

Atténuation de l'utilisation malveillante du DNS

Séance 6

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. 10
------------------------	-----	--	------	-------------------------------------	------	-----------------------------------	-------

Objectifs de la séance

Cette séance a pour but de poursuivre l'examen par le GAC des initiatives de l'organisation ICANN et de la communauté de l'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

- 1. Examiner les progrès des activités de l'organisation ICANN** liées à l'utilisation malveillante du DNS dans le cadre de ses programmes d'atténuation des menaces à la sécurité du DNS (par exemple DAAR, DNSTICR et renforcement des capacités/formation) et de conformité contractuelle, notamment les récentes mises à jour faites au GAC lors de l'appel du Groupe d'interaction Conseil d'administration-GAC (31 août) et la très attendue séance d'information pré-ICANN75 de l'organisation ICANN à destination du GAC¹.
- 2. Évaluer les progrès des discussions et travaux de mise en œuvre de la communauté de l'ICANN** liés à l'utilisation malveillante du DNS, dont les délibérations du petit Groupe de la GNSO sur l'utilisation malveillante du DNS qui a récemment indiqué qu'il se préparait à publier un rapport préliminaire aux alentours de l'« ICANN75 ² ».

¹ Voir <https://gac.icann.org/sessions/boardgac-interaction-group-bgig-call-31-august-2022> (31 août 2022) et <https://gac.icann.org/sessions/icann-org-preicann75-oral-briefing-to-the-gac> (6 septembre 2022) [connexion requise]

² Voir le [procès-verbal préliminaire](#) de la réunion du Conseil de la GNSO du 25 août 2022.

Situation actuelle et faits récents

- Depuis l'ICANN66, les dirigeants du Groupe de travail sur la sécurité publique du GAC ont renseigné le GAC sur la question de l'utilisation malveillante du DNS³, conformément au [plan de travail 2020-2021 du PSWG](#) et à son objectif stratégique n° 1 consistant à renforcer les capacités d'atténuation de l'utilisation malveillante du DNS et de la cybercriminalité.
 - Le GAC a examiné les **mesures mises à la disposition des opérateurs de registre et des bureaux d'enregistrement pour 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 donné⁴.
 - Le GAC a également été informé des **initiatives en cours et éventuelles initiatives permettant de traiter plus efficacement l'utilisation malveillante du DNS au niveau du Conseil d'administration de l'ICANN et de l'organisation ICANN**, notamment les révisions des contrats de l'ICANN conclus avec les opérateurs de registre et les bureaux d'enregistrement, l'application des exigences actuelles, la mise en œuvre des recommandations pertinentes issues de la révision de la CCT et de la SSR2 et des recommandations politiques 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 des cas d'utilisation malveillante de noms de domaine.
 - Dans le [communiqué de l'ICANN72](#) (1er novembre 2021), le GAC soulignait également **« la nécessité d'améliorer les conditions contractuelles pour traiter plus efficacement la question de l'utilisation malveillante du DNS. À cet égard, le rôle de l'ICANN dans le cadre des statuts constitutifs comprend la prise en compte des préoccupations de politique publique des gouvernements et des autorités publiques et le fait d'agir au bénéfice du public. Les statuts constitutifs autorisent également l'ICANN à négocier des accords, y compris des engagements d'intérêt public, au service de sa mission. Par conséquent, l'ICANN est particulièrement bien placée pour négocier des améliorations aux contrats existants afin de réduire plus efficacement l'utilisation malveillante du DNS, comme l'avaient mis en avant le GAC et d'autres parties prenantes défendant l'intérêt public. »**
 - Lors de l'ICANN73, le GAC s'est penché sur une étude sur l'utilisation malveillante du DNS publiée par la Commission européenne (voir le [rapport](#) et son [annexe technique](#), 31 janvier 2022) et a indiqué dans le [communiqué du GAC de l'ICANN73](#) que cette étude : **« fournit un grand nombre d'études de cas utiles, clarifie les différents acteurs de l'écosystème de l'Internet, et donne des recommandations sur la réponse que peuvent**

³ Voir les documents de la séance plénière du GAC y afférente lors de l'[ICANN66](#), l'[ICANN68](#), l'[ICANN69](#), l'[ICANN70](#), l'[ICANN71](#), l'[ICANN72](#), l'[ICANN73](#) et l'[ICANN74](#).

