ICANN | GAC
Governmental Advisory Committee

ICANN 77
WASHINGTON, D.C.

Atténuation de l'utilisation malveillante du DNS

Séance 8

Table des matières

Objectifs de la séance

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

Proposition des dirigeants pour la ligne d'action du GAC

1. **Envisager l'élaboration d'un commentaire du GAC sur les modifications proposées aux contrats de registre et de bureau d'enregistrement concernant l'utilisation malveillante du DNS en tenant compte des discussions au cours de l'atelier de renforcement des capacités du GAC avant l'ICANN77** (qui se tiendra le dimanche 11 juin), **de la contribution du Groupe de travail sur la sécurité publique du GAC (PSWG), ainsi que la contribution de la communauté de l'ICANN dans son ensemble.** Les modifications proposées ont été récemment publiées à la suite des négociations entre l'ICANN et les parties contractantes depuis la fin de 2022[1]. Dans le Communiqué de La Haye (20 juin 2022), le GAC a déclaré que « *l'organisation ICANN est particulièrement bien placée pour recevoir les contributions de la communauté de l'ICANN en*

[1] Voir le blog du PDG de l'ICANN « L'ICANN et les parties contractantes négocient l'amélioration des exigences en matière d'utilisation malveillante du DNS » du 18 janvier 2023 et la procédure de consultation publique sur les amendements aux contrats de registre et de bureau d'enregistrement de base pour modifier les obligations contractuelles en matière d'utilisation malveillante du DNS (29 mai 2023)

matière de politique publique et pour négocier les mises à jour des contrats de registre et de bureau d'enregistrement standard ».

2. **Discuter de la portée de l'élaboration de politiques souhaitables pour améliorer la prévention et l'atténuation de l'utilisation malveillante du DNS**, suite à la 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[2].

3. **Examiner l'état d'avancement des recommandations relatives à l'atténuation de l'utilisation malveillante du DNS** , en particulier dans le rapport final de la révision de la CCT (8 septembre 2018) et le rapport final de la révision de la SSR2 (25 janvier 2021).

Situation actuelle et faits récents

- **Propositions de modification 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**, tels que 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 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

[2] 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 » le 25 avril 2023

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

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 sur 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 novembre 2022, les groupes des représentants des opérateurs de registre et des bureaux d'enregistrement ont signalé leur **volonté de « *poursuivre les améliorations possibles aux obligations en matière d'utilisation malveillante du DNS* *contenues dans [leurs] contrats respectifs avec l'ICANN* ». Le 30 novembre 2022, l'organisation ICANN a répondu que l'organisation*« s'aligne sur les propositions de lignes directrices énoncées dans [la] lettre pour toute négociation »*. Ces *lignes directrices* ont été fournies dans la correspondance des parties contractantes à l'ICANN comme suit :
  - *Les nouvelles dispositions seront axées sur l'utilisation malveillante du DNS, tel que cela est défini dans les contrats de l'ICANN existants, et renforcé par la petite équipe de la GNSO consacrée à l'utilisation malveillante du DNS ;*
  - *Les modifications ne comprendront ni des questions relatives aux abus de contenu du site Web ni à l'accès aux données d'enregistrement ; et*
  - *Toute nouvelle disposition [...] ne cherche pas à imposer des exigences de passage à l'un ou l'autre des groupes.*
- 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 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 de perturber et/ou d'atténuer l'utilisation malveillante du système de 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 récent (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 espérant que cela « *aide l'équipe de conformité contractuelle de l'ICANN dans ses*

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

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 la communauté de l'ICANN « *de discuter et de déterminer si d'autres obligations sont requises par le biais d'un processus d'élaboration de politiques ».* **La PDG de l'ICANN a pour objectif de « *partager des versions préliminaires avec la communauté avant l'ICANN77* ».**

