Concurrence, confiance et choix du consommateur (CCT) : nouveaux articles

Nouveaux articles ajoutés au précédent rapport préliminaire

Équipe de révision sur la concurrence, la confiance et le choix du consommateur (CCT)
27 novembre 2017

ICANN

TABLE DES MATIÈRES

Résumé analytique

Le 7 mars 2017, l'équipe de révision chargée de la concurrence, la confiance et le choix du consommateur a publié son rapport préliminaire pour commentaire public. 24 commentaires ont été reçus. L'équipe est en train de les examiner et tente, selon les cas, de les intégrer à la version préliminaire finale. En même temps que la période de consultation publique, trois mesures analytiques supplémentaires avaient lieu : une discussion sur le 'parking', une enquête des membres de l'INTA sur le coût du programme des nouveaux gTLD pour les propriétaires de marques, et une étude sur l'utilisation malveillante du DNS dans les nouveaux gTLD. Chacune de ces analyses a conduit à des mises à jour de la version préliminaire initiale du rapport CCT sur lequel le public n'a pas encore eu la possibilité de s'exprimer. En conséquence, la décision prise a été de publier un ajout au rapport préliminaire pour offrir cette possibilité.

Étant donné la pléthore de commentaires déjà reçus pendant la période de consultation publique initiale, l'équipe de révision demande des commentaires uniquement sur les modifications apportées par les nouvelles analyses autour de la question du parking, de la gestion des marques et de l'utilisation malveillante du DNS. Comme mentionné ci-dessus, l'équipe de révision travaille simultanément sur la gestion des commentaires publics initiaux et l'intégration de ces commentaires dans le rapport final devant être publié début janvier 2018. Pour plus de facilité, nous vous demandons d'inclure la référence à la (aux) recommandation(s) à laquelle (auxquelles) votre (vos) commentaire(s) fait (font) référence.

Pour finir, l'équipe de révision voudrait attirer votre attention sur la recommandation 4 qui fait référence à l'utilisation malveillante du DNS. Cette recommandation pour une politique de règlement de litiges relatifs à l'utilisation malveillante du DNS (DADRP) est la première recommandation de la CCTRT à n'avoir pas obtenu le soutien unanime de l'équipe de révision. Une minorité significative de l'équipe s'est associée pour une « déclaration de la minorité » concernant cette recommandation. La CCTRT a été interrogée et la majorité soutient la recommandation telle qu'elle est formulée avec un débat supplémentaire nécessaire. Cette recommandation sera ou non dans le rapport final mais l'équipe de révision a conclu qu'elle valait la peine d'être soumise à commentaire public. Merci d'accorder une attention particulière à cette proposition et à la raison pour laquelle elle est proposée au moment du dépôt des commentaires publics pour que l'équipe de révision puisse mieux évaluer l'opinion de la communauté concernant cette mesure. Il est inquiétant de voir que les taux d'utilisations malveillantes du DNS sont élevés dans certains TLD et la conformité contractuelle semble incapable ou peu désireuse d'aborder le problème de manière globale et une DADARP pourrait être une solution, bien qu'elle soulève un certain nombre d'inquiétudes.

1.1 Parking

Au vue du pourcentage élevé d'enregistrements 'en parking' dans les nouveaux gTLD, même par rapport au pourcentage élevé d'enregistrements en parking dans les anciens gTLD, l'équipe de révision cherche à savoir si le phénomène pourrait avoir un impact sur ses conclusions concernant l'incidence du programme des nouveaux gTLD sur la concurrence. Bien que diverses hypothèses relatives à l'impact éventuel des enregistrements en parking aient été avancées, aucune preuve concluante n'a été présentée qui soutienne ces hypothèses à court terme. Bien que l'équipe de révision n'ait pas trouvé de preuve concluante des effets des enregistrements en parking sur la concurrence, nous avons trouvé des différences entre les régions concernant cette question. En effet, il semble y avoir plus de domaines en parking dans les domaines en langue chinoise pour lesquels il y aurait plus de spéculation.

Il peut y avoir une certaine corrélation entre les taux de parking et les programmes malveillants mais elle n'est pas aussi forte et révélatrice que la tendance mondiale visant à des taux de distribution plus bas que ceux des anciens gTLD. Néanmoins, l'écart dans le taux de distribution de programmes malveillants entre les anciens et les nouveaux gTLD semble se réduire et il convient à la communauté de mieux examiner la corrélation entre les taux de parking et la distribution de programmes malveillants.

Le bilan global des observations de l'équipe de révision sur la question du parking n'est pas concluant et requière davantage de recherches ne se limitant pas à l'impact des nouveaux gTLD. Pour cela l'équipe de révision recommande une collecte des données plus rigoureuse autour de divers types de parking afin de faciliter un examen plus approfondi par la communauté de l'impact des domaines en parking sur la concurrence, la confiance du consommateur, l'utilisation malveillante du DNS et ses services d'anonymisation.

1.2 Coût pour les propriétaires de marques

L'association internationale des marques de commerce (INTA) a mené une étude auprès de ses membres pour commencer à examiner l'expérience des propriétaires de marques déposées. L'équipe de révision a examiné l'enquête et l'a complétée avec sa propre analyse. Malgré le nombre assez faible de participants, l'enquête de l'INTA offre des conclusions intéressantes concernant les propriétaires de marques. L'enquête a conclu que « les enregistrements de nouveaux TLD reproduisent principalement les enregistrements des TLD ou ccTLD historiques », et qu'en particulier, seulement 17 % des personnes ayant répondu ont enregistré pour la première fois des noms dans les nouveaux gTLD par rapport à l'enregistrement en double de domaines existants dans les gTLD ou ccTLD historiques. Cela montre que l'enregistrement défensif reste un problème dans le programme des nouveaux gTLD. Alors que l'un des objectifs énoncés du programme des nouveaux gTLD était d'offrir un meilleur choix pour les propriétaires de marques, la raison principale pour justifier d'enregistrements de domaines par marque est l'aspect 'défensif'.

Cependant, l'enquête montre également que l'expansion du programme des nouveaux gTLD a rendu moins efficace l'enregistrement défensif comme moyen de protection. En conséquence, les fonds ont été déplacés vers des solutions alternatives et une surveillance étendue.

En outre, l'enquête révèle que plus de 75 % des cas impliquent les services d'anonymisation et d'enregistrement fiduciaire, ce qui montre qu'il est nécessaire de poursuivre les recherches.

Pour finir, on constate que les coûts liés à l'application ont augmenté au sein des nouveaux domaines, ce qui montre des cas d'atteintes plus importants dans ces nouveaux domaines que dans les gTLD et ccTLD historiques.

L'enquête de l'INTA montre qu'une recherche approfondie est dans tous les cas nécessaire, peut-être avec une enquête simplifiée et avec plus de personnes interrogées. Mais il est évident que les propriétaires de marques ont connu quelques frustrations avec le programme des nouveaux gTLD et les mécanismes de protection des droits qui ont été mis en place.

1.3 Utilisation malveillante du DNS

Dans la mesure du possible, la CCT-RT a cherché à évaluer la capacité des sauvegardes techniques développées pour le programme des nouveaux gTLD à réduire les diverses formes d'utilisations malveillantes du DNS. Dans le cadre de ce processus, la CCTRT a demandé que soit menée une étude complète sur l'utilisation malveillante du DNS afin

d'analyser les niveaux de malveillance au sein des nouveaux et des anciens gTLD, d'alimenter cette révision et d'éventuellement servir de base pour de futures analyses.

De manière générale, l'étude sur l'utilisation malveillante du DNS montre que l'introduction des nouveaux gTLD n'a pas augmenté le nombre total d'utilisations malveillantes pour l'ensemble des gTLD. Néanmoins, les résultats montrent que les neuf sauvegardes susmentionnées seules ne garantissent pas un taux inférieur d'utilisations malveillantes dans chaque nouveau gTLD par rapport aux anciens gTLD. Au contraire, des facteurs comme les restrictions d'enregistrement, le prix et les pratiques spécifiques aux bureaux d'enregistrement semblent plus susceptibles d'avoir un impact sur le taux d'utilisations malveillantes.

Les résultats de l'étude montrent que l'introduction des nouveaux gTLD correspondait avec une baisse du nombre de spams associés à des enregistrements auprès d'anciens gTLD, alors que les enregistrements malveillants ont augmenté auprès de nouveaux gTLD.

La conclusion du rapport et de l'équipe de révision est donc que ces sauvegardes existantes ne sont pas une protection suffisante contre l'utilisation malveillante du DNS et que des solutions innovantes doivent être envisagées. Nous attendons les commentaires publics à propos des solutions soumises.

2 Recommandations de l'équipe de révision CCT

Les recommandations sont résumées dans ce tableau. La recommandation complète, avec les conclusions et fondements connexes, est disponible dans les chapitres cités.

- **Condition préalable ou niveau de priorité** : Conformément aux statuts constitutifs de l'ICANN, l'équipe de révision CCT a indiqué si chacune des recommandations doit être mise en place avant le lancement des prochaines procédures pour les nouveaux gTLD. L'équipe de révision s'est mise d'accord sur le fait que ces recommandations qui n'étaient pas considérées comme des conditions préalables auraient un niveau de priorité délimité dans le temps :
- **Priorité élevée** : doivent être mises en œuvre dans les 18 mois suivants l'émission du rapport final
- **Priorité moyenne**: doivent être mises en œuvre dans les 36 mois suivants l'émission du rapport final
- **Priorité basse** : Doivent être mises en œuvre avant le début de la prochaine révision CCT

Numéro	Recommandation	à	Condition préalable ou niveau de priorité
Chapitre 3. Concurrence			
3	Recueillir des données relatives au parking.	organisation de l'ICANN	élevée.
Chapitre 4. Choix du consommateur			
9	Réaliser des enquêtes périodiques sur les titulaires de noms de domaine.	organisation de l'ICANN	condition préalable
Chapitre 5. Sauvegardes			
A	Prendre en considération les dirigeants de l'organisation de l'ICANN, dans leurs discussions avec les registres pour négocier des amendements aux contrats de registre existants, ou dans les négociations des nouveaux contrats de registre liés aux futures séries de nouveaux gTLD, afin d'inclure des dispositions visant à apporter des incitations, y compris des incitations financières aux registres et en particulier aux registres ouverts, afin d'adopter des mesures anti-malveillance proactives.	Le Conseil d'administration de l'ICANN, le groupe des représentants des opérateurs de registre, le groupe des représentants des bureaux d'enregistrement, l'organisation de soutien aux extensions génériques et le groupe de travail PDP consacré aux procédures futures.	élevée
B	Prendre en considération les dirigeants de l'organisation de l'ICANN, dans leurs discussions avec les bureaux d'enregistrement et les registres pour négocier des amendements aux contrats d'accréditation de	Le Conseil d'administration de l'ICANN, le groupe des représentants des opérateurs de	élevée

	bureau d'enregistrement et aux contrats de registre afin qu'ils intègrent des dispositions visant à empêcher une utilisation systémique de bureaux d'enregistrement spécifiques pour l'utilisation malveillante technique du DNS.	registre, le groupe des représentants des bureaux d'enregistrement, l'organisation de soutien aux extensions génériques et le groupe de travail PDP consacré aux procédures futures.	
C	Une étude plus approfondie a été menée sur la relation entre des opérateurs de registre, des bureaux d'enregistrement spécifiques et l'utilisation malveillante du DNS en demandant une collecte continue de données, y compris mais sans s'y limiter, des initiatives de signalement des cas d'utilisations malveillantes des noms de domaine (DAAR). À des fins de transparence, ces informations devraient être régulièrement publiées de façon à pouvoir identifier les registres et bureaux d'enregistrement qui ont besoin d'un examen plus approfondi et pour lesquels le département de la conformité de l'ICANN doit en faire une priorité. En identifiant des phénomènes de malveillance, l'ICANN devrait mettre en place un plan d'action pour répondre à ces études, remédier aux problèmes identifiés, et définir une future collecte de données.	Le Conseil d'administration de l'ICANN, le groupe des représentants des opérateurs de registre, le groupe des représentants des bureaux d'enregistrement, l'organisation de soutien aux extensions génériques et le groupe de travail PDP consacré aux procédures futures, la deuxième équipe de révision de la sécurité, la stabilité et la résilience du DNS.	élevée
D	Une politique de règlement de litiges relatifs à l'utilisation malveillante du DNS (DADRP) doit être envisagée par la communauté afin de traiter les opérateurs de registre et bureaux d'enregistrement qui sont identifiés comme ayant des niveaux excessifs de malveillance (à définir, p.ex., plus de 10 % de leurs noms de domaine sont sur une liste noire). En premier lieu, il s'agirait de demander à ces opérateurs de registre et bureaux d'enregistrement de a) expliquer la situation au département de conformité de l'ICANN, b) s'engager à changer ces comportements dans un délai précis, et/ou d'adopter des politiques d'enregistrement strictes dans un délai précis. Si l'ICANN ne prend pas elle-même les mesures nécessaires, une DADRP peut être mise en place.	Le Conseil d'administration de l'ICANN, le groupe des représentants des opérateurs de registre, le groupe des représentants des bureaux d'enregistrement, l'organisation de soutien aux extensions génériques et le groupe de travail PDP consacré aux procédures futures, la deuxième équipe de révision de la sécurité, la stabilité et la résilience du DNS.	élevée

