Compte-rendu sur les évolutions relatives au cyberespace au sein de l'ONU

Rapport sur les discussions relatives au cyberespace au sein des Nations Unies

Veni Markovski
Alexey Trepykhalin
3 juin 2021
GE-009

ICANN

TABLE DES MATIERES

Introduction

Ce document fait état des échanges récents qui ont eu lieu au sein des différents groupes de l'Assemblée Générale des Nations Unies (ONU), dans lesquels se tiennent les discussions relatives aux questions de cybersécurité. Il comprend un compte-rendu des délibérations récentes qui ont eu lieu au sein du premier Groupe de travail à composition non limitée (OEWG), du Groupe d'experts gouvernementaux (GGE) et du Comité spécial d'experts à composition non limitée (AHC[1]) entre le 1er juillet 2020 et le 3 juin 2021.

Ce document fait partie d'une série de rapports périodiques qui donnent un aperçu des activités qui ont lieu à l'ONU et qui sont pertinentes pour l'écosystème de l'Internet et la mission de l'ICANN.[2] Le suivi de ces activités démontre l'engagement et la responsabilité de l'équipe en charge de la relation avec les gouvernements et les organisations intergouvernementales (GE) de l'organisation ICANN (ICANN Org), qui tient la communauté élargie de l'ICANN informée des questions d'importance pour un Internet mondial, unique et interopérable et pour son système d'identificateurs uniques.[3]

Compte-rendu du Groupe de travail à composition non limitée (OEWG)

Depuis la publication en juillet 2020 par l'organisation ICANN des discussions relatives au cyberespace ayant eu lieu à l'ONU, le Groupe de travail a tenu cette année trois autres séries de consultations informelles (du 29 septembre au 1er octobre, du 17 au 19 novembre et du 1er au 3 décembre). Au cours de ces consultations, le secrétariat du Groupe de travail a reçu un certain nombre de commentaires et de contributions des États membres dans le cadre du processus officiel et des organisations non gouvernementales dans le cadre des consultations informelles engagées par le président du Groupe de travail.

Ci-dessous figure le résumé de l'équipe GE de l'organisation ICANN. Il se limite aux contributions au Groupe de travail qui sont en lien avec la mission de l'ICANN. Voici une liste de ces contributions, organisées par date.

Le 2 juillet 2020, République de Finlande : « De même, nous tenons à soutenir fermement la proposition des Pays-Bas sur la protection de l'intégrité et de la disponibilité du noyau public de l'Internet ainsi que ses suggestions concrètes concernant la portée des normes relatives aux infrastructures critiques (13f et 13g). »[4]

---

[1] Dans les compte-rendu précédents, nous avons utilisé l'abréviation OECE. Or, lors de la séance d'inauguration du comité, nous avons noté que les États membres de l'ONU utilisent l'abréviation AHC (Comité ad-hoc). Dans un souci de cohérence, l'ICANN a donc modifié la formule utilisée. Le nom complet de ce comité est « Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles ».

[2] Consulter les rapports précédents de l'équipe GE : https://www.icann.org/resources/pages/government-engagement-publications-2020-03-02-en. L'accès à cette URL, ainsi qu'à toutes les autres URL qui figurent dans les notes en bas de page et dans les annexes, a été effectué le 3 juin 2021.

[3] « Plans opérationnels et financiers de l'ICANN », p. 47, organisation ICANN, décembre 2020 https://www.icann.org/en/system/files/files/draft-op-financial-plan-fy21-25-opplan-fy21-20dec19-en.pdf

[4] « Déclarations de la République de Finlande » au Groupe de travail à composition non limitée sur l'évolution de la situation dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale, consultations virtuelles officieuses, 19 juin et 2 juillet 2020,

Le 19 novembre 2020, République islamique d'Iran : « Ces sanctions numériques [unilatérales] ont affecté les investissements dans les infrastructures des TIC ainsi que l'accès aux technologies numériques, aux ressources numériques telles que les IP et le système du DNS et aux réseaux, ce qui constitue non seulement un obstacle à la réalisation des objectifs nationaux de développement liés aux TIC, mais aussi une violation des droits humains. »[5]

