Rapport de pays : les Pays-Bas et le « noyau public de l'Internet »

Alexey Trepykhalin et Veni Markovski
28 mai 2021
GE-008

ICANN

TABLE DES MATIÈRES

Introduction

Ce document passe en revue les initiatives nationales et internationales liées à l'Internet mises en place par le gouvernement néerlandais. Il fait partie d'une série de rapports de pays destinés à donner un aperçu des activités liées à l'écosystème de l'Internet et à la mission de l'ICANN. Cette veille informationnelle menée par l'équipe en charge de la relation avec les gouvernements et les organisations intergouvernementales (GE) de l'organisation ICANN témoigne de son engagement et de sa volonté de tenir l'ensemble de la communauté de l'ICANN informée des principaux enjeux dont il faut tenir compte pour préserver un Internet mondial, unique et interopérable, et son système d'identificateurs uniques.[1]

À l'instar des articles précédents de l'équipe GE, les analyses sont basées sur des textes sources primaires portant sur des politiques et des technologies Internet, comme celles liées au système des noms de domaine (DNS), aux adresses de protocole Internet (IP) et aux paramètres de protocole, entre autres. Ce document s'appuie également sur des textes et des déclarations concernant les positions du gouvernement néerlandais sur ces mêmes questions au sein des Nations Unies (ONU). Il s'agit de mettre à la disposition de la communauté de l'ICANN des informations qui lui permettront de mieux comprendre les délibérations en cours à l'ONU.

Enfin, ce document se concentre sur un terme promu par les Pays-Bas dans les espaces privés et publics : le « noyau public de l'Internet ». Aux Nations Unies, ce terme est utilisé dans le cadre des contributions faites par les Pays-Bas au Groupe de travail à composition non limitée de l'Assemblée générale des Nations Unies sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale (OEWG).[2,3]

Contexte : le « noyau public » au fil des années

Au cours des dernières années, le terme « noyau public de l'Internet » a été utilisé à plusieurs reprises dans différents contextes. Ce qui suit est une sélection d'exemples de son utilisation.

En 2015, le Conseil scientifique néerlandais pour la politique gouvernementale a présenté au ministre néerlandais des Affaires étrangères, Bert Koenders, un rapport intitulé « Le noyau public de l'Internet ».[4]

---

[1] *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 [2] *Réponse du Royaume des Pays-Bas au rapport préliminaire de l'OEWG*. Création d'un groupe de travail à composition non limitée (OEWG) par l'Assemblée générale, 2020, https://front.un-arm.org/wp-content/uploads/2020/04/kingdom-of-the-netherlands-response-pre-draft-oewg.pdf

[3] *Document de position des Pays-Bas auprès du Groupe de travail à composition non limitée des Nations Unies sur 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*, Groupe de travail à composition non limitée, février 2020, https://unoda- web.s3.amazonaws.com/wp-content/uploads/2020/02/letter-to-chair-of-oewg-kingdom-of-the- netherlands.pdf

[4] BROEDERS, Dennis, *The Public Core of the Internet. An International Agenda for Internet Governance* [Le noyau public de l'Internet. Un programme international pour la gouvernance de l'Internet], Conseil scientifique néerlandais pour la politique gouvernementale, janvier 2015, https://english.wrr.nl/publications/reports/2015/10/01/the-public-core-of-the-internet

En 2016, le ministère néerlandais des Affaires étrangères a organisé un atelier consultatif avec des membres de la communauté technique et de la communauté des organisations à but non lucratif. Au cours de l'atelier, le constat suivant a été fait :

« La protection du noyau public a été définie comme étant la protection de la disponibilité générale des fonctions de transmission et de nommage qui sous-tendent l'Internet mondial ».[5]

Les Pays-Bas ont présenté ce terme au Groupe d'experts gouvernementaux (GGE) des Nations Unies de 2016 - 2017[6]. Comme le GGE n'a pas publié de rapport de consensus, on ignore si le terme aurait été inclus dans le texte final.[7]

