Atténuation de l'utilisation malveillante du système des noms de domaine (DNS)

Séance 15

Table des matières

Objectifs de la séance

L'utilisation malveillante du DNS est une question prioritaire pour le Comité consultatif gouvernemental (GAC). En collaboration avec les membres du Comité consultatif sur la sécurité et la stabilité (SSAC), les co-responsables du GAC pour l'utilisation malveillante du DNS (Commission européenne, Japon et États-Unis) planifient un programme pour l'ICANN81 et l'ICANN82 qui :

- Introduise les représentants du GAC au sujet (y compris lors d'un séminaire en ligne pré-ICANN81),
- Décrive le travail sur l'utilisation malveillante du DNS qui a lieu au sein de l'ICANN (c'est-à-dire le travail que le GAC peut influencer), et aussi
- Sensibilise aux efforts déployés en dehors de l'ICANN pour lutter contre les activités abusives.

Proposition des dirigeants pour la ligne d'action du GAC

1. **Continuer à discuter de la portée de l'élaboration de politiques souhaitable pour continuer à améliorer la prévention et l'atténuation de l'utilisation malveillante du DNS**, en tenant compte des éléments suivants :
    - Recommandation de la petite équipe de la GNSO sur l'utilisation malveillante du DNS (7 octobre 2022) d'**initier un processus d'élaboration de politiques sur les enregistrements malveillants**, et des négociations contractuelles potentielles sur cette question qui devraient, éventuellement, être informées par les conclusions du projet

récemment lancé dénommé Analyse inférentielle des domaines enregistrés à des fins malveillantes (INFERMAL), pour explorer les pilotes des enregistrements de noms de domaine malveillants[1].

- La déclaration du GAC dans les commentaires du GAC (17 juillet 2023) sur les amendements proposés disant que « *le travail ultérieur avec la communauté multipartite sur l'utilisation malveillante du DNS [...] devrait inclure des processus d'élaboration de politiques (PDP) afin de mieux informer les RA et RAA actualisés, ainsi que d'autres travaux sur les questions en suspens à traiter avant la prochaine série de candidatures aux nouveaux gTLD ».*
- Dans son rapport de synthèse des commentaires publics sur les nouveaux amendements (1er août 2023), l'organisation ICANN a noté que « *la communauté de l'ICANN aura l'occasion de discuter de ces obligations et de déterminer si d'autres obligations s'avèrent nécessaires […].* ***L'organisation ICANN et la CPH NT (Équipe de négociation de la Chambre des parties contractantes) soutiennent les commentaires du GAC disant qu'après l'adoption des amendements proposés, le travail devrait inclure des processus d'élaboration de politiques (PDP) pour informer davantage le RA de base et le RAA actualisés*** *».*
- Plans du département de la conformité contractuelle de l'ICANN pour appliquer les nouveaux amendements, comme indiqué au GAC lors de l'ICANN79 :
  - Effectuer un suivi spécifique et hiérarchiser le traitement des plaintes déposées par les organismes d'application de la loi et les professionnels de la cybersécurité
  - Faciliter la présentation de plaintes valables qui fournissent suffisamment d'informations pour que des mesures rapides puissent être prises
  - Inclure les nouvelles obligations en matière d'utilisation malveillante du DNS dans le champ d'application des audits proactifs futurs
  - Produire un rapport dédié sur l'application des nouvelles exigences en matière d'utilisation malveillante du DNS, publié mensuellement à partir de juin 2024
  - Préparer un rapport spécifique sur l'exécution des nouvelles obligations après 6 mois (à publier au deuxième trimestre 2025)
- **L'indication du Conseil d'administration de l'ICANN**, lors d'une interaction GAC/Conseil d'administration sur le communiqué de San Juan de l'ICANN79 (13 mai 2024)[2], disant qu'alors que les rapports de conformité devraient contribuer à mesurer l'impact des amendements de l'utilisation malveillante du DNS, **il appartiendrait à un effort mené par la communauté, facilité et soutenu par l'ICANN, de déterminer les indicateurs et les ensembles de données spécifiques qui permettront de mesurer** un tel impact. En réponse à des questions importantes dans le communiqué de Kigali de l'ICANN80 (15 octobre 2024), le Conseil d'administration de l'ICANN a ajouté « qu'*il est important de*

[1] Voir le blog de l'OCTO de l'ICANN « Le nouveau projet de l'ICANN explore les pilotes des enregistrements de noms de domaine malveillants » du 25 avril 2023

[2] Voir les commentaires du Conseil d'administration de l'ICANN sur des questions d'importance dans le communiqué de San Juan de l'ICANN79 (9 mai 2024)

prévoir suffisamment de temps pour la mise en œuvre des nouveaux amendements et de mesurer l'impact avec précision. Par exemple, les ***indicateurs de conformité, bien qu'ils constituent une source de données importante, ne peuvent pas être utilisés à eux seuls pour mesurer l'impact global des modifications de l'utilisation malveillante du DNS****. La conformité a une visibilité sur les instances d'utilisation malveillante du DNS qui font l'objet des cas de conformité, mais pas sur l'ensemble du marché du DNS ni sur la façon dont les parties contractantes ou d'autres acteurs au sein de l'écosystème DNS traitent l'utilisation malveillante du DNS* ».

Situation actuelle et faits récents

- **Amendements des contrats de registre et de bureau d'enregistrement afin d'améliorer les obligations en matière d'atténuation de l'utilisation malveillante du DNS**

  - Depuis l'ICANN66, **les dirigeants du Groupe de travail sur la sécurité publique du GAC ont informé le GAC** de la question de l'atténuation de l'utilisation malveillante du DNS[3] , y compris **des mesures 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 les stratégies de tarification comme déterminants clés des niveaux d'utilisation malveillante dans n'importe quel TLD donné, ainsi que sur **les moyens possibles de traiter l'utilisation malveillante du DNS plus efficacement au niveau du Conseil d'administration de l'ICANN et de l'organisation ICANN**, comme les révisions des contrats de l'ICANN avec les opérateurs de registre et les bureaux d'enregistrement, l'application des exigences existantes, la mise en œuvre des recommandations pertinentes des révisions de la CCT et de la SSR2, les recommandations de politique pour les fournisseurs de services d'anonymisation et d'enregistrement fiduciaire, l'amélioration de l'exactitude des données d'enregistrement et la publication de données plus détaillées sur les cas d'utilisation malveillante de noms de domaine.
  - Dans ses communiqués des années récentes, 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 proposé 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 souligné que l'ICANN est « *particulièrement bien placée pour négocier des améliorations aux contrats existants* » et « *pour recevoir les contributions de la communauté de l'ICANN* ».
  - Au cours de l'ICANN75, la **petite équipe de la GNSO consacrée à l'utilisation malveillante du DNS a discuté des « lacunes dans l'interprétation et/ou l'application » des contrats actuels de l'ICANN** , comme indiqué plus tard dans 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 de dispositions contractuelles proposées applicables à tous les gTLD pour améliorer les réponses à l'utilisation malveillante du DNS[4], par exemple celles identifiées dans les révisions de la SSR2 et de la CCT ».***
  - En décembre 2022, le Groupe des représentants des bureaux d'enregistrement (RrSG) et le Groupe des représentants des opérateurs de registre (RySG) ont **officiellement notifié**

[3] Voir les documents des séances plénières du GAC lors de l'ICANN66, l'ICANN68, l'ICANN69, l'ICANN70, l'ICANN71, l'ICANN72, l'ICANN73 et l'ICANN74.

