ICANN | GAC
Governmental Advisory Committee

80 POLICY FORUM

Atténuation de l'utilisation malveillante du DNS

Séance 5

Sommaire

Objectifs de la séance

La séance plénière du GAC de l'ICANN80 sur l'utilisation malveillante du DNS vise à poursuivre l'examen, par le GAC, des initiatives entreprises par l'organisation ICANN et la communauté de l'ICANN pour prévenir et atténuer l'utilisation malveillante du DNS. Cet examen englobe les résultats obtenus et les prochaines étapes concernant les nouvelles responsabilités en matière de lutte contre l'hameçonnage, les logiciels malveillants, les réseaux zombies, le dévoiement et le courrier indésirable, incombant aux opérateurs de registres et bureaux d'enregistrement de noms de domaine de l'ICANN.

La séance comprendra une discussion sur les tendances actuelles et les perspectives de l'utilisation malveillante du DNS en Afrique, ainsi qu'une réflexion sur les effets potentiels, pour la région, des nouvelles obligations des parties contractantes quant à la perturbation/atténuation de l'utilisation malveillante du DNS dans les gTLD. Le panel comprendra des intervenants d'autorités de régulation nationales, d'autorités de cybersécurité et d'organisations africaines.

Proposition de la direction sur la ligne d'action du GAC

1. Discuter des tendances actuelles et des perspectives de l'utilisation malveillante du DNS en Afrique et réfléchir aux effets potentiels, pour la région, des nouvelles obligations des parties contractantes quant à la perturbation/atténuation de l'utilisation malveillante du DNS dans les gTLD. La discussion et la réflexion s'articuleront autour d'une série de questions proposées par les responsables thématiques du GAC sur l'utilisation malveillante du DNS.

Tendances et cas d'utilisation malveillante du DNS

1. Pourriez-vous partager des données/informations sur les tendances de l'utilisation malveillante du DNS dans votre pays/région, et sur l'évolution de ces tendances au fil du temps ?
2. Constatez-vous un schéma particulier d'utilisation malveillante du DNS, spécifique à la région africaine ?
    a. Pourriez-vous citer (le cas échéant) un cas de ce type ?
3. Pourriez-vous décrire (le cas échéant) quelques affaires [pénales] portant sur l'utilisation malveillante du DNS dans votre pays (ou région) qui vous frustrent, en tant qu'organisme public ?
    a. Pourriez-vous citer (le cas échéant) quelques cas qui ont suscité une forte attention politique ?
4. Selon votre expérience, quelle proportion de cette utilisation malveillante du DNS est exécutée à l'aide de domaines enregistrés dans des ccTLD africains versus des domaines enregistrés dans des gTLD ?
5. Voyez-vous des différences dans la manière dont les opérateurs de registre du ccTLD traitent cette utilisation malveillante du DNS, par rapport aux opérateurs de registre gTLD ?

Politiques et solutions

6. À votre connaissance, quelles mesures prises par les opérateurs DNS africains ont été les plus efficaces pour atténuer l'utilisation malveillante du DNS ?
7. Pourriez-vous citer (le cas échéant) un ou plusieurs exemples de politiques (ou de mesures réglementaires) prises par des opérateurs de registres ccTLD pour lutter contre l'utilisation malveillante du DNS ?
8. Dans les catégories relatives à l'utilisation malveillante du DNS, y a-t-il une priorité de politique visant à prévenir/atténuer l'utilisation malveillante du DNS dans votre pays (ou région) ?
    a. Pourriez-vous nous en expliquer les raisons, si possible ?

Prochaines étapes pour le GAC et l'ICANN

9. Quels effets positifs pensez-vous que les nouvelles dispositions contractuelles de l'ICANN auront sur les activités d'utilisation malveillante du DNS dans la région africaine *?*
10. Selon vous, sur quoi le GAC devrait-il se concentrer lorsqu'il soutient la communauté de l'ICANN dans sa réflexion sur l'utilisation malveillante du DNS ? Quelles priorités le GAC devrait-il inscrire à son ordre du jour ?
11. Selon vous, quelles améliorations faut-il apporter à la détection et au signalement des domaines exploités à des fins malveillantes et à l'atténuation de ce phénomène ? Quel serait le rôle de l'ICANN dans ces améliorations ?

2. **Continuer à examiner la portée de l'élaboration souhaitée d'une politique visant à renforcer davantage la prévention et l'atténuation de l'utilisation malveillante du DNS**, à la lumière des éléments suivants :

    - la recommandation de la petite équipe de la GNSO sur l'utilisation malveillante du DNS (7 octobre 2022) **d'engager un processus d'élaboration de politique sur les enregistrements malveillants**, et les négociations contractuelles potentielles sur cette question, qui devraient finalement être guidées par les résultats du projet INFERMAL (Inferential Analysis of Maliciously Registered Domains), afin d'explorer les principaux facteurs qui motivent l'enregistrement malveillant de noms de domaine[1].
    - la déclaration du GAC figurant dans ses commentaires (17 juillet 2023) sur les modifications proposées, spécifiant que *« les futurs travaux sur l'utilisation malveillante du DNS menés avec la communauté multipartite […] devraient inclure des processus d'élaboration de politiques (PDP) visant à mieux informer les RA et RAA mis à jour, ainsi que d'autres travaux sur les questions en suspens à traiter en amont de la prochaine série de candidatures pour les nouveaux gTLD » ;*
    - le Compte rendu sommaire des commentaires publics sur les nouvelles modifications (1er août 2023) dans lequel l'organisation ICANN fait remarquer que « *la communauté de l'ICANN aura l'occasion de discuter de ces obligations pour déterminer si d'autres sont nécessaires […]*. ***L'organisation ICANN et l'équipe de négociation de la Chambre des parties contractantes (CPH NT) appuient les commentaires du GAC selon lesquels, après l'adoption des modifications proposées, le travail devrait inclure des processus d'élaboration de politiques (PDP) pour informer davantage le RA de base et le RAA mis à jour*** *» ;*
    - les plans du Département en charge de la conformité contractuelle de l'ICANN (département conformité) quant à l'application des nouvelles modifications, comme exposés au GAC lors de l'ICANN79 :
        - réaliser un suivi spécifique et prioriser le traitement des plaintes soumises par les professionnels de l'application de la loi et de la cybersécurité ;
        - faciliter la soumission des plaintes valides, suffisamment étayées pour permettre une action rapide ;
        - inclure les nouvelles obligations relatives à l'utilisation malveillante du DNS dans le champ des futurs audits proactifs ;
        - à partir de juin 2024, produire et publier mensuellement un rapport dédié à l'application des nouvelles exigences relatives à l'utilisation malveillante du DNS ;
        - préparer un rapport spécifique sur l'application des nouvelles obligations à 6 mois (à publier au deuxième trimestre 2025) ;

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

- **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] que si les rapports du département conformité sont censés aider à mesurer l'effet des modifications sur l'utilisation malveillante du DNS, **c'est à la communauté qu'il incombera de mener un effort facilité et soutenu par l'ICANN pour déterminer les indicateurs et ensembles de données spécifiques qui permettront la mesure de cet effet.**

[2] Voir 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).

