ICANN | GAC
Governmental Advisory Committee

ICANN 65 POLICY FORUM
MARRAKECH
24–27 June 2019

Atténuation de l'utilisation malveillante du DNS

Séance 5.1

Contenus

Objectifs de la séance

- Examiner les évolutions et discussions récentes concernant la définition, la détection et l'atténuation de l'utilisation malveillante du DNS ainsi que l'impact de la conformité du WHOIS par rapport aux initiatives du RGPD.
- Discuter des positions et prochaines étapes possibles du groupe de travail du GAC sur la sécurité publique (PSWG).

Contexte

Des activités malveillantes sur Internet menacent et affectent les titulaires de noms de domaine ainsi que les utilisateurs finaux en exploitant les failles dans tous les aspects des écosystèmes du DNS et de l'Internet (protocoles, systèmes informatiques, transactions personnelles et individuelles, procédures d'enregistrement de domaines, etc.). Certaines de ces activités malfaisantes menacent la sécurité, stabilité et 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. L'utilisation malveillante du DNS est en général considérée comme incluant tout ou partie d'activités comme : déni de service distribué (DDOS), courrier indésirable, hameçonnage, logiciel malveillant, réseau zombie et diffusion de documents illégaux. Alors que tout le monde semble s'accorder à dire que l'utilisation malveillante est un problème qui doit être traité, il existe des divergences d'opinion quant à savoir à qui incombe la responsabilité. Les registres et bureaux d'enregistrement en particulier, s'inquiètent de devoir en faire plus, car ceci impacterait leur modèle commercial et leur bénéfice net.

Dans le cadre de ces discussions, 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 entreprises au sein de la communauté de l'ICANN pour traiter la question de l'utilisation malveillante du DNS, certaines ont bénéficié de la participation du GAC :

- **L'organisation de soutien aux extensions génériques (GNSO)** de l'ICANN créant le groupe de travail sur les politiques en matière d'enregistrements frauduleux en 2008. Ce dernier a identifié un ensemble de problèmes spécifiques mais n'a pas proposé de politiques ni de discussions concernant la mise en place de meilleures pratiques non contraignantes pour les registres et bureaux d'enregistrement (notamment des ateliers pendant l'ICANN41 et l'ICANN42).

- **Dans le cadre du programme des nouveaux gTLD,** une série de nouvelles exigences[2] adoptée par l'ICANN conformément à son protocole Réduire les comportements malveillants (3 octobre 2009). Son efficacité a finalement été évaluée dans le rapport de l'ICANN sur les sauvegardes du programme des nouveaux gTLD (18 juillet 2016), en préparation de la révision prévue dans les statuts constitutifs (révision CCT).

- Avant la création du groupe de travail du GAC sur la sécurité publique (PSWG), **les représentants des organismes d'application de la loi (LEA)** ont eu un rôle majeur dans les

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

[2] Le contrôle des opérateurs de registre, exigeant un plan démontré pour le déploiement des DNSSEC, interdisant l'utilisation de caractères génériques, supprimant l'enregistrement orphelin de type glue lorsqu'une entrée de serveur de nom est supprimée de la zone, exigeant la maintenance des enregistrements du WHOIS détaillé, la centralisation de l'accès aux fichiers de zone, exigeant des points de contacts et des procédures pour le signalement d'abus au niveau du registre

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

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

- **L'organisation de l'ICANN**, par le biais de son **équipe en charge de la sécurité, stabilité et résilience (SSR)** forme régulièrement les communautés responsables de la sécurité publique et répond aux cyber-incidents 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 mené un projet 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 permet de créer de la transparence et d'identifier les sources de problèmes qui pourront ensuite être traités grâce aux politiques de conformité, ou si besoin, grâce à la création 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 existantes pour atténuer l'utilisation malveillante du DNS, les engagements de la communauté pilotés par le GAC ainsi que la révision par la CCT de l'analyse statistique de l'utilisation malveillante du DNS dans les gTLD (9 août 2017), qui ont mis en évidence des tendances d'abus, des pratiques commerciales entrainant des abus et des preuves qu'il existe « *un espace de développement et de renforcement de mesures d'atténuation et des sauvegardes* » ainsi qu'une possibilité d'élaboration de politiques futures[4].

