Union interparlementaire
Pour la démocratie. Pour tous.

146e ASSEMBLÉE DE L'UIP
المنامـــة، البحريـــن
MANAMA, BAHREÏN
11-15 MARS 2023 - ١١-١٥ مـارس ٢٠٢٣

146e Assemblée de l'UIP

Manama (11-15 mars 2023)

Commission permanente
de la paix et de la sécurité internationale

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

Cyberattaques et cybercriminalité : les nouveaux risques pour la sécurité mondiale

<u>Amendements au projet de résolution</u> présentés dans les délais statutaires par les délégations de l'Afrique du Sud, de l'Allemagne, de l'Argentine, de la Belgique, du Canada, de l'Égypte, de la Fédération de Russie, de la Finlande, de la France, de l'Inde, de l'Iran (République islamique d'), du Japon, de la Lituanie, du Nicaragua, du Pakistan, des Philippines, de la République de Corée, de la République tchèque, de la Roumanie, de Singapour, du Soudan du Sud, de la Suède, de la Suisse, de la Thaïlande, de la Türkiye, de l'Ukraine et du Viet Nam

PRÉAMBULE

<u>Alinéa 1</u>

Modifier l'alinéa existant comme suit :

1) *condamnant* toutes les formes ~~de cybercriminalité~~ **d'utilisation des technologies de l'information et de la communication à des fins criminelles** et de cyberattaques et *réaffirmant* la nécessité de lutter contre ces actes par la coopération internationale et l'élaboration de cadres ~~juridiques~~ **internationaux juridiquement contraignants** adaptés **aux caractéristiques spécifiques des technologies de l'information et de la communication (TIC)**, **1**

(Iran, République islamique d')

Modifier l'alinéa existant comme suit :

1) *condamnant* toutes les formes de ~~cybercriminalité~~ **détournement des TIC à des fins criminelles** et de cyberattaques et *réaffirmant* la nécessité de lutter contre ces actes par la coopération internationale et l'élaboration de cadres juridiques adaptés, **2**

(Pakistan)

Modifier l'alinéa existant comme suit :

1) *condamnant* toutes les formes ~~de~~ **d'utilisation des technologies de l'information et de la communication à des fins criminelles, ci-après dénommées "**cybercriminalité**"** et ~~de~~ **d'attaques informatiques, ci-après dénommées "**cyberattaques**"** et *réaffirmant* la nécessité de lutter contre ces actes par la coopération internationale et l'élaboration de cadres juridiques adaptés, **3**

(Fédération de Russie)

Modifier l'alinéa existant comme suit :

1) *condamnant* toutes les formes de cybercriminalité ~~et de cyberattaques~~ et *réaffirmant* la nécessité de lutter contre ces actes par la coopération internationale et l'élaboration de cadres juridiques adaptés, **4**

(République tchèque, Suède)

Modifier l'alinéa existant comme suit :

1) *condamnant* toutes les formes de cybercriminalité et de ~~cyberattaques~~ **cyberincidents** et *réaffirmant* la nécessité de lutter contre ces actes par la coopération internationale et l'élaboration de cadres juridiques adaptés, **5**

(Inde)

Modifier l'alinéa existant comme suit :

1) *condamnant* toutes les formes de cybercriminalité et de cyberattaques **malveillantes** et *réaffirmant* la nécessité de lutter contre ces ~~actes~~ **infractions** par la coopération internationale et l'élaboration de cadres juridiques adaptés, **6**

(Belgique)

Modifier l'alinéa existant comme suit :

1) *condamnant* toutes les formes de cybercriminalité et de cyberattaques ~~et *réaffirmant* la nécessité de lutter contre ces actes par la coopération internationale et l'élaboration de cadres juridiques adaptés~~ **ainsi que tous les crimes odieux qui y sont associés**, **7**

(Soudan du Sud)

Modifier l'alinéa existant comme suit :

1) *condamnant* toutes les formes de cybercriminalité et de cyberattaques et *réaffirmant* la nécessité de lutter contre ces actes par la coopération internationale ~~et l'élaboration de cadres juridiques adaptés~~, **8**

(Allemagne)

Modifier l'alinéa existant comme suit :

1) *condamnant* toutes les formes de cybercriminalité et de cyberattaques et *réaffirmant* la nécessité de lutter contre ces actes par la coopération internationale et ~~l'élaboration de cadres juridiques~~ **de débats** adaptés **sur les questions d'ordre juridique**, **9**

(Japon)

Modifier l'alinéa existant comme suit :

1) *condamnant* toutes les formes de cybercriminalité et de cyberattaques et *réaffirmant* la nécessité de lutter contre ces actes par la coopération internationale **et la coordination entre les parties prenantes au sein des pays et entre eux, notamment par le partage d'informations sur les menaces de cybercriminalité,** et l'élaboration de cadres juridiques adaptés, **10**

(Afrique du Sud)

Modifier l'alinéa existant comme suit :

1) *condamnant* toutes les formes de cybercriminalité et de cyberattaques et *réaffirmant* la nécessité de lutter contre ces actes par la coopération internationale et **l'application ou, le cas échéant,** l'élaboration de cadres juridiques adaptés, **11**

(Suisse)

Modifier l'alinéa existant comme suit :

1) *condamnant* toutes les formes de cybercriminalité et de cyberattaques et *réaffirmant* la nécessité de lutter contre ces actes par la coopération internationale et l'élaboration de cadres juridiques adaptés **qui reflètent le système international fondé sur des règles**, **12**

(Canada)

Nouvel alinéa 1bis

1bis) *reconnaissant* que la cybercriminalité et les cyberattaques sont des phénomènes distincts mais interdépendants, de nature criminelle et propres à l'ère numérique, associés à divers types d'utilisation malveillante des technologies de l'information et de la communication, **13**

(Argentine)

1bis) *réaffirmant* le cadre de l'ONU relatif au comportement responsable des États dans l'utilisation des TIC et la nécessité de mettre en œuvre ce cadre, **14**

(Allemagne)

1bis) *affirmant* la nécessité de lutter contre ces actes par la coopération nationale, régionale et internationale et par l'élaboration de cadres juridiques adaptés, **15**

(Soudan du Sud)

Alinéa 2

Modifier l'alinéa existant comme suit :

2) *considérant* qu'il faut instaurer la confiance entre les pays ~~face aux cybercriminels, lesquels ne connaissent ni frontières ni limites~~ **pour lutter contre les risques qui pèsent sur la cybersécurité**, **16**

(Inde)

Modifier l'alinéa existant comme suit :

2) *considérant* qu'il faut instaurer la confiance entre les pays face ~~aux cybercriminels~~ **à l'utilisation malveillante des TIC par des acteurs étatiques et non étatiques**, lesquels ne connaissent ni frontières ni limites, **17**

(Allemagne)

Modifier l'alinéa existant comme suit:

(2) *considérant* qu'il faut instaurer la confiance entre les pays face aux cybercriminels **et aux acteurs malveillants**, lesquels ne connaissent ni frontières ni limites, **18**

(Iran, République islamique d')

Modifier l'alinéa existant comme suit :

2) *considérant* qu'il faut instaurer la confiance **et la compréhension mutuelle** entre les pays face aux cybercriminels, lesquels ne connaissent ni frontières ni limites, **19**

(Thaïlande)

Alinéa 3

Modifier l'alinéa existant comme suit :

3) *constatant* **le recours et** la dépendance ~~croissante~~ **croissants** ~~des personnes, des institutions et des pays à l'égard du cyberespace~~ **aux TIC à travers le monde**, **20**

(Allemagne)

Modifier l'alinéa existant comme suit :

3) *constatant* la dépendance croissante des personnes, des institutions et des pays à l'égard ~~du cyberespace~~ **de l'environnement des TIC**, **21**

(Iran, République islamique d')

Modifier l'alinéa existant comme suit :

3) *constatant* la dépendance croissante des personnes, des institutions et des pays à l'égard ~~du~~ **de l'environnement dans lequel sont utilisées les technologies de l'information et de la communication, ci-après dénommé "**cyberespace**"**, **22**

(Fédération de Russie)

Alinéa 4

Modifier l'alinéa existant comme suit :

4) *consciente* de l'augmentation de ~~la cybercriminalité~~ **l'utilisation des technologies de l'information et de la communication à des fins criminelles** et ~~des cyberattaques~~ **de la menace que représentent les TIC** ~~liée à~~ **en raison de** l'accélération de la transformation numérique, notamment celle imposée par la pandémie de COVID-19, **23**

(Iran, République islamique d')

Modifier l'alinéa existant comme suit :

4) *consciente* de l'augmentation ~~de la cybercriminalité~~ **du détournement des TIC à des fins criminelles** et des cyberattaques liée à l'accélération de la transformation numérique, notamment celle imposée par la pandémie de COVID-19, **24**

(Pakistan)

Modifier l'alinéa existant comme suit :

4) *consciente* de l'augmentation de la cybercriminalité ~~et des cyberattaques~~ liée à l'accélération de la transformation numérique~~, notamment celle imposée par~~ **pendant et après** la pandémie de COVID-19, **25**

(République tchèque)

Modifier l'alinéa existant comme suit :

4) *consciente* de l'augmentation de la cybercriminalité ~~et des cyberattaques~~ **et de son utilisation croissante dans les opérations de cyberguerre, par exemple avec les rançongiciels utilisés pour mener des cyberattaques destructrices contre des infrastructures civiles essentielles,** liée à l'accélération de la transformation numérique, notamment celle imposée par la pandémie de COVID-19, **26**

(Suède)

Modifier l'alinéa existant comme suit :

4) *consciente* de l'augmentation de la cybercriminalité et des ~~cyberattaques~~ **cyberincidents** liée à l'accélération de la transformation numérique, notamment ~~celle imposée par~~ **depuis le début de** la pandémie de COVID-19, **27**

(Inde)

Modifier l'alinéa existant comme suit :

4) *consciente* de l'augmentation ~~de la~~ **des activités de** cybercriminalité et des cyberattaques liée à l'accélération de la transformation numérique, ~~notamment celle imposée~~ **accentuée** par la pandémie de COVID-19, **28**

(Allemagne)

Modifier l'alinéa existant comme suit :

4) *consciente* de l'augmentation de la cybercriminalité et des cyberattaques **malveillantes** liée à l'accélération de la transformation numérique, notamment celle imposée par la pandémie de COVID-19, **29**

(Belgique)

Aucune incidence sur le français **30**

(Lituanie)

Amend to read as follows:

4) *consciente* de l'augmentation de la cybercriminalité et des cyberattaques **contre les infrastructures vitales des États et des entreprises qui fournissent des services essentiels aux citoyens, et contre le bien-être des personnes,** liée à l'accélération de la transformation numérique, notamment celle imposée par la pandémie de COVID-19, **31**

(Afrique du Sud)

Nouvel alinéa 4bis

4bis) *consciente* également des difficultés rencontrées par les États dans la lutte contre les cyberattaques et la cybercriminalité, et *soulignant* la nécessité de renforcer, sur demande, les activités d'assistance technique et de renforcement des capacités afin d'accroître la capacité des autorités nationales à lutter contre les cyberattaques et la cybercriminalité, **32**

(Afrique du Sud)

Alinéa 5

Modifier l'alinéa existant comme suit :

5) *prenant note* de la responsabilité des parlements de protéger les citoyens dans ~~le cyberespace~~ **l'environnement des TIC** à l'aide de nouvelles infrastructures et ressources, de la même manière que dans le monde physique, **33**

(Iran, République islamique d')

Modifier l'alinéa existant comme suit :

5) *prenant note* de la responsabilité des parlements de protéger les citoyens dans le cyberespace ~~à l'aide de nouvelles infrastructures et ressources,~~ de la même manière que dans le monde physique, **34**

(Inde)

Modifier l'alinéa existant comme suit :

5) *prenant note* de la responsabilité des parlements de ~~protéger~~ **mettre en place un cadre réglementaire qui protège** les citoyens dans le cyberespace à l'aide de nouvelles infrastructures et ressources, de la même manière que dans le monde physique, **35**

(Argentine)

Modifier l'alinéa existant comme suit :

5) *prenant note* de la responsabilité des parlements ~~de protéger les~~ **d'assurer la protection de leurs** citoyens dans le cyberespace à l'aide de nouvelles infrastructures et ressources, de la même manière que dans le monde physique, **36**

(Thaïlande)

Modifier l'alinéa existant comme suit :

5) *prenant note* ~~de la responsabilité~~ **du rôle** des parlements ~~de~~ **pour ce qui est de** protéger les citoyens dans le cyberespace à l'aide de nouvelles infrastructures et ressources, de la même manière que dans le monde physique, **37**

(Lituanie)

Modifier l'alinéa existant comme suit :

5) *prenant note* de la responsabilité des parlements de protéger les citoyens dans le cyberespace à l'aide de nouvelles infrastructures et ressources, de la même manière que dans le monde physique, **lorsqu'elles n'existent pas encore dans leur pays,** **38**

(Nicaragua)

Nouvel alinéa 5bis

5bis) *consciente* que, compte tenu du rythme de l'évolution technologique dans le monde, de nouveaux cadres politiques et juridiques complets doivent également être élaborés rapidement, **39**

(Philippines)

(5bis) *réaffirmant* que l'ONU doit jouer un rôle moteur dans la facilitation du dialogue sur l'utilisation des technologies de l'information et de la communication par les États, conformément à la résolution 76/19 de l'Assemblée générale des Nations Unies, **40**

(Fédération de Russie)

5bis) *soulignant* la dépendance à l'égard des plateformes et infrastructures technologiques numériques, ainsi que le risque de cyberattaques, lorsque les gouvernements déploient des applications de service public en ligne, **41**

(Viet Nam)

Nouvel alinéa 5ter

5ter) *soutenant* le Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), et *reconnaissant* son mandat conformément à la résolution 75/240 de l'Assemblée générale des Nations Unies, **42**

(Fédération de Russie)

5ter) *affirmant* que la protection des droits de l'homme dans le cybermonde est similaire à celle du monde réel, conformément aux engagements internationaux pris par les États membres de l'ONU, **43**

(Viet Nam)

Alinéa 6

Modifier l'alinéa existant comme suit :

6) *rappelant* le résolutions suivantes de l'Assemblée générale des Nations Unies : 31/72 du 10 décembre 1976 intitulée *Convention sur l'interdiction d'utiliser des techniques de modification de l'environnement à des fins militaires ou toutes autres fins hostiles*, 55/63 du 4 décembre 2000 et 56/121 du 19 décembre 2001 intitulées *Lutte contre l'exploitation des technologies de l'information à des fins criminelles*, ~~57/239 du 31 janvier 2003 intitulée *Création d'une culture mondiale de la cybersécurité*~~, ~~et~~ **ainsi que les résolutions** 69/28 du 2 décembre 2014**, 70/237 du 23 décembre 2015, 71/28 du 5 décembre 2016, 73/27 du 5 décembre 2018, 74/29 du 12 décembre 2019, 75/240 du 31 décembre 2020 et 77/36 du 7 décembre 2022** ~~intitulée~~ **intitulées** *Progrès de l'informatique et des télécommunications et sécurité internationale*, **et la résolution 76/19 du 6 décembre 2021 intitulée *Progrès de l'informatique et des télécommunications et sécurité internationale, et promotion du comportement responsable des États dans l'utilisation du numérique*,** **44**

(Fédération de Russie)

Modifier l'alinéa existant comme suit :

6) *rappelant* les résolutions suivantes de l'Assemblée générale des Nations Unies : 31/72 du 10 décembre 1976 intitulée *Convention sur l'interdiction d'utiliser des techniques de modification de l'environnement à des fins militaires ou toutes autres fins hostiles*, 55/63 du 4 décembre 2000 et 56/121 du 19 décembre 2001 intitulées *Lutte contre l'exploitation des technologies de l'information à des fins criminelles*, 57/239 du 31 janvier 2003 intitulée *Création d'une culture mondiale de la cybersécurité*, ~~et 69/28 du 2 décembre 2014~~ **76/19 du 6 décembre 2021** intitulée ~~*Progrès de la téléinformatique dans le contexte de la sécurité internationale*~~ ***Progrès de l'informatique et des télécommunications et sécurité internationale, et promotion du comportement responsable des États dans l'utilisation du numérique,* 77/36 du 7 décembre 2022 intitulée *Progrès de l'informatique et des télécommunications et sécurité internationale*, et 77/37 du 7 décembre 2022 intitulée *Programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale*,** **45**

(Égypte)

Modifier l'alinéa existant comme suit :

6) *rappelant* les résolutions suivantes de l'Assemblée générale des Nations Unies : 31/72 du 10 décembre 1976 intitulée *Convention sur l'interdiction d'utiliser des techniques de modification de l'environnement à des fins militaires ou toutes autres fins hostiles*, 55/63 du 4 décembre 2000 et 56/121 du 19 décembre 2001 intitulées *Lutte contre l'exploitation des technologies de l'information à des fins criminelles*, 57/239 du 31 janvier 2003 intitulée *Création d'une culture mondiale de la cybersécurité*, ~~et~~ **ainsi que les résolutions** 69/28 du 2 décembre 2014**, 73/27 du 5 décembre 2018, 75/240 du 31 décembre 2020 et 77/36 du 7 décembre 2022 intitulées** *Progrès de l'informatique et des télécommunications et sécurité internationale*, **46**