Situation actuelle et faits récents

- **Modifications apportées aux contrats de registre et de bureau d'enregistrement afin d'introduire des obligations plus strictes au titre de l'atténuation de l'utilisation malveillante du DNS**

  - Depuis l'ICANN66, **les dirigeants du Groupe de travail du GAC sur la sécurité publique ont informé ce dernier** sur la question de l'atténuation de l'utilisation malveillante du DNS[3], notamment **les mesures dont disposent les opérateurs de registre et les bureaux d'enregistrement pour prévenir ce phénomène**, en mettant l'accent sur le rôle des politiques d'enregistrement (en ce compris la vérification de l'identité) et des stratégies de tarification en tant que déterminants clés des niveaux d'utilisation malveillante dans un TLD donné. Ils ont également fait part au GAC des **possibilités qui s'offrent au Conseil d'administration de l'ICANN et à l'organisation ICANN de s'attaquer plus efficacement au phénomène**, à savoir les révisions au RA et au RAA, l'application des exigences existantes, la mise en œuvre des recommandations pertinentes de la révision de la CCT et de la SSR2 et celles concernant la politique relative aux fournisseurs de service d'enregistrement fiduciaire/d'anonymisation, l'amélioration de l'exactitude des données d'enregistrement et la publication de données plus détaillées sur les activités malveillantes.
  - Dans des communiqués qu'il a publiés ces dernières années, le GAC a souligné « ***la nécessité d'améliorer les exigences contractuelles pour traiter plus efficacement la question de l'utilisation malveillante du DNS*** » (communiqué du GAC de l'ICANN72, 1er novembre 2021) et a indiqué que « *l'amélioration des dispositions contractuelles pourrait être axée sur le signalement et le traitement des cas d'utilisation malveillante du DNS et sur la mise en œuvre des exigences contractuelles connexes* » (communiqué de La Haye, 20 juin 2022). Le GAC a également mis en exergue le fait que l'ICANN est « *particulièrement bien placée pour négocier des améliorations aux contrats existants* » et « *pour recevoir des commentaires publics de la communauté de l'ICANN* ».
  - Au cours de l'ICANN75, **la petite équipe de la GNSO sur l'utilisation malveillante du DNS s'est penchée sur les « lacunes dans l'interprétation et/ou l'application » des contrats actuels de l'ICANN**, comme le reflètent ensuite ses recommandations au conseil de la GNSO (7 octobre 2022).
  - Dans son communiqué de Kuala Lumpur (26 septembre 2022), le **GAC a rappelé son « *soutien à l'élaboration des dispositions contractuelles proposées, applicables à tous les gTLD et visant à améliorer les réponses à l'utilisation malveillante du DNS* »[4], *dont celles indiquées par la SSR2 et par la révision 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 formellement **notifié**

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

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

à l'ICANN l'ouverture de négociations visant respectivement à « *intégrer des exigences contractuelles de base à l'article 3.18 du RAA pour que les bureaux d'enregistrement perturbent et/ou atténuent l'utilisation malveillante du système de noms de domaine* » et à « *renforcer les obligations relatives à l'utilisation malveillante du DNS contenues dans [le contrat de registre]* ». Un récent billet de blog de la **PDG de l'ICANN** (18 janvier 2023), confirmant le travail en cours sur « ***définition d'obligations de base exigeant des opérateurs de registre et des bureaux d'enregistrement l'atténuation ou la perturbation de l'utilisation malveillante du DNS*** », a indiqué s'attendre à ce que ces obligations « *facilitent les efforts d'application que déploie le département conformité auprès des bureaux d'enregistrement ou opérateurs de registres qui ne s'attaquent pas adéquatement à l'utilisation malveillante du DNS* ». La PDG y mentionnait également que ce travail serait l'occasion, pour la communauté de l'ICANN, « *de se concerter pour évaluer la nécessité d'obligations supplémentaires par le biais d'un processus d'élaboration de politiques* ».

- Entre-temps, l'Unité constitutive des utilisateurs commerciaux (**BC)**, l'Unité constitutive des représentants de la propriété intellectuelle (**IPC**) de la GNSO et le Comité consultatif At-Large (**ALAC**) ont demandé (20 janvier 2023) que « *les contributions de la communauté soient dûment prises en compte, et de soutenir l'organisation ICANN dans son rôle établi de défenseur des besoins de la communauté et d'arbitre de l'intérêt public* ».
  Dans sa réponse (27 mars 2023), le Conseil d'administration de l'ICANN a affirmé que « *le Conseil d'administration de l'ICANN et l'organisation ICANN ont été à l'écoute de la communauté, ces dernières années, en ce qui concerne l'utilisation malveillante du DNS*. *L'adoption de* ***cette approche visant à apporter des améliorations ciblées aux contrats en introduisant l'obligation explicite pour les opérateurs de registre et les bureaux d'enregistrement d'atténuer l'utilisation malveillante du DNS sera une composante d'un parcours plus long qui envisage des discussions potentielles sur les politiques,*** *ouvertes à toute la communauté de l'ICANN,* ***et possiblement des négociations futures*** *entre le CPH et l'organisation ICANN* ».
- Lors d'une séance d'information pré-ICANN76 du GAC sur les négociations contractuelles concernant l'atténuation de l'utilisation malveillante du DNS (28 février 2023) [*connexion requise au site Web du GAC*], **les responsables thématiques du GAC ont discuté des améliorations possibles aux dispositions contractuelles existantes** en faveur d'une plus grande clarté et d'une meilleure application, **ainsi que des domaines envisageables pour de nouvelles dispositions contractuelles** telles que discutées par la communauté de l'ICANN (notamment par les révisions de la CCT et de la SSR2), **à savoir : les incitations financières et de réputation, les seuils d'utilisation malveillante et les déclencheurs de conformité, les meilleures pratiques et la centralisation du signalement de l'utilisation malveillante.**
- Lors de la réunion bilatérale du GAC avec le Conseil d'administration de l'ICANN pendant l'ICANN76, **le GAC a encouragé ce dernier à envisager l'organisation d'une séance d'écoute de la communauté de l'ICANN** concernant les négociations (voir p.11 du procès-verbal de la réunion du GAC de l'ICANN76).

- Dans son communiqué de Cancún de l'ICANN76 (20 mars 2023), le GAC a encouragé les négociations en cours *« à progresser rapidement »*, soulignant qu'il *« estime que* des ***efforts continus dans ce domaine seront nécessaires avant le lancement d'une deuxième série de nouveaux domaines génériques de premier niveau (nouveaux gTLD), notamment des améliorations supplémentaires aux obligations contractuelles et/ou des processus ciblés d'élaboration de politiques*** *».* En outre, le GAC a *recommandé aux « parties contractantes et à l'ICANN d'envisager, entre autres, des mesures proactives ainsi que des incitations positives pour les opérateurs de registre et les bureaux d'enregistrement, dans le cadre de futurs travaux sur l'atténuation ou la perturbation de l'utilisation malveillante du DNS* ».
- En préparation de l'ICANN77, le **Groupe de travail du GAC chargé des régions faiblement desservies** (USRWG) a organisé deux **séminaires Web** pour préparer les nouveaux arrivants et les représentants du GAC des régions faiblement desservies à contribuer à un commentaire sur les modifications attendues aux contrats de registre et de bureau d'enregistrement[5].
- **L'organisation ICANN a lancé une procédure de consultation publique** sur les modifications au RA et au RAA de base des gTLD. Ces modifications, qui visent à renforcer les obligations contractuelles relatives à l'utilisation malveillante du DNS (29 mai 2023), ont ensuite été présentées lors d'un séminaire Web organisé à l'occasion de la semaine de préparation à l'ICANN77 (30 mai 2023). Les diverses propositions de modification aux contrats de l'ICANN comprennent une **nouvelle obligation pour les parties contractantes de prendre rapidement des mesures d'atténuation appropriées à l'encontre des domaines pour lesquels elles disposent de preuves concrètes** d'utilisation malveillante du DNS. Outre les modifications contractuelles proposées, une version provisoire d'un avis de l'ICANN fournit une explication détaillée sur les nouvelles dispositions et définit les attentes quant à leur interprétation.
- À la suite des discussions qu'il a tenues au cours de l'ICANN77 sur les propositions de modification[6], le GAC a contribué par des commentaires (17 juillet 2023) à la procédure de consultation publique :
  - le GAC a jugé ces modifications « *opportunes et pertinentes » et a estimé qu'« elles constitueront, une fois adoptées, un premier pas important dans la lutte contre l'utilisation malveillante du DNS* » ;
  - le GAC a souligné que « *compte tenu de la menace permanente que représente l'utilisation malveillante du DNS pour les consommateurs et les secteurs public et privé »,* « *il est impératif que les contrats améliorés soient rapidement adoptés après la clôture de la procédure de consultation publique » ;*
  - **le GAC a manifesté son soutien « *général aux propositions de modification »,* tout**

