
Atténuation de l'utilisation malveillante du DNS

Séances 4 et 9

Table des matières

Objectifs de la séance	p.1	Proposition des dirigeants pour la ligne d'action du GAC	p.1	Situation actuelle et faits récents	p.2	Principaux documents de référence	p.14
------------------------	-----	--	-----	-------------------------------------	-----	-----------------------------------	------

Objectifs de la séance

Cette séance a pour but de poursuivre l'examen par le GAC des initiatives de l'organisation et de la communauté ICANN visant à prévenir et atténuer l'utilisation malveillante du DNS. Le GAC sera informé des faits nouveaux et continuera ses discussions sur les éventuels efforts qu'il pourrait déployer afin de se mobiliser avec l'ensemble de la communauté de l'ICANN pour apporter un soutien au renforcement des dispositions contractuelles et aux éventuels processus d'élaboration de politiques visant à favoriser l'atténuation de l'utilisation malveillante du DNS.

Proposition des dirigeants pour la ligne d'action du GAC

- Penser à des améliorations possibles aux contrats de l'ICANN avec les opérateurs de registres et les bureaux d'enregistrement en vue de l'atténuation efficace de l'utilisation malveillante du DNS**, dans le contexte des négociations contractuelles en cours entre l'ICANN et les parties contractantes¹.
- Faire un suivi sur [le Communiqué de LaHaye](#) (20 juin 2022) et sur la position du GAC selon laquelle «*l'organisation ICANN est particulièrement bien placée pour recevoir des retours de la communauté de l'ICANN sur les questions de politique publique et de négocier des mises à jour aux contrats de base des registres et des bureaux d'enregistrement*».**
- Examiner l'état des recommandations de révision relatives à l'atténuation de l'utilisation malveillante du DNS**, en particulier celles du [rapport final de la révision de la CCT](#) (8 septembre 2018) et du [rapport final de la révision SSR2](#) (25 janvier 2021).

¹ Voir le blog du PDG de l'ICANN, du 18 janvier 2023 : « [L'ICANN et les parties contractantes négocient le renforcement des exigences en matière d'abus du DNS](#) ».

4. **Discuter de la portée de l'élaboration d'une politique souhaitable destinée à améliorer la prévention et l'atténuation de l'utilisation malveillante du DNS**, dans le prolongement de la [recommandation de la petite équipe de la GNSO sur l'utilisation malveillante du DNS](#) (7 octobre 2022) qui préconise le lancement d'un processus d'élaboration d'une politique relative aux enregistrements malveillants, et de la portée éventuellement limitée des négociations contractuelles en cours sur cette question.

Situation actuelle et faits récents

- **Les négociations contractuelles en cours visent à définir des obligations de base pour exiger des opérateurs de registre et bureaux d'enregistrement qu'ils atténuent ou démasquent l'utilisation malveillante du DNS.**
 - Depuis l'ICANN66, **les dirigeants du Groupe de travail du GAC sur la sécurité publique ont informé le GAC** sur la question de l'atténuation de l'utilisation malveillante du DNS,² notamment **les mesures à la disposition des opérateurs de registre et bureaux d'enregistrement pour prévenir ce phénomène**, en particulier le rôle des politiques d'enregistrement (en ce compris la vérification de l'identité) et des stratégies de tarification en tant que déterminants clés des niveaux d'utilisation malveillante dans un TLD donné; ainsi que sur les **possibilités qui s'offrent au Conseil d'administration de l'ICANN et à l'organisation ICANN de s'attaquer plus efficacement à l'utilisation malveillante du DNS**, notamment les révisions aux contrats de l'ICANN avec les opérateurs de registre et les bureaux d'enregistrement, l'application effective des exigences existantes, la mise en œuvre des recommandations pertinentes de la révision de la CCT et de la SSR2, les recommandations concernant la politique relative aux fournisseurs de service d'enregistrement fiduciaire/d'anonymisation, l'amélioration de l'exactitude des données d'enregistrement et la publication de données plus détaillées sur les activités malveillantes.
 - Dans des communiqués récents, le GAC a souligné «la nécessité d'améliorer les conditions contractuelles pour traiter plus efficacement la question de l'utilisation malveillante du DNS» ([Communiqué du GAC de l'ICANN72](#), 1er novembre 2021) et a indiqué que «l'amélioration des dispositions contractuelles pourrait permettre de se concentrer sur le signalement et le traitement des cas d'utilisation malveillante du DNS et la mise en œuvre des exigences contractuelles connexes» ([Communiqué de La Haye](#), 20 juin 2022). Le GAC a également mis en exergue le fait que l'ICANN est «*particulièrement bien placée pour négocier des améliorations aux contrats existants*» et «*pour recevoir des retours de la communauté de l'ICANN sur les questions de politique publique*».
 - Au cours de l'ICANN75, **la petite équipe de la GNSO sur l'utilisation malveillante du DNS a discuté des «lacunes dans l'interprétation et/ou l'application» des contrats actuels de l'ICANN**, comme le reflètent ensuite ses [recommandations au conseil de la GNSO](#) (7

