Mise à jour des Nations Unies : discussions au sujet de l'Internet

Relations de l'ICANN avec les organisations gouvernementales et intergouvernementales (OIG)

M. Veni Markovski
GE-005
15 juillet 2020

ICANN

TABLE DES MATIERES

Avant-propos

Le présent document présente une mise à jour des délibérations des groupes de travail de l'Assemblée générale des Nations Unies (AGNU), où ont lieu des discussions sur des questions liées à l'Internet et à la cybersécurité.

Au cours de ces discussions, les questions qui touchent à la mission de l'ICANN sont soulevées de temps en temps, et elles pourraient continuer à être abordées à l'avenir. Le suivi des discussions fait partie du travail de soutien de la mission de l'ICANN dont la fonction en charge de la participation gouvernementale (GE) de l'organisation ICANN est responsable et montre également l'engagement et la responsabilité du département de la GE de tenir la communauté ICANN élargie au courant des questions importantes pour l'Internet mondial, unique et interopérable et son système d'identificateurs uniques.[1]

Dans notre article précédent, « bref aperçu des délibérations de l'ONU sur la cybersécurité et la cybercriminalité », nous avons fourni des informations sur la création des différents groupes de travail et processus des Nations Unies (ONU).[2] Dans le présent document, nous nous concentrons sur les mises à jour concernant le Groupe de travail à composition non limitée (OEWG) et le Comité intergouvernemental spécial d'experts à composition non limitée (OECE).

[1] Aux termes de notre plan opérationnel et financier quinquennal, à la p.47 : « surveiller la législation, les réglementations, les normes, les principes et les initiatives susceptibles d'avoir un impact sur la mission de l'ICANN »

[2] Le présent document fait partie d'une série publiée par le département en charge de la relation avec les gouvernements à compter du 28 février 2020. Pour tous les documents sur la relation avec les gouvernements, veuillez visiter notre page Web ici.

Mises à jour sur l'OECE, l'OEWG et le GGE

OECE

L'OECE[3] a commencé ses travaux sur la « lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles » par la publication d'un document contenant un projet de plan et de modalités pour les quatre prochaines années.[4] Ce document, qui devrait être examiné lors de la première réunion du groupe en août 2020, fournit un cadre pour les travaux de l'OECE jusqu'à sa conclusion en juin 2024.

Le 10 juillet, une réunion informelle virtuelle relative à la session d'organisation du Comité spécial sur la cybercriminalité a eu lieu. Au cours de la réunion, l'ONUDC a fait le point sur les questions de procédure relatives à la session d'organisation d'août du comité spécial, puis les États membres ont examiné l'ordre du jour provisoire de la session d'organisation du comité spécial.[5] Plus d'information sur cette réunion virtuelle informelle de juillet est disponible sur le site Web de l'OECE, en particulier dans le document intitulé « Résumé des informations fournies par le Directeur de la DTA, ONUDC, lors de la réunion informelle du 10 juillet 2020 ».[6]

Au 13 juillet 2020, l'OECE a publié sur sa page web les commentaires des États membres suivants : Australie, Canada, République dominicaine, Union européenne, République islamique d'Iran, Japon, Fédération de Russie, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord et États-Unis d'Amérique.

OEWG

Depuis mars 2020, le président de l'OEWG[7] a publié un rapport préliminaire initial le 11 mars 2020.[8] Le présent document était ouvert aux commentaires de toutes les parties prenantes dans l'intention d'en discuter lors d'une réunion en personne à la fin de mars 2020. Toutefois, en raison du COVID-19, cette réunion n'a pas eu lieu.[9] Au lieu de cela, les États membres ont été invités à envoyer des commentaires écrits. Des dizaines d'États membres, d'organisations

