ICANN | GAC
Governmental Advisory Committee

ICANN 70
VIRTUAL COMMUNITY FORUM

Atténuation de l'utilisation malveillante du DNS

Séances 8 et 16

Table des matières

Objectifs de la séance

Le GAC se penchera sur les développements récents qui ont eu lieu dans la communauté de l'ICANN, à savoir la conclusion de la révision de la SSR2 et celle du PDP consacré aux procédures ultérieures, afin de définir de prochaines étapes garantissant la prise des mesures qui s'imposent pour prévenir et atténuer l'utilisation malveillante du DNS dans les gTLD. Il examinera, à ce titre, des propositions concrètes visant à améliorer les dispositions contractuelles et à garantir leur respect.

Contexte

Des activités malveillantes sur Internet menacent et affectent les titulaires de noms de domaine ainsi que les utilisateurs finaux en exploitant les failles dans tous les aspects des écosystèmes du DNS et de l'Internet (protocoles, systèmes informatiques, transactions personnelles et individuelles, procédures d'enregistrement de domaines, etc.). Elles menacent la sécurité, la stabilité et la résilience des infrastructures du DNS et, qui plus est, mettent en péril l'ensemble du DNS.

Ces menaces et activités malveillantes sont en général qualifiées d'« utilisation malveillante du DNS » par la communauté de l'ICANN. On entend par utilisation malveillante du DNS tout ou partie de certaines activités, dont l'hameçonnage, les logiciels malveillants, les réseaux zombie, le déni de service distribué (DDOS), le courrier indésirable, et la diffusion de contenu illégal. Il convient toutefois de noter que même la définition exacte d'« utilisation malveillante du DNS » fait l'objet d'intenses discussions.

Si les parties prenantes de la communauté de l'ICANN semblent généralement s'accorder à dire que l'utilisation malveillante est un problème qui doit être traité, les avis divergent quant à la part de responsabilité des différentes parties concernées. Les registres et les bureaux d'enregistrement, par exemple, craignent devoir endosser plus d'obligations contractuelles (ce qui pourrait perturber leurs modèles commerciaux). Ils soutiennent que les outils dont ils disposent pour atténuer l'utilisation malveillante sont limités et risquent d'être inadéquats (certains cas auraient besoin d'être traités par les fournisseurs d'hébergement alors que d'autres exigeraient de la part des registres et bureaux d'enregistrement de mesures susceptibles d'entrainer des dommages collatéraux et d'accroitre leur responsabilité).

À ce jour, la communauté de l'ICANN a accompli, avec plus ou moins de succès, un travail remarquable pour lutter contre l'utilisation malveillante du DNS :

- **L'Organisation de soutien aux extensions génériques (GNSO)** de l'ICANN a établi, en 2008, le groupe de travail sur les politiques en matière d'enregistrements frauduleux. Ce dernier a recensé un ensemble de problèmes spécifiques, sans toutefois produire de propositions de politiques ; la discussion consécutive sur la création d'une liste de meilleures pratiques indicatives pour les registres et bureaux d'enregistrement n'en a pas produit non plus (en ce compris des ateliers pendant l'ICANN41 et l'ICANN42).
- **Dans le cadre du programme des nouveaux gTLD,** l'organisation ICANN a adopté une série de nouvelles exigences[1] conformément à son protocole de réduction des comportements malveillants (3 octobre 2009). Le rapport de l'ICANN sur les sauvegardes du programme des nouveaux gTLD (18 juillet 2016) a évalué leur efficacité en vue de la révision de la

[1] Contrôle des opérateurs de registre, élaboration d'un plan bien défini pour le déploiement des DNSSEC, interdiction des caractères génériques, suppression des enregistrements orphelins de type glue lorsqu'une entrée de serveur de nom est supprimée de la zone, obligation d'assurer la maintenance des enregistrements du WHOIS détaillé, centralisation de l'accès aux fichiers de zone, établissement de points de contact et de procédures pour le signalement d'abus au niveau du registre.

concurrence, la confiance et le choix du consommateur (CCT) mandatée par les statuts, laquelle a rendu ses recommandations le 8 septembre 2018.

- Avant la création du groupe de travail du GAC sur la sécurité publique (PSWG), **les représentants des organismes d'application de la loi** ont joué un rôle de premier plan dans les négociations du **contrat d'accréditation de bureau d'enregistrement** de 2013[2], ainsi que dans l'élaboration de l'avis du GAC relatif aux menaces à la sécurité qui a conduit à l'introduction, dans le contrat de base des nouveaux gTLD, de nouvelles dispositions précisant les responsabilités des registres[3].

- **Plus récemment, l'organisation de l'ICANN**, par les soins du bureau du directeur de la technologie (OCTO), a mis au point le signalement des cas d'utilisation malveillante des noms de domaine (DAAR) qui produit des rapports mensuels et contribue au suivi des tendances comme vient d'en être informé le GAC (24 février 2021). Le suivi et le signalement des cas d'utilisation malveillante du DNS ont fait l'objet d'un soutien actif de la part du GAC et des équipes de révision, qui ont recommandé des améliorations. Ces outils devraient garantir la transparence et permettre de préciser les sources de problèmes, lesquelles seraient alors traitées soit par une action du service de la conformité, soit, le cas échéant, par l'élaboration d'une politique en connaissance de cause.

Problématique

Les initiatives passées n'ayant pas réussi à réduire effectivement l'utilisation malveillante du DNS, force est de constater qu'il reste beaucoup à faire. Malgré l'attention que porte la communauté de l'ICANN à l'utilisation malveillante du DNS, et malgré les meilleures pratiques qu'applique actuellement le secteur pour atténuer ce problème, les engagements communautaires pilotés par le GAC et les équipes de révision ont dégagé des tendances marquées d'utilisation malveillante, des pratiques commerciales qui peuvent y concourir, ainsi que des preuves qu'on peut encore « multiplier et renforcer les mesures d'atténuation et les sauvegardes » et élaborer de nouvelles politiques[4].

De plus, les inquiétudes quant à la capacité à atténuer l'utilisation malveillante du DNS se sont accrues dans les secteurs de la protection de la propriété intellectuelle, de l'application des lois, de la cybersécurité et de la protection des consommateurs[5] à la suite de l'entrée en vigueur du

[2] Voir les recommandations relatives à la diligence raisonnable dans l'application de la loi (octobre 2019) ainsi que les 12 recommandations des organismes d'application de la loi (1er mars 2012)

[3] Ces dispositions ont par la suite été complétées par un cadre de mesures non contraignantes à mettre en œuvre par les opérateurs de registre pour répondre à des menaces à la sécurité (20 octobre 2017) négocié entre l'organisation ICANN, les registres et le PSWG du GAC.

[4] Voir le commentaire du GAC (19 septembre 2017) sur le rapport final de l'Analyse statistique de l'utilisation malveillante du DNS dans les gTLD.

[5] Voir article III.2 et IV.2 du communiqué de Barcelone du GAC (25 octobre 2018) relatif aux enquêtes concernant l'impact sur l'application de la loi, voir l'article 5.3.1 du rapport préliminaire de l'équipe de révision RDS (31 aout 2018) et la publication des groupes de travail anti-hameçonnage et anti-abus pour la messagerie, les programmes malveillants et les mobiles (18 octobre 2018).

Règlement général sur la protection des données (RGPD) de l'Union européenne et des efforts concomitants visant la mise en conformité du système WHOIS, outil majeur d'enquête sur les cas d'utilisation malveillante et de crime. La crise sanitaire mondiale tout récente due à la COVID-19 a bien mis en évidence les problèmes existants, avec l'explosion du nombre d'enregistrements de domaines en rapport avec la pandémie.

Les comités consultatifs de l'ICANN, en particulier le GAC, le SSAC et l'ALAC, ainsi que plusieurs tiers touchés, ont demandé à l'organisation ICANN et à la communauté de l'ICANN de prendre davantage de mesures[6].

De telles mesures exigeraient de la communauté de l'ICANN qu'elle parvienne à une forme de consensus autour d'un certain nombre de questions ouvertes.