² Voir les documents des plénières du GAC de [l'ICANN66](#), [l'ICANN68](#), [l'ICANN69](#), [l'ICANN70](#), [l'ICANN71](#), [l'ICANN72](#), [l'ICANN73](#) et [l'ICANN74](#).

octobre 2022).

- Dans le [communiqué de Kuala Lumpur](#) (26 septembre 2022), le **GAC a rappelé son « soutien à l'élaboration des dispositions contractuelles proposées applicables à tous les gTLD afin d'améliorer les réponses à l'utilisation malveillante du DNS »³, dont celles recensées par la SSR2 et par la révision de la CCT ».**
- En novembre 2022, les groupes de représentants des opérateurs de registre et des bureaux d'enregistrement ont [fait part](#) de leur **volonté de «rechercher des améliorations possibles aux obligations en matière d'utilisation malveillante du DNS** contenues dans [leurs] accords respectifs avec l'ICANN», ce à quoi [l'organisation ICANN a répondu](#) (30 nov. 2022) qu'elle «s'alignait sur les orientations proposées dans [la] lettre pour toute négociation». Ces orientations ont été énoncées comme suit dans la correspondance des parties contractantes avec l'ICANN :
 - *Les nouvelles dispositions se concentreront sur l'utilisation malveillante du DNS telle qu'elle est définie dans les contrats existants de l'ICANN, et renforcée par la petite équipe de la GNSO sur l'utilisation malveillante du DNS;*
 - *Les modifications n'incluront pas les questions relatives aux abus de contenu des sites Web ni l'accès aux données d'enregistrement; et*
 - *Toute nouvelle disposition [...] ne cherchera pas à imposer des exigences de transmission à l'un ou l'autre groupe.*
- En décembre 2022, le [Groupe des représentants des bureaux d'enregistrement \(RrSG\)](#) et le [Groupe des représentants des opérateurs de registre \(RySG\)](#) ont formellement **notifié à l'ICANN l'ouverture de négociations** visant respectivement à «*incorporer des exigences contractuelles de base à l'article 3.18 du RAA pour que les bureaux d'enregistrement démasquent et/ou atténuent l'utilisation malveillante du système de noms de domaine*» et à «*améliorer les obligations relatives à l'utilisation malveillante du DNS contenues dans [le contrat de registre]*».
- Un récent [blog](#) du **PDG de l'ICANN** (18 janvier 2023) a confirmé le travail en cours «*visant à définir les obligations de base afin d'exiger des registres et des bureaux d'enregistrement qu'ils atténuent ou démasquent l'utilisation malveillante du DNS*», s'attendant à ce que cela «*aide l'équipe de conformité contractuelle de l'ICANN dans ses efforts de mise en œuvre avec les bureaux d'enregistrement ou les opérateurs de registres qui ne parviennent pas à s'attaquer de manière suffisante à l'utilisation malveillante du DNS*». Il y est également mentionné que ce travail serait une occasion pour la communauté de l'ICANN «*de discuter et de déterminer s'il est nécessaire de définir d'autres obligations par le biais d'un processus d'élaboration de politiques*». **Le PDG de l'ICANN souhaite «partager les versions préliminaires avec la communauté avant l'ICANN77».**
- Entre-temps, l'Unité constitutive des utilisateurs commerciaux (BC) et l'Unité constitutive des représentants de la propriété intellectuelle (IPC) de la GNSO, ainsi que le Comité

³ [Communiqué du GAC de l'ICANN70](#), section IV.1 p. 5

consultatif At-Large (ALAC) ont [demandé](#) (20 janvier 2023) que «les contributions de la communauté soient prises en compte de manière appropriée, et d'aider l'organisation ICANN dans son rôle établi de défenseur des besoins de la communauté et d'arbitre de l'intérêt public».