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

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

en invitant *« l'organisation ICANN et le CPH NT à se pencher sur certaines questions liées au libellé des modifications »*. Il s'agit notamment de la définition de l'utilisation malveillante du DNS, des rapports et du suivi à effectuer par les parties contractantes, des conséquences en cas de non-respect, de la possibilité pour la communauté de l'ICANN de surveiller la mise en conformité, de la nécessité de mettre à jour périodiquement l'avis du Conseil d'administration et de la nécessité de s'attaquer à l'utilisation malveillante du DNS tant au sein qu'à l'extérieur de l'ICANN ;

- **le GAC s'est dit enthousiaste à l'idée de « *collaborer*** *avec la communauté multipartite,* ***après l'adoption des modifications, sur des travaux futurs*** *sur l'utilisation malveillante du DNS.* ***Ceux-ci devraient inclure des processus d'élaboration de politiques (PDP) visant à mieux informer le RA et le RAA mis à jour, ainsi que d'autres activités ciblant les questions encore en suspens,*** *à traiter en amont de la prochaine série de candidatures pour les nouveaux gTLD ».*

- Dans son Compte rendu sommaire des commentaires publics (1er août 2023), **l'organisation ICANN a indiqué que le vote des opérateurs de registre et des bureaux d'enregistrement se déroulera sur les modifications, telles qu'elles ont été initialement proposées.** Quant aux « *commentaires signalant que les propositions de modification ne suffisent pas pour relever le défi de l'utilisation malveillante du DNS* », *elle a fait observer que « l'organisation ICANN prend acte de ces commentaires et rappelle à la communauté que celle-ci aura l'occasion de discuter de ces obligations pour déterminer si d'autres sont nécessaires […].* ***L'organisation ICANN et l'équipe de négociation de la Chambre des parties contractantes (CPH NT) soutiennent les commentaires du GAC selon lesquels, après l'adoption des modifications proposées, le travail devrait inclure des processus d'élaboration de politiques (PDP) visant à mieux informer le RA de base et le RAA mis à jour*** *».*
- La période de vote des registres et des bureaux d'enregistrement sur les modifications s'est ouverte le 9 octobre 2023 et a duré 60 jours. Elle s'est conclue favorablement, les modifications ayant été approuvées par 80 % des bureaux d'enregistrement et 94 % des bureaux d'enregistrement[7].
- Le Conseil d'administration de l'ICANN a ensuite résolu d'approuver les modifications (21 janvier 2024), déterminant qu'« ***aucune autre révision aux propositions d'amendements globaux n'est nécessaire à la lumière des commentaires publics*** *et des résultats du vote ».*
- L'Amendement global aux contrats de registre, l'Amendement global aux contrats d'accréditation de bureau d'enregistrement et le bulletin d'information y afférant :Respect des obligations en matière d'utilisation malveillante du DNS prévues dans le Contrat d'accréditation de bureau d'enregistrement et le Contrat de registre ont

[7] Les résultats détaillés des votes sont disponibles à l'adresse suivante https://www.icann.org/resources/pages/global-amendment-2024-en

été publiés le 5 février 2024, avec prise d'effet le 5 avril 2024[8].

- Lors de la réunion de l'ICANN79, le département conformité a présenté au GAC ses plans concernant l'application des obligations, notamment :
  - assurer un suivi spécifique des plaintes soumises par les organismes d'application de la loi et les professionnels de la cybersécurité, et prioriser leur traitement ;
  - faciliter la soumission de plaintes valides, suffisamment étayées pour permettre une action rapide ;
  - inclure les nouvelles obligations relatives à l'utilisation malveillante du DNS dans le champ des futurs audits proactifs ;
  - publier un rapport dédié à l'application des nouvelles exigences relatives à l'utilisation malveillante du DNS, et le mettre à jour tous les mois, en y incluant des données telles que :
    - le nombre de plaintes reçues, ventilées par type d'utilisation malveillante du DNS ;
    - le nombre d'avis de conformité envoyés aux parties contractantes au titre des exigences en matière d'utilisation malveillante du DNS ;
    - le nombre de cas résolus avec les parties contractantes, et leurs issues, notamment si des mesures ont été prises par la partie contractante pour perturber l'utilisation malveillante du DNS ou y mettre fin ou si aucune mesure n'a été prise faute de données probantes ; et
    - le nombre de cas correspondant à des plaintes déposées par des organismes d'application de la loi sur le territoire du bureau d'enregistrement et résolues avec les parties contractantes, ainsi l'issue de ces cas.
  - D'ici le deuxième trimestre 2025, le département conformité prévoit d'élaborer un rapport plus détaillé sur l'application des exigences en matière d'utilisation malveillante du DNS au cours des six premiers mois de leur prise d'effet.
- Dans son communiqué de San Juan du GAC de l'ICANN79 (11 mars 2024), le GAC a déclaré qu'il *« suivra les rapports du département conformité sur l'application des exigences relatives à l'utilisation malveillante du DNS »* et qu'« *il reste une attente générale de voir des progrès notables avant la prochaine série de candidatures aux nouveaux gTLD »*.
- Dans ses commentaires sur les questions d'importance du communiqué de San Juan de l'ICANN79 (9 mai 2024), le Conseil d'administration de l'ICANN a déclaré : « ***le but poursuivi est que les rapports de conformité contribuent à mesurer l'effet des Amendements globaux relatifs à l'utilisation malveillante du DNS***. *Cependant, la* ***définition des indicateurs spécifiques et des ensembles de données qui permettront de mesurer un tel effet devrait être un effort mené par la communauté, et facilité et soutenu par l'ICANN*** *».* Il a aussi précisé qu'« *une équipe interdisciplinaire de*

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

l'organisation ICANN travaille à l'analyse des données pour déterminer la manière d'aborder ces efforts ».

- Lors du récent Sommet des Parties contractantes (6-9 mai 2024), celles-ci se sont entretenues sur la mise en œuvre des Amendements, et sur l'effet de ces derniers de leur point de vue. Il a été signalé que le sous-groupe de la CPH consacré à l'utilisation malveillante du DNS échange actuellement avec le département conformité sur la manière dont les modifications aux contrats sont en train d'être appliquées.

