ICANN | GAC
Governmental Advisory Committee

ICANN 68
VIRTUAL POLICY FORUM
22–25 June 2020

# Atténuation de l'utilisation malveillante du DNS

## Séances 2 et 8

## Table des matières



### Objectifs des séances

Le GAC discutera des récentes évolutions liées à l'utilisation malveillante du DNS, notamment en cette période de crise du Covid-19, en lien avec une séance plénière intercommunautaire prévue à ce sujet lors de l'ICANN68. Cette séance sera également l'occasion d'examiner et de discuter des faits pertinents relatifs à la prévention et l'atténuation de l'utilisation malveillante du DNS et des menaces à sa sécurité.

## 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 éléments des écosystèmes du DNS et de l'Internet (protocoles, systèmes informatiques, transactions personnelles et commerciales, procédures d'enregistrement de domaines, etc.). Certaines de ces activités malfaisantes menacent la sécurité, la stabilité et la résilience des infrastructures du DNS ainsi que le DNS dans sa globalité.

Ces menaces et activités malveillantes sont en général qualifiées d'« utilisation malveillante du DNS » au sein de la communauté de l'ICANN. On considère en général que l'utilisation malveillante du DNS comprend tout ou partie d'activités telles que le déni de service distribué (DDoS), les courriers indésirables, l'hameçonnage, les logiciels malveillants, les réseaux zombies et la diffusion de documents illégaux. Alors que tout le monde semble s'accorder à dire que l'utilisation malveillante du DNS est un problème qui doit être traité, il existe des divergences d'opinion quant à savoir à qui en incombe la responsabilité. Les registres et en particulier les bureaux d'enregistrement s'inquiètent de devoir en faire plus, car ceci a un impact sur leur modèle commercial et leur bénéfice net.

Dans le cadre de cette discussion, il convient de noter que même la définition exacte d'« utilisation malveillante du DNS » fait l'objet de débats[1].

Néanmoins, des progrès ont été réalisés ces dernières années. Voici un résumé des précédentes initiatives menées au sein de la communauté de l'ICANN afin de lutter contre l'utilisation malveillante du DNS, certaines ayant bénéficié de la participation du GAC :

- L'**Organisation de soutien aux extensions génériques (GNSO)** de l'ICANN a formé en 2008 un Groupe de travail sur les politiques en matière d'enregistrements frauduleux. Ce dernier a identifié un ensemble de problèmes spécifiques mais n'a pas proposé de politiques et n'a pas non plus engagé par la suite de discussions concernant l'élaboration de meilleures pratiques non contraignantes pour les registres et bureaux d'enregistrement (notamment lors des ateliers organisés pendant l'ICANN41 et l'ICANN42).

- **Dans le cadre du programme des nouveaux gTLD,** l'organisation ICANN a adopté une série de nouvelles exigences[2] 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 (en date du 18 juillet 2016) a évalué leur efficacité dans la perspective de la révision de la concurrence, de la confiance et du choix du consommateur (CCT) prévue par les statuts constitutifs qui a abouti à la formulation de recommandations le 8 septembre 2018.

[1] Comme le prouvent les discussions sur l'utilisation malveillante du DNS et la protection des consommateurs lors du sommet de la GDD (7-8 mai 2019).

[2] 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.

- 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 majeur dans les négociations du contrat d'accréditation de bureau d'enregistrement de 2013[3] ainsi que dans l'élaboration de l'avis du GAC relatif aux menaces à la sécurité qui a conduit à la création de nouvelles dispositions dans le contrat de base des nouveaux gTLD précisant les responsabilités des registres. Ces dispositions ont par la suite été complétées par un cadre d'actions non contraignantes à mettre en œuvre par les opérateurs de registre pour répondre aux menaces à la sécurité (20 octobre 2017) négocié entre **l'organisation ICANN, les registres et le PSWG du GAC.**

- Le **Comité consultatif sur la sécurité et la stabilité (SSAC)** a transmis des recommandations à la communauté de l'ICANN, notamment dans le SAC038 : point de contact au sein du bureau d'enregistrement pour le signalement d'abus (26 février 2009) et SAC040 : mesures de protection des services d'enregistrement de domaines contre l'exploitation ou les abus (19 août 2009).

- **L'organisation ICANN**, par le biais de son **Équipe en charge de la sécurité, la stabilité et la résilience (SSR),** forme régulièrement les communautés responsables de la sécurité publique et apporte une aide en cas de cyberincident à grande échelle, notamment grâce au processus accéléré de demande de dérogation pour incident de sécurité des registres (ERSR). Plus récemment, le **bureau du directeur de la technologie** (OCTO) de l'ICANN a mis au point un système de signalement des cas d'utilisation malveillante des noms de domaine (DAAR) qui produit des rapports mensuels. Cet outil a obtenu le soutien actif du GAC et de plusieurs équipes en charge de révisions spécifiques car il renforce la transparence et permet d'identifier la source des problèmes qui pourront ensuite être traités grâce aux politiques de conformité, ou si besoin, grâce à la définition d'une nouvelle politique.