En 2017, le gouvernement néerlandais a soutenu la création d'une entité privée appelée Commission mondiale sur la stabilité du cyberespace (GCSC)[8]. En 2018, la GCSC a publié une définition selon laquelle l'expression « le noyau public de l'Internet » comprend « des éléments critiques de l'infrastructure de l'Internet comme le routage et la transmission de paquets, les systèmes de nommage et de numéros, les mécanismes cryptographiques de sécurité et d'identité, les supports de transmission, les logiciels et les centres de données ».[9]

En 2017, le ministère des Affaires étrangères des Pays-Bas a présenté une cyberstratégie internationale qui reconnaissait que « compte tenu de la nature du cyberespace et de notre dépendance à son égard, il est nécessaire de faire preuve de prudence lorsqu'il s'agit de mener des activités susceptibles d'affecter ce noyau public »[10]. Cette stratégie reconnaissait également que « dans la mesure du possible, la responsabilité de maintenir et de développer ce noyau public devrait incomber à la communauté technologique, tandis que l'État devrait jouer un rôle de soutien ».

En 2017 et 2018, un groupe de travail de la GCSC a mené une enquête auprès d'experts des infrastructures de communication et de la cyberdéfense « afin d'évaluer les infrastructures jugées prioritaires du point de vue de leur protection »[11]. Ainsi, la GCSC a défini le « noyau public » comme étant les « systèmes de routage et de transmission de paquets, les systèmes de nommage et de numéros, les mécanismes cryptographiques de sécurité et d'identité et les supports de transmission physique » (voir Annexe III).[12]

---

[5] BROEDERS, Dennis, *Aligning the International Protection of 'the Public Core of the Internet' with State Sovereignty and National Security* [Aligner la protection internationale du « noyau public de l'Internet » sur la souveraineté de l'État et la sécurité nationale], Journal of Cyber Policy, volume 2, numéro 4, novembre 2017, p. 369, https://www.researchgate.net/publication/321237654_Aligning_the_international_protection_of_'the_public_core_of_the_internet'_with_state_sovereignty_and_national_security

[6] Groupe d'experts gouvernementaux, Bureau des affaires de désarmement de l'ONU, mai 2021, https://www.un.org/disarmament/group-of-governmental-experts/

[7] *Fact Sheet: Developments In the Field of Information and Telecommunications in the Context of International Security* [Fiche d'information : Progrès de l'informatique et des télécommunications et sécurité internationale], Bureau des affaires de désarmement de l'ONU, juillet 2019, https://unoda- web.s3.amazonaws.com/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf [8] *Lancement de la Commission mondiale sur la stabilité du cyberespace*, Commission mondiale sur la stabilité du cyberespace, 18 février 2017, https://cyberstability.org/news/launch-of-global-commission-on-the- stability-of-cyberspace/

[9] *Definition of the Public Core, to Which the Norm Applies* [Définition du noyau public auquel s'applique la norme], Commission mondiale sur la stabilité dans le cyberespace, mai 2018, https://cyberstability.org/wp-content/uploads/2018/07/Definition-of-the-Public- Core-of-the-Internet.pdf

[10] Ministère des Affaires étrangères, *Building Digital Bridges. International Cyber Strategy. Towards an Integrated International Cyber Policy* [Jeter des ponts numériques. Cyberstratégie internationale. Vers une politique internationale intégrée en matière de cyberespace]. Lettre au Parlement, 2017, https://www.government.nl/documents/parliamentary-documents/2017/02/12/international-cyber- strategy

[11] FAESEN, Louk, *Call to Protect the Public Core of the Internet* [Appel à la protection du noyau public de l'Internet], Commission mondiale sur la stabilité du cyberespace, décembre 2017, https://cyberstability.org/category/front/

[12] *Definition of the Public Core, to Which the Norm Applies* [Définition du noyau public, auquel s'applique la norme], Commission mondiale sur la stabilité dans le cyberespace, mai 2018.