⁴ Voir notamment la discussion sur les mesures préventives mises à la disposition des opérateurs de registre et des bureaux d'enregistrement tenue lors de l'[ICANN66](#) et les enseignements tirés de la mise en œuvre de la vérification d'identité dans le ccTLD .DK lors de l'[ICANN69](#).

apporter les différents acteurs (par exemple les opérateurs de registre, bureaux d'enregistrement, revendeurs, fournisseurs d'hébergement, titulaires de noms de domaine, etc.) aux cas d'utilisation malveillante du DNS qui surviennent au sein des différentes couches du système du DNS ». Et ce même communiqué de préciser que « toutes les activités nuisibles ou illégales couvertes par l'étude ne relèvent pas de la mission de l'ICANN », tout en notant que le GAC pourrait demeurer une « importante tribune permettant aux gouvernements » de poursuivre leurs discussions sur l'utilisation malveillante du DNS.

- Lors de l'ICANN74, le GAC a débattu du rapport de l'ICANN intitulé [The Last Four years in Retrospect: A brief Review of DNS Abuse Trends](#) (Rétrospective des quatre dernières années : bref examen des tendances en matière d'utilisation malveillante du DNS) (22 mars 2022). Il a été constaté qu'il était trop tôt pour tirer des conclusions sur les tendances émergentes à ce stade au vu des difficultés à dégager les tendances actuelles concernant les menaces les plus sérieuses telles que la diffusion de programmes malveillants, l'hameçonnage et les réseaux zombies. A été mise en avant l'importance de compléter ces considérations par un examen des préjudices économiques et humains causés par l'utilisation malveillante du DNS, dans le but de dresser un tableau global des tendances, de favoriser une meilleure compréhension des facteurs déterminants, et de mettre en place des mesures incitatives permettant de mener une action efficace dans le secteur. Dans le [communiqué de l'ICANN74 de La Haye](#) (20 juin 2022), le GAC a réclamé « une ventilation plus détaillée des types d'utilisation malveillante du DNS mesurés ; et la mise à disposition de données brutes agrégées ».
- Lors de l'ICANN74, le GAC a invité l'Institut de lutte contre l'utilisation malveillante du DNS à présenter son [nouvel 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.
- Dans le [communiqué de l'ICANN74 de La Haye](#) (20 juin 2022), le GAC a déclaré que « **tout PDP sur l'utilisation malveillante du DNS doit être adapté précisément afin d'obtenir des résultats exploitables en temps opportun** », ce à quoi le Conseil d'administration de l'ICANN a répondu⁵ qu'il partageait cet avis et qu'il était prêt à soutenir la communauté de l'ICANN dans cette quête.
- **Le petit Groupe de la GNSO sur l'utilisation malveillante du DNS [devrait](#)** communiquer « aux alentours » de l'ICANN75 ses conclusions concernant « *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* ».

⁵ Voir <https://gac.icann.org/sessions/boardgac-interaction-group-bgig-call-31-august-2022> (31 août 2022) [connexion requise]

- Le 31 janvier 2022, le Conseil de la GNSO a [annoncé](#) la formation de ce **petit Groupe de la GNSO** dont la mission consiste à « *venir en aide aux entités de la communauté qui se sont fait entendre sur ce sujet (telles que le Comité consultatif gouvernemental [...]) de sorte à mieux comprendre leurs attentes vis-à-vis de la GNSO et si/comment elles souhaiteraient que d'autres travaux politiques soient menés afin de contribuer (ou pas) aux initiatives déjà en cours* ».
- Dans la [réponse du GAC](#) (4 avril 2022) 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, le président du GAC a rappelé l'importance de cette « *question présentant depuis longtemps un intérêt pour le GAC* » et l'intérêt du GAC « *à faire avancer les discussions de la communauté, à favoriser la réalisation de progrès et la convergence des points de vue avant le lancement des futurs nouveaux gTLD* ». Étant donné que les « *travaux actuellement menés par la communauté peuvent générer des initiatives et résultats bénéfiques qui permettraient d'éviter un PDP* », la lettre indiquait ce qui suit : « *À ce stade [...] effectuer un exercice de cadrage d'un PDP pourrait s'avérer prématuré* ». D'autres réponses communautaires de l'ALAC, du SSAC, de la BC, du RySG et de l'Institut de lutte contre l'utilisation malveillante du DNS sont disponibles dans la section « *Prochaines étapes en matière d'utilisation malveillante du DNS* » sur l'[espace de travail des petites équipes de la GNSO](#).
- **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 gTLD⁶**. 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 rendu compte⁷ de leur collaboration afin de faciliter les rapports, leur révision et leur renvoi à la juridiction compétente via 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](#)

⁶ 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)

⁷ Voir les présentations des parties contractantes [avant](#) et [pendant l'ICANN68](#) et [le document d'information du PSWG transmis au GAC](#) lors de l'ICANN68.