- **Perspectives d'élaboration de politique pour la prévention et l'atténuation de l'utilisation malveillante du DNS**
  - Comme il est indiqué dans le communiqué du GAC de l'ICANN69 (23 octobre 2020), « ***du point de vue du GAC, une véritable dynamique, propice à l'adoption de mesures concrètes, s'est créée*** *dans la mesure où la communauté a progressivement engagé un dialogue constructif afin de faire avancer les travaux dans un but commun, l'atténuation de l'utilisation malveillante du DNS. Suite aux recommandations de la CCT-RT et de la SSR2-RT, puis aux multiples séances intercommunautaires qui se sont tenues et enfin aux plus récents travaux portant sur un cadre de lutte contre l'utilisation malveillante du DNS,* ***le GAC estime à présent qu'il existe un soutien massif à l'adoption de mesures concrètes mettant en place les principales composantes d'une atténuation efficace de l'utilisation malveillante du DNS*** *».*
  - Avant même la réunion de l'ICANN68, **la direction du GAC a cherché à établir, en concertation avec la direction du conseil de la GNSO, un cadre de travail communautaire et d'élaboration de politiques possibles pour traiter le problème de l'utilisation malveillante du DNS.** Pendant la réunion bilatérale GAC-GNSO organisée dans le cadre de l'ICANN72, comme en fait état le procès-verbal de la réunion du GAC de l'ICANN72, la présidence du GAC a réitéré que l'utilisation malveillante du DNS « *est une question qui intéresse le GAC depuis longtemps et que le GAC souhaite faire avancer les discussions au sein de la communauté, de manière à favoriser les progrès et la convergence des points de vue avant le lancement des nouveaux gTLD* » et a ajouté que « *le GAC est impatient de trouver un accord sur la manière de gérer les discussions communautaires sur l'atténuation de l'utilisation malveillante du DNS (PDP, CCWG, etc.)* ».
  - Le 31 janvier 2022, le conseil de la GNSO a constitué une **petite équipe de la GNSO sur l'utilisation malveillante du DNS** qui devrait déterminer « *les efforts de politiques, le cas échéant, que le conseil de la GNSO devrait envisager de mettre en place afin de soutenir les travaux déjà en cours dans les différentes parties de la communauté et visant à lutter contre l'utilisation malveillante du DNS* ».
  - Dans son communiqué de La Haye (20 juin 2022), le GAC a déclaré que « ***tout PDP sur l'utilisation malveillante du DNS doit être défini de manière rigoureuse de manière à produire un résultat exploitable en temps voulu*** », ce à quoi le Conseil d'administration

de l'ICANN a répondu qu'il partageait cet avis et qu'il était prêt à soutenir la communauté de l'ICANN dans cette quête[9].

- Dans un rapport au conseil de la GNSO (7 octobre 2022), **la petite équipe de la GNSO a recommandé : le lancement d'un travail d'élaboration de politique à portée étroite portant sur les enregistrements malveillants** (recommandation 1), **un examen plus approfondi du rôle que joue l'enregistrement en masse dans l'utilisation malveillante du DNS** et des mesures déjà en place pour y remédier (recommandation 2), **l'incitation à la poursuite des travaux en vue d'un signalement plus facile, meilleur et exploitable** de l'utilisation malveillante du DNS (recommandation 3), et une éventuelle concertation entre les parties contractantes et le département conformité concernant ses conclusions sur les lacunes potentielles dans l'interprétation et/ou l'application des contrats actuels de l'ICANN (recommandation 4). Le conseil de la GNSO a procédé à la sensibilisation recommandée des parties contractantes concernant la recommandation 3 et des parties contractantes, de l'Institut de lutte contre l'utilisation malveillante du DNS et du département conformité de l'ICANN concernant la recommandation 2 (6 janvier 2023).
- **En ce qui concerne l'enregistrement en masse**, la réponse du département conformité de l'ICANN au conseil de la GNSO (22 février 2023) indique que « *les contrats et politiques de l'ICANN ne prévoient pas d'exigences ou de limitations liées à l'enregistrement en masse de noms de domaine. Par conséquent,* ***le département conformité de l'ICANN ne recueille pas et ne suit pas les informations sur les enregistrements en masse*** *et le rôle potentiel qu'ils peuvent jouer dans l'utilisation malveillante du système des noms de domaine (DNS) ».* La réponse du l'Institut de la lutte contre l'utilisation malveillante du DNS (24 février 2023) proposait que « ***des recherches devraient être menées pour déterminer l'ampleur de tout problème lié à [l'enregistrement en masse de domaines] avant d'entreprendre un travail de politiques*** », et notait la pertinence du cadre pour les algorithmes générés par les domaines associés aux réseaux zombies et aux programmes malveillants, élaboré par le RySG et le PSWG du GAC. **L'Institut de la lutte contre l'utilisation malveillante du DNS s'est dit en faveur d'approches basées sur le paiement pour lutter contre l'utilisation malveillante du DNS, faisant observer qu'il serait utile « *d'encourager les bureaux d'enregistrement à enquêter sur tous les domaines d'un compte client lorsque l'un de ces domaines est recensé comme malveillant* »** dans le cadre des « *options sensées et pratiques à la disposition des bureaux d'enregistrement afin de réduire dès maintenant l'utilisation malveillante du DNS […]* », en plus des « *frictions au moment de l'enregistrement* ».
- Sur la base d'autres contributions reçues des parties contractantes[10], **la petite équipe de la GNSO sur l'utilisation malveillante du DNS a conclu**, dans le cadre de ses conclusions préliminaires sur les enregistrements de masse (15 mai 2023), que **les enregistrements**

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

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

de masse « *ne relèvent pas du domaine de la politique de consensus à l'heure actuelle* » dans la mesure où :

- *les plaintes relatives à des enregistrements uniques ou multiples sont traitées de manière uniforme, sans qu'il soit clair ce qui peut constituer des enregistrements de masse justifiant des réactions ciblées ;*
- *l'absence de définition claire n'a pas suscité de réponse claire ;*
- *d'autres outils de connaissance du client sont jugés plus efficaces pour détecter les utilisations malveillantes potentielles et devraient faire l'objet d'une plus grande attention ;*
- *le projet INFERMAL (Inferential Analysis of Maliciously Registered Domains), récemment lancé par l'ICANN, semble indiquer une volonté de l'organisation de se pencher sur cette question et de fournir […] de meilleures statistiques et informations* [sur ce sujet].