[4] Communiqué du GAC de l'ICANN70, section IV.1 p. 5

à l'ICANN d'engager des négociations pour « *intégrer les exigences contractuelles de base à l'article 3.18 du RAA pour les bureaux d'enregistrement afin d'interrompre et/ou d'atténuer l'utilisation malveillante du système des noms de domaine* » et « *renforcer les obligations relatives à l'utilisation malveillante du DNS contenues dans le [Contrat de registre]* ». **La PDG de l'ICANN**, dans un Blog (18 janvier 2023) a confirmé le travail en cours afin de « ***définir les obligations de base pour exiger aux opérateurs de registre et aux bureaux d'enregistrement d'atténuer ou d'interrompre l'utilisation malveillante du DNS*** » en s'attendant à ce que cela « *aide l'équipe chargée de la conformité contractuelle de l'ICANN dans ses efforts d'application avec les opérateurs de registre et les bureaux d'enregistrement qui ne parviennent pas à traiter correctement l'utilisation malveillante du DNS* ». Elle a également noté que ce serait une occasion pour que la communauté de l'ICANN « *discute et détermine si d'autres obligations sont requises par le biais d'un processus d'élaboration de politiques ».*

- Entre-temps, l'unité constitutive des utilisateurs commerciaux (**BC**) de la GNSO, l'unité constitutive des représentants de la propriété intellectuelle (**IPC**), et le comité consultatif At-Large (**ALAC**) ont demandé (20 janvier 2023) que « *la contribution de la communauté soit considérée comme appropriée, et d'aider l'organisation ICANN à jouer son rôle 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 déclaré que « *le Conseil d'administration et l'organisation ICANN ont écouté attentivement la communauté au cours des dernières années en ce concernant l'utilisation malveillante du DNS. Adopter **cette approche pour apporter des améliorations ciblées aux contrats, afin d'ajouter une obligation claire pour que les opérateurs de registre et les bureaux d'enregistrement atténuent l'utilisation malveillante du DNS, sera un élément de base important dans un long parcours qui envisage des discussions politiques potentielles** ouvertes à la communauté de l'ICANN dans son ensemble, **et potentiellement des négociations** futures entre la Chambre des parties contractantes (CPH) et l'organisation ICANN* ».
- Dans un document d'information du GAC pré-ICANN76 sur la négociation des contrats concernant l'atténuation de l'utilisation malveillante du DNS (28 février 2023) [*connexion au site Web du GAC requise*] les responsables thématiques du GAC **ont discuté des améliorations possibles aux dispositions contractuelles existantes** pour une plus grande clarté et une meilleure applicabilité, **ainsi que les domaines possibles pour les nouvelles dispositions contractuelles** discutées au sein de la communauté de l'ICANN (notamment par les révisions de la CCT et de la SSR2) **, y compris les encouragements financiers et de réputation, les seuils des déclencheurs d'utilisation malveillante et de conformité, les meilleures pratiques et les rapports d'abus centralisés.**
- Au cours de la réunion bilatérale du GAC avec le Conseil d'administration de l'ICANN pendant l'ICANN76, **le GAC a encouragé le Conseil d'administration à envisager de mener une séance d'écoute avec la communauté de l'ICANN** sur les négociations (voir

p.11 du procès-verbal de la réunion du GAC de l'ICANN76)

- Dans le Communiqué de Cancun de l'ICANN76 (20 mars 2023), le GAC a encouragé les négociations en cours pour « procéder avec célérité » et a noté qu'il « *considère que* ***des efforts continus dans ce domaine seront nécessaires, y compris une amélioration supplémentaire des obligations contractuelles et/ou des processus d'élaboration de politiques ciblés avant le lancement d'une deuxième série de nouveaux domaines génériques de premier niveau*** *(nouveaux gTLD)* ». En outre, le GAC a encouragé *« les parties contractantes et l'ICANN à examiner, entre autres, les mesures proactives et les encouragements positifs pour les opérateurs de registre et les bureaux d'enregistrement dans les travaux futurs sur l'atténuation ou l'interruption de l'utilisation malveillante du DNS ».*
- En préparation pour l'ICANN77, le groupe **de travail du GAC chargé des régions faiblement desservies** (USRWG) a organisé deux **séminaires en ligne** pour préparer les nouveaux arrivants et les représentants des régions faiblement desservies auprès du GAC à contribuer à un commentaire sur les amendements attendus aux contrats de registre et de bureau d'enregistrement[5].
- **L'organisation ICANN a lancé une procédure de commentaires publics** sur les amendements aux contrats de registre de base et aux contrats de bureau d'enregistrement pour modifier les obligations contractuelles en matière d'utilisation malveillante du DNS (29 mai 2023) qui ont ensuite été présentées dans un séminaire en ligne au cours de la semaine de préparation à l'ICANN77 (30 mai 2023). Parmi les différents changements proposés aux contrats de l'ICANN, les amendements incluent une **nouvelle exigence de prendre rapidement des mesures d'atténuation appropriées contre les domaines pour lesquels la partie contractante dispose d'éléments de preuve pouvant donner lieu à une action** démontrant que les domaines font l'objet d'utilisation malveillante du DNS. En plus des amendements proposés au contrat, un avis préliminaire de l'ICANN fournit une explication détaillée des nouvelles dispositions et définit les attentes quant à leur interprétation.
- À la suite de ses discussions sur les amendements proposés au cours de l'ICANN77[6], les commentaires du GAC (17 juillet 2023) ont été soumis à une procédure de commentaires publics :
  - Le GAC a noté que les amendements sont « *opportuns et pertinents et, lorsqu'ils seront adoptés, représenteront un premier pas important dans la lutte contre l'utilisation malveillante du DNS* ».
  - Le GAC a souligné que : « *à la lumière de la menace continue que l'utilisation malveillante du DNS représente pour les consommateurs et les secteurs public et privé, il est impératif que les contrats améliorés soient adoptés rapidement après*

[5] Voir le 1er et le 2e séminaires en ligne du 4 et du 22 mai 2023 concernant le renforcement des capacités du GAC pré-ICANN77 sur l'utilisation malveillante du DNS

[6] Voir l'Atelier de renforcement des capacités du GAC sur l'utilisation malveillante du DNS (dimanche 11 juin) et la discussion du GAC sur l'utilisation malveillante du DNS (mercredi 14 juin)

l'achèvement de la procédure de commentaires publics »

- **Le GAC a exprimé son soutien pour « *les amendements proposés en tant que question générale* » , mais a invité « *l'organisation ICANN et l'équipe de négociation de la Chambre des parties contractantes (CPH NT) à examiner certaines questions spécifiques liées au texte des amendements* »**. 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 a indiqué qu'il attendait avec impatience « *de s'engager dans des travaux ultérieurs* *avec la communauté multipartite sur l'utilisation malveillante du DNS après l'adoption des amendements.* *Ce travail devrait inclure des processus d'élaboration de politiques (PDP) pour éclairer davantage les RA et RAA actualisés, ainsi que d'autres travaux sur les questions en suspens* *à régler avant la prochaine série de candidatures aux nouveaux gTLD ».***