[3] L'OECE est l'acronyme du nom en anglais du Comité intergouvernemental spécial d'experts à composition non limitée (OECE) ; il est composé de tous les États membres de l'ONU et son mandat est d'élaborer une nouvelle convention des Nations Unies sur la cybercriminalité. Dans ce document, nous parlons de la « convention sur la cybercriminalité », alors que l'ONU l'évoque comme la « convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles ».
[4] Le document est disponible ici.
[5] Office des Nations Unies contre la drogue et le crime, https://www.unodc.org/
[6] Téléchargez le PDF ici.
[7] OEWG est l'acronyme du Groupe de travail à composition non limitée sur les développements dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale ; nous utilisons le terme « cybersécurité » dans notre document.
[8] Téléchargez le PDF ici.
[9] Note : Le COVID-19 a eu des répercussions sur le fonctionnement habituel de l'ONU et des groupes de travail susmentionnés. Par exemple, l'OEWG a tenu la première série de réunions informelles virtuelles en juin et juillet 2020.

intergouvernementales et d'organisations non gouvernementales ont envoyé leurs commentaires, qui ont été publiés sur le site Web du groupe.[10]

Dans ce document, nous citons certains des commentaires soumis en réponse à l'appel à commentaires de la présidence.[11] Nous ne nous concentrons que sur les commentaires qui pourraient être interprétés comme touchant la mission ou les attributions de l'ICANN.

***

Le point 38 du projet de rapport préliminaire commence par :

« *les États ont également proposé, au cours des discussions et par la voie de communications écrites, des suggestions pour la «mise à niveau » ainsi que pour la poursuite de l'élaboration de normes. Les propositions comprenaient, entre autres questions, que les États devraient affirmer leur attachement à la paix et à la sécurité internationales dans l'utilisation des TIC ; qu'il faudrait réaffirmer que les États détiennent la responsabilité première du maintien d'un environnement des TIC sûr, sécurisé et digne de confiance ; que la disponibilité ou l'intégrité générale du noyau public de l'Internet devrait être protégée ; [... couper...] ».*

Commentaires de certains États membres (par ordre alphabétique) sur le rapport préliminaire

> Brésil : « *Du point de vue du Brésil, les infrastructures informatiques qui sous-tendent les procédures électorales méritent la même protection que le noyau public de l'Internet (paragraphe 38) ».*
>
> Chine : *« Étant donné le temps limité dont nous disposons, il faut également faire attention aux fins d'éviter d'introduire dans le rapport des concepts qui n'ont pas encore fait l'objet d'un consensus mondial (« noyau public » par exemple) ».*
> et : *« Au cours des deux sessions précédentes, des parties, dont la Chine, ont présenté des dizaines de propositions constructives sur des questions telles que la cybersouveraineté, la sécurité de la chaîne d'approvisionnement, la protection des infrastructures essentielles, l'abstention de sanctions unilatérales et la lutte contre le cyber-terrorisme. Il est à espérer que ces propositions puissent être intégrées dans le rapport ».*
>
> Égypte : « *Les États membres devraient être encouragés à parvenir à une définition commune convenue de ce qui constitue une « infrastructure critique », en vue de parvenir à un accord, le cas échéant, sur l'interdiction de tout acte qui utilise sciemment ou intentionnellement des capacités TIC offensives pour endommager ou autrement nuire à l'utilisation et au fonctionnement des infrastructures critiques ».*
>
> Allemagne : *« Les acteurs étatiques et non étatiques ne doivent ni conduire ni autoriser sciemment une activité qui porte atteinte intentionnellement et de manière substantielle à la disponibilité ou à l'intégrité générale du noyau public de l'Internet, et donc, à la stabilité du cyberespace » [serait] une orientation pour la mise en œuvre de la*

[10] https://www.un.org/disarmament/open-ended-working-group/
[11] Consultez l'invitation ici.