Le 19 janvier 2021, Royaume des Pays-Bas : « La phrase 'les acteurs étatiques et non étatiques ne doivent ni conduire ni autoriser sciemment une activité qui nuit intentionnellement et substantiellement à la disponibilité ou à l'intégrité générales du noyau public de l'Internet, et par conséquent à la stabilité du cyberespace' [pourrait être] une orientation pour la mise en œuvre de la recommandation 13(f) de 2015 du GGE de l'ONU et, par conséquent, pourrait également relever du champ d'application de la recommandation 13(g) de 2015 du GGE de l'ONU. »[6]

Le 19 février 2021, République de Slovénie : « Nous souhaitons également soutenir les appels lancés par les Pays-Bas à mettre davantage l'accent sur la protection du noyau public de l'Internet. »[7]

Le 19 février 2021, République Fédérale d'Allemagne : « Suggestion d'inclure une référence aux menaces pour le noyau public de l'Internet, comme par ailleurs mentionné au paragraphe 50 de l'avant-projet, dans la section sur les menaces existantes et potentielles »[8]

Du 19 au 22 février 2021, Royaume des Pays-Bas : « Au fil des années, les cyber-opérations portant atteinte à l'intégrité, au bon fonctionnement et à la disponibilité de l'Internet se sont révélées une menace réelle et crédible. Cela a été évoqué sous le terme « noyau public » dans la version préalable au projet du Groupe de travail. Alors que nous nous efforçons de parvenir à un consensus, nous avons contacté les pays qui avaient exprimé des préoccupations au cours de nos discussions précédentes et nous sommes parvenus à un nouveau libellé qui semble répondre à cette préoccupation. Je cite : 'l'infrastructure technique essentielle à la disponibilité ou à l'intégrité générale de l'Internet'. »[9]

---

https://front.un-arm.org/wp-content/uploads/2020/09/oewg-informal-virtual-meetings-statement-by-finland-19-june-and-2-july-2020.pdf

[5] « Version préalable révisée du rapport du Groupe de travail », troisième réunion virtuelle informelle du Groupe de travail, intervention de la délégation de la République islamique d'Iran, « renforcement des capacités » du 19 novembre 2020, https://front.un-arm.org/wp-content/uploads/2020/11/iran-intervention-on-capacity-building-19-nov-2020.pdf

[6] « Document officieux énumérant des propositions linguistiques spécifiques au titre du point de l'ordre du jour 'règles, normes et principes' provenant des communications écrites des délégations », version du 18 janvier 2021, https://front.un-arm.org/wp-content/uploads/2021/01/OEWG-Non-paper-rules-norms-and-principles-19-01-2021.pdf

[7] Groupe de travail à composition non limitée sur l'évolution de la situation dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale, réunion virtuelle informelle (18, 19 et 22 février 2021), Slovénie, déclaration, 19 février 2021, https://front.un-arm.org/wp-content/uploads/2021/02/Slovenia-19-February-2021-FINAL.pdf

[8] Commentaires de l'Allemagne sur l'avant-projet du rapport du Groupe de travail, 19 février 2021, https://front.un-arm.org/wp-content/uploads/2021/02/Germany-Written-Contribution-OEWG-Zero-Draft-Report_clean.pdf

[9] Déclaration de Son Excellence Nathalie Jaarsma, Royaume des Pays-Bas, auprès de l'Organisation des Nations Unies, (18,19 et 22 février 2021), https://front.un-arm.org/wp-content/uploads/2021/02/Netherlands-OEWG-informals-intervention-Feb-2021.pdf

Le 23 février 2021, Royaume-Uni : « Nous remercions les Pays-Bas de travailler avec nous et avec d'autres en vue de clarifier leur proposition sur le « noyau public » et nous saluons l'inclusion du texte de compromis. »[10]

Le 25 février 2021, Royaume des Pays-Bas : « Conformément au texte sur la protection du noyau public qui a été inclus dans la version préalable au projet, compte tenu de la convergence sur le libellé exact, nous proposons ce qui suit : nous souhaitons proposer de modifier la formulation de la dernière phrase du paragraphe 21 sur « l'intégrité, le fonctionnement et la disponibilité » et de mentionner la [nécessité de protéger] « l'infrastructure technique essentielle à la disponibilité ou à l'intégrité générales de l'Internet.