- Dans son rapport de synthèse des commentaires publics (1er août 2023), l'**organisation ICANN a indiqué que le vote par les opérateurs de registre et les bureaux d'enregistrement se poursuivra sur les amendements proposés initialement** et a noté qu'*« en ce qui concerne les commentaires selon lesquels les amendements proposés sont insuffisants pour relever le défi de l'abus de DNS » : l'organisation ICANN prend note des commentaires et rappelle à la communauté que la communauté de l'ICANN aura l'occasion de discuter de ces obligations et de déterminer si d'autres obligations sont nécessaires […].* ***L'organisation ICANN et le CPH [équipe de négociation] appuient les commentaires du GAC qui a déclaré qu'après l'adoption des amendements proposés, le travail devrait inclure des processus d'élaboration de politiques (PDP) pour informer davantage les RA de base et les RAA actualisés*** *».*
- La période de vote pour les opérateurs de registre et les bureaux d'enregistrement sur les amendements a commencé le 9 octobre 2023 pour une durée de 60 jours. Elle a conclu avec succès, les opérateurs de registre ayant atteint 80 % des votes affirmatifs et les bureaux d'enregistrement 94 % d'approbation[7].
- Le Conseil d'administration de l'ICANN a par la suite décidé d'approuver les amendements (21 janvier 2024) et a déterminé qu'« ***aucune révision supplémentaire des amendements globaux proposés n'est nécessaire après avoir pris en compte les commentaires publics et les résultats du vote*** *».*
- L'amendement au contrat de registre, l'amendement au contrat d'accréditation du bureau d'enregistrement et l'avis connexe : La conformité avec les obligations en matière d'utilisation malveillante DNS dans le contrat d'accréditation de bureau d'enregistrement et le contrat de registre ont été publiés le 5 février 2024 et sont entrés en vigueur le 5

[7] Les résultats détaillés du vote sont disponibles sur https://www.icann.org/resources/pages/global-amendment-2024-en

avril 2024[8].

- Au cours de la réunion ICANN79, le département chargé de la conformité contractuelle de l'ICANN a présenté ses plans d'exécution au GAC. Il s'agit notamment des éléments suivants :
  - Suivre spécifiquement les plaintes déposées par les organismes d'application de la loi et les professionnels de la cybersécurité et la hiérarchisation de leur traitement.
  - Faciliter la présentation de plaintes valables qui fournissent suffisamment d'informations pour que des mesures rapides puissent être prises.
  - Inclure de nouvelles obligations en matière d'utilisation malveillante du DNS dans le champ d'application des futurs audits proactifs
  - Un rapport spécifique sur l'application des nouvelles exigences en matière d'utilisation malveillante du DNS, qui sera publié et mis à jour chaque mois, et qui comprendra des données telles que :
    - Le nombre de plaintes reçues ventilées par type d'utilisation malveillante du DNS ;
    - Le nombre de notifications de conformité envoyées aux parties contractantes en vertu des exigences en matière d'utilisation malveillante du DNS ;
    - Le nombre de cas résolus avec les parties contractantes et leurs résultats, y compris si la partie contractante a pris des mesures pour arrêter ou perturber l'utilisation malveillante du DNS ou si aucune mesure n'a été prise parce qu'il n'y avait pas de preuve donnant lieu à une action ; et
    - Le nombre de cas résolus avec les parties contractantes, et leurs résultats, qui résultent de plaintes soumises par les organismes d'application de la loi relevant de la juridiction du bureau d'enregistrement.
  - D'ici le deuxième trimestre 2025, le département chargé de la conformité contractuelle de l'ICANN a l'intention de préparer un rapport plus détaillé sur l'application des exigences en matière d' utilisation malveillante du DNS au cours des 6 premiers mois en vigueur.
- Dans le communiqué du GAC de San Juan de l'ICANN79 (11 mars 2024), le GAC a déclaré qu'il *« suivra les rapports de conformité de l'ICANN sur l'application de l'utilisation malveillante du DNS »* et « *que l'on s'attend toujours à ce que des progrès significatifs se produisent avant la prochaine série de candidatures aux nouveaux gTLD »*.
- Dans les commentaires du Conseil d'administration de l'ICANN sur les questions d'importance du communiqué de San Juan de l'ICANN79 (9 mai 2024) concernant le communiqué de l'ICANN79, le Conseil d'administration de l'ICANN a déclaré : « ***L'intention est que les rapports de conformité contribuent à mesurer l'impact des modifications relatives à l'utilisation malveillante du DNS***. *Cependant,* ***la détermination***

[8] Voir les avis envoyés par l'organisation ICANN aux opérateurs de registre et aux bureaux d'enregistrement (5 février 2024)

des indicateurs et des ensembles de données spécifiques qui permettront de mesurer un tel impact devrait être un effort mené par la communauté, facilité et soutenu par l'ICANN ». Il a en outre indiqué qu'« *une équipe interdisciplinaire de l'organisation ICANN travaille à analyser les informations et à déterminer comment aborder ces efforts* ».

- Au cours du récent Sommet des parties contractantes (6 au 9 mai 2024), les parties contractantes ont discuté de la mise en œuvre et de l'impact des amendements de leur point de vue. Il a été signalé que le sous-groupe d'utilisation malveillante du DNS de la Chambre des parties contractantes (CPH) engage actuellement la conformité de l'ICANN sur la façon dont les amendements sont appliqués.
- Au cours de la discussion entre le Conseil d'administration de l'ICANN et le GAC (21 octobre 2024) sur les questions d'importance identifiées dans le Communiqué de Kigali de l'ICANN80 (17 juin 2024), le Conseil d'administration de l'ICANN a souligné que les nouveaux amendements « *autorisent le département chargé de* la *conformité contractuelle de l'ICANN à prendre des mesures d'application contre les bureaux d'enregistrement ou les opérateurs de registre qui ne parviennent pas à atténuer ou à interrompre de manière adéquate l'utilisation malveillante du DNS bien documentée* » et a signalé que la **conformité contractuelle de l'ICANN a pris plusieurs mesures basées sur ces amendements**, notamment :
  - *A émis un avis formel de manquement contre un opérateur de registre et un avis formel de manquement contre un bureau d'enregistrement pour non-respect des exigences d'atténuation de l'utilisation malveillante du DNS.*
  - *A initié des enquêtes qui ont abouti à la suspension de plus de 2600 noms de domaine malveillants et à la désactivation de plus de 328 sites Web d'hameçonnage.*
  - *A commencé à publier des rapports mensuels qui détaillent le nombre de cas signalés d'hameçonnage, de distribution de logiciels malveillants, de réseaux zombies, de dévoiement et de spam utilisés pour commettre des abus dans le DNS, ainsi que la manière dont ces problèmes ont été résolus. Les rapports récemment lancés sont ventilés par type d'utilisation malveillante du DNS signalé et contiennent une quantité importante de données recueillies à partir des plaintes reçues et des mesures d'application connexes*
  - *Lancement d'un audit des opérateurs de registre pour confirmer, entre autres, que les entités auditées respectent les nouvelles obligations en matière d'utilisation malveillante du DNS*
- En ce qui concerne la mesure de l'**impact et de l'efficacité des nouveaux amendements relatifs à l'utilisation malveillante du DNS**, le Conseil d'administration de l'ICANN a déclaré : « *il est important de prévoir suffisamment de temps pour la mise en œuvre des nouveaux amendements et de mesurer l'impact avec précision. Par exemple, les* ***indicateurs de conformité, bien qu'ils constituent une source de données importante, ne peuvent pas être utilisés à eux seuls pour mesurer l'impact global des modifications de l'utilisation malveillante du DNS****. La conformité a une visibilité sur les instances d'utilisation malveillante du DNS qui font l'objet de cas de conformité, mais pas sur*