- Dans son communiqué de Hambourg (30 octobre 2023), le GAC a exprimé son intention « *d'engager avec la communauté des discussions sur les efforts de politiques autour de […] thèmes clés liés à la mise en œuvre efficace des modifications, comme la clarification des termes clés des modifications (c.-à-d., "raisonnable", "réalisable", "rapide"), et d'autres mesures d'atténuation de l'utilisation malveillante du DNS, comme les efforts de renforcement des capacités* ».
- Lors de l'appel préparatoire de l'ICANN79 entre la direction du GAC et le conseil de la GNSO, celui-ci a indiqué ne pas envisager activement l'élaboration d'une politique sur les questions liées à l'utilisation malveillante du DNS à l'heure actuelle, précisant que cela faisait l'objet de discussions au sein des groupes de parties prenantes de la GNSO et entre eux.
- Lors d'une réunion bilatérale avec le GAC à San Juan (6 mars 2024), le conseil de la GNSO a fait observer que la petite équipe de la GNSO est actuellement en pause, en attendant la collecte de données auprès du département conformité de l'ICANN sur l'effet des modifications aux contrats, et qu'elle reprendra une fois que plus d'informations lui auront été fournies pour déterminer quel type d'élaboration de politiques, le cas échéant, serait indiqué 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 la perturbation de l'utilisation malveillante du DNS[11]**
  - **L'équipe de révision SSR2 a publié 63 recommandations** dans son rapport final (25 janvier 2021), en accordant une attention particulière aux mesures de prévention et d'atténuation de l'utilisation malveillante du DNS.
    - Le GAC a examiné un rapport préliminaire de la révision SSR2 (24 janvier 2020) et a souscrit à un certain nombre des recommandations préliminaires dans un

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

commentaire du GAC (3 avril 2020). Par la suite, dans ses commentaires (8 avril 2021) sur les recommandations finales et dans son avis ultérieur émis dans le communiqué de l'ICANN72 (1er novembre 2021), le GAC a demandé un suivi et des informations complémentaires sur le degré de mise en œuvre de certaines recommandations. Le Conseil d'administration de l'ICANN a répondu (16 janvier 2022), le tout donnant lieu à d'autres discussions au cours de l'ICANN73[12] et à des communications de l'organisation ICANN au GAC sous la forme d'une lettre (18 mars 2022) et d'un courriel de suivi (12 avril 2022).

- Selon le rapport trimestriel sur les révisions spécifiques de l'ICANN (31 mars 2024) et sur la base de plusieurs résolutions du Conseil d'administration de l'ICANN (22 juillet 2021, 1er mai 2022, 16 novembre 2022 et 10 septembre 2023) : **23 recommandations** sont **approuvées** (dont 14 soumises à un ordre de priorité pour la mise en œuvre), **38 rejetées**, et **1 en attente** de plus amples informations.
- Le 10 septembre 2023, **le Conseil d'administration de l'ICANN a rejeté**, sur la base d'une évaluation menée par l'organisation ICANN, **6 des 7 recommandations en attente relatives à l'utilisation malveillante du DNS** – **12.1** (*créer une équipe consultative pour l'analyse de l'utilisation malveillante du DNS*), **12.2** (*structurer des accords avec les fournisseurs de données pour permettre un plus grand partage des données*), **12.3** (*publier des rapports qui identifient les registres et bureaux d'enregistrement dont les domaines contribuent le plus à l'utilisation malveillante du DNS*), **12.4** (*faire rapport des mesures prises par les opérateurs de registre et bureaux d'enregistrement pour répondre aux plaintes de conduite illégale et/ou malveillante*), **13.1** (*établir un portail centralisé pour le dépôt des plaintes d'utilisation malveillante du DNS obligatoire pour tous les gTLD*), **13.2** (*publier les données de plaintes pour analyse par des tiers*) et **14.2** (*fournir aux parties contractantes des listes de domaines recensés comme utilisés à des fins malveillantes et faisant partie de leurs portefeuilles*)**.**
- **Dans sa discussion sur les négociations contractuelles concernant l'utilisation malveillante du DNS, le PSWG du GAC s'est penché[13] sur plusieurs recommandations de la SSR2 qui, selon la** Fiche de suivi du Conseil d'administration (22 juillet 2021), **ont été rejetées** par le Conseil d'administration de l'ICANN – **8.1** (*mandater une équipe de négociation comprenant des spécialistes en utilisation malveillante et en sécurité pour renégocier les contrats des parties contractantes*), **9.4** (*établir des rapports périodiques de conformité, où sont recensés les outils manquants*), **14.4** (*accorder aux parties contractantes un délai de 30 jours pour faire baisser la proportion des domaines utilisés à des fins malveillantes en deçà d'un seuil déterminé)* et **14.5** *(envisager d'offrir des incitations financières*) – et **pour lesquelles le GAC**, dans son communiqué de l'ICANN72 (1er novembre 2021), **s'est dit conscient** « *des bases procédurales du rejet par le Conseil d'administration* », tout **en soulignant**, néanmoins, « ***l'utilité des aspects substantiels de certaines***

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

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

recommandations rejetées, *notamment celles visant à* ***doter l'organisation ICANN et le département conformité de celle-ci des outils adéquats pour prévenir et atténuer l'utilisation malveillante du DNS*** ».

- Le rapport final de **l'équipe de révision de la concurrence, de la confiance et du choix des consommateurs** (8 septembre 2018) a contenu 35 recommandations. Dans son communiqué de Montréal (6 novembre 2019), comme il l'a clarifié dans une correspondance ultérieure au Conseil d'administration de l'ICANN (janvier 2020), **le GAC a conseillé au Conseil d'administration « *de ne pas procéder à une nouvelle série de gTLD avant la mise en œuvre complète des recommandations* *[…] ayant été recensées comme des "conditions préalables" [14 recommandations] ou comme des "priorités élevées" [10 recommandations]*** ».
  À la suite de discussions liées aux communiqués de l'ICANN70 et de l'ICANN71[14], le GAC et le Conseil d'administration de l'ICANN ont convenu, comme exprimé lors d'un appel du BGIG (5 octobre 2021) *[connexion requise au site Web du GAC]*, que « *le GAC envisagerait un suivi sur le fond des recommandations de la révision CCT et non sur les recommandations 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** (*collecter des données sur la chaîne des parties responsables de l'enregistrement des noms de domaine et la rendre publique)* **a été approuvée et sa mise en œuvre est achevée** conformément à sa documentation de mise en œuvre le 14 septembre 2022 ;
  - la **recommandation 13** (*recueillir des données sur l'impact des restrictions d'enregistrement,* le GAC ayant noté qu'elle *« permettrait une décision et une élaboration de politiques plus éclairée en ce qui concerne les futures dispositions contractuelles standard des opérateurs de registre et bureaux d'enregistrement* ») et la **recommandation 20** (*évaluer des mécanismes de signalement et de traitement des plaintes et éventuellement envisager de modifier les futurs contrats de registre standard pour exiger que les opérateurs de registre révèlent de manière plus évidente leurs points de contact de l'utilisation malveillante et fournissent des informations plus granulaires à l'ICANN*) ont été approuvées en partie selon la Fiche de suivi du Conseil d'administration du 22 octobre 2020, et **leur mise en œuvre, qui est en cours, devrait être achevée entre le T3 2023 et le T2 2024** selon le Rapport trimestriel sur les révisions spécifiques de l'ICANN du premier trimestre 2023 (31 mars 2023) ;
  - la **recommandation 14** (*inciter à l'adoption de mesures proactives contre l'utilisation malveillante du DNS*) et la **recommandation 15** (*négocier des modifications visant à*

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

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

inclure des dispositions préventives de l'utilisation systémique de certains bureaux d'enregistrement ou registres pour les atteintes à la sécurité du DNS, et établir des seuils d'utilisation malveillante qui déclenchent automatiquement la conformité) **ont été rejetées par le Conseil d'administration de l'ICANN** dans sa résolution du 10 septembre 2023.

- Les **recommandations LE.1 et LE.2 de la révision du RDS-WHOIS2**, qui demandaient « *la collecte régulière de données par le biais d'enquêtes et d'études afin d'éclairer une évaluation future de l'efficacité du RDS (WHOIS) pour répondre aux besoins des autorités d'application de la loi* » et « *la réalisation d'enquêtes et/ou d'études comparables avec d'autres utilisateurs du RDS (WHOIS) travaillant régulièrement avec les organismes d'application de la loi* », sont désormais **considérées comme « *mises en œuvre dans la mesure du possible* »** dans le cadre des travaux des étapes 2 et 2A de l'EPDP ainsi que de l'OPD du SSAD, conformément à la documentation relative à la mise en œuvre (11 octobre 2022).