En outre, nous tenons à ce que l'importance de la « protection de l'infrastructure technique essentielle à la disponibilité ou à l'intégrité générales de l'Internet » soit aussi mentionnée dans la section conclusion/recommandation des règles, normes et principes. »[11]

Le 3 mars 2021, Commission mondiale sur la stabilité du cyberespace (GCSC) : « Si la Commission a été satisfaite de constater que, dans le rapport préalable précédent, un certain nombre des recommandations de la GCSC avaient été prises en compte, nous regrettons que bon nombre de ces recommandations n'aient été incluses ni dans l'avant-projet, ni dans la première version actuelle. Ceci concerne en particulier la norme visant à protéger le noyau public de l'Internet, qui, selon nous, a été bien accueillie par de nombreux États, ainsi que par les observateurs de la société civile et du secteur privé. »[12]

Le 8 mars 2021, République islamique d'Iran : « Les plateformes et les sociétés transnationales comme l'ICANN doivent être tenues responsables. »[13]

Le 8 mars 2021, Cybersecurity Tech Accord : « L'attaque récente de SolarWinds a mis en évidence qu'aucune organisation ne pouvait se considérer à l'abri d'un adversaire doté des ressources nécessaires et suffisamment déterminé. Elle a également montré à quel point les acteurs de la menace les plus habiles sont prêts à tout pour saper la confiance en des processus essentiels et en le noyau public de l'Internet par la conduite d'une attaque. »[14]

---

[10] Commentaires du Royaume-Uni sur l'avant-projet du Groupe de travail concernant l'évolution de la situation dans le domaine des TIC dans le contexte de la sécurité internationale, 23 février 2021, https://front.un-arm.org/wp-content/uploads/2021/02/UK-submission-to-OEWG-ICTs-zero-draft-002.pdf

[11] Pays-Bas – propositions incluses dans l'avant-projet du Groupe de travail, février 2021, https://front.un-arm.org/wp-content/uploads/2021/02/Netherlands-OEWG-written-comments-to-zero-draft.pdf

[12] Commentaires de la GCSC sur la première version du rapport de fond du Groupe de travail à composition non limitée, 3 mars 2021, https://front.un-arm.org/wp-content/uploads/2021/03/GCSC-Submission-to-OEWG-First-Draft-Report-March-2021.pdf

[13] 1re réunion - Groupe de travail à composition non limitée sur l'évolution de la situation dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale, troisième session de fond (8 au 12 mars 2021), UN Web TV, 8 mars 2021 (commence à 1:29:40) https://media.un.org/en/asset/k1o/k1obxycc3u

[14] Réponse de Cybersecurity Tech Accord au rapport de fond du Groupe de travail de l'ONU [PREMIÈRE VERSION], https://front.un-arm.org/wp-content/uploads/2021/03/Tech-Accord-OEWG-response-March-2021-FINAL.pdf

Le 9 mars 2021, la République Fédérale d'Allemagne a approuvé le nouveau libellé de compromis « ...en particulier sur le noyau public de l'Internet ».[15]

Le 9 mars 2021, une coalition de neuf organisations de la société civile a recommandé que le rapport du Groupe de travail : « … fasse référence à la nécessité que tous les acteurs protègent la disponibilité et l'intégrité de base de l'Internet mondial, ce qui implique de ne pas interférer avec le noyau public de l'Internet. »[16]

Le 10 mars 2021, République populaire de Chine : « Les États doivent participer à la gestion et à la distribution des ressources internationales d'Internet sur un pied d'égalité. »[17]

Le 12 mars 2021, la GCSC a exprimé son « regret de constater que le terme « noyau public » n'avait pas été utilisé dans la version finale du rapport du Groupe de travail. »[18]