## Problématiques

Les initiatives passées n'ont pas encore permis une réduction effective de l'utilisation malveillante du DNS ; il reste en effet encore beaucoup à faire. Malgré l'attention que porte la communauté de l'ICANN et les meilleures pratiques du secteur existantes visant à atténuer l'utilisation malveillante du DNS, les engagements de la communauté pilotés par le GAC ainsi que l'analyse statistique de l'utilisation malveillante du DNS dans les gTLD effectuée dans le cadre de la révision CCT (9 août 2017) ont mis en évidence des tendances marquées en termes d'utilisation malveillante, des pratiques commerciales entraînant des abus et des preuves qu'il existe « *des possibilités de développement et de renforcement des mesures d'atténuation et des sauvegardes actuelles* » ainsi qu'une possibilité d'élaboration de politiques futures[4].

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

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

De plus, des craintes quant à la capacité à atténuer réellement l'utilisation malveillante du DNS se sont amplifiées 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] suite à l'entrée en vigueur du règlement général sur la protection des données (RGPD) de l'Union européenne et suite aux initiatives de mise en conformité du système WHOIS, outil majeur de recherche des cas d'utilisation malveillante et crimes, au RGPD. Plus récemment, l'urgence sanitaire mondiale liée au Covid-19 est un bon exemple des problèmes se posant actuellement alors que les enregistrements de domaines liés au virus se sont envolés, un faible pourcentage[6] d'entre eux ayant été enregistrés à différentes fins frauduleuses et opportunistes.

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[7].

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 concernant l'atténuation de l'utilisation malveillante et l'éventuel travail d'élaboration de politiques au sein de la communauté de l'ICANN tournent en général autour de :

- **La définition de l'utilisation malveillante du DNS :**
  Qu'est-ce qui constitue une utilisation malveillante compte tenu des compétences de l'ICANN et de ses contrats avec les registres et bureaux d'enregistrement ?
- **La détection et le signalement de cas d'utilisation malveillante du DNS (dans une perspective de sensibilisation et de transparence) :**
  Comment garantir que l'utilisation malveillante du DNS est détectée et portée à la connaissance des parties prenantes concernées, dont les consommateurs et les internautes ?
- **La prévention et l'atténuation de l'utilisation malveillante du DNS (dans une perspective d'efficacité) :**
  Quels outils et quelles procédures peuvent utiliser l'organisation ICANN, les acteurs du secteur et les parties prenantes intéressées afin de réduire les cas d'utilisation malveillante et afin d'y répondre de manière appropriée lorsqu'ils se présentent ? Qui est responsable de telle ou telle partie du puzzle, et comment les différents acteurs peuvent-ils coopérer ?

Le GAC, qui cherche à renforcer la sécurité et la stabilité au profit de l'ensemble des internautes, pourrait vouloir participer activement aux discussions sur ces questions (décrites en détail dans le présent document d'information) pour que des progrès soient réalisés en vue d'une prévention et d'une atténuation plus efficaces des cas d'utilisation malveillante.

---

[5] Voir les articles III.2 et IV.2 du communiqué du GAC de Barcelone (du 25 octobre 2018) qui renvoient à des études concernant l'impact sur l'application de la loi dont traite l'article 5.3.1 du rapport préliminaire de l'équipe de révision RDS (31 août 2018) et la publication des groupes de travail anti-abus pour la messagerie, les programmes malveillants et les mobiles (18 octobre 2018).

[6] Tel qu'indiqué au GAC par les dirigeants du Groupe des représentants des bureaux d'enregistrement le 9 avril 2020.

[7] Voir les discussions sur l'utilisation malveillante du DNS et la protection des consommateurs menées lors du sommet de la GDD (7-8 mai 2019).

## Proposition des dirigeants sur la ligne d'action du GAC lors de l'ICANN68

1. **Examiner les enseignements tirés** jusqu'à présent **des cas d'utilisation malveillante du DNS liés au Covid-19** signalés par les parties concernées, dont les autorités publiques, les bureaux d'enregistrement, les opérateurs de ccTLD et l'organisation ICANN, **et préparer la participation de la communauté de l'ICANN selon les besoins,** en commençant par la séance plénière intercommunautaire sur l'utilisation malveillante du DNS et les enregistrements malveillants lors de l'épidémie de Covid-19 prévue pour le 22 juin 2020 dans le cadre de l'ICANN68.

2. **Débattre sur les éventuelles prochaines étapes visant à lutter contre les principaux problèmes de politique publique liés à l'utilisation malveillante du DNS** tels qu'identifiés dans les précédents retours du GAC, et **notamment envisager de mettre en place un suivi** avec le Conseil de la GNSO, l'ALAC, la ccNSO et éventuellement le Conseil d'administration de l'ICANN **sur les différentes manières de donner suite aux recommandations issues de la révision CCT relatives à l'utilisation malveillante du DNS avant le lancement des prochaines séries de nouveaux gTLD** dans le respect de l'avis du communiqué du GAC de Montréal (6 novembre 2019).

