146TH IPU ASSEMBLY
المنامة، البحرين
MANAMA, BAHRAIN
11-15 MARCH 2023 - ١٥-١١ 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
17 كانون الثاني/يناير 2023

الهجمات والجرائم الإلكترونية:
المخاطر الجديدة على الأمن العالمي

مشروع قرار مقدم من قبل المقرّرَين المشاركَين

السيد ج. سيبيدا (إسبانيا)، وسعادة السيدة سارة فلكناز (دولة الإمارات العربية المتحدة)

إن الجمعية العامة الـ146 للاتحاد البرلماني الدولي،

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

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

(3) *وإذ تلاحظ* تزايد الاعتماد على الفضاء الإلكتروني بين الأفراد والمؤسسات والدول،

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

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

(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 استعمال تكنولوجيا المعلومات لأغراض إجرامية، القرار 239/57 المؤرخ 31 كانون

ترجمة الأمانة العامة للاتحاد البرلماني العربي

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،

(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،

(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،

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

(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 هذه الاتفاقية،

(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،

(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 وحماية السلام والأمن والاستقرار الاقتصادي على الصعيد العالمي،

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

(14) *وإذ تعترف أيضاً* بالحاجة إلى اتخاذ إجراءات برلمانية دولية مشتركة لتوفير درع وقائي للمواطنين والحكومات والدول، وجميعهم جهات معنية في هذه المهمة،

(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،

(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،

(17) *وإذ تلاحظ أيضاً* أن الجرائم والهجمات الإلكترونية لا تشملان الهجمات على تكنولوجيات المعلومات والاتصالات فحسب، وانتهاكات الخصوصية، وإنشاء البرامج الضارة ونشرها، ولكن أيضاً الهجمات على البنية التحتية الأساسية، 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،

(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،

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؛
2. *وتشجع* البرلمانات على دعوة حكوماتها إلى دعم جهود الأمم المتحدة الرامية إلى سن اتفاقية جديدة بشأن الجرائم الإلكترونية من خلال المشاركة بنشاط في صياغتها؛
3. *وتحث* البرلمانات وحكوماتها على أن تدرج في الاتفاقية تعاريف شاملة للجرائم والهجمات الإلكترونية، إلى جانب آليات تدعم التعاون الدولي لمكافحة الجرائم والهجمات الإلكترونية؛
4. *وتدعو* البرلمانات وحكوماتها إلى استخدام هذه الاتفاقية، بمجرد اعتمادها، كوسيلة لتعزيز التشريعات الوطنية وزيادة التعاون الدولي لمكافحة الجرائم والهجمات الإلكترونية؛

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

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؛

7. *وتوصي بشدة* بأن تضع البرلمانات أطراً تشريعية ترمي إلى حماية البنية التحتية الأساسية 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؛

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 لمساعدتها في منع وقوع حوادث في المستقبل، وعلى وجه الخصوص دعم وحماية جميع فرق الاستجابة للحوادث الإلكترونية داخل حدودها وخارجها؛

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؛

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

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 البنية التحتية الأساسية والمؤسسات العامة والشركات والمواطنين؛

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؛

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؛

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

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؛

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

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؛

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 الصحيح للأجهزة التكنولوجية، تغطي كلا من الفرص الكبيرة التي تتيحها والمخاطر الجسيمة التي تشكلها؛

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

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 التي تسعى إلى التأثير في حرية تشكيل الرأي العام أو تغييره أو انتهاكه أثناء العملية الانتخابية؛

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 البنية التحتية الوطنية الأساسية، والخدمات الأساسية؛

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

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

24. *وتوصي* بأن يقوم الاتحاد البرلماني الدولي، بوصفه المنظمة العالمية للبرلمانات، الاضطلاع بدور قيادي في 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.

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
17 January 2023

Cyberattacks and cybercrimes: The new risks to global security

***Draft resolution* submitted by the co-Rapporteurs**
Mr. J. Cepeda (Spain) and Ms. S. Falaknaz (United Arab Emirates)

The 146th Assembly of the Inter-Parliamentary Union,

(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,

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

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

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

(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,

(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*,

(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,

(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,

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

(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 this convention,

(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,

(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,

(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,

(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,

(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,

(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,

(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,

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

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;

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

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;

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;

5. *Calls upon* parliaments to enact 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;

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;

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;

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 assist them in preventing future incidents, and in particular to support and protect all cyber incident response teams within and beyond their borders;

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;

10. *Recommends* that parliaments establish 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;

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;

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;

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;

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

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

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

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;

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 technological devices, covering both the great opportunities they present and the serious risks they pose;

19. *Recommends* that parliaments broaden protections for women, 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;

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;

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 infrastructure and essential services;

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;

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

24. *Recommends* that the IPU, as the global organization of parliaments, play a leading role in 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.