l'ensemble du marché du DNS et sur la façon dont les parties contractantes ou d'autres acteurs au sein de l'écosystème du DNS traitent l'utilisation malveillante du DNS. Par conséquent, ***les données de conformité peuvent être considérées aux côtés de celles d'autres experts tiers qui capturent également des indicateurs nuancés****. Par exemple, la CARTE de Net Beacon contient des indicateurs sur le marché mondial des noms de domaine gTLD tels que les taux normalisés d'abus, le temps médian pour atténuer, et le point de vue des noms malveillants par rapport aux noms compromis* ».

- **Perspectives d'élaboration de politiques concernant la prévention et l'atténuation de l'utilisation malveillante du DNS**
    - Selon 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. En commençant par les recommandations de la CCT-RT et de la SSR2-RT, puis suite aux multiples séances intercommunautaires et plus récemment suite aux 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***.
    - Depuis avant la réunion ICANN68, **les dirigeants du GAC ont cherché à établir, en collaboration avec la direction du conseil de la GNSO, un cadre de travail communautaire et d'élaboration de politiques possible pour lutter contre 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 la **petite équipe de la GNSO consacrée à l'utilisation malveillante du DNS** qui devrait déterminer quels sont « *les efforts politiques que, le cas échéant, le conseil de la GNSO devrait envisager d'entreprendre pour soutenir les efforts déjà en cours dans les différentes parties de la communauté pour lutter contre l'utilisation malveillante du DNS* ».
    - 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 étroitement adapté pour produire un résultat opportun et réalisable*** », 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 de telles activités[9].
    - **La petite équipe de la GNSO a recommandé** dans un rapport au conseil de la GNSO (7 octobre 2022) **le lancement d'élaboration de politiques sur les enregistrements malveillants à portée limitée** (Rec. 1) **l'exploration ultérieure du rôle des enregistrements groupés dans l'utilisation malveillante du DNS** et les mesures déjà en place pour y remédier (Rec. 2) **en encourageant d'autres travaux vers des rapports plus faciles, meilleurs et exploitables** sur l'utilisation malveillante du DNS (Rec. 3) et les travaux possibles entre les parties contractantes et le département chargé de la

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

conformité contractuelle de l'ICANN concernant ses conclusions sur les lacunes potentielles dans l'interprétation et/ou l'application des contrats actuels de l'ICANN (Rec. 4). Le conseil de la GNSO a procédé à la sensibilisation recommandée aux parties contractantes concernant la Recommandation 3 et aux parties contractantes, à l'Institut de lutte contre l'utilisation malveillante du DNS et au département chargé de la conformité contractuelle de l'ICANN concernant la Recommandation 2 (6 janvier 2023).

- **En ce qui concerne les enregistrements groupés**, la réponse du département chargé de la conformité contractuelle de l'ICANN au conseil de la GNSO (22 février 2023) indique que « *les contrats et les politiques de l'ICANN ne contiennent pas d'exigences ou de limitations liées à l'enregistrement groupé de noms de domaine. Par conséquent,* ***le département chargé de la conformité contractuelle de l'ICANN ne collecte pas ou ne suit pas les informations sur les enregistrements groupés*** *[ou] le rôle potentiel que ces enregistrements peuvent jouer dans l'utilisation malveillante du DNS (Système des noms de domaine) ».* La réponse de l'Institut de lutte contre l'utilisation malveillante du DNS (24 février 2023) a proposé que « ***des recherches devraient être menées pour déterminer l'ampleur de tous les problèmes liés à [l'enregistrement groupé de noms de domaine] avant tout travail de politique*** *»,* et a souligné la pertinence du cadre pour les algorithmes générés par les domaines associés aux réseaux zombies et aux programmes malveillants mis au point par le RySG et le PSWG du GAC. **L'Institut de la lutte contre l'utilisation malveillante du DNS a exprimé son soutien aux 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 identifié comme malveillant* »** dans le cadre des « *options raisonnables 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 de commentaires supplémentaires reçus des parties contractantes[10], dans le cadre de ses conclusions préliminaires sur les enregistrements groupés (15 mai 2023), **la petite équipe de la GNSO consacrée à l'utilisation malveillante du DNS** a conclu que **« *cela ne relève pas du domaine de la politique de consensus pour le moment* »** dans la mesure où :
  - *les plaintes provenant d'enregistrements uniques ou multiples sont traitées uniformément, sans clarté sur ce qui pourrait constituer des enregistrements groupés justifiant des réactions ciblées.*
  - *L'absence d'une définition claire n'a pas donné lieu à une réponse claire.*
  - *D'autres outils de connaissance du client sont considérés comme plus efficaces pour détecter les abus potentiels et devraient faire l'objet d'une plus grande attention.*
  - *Le projet INFERMAL (Analyse inférentielle des domaines enregistrés à des fins malveillantes) récemment lancé par l'ICANN semble indiquer la volonté de*

[10] Voir la correspondance 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)

l'organisation d'examiner cette question et de fournir [...] de meilleures statistiques et renseignements [en la matière]

- Dans le Communiqué de Hambourg (30 octobre 2023), le GAC a manifesté son intention de « *s'engager avec la communauté dans des discussions sur les efforts politiques autour [...] ainsi que sur d'autres thèmes clés liés à la mise en œuvre efficace des amendements, comme la clarification des termes clés des amendements (c.-à-d., « raisonnable », « réalisable », « rapide »), et d'autres actions pour atténuer l'utilisation malveillante du DNS, comme les efforts en matière de renforcement des capacités* ».
- Au cours de l'appel de préparation à l'ICANN79 entre le conseil de la GNSO et les dirigeants du GAC, il a été indiqué qu'à l'heure actuelle, le conseil de la GNSO n'envisage pas activement l'élaboration de politiques sur les questions liées à l'utilisation malveillante du DNS et que cela fait actuellement l'objet de discussions au sein et entre les groupes de parties prenantes de la GNSO.
- Au cours d'une réunion bilatérale avec le GAC à San Juan (6 mars 2024), le conseil de la GNSO a noté que la petite équipe de la GNSO est actuellement suspendue en attendant que les données soient collectées auprès du service de conformité de l'ICANN sur l'impact des amendements, et reprendra une fois que de plus amples informations sont fournies pour déterminer ce qui, le cas échéant, pourrait être approprié pour combler les lacunes dans l'atténuation de l'utilisation malveillante du DNS.