- En préparation d'une mise à jour par les parties contractantes sur les négociations en cours, une [séance d'information pré-ICANN76 du GAC sur la négociation des contrats concernant l'atténuation de l'utilisation malveillante du DNS](#) (28 février 2023) [*connexion requise au site Web du GAC*], **les responsables thématiques du GAC ont discuté des améliorations possibles aux dispositions contractuelles existantes** en faveur d'une plus grande clarté et d'une meilleure application, **ainsi que des domaines envisageables pour de nouvelles dispositions contractuelles** telles que discutées par la communauté de l'ICANN (notamment dans les recommandations de la révision de la CCT et de la SSR2), à **savoir : les incitations financières et de réputation, les seuils d'utilisation malveillante et les déclencheurs de conformité, les meilleures pratiques et la centralisation du signalement de l'utilisation malveillante.**

- **Perspectives d'élaboration de politique pour la prévention et l'atténuation de l'utilisation malveillante du DNS**

- Comme il est indiqué dans le communiqué du GAC de l'ICANN69 (23 octobre 2020), **«du point de vue du GAC, une véritable dynamique, propice à l'adoption de mesures concrètes, s'est créée dans la mesure où la communauté a progressivement engagé un dialogue constructif afin de faire avancer les travaux dans un but commun, l'atténuation de l'utilisation malveillante du DNS. Suite aux recommandations de la CCT-RT et de la SSR2-RT, puis aux multiples séances intercommunautaires qui se sont tenues et enfin aux plus récents travaux portant sur un cadre de lutte contre l'utilisation malveillante du DNS, le GAC estime à présent qu'il existe un soutien massif à l'adoption de mesures concrètes mettant en place les principales composantes d'une atténuation efficace de l'utilisation malveillante du DNS»**. Le GAC a également pris note du *«fondement de la décision du Conseil d'administration de l'ICANN de prolonger le contrat du PDG de l'ICANN, qui mentionne expressément les travaux en cours au sein de la communauté sur l'utilisation malveillante du DNS qui pourraient déboucher sur des recommandations de politiques»*.
- Avant même la réunion de l'ICANN68, **la direction du GAC a cherché à établir, en collaboration avec la direction du conseil de la GNSO, un cadre de travail communautaire et d'élaboration de politiques possibles pour traiter le problème de l'utilisation malveillante du DNS**. Pendant la réunion bilatérale GAC-GNSO organisée dans le cadre de l'ICANN72, comme en fait état le [procès-verbal de la réunion du GAC de l'ICANN72](#), la présidence du GAC a réitéré que l'utilisation malveillante du DNS *«est une question qui intéresse le GAC depuis longtemps et que le GAC souhaite faire avancer les discussions au sein de la communauté, de manière à favoriser les progrès et la convergence des points de vue avant le lancement des nouveaux gTLD»* et a ajouté que

«le GAC est impatient de trouver un accord sur la manière de gérer les discussions communautaires sur l'atténuation de l'utilisation malveillante du DNS (PDP, CCWG, etc.)».

- Le 31 janvier 2022, le conseil de la GNSO a [formé](#) une **petite équipe de la GNSO sur l'utilisation malveillante du DNS** qui devrait déterminer «les mesures politiques, le cas échéant, que le Conseil de la GNSO devrait envisager de mettre en place afin de soutenir les travaux déjà en cours dans les différents segments de la communauté visant à lutter contre l'utilisation malveillante du DNS».
- Dans la [réponse du GAC](#) (4 avril 2022) à la demande de la GNSO de contributions de la communauté sur l'élaboration de politiques relatives à l'utilisation malveillante du DNS, la présidence du GAC a suggéré que, compte tenu du fait que «les efforts continus de la communauté peuvent produire des initiatives et des résultats bénéfiques qui peuvent rendre inutile le lancement d'un PDP», «à l'heure actuelle [...] il serait prématuré de chercher à réaliser un exercice de cadrage du PDP».
- Dans le [communiqué de La Haye](#) (20 juin 2022), le GAC a déclaré que «**tout PDP sur l'utilisation malveillante du DNS doit être formulé de manière restrictive de manière à obtenir des résultats exploitables en temps opportun**», ce à quoi le Conseil d'administration de l'ICANN a répondu qu'il partageait cet avis et qu'il était prêt à soutenir la communauté de l'ICANN dans cette quête⁴.
- Dans un [rapport au conseil de la GNSO](#) (7 octobre 2022), la **petite équipe de la GNSO a recommandé : le lancement d'un travail d'élaboration de politique à portée étroite portant sur les enregistrements malveillants** (recommandation 1), **un examen plus approfondi du rôle que joue l'enregistrement en masse dans l'utilisation malveillante du DNS** et des mesures déjà en place pour y remédier (recommandation 2), **l'incitation à la poursuite des travaux en vue d'un signalement plus facile, meilleur et exploitable** de l'utilisation malveillante du DNS (recommandation 3), et une éventuelle concertation entre les parties contractantes et la conformité de l'ICANN concernant ses conclusions sur les lacunes potentielles dans l'interprétation et/ou l'application des contrats actuels de l'ICANN (recommandation 4). Le conseil de la GNSO a procédé à la sensibilisation recommandée des [parties contractantes](#) concernant la recommandation 3 et des [parties contractantes, de l'Institut de lutte contre l'utilisation malveillante du DNS et de la conformité de l'ICANN](#) concernant la recommandation 2 (6 janvier 2023).
- **En ce qui concerne l'enregistrement en masse**, la [réponse de la conformité de l'ICANN au conseil de la GNSO](#) (22 février 2023) indique que «les contrats et politiques de l'ICANN ne prévoient pas d'exigences ou de limitations liées à l'enregistrement en masse de noms de domaine. Par conséquent, **la conformité contractuelle de l'ICANN ne recueille pas et ne suit pas les informations sur les enregistrements en masse et le rôle potentiel qu'ils peuvent jouer dans l'utilisation malveillante du système des noms de domaine (DNS)**». La [réponse du l'Institut de la lutte contre l'utilisation malveillante du DNS](#) (24 février 2023) proposait que «**des recherches devraient être menées pour déterminer l'ampleur de tout problème lié à [l'enregistrement en masse de domaines] avant d'entreprendre un**