- **Mesures et initiatives visant à atténuer l'utilisation malveillante du DNS par les opérateurs de registre et les bureaux d'enregistrement**
  - Le 27 mars 2020, l'organisation ICANN a ratifié la proposition de modification au contrat de registre de .COM, qui **étend les dispositions contractuelles afin de faciliter la détection et le signalement de cas d'utilisation malveillante du DNS aux trois quarts de l'espace de noms des gTLD**[16]. En outre, une lettre d'intention contraignante entre l'organisation ICANN et Verisign établit un cadre de coopération au développement de meilleures pratiques et de nouvelles obligations contractuelles potentielles, ainsi que d'indicateurs 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 visant à faciliter les rapports, leur révision et leur renvoi à la juridiction compétente par l'adoption d'un formulaire normalisé et l'établissement d'un point de contact unique pour les autorités compétentes. Ces efforts s'appuient sur les relations de travail établies entre les organismes d'application de la loi et les bureaux d'enregistrement, et s'inspirent du Guide des bureaux d'enregistrement pour le signalement de cas d'utilisation malveillante, publié par le **Groupe des représentants des bureaux d'enregistrement** lors de l'ICANN67. Ce guide a été mis à jour (janvier 2022) et approuvé par le **Groupe des représentants des opérateurs de registre**.

[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 le secteur des noms de domaine de juin 2022).

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

- Le **Registre d'intérêt public (PIR)**, opérateur de registre de .ORG et de plusieurs nouveaux gTLD, a créé (17 février 2021) l'**Institut de lutte contre l'utilisation malveillante du DNS**. Cette initiative a été présentée au PSWG du GAC (3 mars 2021). Dans son communiqué de l'ICANN70, le GAC s'est félicité de la création de l'Institut de la lutte contre l'utilisation malveillante du DNS et *« a encouragé les initiatives de la communauté qui visent à lutter de concert et de manière holistique contre l'utilisation malveillante du DNS »*. Depuis, l'Institut de la lutte contre l'utilisation malveillante du DNS a publié une feuille de route (14 juin 2021), discuté régulièrement des meilleures pratiques et mis au point une initiative visant à mesurer l'utilisation du DNS dans les activités d'hameçonnage et de logiciel malveillant. Lors de l'ICANN74, le GAC a invité l'Institut de lutte contre l'utilisation malveillante du DNS à présenter l'outil Net Beacon (anciennement connu sous le nom d'**Outil centralisé de signalement des cas d'utilisation malveillante**), que l'Institut est en train de mettre au point en réponse au 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 la 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 examine les positions du GAC, l'activité connexe de la communauté et les « lacunes actuelles ».
- **Plusieurs acteurs du secteur du DNS cherchent activement à contribuer à la mesure de l'utilisation malveillante du DNS** et des effets qu'auront les Amendements récemment approuvés du Contrat de registre et du Contrat d'accréditation de bureau d'enregistrement :
  - lors de l'ICANN78, l'**Institut de la lutte contre l'utilisation malveillante du DNS** a présenté au GAC son projet et sa méthodologie Compass qui visent à fournir une démarche rigoureuse et transparente de mesure de l'utilisation malveillante du DNS. Ce projet produit actuellement des rapports mensuels sur ce phénomène qui abordent les tendances du secteur, ainsi que les tendances de bureaux d'enregistrement et registres spécifiques qui accusent soit des taux élevés, soit des taux faibles d'utilisation malveillante du DNS. S'appuyant sur les données ainsi recueillies, l'Institut rapporte que 80 % des cas d'utilisation malveillante du DNS sont atténués dans les 30 et jours et prévoit une évolution favorable des tendances en matière d'atténuation grâce aux modifications des contrats de l'ICANN ;
  - **CleanDNS**, un fournisseur de services qui gère l'utilisation malveillante du DNS pour le compte de bureaux d'enregistrement, d'opérateur de registre et de fournisseurs d'hébergement, a échangé avec le GAC, lors de l'ICANN78 et de l'ICANN79, de l'importance de solidement étayer les rapports d'utilisation malveillante du DNS, lesquels doivent être communiqués à la partie la plus appropriée (opérateur de registre, bureau d'enregistrement, fournisseur d'hébergement ou titulaire de nom de domaine), afin de réduire le plus possible le délai requis pour l'atténuation et, ce faisant, limiter les dommages potentiels.
- Lors du récent Sommet des parties contractantes (6-9 mai 2024), l'ICANN et les Parties contractantes ont tenu un « atelier sur la lutte contre l'utilisation malveillante du DNS. Au

nombre des sujets abordés figuraient les « Préoccupations et défis les plus pressants en matière d'utilisation malveillante du DNS », ainsi que des « Études de cas et enseignements tirés de la contestation des rapports d'utilisation malveillante du DNS » Les enregistrements des séances publiques sont disponibles sur : 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 mise en conformité contractuelle**
  - L'organisation ICANN a présenté (22 juillet 2021) son programme d'atténuation des menaces à la sécurité du DNS, qui vise à fournir davantage de visibilité et de clarté aux divers projets et initiatives liés aux menaces à la sécurité du DNS et permet la définition et l'exécution d'une stratégie centralisée.
  - **Le Bureau du directeur de la technologie (OCTO) de l'ICANN et son équipe consacrée à la sécurité, la stabilité et la résilience** (SSR) mènent des recherches et assurent l'expertise de l'ICANN en matière de sécurité du DNS au profit de la communauté. Ils participent à des forums de veille sur les cybermenaces et de réponse aux incidents, et mettent au point des systèmes et outils de détection, d'analyse et de signalement de l'utilisation malveillante du DNS[19].
    - Face à la crise du COVID-19, l'OCTO a mis au point l'outil de **Signalement et de collecte d'information sur des menaces à la sécurité des noms de domaine** (DNSTICR) pour aider à repérer les noms de domaine liés au COVID-19 qui sont utilisés à des fins malveillantes et pour faciliter le partage de ces données avec les entités appropriées. Le GAC a été mis au courant du DNSTICR avant l'ICANN68 (12 juin 2020) et ses membres ont été invités à contribuer à la diversité linguistique de l'outil.
    - Sur 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[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,

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

[19] Lors d'un appel du GAC portant sur les questions liées à l'utilisation malveillante du DNS (24 février 2021), l'organisation ICANN a fait le point sur les activités de l'OCTO liées à ce phénomène, notamment la définition des menaces à la sécurité du DNS, la définition de l'utilisation malveillante du DNS et les obligations des Parties contractantes, ainsi que sur le DAAR, le DNSTICR, la DFSI, la KINDNS et les travaux que mène l'OCTO aux fins de la formation et du renforcement des capacités dans le monde.

[20] Plusieurs parties prenantes et initiatives de l'ICANN ont fait part des limites du DAAR, en particulier une lettre du M3AAWG transmise à l'organisation ICANN (5 avril 2019) et le rapport préliminaire de l'équipe de révision SSR2 (24 janvier 2020). Le Groupe des représentants des opérateurs de registre, qui avait également exprimé des préoccupations, a formulé des recommandations dans une correspondance adressée au CTO de l'ICANN (9 septembre 2020).

