

Atténuation de l'utilisation malveillante du DNS

Séance 10

Sommaire

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 objectif de poursuivre l'examen, par le GAC, des initiatives lancées par l'organisation ICANN et la communauté de l'ICANN pour prévenir et atténuer l'utilisation malveillante du DNS, notamment les résultats et les prochaines étapes concernant les améliorations aux dispositions contractuelles, proposées et discutées au cours de l'ICANN77, et au sujet desquelles le GAC a formulé des commentaires publics. En outre, le Comité permanent de la ccNSO sur l'utilisation malveillante du DNS fournira également une mise à jour sur ses efforts visant à mieux comprendre et à soutenir les pratiques d'atténuation de l'utilisation malveillante dans les ccTLD.

Proposition des dirigeants pour la ligne d'action du GAC

- Réfléchir aux prochaines étapes, à la lumière de la procédure de consultation publique sur les modifications proposées aux contrats des registres et des bureaux d'enregistrement concernant l'utilisation malveillante du DNS.** Cette consultation a reçu 36 contributions, dont des [commentaires du GAC](#) (17 juillet 2023).

Dans son [Compte rendu sommaire des commentaires publics](#) (1er août 2023), l'ICANN a indiqué que **le vote des registres et des bureaux d'enregistrement se poursuivrait sur les modifications initialement proposées**. Quant aux « *commentaires signalant que les modifications proposées ne suffisent pas pour relever le défi de l'utilisation malveillante du DNS* », elle a fait observer que « *l'organisation ICANN prend acte de ces commentaires et rappelle à la communauté que celle-ci aura l'occasion de discuter de ces obligations pour déterminer si d'autres sont nécessaires [...]. L'organisation ICANN et l'équipe de négociation de la Chambre des parties contractantes (CPH NT) soutiennent les commentaires du GAC* ».

selon lesquels, après l'adoption des modifications proposées, le travail devrait inclure des processus d'élaboration de politiques (PDP) pour informer davantage le RA de base et le RAA mis à jour ».

2. Assurer un suivi avec le Conseil d'administration de l'ICANN au sujet de la proposition du GAC de l'ICANN76 sur l'organisation d'une séance d'écoute de la communauté en vue de l'élaboration éventuelle d'une politique à la suite de la période de vote actuelle sur les modifications contractuelles¹.

3. Débattre de l'étendue de l'élaboration souhaitée d'une politique visant à améliorer la prévention et l'atténuation de l'utilisation malveillante du DNS, en tenant compte des éléments suivants :

- la déclaration du GAC figurant dans ses [commentaires](#) (17 juillet 2023) sur les modifications proposées, spécifiant que *« les futurs travaux sur l'utilisation malveillante du DNS menés avec la communauté multipartite [...] devraient inclure des processus d'élaboration de politiques (PDP) visant à mieux informer les RA et RAA mis à jour, ainsi que d'autres travaux sur les questions en suspens à traiter en amont de la prochaine série de candidatures pour les nouveaux gTLD »* ;
- **les recommandations des équipes de révision de la CCT et de la SSR2**, sur lesquelles le GAC a déjà formulé des commentaires², notamment :
 - la discussion entre le GAC et le Conseil d'administration de l'ICANN, faisant suite à l'avis formulé dans le [communiqué de Montréal du GAC](#) (6 nov. 2019)³, sur le suivi possible de la substance des recommandations de la révision de la CCT (et non des recommandations spécifiques elles-mêmes) ;
 - Dans son [communiqué de l'ICANN72](#) (1er novembre 2021), le GAC s'est dit conscient *« des bases procédurales du rejet par le Conseil d'administration »* de certaines recommandations de la révision SSR2, **tout en soulignant « l'utilité des aspects substantiels de certaines recommandations rejetées, notamment celles visant à fournir à l'organisation ICANN et au service de la conformité contractuelle de celle-ci des outils appropriés pour prévenir et atténuer l'utilisation malveillante du DNS »** ;

¹ Voir p.11 des [procès-verbaux des réunions du GAC de l'ICANN76](#)