⁴ Voir <https://gac.icann.org/sessions/boardgac-interaction-group-bgig-call-31-august-2022> (31 août 2022) [connexion requise]

travail de politiques», et notait la pertinence du [cadre pour les algorithmes générés par les domaines associés aux réseaux zombies et aux programmes malveillants](#) élaboré par le RySG et le PSWG du GAC. **L’Institut de la lutte contre l’utilisation malveillante du DNS s’est dit en faveur d’approches basées sur le paiement pour lutter contre l’utilisation malveillante du DNS, faisant observer qu’il serait utile «d’encourager les bureaux d’enregistrement à enquêter sur tous les domaines d’un compte client lorsque l’un de ces domaines est recensé comme malveillant»** dans le cadre des «options sensées et pratiques à la disposition des bureaux d’enregistrement afin de réduire dès maintenant l’utilisation malveillante du DNS [...]», en plus des «frictions au moment de l’enregistrement».

- **État et perspectives de mise en œuvre des recommandations des révisions spécifiques relatives à la perturbation de l’utilisation malveillante du DNS⁵**

- **L’équipe de révision SSR2** a publié 63 recommandations dans son [rapport final](#) (25 février 2021), en accordant une attention particulière aux mesures de prévention et d’atténuation de l’utilisation malveillante du DNS.
 - Le GAC a examiné un [rapport préliminaire de révision de la SSR2](#) (24 janvier 2020) et a approuvé un certain nombre des recommandations préliminaires dans un [commentaire du GAC](#) (3 avril 2020). Ils ont été suivis par les [commentaires du GAC](#) (8 avril 2021) sur les recommandations finales, et l’avis ultérieur du GAC exprimé dans le [communiqué de l’ICANN72](#) (1er novembre 2021) demandant un suivi et des informations supplémentaires sur le degré de mise en œuvre de certaines recommandations, auxquels le Conseil d’administration de l’ICANN a [répondu](#) (16 janvier 2022), ce qui a conduit à d’autres discussions au cours de l’ICANN73⁶, et à des communications de l’organisation ICANN au GAC dans une [lettre](#) (18 mars 2022) et un [courriel de suivi](#) (12 avril 2022).
 - À ce jour, selon le dernier [rapport trimestriel sur les révisions spécifiques de l’ICANN](#) (21 février 2023), sur la base de trois résolutions du Conseil d’administration de l’ICANN ([22 juillet 2021](#), [1er mai 2022](#) et [16 novembre 2022](#)) : **23 recommandations** ont déjà été **approuvées** (dont 14 soumises à un ordre de priorité pour la mise en œuvre), **30 rejetées**, et **10 en attente** d’un examen supplémentaire du Conseil d’administration.
 - **7 Recommandations en attente relatives à l’utilisation malveillante du DNS - 12.1** (*équipe consultative pour l’analyse de l’utilisation malveillante du DNS*), **12.2** (*structurer les accords avec les fournisseurs de données pour permettre un plus grand partage des données*), **12.3** (*publier des rapports qui identifient les registres et les bureaux d’enregistrement dont les domaines contribuent le plus à l’utilisation malveillante du DNS*), **12.4** (*faire rapport des mesures prises par les*