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

dans le DAAR, des informations liées aux bureaux d'enregistrement, comme salué par le GAC dans une lettre à l'ICANN (21 février 2022). Ces changements ont été inclus dans la proposition de modifications aux RA et RAA de base des gTLD pour ajouter des obligations contractuelles liées au RDAP (6 septembre 2022), que le GAC a accueilli favorablement dans ses commentaires (16 novembre 2022). Ces modifications ont été récemment approuvées par le Conseil d'administration de l'ICANN (30 avril 2023) et devraient prendre effet le 3 février 2024.

- L'OCTO a soutenu le **Groupe d'étude technique chargé de l'initiative de facilitation de la sécurité du DNS**, créé en mai 2020 dans le cadre de la mise en œuvre du plan stratégique pour les exercices fiscaux 2021-2025, dans le but de *« réfléchir à ce que l'ICANN peut et devrait faire pour augmenter le niveau de collaboration et d'engagement avec les parties prenantes de l'écosystème du DNS et améliorer ainsi le profil de sécurité du DNS »*. Son rapport final (15 octobre 2021) a été publié au terme de 18 mois de délibérations. L'organisation ICANN a indiqué au GAC (16 février 2022) qu'elle travaillait, en tenant compte de ce rapport, à l'élaboration d'un plan d'action. Le 20 avril 2022, le processus de mise en œuvre ainsi qu'une page Wiki permettant de suivre les progrès effectués ont été présentés à la communauté. Lors de l'ICANN74, le GAC a discuté de l'utilité de prioriser la recommandation E5, qui consiste à établir une plateforme de **partage d'informations sur les menaces et les incidents** et la mettre à la disposition des parties prenantes concernées de la communauté de l'ICANN[22].
- Un nouveau projet qui sera supervisé par l'OCTO de l'ICANN, baptisé Analyse inférentielle des domaines enregistrés à des fins malveillantes (INFERMAL), se propose d'**analyser systématiquement les préférences des cyberattaquants, notamment leur prédilection pour certains des noms de domaine de certains bureaux d'enregistrement par rapport à d'autres**, ainsi que les mesures susceptibles d'atténuer les activités malveillantes dans l'ensemble des domaines de premier niveau (TLD). Ce projet trouve en partie son origine dans les données recueillies lors de l'analyse statistique de l'utilisation malveillante du DNS dans les gTLD (9 août 2017)[23]. Ces données donnent à penser que les acteurs malveillants tendent à privilégier des bureaux d'enregistrement proposant des coûts d'enregistrement bas, acceptant des modes de paiement spécifiques, offrant des interfaces de programmation d'application (API) gratuites pour les enregistrements de masse, ou à éviter ceux qui exigent certaines informations au moment de l'achat.
  Dans une mise à jour préalable à l'ICANN78 (25 octobre 2023), il a été signalé que l'équipe de recherche envisageait « *d'effectuer une analyse des mesures de sécurité recensées comme contribuant à atténuer l'utilisation malveillante du DNS* » et prévoyait de « *résumer une étude sur la rapidité avec laquelle les noms de domaine*

[22] Recommandation E5 *Réponse aux incidents* du rapport final DSFI-TSG *(13 octobre 2021)* : « *L'organisation ICANN, en collaboration avec les parties concernées, devrait faciliter l'élaboration et le déploiement d'un processus formel de réponse aux incidents dans le secteur du DNS, qui permet l'interaction avec d'autres entités de l'écosystème. Une telle initiative devrait inclure la gestion de la réponse à l'incident ainsi que le partage sécurisé de l'information relative à la menace ou à l'incident* ».

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

utilisés à des fins malveillantes sont suspendus après notification aux opérateurs ». Un rapport final « *sous la forme d'un document de recherche* » devrait être publié d'ici septembre 2024, proposant, entre autres, de « *meilleures pratiques pour l'atténuation efficace de l'utilisation malveillante* ».

- Pour ce qui est de **la mise en conformité contractuelle,** le PDG de l'ICANN avait rappelé dans son billet de blog (20 avril 2020) ce qui suit : « *Le département conformité de l'ICANN veille au respect des obligations contractuelles prévues dans les politiques et contrats de l'ICANN, en particulier le Contrat de registre (RA) et le Contrat d'accréditation de bureau d'enregistrement (RAA). Par ailleurs, ce service collabore étroitement avec l'OCTO au recensement des menaces à la sécurité du DNS […] et à la mise en correspondance de ces menaces avec les parties contractantes concernées. Le département conformité de l'ICANN se sert des données collectées pendant les audits […] pour évaluer si les opérateurs de registre et bureaux d'enregistrement se conforment à leurs obligations en matière d'atténuation des menaces à la sécurité du DNS. En dehors de ces audits, le département conformité de l'ICANN utilisera les données collectées par l'OCTO et d'autres pour contacter de manière proactive les opérateurs de registre et les bureaux d'enregistrement responsables d'un nombre disproportionné de menaces à la sécurité du DNS. Dans le cas où le dialogue constructif n'aboutit pas, le département conformité de l'ICANN n'hésitera pas à prendre des mesures coercitives pour appliquer les dispositions contractuelles de tous ceux qui refuseraient de se conformer à leurs obligations en matière de menaces à la sécurité du DNS* ».
  - À la suite d'un précédent **audit de la conformité contractuelle** des opérateurs de registre, axé sur l'utilisation malveillante de l'infrastructure du DNS et achevé en juin 2019[24], l'ICANN a présenté (24 août 2021) les résultats de l'audit sur **la conformité des bureaux d'enregistrement aux obligations d'atténuation de l'utilisation malveillante du DNS** : 126 bureaux d'enregistrement audités (gérant plus de 90 % de tous les domaines enregistrés dans les gTLD) ; 111 bureaux d'enregistrement ne respectant pas entièrement les exigences relatives à la réception et au traitement des rapports d'utilisation malveillante du DNS (articles 3.18.1 – 3.18.3 du RAA) ; et 92 bureaux d'enregistrement ayant pris des mesures pour se conformer entièrement aux exigences.
  - Le 9 mars 2022, l'ICANN a annoncé son déploiement de nouveaux mécanismes de compte rendu renforçant la visibilité des volumes de plaintes et des tendances en la matière.
  - **Une nouvelle série d'audits portera sur** 28 opérateurs de registre gTLD[25] exploitant des gTLD, qui n'ont pas précédemment fait l'objet d'un audit complet et qui présentent des niveaux d'utilisation malveillante parmi les plus élevés, comme

[24] Voir le billet de blog de l'ICANN « Conformité contractuelle :traiter les cas d'utilisation malveillante de l'infrastructure du système des noms de domaine (DNS) » (8 novembre 2018) et le « Rapport d'audit du département chargé de la conformité contractuelle sur la réponse des opérateurs de registre aux menaces à la sécurité du DNS » (17 septembre 2019).

[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)

indiqué par les listes de blocage de réputation mises à la disposition du public (à l'exclusion des courriers indésirables), a été annoncée le 13 avril 2022 et s'est conclue avec la publication d'un rapport d'audit le 16 septembre 2022. Le GAC a discuté des résultats lors de sa séance plénière sur l'utilisation malveillante du DNS au cours de l'ICANN75 (20 septembre 2022).