De plus, suite à l'entrée en vigueur du Règlement général sur la protection des données (RGPD) de l'Union Européenne et suite aux initiatives pour rendre conforme le système WHOIS, outil de recherche pour les utilisations malveillantes et crimes majeurs, des inquiétudes quant à la capacité

[3] Voir les recommandations relatives à la diligence raisonnable et à l'application de la loi (Oct. 2019) ainsi que les12 recommandations relatives à l'application de la loi (1er mars 2012)
[4] Voir commentaire du GAC (19 septembre 2017) sur le rapport final de l'analyse statistique de l'utilisation malveillante du DNS dans les gTLD.

à atténuer l'utilisation malveillante du DNS se sont accrues dans le secteur de la protection de la propriété intellectuelle, de l'application des lois, de la cybersécurité et de la protection des consommateurs[5].

Dans ce contexte, les comités consultatifs de l'ICANN, en particulier le GAC, le SSAC et l'ALAC, ainsi que plusieurs tierces parties impactées, ont été signalés par le département de l'ICANN en charge de la conformité contractuelle et de la protection des consommateurs comme demandant à l'organisation de l'ICANN et à la communauté de l'ICANN de prendre davantage de mesures[6].

De telles mesures exigeraient de la communauté de l'ICANN qu'elle parvienne à une forme de consensus autour d'un certain nombre de questions ouvertes. Les discussions concernant l'atténuation des abus et l'éventuel travail de politique 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 un abus, compte tenu des compétences de l'ICANN et de ses contrats avec les registres et bureaux d'enregistrement ?
- **la détection et le signalement de l'utilisation malveillante du DNS (sensibilisation et transparence) :**
  comment garantir que l'utilisation malveillante du DNS est détectée et portée à la connaissance des parties prenantes concernées, dont les consommateurs et utilisateurs d'Internet ?
- **la prévention et l'atténuation de l'utilisation malveillante du DNS (perspective d'efficacité) :**
  quels outils et quelles procédures peuvent utiliser l'organisation de l'ICANN, les acteurs du secteur et les parties prenantes intéressées pour réduire les abus et y répondre de manière appropriée lorsqu'ils surviennent ? 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 utilisateurs Internet, pourrait vouloir activement participer aux discussions sur ces questions pour que des progrès soient réalisés en vue d'une prévention et d'une atténuation plus efficaces des abus.

[5] Voir article III.2 et IV.2 du communiqué de Barcelone du GAC (25 octobre 2018) relatif aux enquêtes concernant l'impact sur l'application de la loi, voir l'article 5.3.1 du rapport préliminaire de l'équipe de révision RDS (31 août 2018) et la publication des groupes de travail 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 pendant le sommet GDD (7-8 mai 2019)

Proposition des dirigeants pour l'action du GAC

Lors de la réunion ICANN65 à Marrakech, le GAC peut vouloir :

1. **Mettre en place un processus pour clarifier ce qui constitue une utilisation malveillante du DNS** vis-à-vis de la mission de l'ICANN, et faire part de sa position sur cette question. Cela pourrait être utile pour faire avancer les discussions au sein de la communauté de l'ICANN concernant l'existence d'une telle définition, les recommandations de l'équipe de révision CCT sur l'utilisation malveillante du DNS, sa prise en considération par le Conseil d'administration, ainsi que les initiatives actuelles du rôle de l'ICANN dans la protection des consommateurs.

2. **Prendre en considération le besoin et l'opportunité pour l'élaboration de politiques**, en lien avec les discussions récentes sur cette possibilité pendant le sommet GDD[7], et en prenant note des positions préalables du GAC sur ce sujet[8].

3. **Examiner les mesures prises suite aux recommandations de la révision CCT** relatives à l'utilisation malveillante du DNS (recommandations 14 à 19), y compris leur prise en compte par le Conseil d'administration de l'ICANN et le travail demandé à l'organisation de l'ICANN, ainsi qu'un examen plus poussé par les unités constitutives de l'ICANN.

4. **Envisager de mettre en valeur les meilleures pratiques de l'industrie dans l'espace de nom des ccTLD**, comme celui de .DK présenté lors de l'ICANN64[9] et sa candidature pour l'industrie gTLD.

---

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

[8] En effet, dans son commentaire (19 septembre 2017) sur le rapport final de l'analyse statistique de l'utilisation malveillante du DNS dans les gTLD, le GAC a noté que :

- « l'étude relative à l'utilisation malveillante du DNS fait rapidement référence à la conclusion selon laquelle certaines URL sont utilisées plus largement pour diffuser du contenu pédopornographique […] Il serait utile que le rapport explique, précise et/ou quantifie plus clairement cette déclaration et qu'ainsi, les parties prenantes comprennent dans quelle mesure cette étude a examiné cette question, et qu'il donne des informations sur toutes considérations politiques futures »
- « Les corrélations entre des politiques d'enregistrement plus strictes et la diminution des abus montrent qu'il existe des domaines où l'élaboration de futures politiques serait utile. »
- « L'utilisation d'une analyse statistique devrait être prise en compte dans les futures politiques sur l'utilisation malveillante du DNS, et davantage d'analyses devraient être effectuées pour étudier comment ces informations pourraient étayer les initiatives de l'ICANN et de ses équipes en charge de la sécurité et de la conformité contractuelle afin de répondre avec efficacité à la question de l'utilisation malveillante du DNS et d'empêcher de futurs abus. »

[9] Voir la séance sur les leçons retenues : Comment .DK a réussi à réduire les domaines malveillants (13 mars 2019) puis les discussions du PSWG (17 avril 2019)

Développements pertinents

Définition de l'utilisation malveillante du DNS : un consensus sur l'utilisation malveillante de l'infrastructure ?

Comme souligné récemment lors du sommet GDD (7-9 mai 2019), il n'existe **pas d'accord communautaire sur ce qui constitue une utilisation malveillante du DNS**, en partie à cause des inquiétudes de certaines parties prenantes sur le fait que l'ICANN outrepasse son mandat, des inquiétudes à propos des impacts sur le droit des utilisateurs et de l'impact sur le bénéfice net des parties contractantes[10].

Cependant, selon l'équipe de révision CCT il existe **un consensus sur ce qui constitue 'les abus en matière de sécurité du DNS' ou 'les abus en matière de sécurité de l'infrastructure du DNS**'. On comprend qu'ils incluent « davantage de formes techniques de l'activité malveillante », telles que : logiciel malveillant, hameçonnage et réseau zombie, ainsi que le spam *« lorsqu'il est utilisé comme une méthode de diffusion pour d'autres formes d'abus »*[11].

Récemment, **le département de l'ICANN en charge de la conformité contractuelle a fait référence à 'l'utilisation malveillante de l'infrastructure du DNS'** dans ses communications concernant les audits de registres et de bureaux d'enregistrement concernant la mise en place de dispositions contractuelles dans le contrat de registre des nouveaux gTLD (spécification 11 3b), qui fait référence aux « *menaces à la sécurité comme le détournement (pharming), l'hameçonnage, les programmes malveillants et les réseaux zombie*s »[12], dans le contrat d'accréditation de bureau d'enregistrement (article 3.18), qui fait référence aux « *contacts en cas d'abus* » et aux « *signalements d'abus* » sans donner de définition du terme 'abus' en particulier, mais en incluant 'l'activité illégale'.

Du point de vue du GAC, la définition de 'menaces à la sécurité' dans le contrat de registre des nouveaux gTLD est en réalité l'exacte transcription de **la définition donnée dans l'avis du GAC relatif aux sauvegardes de 'vérifications de sécurité'** applicables à l'ensemble des nouveaux gTLD dans le Communiqué de Beijing (11 avril 2013).

Suite à la résolution du Conseil d'administration (1er mars 2019) demandant à l'organisation de l'ICANN de « *faciliter les initiatives de la communauté pour qu'elle développe une définition « d'abus » afin d'éclairer les futures mesures à prendre concernant cette recommandation*. » [13], et

[10] En effet, la définition d'atténuation de l'utilisation malveillante peut avoir des conséquences sur la portée des activités supervisées par les contrats et politiques de l'ICANN. Alors que des gouvernements ainsi que d'autres parties prenantes s'inquiètent de 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, leur compétitivité, l'augmentation des coûts de fonctionnement et la responsabilité que peuvent devoir assumer les titulaires de noms de domaine lorsqu'une mesure est prise face à des domaines malveillants. De leur côté, les parties prenantes non-commerciales s'inquiètent de la violation de la liberté d'expression et le respect de la vie privée des titulaires de noms de domaine et des utilisateurs Internet, et partagent avec des parties contractantes des inquiétudes concernant le fait que l'ICANN outrepasse sa mission.

[11] Voir p.88 du rapport final de révision CCT (8 septembre 2018)

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

[13] Voir p.5 de la fiche de suivi sur l'action du Conseil d'administration vis-à-vis des recommandations finales du CCT

suite aux activités de renforcement de la fonction de protection des consommateurs de l'organisation de l'ICANN, **davantage de discussions sur la définition d'abus sont attendues d'ici l'ICANN66** à Montréal (2-7 novembre 2019).

Définition de l'utilisation malveillante du DNS : dialogue sur la protection des consommateurs

Depuis que la fonction de conformité contractuelle de l'ICANN a évolué afin d'inclure la protection des consommateurs en 2017[14], le GAC a participé à plusieurs développements :

- l' introduction d'un directeur de la protection des consommateurs (27 juin 2017) qui a discuté de la mise en place de discussions communautaires informelles pour renforcer la sensibilisation et la compréhension communautaire, et identifier des manières pour l'organisation de l'ICANN d'améliorer ses performances en matière de conformité contractuelle et de protection des consommateurs.

- des discussions en séminaire web sur la conformité contractuelle et la protection des consommateurs (25 septembre 2017), auxquelles ont assisté près de 100 membres de la communauté, y compris des discussions sur un résumé des sauvegardes qui relèvent de l'ICANN (11 septembre 2017) suivi de questions soumises aux commentaires de la communauté dans un article de blog ultérieur (11 octobre 2017) :
    - Quel rôle devrait tenir l'ICANN dans la gestion de l'utilisation malveillante du DNS ?
    - Existe-t-il un écart entre l'utilisation malveillante du DNS et la compétence de l'ICANN à traiter les problèmes d'abus ?
    - Quels outils ou quelles données supplémentaires pourraient être utiles à l'évaluation de l'utilisation malveillante du DNS ?
    - Est-ce qu'il y a des domaines où des mesures volontaires pourraient être utiles ?
    - Comment l'ICANN devrait collaborer avec d'autres parties prenantes pour traiter ces problèmes d'abus ?
    - Existe-t-il une menace d'intervention gouvernementale si la communauté de l'ICANN ne peut traiter de manière satisfaisante la question de l'utilisation malveillante du DNS ?

- une réunion des représentants de la communauté à Washington DC (11 janvier 2019) a été organisée pour examiner davantage cette problématique en vue d'une éventuelle participation de la communauté lors des réunions ICANN.

Plus récemment, lors du sommet GDD (9 mai 2019), le département en charge de la conformité contractuelle et de la protection des consommateurs a organisé une séance pour poursuivre les discussions :

- **Certaines parties contractantes considèrent que leurs pratiques anti-abus sont appropriées et s'opposent aux obligations à venir**, notamment à cause de la portée limitée des attributions de l'ICANN et du fardeau que représentent les signalements d'abus qui ne feront pas l'objet de mesures (souvent soumis par des parties qui ne connaissent pas la

[14] Avec l'embauche d'un directeur de la protection des consommateurs (23 mai 2017) chargé de « *sensibiliser aux sauvegardes existantes de l'ICANN, de faciliter des discussions parmi les parties prenantes concernant la façon dont l'ICANN pourrait éventuellement améliorer ses mécanismes de sauvegardes* »

portée limitée des mesures d'atténuation disponibles pour les registres[15] et bureaux d'enregistrement).

- D'autres représentants ont suggéré **que l'ICANN avait le devoir d'établir des règles et des mesures d'incitation** appropriées pour dissuader les personnes malveillantes sans pour autant nuire aux acteurs responsables (**principe 'pollueur-payeur**') et ont suggéré que ces **parties coupables d'abus devraient être citées** dans les rapports pertinents de l'ICANN.
- **L'organisation de l'ICANN a introduit l'idée qu'un processus d'élaboration de politiques** harmonise les contrats avec les attentes des comités consultatifs et tierces parties, et qu'il limite l'impact de futures législations hétérogènes qui pourraient être mises en œuvre à la place des politiques de l'ICANN.
- Cette suggestion a rencontré une **vive opposition et la demande d'alternatives pour traiter le problème**, notamment en conciliant les définitions existantes au sein de l'ensemble des parties de la communauté ou en engageant des négociations sur le contrat de registre comme ce qui avait été fait pour le RAA 2013.
- **Les parties contractantes** ont demandé à ce que **l'organisation de l'ICANN facilitent des initiatives visant à instruire la communauté de l'ICANN** pour leur compte lors de l'ICANN66 à Montréal, avec notamment une présentation des meilleures pratiques et en apportant des données qui montrent la prévalence des plaintes qui ne font pas l'objet de mesures.

Sensibilisation et transparence : participation de la communauté guidée par le GAC

Le GAC et son groupe de travail sur la sécurité publique (PSWG) a guidé plusieurs participations intercommunautaires lors de réunions de l'ICANN ces dernières années, cherchant à **accroître la sensibilisation et à explorer des solutions avec les experts pertinents**, principalement :

- 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 abus 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 qui constitue une utilisation malveillante du DNS ;
  - la diversité des modèles commerciaux, des pratiques et des compétences influençant les approches visant à atténuer les abus ; et
  - le besoin de plus de coopération dans l'ensemble du secteur, en s'appuyant sur des données partagées sur les menaces à la sécurité.
- Lors de l'ICANN58 à Copenhague (13 mars 2017), le PSWG du GAC a animé une séance intercommunautaire Vers une atténuation efficace de l'utilisation malveillante du DNS :

[15] Voir par exemple les *Catégories de mesures des registres pour répondre aux menaces à la sécurité* au sein du cadre de référence des opérateurs de registre pour répondre aux menaces contre la sécurité

prévention, atténuation et réponse qui a abordé la question des tendances récentes dans l'utilisation malveillante du DNS, en particulier l'hameçonnage, ainsi que les comportements comme le saut de nom de domaine parmi les bureaux d'enregistrement et les TLD qui pourraient demander des réponses plus coordonnées et détaillées au sein du secteur. La séance a également permis de mettre en avant :
    - l'émergence de l'initiative Signalement des cas d'utilisation malveillante des noms de domaine (DAAR),
    - la collaboration actuelle entre le département de conformité contractuelle et les fonctions SSR de l'organisation de l'ICANN, et
    - l'occasion de tirer profit des procédures d'enchères des nouveaux gTLD pour financer l'atténuation des abus

- 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 en vue de politiques fondées sur les faits et d'une atténuation efficace pour discuter de la mise en place de mécanismes de signalement fiables, publics et exploitables pour la prévention et l'atténuation des abus, et pour permettre la création de politiques basées sur des preuves. La séance a confirmé la nécessité que soient publiées des données fiables et détaillées sur l'utilisation malveillante du DNS, telles qu'elles sont 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[16].

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

Un certain nombre de sauvegardes face à l'utilisation malveillante du DNS ont été mises en place au sein du programme des nouveaux gTLD avec de nouvelles exigences[17] adoptées par l'organisation de l'ICANN conformément à son protocole Réduire les comportements malveillants (3 octobre 2009) et l'avis du GAC relatif aux sauvegardes sur les contrôles de sécurité.

En s'appuyant sur l'évaluation par l'organisation de l'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 a cherché une analyse comparative plus complète des taux d'abus dans les nouveaux gTLD et gTLD historiques, avec notamment une analyse statistique inférentielle des hypothèses comme les corrélations entre le prix de vente d'un nom de domaine et les taux d'abus.

Les conclusions de cette analyse statistique de l'utilisation malveillante du DNS dans les gTLD (9 août 2017) ont été soumises pour commentaire public. Les commentaires de la communauté ont été rapportés (13 octobre 2017) comme étant constructifs, saluant la rigueur scientifique de l'analyse et demandant davantage d'études.

Dans ses commentaires (19 septembre 2017), le GAC a souligné, parmi les conclusions, que :

[16] Voir annexe 1 : principes d'atténuation des abus au sein de la présentation du GAC lors de l'ICANN60 sur l'utilisation malveillante du DNS ainsi que le rapport de séance dans le Communiqué d'Abu Dhabi du GAC (p.3)

[17] Le contrôle des opérateurs de registre, exigeant un plan démontré pour le déploiement des DNSSEC, interdisant l'utilisation de caractères génériques, supprimant l'enregistrement orphelin de type glue lorsqu'une entrée de serveur de nom est supprimée de la zone, exigeant la maintenance des enregistrements du WHOIS détaillé, la centralisation de l'accès aux fichiers de zone, exigeant des points de contacts et des procédures pour le signalement d'abus au niveau du registre

- l'étude avait clairement mis en avant l'existence de problèmes d'abus au sein du DNS :
    - dans certains nouveaux gTLD, plus de 50 % des enregistrements sont abusifs
    - cinq nouveaux gTLD représentaient 58,7 % des domaines blacklistés pour hameçonnage au sein des nouveaux gTLD
- l'utilisation malveillante est en lien direct avec les politiques des opérateurs de registre :
    - les opérateurs de registre qui pratiquent une concurrence des prix ont le plus grand nombre de nouveaux gTLD victimes de malveillances ;
    - Les personnes malveillantes préfèrent enregistrer des domaines au sein de nouveaux gTLD standards (ouverts pour enregistrement public) plutôt qu'au sein des nouveaux gTLD communautaires (restrictions quant à qui peut enregistrer des noms de domaine)
- Il convient d'envisager l'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 mesures de protection contre les abus, 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 des informations avec la communauté concernant les niveaux d'utilisation malveillante du DNS.

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 de l'ICANN est apparu comme un projet de recherche parallèlement à la participation du PSWG et du GAC au projet du Conseil d'administration et de la communauté de l'ICANN sur l'efficacité des mesures d'atténuation de l'utilisation malveillante du DNS, entre les réunions ICANN57 (nov. 2016) et ICANN60 (Nov. 2017)[18].

L'objectif annoncé du DAAR est de « *signaler les menaces à la sécurité à la communauté de l'ICANN, pour 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, à partir de la compilation des données d'enregistrement TLD avec des informations issues de flux de données hautement fiables relatives aux menaces à la sécurité[19].

À cet effet, le DAAR contribue aux exigences identifiées par le GAC pour la publication de « données détaillées et fiables sur l'utilisation malveillante du DNS » dans le Communiqué du GAC d'Abu Dhabi (1er novembre 2017). Cependant, comme souligné dans une récente lettre du

[18] Voir séances intercommunautaires menées par le PSWG du GAC lors de l'ICANN57 (nov. 2016), ICANN58 (mars 2017) et ICANN60 (octobre 2017), ainsi que les questions au Conseil d'administration de l'ICANN concernant l'efficacité des sauvegardes de l'utilisation malveillante du DNS dans le Communiqué d'Hyderabad (8 novembre 2016), les questions de suivi dans le Communiqué de Copenhague du GAC (15 mars 2017)

[19] Pour plus d'informations, voir https://www.icann.org/octo-ssr/daar-faqs

M3AAWG[20] à l'organisation de l'ICANN (5 avril 2019), en n'intégrant pas les informations de menaces à la sécurité pour chaque bureau d'enregistrement, chaque TLD, le DAAR n'est toujours pas à la hauteur des attentes des membres du PSWG du GAC et des partenaires en charge de la cybersécurité sur le fait qu'il apporte des informations exploitables.

Efficacité : sauvegardes actuelles quant à l'utilisation malveillante du DNS au sein des contrats de registres et de bureaux d'enregistrement

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

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

Après les premières années de fonctionnement des nouveaux gTLD, lors de la réunion ICANN 57 (novembre 2016), **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 des éclaircissements quant à leur mise en œuvre par le Conseil d'administration de l'ICANN. Des discussions ont alors eu lieu entre le GAC et l'organisation de l'ICANN, avec des questions de suivi dans le Communiqué de Copenhague du GAC (15 mars 2017) et un ensemble de réponses préliminaires (30 mai 2017) qui ont été abordées lors d'une téléconférence entre le GAC et le président-directeur général de l'ICANN (15 juin 2017). Plusieurs questions sont toujours ouvertes et de nouvelles questions ont été identifiées, comme le reflète le 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 pour les nouveaux gTLD a été publié le 8 juin 2017 en réponse aux questions de certains opérateurs de registre qui cherchaient à savoir comment garantir la conformité avec l'article 3b de la spécification 11 du contrat de registre des nouveaux gTLD. **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, comme requis par la spécification 11.3b.

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

Dans le cadre d'audits réguliers réalisés par le département contractuel de l'ICANN, un audit ciblé sur 20 gTLD relatif à leurs « *processus, procédures, et gestion de l'infrastructure du DNS* », entre mars et septembre 2018, a révélé « *qu'il y avait des rapports de sécurité et des analyses incomplets pour 13 domaines de premier niveau (TLD), ainsi qu'un manque de procédures de gestion des abus normalisées ou documentées et aucune action entreprise pour les menaces identifiées* »[21].
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 dans le cadre des menaces à la sécurité et à l'utilisation malveillante de l'infrastructure du DNS* ». Comme rapporté lors du sommet GDD (9 mai 2019), l'organisation de l'ICANN devrait publier le rapport final de cet audit (à l'origine prévu pour mai 2019) et prévoit actuellement de lancer un audit similaire pour les bureaux d'enregistrement, à partir de juillet 2019.

Des parties contractantes ont remis en question ces audits qui dépasseraient leurs obligations contractuelles[22]. Des groupes de représentants des bureaux d'enregistrement et des registre **sont considérés comme travaillant avec le département de la conformité contractuelle de l'ICANN** afin de garantir que le rapport final de l'audit des registres sur l'infrastructure du DNS explique clairement les attributions de l'ICANN (pour éviter que des inquiétudes entrainent des téléconférences avec la communauté pour le lancement d'un processus d'élaboration de politiques), et s'assurer que les inquiétudes des bureaux d'enregistrement soient prises en compte avant le démarrage de leur audit.

Efficacité : cadre de mesures non-contraignantes à mettre en œuvre par les registres pour répondre à des menaces à la sécurité

Dans le cadre du programme des nouveaux gTLD, le Conseil d'administration de l'ICANN a stipulé (25 juin 2013) inclure lesdites « menaces à la sécurité » (Communiqué de Beijing sur l'avis du GAC relatif aux sauvegardes) 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, bureaux d'enregistrement et du GAC (dont des membres du PSWG) qui ont développé le

[21] Comme rapporté dans l'article de blog du 8 novembre 2018, conformité contractuelle : répondre à l'utilisation malveillante de l'infrastructure du DNS : https://www.icann.org/news/blog/contractual-compliance-addressing-domain-name-system-dns-infrastructure-abuse

[22] Voir les correspondances du RySG (2 novembre 2019) auxquelles l'organisation de l'ICANN a répondu (8 novembre), et dans 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 leurs obligations contractuelles [en particulier selon la spécification 11 3b] *et ont* indiqué leur réticence à « *partager avec l'ICANN et la communauté des informations pertinentes concernant nos efforts en cours pour 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* »

cadre de mesures à mettre en œuvre par les opérateurs de registre pour répondre à des menaces à la sécurité publié le 20 octobre 2017 après commentaires publics.

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, dont notamment des rapports d'application de la loi. Il introduit une fenêtre de 24 h maximum pour répondre aux demandes avec une priorité élevée (menace imminente pour la vie humaine, infrastructure critique ou exploitation de mineurs) à partir d'une origine crédible et légitime comme une autorité gouvernementale 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 son rôle d'évaluateur de l'efficacité du cadre lors d'une prochaine révision[23].

Efficacité : mesures proactives et prévention des abus généralisés

À partir de son analyse du paysage de l'utilisation malveillante du DNS[24], avec la prise en 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 **empêcher l'utilisation généralisée de bureaux d'enregistrement ou registres spécifiques** pour les abus de sécurité du DNS, avec notamment des seuils d'abus à partir desquels des enquêtes de conformité sont systématiquement déclenchées et envisager une politique de règlement de litiges relatifs à l'utilisation malveillante du DNS (DADRP) si la communauté détermine que l'organisation de l'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 stipulé (1er mars 2019) mettre ces recommandations « en attente » car il a demandé à l'organisation de l'ICANN de « *faciliter les initiatives de la communauté pour qu'elle développe une définition « d'abus » afin d'éclairer les futures mesures à prendre concernant cette recommandation*. »[25]

[23] Recommandation 19 de la révision CCT : *la prochaine CCT-RT devrait examiner le « cadre de mesures à mettre en œuvre par les opérateurs de registre pour répondre à des menaces à la sécurité » et déterminer si ce cadre constitue un mécanisme suffisamment clair et efficace afin de réduire les abus en fournissant des actions précises en réponse à des menaces à la sécurité.*

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

[25] Voir p.5 de la fiche de suivi sur l'action du Conseil d'administration vis-à-vis des recommandations finales du CCT

Positions actuelles

- Communiqué de Nairobi du GAC (10 mars 2010) article VI. Recommandations relatives à la diligence raisonnable et l'application de la loi
- Communiqué de Dakar du GAC (27 octobre 2011) article III. Recommandations sur l'application de la loi (LEA)
- Communiqué de Beijing du GAC (11 avril 2013), en particulier sur les sauvegardes relatives aux 'vérifications de sécurité' applicables à tous les nouveaux gTLD (p.7)
- Communiqué d'Hyderabad du GAC (8 novembre 2016) comprenant l'avis relatif à l'atténuation des abus exigeant des réponses à l'annexe 1 : questions au Conseil d'administration de l'ICANN sur l'atténuation de l'utilisation malveillante du DNS par l'ICANN et les parties contractantes (pp.14-17)
- Communiqué de Copenhague du GAC (15 mars 2017) comprenant l'avis relatif à l'atténuation des abus exigeant des réponses à la fiche de suivi du GAC à l'annexe 1 du Communiqué d'Hyderabad du GAC (pp. 11-32)
- Communiqué de Barcelone du GAC (25 octobre 2018) en particulier les articles III.2 Groupe de travail du GAC sur la sécurité publique (p.3) et IV.2 le WHOIS et les lois de protection des données (p.5)
- Commentaire du GAC sur le rapport initial du SADAG (21 mai 2016)
- 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 final de la révision CCT et de ses recommandations (11 décembre 2018)

Documents de référence principaux

- Recommandations relatives à la diligence raisonnable et l'application de la loi (Oct. 2019)
- Recommandations des LEA concernant les amendements au contrat de registre (1er mars 2012)
- Avis du GAC relatif aux sauvegardes de 'vérifications de sécurité' applicables à tous les nouveaux gTLD (9.7) Communiqué de Beijing (11 avril 2013)
- Questions du GAC sur l'atténuation des abus et réponses préliminaires de l'ICANN (30 mai 2017) conformément à l'avis dans le Communiqué d'Hyderabad du GAC (8 novembre 2016) et le suivi dans le Communiqué de Copenhague du GAC (15 mars 2017)
- Analyse statistique de l'utilisation malveillante du DNS (9 août 2017)
- Commentaire du GAC sur l'analyse statistique de l'utilisation malveillante du DNS dans les gTLD (19 septembre 2017)
- Commentaire du GAC (16 janvier 2018) sur les nouveaux articles du rapport préliminaire de l'équipe de révision CCT (27 novembre 2017)

- Recommandations et rapport final de la révision CCT (8 septembre 2018), en particulier l'article 9 sur les sauvegardes (p.88)
- Commentaire du GAC sur le rapport final de la révision CCT et de ses recommandations (11 décembre 2018)
- Fiche de suivi sur l'action du Conseil d'administration de l'ICANN quant aux recommandations finales du CCT (1er mars 2019)

Informations connexes

- Séance 11.1 du GAC lors de l'ICANN65 sur les révisions ICANN (avec une présentation importante sur le statut de la mise en œuvre des recommandations de la révision CCT)
- Séance 8.1 du GAC lors de l'ICANN65 sur le WHOIS et la politique de protection des données
- Séance 4.1 du GAC lors de l'ICANN65 sur le PDP relatif aux procédures pour des séries ultérieures de nouveaux gTLD

Gestion des documents

Réunion	ICANN65, Marrakech, 24-27 juin 2019
Titre	Atténuation de l'utilisation malveillante du DNS
Distribution	Membres du GAC et public (après la réunion)
Date de distribution	Version 1 : 6 juin 2019