⁵ L’état de toutes les recommandations peut être consulté dans le [rapport trimestriel sur les révisions spécifiques de l’ICANN du quatrième trimestre 2022](#) (21 février 2023), à partir de la page 28, ainsi que dans d’autres documents disponibles à l’adresse suivante : <https://www.icann.org/resources/reviews/specific-reviews/whois>

⁶ Voir le [procès-verbal du GAC de l’ICANN73](#) p.13

opérateurs de registre et les bureaux d'enregistrement pour répondre aux plaintes de conduite illégale et/ou malveillante), **13.1** (portail centralisé pour le dépôt des plaintes d'utilisation malveillante du DNS obligatoire pour tous les gTLD), **13.2** (publier les données de plaintes pour analyse par des tiers) et **14.2** (fournir aux parties contractantes des listes de domaines recensés comme abusifs et faisant partie de leurs portefeuilles) - **sont provisoirement prévues pour être examinées par le Conseil d'administration de l'ICANN au cours du troisième trimestre 2023.** Dans la [fiche de suivi du Conseil d'administration](#) (22 juillet 2021), le Conseil d'administration de l'ICANN a salué «*les efforts considérables de la communauté et de l'organisation ICANN concernant les menaces à la sécurité du DNS*» et a demandé à l'organisation ICANN «*d'évaluer comment cet assemblage de recommandations, ainsi que d'autres recommandations relatives aux menaces à la sécurité du DNS, devrait être pris en compte de manière coordonnée*» afin d'éclairer le Conseil d'administration dans sa décision sur les prochaines étapes.

- **Dans sa récente discussion sur les négociations contractuelles en cours concernant l'utilisation malveillante du DNS, le PSWG du GAC a discuté⁷ de plusieurs recommandations de la SSR2 qui ont été rejetées** par le Conseil d'administration de l'ICANN selon la [fiche de suivi du Conseil d'administration](#) (22 juillet 2021) - **8.1** (commissionner une équipe de négociation qui comprend des experts en abus et en sécurité pour renégocier les contrats des parties contractantes), **9.4** (rapports de conformité réguliers énumérant les outils manquants), **14.4** (fournir aux parties contractantes 30 jours pour réduire la fraction des domaines abusifs en dessous du seuil) et **14.5** (envisager d'offrir des incitations financières) - **pour lesquelles le GAC a reconnu** dans son [communiqué de l'ICANN72](#) (1er novembre 2021) «*les bases procédurales du rejet par le Conseil d'administration*» notant, néanmoins, «*les aspects substantiels utiles de certaines recommandations rejetées, notamment celles qui visent à fournir à l'organisation ICANN et à la conformité contractuelle de l'ICANN des outils appropriés pour prévenir et atténuer l'utilisation malveillante du DNS*».

- o Le [rapport final](#) de l'équipe de révision de la concurrence, de la confiance et du choix des consommateurs (8 septembre 2018) a contenu 35 recommandations. Dans son [communiqué de Montréal](#) (6 novembre 2019), tel que clarifié dans une [correspondance ultérieure avec le Conseil d'administration de l'ICANN](#) (janvier 2020), **le GAC a conseillé au Conseil d'administration «de ne pas procéder à une nouvelle série de gTLD avant la mise en œuvre complète des recommandations [...] qui ont été recensées comme des “conditions préalables” [14 recommandations] ou comme des “priorités élevées” [10 recommandations]».**

Plusieurs de ces recommandations sont pertinentes pour les négociations contractuelles sur l'utilisation malveillante du DNS et ont été discutées récemment par le PSWG du

⁷ Voir la [conférence téléphonique du PSWG](#) du 14 février 2023 [connexion requise au site Web du GAC]

GAC⁸ :