En 2019, les membres de la GCSC ont introduit le terme « noyau public » lors des réunions ICANN64 et ICANN65, tenues respectivement à Kobe et à Marrakech. Le terme a été discuté pour la première fois à Kobe lors d'une réunion de l'Unité constitutive des fournisseurs de services Internet et de services de connectivité

(ISPCP) de l'Organisation de soutien aux extensions génériques (GNSO).[13] La même année, à Marrakech, la GCSC a présenté son rapport préliminaire à l'ensemble de la communauté Internet dans le cadre de ses efforts de sensibilisation. Lors de la réunion de Marrakech, le représentant du Royaume-Uni auprès du Comité consultatif gouvernemental de l'ICANN (GAC) a alerté la GCSC sur le fait que « l'introduction du terme noyau public, qui est mal compris ou difficile à définir, pourrait entraîner davantage de problèmes ».

Utilisation du terme « noyau public » dans les discussions sur le cyberespace menées aux Nations Unies[15]

En 2020, le terme « noyau public » est apparu dans certains documents publiés sur la page Web officielle de l'OEWG.[16]

Dans la première version du rapport préliminaire du président, on retrouve le terme au point 38 : « Les États ont également proposé, au cours des discussions et par voie de communications écrites, des suggestions pour la "mise à niveau" et la poursuite de l'élaboration de normes. Parmi les propositions on peut citer, entre autres, 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 générale ou l'intégrité du noyau public de l'Internet doit être protégée [...] ».[17]

[13] Transcription de la réunion de l'ISPCP, organisation ICANN, mars 2019 à 15h15 JST (p.22, 23, 26), https://gnso.icann.org/sites/default/files/file/field-file-attach/transcript-gnso-ispcp-12mar19-en.pdf

[14] GAC : réunion conjointe avec la Commission mondiale sur la stabilité du cyberespace (GCSC), organisation ICANN, 27 juin 2019 (commence à 22h39), https://icann.zoom.us/recording/share/yW2zWMtn2QzqJTmj0u3sh-zWa6- FuQeI7V72gUoFfaewIumekTziMw?startTime=1561633270000

[15] Avant d'expliquer où et comment le terme est utilisé lors des différentes délibérations de l'ONU, il est important de souligner que bien que ce terme existe dans certaines législations et politiques, comme la Cyberstratégie internationale des Pays-Bas ou la Loi sur la cybersécurité de l'UE, l'ONU n'introduit pas directement des textes des lois et des règlementations nationales dans ses documents finaux.

[16] Groupe de travail à composition non limitée, Assemblé générale de l'ONU, mai 2021 https://www.un.org/disarmament/open-ended-working-group/

[17] *Rapport préliminaire du président*, mars 2020, https://unoda-web.s3.amazonaws.com/wp- content/upload/2020/03/200311-Pre-Draft-OEWG-ICT.pdf

Dans la deuxième version du rapport préliminaire du président, on retrouve le terme au point 42 : « Les États ont également fait des propositions pour le renforcement et la poursuite de l'élaboration de normes. Parmi les propositions on peut citer, entre autres, que les États devraient affirmer leur attachement à une culture de prudence, ainsi qu'à la paix et à la sécurité internationales dans l'utilisation des TIC ; que les États devraient réaffirmer leur responsabilité première du maintien d'un environnement des TIC sûr, sécurisé et digne de confiance ; que la disponibilité générale ou l'intégrité du noyau public de l'Internet doit être protégée [...]. » [18]

Dans leur contribution de février 2020 à l'OEWG, les Pays-Bas ont suggéré que la protection du noyau public devrait être considérée à la fois par l'OEWG et le GGE.[19] D'autres États membres ont également évoqué ce terme dans leurs communications, dont l'Allemagne, la Suisse et l'UE. [20,21,22] Il a par ailleurs été mentionné dans les contributions d'autres parties prenantes, dont 12 organisations non gouvernementales, Microsoft Corporation, Global Partners Digital et l'Internet Society. [23,24,25,26,27] Cette dernière en a donné la définition suivante : « le noyau public de l'Internet englobe les systèmes de routage, de nommage et de numéros de l'Internet (le système des noms de domaine), les mécanismes cryptographiques de sécurité et d'identité et les câbles de communication ».

