ICANN | GAC
Governmental Advisory Committee

ICANN 71
14–17 June 2021
VIRTUAL POLICY FORUM

Atténuation de l'utilisation malveillante du DNS

Séance 3

Table des matières

Contexte 2

Problématiques 3

Proposition des dirigeants sur la ligne d'action du GAC 6

Faits importants 10

- Aperçu des faits récents 10
- Coup de projecteur sur : la définition de l'utilisation malveillante du DNS 13
- Coup de projecteur sur : les sauvegardes en cas d'utilisation malveillante du DNS actuellement prévues dans les contrats de registres et de bureaux d'enregistrement 17
- Coup de projecteur sur : le cadre non contraignant d'actions à mettre en œuvre par les opérateurs de registre pour répondre aux menaces à la sécurité 18
- Coup de projecteur sur : l'examen des recommandations issues de la révision CCT relatives à l'utilisation malveillante du DNS 20
- Coup de projecteur sur : la discussion sur l'élaboration d'une politique de la GNSO relative à l'atténuation de l'utilisation malveillante du DNS 22
- Coup de projecteur sur : le système de signalement des cas d'utilisation malveillante des noms de domaine (DAAR) 23

Positions actuelles 24

Documents de référence clés 28

Objectifs de la séance

La séance a pour but de poursuivre l'examen par le GAC des initiatives de l'ICANN et de la communauté de l'ICANN visant à prévenir et atténuer l'utilisation malveillante du DNS, notamment en réponse aux recommandations des révisions CCT et SSR2 et aux discussions faisant suite au rapport final du Groupe de travail de la GNSO chargé du processus d'élaboration de politiques concernant des procédures pour des séries ultérieures de nouveaux gTLD (le Sub Pro PDP WG) de la GNSO. Cette séance comprendra également la poursuite de la discussion sur les éventuelles propositions concrètes du GAC à cet égard.

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.). Ces activités peuvent menacer la sécurité, la stabilité et la résilience des infrastructures du DNS ainsi que celles du 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 estime en général que l'utilisation malveillante du DNS comprend tout ou partie des activités telles que l'hameçonnage, les logiciels malveillants, les réseaux zombies, le déni de service distribué (DDoS), les courriers indésirables et la diffusion de documents illégaux. Toutefois, il convient de noter que même la définition exacte d'« utilisation malveillante du DNS » fait l'objet de débats animés.

Alors que les parties prenantes de la communauté de l'ICANN semblent en général 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 l'étendue des responsabilités des parties concernées. Par exemple, les registres et bureaux d'enregistrement s'inquiètent de devoir assumer davantage d'obligations contractuelles (ce qui pourrait avoir un impact sur leurs modèles commerciaux) et soutiennent que leurs outils d'atténuation de l'utilisation malveillante sont limités et pourraient ne pas être appropriés (il se peut que des cas d'utilisation malveillante doivent être traités par des fournisseurs d'hébergement et certaines mesures des registres/bureaux d'enregistrement pourraient entraîner des dommages collatéraux et engager leur responsabilité).

D'importants efforts de la communauté de l'ICANN visant à résoudre le problème de l'utilisation malveillante du DNS ont été menés jusqu'à présent avec plus ou moins de succès :

- 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 bonnes pratiques non contraignantes pour les registres et bureaux d'enregistrement (notamment lors des ateliers organisés lors de 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 visant à réduire les 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.

- 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**[2] ainsi que dans l'élaboration de l'avis du GAC relatif aux menaces à la sécurité qui a conduit à la formulation de nouvelles dispositions dans le contrat de base des nouveaux gTLD précisant les responsabilités des registres[3].

- **Plus récemment, l'organisation ICANN**, via son **Bureau du CTO**, a mis au point le système de signalement des cas d'utilisation malveillante des noms de domaine (DAAR) de l'ICANN qui soutient l'élaboration de rapports mensuels sur l'utilisation malveillante et le suivi des dernières tendances observées par le GAC (24 février 2021). Le suivi et le signalement des cas d'utilisation malveillante du DNS ont bénéficié du soutien actif du GAC et des équipes de révision, qui ont recommandé des améliorations. Ces outils devraient garantir la transparence et aider à identifier les causes des problèmes, qui pourront alors être résolus via la mise en conformité ou, le cas échéant, de nouvelles politiques éclairées.

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 l'existence de bonnes pratiques du secteur visant à atténuer l'utilisation malveillante du DNS, les engagements de la communauté pilotés par le GAC ainsi que les équipes de révision ont mis en évidence des tendances marquées en termes d'utilisation malveillante, des pratiques commerciales entraînant des abus, des preuves qu'il existe « *des possibilités de développement et*

[1] Contrôle des opérateurs de registre, obligation d'élaborer 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, obligation d'établir des points de contact et des procédures pour le signalement d'abus au niveau du registre.

[2] 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).

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

de renforcement des mesures d'atténuation et des sauvegardes actuelles » ainsi qu'une possibilité d'élaboration future de politiques[4].

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'état d'urgence de santé publique lié au COVID-19 a mis en exergue les défis actuels alors qu'on recense une hausse substantielle des enregistrements de domaines liés à 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].

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

[6] 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).

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 :** 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 :** 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 pour que des progrès soient réalisés en vue d'une prévention et d'une atténuation plus efficaces des abus.

Proposition des dirigeants sur la ligne d'action du GAC

1. **Tenir compte du rapport du Groupe de travail du SSAC sur l'utilisation malveillante du DNS** qui propose une approche interopérable pour la gestion de l'utilisation malveillante du DNS (19 mars 2021) de sorte à évaluer notamment la proposition de création d'un « facilitateur de réponse commune aux abus » sous la forme d'une organisation non gouvernementale à but non lucratif indépendante qui ferait office de facilitateur pour l'ensemble de l'écosystème du DNS, qui comprendrait les parties contractantes de l'ICANN, les fournisseurs d'hébergement, les fournisseurs de services Internet (FSI) et les réseaux de diffusion de contenu (CDN), afin d'optimiser le signalement des cas d'utilisation malveillante et de minimiser le nombre de victimes des abus.

2. **Tenir compte des délibérations de la GNSO portant sur l'utilisation malveillante du DNS** à la lumière des discussions menées entre le GAC et le Conseil de la GNSO lors de l'ICANN70 et des vives inquiétudes dont le GAC a précédemment fait part suite à la décision 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 recommandations dans ce domaine.

3. **Débattre des éventuelles prochaines étapes,** notamment via des **propositions concrètes visant à améliorer les politiques et/ou améliorer les dispositions contractuelles et leur mise en d'œuvre**[7] afin de résoudre les problèmes de politique publique liés à l'utilisation malveillante du DNS identifiés grâce aux initiatives de la communauté et aux contributions du GAC :

    a. **Les recommandations issues de la révision CCT** contenues dans son rapport final (8 septembre 2018), notamment :

        – La décision du Conseil d'administration de l'ICANN (1er mars 2019) sur l'ensemble des 35 recommandations, son adoption ultérieure (26 janvier 2020) d'un plan de mise en œuvre proposé pour les 6 recommandations qu'il a acceptées (6 septembre 2019), et la résolution la plus récente du Conseil d'administration de l'ICANN (22 octobre 2020) comprenant une décision sur 11 des 17 recommandations initialement mises en attente, tel qu'indiqué par une évaluation détaillée de l'organisation ICANN ;

        – Les retours du GAC sur les commentaires relatifs au rapport préliminaire (19 mai 2017), les commentaires relatifs à l'analyse statistique de l'utilisation malveillante du DNS dans les gTLD (19 septembre 2017), les commentaires relatifs aux nouvelles recommandations préliminaires (15 janvier

[7] Selon la section IV.2 du communiqué du GAC de l'ICANN69 : « le GAC estime qu'il existe désormais un large soutien en faveur de l'adoption de mesures concrètes visant à s'attaquer aux principaux aspects d'une atténuation efficace de l'utilisation malveillante du DNS » ; et la section 2.2 du procès-verbal du GAC de l'ICANN69 : « Points d'action : Le PSWG du GAC doit envisager de formuler une proposition concrète pour l'adoption de mesures d'atténuation de l'utilisation malveillante du DNS de sorte à préparer le GAC à de nouvelles discussions lors de l'ICANN70 (conformément aux discussions de la séance de synthèse du GAC). »

2018), les commentaires relatifs au rapport final de la révision CCT (11 décembre 2018), les commentaires relatifs au plan de mise en œuvre (21 octobre 2019) ;

- L'avis du GAC du communiqué de Montréal (6 novembre 2019) selon lequel il conviendrait *de ne pas procéder à une nouvelle série de gTLD tant que les recommandations issues de la révision de la concurrence, de la confiance et du choix du consommateur qualifiées de « conditions préalables » ou de « hautement prioritaires » n'auront pas été pleinement mises en œuvre* ».
- Les questions de clarification du Conseil d'administration (16 décembre 2019) concernant l'avis du GAC de Montréal, y compris les questions liées à la révision CCT et aux procédures pour les séries ultérieures de nouveaux gTLD, et la définition de « pleinement mises en œuvre ».
- La réponse du GAC aux questions de clarification du Conseil d'administration (22 janvier 2020).
- La réponse du Conseil d'administration à la réponse du GAC aux questions de clarification du Conseil d'administration (11 février 2020) renvoyant à sa décision (26 janvier 2020) de ne pas accepter mais de ne pas rejeter non plus l'avis.

b. **Les recommandations issues de la révision de la sécurité, de la stabilité et de la résilience (SSR2)** contenues dans son rapport final (25 janvier 2021), sur lesquelles le GAC a formulé des commentaires (8 avril 2021) et que le Conseil d'administration doit officiellement examiner avant le 25 juillet 2021.

c. **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 indiqué dans son rapport final (1er février 2021) que *« ce Groupe de travail chargé du PDP ne formule aucune recommandation eu égard à l'atténuation de l'utilisation malveillante des noms de domaine autre que celle consistant à indiquer que toute future initiative doit s'appliquer aux gTLD existants ainsi qu'aux nouveaux gTLD (et éventuellement aux ccTLDs) »* en dépit des recommandations pertinentes qui lui ont été adressées par l'équipe de révision CCT[8]. Le GAC a fait part de ses vives inquiétudes concernant cette décision dans les commentaires du GAC (29 septembre 2020) sur le rapport final préliminaire de ce Groupe de travail chargé du PDP, et a indiqué qu'il espérait que le Conseil de la GNSO prendrait rapidement des mesures à cet égard.

d. **La mise en œuvre et l'application des principales obligations contractuelles** des contrats de registre et bureaux d'enregistrement, notamment :

- **La spécification 11 du contrat de registre des nouveaux gTLD** et l'avis du GAC relatif aux sauvegardes du communiqué de Beijing (11 avril 2013), en tenant compte des conclusions du rapport d'audit sur la réponse des opérateurs de registre aux menaces à la sécurité du DNS (17 septembre 2019) et des discussions

[8] Voir la recommandation 9.15 du rapport final du Sub Pro PDP WG (p. 42) et les décisions connexes du Conseil d'administration sur les recommandations CCT.

liées à la séance de questions-réponses GAC/ICANN (30 mai 2017), aux commentaires du GAC sur le rapport préliminaire CCT (19 mai 2017) et aux commentaires du GAC sur le rapport préliminaire SSR2 (3 avril 2020)

- **La spécification relative au programme d'exactitude du WHOIS** du contrat d'accréditation de bureau d'enregistrement de 2013 qui comprend des dispositions relatives à la vérification, la validation et l'exactitude des données d'enregistrement de nom de domaine, tel que décrit dans le commentaire du GAC sur le rapport final de la révision RDS-WHOIS2 (23 décembre 2019), et **l'obligation de disposer d'un point de contact du bureau d'enregistrement chargé de signaler des cas d'abus et d'enquêter sur les plaintes pour abus** (section 3.18) qui fait actuellement l'objet d'un audit par le département en charge de la conformité contractuelle, audit mené pour 153 bureaux d'enregistrement sélectionnés (15 janvier 2021). Ces deux thèmes ont également été abordés lors de la séance de questions-réponses GAC/ICANN (30 mai 2017) faisant suite à l'avis du GAC du communiqué d'Hyderabad (8 novembre 2016).

e. **Les discussions de la communauté sur l'utilisation malveillante du DNS et l'efficacité des dispositions contractuelles connexes**, à la fois en termes d'application et d'applicabilité :
   - **Séances des réunions de l'ICANN :** séminaire web pré-ICANN66 (15 octobre 2019), séance At-Large de l'ICANN66 sur les inquiétudes des utilisateurs finaux (3 novembre 2019), séance intercommunautaire de l'ICANN66 sur l'utilisation malveillante du DNS (6 novembre 2019), séance At-Large de l'ICANN67 sur la conformité contractuelle (9 mars 2020), séance de l'ALAC de l'ICANN68 sur les engagements d'intérêt public et la procédure de règlement de litiges associée (22 juin 2020), réunion entre le Conseil d'administration et le Conseil de la GNSO de l'ICANN68 qui a abordé la question des éventuelles prochaines étapes en matière d'utilisation malveillante du DNS (14 juin 2020) et séance plénière sur les questions liées à l'utilisation malveillante du DNS de l'ICANN69 (20 octobre 2020)
   - Les échanges entre le Conseil d'administration de l'ICANN et l'unité constitutive des utilisateurs commerciaux et l'unité constitutive des représentants de la propriété intellectuelle de la GNSO, dont : la déclaration de la BC concernant la discussion communautaire sur l'utilisation malveillante du DNS (28 octobre 2019), une lettre de la BC au Conseil d'administration de l'ICANN (9 décembre 2019), la réponse à cette lettre (12 février 2020), et une lettre de l'IPC au Conseil d'administration de l'ICANN (24 avril 2020)

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

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

g. **Les recommandations issues de la révision RDS-WHOIS2** telles que détaillées dans son rapport final (8 octobre 2019) qui concernent l'utilisation légitime du WHOIS en tant qu'outil majeur d'enquête sur les crimes et cas d'utilisation malveillante, en tenant compte des commentaires du GAC (23 décembre 2019) et des décisions du Conseil d'administration de l'ICANN (25 février 2020)

4. **Prendre en compte et continuer de suivre les progrès des principales initiatives d'atténuation de l'utilisation malveillante du DNS** au sein de la communauté de l'ICANN afin de guider et de promouvoir l'élaboration de normes strictes dans les pratiques et les contrats :
   a. **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 émanant du secteur et aux discussions en cours du réseau politique Internet et juridiction[10]
   b. **Les 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, le SSAC et le Bureau du directeur de la technologie de l'ICANN[11]
   c. Le 27 mars 2020, l'organisation ICANN a approuvé la proposition d'amendement du contrat de registre de .COM qui **étend les dispositions contractuelles afin de faciliter la détection et la signalisation de cas d'utilisation malveillante du DNS** (y compris la spécification 11 3b) **aux deux tiers de l'espace de noms des gTLD** (qui, jusqu'à présent, n'étaient applicables qu'aux nouveaux gTLD). En outre, une lettre d'intention contraignante entre l'organisation ICANN et Verisign établit un cadre de coopération pour développer de bonnes pratiques, d'éventuelles nouvelles obligations contractuelles ainsi que des mesures visant à mesurer et à atténuer les menaces à la sécurité du DNS.

[10] Le réseau politique Internet et juridiction a récemment annoncé (22 février 2021) le lancement d'une boîte à outils pour l'adoption de mesures d'atténuation de l'utilisation malveillante au niveau du DNS, qu'il devrait présenter lors d'une conférence le jeudi 18 mars.

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

Faits importants

Aperçu des faits récents

- **Lors de récentes réunions de l'ICANN**, les dirigeants du PSWG du GAC ont fourni des documents d'information détaillés au GAC sur la question de l'utilisation malveillante du DNS (voir les supports de la séance du GAC de l'ICANN66, des séances de l'ICANN68, le document d'information du GAC de l'ICANN68 sur l'utilisation malveillante du DNS, la mise à jour du PSWG de l'ICANN69 au GAC et la séance de l'ICANN70).
    - Le GAC a examiné les mesures mises à la disposition des registres 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'abus dans un TLD donné.
    - Le GAC a également examiné les initiatives en cours ou potentielles visant à lutter contre l'utilisation malveillante du DNS plus efficacement au niveau du Conseil d'administration et de l'organisation ICANN (consulter les procès-verbaux de l'ICANN66, le communiqué du GAC et les procès-verbaux de l'ICANN68, le communiqué et les procès-verbaux de l'ICANN69, et le communiqué et les procès-verbaux de l'ICANN70).
    - 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 d'atténuation de l'utilisation malveillante du DNS et de lutte contre la cybercriminalité.
- **Recommandations issues de la révision SSR2**
    - L'équipe de révision 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) a été examiné par le GAC lors de l'ICANN70 en vue de la soumission finale des commentaires du GAC (8 avril 2021) dans le cadre de la procédure de consultation publique.
    - Le Conseil d'administration de l'ICANN devrait à présent examiner officiellement le rapport final issu de la révision SSR2 avant le 25 juillet 2021, dans le respect du délai de 6 mois prévu par les statuts constitutifs de l'ICANN.
- **L'Équipe de travail consacrée à l'utilisation malveillante du DNS du Comité consultatif sur la sécurité et la stabilité (SSAC)** a publié son rapport SAC115 (19 mars 2021) qui propose une approche interopérable pour la gestion de l'utilisation malveillante du DNS.
    - Au cours de l'ICANN66, le SSAC a informé le PSWG de la création d'une Équipe de travail consacrée à l'utilisation malveillante du DNS, à laquelle **a participé un coprésident du PSWG du GAC**.

- Dans ce rapport, le **SSAC propose un cadre général de bonnes pratiques et de processus** visant à optimiser le signalement des cas d'utilisation malveillante du DNS et des cas d'abus sur Internet en général, prévoyant notamment : un responsable principal pour le règlement de litiges relatif à l'utilisation malveillante, des normes en matière de preuve, des mécanismes d'intervention progressive, un calendrier d'action raisonnable et la mise à disposition de coordonnées de qualité.
- **La principale proposition,** que le SSAC recommande de faire examiner et peaufiner par la communauté de l'ICANN en lien avec l'ensemble de la communauté chargée des infrastructures du DNS, **est la création d'un « facilitateur de réponse commune aux abus »** sous la forme d'une organisation non gouvernementale à but non lucratif pleinement indépendante qui ferait office de facilitateur pour l'ensemble de l'écosystème du DNS, qui comprendrait les parties contractantes de l'ICANN, les fournisseurs d'hébergement, les fournisseurs de services Internet (FSI) et les réseaux de diffusion de contenu (CDN), afin d'optimiser le signalement des cas d'utilisation malveillante et de minimiser le nombre de victimes des abus.

- **Mesures et initiatives visant à atténuer l'utilisation malveillante du DNS par les registres et les bureaux d'enregistrement**
  - Le 27 mars 2020, l'organisation ICANN a approuvé la proposition d'amendement du contrat de registre de .COM qui **étend les dispositions contractuelles afin de faciliter la détection et la signalisation de cas d'utilisation malveillante du DNS** (y compris la spécification 11 3b) **aux deux tiers de l'espace de noms des gTLD** (qui, jusqu'à présent, n'étaient applicables qu'aux nouveaux gTLD). En outre, une lettre d'intention contraignante entre l'organisation ICANN et Verisign établit un cadre de coopération pour développer de bonnes pratiques, d'éventuelles nouvelles obligations contractuelles ainsi que des mesures visant à mesurer et à atténuer les menaces à la sécurité du DNS.
  - **Dans le contexte de la crise du COVID-19, les parties contractantes ont présenté leurs actions et les enseignements tirés** avant et pendant l'ICANN68, tandis que les parties prenantes du PSWG ont fait état des efforts en cours en collaboration avec les États membres de l'UE, Europol, les ccTLD et les bureaux d'enregistrement pour faciliter les rapports, leur examen et leur renvoi à la juridiction compétente grâce à l'adoption d'un formulaire normalisé permettant de signaler les domaines/contenus liés au COVID-19 et à 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 s'inspirent de la publication par le **Groupe des représentants des bureaux d'enregistrement** d'un Guide des bureaux d'enregistrement pour le signalement d'abus, qui a été présenté dans le cadre de l'ICANN67.
  - Le **Registre d'intérêt public (PIR)**, l'opérateur de registre de .ORG et plusieurs nouveaux gTLD ont créé (17 février 2021) l'Institut de lutte contre l'utilisation malveillante du DNS (**DNS Abuse Institute**) dont l'objectif énoncé est de *« rassembler les dirigeants dans l'espace de lutte contre l'utilisation malveillante afin de : financer les recherches, publier des pratiques recommandées, partager des données et fournir des outils visant à*

identifier et à signaler les cas d'utilisation malveillante du DNS ». Cette initiative a été présentée au PSWG du GAC (3 mars 2021) préalablement à un séminaire web qui s'est tenu à l'Institut de lutte contre l'utilisation malveillante du DNS le 16 mars 2021. Dans le communiqué de l'ICANN70, le GAC salue la création de l'Institut de lutte contre l'utilisation malveillante du DNS et *« encourage les efforts de la communauté visant à s'attaquer ensemble à la lutte contre l'utilisation malveillante du DNS de manière holistique »*.

- **Réponse multidimensionnelle de l'organisation ICANN et conformité contractuelle**
  - Le PDG de l'ICANN a publié un billet de blog le 20 avril 2020 détaillant la réponse multidimensionnelle de l'organisation ICANN à l'utilisation malveillante du DNS.
  - **Le Bureau du directeur de la technologie (OCTO) de l'ICANN et son Équipe consacrée à la sécurité, la stabilité et la résilience** (SSR) mènent des recherches et assurent le maintien du niveau d'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 antihameçonnage (APWG), l'Alliance nationale d'intervention judiciaire et de formation contre la cybercriminalité (NCFTA) des États-Unis et la récente Coalition contre la cybermenace du COVID-19 (CTC) et la Ligue des renseignements (CTI).
    Elle développe également des systèmes et des outils pour aider à identifier, analyser et signaler les cas d'utilisation malveillante du DNS :
    - En réponse à la crise du COVID-19, l'OCTO a développé l'outil de **signalement et de collecte d'informations sur les menaces à la sécurité des noms de domaine (DNSTICR)** pour aider à identifier les noms de domaine utilisés pour les abus liés au COVID-19 et pour pouvoir partager les données avec les parties concernées. Le GAC a été informé de cette question avant l'ICANN68 (12 juin 2020), tout comme l'ensemble de la communauté de l'ICANN, lors de l'ICANN68.
    - Grâce à sa **plateforme de signalement des cas d'utilisation malveillante des noms de domaine (DAAR)**, l'ICANN rend compte tous les mois, depuis janvier 2018, de l'enregistrement de noms de domaine et des menaces à la sécurité observées dans le DNS. Elle 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 DAAR, en particulier une lettre du M3AAWG à l'organisation ICANN (5 avril 2019) et le rapport préliminaire de l'équipe de révision SSR2 (24 janvier 2020), auquel le GAC a apporté son soutien (voir ci-dessous). Le Groupe des représentants des opérateurs de registre, qui avait également exprimé ses craintes vis-à-vis du DAAR et qui travaillait avec l'ICANN à son évolution, 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 **Groupe d'étude technique chargé de l'initiative de facilitation de la sécurité du DNS**, récemment créé (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 *« réfléchir à ce que l'ICANN peut et doit faire pour augmenter le niveau de collaboration et d'engagement avec les parties prenantes de l'écosystème du DNS afin d'améliorer le profil de sécurité du DNS »*. Des recommandations devraient être publiées d'ici mai 2021.
- Lors d'un appel du GAC portant sur des questions liées à l'utilisation malveillante du DNS (24 février 2021), **l'organisation ICANN a fait le point sur les activités liées à l'utilisation malveillante du DNS de l'OCTO**, dont 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 système de signalement des cas d'utilisation malveillante des noms de domaine (DAAR), les informations relatives aux menaces à la sécurité des noms de domaine, l'outil de signalement et de collecte d'informations sur les menaces à la sécurité des noms de domaine (DNSTICR), la nouvelle initiative visant à élaborer des normes pour le partage des connaissances et l'instanciation pour la sécurité des noms de domaine (KINDNS), et un examen des efforts de l'OCTO dans le domaine de la formation et du renforcement des capacités à travers le monde.
- **Mise en conformité contractuelle** : dans son billet de blog (20 avril 2020), le PDG de l'ICANN a rappelé ce qui suit : « *Le département de l'ICANN en charge de la conformité veille au respect des obligations contractuelles 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). Ce département travaille également étroitement avec l'OCTO à l'identification des menaces à la sécurité du DNS [...] et tâche de les relier aux parties contractantes concernées. Le département de l'ICANN en charge de la conformité se sert des données collectées lors des audits [...] pour évaluer si les registres et les bureaux d'enregistrement se conforment à leurs obligations en matière d'atténuation des menaces à la sécurité du DNS. En dehors de ces audits, le département de l'ICANN en charge de la conformité utilisera les données collectées par l'OCTO et d'autres pour contacter de manière proactive des 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 département de l'ICANN en charge de la conformité n'hésitera pas à prendre des mesures d'exécution à l'encontre de tous ceux qui refuseraient de se conformer à leurs obligations en matière de menaces à la sécurité du DNS ».* Le billet de blog a également fourni un aperçu du volume de plaintes, des ressources allouées à leur traitement et des statistiques sur la résolution de ces plaintes.

Coup de projecteur sur : la définition de l'utilisation malveillante du DNS

Comme souligné 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[12].

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 d'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 d'autres formes d'abus »* [13].

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 »[14] 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 dites « contrôles de sécurité »** du communiqué de Beijing (11 avril 2013) applicables à l'ensemble des nouveaux gTLD.

Lors d'un séminaire web pré-ICANN66 qui s'est tenu le 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 de 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 2019), et l'Unité constitutive des utilisateurs commerciaux y a aussi répondu (28 octobre 2019). Dans sa déclaration, le GAC a reconnu la définition de l'équipe de révision CCT pour qui l'utilisation malveillante du DNS désigne des « *activités intentionnellement trompeuses,*

---

[12] 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.

[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 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 ».

complaisantes ou non sollicitées qui utilisent activement le DNS et/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 ainsi que les courriers indésirables lorsqu'ils sont utilisés comme méthode de diffusion de ces formes d'abus* ». Le GAC a reconnu que le contrat de registre des nouveaux gTLD reprend cette définition dans sa spécification 11, en particulier les sections 3a[15] et 3b[16].

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). Notamment, ce cadre inclut dans le champ d'action possible des entités qui l'adopteront certaines formes d'« abus de contenu de sites web » qu'il considère « si flagrantes que la partie contractante devrait agir après réception d'un avis spécifique et crédible ». Depuis sa publication et la tenue de discussions au cours de l'ICANN66, la liste des signataires de ce cadre s'est élargie et inclut d'autres fournisseurs de services de registres et de bureaux d'enregistrement 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 du 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 qu'ils avaient **adopté** une définition de l'utilisation malveillante du DNS qui reprend exactement celle du cadre de lutte contre l'utilisation malveillante émanant du secteur :

> *L'utilisation malveillante du DNS se compose de cinq grandes catégories d'activités nuisibles dans la mesure où elles ont un lien avec le DNS : les logiciels malveillants, les réseaux zombies, l'hameçonnage, le dévoiement et les courriers indésirables lorsqu'ils servent de mécanisme de diffusion des autres formes d'utilisation malveillante du DNS* [en référence aux approches opérationnelles, aux normes, aux critères et aux mécanismes du réseau politique Internet et juridiction pour la définition de chacune de ces activités].

Cette définition **semble confirmer ce que l'équipe de révision CCT a appelé un consensus existant sur « l'utilisation malveillante du DNS** ou « l'atteinte à la sécurité de l'infrastructure du DNS » (rapport final CCT, p. 8) et **se conforme à la définition illustrative des « menaces de sécurité » du GAC** dans l'avis du GAC relatif aux sauvegardes dites « contrôles de sécurité » applicables à tous

[15] La spécification 11(3)(a) 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 les bureaux d'enregistrement devront inclure dans leurs contrats d'enregistrement une disposition 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 applicables et aux procédures y afférentes) des conséquences pour ce genre d'activités, y compris la suspension du nom de domaine ».

[16] La spécification 11(3)(b) 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 générer des rapports statistiques sur le nombre des menaces à la sécurité identifiées et les mesures prises suite aux contrôles de sécurité périodiques. L'opérateur de registre rédigera 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. »

les nouveaux gTLD du communiqué de Beijing (11 avril 2013) incorporé dans le contrat de registre de gTLD conformément à la spécification 11(3)(b).

Coup de projecteur sur : les 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** conclus 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).

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 dont 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 la section 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%23specification11. **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 registres de 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 sur cet 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.

En janvier 2021, le département de l'ICANN en charge de la conformité contractuelle a lancé un audit afin d'évaluer **le respect par les bureaux d'enregistrement de leurs obligations liées aux menaces à la sécurité du DNS.** Après avoir collaboré avec le Groupe des représentants des bureaux d'enregistrement au développement de la demande d'informations (comprenant des documents portant sur la façon dont les bureaux d'enregistrement ont pu traiter les domaines potentiellement malveillants), le département de l'ICANN en charge de la conformité contractuelle a inclus dans l'audit 127 bureaux d'enregistrement ayant au moins 5 noms de domaine figurant dans des rapports sur les menaces à la sécurité fournis par des registres lors d'un précédent audit, ou dans le rapport sur l'utilisation malveillante de novembre 2020 élaboré par le Bureau du directeur de la technologie de l'ICANN. Lors d'un point sur la conformité pré-ICANN70, l'organisation ICANN a indiqué qu'il comptait rendre compte de cet audit début juin 2021.

Coup de projecteur sur : le cadre non contraignant d'actions 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

[17] Tel qu'indiqué dans le billet 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

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 à la vie humaine, infrastructure critique ou exploitation de mineurs) ayant « *une origine crédible et légitime* » comme « *une autorité nationale d'application de la loi ou une agence de sécurité publique 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[18], le cadre n'existant en effet pas depuis assez longtemps pour que son efficacité puisse être évaluée.

[18] 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.*

Coup de projecteur sur : l'examen des recommandations issues de la révision CCT relatives à l'utilisation malveillante du DNS

À partir de son analyse de la situation de l'utilisation malveillante du DNS[19], 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 proactives de lutte contre l'utilisation malveillante** (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 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* »[20].

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 préconisant de *« ne pas procéder à une nouvelle série de gTLD tant que les recommandations [...] qualifiées de « conditions préalables » ou de « hautement prioritaires » n'auront pas été pleinement mises en œuvre* », et de la réponse du Conseil d'administration 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 encourageant la prise de mesures proactives de lutte contre l'utilisation malveillante (rec. 14) et prévenant l'utilisation systémique des opérateurs de registre et des bureaux d'enregistrement pour utiliser le DNS à des fins malveillantes (rec. 15) ; l'amélioration des recherches sur l'utilisation malveillante du DNS (rec. 16) ; l'amélioration de l'exactitude du WHOIS (rec. 18) ; et l'efficacité du traitement des plaintes en matière de conformité contractuelle (rec. 20).

Le PSWG du GAC a également examiné la résolution du Conseil d'administration visant à procéder au plan de mise en œuvre de l'ICANN (23 août 2019) pour les recommandations 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 mis en avant certaines lacunes concernant des recommandations importantes pour la lutte contre l'utilisation malveillante du

[19] Voir la section 9 relative aux sauvegardes (p. 88) du rapport final de la révision CCT (8 septembre 2018).

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

DNS, y compris la publication de la chaîne des parties responsables des enregistrements de noms de 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).

Suite à l'adoption par les parties contractantes d'une définition de l'utilisation malveillante du DNS, le **GAC a souhaité obtenir des précisions auprès du Conseil d'administration de l'ICANN au cours de l'ICANN68** (voir les documents de la réunion conjointe du GAC et du Conseil d'administration du 24 juin 2020), dans le cadre de la mise en œuvre de la Rec. 14 de la CCT-RT (*« l'ICANN doit négocier des dispositions contractuelles prévoyant des incitations financières pour les parties contractantes afin qu'elles adoptent des mesures proactives de lutte contre l'utilisation malveillante* »), quant au statut et au plan concernant la facilitation des efforts communautaires pour élaborer une définition de « utilisation malveillante » et pour éclairer les futures décisions du Conseil d'administration eu égard à cette recommandation. Le GAC a indiqué dans ses procès-verbaux de l'ICANN68 que « *le Conseil d'administration continuera de soutenir le dialogue communautaire comme il l'a fait en facilitant les discussions régionales et intercommunautaires, en menant des recherches et en développant des outils pour aider à orienter les discussions de la communauté, et en fournissant des intervenants sur demande* ».

Au cours de l'ICANN68, le PSWG et les parties prenantes de l'ALAC ont constaté que les progrès effectués en matière de mise en œuvre de la recommandation acceptée de la CCT-RT et d'examen de la recommandation en attente ne sont pas clairs. De l'insatisfaction a également été exprimée lors d'une communication (29 avril 2020) du **Groupe de travail chargé du processus d'élaboration de politiques concernant des procédures pour des séries ultérieures de nouveaux gTLD de la GNSO** indiquant qu'il « *ne prévoit pas de formuler de recommandations eu égard à l'atténuation de l'utilisation malveillante des noms de domaine autres que celle consistant à indiquer que toute future initiative doit s'appliquer aux gTLD existants ainsi qu'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 sur ces recommandations, 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).

Dans son rapport final (1er février 2021), le Groupe de travail chargé du processus d'élaboration de politiques concernant des procédures pour des séries ultérieures de nouveaux gTLD de la GNSO a confirmé sa décision[21]. Le GAC a fait part de ses vives inquiétudes concernant cette décision dans les commentaires du GAC (29 septembre 2020) sur le rapport final préliminaire de ce Groupe de travail chargé du PDP, et a indiqué qu'il espérait que le Conseil de la GNSO prendrait rapidement des mesures à cet égard.

[21] Voir la recommandation 9.15 du rapport final du Sub Pro PDP WG (p. 42).

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

Suite à la décision initiale du Groupe de travail chargé du PDP concernant des procédures pour des séries ultérieures de nouveaux gTLD de ne pas formuler de recommandations dans le domaine de l'utilisation malveillante du DNS pour les futurs contrats de nouveaux gTLD, le **Conseil de la GNSO a débattu**, 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 de lancer par la suite un PDP de la GNSO s'il avérait nécessaire d'imposer de nouvelles exigences contractuelles.

Il 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 de ccTLD, afin de déterminer le champ d'action d'une future politique.

Au 20 mai 2021, cette question est toujours qualifiée de « Non prévue » dans l'inventaire des actions/décisions du Conseil de la GNSO, le Conseil de la GNSO devant *« déterminer les prochaines étapes, le cas échéant, en matière d'utilisation malveillante du DNS »*.

Depuis l'ICANN70 et l'appel des dirigeants du GAC/de la GNSO pré-ICANN70 (8 mars 2021) et la réunion de l'ICANN70 entre le GAC et la GNSO (24 mars 2021), le Conseil de la GNSO a discuté des documents d'information qu'il a reçus sur la question de l'utilisation malveillante du DNS lors de ses récentes réunions mensuelles :

- Le 22 avril 2021, le **Groupe chargé de l'utilisation malveillante du DNS de la Chambre des parties contractantes de la GNSO** a examiné différentes initiatives menées par les parties contractantes au cours des dernières années et dont le GAC a été informé préalablement par son PSWG. Concernant les travaux en cours et futurs, plusieurs initiatives ont été mentionnées :
    - La collaboration avec le PSWG du GAC afin de régler, à grande échelle, le problème des logiciels malveillants et des réseaux zombies
    - La prise en compte, par les bureaux d'enregistrement, de programmes d'encouragement
    - Des activités de sensibilisation auprès d'autres unités constitutives de l'ICANN, comprenant des séances de questions-réponses, une enquête menée auprès de la communauté et d'autres ressources informatives
- Le 20 mai 2021, le Conseil de la GNSO a reçu un document d'information des dirigeants du SSAC sur le rapport SAC115 récemment publié qui propose une approche interopérable pour la gestion de l'utilisation malveillante du DNS (19 mars 2021). Il n'y a pas eu de discussion de suivi du Conseil de la GNSO sur le SAC115 ou, plus généralement, sur les prochaines étapes de la gestion de l'utilisation malveillante du DNS lors de cette réunion.

Coup de projecteur sur : le système de 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)[22].

L'objectif 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 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[23].

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[24] 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 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). La réponse du directeur de la technologie de l'ICANN (30 septembre 2020) est la suivante : *« la majorité des recommandations*

[22] 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.

[23] Pour de plus amples informations, consulter le lien suivant : https://www.icann.org/octo-ssr/daar-faqs

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

contenues dans la lettre portent sur l'amélioration des communications liées aux données qui sont exportées depuis le système DDAR, dans la mesure où ces communications sont perçues par le Groupe de travail comme potentiellement ambiguës, à la fois les documents sur la méthodologie actuelle du DAAR et les rapports mensuels du DAAR. Alors que la plupart des recommandations se concentrent sur des changements précis d'éléments du rapport, certaines (par exemple la recommandation 3 qui invite à mesurer la « persistance » des activités malveillantes signalées) peuvent impliquer des recherches et analyses à long terme. »

Lors de la mise à jour de l'OCTO au GAC (24 février 2021), le directeur de la technologie de l'ICANN a discuté des futurs plans de développement du DAAR : ajouter davantage de ccTLD au champ d'application du DAAR, poursuivre les travaux avec le Groupe de travail sur le DAAR du RySG, et réfléchir à de nouvelles solutions qui permettraient de relever les défis liés à l'accès aux données WHOIS de sorte à construire des indicateurs au niveau des bureaux d'enregistrement, notamment : les requêtes WHOIS quotidiennes uniquement pour les domaines figurant sur la liste de blocage, l'échantillonnage aléatoire de domaines ou l'obtention de l'approbation pour utiliser les données via l'accès groupé aux données d'enregistrement résumées (BRDA).

Positions actuelles

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

- Commentaires du GAC (8 avril 2021) sur le rapport final de l'équipe de révision SSR2 à des fins d'examen par le Conseil d'administration de l'ICANN
- Communiqué du GAC de l'ICANN70 (25 mars 2021) *selon lequel « la question de l'utilisation malveillante du DNS doit être abordée en collaboration avec la communauté de l'ICANN et l'organisation ICANN avant le lancement d'une seconde série de nouveaux gTLD. Le GAC soutient l'élaboration de propositions de dispositions contractuelles applicables à tous les gTLD afin d'améliorer les réponses apportées en cas d'utilisation malveillante du DNS. Le GAC a également souligné l'importance d'adopter des mesures visant à veiller à ce que les registres, les bureaux d'enregistrement et les fournisseurs de services d'anonymisation et d'enregistrement fiduciaire respectent les dispositions des contrats conclus avec l'ICANN, et notamment les audits. Le GAC salue la récente création de l'Institut de lutte contre l'utilisation malveillante du DNS et encourage les efforts de la communauté visant à s'attaquer ensemble à la lutte contre l'utilisation malveillante du DNS de manière holistique. »*
- Communiqué du GAC de l'ICANN69 (23 octobre 2020) dans lequel le GAC estime *« qu'il existe désormais un large soutien en faveur de l'adoption de mesures concrètes visant à s'attaquer aux principaux aspects d'une atténuation efficace de l'utilisation malveillante du DNS »* au vu de la dynamique actuelle et du dialogue constructif qui a lieu au sein de la communauté de l'ICANN (voir la section IV.2 p.6).
- Communiqué du GAC de l'ICANN68 (27 juin 2020) selon lequel *« les nouvelles initiatives visant à atténuer l'utilisation malveillante du DNS ne devraient pas remplacer, mais plutôt compléter, les initiatives existantes visant à renforcer l'exactitude des données d'enregistrement, telles que le système de signalement de problèmes liés à l'exactitude, et à*

mettre en œuvre des politiques relatives aux services d'anonymisation et d'enregistrement fiduciaire, qui sont actuellement suspendues » (voir la section IV.3 p.7).

- Commentaire du GAC (3 avril 2020) sur le rapport préliminaire de l'équipe de révision SSR2
- Commentaire du GAC sur les recommandations finales issues de la révision RDS-WHOIS2 (23 décembre 2019)
- Déclaration du GAC sur l'utilisation malveillante du DNS (18 septembre 2019)
- Commentaires du GAC sur le rapport final de la révision CCT (11 décembre 2018)
- Commentaire du GAC (16 janvier 2018) sur les nouvelles sections 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 sur les sauvegardes du programme des nouveaux gTLD visant à réduire les risques d'utilisation malveillante du DNS (21 mai 2016)
- Communiqué du GAC de Barcelone (25 octobre 2018), en particulier les sections 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 dites « contrôles de sécurité » applicables à tous les nouveaux gTLD (p.7)
- Section III du communiqué du GAC de Dakar (27 octobre 2011) Recommandations des organismes d'application de la loi
- Section 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)

Questions à soumettre à l'examen des représentants du GAC

En vue de cette séance et d'autres séances du GAC qui se tiendront lors de l'ICANN71 et de futures réunions, il a été avancé que les représentants du GAC pourraient tirer profit d'une discussion plus

approfondie sur différentes questions liées à l'ICANN au sein de leur propre gouvernement ou organisation. À des fins d'expérimentation pour l'ICANN71, le personnel de l'organisation ICANN a travaillé à la rédaction de questions types (ci-dessous) que les représentants du GAC devraient prendre en compte dans le cadre des préparatifs de leurs séances et du partage d'informations lors des réunions, afin de faciliter les débats, de partager de bonnes pratiques et éventuellement d'identifier différentes approches ou stratégies adoptées par des gouvernements eu égard à ces thématiques. Les questions suivantes peuvent être utilisées de sorte à axer les préparatifs ou à rendre les échanges des futures réunions plus inclusifs. Veuillez indiquer au personnel de soutien du GAC si vous trouvez que ces types de questions présentent un intérêt pour la préparation de la réunion.

Concernant le respect des dispositions des contrats de registres et de bureaux d'enregistrement relatives à l'utilisation malveillante :

- Votre gouvernement dispose-t-il d'une définition de l'utilisation malveillante du DNS ? Dans l'affirmative, quelle est-elle ?
- Les autorités publiques de votre pays ont-elles été confrontées à des noms de domaine semblant avoir été utilisés à des fins d'utilisation malveillante du DNS et ont-elles signalé ces noms de domaine à l'opérateur de registre ou au bureau d'enregistrement concerné ? Dans l'affirmative, dans quelle proportion les noms de domaine gTLD signalés à l'opérateur de registre ou au bureau d'enregistrement ont-ils été signalés au département de l'ICANN en charge de la conformité du fait de l'incapacité des parties contractantes à prendre des mesures opportunes et raisonnables en réponse audit signalement ?
- Dans quelle proportion les noms semblant avoir été utilisés à des fins d'utilisation malveillante du DNS ont-ils été enregistrés dans les gTLD (par rapport à l'enregistrement dans des ccTLD) ?
- Les autorités publiques de votre pays ont-elles pris connaissance des directives publiées par le Groupe des représentants des bureaux d'enregistrement qui fournissent des informations pouvant être utiles pour le dépôt de plaintes liées à des cas d'abus auprès des bureaux d'enregistrement ?
- Les autorités publiques de votre pays connaissent-elles les dispositions du contrat de registre (RA) et du contrat d'accréditation de bureau d'enregistrement (RAA) devant être appliquées et dont l'ICANN assure le respect ? (notamment la spécification 11(3a) et (3b) du RA et 3.18 du RAA)
- Selon les autorités publiques de votre pays, de quels pouvoirs et mécanismes de contrainte l'ICANN dispose-t-elle eu égard aux domaines malveillants ?

Concernant les initiatives de l'organisation ICANN visant à détecter et signaler les menaces à la sécurité :

- Le système de signalement des cas d'utilisation malveillante des noms de domaine (DAAR) de l'ICANN a pour but de fournir à la communauté de l'ICANN des données factuelles, fiables, persistantes et objectives à l'aide d'une méthodologie ouverte et approuvée par la communauté qui peut être utilisée afin d'aider à éclairer les discussions politiques. Selon votre gouvernement ou les autorités publiques compétentes de votre pays, quelles améliorations devraient être apportées au DAAR ?
- Selon votre gouvernement ou les autorités publiques compétentes de votre pays, quelles améliorations devraient être apportées à l'outil de signalement et de collecte d'informations sur les menaces à la sécurité des noms de domaine (DNSTICR) de l'ICANN qui vise à identifier les logiciels malveillants et tentatives d'hameçonnage liés au COVID-19 ?
- Votre gouvernement est-il au fait des résultats de ces initiatives ? Sait-il notamment que des problèmes devant être signalés aux parties contractantes ont été détectés dans quelques centaines de noms de domaine ?

Concernant les efforts de l'ICANN visant à soutenir l'atténuation des menaces à la sécurité du DNS :

- Votre gouvernement estime-t-il qu'il est judicieux que l'ICANN se concentre sur le soutien à l'atténuation des menaces à la sécurité du DNS dans les gTLD, tel que défini par le GAC (hameçonnage, logiciels malveillants, commande et contrôle de réseaux zombies, dévoiement et courriers indésirables lorsqu'ils sont utilisés comme vecteur de diffusion des autres types de menaces à la sécurité), à la lumière de l'interdiction, posée par les statuts constitutifs de l'ICANN, de la régulation des contenus et de l'absence de compétence eu égard aux ccTLD ?
- Votre gouvernement pourrait-il contribuer aux délibérations en cours de la communauté de l'ICANN visant à définir le problème et à déterminer la meilleure marche à suivre pour atténuer l'utilisation malveillante du DNS, à savoir de bonnes pratiques volontaires, une politique de consensus ou une combinaison de ces options ?
- Selon votre gouvernement, quelles données objectives et factuelles l'organisation ICANN pourrait-elle fournir afin de faciliter les discussions de la communauté ?

Documents de référence clés

- Documents du GAC sur l'utilisation malveillante du DNS
  - Séance du GAC de l'ICANN70 sur l'utilisation malveillante du DNS (23 mars 2020)
  - Document d'information du GAC sur l'utilisation malveillante du DNS de l'ICANN68 (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 du communiqué du GAC d'Hyderabad (8 novembre 2016) et au suivi du communiqué du GAC de Copenhague (15 mars 2017)
- Définition de l'utilisation malveillante du DNS (comprenant les perspectives des parties prenantes du secteur)
  - Définition de l'utilisation malveillante du DNS des parties contractantes (octobre 2020)
  - Cadre de lutte contre l'utilisation malveillante (17 octobre 2019)
  - Déclaration du GAC sur l'utilisation malveillante du DNS (18 septembre 2019)
- Rapport final de la révision SSR2 (25 janvier 2021)
- Révision RDS/WHOIS2
  - Fiche de suivi des décisions du Conseil d'administration de l'ICANN (25 février 2020) sur les recommandations finales issues de la révision RDS-WHOIS2
  - Recommandations finales issues de la révision RDS-WHOIS2 (3 septembre 2019)
- Révision de la concurrence, de la confiance et du choix du consommateur
  - Fiche de suivi des décisions du Conseil d'administration de l'ICANN (22 octobre 2020) sur 11 des 17 recommandations CCT et suite à l'évaluation détaillée fournie par l'organisation ICANN
  - Fiche de suivi des décisions du Conseil d'administration de l'ICANN sur les recommandations finales CCT (1er mars 2019)
  - Recommandations et rapport final de la révision CCT (8 septembre 2018), en particulier la section 9 relative aux sauvegardes (p. 88)
  - Analyse statistique de l'utilisation malveillante du DNS dans les gTLD (9 août 2017)

Gestion des documents

Réunion	Forum virtuel de politiques de l'ICANN71, 14-17 juin 2021
Titre	Document d'information du GAC sur l'ICANN71 - Séance 3 - Utilisation malveillante du DNS
Distribution	Membres du GAC (avant la réunion) et public (après la réunion)
Date de distribution	Version 1 : 1er juin 2021