- **État et perspectives de mise en œuvre des recommandations des révisions spécifiques relatives à l'interruption de l'utilisation malveillante du DNS[11]**
  - Dans son rapport final (25 janvier 2021), **la révision de la SSR2 a formulé 63 recommandations** qui mettent l'accent sur les mesures visant à prévenir et à atténuer l'utilisation malveillante du DNS.
    - Le GAC a examiné un rapport préliminaire de l'équipe de révision de la SSR2 (24 janvier 2020) et a approuvé bon nombre des recommandations préliminaires dans un commentaire du GAC (3 avril 2020). Ces recommandations ont été suivies des commentaires du GAC (8 avril 2021) sur les recommandations finales, et son avis ultérieur du Communiqué de l'ICANN72 (1er novembre 2021) demandant une action de suivi et des informations complémentaires sur les niveaux de mise en œuvre de certaines recommandations, auxquels le Conseil d'administration de l'ICANN a répondu (16 janvier 2022) ; cela a conduit à de nouvelles discussions au cours de l'ICANN73[12] et à des communications de l'organisation ICANN au GAC dans une lettre (18 mars 2022) et un e-mail de suivi (12 avril 2022).
    - Sur la base du dernier rapport trimestriel sur la révision spécifique de l'ICANN (21 février 2023) et des 3 résolutions du Conseil d'administration de l'ICANN (22 juillet 2021, 1er mai 2022 et 16 novembre 2022) et 10 septembre 2023 : **23 recommandations** sont maintenant **approuvées** (dont 14 sous réserve de

[11] Le statut de toutes les recommandations peut être consulté dans les rapports trimestriels de l'ICANN, la page d'accueil de chaque révision, accessibles sur https://www.icann.org/resources/reviews/specific-reviews

[12] Voir le procès-verbal du GAC de l'ICANN73 p.13

l'établissement des priorités pour la mise en œuvre), **38 ont été rejetées** et **1 reste en attente** d'autres informations.

- Le 10 septembre 2023, le **Conseil d'administration de l'ICANN a rejeté 6 des 7 recommandations relatives à l'utilisation malveillante du DNS en attente** sur la base de l'évaluation de l'organisation ICANN - **12.1** (*équipe consultative d'analyse de l'utilisation malveillante du DNS*), **12.2** (*structurer les accords avec les fournisseurs de données pour permettre un partage ultérieur des données*), **12.3** (*publier des rapports identifiant les registres et les bureaux d'enregistrement dont les domaines contribuent le plus à l'utilisation malveillante*), **12.4** *(signaler des mesures prises par les registres et les bureaux d'enregistrement pour répondre aux plaintes de conduite illégale et/ou malveillante*), **13.1** (*portail central des plaintes relatives à l'utilisation malveillante du DNS obligatoire pour tous les gTLD*), **13.2** (*publier des données sur les plaintes pour analyse par des tiers*) et **14.2** *(fournir aux parties contractantes des listes de domaines dans leurs portefeuilles identifiés comme abusifs*)
- **Dans sa discussion sur les négociations contractuelles concernant l'utilisation malveillante du DNS, le PSWG du GAC a discuté[13] de plusieurs recommandations de la SSR2 ayant été rejetées** par le Conseil d'administration de l'ICANN conformément à la fiche de suivi du Conseil (22 juillet 2021) - **8.1** *(faire appel à une équipe de négociation comprenant des experts en matière d'utilisation malveillante et de 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 portion de domaines abusifs en dessous du seuil*) et **14.5** *(envisager d'offrir des encouragements financiers*) - **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 de fond utiles de certaines recommandations rejetées**, y compris ceux qui visent **à fournir à l'organisation ICANN et au département chargé de la conformité contractuelle l'ICANN des outils appropriés pour prévenir et atténuer l'utilisation malveillante du DNS*** ».

- Le rapport final de **l'équipe de révision de la concurrence, la confiance et le choix du consommateur** (8 septembre 2018) a formulé 35 recommandations. Dans le Communiqué de Montréal (6 novembre 2019), comme précisé dans une correspondance ultérieure avec le Conseil d'administration de l'ICANN (janvier 2020), **le GAC a conseillé au Conseil d'administration de l'ICANN de « *ne pas procéder à une nouvelle série de gTLD avant la mise en œuvre complète** des recommandations [...] ayant été identifiées comme « conditions préalables » [14 recommandations] ou comme de « haute priorité » [10 recommandations] »*.

[13] Voir la conférence téléphonique du PSWG du 14 février 2023 [*connexion préalable au site Web du GAC requise*]

À la suite de discussions relatives aux communiqués de l'ICANN70 et de l'ICANN71[14], le Conseil d'administration de l'ICANN et le GAC ont convenu d'un accord énoncé dans un appel entre le BGIG, le GAC et le Conseil d'administration (5 octobre 2021) *[connexion au site Web du GAC requise]* selon lequel « *le GAC envisagerait un suivi sur le fond des recommandations de la révision de la 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 GAC[15] :

- **La recommandation 17** (*recueillir des données et faire connaître la chaîne des parties responsables de l'enregistrement des noms de domaine)* **a été approuvée et,** au 14 septembre 2022**, la mise en œuvre a été complétée** conformément à sa documentation de mise en œuvre.
- **La Recommandation 13** (*recueillir des données sur l'impact des restrictions à l'enregistrement*, ce qui, selon le GAC, *« permettrait de prendre des décisions plus éclairées et d'élaborer des politiques concernant les futures dispositions standard des contrats de registre et de bureau d'enregistrement »)* et **la Recommandation 20** *(évaluer les mécanismes de signalement et de traitement des plaintes et envisager éventuellement de modifier les futurs contrats de registre standard pour obliger les registres à divulguer plus clairement leurs points de contact pour le signalement d'abus et à fournir des informations plus granulaires à l'ICANN*) ont été approuvées en partie par la fiche de suivi du Conseil d'administration du 22 octobre 2020, et **leur mise en œuvre est en cours**, **la concurrence étant estimée entre le troisième trimestre (Q3) 2023 et le deuxième trimestre (Q2) 2024** conformément au rapport trimestriel du premier trimestre (Q1) 2023 sur les révisions spécifiques de l'ICANN (31 mars 2023)
- La **Recommandation 14** *(encouragements pour adopter des mesures proactives de lutte contre l'utilisation malveillante du DNS)* et la **Recommandation 15** *(négocier des amendements pour inclure des dispositions visant à prévenir l'utilisation systémique des bureaux d'enregistrement ou des opérateurs de registre spécifiques pour l'utilisation malveillante du DNS, et établir des seuils d'abus pour les déclencheurs automatiques de conformité)* **ont été rejetées par une** résolution **du Conseil d'administration de l'ICANN** du 10 septembre 2023.

- **Les Recommandations LE.1 et LE.2 de la révision RDS-WHOIS2** , qui visaient à « *recueillir régulièrement des données par le biais d'enquêtes et d'études dans le but d'éclairer une évaluation future de l'efficacité du RDS (WHOIS) afin de répondre aux besoins des*

[14] Voir les discussions de clarification du communiqué et les réponses éventuelles du Conseil d'administration au suivi du GAC sur les avis précédents dans les communiqués de l'ICANN70 et de l'ICANN71 : Appel de clarification de l'ICANN70 (21 avril 2021) et 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).

