international parliamentary action to provide a protective shield for citizens, governments and States, which are all stakeholders in this task, **as well as for the necessary legislative coordination at the subnational level,** **104**

(Argentina)

New preambular paragraph 14bis

(14bis) *Noting* that cybercrime may constitute a serious threat to democratic processes, notably interference in elections through cybersecurity breaches or false social media accounts, **105**

(Finland)

(14bis) *Recalling* the damaging impacts of unilateral coercive measures and other restrictions during the COVID-19 pandemic, which have been widely acknowledged, including in United Nations reports, **106**

(Islamic Republic of Iran)

New preambular paragraph 14ter

(14ter) *Urging* parliaments to call upon their governments to refrain from promulgating or applying any unilateral coercive measures (unilateral financial, economic or trade measures) that impede or negatively affect the ability of States to prevent and combat cybercrime or to render cooperation and assistance to each other in that regard, **107**

(Islamic Republic of Iran)

Preambular paragraph 15

Amend to read as follows:

(15) *Acknowledging* that women~~, young people and children are the most vulnerable and suffer the greatest aggressions on the internet, and are personally, socially, culturally and economically affected by cybercriminals~~ **and girls, the elderly and children, among others, are most at risk of being exposed to threats in cyberspace**, **108**

(Germany)

Amend to read as follows:

(15) *Acknowledging* that women, young people, **elderly people, disabled persons** and children are ~~the most~~ **particularly** vulnerable and suffer the greatest **number of** aggressions on the internet,~~ and are personally, socially, culturally and economically affected by cybercriminals.~~ **109**

(Belgium)

Amend to read as follows:

(15) *Acknowledging* that women~~, young people~~ and children, **as well as elderly people,** are the most vulnerable and suffer the greatest aggressions on the internet, and are personally, socially, culturally and economically affected by ~~cybercriminals~~ **cybercrimes**, **110**

(Czech Republic)

Amend to read as follows:

(15) *Acknowledging* that women, young people and children are the most vulnerable and suffer the greatest aggressions ~~on the internet~~ **in cyberspace**, and are personally, socially, culturally and economically affected by cybercriminals, **111**

(Lithuania)

Amend to read as follows:

(15) *Acknowledging* that women, young people and children are the most vulnerable and suffer the greatest aggressions on the internet, and are personally, socially, culturally and economically affected by cybercriminals, **while *emphasizing* the need to increase cooperation with the private sector and service providers in order to protect those affected,** **112**

(Thailand)

Amend to read as follows:

(15) *Acknowledging* that women, young people**,** ~~and~~ children **and racialized communities** are the most vulnerable and suffer the greatest aggressions on the internet, and are personally, socially, culturally and economically affected by cybercriminals, **113**

(Canada)

Amend to read as follows:

(15) *Acknowledging* that women, young people and children**, and persons with disabilities** are the most vulnerable and suffer the greatest aggressions on the internet, and are personally, socially, culturally and economically affected by cybercriminals, **114**

(Finland)

Amend to read as follows:

(15) *Acknowledging* that women, young **and elderly** people**,** and children are the most vulnerable and suffer the greatest aggressions on the internet, and are personally, socially, culturally and economically affected by cybercriminals, **115**

(Viet Nam)

Amend to read as follows:

(15) *Acknowledging* that women, young people**, the elderly** and children are the most vulnerable and suffer the greatest aggressions on the internet, and are personally, socially, culturally and economically affected by cybercriminals, **116**

(Türkiye)

New preambular paragraph 15bis

(15bis) *Bearing in mind* that research shows that, in times of COVID-19, more women and girls have become victims of online violence through physical threats, sexual harassment and stalking, among others, **117**

(Philippines)

(15bis) *Acknowledging* 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, **118**

(Sweden)

Preambular paragraph 16

Amend to read as follows:

(16) *Noting* the nature of the threats and risks of **the** transnational ~~cybercrime~~ **use of information and communications technologies for criminal purposes** and ~~cyberattacks~~ **ICT threats** to international peace and security, and the tremendous developments in ~~cyberspace~~ **the ICT environment**, as a result of which the methods used by cybercriminals **and malicious actors** are becoming increasingly sophisticated, **119**

(Islamic Republic of Iran)

Amend to read as follows:

(16) *Noting* the nature of the threats and risks of transnational ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks 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, **120**

(Pakistan)

Amend to read as follows:

(16) *Noting* the nature of the threats and risks of transnational cybercrime ~~and cyberattacks~~ 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, **121**

(Sweden)

Amend to read as follows:

(16) *Noting* the nature of the threats and risks of transnational cybercrime and ~~cyberattacks~~ **cyber incidents** 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, **122**

(India)

Amend to read as follows:

(16) *Noting* the nature of the threats and risks of transnational cybercrime and **malicious** cyberattacks 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, **123**

(Belgium)

New preambular paragraph 16bis

(16bis) *Expressing concern* about the indiscriminate use of cyberattacks against objects of civilian infrastructure, which cause disproportionate and unnecessary damage to energy generation and distribution facilities, hospitals, bank systems and other critical national infrastructure, **124**

(Ukraine)

Preambular paragraph 17

Amend to read as follows:

(17) *Noting also* that cybercrime ~~and cyberattacks encompass~~ not only **encompasses** attacks on ~~information and communications technologies (ICTs)~~ **computer systems**, breaches of privacy, and the creation and deployment of malware, but **is** also ~~attacks~~ **increasingly facilitating cyberattacks** on critical ~~national~~ **civilian** infrastructure, as well as other acts that can occur offline and be facilitated by ~~ICTs~~ **computer systems**, including online fraud, drug purchases, money-laundering, hate crimes, ~~propaganda, extremist indoctrination,~~ and the sexual exploitation of women and children via the internet – all of which negatively affect global security and economic stability, **125**

(Sweden)

Amend to read as follows:

(17) *Noting also* that cybercrime and cyberattacks encompass ~~not only~~ **in particular** attacks on information and communications technologies (ICTs), breaches of privacy, and the creation and deployment of malware, ~~but also attacks on critical national infrastructure, as well as other acts that can occur offline and be facilitated by ICTs, including online fraud, drug purchases, money-laundering, hate crimes, propaganda, extremist indoctrination, and the sexual exploitation of women and children via the internet – all of which negatively affect global security and economic stability~~ **while also acknowledging the need for international cooperation on other serious crimes that can be facilitated by ICTs**, **126**

(Germany)

Amend to read as follows:

(17) *Noting also* that ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** and ~~cyberattacks~~ **ICT threats** encompass not only attacks on information and communications technologies (ICTs), breaches of privacy, **disinformation campaigns, fabricated image-building, xenophobia, interference in the internal affairs of States,** and the creation and deployment of malware, but also attacks on critical national infrastructure, as well as other acts that can occur offline and be facilitated by ICTs, including online fraud, drug purchases, money-laundering, hate crimes, propaganda, extremist indoctrination, and the sexual exploitation of women and children via the internet – all of which negatively affect global security**, as well as** economic **and cultural** stability, **127**

(Islamic Republic of Iran)

Amend to read as follows:

(17) *Noting also* that cybercrime and ~~cyberattacks~~ **cyber incidents** encompass not only attacks on information and communications technologies (ICTs), breaches of privacy, and the creation and deployment of malware, but also attacks on critical national infrastructure, as well as other acts that can occur offline and be facilitated by ICTs, including online fraud, drug purchases, money-laundering, hate crimes, propaganda, extremist indoctrination, and the sexual exploitation of women and children via the internet – all of which negatively affect global security and economic stability, **128**

(India)

Amend to read as follows:

(17) *Noting also* that ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks encompass not only attacks on information and communications technologies (ICTs), breaches of privacy, and the creation and deployment of malware, but also attacks on critical national infrastructure, as well as other acts that can occur offline and be facilitated by ICTs, including online fraud, drug purchases, money-laundering, hate crimes, propaganda, extremist indoctrination, and the sexual exploitation of women and children via the internet – all of which negatively affect global security and economic stability, **129**

(Pakistan)

Amend to read as follows:

(17) *Noting also* that cybercrime and cyberattacks encompass not only attacks on ~~information and communications technologies (ICTs)~~ **computer systems**, breaches of privacy, and the creation and deployment of malware, but also attacks on critical national infrastructure, as well as other acts that can occur offline ~~and be facilitated by ICTs~~ **but that now take place in cyberspace with the facilitation of computer systems**, including online fraud, drug purchases, money-laundering, hate crimes, propaganda, extremist indoctrination, and the sexual exploitation of women and children via the internet – all of which negatively affect global security and economic stability, **130**

(Singapore)

Amend to read as follows:

(17) *Noting also* that cybercrime and cyberattacks ~~encompass not only~~ **include but are not limited to** attacks on information and communications technologies (ICTs), breaches of privacy, ~~and~~ the creation and deployment of malware, ~~but also~~ **and** attacks on critical national infrastructure, as well as other acts that can occur offline and be facilitated by ICTs, including online fraud, drug purchases, money-laundering, hate crimes, propaganda, extremist indoctrination, and the sexual exploitation of women and children via the internet – all of which negatively affect global security and economic stability, **131**

(Canada)

Amend to read as follows:

(17) *Noting also* that cybercrime and cyberattacks encompass not only attacks on information and communications technologies (ICTs), breaches of privacy, and the creation and deployment of malware, but also attacks on critical national infrastructure, as well as other acts that can occur offline and be facilitated by ICTs, including online fraud, drug purchases, money-laundering, ~~hate crimes, propaganda, extremist indoctrination,~~ and the sexual exploitation of women and children via the internet – all of which negatively affect global security and economic stability, **132**

(Belgium)

Amend to read as follows:

(17) *Noting also* that cybercrime and cyberattacks encompass not only attacks on information and communications technologies (ICTs), breaches of privacy, and the creation and deployment of malware, but also attacks on critical national infrastructure, as well as other acts that can occur offline and be facilitated by ICTs, including online fraud, drug purchases, money-laundering, hate crimes, propaganda, extremist indoctrination, **cyberbullying and stalking, trafficking in persons,** and the sexual exploitation of women and children via the internet – all of which negatively affect global security and economic stability, **133**

(South Africa)

Amend to read as follows:

(17) *Noting also* that cybercrime and cyberattacks encompass not only attacks on information and communications technologies (ICTs), breaches of privacy, and the creation and deployment of malware, but also attacks on critical national infrastructure, as well as other acts that can occur offline and be facilitated by ICTs, including online fraud, drug purchases, money-laundering, **human trafficking,** hate crimes, propaganda, extremist indoctrination, and the sexual exploitation of women and children via the internet – all of which negatively affect global security and economic stability, **134**

(Romania)

Amend to read as follows:

(17) *Noting also* that cybercrime and cyberattacks encompass not only attacks on information and communications technologies (ICTs), breaches of privacy, and the creation and deployment of malware, but also attacks on critical national infrastructure, as well as other acts that can occur offline and be facilitated by ICTs, including online fraud, drug purchases, money-laundering, hate crimes, propaganda, extremist indoctrination, and the sexual exploitation**, especially** of women and children**,** via the internet – all of which negatively affect global security and economic stability, **135**

(Lithuania)

New preambular paragraph 17bis

(17bis) *Acknowledging* the value of exchanging experiences with different definitions of cybercrime and cyberattacks in order to build a broader foundation for developing confidence-building measures, **136**

(Canada)

(17bis) *Recognizing* that the lack of responsibility of service providers and transnational platforms also poses a serious threat in the field of ICTs, which needs to be addressed by the international community, **137**

(Islamic Republic of Iran)

Preambular paragraph 18

Delete the paragraph. **138**

(Japan)

Amend to read as follows:

(18) *Considering* that most national laws were enacted ~~long~~ before cybercrime ~~and cyberattacks~~ arose and therefore do not always adequately address these threats, **139**

(Czech Republic)

Amend to read as follows:

(18) *Considering* that most national laws were enacted long before cybercrime ~~and cyberattacks~~ arose and therefore do not always adequately address these threats, **140**

(Sweden)

Amend to read as follows:

(18) *Considering* that most national laws were enacted long before ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** and ~~cyberattacks~~ **ICT threats** arose and therefore do not always adequately address these threats, **141**

(Islamic Republic of Iran)

Amend to read as follows:

(18) *Considering* that most national laws were enacted long before ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks arose and therefore do not always adequately address these threats, **142**

(Pakistan)

Amend to read as follows:

(18) *Considering* that most national laws were enacted long before **the spread of** cybercrime and cyberattacks ~~arose~~ and therefore do not always adequately address these threats, **143**

(Thailand)

Amend to read as follows:

(18) *Considering* that most national laws were enacted long before cybercrime and **malicious** cyberattacks arose and therefore do not always adequately address these threats, **144**

(Belgium)

New preambular paragraph 18bis

Amend to read as follows:

(18bis) *Stressing* the need for enhanced efforts to close the digital divide by facilitating the transfer of information technology and capacity-building to developing countries in the areas of the use of information and communications technologies for criminal purposes and ICT security, **145**

(Islamic Republic of Iran)

OPERATIVE PART

Operative paragraph 1

Delete the paragraph. **146**

(Belgium, Canada, Japan, Switzerland)

Amend to read as follows:

1. *Calls upon* the international community, through the United Nations, to **adapt and** adopt **a** common global ~~definitions~~ **definition** of cybercrime ~~and cyberattacks that include every variation of such acts and the acts they may facilitate~~; **147**

(Sweden)

Amend to read as follows:

1. *Calls upon* the international community, through the United Nations, to adopt common global definitions of cybercrime and cyberattacks ~~that include every variation of such acts and the acts they may facilitate~~; **148**

(Germany, Republic of Korea, Singapore)

Amend to read as follows:

1. *Calls upon* the international community, through the United Nations, to adopt **a** common global ~~definitions~~ **definition** of cybercrime ~~and cyberattacks~~ that ~~include~~ **includes** every variation of such ~~acts~~ **act** and the acts ~~they~~ **it** may facilitate**, including a clear differentiation between cybercrime and cyberwar, and between cybersecurity and cyberdefence**; **149**

(Argentina)

Amend to read as follows:

1. *Calls upon* the international community, through the United Nations, to adopt **a** common global ~~definitions~~ **definition** of cybercrime ~~and cyberattacks~~ that ~~include~~ **includes** every variation of such acts and the acts they may facilitate; **150**

(Czech Republic)

Amend to read as follows:

1. *Calls upon* the international community, through the United Nations, to adopt common**,** global**,** ~~definitions of cybercrime and cyberattacks~~ **universal terminology in the field of ICT security** that ~~include~~ **includes** every variation of such acts and the acts they may facilitate; **151**

(Islamic Republic of Iran)

Amend to read as follows:

1. *Calls upon* the international community, through the United Nations, to adopt common global definitions of ~~cybercrime~~ **crimes committed with the use of ICTs** and ~~cyberattacks~~ **cyber incidents** that include every variation of such acts and the acts they may facilitate; **152**

(India)

Amend to read as follows:

1. *Calls upon* the international community, through the United Nations, to adopt common global definitions of ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks that include every variation of such acts and the acts they may facilitate; **153**

(Pakistan)

Amend to read as follows:

1. *Calls upon* the international community, through the United Nations, to adopt common global definitions of cybercrime and cyberattacks that include every variation of such acts and the acts they may facilitate**, taking into account the realities of each nation**; **154**

(Nicaragua)

Operative paragraph 2

Delete the paragraph. **155**

(Belgium, Canada)

Amend to read as follows:

2. *Encourages* parliaments to call upon their governments to support the efforts of the United Nations to enact a ~~new~~ **comprehensive international** convention on ~~cybercrime~~ **countering the use of information and communications technologies for criminal purposes** by participating actively in its drafting; **156**

(India, Russian Federation)

Amend to read as follows:

2. *Encourages* parliaments to call upon their governments to support the efforts of the United Nations to enact a new convention on ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** by participating actively in its drafting; **157**

(Islamic Republic of Iran)

Amend to read as follows:

2. *Encourages* parliaments to call upon their governments to support the efforts of the United Nations to enact a new convention on ~~cybercrime~~ **misuse of ICT for criminal purposes** by participating actively in its drafting; **158**

(Pakistan)

New operative paragraph 2bis

2bis. *Also encourages* parliaments to call upon their governments to support the efforts of the United Nations OEWG on security of and in the use of information and communications technologies (ICTs) by participating actively in its sessions; **159**

(Islamic Republic of Iran)

Operative paragraph 3

Delete the paragraph. **160**

(Belgium, Canada)

Amend to read as follows:

3. *Urges* parliaments and their governments to convey the need to include, in the convention, ~~comprehensive definitions of cybercrime and cyberattacks, along with~~ mechanisms supporting international cooperation to combat cybercrime ~~and cyberattacks,~~ **with adequate safeguards**; **161**

(Sweden)

Amend to read as follows:

3. *Urges* parliaments and their governments to convey the need to include, in the convention, ~~comprehensive definitions of cybercrime and cyberattacks, along with~~ mechanisms supporting international cooperation to combat cybercrime ~~and cyberattacks~~; **162**

(Japan)

Amend to read as follows:

3. *Urges* parliaments and their governments to convey the need to include, in the convention, ~~comprehensive definitions of cybercrime and cyberattacks, along with~~ mechanisms supporting international cooperation to combat cybercrime and cyberattacks; **163**

(Lithuania, Republic of Korea)

Amend to read as follows:

3. *Urges* parliaments and their governments to convey the need to include, in the convention, **a** comprehensive ~~definitions of cybercrime and cyberattacks~~ **catalogue of clearly defined cybercrimes**, along with mechanisms supporting international cooperation to combat cybercrime and cyberattacks; **164**

(Switzerland)

Amend to read as follows:

3. *Urges* parliaments and their governments to convey the need to include, in the convention, **a** comprehensive ~~definitions~~ **definition** of cybercrime ~~and cyberattacks~~, along with mechanisms supporting international cooperation to combat **such crime** ~~cybercrime and cyberattacks~~**, without prejudice to the application of current national legislation on cybersecurity and the protection of personal data**; **165**

(Argentina)

Amend to read as follows:

3. *Urges* parliaments and their governments to convey the need to include, in the convention, comprehensive definitions of cybercrime ~~and cyberattacks~~, along with mechanisms supporting international cooperation to combat cybercrime ~~and cyberattacks~~; **166**

(Germany)

Amend to read as follows:

3. *Urges* parliaments and their governments to convey the need to include, in the convention**,** ~~comprehensive definitions of cybercrime and cyberattacks~~ **as well as the outcomes of the OEWG on ICT security, universal terminology in the field of ICT security**, along with mechanisms supporting international cooperation to combat ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** and ~~cyberattacks~~ **ICT threats**; **167**

(Islamic Republic of Iran)

Amend to read as follows:

3. *Urges* parliaments and their governments to convey the need to include, in the convention, comprehensive definitions of ~~cybercrime~~ **crimes committed with the use of ICTs** and ~~cyberattacks~~ **cyber incidents**, along with mechanisms supporting international cooperation to combat cybercrime and ~~cyberattacks~~ **cyber incidents**; **168**

(India)

Amend to read as follows:

3. *Urges* parliaments and their governments to convey the need to include, in the convention, comprehensive definitions of ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks, along with mechanisms supporting international cooperation to combat ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks; **169**

(Pakistan)

Amend to read as follows:

3. *Urges* parliaments and their governments to convey the need to include, in the convention, comprehensive definitions of cybercrime and cyberattacks **including related criminal offences**, **and safeguards required to protect human rights and fundamental freedoms**, along with mechanisms supporting international cooperation **and technical assistance** to combat **and prevent** cybercrime and cyberattacks; **170**

(South Africa)

Amend to read as follows:

3. *Urges* parliaments and their governments to convey the need to include, in the convention, comprehensive definitions of cybercrime and cyberattacks, along with mechanisms supporting international **and multi-stakeholder** cooperation**, as well as their guidelines for implementation and evaluation,** to **effectively** combat cybercrime and cyberattacks; **171**

(Thailand)

New operative paragraph 3bis

3bis. *Also urges* parliaments and their governments to ensure that the new convention complements existing international and regional instruments on cybercrime and on transnational organized crime, as well as other relevant instruments, in particular those relating to the protection of human rights; **172**

(Romania)

3bis. *Also urges* parliaments and their governments to emphasize the importance of including strong protection of human rights and fundamental freedoms in the new convention; **173**

(Sweden)

Operative paragraph 4

Delete the paragraph. **174**

(Belgium, Canada)

Amend to read as follows:

4. *Invites* parliaments and their governments to use this convention, once adopted, as a means to strengthen national legislation and to increase international cooperation to combat cybercrime ~~and cyberattacks~~; **175**

(Argentina, Czech Republic, Germany, Sweden)

Amend to read as follows:

4. *Invites* parliaments and their governments to use this convention, once adopted, as a means to strengthen national legislation and to increase international cooperation to combat ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** and ~~cyberattacks~~ **ICT threats**; **176**

(Islamic Republic of Iran)

Amend to read as follows:

4. *Invites* parliaments and their governments to use this convention, once adopted, as a means to strengthen national legislation and to increase international cooperation to combat ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks; **177**

(Pakistan)

Amend to read as follows:

4. *Invites* parliaments and their governments to use this convention, once adopted, as a means to ~~strengthen~~ **update** national legislation and to increase international cooperation to combat cybercrime and cyberattacks; **178**

(Japan)

Amend to read as follows:

4. *Invites* parliaments and their governments to use this convention, once adopted **and in force**, as a means to strengthen national legislation and to increase international cooperation to combat cybercrime and cyberattacks; **179**