Les discussions de la communauté de l'ICANN sur l'atténuation de l'utilisation malveillante et sur l'éventuel travail de politique tournent en général autour de :

- **la définition de l'utilisation malveillante du DNS :** qu'est-ce qui constitue une utilisation malveillante, au regard du ressort de l'ICANN et des contrats conclus avec les registres et bureaux d'enregistrement ?
- **la détection et le signalement des cas d'utilisation malveillante du DNS :** comment garantir que l'utilisation malveillante du DNS est détectée et portée à la connaissance des parties prenantes concernées, au nombre desquelles figurent les consommateurs et les utilisateurs d'Internet ?
- **la prévention et l'atténuation de l'utilisation malveillante du DNS :** quels sont les outils et procédures que peuvent utiliser l'organisation de l'ICANN, les acteurs du secteur et les parties prenantes intéressées pour réduire l'utilisation malveillante et y répondre de manière appropriée le cas échéant ? qui devrait être chargé de telle ou telle partie de ce casse-tête, et quel serait pour les différents acteurs le meilleur moyen de coopérer ?

Le GAC, soucieux de renforcer la sécurité et la stabilité pour le bien de tous les utilisateurs d'Internet, pourrait vouloir activement contribuer à faire avancer le débat sur ces questions de sorte à progresser vers une prévention et une atténuation plus efficaces de l'utilisation malveillante.

[6] Voir les discussions sur l'utilisation malveillante du DNS et la protection des consommateurs pendant le sommet GDD (7-8 mai 2019)

Proposition soumise par la direction du GAC pour décision de la plénière

1. **Examiner les recommandations de la Deuxième équipe de révision de la sécurité, la stabilité et la résilience du DNS (SSR2),** incluses dans le rapport final (25 janvier 2021) de celle-ci, en **vue de fournir des apports du GAC avant** l'examen formel par le Conseil d'administration de l'ICANN prévu avant le 25 juillet 2021.

2. **Envisager de nouvelles contributions à la définition de l'utilisation malveillante du DNS** pour refléter le paysage des menaces tel qu'il est vécu par les organismes chargés de l'application de la loi, conformément à la déclaration du GAC sur l'utilisation malveillante du DNS (18 septembre 2019), en complément de la définition adoptée par les parties contractantes (octobre 2020) après l'émergence d'un cadre de lutte contre l'utilisation malveillante dirigé par les acteurs du secteur (17 octobre 2019).

3. **Délibérer sur des mesures éventuelles à prendre,** entre autres par **des propositions concrètes qui visent à améliorer les politiques, les dispositions contractuelles, et l'application de celles-ci,**[7] afin de faire face aux problèmes de politique publique liés à l'utilisation malveillante du DNS, tels que répertoriés par divers efforts de la communauté et contributions du GAC, notamment :

    a. **Les recommandations de l'équipe de révision CCT,** présentées dans le rapport final de l'équipe (8 sept. 2018), eu égard à ce qui suit :

        - La décision du Conseil d'administration de l'ICANN (1er mars 2019) sur l'ensemble des 35 recommandations et son adoption, par la suite (26 janvier 2020), d'un plan de mise en œuvre proposé pour les 6 recommandations qu'il avait acceptées (6 septembre 2019) ;
        - les observations formulées par le GAC dans les Commentaires sur le rapport préliminaire (19 mai 2017), les Commentaires sur l'Analyse statistique de l'utilisation malveillante du DNS dans les gTLD (19 septembre 2017), les Commentaires sur la version préliminaire de recommandations supplémentaires (15 janvier 2018), les Commentaires sur le Rapport final de la révision CCT (11 décembre 2018), les Commentaires sur le Plan de mise en œuvre (21 octobre 2019) ;
        - l'avis du GAC contenu dans le communiqué de Montréal (6 novembre 2019), où le GAC demandait de *ne pas procéder à une nouvelle série de gTLD jusqu'à la mise en œuvre des recommandations issues de la révision de la concurrence, de la confiance et du choix du consommateur et qualifiées de « conditions préalables » ou de « hautement prioritaires »*

[7] Conformément au Communiqué du GAC de l'ICANN69 Section IV.2 : « le GAC estime que, à l'heure actuelle, on observe un large appui, fermement exprimé, en faveur de la prise de mesures concrètes pour la mise en place des principales composantes d'une atténuation efficace de l'utilisation malveillante du DNS » *; et aux* procès-verbaux du GAC de l'ICANN69 : Section 2.2 *« Points d'action » : Le PSWG du GAC doit envisager d'élaborer une proposition concrète concernant les mesures à prendre pour atténuer l'utilisation malveillante du DNS, et ce afin de préparer le GAC à des discussions plus approfondies lors de l'ICANN70 (conformément à la discussion qu'a eue le GAC au cours de sa séance de clôture).* »

- les Questions de clarification du Conseil d'administration (16 décembre 2019) (16 décembre 2019) concernant l'avis du GAC de Montréal - notamment, les questions ayant trait à la révision CCT, aux séries ultérieures de nouveaux gTLD et à la définition de la « mise en œuvre complète »
- la Réponse du GAC aux questions de clarification du Conseil (22 janvier 2020)
- la Réponse du Conseil à la réponse du GAC aux questions de clarification (11 février 2020), où il faisait référence à sa décision (26 janvier 2020) de ne pas accepter ni rejeter l'avis.

b. **Le Groupe de travail de la GNSO chargé du processus d'élaboration de politiques concernant des procédures pour des séries ultérieures de nouveaux gTLD**, qui a déterminé dans son rapport final (1er février 2021) que « *ce groupe de travail PDP ne formule aucune recommandation sur l'atténuation de l'utilisation malveillante de noms de domaine, si ce n'est que toute future initiative à cet égard s'applique à la fois aux gTLD existants et aux nouveaux gTLD (et éventuellement aux ccTLD) »,* malgré les recommandations pertinentes sur l'utilisation malveillante du DNS qui lui ont été adressées par l'équipe de révision CCT[8]. Dans ses Commentaires (29 septembre 2020), le GAC s'est dit vivement préoccupé de la décision émise par le groupe de travail PDP dans la version préliminaire du rapport final, et a affirmé compter sur le conseil de la GNSO pour intervenir rapidement à ce sujet.

c. **La mise en œuvre et l'application de certaines obligations contractuelles clés** du contrat de registre et du contrat de bureau d'enregistrement, en particulier :
   - la **spécification 11 du contrat de registre des nouveaux gTLD** et l'avis du GAC relatif au GAC qui y correspond, qu'a formulé le GAC dans le communiqué de Pékin (11 avril 2013), l'examen des conclusions de l'audit sur la réponse des opérateurs de registres aux menaces pour la sécurité du DNS (17 septembre 2019) et de la discussion associée aux Questions et réponses GAC/ICANN (30 mai 2017), les commentaires du GAC sur la version préliminaire du rapport CCT (19 mai 2017), ainsi que les commentaires du GAC sur la version préliminaire du rapport de la SSR2 (3 avril 2020) ;
   - **la spécification relative au programme d'exactitude du WHOIS** contenue dans le contrat d'accréditation de bureau d'enregistrement de 2013, qui comprend des dispositions relatives à la vérification, à la validation et à l'exactitude des données d'enregistrement des noms de domaine, comme discuté dans le commentaire du GAC sur le rapport final de l'équipe de révision RDS/WHOIS2 (23 décembre 2019) ; **l'obligation, du bureau d'enregistrement, d'avoir un point de contact chargé de signaler les cas d'utilisation malveillante et le devoir d'enquêter sur les plaintes connexes** (section 3.18), qui fait actuellement l'objet d'un audit de conformité contractuelle pour une sélection de 153 bureaux d'enregistrement (15 janvier

[8] Voir la Recommandation 9.15 (p. 42) du Rapport final du groupe de travail Sub Pro PDP et les décisions connexes du Conseil d'administration de l'ICANN sur les recommandations de l'équipe CCT.