- 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, pour ajouter une obligation claire afin que les opérateurs de registre et les bureaux d'enregistrement atténuent l'utilisation malveillante du DNS, sera un élément de construction 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* ».
- En vue d'une mise à jour des négociations en cours par les parties contractantes, 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 meilleure clarté et une meilleure applicabilité, **ainsi que les domaines possibles pour les nouvelles dispositions contractuelles** comme discuté 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.**
- Dans le Communiqué de Cancun de l'ICANN76 (20 mars 2023), le GAC a encouragé les négociations en cours pour « *procéder rapidement* » 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 du GAC à contribuer à un futur commentaire du GAC sur les modifications attendues des contrats de registre et de bureau d'enregistrement :

- Le 1er séminaire en ligne concernant le renforcement des capacités du GAC pré-ICANN77 sur l'utilisation malveillante du DNS (4 mai 2023) a discuté sur ce qui suit :
  - Quand traiter l'utilisation malveillante au niveau du DNS
  - Un aperçu et des exemples concrets les programmes malveillants, les réseaux zombies, l'hameçonnage, le dévoiement et le spam
  - Le rôle de l'ICANN
  - Les rôles des opérateurs de registre et des bureaux d'enregistrement
  - Le rôle du GAC
- Le 2er séminaire en ligne sur le renforcement des capacités du GAC pré- ICANN77 sur l'utilisation malveillante du DNS (22 mai 2023) a discuté sur ce qui suit :
  - L'aperçu des négociations contractuelles et du processus de consultation publique
  - Le développement des commentaires publics du GAC – processus et calendrier

- **L'organisation ICANN a lancé une procédure de commentaires publics** sur les amendements aux contrats de base des opérateurs de registre et des bureaux d'enregistrement pour modifier les obligations contractuelles en matière d'utilisation malveillante du DNS (29 mai 2023) qui devaient être présentés 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 sont utilisés pour l'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.
- Au cours de l'ICANN77, **le GAC devrait discuter de ces amendements** dans au moins deux contextes **pour préparer un commentaire du GAC** (dont l'échéance est fixée au 13 juillet 2023) :
  - L'Atelier sur le renforcement des capacités du GAC pré- ICANN77 sur l'utilisation malveillante du DNS(dimanche 11 juin)
  - Discussion du GAC sur l'utilisation malveillante du DNS (mercredi 14 juin)

- **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**. Au cours de la réunion bilatérale entre le GAC et la GNSO à l'ICANN72, comme indiqué dans le procès-verbal 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, que le GAC est intéressé à faire avancer les discussions communautaires, favoriser les progrès et la convergence des points de vue avant le lancement de nouveaux gTLD » et a ajouté que « le GAC se réjouit à la perspective de convenir de la manière de traiter les discussions à l'échelle de la communauté sur l'atténuation de l'utilisation malveillante du DNS (un PDP, CCWG, etc.)*»
    - Le 31 janvier 2022, le conseil de la GNSO a formé la **petite équipe du conseil 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 la réponse du GAC (4 avril 2022) à la demande de la GNSO pour que la communauté contribue à l'élaboration de la politique de lutte contre l'utilisation malveillante du DNS, la présidence du GAC a suggéré que, à la lumière du fait que « *les efforts communautaires en cours peuvent produire des initiatives et des résultats bénéfiques pouvant éviter la nécessité d'un PDP* », *« à ce moment [...] la poursuite d'un exercice d'établissement de la portée du PDP peut être prématurée* ».
    - 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[5].

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

- **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 étroitement délimitée** (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 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 le Rec. 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 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****, 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 lutte contre l'utilisation malveillante du DNS a exprimé son soutien pour les approches fondées sur les paiements pour lutter contre l'utilisation malveillante du DNS, et a proposé qu'il serait utile « *d'encourager les bureaux d'enregistrement à enquêter sur tous les domaines dans un compte client identifié comme malveillant* »** dans le cadre « d'*options raisonnables et pratiques disponibles pour les bureaux d'enregistrement qui réduiront l'utilisation malveillante du DNS [...] en ce moment* », en plus de *« friction au moment de l'enregistrement »***.**
- Sur la base de commentaires supplémentaires reçus des parties contractantes[6], 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 :

[6] 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)