(Viet Nam)

Amend to read as follows:

4. *Invites* parliaments and their governments to use ~~this~~ **the** convention **referred to in operative paragraphs 2 and 3 above**, once adopted, as a means to strengthen national legislation and to increase international cooperation to combat cybercrime and cyber attacks; **180**

(South Sudan)

New operative paragraph 4bis

4bis. *Encourages* parliaments to take full account of the disruptive and destructive potential of cyberattacks by addressing the issue of critical national infrastructure protection, including but not limited to electricity, water, gas, communication, nuclear power plants, transportation, finance and food supply; **181**

(Argentina)

4bis. *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* of 23 November 2001 (the "Budapest Convention"), which is the most comprehensive multilateral cybercrime treaty in force and is open for accession by all States; **182**

(Romania)

Operative paragraph 5

Amend to read as follows:

5. *Calls upon* parliaments to ~~enact new~~ **make sure their** legislation on cybercrime ~~and cyberattacks~~ **is up to date and relevant**, considering the ongoing increase in the scale and frequency of such acts and their implications for international peace and security and global economic stability; **183**

(Sweden)

Amend to read as follows:

5. *Calls upon* parliaments to enact, **where appropriate,** new legislation on cybercrime ~~and cyberattacks~~, considering the ongoing increase in the scale and frequency of such acts and their implications for international peace and security and global economic stability; **184**

(Czech Republic)

Amend to read as follows:

5. *Calls upon* parliaments to enact new legislation on ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** and ~~cyberattacks~~ **ICT threats**, considering the ongoing increase in the scale and frequency of such acts and their implications for international peace and security and global economic stability; **185**

(Islamic Republic of Iran)

Amend to read as follows:

5. *Calls upon* parliaments to enact new legislation on cybercrime and ~~cyberattacks~~ **cybersecurity**, considering the ongoing increase in the scale and frequency of ~~such acts~~ **cybercrime and malicious cyberattacks** and their implications for international peace and security and global economic stability; **186**

(Belgium)

Amend to read as follows:

5. *Calls upon* parliaments to enact new legislation on ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks, considering the ongoing increase in the scale and frequency of such acts and their implications for international peace and security and global economic stability; **187**

(Pakistan)

Amend to read as follows:

5. *Calls upon* parliaments to ~~enact new~~ **update national** legislation on cybercrime and cyberattacks, considering the ongoing increase in the scale and frequency of such acts and their implications for international peace and security and global economic stability; **188**

(Japan)

Amend to read as follows:

5. *Calls upon* parliaments ~~to enact~~ **that have yet to enact a** new ~~legislation~~ **law** on cybercrime and cyberattacks **to do so**, considering the ongoing increase in the scale and frequency ~~of such~~ **of commission of these illicit** acts and their **high-risk** implications for international peace and security and global economic stability; **189**

(Nicaragua)

Amend to read as follows:

5. *Calls upon* parliaments to enact new legislation on cybercrime and cyberattacks **in accordance with international law, including international human rights instruments**, considering the ongoing increase in the scale and frequency of such acts and their implications for international peace and security and global economic stability**, and 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**; **190**

(South Africa)

Amend to read as follows:

5. *Calls upon* parliaments to enact new legislation on cybercrime and cyberattacks**, by engaging all stakeholders, including the private sector, academia, civil society and the technical community**, considering the ongoing increase in the scale and frequency of such acts and their implications for **national security,** international peace and security**,** and global economic stability; **191**

(Romania)

Amend to read as follows:

5. *Calls upon* parliaments to enact new legislation or **revise laws** on cybercrime and cyberattacks, considering the ongoing increase in the scale and frequency of such acts and their implications for international peace and security and global economic stability; **192**

(Viet Nam)

Amend to read as follows:

5. *Calls upon* parliaments to enact new legislation on cybercrime and cyberattacks, **and to allocate the necessary resources to this end**, considering the ongoing increase in the scale and frequency of such acts and their implications for international peace and security and global economic stability; **193**

(France)

Amend to read as follows:

5. *Calls upon* parliaments to enact new legislation on cybercrime and cyberattacks, considering the ongoing increase in the scale**, scope, speed, complexity** and frequency of such acts and their implications for international peace and security and global economic stability; **194**

(India)

New operative paragraph 5bis

5bis. *Also calls upon* the international community not to use information and communications technologies and information and communications networks to interfere in the internal affairs of other States or with the aim of undermining their political, economic and social stability; **195**

(Islamic Republic of Iran)

5bis. *Urges* parliaments to ensure that human rights impact assessments are embedded in all legislative processes on cybercrime and cyberattacks; **196**

(Romania)

5bis. *Also calls upon* parliaments to enhance the capacity of law enforcement officers, including investigative authorities, prosecutors and judges, in the field of cyberattacks and cybercrime, and to equip them to effectively investigate, prosecute and adjudicate cases of cyberattacks and cybercrime offences; **197**

(South Africa)

5bis. *Urges* parliaments and governments to devise and adopt a universal legal framework for cyberwarfare, incorporating the concepts of distinction and proportionality, to prevent cyberattacks against critical civilian infrastructure; **198**

(Ukraine)

Operative paragraph 6

Amend to read as follows:

6. *Encourages* parliaments to make full use of their oversight function to ensure that governments have the tools to control the rapid increase in ~~cybercrime and cyberattacks~~ **cybercrimes** and to protect the ~~digital security~~ **cybersecurity**, identity, privacy and data of citizens, especially the most vulnerable; **199**

(Czech Republic)

Amend to read as follows:

6. *Encourages* parliaments to make full use of their oversight function to ensure that governments have the tools to ~~control~~ **prevent and combat** the rapid increase in cybercrime ~~and cyberattacks~~ and to protect the digital security, identity, privacy and data of citizens, especially the most vulnerable; **200**

(Belgium)

Amend to read as follows:

6. *Encourages* parliaments to make full use of their oversight function to ensure that governments have the tools to control the rapid increase in cybercrime ~~and cyberattacks~~ and to protect the digital security, identity, privacy and data of citizens, especially the most vulnerable**, while safeguarding human rights and freedoms**; **201**

(Sweden)

Amend to read as follows:

6. *Encourages* parliaments to make full use of their oversight function to ensure that governments have the tools to control the rapid increase in ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** and ~~cyberattacks~~ **ICT threats** and to protect the digital security, identity, privacy and data of citizens, especially the most vulnerable; **202**

(Islamic Republic of Iran)

Amend to read as follows:

6. *Encourages* parliaments to make full use of their oversight function to ensure that governments have the tools to control the rapid increase in ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks and to protect the digital security, identity, privacy and data of citizens, especially the most vulnerable; **203**

(Pakistan)

Amend to read as follows:

6. *Encourages* parliaments to make full use of their ~~oversight~~ function to ensure that governments have the tools ~~to control~~ **against** the rapid increase in cybercrime and cyberattacks and to protect the digital security, identity, privacy and data of citizens, especially the most vulnerable; **204**

(Japan)

Amend to read as follows:

6. *Encourages* parliaments to make full use of their oversight function to ensure that governments have the tools to control the rapid increase in cybercrime and cyberattacks and to protect the digital security, identity, privacy and data of citizens~~, especially the most vulnerable~~; **205**

(India)

Amend to read as follows:

6. *Encourages* parliaments to make full use of their oversight function to ensure that governments have the tools, **including appropriate resources and capacity,** to control the rapid increase in cybercrime and cyberattacks and to protect the digital security, identity, privacy and data of citizens, especially the most vulnerable; **206**

(South Africa)

Amend to read as follows:

6. *Encourages* parliaments to make full use of their oversight function to ensure that governments have the tools to control the rapid increase in cybercrime and cyberattacks and to protect **human rights in cyberspace, including** the digital security, identity, privacy and data of citizens, especially the most vulnerable; **207**

(Argentina)

New operative paragraph 6bis

6bis. *Calls upon* parliaments and governments of developed countries to assist developing countries in their efforts to enhance capacity-building on ICT security and to close the digital divide; **208**

(Islamic Republic of Iran)

New operative paragraph 6ter

6ter. *Also calls upon* parliaments and their governments to refrain from adopting any unilateral coercive measures that restrict or prevent universal access to the benefits of ICTs; **209**

(Islamic Republic of Iran)

Operative paragraph 7

Amend to read as follows:

7. *Strongly recommends* that parliaments **ensure that their national legislative framework on the protection of critical national infrastructure, including the infrastructure that supports the internet, is up to date, and that they review or** establish legislative frameworks ~~aimed at protecting the infrastructure that supports the internet, in particular submarine cables, satellite networks and critical internet services, as well as large public and private data centres providing cloud services, which in turn should exchange information on cyber incidents, in real time, through relevant national and supranational bodies~~ **where necessary**; **210**

(Switzerland)

Amend to read as follows:

7. *Strongly recommends* that parliaments establish legislative frameworks aimed at protecting ~~the~~ **critical civilian** infrastructure ~~that supports the internet, in particular submarine cables, satellite networks and critical internet services, as well as large public and private data centres providing cloud services~~, which in turn should exchange information on cyber incidents, in real time, through relevant national and supranational bodies; **211**

(Sweden)

Amend to read as follows:

7. *Strongly recommends* that parliaments establish legislative frameworks aimed at protecting the infrastructure that supports the internet, in particular submarine cables, satellite networks and critical internet services, ~~as well as large public and private data centres providing cloud services, which in turn should exchange information on cyber incidents, in real time, through relevant national and supranational bodies~~ **and at facilitating collaboration with the private sector**; **212**

(Germany)

Amend to read as follows:

7. *Strongly recommends* that parliaments establish legislative frameworks ~~aimed at protecting~~ **for internet service providers, in order to protect** the infrastructure that supports the internet, in particular submarine cables, satellite networks and critical internet services, as well as large public and private data centres providing cloud services, which in turn should exchange information on cyber incidents, in real time, through relevant national and supranational bodies; **213**

(Nicaragua)

Amend to read as follows:

7. *Strongly recommends* that parliaments establish legislative frameworks aimed at protecting the infrastructure that supports the internet, in particular submarine cables, satellite networks and critical internet services, as well as large public and private data centres providing cloud services, which in turn should exchange information on cyber incidents, in real time, through relevant national and ~~supranational~~ **international** bodies; **214**

(India)

Amend to read as follows:

7. *Strongly recommends* that parliaments establish legislative frameworks aimed at protecting the infrastructure that supports the internet, in particular submarine cables, satellite networks and critical internet services, as well as large public and private data centres providing cloud services, which in turn should exchange information on cyber incidents~~, in real time,~~ through relevant national and supranational bodies; **215**

(Belgium)

Amend to read as follows:

7. *Strongly recommends* that parliaments establish legislative frameworks aimed at protecting the infrastructure that supports ~~the internet~~ **cyberspace**, in particular submarine cables, satellite networks and critical internet services, as well as large public and private data centres providing cloud services, which in turn should exchange information on cyber incidents, in real time, through relevant national and supranational bodies; **216**

(Lithuania)

Amend to read as follows:

7. *Strongly recommends* that parliaments establish legislative frameworks aimed at protecting **from cyberattacks** the infrastructure that supports the internet, in particular submarine cables, satellite networks and critical internet services, as well as large public and private data centres providing cloud services, which in turn should exchange information on cyber incidents, in real time, through relevant national and supranational bodies; **217**

(Argentina)

New operative paragraph 7bis

7bis. ***Also recommends*** **that all States play the same role in, and carry equal responsibility for, international governance of the internet through the establishment of a multilateral, transparent and democratic international internet governance mechanism;** **218**

(Islamic Republic of Iran)

Operative paragraph 8

Amend to read as follows:

8. *Encourages* parliaments to promote a secure ~~cyberspace~~ **ICT environment** by calling on their governments to cooperate in stopping ~~cybercrime~~ **the use of information and communications technologies for criminal purposes**, ~~and~~ **as well as** cybercriminals **and malicious actors**, to respond to requests for assistance **and capacity-building**, if possible in real time, 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; **219**

(Islamic Republic of Iran)

Amend to read as follows:

8. *Encourages* parliaments to promote a secure cyberspace by calling on their governments to cooperate in stopping ~~cybercrime~~ **misuse of ICT for criminal purposes** and cybercriminals, to respond to requests for assistance, if possible in real time, to secure the supply chain of companies in their countries, to report 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; **220**

(Pakistan)

Amend to read as follows:

8. ~~*Encourages*~~ ***Urges*** parliaments to promote a secure cyberspace by calling on their governments to cooperate in stopping cybercrime and cybercriminals, to respond to requests for assistance, if possible in real time, to secure the supply chain ~~of companies in their countries~~ **with service providers in each country**, to report 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; **221**

(Nicaragua)

Amend to read as follows:

8. *Encourages* parliaments to promote ~~a~~ **an open, free and** secure cyberspace by calling on their governments to cooperate in ~~stopping~~ **fighting** cybercrime and cybercriminals, to respond to requests for assistance, if possible in real time, to secure the supply chain of companies in their countries, to report 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; **222**

(Czech Republic)

Amend to read as follows:

8. *Encourages* parliaments to promote a secure cyberspace by calling on their governments to **abide by the United Nations norms of responsible State behaviour in cyberspace and** cooperate in stopping cybercrime and cybercriminals, to respond to requests for assistance, if possible in real time, to secure the supply chain of companies in their countries, to report 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; **223**

(Canada)

Amend to read as follows:

8. *Encourages* parliaments to promote a secure cyberspace by calling on their governments to cooperate in ~~stopping~~ **preventing and fighting** cybercrime ~~and cybercriminals~~, to respond to requests for assistance, if possible in real time, to secure the supply chain of companies in their countries, to report 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; **224**

(Lithuania)

Amend to read as follows:

8. *Encourages* parliaments to promote a secure cyberspace by calling on their governments to cooperate in ~~stopping~~ **mitigating the consequences of** ~~cybercrime~~ **cyberattacks** and ~~cybercriminals~~ **cybercrime**, to respond to requests for assistance, if possible in real time, to secure the supply chain of companies in their countries, to report 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; **225**

(Argentina)

Amend to read as follows:

8. *Encourages* parliaments to promote a secure cyberspace by calling on their governments to cooperate in stopping cybercrime and cybercriminals, to respond to requests for assistance **and exchange of information on cyber incidents and cybercriminals**, if possible in real time, to secure the supply chain of companies in their countries, to report 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; **226**

(Ukraine)

Amend to read as follows:

8. *Encourages* parliaments to promote a secure cyberspace by calling on their governments to cooperate in stopping cybercrime and cybercriminals, to respond to requests for assistance, 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 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; **227**

(Germany)

Amend to read as follows:

8. *Encourages* parliaments to promote a secure cyberspace by calling on their governments to cooperate in stopping cybercrime and cybercriminals, to respond to requests for assistance, if possible in real time, to secure the supply chain of companies in their countries, to report on potential vulnerabilities ~~to third parties to~~ **and** assist ~~them~~ in preventing future incidents, and in particular to support and protect all cyber incident response teams within and beyond their borders; **228**

(India)

Operative paragraph 9

Amend to read as follows:

9. *Also encourages* parliaments to draft 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~~ **ICT** threats; **229**

(Islamic Republic of Iran)

Amend to read as follows:

9. *Also encourages* parliaments to draft 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**, where they do not yet exist in their country**; **230**

(Nicaragua)

Amend to read as follows:

9. *Also encourages* parliaments to draft legislation promoting cross-cutting ~~cybersecurity~~ services **for security in the use of information and communications technologies, hereinafter referred to as "cybersecurity",** 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 **threats to security in the use of information and communications technologies, hereinafter referred to as "**cyber threats**"**; **231**

(Russian Federation)

Operative paragraph 10

Amend to read as follows:

10. *Recommends* that parliaments ~~establish~~ **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; **232**

(Romania)

Amend to read as follows:

10. *Recommends* that parliaments **advise their respective governments to** establish relevant institutions and bodies **for cybercrime and cyberattack prevention** – 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; **233**

(Thailand)

Operative paragraph 11

Amend to read as follows:

11. *Also recommends* that ~~all~~ parliaments ensure that such institutions and bodies have adequate budgetary resources and specialized personnel to allow for an agile and effective response to cyberattacks and to protect critical infrastructure, public institutions, companies and citizens; **234**

(Republic of Korea)

Amend to read as follows:

11. *Also recommends* that all parliaments ensure that such institutions and bodies have adequate budgetary resources and specialized personnel, **trained in human rights principles and practices,** to allow for an agile and effective response to cyberattacks and to protect critical infrastructure, public institutions, companies and citizens; **235**

(Canada)

Amend to read as follows:

11. *Also recommends* that all parliaments ensure that such institutions and bodies have adequate budgetary resources and specialized personnel to allow for **the prevention and detection of, and** an agile and effective response to**,** cyberattacks**,** ~~and to protect~~ **particularly the protection of vulnerable and** critical infrastructure **(such as air traffic management systems and electrical power grids)**, public institutions **(such as hospitals and health services)**, companies and citizens; **236**

(Philippines)

Amend to read as follows:

11. *Also recommends* that all parliaments ensure that such institutions and bodies have adequate budgetary resources and specialized personnel to allow for an agile and effective response to **cybercrime and** cyberattacks and to protect critical infrastructure, public institutions, companies and citizens; **237**

(Belgium)

Amend to read as follows:

11. *Also recommends* that all parliaments ensure that such institutions and bodies have adequate budgetary resources and specialized personnel to allow for an agile and effective response to ~~cyberattacks~~ **ICT threats** and to protect critical infrastructure, public institutions, companies and citizens; **238**

(Islamic Republic of Iran)

Amend to read as follows:

11. *Also recommends* that all parliaments ensure that such institutions and bodies have adequate budgetary resources and specialized personnel to allow for an agile**, timely** and effective response to cyberattacks and to protect critical infrastructure, public institutions, companies and citizens **without breaching privacy**; **239**

(Thailand)

Amend to read as follows:

11. *Also recommends* that all parliaments ensure that such institutions and bodies have adequate budgetary resources and specialized personnel to allow for an agile and effective response to cyberattacks and to protect critical **civilian** infrastructure, public institutions, companies and citizens; **240**

(Sweden)

Amend to read as follows:

11. *Also recommends* that all parliaments ensure that such institutions and bodies have adequate budgetary resources and specialized personnel to allow for an agile and effective response to cyberattacks and to protect critical infrastructure, public institutions, companies and citizens**, taking into account that the increasing digitalization of public services and utilities could imply major exposure to digital risks**; **241**

(Argentina)

New operative paragraph 11bis

11bis. *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; **242**

(Thailand)

Operative paragraph 12

Delete the paragraph. **243**

(Belgium, Canada, Egypt, Japan, Russian Federation)

Amend to read as follows:

12. *Urges* parliaments to promote international coordination between such institutions and bodies ~~and the creation of a global security operations centre, under the auspices of the United Nations,~~ in order to ~~constantly~~ monitor, prevent, detect, investigate and respond to cyber threats; **244**

(Switzerland)

Amend to read as follows:

12. *Urges* parliaments to promote international coordination between such institutions and bodies ~~and the creation of a global security operations centre, under the auspices of the United Nations,~~ in order to constantly monitor, prevent, detect, investigate and respond to cyber threats; **245**

(Germany)

Amend to read as follows:

12. *Urges* parliaments to promote international coordination between such institutions and bodies and the creation of a global ~~security operations~~ **cybersecurity** centre, under the auspices of the United Nations, in order to constantly monitor, prevent, detect, investigate and respond to cyber threats; **246**

(France)

Amend to read as follows:

12. *Urges* parliaments to promote international coordination between such institutions and bodies and the creation of a global security operations centre, under the auspices of the United Nations, in order to constantly monitor, ~~prevent,~~ detect, investigate, and respond to **global** cyber threats **in cooperation with the national cyber incident response teams of Member States so as to support the prevention of these threats**; **247**

(Türkiye)

Amend to read as follows:

12. *Urges* parliaments to promote international coordination between such institutions and bodies and the creation of a global security operations centre, under the auspices of the United Nations, in order to constantly monitor, prevent, detect, investigate and respond to ~~cyber~~ **ICT** threats; **248**

(Islamic Republic of Iran)

Amend to read as follows:

12. *Urges* parliaments to promote international coordination between such institutions and bodies and the creation of a global security operations centre, under the auspices of the United Nations, in order to constantly monitor, prevent, detect, investigate and respond to cyber threats**, while clearly defining the scope of its mandate in relation to other relevant United Nations bodies, such as the United Nations Chief Executives Board, through the High-Level Committee on Programmes and the United Nations-wide framework on cybersecurity and cybercrime**; **249**

(Sweden)

New operative paragraph 12bis

12bis. *Calls on* governments and the international community to collaborate on ways to expose the actors and entities behind these cyberattacks and to make them accountable for their actions through the filing of criminal cases and the imposition of applicable sanctions; **250**

(Philippines)

Operative paragraph 13

Delete the paragraph. **251**

(Belgium, Canada, Egypt, Germany, Russian Federation, Switzerland)

Amend to read as follows:

13. *Recommends* that ~~such an entity support~~ **technical assistance and capacity-building be provided to** all States, and especially those with fewer resources, in developing action and response capabilities, in sharing intelligence, knowledge and research in anticipation of future ~~technology-related challenges such as quantum computing, 5G, the metaverse or Artificial Intelligence~~ **technologies**, and in ~~raising the alarm should~~ **alerting if, in any circumstances,** the Universal Declaration of Human Rights **were to** be violated ~~in any circumstances~~; **252**

(Czech Republic)