2021). Ces deux questions ont également été abordées dans les Questions et réponses GAC/ICANN (30 mai 2017) à la suite de l'avis du GAC du Communiqué d'Hyderabad (8 novembre 2016).

d. **Divers débats qui ont eu lieu au sein de la communauté au sujet de l'utilisation malveillante du DNS et de l'efficacité des dispositions contractuelles y afférentes** tant au regard des mesures assurant leur respect qu'au regard de leur effet obligatoire :
   - **les réunions de l'ICANN :** le séminaire web pré-ICANN66 (15 octobre 2019), la séance At-Large de l'ICANN66 sur les préoccupations des utilisateurs finaux (3 novembre 2019), la séance intercommunautaire de l'ICANN66 sur l'utilisation malveillante du DNS (6 novembre 2019), la séance At-Large de l'ICANN67 sur la conformité contractuelle (9 mars 2020), la séance ALAC de l'ICANN68 sur les engagements d'intérêt public et la procédure de résolution de litiges y associée (22 juin 2020), la réunion du conseil de la GNSO et du Conseil d'administration lors de l'ICANN68 qui a abordé d'éventuelles mesures à prendre pour lutter contre l'utilisation malveillante du DNS (14 juin 2020), et la séance plénière de l'ICANN69 sur les questions liées à l'utilisation malveillante du DNS (20 octobre 2020) ;
   - **les échanges entre le Conseil d'administration de l'ICANN et les unités constitutives des utilisateurs commerciaux (BC) et des représentants de la propriété intellectuelle (IPC)** de la GNSO, notamment : la Déclaration de la BC concernant la discussion communautaire sur l'utilisation malveillante du DNS (28 octobre 2019), une lettre du BC au Conseil d'administration de l'ICANN (9 décembre 2019) ainsi que la réponse du Conseil à cette lettre (12 février 2020) suivie de la lettre de l'IPC au Conseil (24 avril 2020).

e. **La mise en œuvre, par les opérateurs de ccTLD, de mesures proactives de lutte contre l'utilisation malveillante,** susceptibles de guider les pratiques des registres de gTLD comme celles présentées par les ccTLD .EU et .DK.[9].

f. **Les recommandations issues de la RDS-WHOIS2**, détaillées dans le rapport final de l'équipe (8 octobre 2019), qui sont pertinentes pour l'utilisation légitime du WHOIS en tant qu'outil clé d'enquête sur les crimes et les ,cas d'utilisation malveillante, au regard des commentaires du GAC (23 décembre 2019) et de la décision du Conseil d'administration de l'ICANN à ce jour (25 février 2020).

4. **Étudier les progrès des principaux efforts entrepris dans la communauté de l'ICANN pour atténuer l'utilisation malveillante du DNS, et continuer à suivre leur évolution,** de sorte à orienter et à promouvoir des normes exigeantes dans les pratiques et les contrats :

   a. Les **Propositions** pour la normalisation des stratégies et des processus de détection et d'atténuation de l'utilisation malveillante du DNS, **que devrait émettre le SSAC** dans le

[9]Voir notamment la Présentation de l'EURid (28 janvier 2016) et la présentation de .DK de l'ICANN64 (12 mars 2018).

rapport de son équipe de travail sur l'utilisation malveillante du DNS à paraitre avant l'ICANN70.

b. **La mise en œuvre de mesures volontaires par les bureaux d'enregistrement et registres des gTLD,** conformément au cadre de lutte contre l'utilisation malveillante élaboré par les acteurs du secteur et aux discussions en cours au sein du Réseau des politiques Internet et juridiction[10].

c. **Les améliorations au système de signalement des cas d'utilisation malveillante des noms de domaine (DAAR) de l'ICANN** tel qu'en ont déjà discuté les registres, le GAC et le SSAC, et le Bureau du directeur de la technologie (OCTO) de l'ICANN[11].

d. Le 27 mars 2020, l'organisation ICANN a mis en œuvre la proposition de modification au contrat de registre .COM. Celle-ci étend **les dispositions contractuelles visant à faciliter la détection et le signalement des cas d'utilisation malveillante du DNS**, y compris la spécification 11 3b, **aux deux tiers de l'espace de noms des gTLD** (ces dispositions n'étaient applicables jusqu'à présent qu'aux nouveaux gTLD). En outre, une lettre d'intention contraignante entre l'organisation ICANN et Verisign a établi un cadre de coopération propre à permettre la mise au point de meilleures pratiques et de nouvelles obligations contractuelles potentielles, ainsi que des mesures visant à mesurer et à atténuer les menaces à la sécurité du DNS.

5. **Examiner,** à la lumière des récents développements dans la mise en œuvre des technologies DNS cryptées, **les aspects liés au DNS sur HTTPS (DoH) et relevant de la politique publique**, conformément à la demande des membres du GAC lors de l'ICANN69 et aux travaux en cours du groupe de travail du GAC sur la sécurité publique (PSWG) prévus dans son plan de travail 2020-2021.

[10] Le Réseau des politiques Internet et juridiction a récemment annoncé (22 février 2021) le lancement d'une boite à outils sur l'action à prendre au niveau du DNS pour lutter contre l'utilisation malveillante. Il prévoit de présenter cette boite à outils au cours d'une conférence le jeudi 18 mars.

[11] Voir le Rapport du groupe de travail du RySG sur le DAAR (9 septembre 2020), une réponse par le directeur de la technologie de l'ICANN (30 septembre 2020) et la mise à jour fournie au GAC par l'OCTO (24 février 2021), plus récents.

Faits saillants

Aperçu des faits nouveaux

- **Au cours des récentes réunions de l'ICANN**, les responsables du PSWG du GAC ont présenté au GAC des exposés détaillés sur la question de l'utilisation malveillante du DNS (voir les documents des séances du GAC d'ICANN66 et d'CANN68, ainsi que la séance d'information du GAC de l'ICANN68 sur l'utilisation malveillante du DNS et la mise à jour fournie par le PSWG au GAC à l'occasion de l'ICANN69).
    - Le GAC a examiné les mesures mises à la disposition des opérateurs de registre et des bureaux d'enregistrement pour prévenir l'utilisation malveillante du DNS, en particulier le rôle des politiques d'enregistrement (y compris la vérification d'identité) et des stratégies de tarification comme déterminants clés des niveaux d'utilisation malveillante dans un TLD donné.
    - Le GAC a également examiné les initiatives en cours ou possibles pour aborder l'utilisation malveillante du DNS plus efficacement au niveau du Conseil d'administration et de l'organisation ICANN (voir les procès-verbaux de l'ICANN66, le Communiqué du GAC de l'ICANN68 et les procès-verbaux correspondants, ainsi que le Communiqué du GAC de l'ICANN69 et les procès-verbaux correspondants).
    - Le plan de travail du PSWG 2020- 2021 comprend tous ces domaines dans le cadre de l'objectif stratégique nº 1 visant à développer les capacités de lutte contre l'utilisation malveillante du DNS et d'atténuation de la cybercriminalité.

- **Recommandations de la Deuxième équipe de révision de la sécurité, la stabilité et la résilience du DNS**
    - L'équipe de la SSR2 a présenté un rapport préliminaire (24 janvier 2020) qui met l'accent sur les mesures visant à prévenir et à atténuer l'utilisation malveillante du DNS. Le commentaire du GAC (3 avril 2020) soutenait bon nombre des recommandations et notamment celles portant sur l'amélioration du système de signalement des cas d'utilisation malveillante des noms de domaine (DAAR) et le renforcement des mécanismes de conformité.
    - Le rapport final (25 janvier 2021) est maintenant soumis aux commentaires publics (clôture le 8 avril 2021). Des modifications notables ont été apportées à la structure du rapport. Les responsables chargés par le GAC de différents sujets examinent actuellement le rapport et proposeront au GAC une version préliminaire de commentaire pour examen.

- Il est prévu que **l'équipe de travail sur l'utilisation malveillante du DNS du Comité consultatif sur la sécurité et la stabilité (SSAC)** fasse rapport de ses activités et constats avant l'ICANN70.
    - Au cours de la réunion ICANN66, le SSAC a informé le PSWG de sa création d'une équipe de travail consacrée à l'utilisation malveillante du DNS, à laquelle **a participé un représentant du PSWG**.

- Depuis lors, le SSAC a signalé son intention de ne pas formuler une définition de l'utilisation malveillante du DNS. Au lieu de cela, l'équipe de travail devrait se concentrer sur les rôles des parties appropriées, étayant son travail sur les perspectives communautaires et les cadres existants. L'objectif du groupe de travail est de produire un rapport qui décrive les efforts potentiels pour normaliser les stratégies et les processus communautaires autour de la détection et l'atténuation des cas d'utilisation malveillante.