- La **recommandation 17** (*collecter des données sur la chaîne des parties responsables de l'enregistrement des noms de domaine et la rendre publique*) a **été approuvée et sa mise en œuvre est achevée** conformément à sa [documentation de mise en œuvre](#) le 14 septembre 2022.
- La **recommandation 13** (*recueillir des données sur l'impact des restrictions d'enregistrement*, le GAC ayant noté qu'elle «*permettrait une décision et une élaboration de politiques plus éclairée en ce qui concerne les futures dispositions contractuelles standard des opérateurs de registre et bureaux d'enregistrement*») et la **recommandation 20** (*évaluer les mécanismes pour signaler et traiter les plaintes et éventuellement envisager de modifier les futurs contrats de registre standard pour exiger que les opérateurs de registre divulguent de manière plus évidente leurs points de contact de l'utilisation malveillante et fournissent des informations plus granulaires à l'ICANN*) ont été approuvées en partie selon la [fiche de suivi du 22 octobre 2020](#), et leur **mise en œuvre est en cours avec une concurrence estimée pour le T2/T3 2023** selon le [rapport trimestriel sur les révisions spécifiques de l'ICANN du quatrième trimestre 2022](#) (21 février 2023).
- La **recommandation 14** (*incitations à adopter des mesures proactives contre l'utilisation malveillante du DNS*) et la **recommandation 15** (*négozier des modifications pour inclure des dispositions visant à prévenir l'utilisation systémique de bureaux d'enregistrement ou de registres spécifiques pour les abus de sécurité du DNS, et établir des seuils d'utilisation malveillante pour les déclencheurs automatiques de la conformité*) qui ont été placées **en attente** sur la [fiche de suivi du 1er mars 2019 du Conseil d'administration](#) en considération des discussions communautaires en cours sur l'utilisation malveillante du DNS, **sont provisoirement prévues pour être examinées par le Conseil d'administration de l'ICANN au cours du troisième trimestre 2023**. Dans l'intervalle, l'organisation ICANN traite ces recommandations ainsi que d'autres recommandations de révisions spécifiques et avis pertinents au Conseil d'administration.
- Les **recommandations LE.1 et LE.2 de la révision du RDS-WHOIS2**, qui demandaient «*la collecte régulière de données par le biais d'enquêtes et d'études afin d'éclairer une évaluation future de l'efficacité du RDS (WHOIS) pour répondre aux besoins des autorités d'application de la loi*» et la réalisation «*d'enquêtes et/ou d'études comparables avec d'autres utilisateurs du RDS (WHOIS) travaillant régulièrement avec les autorités d'application de la loi*», sont désormais **considérées comme «mises en œuvre dans la mesure du possible»** dans le cadre des travaux des étapes 2 et 2A de l'EPDP ainsi que de l'OPD du SSAD, conformément à la [documentation relative à la mise en œuvre](#) (11 octobre 2022)

⁸ Voir la [conférence téléphonique du PSWG](#) du 14 février 2023 [connexion requise au site Web du GAC]

- **Mesures et initiatives visant à atténuer l'utilisation malveillante du DNS par les opérateurs de registre et les bureaux d'enregistrement**
 - Le 27 mars 2020, l'organisation ICANN a [approuvé](#) la [proposition d'amendement du contrat de registre de .COM](#) qui **étend les dispositions contractuelles afin de faciliter la détection et la signalisation de cas d'utilisation malveillante du DNS aux trois quarts de l'espace de noms des gTLD**⁹. En outre, une [lettre d'intention](#) contraignante entre l'organisation ICANN et Verisign établit un cadre de coopération pour développer les meilleures pratiques et les nouvelles obligations contractuelles potentielles, ainsi que des mesures visant à mesurer et à atténuer les menaces à la sécurité du DNS.
 - **Dans le contexte de la crise du COVID-19, les parties contractantes et les parties prenantes de la sécurité publique** ont fait rapport¹⁰ sur leur collaboration pour 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 chargés de l'application de la loi et les bureaux d'enregistrement, et s'inspirent de la publication par le **Groupe des représentants des bureaux d'enregistrement** d'un [Guide des bureaux d'enregistrement pour le signalement de cas d'utilisation malveillante](#) lors 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 créé](#) (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 son [communiqué de l'ICANN70](#), le GAC salue la création de l'Institut de lutte contre l'utilisation malveillante du DNS et *«encourage les efforts de la communauté visant à s'attaquer ensemble à la lutte contre l'utilisation malveillante du DNS de manière holistique»*. Depuis, l'Institut de lutte contre l'utilisation malveillante du DNS a publié une [feuille de route](#) (14 juin 2021), discuté régulièrement des meilleures pratiques et a mis au point [une initiative visant à mesurer l'utilisation du DNS dans des activités de hameçonnage et de logiciel malveillant](#). Lors de l'ICANN74, l'Institut de lutte contre l'utilisation malveillante du DNS a été invité par le GAC à présenter son outil [Net Beacon](#) (anciennement connu sous le nom d'**Outil centralisé de signalement des cas d'utilisation malveillante**), outil qu'il développe en réponse au SAC115, à la recommandation 13.1 de la SSR2, et dans le respect de la recommandation 20 de la CCT-RT.

⁹ Ces dispositions incluent la [spécification 11 3b](#) qui n'était applicable, jusqu'à présent, qu'aux nouveaux gTLD. En mars 2022, .COM totalisait 161,3 millions d'enregistrements de noms de domaine, ce qui, si l'on exclut les 133,4 millions de domaines ccTLD parmi les 350,5 millions de domaines TLD, représente 74 % de l'ensemble des enregistrements de domaines gTLD (voir le [rapport de Verisign sur l'industrie des noms de domaine](#) de juin 2022).