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

organismes chargés de l'application de la loi » et à « *mener des enquêtes et/ou des études comparables avec d'autres utilisateurs du RDS (WHOIS) travaillant régulièrement avec les organismes chargés de l'application de la loi* » sont maintenant **considérées comme *« mises en œuvre dans la mesure du possible »*** dans le cadre des travaux de l'étape 2 et 2A de l'EPDP et du SSAD ODP, conformément à la documentation de mise en œuvre (11 octobre 2022)

- **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 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 gTLD**[16]. 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 compte[17] de 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 ont renforcé les relations de travail établies entre les organismes d'application de la loi et les bureaux d'enregistrement ainsi que la publication par le **Groupe des représentants des bureaux d'enregistrement** d'un Guide des bureaux d'enregistrement pour le signalement d'abus, dans le cadre de l'ICANN67. Ce guide a été mis à jour (janvier 2022) et approuvé par le **Groupe des représentants des opérateurs de registre**.
  - Le **Registre d'intérêt public (PIR)**, opérateur de registre de .ORG et de plusieurs nouveaux gTLD, a lancé le **DNS Abuse Institute** (DNSAI) (17 février 2021). Cette initiative a été présentée au PSWG du GAC (3 mars 2021). Dans son communiqué de l'ICANN70, le GAC salue la création du DNS Abuse Institute et *« encourage les efforts de la communauté visant à s'attaquer de manière coopérative à la lutte contre l'utilisation malveillante du DNS de façon holistique »*. Le DNS Abuse Institute a depuis publié une feuille de route (14 juin 2021), discute régulièrement des meilleures pratiques, et a développé une initiative pour mesurer l'utilisation du DNS pour les activités d'hameçonnage et de programmes malveillants. Lors de l'ICANN74, le GAC a invité le DNS Abuse Institute à présenter son nouvel outil Net Beacon (anciennement connu sous le nom d'**Outil centralisé de**

[16] 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).

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

signalement des cas d'utilisation malveillante), qu'il développe en réponse au document SAC115, à la Recommandation 13.1 de la SSR2, et dans le respect de la Recommandation 20 de la CCT-RT. En amont de l'ICANN79, l'Institut de lutte contre l'utilisation malveillante du DNS a publié une analyse des communiqués du GAC et de l'activité de la communauté sur l'utilisation malveillante du DNS (8 février 2024) dans laquelle il discute des positions du GAC, de l'activité de la communauté connexe et des « lacunes actuelles ».

- **Plusieurs acteurs de l'industrie du DNS cherchent activement à contribuer à mesurer l'utilisation malveillante du DNS** et l'effet que les amendements récemment approuvés aux contrats de registre et de bureau d'enregistrement auront :
  - Au cours de l'ICANN78, le DNS Abuse Institute a présenté au GAC son projet Compass et sa méthodologie qui visent à fournir une approche rigoureuse et transparente pour mesurer l'utilisation malveillante du DNS, et produit actuellement des rapports d'abus mensuels qui discutent des tendances dans l'industrie et les bureaux d'enregistrement et les opérateurs de registre spécifiques qui ont des taux élevés ou faibles d'utilisation malveillante du DNS. Sur la base de ses mesures, le DNS Abuse Institute informe que 80 % des utilisations malveillantes du DNS sont atténués dans les 30 jours. Il s'attend à ce que les tendances d'atténuation évoluent favorablement à l'avenir grâce aux amendements aux contrats de l'ICANN.
  - Au cours de l'ICANN78 et de l'ICANN79, **CleanDNS**, un fournisseur de services qui gère l'utilisation malveillante du DNS pour le compte des bureaux d'enregistrement, des opérateurs de registre et des fournisseurs d'hébergement a discuté avec le GAC de l'importance des rapports bien documentés sur l'utilisation malveillante du DNS qui doivent être communiqués à la partie la plus appropriée (opérateur de registre, bureau d'enregistrement , hébergeur ou titulaire de nom de domaine), afin que le délai nécessaire pour atténuer les abus soit le plus court possible et que la victimisation soit réduite au minimum.
- Au cours du récent Sommet des parties contractantes (6 au 9 mai 2024), l'ICANN et les parties contractantes ont organisé un « atelier sur la lutte contre l'utilisation malveillante du DNS » où l'on a discuté, entre autres, des « préoccupations et défis les plus pressants en matière d'utilisation malveillante du DNS », des « études de cas et des leçons tirées de la remise en question des rapports d'abus du DNS ». L'enregistrement des séances publiques est disponible à l'adresse https://cpsummit2024.sched.com/.

- **Réponse multidimensionnelle de l'organisation ICANN[18] (qui fait désormais partie du programme d'atténuation des menaces à la sécurité du DNS) et de 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.

[18] Voir le billet de blog publié par le PDG de l'ICANN le 20 avril 2020 détaillant la réponse multidimensionnelle de l'organisation ICANN à l'utilisation malveillante du DNS.

- **Le Bureau du directeur de la technologie (OCTO) de l'ICANN et son équipe consacrée à la sécurité, la stabilité et la résilience** (SSR) mènent des recherches et assurent l'expertise de l'ICANN en matière de sécurité du DNS au profit de la communauté. Ils sont engagés dans des forums de veille en matière de cybermenaces et de réponse aux incidents, et mettent au point des systèmes et des outils permettant de détecter, d'analyser et de signaler l'utilisation malveillante du DNS[19].
  - En réponse à la crise du COVID-19, l'OCTO a développé l'outil de **signalement et collecte d'informations sur des menaces à la sécurité des noms de domaine (DNSTICR)** pour aider à identifier 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 été informé de cette question avant l'ICANN68 (12 juin 2020) et les membres du GAC ont été invités à contribuer à la diversité linguistique de l'outil.
  - Depuis janvier 2018, grâce à sa **plateforme de signalement des cas d'utilisation malveillante des noms de domaine (DAAR)**, l'ICANN rend compte tous les mois de l'enregistrement de noms de domaine et des menaces à la sécurité observées dans le DNS[20]. En octobre 2021, l'organisation ICANN et le Groupe des représentants des opérateurs de registre ont fait part de leur accord de principe visant[21] à utiliser les données d'enregistrement détenues par les opérateurs de registre afin de fournir des informations liées aux bureaux d'enregistrement au DAAR, comme rapporté par le GAC dans une lettre transmise à l'ICANN (21 février 2022). Ces changements ont été inclus dans les amendements proposés au RA de base et au RAA pour les gTLD afin d'ajouter des obligations contractuelles liées au RDAP (6 septembre 2022) que le GAC a accueilli dans ses commentaires (16 novembre 2022). Ces amendements ont été récemment approuvés par le Conseil d'administration de l'ICANN (30 avril 2023) et devraient entrer en vigueur le 3 février 2024.
    Le 28 février 2024, l'ICANN a annoncé que le **DAAR devait être remplacé par une nouvelle plateforme, « Domain Metrica de l'ICANN »**, pour fournir un ensemble étendu d'indicateurs et de métadonnées sur les noms de domaine, y compris la concentration de l'utilisation malveillante du DNS dans les registres et les bureaux d'enregistrement des gTLD, les scores de risque d'abus, la catégorisation de la malveillance et d'autres informations liées au DNS. Selon une mise à jour sur l'état d'avancement du projet (22 octobre 2024), le premier module fournissant des données sur la concentration de l'utilisation malveillante du DNS a fait l'objet d'une

[19] Au cours d'un appel du GAC sur les questions relatives à l'utilisation malveillante du DNS (24 février 2021), l'organisation ICANN a fourni des mises à jour sur les activités de l'OCTO liées à l'utilisation malveillante du DNS, qui ont inclus 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 les mises à jour sur DAAR, DNSTICR, DSFI, KINDNS, et les efforts de l'OCTO dans le domaine de la formation et du renforcement des capacités dans le monde entier.