- **Mesures et initiatives concernant les opérateurs de registre et bureaux d'enregistrement et visant à atténuer l'utilisation malveillante du DNS**
  - Le 27 mars 2020, l'organisation ICANN a mis en œuvre la proposition de modification au contrat de registre .COM. Celle-ci étend **les dispositions contractuelles visant à faciliter la détection et le signalement des cas d'utilisation malveillante du DNS**, y compris la spécification 11 3b, **aux deux tiers de l'espace de noms des gTLD** (ces dispositions n'étaient applicables jusqu'à présent qu'aux nouveaux gTLD). En outre, une lettre d'intention contraignante entre l'organisation ICANN et Verisign a établi un cadre de coopération propre à permettre la mise au point de meilleures pratiques et de nouvelles obligations contractuelles potentielles, ainsi que des mesures visant à mesurer et à atténuer les menaces à la sécurité du DNS.
  - **Dans le contexte de la crise due à la COVID-19, les parties contractantes ont présenté les mesures prises et** les enseignements tirés avant et pendant la réunion ICANN68, tandis que les parties prenantes du PSWG ont fait état d'efforts en cours, concertés avec les États membres de l'UE, Europol, les ccTLD et les bureaux d'enregistrement, visant à faciliter les rapports, leur examen et leur renvoi à la juridiction compétente grâce à l'adoption d'un formulaire normalisé pour signaler les domaines/contenus liés à la COVID-19, ainsi que de l'établissement d'un point de contact unique pour les autorités compétentes. Ces efforts renforcent les relations de travail établies entre les organismes d'application de la loi et les bureaux d'enregistrement, et se situent dans le prolongement du Guide des bureaux d'enregistrement pour le signalement d'abus, publié par le **Groupe des représentants des bureaux d'enregistrement** et présenté lors de l'ICANN67.
  - **Le registre d'intérêt public (PIR**), opérateur de registre de .ORG et de plusieurs nouveaux gTLD, a lancé (le 17 février 2021) le **DNS Abuse Institute** dont l'objectif déclaré est de « *rassembler les leadeurs de l'espace de lutte contre l'utilisation malveillante pour : financer la recherche, publier des pratiques recommandées, partager les données et fournir des outils facilitant la détection et le signalement des cas d'utilisation malveillante du DNS* ». Cette initiative a été présentée au PSWG du GAC (3 mars 2021) en prévision d'un séminaire web qui sera organisé par l'Institut sur la situation de l'utilisation malveillante du DNS le 16 mars 2021.

- **Réponse multidimensionnelle de l'organisation ICANN et mesures garantissant le respect des clauses contractuelles**
  - Le 20 avril 2020, le PDG de l'ICANN a publié un blog détaillant la réponse multidimensionnelle de l'organisation ICANN à l'utilisation malveillante du DNS.

- **Le Bureau du directeur de la technologie (OCTO) de l'ICANN et son équipe consacrée à la sécurité, la stabilité et la résilience** (SSR) mènent des recherches et assurent l'expertise de l'ICANN en matière de sécurité du DNS au profit de la communauté. L'organisation participe à divers forums de renseignements sur les cybermenaces et de réponse aux incidents, notamment le Forum des équipes de sécurité et de réponse aux incidents (FIRST), le Groupe de travail anti-abus pour la messagerie, les programmes malveillants et les mobiles (M3AAWG), le Groupe de travail anti-hameçonnage (APWG), l'Alliance nationale d'informatique judiciaire et de formation contre la cybercriminalité (NCFTA) des États-Unis et, plus récemment, la Coalition contre les cybermenaces COVID-19 (CTC) et la Ligue de renseignement sur les cybermenaces COVID-19 (CTI).
  Elle met au point également des systèmes et des outils pour aider à détecter, analyser et signaler les cas d'utilisation malveillante du DNS :
  - En réponse à la crise de la COVID-19, l'OCTO a mis au point l'outil de **signalement et de collecte d'informations sur les menaces à la sécurité des noms de domaine (DNSTICR)** qui aide à recenser les noms de domaine utilisés de façon malveillante en lien avec la COVID-19 et à partager les données avec les parties concernées. Le GAC a été renseigné sur cette démarche avant l'ICANN68 (12 juin 2020), et l'ensemble de la communauté de l'ICANN, lors de la réunion ICANN68.
  - Grâce à sa **plateforme de signalement des cas d'utilisation malveillante des noms de domaine (DAAR)**, l'ICANN a informé mensuellement depuis janvier 2018 des comportements abusifs ou des menaces à la sécurité des noms de domaine observés dans le DNS. L'ICANN surveille également les tendances par le biais de ses indicateurs de santé des technologies des identificateurs (ITHI). Plusieurs parties prenantes et initiatives de l'ICANN ont commenté les limites du système DAAR, en particulier une lettre du M3AAWG à l'organisation ICANN (5 avril 2019) et le rapport préliminaire de l'équipe de la SSR2 (24 janvier 2020), que le GAC a soutenu (voir ci-dessous). Le Groupe des représentants des opérateurs de registre, qui avait également exprimé ses préoccupations vis-à-vis du DAAR et qui travaillait avec l'ICANN à le faire évoluer, a récemment formulé des recommandations dans sa correspondance adressée au CTO de l'ICANN (9 septembre 2020).
- L'OCTO de l'ICANN soutient également le **Goupe d'étude technique chargé de l'initiative de facilitation de la sécurité du DNS**, récemment établi (6 mai 2020) dans le cadre de la mise en œuvre du Plan stratégique pour les exercices fiscaux 2021 à 2025, dans le but de *« rechercher et d'étudier des idées concernant ce que l'ICANN peut et doit faire pour accroitre la concertation et l'engagement avec les parties prenantes de l'écosystème du DNS et, essentiellement, renforcer le niveau de sécurité du DNS »*. Des recommandations devraient être publiées d'ici mai 2021.
- Au cours d'un appel du GAC sur la question de l'utilisation malveillante du DNS (24 février 2021), **l'ICANN org a fourni des mises à jour sur les activités de l'OCTO** dans ce domaine, ce qui a compris une discussion sur la définition des menaces à la sécurité du DNS et de l'utilisation malveillante du DNS, les obligations des parties contractantes, le signalement

des cas d'utilisation malveillante des noms de domaine (DAAR), l'information sur les menaces à la sécurité des noms de domaine, la collecte et les rapports (DNSTICR), l'état de l'initiative de facilitation de la sécurité des noms de domaine (DSFI), la nouvelle initiative de mise en commun des connaissances et d'instauration de normes pour la sécurité des noms de domaine (KINDNS), ainsi que le passage en revue des efforts de l'OCTO dans le domaine de la formation et du renforcement des capacités dans le monde entier.

- **Garantir le respect des clauses contractuelles** : dans son blog (20 avril 2020), le PDG de l'ICANN a rappelé ce qui suit : « *le service Conformité de l'ICANN veille au respect des obligations établies dans les politiques et les contrats de l'ICANN, en particulier le contrat de registre (RA) et le contrat d'accréditation des bureaux d'enregistrement (RAA). Par ailleurs, ce service travaille en étroite collaboration avec l'OCTO à identifier des menaces à la sécurité du DNS [...] et à les relier aux parties contractantes concernées. Il utilise des données collectées pendant les audits [...] pour évaluer si les opérateurs de registres et les bureaux d'enregistrement se conforment à leur obligation d'atténuation de risques à la sécurité du DNS. En dehors de ces audits, le service utilise les données collectées par l'OCTO et d'autres pour contacter de manière proactive des opérateurs de registres 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 service n'hésite 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 ».* Le blog a également fourni un aperçu du volume des plaintes, des ressources allouées à leur traitement et des statistiques sur la résolution de ces plaintes.

Arrêt sur : la définition de l'utilisation malveillante du DNS

Comme souligné récemment lors du Sommet de la GDD (7 à 9 mai 2019), il n'existe **pas d'accord communautaire sur ce qui constitue une « utilisation malveillante du DNS », en partie à cause des inquiétudes de certaines parties prenantes qui craignent que l'**, en partie à cause des inquiétudes de certaines parties prenantes qui craignent que l'ICANN outrepasse son mandat, des répercussions sur les droits des utilisateurs et de l'impact sur le bénéfice net des parties contractantes[12].

Cependant, selon l'équipe de révision CCT, il existe **un consensus sur ce qui constitue « une menace à la sécurité du DNS » ou « une atteinte à la sécurité de l'infrastructure du DNS** », qui l'une comme l'autre incluent « davantage de formes techniques d'activité malveillante », parmi lesquelles les logiciels malveillants, l'hameçonnage et les réseaux zombies, ainsi que le courrier indésirable *« lorsqu'il sert de méthode de diffusion d'autres formes d'utilisation malveillante »* [13].

Récemment, **le département de l'ICANN en charge de la conformité contractuelle a fait référence à « l'atteinte à la sécurité de l'infrastructure du DNS » et aux « menaces à la sécurité »** dans ses communications relatives aux audits des registres et des bureaux d'enregistrement portant sur leur mise en œuvre de dispositions contractuelles du contrat de registre des nouveaux gTLD (spécification 11 3b) qui visent les « *menaces à la sécurité comme le dévoiement, l'hameçonnage, les logiciels malveillants et les réseaux zombie*s »[14] et du contrat d'accréditation de bureau d'enregistrement (article 3.18) qui font référence à des « *points de contact pour l'utilisation malveillante* » et à des « *signalements des cas d'utilisation malveillante* » sans donner de définition spécifique du terme « utilisation malveillante », mais en y incluant les « activités illégales ».

Du point de vue du GAC, la définition de « menaces à la sécurité » dans le contrat de registre des nouveaux gTLD est en réalité la transcription de **la définition que donne le GAC dans son avis relatif aux sauvegardes du** communiqué de Beijing (11 avril 2013) et qui peut s'appliquer à l'ensemble des nouveaux gTLD.

Suite à la résolution du Conseil d'administration de l'ICANN (1er mars 2019) enjoignant à l'organisation ICANN de « *faciliter les efforts communautaires visant à définir "l'utilisation malveillante" afin d'éclairer les futures mesures à prendre concernant cette recommandation* ».[15]

---

12 En effet, la définition de l'atténuation de l'utilisation malveillante peut avoir des conséquences sur la portée des activités supervisées par les contrats et politiques de l'ICANN. Alors que certains gouvernements ainsi que d'autres parties prenantes craignent l'impact de l'utilisation malveillante du DNS sur l'intérêt public, dont la sécurité du public et la violation des droits de propriété intellectuelle, les registres et bureaux d'enregistrement s'inquiètent des restrictions sur leurs activités commerciales, de leur aptitude à faire la concurrence, de l'augmentation des couts de fonctionnement et de la responsabilité que pourraient devoir assumer les titulaires de noms de domaine si une mesure était prise à l'encontre des domaines malveillants. De leur côté, les parties prenantes non commerciales s'inquiètent de la violation de la liberté d'expression et le respect de la vie privée des titulaires de noms de domaine et des utilisateurs Internet, et partagent avec des parties contractantes des inquiétudes concernant le fait que l'ICANN outrepasse sa mission.

13 Voir p. 88 du rapport final de la révision CCT (8 septembre 2018) qui a été mentionné plus récemment dans la déclaration du GAC sur l'utilisation malveillante du DNS (18 septembre 2019).

14 Le bulletin d'information sur la spécification 11 (3)(b) du contrat de registre pour les nouveaux gTLD (8 juin 2017) donne une définition de « menaces à la sécurité » en incluant « le dévoiement, l'hameçonnage, les logiciels malveillants et les réseaux zombie, ainsi que d'autres types de menaces à la sécurité. »

15 Voir p. 5 de la fiche de suivi des décisions du Conseil d'administration sur les recommandations finales de la révision CCT.

Lors d'un séminaire web pré-ICANN66 du 15 octobre 2019, **le PSWG et les parties contractantes ont discuté des problèmes actuels et des pratiques du secteur**. Dans la perspective de ce séminaire web, le Groupe des représentants des opérateurs de registre avait publié une lettre ouverte (19 aout 2019) faisant part des opinions des registres sur la définition de l'utilisation malveillante du DNS, des options limitées dont les registres disposent afin de prendre des mesures répondant aux menaces à la sécurité, et de leurs craintes au sujet du système de signalement des cas d'utilisation malveillante des noms de domaine de l'ICANN.

Ce à quoi le GAC a répondu en publiant une déclaration sur l'utilisation malveillante du DNS (18 septembre), puis l'Unité constitutive des utilisateurs commerciaux a fait de même (28 octobre). Dans sa déclaration sur l'utilisation malveillante du DNS (18 septembre 2019), le GAC a accepté la définition de l'utilisation malveillante du DNS de l'équipe de révision de la CCT, à savoir, « *les activités intentionnellement trompeuses, complaisantes ou non sollicitées qui utilisent activement le DNS ou les procédures utilisées pour enregistrer des noms de domaine »,* qui, en termes techniques, peuvent prendre la forme de menaces à la sécurité telles que *« les logiciels malveillants, l'hameçonnage, les réseaux zombies, et le spam lorsqu'ils sont utilisés pour exécuter ces formes d'abus* ». Le GAC a reconnu que le Contrat de registre des nouveaux gTLD fait ressortir cette idée dans la spécification 11, en particulier les articles 3a[16] et 3b[17].

À la suite de la publication de la déclaration du GAC sur l'utilisation malveillante du DNS (18 septembre 2019), un ensemble **d'opérateurs de registre et de bureaux d'enregistrement de gTLD de première ligne ont proposé** un cadre volontaire de lutte contre l'utilisation malveillante (17 octobre 2019). On notera tout particulièrement que ce cadre prévoit, au titre des actions éventuelles à mener par ses adhérents, certaines formes d'« utilisation malveillante du contenu d'un site web » qu'il considère « tellement inacceptable que la partie contractante est tenue d'agir après en avoir pris connaissance de façon spécifique et fiable ». Depuis sa publication et sa discussion au cours de l'ICANN66, la liste des signataires de ce cadre s'est élargie pour inclure d'autres fournisseurs de services de registre et de bureaux d'enregistrement de gTLD de première ligne, ainsi qu'un certain nombre de petits acteurs de l'industrie.

Le 18 juin 2020, les présidents du **groupe des représentants des bureaux d'enregistrement et le groupe des représentants des opérateurs de registre** (collectivement appelés la Chambre des parties contractantes de la GNSO, ou CPH) ont annoncé aux dirigeants de la communauté avoir

[16] La spécification 13 11 3a établit que *« Les opérateurs de registre incluront dans leurs contrats entre opérateurs de registre et bureaux d'enregistrement (RRA) une disposition en vertu de laquelle ces derniers devront inclure dans leurs contrats d'enregistrement une clause interdisant aux titulaires de noms enregistrés la distribution de programmes malveillants, réseaux zombies abusifs, hameçonnage, piraterie, violation de marques ou de propriété intellectuelle, pratiques frauduleuses ou nuisibles, contrefaçon ou autres modalités contraires aux lois applicables, et prévoir (conformément aux lois en vigueur et aux procédures y afférentes) des conséquences pour ce genre d'activités, y compris la suspension du nom de domaine ».*

[17] La spécification 11 3b établit que « *L'opérateur de registre procèdera périodiquement à une analyse technique afin d'évaluer si les domaines de son TLD sont utilisés pour perpétrer des menaces à la sécurité comme le dévoiement, l'hameçonnage, les logiciels malveillants et les réseaux zombies. L'opérateur de registre devra assurer des rapports statistiques sur le nombre des menaces à la sécurité recensées et sur les mesures prises suite aux vérifications périodiques en matière de sécurité. L'opérateur de registre continuera à produire ces rapports pendant la durée du contrat, sauf si un délai plus court est requis par la loi ou approuvé par l'ICANN, et il les présentera à l'ICANN sur demande. »*

adopté une définition de l'utilisation malveillante du DNS qui reprend exactement celle du Cadre de lutte contre l'utilisation malveillante élaboré par les acteurs de l'industrie :

> *L'utilisation malveillante du DNS se compose de cinq grandes catégories d'activités nuisibles dans la mesure où elles intersectent avec le DNS : logiciels malveillants, réseaux zombies, hameçonnage, dévoiement et spam lorsqu'ils servent à diffuser d'autres formes d'utilisation malveillante du DNS* [en référence aux approches opérationnelles, aux normes, aux critères et aux mécanismes du Réseau des politiques Internet et juridictions pour définir chacune de ces activités].

Cette définition **semble confirmer ce que l'équipe de révision de la CCT a appelé un consensus existant sur ce qui constitue « une menace à la sécurité du DNS ou une atteinte à la sécurité de l'infrastructure du DNS** » (Rapport final de la CCT, p. 8) et s'accorde avec la **définition illustrative des « menaces de sécurité » du GAC** figurant au titre des « vérifications de la sécurité » de l'avis du GAC relatif aux sauvegardes applicables à tous les nouveaux gTLD du Communiqué de Beijing (11 avril 2013) et incorporée dans le contrat de registre de gTLD, à la Spécification 11 3b.

Arrêt sur : les sauvegardes relatives à l'utilisation malveillante du DNS prévues dans le contrat de registre et le contrat de bureau d'enregistrement

En s'appuyant sur les recommandations en matière de diligence raisonnable et d'application de la loi (octobre 2009), le GAC a cherché à inclure **des sauvegardes visant l'atténuation de l'utilisation malveillante du DNS dans les contrats de l'ICANN** avec les registres et bureaux d'enregistrement :

- Le contrat d'accréditation de bureau d'enregistrement de 2013 (17 septembre 2013) a été approuvé par le Conseil d'administration de l'ICANN (27 juin 2013) après y avoir intégré des dispositions répondant aux12 recommandations des organismes d'application de la loi (1er mars 2012).
- Le contrat de registre des nouveaux gTLD a été approuvé par le Conseil d'administration de l'ICANN (2 juillet 2013) après y avoir intégré des dispositions relatives à l'avis du GAC relatif aux sauvegardes du Communiqué de Beijing (11 avril 2013), dans le respect de la proposition du Conseil d'administration pour la mise en œuvre des sauvegardes du GAC applicables à l'ensemble des nouveaux gTLD (19 juin 2013).

Après les premières années de fonctionnement des nouveaux gTLD, lors de l'ICANN57, **le GAC a recensé un certain nombre de dispositions et de sauvegardes connexes dont il ne pouvait évaluer l'efficacité.** Par conséquent, dans son Communiqué d'Hyderabad (8 novembre 2016), le GAC a demandé au Conseil d'administration de l'ICANN des éclaircissements quant à leur mise en œuvre. Des échanges ont alors eu lieu entre le GAC et l'organisation ICANN, avec des questions de suivi dans le Communiqué de Copenhague du GAC (15 mars 2017) et un ensemble de réponses préliminaires (30 mai 2017) qui ont été abordées lors d'une téléconférence entre le GAC et le président-directeur général de l'ICANN (15 juin 2017). Plusieurs questions sont restées ouvertes et de nouvelles questions ont émergé, comme le reflète le document de travail ultérieur (17 juillet 2017).

Parmi les principaux sujets d'intérêt du GAC, un avis sur la spécification 11 (3)(b) du contrat de registre pour les nouveaux gTLD a été publié le 8 juin 2017 en réponse aux questions de certains opérateurs de registre qui cherchaient à savoir comment garantir la conformité avec l'article 3b de la spécification 11 du contrat de registre des nouveaux gTLDhttps://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.html - specification11. **Cet avis propose une démarche volontaire que les opérateurs de registre peuvent adopter** pour effectuer des analyses techniques permettant d'évaluer les menaces à la sécurité et de produire des rapports statistiques, comme requis par la spécification 11.3b.

Dans le cadre des **audits réguliers que mène le département contractuel de l'ICANN**, un audit ciblé de 20 gTLD a été effectué entre mars et septembre 2018. Cet audit, qui a porté sur **les « processus, procédures et gestion de l'infrastructure du DNS »,** *a révélé* « *des analyses et des rapports de sécurité incomplets pour 13 domaines de premier niveau (TLD), un manque de procédures normalisées ou documentées de traitement des cas d'utilisation malveillante et aucune*

mesure prise contre des menaces détectées »[18]. Peu après, en novembre 2018, un audit sur les atteintes à l'infrastructure du DNS concernant quasiment l'ensemble des gTLD a été mené afin de « *s'assurer que les parties contractantes respectent leurs obligations contractuelles au regard des menaces à la sécurité et aux atteintes à l'infrastructure du DNS* ». Dans son rapport du dernier audit (17 septembre 2019), l'ICANN est arrivée aux conclusions suivantes :

- La grande majorité des opérateurs de registre se sont engagés à lutter contre les menaces à la sécurité du DNS.
- Seul un petit nombre d'opérateurs de registre est associé à une fréquence élevée de menaces à la sécurité du DNS.
- La façon dont certains des opérateurs de registre interprètent le libellé de la spécification 11 3(b) rend difficile de jauger la conformité et l'efficacité des efforts qu'ils entreprennent pour atténuer les menaces à la sécurité du DNS.

Certaines parties contractantes ont contesté ces audits, car ils dépasseraient la portée de leurs obligations contractuelles[19]. L'organisation ICANN a fait savoir qu'elle entreprendrait un audit des bureaux d'enregistrement qui serait axé sur les menaces à la sécurité du DNS.

Arrêt sur : le cadre non contraignant de mesures à mettre en œuvre par les registres pour répondre à des menaces à la sécurité

Dans le cadre du programme des nouveaux gTLD, le Conseil d'administration de l'ICANN a adopté une résolution (25 juin 2013) par laquelle il inclut lesdites « menaces à la sécurité » (avis du GAC relatif aux sauvegardes formulé dans le Communiqué de Beijing) dans la Spécification 11 du contrat de registre des nouveaux gTLD. Toutefois, ayant déterminé que ces dispositions ne comportaient pas toutes les modalités de mise en œuvre, il a décidé de solliciter la participation de la communauté afin d'élaborer un cadre qui permette aux « *opérateurs de registre de faire face à des risques détectés en matière de sécurité qui posent un réel risque de préjudice* (…) ».
En juillet 2015, l'ICANN forme une équipe de rédaction composée de volontaires provenant des registres, des bureaux d'enregistrement et du GAC (dont des membres du PSWG). L'équipe élabore le cadre de mesures à mettre en œuvre par les opérateurs de registre pour répondre à des menaces à la sécurité, publié le 20 octobre 2017 après avoir été soumis aux commentaires publics.

[18] Tel qu'indiqué dans l'article de blog du 8 novembre 2018 intitulé Conformité contractuelle : répondre aux atteintes à l'infrastructure du DNS : https://www.icann.org/news/blog/contractual-compliance-addressing-domain-name-system-dns-infrastructure-abuse

[19] Voir les correspondances du RySG (2 novembre 2019) auxquelles l'organisation ICANN a répondu (8 novembre), et les commentaires postés sur la page de l'a répondu (8 novembre), et les commentaires postés sur la page de l'annonce (15 novembre) : les registres se sont inscrits en faux contre les questions de l'audit, les considérant comme brandissant la menace des mesures d'exécution contractuelles bien au-delà de la portée des obligations incombant aux registres [en particulier selon la spécification 11 3b], et ont indiqué leur réticence à « *partager avec l'organisation ICANN et la communauté de l'ICANN des informations pertinentes concernant nos efforts en cours visant à lutter contre l'utilisation malveillante du DNS […] dans le cadre d'un effort de conformité de l'ICANN qui va au-delà de ce qui est autorisé par le contrat de registre* ».

Ce cadre est un instrument volontaire et non contraignant visant à orienter les registres sur la manière dont ils peuvent répondre aux menaces de sécurité détectées, et pouvant inclure les rapports des organismes d'application de la loi. Il introduit une fenêtre de 24 h maximum pour répondre aux demandes hautement prioritaires (menace imminente pour la vie humaine, infrastructure critique ou exploitation de mineurs) provenant « *d'une source crédible et légitime* » comme « *une autorité nationale d'application de la loi ou une agence de sécurité publique d'une juridiction compétente* ».

Conformément à sa recommandation 19, l'équipe de révision CCT a reporté le travail d'évaluation de l'efficacité du cadre à une prochaine révision[20], le cadre n'existant pas depuis assez longtemps pour que son efficacité puisse être évaluée.

[20] Recommandation 19 de l'équipe de révision CCT : la prochaine CCT-RT devrait examiner le « cadre de mesures à mettre en œuvre par les opérateurs de registre pour répondre à des menaces à la sécurité » et déterminer si ce cadre constitue un mécanisme suffisamment clair et efficace, propre à réduire l'utilisation malveillante en proposant des mesures systémiques et d'autres ciblées en réponse aux menaces pour la sécurité.

Arrêt sur : l'examen des recommandations de l'équipe de révision CCT au sujet de l'utilisation malveillante du DNS

À partir de son analyse du paysage de l'utilisation malveillante du DNS[21], et en tenant notamment compte du rapport de l'ICANN sur les sauvegardes du programme des nouveaux gTLD (15 mars 2016) et de l'analyse statistique indépendante de l'utilisation malveillante du DNS (9 aout 2017), l'équipe de révision CCT a recommandé, en lien avec cette problématique :

- l'intégration, **dans les contrats de registre, de dispositions visant à encourager l'adoption de mesures proactives de lutte contre l'utilisation malveillante** (recommandation 14) ;
- l'intégration de dispositions contractuelles visant à **empêcher une utilisation systémique de bureaux d'enregistrement ou registres spécifiques** pour l'utilisation malveillante du DNS, avec notamment des seuils de cas d'utilisation malveillante qui déclenchent automatiquement des enquêtes de conformité, tout en envisageant une politique de règlement de litiges relatifs à l'utilisation malveillante du DNS (DADRP) si la communauté détermine que l'organisation ICANN elle-même n'est pas adaptée ou pas en mesure d'appliquer ces dispositions (recommandation 15).

Le Conseil d'administration de l'ICANN a adopté une résolution (1er mars 2019) par laquelle il met ces recommandations « en attente », ayant demandé à l'organisation ICANN de « *faciliter les efforts communautaires visant à définir "l'utilisation malveillante" afin d'éclairer les futures mesures à prendre concernant cette recommandation* ».[22]

À la lumière de l'avis contenu dans le Communiqué du GAC de Montréal (6 novembre 2019) à l'intention du Conseil d'administration de l'ICANN de *« ne pas procéder à une nouvelle série de gTLD avant la mise en œuvre complète des recommandations [...] identifiées comme "conditions préalables" ou "à priorité élevée"*, et de la réponse du Conseil à cet avis (26 janvier 2020), le PSWG continue de surveiller l'examen des principales recommandations de la CCT-RT (6 septembre 2018) visant à l'adoption de dispositions contractuelles pour encourager des mesures proactives de lutte contre l'utilisation malveillante (rec. 14) et à la prévention de l'utilisation systémique des opérateurs de registre et des bureaux d'enregistrement pour utiliser le DNS à des fins malveillantes (rec. 15) ; à l'amélioration de la recherche sur l'utilisation malveillante du DNS (rec. 16) ; à l'amélioration de l'exactitude du WHOIS (rec. 18) ; et à l'efficacité du traitement des plaintes liées à la conformité contractuelle (rec. 20).

Le PSWG analyse également la résolution du Conseil d'administration d'aller de l'avant avec le plan de mise en œuvre de l'ICANN (23 aout 2019) pour les recommandations de la CCT qui ont été acceptées dans la fiche de suivi des décisions du Conseil d'administration de l'ICANN (1er mars 2019). Le GAC a commenté (21 octobre 2019) ce plan et a fait remarquer certaines lacunes concernant des recommandations importantes pour lutter contre l'utilisation malveillante du DNS, y compris la publication de la chaine des parties responsables des enregistrements de noms de

[21] Voir article 9 des sauvegardes (p.88) dans le rapport final de révision CCT (8 septembre 2018)

[22] Voir p. 5 de la fiche de suivi des décisions du Conseil d'administration sur les recommandations finales de la révision CCT.

domaine gTLD (rec. 17), des renseignements plus détaillés sur les plaintes relatives à la conformité contractuelle (rec. 21) et des mesures de sécurité correspondant à l'offre de services qui impliquent la collecte d'informations sensibles sur la santé et les finances (rec. 22).

Dans le sillage de l'adoption par les parties contractantes d'une définition de l'utilisation malveillante du DNS, le **GAC a demandé au Conseil d'administration de l'ICANN, pendant l'ICANN68** (voir les documents de la réunion GAC/Conseil d'administration du 24 juin 2020)**, des clarifications** liées à la mise en œuvre de la Rec. 14 de la CCT-RT (« *l'ICANN devrait négocier des dispositions contractuelles proposant des incitations financières aux parties contractantes pour qu'elles adoptent des mesures proactives de lutte contre l'utilisation malveillante*). Plus précisément, ces clarifications concernaient l'état d'avancement et le plan s'agissant de la facilitation des efforts communautaires visant à définir « l'utilisation malveillante » et à éclairer les décisions du Conseil d'administration sur cette recommandation. Le GAC a enregistré dans ses procès-verbaux de l'ICANN68 que « *le Conseil continuera de soutenir le dialogue communautaire comme il l'a fait en facilitant les discussions régionales et intercommunautaires, en menant des recherches et en mettant au point des outils pour aider à informer les discussions communautaires, et en fournissant des orateurs sur demande* ».

Au cours de la réunion ICANN68, le PSWG et les parties prenantes de l'ALAC ont constaté que les progrès sur la mise en œuvre de la recommandation acceptée de la CCT-RT et sur l'examen de la recommandation en attente ne sont pas clairs. De l'insatisfaction a également été exprimée par rapport à une communication récente (29 avril 2020) du **groupe de travail de la GNSO chargé du processus d'élaboration de politiques concernant des procédures pour des séries ultérieures de nouveaux gTLD** selon laquelle ce dernier « *n'envisage pas de formuler des recommandations sur l'atténuation de l'utilisation malveillante des noms de domaine autre que celle suggérant que toute future initiative à cet égard s'applique à la fois aux gTLD existants et aux nouveaux gTLD (et éventuellement aux ccTLD) ».* Et ce en dépit des recommandations pertinentes que l'équipe de révision CCT lui a adressées, également soutenues par les décisions du Conseil d'administration de l'ICANN, par l'avis du Communiqué du GAC de Montréal (6 novembre 2019) et par d'autres apports du GAC consignés dans le Communiqué du GAC de l'ICANN67 (16 mars 2020).

Dans son rapport final (1er février 2021), le Groupe de travail de la GNSO chargé du processus d'élaboration de politiques concernant des procédures pour des séries ultérieures de nouveaux gTLD a confirmé sa décision[23]. Dans ses Commentaires (29 septembre 2020), le GAC s'est dit vivement préoccupé de cette décision émise par le groupe de travail PDP dans la version préliminaire du rapport final et a affirmé compter sur le conseil de la GNSO pour intervenir rapidement à ce sujet.

[23] Voir la recommandation 9.15 (p. 42) du Rapport final du groupe de travail Sub Pro PDP.

Arrêt sur : la discussion sur l'élaboration d'une politique de la GNSO relative à l'atténuation de l'utilisation malveillante du DNS

Suivant la décision initiale du Groupe de travail de la GNSO chargé du processus d'élaboration de politiques concernant des procédures pour des séries ultérieures de nouveaux gTLD de ne pas formuler de recommandation sur l'utilisation malveillante du DNS pour les futurs contrats de nouveaux gTLD, le **conseil de la GNSO a discuté**, lors de sa réunion du 21 mars 2020, de **la possibilité de créer un groupe de travail intercommunautaire (CCWG)** consacré à la question de l'utilisation malveillante du DNS, et éventuellement un PDP de la GNSO s'il s'avère nécessaire de rédiger de nouvelles exigences contractuelles.

Elle n'a pas examiné la proposition informelle des dirigeants du GAC (12 mai 2020) d'organiser une séance d'intérêt commun entre des experts en la matière, dont des opérateurs des ccTLD, afin de déterminer le champ d'action d'une future politique.

En date du 18 février 2021, cette question est toujours désignée comme « non planifiée » dans l'inventaire des décisions et des mesures à prendre du conseil de la GNSO, le Conseil du GNSO devant « *déterminer les prochaines étapes, le cas échéant, concernant l'utilisation malveillante du DNS* ». La direction du GAC et les responsables chargés des thèmes pertinents doivent discuter de cette question lors d'un appel de la direction du GAC/de la GNSO avant ICANN70 (8 mars 2021), en préparation de la réunion du GAC de l'ICANN70 avec la GNSO (24 mars 2021).

Arrêt sur : le signalement des cas d'utilisation malveillante des noms de domaine (DAAR)

Le projet de signalement des cas d'utilisation malveillante des noms de domaine de l'organisation ICANN est venu s'ajouter, sous la forme d'un projet de recherche, aux séances d'échange du PSWG et du GAC avec le Conseil d'administration et la communauté de l'ICANN sur l'efficacité des mesures d'atténuation de l'utilisation malveillante du DNS, entre l'ICANN57 (novembre 2016) et l'ICANN60 (novembre 2017)[24].

L'objectif déclaré du DAAR est de « *signaler les menaces à la sécurité à la communauté de l'ICANN, afin que celle-ci puisse ensuite se servir de ces données pour prendre des décisions de politique en connaissance de cause* ». Cet objectif est atteint depuis janvier 2018 avec la publication de rapports mensuels fondés sur la compilation des données d'enregistrement TLD avec des informations provenant d'un imposant ensemble de flux de données hautement fiables relatives à la réputation et aux menaces à la sécurité[25].

À cet effet, le DAAR contribue aux exigences que le GAC a définies dans le Communiqué du GAC d'Abu Dhabi (1er novembre 2017) pour la publication de « données détaillées et fiables sur l'utilisation malveillante du DNS ». Cependant, comme le souligne une lettre envoyée par le M3AAWG[26] à l'organisation ICANN (en date du 5 avril 2019), étant donné qu'il n'intègre pas encore les informations relatives aux menaces à la sécurité pour chaque bureau d'enregistrement et chaque TLD, le DAAR n'est toujours pas à la hauteur des attentes des membres du PSWG du GAC et de leurs partenaires de cybersécurité qui espéraient qu'il apporterait des informations exploitables.