² Voir les détails dans cette note d'information p. 8-9

³ Dans son communiqué de Montréal (6 novembre 2019), le GAC avait recommandé au Conseil d'administration de l'ICANN de « ne pas procéder à une nouvelle série de gTLD jusqu'à la mise en œuvre complète des recommandations [...] déterminées comme des « conditions préalables » ou « hautement prioritaires ». Cet avis a fait l'objet d'une correspondance avec le Conseil d'administration de l'ICANN, ainsi que d'un suivi dans les communiqués de l'ICANN70 et de l'ICANN71, de réponses du Conseil d'administration de l'ICANN et d'un accord final lors d'un appel du BGIG (5 octobre 2021) [Connexion au site Web du GAC requise], selon lequel « le GAC envisagerait un suivi sur la substance des recommandations de la révision de la CCT et non sur les recommandations spécifiques elles-mêmes »

- la recommandation de la [petite équipe de la GNSO sur l'utilisation malveillante du DNS](#) (7 octobre 2022) **d'engager un processus d'élaboration de politique sur les enregistrements malveillants**, et les négociations contractuelles potentielles sur cette question, qui devraient finalement être guidées par les résultats du projet INFERMAL (Inferential Analysis of Maliciously Registered Domains), afin d'explorer les principaux facteurs qui motivent l'enregistrement malveillant de noms de domaine⁴.

4. Assurer un suivi des contributions antérieures du GAC⁵ concernant l'inclusion de données sur les bureaux d'enregistrement dans le signalement des cas d'utilisation malveillante des noms de domaine (DAAR) de l'ICANN, comme envisagé dans les modifications au contrat de registre récemment [approuvées par le Conseil d'administration de l'ICANN](#) (30 avril 2023), qui prendront effet le 3 février 2024.

⁴ Voir le blog de l'OCTO de l'ICANN « [Un nouveau projet de l'ICANN explore les ressorts des enregistrements malveillants de noms de domaine](#) » du 25 avril 2023

⁵ Voir la section IV.1 du [Communiqué de l'ICANN72](#) (1er novembre 2021), la [lettre du président du GAC au CTO de l'ICANN](#) (21 février 2022) sur l'accord visant à étendre la collecte de données pour permettre le signalement des activités d'utilisation malveillante du DNS au niveau des bureaux d'enregistrement dans le DAAR et le [commentaire du GAC](#) (16 nov. 2022) sur la proposition ultérieure de modifications au contrat.

Situation actuelle et faits récents

- **Proposition de modifications aux contrats des registres et des bureaux d'enregistrement visant à renforcer les obligations en matière d'atténuation de 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 DNS⁶, 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'application⁷ » des contrats actuels de l'ICANN**, comme le reflètent ensuite ses [recommandations au conseil de la GNSO](#) (7 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** », dont celles recensées par la SSR2 et par la révision de la CCT ».

⁶ Voir les documents des plénières du GAC de l'[ICANN66](#), l'[ICANN68](#), l'[ICANN69](#), l'[ICANN70](#), l'[ICANN71](#), l'[ICANN72](#), l'[ICANN73](#) and l'[ICANN74](#).

⁷ [Communiqué du GAC de l'ICANN70](#), section IV.1 p. 5

- 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 [article de 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* ».

- Entre-temps, l'Unité constitutive des utilisateurs commerciaux (**BC**), l'Unité constitutive des représentants de la propriété intellectuelle (**IPC**) de la GNSO et le Comité consultatif At-Large (**ALAC**) ont [demandé](#) (20 janvier 2023) que « *les contributions de la communauté soient dûment prises en compte, et de soutenir l'organisation ICANN dans son rôle établi de défenseur des besoins de la communauté et d'arbitre de l'intérêt public* ». Dans sa [réponse](#) (27 mars 2023), le Conseil d'administration de l'ICANN a affirmé que « *le Conseil d'administration de l'ICANN et l'organisation ICANN ont été à l'écoute de la communauté, ces dernières années, en ce qui concerne l'utilisation malveillante du DNS. L'adoption de **cette approche visant à apporter des améliorations ciblées aux contrats, introduisant une obligation explicite pour les opérateurs de registre et bureaux d'enregistrement d'atténuer l'utilisation malveillante du DNS, sera une composante d'un parcours plus long qui envisage des discussions potentielles sur les politiques, ouvertes à toute la communauté de l'ICANN, et possiblement des négociations futures entre le CPH et l'organisation ICANN*** ».