(Iran, République islamique d')

Modifier l'alinéa existant comme suit :

6) *rappelant* les résolutions suivantes de l'Assemblée générale des Nations Unies : 31/72 du 10 décembre 1976 intitulée *Convention sur l'interdiction d'utiliser des techniques de modification de l'environnement à des fins militaires ou toutes autres fins hostiles*, 55/63 du 4 décembre 2000 et 56/121 du 19 décembre 2001 intitulées *Lutte contre l'exploitation des technologies de l'information à des fins criminelles*, 57/239 du 31 janvier 2003 intitulée *Création d'une culture mondiale de la cybersécurité*, et 69/28 du 2 décembre 2014 intitulée *Progrès de la téléinformatique dans le contexte de la sécurité internationale*, **ainsi que les rapports finaux consensuels de 2021 du Groupe de travail à composition non limitée des Nations Unies chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, et du Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale,** **47**

(Allemagne)

Modifier l'alinéa existant comme suit :

6) *rappelant* les résolutions suivantes de l'Assemblée générale des Nations Unies : 31/72 du 10 décembre 1976 intitulée *Convention sur l'interdiction d'utiliser des techniques de modification de l'environnement à des fins militaires ou toutes autres fins hostiles*, 55/63 du 4 décembre 2000 et 56/121 du 19 décembre 2001 intitulées *Lutte contre l'exploitation des technologies de l'information à des fins criminelles*, 57/239 du 31 janvier 2003 intitulée *Création d'une culture mondiale de la cybersécurité*, et 69/28 du 2 décembre 2014 intitulée *Progrès de la téléinformatique dans le contexte de la sécurité internationale*, **ainsi que la résolution 73/266 du 22 décembre 2018 intitulée *Favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale***, **48**

(Thaïlande)

Nouvel alinéa 6bis

6bis) *rappelant aussi* la résolution 70/237 de l'Assemblée générale des Nations Unies du 23 décembre 2015, également intitulée *Progrès de l'informatique et des télécommunications et sécurité internationale*, qui approuve la mise en place de normes facultatives et non contraignantes de comportement responsable des États en matière d'utilisation des technologies de l'information et de la communication élaborées par le Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, et invite les États membres à s'inspirer de ces normes, **49**

(Canada)

Alinéa 7

Modifier l'alinéa existant comme suit :

7) *soulignant* l'importance des conventions régionales sur ~~la cybercriminalité, la criminalité transnationale organisée~~ **l'utilisation des technologies de l'information et de la communication à des fins criminelles~~,~~ et sur** l'échange d'informations et l'assistance administrative, notamment la *Convention sur la cybercriminalité* du Conseil de l'Europe du 23 novembre 2001 et son *Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques* du 28 janvier 2003, l'*Accord de coopération visant à assurer la sécurité internationale de l'information entre les États membres de l'Organisation de coopération de Shanghai* du 16 juin 2009, et la *Convention arabe sur la lutte contre les infractions liées aux technologies de l'information* du 21 décembre 2010, **50**

(Iran, République islamique d')

Modifier l'alinéa existant comme suit :

7) *soulignant* l'importance des conventions régionales sur ~~la cybercriminalité~~ **le détournement des TIC à des fins criminelles**, la criminalité transnationale organisée, l'échange d'informations et l'assistance administrative, notamment la *Convention sur ~~la~~ cybercriminalité* du Conseil de l'Europe du 23 novembre 2001 et son *Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques* du 28 janvier 2003, l'*Accord de coopération visant à assurer la sécurité internationale de l'information entre les États membres de l'Organisation de coopération de Shanghai* du 16 juin 2009, et la *Convention arabe sur la lutte contre les infractions liées aux technologies de l'information* du 21 décembre 2010, **51**

(Pakistan)

Modifier l'alinéa existant comme suit :

7) *soulignant* l'importance des conventions régionales sur la cybercriminalité, la criminalité transnationale organisée, l'échange d'informations et l'assistance administrative, ~~notamment la *Convention sur la cybercriminalité* du Conseil de l'Europe du 23 novembre 2001 et son *Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques* du 28 janvier 2003, l'*Accord de coopération visant à assurer la sécurité internationale de l'information entre les États membres de l'Organisation de coopération de Shanghai* du 16 juin 2009, et la *Convention arabe sur la lutte contre les infractions liées aux technologies de l'information* du 21 décembre 2010,~~ **52**

(Inde)

Modifier l'alinéa existant comme suit :

7) ~~*soulignant* l'importance~~ ***prenant note*** des conventions régionales sur la cybercriminalité, la criminalité transnationale organisée, l'échange d'informations et l'assistance administrative, notamment la *Convention sur la cybercriminalité* du Conseil de l'Europe du 23 novembre 2001 et son *Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques* du 28 janvier 2003, l'*Accord de coopération visant à assurer la sécurité internationale de l'information entre les États membres de l'Organisation de coopération de Shanghai* du 16 juin 2009, et la *Convention arabe sur la lutte contre les infractions liées aux technologies de l'information* du 21 décembre 2010, **53**

(Singapour)

7) *soulignant* l'importance des conventions **internationales et** régionales **existantes** sur la cybercriminalité, la criminalité transnationale organisée, l'échange d'informations et l'assistance administrative, notamment **la *Convention contre la criminalité transnationale organisée* des Nations Unies du 15 novembre 2000, la *Convention contre la corruption* des Nations Unies du 31 octobre 2003,** la *Convention sur la cybercriminalité* du Conseil de l'Europe du 23 novembre 2001 et son *Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques* du 28 janvier 2003, l'*Accord de coopération visant à assurer la sécurité internationale de l'information entre les États membres de l'Organisation de coopération de Shanghai* du 16 juin 2009, et la *Convention arabe sur la lutte contre les infractions liées aux technologies de l'information* du 21 décembre 2010, **54**

(Belgique)

Modifier l'alinéa existant comme suit :

7) *soulignant* l'importance des conventions régionales sur la cybercriminalité, la criminalité transnationale organisée, l'échange d'informations et l'assistance administrative, notamment la *Convention sur la cybercriminalité* du Conseil de l'Europe du 23 novembre 2001 et son *Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques* du 28 janvier 2003, l'*Accord de coopération visant à assurer la sécurité internationale de l'information entre les États membres de l'Organisation de coopération de Shanghai* du 16 juin 2009, et la *Convention arabe sur la lutte contre les infractions liées aux technologies de l'information* du 21 décembre 2010, **ainsi que les lois types du Parlement de l'Amérique latine et des Caraïbes (Parlatino) sur la cybercriminalité (novembre 2013) et ses mises à jour, la prévention sociale de la violence et de la criminalité (novembre 2015), la criminalité informatique (février 2021) et la lutte contre le commerce illicite et la criminalité transnationale (février 2021),** **55**

(Argentine)

Modifier l'alinéa existant comme suit :

7) *soulignant* l'importance des conventions régionales sur la cybercriminalité, la criminalité transnationale organisée, l'échange d'informations et l'assistance administrative, notamment la *Convention sur la cybercriminalité* du Conseil de l'Europe du 23 novembre 2001 et son *Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques* du 28 janvier 2003, l'*Accord de coopération visant à assurer la sécurité internationale de l'information entre les États membres de l'Organisation de coopération de Shanghai* du 16 juin 2009, et la *Convention arabe sur la lutte contre les infractions liées aux technologies de l'information* du 21 décembre 2010, **l'*Accord de coopération entre les États membres de la Communauté d'États indépendants concernant la garantie de la sécurité de l'information* du 20 novembre 2013, et l'*Accord de coopération entre les États membres de la Communauté d'États indépendants relatif à la lutte contre la criminalité dans le domaine des technologies de l'information* du 28 septembre 2018,** **56**

(Fédération de Russie)

Modifier l'alinéa existant comme suit :

7) *soulignant* l'importance des conventions régionales sur la cybercriminalité, la criminalité transnationale organisée, l'échange d'informations et l'assistance administrative, notamment la *Convention sur la cybercriminalité* du Conseil de l'Europe du 23 novembre 2001 et son *Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques* du 28 janvier 2003, l'*Accord de coopération visant à assurer la sécurité internationale de l'information entre les États membres de l'Organisation de coopération de Shanghai* du 16 juin 2009, et la *Convention arabe sur la lutte contre les infractions liées aux technologies de l'information* du 21 décembre 2010 **et la *Convention sur la cybersécurité et la protection des données personnelles* de l'Union africaine du 27 juin 2014**, **57**

(Afrique du Sud)

Nouvel alinéa 7bis

7bis) *soulignant également* que la *Convention sur la cybercriminalité* du Conseil de l'Europe du 23 novembre 2001 (la "Convention de Budapest"), qui est ouverte à l'adhésion de tous les pays, est devenue un instrument d'importance mondiale qui compte des États parties de toutes les régions du monde et a un impact sur ces derniers, **58**

(Roumanie)

Alinéa 8

Modifier l'alinéa existant comme suit :

8) *rappelant* les travaux de l'UIP sur les différents nouveaux risques auxquels sont exposées nos sociétés de plus en plus numérisées, notamment les résolutions de l'UIP intitulées *La cyber-guerre : une grave menace pour la paix et la sécurité mondiale* (adoptée le 1er avril 2015 lors de la 132e Assemblée, à Hanoï) et *Législation dans le monde pour la lutte contre l'exploitation et les abus sexuels en ligne à l'égard des enfants* (adoptée le 30 novembre 2021 lors de la 143e Assemblée, à Madrid), ~~laquelle rappelle également la Convention du Conseil de l'Europe intitulée *La protection des enfants contre l'exploitation et les abus sexuels* (Convention de Lanzarote) du 25 octobre 2007,~~ **59**

(Inde)

Modifier l'alinéa existant comme suit :

8) *rappelant* les travaux de l'UIP sur les différents nouveaux risques auxquels sont exposées nos sociétés de plus en plus numérisées, notamment les résolutions de l'UIP intitulées *La cyber-guerre : une grave menace pour la paix et la sécurité mondiale* (adoptée le 1er avril 2015 lors de la 132e Assemblée, à Hanoï) et *Législation dans le monde pour la lutte contre l'exploitation et les abus sexuels en ligne à l'égard des enfants* (adoptée le 30 novembre 2021 lors de la 143e Assemblée, à Madrid), laquelle rappelle également la Convention du Conseil de l'Europe intitulée *La protection des enfants contre l'exploitation et les abus sexuels* (Convention de Lanzarote) du 25 octobre 2007, **ainsi que les lois types du Parlement de l'Amérique latine et des Caraïbes (Parlatino) sur la prévention de la violence scolaire (novembre 2015), la prévention, la prise en charge et la répression de la violence sexuelle à l'encontre des enfants et des adolescents (novembre 2015) et la lutte contre les sollicitations à des fins sexuelles (juin 2019),** **60**

(Argentine)

Nouvel alinéa 8bis

8bis) ***prenant note*** **des principes en matière de cybersécurité qui ont été convenus dans le *Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale* du 22 juillet 2015 (A/70/174) présenté devant l'Assemblée générale des Nations Unies**, **61**

(Viet Nam)

Alinéa 9

Supprimer l'alinéa. **62**

(Belgique, Canada, Suisse)

Modifier l'alinéa existant comme suit :

9) ~~*préoccupée* par l'absence d'instruments juridiques universels visant à réprimer la cybercriminalité et les cyberattaques~~ ***se félicitant*** **des travaux menés par l'ONU pour promouvoir le comportement responsable des États dans le cyberespace,** **63**

(Allemagne)

Modifier l'alinéa existant comme suit :

9) *préoccupée* par l'absence d'instruments juridiques universels visant à réprimer ~~la cybercriminalité~~ **l'utilisation des technologies de l'information et de la communication à des fins criminelles** et les ~~cyberattaques~~ **menaces liées aux TIC**, **64**

(Iran, République islamique d')

Modifier l'alinéa existant comme suit :

9) *préoccupée* par l'absence d'instruments juridiques universels visant à réprimer ~~la cybercriminalité~~ **le détournement des TIC à des fins criminelles** et les cyberattaques, **65**

(Pakistan)

Modifier l'alinéa existant comme suit :

9) *préoccupée* par ~~l'absence d'instruments juridiques universels~~ **la lenteur de la ratification des outils juridiques existants** visant à réprimer la cybercriminalité ~~et les cyberattaques~~**, tels que la *Convention sur la cybercriminalité* du Conseil de l'Europe du 23 novembre 2001 et ses Protocoles additionnels**, **66**

(Suède)

Modifier l'alinéa existant comme suit :

9) *préoccupée* par l'absence d'instruments juridiques universels visant à réprimer la cybercriminalité ~~et les cyberattaques~~, **67**

(Japon)

Modifier l'alinéa existant comme suit :

9) *préoccupée* par l'absence d'instruments juridiques universels visant à ~~réprimer~~ **prévenir et combattre** la cybercriminalité et les ~~cyberattaques~~ **cyberincidents**, **68**

(Inde)

Modifier l'alinéa existant comme suit :

9) *préoccupée* par l'absence d'instruments juridiques universels visant à réprimer la cybercriminalité et les cyberattaques, **et à prévenir les actes de cyberguerre,** **69**

(Argentine)

Modifier l'alinéa existant comme suit :

9) *préoccupée* par l'absence **d'une stratégie universelle et** d'instruments juridiques ~~universels~~ visant à réprimer la cybercriminalité et les cyberattaques, **70**

(Philippines)

Alinéa 10

Supprimer l'alinéa. **71**

(Canada)

Modifier l'alinéa existant comme suit :

10) *saluant* les efforts déployés par l'ONU pour adopter, par le biais de la résolution 74/247 de l'Assemblée générale du 27 décembre 2019, une convention internationale ~~générale~~ sur la **cybercriminalité** ~~sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles~~, et *saluant* la création d'un comité spécial chargé d'élaborer cette convention, **72**

(Suède)

Aucune incidence sur le français. **73**

(Singapour)

Nouvel alinéa 10bis

10bis) *saluant également* les efforts déployés par l'ONU pour convoquer, par le biais des résolutions 73/27 du 5 décembre 2018, 75/240 du 31 décembre 2020 et 77/36 du 7 décembre 2022 de l'Assemblée générale des Nations Unies, un Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation, en vue de rendre plus démocratique, plus inclusif et plus transparent le processus de négociation de l'ONU sur les questions de sécurité liées à l'utilisation des TIC, **74**

(Iran, République islamique d')

Alinéa 11

Modifier l'alinéa existant comme suit :

11) *se félicitant* du fait que l'UIP participe ~~au processus de consultation multipartite de ce comité spécial~~ **à toutes les consultations multipartites visant à faire connaître et à mettre en œuvre les normes facultatives et non contraignantes de comportement responsable des États en matière d'utilisation des technologies de l'information et de la communication**~~,~~ pour faire entendre la voix des parlements, **75**

(Canada)

Modifier l'alinéa existant comme suit :

11) *se félicitant* du fait que l'UIP participe au processus de consultation multipartite de ce comité spécial**, ainsi qu'aux travaux du Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation,** pour faire entendre la voix des parlements, **76**

(Iran, République islamique d')

Modifier l'alinéa existant comme suit :

11) *se félicitant* du fait que l'UIP participe au processus de consultation multipartite de ce comité spécial pour faire entendre la voix des parlements, **après consultation des États parties,** **77**

(Nicaragua)

Modifier l'alinéa existant comme suit :

11) *se félicitant* du fait que l'UIP participe au processus de consultation multipartite de ce comité spécial pour faire entendre la voix des parlements **en vue de lutter contre la cybercriminalité et les cyberattaques**, **78**

(Thaïlande)

Nouvel alinéa 11bis

11bis) *soutenant* le Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) créé en vertu de la résolution 75/240 de l'Assemblée générale des Nations Unies, et *l'encourageant* en outre à tenir compte des résultats des rapports 2010, 2013, 2015 et 2021 des groupes d'experts gouvernementaux et du rapport 2021 du Groupe de travail à composition non limitée chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, et à contribuer aux efforts entrepris par ceux-ci, **79**

(Égypte)

Nouvel alinéa 11ter

(11ter) *saluant* la proposition, approuvée par l'Assemblée générale des Nations Unies dans sa résolution 77/37 du 7 décembre 2022, de créer un programme d'action des Nations Unies destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale, mécanisme permanent, inclusif et orienté vers l'action qui permettra d'examiner les menaces existantes et potentielles ; de renforcer les capacités des États et d'appuyer les efforts faits par les États pour mettre en œuvre et promouvoir les engagements pris au titre du cadre ; de promouvoir le dialogue et la coopération avec les parties concernées ; et d'examiner périodiquement les progrès accomplis dans la mise en œuvre du programme d'action ainsi que les futurs travaux devant être entrepris dans ce contexte, **80**