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

- **État et perspectives de mise en œuvre des recommandations des révisions spécifiques relatives à l'interruption de l'utilisation malveillante du DNS**[7]
    - **La révision de la SSR2** a formulé 63 recommandations dans son rapport final (25 janvier 2020) 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 projets de recommandations 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[8] 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).
        - À ce jour, selon le dernier rapport trimestriel sur la révision spécifique de l'ICANN (21 février 2023), basé sur 3 résolutions du Conseil d'administration de l'ICANN (22 juillet 2021, 1er mai 2022 et 16 novembre 2022) : **23 recommandations** sont maintenant **approuvées** (dont 14 sous réserve de l'établissement des priorités pour la mise en œuvre), **30 ont été rejetées** et **10 restent en attente** d'un examen plus approfondi de la part du Conseil d'administration.
        - **7 recommandations relatives à l'utilisation malveillante du DNS en attente** - **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*) - **sont censées être considérées par le Conseil d'administration de l'ICANN au cours du 3e trimestre 2023**. Dans la fiche de suivi pertinente (22 juillet 2021), le Conseil d'administration de l'ICANN a reconnu « *les efforts étendus de la communauté et de l'organisation ICANN faits actuellement autour des menaces à la sécurité du DNS* » et a demandé à l'organisation ICANN « *d'évaluer comment ce regroupement de recommandations, ainsi que d'autres recommandations qui se rapportent aux menaces à la sécurité du DNS devraient être*

[7] Le statut de toutes les recommandations peut être consulté dans le rapport du premier trimestre 2023 (Q1) 2023 sur les révisions spécifiques de l'ICANN (31 mars 2023) à partir de la p.28, ainsi que d'autres documents à l'adresse suivante : https://www.icann.org/resources/reviews/specific-reviews/whois

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

pris en considération de manière coordonnée » et informer la décision du Conseil sur les prochaines étapes.

- **Dans sa récente discussion sur les négociations en cours concernant les négociations contractuelles sur l'utilisation malveillante du DNS, le PSWG du GAC a discuté[9] 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'abus 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, de la confiance et du choix des consommateurs** (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] »*.
  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[10] :
  - **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 la mise en œuvre est complète** conformément à sa documentation de mise en œuvre au 14 septembre 2022.
  - **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*

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

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

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** selon le 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 modifications pour inclure des dispositions visant à prévenir l'utilisation systémique des opérateurs de registre ou des bureaux d'enregistrement spécifiques pour l'utilisation malveillante du DNS, et établir des seuils d'abus pour les déclencheurs automatiques de conformité) sont* actuellement **en attente** en vertu de la fiche de suivi du Conseil d'administration du 1er mars 2019. Et, compte tenu des discussions communautaires en cours sur l'utilisation malveillante du DNS, **devraient être examinées par le Conseil d'administration de l'ICANN au cours du troisième trimestre (Q3) 2023.** Entre-temps, l'organisation ICANN traite ces recommandations ainsi que d'autres recommandations et avis sur les révisions spécifiques au Conseil.

- **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 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 de l'ODP du SSAD, conformément à la documentation de mise en œuvre (11 octobre 2022)

- **Mesures et initiatives visant à atténuer l'utilisation malveillante du DNS par les registres et les bureaux d'enregistrement**
  - Le 27 mars 2020, l'organisation ICANN a 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**[11]. 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.

[11] 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).

- **Dans le contexte de la crise du COVID-19, les parties contractantes et les parties prenantes de la sécurité publique** ont rendu compte[12] de leur collaboration afin de faciliter les rapports, leur révision et leur renvoi à la juridiction compétente via l'adoption d'un formulaire normalisé et l'établissement d'un point de contact unique pour les autorités compétentes. Ces efforts 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 (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 »*. L'Institut de lutte contre l'utilisation malveillante du DNS 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 l'Institut de lutte contre l'utilisation malveillante du DNS à présenter son nouvel outil Net Beacon (anciennement connu sous le nom d'**Outil centralisé de signalement des cas d'utilisation malveillante**), 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.