- Lors d'une [séance d'information pré-ICANN76 du GAC sur les négociations contractuelles 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 par les révisions 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.**

- Lors de la réunion bilatérale du GAC avec le Conseil d'administration de l'ICANN pendant l'ICANN76, **le GAC a encouragé ce dernier à envisager l'organisation d'une séance d'écoute de la communauté de l'ICANN** concernant les négociations (voir p.11 du [procès-verbal de la réunion du GAC de l'ICANN76](#)).
- Dans son [communiqué de Cancún](#) lors de l'ICANN76 (20 mars 2023), le GAC a encouragé les négociations en cours « *à progresser rapidement* », soulignant qu'il « *estime que des efforts continus dans ce domaine seront nécessaires avant le lancement d'une deuxième série de nouveaux domaines génériques de premier niveau (nouveaux gTLD), notamment des améliorations supplémentaires aux obligations contractuelles et/ou des processus ciblés d'élaboration de politiques* ». En outre, le GAC a recommandé aux « *parties contractantes et à l'ICANN d'envisager, entre autres, des mesures proactives ainsi que des incitations positives pour les opérateurs de registre et les bureaux d'enregistrement, dans le cadre de futurs travaux sur l'atténuation ou la perturbation de l'utilisation malveillante du DNS* ».
- En préparation de l'ICANN77, le **Groupe de travail du GAC chargé des régions faiblement desservies** (USRWG) a organisé deux **séminaires Web** pour préparer les nouveaux arrivants et les représentants du GAC des régions faiblement desservies à contribuer à un commentaire sur les modifications attendues aux contrats de registre et de bureau d'enregistrement⁸.
- **L'organisation ICANN a lancé une procédure de consultation publique** sur les [modifications au RA et au RAA de base des gTLD. Ces modifications, qui visent à renforcer les obligations contractuelles relatives à l'utilisation malveillante du DNS](#) (29 mai 2023), ont ensuite été présentées lors d'un [séminaire Web organisé à l'occasion de la semaine de préparation à l'ICANN77](#) (30 mai 2023). Les diverses modifications proposées aux contrats de l'ICANN comprennent une **nouvelle obligation pour les parties contractantes de prendre rapidement des mesures d'atténuation appropriées à l'encontre des domaines pour lesquels elles disposent de preuves concrètes d'utilisation malveillante du DNS**. Outre les [modifications contractuelles proposées](#), une [version provisoire d'un avis de l'ICANN](#) fournit une explication détaillée sur ces nouvelles dispositions et définit les attentes quant à leur interprétation.
- À la suite des discussions qu'il a tenues au cours de l'ICANN77 sur les modifications proposées⁹, le GAC a formulé des [commentaires](#) (17 juillet 2023) dans le cadre de la procédure de consultation publique :
 - le GAC a jugé ces modifications « *opportunes et pertinentes* » et a estimé qu'« *elles représenteront, une fois adoptées, un premier pas important dans la lutte contre l'utilisation malveillante du DNS* » ;
 - le GAC a souligné que « *compte tenu de la menace permanente pour les consommateurs et les secteurs public et privé qu'est l'utilisation malveillante du*

⁸ Voir le [séminaire Web de développement des capacités du GAC pré-ICANN77 sur l'utilisation malveillante du DNS n° 1](#) (4 mai 2023) et le [séminaire Web n° 2](#) (22 mai 2023).