[20] Plusieurs parties prenantes et initiatives de l'ICANN ont commenté les limites du DAAR, en particulier une lettre du Groupe de travail anti-abus pour la messagerie, les programmes malveillants et les mobiles (M3AAWG) à l'organisation ICANN (5 avril 2019) et le rapport préliminaire de l'équipe de révision de la 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).

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

étape de test pilote et devrait être ouvert à tous les registres et bureaux d'enregistrement avant l'ICANN81, au cours de laquelle la plateforme sera présentée à la communauté de l'ICANN lors d'une séance de mise à jour de l'utilisation malveillante du DNS le 13 novembre 2024. Pour de plus amples informations, n'hésitez pas à consulter la foire aux questions (FAQ) du projet.

- L'OCTO de l'ICANN a soutenu le **Groupe d'étude technique chargé de l'initiative de facilitation de la sécurité du DNS**, créé en mai 2020 dans le cadre de la mise en œuvre du plan stratégique pour les exercices fiscaux 2021 à 2025, dans le but de *« réfléchir à ce que l'ICANN peut et devrait faire pour augmenter le niveau de collaboration et d'engagement avec les parties prenantes de l'écosystème du DNS afin d'améliorer le profil de sécurité du DNS »*. Son rapport final (15 octobre 2021) a été publié après 18 mois de délibérations. L'organisation ICANN a indiqué au GAC (16 février 2022) qu'elle travaillait à l'élaboration 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'ICANN[22].
- Un nouveau projet, supervisé par l'OCTO de l'ICANN, Analyse inférentielle des domaines enregistrés à des fins malveillantes (INFERMAL), vise à **analyser systématiquement les préférences des cybercriminels, y compris l'utilisation des noms de domaine de certains bureaux d'enregistrement par rapport à d'autres**, et les mesures possibles pour atténuer les activités malveillantes dans les domaines de premier niveau (TLD). Ce projet découle en partie des données recueillies dans l'analyse statistique de l'utilisation malveillante du DNS dans les gTLD (9 août 2017)[23], suggérant que les acteurs malveillants peuvent préférer les bureaux d'enregistrement qui offrent des prix d'enregistrement réduits, acceptent des méthodes de paiement spécifiques, offrent des interfaces de programmation d'application (API) gratuites pour les enregistrements groupés ou éviter les bureaux d'enregistrement qui exigent certaines informations dans le processus d'achat.
  Dans une mise à jour pré-ICANN78 (25 octobre 2023), il a été indiqué que l'équipe de recherche prévoyait « *d'effectuer une analyse des mesures de sécurité identifiées qui aident à atténuer l'utilisation malveillante du DNS »* et avait l'intention de « *résumer une étude sur la rapidité avec laquelle les noms de domaine abusifs sont suspendus une fois que les opérateurs sont informés de l'abus* ». Elle s'attendait à ce qu'un rapport final « *sous la forme d'un document de recherche* » soit partagé d'ici

[22] Recommandation E5 *Réponse à l'incident* du rapport final du DSFI-TSG (groupe d'étude technique sur l'initiative de facilitation de la sécurité du système des noms de domaine) *(13 octobre 2021)* : « *L'organisation ICANN devrait, 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 devrait comprendre la gestion de l'intervention en cas d'incident ainsi que le partage protégé d'informations relatives aux menaces et aux incidents ».*

[23] Cette étude a été réalisée dans le cadre de la révision de la CCT et un commentaire du GAC (19 septembre 2017) a été soumis sur ce rapport.

septembre 2024 et que des « *meilleures pratiques pour atténuer efficacement les abus* » soient proposées. Une mise à jour sur ce projet est prévue lors de l'ICANN81 dans une séance de mise à jour sur l'utilisation malveillante du DNS qui se tiendra le 13 novembre 2024.

- Pour ce qui est de **l'application de la 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 établies 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 travaille aussi en étroite collaboration avec l'OCTO pour identifier des menaces à la sécurité du DNS [...] et les relier aux 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 des opérateurs de registre et des bureaux d'enregistrement qui affichent un nombre disproportionné de menaces à la sécurité du DNS. En cas d'échec du 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 **audit de conformité contractuelle** préalable des opérateurs de registre axé **sur l'utilisation malveillante de l'infrastructure du DNS** achevé en juin 2019[24], l'ICANN a présenté (le 24 août 2021) les résultats de l'audit sur **la conformité des bureaux d'enregistrement aux obligations en matière d'atténuation des risques liés à la sécurité du DNS** : 126 bureaux d'enregistrement (gérant plus de 90 % de tous les domaines enregistrés dans les gTLD) ont été audités ; 111 bureaux d'enregistrement n'ont pas été entièrement conformes aux exigences relatives à la réception et au traitement des rapports d'abus du DNS (articles 3.18.1 à 3.18.3 du RAA) ; et 92 bureaux d'enregistrement ont pris des mesures pour devenir entièrement conformes.
  - **Une nouvelle série d'audits pour 28 opérateurs de registre** gTLD[25] exploitant des gTLD n'ayant pas été précédemment audités dans le cadre d'un audit standard complet et qui ont obtenu le taux d'abus le plus élevé comme signalé par les listes noires de réputation publiquement disponibles (à l'exception du spam), a été annoncée le 13 avril 2022 et a conclu avec la publication du rapport d'audit le 16 septembre 2022. Le GAC a examiné les conclusions de sa séance plénière sur l'utilisation malveillante du DNS lors de l'ICANN75 (20 septembre 2022).

[24] Voir le 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).