[d'utilisation malveillante](#) lors de l'ICANN67. Ce guide a été [mis à jour](#) (janvier 2022) et approuvé par le **Groupe des représentants des bureaux d'enregistrement**.

- 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 le [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* ».
- L'Institut de lutte contre l'utilisation malveillante du DNS a depuis [publié](#) une [feuille de route](#) (14 juin 2021), discuté de [l'atténuation des préjudices au sein des différentes couches de l'infrastructure de l'Internet](#) (24 août 2021) et a élaboré un document regroupant les [meilleures pratiques relatives à l'identification des enregistrements malveillants](#) (2 décembre 2021). Lors de l'ICANN74, l'Institut de lutte contre l'utilisation malveillante du DNS a été invité à présenter son [nouvel 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.

- **Réponse multidimensionnelle de l'organisation ICANN⁸ (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. Il est engagé dans des forums de veille en matière de cybermenaces et de réponse aux incidents, et développe des systèmes et des outils pour aider à identifier, analyser et signaler l'utilisation malveillante du DNS⁹.
 - En réponse à la crise du COVID-19, l'OCTO a développé l'outil de **signalement et de collecte d'informations sur les menaces à la sécurité des noms de domaine**

⁸ Le PDG 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](#).

⁹ 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 liées à l'utilisation malveillante du DNS de l'OCTO, 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, le système de signalement des cas d'utilisation malveillante des noms de domaine (DAAR), l'outil de signalement et de collecte d'informations sur les menaces à la sécurité des noms de domaine (DNSTICR), la nouvelle initiative « Normes relatives au partage des connaissances et à l'instanciation pour la sécurité du DNS et du nommage » (KINDNS), et une révision des travaux de l'OCTO menés dans le domaine de la formation et du renforcement des capacités à travers le monde.

(DNSTICR) pour aider à identifier les noms de domaine liés au COVID-19 et utilisés à des fins d'abus et pour pouvoir partager les données avec les parties concernées. 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 DNS¹⁰. En octobre 2021, l'organisation ICANN et le Groupe des représentants des opérateurs de registre ont fait part de leur accord de principe visant¹¹ 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). Le Conseil d'administration de l'ICANN a confirmé que cela serait reflété dans les modifications contractuelles qui devraient être publiées avant ou peu après l'ICANN75¹². Le [rapport sur le DAAR de juillet 2022](#) de l'organisation ICANN indiquait ce qui suit : « *pour pouvoir rendre compte des portefeuilles des bureaux d'enregistrement, les données d'enregistrement de noms de domaine doivent être en mesure d'identifier quels domaines sont parrainés par quels bureaux d'enregistrement. Le développement d'un système capable de collecter et d'analyser quotidiennement les données des bureaux d'enregistrement nécessaires est encore en cours. Nous espérons pouvoir fournir des informations sur les bureaux d'enregistrement dans de futurs rapports* ».
- 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](#) à l'issue 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

¹⁰ 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 directeur de la technologie de l'ICANN (9 septembre 2020).

¹¹ Voir la lettre du RySG transmise à l'ICANN (22 octobre 2021) et le billet de blog de l'ICANN (28 octobre 2021).

¹² Voir <https://gac.icann.org/sessions/boardgac-interaction-group-bgig-call-31-august-2022> (31 août 2022) [connexion requise]

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'ICANN¹³.

- 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 les 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 achevé en juin 2019¹⁴, 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 satisfaisant pas entièrement aux exigences relatives à la réception et au traitement du signalement de cas d'utilisation malveillante du DNS (sections 3.18.1 à 3.18.3 du RAA)
 - 92 bureaux d'enregistrement ont pris des mesures pour se mettre pleinement en conformité et 19 mettent en œuvre des changements
 - **Une nouvelle série d'audits pour des opérateurs de registre sélectionnés** a été [annoncée](#) le 13 avril 2022. Elle concernera 28 opérateurs de registre gTLD 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, tel

¹³ 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. »

¹⁴ 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).

qu'indiqué par les listes de blocage de réputation mises à la disposition du public (à l'exclusion des courriers indésirables). Cette série devrait être menée avant le troisième trimestre 2022.