3. **Discuter de l'état d'avancement** de l'examen et de la mise en œuvre des **recommandations liées à l'utilisation malveillante du DNS formulées par les équipes de révision CCT et RDS-WHOIS2**, à la lumière des décisions prises par le Conseil d'administration de l'ICANN et indiquées dans :
    a. La fiche de suivi des décisions du Conseil d'administration sur les recommandations issues de la révision CCT (1er mars 2019)
    b. La fiche de suivi des décisions du Conseil d'administration sur les recommandations issues de la révision RDS-WHOIS2 (25 février 2020)

4. **Évaluer de façon plus générale les progrès des principales initiatives d'atténuation de l'utilisation malveillante du DNS, au niveau de la communauté de l'ICANN** ainsi qu'au niveau des parties contractantes, des opérateurs de ccTLD et de l'organisation ICANN, notamment afin de promouvoir des standards de qualité en termes de pratiques et de contrats :
    a. **Mise en œuvre de mesures volontaires par les bureaux d'enregistrement et registres des gTLD** conformément au cadre de lutte contre l'utilisation malveillante émanant du secteur
    b. **Mise en œuvre de mesures anti-abus proactives par les opérateurs de ccTLD** susceptibles de guider les pratiques des registres gTLD
    c. **Audit de conformité contractuelle des bureaux d'enregistrement** concernant les menaces à la sécurité du DNS qui devait faire suite aux conclusions d'un audit similaire des registres

d. **Améliorations du système de signalement des cas d'utilisation malveillante des noms de domaine (DAAR) de l'ICANN** telles que précédemment débattues par les registres, le GAC et le SSAC

## Évolutions récentes

**Aperçu des dernières évolutions**

- **La crise du Covid-19 a conduit à des échanges entre le GAC et les parties prenantes concernées** qui ont permis de mettre en lumière différentes **initiatives visant à apporter une réponse** aux activités frauduleuses et criminelles **et à assurer la coordination de cette réponse** :
    - **Les dirigeants du GAC ont** rendu compte d'une discussion (9 avril) tenue à la demande du Groupe des représentants des bureaux d'enregistrement (RrSG) et ont continué à en discuter lors d'un appel conjoint de la direction (3 juin 2020) dans la perspective de l'ICANN68.
    - Dans leur réponse aux activités potentiellement frauduleuses liées au Covid-19, les **bureaux d'enregistrement** ont fait part des difficultés relatives à l'évaluation du caractère frauduleux dans les juridictions concernées et ont demandé de l'aide aux autorités publiques. Le RrSG a décrit à ses membres les approches communes adoptées par les bureaux d'enregistrement face à la crise du Covid-19.
    - Les membres du GAC ont été invités à partager les ressources pertinentes mises à disposition par leurs autorités publiques respectives telles que les ressources diffusées par des organismes d'application de la loi (le FBI aux États-Unis, la NCA au Royaume-Uni, Europol) et des agences de défense des consommateurs (la FTC aux États-Unis).
    - La **Commission européenne** a fait état des efforts en cours, en lien avec les États membres de l'UE, Europol, les ccTLD et les bureaux d'enregistrement, visant à faciliter l'élaboration de rapports, leur examen et leur renvoi devant des juridictions compétentes via l'adoption d'un formulaire type permettant de signaler un domaine/contenu lié au Covid-19 et l'instauration de points de contact uniques pour les autorités concernées des États membres.
    - **Les opérateurs de ccTLD** du monde entier doivent faire part au GAC (4-5 juin 2020) des enseignements qu'ils ont tirés de leurs opérations lors de la crise.
    - Un exposé du **bureau du directeur de la technologie (OCTO) de l'ICANN** auprès du GAC, prévu avant l'ICANN68, devrait mettre en avant les initiatives et les ressources de l'ICANN visant à soutenir la réponse des parties contractantes.

- En attendant, **les parties contractantes, le Comité consultatif sur la sécurité et la stabilité (SSAC) et l'organisation ICANN ont engagé de nouveaux travaux** dont le but est de faire face aux menaces à la sécurité :
    - Tel qu'indiqué par le Groupe de travail du GAC sur la sécurité publique lors de l'ICANN67, le **Groupe des représentants des bureaux d'enregistrement** a publié un Guide de signalement de cas d'utilisation malveillante aux bureaux d'enregistrement

- Le cadre de lutte contre l'utilisation malveillante du DNS (17 octobre 2019), proposé en tant qu'**initiative volontaire des principales parties prenantes de l'industrie du DNS**, compte désormais, au 29 mars 2020, 56 signataires.
- Le **SSAC** a créé une équipe de travail sur l'utilisation malveillante du DNS au sein de laquelle un représentant du PSWG a été invité à prendre part.
- **L'organisation ICANN**, dans le cadre de la mise en œuvre du plan stratégique pour les exercices fiscaux 2021 à 2025, a annoncé le lancement d'un Groupe d'étude technique des initiatives de renforcement de la sécurité du DNS (6 mai 2020) chargé « *de réfléchir à ce que l'ICANN peut et devrait faire afin d'augmenter le niveau de collaboration et d'engagement avec les parties prenantes de l'écosystème de l'ICANN et de renforcer ainsi le dispositif de sécurité du DNS* ». Des recommandations devraient être publiées d'ici mai 2021.

- Depuis l'ICANN66, plusieurs **processus communautaires de l'ICANN ont formulé de nouvelles recommandations liées à l'utilisation malveillante du DNS**. Le GAC a donné un retour sur certaines d'entre elles, et d'autres seront soumises à un suivi du GAC :
  - Après examen par le Conseil d'administration de l'ICANN des recommandations finales de l'équipe de révision RDS-WHOIS2 (3 septembre 2019), dont l'intérêt eu égard à l'atténuation de l'utilisation malveillante du DNS a été mis en avant dans un commentaire du GAC (23 décembre 2019), conformément à la fiche de suivi des décisions du Conseil d'administration (25 février 2020) et dans le cadre de ses résolutions 2020.02.25.01 à 2020.02.25.06, 15 recommandations ont été acceptées, 4 ont été mises en attente, 2 ont été transmises à la GNSO et 2 ont été rejetées.
  - **L'équipe de révision SSR2** a publié un rapport préliminaire (24 janvier 2020) largement axé sur les mesures de prévention et d'atténuation de 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. Les recommandations finales de la SSR2 RT devraient être publiées en octobre 2020 (selon les récentes délibérations).
  - **Le Groupe de travail consacré au processus d'élaboration de politiques relatif aux procédures pour des séries ultérieures de nouveaux gTLD de la GNSO** a récemment indiqué (29 avril 2020) qu'il *« n'envisage pas de formuler des recommandations sur l'atténuation de l'utilisation malveillante des noms de domaine autres 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 prises par le Conseil d'administration de l'ICANN, de l'avis du communiqué du GAC de Montréal (6 novembre 2019) et d'autres retours du GAC consignés dans le communiqué du GAC de l'ICANN67 (16 mars 2020). Une récente réunion du Conseil de la GNSO (21 mars

2020) a abordé la possibilité de former un groupe de travail intercommunautaire (CCWG) et éventuellement de lancer par la suite un PDP de la GNSO dans l'hypothèse où de nouvelles exigences contractuelles s'avéreraient nécessaires. 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.

**Problématiques - Définition de l'utilisation malveillante du DNS**

Comme souligné récemment lors du sommet de la GDD (7-9 mai 2019), il n'existe **pas d'accord communautaire sur ce que constitue une « utilisation malveillante du DNS »**, en partie à cause des inquiétudes de certaines parties prenantes qui craignent que l'ICANN outrepasse son mandat, des impacts sur les droits des utilisateurs et de l'impact sur le bénéfice net des parties contractantes[8].

Cependant, selon l'équipe de révision CCT, il existe **un consensus sur ce que constitue les « menaces à la sécurité du DNS » ou les « menaces à la sécurité de l'infrastructure du DNS »**, à savoir qu'elles comprennent « *davantage de formes techniques de l'activité malveillante* » telles que les logiciels malveillants, l'hameçonnage et les réseaux zombies ainsi que les courriers indésirables *« lorsqu'ils sont utilisés en tant que méthode de diffusion pour d'autres formes d'utilisation malveillante »* [9].

Récemment, **le département de l'ICANN en charge de la conformité contractuelle a fait référence à « l'utilisation malveillante 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 programmes malveillants et les réseaux zombie*s »[10] et du contrat d'accréditation de bureau d'enregistrement (article 3.18) qui visent les « *contacts en cas d'utilisation malveillante* » et les « *signalements de 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 donnée dans l'avis du GAC relatif aux sauvegardes des contrôles de sécurité** du communiqué de Beijing (11 avril 2013) applicables à l'ensemble des nouveaux gTLD.

Suite à la résolution du Conseil d'administration (1er mars 2019) enjoignant à l'organisation de l'ICANN de « *faciliter les initiatives de la communauté visant à développer une définition de « l'utilisation malveillante » afin d'éclairer les futures mesures à prendre concernant cette recommandation* »[11], et suite aux activités de renforcement de la fonction de protection des

---

[8] En effet, la définition de l'atténuation de l'utilisation malveillante peut avoir des conséquences sur la portée des activités régies par les contrats et politiques de l'ICANN. Alors que des 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 compétitivité, de l'augmentation des coûts 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 du non-respect de la vie privée des titulaires de noms de domaine et des internautes, et craignent, tout comme les parties contractantes, que l'ICANN outrepasse sa mission.

[9] 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).

[10] Le bulletin d'information sur la spécification 11 (3)(b) du contrat de registre des nouveaux gTLD (8 juin 2017) donne une définition des « menaces à la sécurité » qui comprennent « *le dévoiement, l'hameçonnage, les programmes malveillants, les réseaux zombies ainsi que d'autres types de menaces à la sécurité* ».

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

consommateurs de l'organisation ICANN, **d'autres discussions sur la définition de l'utilisation malveillante devraient avoir lieu avant et lors de l'ICANN66** à Montréal.

Plus précisément, 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 août 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 à leurs craintes liées au 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), et l'Unité constitutive des utilisateurs commerciaux y a aussi répondu (28 octobre).

**Problématiques - Sensibilisation et transparence : séances d'échange de la communauté sur l'utilisation malveillante du DNS**

Au cours des dernières années, le GAC et son Groupe de travail sur la sécurité publique (PSWG) ont animé plusieurs séances d'échange intercommunautaires lors de réunions de l'ICANN dans le but d'**accroître la sensibilisation et de chercher des solutions avec des experts en la matière**. Plus récemment, les dirigeants des organisations de soutien et comités consultatifs (SO/AC) de l'ICANN et l'ALAC ont organisé des séances d'échange très suivies sur cette question.

- Lors de l'ICANN57 à Hyderabad (5 novembre 2016), le PSWG du GAC a mené une séance sur des sujets d'actualité à propos de l'atténuation des cas d'utilisation malveillante au sein des gTLD qui s'est tenue sous la forme d'un échange d'opinions parmi la communauté de l'ICANN et qui a mis en avant :
    - le manque de compréhension commune de ce que constitue une utilisation malveillante du DNS ;
    - la diversité des modèles commerciaux, des pratiques et des compétences influençant les approches visant à atténuer l'utilisation malveillante ; et
    - la nécessité d'intensifier la coopération dans l'ensemble du secteur, en s'appuyant sur des données partagées relatives aux menaces à la sécurité.

- Lors de l'ICANN58 à Copenhague (13 mars 2017), le PSWG du GAC a animé une séance intercommunautaire intitulée Vers une atténuation réelle de l'utilisation malveillante du DNS :prévention, atténuation et réponse qui a abordé les tendances récentes en matière d'utilisation malveillante du DNS, en particulier l'hameçonnage, ainsi que les comportements comme le va-et-vient des domaines entre les bureaux d'enregistrement et les TLD qui pourraient exiger des réponses plus coordonnées et complexes de la part du secteur. La séance a également permis de mettre en avant :
    - l'émergence du projet de signalement des cas d'utilisation malveillante des noms de domaine (DAAR),
    - la collaboration actuelle entre le département en charge de la conformité contractuelle et les fonctions SSR de l'organisation ICANN, et
    - la possibilité de débloquer des recettes provenant de la mise aux enchères des nouveaux gTLD pour financer l'atténuation de l'utilisation malveillante.

- Lors de l'ICANN60 à Abu Dhabi (30 octobre 2017), le PSWG a organisé une séance intercommunautaire sur le signalement de l'utilisation malveillante du DNS à des fins d'élaboration de politiques fondées sur les faits et d'atténuation réelle pour discuter de la mise en place de mécanismes de signalement des cas d'utilisation malveillante du DNS fiables, publics et opposables pour la prévention et l'atténuation de l'utilisation malveillante, et pour permettre l'élaboration de politiques basées sur des données factuelles. La séance a confirmé la nécessité de publier des données fiables et détaillées sur l'utilisation malveillante du DNS, telles que celles contenues dans l'outil de signalement des

cas d'utilisation malveillante des noms de domaine (DAAR). Le PSWG a envisagé de continuer à développer des principes du GAC[12].

- Lors de l'ICANN66 à Montréal (6 novembre 2019), la communauté de l'ICANN a tenu une séance plénière intercommunautaire sur l'utilisation malveillante du DNS.

- Lors de la réunion virtuelle de l'ICANN67 (9 mars 2020), l'ALAC a organisé deux séances auxquelles ont participé à distance de nombreux membres de la communauté de l'ICANN, l'une assurant une présentation de l'utilisation malveillante du DNS (qui comprenait une vidéo éducative) et l'autre procédant à un examen pratique de la mise en conformité contractuelle en réponse à des cas typiques d'utilisation malveillante du DNS.

**Problématiques - Sensibilisation et transparence : études sur l'utilisation malveillante du DNS**

Un certain nombre de sauvegardes en cas d'utilisation malveillante du DNS ont été mises en place dans le cadre du programme des nouveaux gTLD via de nouvelles exigences[13] adoptées par l'organisation ICANN conformément à son protocole de réduction des comportements malveillants (3 octobre 2009) et à l'avis du GAC relatif aux sauvegardes des contrôles de sécurité.

En s'appuyant sur l'évaluation effectuée par l'organisation ICANN de l'efficacité de ces sauvegardes du programme des nouveaux gTLD (18 juillet 2016), à laquelle le GAC a contribué (20 mai 2016), l'équipe de révision CCT s'est attelée à procéder à une analyse comparative plus complète des taux d'utilisation malveillante dans les nouveaux gTLD et les gTLD historiques, cette analyse comprenant notamment une analyse statistique inférentielle des hypothèses comme les corrélations entre le prix de vente d'un nom de domaine et les taux d'utilisation malveillante.

Les conclusions de cette analyse statistique de l'utilisation malveillante du DNS dans les gTLD (9 août 2017) ont été soumises à consultation publique. Les commentaires de la communauté ont été qualifiés (13 octobre 2017) de constructifs, saluant la rigueur scientifique de l'analyse et invitant à mener davantage d'études de ce type.

Dans ses commentaires (19 septembre 2017), le GAC est arrivé, entre autres, aux conclusions suivantes :

- L'étude a clairement mis en évidence l'existence de problèmes importants d'utilisation malveillante du DNS :
    - Dans certains nouveaux gTLD, plus de 50 % des enregistrements sont effectués à des fins d'utilisation malveillante.
    - Cinq nouveaux gTLD représentaient à eux seuls 58,7 % des domaines blacklistés pour hameçonnage dans les nouveaux gTLD
- L'utilisation malveillante est directement liée aux politiques des opérateurs de registre :

[12] Voir l'Annexe 1 : Principes d'atténuation de l'utilisation malveillante dans le document d'information du GAC de l'ICANN60 sur l'utilisation malveillante du DNS et le rapport de la séance dans le communiqué du GAC d'Abu Dhabi (p. 3).

[13] 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.

    - Les nouveaux gTLD les plus utilisés à des fins d'utilisation malveillante sont exploités par des opérateurs de registre qui se livrent à une concurrence par les prix ;
    - Les personnes malveillantes préfèrent enregistrer des domaines dans des nouveaux gTLD standards (ouverts à l'enregistrement public) plutôt que dans des nouveaux gTLD communautaires (restrictions quant à qui peut enregistrer des noms de domaine).
- Il existe un potentiel d'élaboration de futures politiques concernant :
    - Les séries ultérieures de nouveaux gTLD, en lien avec le fait qu'il est prouvé que le risque varie selon les catégories de TLD et le caractère strict de la politique d'enregistrement.
    - Le renforcement des mesures actuelles d'atténuation et des protections contre l'utilisation malveillante, comme le montre cette analyse statistique
- L'ICANN devrait poursuivre et étendre l'utilisation de l'analyse statistique et des données pour mesurer et partager avec la communauté des informations relatives aux niveaux d'utilisation malveillante du DNS.

Le 17 octobre 2019, une étude sur l'utilisation malveillante de l'accès groupé aux données d'enregistrement et coordonnées des noms de domaine à des fins criminelles a été publiée par une société de conseil (Interisle Consulting Group). Cette étude présente un intérêt direct pour les discussions de la communauté en cours et passe en revue les points suivants :

- Comment les cybercriminels profitent des services d'enregistrement en masse afin de « militariser » un grand nombre de noms de domaine pour leurs attaques.
- Les effets de la suppression, par le biais des politiques provisoires de l'ICANN, des données relatives aux points de contact du WHOIS afin de respecter les dispositions du RGPD relatives aux enquêtes de cybercriminalité.
- Les recommandations politiques devant faire l'objet d'un examen par l'organisation ICANN et la communauté de l'ICANN.

**Problématiques - Sensibilisation et transparence : 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)[14].

L'objectif annoncé du DAAR est de « *signaler les activités menaçant la sécurité à la communauté de l'ICANN, pour que cette dernière puisse ensuite se servir de ces données pour faciliter l'élaboration de politiques basées sur des décisions éclairées* ». Cet objectif est atteint depuis

[14] 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.

janvier 2018 avec la publication de rapports mensuels fondés sur la compilation des données d'enregistrement TLD avec des informations issues d'un important flux de données hautement fiables relatives à la réputation et aux menaces à la sécurité[15].

À cet effet, le DAAR contribue au respect de l'obligation de publication de « *données détaillées et fiables sur l'utilisation malveillante du DNS* » identifiée par le GAC dans le communiqué du GAC d'Abu Dhabi (1er novembre 2017). Cependant, comme le souligne une lettre envoyée par le M3AAWG[16] 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 août 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 généralisé 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* ».

**Problématiques - Efficacité : sauvegardes en cas d'utilisation malveillante du DNS actuellement prévues dans les contrats de registres et de bureaux d'enregistrement**

En s'appuyant sur les recommandations relatives à la diligence raisonnable dans l'application de la loi (octobre 2009), le GAC a souhaité **inclure des sauvegardes pour l'atténuation de l'utilisation malveillante du DNS dans les contrats de l'ICANN** avec les registres et les 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 aux 12 recommandations relatives à l'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 conformes 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 de l'ICANN pour la mise en œuvre des sauvegardes du GAC applicables à l'ensemble des nouveaux gTLD (19 juin 2013).

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

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

Après les premières années de fonctionnement des nouveaux gTLD, lors de l'ICANN57, **le GAC a identifié un certain nombre de dispositions et de sauvegardes connexes pour lesquelles il n'était pas en mesure d'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 précisions quant à leur mise en œuvre. Cela a abouti à des discussions entre le GAC et l'organisation ICANN, à des questions de suivi dans le communiqué du GAC de Copenhague (15 mars 2017) et à un ensemble de réponses préliminaires (30 mai 2017) qui ont été traitées lors d'une téléconférence entre le GAC et le président-directeur général de l'ICANN (15 juin 2017). Plusieurs questions sont toujours en suspens et de nouvelles questions ont été identifiées, comme l'indique un document de travail ultérieur (17 juillet 2017).

Parmi les principaux sujets d'intérêt du GAC, un bulletin d'information sur la spécification 11 (3)(b) du contrat de registre des 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 gTLD https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.html - specification11. **Ce bulletin d'information propose une approche volontaire que les opérateurs de registre peuvent adopter** pour effectuer des analyses techniques destinées à évaluer les menaces à la sécurité et produire des rapports statistiques, tel que requis par la spécification 11 3(b).

Dans le cadre des **audits réguliers réalisés par le département de l'ICANN en charge de la conformité contractuelle,** un audit ciblé de 20 gTLD relatif à leurs « *processus, procédures et gestion de l'infrastructure du DNS* », mené entre mars et septembre 2018, a révélé « *qu'il y avait des analyses et rapports de sécurité incomplets pour 13 domaines de premier niveau (TLD) ainsi qu'un manque de procédures de gestion des cas d'utilisation malveillante normalisées ou documentées et qu'aucune mesure n'était prise contre les menaces identifiées* »[17]. Peu après, en novembre 2018, un audit sur l'utilisation malveillante de l'infrastructure du DNS concernant quasiment l'ensemble des gTLD a été mené afin de « *garantir que les parties contractantes respectent leurs obligations contractuelles eu égard aux menaces à la sécurité et à l'utilisation malveillante de 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.
- La prévalence des menaces à la sécurité du DNS se concentre sur un petit nombre d'opérateurs de registre.
- Certains opérateurs de registre font une interprétation de la terminologie contractuelle de la spécification 11 3(b) rendant difficile le prononcé d'un jugement sur la question de savoir si leurs efforts visant à atténuer les menaces à la sécurité du DNS sont conformes et efficaces.

[17] Tel qu'indiqué dans l'article de blog du 8 novembre 2018 intitulé Conformité contractuelle : lutter contre l'utilisation malveillante de l'infrastructure du DNS : https://www.icann.org/news/blog/contractual-compliance-addressing-domain-name-system-dns-infrastructure-abuse

**Des parties contractantes ont remis en question ces audits** car ils dépasseraient la portée de leurs obligations contractuelles[18]. L'organisation ICANN a fait savoir qu'elle engagerait un audit des bureaux d'enregistrement axé sur les menaces à la sécurité du DNS.

[18] 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'annonce (15 novembre) : les registres ont remis en question les audits car ils menaceraient les mesures d'application de la loi, allant au-delà de la portée de leurs obligations contractuelles [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* ».

**Efficacité : cadre d'actions non contraignantes à mettre en œuvre par les opérateurs de registre pour répondre aux menaces à la sécurité**

Dans le cadre du programme des nouveaux gTLD, le Conseil d'administration de l'ICANN a décidé, via l'adoption d'une résolution (en date du 25 juin 2013), d'inclure lesdits « contrôles de sécurité » (avis relatif aux sauvegardes du GAC du communiqué de Beijing) dans la spécification 11 du contrat de registre des nouveaux gTLD. Cependant, comme il a déterminé que ces dispositions ne donnaient pas assez de détails concernant leur mise en œuvre, il a décidé de solliciter la participation de la communauté afin de développer un cadre pour que « *les opérateurs de registre répondent aux menaces à la sécurité identifiées qui posent un réel risque de préjudice (…)* ».
En juillet 2015, l'ICANN a formé une équipe de rédaction composée de volontaires provenant des registres, des bureaux d'enregistrement et du GAC (dont des membres du PSWG) qui ont développé le cadre d'actions à mettre en œuvre par les opérateurs de registre pour répondre aux menaces à la sécurité publié le 20 octobre 2017 après avoir été soumis à consultation publique.

Ce cadre est un instrument volontaire et non contraignant conçu pour donner une orientation sur la manière dont les registres peuvent répondre aux menaces à la sécurité identifiées, comprenant notamment des rapports d'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 origine 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 sa mission d'évaluation de l'efficacité du cadre à une prochaine révision[19], le cadre n'existant en effet pas depuis assez longtemps pour que son efficacité puisse être évaluée.

**Efficacité : mesures proactives et prévention de l'utilisation malveillante généralisée**

À partir de son analyse du paysage de l'utilisation malveillante du DNS[20], 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 août 2017), l'équipe de révision CCT a recommandé, en lien avec cette problématique :

- L'intégration de **dispositions dans les contrats de registre visant à encourager l'adoption de mesures anti-abus proactives** (recommandation 14)
- L'intégration de dispositions contractuelles visant à **prévenir l'utilisation généralisée de bureaux d'enregistrement ou de registres spécifiques** à des fins d'utilisation malveillante du DNS, avec notamment des seuils d'utilisation malveillante à partir desquels des

[19] Recommandation 19 de la révision CCT : *La prochaine CCT-RT devrait examiner le « cadre d'actions à mettre en œuvre par les opérateurs de registre pour répondre aux menaces à la sécurité » et déterminer si ce cadre constitue un mécanisme suffisamment clair et efficace afin d'atténuer les cas d'utilisation malveillante en fournissant des actions systémiques et précises en réponse aux menaces à la sécurité.*

[20] Voir l'article 9 relatif aux sauvegardes (p. 88) dans le rapport final de la révision CCT (8 septembre 2018).

enquêtes de conformité sont automatiquement déclenchées et éventuellement 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 décidé, via l'adoption d'une résolution (en date du 1er mars 2019), de mettre ces recommandations « en attente » car il a demandé à l'organisation ICANN de « *faciliter les initiatives de la communauté visant à développer une définition de « l'utilisation malveillante » afin d'éclairer les futures mesures à prendre concernant cette recommandation* »[21].

## Positions actuelles

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

- Commentaire du GAC (3 avril 2020) sur le rapport préliminaire de l'équipe de révision SSR2
- Commentaire du GAC (23 décembre 2019) sur les recommandations finales de l'équipe de révision RDS-WHOIS2
- Déclaration du GAC sur l'utilisation malveillante du DNS (18 septembre 2019)
- Commentaire du GAC (11 décembre 2018) sur les recommandations finales de l'équipe de révision CCT
- Commentaire du GAC (16 janvier 2018) sur les nouveaux articles du rapport préliminaire de l'équipe de révision CCT (27 novembre 2017)
- Commentaire du GAC sur l'analyse statistique de l'utilisation malveillante du DNS dans les gTLD (19 septembre 2017)
- Commentaire du GAC sur le rapport initial de la SADAG (21 mai 2016)
- Communiqué du GAC de Barcelone (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)
- Communiqué du GAC de Copenhague (15 mars 2017) comprenant l'avis relatif à l'atténuation de l'utilisation malveillante exigeant des réponses à la fiche de suivi du GAC sur l'Annexe 1 du communiqué du GAC d'Hyderabad (p. 11-32)
- Communiqué du GAC d'Hyderabad (8 novembre 2016) comprenant l'avis relatif à l'atténuation de l'utilisation malveillante exigeant des réponses de l'ICANN et des parties contractantes à l'Annexe 1 - Questions au Conseil d'administration de l'ICANN sur l'atténuation de l'utilisation malveillante du DNS (p.14-17)
- Communiqué du GAC de Beijing (11 avril 2013), en particulier sur les sauvegardes des contrôles de sécurité applicables à tous les nouveaux gTLD (p.7)
- Article III du communiqué du GAC de Dakar (27 octobre 2011) Recommandations des organismes d'application de la loi

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

- Article VI du communiqué du GAC de Nairobi (10 mars 2010). Recommandations relatives à la diligence raisonnable dans l'application de la loi.
- Recommandations des organismes d'application de la loi concernant les amendements au contrat de registre (1er mars 2012)
- Recommandations relatives à la diligence raisonnable dans l'application de la loi (octobre 2009)

### Documents de référence clés

- Fiche de suivi des décisions du Conseil d'administration sur les recommandations finales de la révision RDS-WHOIS2 (25 février 2020)
- Fiche de suivi des décisions du Conseil d'administration sur les recommandations finales de la révision CCT (1er mars 2019)
- Recommandations et rapport final de la révision CCT (8 septembre 2018), en particulier l'article 9 sur les sauvegardes (p. 88)
- Analyse statistique de l'utilisation malveillante du DNS dans les gTLD (9 août 2017)
- Questions du GAC sur l'atténuation de l'utilisation malveillante et réponses préliminaires de l'ICANN (30 mai 2017) conformément à l'avis du communiqué du GAC d'Hyderabad (8 novembre 2016) et au suivi du communiqué du GAC de Copenhague (15 mars 2017)

## Gestion des documents

| | |
|---|---|
| **Réunion** | Forum de politiques virtuel de l'ICANN68, 22-25 juin 2020 |
| **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 : 3 juin 2020 |