Outre la publication du rapport final du Groupe de travail, le président du Groupe de travail a publié une synthèse du président incluant le libellé antérieur sur le noyau public, tel que proposé par les Pays-Bas le 19 janvier.[19]

Le texte de compromis du rapport final du Groupe de travail de 2021, avec le nouveau libellé convenu entre les États membres, points 18 et 26, est le suivant :

« 18. Les États ont conclu que les activités malveillantes des TIC sur les infrastructures critiques (CI) et infrastructures critiques d'information (CII) des services essentiels au public peuvent avoir des conséquences dévastatrices sur la sécurité, l'économie, la société et la situation humanitaire. Bien qu'il revienne à chaque État de déterminer quelles infrastructures désigner comme étant critiques, ces dernières pourront inclure les installations médicales, les services financiers, l'énergie, l'eau, les transports et l'assainissement. Les activités malveillantes des TIC contre les CI et les CII qui minent la confiance dans les processus politiques et électoraux, les institutions publiques ou qui ont une incidence sur la disponibilité ou l'intégrité générales de l'Internet constituent également une préoccupation réelle et croissante. Ces infrastructures sont parfois détenues, gérées ou exploitées par le secteur privé, partagées ou mises en réseau en coopération avec un autre État ou exploitées par plusieurs États. Par conséquence, une coopération entre États ou entre les secteurs public

[15] 3e réunion - Groupe de travail à composition non limitée sur l'évolution de la situation dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale, troisième session de fond (8 au 12 mars 2021), UN Web TV, 9 mars 2021 (commence à 38:20), https://media.un.org/en/asset/k13/k13uzdidth

[16] « Commentaires conjoints de la société civile sur la première version du rapport du Groupe de travail sur les TIC », bibliothèque des documents du Groupe de travail, 9 mars 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Joint-CS-feedback-on-first-draft-1.pdf

[17] Groupe de travail à composition non limitée sur l'évolution de la situation dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale, troisième session de fond, 8 au 12 mars 2021, Synthèse du président du Groupe de travail, document de séance, 10 mars 2021, A/AC.290/2021/CRP.3*, https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf

[18] Déclaration de la GSCS sur le projet final du rapport de fond du Groupe de travail à composition non limitée des Nations Unies, 12 mars 2021, https://front.un-arm.org/wp-content/uploads/2021/03/GCSC-Statement-OEWG-Multistakeholder-Consultation-Final-Draft-Report-March-2021.pdf

[19] Groupe de travail à composition non limitée sur l'évolution de la situation dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale, troisième session de fond, 8 au 12 mars 2021, Synthèse du président, document de séance, 10 mars 2021, A/AC.290/2021/CRP.3*, https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf

et privé peut s'avérer nécessaire pour protéger leur intégrité, leur fonctionnement et leur disponibilité. »[20]

« 26. Tout en s'accordant sur la nécessité de protéger toutes les infrastructures critiques (CI) et les infrastructures critiques d'information (CII) des services essentiels au public, et en s'efforçant d'assurer la disponibilité et l'intégrité générales de l'Internet, les États ont en outre conclu que la pandémie de COVID-19 avait mis en évidence l'importance de protéger les infrastructures de santé, notamment les services médicaux et les installations médicales, par la mise en œuvre de normes relatives aux infrastructures critiques telles que celles définies par consensus dans la résolution 70/237 de l'Assemblée générale des Nations Unies. »[21]

La délégation des Pays-Bas, dans ses observations sur le rapport de consensus du Groupe de travail, a noté que « les Pays-Bas se félicitent vivement de l'inclusion de la disponibilité et de l'intégrité générales de l'Internet - ce que nous considérons comme le noyau public de l'Internet. »[22]

Compte-rendu du Groupe d'experts gouvernementaux (GGE)

Le rapport de consensus du GGE a été adopté le 28 mai 2021.[23] Plusieurs points du rapport sont pertinents pour la communauté de l'ICANN, dans le contexte international des délibérations sur le cyberespace à l'ONU auxquelles nous avons assisté ces dernières années. Les points cités ci-dessous (dans certains cas cités partiellement) sont tirés de la *Copie préliminaire du rapport du Groupe d'experts gouvernementaux sur la promotion d'un comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale* et de la « lettre de transmission » du rapport.[24]