40	Une étude de l'impact visant à déterminer l'impact du programme des nouveaux gTLD sur le coût et les efforts requis pour protéger les marques déposées dans le DNS devrait être répétée à intervalles réguliers afin d'observer l'évolution du programme des nouveaux gTLD au fil du temps et l'augmentation des enregistrements de nouveaux gTLD. Nous recommandons en particulier que la prochaine étude d'impact soit achevée dans les 18 mois suivant la publication du rapport final de la CCT-RT et que d'autres études soient effectuées tous les 18 à 24 mois. La CCTRT reconnaît qu'elle a été réalisée en 2017 par Nielsen concernant les membres de l'INTA et nous encourageons à poursuivre cela en notant que les études doivent être plus accessibles.	Organisation de l'ICANN.	élevée
41	Une révision complète de l'URS devrait être effectuée et il conviendrait de tenir compte de la façon dont il devrait fonctionner avec l'UDRP. Toutefois, compte tenu de la révision PDP de tous les mécanismes de protection des droits dans tous les gTLD, actuellement en cours, une telle révision doit prendre en considération ce rapport lors de sa publication et pourrait même ne pas être nécessaire si ce rapport pose des conclusions substantielles et examine pleinement les modifications éventuelles.	Organisation de soutien aux extensions génériques	condition préalable
42	Une analyse coût-bénéfice et une révision du TMCH et de sa portée devraient être réalisées afin de fournir des informations quantifiables sur les coûts et bénéfices liés à l'état actuel des services du TMCH et permettre ainsi une révision des politiques efficace.	Organisation de soutien aux extensions génériques	condition préalable

3 Concurrence

3.1 Répercussions éventuelles des domaines « en parking » sur les mesures de la concurrence.

Généralement, dans nos discussions sur les répercussions des nouveaux gTLD sur la concurrence, nous traitons tous les domaines équitablement. Cependant, il faut noter que la majorité des domaines à la fois au sein des nouveaux et des anciens gTLD ne sont pas les identificateurs principaux de sites Web classiques. Ces domaines sont plutôt acheminés vers d'autres domaines (dont des sous-domaines), utilisés uniquement pour des courriers électroniques, monétisés via la publicité ou dont la résolution ne s'effectue pas, ils sont éventuellement gardés en réserve par des spéculateurs ou en tant que domaine bonus par des registres. Afin de réaliser une évaluation à haut niveau des répercussions, ces domaines, faute d'avoir un meilleur terme, ont été considérés comme étant « en parking »

par l'équipe de révision. L'équipe de révision a seulement essayé de savoir si les taux de ces activités étaient différents entre les anciens et les nouveaux gTLD, et si tel est le cas, de savoir si ces différences soulignent un besoin de recherche approfondie. Bien que nous pensions que davantage de recherches sont nécessaires, le contexte du programme des nouveaux gTLD pourrait ne pas s'y prêter. En utilisant une définition large de 'parking', selon des données rassemblées par nTLDstats, environ 68 % des enregistrements de nouveaux gTLD sont actuellement en parking.[1] À titre de comparaison, 56 % des enregistrements dans les anciens gTLD sont actuellement en parking. Halvorsen et al attribue l'enregistrement en parking à : (1) la spéculation visant à vendre à profit le domaine plus tard ; (2) aux plans de développement du domaine à une date ultérieure ; ou (3) à un développement infructueux.[2]

Voici des exemples de comportements pouvant être qualifiés de comportements en parking :

- La résolution du nom de domaine ne s'effectue pas.
- La résolution du nom de domaine s'effectue mais le nom de domaine essaie de se connecter via un renvoi HTTP ou un message d'erreur.
- Les connexions HTTP ont réussi mais le résultat est une page qui affiche des publicités et/ou offre le domaine à la vente. Ces pages peuvent également être utilisées comme vecteur de diffusion d'un programme malveillant.
- La page qui est renvoyée est vide ou indique que le titulaire de nom de domaine ne fournit aucun contenu.
- La page qui est renvoyée est un modèle fourni par le registre sans personnalisation offerte par le titulaire de nom de domaine.
- Le domaine a été enregistré par une entité affiliée de l'opérateur de registre et utilise un modèle standard sans contenu unique.
- Le domaine redirige vers un autre domaine dans un TLD différent.

Bien entendu, c'est une représentation assez globale de l'enregistrement 'en parking' car les répercussions sur la concurrence de chacun de ces scénarios sont assez différentes. Pour réaliser une recherche approfondie il faudrait analyser chacune de ces catégories de manière individuelle afin de déterminer les répercussions sur la concurrence.

Cependant, comme le pourcentage d'enregistrement 'en parking' dans les nouveaux gTLD est important, l'équipe de révision cherche à comprendre si le phénomène pourrait avoir un impact sur ses conclusions concernant les répercussions de l'introduction de nouveaux gTLD sur le marché et ainsi justifier une recherche approfondie. Hypothèse avancée : comptabiliser certains types de domaines en parking différemment selon que l'on évalue les parts de marché et le niveau de concentration. Par exemple, l'une des raisons justifiant la prise en compte des taux de parking est que les taux de renouvellement des enregistrements peuvent être corrélés négativement avec certains types d'enregistrements 'en parking' et que les parts de marché actuelles des TLD ayant des taux de parking assez élevés risquent de surévaluer la situation concurrentielle sur le long terme. Par exemple, certains enregistrements anticipés au sein des nouveaux gTLD sont la conséquence d'une ruée des spéculateurs. Il y a également eu une augmentation fulgurante des enregistrements provenant de Chine à la fois au sein des anciens et des nouveaux gTLD, certains sont le résultat d'une spéculation et certains sont le résultat de changements de règlementations dans le temps. Pour finir, une différence de prix entre un enregistrement initial et un renouvellement peut avoir une répercussion significative sur les

[1] « Aperçu des nouveaux gTLD en parking », consulté le 21 mars 2017, https://ntldstats.com/parking/tld
[2] T. Halvorson, M.F. Der, I. Foster, S. Savage, L.K. Saul, and G.M. Voelker, « De.academy à .zone : une analyse de la ruée vers les nouveaux TLD », Conférence ACM 2015 sur la mesure d'Internet.

renouvellements.[3] Dans ce cas, ces nouveaux domaines devraient avoir un taux réduit correspondant à la corrélation. En d'autres termes, si les enregistrements spéculatifs sont isolés et ont moitié moins de chance d'être renouvelés, leur nombre devrait être réduit de 50 % dans les calculs de part de marché et de concentration du marché. Bien entendu, il faut prendre en compte le fait que le comportement spéculatif est fondamentalement différent entre les nouveaux et les anciens gTLD avec des attentes du marché établies. Autre hypothèse : l'utilisation de domaines comme curseurs impliquent une transition hors du domaine existant. Autrement dit, un curseur peut être l'indication d'une acceptation provisoire d'un nouveau gTLD par le marché et l'ancien domaine est maintenu à court terme uniquement pour préparer une transition. Dans ce cas, les domaines auxquels d'autres sont signalés devraient avoir un taux réduit. Bien entendu, il y a des cas où des redirections ne représentent qu'un 'sur-enregistrement' soit pour capturer les erreurs typographiques ou protéger l'identité de la marque. Afin de mieux analyser une redirection il faudrait déterminer quel domaine est utilisé pour promouvoir le site. En conclusion, il est probable que la spéculation ait pour effet de favoriser la concurrence, non pris en compte directement par les calculs de parts de marché et de concentration du marché, en accompagnant les nouveaux gTLD jusqu'à maturité, ce qui prend environ 3 à 5 ans. Compte tenu du mandat pour examiner l'impact des nouveaux gTLD sur la concurrence, la première question est de savoir si le taux de parking est très différent entre les anciens et les nouveaux gTLD.

Pour mieux comprendre ce sujet, l'équipe de révision a utilisé des données existantes relatives au parking pour les nouveaux gTLD que nTLDstats calcule régulièrement. Nous avons également demandé que l'ICANN signe un contrat avec nTLDstats pour développer des données relatives au parking pour les anciens gTLD spécialement pour ce projet.[4] Nous avons utilisé les données d'enregistrement pour décembre 2016, mois sur lequel se basent les autres statistiques du rapport, et les mesures les plus complètes fournies par nTLDstats, le total des 7 sources de parking séparées qu'il a identifiées.[5]

En utilisant ces données, nous avons fait une comparaison initiale des taux globaux de parking entre les anciens et les nouveaux gTLD. nTLDstats a estimé que le taux moyen pondéré de parking pour les anciens gTLD ce mois-ci était d'environ 56 % et que le taux moyen pondéré de parking pour les nouveaux gTLD le même mois était d'environ 68 %, un taux qui est de presque 20 % supérieur à celui des anciens gTLD.[6] Nous ne sommes pas sûrs de l'impact des domaines en parking sur la concurrence mais si les domaines en parking sont en quelque sorte des marqueurs de concurrence moins importants, c'est une différence conséquente qui pourrait affecter le calcul de nos indicateurs de concurrence.[7]

En ayant une idée générale de l'importance éventuelle des taux de parking sur le marché futur, nous avons tenté de déterminer s'il existait un lien entre les taux de renouvellement et les taux de parking. Pour réaliser cette analyse, nous avons comparé les taux de parking

[3] Par exemple, le prix initial du .XYZ était libre dans de nombreux cas mais le renouvellement était à plein tarif.

[4] nTLDstats a appliqué ses analyses relatives au parking à chaque ancien gTLD à partir du nombre de noms dans son fichier de zone. Pour les TLD ayant 10 000 noms ou moins, nTLDstats a analysé tous les noms enregistrés, pour les TLD ayant entre 10 001 et 100 000 noms, il a analysé 10 % des noms enregistrés, pour les TLD ayant plus de 100 000 noms, il a analysé 1 % des noms enregistrés. nTLDstats a également mené une révision manuelle sur 10 % de l'échantillon total afin de vérifier les faux positifs.

[5] Nous avons ajusté le nombre d'enregistrements pour chaque gTLD afin de refléter le nombre d'enregistrements qui n'étaient pas en parking, c'est-à-dire que nous avons calculé (1 moins le taux de parking) le nombre d'enregistrements pour chaque gTLD.
20 % de 55,6 = 11,2 et 55,6+11,12 = 66,72 (environ 68 %).

[7] Dans ce cas, si nous devions exclure les enregistrements en parking de toutes nos analyses du marché, nous nous retrouverions avec une part de marché 'hors-parking' des enregistrements de nouveaux gTLD représentant une partie de l'ensemble des gTLD de 10,9 %, environ 23 % de moins que les 14,2 % lorsque les domaines en parking sont inclus. (Faire un ajustement similaire dans nos calculs sur la concentration du marché n'a pas fait une grande différence entre les domaines en parking inclus ou non inclus).

dans chaque TLD depuis décembre 2016, avec un taux de renouvellement calculé sur la base des rapports de transaction mensuels des registres [8] pour la période de juillet à décembre 2016[9]. En utilisant une analyse de corrélation de Pearson, nous n'avons pas pu trouver une corrélation statistique significative entre les taux de renouvellement et les taux de parking que ce soit pour les anciens ou nouveaux gTLD. Bien que le fait d'identifier une liaison ait été intéressant, les résultats de ce test ne montrent en aucun cas une corrélation éventuelle. Nous recommandons des études plus rigoureuses sur ce sujet afin de mieux analyser l'existence d'une telle liaison. Ces études pourraient inclure, entre autres, un examen plus minutieux des facteurs suivants : 1) quelles mesures du taux de parking évaluent le mieux le marché de la concurrence ; 2) quels taux de renouvellement devraient être utilisés ; 3) quels facteurs autre que le parking sont susceptibles d'avoir des répercussions sur les taux de renouvellement ; 4) quelle est la forme de la fonction (p.ex., linéaire, logarithmique, etc.) du lien entre le parking et les renouvellements ; 5) quel est le 'décalage' entre le parking et les non-renouvellements (c'est-à-dire, combien de temps existe entre le moment où un domaine est mis en parking et le moment où il n'est pas renouvelé) ?

3.2 Différences géographiques des domaines en parking

L'équipe de révision a également cherché à déterminer si la quantité de domaines en parking variait selon la région. Par exemple, l'étude sur le marché des noms de domaine de la région Amérique latine et Caraïbes (étude LAC) rapporte que « dans toute la région, 78 % des noms de domaine gTLD sont actifs, et 22 % ne sont pas utilisés (expirés ou hors-service).[10] À titre comparatif, selon nTLDstats, dans l'ensemble des nouveaux gTLD environ 33 % des domaines n'avaient pas de DNS valide ou ont retourné des réponses HTTP invalides.