(Égypte)

Alinéa 12

Supprimer l'alinéa. **81**

(Canada)

Modifier l'alinéa existant comme suit :

12) *prenant note* de la nécessité d'appliquer une approche globale et mondiale ~~au problème de la cybercriminalité et des cyberattaques, notamment en élaborant un cadre juridique international afin de lutter contre la cybercriminalité et les cyberattaques et leurs graves conséquences pour les citoyens~~ **pour lutter contre l'utilisation malveillante des TIC** et ~~de~~ protéger la paix, la sécurité et la stabilité ~~économique~~ mondiales, **82**

(Allemagne)

Modifier l'alinéa existant comme suit :

12) *prenant note* de la nécessité d'appliquer une approche ~~globale et~~ mondiale au problème de la cybercriminalité ~~et des cyberattaques, notamment en élaborant un cadre juridique international afin de lutter contre la cybercriminalité et les cyberattaques~~ et ~~leurs~~ **de ses** graves conséquences pour les citoyens**,** ~~et~~ **ainsi que de la nécessité** de protéger la paix, la sécurité et la stabilité économique mondiales, **tout en défendant les principes fondamentaux des droits de l'homme, notamment la liberté d'expression,** **83**

(Suède)

Modifier l'alinéa existant comme suit :

12) *prenant note* de la nécessité d'appliquer une approche globale et mondiale ~~au problème de la cybercriminalité et des cyberattaques, notamment en élaborant un cadre juridique international~~ afin de lutter contre la cybercriminalité et les cyberattaques et leurs graves conséquences pour les citoyens et de protéger la paix, la sécurité et la stabilité économique mondiales, **84**

(Suisse)

Modifier l'alinéa existant comme suit :

12) *prenant note* de la nécessité d'appliquer une approche globale et mondiale au problème de ~~la cybercriminalité~~ **l'utilisation des technologies de l'information et de la communication à des fins criminelles** et des ~~cyberattaques~~ **menaces liées aux TIC**, notamment en élaborant ~~un cadre juridique international~~ **des cadres internationaux juridiquement contraignants adaptés aux caractéristiques spécifiques des TIC** afin de lutter contre ~~la cybercriminalité~~ **l'utilisation des technologies de l'information et de la communication à des fins criminelles** et les ~~cyberattaques~~ **menaces liées aux TIC** et leurs graves conséquences pour les citoyens et de protéger la paix, la sécurité et la stabilité économique mondiales, **85**

(Iran, République islamique d')

Modifier l'alinéa existant comme suit :

12) *prenant note* de la nécessité d'appliquer une approche globale et mondiale au problème ~~de la cybercriminalité~~ **du détournement des TIC à des fins criminelles** et des cyberattaques, notamment en élaborant un cadre juridique international afin de lutter contre ~~la cybercriminalité~~ **le détournement des TIC à des fins criminelles** et les cyberattaques et leurs graves conséquences pour les citoyens et de protéger la paix, la sécurité et la stabilité économique mondiales, **86**

(Pakistan)

Modifier l'alinéa existant comme suit :

12) *prenant note* de la nécessité d'appliquer une approche globale et mondiale au problème de la cybercriminalité ~~et des cyberattaques~~, notamment en élaborant un cadre juridique international afin de lutter contre la cybercriminalité ~~et les cyberattaques~~ et leurs graves conséquences pour les citoyens et de protéger la paix, la sécurité et la stabilité économique mondiales, **87**

(Japon)

Modifier l'alinéa existant comme suit :

12) *prenant note* de la nécessité d'appliquer une approche globale et mondiale au problème de la cybercriminalité et des ~~cyberattaques~~ **cyberincidents**, notamment en élaborant un cadre juridique international afin de lutter contre la cybercriminalité et les cyberattaques et leurs graves conséquences pour les citoyens et de protéger la paix, la sécurité et la stabilité économique mondiales, **88**

(Inde)

Modifier l'alinéa existant comme suit :

12) *prenant note* de la nécessité d'appliquer une approche globale et mondiale au problème de la cybercriminalité et des cyberattaques, notamment en élaborant un cadre juridique international afin de lutter contre la cybercriminalité et les cyberattaques et leurs graves conséquences pour les citoyens **et les infrastructures,** et de protéger la paix, la sécurité et la stabilité économique mondiales, **89**

(Lituanie)

Nouvel alinéa 12bis

12bis) *prenant note également* que la communauté internationale doit adopter une approche globale pour lutter contre les menaces sur la sécurité informatique, qui tienne compte non seulement de la dimension technologique des menaces dans ce domaine, mais aussi de leur dimension politique et idéologique, notamment l'utilisation des TIC en vue de s'ingérer dans les affaires intérieures d'autres États et de porter atteinte à leur stabilité politique, économique et sociale, **90**

(Iran, République islamique d')

12bis) *se félicitant* des efforts en cours visant à adapter et à appliquer à la réglementation du cyberespace les régimes juridiques internationaux existants, notamment l'élaboration du *Manuel de Tallinn sur le droit international applicable à la cyberguerre*, **91**

(Ukraine)

Alinéa 13

Modifier l'alinéa existant comme suit :

13) *considérant* que les législateurs et les gouvernements doivent prendre d'urgence des mesures plus énergiques au niveau national pour lutter contre ~~la cybercriminalité~~ **l'utilisation des technologies de l'information et de la communication à des fins criminelles** et les ~~cyberattaques~~ **menaces liées aux TIC**, compte tenu de leur multiplication et de leur évolution rapide, **92**

(Iran, République islamique d')

Modifier l'alinéa existant comme suit :

13) *considérant* que les législateurs et les gouvernements doivent prendre d'urgence des mesures plus énergiques au niveau national pour lutter contre la cybercriminalité ~~et les cyberattaques~~, compte tenu de ~~leur~~ **sa** multiplication et de ~~leur~~ **son** évolution rapide, **93**

(République tchèque, Suède)

Modifier l'alinéa existant comme suit :

13) *considérant* que les législateurs et les gouvernements doivent prendre d'urgence des mesures plus énergiques au niveau national pour lutter contre la cybercriminalité et les ~~cyberattaques~~ **cyberincidents**, compte tenu de leur ~~multiplication~~ **intensification** et de leur évolution rapide, **94**

(Inde*)*

Modifier l'alinéa existant comme suit :

13) *considérant* que les législateurs et les gouvernements doivent prendre d'urgence des mesures plus énergiques au niveau national pour lutter contre ~~la cybercriminalité~~ **le détournement des TIC à des fins criminelles** et les cyberattaques, compte tenu de leur multiplication et de leur évolution rapide, **95**

(Pakistan)

Modifier l'alinéa existant comme suit :

13) *considérant* que les législateurs ~~et~~, les gouvernements **et l'ensemble des parties prenantes** doivent prendre d'urgence des mesures plus énergiques au niveau national pour lutter contre la cybercriminalité et les cyberattaques, compte tenu de leur multiplication et de leur évolution rapide, **96**

(Thaïlande)

Modifier l'alinéa existant comme suit :

13) *considérant* que les législateurs et les gouvernements doivent prendre d'urgence des mesures plus énergiques au niveau national pour lutter contre la cybercriminalité et les cyberattaques, compte tenu de leur multiplication et de leur évolution rapide, **tout en respectant pleinement les droits de l'homme, les libertés fondamentales et l'état de droit, ainsi que les obligations qui leur incombent en vertu du droit international des droits de l'homme,** **97**

(Canada)

Modifier l'alinéa existant comme suit :

13) *considérant* que les législateurs et les gouvernements doivent prendre d'urgence des mesures plus énergiques au niveau national pour lutter contre la cybercriminalité et les cyberattaques, compte tenu de leur multiplication et de leur évolution rapide, **et également pour renforcer la protection de la liberté d'expression et des autres droits fondamentaux,** **98**

(Afrique du Sud)

Nouvel alinéa 13bis

13bis) *considérant* que toutes les mesures prises dans ce domaine doivent garantir le respect des droits de l'homme et des droits fondamentaux, **99**

(Suède)

13bis) *notant* l'évolution inégale des capacités informatiques des pays et de leur aptitude à protéger les infrastructures informatiques, et *soulignant* la nécessité d'accroître l'assistance et la collaboration techniques, notamment en faveur des pays en développement, **100**

(Viet Nam)

Nouvel alinéa 13bis

13ter) *notant* que les États doivent agir conformément aux obligations qui leur incombent en vertu du droit international des droits de l'homme, notamment le *Pacte international relatif aux droits civils et politiques*, la *Convention relative aux droits de l'enfant*, la *Convention contre la torture et autres peines ou traitements cruels, inhumains ou dégradants*, la *Convention sur l'élimination de toutes les formes de discrimination à l'égard des femmes*, ainsi que leurs protocoles additionnels et les autres instruments internationaux pertinents relatifs aux droits de l'homme, **101**

(Suède)

Alinéa 14

Supprimer l'alinéa. **102**

(Inde)

Modifier l'alinéa existant comme suit :

14) *considérant également* qu'une action parlementaire commune de portée internationale est nécessaire pour ~~offrir un bouclier protecteur aux citoyens, aux gouvernements et aux pays, qui sont tous parties prenantes dans cette entreprise,~~ **faire connaître et mettre en œuvre les normes facultatives et non contraignantes de comportement responsable des États en matière d'utilisation des technologies de l'information et de la communication,** **103**

(Canada)

Modifier l'alinéa existant comme suit :

14) *considérant également* qu'une action parlementaire commune de portée **régionale et** internationale est nécessaire pour offrir un bouclier protecteur aux citoyens, aux gouvernements et aux pays, qui sont tous parties prenantes dans cette entreprise, **ainsi que pour assurer la coordination législative nécessaire au niveau infranational,** **104**

(Argentine)

Nouvel alinéa 14ter

14bis) *notant* que la cybercriminalité peut constituer une grave menace pour les processus démocratiques, notamment en ce qui concerne l'ingérence dans les élections en utilisant les failles de cybersécurité ou de faux comptes sur les réseaux sociaux, **105**

(Finlande)

14bis) *rappelant* les effets néfastes des mesures coercitives unilatérales et autres restrictions prises pendant la pandémie de COVID-19, qui ont été largement soulignés, notamment dans les rapports de l'ONU, **106**

(Iran, République islamique d')

Nouvel alinéa 14ter

14ter) *exhortant* les parlements à demander à leur gouvernement de ne pas adopter ou appliquer de mesures coercitives unilatérales (financières, économiques ou commerciales) susceptibles d'entraver ou d'avoir une incidence négative sur la capacité des États à prévenir et à combattre la cybercriminalité ou à coopérer et à se prêter mutuellement assistance dans ce domaine, **107**

(Iran, République islamique d')

Alinéa 15

Modifier l'alinéa existant comme suit :

15) *reconnaissant* que les femmes~~, les jeunes et les enfants sont les plus vulnérables et sont les premières victimes d'agressions sur Internet, et qu'ils pâtissent personnellement, socialement, culturellement et économiquement des actions des cybercriminels~~ **et les filles, les personnes âgées et les enfants, entre autres, sont les plus exposés aux menaces dans le cyberespace**, **108**

(Allemagne)

Modifier l'alinéa existant comme suit :

15) *reconnaissant* que les femmes, les jeunes, **les personnes âgées, les personnes handicapées** et les enfants sont ~~les plus~~ **particulièrement** vulnérables et sont les premières victimes d'agressions sur Internet, ~~et qu'ils pâtissent personnellement, socialement, culturellement et économiquement des actions des cybercriminels,~~ **109**

(Belgique)

Modifier l'alinéa existant comme suit :

15) *reconnaissant* que les femmes~~, les jeunes~~ et les enfants**, ainsi que les personnes âgées,** sont les plus vulnérables et sont les premières victimes d'agressions sur Internet, et qu'ils pâtissent personnellement, socialement, culturellement et économiquement ~~des actions des cybercriminels~~ **de la cybercriminalité**, **110**

(République tchèque)

Modifier l'alinéa existant comme suit :

15) *reconnaissant* que les femmes, les jeunes et les enfants sont les plus vulnérables et sont les premières victimes d'agressions ~~sur Internet~~ **dans le cyberespace**, et qu'ils pâtissent personnellement, socialement, culturellement et économiquement des actions des cybercriminels, **111**

(Lituanie)

Modifier l'alinéa existant comme suit :

15) *reconnaissant* que les femmes, les jeunes et les enfants sont les plus vulnérables et sont les premières victimes d'agressions sur Internet, et qu'ils pâtissent personnellement, socialement, culturellement et économiquement des actions des cybercriminels, **tout en *soulignant* la nécessité d'accroître la coopération avec le secteur privé et les prestataires de services afin de protéger les victimes,** **112**

(Thaïlande)

Modifier l'alinéa existant comme suit :

15) *reconnaissant* que les femmes, les jeunes, ~~et~~ les enfants et **les populations racisées** sont les plus vulnérables et sont les premières victimes d'agressions sur Internet, et qu'ils pâtissent personnellement, socialement, culturellement et économiquement des actions des cybercriminels, **113**

(Canada)

Modifier l'alinéa existant comme suit :

15) *reconnaissant* que les femmes, les jeunes et les enfants**, ainsi que les personnes handicapées,** sont les plus vulnérables et sont les premières victimes d'agressions sur Internet, et qu'ils pâtissent personnellement, socialement, culturellement et économiquement des actions des cybercriminels, **114**

(Finlande)

Modifier l'alinéa existant comme suit :

15) *reconnaissant* que les femmes, les jeunes **et les personnes âgées,** ~~et~~ **ainsi que** les enfants**,** sont les plus vulnérables et sont les premières victimes d'agressions sur Internet, et qu'ils pâtissent personnellement, socialement, culturellement et économiquement des actions des cybercriminels, **115**

(Viet Nam)

Modifier l'alinéa existant comme suit :

15) *reconnaissant* que les femmes, les jeunes**, les personnes âgées** et les enfants sont les plus vulnérables et sont les premières victimes d'agressions sur Internet, et qu'ils pâtissent personnellement, socialement, culturellement et économiquement des actions des cybercriminels, **116**

(Türkiye)

Nouvel alinéa 15bis

15bis) *sachant* que les recherches montrent qu'en période de COVID-19, le nombre de femmes et de filles victimes de violence en ligne, sous forme de menaces physiques, d'harcèlement sexuel et d'harcèlement obsessionnel, entre autres, a augmenté, **117**

(Philippines)

15bis) *consciente* de la nécessité de promouvoir l'égalité des sexes et l'autonomisation des femmes et des filles dans toute leur diversité, notamment par l'intégration de la dimension de genre et lors de l'élaboration, de la mise en œuvre et de l'application des politiques, des programmes et de la législation sur ces questions, **118**

(Suède)

Alinéa 16

Modifier l'alinéa existant comme suit :

16) *prenant note* de la nature des menaces et des risques ~~de la cybercriminalité~~ **posés par l'utilisation** transnationale **des technologies de l'information et de la communication à des fins criminelles** et ~~des cyberattaques~~ **de la menace des TIC** pour la paix et la sécurité internationale, ainsi que du développement fulgurant ~~du cyberespace~~ **de l'environnement des TIC**, qui fait que les méthodes utilisées par les cybercriminels **et les acteurs malveillants** sont de plus en plus sophistiquées, **119**

(Iran, République islamique d')

Modifier l'alinéa existant comme suit :

16) *prenant note* de la nature des menaces et des risques de ~~la cybercriminalité~~ **l'utilisation** transnationale **détournée des TIC à des fins criminelles** et des cyberattaques pour la paix et la sécurité internationale, ainsi que du développement fulgurant du cyberespace, qui fait que les méthodes utilisées par les cybercriminels sont de plus en plus sophistiquées, **120**

(Pakistan)

Modifier l'alinéa existant comme suit :

16) *prenant note* de la nature des menaces et des risques de la cybercriminalité transnationale ~~et des cyberattaques~~ pour la paix et la sécurité internationale, ainsi que du développement fulgurant du cyberespace, qui fait que les méthodes utilisées par les cybercriminels sont de plus en plus sophistiquées, **121**

(Suède)

Modifier l'alinéa existant comme suit :

16) *prenant note* de la nature des menaces et des risques de la cybercriminalité transnationale et des ~~cyberattaques~~ **cyberincidents** pour la paix et la sécurité internationale, ainsi que du développement fulgurant du cyberespace, qui fait que les méthodes utilisées par les cybercriminels sont de plus en plus sophistiquées, **122**

(Inde)

Modifier l'alinéa existant comme suit :

16) *prenant note* de la nature des menaces et des risques de la cybercriminalité transnationale et des cyberattaques **malveillantes** pour la paix et la sécurité internationale, ainsi que du développement fulgurant du cyberespace, qui fait que les méthodes utilisées par les cybercriminels sont de plus en plus sophistiquées, **123**

(Belgique)