Point 10 : « Les activités nuisibles des TIC attaquant les infrastructures critiques qui fournissent des services aux niveaux national, régional ou mondial, exposées dans les rapports précédents du GGE sont de plus en plus graves. Les activités malveillantes des TIC qui affectent les infrastructures critiques de l'information, les infrastructures fournissant des services essentiels au public, les infrastructures techniques essentielles à la disponibilité ou à l'intégrité générales de l'Internet et aux entités du secteur de la santé sont particulièrement préoccupantes. »

---

[20] Groupe de travail à composition non limitée sur l'évolution de la situation dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale, Rapport final de fond, document de séance, 10 mars 2021, A/AC.290/2021/CRP.2, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

[21] Groupe de travail à composition non limitée sur l'évolution de la situation dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale, Rapport final de fond, document de séance, 10 mars 2021, A/AC.290/2021/CRP.2.

[22] 9e réunion - Groupe de travail à composition non limitée sur l'évolution de la situation dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale, troisième session de fond (8 au 12 mars 2021), UN Web TV, 12 mars 2021 (commence à 35:23), https://media.un.org/en/asset/k1r/k1rf2exuhz

[23] Message Twitter du Département d'État des États-Unis, 28 mai 2021, https://twitter.com/State_Cyber/status/1398314450743091201?s=20

[24] Copie préliminaire, Rapport du Groupe d'experts gouvernementaux sur la promotion d'un comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale et lettre de transmission, 28 mai 2021, https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf

Point 17 : « Le Groupe a également pris note de la proposition de la Chine, du Kazakhstan, du Kirghizistan, de la Fédération de Russie, du Tadjikistan et de l'Ouzbékistan d'un code de conduite international pour la sécurité de l'information (voir A/69/723). »[25]

Point 44 : « Comme il est indiqué dans la norme 13 (g), les États doivent prendre des mesures appropriées pour protéger leurs infrastructures critiques. À cet égard, chaque État déterminera quelles sont les infrastructures ou secteurs qu'il juge critiques conformément à son domaine de compétence, aux priorités nationales et aux méthodes de catégorisation des infrastructures critiques. »

Point 45 : « Les infrastructures critiques peuvent également faire référence aux infrastructures qui fournissent des services dans plusieurs États, comme l'infrastructure technique essentielle à la disponibilité ou à l'intégrité générales de l'Internet. »

Point 48 : « La désignation par un État d'une infrastructure ou d'un secteur comme étant critique peut être utile pour protéger cette infrastructure ou ce secteur. En plus de déterminer quelle sont les infrastructures ou les secteurs d'infrastructure jugés critiques, chaque État définira les mesures structurelles, techniques, organisationnelles, législatives et réglementaires nécessaires pour protéger ses infrastructures critiques et en rétablir la fonctionnalité en cas d'incident. »

Point 49 : « Certains États hébergent des infrastructures qui fournissent des services à l'échelle régionale ou internationale. Les menaces des TIC contre ces infrastructures pourraient avoir des effets déstabilisateurs. Les États concernés par de telles dispositions pourraient encourager la coopération transfrontalière avec les propriétaires et les opérateurs de ces infrastructures afin d'améliorer les mesures de sécurité des TIC accordées à ces infrastructures et de renforcer, s'ils existent, ou de mettre en place, en complément, des processus et procédures permettant de détecter et d'atténuer les incidents technologiques affectant ces infrastructures. »

Point 63 : « En outre, et en consultation avec les acteurs pertinents de l'industrie et autres acteurs de la sécurité des TIC, les États peuvent élaborer des directives et incitations, conformément aux normes techniques internationales pertinentes, sur la notification et la gestion responsables des vulnérabilités et sur les rôles et responsabilités respectifs des différentes parties prenantes dans les processus de signalement ; les types d'informations techniques à divulguer ou à partager publiquement, y compris le partage d'informations techniques sur les incidents graves liés aux TIC, et la façon de traiter les données sensibles et d'assurer la sécurité et la confidentialité des informations. »