[18] *Rapport préliminaire du président*, mai 2020, https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf

[19] *Document de position des Pays-Bas auprès du Groupe de travail à composition non limitée des Nations Unies sur 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*, Groupe de travail à composition non limitée, Assemblée générale des Nations Unies, mars 2020.

https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/letter-to-chair-of-oewg-kingdom- of-the-netherlands.pdf

[20] *Rapport préliminaire initial de l'OEWG sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale* et Document de travail contenant des propositions de texte spécifiques pour le point de l'ordre du jour « Règles, normes et principes ». Extrait des communications écrites reçues avant le 2 mars 2020. Commentaires de l'Allemagne, Groupe de travail à composition non limitée, Assemblée générale de l'ONU, avril 2020, https://front.un-arm.org/wp-content/uploads/2020/04/20200401-oewg-german- written-contribution-to-pre-draft-report-1.pdf

[21] Ambassadrice Nadine Olivieri Lozano, *Lettre à la présidente du Groupe de travail à composition non limitée des Nations Unies sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale*, Groupe de travail à composition non limitée, Assemblée générale de l'ONU, 9 avril 2020, https://front.un- arm.org/wp-content/uploads/2020/04/20200409-switzerland-remarks-oewg-pre-draft.pdf

[22] *Commentaires de l'UE et de ses États membres sur le rapport initial préliminaire du Groupe de travail à composition non limitée des Nations Unies sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale*, Groupe de travail à composition non limitée, Assemblée générale de l'ONU, mai 2020, https://front.un-arm.org/wp-content/uploads/2020/05/eu-contribution-alignments-oewg.pdf

[23] *Perspectives de la société civile sur le Rapport préliminaire initial du Groupe de travail à composition non limitée des Nations Unies sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale*, Groupe de travail à composition non limitée, Assemblée générale de l'ONU, avril 2020, https://front.un-arm.org/wp-content/uploads/2020/04/cs- coordination-perspectives-on-oewg-pre-draft.pdf

[24] *Réponse de Global Partners Digital au Rapport préliminaire*, Global Partners Digital, mars 2020, https://front.un-arm.org/wp-content/uploads/2020/04/oewg-pre-draft-gpd-response-final.pdf

[25] *Contribution de Microsoft au Rapport préliminaire de l'OEWG sur la cybersécurité*, Microsoft Inc., avril 2020, https://front.un-arm.org/wp-content/uploads/2020/04/microsoft-response-to-draft-oewg-report.pdf

[26] *Réponse de l'Internet Society au Rapport préliminaire initial de l'OEWG*, https://front.un-arm.org/wp-content/uploads/2020/04/internet-society-response-pre-draft-report-of-oewg-04-14-20-en.pdf

[27] *Protecting People In Cyberspace: The Vital Role Of The United Nations In 2020* [Protection des personnes dans le cyberespace : le rôle central des Nations Unies en 2020], Microsoft Inc., avril 2020, https://front.un-arm.org/wp-content/uploads/2020/04/protecting-people-in-cyberspace- december-2019.pdf

L'utilisation de ce terme n'a pas été universellement acceptée. La Chine, par exemple, a exprimé des doutes quant à son inclusion dans le rapport du président, en précisant que : « Étant donné le temps limité dont nous disposons, il convient également d'attirer l'attention sur la nécessité 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) ».[28]

En mars 2020, un document de travail citait la proposition linguistique spécifique des Pays-Bas : « [La phrase] Les acteurs étatiques et non étatiques ne devraient ni mener ni permettre sciemment des activités qui portent intentionnellement et substantiellement atteinte à la disponibilité générale ou à l'intégrité du noyau public de l'Internet, et par conséquent à la stabilité du cyberespace [serait] une orientation pour la mise en œuvre de la recommandation 13(f) du GGE de l'ONU de 2015, ce qui ferait également entrer cette question dans le champ d'application de la recommandation 13(g) du GGE de l'ONU de 2015 ».[29]

En décembre 2020, dans le cadre du « Cyberdialogue multipartite pour soutenir la discussion en cours au sein du Groupe de travail à composition non limitée des Nations Unies (OEWG) sur les progrès de l'informatique et des télécommunications (TIC) dans le contexte de la sécurité internationale », les représentants de la GCSC et de l'ISOC ont examiné la faisabilité de l'utilisation du terme « noyau public ».[30]