recommandation 13(f) du GGE 2015 de l'ONU et, par conséquent, pour l'intégrer également au champ d'application de la recommandation 13(g) du GGE 2015 de l'ONU et : *« En ce qui concerne le paragraphe 31, l'Allemagne tient à souligner que l'OEWG devrait mettre l'accent sur le renforcement des normes existantes et l'amélioration de leur compréhension et de leur application. À cet égard, nous examinons les propositions visant à protéger le noyau public de l'Internet, et non à perturber l'infrastructure essentielle aux processus politiques, à ne pas nuire aux installations médicales et à mettre en évidence les infrastructures transnationales comme des ajouts utiles aux normes déjà existantes sur la protection des infrastructures critiques, telles que contenues dans le rapport du GGE de 2015 ».*

Iran : *« Le projet préliminaire n'a cependant pas reconnu certaines menaces d'importance, notamment des mesures coercitives unilatérales, le monopole de la gouvernance de l'Internet, l'anonymat des personnes et des dispositifs, des stratégies et des politiques cybernétiques offensives, etc., qui affectent clairement la conscience, la résilience et les capacités des pays ».*

Pays-Bas : *« Pour répondre à ces menaces, les Pays-Bas souhaitent suggérer que l'OEWG considère la recommandation selon laquelle "les acteurs étatiques et non étatiques ne doivent ni conduire ni autoriser sciemment des activités qui portent atteinte intentionnellement et substantiellement à la disponibilité ou à l'intégrité générale du noyau public de l'Internet, et donc à la stabilité du cyberespace" comme guide pour la mise en œuvre de la recommandation 13(f) du GGE 2015 de l'ONU et, par conséquent, pour l'intégrer également au champ d'application de la recommandation 13(g) du GGE 2015 de l'ONU ».*
et : *« les Pays-Bas souhaitent proposer que le rapport de l'OEWG examine la menace que représentent les cyberopérations contre la disponibilité ou l'intégrité générale du noyau public de l'Internet. Au fil des ans, les cyberopérations contre l'intégrité, le fonctionnement et la disponibilité de l'Internet se sont avérées des menaces réelles et crédibles ».*

Nicaragua : note que « *l'insuffisance actuelle de réglementation des activités du secteur privé dans le domaine des TIC* » constitue une « *menace majeure pour le développement d'un environnement pacifique des TIC ».*

Pakistan : *« Les États membres devraient être encouragés à parvenir à une définition commune convenue de ce qui constitue une "infrastructure critique", en vue de s'entendre sur l'interdiction de l'activité des TIC qui nuit sciemment ou intentionnellement à l'infrastructure critique ou qui nuit autrement à l'utilisation et au fonctionnement des infrastructures critiques ».*

Russie : *« L'importance de "l'approche multipartite", en mettant l'accent sur la contribution du secteur non gouvernemental, des entreprises et des universités pour garantir un comportement responsable dans l'espace de l'information, est artificiellement exagérée. En même temps, le problème de l'insuffisance de réglementation des activités du secteur privé dans le domaine des TIC et la question de plus en plus urgente de la monopolisation de ce domaine sont omis comme l'une des principales menaces au développement d'un environnement pacifique et concurrentiel des TIC ».*

Suisse : *« Par exemple, les propositions relatives à la protection du noyau public de l'Internet, à la volonté de ne pas nuire aux installations médicales ni perturber les infrastructures essentielles aux processus politiques et aux infrastructures critiques transnationales pourraient, à notre avis, fournir des indications précieuses sur les normes existantes ».*

États-Unis : *« ...l'élaboration sélective de normes ou l'identification de secteurs d'infrastructure critique spécifiques comporte un certain risque de donner la priorité à certaines questions par-dessus d'autres ».*

Union européenne : *« Par conséquent, la protection des infrastructures critiques est d'une telle importance que l'UE et ses États membres suggéraient au rapport de l'OEWG de tenir compte de ces menaces, y compris celle qui est posée contre la disponibilité ou l'intégrité générale du noyau public de l'Internet ».*