⁹ Voir [l'atelier de développement des capacités du GAC de l'ICANN77 sur l'utilisation malveillante du DNS](#) (dimanche 11 juin) et [la discussion du GAC sur l'utilisation malveillante du DNS](#) (mercredi 14 juin)

DNS », "il est impératif que les contrats améliorés soient rapidement adoptés après la clôture de la procédure de consultation publique » ;

- **le GAC a manifesté son soutien aux « modifications proposées de manière générale », mais a également invité « l'organisation ICANN et le CPH NT à se pencher sur certaines questions relatives au libellé des modifications ».** Il s'agit notamment de la définition de l'utilisation malveillante du DNS, des rapports et du suivi à effectuer par les parties contractantes, des conséquences en cas de non-respect, de la possibilité pour la communauté de l'ICANN de surveiller la mise en conformité, de la nécessité de mettre à jour périodiquement l'avis du Conseil d'administration et de l'importance de traiter l'utilisation malveillante du DNS tant au sein qu'à l'extérieur de l'ICANN ;
- **le GAC s'est dit enthousiaste à l'idée de « collaborer sur des travaux futurs sur l'utilisation malveillante du DNS avec la communauté des parties prenantes, après l'adoption des modifications. Ces travaux devraient inclure des processus d'élaboration de politiques (PDP) visant à mieux informer le RA et le RAA mis à jour, ainsi que d'autres activités ciblant les questions encore en suspens, à traiter en amont de la prochaine série de candidatures pour les nouveaux gTLD ».**
- Dans son [Compte rendu sommaire des commentaires publics](#) (1er août 2023), **l'organisation ICANN a indiqué que le vote des registres et des bureaux d'enregistrement continuerait sur les modifications, telles qu'elles ont été initialement proposées.** Quant aux « commentaires signalant que les modifications proposées ne suffisent pas pour relever le défi de l'utilisation malveillante du DNS », elle a fait observer que « l'organisation ICANN prend acte de ces commentaires et rappelle à la communauté que celle-ci aura l'occasion de discuter de ces obligations pour déterminer si d'autres sont nécessaires [...]. **L'organisation ICANN et l'équipe de négociation de la Chambre des parties contractantes (CPH NT) soutiennent les commentaires du GAC selon lesquels, après l'adoption des modifications proposées, le travail devrait inclure des processus d'élaboration de politiques (PDP) visant à mieux informer le RA de base et le RAA mis à jour ».**
- Le [vote des registres et des bureaux d'enregistrement](#) sur les modifications **a commencé le 9 octobre 2023 et se poursuivra pendant 60 jours** (jusqu'au 8 décembre 2023). Après la clôture de la période de vote, si les modifications sont adoptées, elles seront transmises au Conseil d'administration de l'ICANN pour examen. Si elles obtiennent l'approbation de celui-ci, elles prendront effet au terme d'un préavis de 60 jours notifié par l'ICANN. Celle-ci prévoit que « le travail devrait [alors] inclure des processus d'élaboration de politiques (PDP) visant à mieux informer le RA de base et le RAA mis à jour ». ¹⁰ Dans le cas où les modifications ne seraient pas approuvées, elles seraient retournées aux équipes de négociation pour que celles-ci discutent de prochaines étapes.

¹⁰ Voir la « Section 4 : analyse des commentaires formulés », à la page 9 du [Compte rendu sommaire des commentaires publics de l'ICANN](#) (1er août 2023).

- **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** ».
 - 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* », ajoutant 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 et visant à lutter contre l'utilisation malveillante du DNS* ».
 - 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 répondu¹¹ qu'il partageait cet avis et qu'il était prêt à soutenir la communauté de l'ICANN dans cette quête.
 - 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**

¹¹ Voir <https://gac.icann.org/sessions/boardgac-interaction-group-bgig-call-31-august-2022> (31 août 2022) [connexion requise au site Web du GAC]

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 ni ne suit 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 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* ».
- Sur la base d'autres contributions reçues des parties contractantes¹², **la petite équipe de la GNSO sur l'utilisation malveillante du DNS a conclu**, dans le cadre de ses [conclusions préliminaires sur les enregistrements de masse](#) (15 mai 2023), que **les enregistrements de masse « ne relèvent pas du domaine de la politique de consensus à l'heure actuelle »** dans la mesure où :
 - *Les plaintes relatives à des enregistrements uniques ou multiples sont traitées de manière uniforme, sans qu'il soit clair ce qui peut constituer des enregistrements de masse justifiant des réactions ciblées.*
 - *L'absence de définition claire n'a pas suscité de réponse claire.*
 - *D'autres outils de connaissance du client sont jugés plus efficaces pour détecter les utilisations malveillantes potentielles et devraient faire l'objet d'une plus grande attention.*
 - *Le projet [INFERMAL \(Inferential Analysis of Maliciously Registered Domains\)](#), récemment lancé par l'ICANN, semble indiquer une volonté de l'organisation de se*