Le 19 janvier 2021, l'OEWG a publié le *Projet de rapport sur le fond de la question (avant-projet)*, dans lequel le terme « noyau public » n'a pas été mentionné.[31] Il en est de même dans le *Premier projet de rapport*, publié le 1er mars 2021.[32]

Du 8 au 12 mars 2021, l'OEWG a tenu sa troisième session de fond, au cours de laquelle la délégation néerlandaise a suggéré la correction suivante concernant le noyau public dans le *Projet de rapport sur le fond de la question (avant-projet) :*

[28] *Contribution de la Chine au Rapport préliminaire initial de l'OEWG*, Groupe de travail à composition non limitée, Assemblée générale de l'ONU, avril 2020, https://front.un-arm.org/wp-content/uploads/2020/04/china-contribution-to-oewg-pre-draft-report-final.pdf

[29] Document de travail contenant des propositions de texte spécifiques pour le point de l'ordre du jour « Règles, normes et principes ». Extrait des communications écrites reçues avant le 2 mars 2020, OEWG, mars 2020, https://unoda- web.s3.amazonaws.com/wp-content/uploads/2020/03/200311-OEWG-ICT-non-paper.pdf

[30] *Lets' Talk Cyber: Rules, Norms and Principles* [Parlons cyber : règles, normes et principes], Livecasts, décembre 2020, (commence à 1:59:00), https://letstalkcyber.livecasts.eu/rules-norms-and-principles

[31] *Projet de rapport sur le fond de la question (avant-projet)*, Groupe de travail à composition non limitée, Assemblée générale de l'ONU, 19 janvier 2021, https://front.un-arm.org/wp-content/uploads/2021/01/OEWG-Zero-Draft-19-01-2021.pdf

[32] *Premier projet rapport de fond*, 1er mars 2020, Groupe de travail à composition non limitée, Assemblée générale de l'ONU, https://front.un-arm.org/wp-content/uploads/2021/03/210301-First-Draft.pdf

« Conformément au texte sur la protection du noyau public qui a été inclus dans l'avant-projet et compte tenu de la convergence par rapport au libellé exact, nous proposons ce qui suit. Nous souhaitons proposer de modifier 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 générale ou à l'intégrité de l'Internet ». Cela vaut également pour le paragraphe 50. En outre, nous aimerions aussi évoquer l'importance de la « protection de l'infrastructure technique essentielle à la disponibilité générale ou à l'intégrité de l'Internet » dans la section conclusion/recommandation des *règles, normes et principes* ».[33]

D'autres pays ont soutenu la position des Pays-Bas, aussi bien oralement que dans des contributions écrites au cours de la session. Le Royaume-Uni a ainsi noté : « Nous remercions les Pays-Bas d'avoir travaillé 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 ».[34]

À deux reprises, il y a eu des échanges informels virtuels et multipartites d'une heure et demie, au cours desquels les États membres ont entendu les opinions d'autres parties prenantes sur le contenu du premier projet de rapport. Certains de ces avis évoquent le « noyau public », à savoir le commentaire et la déclaration de la GCSC, qui regrette que le terme n'ait pas été inclus dans le rapport de consensus.[35, 36, 37]

Enfin, le rapport final de l'OEWG a inclus le libellé suivant à ce sujet, aux points 18 et 26 du rapport : [38]

« 18. Les États ont conclu que les activités malveillantes menées par le biais des TIC sur des infrastructures critiques (IC) et des infrastructures d'information critiques (IIC) qui assurent des services essentiels au public peuvent avoir des conséquences dévastatrices sur le plan de la sécurité, de l'économie, de la société et de la situation humanitaire. Bien qu'il revienne à chaque État de déterminer les infrastructures jugées critiques, celles-ci peuvent inclure les installations médicales, les services financiers, l'énergie, l'eau, les transports et l'assainissement. Les activités malveillantes menées au moyen des TIC à l'encontre des IC et des IIC qui sapent la confiance dans les processus politiques et électoraux et dans les institutions publiques, ou qui ont une incidence sur la disponibilité générale ou l'intégrité 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. En conséquence, une coopération entre États ou entre les secteurs public et privé peut s'avérer nécessaire pour protéger leur intégrité, leur fonctionnement et leur disponibilité. »