Commentaires des organisations non gouvernementales

Global Partners Digital : *« Recommandation :* n*ous appuyons les recommandations des Pays-Bas dans le « document officieux », visant à élaborer et à fournir des directives supplémentaires sur les normes f) et g) du rapport du GGE 2015 de l'ONU (résolution 70/237)— à savoir que « les acteurs étatiques et non étatiques ne doivent ni conduire ni autoriser sciemment une activité qui porte atteinte intentionnellement et de manière substantielle à la disponibilité ou à l'intégrité générale du noyau public de l'Internet, et donc à la stabilité du cyberespace ».*

Internet Society : *« le noyau public de l'Internet encapsule les systèmes de routage, d'attribution de noms et de numérotation de l'Internet (le système de noms de domaine), les mécanismes de cryptographie de sécurité et d'identité et les câbles de communication. Ce sont les fonctions essentielles qui font fonctionner l'Internet et doivent être protégées pour assurer que l'Internet reste une technologie habilitante qui a une portée et une intégrité mondiales. Nous encourageons l'OEWG à tenir dûment compte des valeurs de la norme du GCSC pour protéger le noyau public, qui souligne la nécessité que les acteurs étatiques et non étatiques s'abstiennent d'autoriser toute activité susceptible de nuire intentionnellement ou substantiellement à la disponibilité ou à l'intégrité du cœur public d'Internet, et donc à la stabilité du cyberespace ».*

Microsoft : dans sa première communication dit *« soutenir fortement plusieurs des nouvelles normes proposées par les États membres qui, de notre avis, sont des ajouts critiques à la base existante des normes informatiques précédemment convenues dans le contexte du GGE : les acteurs étatiques et non étatiques ne doivent ni conduire ni autoriser sciemment une activité qui porte atteinte intentionnellement et substantiellement à la disponibilité ou à l'intégrité générale du noyau public d'Internet, et donc à la stabilité du cyberespace ».* Microsoft appelle également ses membres à suivre le principe de l'appel de Paris pour *« empêcher toute activité qui nuit intentionnellement et substantiellement à la disponibilité ou à l'intégrité générale du cœur public d'Internet ».*

Microsoft, dans une deuxième présentation, déclare *: « les engagements précédents du GGE reflètent cette importance, et plusieurs déclarations depuis, y compris l'appel de Paris et le GCSC, reflètent l'engagement croissant à protéger la technologie qui*

constitue l'épine dorsale de l'Internet lui-même contre les cyberattaques. Certains efforts font référence à la protection de la disponibilité ou de l'intégrité générale du « noyau public » de l'Internet ; d'autres préfèrent faire allusion aux composantes techniques de l'Internet. Il est important que les États s'entendent sur une nouvelle norme pour protéger ces composantes centrales sans lesquelles l'Internet mondial cesserait de fonctionner. Le GCSC définit ces composantes comme : le routage et le transfert de paquets ; les systèmes de dénomination et de numérotation ; les mécanismes cryptographiques de sécurité et d'identité ; les supports de transmission, les logiciels et les centres de données ».

Douze ONG[12] ont publié une déclaration commune : *« Les attaques contre les infrastructures critiques, et ici aussi contre "l'infrastructure d'information critique supranationale" (qui devrait comprendre le système de noms de domaine et d'autres éléments du noyau public de l'Internet), constituent non seulement une "menace pour la sécurité, mais aussi pour le développement économique et les moyens de subsistance des populations" (paragraphe 19). Nous suggérons que ce coût humain des attaques contre les infrastructures critiques et leur impact sur les droits de l'homme soient directement et clairement mentionnés dans le rapport »* et *« nous appuyons la recommandation du paragraphe 38 que la disponibilité ou l'intégrité générale du noyau public de l'Internet devrait être protégée, ce qui devrait être compris comme une spécification ou une élaboration plus poussée des normes déjà convenues dans le GGE 2015 pour protéger les infrastructures critiques. Le noyau public fait référence aux éléments critiques de l'infrastructure de l'Internet, à savoir le routage et le transfert de paquets, les systèmes d'attribution de noms et de numérotation, les mécanismes cryptographiques de sécurité et d'identité, les supports de transmission, les logiciels et les centres de données ».*