¹² Voir les correspondances de la [Chambre des parties contractantes \(CPH\)](#), du [Groupe des représentants des opérateurs de registre \(RySG\)](#) et du [Groupe des représentants des bureaux d'enregistrement \(RrSG\)](#).

pencher sur cette question et de fournir [...] de meilleures statistiques et informations [sur ce sujet].

- **État et perspectives de mise en œuvre des recommandations des révisions spécifiques relatives à la perturbation de l'utilisation malveillante du DNS¹³**
 - **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). Par la suite, 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) ont demandé un suivi et des informations supplémentaires sur le degré de mise en œuvre de certaines recommandations. Le Conseil d'administration de l'ICANN y a [répondu](#) (16 janvier 2022), ce qui a conduit à d'autres discussions au cours de l'ICANN73¹⁴ et à des communications de l'organisation ICANN au GAC dans la forme d'une [lettre](#) (18 mars 2022) et d'un [courriel de suivi](#) (12 avril 2022).
 - 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.
 - Le [10 septembre 2023](#), le **Conseil d'administration de l'ICANN a rejeté**, sur la base d'une [évaluation menée par l'organisation ICANN](#), **7 recommandations en attente relatives à l'utilisation malveillante du DNS – 12.1** (*créer une équipe consultative pour l'analyse de l'utilisation malveillante du DNS*), **12.2** (*structurer des accords avec les fournisseurs de données pour permettre un plus grand partage des données*), **12.3** (*publier des rapports qui identifient les registres et bureaux d'enregistrement dont les domaines contribuent le plus à l'utilisation malveillante du DNS*), **12.4** (*faire rapport des mesures prises par les opérateurs de registre et bureaux d'enregistrement pour répondre aux plaintes de conduite illégale et/ou malveillante*), **13.1** (*établir un 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*).
 - **Dans sa discussion sur les négociations contractuelles concernant l'utilisation malveillante du DNS, le PSWG du GAC a discuté¹⁵ 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*

¹³ Le statut de toutes les recommandations peut être consulté dans les rapports trimestriels de l'ICANN et sur la page d'accueil de chaque révision, accessibles à partir de la page <https://www.icann.org/resources/reviews/specific-reviews>.

¹⁴ Voir le [procès-verbal du GAC de l'ICANN73](#) p.13.

¹⁵ Voir la [conférence téléphonique du PSWG](#) du 14 février 2023 [*connexion requise au site Web du GAC*]

de négociation qui comprend des spécialistes en utilisation malveillante et en sécurité pour renégocier les contrats des parties contractantes), **9.4** (établir des 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, dans son [communiqué de l'ICANN72](#) (1er novembre 2021), **s'est dit conscient** « des bases procédurales du rejet par le Conseil d'administration », tout **en soulignant**, néanmoins, « **l'utilité des aspects substantiels de certaines recommandations rejetées, notamment celles visant à fournir à l'organisation ICANN et au service de la conformité contractuelle de celle-ci des outils appropriés pour prévenir et atténuer l'utilisation malveillante du DNS** ».

- 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), comme il l'a 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 [...] ayant été recensées comme des "conditions préalables" [14 recommandations] ou comme des "priorités élevées" [10 recommandations]** ».

À la suite de discussions liées aux communiqués de l'ICANN70 et de l'ICANN71¹⁶, le GAC et le Conseil d'administration de l'ICANN sont parvenus à un accord, exprimé lors d'un [appel du BGIG](#) (5 octobre 2021) [*connexion requise au site Web du GAC*] et selon lequel « le GAC envisagerait un suivi sur la substance des recommandations de la révision du CCT et non sur les recommandations spécifiques elles-mêmes ».