---

[33] *Pays-Bas : propositions écrites pour l'avant-projet de l'OEWG*, Groupe de travail à composition non limitée, Assemblée générale de l'ONU, février 2021, https://front.un-arm.org/wp-content/uploads/2021/02/Netherlands-OEWG-written-comments-to-zero-draft.pdf

[34] *Commentaires du Royaume-Uni sur l'avant-projet*, Groupe de travail à composition non limitée, Assemblée générale de l'ONU, février 2020, https://front.un-arm.org/wp-content/uploads/2021/02/UK-submission-to-OEWG-ICTs-zero-draft-002.pdf

[35] *Contributions des organisations intergouvernementales (OIG) et des organisations non gouvernementales (ONG)*, Groupe de travail à composition non limitée, Assemblée générale de l'ONU, 2020, https://www.un.org/disarmament/open-ended-working-group/

[36] *Commentaires de la GCSC sur le premier projet de rapport de fond du Groupe de travail à composition non limitée de l'ONU*, Commission mondiale sur la stabilité du cyberespace, 3 mars 2021, https://front.un-arm.org/wp-content/uploads/2021/03/GCSC-Submission-to-OEWG-First-Draft-Report-March-2021.pdf

[37] *Déclaration de la GCSC sur le projet final de rapport de fond du Groupe de travail à composition non limitée de l'ONU*, Commission mondiale sur la stabilité du cyberespace, 12 mars 2021, https://front.un- arm.org/wp-content/uploads/2021/03/GCSC-Statement-OEWG-Multistakeholder-Consultation-Final- Draft-Report-March-2021.pdf

[38] *Rapport de fond final*, Groupe de travail à composition non limitée, Assemblée générale de l'ONU, 10 mars 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

« 26. Tout en s'accordant sur la nécessité de protéger l'ensemble des infrastructures critiques (IC) et des infrastructures critiques d'information (ICC) qui assurent des services essentiels pour le public, et sur la nécessité de veiller à garantir la disponibilité générale et l'intégrité 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. »

Conclusion

Certains considèrent que le terme « noyau public » est utilisé non seulement dans le contexte du GGE et de l'OEWG mais aussi au-delà. Ainsi, un membre de la GCSC a écrit ce qui suit à propos de la norme de la GCSC relative au noyau public : « Cette norme a beaucoup de potentiel pour un développement plus poussé et pourrait être le point de départ pour la rédaction d'un nouveau type d'accord international qui établirait des droits et des responsabilités non seulement pour les États mais aussi pour les acteurs non étatiques ».[39]

L'introduction dans un document de l'ONU d'un nouveau terme tel que « noyau public », qui « ne fait pas l'objet d'un consensus mondial »[40] et qui n'a pas été défini par les Nations Unies, pourrait ouvrir la voie à de multiples interprétations et à des définitions concurrentes, ainsi qu'à la possibilité pour les Nations Unies et d'autres OIG d'utiliser le terme « noyau public » comme référence dans leur propre travail. Cela peut à son tour élargir la compétence ou le champ d'action de ces OIG pour inclure des éléments qui relèvent actuellement des missions et des attributions d'autres entités multipartites.

L'organisation ICANN, par le biais de son équipe GE, continuera à faire régulièrement des points avec la communauté de l'ICANN pour la tenir informée de toute déclaration ou proposition touchant à la gouvernance technique de l'Internet ou à la mission de l'ICANN.