Amend to read as follows:

13. *Recommends* that such an entity support ~~all~~ States, and especially those with fewer resources, in developing action and response capabilities, in sharing intelligence, knowledge and research in anticipation of future technology-related challenges such as quantum computing, 5G, the metaverse and artificial intelligence, and in raising the alarm should the Universal Declaration of Human Rights be violated in any circumstances; **253**

(Republic of Korea)

Amend to read as follows:

13. *Recommends* that such an entity support all States, and especially ~~those with fewer resources~~ **developing ones**, in developing action and response capabilities, in sharing intelligence, knowledge and research in anticipation of future technology-related challenges such as quantum computing, 5G, the metaverse and artificial intelligence, and in raising the alarm should the Universal Declaration of Human Rights be violated in any circumstances; **254**

(Islamic Republic of Iran)

Amend to read as follows:

13. *Recommends* that such an entity support all States, and especially those with fewer resources, in developing action and response capabilities, **and** in sharing intelligence, knowledge and research in anticipation of future technology-related challenges such as quantum computing, 5G, the metaverse and artificial intelligence~~, and in raising the alarm should the Universal Declaration of Human Rights be violated in any circumstances~~; **255**

(India)

Amend to read as follows:

13. *Recommends* that such an entity support all States, and especially those with fewer resources, in developing action and response capabilities, in sharing intelligence, knowledge and research in anticipation of future technology-related challenges such as quantum computing, 5G, the metaverse and artificial intelligence, and in~~ raising the alarm should the Universal Declaration of Human Rights be violated in any circumstances~~ **increasing their resilience to cyber threats**; **256**

(France)

Amend to read as follows:

13. *Recommends* that such an entity support all States, and especially those with fewer resources, in developing action and response capabilities, in sharing intelligence, knowledge and research in anticipation of future technology-related challenges such as quantum computing, 5G, the metaverse and artificial intelligence, and in raising the alarm should ~~the Universal Declaration of Human Rights be violated in any circumstances~~ **violations of universally recognized human rights be caused by developments in its area of responsibility**; **257**

(Ukraine)

Amend to read as follows:

13. *Recommends* that such an entity support all States, and especially those with fewer resources, in developing action and response capabilities, in sharing intelligence, knowledge and research in anticipation of future technology-related challenges such as quantum computing, 5G, the metaverse and artificial intelligence, and in raising the alarm should the Universal Declaration of Human Rights **or other human rights instruments** be violated in any circumstances; **258**

(Sweden)

New operative paragraph 13bis

13bis. *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; **259**

(Germany)

Operative paragraph 14

Delete the paragraph. **260**

(India)

Amend to read as follows:

14. *Calls upon* parliaments to encourage investment in research and development, incorporating into the design of each project specific ~~cybersecurity~~ **ICT security** provisions, with appropriate budget allocation, in order to anticipate and protect against possible emerging ~~cyber~~ **ICT** threats; **261**

(Islamic Republic of Iran)

Operative paragraph 15

Delete the paragraph. **262**

(India)

Amend to read as follows:

15. *Encourages* parliaments to partner with industry, academia and all other stakeholders, including civil society, in order to foster a strong and collaborative ~~cybersecurity~~ **ICT security** ecosystem; **263**

(Islamic Republic of Iran)

Amend to read as follows:

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; **264**

(Thailand)

Amend to read as follows:

15. *Encourages* parliaments to partner with industry, academia and all other stakeholders, including civil society, in order to foster a strong and collaborative cybersecurity ecosystem **that fully respects human rights principles and international human rights obligations**; **265**

(Canada)

Amend to read as follows:

15. *Encourages* parliaments to partner with industry, academia and all other stakeholders, including civil society, in order to foster a strong and collaborative cybersecurity ecosystem**, without prejudice to the establishment of regimes that guarantee that internet service and application providers deliver information promptly on the traces and indications that the judicial courts of different countries request, to the extent that such information may constitute digital evidence for the investigation of cybercrime at the local level, regardless of their regional headquarters or the privacy regulations of the country in which such information is stored**; **266**

(Argentina)

Operative paragraph 16

Delete the paragraph. **267**

(Belgium, Canada)

Amend to read as follows:

16. *Also encourages* parliaments to develop ~~legislative spaces where~~ **trust, such that** parliaments, governments, companies, academia and civil society can cooperate in real time in order to defend the general interests of all States; **268**

(India)

Amend to read as follows:

16. *Also encourages* parliaments to develop legislative spaces where parliaments, governments, companies, academia and civil society can cooperate in real time**, in accordance with rule of law and fully respecting international human rights law and fundamental freedoms,** in order to defend the general interests of all States; **269**

(Germany)

New operative paragraph 16bis

16bis. *Calls upon* parliaments and their governments to address the lack of responsibility of service providers and transnational platforms, which poses a serious threat in the ICT environment; **270**

(Islamic Republic of Iran)

Operative paragraph 17

Amend to read as follows:

17. *Calls upon* parliaments and parliamentarians to actively engage in promoting a shared, up-to-date national understanding of the nature of ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** and ~~cyberattacks~~ **ICT threats** as experienced by citizens, organizations and institutions; **271**

(Islamic Republic of Iran)

Amend to read as follows:

17. *Calls upon* parliaments and parliamentarians to actively engage in promoting a shared, up-to-date national understanding of the nature of ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks as experienced by citizens, organizations and institutions; **272**

(Pakistan)

Amend to read as follows:

17. *Calls upon* parliaments and parliamentarians to actively engage in promoting a shared, up-to-date national understanding of the nature of cybercrime ~~and cyberattacks~~ as experienced by citizens, organizations and institutions; **273**

(Belgium, Czech-Republic, Sweden)

Amend to read as follows:

17. *Calls upon* parliaments and parliamentarians to actively engage in promoting a shared, up-to-date national understanding of the nature of cybercrime and cyberattacks as experienced by citizens, organizations and institutions**, where they do not yet exist in their country**; **274**

(Nicaragua)

Operative paragraph 18

Delete the paragraph. **275**

(India)

Amend to read as follows:

18. *Urges* parliaments to help foster a true “culture of cybersecurity” by developing educational curricula focused on training future generations, from childhood onwards, in ~~the correct use of~~ **digital literacy and** technological ~~devices~~ **know-how**, covering both the great opportunities they present and the serious risks they pose; **276**

(Thailand)

New operative paragraph 18bis

18bis. *Also urges* parliaments, in all their activities related to combating cybercrime and malicious cyber incidents, to promote obligations under international human rights law and full respect for human rights and fundamental freedoms and the rule of law; **277**

(Canada)

Operative paragraph 19

Delete the paragraph. **278**

(Islamic Republic of Iran)

Amend to read as follows:

19. *Recommends* that parliaments broaden protections for ~~women, young people and other~~ vulnerable groups, **especially children and the elderly,** 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; **279**

(Germany)

Amend to read as follows:

19. *Recommends* that parliaments broaden protections for women, ~~young people~~ **children, the elderly** and other vulnerable groups in cyberspace, taking **into account** 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; **280**

(Czech Republic)

Amend to read as follows:

19. *Recommends* that parliaments broaden protections for women, young **and elderly** people, **children** and other vulnerable groups 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; **281**

(Viet Nam)

Amend to read as follows:

19. *Recommends* that parliaments broaden protections for women, **children,** young people and other vulnerable groups 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; **282**