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 GAC¹⁷ :

- 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 des mécanismes de signalement et de traitement des

¹⁶ Voir les discussions de clarification du communiqué, ainsi que les réponses du Conseil d'administration au suivi du GAC sur les avis antérieurs des communiqués de l'ICANN70 et de l'ICANN71 : [appel de clarification](#) de l'ICANN70 (21 avril 2021), [réponse du Conseil d'administration](#) (12 mai 2021), [appel de clarification](#) de l'ICANN71 (29 juillet 2021) et [réponse du Conseil d'administration](#) (12 septembre 2021).

¹⁷ Voir la [conférence téléphonique du PSWG](#) du 14 février 2023 [*connexion requise au site Web du GAC*].

plaintes et éventuellement envisager de modifier les futurs contrats de registre standard pour exiger que les opérateurs de registre révèlent 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 Conseil d'administration du 22 octobre 2020](#), et leur mise en œuvre, qui est en cours, devrait être achevée entre le T2 et le T3 2024 selon le [rapport trimestriel sur les révisions spécifiques de l'ICANN du premier trimestre 2023](#) (31 mars 2023).

- La **recommandation 14** (*inciter à l'adoption de mesures proactives contre l'utilisation malveillante du DNS*) et la **recommandation 15** (*négoier des modifications pour inclure des dispositions visant à prévenir l'utilisation systématique de certains bureaux d'enregistrement ou registres pour les abus de sécurité du DNS, et établir des seuils d'utilisation malveillante qui déclenchent automatiquement la conformité*) **viennent d'être rejetées par le Conseil d'administration de l'ICANN** dans une [résolution](#) récente (10 septembre 2023).

- 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).

- **Mesures et initiatives visant à atténuer l'utilisation malveillante du DNS par les opérateurs de registre et bureaux d'enregistrement**

- Le 27 mars 2020, l'organisation ICANN a [approuvé](#) la [proposition de modification au contrat de registre de .COM](#), qui étend les dispositions contractuelles afin de faciliter la détection et le signalement de cas d'utilisation malveillante du DNS aux trois quarts de l'espace de noms des gTLD¹⁸. 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 rapport¹⁹ sur leur collaboration pour faciliter

¹⁸ 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).

¹⁹ 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.

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**, lors de l'ICANN67, d'un [Guide des bureaux d'enregistrement pour le signalement de cas d'utilisation malveillante](#). 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 d'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.

- **Réponse multidimensionnelle de l'organisation ICANN²⁰ (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 à ce type de menaces 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 DNS²¹.

²⁰ 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](#).

²¹ 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 de ce dernier, ainsi que sur 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 aux fins de la formation et du renforcement des capacités à travers le monde.

- En réponse à la crise du COVID-19, l’OCTO a élaboré l’outil de **signalement et de collecte d’informations sur les menaces à la sécurité des noms de domaine (DNSTICR)**. Cet outil vise à recenser les noms de domaine impliqués dans une utilisation malveillante en lien avec le COVID-19 et à faciliter la communication de ces données aux entités 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 DNS²². En octobre 2021, l’organisation ICANN et le Groupe des représentants des opérateurs de registre ont fait part de leur accord de principe visant²³ 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). Ces modifications ont été récemment [approuvées par le Conseil d’administration de l’ICANN](#) (30 avril 2023) et devraient prendre effet le 3 février 2024.
- 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’ICANN²⁴.

²² 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).

²³ Voir la lettre du RySG à l’ICANN (22 octobre 2021) et le billet de blog de l’ICANN (28 octobre 2021).

²⁴ 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.* »

- Un nouveau projet qui sera supervisé par l’OCTO de l’ICANN, intitulé [Inferential Analysis of Maliciously Registered Domains \(INFERMAL\)](#), vise à **analyser systématiquement les préférences des cyberattaquants. Il s’intéresse notamment à leur utilisation des noms de domaine de certains bureaux d’enregistrement plutôt que d’autres**, ainsi qu’aux mesures possibles pour atténuer les activités malveillantes dans l’ensemble des domaines de premier niveau (TLD). Ce projet trouve en partie son origine dans les données recueillies lors de l’[analyse statistique de l’utilisation malveillante du DNS dans les gTLD](#) (9 août 2017)²⁵. Celles-ci suggèrent que les acteurs malveillants pourraient privilégier des bureaux d’enregistrement proposant des coûts d’enregistrement bas, acceptant des modes de paiement spécifiques, offrant des interfaces de programmation d’application (API) gratuites pour les enregistrements de masse, ou éviter ceux qui exigent certaines informations lors du processus d’achat.
- 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 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 au recensement 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 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 responsables d’un nombre disproportionné de menaces à la sécurité du DNS. En cas d’impossibilité de mener un dialogue constructif, le département 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 2019²⁶, 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