Nouvel alinéa 16bis

16bis) *préoccupée* par l'utilisation aveugle des cyberattaques contre les infrastructures civiles, qui causent des dommages démesurés et inutiles aux installations de production et de distribution d'énergie, aux hôpitaux, aux systèmes bancaires et à d'autres infrastructures nationales essentielles, **124**

(Ukraine)

Alinéa 17

Modifier l'alinéa existant comme suit :

17) *prenant note également* que la cybercriminalité ~~et les cyberattaques englobent~~ **englobe** non seulement les attaques contre les ~~technologies de l'information et de la communication (TIC)~~ **systèmes informatiques**, les atteintes à la vie privée et la création et le déploiement de logiciels malveillants, mais **qu'elle facilite** aussi les ~~attaques~~ **cyberattaques** contre des infrastructures ~~nationales~~ **civiles** stratégiques, ainsi que d'autres actes qui peuvent se produire hors ligne et être facilités par les ~~TIC~~ **systèmes informatiques**, notamment la fraude en ligne, l'achat de drogue, le blanchiment d'argent, les crimes de haine~~, la propagande, l'endoctrinement extrémiste~~ et l'exploitation sexuelle des femmes et des enfants via Internet, autant d'actes qui ont une incidence négative sur la sécurité mondiale et la stabilité économique, **125**

(Suède)

Modifier l'alinéa existant comme suit :

17) *prenant note également* que la cybercriminalité et les cyberattaques englobent ~~non seulement~~ **en particulier** les attaques contre les technologies de l'information et de la communication (TIC), les atteintes à la vie privée et la création et le déploiement de logiciels malveillants, ~~mais aussi les attaques contre des infrastructures nationales stratégiques, ainsi que d'autres actes qui peuvent se produire hors ligne et être facilités par les TIC, notamment la fraude en ligne, l'achat de drogue, le blanchiment d'argent, les crimes de haine, la propagande, l'endoctrinement extrémiste et l'exploitation sexuelle des femmes et des enfants via Internet, autant d'actes qui ont une incidence négative sur la sécurité mondiale et la stabilité économique,~~ **126**
et *consciente en outre* de la nécessité de développer la coopération internationale pour lutter contre d'autres infractions graves qui peuvent être facilitées par les TIC,

(Allemagne)

Modifier l'alinéa existant comme suit :

17) *prenant note également* que ~~la cybercriminalité~~ **l'utilisation des technologies de l'information et de la communication à des fins criminelles** et les ~~cyberattaques~~ **menaces liées aux TIC** englobent non seulement les attaques contre les technologies de l'information et de la communication (TIC), les atteintes à la vie privée**, les campagnes de désinformation, la production d'images truquées, la xénophobie, l'ingérence dans les affaires intérieures des États** et la création et le déploiement de logiciels malveillants, mais aussi les attaques contre des infrastructures nationales stratégiques, ainsi que d'autres actes qui peuvent se produire hors ligne et être facilités par les TIC, notamment la fraude en ligne, l'achat de drogue, le blanchiment d'argent, les crimes de haine, la propagande, l'endoctrinement extrémiste et l'exploitation sexuelle des femmes et des enfants via Internet, autant d'actes qui ont une incidence négative sur la sécurité mondiale**,** ~~et~~ **ainsi que sur** la stabilité économique **et culturelle**, **127**

(Iran, République islamique d')

Modifier l'alinéa existant comme suit :

17) *prenant note également* que la cybercriminalité et les ~~cyberattaques~~ **cyberincidents** englobent non seulement les attaques contre les technologies de l'information et de la communication (TIC), les atteintes à la vie privée et la création et le déploiement de logiciels malveillants, mais aussi les attaques contre des infrastructures nationales stratégiques, ainsi que d'autres actes qui peuvent se produire hors ligne et être facilités par les TIC, notamment la fraude en ligne, l'achat de drogue, le blanchiment d'argent, les crimes de haine, la propagande, l'endoctrinement extrémiste et l'exploitation sexuelle des femmes et des enfants via Internet, autant d'actes qui ont une incidence négative sur la sécurité mondiale et la stabilité économique, **128**

(Inde)

Modifier l'alinéa existant comme suit :

17) *prenant note également* que ~~la cybercriminalité~~ **le détournement des TIC à des fins criminelles** et les cyberattaques englobent non seulement les attaques contre les technologies de l'information et de la communication (TIC), les atteintes à la vie privée et la création et le déploiement de logiciels malveillants, mais aussi les attaques contre des infrastructures nationales stratégiques, ainsi que d'autres actes qui peuvent se produire hors ligne et être facilités par les TIC, notamment la fraude en ligne, l'achat de drogue, le blanchiment d'argent, les crimes de haine, la propagande, l'endoctrinement extrémiste et l'exploitation sexuelle des femmes et des enfants via Internet, autant d'actes qui ont une incidence négative sur la sécurité mondiale et la stabilité économique, **129**

(Pakistan)

Modifier l'alinéa existant comme suit :

17) *prenant note également* que la cybercriminalité et les cyberattaques englobent non seulement les attaques contre les ~~technologies de l'information et de la communication (TIC)~~ **systèmes informatiques**, les atteintes à la vie privée et la création et le déploiement de logiciels malveillants, mais aussi les attaques contre des infrastructures nationales stratégiques, ainsi que d'autres actes qui peuvent se produire hors ligne ~~et être facilités par les TIC~~ **mais qui sont désormais commis dans le cyberespace via les systèmes informatiques**, notamment la fraude en ligne, l'achat de drogue, le blanchiment d'argent, les crimes de haine, la propagande, l'endoctrinement extrémiste et l'exploitation sexuelle des femmes et des enfants via Internet, autant d'actes qui ont une incidence négative sur la sécurité mondiale et la stabilité économique, **130**

(Singapour)

Modifier l'alinéa existant comme suit :

17) *prenant note également* que la cybercriminalité et les cyberattaques ~~englobent non seulement~~ **comprennent, sans s'y limiter,** les attaques contre les technologies de l'information et de la communication (TIC), les atteintes à la vie privée**,** ~~et~~ la création et le déploiement de logiciels malveillants~~, mais aussi~~ **et** les attaques contre des infrastructures nationales stratégiques, ainsi que d'autres actes qui peuvent se produire hors ligne et être facilités par les TIC, notamment la fraude en ligne, l'achat de drogue, le blanchiment d'argent, les crimes de haine, la propagande, l'endoctrinement extrémiste et l'exploitation sexuelle des femmes et des enfants via Internet, autant d'actes qui ont une incidence négative sur la sécurité mondiale et la stabilité économique, **131**

(Canada)

Modifier l'alinéa existant comme suit :

17) *prenant note également* que la cybercriminalité et les cyberattaques englobent non seulement les attaques contre les technologies de l'information et de la communication (TIC), les atteintes à la vie privée et la création et le déploiement de logiciels malveillants, mais aussi les attaques contre des infrastructures nationales stratégiques, ainsi que d'autres actes qui peuvent se produire hors ligne et être facilités par les TIC, notamment la fraude en ligne, l'achat de drogue, le blanchiment d'argent~~, les crimes de haine, la propagande, l'endoctrinement extrémiste~~ et l'exploitation sexuelle des femmes et des enfants via Internet, autant d'actes qui ont une incidence négative sur la sécurité mondiale et la stabilité économique, **132**

(Belgique)

Modifier l'alinéa existant comme suit :

17) *prenant note également* que la cybercriminalité et les cyberattaques englobent non seulement les attaques contre les technologies de l'information et de la communication (TIC), les atteintes à la vie privée et la création et le déploiement de logiciels malveillants, mais aussi les attaques contre des infrastructures nationales stratégiques, ainsi que d'autres actes qui peuvent se produire hors ligne et être facilités par les TIC, notamment la fraude en ligne, l'achat de drogue, le blanchiment d'argent, les crimes de haine, la propagande, l'endoctrinement extrémiste**, le cyberharcèlement et le harcèlement obsessionnel, la traite des personnes** et l'exploitation sexuelle des femmes et des enfants via Internet, autant d'actes qui ont une incidence négative sur la sécurité mondiale et la stabilité économique, **133**

(Afrique du Sud)

Modifier l'alinéa existant comme suit :

17) *prenant note également* que la cybercriminalité et les cyberattaques englobent non seulement les attaques contre les technologies de l'information et de la communication (TIC), les atteintes à la vie privée et la création et le déploiement de logiciels malveillants, mais aussi les attaques contre des infrastructures nationales stratégiques, ainsi que d'autres actes qui peuvent se produire hors ligne et être facilités par les TIC, notamment la fraude en ligne, l'achat de drogue, le blanchiment d'argent, **la traite des êtres humains,** les crimes de haine, la propagande, l'endoctrinement extrémiste et l'exploitation sexuelle des femmes et des enfants via Internet, autant d'actes qui ont une incidence négative sur la sécurité mondiale et la stabilité économique, **134**

(Roumanie)

Modifier l'alinéa existant comme suit :

17) *prenant note également* que la cybercriminalité et les cyberattaques englobent non seulement les attaques contre les technologies de l'information et de la communication (TIC), les atteintes à la vie privée et la création et le déploiement de logiciels malveillants, mais aussi les attaques contre des infrastructures nationales stratégiques, ainsi que d'autres actes qui peuvent se produire hors ligne et être facilités par les TIC, notamment la fraude en ligne, l'achat de drogue, le blanchiment d'argent, les crimes de haine, la propagande, l'endoctrinement extrémiste et l'exploitation sexuelle**, notamment** des femmes et des enfants**,** via Internet, autant d'actes qui ont une incidence négative sur la sécurité mondiale et la stabilité économique, **135**

(Lituanie)

Nouvel alinéa 17bis

17bis) *consciente* de l'intérêt d'échanger les données d'expérience sur les différentes définitions de la cybercriminalité et des cyberattaques afin d'établir une base plus large pour mettre au point des mesures de confiance, **136**

(Canada)

17bis) *considérant* que le manque de responsabilité des fournisseurs de services et des plateformes transnationales constitue également une grave menace dans le domaine des TIC, qui doit être traitée par la communauté internationale, **137**

(Iran, République islamique d')

Alinéa 18

Supprimer l'alinéa. **138**

(Japon)

Modifier l'alinéa existant comme suit :

18) *considérant* que la plupart des lois nationales ont été promulguées ~~bien~~ avant l'apparition de la cybercriminalité ~~et des cyberattaques~~ et ne permettent donc pas toujours de répondre efficacement à ces menaces, **139**

(République tchèque)

Modifier l'alinéa existant comme suit :

18) *considérant* que la plupart des lois nationales ont été promulguées bien avant l'apparition de la cybercriminalité ~~et des cyberattaques~~ et ne permettent donc pas toujours de répondre efficacement à ces menaces, **140**

(Suède)

Modifier l'alinéa existant comme suit :

18) *considérant* que la plupart des lois nationales ont été promulguées bien avant ~~l'apparition de la cybercriminalité~~ **l'utilisation des technologies de l'information et de la communication à des fins criminelles** et ~~des cyberattaques~~ **l'apparition des menaces liées aux TIC** et ne permettent donc pas toujours de répondre efficacement à ces menaces, **141**

(Iran, République islamique d')

Modifier l'alinéa existant comme suit :

18) *considérant* que la plupart des lois nationales ont été promulguées bien avant ~~l'apparition de la cybercriminalité~~ **le détournement des TIC à des fins criminelles** et **l'apparition** des cyberattaques et ne permettent donc pas toujours de répondre efficacement à ces menaces, **142**

(Pakistan)

Modifier l'alinéa existant comme suit :

18) *considérant* que la plupart des lois nationales ont été promulguées bien avant ~~l'apparition~~ **la propagation** de la cybercriminalité et des cyberattaques et ne permettent donc pas toujours de répondre efficacement à ces menaces, **143**

(Thaïlande)

Modifier l'alinéa existant comme suit :

18) *considérant* que la plupart des lois nationales ont été promulguées bien avant l'apparition de la cybercriminalité et des cyberattaques **malveillantes** et ne permettent donc pas toujours de répondre efficacement à ces menaces, **144**

(Belgique)

Nouvel alinéa 18bis

18bis) *soulignant* la nécessité de redoubler d'efforts pour réduire la fracture numérique en facilitant le transfert des technologies de l'information et le renforcement des capacités dans les pays en développement concernant l'utilisation des technologies de l'information et de la communication à des fins criminelles et la sécurité des TIC, **145**

(Iran, République islamique d')

DISPOSITIF

Paragraphe 1

Supprimer le paragraphe. **146**

(Belgique, Canada, Japon, Suisse)

Modifier le paragraphe existant comme suit :

1. *demande* à la communauté internationale, par l'intermédiaire de l'ONU, **d'élaborer et** d'adopter une définition mondiale commune concernant la cybercriminalité ~~et les cyberattaques, qui couvre toutes les variantes de ces activités et les agissements qu'elles peuvent provoquer~~ ; **147**

(Suède)

Modifier le paragraphe existant comme suit :

1. *demande* à la communauté internationale, par l'intermédiaire de l'ONU, d'adopter une définition mondiale commune concernant la cybercriminalité et les cyberattaques~~, qui couvre toutes les variantes de ces activités et les agissements qu'elles peuvent provoquer~~ ; **148**

(Allemagne, République de Corée, Singapour)

Modifier le paragraphe existant comme suit :

1. *demande* à la communauté internationale, par l'intermédiaire de l'ONU, d'adopter une définition mondiale commune concernant la cybercriminalité ~~et les cyberattaques~~, qui couvre toutes les variantes de ~~ces activités~~ **cette activité** et les agissements ~~qu'elles peuvent~~ **qu'elle peut** provoquer, **notamment une distinction claire entre la cybercriminalité et la cyberguerre, et entre la cybersécurité et la cyberdéfense** ; **149**

(Argentine)

Modifier le paragraphe existant comme suit :

1. *demande* à la communauté internationale, par l'intermédiaire de l'ONU, d'adopter une définition mondiale commune concernant la cybercriminalité ~~et les cyberattaques~~, qui couvre toutes les variantes de ~~ces activités~~ **cette activité** et les agissements ~~qu'elles peuvent~~ **qu'elle peut** provoquer ; **150**

(République tchèque)

Modifier le paragraphe existant comme suit :

1. *demande* à la communauté internationale, par l'intermédiaire de l'ONU, d'adopter une ~~définition~~ **terminologie commune,** mondiale **et universelle** ~~commune concernant la cybercriminalité et les cyberattaques~~ **dans le domaine de la sécurité des TIC**, qui couvre toutes les variantes de ~~ces activités~~ **cette activité** et les agissements ~~qu'elles peuvent~~ **qu'elle peut** provoquer ; **151**

(Iran, République islamique d')

Modifier le paragraphe existant comme suit :

1. *demande* à la communauté internationale, par l'intermédiaire de l'ONU, d'adopter une définition mondiale commune concernant ~~la cybercriminalité~~ **les infractions commises à l'aide des TIC** et les ~~cyberattaques~~ **cyberincidents**, qui couvre toutes les variantes de ces activités et les agissements qu'elles peuvent provoquer ; **152**

(Inde)

Modifier le paragraphe existant comme suit :

1. *demande* à la communauté internationale, par l'intermédiaire de l'ONU, d'adopter une définition mondiale commune concernant ~~la cybercriminalité~~ **le détournement des TIC à des fins criminelles** et les cyberattaques, qui couvre toutes les variantes de ces activités et les agissements qu'elles peuvent provoquer ; **153**

(Pakistan)

Modifier le paragraphe existant comme suit :

1. *demande* à la communauté internationale, par l'intermédiaire de l'ONU, d'adopter une définition mondiale commune concernant la cybercriminalité et les cyberattaques, qui couvre toutes les variantes de ces activités et les agissements qu'elles peuvent provoquer**, en tenant compte du contexte de chaque pays** ; **154**

(Nicaragua)

Paragraphe 2

Supprimer le paragraphe. **155**

(Belgique, Canada)

Modifier le paragraphe existant comme suit :

2. *encourage* les parlements à demander à l'exécutif de soutenir les efforts déployés par l'ONU en vue d'adopter une ~~nouvelle~~ convention **internationale générale** sur la ~~cybercriminalité~~ **lutte contre l'utilisation des technologies de l'information et de la communication à des fins criminelles** en participant activement à sa rédaction ; **156**

(Inde, Fédération de Russie)

Modifier le paragraphe existant comme suit :

2. *encourage* les parlements à demander à l'exécutif de soutenir les efforts déployés par l'ONU en vue d'adopter une nouvelle convention sur ~~la cybercriminalité~~ **l'utilisation des technologies de l'information et de la communication à des fins criminelles** en participant activement à sa rédaction ; **157**

(Iran, République islamique d')

Modifier le paragraphe existant comme suit :

2. *encourage* les parlements à demander à l'exécutif de soutenir les efforts déployés par l'ONU en vue d'adopter une nouvelle convention sur ~~la cybercriminalité~~ **le détournement des TIC à des fins criminelles** en participant activement à sa rédaction ; **158**