- Lors de la [séance d'information pré-ICANN73 du PDG de l'ICANN à destination du GAC](#) (16 février 2022), le département de l'ICANN chargé de la conformité contractuelle a examiné les obligations en matière d'atténuation de l'utilisation malveillante du DNS prévues dans les contrats de l'ICANN et a présenté les résultats, obtenus à partir d'un échantillon de 3378 plaintes, eu égard au traitement du signalement de cas d'utilisation malveillante par des bureaux d'enregistrement : 456 enquêtes de conformité et 1 avis de non-conformité.
- 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.
- Dans le cadre de la semaine de préparation à l'ICANN75, le [département chargé de la conformité contractuelle devrait mettre à jour la communauté](#) (6 septembre 2022) sur les faits récents et, éventuellement, sur les progrès réalisés lors de sa dernière série d'audits susmentionnée.

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, y compris celles portant sur l'amélioration du système de signalement des cas d'utilisation malveillante des noms de domaine (DAAR) et le renforcement des mécanismes de conformité.
- Le [rapport final](#) (25 janvier 2021) a été examiné par le GAC lors de l'ICANN70 en vue de la soumission finale des [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 mesures](#) (22 juillet 2021) concernant les 63 recommandations finales de l'équipe de révision (25 janvier 2021). Un [billet de blog](#) a résumé les mesures prises :
 - 13 recommandations ont été approuvées (en attente de la planification de leur mise en œuvre),
 - 16 recommandations ont été rejetées (y compris 6 qui n'ont pas pu être entièrement approuvées),
 - 34 recommandations sont en attente d'informations et d'analyses complémentaires.

- Dans le [communiqué de l'ICANN72](#) (1er novembre 2021), le GAC a conseillé au Conseil d'administration de l'ICANN de :
 - *Implanter en priorité les mesures de suivi nécessaires pour appuyer la mise en œuvre rapide de la fiche de suivi du Conseil d'administration [...]*
 - *Fournir de plus amples renseignements sur l'interprétation divergente du Conseil d'administration et de l'équipe de révision de la SSR2 sur le niveau de mise en œuvre de certaines recommandations.*
- Le Conseil d'administration de l'ICANN a fourni des informations complémentaires dans sa [réponse](#) au communiqué de l'ICANN72 (16 janvier 2022). Cette réponse a fait l'objet de nouvelles discussions entre le GAC et le Conseil d'administration de l'ICANN73¹⁵ et de communications ultérieures transmises par l'organisation ICANN au GAC dans une [lettre](#) (18 mars 2022) et un [e-mail de suivi](#) (12 avril 2022).
- **L'équipe de travail consacrée à l'utilisation malveillante du DNS du Comité consultatif sur la sécurité et la stabilité (SSAC)** a publié son rapport [SAC115](#) (19 mars 2021) qui propose une approche interopérable pour la gestion de l'utilisation malveillante du DNS.
 - 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 de coordonnées 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 de réponse commune aux abus »** prenant la forme d'une organisation non gouvernementale à but non lucratif pleinement indépendante qui ferait office de facilitateur pour l'ensemble de l'écosystème du DNS, y 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.
 - Tel qu'indiqué précédemment, l'Institut de lutte contre l'utilisation malveillante du DNS a pris des mesures, depuis la publication du rapport SAC115, visant à créer une plateforme commune de signalement des cas d'utilisation malveillante, l'[outil de signalement Net Beacon](#) (juin 2022). Les fonctionnalités de Net Beacon ont été présentées au GAC par l'Institut de lutte contre l'utilisation malveillante du DNS lors de l'ICANN74.

¹⁵Voir la p. 13 du [procès-verbal du GAC de l'ICANN73](#).

Principaux documents de référence

- [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: A Brief Review of DNS Abuse](#) (Rétrospective des quatre dernières années : bref examen des tendances en matière d'utilisation malveillante du DNS) (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 [fiche de suivi des mesures prises par le Conseil d'administration](#) (22 juillet 2021)
- [Annonce](#) et [rapport](#) de l'ICANN (24 août 2021) sur l'audit relatif à la conformité des bureaux d'enregistrement aux obligations en matière d'atténuation de l'utilisation malveillante du DNS.
- Le [rapport SAC115](#) (19 mars 2021) du SSAC, qui propose une approche interopérable pour 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	Document d'information du GAC sur l'ICANN75 - Utilisation malveillante du DNS
Distribution	Membres du GAC (avant la réunion) et public (après la réunion)
Date de distribution	Version 1 : 2 septembre 2022