- **Réponse multidimensionnelle de l'organisation ICANN[13] (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.
  - **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

12 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.

13 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.

incidents, et mettent au point des systèmes et des outils permettant de détecter, d'analyser et de signaler l'utilisation malveillante du DNS[14].

- En réponse à la crise du COVID-19, l'OCTO a développé l'outil de **signalement et de collecte d'informations sur les menaces à la sécurité des noms de domaine (DNSTICR)** pour aider à identifier les noms de domaine liés au COVID-19 et utilisés à des fins d'abus et pour pouvoir partager les données avec les parties concernées. Le GAC a 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.
- Grâce à sa **plateforme de signalement des cas d'utilisation malveillante des noms de domaine (DAAR)**, l'ICANN rend compte tous les mois, depuis janvier 2018, de l'enregistrement de noms de domaine et des menaces à la sécurité observées dans le DNS[15]. En octobre 2021, l'organisation ICANN et le Groupe des représentants des opérateurs de registre ont fait part de leur accord de principe visant[16] 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 modifications proposées aux RA et RAA de base 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), et qui devraient faire l'objet d'une période de vote de 60 jours avant la considération du Conseil d'administration de l'ICANN.
- 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 à l'issue de 18 mois de délibérations. L'organisation ICANN a indiqué au GAC (16 février 2022) qu'elle travaillait 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

[14] 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.

[15] 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).

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

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[17].

- 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)[18], suggérant que les acteurs malveillants peuvent préférer les bureaux d'enregistrement qui fournissent 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.

- 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 contractuelles prévues dans les politiques et les contrats de l'ICANN, en particulier le contrat de registre (RA) et le contrat d'accréditation de bureau d'enregistrement (RAA). Ce département 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 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 de l'opérateur de registre axé sur l'utilisation malveillante de l'infrastructure du DNS qui s'est achevé en juin 2019[19] , l'ICANN a présenté (le 24 août 2021) les résultats de l'audit sur **la conformité**

---

17 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* ».

18 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.

19 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).

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.

- Le 9 mars 2022, l'ICANN a annoncé le déploiement de nouveaux rapports améliorant la visibilité des volumes et des tendances de plaintes.
- **Une nouvelle série d'audits pour** 28 opérateurs de registre gTLD[20] 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 tel que 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).
- Dans le cadre de la semaine de préparation pour l'ICANN76, le département chargé de la conformité contractuelle a fait état de ses activités (28 février 2023)

[20] .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)

Principaux documents de référence :

- Amendements au RA et au RAA de base pour les gTLD afin d'ajouter des obligations contractuelles liées au DNS (29 May 2023)
- Annonce de l'analyse inférentielle des domaines enregistrés à des fins malveillantes (INFERMAL) (25 avril 2023)
- Premier rapport trimestriel (Q1) 2023 sur les révisions spécifiques de l'ICANN (31 mars 2023)
- Quatrième rapport trimestriel (Q4) 2022 sur les révisions spécifiques de l'ICANN (21 février 2023)
- Communication des RySG – RrSG sur les obligations d'interruption/d'atténuation de l'utilisation malveillante du DNS (4 novembre 2022)
- Rapport au conseil de la GNSO de la Petite équipe de la GNSO sur l'utilisation malveillante du DNS (7 octobre 2022)
- Réponse du GAC à la demande de la GNSO concernant les commentaires de la communauté sur l'élaboration de politiques en matière d'utilisation malveillante du DNS (4 avril 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 fiche de suivi des mesures prises par le Conseil d'administration (8 avril 2021)
- Annonce et rapport de l'ICANN (24 août 2021) concernant l'audit sur la conformité des bureaux d'enregistrement aux obligations en matière d'atténuation des risques liés à la sécurité du DNS.
- Rapport SAC115 du SSAC (19 mars 2021), qui propose une approche interopérable pour traiter la gestion de l'utilisation malveillante du DNS

Gestion des documents

Titre	Document d'information du GAC sur l'ICANN77 - 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 : 31 mai 2023