(Pakistan)

Nouveau paragraphe 2bis

2bis. *encourage également* les parlements à demander à leur gouvernement de soutenir les efforts du Groupe de travail à composition non limitée de l'ONU sur la sécurité et l'utilisation des technologies de l'information et de la communication (TIC) en participant activement à ses travaux ; **159**

(Iran, République islamique d')

Paragraphe 3

Supprimer le paragraphe. **160**

(Belgique, Canada)

Modifier le paragraphe existant comme suit :

3. *exhorte* les parlements et les gouvernements à insister sur la nécessité d'inclure, dans la convention, ~~une définition complète de la cybercriminalité et des cyberattaques, ainsi que~~ des mécanismes d'appui à la coopération internationale pour lutter contre la cybercriminalité ~~et les cyberattaques~~**, assortis de garanties adéquates** ; **161**

(Suède)

Modifier le paragraphe existant comme suit :

3. *exhorte* les parlements et les gouvernements à insister sur la nécessité d'inclure, dans la convention, ~~une définition complète de la cybercriminalité et des cyberattaques, ainsi que~~ des mécanismes d'appui à la coopération internationale pour lutter contre la cybercriminalité ~~et les cyberattaques~~ ; **162**

(Japon)

Modifier le paragraphe existant comme suit :

3. *exhorte* les parlements et les gouvernements à insister sur la nécessité d'inclure, dans la convention, ~~une définition complète de la cybercriminalité et des cyberattaques, ainsi que~~ des mécanismes d'appui à la coopération internationale pour lutter contre la cybercriminalité et les cyberattaques ; **163**

(Lituanie, République de Corée)

Modifier le paragraphe existant comme suit :

3. *exhorte* les parlements et les gouvernements à insister sur la nécessité d'inclure, dans la convention, ~~une définition complète de la cybercriminalité et des cyberattaques~~ **un inventaire complet de cybercrimes clairement définis**, ainsi que des mécanismes d'appui à la coopération internationale pour lutter contre la cybercriminalité et les cyberattaques ; **164**

(Suisse)

Modifier le paragraphe existant comme suit :

3. *exhorte* les parlements et les gouvernements à insister sur la nécessité d'inclure, dans la convention, une définition complète de la cybercriminalité ~~et des cyberattaques~~, ainsi que des mécanismes d'appui à la coopération internationale pour lutter contre **ce type de criminalité** ~~la cybercriminalité et les cyberattaques~~**, sans préjudice de l'application de la législation nationale en vigueur en matière de cybersécurité et de protection des données personnelles** ; **165**

(Argentine)

Modifier le paragraphe existant comme suit :

3. *exhorte* les parlements et les gouvernements à insister sur la nécessité d'inclure, dans la convention, une définition complète de la cybercriminalité ~~et des cyberattaques~~, ainsi que des mécanismes d'appui à la coopération internationale pour lutter contre la cybercriminalité ~~et les cyberattaques~~ ; **166**

(Allemagne)

Modifier le paragraphe existant comme suit :

3. *exhorte* les parlements et les gouvernements à insister sur la nécessité d'inclure, dans la convention, ~~une définition complète de la cybercriminalité et des cyberattaques,~~ **et dans les résultats des travaux du Groupe de travail à composition non limitée sur la sécurité des TIC, une terminologie universelle dans le domaine de la sécurité des TIC**, ainsi que des mécanismes d'appui à la coopération internationale pour lutter contre la ~~cybercriminalité~~ **l'utilisation des technologies de l'information et de la communication à des fins criminelles** et les ~~cyberattaques~~ **menaces liées aux TIC** ; **167**

(Iran, République islamique d')

Modifier le paragraphe existant comme suit :

3. *exhorte* les parlements et les gouvernements à insister sur la nécessité d'inclure, dans la convention, une définition complète ~~de la cybercriminalité~~ **des infractions commises en utilisant les TIC** et des ~~cyberattaques~~ **cyberincidents**, ainsi que des mécanismes d'appui à la coopération internationale pour lutter contre la cybercriminalité et les ~~cyberattaques~~ **cyberincidents** ; **168**

(Inde)

Modifier le paragraphe existant comme suit :

3. *exhorte* les parlements et les gouvernements à insister sur la nécessité d'inclure, dans la convention, une définition complète ~~de la cybercriminalité~~ **du détournement des TIC à des fins criminelles** et des cyberattaques, ainsi que des mécanismes d'appui à la coopération internationale pour lutter contre ~~la cybercriminalité~~ **le détournement des TIC à des fins criminelles** et les cyberattaques ; **169**

(Pakistan)

Modifier le paragraphe existant comme suit :

3. *exhorte* les parlements et les gouvernements à insister sur la nécessité d'inclure, dans la convention, une définition complète de la cybercriminalité et des cyberattaques, **y compris des infractions pénales correspondantes, et les garanties nécessaires pour protéger les droits de l'homme et les libertés fondamentales,** ainsi que des mécanismes d'appui à la coopération internationale **et à l'assistance technique** pour ~~lutter contre~~ **combattre et prévenir** la cybercriminalité et les cyberattaques ; **170**

(Afrique du Sud)

Modifier le paragraphe existant comme suit :

3. *exhorte* les parlements et les gouvernements à insister sur la nécessité d'inclure, dans la convention, une définition complète de la cybercriminalité et des cyberattaques, ainsi que des mécanismes d'appui à la coopération internationale **et multipartite, et les lignes directrices relatives à leur mise en œuvre et à leur évaluation**, pour lutter **efficacement** contre la cybercriminalité et les cyberattaques ; **171**

(Thaïlande)

Nouveau paragraphe 3bis

3bis. *exhorte également* les parlements et les gouvernements à veiller à ce que la nouvelle convention complète les instruments internationaux et régionaux existants sur la cybercriminalité et la criminalité transnationale organisée, ainsi que les autres instruments pertinents, en particulier ceux relatifs à la protection des droits de l'homme ; **172**

(Roumanie)

3bis. *exhorte également* les parlements et les gouvernements à souligner l'importance de prévoir dans la nouvelle convention une forte protection des droits de l'homme et des libertés fondamentales ; **173**

(Suède)

Paragraphe 4

Supprimer le paragraphe. **174**

(Belgique, Canada)

Modifier le paragraphe existant comme suit :

4. *invite* les parlements et les gouvernements à utiliser cette convention, une fois qu'elle aura été adoptée, comme un moyen de renforcer la législation nationale et d'accroître la coopération internationale pour lutter contre la cybercriminalité ~~et les cyberattaques~~ ; **175**

(Argentine, République tchèque, Allemagne, Suède)

Modifier le paragraphe existant comme suit :

4. *invite* les parlements et les gouvernements à utiliser cette convention, une fois qu'elle aura été adoptée, comme un moyen de renforcer la législation nationale et d'accroître la coopération internationale pour lutter contre ~~la cybercriminalité~~ **l'utilisation des technologies de l'information et de la communication à des fins criminelles** et les ~~cyberattaques~~ **menaces liées aux TIC** ; **176**

(Iran, République islamique d')

Modifier le paragraphe existant comme suit :

4. *invite* les parlements et les gouvernements à utiliser cette convention, une fois qu'elle aura été adoptée, comme un moyen de renforcer la législation nationale et d'accroître la coopération internationale pour lutter contre ~~la cybercriminalité~~ **le détournement des TIC à des fins criminelles** et les cyberattaques ; **177**

(Pakistan)

Modifier le paragraphe existant comme suit :

4. *invite* les parlements et les gouvernements à utiliser cette convention, une fois qu'elle aura été adoptée, comme un moyen ~~de renforcer~~ **d'actualiser** la législation nationale et d'accroître la coopération internationale pour lutter contre la cybercriminalité et les cyberattaques ; **178**

(Japon)

Modifier le paragraphe existant comme suit :

4. *invite* les parlements et les gouvernements à utiliser cette convention, une fois qu'elle aura été adoptée **et sera entrée en vigueur**, comme un moyen de renforcer la législation nationale et d'accroître la coopération internationale pour lutter contre la cybercriminalité et les cyberattaques ; **179**

(Viet Nam)

Modifier le paragraphe existant comme suit :

4. *invite* les parlements et les gouvernements à utiliser ~~cette~~ **la** convention **visée aux paragraphes 2 et 3 ci-dessus**, une fois qu'elle aura été adoptée, comme un moyen de renforcer la législation nationale et d'accroître la coopération internationale pour lutter contre la cybercriminalité et les cyberattaques ; **180**

(Soudan du Sud)

Nouveau paragraphe 4bis

4bis. ***encourage*** **les parlements à prendre pleinement en compte le pouvoir perturbateur et destructeur des cyberattaques en se penchant sur la question de la protection des infrastructures nationales stratégiques, notamment l'électricité, l'eau, le gaz, les communications, les centrales nucléaires, les transports, la finance et l'approvisionnement en nourriture ;** **181**

(Argentine)

4bis. ***encourage*** **les parlements à prendre les mesures nécessaires pour que leur pays adhère, s'il ne l'a pas encore fait, aux instruments internationaux existants qui portent sur l'utilisation des TIC à des fins criminelles, notamment la *Convention sur la cybercriminalité* du Conseil de l'Europe du 23 novembre 2001 (la "Convention de Budapest"), qui constitue le traité multilatéral sur la cybercriminalité le plus complet actuellement en vigueur et qui est ouverte à l'adhésion de tous les États ;** **182**

(Roumanie)

Paragraphe 5

Modifier le paragraphe existant comme suit :

5. *demande* aux parlements ~~d'adopter de nouvelles lois~~ **de s'assurer que la législation** sur la cybercriminalité et les cyberattaques **est à jour et pertinente**, compte tenu de l'augmentation constante de l'ampleur et de la fréquence de ces activités et de leurs conséquences pour la paix et la sécurité internationale et la stabilité économique mondiale ; **183**

(Suède)

Modifier le paragraphe existant comme suit :

5. *demande* aux parlements d'adopter**, le cas échéant,** de nouvelles lois sur la cybercriminalité ~~et les cyberattaques~~, compte tenu de l'augmentation constante de l'ampleur et de la fréquence de ces activités et de leurs conséquences pour la paix et la sécurité internationale et la stabilité économique mondiale ; **184**

(République tchèque)

Modifier le paragraphe existant comme suit :

5. *demande* aux parlements d'adopter de nouvelles lois sur ~~la cybercriminalité~~ **l'utilisation des technologies de l'information et de la communication à des fins criminelles** et les ~~cyberattaques~~ **menaces liées aux TIC**, compte tenu de l'augmentation constante de l'ampleur et de la fréquence de ces activités et de leurs conséquences pour la paix et la sécurité internationale et la stabilité économique mondiale ; **185**

(Iran, République islamique d')

Modifier le paragraphe existant comme suit :

5. *demande* aux parlements d'adopter de nouvelles lois sur la cybercriminalité et ~~les~~ ~~cyberattaques~~ **la cybersécurité**, compte tenu de l'augmentation constante de l'ampleur et de la fréquence de ~~ces activités~~ **la cybercriminalité et des cyberattaques malveillantes** et de leurs conséquences pour la paix et la sécurité internationale et la stabilité économique mondiale ; **186**

(Belgique)

Modifier le paragraphe existant comme suit :

5. *demande* aux parlements d'adopter de nouvelles lois sur ~~la cybercriminalité~~ **le détournement des TIC à des fins criminelles** et les cyberattaques, compte tenu de l'augmentation constante de l'ampleur et de la fréquence de ces activités et de leurs conséquences pour la paix et la sécurité internationale et la stabilité économique mondiale ; **187**

(Pakistan)

Modifier le paragraphe existant comme suit :

5. *demande* aux parlements ~~d'adopter de nouvelles lois~~ **d'actualiser la législation nationale** sur la cybercriminalité et les cyberattaques, compte tenu de l'augmentation constante de l'ampleur et de la fréquence de ces activités et de leurs conséquences pour la paix et la sécurité internationale et la stabilité économique mondiale ; **188**

(Japon)

Modifier le paragraphe existant comme suit :

5. *demande* aux parlements ~~d'adopter de nouvelles lois~~ **qui ne l'ont pas encore fait d'adopter une nouvelle loi** sur la cybercriminalité et les cyberattaques, compte tenu de l'augmentation constante de l'ampleur et de la fréquence de ces activités **illicites** et de leurs conséquences **à haut risque** pour la paix et la sécurité internationale et la stabilité économique mondiale ; **189**

(Nicaragua)

Modifier le paragraphe existant comme suit :

5. *demande* aux parlements d'adopter de nouvelles lois sur la cybercriminalité et les cyberattaques **conformément au droit international, notamment aux instruments internationaux relatifs aux droits de l'homme**, compte tenu de l'augmentation constante de l'ampleur et de la fréquence de ces activités et de leurs conséquences pour la paix et la sécurité internationale et la stabilité économique mondiale**, et de prévoir dans ces lois une compétence extraterritoriale pour permettre la poursuite des auteurs d'actes criminels, indépendamment du lieu où ces actes ont été commis et du fait qu'ils constituent ou non une infraction dans la juridiction étrangère concernée** ; **190**

(Afrique du Sud)

Modifier le paragraphe existant comme suit :

5. *demande* aux parlements d'adopter de nouvelles lois sur la cybercriminalité et les cyberattaques**, en mobilisant l'ensemble des parties prenantes, notamment le secteur privé, le monde universitaire, la société civile et les milieux techniques**, compte tenu de l'augmentation constante de l'ampleur et de la fréquence de ces activités et de leurs conséquences pour **la sécurité nationale,** la paix et la sécurité internationale et la stabilité économique mondiale ; **191**

(Roumanie)

Modifier le paragraphe existant comme suit :

5. *demande* aux parlements d'adopter de nouvelles lois **ou de réviser celles existantes** sur la cybercriminalité et les cyberattaques, compte tenu de l'augmentation constante de l'ampleur et de la fréquence de ces activités et de leurs conséquences pour la paix et la sécurité internationale et la stabilité économique mondiale ; **192**

(Viet Nam)

Modifier le paragraphe existant comme suit :

5. *demande* aux parlements d'adopter de nouvelles lois sur la cybercriminalité et les cyberattaques, **en y affectant les moyens nécessaires,** compte tenu de l'augmentation constante de l'ampleur et de la fréquence de ces activités et de leurs conséquences pour la paix et la sécurité internationale et la stabilité économique mondiale ; **193**

(France)

Modifier le paragraphe existant comme suit :

5. *demande* aux parlements d'adopter de nouvelles lois sur la cybercriminalité et les cyberattaques, compte tenu de l'augmentation constante de l'ampleur**, de la portée, de la rapidité, de la complexité** et de la fréquence de ces activités et de leurs conséquences pour la paix et la sécurité internationale et la stabilité économique mondiale ; **194**

(Inde)

Nouveau paragraphe 5bis

5bis. *demande également* à la communauté internationale de ne pas utiliser les technologies de l'information et de la communication et les réseaux d'information et de communication pour s'ingérer dans les affaires intérieures d'autres États ou pour porter atteinte à leur stabilité politique, économique et sociale ; **195**

(Iran, République islamique d')

5bis. *exhorte* les parlements à veiller à ce que des évaluations d'impact sur les droits de l'homme soient intégrées dans l'ensemble des processus législatifs relatifs à la cybercriminalité et aux cyberattaques ; **196**

(Roumanie)

5bis. *demande également* aux parlements de renforcer les capacités des agents de la force publique, notamment les services d'enquête, les procureurs et les juges, dans le domaine des cyberattaques et de la cybercriminalité, et de leur donner les moyens d'enquêter, de poursuivre les auteurs et de juger efficacement les affaires de cyberattaques et de cybercriminalité; **197**

(Afrique du Sud)

5bis. *exhorte* les parlements et les gouvernements à élaborer et à adopter un cadre juridique universel sur la cyberguerre, qui tienne compte des notions de distinction et de proportionnalité, afin de prévenir les cyberattaques contre les infrastructures civiles essentielles ; **198**

(Ukraine)

Paragraphe 6

Modifier le paragraphe existant comme suit :

6. *encourage* les parlements à faire pleinement usage de leur fonction de contrôle afin de s'assurer que les gouvernements disposent des outils nécessaires pour lutter contre l'augmentation rapide de la cybercriminalité ~~et des cyberattaques~~ et protéger la ~~sécurité numérique~~ **cybersécurité**, l'identité, la vie privée et les données des citoyens, notamment des personnes les plus vulnérables ; **199**

(République tchèque)

Modifier le paragraphe existant comme suit :

6. *encourage* les parlements à faire pleinement usage de leur fonction de contrôle afin de s'assurer que les gouvernements disposent des outils nécessaires pour **prévenir et** lutter contre l'augmentation rapide de la cybercriminalité ~~et des cyberattaques~~ et protéger la sécurité numérique, l'identité, la vie privée et les données des citoyens, notamment des personnes les plus vulnérables ; **200**

(Belgique)

Modifier le paragraphe existant comme suit :