Point 79 : « Le dialogue, par le biais de consultations et d'engagements bilatéraux, sous-régionaux, régionaux et multilatéraux, peut faire progresser la compréhension entre les États, encourager une plus grande confiance et contribuer à une coopération plus étroite entre les États pour l'atténuation des incidents liés aux TIC, tout en réduisant les risques de perception erronée et d'escalade. D'autres parties prenantes comme le secteur privé, le milieu universitaire, la société civile et la communauté technique peuvent contribuer de manière significative à faciliter ces consultations et cet engagement. »

[25] Annexe à la lettre en date du 9 janvier 2015 des représentants permanents de la Chine, du Kazakhstan, du Kirghizistan, de la Fédération de Russie, du Tadjikistan et de l'Ouzbékistan à l'intention du Secrétaire général de l'Organisation des Nations Unies [Original : chinois et russe], Code de conduite international pour la sécurité de l'information, A/69/723, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/014/02/PDF/N1501402.pdf?OpenElement

Point 87 : « Le groupe souligne l'importance de la coopération et de l'assistance dans le domaine de la sécurité et du renforcement des capacités relatives aux TIC, ainsi que leur importance pour tous les éléments du mandat du groupe. Une coopération accrue, en plus d'une assistance plus efficace et d'un renforcement des capacités dans le domaine de la sécurité des TIC, impliquant d'autres parties prenantes telles que le secteur privé, le milieu universitaire, la société civile et la communauté technique, pourront aider les États à appliquer le cadre de comportement responsable des États dans leur utilisation des TIC. Ces approches sont critiques pour combler les clivages existants au sein des États et entre les États sur les questions de politiques, les questions juridiques et les questions techniques relatives à la sécurité des TIC. Elles pourront également contribuer à la réalisation d'autres objectifs de la communauté internationale, tels que les ODD. »

Point 95 : « le Groupe a également identifié des domaines potentiels pour les travaux futurs, dont entre autres : [...] (d) : « l'identification des mécanismes qui facilitent la participation d'autres parties prenantes essentielles, notamment le secteur privé, le milieu universitaire, la société civile et la communauté technique aux efforts visant à mettre en œuvre le cadre d'un comportement responsable, le cas échéant. »

Compte-rendu du Comité spécial d'experts à composition non limitée (AHC)

L'AHC devait commencer ses travaux en août 2020, mais en raison de la pandémie de COVID-19, sa première session d'organisation s'est tenue du 10 au 12 mai 2021.[26] Depuis le document de juillet 2020 de l'organisation ICANN, de nouvelles contributions ont été publiées sur la page Web de l'AHC.[27] Lors de la première réunion de sa session d'organisation le 10 mai 2021, le Comité a élu le président du Comité, son rapporteur et 13 vice-présidents qui représentent différentes régions géographiques.[28] L'AHC n'est pas parvenu à atteindre le consensus sur les modalités d'organisation de ses futures réunions dans les délais impartis. Le président a donc annoncé que des consultations officieuses suivraient.[29]

Le 26 mai 2021, lors de sa 71e séance plénière, l'Assemblée générale de l'ONU a adopté, sans vote, le texte de la résolution A/RES/75/282 pour « Lutter contre l'utilisation des technologies de l'information et des communications à des fins criminelles ».[30] Les

---

[26] Les réunions de la session d'organisation de l'AHC peuvent être consultées ici :
Première réunion : https://media.un.org/en/asset/k1v/k1vgo4a624 (La deuxième réunion n'a pas eu lieu parce que toutes les questions d'organisation ont été résolues au cours de la première réunion.)
Troisième réunion : https://media.un.org/en/asset/k1z/k1zsp4exqc
Quatrième réunion : https://media.un.org/en/asset/k12/k12bsxlcak
Cinquième réunion : https://media.un.org/en/asset/k1m/k1ma80pf1p
Sixième réunion : https://media.un.org/en/asset/k1m/k1m0si6d6n