Récemment, les registres ont indiqué dans une lettre ouverte (en date du 19 aout 2019) qu'ils échangeaient avec le bureau du directeur de la technologie de l'ICANN « *afin d'analyser le DAAR et de recommander ainsi à l'OCTO des améliorations visant à permettre au DAAR de mieux remplir sa mission et de fournir à la communauté de l'ICANN de précieuses ressources* ». Bien que les registres aient reconnu que « *certains membres de la communauté peuvent se baser sur les données fournies dans le système de signalement des cas d'utilisation malveillante des noms de domaine (DAAR) de l'ICANN afin de fonder des plaintes pour utilisation malveillante systémique ou généralisée du DNS* », ils estiment que « *l'outil comporte d'importantes limites, ne peut être raisonnablement invoqué afin de signaler, précisément et de manière fiable, la présence de menaces à la sécurité, et n'atteint pas encore ses objectifs* ».

Le Groupe des représentants des opérateurs de registre a rendu compte de ses travaux dans son rapport du groupe de travail sur le DAAR (9 septembre 2020), auquel le CTO de l'ICANN a répondu (30 septembre 2020) : « *La majorité des recommandations que contient la lettre mettent l'accent sur l'amélioration de la transmission des données exportées du système DAAR, car cette*

[24] Voir les séances intercommunautaires menées par le PSWG du GAC lors de l'ICANN57 (novembre 2016), l'ICANN58 (mars 2017) et l'ICANN60 (octobre 2017), ainsi que les questions posées au Conseil d'administration de l'ICANN concernant l'efficacité des sauvegardes en cas d'utilisation malveillante du DNS dans le communiqué d'Hyderabad (8 novembre 2016), les questions de suivi dans le Communiqué du GAC de Copenhague (15 mars 2017) et un ensemble de réponses préliminaires (30 mai 2017) de l'organisation ICANN.

[25] Pour de plus amples informations, consulter l'adresse suivante : https://www.icann.org/octo-ssr/daar-faqs.

[26] Groupe de travail anti-abus pour la messagerie, les programmes malveillants et les mobiles.

transmission est considérée par le groupe de travail comme potentiellement peu claire, tant au regard de la documentation sur la méthodologie actuelle du DAAR qu'au regard des rapports mensuels du DAAR. Si la plupart des recommandations portent sur des changements spécifiques au rapport, certaines (comme la recommandation 3 qui demande de mesurer la « persistance » des activités malveillantes signalées) peuvent nécessiter une enquête et une analyse à plus long terme ».

Au cours de la mise à jour de l'OCTO au GAC (24 février 2021), le CTO de l'ICANN a discuté des plans de développement futur du DAAR, notamment : l'ajout d'autres ccTLD au champ d'application du DAAR, la poursuite de la collaboration avec le groupe de travail du RySG qui se consacre au DAAR et la recherche et l'analyse de solutions pour surmonter les difficultés d'accès aux données WHOIS afin de mettre au point des indicateurs au niveau des bureaux d'enregistrement, portant sur : les requêtes WHOIS quotidiennes uniquement pour les domaines bloqués, l'échantillonnage aléatoire des domaines ou l'obtention de l'autorisation d'utiliser les données de l'accès aux données d'enregistrement en masse (BRDA).

Positions actuelles

Les positions actuelles du GAC sont indiquées ci-dessous dans l'ordre chronologique inversé :

- Le Communiqué du GAC de l'ICANN69 (23 octobre 2020) notant la conviction du GAC que, « *à l'heure actuelle, on observe un large appui, fermement exprimé, en faveur de la prise de mesures concrètes pour la mise en place des principales composantes d'une atténuation efficace de l'utilisation malveillante du DNS* » à la lumière d'un élan croissant et d'un dialogue constructif au sein de la communauté de l'ICANN (voir section IV.2 p.6).
- Le Communiqué du GAC de l'ICANN68 (27 juin 2020) notant « *que les nouveaux efforts entrepris pour lutter contre l'utilisation malveillante du DNS ne devraient pas remplacer, mais plutôt compléter, les initiatives existantes visant à améliorer l'exactitude des données d'enregistrement, telles que le système de signalement de problèmes liés à l'exactitude du WHOIS, et à mettre en œuvre la politique relative aux services d'anonymisation et d'enregistrement fiduciaire, qui est actuellement en attente* » (voir Section IV.3 p.7).
- Le Commentaire du GAC (3 avril 2020) sur le rapport préliminaire de l'équipe de révision SSR2.
- Le Commentaire du GAC sur le rapport final de la révision des recommandations de la RDS-WHOIS2 (23 décembre 2019).
- La Déclaration du GAC sur l'utilisation malveillante du DNS (18 septembre 2019).
- Le Commentaire du GAC sur le rapport final de la révision CCT et de ses recommandations (11 décembre 2018).
- Le Commentaire du GAC (16 janvier 2018) sur les nouveaux articles du rapport préliminaire de l'équipe de révision CCT (27 novembre 2017).
- Le Commentaire du GAC sur l'analyse statistique de l'utilisation malveillante du DNS dans les gTLD (19 septembre 2017).

- Le Commentaire du GAC sur le rapport sur les sauvegardes du programme des nouveaux gTLD pour réduire les risques d'utilisation malveillante du DNS (21 mai 2016).
- Le Communiqué de Barcelone du GAC (25 octobre 2018), en particulier les articles III.2 Groupe de travail du GAC sur la sécurité publique (p.3) et IV.2 Le WHOIS et les lois de protection des données (p.5).
- Le Communiqué de Copenhague du GAC (15 mars 2017) comprenant l'avis relatif à l'avis relatif à l'atténuation de l'utilisation malveillante, où le GAC demandait des réponses à la fiche de suivi du GAC à l'annexe 1 du Communiqué d'Hyderabad (p. 11 à 32).
- Le Communiqué d'Hyderabad du GAC (8 novembre 2016) comprenant l'avis relatif à l'avis relatif à l'atténuation de l'utilisation malveillante, où le GAC demandait des réponses à l'annexe 1 : questions au Conseil d'administration de l'ICANN sur l'atténuation de l'utilisation malveillante du DNS par l'ICANN et les parties contractantes (p.14 à 17).
- Le Communiqué de Beijing du GAC (11 avril 2013), en particulier concernant les sauvegardes relatives aux « vérifications de sécurité » applicables à tous les nouveaux gTLD (p.7).
- Le Communiqué de Dakar du GAC (27 octobre 2011) article III. Recommandations des organismes d'application de la loi.
- Le Communiqué de Nairobi du GAC (10 mars 2010) article VI. Recommandations relatives à la diligence raisonnable dans l'application de la loi.
- Les Recommandations des organismes d'application de la loi concernant les modifications au contrat de registre (1er mars 2012).
- Les Recommandations relatives à la diligence raisonnable et l'application de la loi (octobre 2009).

Principaux documents de référence

- Documents du GAC sur l'utilisation malveillante du DNS
    - Séance d'information du GAC de l'ICANN68 sur l'utilisation malveillante du DNS (18 juin 2020).
    - Questions du GAC sur l'atténuation de l'utilisation malveillante et réponses préliminaires de l'ICANN (30 mai 2017) conformément à l'avis formulé dans le Communiqué d'Hyderabad du GAC (8 novembre 2016) et le suivi contenu dans le Communiqué de Copenhague du GAC (15 mars 2017).
- Définition de l'utilisation malveillante du DNS (entre autres, le point de vue des parties prenantes de l'industrie)
    - La définition de l'utilisation malveillante du DNS selon les parties contractantes (octobre 2020).
    - Le Cadre de lutte contre l'utilisation malveillante (17 octobre 2019).
    - La Déclaration du GAC sur l'utilisation malveillante du DNS (18 septembre 2019).
- Rapport final de la SSR2 (25 janvier 2021)
- RDS-WHOIS2
    - La fiche de suivi des décisions du Conseil d'administration de l'ICANN (25 février 2020) concernant les recommandations finales de la RDS-WHOIS2.
    - Les recommandations de la RDS/WHOIS2 (8 septembre 2019).
- Révision de la concurrence, la confiance et le choix du consommateur
    - Les recommandations et le rapport final de la révision CCT (8 septembre 2018), en particulier l'article 9 sur les sauvegardes (p. 88).
    - La fiche de suivi des décisions du Conseil d'administration sur les recommandations finales de la révision CCT (1er mars 2019).
    - L'analyse statistique de l'utilisation malveillante du DNS (9 aout 2017).

Gestion des documents

Réunion	Forum virtuel de la communauté - ICANN68, 22 à 25 juin 2021
Titre	Atténuation de l'utilisation malveillante du DNS
Distribution	Membres du GAC (avant la réunion) et public (après la réunion)
Date de distribution	Version 1 : 11 mars 2021