***

Le 27 mai 2020, le président de l'OEWG a publié[13] un projet de rapport préliminaire révisé et un document officieux mis à jour[14] qui reflètent, selon la lettre du président, les « nouvelles propositions reçues au titre du point de l'ordre du jour "règles, normes et principes" ».[15] Ce projet de rapport préliminaire mis à jour et le document officieux ont été examinés lors d'une réunion virtuelle qui s'est tenue les 15, 17 et 19 juin et le 2 juillet 2020. Selon une lettre publiée le 16 juillet 2020 par le président de l'OEWG et le Représentant permanent de la Suisse auprès de l'ONU, l'Ambassadeur Jürg Lauber, le calendrier des prochaines réunions informelles pour discuter du projet préliminaire est le suivant : deuxième série du 29 septembre au 1er octobre 2020 ; troisième série du 17 au 19 novembre 2020 ; et quatrième série du 1er au 3 décembre 2020.[16]

[12] Ces 12 ONG sont : Access Now, Association for Progressive Communications, Centre for Communication Governance at National Law University Delhi, Derechos Digitales, Fundación Karisma, Global Partners Digital, Kenya ICT Action Network (KICTANet), International Center for Not-for-Profit Law, R3D : Red en Defensa de los Derechos Digitales, Research ICT Africa, Media Foundation for West Africa, centre de formation informatique et studio numérique de la YMCA en Gambie.
[13] https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf
[14] https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-non-paper.pdf
[15] La lettre est publiée ici.
[16] La lettre peut être téléchargée (PDF) ici.

La deuxième série de discussions portera sur les questions de droit international ; la troisième portera sur les mesures de confiance et le renforcement des capacités ; et la quatrième portera sur un dialogue institutionnel régulier et des observations générales. Par la suite, le président devrait publier un brouillon zéro (au début de 2021), qui sera examiné lors de la troisième réunion de fond du 8 au 12 mars 2021. Au moment de la publication de la lettre du président, il est prévu que les réunions informelles soient virtuelles ou hybrides et que la réunion de fond se tienne en personne.

Groupe d'experts gouvernementaux (GGE)

Il n'y a pas de nouvelle mise à jour sur les travaux du GGE depuis les informations contenues dans notre document du 28 février 2020.[17]

Engagement de l'ICANN et prochaines étapes

L'équipe de l'organisation ICANN a organisé et co-animé une réunion d'information virtuelle à l'intention des diplomates des missions permanentes auprès de l'ONU le 22 avril 2020. La réunion d'information a été organisée conjointement par les missions permanentes de la Bulgarie et de l'Estonie auprès des Nations Unies à New York et par le Bureau des Nations Unies à Genève. David Conrad, directeur de la technologie de l'ICANN, et Naela Sarras, directrice principale des Services IANA, ont parlé et interagi avec les 116 diplomates qui y ont participé. Ils ont expliqué le rôle de l'ICANN dans l'écosystème de l'Internet et ont abordé les questions soumises par les diplomates.

L'équipe GE de l'ICANN continuera de suivre les délibérations à l'ONU et publiera les mises à jour nécessaires, le cas échéant.

ANNEXE 1

Informations générales sur les comités de l'ONU et de l'AGNU

Fondée le 24 octobre 1945, l'ONU s'implique récemment de plus en plus dans les discussions qui portent sur différentes questions liées à l'Internet. L'AGNU délibère depuis des années sur les résolutions au sein de ses première et deuxième commissions, visant la cybersécurité et la gouvernance de l'Internet (IG).[18]

[17] https://www.un.org/disarmament/group-of-governmental-experts/

[18] Comme expliqué ci-dessus, l'ONU n'utilise pas le terme « cybersécurité », mais nous le faisons aux fins informatives de ce document.