¹⁰ Voir les présentations des parties contractantes [avant](#) et [pendant la réunion ICANN68](#) et [le document d'information du PSWG au GAC](#) dans le cadre de l'ICANN68.

- **Réponse multidimensionnelle de l'organisation ICANN¹¹ (qui fait désormais partie du programme d'atténuation des menaces à la sécurité du DNS) et mise en conformité contractuelle**
 - L'organisation ICANN [a présenté](#) (22 juillet 2021) son [programme d'atténuation des menaces à la sécurité du DNS](#) qui vise à fournir davantage de visibilité et de clarté aux divers projets et initiatives liés aux menaces à la sécurité du DNS et permet la définition 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 DNS¹².
 - 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)** pour aider à repérer les noms de domaine utilisés pour les abus liés au COVID-19 et pour pouvoir partager les données avec les parties pertinentes. Le GAC a pour la première fois [été informé](#) de cette question 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 DNS¹³. En octobre 2021, l'organisation ICANN et le Groupe des représentants des opérateurs de registre ont fait part de leur accord de principe visant¹⁴ à utiliser les données d'enregistrement détenues par les opérateurs de registre afin de fournir des informations liées aux bureaux d'enregistrement au DAAR, tel que [rapporté par le GAC](#) dans une lettre récemment transmise à l'ICANN (21 février 2022). Ces changements ont été inclus dans [la proposition de modifications aux RA et RAA de base des gTLD pour ajouter des obligations contractuelles liées au RDAP](#) (6 septembre 2022) que le GAC a accueillies favorablement dans ses [commentaires](#) (16 novembre 2022), et qui devraient faire

¹¹ Voir le billet de blog du PDG de l'ICANN du 20 avril 2020 détaillant la [réponse multidimensionnelle de l'organisation ICANN à l'utilisation malveillante du DNS](#)

¹² 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, et a notamment engagé une discussion sur la définition des menaces à la sécurité du DNS et de l'utilisation malveillante du DNS, les obligations des parties contractantes, et a fait le point sur le DAAR), le DNSTICR, la DFSI, la KINDNS, et les travaux de l'OCTO menés dans le domaine de la formation et du renforcement des capacités à travers le monde.

¹³ Plusieurs parties prenantes et initiatives de l'ICANN ont fait part des limites du DAAR, en particulier une [lettre](#) du M3AAWG transmise 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).

¹⁴ Voir la lettre du RySG transmise à l'ICANN (22 octobre 2021) et le billet de blog de l'ICANN (28 octobre 2021).

l'objet d'une période de vote de 60 jours avant leur examen par le Conseil d'administration de l'ICANN.

- 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 et améliorer ainsi le profil de sécurité du DNS». Son [rapport final](#) (15 octobre 2021) a été [publié](#) au terme de 18 mois de délibérations. L'organisation ICANN [a indiqué au GAC](#) (16 février 2022) qu'elle travaillait, en tenant compte de ce rapport, au développement d'un plan d'action. Le [processus de mise en œuvre](#) et une [page Wiki](#) permettant de suivre les progrès effectués ont été présentés à la communauté le 20 avril 2022. Lors de l'ICANN74, le GAC a discuté de l'utilité de donner la priorité à la recommandation E5 pour l'établissement d'une plateforme de partage d'informations sur les menaces et les incidents mise à la disposition des parties prenantes concernées au sein de la communauté de l'ICANN¹⁵.
- Pour ce qui est de la **mise en conformité contractuelle**, dans son [billet de blog](#) (20 avril 2020), le PDG de l'ICANN a rappelé ce qui suit : *«Le département de l'ICANN chargé de la conformité contractuelle veille au respect des obligations contractuelles prévues dans les politiques et les contrats de l'ICANN, en particulier le contrat de registre (RA) et le contrat d'accréditation de bureau d'enregistrement (RAA). Ce département collabore aussi étroitement avec l'OCTO à l'identification des menaces à la sécurité du DNS [...] et à la mise en correspondance de ces menaces avec les parties contractantes concernées. Le département de l'ICANN chargé de la conformité contractuelle 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 DNS. En dehors de ces audits, le département de l'ICANN chargé de la conformité contractuelle utilisera les données collectées par l'OCTO et d'autres pour contacter de manière proactive les registres et bureaux d'enregistrement coupables d'un nombre disproportionné de menaces à la sécurité du DNS. En cas d'impossibilité de mener un dialogue constructif, le département de l'ICANN chargé de la conformité contractuelle 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».*
 - À la suite d'un précédent **audit de conformité contractuelle** des opérateurs de registre axé sur l'utilisation malveillante de l'infrastructure du DNS qui s'est