- Dans le cadre de la semaine de préparation de l'ICANN78 (9 octobre 2023), le département conformité de l'ICANN a fait rapport sur les mesures qu'il a prises en réponse à des plaintes[26], ainsi que sur son Programme d'audit, notamment :
  - l'achèvement d'un audit de bureaux d'enregistrement (22 juin 2023) portant sur 15 bureaux d'enregistrement « *représentant 7 familles de bureaux d'enregistrement comprenant au total 619 bureaux d'enregistrement* » établis dans 8 pays, totalisant 83 millions de noms de domaine sous gestion (voir la liste à la p.17). Quarante pour cent des bureaux audités ont pu résoudre les « constatations initiales », tandis que 53 % ne l'ont pas pu et « *mettent en œuvre les changements nécessaires* » pour pallier les lacunes restantes (voir p. 10-14) ;
  - **lancement d'un nouvel audit de conformité des registres** (août 2023) portant sur 19 opérateurs de registres, non audités précédemment, ayant un score DAAR d'utilisation malveillante supérieur à 0 %.

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

- **Enquête sur les initiatives d'atténuation de l'utilisation malveillante du DNS dans les ccTLD par le Comité permanent sur l'utilisation malveillante du DNS (DASC) de la ccNSO**
    - Les plans de travail du Groupe de travail sur la sécurité publique (PSWG) du GAC ont intégré un examen des pratiques d'atténuation de l'utilisation malveillante du DNS par les ccTLD, afin d'éclairer l'élaboration de normes contractuelles renforcées dans l'espace des gTLD. Plus précisément, le plus récent plan de travail 2023-2024 du PSWG comprend le point de travail 1.3 visant à « *revoir et recenser les meilleures pratiques des ccTLD pour adoption dans l'espace des gTLD* » :
        - *examiner et évaluer les meilleures pratiques des ccTLD en matière d'atténuation des menaces de sécurité, telles que la prédiction de l'utilisation malveillante et les politiques de validation et de vérification des titulaires de noms de domaine, en vue de recenser des approches possibles, pratiques et applicables, et d'examiner comment elles pourraient éclairer l'élaboration de normes contractuelles renforcées dans l'espace des gTLD.*
    - Auparavant, des opérateurs de ccTLD du monde entier avaient fait part au GAC, lors d'un séminaire Web de préparation à l'ICANN69 (4 juin 2020), des enseignements qu'ils ont tirés de leurs opérations pendant la crise de COVID-19.
    - En mars 2022, la ccNSO a créé un Comité permanent sur l'utilisation malveillante du DNS (DASC) dans le but de « *sensibiliser aux problèmes liés à l'utilisation malveillante du DNS et mieux les faire connaître, favoriser un dialogue ouvert et constructif et, au bout du compte, aider les gestionnaires de ccTLD dans leurs démarches visant à atténuer l'impact de l'utilisation malveillante du DNS* », tout en notant qu'« *en conformité avec la nature de la ccNSO, l'objectif du Comité n'est pas de formuler des politiques ou des normes, étant donné que l'élaboration de politiques dans ce domaine n'entre pas dans le cadre des attributions de la ccNSO en matière de politiques* ».
    - Au cours de l'atelier de développement des capacités du GAC de l'ICANN76 (11 mars 2023), le DASC a présenté au GAC ses premières conclusions à la suite d'une enquête qu'il a menée entre septembre et novembre 2022, auprès d'environ 100 ccTLD, sur leurs pratiques d'atténuation de l'utilisation malveillante du DNS. La présentation abordait des résultats quantitatifs concernant :
        - les méthodes utilisées pour atténuer l'utilisation malveillante du DNS (politiques d'enregistrement, procédures de plainte, autres outils) et les mesures prises lorsque ce type de phénomène était détecté (avis aux titulaires, suspension, suppression) ;
        - la collaboration avec les CERT nationales, les organismes chargés de l'application de la loi et les mécanismes de notification de confiance ;
        - le signalement de l'utilisation malveillante du DNS.
    - Ces résultats ont été ensuite débattus en profondeur lors de la séance de la ccNSO de l'ICANN77, mettant un accent particulier sur les résultats quantitatifs liés aux vérifications des données d'enregistrement, leur portée, leur calendrier, leurs méthodes et leurs conséquences. La corrélation entre les politiques tarifaires et les niveaux d'utilisation malveillante du DNS a également été examinée.

- Lors de la présentation finale des résultats de cette enquête dans le cadre d'un séminaire Web du DASC en préparation de l'ICANN78, le 28 septembre 2023 (voir l'enregistrement et les diapositives), le DASC s'est concentré sur la distribution quantitative des tendances d'utilisation malveillante du DNS et des pratiques d'atténuation, en fonction des caractéristiques des ccTLD (y compris la région, le modèle de gouvernance, la taille du portefeuille de domaines, etc.).
- 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 dans l'étude des indicateurs de l'utilisation malveillante du DNS et des outils d'atténuation dans les ccTLD.

Principaux documents de référence

- Commentaires du Conseil d'administration de l'ICANN sur les questions d'importance du communiqué de San Juan de l'ICANN79 (9 mai 2024).
- Sommet des Parties contractantes (6-9 mai 2024) et enregistrements des séances publiques.
- L'Amendement au Contrat de registre, l'Amendement au Contrat d'accréditation de bureau d'enregistrement et le bulletin d'information afférent :Respect des obligations en matière d'utilisation malveillante du DNS prévues dans le Contrat d'accréditation de bureau d'enregistrement et le Contrat de registre (publiés le 5 février 2024, avec prise d'effet 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 concernant l'utilisation malveillante du DNS
- Résolution du Conseil d'administration de l'ICANN (10 septembre 2023) basée sur l'évaluation par l'organisation ICANN des révisions CCT et SSR2 en suspens concernant l'atténuation de l'utilisation malveillante du DNS
- Compte rendu sommaire des commentaires publics (1er août 2023) préparé par l'organisation ICANN sur la procédure de consultation publique relative aux propositions de modification aux contrats de registres et de bureau d'enregistrement concernant l'utilisation malveillante du DNS
- Commentaires du GAC (17 juillet 2023) sur la proposition de modifications aux contrats des registres et bureaux d'enregistrement concernant l'utilisation malveillante du DNS
- Rapport du Département chargé de la conformité contractuelle sur le cycle d'audit des bureaux d'enregistrement de novembre 2022 (22 juin 2023)
- Modifications au RA et au RAA de base des gTLD visant à renforcer les obligations contractuelles relatives à l'utilisation malveillante du DNS (29 mai 2023)
- Annonce du projet INFERMAL (Inferential Analysis of Maliciously Registered Domains) (25 avril 2023)
- Rapport de la petite équipe de la GNSO au conseil de la GNSO sur l'utilisation malveillante du DNS (7 octobre 2022)
- The Last Four years in Retrospect: A Brief Review of DNS Abuse élaboré par l'organisation ICANN (22 mars 2022)
- Étude sur l'utilisation malveillante du DNS et son annexe technique, publiés par la Commission européenne (31 janvier 2022)
- Rapport final de la révision de la SSR2 (25 janvier 2021) et commentaires du GAC y afférants (8 avril 2021)

- Le rapport SAC115 (19 mars 2021) du SSAC, qui propose une approche interopérable pour la gestion de l'utilisation malveillante du DNS

Gestion des documents

Titre	Document d'information du GAC pour l'ICANN80 – Utilisation malveillante du DNS
Distribution	Membres du GAC (avant la réunion) et du public (après la réunion)
Date de distribution	Version 1 : le 27 mai 2024