6. *encourage* les parlements à faire pleinement usage de leur fonction de contrôle afin de s'assurer que les gouvernements disposent des outils nécessaires pour lutter contre l'augmentation rapide de la cybercriminalité ~~et des cyberattaques~~ et protéger la sécurité numérique, l'identité, la vie privée et les données des citoyens, notamment des personnes les plus vulnérables**, tout en assurant le respect des droits de l'homme et des libertés** ; **201**

(Suède)

Modifier le paragraphe existant comme suit :

6. *encourage* les parlements à faire pleinement usage de leur fonction de contrôle afin de s'assurer que les gouvernements disposent des outils nécessaires pour lutter contre l'augmentation rapide de ~~la cybercriminalité~~ **l'utilisation des technologies de l'information et de la communication à des fins criminelles** et des ~~cyberattaques~~ **menaces liées aux TIC** et protéger la sécurité numérique, l'identité, la vie privée et les données des citoyens, notamment des personnes les plus vulnérables ; **202**

(Iran, République islamique d')

Modifier le paragraphe existant comme suit :

6. *encourage* les parlements à faire pleinement usage de leur fonction de contrôle afin de s'assurer que les gouvernements disposent des outils nécessaires pour lutter contre l'augmentation rapide ~~de la cybercriminalité~~ **du détournement des TIC à des fins criminelles** et des cyberattaques et protéger la sécurité numérique, l'identité, la vie privée et les données des citoyens, notamment des personnes les plus vulnérables ; **203**

(Pakistan)

Modifier le paragraphe existant comme suit :

6. *encourage* les parlements à ~~faire pleinement usage de~~ **jouer pleinement** leur ~~fonction de contrôle~~ **rôle** afin de s'assurer que les gouvernements disposent des outils nécessaires pour lutter contre l'augmentation rapide de la cybercriminalité et des cyberattaques et protéger la sécurité numérique, l'identité, la vie privée et les données des citoyens, notamment des personnes les plus vulnérables ; **204**

(Japon)

Modifier le paragraphe existant comme suit :

6. *encourage* les parlements à faire pleinement usage de leur fonction de contrôle afin de s'assurer que les gouvernements disposent des outils nécessaires pour lutter contre l'augmentation rapide de la cybercriminalité et des cyberattaques et protéger la sécurité numérique, l'identité, la vie privée et les données des citoyens~~, notamment des personnes les plus vulnérables~~ ; **205**

(Inde)

Modifier le paragraphe existant comme suit :

6. *encourage* les parlements à faire pleinement usage de leur fonction de contrôle afin de s'assurer que les gouvernements disposent des outils nécessaires**, notamment les ressources et les capacités appropriées,** pour lutter contre l'augmentation rapide de la cybercriminalité et des cyberattaques et protéger la sécurité numérique, l'identité, la vie privée et les données des citoyens, notamment des personnes les plus vulnérables ; **206**

(Afrique du Sud)

Modifier le paragraphe existant comme suit :

6. *encourage* les parlements à faire pleinement usage de leur fonction de contrôle afin de s'assurer que les gouvernements disposent des outils nécessaires pour lutter contre l'augmentation rapide de la cybercriminalité et des cyberattaques et protéger **les droits de l'homme dans le cyberespace, notamment** la sécurité numérique, l'identité, la vie privée et les données des citoyens, notamment des personnes les plus vulnérables ; **207**

(Argentine)

Nouveau paragraphe 6bis

6bis. *invite* les parlements et les gouvernements des pays développés à aider les pays en développement à renforcer leurs capacités en matière de sécurité des TIC et à réduire la fracture numérique ; **208**

(Iran, République islamique d')

Nouveau paragraphe 6ter

6ter. *invite également* les parlements et leur gouvernement à ne pas adopter de mesures coercitives unilatérales qui restreignent ou empêchent l'accès de tous aux possibilités offertes par les TIC ; **209**

(Iran, République islamique d')

Paragraphe 7

Modifier le paragraphe existant comme suit :

7. *recommande vivement* aux parlements **de veiller à ce que le cadre législatif national relatif à la protection des infrastructures nationales essentielles, notamment l'infrastructure d'Internet, soit à jour, et de revoir ou** d'établir des cadres législatifs ~~visant à protéger l'infrastructure d'Internet, en particulier les câbles sous-marins, les réseaux satellitaires et les services Internet essentiels, ainsi que les grands centres de données publics et privés qui fournissent des services en nuage, lesquels devraient en retour communiquer en temps réel aux organismes nationaux et supranationaux compétents des informations sur les cyberincidents~~ **si nécessaire** ; **210**

(Suisse)

Modifier le paragraphe existant comme suit :

7. *recommande vivement* aux parlements d'établir des cadres législatifs visant à protéger ~~l'infrastructure d'Internet~~ **les infrastructures civiles essentielles**~~, en particulier les câbles sous-marins, les réseaux satellitaires et les services Internet essentiels, ainsi que les grands centres de données publics et privés qui fournissent des services en nuage, lesquels~~**, lesquelles** devraient en retour communiquer en temps réel aux organismes nationaux et supranationaux compétents des informations sur les cyberincidents ; **211**

(Suède)

Modifier le paragraphe existant comme suit :

7. *recommande vivement* aux parlements d'établir des cadres législatifs visant à protéger l'infrastructure d'Internet, en particulier les câbles sous-marins, les réseaux satellitaires et les services Internet essentiels, ~~ainsi que les grands centres de données publics et privés qui fournissent des services en nuage, lesquels devraient en retour communiquer en temps réel aux organismes nationaux et supranationaux compétents des informations sur les cyberincidents~~ **et à faciliter la collaboration avec le secteur privé** ; **212**

(Allemagne)

Modifier le paragraphe existant comme suit :

7. *recommande vivement* aux parlements d'établir des cadres législatifs ~~visant à protéger~~ **pour les fournisseurs de services Internet, afin de protéger** l'infrastructure d'Internet, en particulier les câbles sous-marins, les réseaux satellitaires et les services Internet essentiels, ainsi que les grands centres de données publics et privés qui fournissent des services en nuage, lesquels devraient en retour communiquer en temps réel aux organismes nationaux et supranationaux compétents des informations sur les cyberincidents ; **213**

(Nicaragua)

Modifier le paragraphe existant comme suit :

7. *recommande vivement* aux parlements d'établir des cadres législatifs visant à protéger l'infrastructure d'Internet, en particulier les câbles sous-marins, les réseaux satellitaires et les services Internet essentiels, ainsi que les grands centres de données publics et privés qui fournissent des services en nuage, lesquels devraient en retour communiquer en temps réel aux organismes nationaux et ~~supranationaux~~ **internationaux** compétents des informations sur les cyberincidents ; **214**

(Inde)

Modifier le paragraphe existant comme suit :

7. *recommande vivement* aux parlements d'établir des cadres législatifs visant à protéger l'infrastructure d'Internet, en particulier les câbles sous-marins, les réseaux satellitaires et les services Internet essentiels, ainsi que les grands centres de données publics et privés qui fournissent des services en nuage, lesquels devraient en retour communiquer ~~en temps réel~~ aux organismes nationaux et supranationaux compétents des informations sur les cyberincidents ; **215**

(Belgique)

Modifier le paragraphe existant comme suit :

7. *recommande vivement* aux parlements d'établir des cadres législatifs visant à protéger l'infrastructure ~~d'Internet~~ **du cyberespace**, en particulier les câbles sous-marins, les réseaux satellitaires et les services Internet essentiels, ainsi que les grands centres de données publics et privés qui fournissent des services en nuage, lesquels devraient en retour communiquer en temps réel aux organismes nationaux et supranationaux compétents des informations sur les cyberincidents ; **216**

(Lituanie)

Modifier le paragraphe existant comme suit :

7. *recommande vivement* aux parlements d'établir des cadres législatifs visant à protéger l'infrastructure d'Internet **contre les cyberattaques**, en particulier les câbles sous-marins, les réseaux satellitaires et les services Internet essentiels, ainsi que les grands centres de données publics et privés qui fournissent des services en nuage, lesquels devraient en retour communiquer en temps réel aux organismes nationaux et supranationaux compétents des informations sur les cyberincidents ; **217**

(Argentine)

Nouveau paragraphe 7bis

7bis. *recommande également* que tous les États jouent le même rôle et assument une responsabilité égale dans la gouvernance internationale d'Internet via un mécanisme multilatéral, transparent et démocratique de gouvernance internationale d'Internet ; **218**

(Iran, République islamique d')

Paragraphe 8

Modifier le paragraphe existant comme suit :

8. *encourage* les parlements à promouvoir un ~~cyberespace~~ **environnement des TIC** sûr en demandant à l'exécutif de coopérer pour ~~éradiquer la cybercriminalité~~ **mettre fin à l'utilisation des technologies de l'information et de la communication à des fins criminelles** et empêcher les cybercriminels **et les acteurs malveillants** d'agir, de donner suite aux demandes d'assistance **et de renforcement des capacités**, si possible en temps réel, de sécuriser la chaîne d'approvisionnement des entreprises de leur pays, de signaler **spontanément** les vulnérabilités potentielles à des tiers pour les aider à prévenir de futurs incidents, et en particulier de soutenir et de protéger toutes les équipes d'intervention en cas de cyberincident à l'intérieur et à l'extérieur des frontières de leur pays ; **219**

(Iran, République islamique d')

Modifier le paragraphe existant comme suit :

8. *encourage* les parlements à promouvoir un cyberespace sûr en demandant à l'exécutif de coopérer pour éradiquer ~~la cybercriminalité~~ **le détournement des TIC à des fins criminelles** et empêcher les cybercriminels d'agir, de donner suite aux demandes d'assistance, si possible en temps réel, de sécuriser la chaîne d'approvisionnement des entreprises de leur pays, de signaler les vulnérabilités potentielles à des tiers pour les aider à prévenir de futurs incidents, et en particulier de soutenir et de protéger toutes les équipes d'intervention en cas de cyberincident à l'intérieur et à l'extérieur des frontières de leur pays ; **220**

(Pakistan)

Modifier le paragraphe existant comme suit :

8. ~~*encourage*~~ ***exhorte*** les parlements à promouvoir un cyberespace sûr en demandant à l'exécutif de coopérer pour éradiquer la cybercriminalité et empêcher les cybercriminels d'agir, de donner suite aux demandes d'assistance, si possible en temps réel, de sécuriser la chaîne d'approvisionnement ~~des entreprises de leur pays~~ **avec des prestataires de services dans chaque pays**, de signaler les vulnérabilités potentielles à des tiers pour les aider à prévenir de futurs incidents, et en particulier de soutenir et de protéger toutes les équipes d'intervention en cas de cyberincident à l'intérieur et à l'extérieur des frontières de leur pays ; **221**

(Nicaragua)

Modifier le paragraphe existant comme suit :

8. *encourage* les parlements à promouvoir un cyberespace **ouvert, libre et** sûr en demandant à l'exécutif de coopérer pour ~~éradiquer~~ **lutter contre** la cybercriminalité et empêcher les cybercriminels d'agir, de donner suite aux demandes d'assistance, si possible en temps réel, de sécuriser la chaîne d'approvisionnement des entreprises de leur pays, de signaler les vulnérabilités potentielles à des tiers pour les aider à prévenir de futurs incidents, et en particulier de soutenir et de protéger toutes les équipes d'intervention en cas de cyberincident à l'intérieur et à l'extérieur des frontières de leur pays ; **222**

(République tchèque)

Modifier le paragraphe existant comme suit :

8. *encourage* les parlements à promouvoir un cyberespace sûr en demandant à l'exécutif de **se conformer aux normes de l'ONU relatives au comportement responsable des États dans le cyberespace et de** coopérer pour éradiquer la cybercriminalité et empêcher les cybercriminels d'agir, de donner suite aux demandes d'assistance, si possible en temps réel, de sécuriser la chaîne d'approvisionnement des entreprises de leur pays, de signaler les vulnérabilités potentielles à des tiers pour les aider à prévenir de futurs incidents, et en particulier de soutenir et de protéger toutes les équipes d'intervention en cas de cyberincident à l'intérieur et à l'extérieur des frontières de leur pays ; **223**

(Canada)

Modifier le paragraphe existant comme suit :

8. *encourage* les parlements à promouvoir un cyberespace sûr en demandant à l'exécutif de coopérer pour ~~éradiquer~~ **prévenir et lutter contre** la cybercriminalité ~~et empêcher les cybercriminels d'agir~~, de donner suite aux demandes d'assistance, si possible en temps réel, de sécuriser la chaîne d'approvisionnement des entreprises de leur pays, de signaler les vulnérabilités potentielles à des tiers pour les aider à prévenir de futurs incidents, et en particulier de soutenir et de protéger toutes les équipes d'intervention en cas de cyberincident à l'intérieur et à l'extérieur des frontières de leur pays ; **224**

(Lituanie)

Modifier le paragraphe existant comme suit :

8. *encourage* les parlements à promouvoir un cyberespace sûr en demandant à l'exécutif de coopérer pour ~~éradiquer~~ **atténuer l'impact des** ~~la cybercriminalité~~ **cyberattaques** et ~~empêcher les cybercriminels d'agir~~ **de la cybercriminalité**, de donner suite aux demandes d'assistance, si possible en temps réel, de sécuriser la chaîne d'approvisionnement des entreprises de leur pays, de signaler les vulnérabilités potentielles à des tiers pour les aider à prévenir de futurs incidents, et en particulier de soutenir et de protéger toutes les équipes d'intervention en cas de cyberincident à l'intérieur et à l'extérieur des frontières de leur pays ; **225**

(Argentine)

Modifier le paragraphe existant comme suit :

8. *encourage* les parlements à promouvoir un cyberespace sûr en demandant à l'exécutif de coopérer pour éradiquer la cybercriminalité et empêcher les cybercriminels d'agir, de donner suite aux demandes d'assistance **et d'échange d'informations sur les cyberincidents et les cybercriminels**, si possible en temps réel, de sécuriser la chaîne d'approvisionnement des entreprises de leur pays, de signaler les vulnérabilités potentielles à des tiers pour les aider à prévenir de futurs incidents, et en particulier de soutenir et de protéger toutes les équipes d'intervention en cas de cyberincident à l'intérieur et à l'extérieur des frontières de leur pays ; **226**

(Ukraine)

Modifier le paragraphe existant comme suit :

8. *encourage* les parlements à promouvoir un cyberespace sûr en demandant à l'exécutif de coopérer pour éradiquer la cybercriminalité et empêcher les cybercriminels d'agir, de donner suite aux demandes d'assistance, si possible en temps réel, **en conformité avec l'état de droit et en respectant pleinement le droit international des droits de l'homme et les libertés fondamentales,** de sécuriser la chaîne d'approvisionnement des entreprises de leur pays, de signaler les vulnérabilités potentielles à des tiers pour les aider à prévenir de futurs incidents, et en particulier de soutenir et de protéger toutes les équipes d'intervention en cas de cyberincident à l'intérieur et à l'extérieur des frontières de leur pays ; **227**

(Allemagne)

Modifier le paragraphe existant comme suit :

8. *encourage* les parlements à promouvoir un cyberespace sûr en demandant à l'exécutif de coopérer pour éradiquer la cybercriminalité et empêcher les cybercriminels d'agir, de donner suite aux demandes d'assistance, si possible en temps réel, de sécuriser la chaîne d'approvisionnement des entreprises de leur pays, de signaler les vulnérabilités potentielles ~~à des tiers pour les~~ **et d'**aider à prévenir de futurs incidents, et en particulier de soutenir et de protéger toutes les équipes d'intervention en cas de cyberincident à l'intérieur et à l'extérieur des frontières de leur pays ; **228**

(Inde)

Paragraphe 9

Modifier le paragraphe existant comme suit :

9. *encourage également* les parlements à élaborer des lois qui promeuvent les services transversaux de cybersécurité axés sur la prévention (sensibilisation, audit et formation) et la détection des incidents (24 heures sur 24 et 7 jours sur 7) et qui permettent de réagir immédiatement et efficacement aux ~~cybermenaces~~ **menaces liées aux TIC** ; **229**

(Iran, République islamique d')

Modifier le paragraphe existant comme suit :

9. *encourage également* les parlements **qui ne l'ont pas encore fait** à élaborer des lois qui promeuvent les services transversaux de cybersécurité axés sur la prévention (sensibilisation, audit et formation) et la détection des incidents (24 heures sur 24 et 7 jours sur 7) et qui permettent de réagir immédiatement et efficacement aux cybermenaces ; **230**

(Nicaragua)

Modifier le paragraphe existant comme suit :

9. *encourage également* les parlements à élaborer des lois qui promeuvent les services transversaux de ~~cybersécurité~~ **sécurité concernant l'utilisation des technologies de l'information et de la communication, ci-après dénommés "cybersécurité",** axés sur la prévention (sensibilisation, audit et formation) et la détection des incidents (24 heures sur 24 et 7 jours sur 7) et qui permettent de réagir immédiatement et efficacement aux **menaces pour la sécurité dans l'utilisation des technologies de l'information et de la communication, ci-après dénommées "**cybermenaces**"** ; **231**