Bien que l'équipe de révision n'a pas été en mesure d'établir une corrélation directe entre les adresses des titulaires de noms de domaine et les noms de domaine en parking, nous avons pu identifier six des 50 plus importants nouveaux gTLD incluant des TLD exploités par des registres basés en Chine montrant des taux de parking nettement plus élevés que la moyenne parmi l'ensemble des nouveaux gTLD, avec des taux allant de 85 % pour .wang à 98 % pour .xin. Le tableau A[11] ci-dessous montre le taux de parking pour chacun des six :

	TAUX DE PARKING (%)
Tous les nouveaux gTLD	68 %
.XIN	97,77 %
.WANG	85,08 %

[8] Les registres ne donnent pas de calcul du taux de renouvellement à l'ICANN. Néanmoins, étant donné que les domaines de second niveau se renouvellent automatiquement, nous avons calculé un taux de renouvellement pour chaque TLD en divisant le nombre de transactions de renouvellement par la somme des transactions de suppression (hors délai de grâce supplémentaire) ajouté aux transactions de renouvellement.
[9] Les taux de renouvellement mensuels peuvent être assez fluctuants et ne représentent qu'une partie des domaines éligibles au renouvellement ce mois-ci, alors que les taux de parking sont calculés pour l'ensemble des domaines au sein d'un TLD. Par conséquent, nous avons calculé le taux de renouvellement sur une période de six mois de façon à réduire les erreurs d'échantillon dans nos analyses.
[10] Oxford Information Labs, LACTLD, EURid et InterConnect Communications, Étude sur le marché des noms de domaine en Amérique latine et aux Caraïbes (septembre 2016), consulté le 23 octobre 2017, https://www.icann.org/en/system/files/files/lac-dns-marketplace-study-22sep16-en.pdf
[11] NTLDStats.com (consulté le 3 mars 2017) : Analyse des taux de parking des anciens gTLD https://community.icann.org/display/CCT/Studies%2C+Research%2C+and+Background+Materials?preview=/56135378/64074447/ICANN%20Parking%20Check.xlsx

.TOP	85,08 %
网址 (xn--ses554g)	83,22 %
.REN	82,82 %

Selon les données de nTLDstats, il y a eu plus de 9 millions d'enregistrements réalisés dans des chaînes de nouveaux gTLD provenant de Chine.[12] Il est possible que l'on constate des taux de parking plus élevés dans les nouveaux gTLD répondant aux besoins des titulaires chinois à cause d'enregistrements de domaines spéculatifs en dehors de la Chine, en particulier concernant les noms de domaine courts (c'est-à-dire, les noms contenant moins de cinq lettres ou chiffres). En 2015, des investisseurs chinois ont acheté un grand nombre de noms de domaine courts car ils étaient considérés comme étant particulièrement intéressants par ces investisseurs.[13] En outre, il semble que les acheteurs chinois achètent également des noms en tenant compte des utilisations finales qui pour eux, prendront de la valeur dans le futur. En conséquence, la prise de conscience de l'investissement dans les noms de domaine en Chine peut avoir contribué à des taux de parking plus élevés pour les nouveaux gTLD en langue chinoise. Cette tendance montre également qu'il existe une bulle spéculative sur le marché chinois ainsi qu'une valeur attendue de ces domaines.

Ces analyses initiales des taux de parking selon la région géographique sont assez sommaires et se basent sur des données limitées, mais elles semblent indiquer que les variations des taux de parking selon la région existent et sont assez significatives. Ces chiffres représentent une mesure globale des taux de parking et il faudra une analyse future avec un examen plus détaillé dans l'ensemble des régions géographiques.

3.3 Lien entre les taux de parking et l'utilisation malveillante du DNS

Même si l'équipe de révision n'était pas en mesure d'identifier un lien direct entre les taux de parking et la concurrence ou le choix du consommateur, nous avons également pris en considération l'éventualité selon laquelle les domaines en parking peuvent être avoir un lien avec la confiance du consommateur, et en particulier avec la possibilité que les taux de parking aient un lien avec l'utilisation malveillante du DNS. Précédemment, Vissers et al[14] ont étudié plus de huit millions de domaines en parking et ont conclu que « les utilisateurs qui ont atterri sur des sites Web en parking s'exposent à des programmes malveillants, du contenu inapproprié, et des arnaques élaborées. »[15]

[12] NTLDStats.com (consulté le 31 octobre 2017) : Analyse des taux de parking des anciens gTLD https://community.icann.org/display/CCT/Studies%2C+Research%2C+and+Background+Materials?preview=/56135378/64074447/ICANN%20Parking%20Check.xlsx

[13] Echo Huang, « La nouvelle mode des investissements en Chine sur les noms de domaine courts, » Quartz, 10 janvier 2016, consulté le 30 octobre 2017. https://qz.com/581248/chinas-latest-investment-craze-is-short-domain-names/

[14] Vissers, Joosen, et Nikiforakis, « Détecteurs de domaines en parking : analyser et détecter les domaines en parking, » (document présenté lors du NDSS, San Diego, USA, 8-11 février 2015). http://dx.doi.org/10.14722/ndss.2015.23053

[15] L'équipe de révision ne sait pas très bien si la propagation d'un programme malveillant est intentionnelle de la part des sites en parking ou des services en parking, ou le résultat de réseaux de publicité corrompus. Vissers et al a soulevé cette possibilité dans leur rapport. « Il est possible que ces chaînes complexes soient la conséquence d'un processus similaire d'arbitrage de publicité, une pratique largement adoptée réalisée par la plupart des agences de publicité [33]. Durant ce processus, les agences font des offres sur des espaces publicitaires disponibles appartenant à d'autres éditeurs ou agences, leur permettant de revendre ces espaces au prochain enchérisseur. Souvent les espaces publicitaires sont soumis à des répétitions multiples de ce processus de revente. En conséquence, les espaces publicitaires ne sont plus sous le contrôle de l'agence avec laquelle l'éditeur original a collaboré. Tous ces échanges et ces intermédiaires sont susceptibles de troubler

En lien avec cette révision, l'analyse statistique de l'utilisation malveillante du DNS dans les gTLD a mis en évidence le fait que de manière générale, au sein des nouveaux gTLD, le nombre total des enregistrements associés à un programme malveillant est inférieur à ceux des anciens gTLD.[16] Tandis que, le taux de programmes malveillants associés aux noms de domaine par volume au sein des nouveaux gTLD est de temps à autre supérieur à celui des anciens gTLD. Cependant, si vous regardez parmi les nouveaux gTLD et si vous observez les taux de parking, vous verrez que s'agissant des programmes malveillants qui se présentent, ils sont plus susceptibles d'apparaître dans des zones avec un taux de parking plus élevé. Il peut y avoir une certaine corrélation entre les taux de parking et les programmes malveillants mais elle n'est pas aussi forte et révélatrice que la tendance mondiale visant à des taux de distribution plus bas que ceux des anciens gTLD. Néanmoins, l'écart dans le taux de distribution de programmes malveillants entre les anciens et les nouveaux gTLD semble se réduire et il convient à la communauté de mieux examiner la corrélation entre les taux de parking et la distribution de programmes malveillants.

3.4 Recommandations

Bien que nous observons que les nouveaux gTLD ont des taux de parking plus élevés (en utilisant la définition la plus large possible) que les anciens gTLD et qu'il existe des variantes selon les régions, nous ne savons pas vraiment si le parking a un impact significatif sur la concurrence ou le choix du consommateur. En conséquence, nous recommandons que l'ICANN réalise davantage de recherches à propos des répercussions éventuelles sur la concurrence des domaines en parking et qu'elle utilise les résultats de cette recherche pour améliorer cette analyse relative au développement du marché du DNS. De plus, nous recommandons que l'ICANN prenne en considération l'utilisation de données sur les suppressions d'enregistrement à venir dans la même optique.

Recommandation 5: Recueillir des données relatives au parking.

Fondements/conclusions connexes : Le taux élevé de domaines en parking laisse entendre un impact sur l'environnement concurrentiel mais des données insuffisantes neutralisent les efforts visant à analyser cet impact.

À: organisation de l'ICANN.

Condition préalable ou niveau de priorité : élevée

Consensus au sein de l'équipe : oui

Détails : L'ICANN devrait régulièrement suivre la proportion des TLD en parking suffisamment précisément pour identifier les tendances à l'échelle régionale et mondiale. On devrait envisager davantage de révisions et d'analyses pour savoir s'il existe une corrélation entre les domaines en parking et les taux de renouvellement ou d'autres facteurs qui pourraient avoir un impact sur la concurrence. Davantage d'analyses devraient être réalisées sur le lien entre le parking et l'utilisation malveillante du DNS.

l'implication directe des services de parking en étant bénéfique pour les programmes malveillants. Dans certains cas cependant, nous observons des programmes malveillants distribués plus directement, par exemple par la société mère des services de parking 8. »

[16] SIDN Labs et Delft University of Technology (août 2017), Rapport final de l'analyse statistique de l'utilisation malveillante du DNS dans les gTLD, consulté le 23 octobre 2017, https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf

Mesures de réussite : La disponibilité de données pertinentes à des fins d'utilisation par l'ICANN, les prestataires et la communauté de l’ICANN dans le cadre de leurs travaux d'évaluation de la concurrence dans l’espace du DNS.

4 Choix du consommateur

L'équipe de révision a également abordé la question de savoir si l'introduction de nouveaux gTLD augmentait les choix offerts aux titulaires de nom de domaine. Tel que vu précédemment dans ce rapport, le développement du programme donne aux titulaires de noms de domaine de nouvelles options en termes de langues, de séries de caractères, d'identités géographiques et de catégories spéciales. Toutefois, nous avons souhaité établir si les enregistrements de nouveaux gTLD représentaient un choix positif à la disposition des titulaires de noms de domaine ou si un nombre non négligeable d'entre eux se sentaient obligés de procéder à des enregistrements défensifs dans des nouveaux gTLD afin de protéger leur marque ou identité. De nombreuses discussions ont notamment été engagées afin de savoir s'il s'avérerait nécessaire pour les détenteurs de marque d'enregistrer les marques en tant que noms de domaine dans des nouveaux gTLD afin d'empêcher d'autres de le faire.

Plusieurs études ont été menées (voir ci-dessous) afin de savoir dans quelle mesure les titulaires de noms de domaine ont procédé à des enregistrements défensifs. Dans l'attente de cette révision, l'ICANN a demandé à Nielsen de réaliser une enquête mondiale sur les titulaires de noms de domaine pour avoir une meilleure idée de ceux-ci. Plus récemment, l'INTA a mené une étude sur ses membres qui reflète l'expérience des propriétaires de marques déposées. L'équipe de révision a examiné chacune de ces études et les a complétées avec sa propre analyse. Nous abordons dans un premier temps le thème général du choix du consommateur, puis nous procédons à une analyse détaillée des propriétaires de marque.[17]

Lors de l'évaluation de ces résultats, il convient de noter que tous les cas d'enregistrement en double ne sont pas forcément « défensifs » par nature. Par exemple, un propriétaire de marque peut enregistrer la même marque dans plusieurs domaines afin d'augmenter la probabilité qu'il soit trouvé via des recherches d'utilisateurs, un aspect de plus en plus important étant donné que le nombre de domaines augmente.[18] En réalité, 52 % des titulaires de noms de domaine interrogés par Nielsen déclarent enregistrer des noms de domaine en double afin « d'aider à garantir que [leur] site apparaisse dans des recherches ».[19] Cependant, 51 % des personnes interrogées indiquent avoir procédé à des enregistrements en double « afin de protéger [leur] marque ou le nom de [leur] organisation » et afin « d'empêcher quelqu'un de prendre le même nom ».[20] L'enquête a conclu que « les enregistrements de nouveaux TLD reproduisent principalement les enregistrements des TLD ou ccTLD historiques »,[21] et qu'en particulier, seulement 17 % des personnes ayant répondu ont enregistré pour la première fois des noms dans les nouveaux gTLD par rapport à l'enregistrement en double de domaines existants dans les gTLD ou ccTLD historiques. Ainsi, il semble que les enregistrements « défensifs » constituent un véritable phénomène, apparemment car les coûts liés à la contestation des enregistrements

17 Dans ce chapitre, le terme « consommateurs » est principalement utilisé afin de désigner des titulaires de nom de domaine et non pas des utilisateurs finaux, le comportement et les croyances de ces derniers étant largement couverts dans le chapitre consacré à la confiance du consommateur.

18 Il convient de prendre en compte les utilisateurs qui cherchent des sites Internet en essayant de deviner les adresses Internet. Plus le nombre de TLD augmente, plus il est difficile de trouver le bon site Internet en essayant de deviner et, en moyenne, le nombre de tentatives augmente considérablement. Devant ce constat, on pourrait s'attendre à ce que les personnes cherchant à deviner le nom d'un site utilisent plus de moteurs de recherche qu'avant. Toutefois, certains titulaires de noms de domaine pourraient encore choisir de s'enregistrer dans plusieurs TLD afin de réduire le nombre de tentatives d'un utilisateur visant à trouver un site.

19 Nielsen, enquête sur les titulaires de nom de domaine partie 2 (2016), p. 13.

20 Ibid. Bon nombre de titulaires de noms de domaine ont choisi les deux réponses ; au total, 60 % des titulaires de noms de domaine de nouveaux gTLD ont choisi l'une des deux réponses. Il convient de noter que quelques personnes interrogées ont indiqué enregistrer en double des noms de domaine pour avoir plus de chances d'être trouvés lors d'une recherche et pour protéger leur marque ou empêcher les autres d'enregistrer leur nom, montrant ainsi qu'il n'est pas toujours possible de catégoriser un enregistrement comme étant strictement « défensif » ou pas du tout.