¹⁵ Recommandation E5 *Intervention en cas d'incident* du [rapport final DSFI-TSG](#) (13 octobre 2021) : «L'organisation ICANN doit, avec les parties concernées, encourager le développement et le déploiement d'un processus formel d'intervention en cas d'incident au sein de l'industrie du DNS permettant des échanges avec d'autres entités de l'écosystème. Une telle initiative doit comprendre la gestion de l'intervention en cas d'incident ainsi que le partage protégé d'informations relatives aux menaces et aux incidents.»

achevé en juin 2019¹⁶, l'ICANN [a présenté](#) (24 août 2021) les résultats de l'audit sur **la conformité des bureaux d'enregistrement aux obligations en matière d'atténuation de l'utilisation malveillante du DNS** : 126 bureaux d'enregistrement audités (gérant plus de 90 % de tous les domaines enregistrés dans les gTLD); 111 bureaux d'enregistrement ne respectant pas entièrement les exigences relatives à la réception et au traitement des rapports d'utilisation malveillante du DNS (articles 3.18.1 - 3.18.3 du RAA); et 92 bureaux d'enregistrement ayant pris des mesures pour se conformer entièrement aux exigences.

- Le 9 mars 2022, l'ICANN [a annoncé](#) son déploiement de nouveaux mécanismes de compte rendu renforçant la visibilité des volumes de plaintes et des tendances en la matière.
- **Une nouvelle série d'audits portera sur 28 opérateurs de registre gTLD¹⁷** exploitant des gTLD, qui n'ont pas précédemment fait l'objet d'un audit complet et qui présentent des niveaux d'utilisation malveillante parmi les plus élevés, comme indiqué par les listes de blocage de réputation mises à la disposition du public (à l'exclusion des courriers indésirables), a été [annoncée](#) le 13 avril 2022 et s'est conclue avec la publication d'un [rapport d'audit](#) le 16 septembre 2022. Le GAC a discuté des résultats lors de sa séance plénière sur l'utilisation malveillante du DNS au cours de l'ICANN75 (20 septembre 2022).
- Dans le cadre de la semaine de préparation à l'ICANN76, la [conformité contractuelle devrait rendre compte de ses activités à la communauté de l'ICANN](#) (28 février 2023).

¹⁶ Voir le billet de blog de l'ICANN «[Conformité contractuelle : Traiter les cas d'utilisation malveillante de l'infrastructure du système des noms de domaine \(DNS\)](#)» (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).

¹⁷ .africa .app .art .bar .best .blog .buzz .cat .cloud .club .com .coop .gift .icu .ink .istanbul .moe .one .ooo .org .ren .ryukyu .tel .tirol .xin 我爱你 (Xn--6qq986b3xl) .닷컴 (Xn--mk1bu44c) .Pyc (Xn--p1acf)

Principaux documents de référence

- [Rapport trimestriel sur les révisions spécifiques de l'ICANN du quatrième trimestre 2022](#) (21 février 2023)
- [Communication du RySG – RrSG sur les obligations de perturbation et d'atténuation de l'utilisation malveillante du DNS](#) (4 novembre 2022)
- [Rapport de la petite équipe de la GNSO au conseil de la GNSO sur l'utilisation malveillante du DNS](#) (7 octobre 2022)
- [Réponse du GAC à la demande de la GNSO visant à obtenir des retours de la communauté sur l'élaboration de politiques relatives à l'utilisation malveillante du DNS](#) (4 avril 2022)
- [The Last Four years in Retrospect: Bref examen de l'utilisation malveillante du DNS](#) élaboré par l'organisation ICANN (22 mars 2022)
- [Étude sur l'utilisation malveillante du DNS](#) de la Commission européenne et son [annexe technique](#) (31 janvier 2022)
- [Rapport final](#) de la révision de la SSR2 (25 janvier 2021) et [commentaires du GAC](#) y afférents (22 juillet 2021)
- [Annonce](#) de l'ICANN et [rapport](#) (24 août 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.
- Le [rapport SAC115](#) (19 mars 2021) du SSAC, qui propose une approche interopérable pour la gestion de l'utilisation malveillante du DNS

Gestion des documents

Titre	Document d'information du GAC pour l'ICANN76 - Utilisation malveillante du DNS
Distribution	Membres du GAC (avant la réunion) et public en général (après la réunion)
Date de distribution	Version 1 : 1er mars 2023