(Romania)

Amend to read as follows:

19. *Recommends* that parliaments broaden protections for women, young people**, the elderly** and other vulnerable groups 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; **283**

(Türkiye)

Amend to read as follows:

19. *Recommends* that parliaments broaden protections for women, young people**, racialized communities** and other vulnerable groups 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; **284**

(Canada)

Amend to read as follows:

19. *Recommends* that parliaments broaden protections for women, young people**, persons with disabilities** and other vulnerable groups 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; **285**

(Finland)

New operative paragraph 19bis

19bis. *Calls on* parliaments to convene a multi-stakeholder collaboration between government and the private sector in order to institutionalize technology as a tool to raise awareness about sexual harassment and to combat cyber violence against women and children; **286**

(Philippines)

Operative paragraph 20

Delete the paragraph. **287**

(India)

Amend to read as follows:

20. *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~~ **prevent interference in a State's internal affairs through the use of information and communications technologies**; **288**

(Russian Federation)

Operative paragraph 21

Delete the paragraph. **289**

(India, Islamic Republic of Iran)

Amend to read as follows:

21. *Calls upon* the international community to take action to protect ~~democracy~~ **the information and communications technology systems of government authorities** 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 national infrastructure and essential services; **290**

(Russian Federation)

Amend to read as follows:

21. *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 ~~national~~ **civilian** infrastructure and essential services; **291**

(Sweden)

New operative paragraph 21bis

21bis. *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; **292**

(Romania)

Operative paragraph 22

Amend to read as follows:

22. *Calls upon* parliaments to deepen their understanding of the complex and rapid nature of ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** and ~~cyberattacks~~ **ICT threats** by holding specialized seminars, workshops and conferences on this subject; **293**

(Islamic Republic of Iran)

Amend to read as follows:

22. *Calls upon* parliaments to deepen their understanding of the complex and rapid nature of cybercrime and ~~cyberattacks~~ **cyber incidents** by holding specialized seminars, workshops and conferences on this subject; **294**

(India)

Amend to read as follows:

22. *Calls upon* parliaments to deepen their understanding of the complex and rapid nature of ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks by holding specialized seminars, workshops and conferences on this subject; **295**

(Pakistan)

Amend to read as follows:

22. *Calls upon* parliaments to deepen their understanding of the complex and ~~rapid~~ **rapidly evolving** nature of cybercrime ~~and cyberattacks~~ by holding specialized seminars, workshops and conferences on this subject; **296**

(Sweden)

Amend to read as follows:

22. Calls upon parliaments to deepen their understanding of the complex and rapid nature of cybercrime and cyberattacks by **enabling the open sharing of knowledge, experience and expertise by** holding specialized seminars, workshops and conferences on this subject; **297**

(South Africa)

Amend to read as follows:

22. *Calls upon* parliaments to deepen their understanding of the complex and rapid nature of cybercrime and cyberattacks by holding specialized seminars, workshops and conferences on this subject**, where they do not yet exist in their country**; **298**

(Nicaragua)

Operative paragraph 23

Delete the paragraph. **299**

(Russian Federation)

Amend to read as follows:

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; **300**

(Belgium)

Amend to read as follows:

23. *Invites* the IPU Secretariat, in partnership with other relevant organizations, to promote this new vision of ~~cybersecurity~~ **ICT security** by supporting parliaments in their capacity-building endeavours; **301**

(Islamic Republic of Iran)

Amend to read as follows:

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**, and to set its strategic goal in encouraging parliaments to create in-house cybersecurity intelligence centres for sharing and exchanging their information, intelligence, expertise and best practices, with a view to expanding common knowledge of cybersecurity**; **302**

(Thailand)

Operative paragraph 24

Amend to read as follows:

24. *Recommends* that the IPU~~, as the global organization of parliaments, play a leading role in international internet governance and 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, in order to anticipate, prepare for, resist, respond to and recover from any cyber threat to the security, livelihood or way of life of the people~~ **contribute to the internationalization of internet management, to the equal participation of all States in this process, and to the preservation of the sovereign right of States to regulate the national segment of the global internet network**. **303**

(Russian Federation)

Amend to read as follows:

24. *Recommends* that the IPU, as the global organization of parliaments, play a leading role in ~~international internet governance~~ **preventing and combating cybercrime** and **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, in order to anticipate, prepare for, resist, respond to and recover from any cyber threat to the security, livelihood, **human rights** or way of life of the people. **304**

(Belgium)

Amend to read as follows:

24. *Recommends* that the IPU, as the global organization of parliaments, play a leading role in international internet governance and cyber resilience by ~~participating in all~~ **strengthening partnerships with** relevant international forums, including those led by the United Nations, with a view to ensuring that the voice of parliaments is heard, in order to anticipate, prepare for, resist, respond to and recover from any cyber threat to the security, livelihood or way of life of the people. **305**

(Republic of Korea)

Amend to read as follows:

24. *Recommends* that the IPU, as the global organization of parliaments, play a leading role in international internet governance and 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~~, in order to anticipate, prepare for, resist, respond to and recover from any cyber threat to the security, livelihood or way of life of the people~~. **306**

(France)

Amend to read as follows:

24. *Recommends* that the IPU, as the global organization of parliaments, play a leading role in international internet governance and 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, in order to anticipate, prepare for, resist, respond to and recover from any ~~cyber~~ **ICT** threat to the security, livelihood or way of life of the people. **307**

(Islamic Republic of Iran)

Amend to read as follows:

24. *Recommends* that the IPU, as the global organization of parliaments, play a leading role in international internet governance and 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, in order to anticipate, prepare for, resist, respond to and recover from any cyber threat to the security, livelihood or way of life of the people**, after consultation with the States Parties**. **308**

(Nicaragua)

New operative paragraph 24bis

24bis. *Promotes* the creation of a working group on cyberattacks and cybercrime, under 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 national Member Parliaments in terms of law-making, oversight and budgeting; **309**

(Argentina)

24bis. ***Also recommends*** **that the IPU raise awareness among parliaments on achieving the SDGs through, above all else, their universal commitments to digital security.** **310**

(Thailand)

New operative paragraph 24ter

24ter. ***Urges*** **international organizations to discuss a convention on acts of cyberwar within the framework of maintaining international peace and security**. **311**

(Argentina)

TITLE

Modify the title as follows:

~~Cyberattacks and~~ ~~cybercrimes~~ **Cybercrimes**: The new risks to global security **312**

(Czech Republic)

Modify the title as follows:

~~Cyberattacks and~~ ~~cybercrimes~~ **Cyber incidents and cyber crimes**: The new risks to global security **313**

(India)

Modify the title as follows:

~~Cyberattacks and~~ ~~cybercrimes~~ **ICT threat and the use of information and communications technologies for criminal purposes**: The new risks to global security **314**

(Islamic Republic of Iran)

Modify the title as follows:

Cyberattacks and cybercrimes: The ~~new~~ **increased** risks to global security **315**

(Lithuania)

Modify the title as follows:

Cyberattacks and ~~cybercrimes~~ **misuse of ICT for criminal purposes**: The new risks to global security **316**

(Pakistan)

Modify the title as follows:

~~Cyberattacks and cybercrimes~~ **Cybercrimes**: The ~~new~~ **evolving** risks to global security **317**

(Sweden)