²⁵ Cette étude a été menée dans le cadre de la révision de la CCT et un [commentaire du GAC](#) (19 septembre 2017) a été formulé au sujet de ce rapport.

²⁶ 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).

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 gTLD²⁷ 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 de l'ICANN78](#) (9 octobre 2023), le département de l'ICANN chargé de la conformité contractuelle a fait rapport sur les mesures qu'il a prises en réponse à des plaintes²⁸, ainsi que sur son [programme d'audit](#), notamment :
 - [l'achèvement d'un audit de bureaux d'enregistrement](#)(22 juin 2023) portant sur 15 bureaux d'enregistrement « *représentant 7 familles de bureaux d'enregistrement comprenant au total 619 bureaux d'enregistrement* » établis dans 8 pays, totalisant 83 millions de noms de domaine sous gestion (voir la liste à la p.17). Quarante pour cent des bureaux audités ont pu résoudre les « constatations initiales », tandis que 53 % ne l'ont pas pu et « *mettent en œuvre les changements nécessaires* » pour pallier les lacunes restantes (voir p. 10-14) ;
 - **lancement d'un nouvel audit de conformité des registres** (août 2023) portant sur 19 opérateurs de registres, non audités précédemment, ayant un score [DAAR](#) d'utilisation malveillante supérieur à 0 %.
- **Enquête sur les initiatives d'atténuation de l'utilisation malveillante du DNS dans les ccTLD par le Comité permanent sur l'utilisation malveillante du DNS (DASC) de la ccNSO**
 - Les plans de travail du Groupe de travail sur la sécurité publique (PSWG) du GAC ont intégré un examen des pratiques d'atténuation de l'utilisation malveillante du DNS par les ccTLD, afin d'éclairer l'élaboration de normes contractuelles renforcées dans l'espace des gTLD. Plus précisément, le plus récent [plan de travail 2023-2024 du PSWG](#) comprend le point de travail 1.3 visant à « *revoir et recenser les meilleures pratiques des ccTLD pour adoption dans l'espace des gTLD* » :
 - *Examiner et évaluer les meilleures pratiques des ccTLD en matière d'atténuation des menaces de sécurité, telles que la prédiction de l'utilisation malveillante et les politiques de validation et de vérification des titulaires de noms de domaine, en vue de*

²⁷ .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)

²⁸ Voir [les diapositives de mise à jour sur la conformité de l'ICANN78](#) pages 9-10 et <https://features.icann.org/compliance> pour des rapports plus détaillés.

recenser des approches possibles, pratiques et applicables, et d'examiner comment elles pourraient éclairer l'élaboration de normes contractuelles renforcées dans l'espace des gTLD.