21 Enquête INTA, diapo 19

par d'autres peuvent être largement supérieurs aux coûts d'enregistrement de leurs marques dans différents domaines.[22]

4.1 Études préalables

Krueger et Van Couvering ont examiné 1 043 noms de marque d'entreprises du palmarès Fortune 100 et ont dégagé les pourcentages d'enregistrement suivants : (1) 100% pour .com ; (2) 76 % pour .org ; (3) 84% pour .net ; (4) 69 % pour .info ; (5) 65 % pour .biz ; et (6) 57 % pour .mobi.[23] Zittrain et Edelman ont constaté que, 6 mois après l'ouverture des enregistrements pour .biz, 91 % d'un échantillon de noms de domaine .biz avaient également un enregistrement .com, 63 % avaient également un enregistrement .net et 49 % avaient également un enregistrement .org.[24] Strategies International a analysé la proportion des enregistrements de nom en double et la présence du même titulaire de nom enregistré dans quatre nouveaux TLD et trois TLD historiques et est arrivée aux conclusions suivantes : « Les chiffres pour .info indiquent que seuls 11 % des titulaires de noms de domaine ont le même nom avec .com, ce qui suggère que .info a créé d'importantes nouvelles possibilités. Eu égard à .biz, 42 % des enregistrements en double semblent l'avoir été avec la même partie, ce qui laisse penser qu'il s'agit d'enregistrements protecteurs par nature. »[25] Katz, Rosston et Sullivan ont analysé les doublons des enregistrements de domaines pour 200 des 500 premières marques mondiales selon le classement de Brand Finance et ont constaté « qu'un pourcentage très élevé d'entre elles étaient enregistrées dans des TLD différents » de ceux qu'ils avaient examinés.[26] Toutefois, ils ont également observé « qu'une grande partie des domaines enregistrés étaient des domaines avec contenu » et que le pourcentage de sites actifs « était relativement faible » sauf pour .com. Enfin, Halvorson et al, qui ont utilisé plusieurs mesures afin d'identifier les correspondances de titulaires de noms de domaine entre .com et .biz, ont constaté « au moins un certain degré de correspondance pour environ 40 % des paires [biz-com] qu'ils ont pu évaluer ».[27] À l'aide ce qu'ils décrivent comme étant de « solides indicateurs », ils ont classé 11,6 % des domaines biz dans la catégorie des domaines « défensifs ».

4.2 Analyse de la CCTRT

Selon la 2e partie de l'enquête mondiale sur les titulaires de noms de domaine, 35 % de l'ensemble des titulaires de noms de domaine interrogés ont enregistré au moins un nom dans un nouveau gTLD.[28] Parmi eux, 60 % ont indiqué avoir procédé à un enregistrement afin de « protéger des domaines existants et de veiller à ce que personne d'autre n'ait un domaine similaire », alors que 34 % ont indiqué après procédé à un enregistrement afin « d'attirer de nouveaux internautes ou de nouveaux types de clients » et 6 % ont procédé à

22 Annexe G : La bibliographie comprend une série de questions susceptibles d'être incluses dans de futures enquêtes sur les titulaires de noms de domaine afin de mieux comprendre les choix qu'ils font lors de l'enregistrement de noms de domaine.

23 F. Krueger et A. Van Couvering, « Analyse des données relatives à l'enregistrement de marques dans les nouveaux gTLD », document de travail de Minds + Machines, (2010-02). 51.

24 Berkman Center for Internet and Society Harvard Law School, Étude sur l'utilisation du TLD .biz (juin 2002), consulté le 25 janvier 2017, https://cyber.law.harvard.edu/tlds/001/

25 Summit Strategies International, Évaluation des nouveaux gTLD : *enjeux politiques et juridiques* (juillet 2004), disponible le 25 janvier 2017, 102. Même titulaire de nom de domaine enregistré pour .com/.net/.org à 102. Toutefois, il convient de noter que les auteurs soulignent que « Les données...sont basées sur un échantillon extrêmement réduit de 100 noms pour .biz and .info ». Cette étude a été préparée pour l'ICANN.

26 M.L. Katz, G.L. Rosston et T. Sullivan, Considérations économiques eu égard au développement des domaines génériques de premier niveau, 2e partie du rapport : études de cas (décembre 2011), consulté le 25 janvier 2017, https://archive.icann.org/en/topics/new-gtlds/phase-two-economic-considerations-03dec10-en.pdf, p. 61. Il s'agissait des domaines .com, .net, .org, .biz, .info, .mobi, et .us. Cette étude a été préparée pour l'ICANN.

27 T. Halvorson, J. Szurdi, G. Maier, M. Felegyhazi, C. Kreibich, N. Weaver, K. Levchenko et V. Paxon, « Le domaine de premier niveau BIZ : dix ans après » dans Passive and Active Measurement, éditions N. Taft et F. Ricciato. (Allemagne : Springer Berlin Heidelberg, 2012), 221-230, 228. http://www.icir.org/vern/papers/dot-biz.pam12.pdf

28 Nielsen, enquête sur les titulaires de noms de domaine partie 2 (2016), p. 164.

un enregistrement car « le nom [qu'ils souhaitaient] n'était plus disponible en utilisant d'anciens gTLD ».

Nous avons également effectué une analyse des chaînes enregistrées en tant que domaines de second niveau dans de nouveaux gTLD et de chaînes comparables enregistrées avec .com, qui est actuellement et de loin le gTLD historique le plus répandu. Notre analyse s'est concentrée sur deux tendances potentielles. Dans le premier cas, nous avons cherché à savoir si la *chaîne identique* enregistrée en tant que domaine de second niveau dans un nouveau gTLD était enregistrée en tant que domaine de second niveau avec .com (par exemple si exemple.tld était enregistré, exemple.com était-il aussi enregistré ?).[29] Nous avons constaté que 82 % des enregistrements dans de nouveaux gTLD avaient des correspondances identiques avec .com. Toutefois, il existe des écarts importants dans les pourcentages de correspondances identiques entre les gTLD. Par exemple, parmi les 414 gTLD avec au moins 1000 enregistrements, 32 affichaient au moins 99 % de correspondance exacte de leurs domaines de second niveau enregistrés avec .com, y compris .wang et .xin qui, en novembre 2016, constituaient les troisième et onzième nouveaux gTLD les plus importants en termes de volume d'enregistrement ; et presque deux-tiers (271) affichaient au moins 95 % de correspondance exacte de leurs domaines de second niveau enregistrés avec .com. En revanche, 10 gTLD affichaient moins de 50 % de correspondance exacte de leurs domaines de second niveau enregistrés avec .com. Parmi ceux-là, la moitié était des IDN. En général, les gTLD IDN contenaient moins de correspondances identiques avec .com, seulement environ 70 % des enregistrements dans des gTLD IDN étant des correspondances identiques avec des domaines .com. Malheureusement, du fait que notre analyse ne comprenait pas de données WHOIS, nous n'avons pu déterminer si le même titulaire de nom de domaine avait enregistré les deux domaines.
Lors d'une seconde analyse, nous avons examiné si la **chaîne combinée** représentant le TLD et le SLD était enregistrée en tant que domaine de second niveau avec .com (par exemple, si exemple.tld était enregistré, exempletld.com était-il aussi enregistré ?). Dans le cadre de cette analyse, nous avons constaté que seuls 8 % des enregistrements dans les nouveaux gTLD l'étaient également avec .com sous la forme combinée.

Globalement, nous arrivons à la conclusion que certains titulaires de noms de domaine sont guidés par des objectifs de défense dans les nouveaux gTLD, et que bon nombre de titulaires de noms de domaine choisissent de procéder à un enregistrement dans les nouveaux gTLD afin de renforcer l'attrait ou l'impact de leurs offres même lorsque des options similaires restent disponibles dans les gTLD historiques.

4.3 Analyse de la CCTRT : Marques déposées

L'enquête de l'INTA a montré que parmi les propriétaires de marques interrogés, « quasiment tous les nouveaux domaines enregistrés en tant que doublon d'un ancien TLD ou ccTLD avaient initialement pour but d'empêcher que le nom soit utilisé par un autre titulaire de nom de domaine. »[30] Afin de mieux comprendre la prévalence des enregistrements défensifs par les propriétaires de marques, nous avons, aux côtés d'Analysis Group, utilisé des données issues de la dernière « série » de nouveaux gTLD afin d'analyser cette question. Plus précisément, nous avons commencé par identifier un certain nombre de marques pour lesquelles on pourrait s'attendre à des enregistrements

29 Analysis Group, Résumé des chaînes de marque *enregistrées dans des chaînes de marque de gTLD historiques qui sont également des TLD de marque* (octobre 2016), consulté le 25 janvier 2017,
https://community.icann.org/download/attachments/56135378/New%20gTLD%20Registrations%20of%20Brand%20TLD%20TM%20Strings%2010-18-16.pdf?version=1&modificationDate=1481305785167&api=v2

30 Enquête INTA, diapo 22

« défensifs » ainsi que l'identité du titulaire de nom de domaine. Les données recueillies par Analysis Group correspondaient à un échantillon aléatoire de 25 % de détenteurs de marque qui a été obtenu via une base de données administrée par Deloitte et qui contient toutes les marques enregistrées dans la base de données du centre d'échange d'information sur les marques. Les identités des titulaires de noms de domaine ont été obtenues à partir de la base de données WHOIS des enregistrements de domaine.[31] Les chaînes de marque analysées ont été limitées aux chaînes de caractères latins vérifiées ou corrigées du Centre d'échange d'information sur les marques. Des correspondances ont été identifiées, telles que des correspondances exactes, conformément aux critères de correspondance de l'ICANN, le titulaire d'un nom de domaine ayant été identifié comme le détenteur d'une marque associée à la chaîne enregistrée sur la base d'une comparaison de texte approximative entre les noms du titulaire de nom de domaine et du détenteur de marque.

À l'aide de ces données, nous avons déterminé : (1) si chacune des marques de notre base de données était enregistrée par le propriétaire de marque dans au moins un ancien gTLD ; (2) si la même chaîne était enregistrée par le propriétaire de marque dans au moins un nouveau gTLD ; et (3) pour les chaînes qui ont été enregistrées par le propriétaire de marque dans au moins un nouveau gTLD, le nombre de nouveaux gTLD dans lesquels le propriétaire de marque avait enregistré la chaîne. Nous avons constaté que 54 % des chaînes qui ont été enregistrées dans un ancien gTLD ont également été enregistrées dans au moins un nouveau gTLD. Nous avons également constaté que, parmi ces chaînes, 3 constituait le nombre moyen d'enregistrements dans des nouveaux gTLD. C'est-à-dire que la moitié des marques qui ont été analysées ont été enregistrées dans 3 nouveaux gTLD ou moins.[32] Nous avons également noté que trois quarts de ces chaînes ont été enregistrées dans 7 nouveaux gTLD ou moins et que 90 % de ces chaînes ont été enregistrées dans 17 nouveaux gTLD ou moins.[33] En même temps, peu de chaînes de marque ont été enregistrées dans un grand nombre de TLD : 4 % des marques ont été enregistrées dans au moins 100 nouveaux gTLD et une a été enregistrée dans 406 nouveaux gTLD. En extrapolant les résultats obtenus à partir de l'échantillon à l'ensemble des marques, nous nous attendions à ce que les propriétaires de marque aient procédé à environ 80 000 enregistrements de leurs marques dans des nouveaux gTLD en septembre 2016, soit 0,3 % de l'ensemble des enregistrements dans les nouveaux gTLD[34]. Nous concluons de cette analyse que, bien que les coûts directs du programme des nouveaux gTLD pour la plupart des détenteurs de marque procédant à des enregistrements défensifs semblent être inférieurs à ce que certaines personnes craignaient avant le lancement du programme, un faible pourcentage des détenteurs de marque pourrait être contraint d'engager des coûts importants.

En plus des enregistrements défensifs, certains registres proposent un service permettant au propriétaire d'une marque d'empêcher d'autres d'utiliser leurs marques sans qu'il n'ait à acheter le nom de domaine. Par exemple, Rightside offre ce qu'il décrit comme « une solution rentable en une étape appliquée à l'ensemble du registre visant à protéger les marques de vos clients contre le cybersquattage...via notre liste de marques protégées pour les extensions (DPML) » au lieu « d'acheter, à titre défensif, des marques et des marques +

31 Analysis Group, *Rapport préliminaire sur la révision indépendante des services du Centre d'échange d'information sur les marques (TMCH)* (juillet 2016), consulté le 25 janvier 2017, https://newgtlds.icann.org/en/reviews/tmch/draft-services-review-25jul16-en.pdf

32 Le nombre moyen d'enregistrements en double était de 8 mais ces chiffres sont fortement influencés par le faible nombre de marques qui ont été enregistrées dans un très grand nombre de domaines. À titre d'exemple, une marque a été enregistrée dans 406 domaines.

33 Afin d'évaluer ces conclusions, il est important de souligner que la quantité observée d'enregistrements en double pourrait avoir été influencée, au moins dans une certaine mesure, par l'utilisation par les détenteurs de marque des services de blocage décrits ci-dessus. C'est-à-dire que si les propriétaires de marque ont obtenu une protection via le blocage, il se peut qu'ils aient moins besoin de procéder à des enregistrements « défensifs ».

34 Selon la révision du TMCH, qui a utilisé un échantillon de 25 %, 19 642 enregistrements par les détenteurs de marque de leur marque ont été recensés. Une extrapolation à 100 % nous donne un total de 78 568 enregistrements. En comparaison, en septembre 2016, on recensait un total de 24 814 743 enregistrements pour l'ensemble des nouveaux gTLD.

termes pour chaque TLD... ». [35]De même, Donuts souligne que « sa liste de marques protégées pour les extensions (ou DPML) protège les propriétaires de marques contre le cybersquattage à un coût très inférieur aux coûts d'enregistrement défensif et individuel des termes pour tous les domaines Donuts ».[36] Au moment de la publication du présent rapport, nous n'avions pas de données relatifs aux coûts engagés par les détenteurs de marque ayant recours à ces services de blocage ; nous espérons toutefois obtenir de plus amples informations avant la publication de notre rapport final.