(Fédération de Russie)

Paragraphe 10

Modifier le paragraphe existant comme suit :

10. *recommande* aux parlements ~~d'établir~~ **de promouvoir la création** ~~des~~ **d'**institutions et ~~des~~ **d'**organes adaptés – par exemple, des centres nationaux de cybersécurité, des équipes d'intervention rapide dans le domaine informatique, des équipes d'intervention en cas d'incident de sécurité informatique et des centres d'opérations de sécurité –, lorsque ceux-ci n'existent pas encore dans leur pays ; **232**

(Roumanie)

Modifier le paragraphe existant comme suit :

10. *recommande* aux parlements **de conseiller à l'exécutif** d'établir des institutions et des organes adaptés **pour prévenir la cybercriminalité et les cyberattaques** – par exemple, des centres nationaux de cybersécurité, des équipes d'intervention rapide dans le domaine informatique, des équipes d'intervention en cas d'incident de sécurité informatique et des centres d'opérations de sécurité –, lorsque ceux-ci n'existent pas encore dans leur pays ; **233**

(Thaïlande)

Paragraphe 11

Modifier le paragraphe existant comme suit :

11. *recommande également* que ~~tous~~ les parlements veillent à ce que ces institutions et organes disposent de ressources budgétaires suffisantes et de personnel spécialisé pour pouvoir réagir avec souplesse et efficacité aux cyberattaques et protéger les infrastructures stratégiques, les institutions publiques, les entreprises et les citoyens ; **234**

(République de Corée)

Modifier le paragraphe existant comme suit :

11. *recommande également* que tous les parlements veillent à ce que ces institutions et organes disposent de ressources budgétaires suffisantes et de personnel spécialisé **formé aux principes et pratiques des droits de l'homme** pour pouvoir réagir avec souplesse et efficacité aux cyberattaques et protéger les infrastructures stratégiques, les institutions publiques, les entreprises et les citoyens ; **235**

(Canada)

Modifier le paragraphe existant comme suit :

11. *recommande également* que tous les parlements veillent à ce que ces institutions et organes disposent de ressources budgétaires suffisantes et de personnel spécialisé pour pouvoir **prévenir et détecter les cyberattaques** ~~réagir~~ **et y répondre** avec souplesse et efficacité**,** ~~aux cyberattaques et protéger~~**, notamment en ce qui concerne la protection** ~~les~~ **des** infrastructures **vulnérables et** stratégiques **(comme les systèmes de gestion du trafic aérien et les réseaux électriques)**, ~~les~~ **des** institutions publiques **(comme les hôpitaux et les services de santé)**, ~~les~~ **des** entreprises et ~~les~~ **des** citoyens ; **236**

(Philippines)

Modifier le paragraphe existant comme suit :

11. *recommande également* que tous les parlements veillent à ce que ces institutions et organes disposent de ressources budgétaires suffisantes et de personnel spécialisé pour pouvoir réagir avec souplesse et efficacité **à la cybercriminalité et** aux cyberattaques et protéger les infrastructures stratégiques, les institutions publiques, les entreprises et les citoyens ; **237**

(Belgique)

Modifier le paragraphe existant comme suit :

11. *recommande également* que tous les parlements veillent à ce que ces institutions et organes disposent de ressources budgétaires suffisantes et de personnel spécialisé pour pouvoir réagir avec souplesse et efficacité aux ~~cyberattaques~~ **menaces liées aux TIC** et protéger les infrastructures stratégiques, les institutions publiques, les entreprises et les citoyens ; **238**

(Iran, République islamique d')

Modifier le paragraphe existant comme suit :

11. *recommande également* que tous les parlements veillent à ce que ces institutions et organes disposent de ressources budgétaires suffisantes et de personnel spécialisé pour pouvoir réagir ~~avec souplesse et efficacité~~ **de façon souple, rapide et efficace** aux cyberattaques et protéger les infrastructures stratégiques, les institutions publiques, les entreprises et les citoyens **sans porter atteinte à la vie privée** ; **239**

(Thaïlande)

Modifier le paragraphe existant comme suit :

11. *recommande également* que tous les parlements veillent à ce que ces institutions et organes disposent de ressources budgétaires suffisantes et de personnel spécialisé pour pouvoir réagir avec souplesse et efficacité aux cyberattaques et protéger les infrastructures **civiles** stratégiques, les institutions publiques, les entreprises et les citoyens ; **240**

(Suède)

Modifier le paragraphe existant comme suit :

11. *recommande également* que tous les parlements veillent à ce que ces institutions et organes disposent de ressources budgétaires suffisantes et de personnel spécialisé pour pouvoir réagir avec souplesse et efficacité aux cyberattaques et protéger les infrastructures stratégiques, les institutions publiques, les entreprises et les citoyens**, en tenant compte du fait que la numérisation croissante des services publics et des services collectifs peut entraîner une exposition importante aux risques numériques** ; **241**

(Argentine)

Nouveau paragraphe 11bis

11bis. *invite* les parlements à encourager l'exécutif à proposer des formations spécifiques en matière de cybersécurité afin d'accroître le nombre de spécialistes de la cybersécurité et de renforcer leurs capacités ; **242**

(Thaïlande)

Paragraphe 12

Supprimer le paragraphe. **243**

(Belgique, Canada, Égypte, Japon, Fédération de Russie)

Modifier le paragraphe existant comme suit :

12. *exhorte* les parlements à promouvoir la coordination internationale entre ces institutions et organismes ~~et la création d'un centre mondial d'opérations de sécurité, placé sous l'égide des Nations Unies, chargé~~ **afin** de surveiller, de prévenir et de détecter ~~en permanence~~ les cybermenaces, d'enquêter à leur sujet et de les combattre ; **244**

(Suisse)

Modifier le paragraphe existant comme suit :

12. *exhorte* les parlements à promouvoir la coordination internationale entre ces institutions et organismes ~~et la création d'un centre mondial d'opérations de sécurité, placé sous l'égide des Nations Unies, chargé~~ **afin** de surveiller, de prévenir et de détecter en permanence les cybermenaces, d'enquêter à leur sujet et de les combattre ; **245**

(Allemagne)

Modifier le paragraphe existant comme suit :

12. *exhorte* les parlements à promouvoir la coordination internationale entre ces institutions et organismes et la création d'un centre mondial ~~d'opérations de sécurité~~ **de cybersécurité**, placé sous l'égide des Nations Unies, chargé de surveiller, de prévenir et de détecter en permanence les cybermenaces, d'enquêter à leur sujet et de les combattre ; **246**

(France)

Modifier le paragraphe existant comme suit :

12. *exhorte* les parlements à promouvoir la coordination internationale entre ces institutions et organismes et la création d'un centre mondial d'opérations de sécurité, placé sous l'égide des Nations Unies, chargé de surveiller~~, de prévenir~~ et de détecter en permanence les cybermenaces **mondiales**, d'enquêter à leur sujet et de les combattre**, en coopération avec les équipes nationales d'intervention en cas de cyberincident des États membres, afin de contribuer à la prévention de ces menaces** ; **247**

(Türkiye)

Modifier le paragraphe existant comme suit :

12. *exhorte* les parlements à promouvoir la coordination internationale entre ces institutions et organismes et la création d'un centre mondial d'opérations de sécurité, placé sous l'égide des Nations Unies, chargé de surveiller, de prévenir et de détecter en permanence les ~~cybermenaces~~ **menaces liées aux TIC**, d'enquêter à leur sujet et de les combattre ; **248**

(Iran, République islamique d')

Modifier le paragraphe existant comme suit :

12. *exhorte* les parlements à promouvoir la coordination internationale entre ces institutions et organismes et la création d'un centre mondial d'opérations de sécurité, placé sous l'égide des Nations Unies, chargé de surveiller, de prévenir et de détecter en permanence les cybermenaces, d'enquêter à leur sujet et de les combattre**, tout en définissant clairement la portée de son mandat par rapport à d'autres organes pertinents des Nations Unies, comme le Conseil des chefs de secrétariat, par le biais du Comité de haut niveau sur les programmes et du cadre sur la cybersécurité et la cybercriminalité à l'échelle du système des Nations Unies** ; **249**

(Suède)

Nouveau paragraphe 12bis

12bis. *demande* aux gouvernements et à la communauté internationale de collaborer sur les moyens permettant de démasquer les acteurs et les entités à l'origine de ces cyberattaques et de les amener à répondre de leurs actes en engageant des poursuites pénales et en appliquant les sanctions correspondantes ; **250**

(Philippines)

Paragraphe 13

Supprimer le paragraphe. **251**

(Belgique, Canada, Égypte, Allemagne, Fédération de Russie, Suisse)

Modifier le paragraphe existant comme suit :

13. *recommande* ~~que cette entité aide~~ **qu'une assistance technique et un renforcement des capacités soient fournis à** tous les pays, en particulier ceux qui disposent de moins de ressources, **pour les aider** à développer leurs capacités d'action et de réaction, à mutualiser leurs informations, leurs connaissances et les résultats de leurs recherches, de manière à anticiper les ~~futurs enjeux technologiques tels que l'informatique quantique, la 5G, le métavers et l'intelligence artificielle~~ **technologies**, et à tirer**, en toutes circonstances,** la sonnette d'alarme en cas de violation de la Déclaration universelle des droits de l'homme~~, et ce en toutes circonstances~~ ; **252**

(République tchèque)

Modifier le paragraphe existant comme suit :

13. *recommande* que cette entité aide ~~tous~~ les pays, en particulier ceux qui disposent de moins de ressources, à développer leurs capacités d'action et de réaction, à mutualiser leurs informations, leurs connaissances et les résultats de leurs recherches, de manière à anticiper les futurs enjeux technologiques tels que l'informatique quantique, la 5G, le métavers et l'intelligence artificielle, et à tirer la sonnette d'alarme en cas de violation de la Déclaration universelle des droits de l'homme, et ce en toutes circonstances ; **253**

(République de Corée)

Modifier le paragraphe existant comme suit :

13. *recommande* que cette entité aide tous les pays, en particulier ~~ceux qui disposent de moins de ressources~~ **les pays en développement**, à développer leurs capacités d'action et de réaction, à mutualiser leurs informations, leurs connaissances et les résultats de leurs recherches, de manière à anticiper les futurs enjeux technologiques tels que l'informatique quantique, la 5G, le métavers et l'intelligence artificielle, et à tirer la sonnette d'alarme en cas de violation de la Déclaration universelle des droits de l'homme, et ce en toutes circonstances ; **254**

(Iran, République islamique d')

Modifier le paragraphe existant comme suit :

13. *recommande* que cette entité aide tous les pays, en particulier ceux qui disposent de moins de ressources, à développer leurs capacités d'action et de réaction~~,~~ **et** à mutualiser leurs informations, leurs connaissances et les résultats de leurs recherches, de manière à anticiper les futurs enjeux technologiques tels que l'informatique quantique, la 5G, le métavers et l'intelligence artificielle~~, et à tirer la sonnette d'alarme en cas de violation de la Déclaration universelle des droits de l'homme, et ce en toutes circonstances~~ ; **255**

(Inde)

Modifier le paragraphe existant comme suit :

13. *recommande* que cette entité aide tous les pays, en particulier ceux qui disposent de moins de ressources, à développer leurs capacités d'action et de réaction, à mutualiser leurs informations, leurs connaissances et les résultats de leurs recherches, de manière à anticiper les futurs enjeux technologiques tels que l'informatique quantique, la 5G, le métavers et l'intelligence artificielle~~,~~ ~~et à tirer la sonnette d'alarme en cas de violation de la Déclaration universelle des droits de l'homme, et ce en toutes circonstances~~ **et à accroître leur résilience face aux cybermenaces ;** **256**

(France)

Modifier le paragraphe existant comme suit :

13. *recommande* que cette entité aide tous les pays, en particulier ceux qui disposent de moins de ressources, à développer leurs capacités d'action et de réaction, à mutualiser leurs informations, leurs connaissances et les résultats de leurs recherches, de manière à anticiper les futurs enjeux technologiques tels que l'informatique quantique, la 5G, le métavers et l'intelligence artificielle, et à tirer la sonnette d'alarme en cas de violation de ~~la Déclaration universelle des droits de l'homme, et ce en toutes circonstances~~ **droits de l'homme universellement reconnus causée par des événements survenant dans leur zone de responsabilité** ; **257**

(Ukraine)

Modifier le paragraphe existant comme suit :

13. *recommande* que cette entité aide tous les pays, en particulier ceux qui disposent de moins de ressources, à développer leurs capacités d'action et de réaction, à mutualiser leurs informations, leurs connaissances et les résultats de leurs recherches, de manière à anticiper les futurs enjeux technologiques tels que l'informatique quantique, la 5G, le métavers et l'intelligence artificielle, et à tirer la sonnette d'alarme en cas de violation de la Déclaration universelle des droits de l'homme **ou d'autres instruments relatifs aux droits de l'homme**, et ce en toutes circonstances ; **258**

(Suède)

Nouveau paragraphe 13bis

13bis. *réaffirme* qu'un environnement des TIC ouvert, sûr, stable, accessible et pacifique est essentiel pour tous et nécessite une coopération efficace entre les États afin de réduire les risques pour la paix et la sécurité internationale, et *invite* la communauté internationale à promouvoir le plein respect des droits de l'homme et des libertés fondamentales ; **259**

(Allemagne)

Paragraphe 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**

(Iran, République islamique d')

Operative paragraph 15

Supprimer le paragraphe. **262**

(Inde)

Modifier le paragraphe existant comme suit :

14. *demande* aux parlements d'encourager l'investissement dans la recherche et le développement, en intégrant dans les projets et propositions de loi des dispositions spécifiques ~~en matière de cybersécurité~~ **relatives à la sécurité des TIC** et en prévoyant des crédits budgétaires suffisants, afin d'anticiper les éventuelles ~~cybermenaces~~ **menaces** émergentes **liées aux TIC** et de s'en protéger ; **263**

(Iran, République islamique d')

Modifier le paragraphe existant comme suit :

15. *encourage* les parlements à établir des partenariats avec les entreprises, le monde universitaire et toutes les autres parties prenantes, y compris la société civile, **en chargeant l'exécutif de jouer le rôle de facilitateur,** afin de développer un écosystème de cybersécurité solide et collaboratif ; **264**

(Thaïlande)

Modifier le paragraphe existant comme suit :

15. *encourage* les parlements à établir des partenariats avec les entreprises, le monde universitaire et toutes les autres parties prenantes, y compris la société civile, afin de développer un écosystème de cybersécurité solide et collaboratif **qui respecte pleinement les principes des droits de l'homme et les obligations internationales en la matière** ; **265**

(Canada)

Modifier le paragraphe existant comme suit :

15. *encourage* les parlements à établir des partenariats avec les entreprises, le monde universitaire et toutes les autres parties prenantes, y compris la société civile, afin de développer un écosystème de cybersécurité solide et collaboratif**, sans préjudice de l'établissement de régimes garantissant que les fournisseurs de services et d'applications Internet communiquent rapidement les informations relatives aux traces et indications réclamées par les tribunaux de différents pays, dans la mesure où ces informations peuvent constituer des preuves numériques pour les enquêtes sur les actes de cybercriminalité au niveau local, quel que soit leur siège régional ou la réglementation en matière de protection de la vie privée du pays dans lequel ces informations sont stockées** ; **266**

(Argentine)

Paragraphe 16

Supprimer le paragraphe. **267**

(Belgique, Canada)

Modifier le paragraphe existant comme suit :

16. *encourage également* les parlements à ~~créer des espaces législatifs qui permettent aux~~ **instaurer la confiance, afin que les** parlements, ~~aux~~ **les** gouvernements, ~~aux~~ **les** entreprises, ~~au~~ **le** monde universitaire et ~~à~~ la société civile ~~de~~ **puissent** coopérer en temps réel pour défendre l'intérêt général de tous les États ; **268**

(Inde)

Modifier le paragraphe existant comme suit :

16. *encourage également* les parlements à créer des espaces législatifs qui permettent aux parlements, aux gouvernements, aux entreprises, au monde universitaire et à la société civile de coopérer en temps réel**, en conformité avec l'état de droit et en respectant pleinement le droit international des droits de l'homme et les libertés fondamentales,** pour défendre l'intérêt général de tous les États ; **269**

(Allemagne)

Nouveau paragraphe 16bis

16bis. *demande* aux parlements et à l'exécutif de traiter la question du manque de responsabilité des fournisseurs de services et des plateformes transnationales, qui constitue une grave menace dans l'environnement des TIC; **270**

(Iran, République islamique d')

Paragraphe 17

Modifier le paragraphe existant comme suit :

17. *demande* aux parlements et aux parlementaires de s'employer activement à faire émerger, au niveau national, une compréhension commune et actualisée de la nature de ~~la cybercriminalité~~ **l'utilisation des technologies de l'information et de la communication à des fins criminelles** et des ~~cyberattaques~~ **menaces liées aux TIC** telles qu'elles sont vécues par les citoyens, les organisations et les institutions ; **271**