La première commission de l'AGNU[19] est le comité qui a historiquement commencé la discussion sur la première résolution relative à la cybercriminalité.[20] En 2018, elle a créé deux groupes de travail sur la cybersécurité – l'OEWG[21] et le GGE, qui ont été présentés dans le document publié en février 2020.[22]

La deuxième commission de l'AGNU[23] traite des questions liées à l'Internet dans le cadre de la résolution sur les technologies de l'information et de la communication (TIC) au service du développement.[24] Les discussions relatives à la gouvernance de l'Internet ont commencé[25] avec la résolution A/RES/56/183 de l'AGNU de 2002[26], au cours du Sommet mondial sur la société de l'information (SMSI). Cette résolution a été mise à jour à plusieurs reprises en 2003 et 2005, en vue du SMSI à Genève (2003) et à Tunis (2005). Entre les phases du SMSI de Genève et de Tunis, un groupe de travail sur la gouvernance de l'Internet (WGIG) qui a publié son propre rapport a été créé.[27]

Le SMSI a adopté un document, l'Agenda de Tunis du SMSI, qui a servi depuis 2005 comme l'un des documents clés expliquant (entre autres) le modèle multipartite de gouvernance de l'Internet.[28]

La deuxième commission de l'AGNU examine chaque année la résolution sur les TIC au service du développement. En 2015, elle a également consacré beaucoup de temps aux *délibérations du SMSI+10 ,* qui ont abouti à la publication du document final du SMSI+10[29] et qui ont résulté à une réunion de haut niveau de l'AGNU les 15 et 16 décembre 2015.[30] Le document final, entre autres, a confirmé de nouveau le modèle multipartite de gouvernance de l'Internet et a prolongé le Forum sur la gouvernance de l'Internet (IGF) pour une autre période de dix ans.[31]

La **troisième commission de l'AGNU**[32] s'est penchée sur la cybercriminalité, avec une résolution[33] de 2019, créant le Comité intergouvernemental spécial d'experts à composition non

---

[19] http://www.un.org/en/ga/first/index.shtml
[20] Le document a/RES/53/70, intitulé « évolution de la situation dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale », a été proposé en 1998.
[21] L'OEWG est destiné à suivre « l'évolution de la situation dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale ».
[22] https://www.icann.org/resources/pages/government-engagement-publications-2020-03-02-en
[23] https://www.un.org/en/ga/second/index.shtml
[24] Depuis 2018, les TIC sont mises au service du développement durable, comme on le voit sur le site Internet de la CNUCED.
[25] Le SMSI a été discuté pour la première fois par l'UIT lors de sa Conférence de plénipotentiaires de 1998, et sa décision de tenir le SMSI a été approuvée par l'Assemblée générale des Nations Unies en 2001.
[26] https://unctad.org/en/PublicationsLibrary/ares56d183_en.pdf
[27] Consultez le site Web du Département d'État des États-Unis ou téléchargez le PDF à partir du site du WGIG lui-même pour plus d'information.
[28] https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html
[29] Le site de l'ONU ne fonctionne pas, mais le document peut être trouvé en faisant une recherche de son nom : UNPAN95735.pdf
[30] Site Web officiel : https://publicadministration.un.org/wsis10/GA-High-Level-Meeting
[31] https://www.intgovforum.org/multilingual/
[32] https://www.un.org/en/ga/third/index.shtml
[33] Téléchargez le document dans l'une des langues de l'ONU ici.

limitée (OECE) dans le but de rédiger une nouvelle convention des Nations Unies sur la cybercriminalité.[34]

[34] Le nom complet de ce groupe est « Comité intergouvernemental spécial d'experts à composition non limitée, représentant toutes les régions, chargé d'élaborer une convention internationale globale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles ».