ICANN | GAC
Governmental Advisory Committee

ICANN 73 VIRTUAL COMMUNITY FORUM

Atténuation de l'utilisation malveillante du DNS

Séance 10

Table des matières

Objet de la séance p.1	Proposition des dirigeants pour la ligne d'action du GAC p.1	État actuel et développements récents p. 2	Principaux documents de référence p.8

Objets de la séance

Cette séance vise à poursuivre l'examen du GAC des initiatives lancées par l'organisation ICANN et la communauté de l'ICANN dans le but de prévenir et d'atténuer l'utilisation malveillante du DNS. Parmi ces initiatives figurent la mise en œuvre des recommandations des révisions de la CCT et de la Deuxième équipe de révision de la sécurité, la stabilité et la résilience du DNS, les discussions ayant suivi la conclusion du Groupe de travail de la GNSO consacré au PDP relatif aux procédures pour des séries ultérieures de nouveaux gTLD, les propositions du SSAC pour l'établissement d'un facilitateur commun de réponse à des abus, et l'étude récemment publiée par la Commission européenne. Cette séance sera également l'occasion de poursuivre le débat sur des propositions concrètes possibles du GAC.

Proposition des dirigeants pour la ligne d'action du GAC

1. **Se pencher sur les conclusions et les recommandations de l'étude sur l'utilisation malveillante du DNS, publiée par la Commission européenne**[1] et présentée au Groupe de travail du GAC sur la sécurité publique avant l'ICANN73.[2]

2. **Examiner l'état d'avancement des activités** de lutte contre l'utilisation malveillante du DNS, **menées par l'organisation ICANN** dans le cadre de ses programmes d'atténuation des menaces liées à la sécurité du DNS et de conformité contractuelle, comme indiqué récemment dans l'exposé du PDG de l'ICANN au GAC en préparation de l'ICANN73[3]

[1] Voir l'Étude de la Commission européenne sur l'utilisation malveillante du DNS et son Annexe technique (31 janvier 2022)

[2] Voir https://gac.icann.org/sessions/pre-icann73-pswg-conference-call (17 février 2022) [connexion requise]

[3] Voir https://gac.icann.org/sessions/icann-org-ceo-pre-icann73-oral-briefing-for-the-gac (16 février 2022) [connexion requise]

3. **Évaluer l'état d'avancement des discussions et efforts de mise en œuvre de la communauté ICANN concernant** les recommandations pertinentes de l'équipe de révision de la CCT, de l'équipe de révision de la SSR2, de l'équipe de travail du SSAC sur l'utilisation malveillante du DNS (SAC115), ainsi que des initiatives volontaires des parties contractantes, à la lumière de l'avis pertinent formulé par le GAC dans ses communiqués de l'ICANN Montréal et de l'ICANN72.

État actuel et développements récents

Discussions de la communauté et mesures concrètes prises à ce jour

- Au cours des récentes réunions de l'ICANN, **les dirigeants du groupe de travail du GAC sur la sécurité publique (PSWG) ont présenté** au GAC un exposé sur la question de l'utilisation malveillante du DNS[4] dans le cadre du Plan de travail du PSWG pour 2020-2021 et son objectif stratégique n° 1, à savoir le développement des capacités d'atténuation de la cybercriminalité et de l'utilisation malveillante du DNS.
    - Le GAC a examiné les **mesures mises à la disposition des opérateurs de registre et des bureaux d'enregistrement et visant à prévenir l'utilisation malveillante du DNS**, en particulier le rôle des politiques d'enregistrement (y compris la vérification d'identité) et des stratégies de tarification comme déterminants clés des niveaux d'utilisation malveillante dans un TLD donné.
    - Le GAC s'est penché sur les initiatives en cours ou possibles visant à traiter plus efficacement l'utilisation malveillante du DNS au niveau du Conseil d'administration de l'ICANN et de l'organisation ICANN[5], notamment des modifications aux contrats de l'ICANN avec les opérateurs de registre et les bureaux d'enregistrement, l'application des exigences existantes, la mise en œuvre des recommandations pertinentes de la révision de la CCT et de la SSR2, les recommandations de politique pour les fournisseurs de service d'anonymisation et d'enregistrement fiduciaire, l'amélioration de l'exactitude des données d'enregistrement et la publication de données plus détaillées sur les cas d'utilisation malveillante de noms de domaine.
    - Dans son communiqué de l'ICANN72 (1er novembre 2021), le GAC a souligné « ***la nécessité d'améliorer les conditions contractuelles de sorte à lutter plus efficacement contre l'utilisation malveillante du DNS.*** *À cet égard, le rôle de l'ICANN selon les statuts constitutifs comprend la prise en compte des préoccupations de politique publique des gouvernements et autorités publiques et le fait d'agir dans l'intérêt public. Les statuts constitutifs autorisent également l'ICANN à négocier des accords, et entre autres des engagements d'intérêt public, aux fins de sa mission. C'est dire que l'ICANN est particulièrement bien placée pour négocier des améliorations aux contrats existants afin*

[4] Voir les documents des séances plénières pertinentes du GAC de l'ICANN66, l'ICANN68, l'ICANN69, l'ICANN70 et l'ICANN71

[5] Voir les procès-verbaux de l'ICANN66, le communiqué du GAC et les procès-verbaux de l'ICANN68, le communiqué du GAC et les procès-verbaux de l'ICANN69, le communiqué du GAC et les procès-verbaux de l'ICANN70, et le communiqué du GAC et les procès-verbaux de l'ICANN71.

de réduire plus efficacement l'utilisation malveillante du DNS, comme cela a été informé par le GAC et d'autres parties prenantes défendant l'intérêt public. »

- **Les dirigeants du GAC et du conseil de la GNSO ont discuté des questions spécifiques du GAC** fournies à la GNSO avant chaque réunion de l'ICANN depuis l'ICANN70[6]
  - **Le GAC a demandé à la GNSO des mises à jour sur le travail communautaire qu'elle envisage de mener**, à la lumière des conclusions du PDP sur les séries ultérieures de nouveaux gTLD (qui s'est abstenu de faire des recommandations sur l'atténuation de l'utilisation malveillante du DNS pour les futurs gTLD uniquement), des recommandations de la révision de la SSR2, et des recommandations formulées par le SSAC dans son document SAC115.
  - **Les dirigeants du conseil de la GNSO ont reconnu l'importance du sujet pour la communauté de l'ICANN** ainsi que la valeur de la longue discussion sur cette question. Ils ont néanmoins fait remarquer que la **poursuite des travaux nécessite un cadrage approprié** et le développement **d'une vision commune**, en particulier en ce qui concerne la définition de l'utilisation malveillante du DNS et la compatibilité de cette définition avec la mission de l'ICANN, **mais n'ont pas précisé d'échéancier pour ces travaux**[7].
  - Le 31 janvier 2022, le conseil de la GNSO a annoncé la formation d'une **petite équipe investie d'un double mandat : examiner « *les efforts éventuels de politiques qu'il devrait envisager d'entreprendre* *à l'appui des efforts de lutte contre l'utilisation malveillante du DNS engagés par différentes parties de la communauté » et « établir avec d'autres parties de la communauté qui se sont exprimées sur le sujet (dont le Comité consultatif gouvernemental […]) un dialogue visant à éclaircir ce qu'elles attendent de la GNSO et si/comment elles souhaitent voir le travail futur de politiques contribuer (ou non) aux initiatives déjà en chantier ».*

- **Mesures et initiatives visant à atténuer l'utilisation malveillante du DNS par les registres et les bureaux d'enregistrement**
  - Le 27 mars 2020, l'organisation ICANN a exécuté les modifications proposées au contrat de registre de .COM. **Celles-ci ont pour effet d'étendre, aux deux tiers de l'espace de noms gTLD, les dispositions contractuelles destinées à faciliter la détection et le signalement de l'utilisation malveillante du DNS[8]**. En outre, une lettre d'intention contraignante entre l'organisation ICANN et Verisign établit un cadre de coopération pour la mise au point de meilleures pratiques, de nouvelles obligations contractuelles potentielles et d'indicateurs visant à mesurer et à atténuer les menaces à la sécurité du DNS.

[6] Voir les messages et questions au conseil de la GNSO en préparation de l'ICANN70

[7] Voir les procès-verbaux de l'ICANN70 (p.16), les procès-verbaux de l'ICANN71 (p.13) et les procès-verbaux de l'ICANN72 (p.9)

[8] Ces dispositions incluent la spécification 11 3b qui n'était applicable, jusqu'à présent, qu'aux nouveaux gTLD.

- **Dans le contexte de la crise du COVID-19, les parties contractantes et les parties prenantes de la sécurité publique** ont fait rapport[9] sur leur collaboration à faciliter les rapports, leur révision et leur renvoi à la juridiction compétente à travers l'adoption d'un formulaire normalisé et l'établissement d'un point de contact unique pour les autorités compétentes. Ces efforts s'appuient sur les relations de travail établies entre les organismes d'application de la loi et les bureaux d'enregistrement ainsi que sur le Guide des bureaux d'enregistrement pour le signalement d'abus, publié par le **Groupe des représentants des bureaux d'enregistrement** à l'occasion de l'ICANN67. Ce guide a été mis à jour (janvier 2022) et approuvé par le **Groupe des représentants des opérateurs de registre**.
- Le **Registre d'intérêt public (PIR)**, opérateur de registre de .ORG et de plusieurs nouveaux gTLD, a lancé (17 février 2021) l'**Institut de lutte contre l'utilisation malveillante du DNS**. Cette initiative a été présentée au PSWG du GAC (3 mars 2021). Dans le communiqué de l'ICANN70, le GAC a salué la création de l'Institut de lutte contre l'utilisation malveillante du DNS et *« encouragé les efforts communautaires visant à s'unir pour lutter de manière holistique contre l'utilisation malveillante du DNS »*. L'Institut de lutte contre l'utilisation malveillante du DNS a depuis publié https://dnsabuseinstitute.org/the-dns-abuse-institute-roadmap/une feuille de route (14 juin 2021) et un article (24 aout 2021) traitant de l'atténuation des dommages à diverses couches de l'infrastructure Internet. Plus récemment, il a signalé la mise au point d'un outil centralisé de signalement de l'utilisation malveillante (18 nov. 2021) et publié une meilleure pratique concernant la détection des enregistrements malveillants (2 déc. 2021).

-

- **Réponse multidimensionnelle de l'organisation ICANN[10] (qui fait désormais partie du programme d'atténuation des menaces à la sécurité du DNS) et conformité contractuelle**
  - L'organisation ICANN a présenté (22 juillet 2021) son programme d'atténuation des menaces à la sécurité du DNS. Le programme vise à fournir une visibilité et une clarté sur les diverses initiatives et projets liés aux menaces à la sécurité du DNS et permet la création et l'exécution d'une stratégie centralisée.
  - **Le Bureau du directeur de la technologie (OCTO) de l'ICANN et son équipe consacrée à la sécurité, la stabilité et la résilience** (SSR) mènent des recherches et assurent l'expertise de l'ICANN en matière de sécurité du DNS au profit de la communauté. Ils sont engagés dans des forums de veille en matière de cybermenaces et de réponse aux incidents, et mettent au point des systèmes et des outils permettant de détecter, d'analyser et de signaler l'utilisation malveillante du DNS[11].

---

[9] Voir les présentations effectuées par les parties prenantes avant et pendant la réunion ICANN68 et la séance d'information du PSWG au GAC réalisée dans le cadre de l'ICANN68.

[10] Le Président et directeur général de l'ICANN a publié un billet de blog le 20 avril 2020 détaillant la réponse multidimensionnelle de l'organisation ICANN à l'utilisation malveillante du DNS

[11] Lors d'un appel du GAC portant sur des questions liées à l'utilisation malveillante du DNS (24 février 2021), l'organisation ICANN a fait le point sur les activités de l'OCTO liées à l'utilisation malveillante du DNS, dont une discussion sur la définition des

- En réponse à la crise du COVID-19, l'OCTO a mis au point l'outil de **signalement et de collecte d'informations sur les menaces à la sécurité des noms de domaine (DNSTICR)** visant à faciliter l'identification des noms de domaine utilisés dans les cas d'abus liés au COVID-19 et le partage des données avec les parties pertinentes. Le GAC a reçu un exposé sur cette initiative avant l'ICANN68 (12 juin 2020) et ses membres ont été invités à contribuer à la diversité linguistique de l'outil.
- Grâce à sa **plateforme de signalement des cas d'utilisation malveillante des noms de domaine (DAAR)**, l'ICANN rend compte tous les mois, depuis janvier 2018, de l'enregistrement de noms de domaine et des menaces à la sécurité observées dans le DNS[12]. En octobre 2021, l'organisation ICANN et le Groupe de représentants des opérateurs de registre ont fait rapport sur leur accord de principe[13] relatif à l'exploitation des données d'enregistrement détenues par les registres et visant la fourniture dans le DAAR d'informations du niveau des bureaux d'enregistrement, comme l'a reconnu le GAC dans sa lettre récemment adressée à l'ICANN (21 février 2022).
- L'OCTO a soutenu le **Groupe d'étude technique chargé de l'initiative de facilitation de la sécurité du DNS**, créé en mai 2020, dans le cadre de la mise en œuvre du plan stratégique pour les exercices fiscaux 2021 à 2025, dans le but de *« réfléchir à ce que l'ICANN peut et devrait faire pour augmenter le niveau de collaboration et d'engagement avec les parties prenantes de l'écosystème du DNS afin d'améliorer le profil de sécurité du DNS »*. Son rapport final (15 octobre 2021) a été publié après 18 mois de délibérations. L'organisation ICANN a indiqué au GAC (16 février 2022) être en train de concevoir un plan d'action en conséquence.

- Pour ce qui est de **l'application de la conformité contractuelle,** le PDG de l'ICANN a rappelé dans son billet de blog (20 avril 2020) ce qui suit : « *Le département de l'ICANN chargé de la conformité contractuelle veille au respect des obligations établies dans les politiques et les contrats de l'ICANN, en particulier le contrat de registre (RA) et le contrat d'accréditation des bureaux d'enregistrement (RAA). Par ailleurs, ce département travaille en étroite collaboration avec l'OCTO pour détecter les menaces à la sécurité du DNS […] et les relier aux parties contractantes concernées. Il se sert des données collectées pendant les audits […] pour évaluer si les opérateurs de registre et les bureaux d'enregistrement se conforment à leurs obligations en matière d'atténuation des menaces à la sécurité du*

menaces à la sécurité du DNS et de l'utilisation malveillante du DNS, les obligations des parties contractantes, le système de signalement des cas d'utilisation malveillante des noms de domaine (DAAR), les informations relatives aux menaces à la sécurité des noms de domaine, l'outil de signalement et de collecte d'information sur des menaces à la sécurité des noms de domaine (DNSTICR), la nouvelle initiative visant à élaborer des normes pour le partage de connaissances et l'instauration de normes pour la sécurité du DNS et du nommage (KINDNS), et une révision des efforts de l'OCTO dans le domaine de la formation et du renforcement des capacités à travers le monde.

[12] Plusieurs parties prenantes et initiatives de l'ICANN ont commenté les limites du DAAR, en particulier une lettre du M3AAWG à l'organisation ICANN (5 avril 2019) et le rapport préliminaire de l'équipe de révision SSR2 (24 janvier 2020). Le groupe des représentants des opérateurs de registre, qui avait également exprimé des préoccupations, a formulé des recommandations dans une correspondance adressée au CTO de l'ICANN (9 septembre 2020).

[13] Voir la Lettre du RySG à l'ICANN (22 octobre 2021) et le billet de blog de l'ICANN (28 octobre 2021)

DNS. En dehors de ces audits, le département chargé de la conformité contractuelle utilisera les données collectées par l'OCTO et d'autres pour contacter de manière proactive des registres et des bureaux d'enregistrement qui affichent un nombre disproportionné de menaces à la sécurité du DNS. Si le dialogue constructif se solde par un échec, le département n'hésitera pas à faire exécuter les contrats de tous ceux qui refuseraient de se conformer à leurs obligations en matière de menaces à la sécurité du DNS ».

- Après un premier **audit de conformité contractuelle** de l'opérateur de registre (achevé en juin 2019)[14], axé sur l'utilisation malveillante de l'infrastructure du DNS, l'ICANN a présenté (le 24 aout 2021) les résultats de l'audit sur **la conformité des bureaux d'enregistrement à leurs obligations en matière d'atténuation des risques liés à la sécurité du DNS** :
  - l'audit a inclus 126 bureaux d'enregistrement (gérant plus de 90 % de tous les domaines enregistrés dans les gTLD) ;
  - 111 bureaux d'enregistrement n'ont pas entièrement satisfait aux exigences relatives à la réception et au traitement des signalements d'utilisation malveillante du DNS (sections 3.18.1 à 3.18.3 du RAA) ;
  - 92 bureaux d'enregistrement ont pris des mesures pour devenir entièrement conformes et 19 mettent en œuvre des changements.
- Au cours de l'exposé présenté par le Président-directeur général de l'ICANN au GAC en préparation de l'ICANN73 (16 février 2022), le service de conformité contractuelle de l'ICANN a passé en revue les obligations relatives à l'atténuation des risques liés à la sécurité du DNS, prévues dans les contrats de l'ICANN ; il a présenté les résultats d'un échantillon de 3378 plaintes concernant le traitement, par les bureaux d'enregistrement, de rapports d'utilisation malveillante, conduisant à 456 enquêtes de conformité et à 1 avis de violation.

Recommandations de la communauté pour les travaux futurs

- **Recommandations issues de la révision SSR2**
  - L'équipe de révision SSR2 a présenté un rapport préliminaire (24 janvier 2020) qui met l'accent sur les mesures visant à prévenir et à atténuer l'utilisation malveillante du DNS. Le commentaire du GAC (3 avril 2020) soutenait bon nombre des recommandations, notamment celles portant sur l'amélioration du système de signalement des cas d'utilisation malveillante des noms de domaine (DAAR) et sur le renforcement des mécanismes de conformité.