Recommandation 9: Réaliser des enquêtes périodiques sur les titulaires de noms de domaine.

Fondements/conclusions connexes : L'incapacité à déterminer les motivations et comportements des titulaires de noms de domaine compromet les efforts visant à examiner la concurrence et le choix sur le marché des TLD.

À: organisation de l'ICANN.

Condition préalable ou niveau de priorité : condition préalable

Consensus au sein de l'équipe : oui

Détails : L'enquête devrait être conçue et améliorée en permanence afin de recueillir les tendances des titulaires de noms de domaine
. Quelques pistes de réflexion sur les éventuelles questions à poser sont disponibles à l'annexe F : Questions possibles pour une future enquête sur les consommateurs.

35 Registre Rightside, « DPML », consulté le 21 septembre 2016, http://rightside.co/registry/dpml/

36 Donuts Registry, « DPML », consulté le 21 septembre 2016, http://www.donuts.domains/services/dpml. Selon nomdedomaine.com : « Trois des nouveaux registres de noms de domaine génériques de premier niveau les plus importants ont [sic] créé un nouvel outil de blocage des noms de domaine. Bon nombre de clients préfèrent éviter des enregistrements défensifs mais ces services permettent de réaliser des économies d'échelle et méritent d'être pris en considération par les principales marques. Le service est proposé par trois fournisseurs de nouveaux gTLD ; Donuts (qui prend en charge 172 TLD), Rightside (36 TLD) et Minds & Machines (16 TLD). L'outil de blocage permet aux propriétaires de marque de bloquer leurs marques et termes connexes, au second niveau, dans tous les nouveaux gTLD pris en charge, moyennant une redevance par registre. Le service est conçu de sorte à donner aux propriétaires de marques un moyen économique de protection de leurs droits contre le cybersquattage. Avec le blocage, les propriétaires de marques ne sont pas tenus de procéder à des enregistrements défensifs auprès des trois fournisseurs de TLD. Afin de bénéficier d'un blocage, le terme que vous souhaitez bloquer doit se fonder sur une marque validée par le centre d'échange d'information sur les marques. »

« Protection à moindre coût des noms de domaines ! », Domain Info, 4 novembre 2015, consulté le 28 septembre 2016, http://domainincite.com/21404-icann-retires-affirmation-of-commitments-with-us-gov

Récemment, Donuts a annoncé une nouvelle version de son service de blocage qui donnera aux propriétaires de marques la possibilité d'obtenir un blocage pour un montant de 10 000 $. [Jack Jack Elis, “Donuts unveils enhanced trademark protection offering; expert urges lower cost options in next gTLD round”, (Donuts dévoile sa nouvelle offre de protection renforcée des marques ; l'expert préconise des options plus économiques lors de la prochaine série de gTLD), World Trademark Review, 29 septembre 2016, consulté le 29 septembre 2016, http://www.worldtrademarkreview.com/blog/Detail.aspx?g=fa934d21-cfa7-459c-9b1f-f9aa61287908

5 Sauvegardes

5.1 Utilisation malveillante du DNS

L'accessibilité des noms de domaine en tant qu'identificateurs mondiaux uniques a fait d'eux un chemin vers les technologies innovantes, y compris celles utilisées à des fins malveillantes. En conséquence, des personnes malveillantes utilisent ces identificateurs universels pour de la cybercriminalité[37] et dirigent les utilisateurs vers des sites Web permettant d'autres formes de crimes, comme l'exploitation d'enfant, l'atteinte à la propriété intellectuelle et la fraude. Chacune de ces activités peut constituer une forme d'utilisation malveillante du DNS. Cependant, les décisions dépendent largement des lois locales, des rôles joués par d'autres fournisseurs d'infrastructure et des interprétations subjectives. Néanmoins, un consensus plus large existe sur de nombreuses formes techniques d'utilisations malveillantes du DNS comme il a été démontré par les conclusions de la communauté et le développement du programme des nouveaux gTLD.

Du fait de l'utilisation malveillante des noms de domaine, la communauté a dans un premier temps fait part de ses inquiétudes quant au développement des gTLD disponibles qui pourrait entraîner une augmentation des utilisations malveillantes du DNS. Il a été demandé à la CCT-RT d'examiner les questions associées au développement du DNS, y compris la mise en œuvre de sauvegardes conçues pour prévenir les risques identifiés.[38]
Avant l'approbation du programme des nouveaux gTLD, l'ICANN a demandé des réactions de la part de la communauté chargée de la cybersécurité sur l'utilisation malveillante du DNS et les risques posés par l'expansion de l'espace des noms du DNS.[39] La communauté a identifié les domaines d'inquiétude suivants :

- Comment s'assurer que des « acteurs mal intentionnés » n'exploitent pas de registres ?
- Comment garantir l'intégrité et l'utilité des informations de registre ?
- Comment garantir des mesures davantage ciblées sur la lutte contre les utilisations malveillantes identifiées ?

[37] Bursztein et. al., « Encadrer les dépendances introduites par la marchandisation illégale, » (document présenté lors de la conférence 2015 sur l'économie de la sécurité de l'information, Delft, Pays-Bas, 22-23 juin 2015),https://research.google.com/pubs/pub43798.html, p. 12.

[38] Le département du commerce des États-Unis et l'affirmation d'engagements de l'ICANN définissent les « problèmes relatifs à l'utilisation malveillante » comme faisant partie des questions à analyser avant l'expansion de l'espace de domaines de premier niveau. En outre, l'AoC impose à l'équipe de révision CCT d'analyser les « sauvegardes mises en place pour atténuer les problèmes liés à l'introduction ou au développement » des nouveaux gTLD. En conséquence, le cahier des charges de l'équipe de révision CCT définit le travail de l'équipe de sorte à incorporer une révision de « l'efficacité des sauvegardes » et « d'autres mesures visant à réduire l'utilisation malveillante du DNS. » De plus, le communiqué de Buenos Aires du GAC de 2015 a demandé à ce que « la communauté de l'ICANN élabore une méthodologie harmonisée pour évaluer le nombre d'enregistrements abusifs de noms de domaine dans le cadre de l'évaluation en cours du programme des nouveaux gTLD. » Voir https://gacweb.icann.org/download/attachments/27132037/BA%20MinutesFINAL.pdf?version=1&modificationDate=1437483824000&api=v2; De la même manière, le communiqué de Dublin de 2015 prévoyait que le Conseil d'administration de l'ICANN « développe et adopte une méthodologie harmonisée pour assurer le suivi des niveaux et de la persistance des comportements abusifs auprès de la communauté de l'ICANN…qui ont eu lieu dans le cadre du programme des nouveaux gTLD. » Voir https://gacweb.icann.org/display/GACADV/2015-10-21+gTLD+Safeguards+%3A+Current+Round

[39] « ICANN (3 octobre 2009), *Réduire les comportements malveillants*, consulté le 9 novembre 2016 https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf. Des commentaires ont été formulés par des groupes comme le groupe de travail anti-hameçonnage (APWG), le groupe de sécurité Internet du registre (RISG), le comité consultatif sur la sécurité et la stabilité (SSAC), les équipes d'intervention informatique d'urgence (CERT), les communautés du secteur bancaire/financier et de la sécurité Internet au sens large.

- Comment fournir un cadre de contrôle amélioré pour les TLD avec un potentiel intrinsèque de comportements malveillants ?[40]

À partir des réactions de la communauté, l'ICANN a identifié diverses recommandations pour des sauvegardes visant à diminuer ces risques.[41] Neuf sauvegardes ont été identifiées et recommandées :

- Vérifier les opérateurs de registre
- Exiger un déploiement des extensions de sécurité du système des noms de domaine (DNSSEC)
- Interdire les « caractères génériques »
- Encourager la suppression des « enregistrements orphelins de type glue »[42]
- Exiger des enregistrements du WHOIS « détaillé »
- Fournir un accès centralisé au fichier de zone
- Indiquer les personnes à contacter et les politiques à mettre en œuvre en cas d'utilisation malveillante au niveau des registres et des bureaux d'enregistrement
- Prévoir un processus accéléré de demande de dérogation pour incident de sécurité des registres
- Créer un projet de cadre pour un programme de vérification des zones de haute sécurité[43]

La CCT-RT a été chargée d'analyser l'efficacité des 9 sauvegardes recommandées. Dans la mesure du possible, la CCT-RT a évalué l'efficacité de chacune de ces sauvegardes en utilisant les données disponibles relatives à leur mise en œuvre et à leur conformité. [44] La CCT-RT a examiné la mise en œuvre de chacune des sauvegardes. De plus, la CCT-RT a demandé une étude quantitative de l'utilisation malveillante du DNS pour donner un aperçu de la relation, le cas échéant, qui peut exister entre les niveaux d'utilisations malveillantes et les sauvegardes mises en œuvre dans l'espace des noms des nouveaux gTLD.[45]

En ce qui concerne la première sauvegarde, à savoir la vérification des opérateurs de registre, il a été demandé à tous les candidats aux nouveaux gTLD de donner une description complète des services techniques back-end auxquels ils pourraient avoir recours, même via la sous-traitance, dans le cadre du processus de candidature. Il s'agissait d'une première évaluation visant à s'assurer qu'ils disposaient des compétences techniques requises. Ces descriptions ont été évaluées seulement au moment de la candidature.[46] De plus, il a été demandé à tous les candidats de passer les tests de pré-délégation (PDT).[47] Les PDT comprenaient des vérifications techniques complètes du protocole d'approvisionnement extensible (EPP), de la configuration du serveur de nom, des

[40] Ibid.

[41] Ibid.

[42] The Security Skeptic, « Enregistrements orphelins de type glue, » 26 octobre 2009, consulté le 2 février 2017 http://www.securityskeptic.com/2009/10/orphaned-glue-records.html. Il s'agit d'enregistrements qui restent une fois que le nom de domaine a été supprimé d'un registre.

[43] ICANN, les « comportements malveillants. »

[44] Voir ICANN, Sauvegardes du programme des nouveaux gTLD (2016).

[45] ICANN (2 août 2016), appel à propositions pour l'étude des taux d'utilisations malveillantes du DNS au sein des nouveaux et anciens domaines de premier niveau, consulté le 2 février 2017, https://www.icann.org/en/system/files/files/rfp-dns-abuse-study-02aug16-en.pdf. L'étude sur l'utilisation malveillante du DNS évalue les formes courantes d'utilisations malveillantes comme le spam, l'hameçonnage, la dissémination de programmes malveillants au sein de tous les gTLD, du 1er janvier 2014 à décembre 2016. SIDN Labs et Delft University of Technology (août 2017), Rapport final de l'analyse statistique de l'utilisation malveillante du DNS dans les gTLD, consulté le 23 octobre 2017, https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf

[46] Les exigences techniques changent tout le temps, ce qui rend difficile les vérifications continues.

[47] ICANN, *Guide de candidature* (juin 2012), article 5-4.

extensions de sécurité du système des noms de domaine (DNSSEC), et d'autres protocoles.[48] Il a été demandé aux candidats de passer tous ces tests avant la délégation d'un nom de domaine.

Au moment de la délégation, il a été demandé aux opérateurs de registre de se conformer aux sauvegardes techniques par le biais de leurs contrats de registre avec l'ICANN. La deuxième sauvegarde prévoyait que les registres des nouveaux gTLD mettent en place le DNSSEC, avec une surveillance active de la conformité et des notifications envoyées aux registres qui ne respectent pas la conformité.[49] Le DNSSEC est un ensemble de protocoles visant à augmenter la sécurité d'Internet en ajoutant l'authentification aux résolutions du DNS pour prévenir les problèmes comme l'usurpation[50] et l'empoisonnement du cache du DNS.[51] Tous les nouveaux gTLD sont des DNSSEC signées au niveau de la zone racine, ce qui n'est pas représentatif des noms de domaine de second niveau signés au sein de la zone racine.[52]

Pour la troisième sauvegarde, le contrat de registre pour les nouveaux gTLD interdit les caractères génériques pour s'assurer que les noms de domaine ne résolvent que les questions de correspondance exacte et que les utilisateurs finaux ne soient pas mal redirigés vers un autre nom de domaine par une réponse synthétisée.[53] Les réclamations face aux opérateurs de registre de façon à permettre les caractères génériques peuvent être soumises à l'ICANN via une interface en ligne.[54] L'utilisation par un registre des caractères génériques est facilement détectable car chaque requête recevra une réponse au lieu d'une « erreur de nom », même si le nom de domaine n'est pas valable.[55]Cela signifie qu'un utilisateur sera redirigé vers un nom de domaine similaire. Il apparaît que tous les opérateurs de nouveaux gTLD respectent cette sauvegarde.[56]

Pour se conformer aux quatre sauvegardes, il est demandé aux registres des nouveaux gTLD de retirer les enregistrements orphelins de type glue lorsqu'il est prouvé que de tels enregistrements ont fait l'objet d'une utilisation malveillante.[57] Les enregistrements orphelins de type glue absolus peuvent être utilisés à des fins malveillantes comme le fast-flux hébergeant les attaques d'un réseau zombie.[58] Cette exigence a pour but d'être réactive mais les opérateurs de registre peuvent rendre techniquement impossible l'existence des

[48] ICANN, « Tests de pré-délégation (PDT), » consulté le 2 février 2017, https://newgtlds.icann.org/en/applicants/pdt
[49] ICANN,« Contrat de registre, » consulté le 2 février 2017, https://www.icann.org/resources/pages/registries/registries-agreements-en, Spécification 6, Clause 1.3.
[50] Institut SANS, Document informatif mondial de certificat d'assurance, consulté le 2 février 2017, https://www.giac.org/paper/gcih/364/dns-spoofing-attack/103863. L'usurpation du DNS survient « lorsqu'un serveur du DNS accepte et utilise des informations fausses de la part d'un hôte qui n'a pas l'autorisation de divulguer ces informations » (p.16).
[51] Sooel Son et Vitaly Shmatikov, « Le guide pour les routards de l'empoisonnement du cache du DNS » (document présenté lors de la 6e conférence internationale ICST sur la sécurité et la confidentialité dans les réseaux informatique, Singapour, 7-9 septembre 2010), https://www.cs.cornell.edu/~shmat/shmat_securecomm10.pdf. L'empoisonnement du cache du DNS survient lorsque les données en cache temporaires stockées par un résolveur du DNS sont modifiées de manière intentionnelle pour procéder à des résolutions du DNS en des adresses IP acheminées vers des destinations non valides ou malveillantes (p.1).
[52] ICANN, « Rapport DNSSEC sur les TLD, » consulté le 26 avril 2017, http://stats.research.icann.org/dns/tld_report/. Cela n'inclut pas .aero.
[53] ICANN, « Contrat de registre », spécification 6, clause 2.2
[54] ICANN, « Formulaire de réclamation relative à l'interdiction des caractères génériques (redirection d'un domaine) », consulté le 2 février 2017, https://forms.icann.org/en/resources/compliance/registries/wildcard-prohibition/form.
[55] https://www.icann.org/groups/ssac/documents/sac-015-en
[56] Depuis le 1e janvier 2017, aucune réclamation n'a été rapportée par ce formulaire. Voir également le « Rapport sur le déploiement des DNSSEC », consulté le 1er janvier 2017https://rick.eng.br/dnssecstat/
[57] ICANN, « Contrat de registre », spécification 6, clause 4.1
[58] Comité consultatif sur la sécurité et la stabilité de l'ICANN (mars 2008), *Rapport consultatif du SSAC sur l'hébergement du fast-flux et le DNS*, consulté le 2 février 2017,https://www.icann.org/en/system/files/files/sac-025-en.pdf

enregistrements orphelins de type glue en premier lieu et certains l'ont fait. Depuis 2013, il n'y a eu aucune réclamation relative à la conformité de l'ICANN et liée aux enregistrements orphelins de type glue.[59]

Dans le cadre de la cinquième sauvegarde, les contrats de registre exigent des opérateurs de nouveaux gTLD qu'ils créent et conservent des enregistrements du WHOIS détaillé pour les enregistrements de noms de domaine. Cela signifie que les informations de contact du titulaire de nom de domaine, ainsi que les informations de contact technique et administratif, sont collectées et affichées en plus des données du WHOIS résumé au niveau du registre.[60] La conformité de l'ICANN veille activement au respect des exigences du WHOIS détaillé à la fois pour l'accessibilité et le format.[61] L'exactitude de la syntaxe et de l'exploitabilité est évaluée par le projet d'un système de signalement de problèmes liés à l'exactitude du WHOIS (ARS).[62] L'impact du chapitre sur les sauvegardes de ce rapport explique davantage l'ARS et les questions de conformité.

Les contrats de registre exigent également des opérateurs de registre de nouveaux gTLD qu'ils publient les détails de contact concernant les utilisations malveillantes sur leurs sites Web et qu'ils notifient à l'ICANN tout changement dans les informations de contact.[63] L'ICANN veille au respect de ces exigences et publie des statistiques, dont les mesures correctives dans son rapport trimestriel.[64] Les contrats de registre exigent des opérateurs de registre qu'ils traitent les réclamations fondées mais qu'ils n'imposent aucune procédure spécifique pour ce faire. En conséquence, il n'existe pas de norme sur laquelle le département chargé de la conformité de l'ICANN pourrait s'appuyer afin d'évaluer les moyens spécifiques utilisés par les opérateurs de registre afin de traiter les plaintes. Il y eut 55 réclamations liées aux données de contact concernant les utilisations malveillantes en 2016,[65] 61 en 2015,[66] 100 en 2014,[67] et 386 en 2013.[68]

Dans la sixième sauvegarde, il a été demandé aux opérateurs de nouveaux gTLD via le contrat de registre de rendre disponibles les fichiers de zone aux demandeurs approuvés via le service centralisé de données de zone.[69] Centraliser ces sources de données améliore la capacité pour les chercheurs en matière de sécurité, les avocats spécialisés en propriété intellectuelle, les responsables de l'application des lois, et d'autres demandeurs approuvés à évaluer les données sans avoir une relation contractuelle à chaque fois. Il y eut 19 réclamations liées au volume d'accès au fichier de zone en 2016,[70] 27 en 2015,[71] et 55 en

[59] ICANN, Rapports sur la conformité contractuelle,https://www.icann.org/resources/pages/compliance-reports-2016-04-15-en
[60] ICANN, « Que sont les entrées détaillées et résumées ? », consulté le 2 février 2017, https://whois.icann.org/en/what-are-thick-and-thin-entries
[61] ICANN, « contrat de registre » spécification 10 article 4
[62] ICANN, « Données du projet de système de signalement de problèmes liés à l'exactitude du WHOIS (ARS), consulté le 2 février 2017, https://whois.icann.org/en/whoisars
[63] ICANN, « contrat de registre » spécification 6 article 4,1
[64] ICANN, « Rapports 2016 sur la conformité contractuelle », consulté le 2 février 2017 https://www.icann.org/resources/pages/compliance-reports-2016-04-15-en
[65] https://www.icann.org/en/system/files/files/annual-2016-31jan17-en.pdf
[66] ICANN, « Rapports 2015 sur la conformité contractuelle », consulté le 2 février 2017 https://www.icann.org/resources/pages/compliance-reports-2016-04-15-en
[67] ICANN, « Rapports 2014 sur la conformité contractuelle », consulté le 2 février 2017 https://www.icann.org/resources/pages/compliance-reports-2014-2015-01-30-en
[68] ICANN, « Rapports 2013 sur la conformité contractuelle », consulté le 2 février 2017 https://www.icann.org/resources/pages/reports-2013-02-06-en
[69] ICANN, « Contrat de registre, » Spécification 4 article 2.1 ; ICANN, « Service centralisé de données de zone », consulté le 2 février 2017 https://czds.icann.org/en
[70] ICANN, « Rapports sur la conformité contractuelle de 2016. »
[71] ICANN, « Rapports sur la conformité contractuelle de 2015. »

2014.[72] Aucune donnée n'était disponible dans le rapport 2013 de l'ICANN sur la conformité contractuelle.

Pour améliorer la stabilité du DNS, l'ICANN a créé le processus accéléré de demande de dérogation pour incident de sécurité des registres (ERSR), qui permet aux registres « de demander une dérogation contractuelle pour les mesures qu'ils pourraient prendre ou qu'ils ont pris pour atténuer ou éliminer » un incident lié à la sécurité, imminent ou présent.[73] Depuis le 5 octobre 2016, l'ICANN rapporte que l'ERSR n'a été invoqué pour aucun nouveau gTLD.[74]

En plus des sauvegardes susmentionnées, l'ICANN en réponse à la participation de la communauté, a proposé la création d'un programme de vérification de zone de sécurité par lequel les opérateurs de registre gTLD pourraient volontairement créer des zones de haute sécurité.[75] Un groupe consultatif a mené des recherches approfondies pour déterminer les normes par lesquelles les registres pourraient être considérés comme une zone de haute sécurité. Toutefois, les propositions n'ont jamais atteint l'étape de mise en œuvre à cause d'une absence de consensus.

Les sauvegardes techniques, mises en œuvre via le département chargé de la conformité contractuelle, ont imposé des exigences aux registres et bureaux d'enregistrement des nouveaux gTLD qui ont soi-disant réduit les risques inhérents au développement du DNS. L'étude sur l'utilisation malveillante du DNS de la CCT-RT[76] cherche à déterminer si la mise en œuvre globale de ces sauvegardes a fait baisser les niveaux d'utilisations malveillantes du DNS par rapport aux anciens gTLD.

5.1.1 Étude sur l'utilisation malveillante du DNS

Pour préparer la révision de la CCT-RT sur « les sauvegardes mises en place pour réduire les problèmes impliqués dans…l'expansion » des gTLD, l'ICANN a émis un rapport analysant l'histoire des sauvegardes relatives à l'utilisation malveillante du DNS liées au programme des nouveaux gTLD.[77] Pour ce faire, le rapport a évalué les diverses façons de définir l'utilisation malveillante du DNS. Certaines difficultés liées à la définition de l'utilisation malveillante du DNS découlent des différentes façons qu'ont les juridictions de définir et traiter l'utilisation malveillante du DNS. Certaines activités sont qualifiées de malveillantes dans certaines juridictions mais pas dans d'autres. Certaines de ces activités, comme celles exclusivement ciblées sur les violations de propriété intellectuelle, sont interprétées de manière différente non seulement sur le fond mais aussi eu égard aux recours prévus selon la juridiction concernée. Autre difficulté : le manque de données disponibles concernant certains types d'utilisations malveillantes. Néanmoins, il y a un noyau dur de comportements techniques malveillants pour lesquels il existe à la fois un consensus et de précieuses données. On peut citer le spam, l'hameçonnage, la dissémination de programmes malveillants et la commande et le contrôle de réseaux zombies.

[72] ICANN, « Rapports sur la conformité contractuelle de 2014. »
[73] ICANN, « Processus accéléré de demande de dérogation pour incident de sécurité des registres », consulté le 2 février 2017https://www.icann.org/resources/pages/ersr-2012-02-25-en.
[74] Services de registre de l'ICANN, discussion par courrier électronique avec l'équipe de révision, juillet 2017.
[75] ICANN (18 novembre 2009), *Un modèle pour un programme de vérification de zone de haute sécurité*, consulté le 2 février 2017, https://archive.icann.org/en/topics/new-gtlds/high-security-zone-verification-04oct09-en.pdf; icann.org, « Commentaires publics : Rapport final sur les zones TLD de haute sécurité », 11 mars 2011, https://www.icann.org/news/announcement-2011-03-11-en
[76] ICANN, *Appel à propositions*. SIDN Labs et Delft University of Technology,« Utilisation malveillante du DNS dans les gTLD ».
[77] ICANN, *Sauvegardes du programme des nouveaux gTLD* (2016).

Le rapport de l'ICANN a reconnu l'absence d'une étude globale sur l'utilisation malveillante du DNS comparant les nouveaux gTLD et les anciens gTLD. Néanmoins, certains indicateurs suggèrent qu'un pourcentage élevé des nouveaux gTLD pourrait être victime d'une utilisation malveillante du DNS. Par exemple, l'organisation Spamhaus classe toujours les nouveaux gTLD dans sa liste « Top 10 des domaines de premier niveau les plus victimes d'utilisations malveillantes » à partir du ratio entre le nombre de noms de domaine associés aux utilisations malveillantes et le nombre de noms de domaine vus au sein d'une zone.[78] Attendu que, en utilisant une méthodologie différente, les recherches précédentes d'Architelos et du groupe de travail anti-hameçonnage ont désigné .com le TLD ayant le plus grand nombre de noms de domaine associés à des utilisations malveillantes.[79] Un rapport de 2017 de PhishLabs a également montré que la moitié des sites d'hameçonnage sont dans la zone .com, dont 2 % de nouveaux gTLD.[80] Cependant, le même rapport a également conclu que les sites d'hameçonnage dans les zones de nouveaux gTLD ont augmenté de 1 000 % depuis l'année dernière. Ceci semble avoir coïncidé avec une augmentation globale des attaques d'hameçonnage pendant l'année 2016.[81]

Les noms de domaine sont souvent une composante majeure de la cybercriminalité et permettent aux cybercriminels de rapidement adapter leur infrastructure.[82] Par exemple, les campagnes de spam correspondent souvent avec l'hameçonnage et d'autres cybercrimes.[83] Les noms de domaine sont également utilisés pour faciliter la dissémination de programmes malveillants ainsi que la commande et le contrôle de réseaux zombies. Des statistiques et des incidents troublants observés par les opérateurs réseaux amènent à penser que de nombreux nouveaux gTLD ne proposent rien d'autre qu'une utilisation malveillante.[84] En réalité, certaines compagnies de sécurité Internet ont conseillé aux clients de bloquer tout le trafic du réseau vers des TLD spécifiques.[85] De telles pratiques vont à l'encontre des efforts d'acceptation universelle de l'ICANN. Attendu que, au-delà des sauvegardes, les mesures pour lutter contre les utilisations malveillantes de noms de domaine varient énormément

[78] Spamhaus, « Les TLD les plus victimes d'utilisations malveillantes au niveau mondial, » consulté le 2 février 2017, https://www.spamhaus.org/statistics/tlds/

[79] Le groupe de travail anti-hameçonnage (29 avril 2015), *Rapport sur l'évolution des activités d'hameçonnage : 4e trimestre 2014, consulté le 2 février 2017,* http://docs.apwg.org/reports/apwg_trends_report_q4_2014.pdf; Architelos (juin 2015), *Rapport du NameSentry℠ sur l'utilisation malveillante : L'état de l'utilisation malveillante des nouveaux gTLD,* consulté le 2 février 2017,http://domainnamewire.com/wp-content/Architelos-StateOfAbuseReport2015.pdf

[80] PhishLabs, rapport 2017 sur les renseignements et les tendances de l'hameçonnage, p. 23-24, https://pages.phishlabs.com/rs/130-BFB-942/images/2017%20PhishLabs%20Phishing%20and%20Threat%20Intelligence%20Report.pdf. Les nouveaux gTLD représentaient 8 % de l'ensemble du marché des TLD lorsque .tk était exclu de l'ensemble des données. Voir Kevin Murphy, l'hameçonnage dans les nouveaux gTLD à la hausse de 1 000 % mais .com est toujours le pire, Domain Incite, 20 février 2017 http://domainincite.com/21552-phishing-in-new-gtlds-up-1000-but-com-still-the-worst

[81] Lindsey Havens, APWG & Kaspersky confirme les conclusions du rapport sur les renseignements et les tendances de l'hameçonnage, 2 mars, 2017, disponible sur https://info.phishlabs.com/blog/apwg-kaspersky-research-confirms-phishing-trends-investigations-report-findings; Darya Gudkova, et. al., le spam et l'hameçonnage en 2016, bulletin de sécurité, 20 février 2017, disponible surhttps://securelist.com/kaspersky-security-bulletin-spam-and-phishing-in-2016/77483/; APWG, Rapport sur les tendances de l'hameçonnage, 23 février 2017, disponible sur http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf

[82] Symantec (avril 2015), Rapport sur la menace de la sécurité Internet, consulté le 2 février 2017, https://its.ny.gov/sites/default/files/documents/symantec-internet-security-threat-report-volume-20-2015-social_v2.pdf

[83] Richard Clayton, Tyler Moore, et Henry Stern, « Corrélations temporaires entre le spam et les sites d'hameçonnage » (document présenté lors de la procédure LEET'09 de la 2e conférence USENIX sur les exploits à grande échelle et les nouvelles menaces, Boston, MA, 21 avril 2009) https://www.cl.cam.ac.uk/~rnc1/leet09.pdf.

[84] Tom Henderson, Les nouveaux domaines Internet sont un terrain vague, Network World, 5 juillet 2016, http://www.networkworld.com/article/3091754/security/the-new-internet-domains-are-a-wasteland.html

[85] Dans un rapport de 2015, Blue Coat a conseillé aux opérateurs réseaux de bloquer tout le trafic vers ou depuis « .work, .gq, .science, .kim and .country ». Voir Blue Coat, NE PAS ENTRER : la recherche de Blue Coat cartographie les environnements les plus suspects du Web, septembre 2015, p. 7, disponible sur https://www.bluecoat.com/documents/download/895c5d97-b024-409f-b678-d8faa38646ab

entre les registres et les bureaux d'enregistrement. Certaines entités n'agissent pas avant la réception d'une plainte. En revanche, d'autres bureaux d'enregistrement prennent des mesures proactives pour vérifier les informations d'identification d'un titulaire de nom de domaine, bloquer les chaînes de noms de domaine similaires à des cibles d'hameçonnage connues, et examiner les revendeurs de noms de domaine qui ne sont pas des parties contractantes de l'ICANN..[86]

À la lumière de l'environnement dynamique du DNS, les aperçus des utilisations malveillantes relatives aux nouveaux gTLD ne tiennent pas compte de la variété des règles d'enregistrement et des sauvegardes dans les centaines de nouveaux gTLD ayant été délégués depuis 2013. En conséquence, il est difficile d'établir des différences nettes entre les taux de malveillance au sein des nouveaux et des anciens gTLD sans réaliser une évaluation complète. Dans la mesure du possible, la CCT-RT a cherché à évaluer la capacité des sauvegardes techniques développées pour le programme des nouveaux gTLD à réduire les diverses formes d'utilisations malveillantes du DNS. Dans le cadre de ce processus, la CCTRT a demandé que soit menée une étude complète sur l'utilisation malveillante du DNS afin d'analyser les niveaux de malveillance[87] au sein des nouveaux et des anciens gTLD, d'alimenter cette révision et d'éventuellement servir de base pour de futures analyses.[88]Le vendeur choisi par l'ICANN, une équipe commune composée de chercheurs de la Delft University of Technology (TU Delft) aux Pays-Bas et de la Fondation pour l'enregistrement de domaines Internet aux Pays-Bas (SIDN), a livré un rapport final le 9 août 2017.[89]

Méthodologie de l'étude sur l'utilisation malveillante du DNS

L'étude sur l'utilisation malveillante du DNS repose sur des fichiers de zone, des enregistrements WHOIS, et 11 listes noires de noms de domaine alimentées pour calculer le taux d'utilisations malveillantes techniques du DNS du 1er janvier 2014[90] au 31 décembre 2016.

L'analyse comprend :

1. le nombre total de noms de domaine malveillants par TLD et bureau d'enregistrement du 1er janvier 2014 au 31 décembre 2016 en prenant en compte la période d'enregistrement prioritaire et les dates de disponibilité générale pour l'enregistrement
2. les taux de malveillance, basés sur un nombre de domaines malveillants pour 10 000 noms de domaine (facteur de normalisation à prendre en compte pour les différentes tailles de TLD), par gTLD et bureau d'enregistrement du 1er janvier 2014 au 31 décembre 2016.
3. les utilisations malveillantes associées à des services d'anonymisation et d'enregistrement fiduciaire
4. les lieux géographiques associés aux activités d'utilisations malveillantes
5. les taux d'utilisations malveillantes catégorisés selon les domaines « enregistrés par malveillance » par rapport aux domaines « compromis ».

[86] Secure Domain Foundation, Le coût de l'inaction, juin 2015, p. 8, https://securedomain.org/Documents/SDF_Report1_June_2015.pdf; Les bureaux d'enregistrement doivent imposer des obligations contractuelles de baisse des flux aux revendeurs avec lesquels ils sont sous contrat. Cependant, les revendeurs ne sont pas accrédités par l'ICANN. Voir le contrat d'accréditation de bureau d'enregistrement, 3.12, Obligations concernant la fourniture de services aux bureaux d'enregistrement par des tiers

[87] Hameçonnage, programme malveillant, et spam. À la base, l'équipe de révision a cherché à inclure les domaines en réseau zombie dans l'analyse. Cependant, les données historiques concernant le réseau zombie n'étaient pas disponibles au moment de l'étude. Néanmoins, les noms de domaine associés à un réseau zombie (hébergement et commande et contrôle) étaient inclus dans la liste de noire des programmes malveillants.

[88] ICANN, Appel à propositions.

[89] SIDN Labs et Delft University of Technology,« Utilisation malveillante du DNS dans les gTLD ».

[90] Les premières délégations de nouveaux gTLD ont commencé en octobre 2013.

6. Une analyse statistique inférentielle sur les effets des indicateurs et les propriétés structurelles des nouveaux gTLD (c'est-à-dire le nombre de noms de domaine signés au niveau du DNSSEC, de noms de domaine en parking, du nombre de noms de domaine dans chaque nouveau gTLD, ainsi que le nombre de noms de domaine qui résolvent du contenu)

Conclusions de l'étude sur l'utilisation malveillante du DNS

Le rapport apporte des conclusions très importantes concernant l'utilisation malveillante du DNS associée aux nouveaux gTLD par rapport aux anciens gTLD. De manière générale, l'étude sur l'utilisation malveillante du DNS montre que l'introduction des nouveaux gTLD n'a pas augmenté le nombre total d'utilisations malveillantes pour l'ensemble des gTLD. Néanmoins, les résultats montrent que les neuf sauvegardes susmentionnées seules ne garantissent pas un taux inférieur d'utilisations malveillantes dans chaque nouveau gTLD par rapport aux anciens gTLD. Au contraire, des facteurs comme les restrictions d'enregistrement, le prix et les pratiques spécifiques aux bureaux d'enregistrement semblent plus susceptibles d'avoir un impact sur le taux d'utilisations malveillantes.[91]

L'utilisation malveillante se déplace vers les nouveaux gTLD

Les anciens gTLD représentent toujours le plus d'enregistrements de noms de domaine et peut-être, en conséquence, un plus grand volume d'hameçonnage, de programmes malveillants associés aux noms de domaine.[92] Néanmoins, le taux global d'utilisations malveillantes dans les anciens et les nouveaux gTLD était le même à la fin de l'année 2016, et les tendances varient selon les types d'utilisations malveillantes. Par exemple, fin 2016, le nombre de spams dans les enregistrements d'anciens gTLD a baissé alors que les nouveaux gTLD ont connu une augmentation importante. Au dernier trimestre 2016, 56,9 sur 10 000 noms de domaine enregistrés auprès d'anciens gTLD étaient sur la liste noire des spams alors que le taux de noms de domaine auprès de nouveaux gTLD était de 526,6 pour 10 000 enregistrements.[93]

Certaines tendances d'utilisations malveillantes ont montré un doublon. Les cinq premiers anciens gTLD ayant le taux le plus élevé d'hameçonnage ont également le taux le plus élevé de noms de domaine liés à la distribution de programmes malveillants.[94] Les taux d'hameçonnage et de programmes malveillants dans les anciens gTLD étaient le plus souvent le résultat de noms de domaine enregistrés par compromis plutôt que d'enregistrements malveillants. Les taux de noms de domaine enregistrés par compromis auprès d'anciens gTLD sont beaucoup plus élevés que pour les nouveaux gTLD.

En ce qui concerne la distribution de programmes malveillants,[95] les 5 nouveaux gTLD ayant le taux le plus élevé de noms de domaine malveillants étaient .top, .wang, .win, .loan, et .xyz. Depuis fin 2015, le TLD .top a eu le plus grand nombre d'enregistrements abusifs pour l'ensemble des anciens et nouveaux gTLD.[96] Chacun de ces TLD proposait un tarif d'enregistrement bas, en général plus bas que pour un enregistrement .com.

L'étude sur l'utilisation malveillante du DNS fait une distinction entre les noms de domaine enregistrés spécifiquement à des fins malveillantes et ceux enregistrés à des fins légitimes

[91] P.24-25
[92] P.24
[93] p.24
[94] p.12
[95] Basé sur les données de StopBadware
[96] p.13

qui ont été par la suite compromis.[97] Les résultats de l'étude montrent que l'introduction des nouveaux gTLD correspondait avec une baisse du nombre de spams associés à des enregistrements auprès d'anciens gTLD, alors que les enregistrements malveillants ont augmenté auprès de nouveaux gTLD.[98] Ajouté au fait que le nombre total d'enregistrements de spams reste stable[99] , cela suggère peut-être que les personnes malveillantes sont en train de passer à des enregistrements de noms de domaine auprès de nouveaux gTLD. Au sein de cette tendance on constate des nouveaux gTLD spécifiques qui servent de cibles principales pour des enregistrements abusifs et ceci est soit dû à des politiques d'enregistrements et d'application de la loi négligentes ou à des prix faibles. En réalité, certains bureaux d'enregistrement sont presque entièrement associés à des enregistrements abusifs plutôt qu'à des enregistrements légitimes.

L'utilisation malveillante n'est pas générale dans les nouveaux gTLD

Même si l'utilisation malveillante prend de l'ampleur dans les nouveaux gTLD, ce n'est en aucun cas une tendance prédominante pour l'ensemble des nouveaux gTLD. Au contraire, fin 2016, ce phénomène était très ciblé. Les cinq nouveaux gTLD souffrant de la plus haute concentration de noms de domaine utilisés dans des attaques d'hameçonnage (APWG, dernier trimestre 2016), comptaient pour 58,7 % de l'ensemble des noms de domaine sur liste noire.[100] Alors que, Spamhaus a mis sur liste noire au moins 10 % de tous les noms de domaine enregistrés auprès de 15 nouveaux gTLD. Néanmoins, environ un tiers de l'ensemble des nouveaux gTLD ne comptaient pas un seul cas d'utilisation malveillante, comme signalisé sur les listes noires, pour le dernier trimestre 2016.

Deux bureaux d'enregistrement mis en évidence par l'étude ont eu des taux d'utilisations malveillantes accablants. Situation inquiétante, plus de 93 % des enregistrements de nouveaux gTLD vendus par Nanjing Imperiosus Technology, basé en Chine, apparaissaient sur la liste de noire de SURBL. Pendant la plus grande partie de l'année 2016, les taux d'utilisations malveillantes associés à ce bureau d'enregistrement ont nettement augmenté. L'ICANN a finalement suspendu Nanjing en janvier 2017 en invoquant le non-respect du RAA.[101] Cependant, les taux élevés, prolongés, intenses n'étaient pas le motif exploitable.

Un autre bureau d'enregistrement, Alpnames Ltd., basé à Gibraltar, avait un volume élevé d'utilisations malveillantes des noms de domaine .science et .top. L'étude note que ce bureau d'enregistrement a utilisé des promotions sur les prix proposés pour l'enregistrement de noms de domaine à 1 $ USD ou même parfois gratuit.[102] De plus, Alpnames a permis à des titulaires de noms de domaine de générer et d'enregistrer au hasard 2 000 noms de domaine au sein de 27 nouveaux gTLD lors d'un processus unique d'enregistrement. Les noms de domaine en vrac utilisant des algorithmes de génération de domaines sont souvent associés à des cas de cybercriminalité.[103] Au moment de ce rapport, Alpnames était toujours accrédité par l'ICANN.