[39] KLEINWACHTER, Wolfgang, *Advancing Cyberstability* : *Protect the Public Internet Core and Improve Cyber Hygiene* [Progrès dans la cyberstabilité : protéger le noyau publique de l'Internet et améliorer la cyber hygiène], CircleID, novembre 2019, https://www.circleid.com/posts/20191124_cyberstability_protecting_public_internet_core_and_cyber_hygiene/

[40] *Contribution de la Chine au Rapport préliminaire initial de l'OEWG*, Groupe de travail à composition non limitée, Assemblée générale de l'ONU, avril 2020, https://front.un-arm.org/wp-content/uploads/2020/04/china-contribution-to-oewg-pre-draft-report-final.pdf

Annexe I
Cyberstratégie internationale

En 2017, le gouvernement néerlandais a déclaré que la publication de sa cyberstratégie internationale lui permettait « d'honorer l'engagement qu'il avait pris dans sa réponse aux rapports consultatifs du Conseil consultatif pour les questions internationales (AIV) (*L'Internet : un espace mondial libre avec un contrôle limité de l'État*) et du Conseil scientifique pour la politique gouvernementale (WRR) (*Le noyau public de l'Internet*) ».[41]

Dans ce document, nous relevons, entre autres, les déclarations suivantes :

- Point 2.4. : « Les avantages économiques et sociaux liés à l'Internet exigent que le "noyau public" de l'Internet fonctionne de manière fiable, prévisible, stable et sûre. Ce noyau possède des caractéristiques propres à un bien public international qui transcendent les intérêts souverains et privés individuels. Les Pays-Bas reconnaissent que, compte tenu de la nature du cyberespace et de notre dépendance à son égard, il est nécessaire de faire preuve de prudence lorsqu'il s'agit de mener des activités susceptibles d'affecter ce noyau public. Dans la mesure du possible, la responsabilité de maintenir et de développer ce noyau public devrait incomber à la communauté technologique, tandis que l'État devrait jouer un rôle de soutien. »[42]

- Point 4.2. : « Étant donné les intérêts publics mondiaux associés à l'Internet, le gouvernement cherche également à faire reconnaître le noyau de l'Internet comme un bien public international. Les Pays-Bas reconnaissent que, compte tenu de la nature du cyberespace et de notre dépendance à son égard, il est nécessaire de faire preuve de prudence lorsqu'il s'agit de mener des activités susceptibles d'affecter ce noyau public. Les Pays-Bas travaillent à l'élaboration et à la promotion de normes et de règles de conduite internationales. À cette fin, les Pays-Bas ont soumis une proposition au Groupe d'experts gouvernementaux des Nations Unies (GGE) sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale. »[43]

[41] Ministère des Affaires étrangères des Pays-Bas, *Building Digital Bridges, International Cyber Strategy Towards an integrated international cyber policy* [Jeter des ponts numériques. Cyberstratégie internationale. Vers une politique internationale intégrée en matière de cyberespace], Lettre au Parlement, 2017, https://www.government.nl/documents/parliamentary-documents/2017/02/12/international-cyber-strategy

[42] Ministère des Affaires étrangères des Pays-Bas, *Building Digital Bridges, International Cyber Strategy Towards an integrated international cyber policy* [Jeter des ponts numériques. Cyberstratégie internationale. Vers une politique internationale intégrée en matière de cyberespace], Lettre au Parlement, 2017, point 2.4, principe 4.

[43] Ministère des Affaires étrangères des Pays-Bas, *Building Digital Bridges, International Cyber Strategy Towards an integrated international cyber policy* [Jeter des ponts numériques. Cyberstratégie internationale. Vers une politique internationale intégrée en matière de cyberespace], Lettre au Parlement, 2017, point 4.2.

Annexe II
Rapport du Conseil consultatif pour les questions internationales (AIV)

Dans son rapport de 2014, *L'Internet : un espace libre mondial avec un contrôle limité de l'État*, le Conseil consultatif pour les questions internationales (AIV) a reconnu que « le système d'adressage et le système des noms de domaine, qui présentent une importance commerciale majeure, doivent également être considérés comme faisant partie de la gouvernance de l'Internet ».[44]

[44] *The Internet: A Global Free Space with Limited State Control* [L'Internet : un espace mondial libre avec un contrôle limité de l'État], Conseil consultatif pour les questions internationales, novembre 2014, p. 48,

https://www.advisorycouncilinternationalaffairs.nl/documents/publications/2014/12/01/the-internet

Annexe III
Définition de « noyau public »