[14] Voir le blog de l'ICANN « Conformité contractuelle :Traiter les cas d'utilisation malveillante de l'infrastructure du DNS (système des noms de domaine) » (8 novembre 2018) et le « Rapport d'audit du département chargé de la conformité contractuelle sur la réponse des opérateurs de registre aux menaces à la sécurité du DNS » (17 septembre 2019)

- Le rapport final (25 janvier 2021) a été examiné par le GAC lors de l'ICANN70 en vue de la soumission possible de commentaires du GAC (8 avril 2021) dans le cadre de la procédure de consultation publique.
- Le Conseil d'administration de l'ICANN a pris des décisions (22 juillet 2021) sur les 63 recommandations finales de l'équipe de révision (25 janvier 2021). Un billet de blog publié par l'organisation ICANN présente un résumé des décisions prises :
  - 13 recommandations ont été approuvées (en attendant la planification de leur mise en œuvre) ;
  - 16 recommandations ont été rejetées (entre autres, 6 qui n'ont pas pu être approuvées dans leur intégralité) ;
  - 34 recommandations sont en attente d'informations et d'analyses complémentaires.
- Dans son communiqué de l'ICANN72 (1er novembre 2021), le GAC a recommandé au Conseil d'administration de l'ICANN :
  - *d'entreprendre à titre prioritaire les actions de suivi qui s'imposent pour soutenir la mise en œuvre rapide de la fiche de suivi du Conseil […] ;*
  - *de fournir de plus amples renseignements sur la divergence d'interprétation par le Conseil d'administration et par l'équipe de révision SSR2 du niveau de mise en œuvre de certaines recommandations.*
- Le Conseil d'administration de l'ICANN a fourni des renseignements supplémentaires dans sa réponse (16 janvier 2022)

- **L'équipe de travail du Comité consultatif sur la sécurité et la stabilité (SSAC) consacrée à l'utilisation malveillante du DNS** a publié son rapport SAC115 (19 mars 2021) qui propose une approche interopérable pour la gestion de l'utilisation malveillante du DNS.
  - Dans ce rapport, le **SSAC propose un cadre général de bonnes pratiques et de processus** visant à optimiser le signalement des cas d'utilisation malveillante du DNS et des cas d'abus sur Internet en général, prévoyant notamment : un responsable principal pour le règlement de litiges relatifs à l'utilisation malveillante, des normes en matière de preuve, des mécanismes d'intervention progressive, un calendrier d'action raisonnable et la mise à disposition d'informations de contact de qualité.
  - **La principale proposition** que le SSAC recommande de faire examiner et peaufiner par la communauté de l'ICANN en lien avec l'ensemble de la communauté chargée des infrastructures du DNS **est la création d'un « facilitateur commun de réponse aux abus »** sous la forme d'une organisation non gouvernementale à but non lucratif pleinement autonome qui ferait office de facilitateur pour l'ensemble de l'écosystème du DNS, en ce compris les parties contractantes de l'ICANN, les fournisseurs d'hébergement, les fournisseurs de services Internet (FSI) et les réseaux de diffusion de contenu (CDN), afin d'optimiser le signalement des cas d'utilisation malveillante et de minimiser le nombre de victimes d'abus.
  - L'Institut de lutte contre l'utilisation malveillante du DNS a signalé la mise au point d'un outil centralisé de signalement des abus (18 nov. 2021)

Principaux documents de référence

- Étude de la Commission européenne sur l'utilisation malveillante du DNS et son annexe technique (31 janvier 2022)
- Rapport final de la révision de la SSR2 (25 janvier 2021) et fiche de suivi des décisions prises par le Conseil d'administration (22 juillet 2021)
- Annonce de l'ICANN et rapport (24 aout 2021) de l'audit sur la conformité des bureaux d'enregistrement aux obligations en matière d'atténuation des risques liés à la sécurité du DNS.
- Rapport SAC115 (19 mars 2021) du SSAC, qui propose une approche interopérable pour traiter la gestion de l'utilisation malveillante du DNS

Informations complémentaires

Document d'information politique du GAC sur l'atténuation de l'utilisation malveillante du DNS
https://gac.icann.org/briefing-materials/public/gac-policy-background-dns-abuse-mitigation.pdf

Gestion des documents

Titre	Séance d'information du GAC pour ICANN73 — Utilisation malveillante du DNS
Distribution	Membres du GAC (avant la réunion) et public en général (après la réunion)
Date de distribution	Version 1 : 24 février 2022