[27] « Comité ad hoc créé par la résolution 74/247 de l'Assemblée générale », ONUDC, https://www.unodc.org/unodc/en/cybercrime/cybercrime-adhoc-committee.html

[28] La session d'organisation du Comité spécial s'est tenue à New York, du 10 au 12 mai 2021, résultats des élections du Comité spécial https://www.unodc.org/unodc/en/cybercrime/cybercrime-adhoc-committee.html

[29] 6e réunion, Comité spécial chargé d'élaborer une convention internationale générale sur la cybercriminalité, UN Web TV, 12 mai 2021 (commence à 3:24:34) https://media.un.org/en/asset/k18/k18lkzt0og

[30] Résolution adoptée par l'Assemblée générale le 26 mai 2021, « 75/282. Lutter contre l'utilisation des technologies de l'information et des communications à des fins criminelles », Distr. : 1er juin 2021, A/RES/75/282, https://undocs.org/a/res/75/282

documents ont établi deux lieux pour les sessions de l'AHC : Vienne et New York. Au total, sept sessions se tiendront en alternance entre Vienne et New York. La première et la dernière sessions auront lieu au siège des Nations Unies à New York. Les décisions de l'AHC sur les questions de fond sans approbation par consensus seront prises à la majorité des deux tiers des représentants présents et votants.

La résolution encourage également le président de l'AHC à tenir des consultations intersessions afin de solliciter les contributions d'un éventail diversifié de parties prenantes sur l'élaboration du projet de convention.

Conclusion

L'équipe GE continuera de suivre les discussions menées à l'AHC et au sein du nouveau Groupe de travail à composition non limitée, qui effectuera son travail de 2021 à 2025. Ce Groupe de travail a tenu sa première réunion d'organisation le 1er juin 2021, au cours de laquelle il a élu à la présidence le Représentant permanent de Singapour.[31]

Des mises à jour régulières sur le travail du Groupe de travail à composition non limitée, du GGE, de l'AHC, ainsi que d'autres publications de l'équipe GE sont disponibles sur la page Web d'engagement des parties prenantes gouvernementales de l'ICANN.[32]

[31] 1er juin, 1re réunion : https://media.un.org/en/asset/k1o/k1oa2ngbsc
1er juin, 2e réunion : https://media.un.org/en/asset/k14/k1443my9hu
[32] Site Web de GE, site Web de l'ICANN : https://www.icann.org/resources/pages/government-engagement-publications-2020-03-02-en

Annexe

Groupe de travail à composition non limitée. Rapport de fond final : https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

Groupe de travail à composition non limitée. Synthèse du président : troisième session de fond du Groupe de travail à composition non limitée sur l'évolution de la situation dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale, 8 au 12 mars 2021
https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf

Groupe de travail à composition non limitée. Vidéo de la troisième réunion de fond, 8 au 12 mars 2021

8 mars 2021
1re journée : 1re réunion
https://media.un.org/en/asset/k1o/k1obxycc3u

1er jour : 2e réunion
https://media.un.org/en/asset/k18/k1893g1q0h

9 mars 2021
2e jour : 3e réunion
https://media.un.org/en/asset/k13/k13uzdidth

2e jour : 4e réunion
https://media.un.org/en/asset/k1h/k1huoxryeo

10 mars 2021
3e jour : 5e réunion
https://media.un.org/en/asset/k1d/k1d4e06j0x

3e jour : 6e réunion
https://media.un.org/en/asset/k1m/k1mqlxrfv4

11 mars 2021
4e jour : les 7e et 8e réunions n'ont pas eu lieu. La journée a été consacrée aux discussions bilatérales et aux consultations avec les capitales.

12 mars 2021
5e jour : 9e réunion
https://media.un.org/en/asset/k1r/k1rf2exuhz

5e jour : 10e réunion (Le site Web de l'ONU ne fournit pas de lien vers l'enregistrement de cette séance).

5e jour : 11e réunion, dernière séance du Groupe de travail (adoption du rapport de fond par consensus) https://media.un.org/en/asset/k1p/k1prn29un6