ICANN | GAC
Governmental Advisory Committee

ICANN 69
VIRTUAL ANNUAL GENERAL

Mise à jour du Groupe de travail sur la sécurité publique (PSWG)

Séance 5 - Mise à jour du PSWG au GAC

Table des matières

Objectif de la séance

Le groupe de travail sur la sécurité publique (PSWG) du GAC fournira une mise à jour de son travail conformément à ses objectifs stratégiques visant à atténuer l'utilisation malveillante et la cybercriminalité liées au DNS, à préserver et à améliorer l'accès aux données d'enregistrement de noms de domaine (et leur exactitude) et à assurer des opérations efficaces du PSWG et des relations avec les parties prenantes.

Contexte

Depuis 2003, les représentants des organismes d'application de la loi et les agences de protection des consommateurs du monde entier participent aux délibérations sur les politiques Internet à l'ICANN et à travers les Registres Internet régionaux (AfriNIC, APNIC, ARIN, LACNIC et RIPE NCC).

Alors qu'au départ les agences de sécurité publique à l'ICANN aient mis l'accent sur la nécessité d'obtenir des informations WHOIS ouvertes et exactes pour les enquêtes internationales sur l'application de la loi, elles ont très rapidement intégré la prévention et la réponse à l'exploitation des enregistrements de noms de domaine à des fins malveillantes ou criminelles ICANN (aussi connue comme « utilisation malveillante du DNS ».

Grâce à leur travail préliminaire avec le GAC et la communauté de l'ICANN, les agences de sécurité publique ont apporté des contributions importantes qui continuent à façonner les délibérations sur les politiques de l'ICANN et les obligations des parties contractantes à ce jour. Cette contribution comprend :

- **La reconnaissance des utilisations légitimes du WHOIS**, énumérées dans les Principes du GAC concernant les services WHOIS des gTLD du Communiqué du GAC de Lisbonne (28 mars 2007). Ces principes sont régulièrement évoqués par le GAC lorsqu'il fournit des commentaires (comme dans les Commentaires récents du GAC sur les recommandations de la révision du RDS-WHOIS2, datant du 23 décembre 2019) ou des avis au Conseil d'administration de l'ICANN (voir les fondements de l'avis contenu dans le Communiqué du GAC de San Juan, 15 mars 2018) ;
- Les r**ecommandations de diligence raisonnable pour l'ICANN**[1] qui ont été approuvées dans le Communiqué du GAC de Bruxelles (25 juin 2010) et ont finalement abouti à des modifications contractuelles dans le Contrat d'accréditation de bureaux d'enregistrement de 2013 (RAA) adopté par le Conseil d'administration de l'ICANN le 27 juin 2013 ; et
- L'i**ntroduction des sauvegardes du GAC pour les nouveaux gTLD** dans le Communiqué du GAC de Beijing (11 avril 2013), qui a abouti à des dispositions spécifiques sur les engagements d'intérêt public dans la spécification 11 du Contrat de registre des nouveaux gTLD

Dans le Communiqué du GAC de Singapour (11 février 2015), le GAC a accepté de créer un groupe de travail sur la sécurité publique et l'application de la loi. Lors de la réunion de l'ICANN à Buenos Aires, le GAC a approuvé le mandat du Groupe de travail sur la sécurité publique (PSWG) dont l'accent était mis sur «*les aspects des politiques et des procédures de l'ICANN qui impliquent la sécurité du public* »

Problématiques

Comme le reflète son plan de travail actuel pour la période 2020-2021 approuvé par le GAC le 16 mars 2020, le PSWG cherche à :

[1]Consultez les Recommandations de diligence raisonnable en matière d'application de la loi (oct. 2009)

- **Développer les capacités de lutte contre l'utilisation malveillante du DNS et d'atténuation de la cybercriminalité** (objectif stratégique n° 1), c'est-à-dire développer les capacités des communautés de l'ICANN et de l'application de la loi pour prévenir et atténuer les abus impliquant le DNS en tant que ressource clé
- **Préserver et améliorer l'efficacité des données d'enregistrement des noms de domaine** (objectif stratégique n° 2), c'est-à-dire assurer l'accessibilité continue et l'amélioration de l'exactitude de l'information des enregistrements de domaines qui soient conformes aux cadres réglementaires applicables en matière de protection de la vie privée

Proposition des dirigeants pour l'action du GAC au cours de l'ICANN69

1. **Considération des développements récents dans la communauté de l'ICANN** liés à la fois à l'atténuation de l'utilisation malveillante du DNS et à l'accès aux données d'enregistrement de gTLD et à leur impact sur les organisations d'application de la loi et de protection des consommateurs des membres.

2. **Examen des prochaines étapes possibles pour traiter les questions de politique publique globales liées à l'utilisation malveillante du DNS**, telles qu'identifiées dans les contributions précédentes du GAC, et **en particulier, considération du suivi** avec le conseil de la GNSO, l'ALAC, la ccNSO et éventuellement le Conseil de l'ICANN sur **les possibilités pour aborder les recommandations de la révision de la CCT sur l'utilisation malveillante du DNS avant le lancement des séries ultérieures de nouveaux gTLD** en conformité avec l'avis du Communiqué du GAC de Montréal (6 novembre 2019).

3. **Discussion sur l'état** d'avancement de l'examen et la mise en œuvre **des recommandations relatives à l'utilisation malveillante du DNS formulées par les révisions de la CCT et RDS-WHOIS2,** à la lumière de l'action du Conseil d'administration de l'ICANN, comme indiqué dans :
    a. La réponse / action du Conseil aux recommandations de la révision de la CCT (1er mars 2019)
    b. La fiche de suivi de l'action du Conseil d'administration suivant les recommandations de la révision RDS-WHOIS2 (25 février 2020)

4. **Examen des progrès des principaux efforts d'atténuation de l'utilisation malveillante du DNS plus généralement, dans la communauté ICANN** et en particulier par les parties contractantes, les opérateurs de ccTLD et l'organisation ICANN, y compris en vue de promouvoir des normes élevées dans les pratiques et les contrats :
    a. **Mise en œuvre de mesures volontaires par les bureaux d'enregistrement et les opérateurs de registre gTLD** conformément au Cadre applicable aux cas d'abus
    b. **Mise en œuvre de mesures proactives de lutte contre l'utilisation malveillante par les opérateurs de ccTLD** qui pourraient Informer les pratiques des opérateurs de registres gTLD

c. **Audit de la conformité contractuelle des bureaux d'enregistrement** concernant les menaces à la sécurité du DNS qui étaient censés suivre la conclusion d'un audit similaire des opérateurs de registre

d. **Améliorations au Signalement des cas d'utilisation malveillante des noms de domaine (DAAR) de l'ICANN,** tel que discuté précédemment par les opérateurs de registre, le GAC et le SSAC

5. **Considération par les membres du GAC d'encourager leurs organismes de sécurité publique pertinents** (organismes d'application de la loi pénale et civile et organismes de protection des consommateurs) à partager leur expérience, leurs défis et leurs réussites dans l'espace du DNS et à se joindre aux travaux du PSWG où leur expérience opérationnelle, leur expertise et leurs préoccupations en matière de politiques sont nécessaires. Le groupe de travail s'appuie sur l'engagement continu de ses parties prenantes et recherche continuellement des bénévoles pour contribuer et jouer un rôle prépondérant pour piloter le travail du PSWG.

Faits importants

Atténuation de l'utilisation malveillante du DNS

Dans sa déclaration sur l'utilisation malveillante du DNS (18 septembre 2019), le GAC a reconnu la définition de l'utilisation malveillante du DNS de l'équipe de révision de la CCT, à savoir, « *les activités intentionnellement trompeuses, complaisantes ou non sollicitées qui utilisent activement le DNS 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 zombis, et le spam lorsqu'ils sont utilisés comme méthode d'exécution de ces formes d'abus* ». Le GAC a reconnu que le Contrat de registre des nouveaux gTLD reflète cette compréhension dans sa spécification 11, en particulier les articles 3a[2] et 3b[3].

Dans ses efforts pour *évaluer en permanence si l'ICANN dispose de mécanismes réactifs et opportuns pour développer et appliquer les obligations contractuelles de l'ICANN avec les opérateurs de registre et les bureaux d'enregistrement gTLD*[4], le PSWG s'est concentré sur les activités suivantes liées à l'atténuation de l'utilisation malveillante du DNS :

- **Au cours des réunions récentes de l'ICANN**, les dirigeants du PSWG ont fourni des rapports informatifs détaillés au GAC sur l'utilisation malveillante du DNS (voir les documents de la réunion ICANN66 et de la réunion ICANN68). Le GAC a examiné les mesures mises à la disposition des opérateurs de registre et des bureaux d'enregistrement pour prévenir l'utilisation malveillante du DNS, en particulier le rôle des politiques d'enregistrement (y compris la vérification d'identité) et des stratégies de tarification comme déterminants clés des niveaux d'abus dans un TLD donné. Le GAC a également examiné les initiatives en cours ou possibles pour aborder l'utilisation malveillante du DNS plus efficacement au niveau du Conseil d'administration et de l'organisation ICANN (pour de plus amples informations, consultez les procès-verbaux de l'ICANN66, le communiqué du GAC de l'ICANN68 et les procès-verbaux de l'ICANN66). Le plan de travail du PSWG comprend tous ces domaines dans le cadre de l'objectif stratégique nº 2 visant à développer les capacités de lutte contre l'utilisation malveillante du DNS et l'atténuation de la cybercriminalité. Le présent document d'information comprend des mises à jour dans plusieurs de ces domaines.

---

[2] La spécification 11 3a établit que *« Les opérateurs de registre incluront dans leurs contrats entre opérateurs de registre et bureaux d'enregistrement (RRA) une disposition en vertu de laquelle 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 »*.

[3] La spécification 11 3b établit que « *L'opérateur de registre procèdera périodiquement à une analyse technique afin d'évaluer si les domaines de son TLD sont utilisés pour perpétrer des menaces à la sécurité comme le dévoiement, l'hameçonnage, les logiciels malveillants et les réseaux zombies. L'opérateur de registre devra entretenir des rapports statistiques sur le nombre des menaces à la sécurité identifiées et les mesures prises suite aux vérifications périodiques en matière de sécurité. 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. »*

[4] Consultez les objectifs du PSWG définis dans ses Termes de référence

- **Recommandations de la révision de la concurrence, la confiance et le choix du consommateur**
    - À la lumière de l'avis contenu dans le Communiqué du GAC de Montréal (6 novembre 2019) à l'intention du Conseil d'administration de l'ICANN de *« ne pas procéder à une nouvelle série de gTLD avant la mise en œuvre complète des recommandations [...] identifiées comme « conditions préalables » ou « à priorité élevée »*, et de la réponse du Conseil à cet avis (26 janvier 2020), le PSWG continue de surveiller l'examen des principales recommandations de la CCT-RT (6 septembre 2018) visant à l'adoption de dispositions contractuelles pour encourager des mesures anti-abus proactives (rec. 14) et à la prévention de l'utilisation systémique des opérateurs de registre et des bureaux d'enregistrement pour utiliser le DNS à des fins malveillantes (rec. 15) ; à l'amélioration de la recherche sur l'utilisation malveillante de DNS (rec. 16) ; à l'amélioration de l'exactitude du WHOIS (rec. 18) ; et à l'efficacité du traitement des plaintes en matière de conformité contractuelle (rec. 20).
    - Le PSWG analyse également la résolution du Conseil d'administration de procéder au plan de mise en œuvre de l'ICANN (23 août 2019) pour les recommandations de la CCT qui ont été acceptées dans la fiche de suivi de l'action du Conseil d'administration de l'ICANN (1er mars 2019). Le GAC a commenté (21 octobre 2019) ce plan et a fait remarquer certaines lacunes concernant des recommandations importantes pour lutter contre l'utilisation malveillante du DNS, y compris la publication de la 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 (voir plus sur ce sujet ci-dessous), **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 les dispositions contractuelles fournissant des incitations financières aux parties contractantes pour qu'elles adoptent des mesures proactives de lutte contre l'utilisation malveillante »*), le **GAC a demandé au Conseil d'administration de l'ICANN des clarifications** quant au statut et au plan concernant la facilitation des efforts communautaires pour élaborer une définition de « utilisation malveillante » et pour informer le Conseil d'administration de la suite à donner à cette recommandation. Le GAC a enregistré dans ses procès-verbaux de l'ICANN68 que « *le Conseil continuera de soutenir le dialogue communautaire comme il l'a fait en facilitant les discussions régionales et intercommunautaires, en menant des recherches et en développant des outils pour aider à informer les discussions communautaires, et en fournissant des orateurs sur demande* ».
    - Au cours de la réunion ICANN68, le PSWG et les parties prenantes de l'ALAC ont constaté que les progrès sur la mise en œuvre de la recommandation acceptée de la CCT-RT et sur l'examen de la recommandation en attente ne sont pas clairs. De l'insatisfaction a également été exprimée lors d'une communication récente (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 disant qu'il « *ne prévoit pas de formuler de recommandations en ce qui concerne l'atténuation de l'utilisation malveillante des noms de domaine autre qu'en déclarant tout effort futur devra s'appliquer à la fois aux gTLD existants et aux nouveaux (et potentiellement aux ccTLD) ».* Cela s'oppose aux recommandations pertinentes qui lui sont adressées par l'équipe de révision de la CCT, soutenue par l'action du Conseil d'administration de l'ICANN vis-à-vis de ces recommandations, ainsi qu'à l'avis du Communiqué du GAC de Montréal (6 novembre 2019) et aux commentaires supplémentaires du GAC tels que consignés dans le Communiqué du GAC de l'ICANN67 (16 mars 2020).

- **Discussion sur la possible élaboration d'une politique de la GNSO relative à l'atténuation de l'utilisation malveillante du DNS**
    - Suivant la décision du groupe de travail consacré au PDP relatif aux procédures pour des séries ultérieures de nouveaux gTLD de ne pas formuler de recommandation dans le domaine de l'utilisation malveillante du DNS pour les futurs contrats de nouveaux gTLD, le **conseil de la GNSO a discuté,** lors de sa réunion du 21 mars 2020, de la possibilité de créer **un groupe de travail intercommunautaire (CCWG)** consacré à la question de l'utilisation malveillante du DNS et éventuellement d'un PDP de la GNSO relatif aux procédures pour des séries ultérieures de nouveaux gTLD s'il était nécessaire d'imposer de nouvelles exigences contractuelles**.** Il n'a pas discuté d'une proposition informelle de l'équipe de direction du GAC (12 mai 2020) d'envisager une séance d'intérêt commun conviant à la discussion les experts concernés, y compris les opérateurs de ccTLD, pour définir un éventuel effort de politique futur.
    - En date du 24 septembre 2020, cette question est identifiée comme « non planifiée » dans l'inventaire des décisions et des mesures à prendre du conseil de la GNSO.

- **Adoption de mesures visant à atténuer l'utilisation malveillante du DNS par les opérateurs de registre et les bureaux d'enregistrement**
    - 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 applicable aux cas d'abus (17 octobre 2019). Notamment, ce cadre inclut dans le champ d'action possible de ses adoptants certaines formes d'« abus de contenu de sites Web » qu'il considère « si flagrantes que la partie contractante devrait agir suivant la réception d'un avis spécifique et crédible ». Depuis sa publication et sa discussion au cours de l'ICANN66, la liste des signataires de ce cadre s'est élargie pour inclure d'autres fournisseurs de services de registre et de bureaux d'enregistrement de gTLD de première ligne, ainsi qu'un certain nombre de petits acteurs de l'industrie.
    - Le 18 juin 2020, les présidents du **groupe des représentants des bureaux d'enregistrement et le groupe des représentants des opérateurs de registre** (collectivement appelés la Chambre des parties contractantes de la GNSO, ou CPH) ont annoncé aux dirigeants de la communauté qu'ils **ont adopté une définition de l'utilisation malveillante du DNS** qui reprend exactement celle du Cadre applicable aux cas d'abus rédigée suivant les pratiques de l'industrie :

        > *L'utilisation malveillante du DNS se compose de cinq grandes catégories d'activités nuisibles dans la mesure où elles intersectent avec le DNS : logiciels malveillants, réseaux zombies, hameçonnage, dévoiement et spam lorsqu'il sert de mécanisme de diffusion pour les 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 définir chacune de ces activités].

        Cette définition **semble confirmer ce que l'équipe de révision de la 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 de la CCT, p. 8) et se conforme à la **définition illustrative des « menaces de sécurité » du GAC** dans les « contrôles de sécurité », l'avis du GAC relatif aux sauvegardes applicable à tous les nouveaux gTLD du Communiqué de Beijing (11 avril 2013) incorporé dans le contrat de registre de gTLD conformément à la Spécification 11 3b.
    - Le 3 janvier 2020, l'organisation ICANN a annoncé une proposition de modification au contrat de registre .COM qui étendrait **les dispositions relatives à l'espace de noms gTLD pour faciliter la détection et le rapport de l'utilisation malveillante du DNS aux 2/3 de l'espace de noms des gTLD** (y compris la spécification 11 3b) qui, jusqu'à présent, n'était applicable qu'aux nouveaux gTLD. En outre, une lettre d'intention contraignante entre l'organisation ICANN et Verisign établit un cadre de coopération pour développer les meilleures pratiques et les nouvelles obligations contractuelles potentielles, ainsi que des mesures visant à mesurer et à atténuer les menaces à la sécurité du DNS.
    - **Dans le contexte de la crise du COVID-19, les parties contractantes ont présenté leurs actions et leçons apprises** avant et pendant la réunion 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 pour signaler les domaines/contenus liés au COVID-19, ainsi que de l'établissement d'un point de contact unique pour les autorités compétentes. Ces efforts renforcent les relations de travail établies entre les organismes d'application de la loi et les bureaux d'enregistrement, et reprennent 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.

- **Réponse multidimensionnelle de l'organisation ICANN à l'utilisation malveillante et à la conformité contractuelle**
    - Le PDG de l'ICANN a publié un 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 l'expertise de l'ICANN en matière de sécurité du DNS au profit de la communauté. L'organisation participe à divers forums de renseignements sur les cybermenaces et de réponse aux incidents, notamment le Forum des équipes de sécurité et de réponse aux incidents (FIRST), le Groupe de travail anti-abus pour la messagerie, les programmes malveillants et les mobiles (M3AAWG), le Groupe de travail anti-hameçonnage (APWG), l'Alliance nationale d'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 l'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 pertinentes. Le GAC a été informé de cette question avant l'ICANN68 (12 juin 2020), et l'ensemble de la communauté de l'ICANN, lors de la réunion ICANN68.
        - Grâce à sa **plateforme de signalement des cas d'utilisation malveillante des noms de domaine (DAAR)**, l'ICANN a informé mensuellement depuis janvier 2018 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 de DAAR, en particulier une lettre du M3AAWG à l'organisation ICANN (5 avril 2019) et le rapport préliminaire de l'équipe de révision tSSR2 (24 janvier 2020), que le GAC a soutenu (voir ci-dessous). Le Groupe des représentants des opérateurs de registre, qui avait également exprimé ses préoccupations vis-à-vis du

DAAR et qui travaillait avec l'ICANN à 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 lancé (6 mai 2020) dans le cadre de la mise en œuvre du Plan stratégique pour les exercices fiscaux 2021 à 2025, dans le but d'*« explorer des idées concernant ce que l'ICANN peut et doit faire pour augmenter le niveau de collaboration et d'engagement avec les parties prenantes de l'écosystème DNS afin d'améliorer le profil de sécurité du DNS »*. Il est prévu que des recommandations soient formulées avant mai 2021.
- **Application de la conformité contractuelle** : dans son blog (20 avril 2020), le PDG de l'ICANN a rappelé : « *le service conformité de l'ICANN veille au respect des obligations établies dans les politiques et les contrats de l'ICANN, en particulier le contrat de registre (RA) et le contrat d'accréditation des bureaux d'enregistrement (RAA). Ce service travaille également étroitement avec l'OCTO à identifier des menaces à la sécurité du DNS [...] et à les relier aux parties contractantes concernées. Le service conformité de l'ICANN se sert des données collectées pendant les audits [...] pour évaluer si les opérateurs de registres et les bureaux d'enregistrement se conforment à leurs obligations en matière d'atténuation de risques liés à la sécurité du DNS. En dehors de ces audits, le service conformité utilisera les données collectées par OCTO et d'autres pour contacter de manière proactive des opérateurs de registres et des bureaux d'enregistrement qui affichent un nombre disproportionné de menaces à la sécurité du DNS. En cas d'échec du dialogue constructif, le service conformité de l'ICANN n'hésitera pas à faire exécuter les contrats de tous ceux qui refuseraient de se conformer à leurs obligations en matière de menaces à la sécurité du DNS ».* Le blog a également fourni un aperçu du volumes de plaintes, des ressources allouées à leur traitement et des statistiques sur la résolution de ces plaintes.
  - Depuis la réunion ICANN66, plusieurs séances ont été consacrées à **la discussion communautaire sur l'efficacité de l'application ainsi que sur l'applicabilité des dispositions contractuelles actuelles** relatives à l'utilisation malveillante du DNS, notamment :
    - Séance intercommunautaire sur l'utilisation malveillante du DNS à l'ICANN66 (6 novembre 2020)
    - Séance d'At-Large sur la conformité contractuelle à l'ICANN67 (9 mars 2020)
    - Séance de l'ALAC sur les engagements d'intérêt public et la procédure de résolution de litiges y associée à l'ICANN68 (22 juin 2020)
  - Les dirigeants du PSWG suivent **la correspondance échangée sur** les questions de l'application et l'applicabilité entre **le Conseil d'administration**

de l'ICANN et les unités constitutives des représentants de la propriété intellectuelle et des parties prenantes commerciales de la GNSO :

- Déclaration de la BC concernant la discussion communautaire sur l'utilisation malveillante du DNS (28 octobre 2019)
- Lettre de la BC au Conseil d'administration de l'ICANN (9 décembre 2019)
- Réponse du président du Conseil d'administration de l'ICANN au président de la BC (12 février 2020)
- Lettre de l'IPC au Conseil d'administration de l'ICANN (24 avril 2020)
- Réponse du président du Conseil d'administration de l'ICANN au président de l'IPC prenant note des questions et signalant une réunion après l'ICANN68 (10 juin 2020)

- Il est prévu que **l'équipe de travail sur l'utilisation malveillante du DNS du Comité consultatif sur la sécurité et la stabilité (SSAC)** fasse rapport de ses activités et constats.
  - Au cours de la réunion ICANN66, le SSAC a informé le PSWG de sa création d'une équipe de travail consacrée à l'utilisation malveillante du DNS, à laquelle **a participé un représentant du PSWG**.
  - Depuis lors, le SSAC a signalé son intention de ne pas formuler une définition d'utilisation malveillante du DNS. Au lieu de cela, l'équipe de travail devrait se concentrer sur les rôles des parties appropriées, étayant son travail sur les perspectives communautaires et les cadres existants. L'objectif du groupe de travail est de produire un rapport qui décrive les efforts potentiels pour normaliser les stratégies et les processus communautaires autour de l'identification et l'atténuation de l'utilisation malveillante.

- **Recommandations en matière de sécurité, de stabilité et de résilience**
  - 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) a appuyé bon nombre des recommandations, en particulier celles concernant l'amélioration du système de Signalement des cas d'utilisation malveillante des noms de domaine (DAAR) et le renforcement des mécanismes de conformité. Les recommandations finales de l'équipe de révision SSR2 sont prévues pour octobre 2020 (selon un blog du 1er juin 2020). Un séminaire en ligne de préparation à l'ICANN69 présentant un rapport des progrès est prévu pour le 7 octobre 2020 à 15h00 UTC.
  - Un certain nombre de recommandations relatives à l'utilisation malveillante du DNS relèvent du plan de travail du PSWG et sont conformes aux recommandations de la CCT-RT ainsi qu'aux commentaires précédents du GAC concernant la définition de l'utilisation malveillante du DNS, les limites du système de signalement des cas d'utilisation malveillante des noms de domaine (DAAR), les nouvelles dispositions

contractuelles et l'efficacité de l'application de la conformité contractuelle. Plusieurs recommandations font état de nouvelles pistes de travail également identifiées dans le Plan de travail 2020- 2021 du PSWG, comme l'inclusion des ccTLD parmi efforts d'atténuation de l'utilisation malveillante du DNS et l'étude des implications des technologies de chiffrement du DNS sur la sécurité (DNS sur HTTPS ou DoH).

- **Deux questions de politique actuelles particulières** revêtent un intérêt pour le PSWG en ce qui concerne l'atténuation de l'utilisation malveillante du DNS : **Accréditation des services d'anonymisation et d'enregistrement fiduciaire** et **exactitude des données d'enregistrement de gTLD**
    - Le PSWG continue de chercher à mettre en œuvre **l'accréditation des fournisseurs de services d'anonymisation et d'enregistrement fiduciaire** avec un cadre de divulgation approprié pour l'application de la loi, conformément aux recommandations de politique de la GNSO de 2013. Au cours de l'ICANN68, des représentants du secteur de l'application de la loi ont signalé au GAC qu'ils avaient eu du mal à identifier des responsables d'abus liés au COVID-19 dans 65 % des cas en raison de la non-divulgation des données d'enregistrement protégées par un service d'anonymisation ou d'enregistrement fiduciaire. Dans les commentaires du GAC au sujet du rapport final de l'équipe de révision RDS-WHOIS2 (23 décembre 2019), le GAC a rappelé que la corrélation entre l'utilisation du service d'anonymisation ou d'enregistrement fiduciaire et l'utilisation malveillante du DNS a été démontrée, et a rappelé ses avis du Communiqué de Kobe et du Communiqué de Montréal au Conseil d'administration de l'ICANN d'envisager de reprendre cette mise en œuvre. Plus récemment, le Conseil d'administration de l'ICANN a répondu (25 février 2020) à une lettre de la Coalition pour la responsabilité en ligne (31 octobre 2019) faisant référence à une révision par l'ICANN de l'impact des recommandations de politique de l'EPDP au sujet de la recommandation de politique PPSAI et les travaux de mise en œuvre achevés à ce jour.
    - **L'exactitude des données d'enregistrement des gTLD** est un domaine de politique qui a un impact élevé sur l'atténuation de l'utilisation malveillante du DNS que poursuit le PSWG. Dans ses commentaires sur le rapport final de l'équipe de révision RDS-WHOIS2 (23 décembre 2019), le GAC a rappelé ses préoccupations concernant ce problème systémique qui affecte négativement la sécurité et la stabilité du DNS, a noté que, à son avis, l'exactitude des données d'enregistrement n'est pas exclusivement une responsabilité des titulaires de noms de domaine, et a conclu que l'application des obligations contractuelles des bureaux d'enregistrement par l'ICANN est critique et nécessite un contrôle proactif des données d'enregistrement à grande échelle. Cette question est actuellement examinée dans le contexte du travail actuel et futur de l'élaboration de politiques de la GNSO, examinée dans la prochaine section du présent document, et aussi lors de la réunion d'information du GAC au sujet du WHOIS et de la protection des données à l'ICANN69.

Le WHOIS : accessibilité et exactitude des données d'enregistrement de noms de domaine

Les efforts déployés par l'ICANN pour mettre le WHOIS en conformité avec le Règlement général sur la protection des données (RGPD) de l'Union européenne ont créé des obstacles pour les organismes d'application de la loi et de protection aux consommateurs pour accéder aux données WHOIS, qui est un outil d'investigation indispensable pour l'application de la loi. Ces obstacles aux investigations[5] ont aggravé les défis existants en raison de l'environnement permanent et croissant des menaces à la sécurité et ont une incidence négative sur la capacité des forces de l'ordre de mener des enquêtes, d'aviser les victimes en temps voulu et de perturber les activités criminelles en cours. Ceci a été reconnu dans le Communiqué du GAC de Barcelone (25 octobre 2018) et dans une lettre du GAC adressée au Conseil d'administration de l'ICANN (24 avril 2019) avant son adoption des recommandations de l'étape 1 du processus accéléré d'élaboration de politiques (EPDP) sur les données d'enregistrement des gTLD.

Cette partie du présent document d'information fournit une mise à jour sur les activités du PSWG dans le but d'assurer l'accessibilité continue et l'amélioration de l'exactitude de l'information sur l'enregistrement de domaines, conformément aux cadres réglementaires applicables en matière de protection de la vie privée et aux positions consensuelles du GAC, et à l'appui *de la capacité des organismes de sécurité publique d'enquêter, prévenir, attribuer, et interrompre les activités illégales, les abus, la fraude aux consommateurs, la tromperie ou la malversation, et/ou les violations des lois nationales*[6].

Depuis l'ICANN66, les représentants du PSWG ont participé à divers aspects des travaux de l'EPDP, à l'appui du petit groupe du GAC et de ses représentants au sein de l'équipe de l'EPDP, ainsi qu'à divers autres processus de l'ICANN présentant une pertinence continue :

- **Obligation pour les parties contractantes de fournir un accès raisonnable** aux données d'enregistrement non publiques des gTLD : le PSWG examine la réponse du Conseil d'administration de l'ICANN (26 janvier 2020) à l'avis contenu dans le Communiqué du GAC de Montréal (6 novembre 2019) et les clarifications subséquentes (20 janvier 2020) fournies par le GAC qui visaient à garantir que pendant que de nouvelles politiques sont élaborées, les mécanismes provisoires seront efficaces et leurs lacunes seront traitées. Comme prévu dans la réponse du Conseil d'administration à l'avis du GAC, le service de conformité contractuelle de l'ICANN a déployé de nouveaux formulaires de plainte et rapporte désormais des données[7] pour des violations présumées de la spécification temporaire sur les données d'enregistrement des gTLD depuis le 1er février 2020.
- **Mise en œuvre des recommandations de l'étape 1 de l'EPDP** : bien que l'étape 2 de l'EPDP ait récemment pris fin et que les prochaines étapes restent actuellement au centre de l'attention

[5] Consultez l'enquête menée auprès des organismes chargés de l'application de la loi par l'équipe de révision RDS-WHOIS2 à la section 5.2.1 de son rapport final (2 septembre 2019)

[6] Suivant les objectifs définis dans les Termes de référence du PSWG

[7] Voir le tableau de bord du service de conformité contractuelle de l'ICANN pour août 2020 sous les en-têtes « Plaintes [des opérateurs de registre / bureaux d'enregistrement] incorporant des preuves d'une violation présumée de la spécification temporaire - 1er février 2020 à ce jour » et « demandes/avis [des opérateurs de registre / bureaux d'enregistrement] concernant les spécifications temporaires envoyées et conclues en août 2020 »

de la communauté de l'ICANN[8], le PSWG suit et contribue également à la mise en œuvre des recommandations de politique de l'étape 1 de l'EPDP. En particulier, à la lumière des avis précédents du GAC, plus récemment dans le Communiqué du GAC de Montréal, les représentants du PSWG visent à s'assurer que la mise en œuvre soit faite en temps opportun et en conformité avec les recommandations de politique.

- **Système normalisé d'accès et de divulgation (SSAD) aux données d'enregistrement de gTLD non publiques** proposé dans le rapport final de l'étape 2 de l'EPDP (7 février 2020)
    - Les participants au PSWG ont apporté leur expérience et leur expertise en matière de cas concrets pour informer les positions et les contributions des représentants du GAC au sein de l'équipe de l'EPDP, en particulier en ce qui concerne les Principes d'accréditation du GAC (21 janvier 2020), l'automatisation des réponses aux demandes des organismes d'application de la loi de chaque juridiction et les conventions de service applicables aux réponses à une demande urgente et plus récemment à la déclaration minoritaire du GAC sur le rapport final de l'étape 2 de l'EPDP (24 août 2020).
    - Le PSWG continue de suivre les progrès des discussions au sein du conseil de la GNSO concernant les questions dites de « priorité 2 » n'ayant pas été abordées à l'étape 2 de l'EPDP, qui comprennent des domaines de politique ayant des répercussions directes sur l'utilisation malveillante du DNS, tels que l'exactitude de l'information du WHOIS et l'accréditation des fournisseurs de services d'anonymisation et d'enregistrement fiduciaire.

- **Recommandations de l'équipe de révision RDS-WHOIS2** : selon le rapport de l'ICANN (6 février 2020) sur la période de consultation publique à propos des recommandations finales de cette révision prévue dans les statuts constitutifs qui comprenait une contribution du GAC (23 décembre 2019), le Conseil d'administration de l'ICANN a adopté un ensemble de décisions du Conseil (25 février 2020).
  Le GAC a souligné l'importance de plusieurs objectifs et activités prévus par l'équipe de révision RDS-WHOIS2 (dans laquelle plusieurs participants du PSWG représentaient le GAC) :
    - L'établissement d'une fonction de prévision stratégique pour les développements réglementaires et législatifs affectant l'ICANN afin de promouvoir un nouvel objectif stratégique adopté par l'ICANN dans son plan stratégique 2021- 2025. Cette recommandation a été acceptée par le Conseil d'administration
    - L'application proactive de la conformité et le rapport sur l'exactitude des données WHOIS, qui d'après le GAC devraient continuer à la même échelle et malgré les obstacles actuels, compte tenu de l'importance des exigences d'exactitude pour prévenir et atténuer l'utilisation malveillante du DNS, et l'étendue de la nature des inexactitudes estimées. Cette recommandation est mise en attente est reste à examiner par le Conseil d'administration de l'ICANN à la fin de l'étape 2 de l'EPDP

[8] Consultez le document d'information du GAC sur le WHOIS et la politique de protection des données

- L'accréditation des services d'anonymisation et d'enregistrement fiduciaire et la validation des données d'enregistrement qui les utilisent, qui a fait l'objet d'un suivi de l'avis du Communiqué du GAC de Montréal (6 novembre 2019), en réponse auquel (26 janvier 2020) le Conseil d'administration de l'ICANN a fait état d'une analyse d'impact menée par l'organisation ICANN dans le cadre de la mise en œuvre de l'étape 1 de l'EPDP. Cette recommandation a également été mise en attente et reste à examiner par le Conseil d'administration de l'ICANN à la fin de l'étape 2 de l'EPDP

Positions actuelles

- Déclaration minoritaire du GAC sur le rapport final de l'étape 2 de l'EPDP (24 août 2020)
- Commentaires du GAC sur le rapport final de la révision des recommandations de la RDS-WHOIS2 (23 décembre 2019)
- Communiqué du GAC de Montréal (6 novembre 2019)
- Déclaration du GAC sur l'utilisation malveillante du DNS (18 septembre 2019)

Principaux documents de référence

- Plan de travail 2020- 2021 du PSWG (16 mars 2020)
- Document d'information du GAC sur l'utilisation malveillante du DNS (30 octobre 2019)

Informations complémentaires

- Document d'information sur l'utilisation malveillante du DNS de l'ICANN68 (18 juin 2020)
- Document d'information du GAC sur le WHOIS et la politique de protection des données (24 septembre 2020)

Gestion des documents

Réunion	Réunion générale annuelle virtuelle ICANN69, du 13 au 22 octobre 2020
Titre	Mise à jour du PSWG
Distribution	Membres du GAC (avant la réunion) et du public (après la réunion)
Date de distribution	Version 1 : 24 septembre 2020