[25] .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) .Рус (Xn--p1acf)

- Dans un Rapport d'audit ultérieur des bureaux d'enregistrement (22 juin 2023) relatif à **15 bureaux d'enregistrement « *représentant 7 familles de bureaux d'enregistrement comprenant 619 bureaux d'enregistrement* » basés dans 8 pays**, totalisant 83 millions de noms de domaine sous gestion (voir la liste à la p.17). 40 % des personnes auditées ont pu résoudre les « constatations initiales », tandis que 53 % ne les ont pas résolues et « *mettent en œuvre les changements nécessaires* » pour résoudre les problèmes en suspens (voir p. 10 à 14).
- Dans un rapport sur l'audit de conformité des registres effectué ultérieurement (22 janvier 2024) impliquant **19 opérateurs de registre,** non audités précédemment, avec un score d'abus DAAR supérieur à 0 % (voir la liste à la p.11), le département chargé de la conformité de l'ICANN a indiqué que « *neuf (9) des 19 registres (47 %) ont reçu un rapport d'audit sans résultats préliminaires. Deux (2) des 19 registres (11 %) qui ont reçu un rapport final avaient des résultats préliminaires notés dans leur rapport préliminaire et ont été en mesure de les résoudre entièrement avant l'achèvement de l'étape de remédiation* » et que « *huit (8) des 19 registres restants (42 %) ont complété l'audit avec des lacunes notées, car ils n'ont pas été en mesure de résoudre entièrement leurs résultats préliminaires avant l'achèvement de l'étape de remédiation* »
- Dans un rapport d'audit de conformité des bureaux d'enregistrement (20 août 2024) de **62 bureaux d'enregistrement totalisant plus de 25 millions de noms de domaine sous gestion**, l'ICANN a rapporté que : « *Dix-huit bureaux d'enregistrement n'ont pas été en mesure de résoudre entièrement leurs résultats préliminaires avant la fin de l'audit* » et ont souligné que les lacunes les plus fréquentes étaient liées aux dispositions requises dans les contrats avec les titulaires de nom de domaine (79 % des bureaux d'enregistrement déficients), au champ requis dans les résultats du WHOIS (43 %), aux renseignements requis sur le site Web du bureau d'enregistrement (40 % à 38 %), à la non-publication des procédures des bureaux d'enregistrement pour gérer les rapports d'abus (34 %) et à l'absence de conditions requises pour les services d'anonymisation et d¡enregistrement fiduciaire (24 %).

- **Enquête sur les efforts 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 inclus la prise en compte des pratiques d'atténuation de l'utilisation malveillante du DNS par les ccTLD afin d'éclairer les normes contractuelles renforcées dans l'espace des gTLD. En particulier, le plan de travail le plus récent du PSWG pour 2023-2024 comprend l'axe de travail 1.3 « *examiner et identifier les meilleures pratiques des ccTLD en vue de leur adoption dans l'espace des gTLD* » :
    - *Examiner et évaluer les meilleures pratiques des ccTLD pour atténuer les menaces à la sécurité, comme les politiques de prédiction de l'utilisation malveillante, de validation et de vérification des titulaires de nom de domaine, en vue d'identifier les approches*

pratiques et réalisables possibles et d'examiner comment elles peuvent éclairer les normes contractuelles renforcées dans l'espace des gTLD.

- Précédemment, les opérateurs de ccTLD du monde entier ont informé le GAC dans un séminaire en ligne pré-ICANN69 (4 juin 2020) sur les leçons qu'ils ont apprises de leurs opérations pendant la crise du 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, en définitive, aider les gestionnaires de ccTLD dans leurs démarches visant à atténuer l'impact de l'utilisation malveillante du DNS* », tout en notant que « *conformément à 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* ».
- Lors de l'atelier de renforcement des capacités du GAC de l'ICANN76 (11 mars 2023), le DASC a présenté au GAC ses premières conclusions sur leurs pratiques pour atténuer l'utilisation malveillante du DNS suite à une enquête qu'il a menée entre septembre et novembre 2022 couvrant environ 100 ccTLD. La présentation a examiné les 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 l'utilisation malveillante du DNS est détectée (avis aux titulaires de nom de domaine, 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 public d'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.).
- Au cours de l'ICANN78, le DASC de la ccNSO a rejoint la discussion plénière du GAC sur l'atténuation de l'utilisation malveillante du DNS et a discuté des prochaines étapes de l'étude des mesures contre l'utilisation malveillante du DNS et des outils d'atténuation dans les ccTLD.
- La deuxième édition de l'enquête mondiale du DASC de la ccNSO sur les pratiques

d'atténuation de l'utilisation malveillante du DNS dans les ccTLD a été menée entre août et septembre 2024. Il est prévu qu'un premier ensemble de résultats soit présenté lors d'une mise à jour par le DASC de la ccNSO lors de l'ICANN81, le mercredi 13 novembre 2024 à 10h15 UTC / 13h15 heure locale.

Principaux documents de référence

- SSAC Rapport SAC115 (19 mars 2021), une proposition pour une approche interopérable pour aborder la gestion des abus dans le DNS et un récent séminaire en ligne pré-ICANN81 GAC sur l'atténuation de l'utilisation malveillante du DNS (4 octobre 2024) qui a fourni l'état d'avancement de la mise en œuvre des recommandations du SSAC.
- Nouveaux rapports mensuels du département de la conformité contractuelle de l'ICANN sur l'utilisation malveillante du DNS (depuis avril 2024)
- Commentaires du Conseil d'administration de l'ICANN sur des questions d'importance dans le communiqué de Kigali de l'ICANN80
  (15 octobre 2024)
- Commentaires du Conseil d'administration de l'ICANN sur des questions d'importance dans le communiqué de San Juan de l'ICANN79
  (9 mai 2024)
- Sommet des parties contractantes (6 au 9 mai 2024) et enregistrements des séances publiques.
- Amendement au contrat de registre, amendement au contrat d'accréditation de bureau d'enregistrement et avis connexes :conformité avec les obligations en matière d'utilisation malveillante du DNS dans les contrats d'accréditation de bureau d'enregistrement et de registre (publié le 5 février 2024 et entré en vigueur le 5 avril 2024).
- Résolution du Conseil d'administration de l'ICANN (21 janvier 2024) approuvant les amendements aux contrats de registre et de bureau d'enregistrement en matière d'utilisation malveillante du DNS.
- Résolution du Conseil d'administration de l'ICANN (10 septembre 2023) basée sur l'évaluation de l'organisation ICANN de la révision de la CCT et de la SSR2 en cours concernant l'atténuation de l'utilisation malveillante du DNS
- Rapport sommaire des commentaires publics de l'organisation ICANN (1er août 2023) sur la procédure de commentaires publics liée aux amendements proposés aux contrats de registre et de bureau d'enregistrement concernant l'utilisation malveillante du DNS
- Commentaires du GAC (17 juillet 2023) sur les amendements proposés aux contrats de registre et de bureau d'enregistrement concernant l'utilisation malveillante du DNS
- Rapport d'audit du département chargé de la conformité contractuelle sur la série de novembre 2022 (22 juin 2023)

- Amendements au RA de base et au RAA pour les gTLD afin d'ajouter des obligations contractuelles liées au DNS (29 mai 2023)
- Annonce de l'analyse inférentielle des domaines enregistrés à des fins malveillantes (INFERMAL) (25 avril 2023)
- Rapport au conseil de la GNSO de la petite équipe de la GNSO sur l'utilisation malveillante du DNS (7 octobre 2022)
- Rétrospective des quatre dernières années : une brève révision de l'utilisation malveillante du DNS par l'organisation ICANN (22 mars 2022)
- Étude de la Commission européenne sur l'utilisation malveillante du DNS et son Annexe technique (31 janvier 2022)
- Rapport final de la révision de la SSR2 (25 janvier 2021) et commentaires du GAC y afférents (8 avril 2021)

Gestion des documents

Titre	ICANN81 - Document d'information du GAC - Atténuation de l'utilisation malveillante du DNS
Distribution	Membres du GAC (avant la réunion) et public en général (après la réunion)
Date de distribution	Version 1 : 25 octobre 2024