(Iran, République islamique d')

Modifier le paragraphe existant comme suit :

17. *demande* aux parlements et aux parlementaires de s'employer activement à faire émerger, au niveau national, une compréhension commune et actualisée de la nature ~~de la cybercriminalité~~ **du détournement des TIC à des fins criminelles** et des cyberattaques ~~telles qu'elles~~ **tels qu'ils** sont ~~vécues~~ **vécus** par les citoyens, les organisations et les institutions ; **272**

(Pakistan)

Modifier le paragraphe existant comme suit :

17. *demande* aux parlements et aux parlementaires de s'employer activement à faire émerger, au niveau national, une compréhension commune et actualisée de la nature de la cybercriminalité ~~et des cyberattaques telles qu'elles sont vécues~~ **telle qu'elle est vécue** par les citoyens, les organisations et les institutions ; **273**

(Belgique, République tchèque, Suède)

Modifier le paragraphe existant comme suit :

17. *demande* aux parlements et aux parlementaires de s'employer activement à faire émerger, au niveau national, une compréhension commune et actualisée de la nature de la cybercriminalité et des cyberattaques telles qu'elles sont vécues par les citoyens, les organisations et les institutions, **lorsque ladite compréhension est inexistante dans le pays** ; **274**

(Nicaragua)

Paragraphe 18

Supprimer le paragraphe. **275**

(Inde)

Modifier le paragraphe existant comme suit :

18. *exhorte* les parlements à contribuer à développer une véritable "culture de la cybersécurité" en élaborant des programmes d'enseignement destinés à former, dès l'enfance, les générations futures à ~~l'utilisation des outils technologiques~~ **l'apprentissage numérique et au savoir-faire technologique**, aussi bien en ce qui concerne les vastes possibilités qu'ils offrent que les risques importants qui y sont associés ; **276**

(Thaïlande)

Nouveau paragraphe 18bis

18bis. *exhorte également* les parlements à promouvoir, dans l'ensemble de leurs activités liées à la lutte contre la cybercriminalité et les cyberincidents malveillants, les obligations découlant du droit international des droits de l'homme et le plein respect des droits de l'homme et des libertés fondamentales ainsi que de l'état de droit ; **277**

(Canada)

Paragraphe 19

Supprimer le paragraphe. **278**

(Iran, République islamique d')

Modifier le paragraphe existant comme suit :

19. *recommande* aux parlements de renforcer la protection des ~~femmes, des jeunes et des autres~~ groupes vulnérables**, notamment des enfants et des personnes âgées,** dans le cyberespace, en veillant au respect des droits de l'homme et en prévoyant dans les politiques pédagogiques relatives à l'utilisation des réseaux sociaux des dispositifs permettant de prévenir la violence sexiste ; **279**

(Allemagne)

Modifier le paragraphe existant comme suit :

19. *recommande* aux parlements de renforcer la protection des femmes, des ~~jeunes~~ **enfants, des personnes âgées** et des autres groupes vulnérables dans le cyberespace, en veillant au respect des droits de l'homme et en prévoyant dans les politiques pédagogiques relatives à l'utilisation des réseaux sociaux des dispositifs permettant de prévenir la violence sexiste ; **280**

(République tchèque)

Modifier le paragraphe existant comme suit :

19. *recommande* aux parlements de renforcer la protection des femmes, des jeunes **et des personnes âgées, des enfants** et des autres groupes vulnérables dans le cyberespace, en veillant au respect des droits de l'homme et en prévoyant dans les politiques pédagogiques relatives à l'utilisation des réseaux sociaux des dispositifs permettant de prévenir la violence sexiste ; **281**

(Viet Nam)

Modifier le paragraphe existant comme suit :

19. *recommande* aux parlements de renforcer la protection des femmes, **des enfants,** des jeunes et des autres groupes vulnérables dans le cyberespace, en veillant au respect des droits de l'homme et en prévoyant dans les politiques pédagogiques relatives à l'utilisation des réseaux sociaux des dispositifs permettant de prévenir la violence sexiste ; **282**

(Roumanie)

Modifier le paragraphe existant comme suit :

19. *recommande* aux parlements de renforcer la protection des femmes, des jeunes**, des personnes âgées** et des autres groupes vulnérables dans le cyberespace, en veillant au respect des droits de l'homme et en prévoyant dans les politiques pédagogiques relatives à l'utilisation des réseaux sociaux des dispositifs permettant de prévenir la violence sexiste ; **283**

(Türkiye)

Modifier le paragraphe existant comme suit :

19. *recommande* aux parlements de renforcer la protection des femmes, des jeunes**, des populations racisées** et des autres groupes vulnérables dans le cyberespace, en veillant au respect des droits de l'homme et en prévoyant dans les politiques pédagogiques relatives à l'utilisation des réseaux sociaux des dispositifs permettant de prévenir la violence sexiste ; **284**

(Canada)

Modifier le paragraphe existant comme suit :

19. *recommande* aux parlements de renforcer la protection des femmes, des jeunes**, des personnes handicapées** et des autres groupes vulnérables dans le cyberespace, en veillant au respect des droits de l'homme et en prévoyant dans les politiques pédagogiques relatives à l'utilisation des réseaux sociaux des dispositifs permettant de prévenir la violence sexiste ; **285**

(Finlande)

Nouveau paragraphe 19bis

19bis. *invite* les parlements à organiser une collaboration multipartite entre le gouvernement et le secteur privé afin d'institutionnaliser la technologie en tant qu'outil permettant de sensibiliser au harcèlement sexuel et de lutter contre la violence en ligne à l'égard des femmes et des enfants ; **286**

(Philippines)

Paragraph 20

Supprimer le paragraphe. **287**

(Inde)

Modifier le paragraphe existant comme suit :

20. *exhorte* les parlements à prendre les mesures nécessaires pour ~~protéger les moments cruciaux de la démocratie, notamment les périodes où les citoyens exercent leur droit de vote, afin d'éviter les attaques et les interférences qui visent à influencer, modifier ou violer la libre formation de l'opinion des citoyens pendant les processus électoraux~~ **empêcher l'ingérence dans les affaires intérieures d'un État par l'utilisation des technologies de l'information et de la communication** ; **288**

(Fédération de Russie)

Paragraphe 21

Supprimer le paragraphe. **289**

(Inde, Iran (République islamique d')

Modifier le paragraphe existant comme suit :

21. *demande* à la communauté internationale de prendre des mesures pour protéger ~~la démocratie~~ **les systèmes de technologies de l'information et de la communication utilisés par les autorités gouvernementales** en veillant à ce que tous les parlements du monde, en tant qu'institutions représentant la volonté du peuple, bénéficient d'une protection particulière du fait de leur inscription sur les listes d'infrastructures nationales critiques et de services essentiels ; **290**

(Fédération de Russie)

Modifier le paragraphe existant comme suit :

21. *demande* à la communauté internationale de prendre des mesures pour protéger la démocratie en veillant à ce que tous les parlements du monde, en tant qu'institutions représentant la volonté du peuple, bénéficient d'une protection particulière du fait de leur inscription sur les listes d'infrastructures ~~nationales~~ **civiles** critiques et de services essentiels ; **291**

(Suède)

Nouveau paragraphe 21bis

21bis. *souligne* la nécessité de renforcer encore la coopération et l'assistance internationales dans le domaine de la sécurité des TIC et du renforcement des capacités, afin de réduire la fracture numérique et de renforcer la lutte contre les cybermenaces à travers le monde ; **292**

(Roumanie)

Paragraphe 22

Modifier le paragraphe existant comme suit :

22. *demande* aux parlements d'appréhender plus en profondeur la nature complexe et évolutive de ~~la cybercriminalité~~ **l'utilisation des technologies de l'information et de la communication à des fins criminelles** et des ~~cyberattaques~~ **menaces liées aux TIC** en organisant des séminaires, ateliers et conférences spécialisés sur cette question ; **293**

(Iran, République islamique d')

Modifier le paragraphe existant comme suit :

22. *demande* aux parlements d'appréhender plus en profondeur la nature complexe et évolutive de la cybercriminalité et des ~~cyberattaques~~ **cyberincidents** en organisant des séminaires, ateliers et conférences spécialisés sur cette question ; **294**

(Inde)

Modifier le paragraphe existant comme suit :

22. *demande* aux parlements d'appréhender plus en profondeur la nature complexe et évolutive ~~de la cybercriminalité~~ **du détournement des TIC à des fins criminelles** et des cyberattaques en organisant des séminaires, ateliers et conférences spécialisés sur cette question ; **295**

(Pakistan)

Modifier le paragraphe existant comme suit :

22. *demande* aux parlements d'appréhender plus en profondeur la nature complexe et ~~évolutive~~ **l'évolution rapide** de la cybercriminalité ~~et des cyberattaques~~ en organisant des séminaires, ateliers et conférences spécialisés sur cette question ; **296**

(Suède)

Modifier le paragraphe existant comme suit :

22. *demande* aux parlements d'appréhender plus en profondeur la nature complexe et évolutive de la cybercriminalité et des cyberattaques en **facilitant le libre partage des connaissances, des données d'expérience et des compétences** ~~organisant des~~ **par la tenue de** séminaires, **d'**ateliers et **de** conférences spécialisés sur cette question ; **297**

(Afrique du Sud)

Modifier le paragraphe existant comme suit :

22. *demande* aux parlements **qui ne l'ont pas encore fait** d'appréhender plus en profondeur la nature complexe et évolutive de la cybercriminalité et des cyberattaques en organisant des séminaires, ateliers et conférences spécialisés sur cette question ; **298**

(Nicaragua)

Paragraphe 23

Supprimer le paragraphe. **299**

(Fédération de Russie)

Modifier le paragraphe existant comme suit :

23. *invite* ~~le Secrétariat de~~ l'UIP, de concert avec les organisations concernées, à promouvoir cette nouvelle vision de la cybersécurité en soutenant les parlements dans leurs efforts de renforcement des capacités ; **300**

(Belgique)

Modifier le paragraphe existant comme suit :

23. *invite* le Secrétariat de l'UIP, de concert avec les organisations concernées, à promouvoir cette nouvelle vision de la ~~cybersécurité~~ **sécurité des TIC** en soutenant les parlements dans leurs efforts de renforcement des capacités ; **301**

(Iran, République islamique d')

Modifier le paragraphe existant comme suit :

23. *invite* le Secrétariat de l'UIP, de concert avec les organisations concernées, à promouvoir cette nouvelle vision de la cybersécurité en soutenant les parlements dans leurs efforts de renforcement des capacités**, et à se fixer comme objectif stratégique d'encourager les parlements à créer des centres internes de renseignement sur la cybersécurité pour partager et échanger leurs informations, leurs renseignements, leur expertise et leurs bonnes pratiques, en vue d'élargir la connaissance commune dans le domaine de la cybersécurité** ; **302**

(Thaïlande)

Paragraphe 24

Modifier le paragraphe existant comme suit :

24. recommande que l'UIP~~, en tant qu'organisation mondiale des parlements, puisse jouer un rôle prépondérant dans la gouvernance internationale d'Internet et la cyber-résilience en participant à tous les forums internationaux pertinents, notamment ceux organisés par les Nations Unies, pour faire entendre la voix des parlements, afin de prévoir toute cybermenace à la sécurité, aux moyens de subsistance ou au mode de vie des citoyens, et de pouvoir s'y préparer, y résister, y répondre et la surmonter~~ **contribue à l'internationalisation de la gestion d'Internet, à la participation égale de tous les États à ce processus et à la préservation du droit souverain des États de réglementer leur segment national du réseau Internet mondial**. **303**

(Fédération de Russie)

Modifier le paragraphe existant comme suit :

24. *recommande* que l'UIP, en tant qu'organisation mondiale des parlements, puisse jouer un rôle prépondérant dans la ~~gouvernance internationale d'Internet~~ **prévention et la lutte contre la cybercriminalité** et la **promotion de la** cyber-résilience en participant à tous les forums internationaux pertinents, notamment ceux organisés par les Nations Unies, pour faire entendre la voix des parlements, afin de prévoir toute cybermenace à la sécurité, aux moyens de subsistance**, aux droits de l'homme** ou au mode de vie des citoyens, et de pouvoir s'y préparer, y résister, y répondre et la surmonter. **304**

(Belgique)

Modifier le paragraphe existant comme suit :

24. *recommande* que l'UIP, en tant qu'organisation mondiale des parlements, puisse jouer un rôle prépondérant dans la gouvernance internationale d'Internet et la cyber-résilience en ~~participant à tous~~ **renforçant ses partenariats avec** les forums internationaux pertinents, notamment ceux organisés par les Nations Unies, pour faire entendre la voix des parlements, afin de prévoir toute cybermenace à la sécurité, aux moyens de subsistance ou au mode de vie des citoyens, et de pouvoir s'y préparer, y résister, y répondre et la surmonter. **305**

(République de Corée)

Modifier le paragraphe existant comme suit :

24. *recommande* que l'UIP, en tant qu'organisation mondiale des parlements, puisse jouer un rôle prépondérant dans la gouvernance internationale d'Internet et la cyber-résilience en participant à tous les forums internationaux pertinents, notamment ceux organisés par les Nations Unies, pour faire entendre la voix des parlements~~, afin de prévoir toute cybermenace à la sécurité, aux moyens de subsistance ou au mode de vie des citoyens, et de pouvoir s'y préparer, y résister, y répondre et la surmonter~~. **306**

(France)

Modifier le paragraphe existant comme suit :

24. *recommande* que l'UIP, en tant qu'organisation mondiale des parlements, puisse jouer un rôle prépondérant dans la gouvernance internationale d'Internet et la cyber-résilience en participant à tous les forums internationaux pertinents, notamment ceux organisés par les Nations Unies, pour faire entendre la voix des parlements, afin de prévoir toute ~~cybermenace~~ **menace posée par les TIC** à la sécurité, aux moyens de subsistance ou au mode de vie des citoyens, et de pouvoir s'y préparer, y résister, y répondre et la surmonter. **307**

(Iran, République islamique d')

Modifier le paragraphe existant comme suit :

24. *recommande* que l'UIP, en tant qu'organisation mondiale des parlements, puisse jouer un rôle prépondérant dans la gouvernance internationale d'Internet et la cyber-résilience en participant à tous les forums internationaux pertinents, notamment ceux organisés par les Nations Unies, pour faire entendre la voix des parlements, afin de prévoir toute cybermenace à la sécurité, aux moyens de subsistance ou au mode de vie des citoyens, et de pouvoir s'y préparer, y résister, y répondre et la surmonter**, après consultation des États parties**. **308**

(*Nicaragua)*

Nouveau paragraphe 24bis

24bis. ***préconise*** **de créer un groupe de travail sur les cyberattaques et la cybercriminalité, sous l'égide du Conseil directeur de l'UIP, avec pour mission de se conformer aux mandats et objectifs établis dans la présente résolution, et qui sera chargé de soutenir le processus de promotion d'une convention internationale sur la cybercriminalité dans le cadre du système des Nations Unies, et de renforcer les capacités des Parlements nationaux membres de l'UIP en matière d'élaboration des lois, de contrôle et de budgétisation.** **309**

(Argentine)

24bis. ***recommande*** **également que l'UIP sensibilise les parlements à la réalisation des ODD en faisant valoir, en premier lieu, leurs engagements universels en matière de sécurité numérique.** **310**

(Thaïlande)

Nouveau paragraphe 24ter

24ter. ***exhorte*** **les organisations internationales à discuter d'une convention sur les actes de cyberguerre dans le cadre des travaux relatifs au maintien de la paix et de la sécurité internationale*.*** **311**

(Argentine)

TITRE

Modifier le titre comme suit :

312

~~Cyberattaques et~~ **Cybercriminalité** : les nouveaux risques pour la sécurité mondiale

(République tchèque)

Modifier le titre comme suit :

313

~~Cyberattaques~~ **Cyberincidents** et cybercriminalité : les nouveaux risques pour la sécurité mondiale

(Inde)

Modifier le titre comme suit :

~~Cyberattaques et cybercriminalité~~ **La menace des TIC et l'utilisation des technologies de l'information et de la communication à des fins criminelles** : les nouveaux risques pour la sécurité mondiale **314**

(Iran, République islamique d')

Modifier le titre comme suit :

Cyberattaques et cybercriminalité : ~~les nouveaux~~ **l'augmentation des** risques pour la sécurité mondiale **315**

(Lituanie)

Modifier le titre comme suit :

Cyberattaques et ~~cybercriminalité~~ **détournement des TIC à des fins criminelles** : les nouveaux risques pour la sécurité mondiale **316**

(Pakistan)

Modifier le titre comme suit :

~~Cyberattaques et~~ Cybercriminalité : ~~les nouveaux~~ **l'évolution** des risques pour la sécurité mondiale **317**

(Suède)