Les éléments constitutifs suivants (routage et transmission de paquets, systèmes de nommage et de numéros, mécanismes cryptographiques de sécurité et d'identité, supports de transmission physique) sont détaillés de manière plus précise dans la définition du noyau public de l'Internet établie par la GCSC à Bratislava en mai 2018 : [45]

« **Le routage et la transmission de paquets** comprennent, sans s'y limiter : l'équipement, les installations, l'information, les protocoles et les systèmes qui facilitent la transmission de communications par paquets de leurs sources à leurs destinations. Cela inclut les points d'échange Internet (les sites physiques où la bande passante Internet est produite) ainsi que les routeurs d'échange de trafic et les routeurs centraux des principaux réseaux qui transportent cette bande passante aux utilisateurs. Les systèmes nécessaires pour garantir l'authenticité du routage et pour défendre le réseau contre des comportements abusifs y sont également inclus. Il en est de même pour la conception, la production et la chaîne d'approvisionnement des équipements utilisés aux fins susmentionnées. Cela inclut également l'intégrité des protocoles de routage eux-mêmes et de leurs processus de développement, de normalisation et de maintenance.
Les systèmes de nommage et de numéros comprennent, sans s'y limiter : les systèmes et les informations à la base du fonctionnement du système des noms de domaine de l'Internet, y compris les registres, les serveurs de noms, le contenu de zone, l'infrastructure et des processus tels que le DNSSEC, utilisé pour la signature cryptographique des enregistrements, ainsi que les services d'information WHOIS pour la zone racine, la hiérarchie d'adresses inverses, les extensions géographiques de premier niveau, les noms géographiques, les domaines de premier niveau internationalisés et les nouveaux domaines génériques et non militaires de premier niveau. Les résolveurs DNS récursifs publics fréquemment utilisés y sont également inclus. Cela comprend les systèmes de l'Autorité chargée de la gestion de l'adressage sur Internet et ceux des registres Internet régionaux qui rendent disponible et assurent l'attribution unique des adresses de protocole Internet, des numéros du système autonome et des identificateurs de protocole Internet. Les protocoles de nommage et de numérotation eux-mêmes ainsi que l'intégrité des processus de normalisation et des résultats pour l'élaboration et la maintenance des protocoles y sont également inclus.
Les mécanismes cryptographiques de sécurité et d'identité comprennent, sans s'y limiter : les clés cryptographiques utilisées pour authentifier les utilisateurs et les dispositifs et sécuriser les transactions sur Internet, ainsi que l'équipement, les installations, l'information, les protocoles et les systèmes qui permettent la production, la communication, l'utilisation et la révocation de ces clés. Cela inclut les serveurs de clés PGP, les autorités de certification et leur infrastructure de clé publique, DANE avec ses protocoles et son infrastructure, les mécanismes de révocation de certificats et les journaux de transparence, les gestionnaires de mots de passe et les authentificateurs d'accès en itinérance. Ils comprennent également l'intégrité des processus et des résultats de la normalisation pour le développement et la maintenance d'algorithmes et de protocoles cryptographiques, ainsi que la conception, la production et la chaîne d'approvisionnement des équipements utilisés pour mettre en œuvre les processus cryptographiques.

[45] *Definition of the Public Core, to Which the Norm Applies* [Définition du noyau public, auquel s'applique la norme], Commission mondiale sur la stabilité dans le cyberespace, mai 2018.

Les supports de transmission physiques comprennent, sans s'y limiter : les systèmes de câbles physiques et les installations pour les communications câblées desservant le public, qu'il s'agisse de fibres ou de cuivre. Cela comprend les câbles terrestres et sous-marins, les stations d'atterrissage, les centres de données et d'autres installations physiques à l'appui. Ils comprennent les systèmes de soutien pour la transmission, la régénération du signal, la dérivation, le multiplexage et la discrimination signal-bruit.

Il est entendu que cela inclut les systèmes de câbles qui desservent des régions ou des populations, mais non pas ceux qui desservent des clients de sociétés individuelles. Certains experts estiment que bien plus de catégories d'infrastructures liées à l'Internet et aux TIC méritent d'être protégées, de sorte que cette définition pourrait être élargie à l'avenir ».