- Auparavant, des opérateurs de ccTLD du monde entier avaient fait part au GAC, lors d'un [séminaire Web de préparation à l'ICANN69](#) (4 juin 2020), des enseignements qu'ils ont tirés de leurs opérations pendant la crise de COVID-19.
- En mars 2022, la ccNSO a créé un [Comité permanent sur l'utilisation malveillante du DNS \(DASC\)](#) dans le but de « *sensibiliser aux problèmes liés à l'utilisation malveillante du DNS et mieux les faire connaître, favoriser un dialogue ouvert et constructif et, au bout du compte, aider les gestionnaires de ccTLD dans leurs démarches visant à atténuer l'impact de l'utilisation malveillante du DNS* », tout en notant que « *en conformité avec la nature de la ccNSO, l'objectif du Comité n'est pas de formuler des politiques ou des normes, étant donné que l'élaboration de politiques dans ce domaine n'entre pas dans le cadre des attributions de la ccNSO en matière de politiques* ».
- Au cours de l'[atelier de développement des capacités du GAC de l'ICANN76](#) (11 mars 2023), le DASC a présenté au GAC ses premières conclusions à la suite d'une enquête qu'il a menée entre septembre et novembre 2022, auprès d'environ 100 ccTLD, sur leurs pratiques d'atténuation de l'utilisation malveillante du DNS. La présentation abordait des résultats quantitatifs concernant :
 - les méthodes utilisées pour atténuer l'utilisation malveillante du DNS (politiques d'enregistrement, procédures de plainte, autres outils) et les mesures prises lorsque ce type de phénomène était détecté (avis aux titulaires, suspension, suppression) ;
 - la collaboration avec les CERT nationales, les organismes chargés de l'application de la loi et les mécanismes de notification de confiance ;
 - le signalement de l'utilisation malveillante du DNS.
- Ces résultats ont été ensuite débattus en profondeur lors de la [séance de la ccNSO de l'ICANN77](#), mettant un accent particulier sur les résultats quantitatifs liés aux vérifications des données d'enregistrement, leur portée, leur calendrier, leurs méthodes et leurs conséquences. La corrélation entre les politiques tarifaires et les niveaux d'utilisation malveillante du DNS a également été examinée.
- Lors de la présentation finale des résultats de cette enquête dans le cadre d'un [séminaire Web du DASC en préparation de l'ICANN78](#), le 28 septembre 2023, (voir [l'enregistrement et les diapositives](#)), le DASC s'est concentré sur la distribution quantitative des tendances d'utilisation malveillante du DNS et des pratiques d'atténuation, en fonction des caractéristiques des ccTLD (y compris la région, le modèle de gouvernance, la taille du portefeuille de domaines, etc.).
- Il est prévu que le DASC de la ccNSO participe à la discussion plénière du GAC sur l'atténuation de l'utilisation malveillante du DNS lors de l'ICANN78. Le DASC abordera également les prochaines étapes de l'étude des mesures de l'utilisation malveillante du DNS et des outils d'atténuation dans les ccTLD, dans le cadre d'une [mise à jour du DASC à la ccNSO](#) à Hambourg.

Principaux documents de référence :

- [Résolution du Conseil d'administration de l'ICANN](#) (10 septembre 2023) basée sur [l'évaluation de l'organisation ICANN](#) des révisions CCT et SSR2 en suspens concernant l'atténuation de l'utilisation malveillante du DNS
- [Compte rendu sommaire des commentaires publics](#) (1er août 2023) préparé par l'organisation ICANN sur la procédure de consultation publique relative à la proposition de modifications aux contrats des registres et bureaux d'enregistrement concernant l'utilisation malveillante du DNS
- [Commentaires du GAC](#) (17 juillet 2023) sur la proposition de modifications aux contrats des registres et bureaux d'enregistrement concernant l'utilisation malveillante du DNS
- [Rapport du département chargé de la conformité contractuelle sur le cycle d'audit des bureaux d'enregistrement de novembre 2022](#) (22 juin 2023)
- [Modifications au RA et au RAA de base des gTLD visant à renforcer les obligations contractuelles relatives à l'utilisation malveillante du DNS](#) (29 mai 2023)
- Annonce du projet [INFERMAL \(Inferential Analysis of Maliciously Registered Domains\)](#) (25 avril 2023)
- [Rapport de la petite équipe de la GNSO au conseil de la GNSO sur l'utilisation malveillante du DNS](#) (7 octobre 2022)
- [The Last Four years in Retrospect: A Brief Review of DNS Abuse](#) élaboré par l'organisation ICANN (22 mars 2022)
- [Étude sur l'utilisation malveillante du DNS](#) et son [annexe technique](#), élaborés par la Commission européenne (31 janvier 2022)
- [Rapport final](#) de la révision de la SSR2 (25 janvier 2021) et [commentaires du GAC](#) y afférents (22 juillet 2021)
- 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'ICANN78 – Utilisation malveillante du DNS
Distribution	Membres du GAC (avant la réunion) et public en général (après la réunion)
Date de distribution	Version 1 : 11 octobre 2023