De nombreuses caractéristiques peuvent jouer un rôle dans le volume ou les taux d'utilisations malveillantes au sein d'un TLD particulier. En matière de valeur absolue, les nouveaux gTLD ne sont pas différents des anciens gTLD, plus la valeur du TLD est grande

[97] Les noms de domaine compromis incluent des noms de domaine pour lesquels l'enregistrement ou le site Web peuvent avoir été piratés.
[98] p. 2
[99] Voir l'étude sur l'utilisation malveillante du DNS, illustrations 24, 36 et 38 correspondant au nombre total de noms de domaine victimes de spams pour différents spams alimentés
[100] P.11
[101] https://www.icann.org/uploads/compliance_notice/attachment/895/serad-to-hansmann-4jan17.pdf
[102] p.20
[103] Aditya K. Sood, Sherali Zeadally, « Une taxonomie des algorithmes de génération de domaines », Sécurité et confidentialité de l'IEE, vol. 14, no. , pp. 46-53, Juillet-Août. 2016, doi:10.1109/MSP.2016.76

plus le nombre total de noms de domaine associés à des utilisations malveillantes est élevé.[104] Attendu que, en analysant les caractéristiques des opérateurs de registre de TLD, l'étude montre que beaucoup d'opérateurs liés aux taux les plus élevés d'utilisations malveillantes offraient des prix bas pour l'enregistrement de noms de domaine.

L'étude a conclu que les noms de domaine enregistrés à des fins malveillantes contenaient souvent des chaînes en lien avec les termes de marques déposées.[105] Plus précisément, sur les 88 noms de domaine .top associés à des utilisations malveillantes pour le quatrième trimestre de 2015, 75 d'entre eux contenaient des versions exactes ou mal orthographiées de Apple, iCloud ou iPhone, laissant entendre que les noms de domaine ont été utilisés lors d'une campagne d'hameçonnage contre les utilisateurs des produits et services Apple, Inc.

L'étude était statistiquement faible mais a mis en évidence une corrélation positive entre le nombre de domaines en parking au sein des nouveaux gTLD et le taux d'utilisation malveillante.[106] Curieusement, il y avait également une corrélation positive faible entre le nombre de noms de domaine signés du DNSSEC et les utilisations malveillantes dans une zone de nouveaux gTLD.[107] L'utilisation de services d'enregistrement fiduciaire/d'anonymisation pour masquer les données WHOIS des titulaires de noms de domaine est plus commune au sein des anciens que des nouveaux gTLD. Dans tous les cas, l'étude n'a pas mis en évidence de lien statistique significatif entre l'utilisation de ces services et l'utilisation malveillante du nom de domaine. Par-dessus tout, l'étude a identifié une corrélation assez forte entre les politiques de restriction des enregistrements et les taux faibles d'utilisations malveillantes. Néanmoins, même les nouveaux gTLD avec des politiques d'enregistrement ouvertes ont des taux d'utilisations malveillantes variables, ce qui suggère que parmi d'autres variables clés comme le prix, les différences de pratiques anti-abus entre les registres et les bureaux d'enregistrement peuvent également influencer les taux.

L'utilisation malveillante du DNS n'est pas aléatoire

Les restrictions de prix et d'enregistrements semblent avoir un impact sur le choix du bureau d'enregistrement et du registre que vont faire les cybercriminels pour une utilisation malveillante du DNS, les noms de domaine avec des prix bas et faciles à enregistrer étant des vecteurs d'attaque attractifs.[108] Néanmoins, les mêmes qualités peuvent être intéressantes pour les titulaires de noms de domaine ayant des intérêts légitimes et qui veulent un Internet libre et ouvert. En conséquence, les avantages financiers peuvent exister pour les opérateurs de registre et bureaux d'enregistrement afin d'empêcher une utilisation malveillante du DNS générale en contrôlant proactivement les enregistrements et en détectant des délits. Par exemple, il existe un précédent où l'ICANN a ajusté sa structure de tarifs pour répondre aux comportements préjudiciables au DNS comme l'abolissement des remboursements de frais pour les échantillons de noms de domaine.[109] De la même manière, l'équipe de révision CCT propose de développer des conditions favorables pour récompenser les meilleures pratiques de prévention de l'utilisation malveillante du DNS et pour renforcer les conséquences de comportements fautifs ou complaisants. Ces recommandations peuvent entrer en vigueur afin de réduire les abus de noms de domaine dans la mesure où la communauté parvient à un consensus sur d'autres formes d'utilisations malveillantes du DNS.

[104] p.15
[105] p. 12
[106] p.16
[107] p.16
[108] p. 25
[109] http://www.washingtonpost.com/wp-dyn/content/article/2008/01/30/AR2008013002178.html

Nous sommes inquiets des taux élevés d'utilisations malveillantes du DNS qui se concentrent au sein d'un nombre assez faible de registres et de bureaux d'enregistrement et de régions géographiques ; cette utilisation malveillante du DNS semble avoir été sans réponse dans certains cas pendant une longue période.

Les recommandations 1 à 5 visent à répondre à la réalité du fait que les sauvegardes de nouveaux gTLD n'ont pas, en tant que telles, empêcher l'utilisation malveillante technique du DNS. En plus des moyens disponibles aujourd'hui pour prévenir et atténuer les risques d'utilisations malveillantes du DNS, nous proposons de nouvelles motivations et de nouveaux outils pour combattre les abus qui vont :

- encourager et favoriser les mesures anti-malveillance en vertu de la recommandation 1
- introduire des mesures pour empêcher l'utilisation malveillante technique du DNS en vertu de la recommandation 2
- garantir que la collecte des données s'effectue et répond à la recommandation 3
- prendre en considération un mécanisme supplémentaire où malgré les recommandations 1, 2 et 3, les opérateurs de registre ou les bureaux d'enregistrement n'ont pas réellement empêché l'utilisation malveillante technique du DNS. Un processus de règlement de litiges devrait être pris en considération pour permettre aux parties lésées de prendre des mesures en vertu de la recommandation 4 (à noter qu'il n'y a pas de consensus de l'équipe de révision. Voir déclaration de la minorité en annexe 6). En effet, il faudrait insister davantage sur la conformité de l'ICANN et lorsqu'un nettoyage a été identifié comme étant nécessaire. Si le niveau d'utilisation malveillante n'a pas baissé conformément à l'engagement du registre, alors le fait que la partie contractante ne mette pas en œuvre le plan devrait être considéré comme une violation du RAA/RA. Si le niveau d'obligation est celui-ci, alors non seulement la DADRP devient moins nécessaire mais elle sera même probablement moins utilisée. Cela se traduit par des résultats positifs pour toutes les parties car on verra une baisse de l'utilisation malveillante du DNS.

Recommandation A : Prendre en considération les dirigeants de l'organisation de l'ICANN, dans leurs discussions avec les registres pour négocier des amendements aux contrats de registre existants, ou dans les négociations des nouveaux contrats de registre liés aux futures séries de nouveaux gTLD, afin d'inclure des dispositions visant à apporter des incitations, y compris des incitations financières aux registres et en particulier aux registres ouverts, afin d'adopter des mesures anti-malveillance proactives.[110]

[110] La CCTRT cherche des exemples illustrant des pratiques qui pourraient aider à réduire l'utilisation malveillante de manière proactive. Un exemple a été proposé par EURid, l'opérateur de registre de l'UE, qui testera prochainement un système de délégation différée. Voirhttps://eurid.eu/en/news/eurid-set-to-launch-first-of-its-kind-domain-name-abuse-prevention-tool/ et https://eurid.eu/media/filer_public/9e/d1/9ed12346-562d-423d-a3a4-bcf89a59f9b4/eutldecosystem.pdf. Ce processus n'empêchera pas les enregistrements mais pourra retarder l'activation d'un enregistrement si un nom de domaine est identifié comme étant potentiellement malveillant par des algorithmes d'apprentissage automatique. Les prochaines équipes de révision pourraient étudier cette mesure et prendre en compte son efficacité et savoir si elle pourrait servir de modèle innovant pour aider à favoriser la confiance et un environnement en ligne sécurisé. De plus, le registre .XYZ peut apporter un autre exemple de mesures proactives pour lutter contre les malveillances. Le registre .XYZ prétend avoir une politique zéro-tolérance face aux activités malveillantes affectant .xyz ou tout autre extension de domaine, en utilisant un outil élaboré de surveillance des abus permettant un contrôle proactif et une détection quasi en temps réel, suspendant les domaines engagés dans toute activité de malveillance. Les prochaines équipes de révision pourraient étudier l'efficacité de cette approche en examinant les taux de malveillance au fil du temps et en comparant les niveaux avant et après cette politique.

Fondements/conclusions connexes : Les sauvegardes des nouveaux gTLD seules ne permettent pas d'empêcher l'utilisation malveillante technique du DNS. Les taux d'utilisations malveillantes sont corrélés aux prix des enregistrements de noms de domaine ainsi qu'aux restrictions d'enregistrement imposées aux titulaires de noms de domaine. Certains registres sont en soi conçus avec des politiques d'enregistrement strictes et/ou des prix élevés. Cependant, un Internet libre, ouvert et accessible comprendra toujours des registres avec des politiques d'enregistrement ouvertes et des prix bas qui doivent adopter d'autres mesures pour empêcher l'utilisation malveillante du DNS. Les registres qui n'imposent pas de restrictions d'enregistrement peuvent réduire l'utilisation malveillante du DNS avec des moyens proactifs comme l'identification des récidivistes, la surveillance d'enregistrements suspects, et la détection active d'abus et ne pas simplement attendre que des plaintes soient déposées. En conséquence, l'ICANN devrait favoriser et récompenser la mise en œuvre de mesures anti-malveillance par ces opérateurs de registre afin de réduire l'utilisation malveillante technique du DNS au sein des gTLD ouverts.

A: Le Conseil d'administration de l'ICANN, le groupe des représentants des opérateurs de registre, le groupe des représentants des bureaux d'enregistrement, l'organisation de soutien aux extensions génériques et le groupe de travail PDP consacré aux procédures futures.

Condition préalable ou niveau de priorité : élevée

Consensus au sein de l'équipe : oui

Détails : Le Conseil d'administration devrait envisager d'encourager l'ICANN à négocier avec des registres pour inclure dans les contrats de registre des réductions disponibles pour les opérateurs de registre ayant des politiques d'enregistrement ouvertes qui mettent en œuvre des mesures proactives visant à empêcher l'utilisation malveillante technique du DNS au sein de leur zone.

Recommandation B : Prendre en considération les dirigeants de l'organisation de l'ICANN, dans leurs discussions avec les bureaux d'enregistrement et les registres pour négocier des amendements aux contrats d'accréditation de bureau d'enregistrement et aux contrats de registre afin qu'ils intègrent des dispositions visant à empêcher une utilisation systémique de bureaux d'enregistrement spécifiques pour l'utilisation malveillante technique du DNS.

Fondements/Conclusions connexes : Les politiques actuelles sont axées sur les plaintes individuelles relatives à l'utilisation malveillante. Cependant, les bureaux d'enregistrement et les opérateurs de registre associés à un taux très élevé d'utilisation malveillante du DNS continuent d'opérer et font face à de légères mesures incitatives pour empêcher l'utilisation malveillante technique du DNS. De plus, il existe actuellement quelques mécanismes d'application pour empêcher les abus systémiques de noms de domaine associés à des revendeurs. L'utilisation systémique de bureaux d'enregistrement et de registres particuliers pour l'utilisation malveillante du DNS menace la sécurité et la stabilité du DNS, l'acceptation universelle des TLD et la confiance du consommateur.

À : Le Conseil d'administration de l'ICANN, le groupe des représentants des opérateurs de registre, le groupe des représentants des bureaux d'enregistrement, l'organisation de soutien aux extensions génériques et le groupe de travail PDP consacré aux procédures futures.

Condition préalable ou niveau de priorité : élevée

Consensus au sein de l'équipe : oui

Détails : Le Conseil d'administration devrait prendre en compte les dirigeants de l'ICANN pour négocier des amendements aux dispositions du contrat d'accréditation de bureau d'enregistrement et du contrat de registre visant à empêcher une utilisation systémique de bureaux d'enregistrement spécifiques pour l'utilisation malveillante technique du DNS. Une telle formulation devrait être imposée aux bureaux d'enregistrement ainsi qu'à leurs entités affiliées comme les revendeurs, une obligation visant à empêcher l'utilisation malveillante du DNS par laquelle l'ICANN peut suspendre un bureau d'enregistrement et un opérateur de registre qui sont associés à des taux intenses, anormaux et très élevés d'utilisations malveillantes techniques. L'ICANN doit baser ces conclusions sur plusieurs sources fiables vérifiables et ces conclusions peuvent être réfutées par le bureau d'enregistrement avec une preuve suffisante de leur inexactitude. Les facteurs suivant peuvent être pris en compte lors de la prise de décisions : le bureau d'enregistrement ou l'opérateur de registre 1) s'engage dans des mesures anti-malveillance proactives pour empêcher l'utilisation malveillante technique du DNS, 2) a lui-même été une victime dans le cas correspondant, 3) a depuis pris des mesures nécessaires et appropriées pour stopper les malveillances et empêcher l'utilisation systémique future de ses services à des fins d'utilisations malveillantes techniques du DNS.

Recommandation C : Une étude plus approfondie a été menée sur la relation entre des opérateurs de registre, des bureaux d'enregistrement spécifiques et l'utilisation malveillante du DNS en demandant une collecte continue de données, y compris mais sans s'y limiter, des initiatives de signalement des cas d'utilisations malveillantes des noms de domaine (DAAR). À des fins de transparence, ces informations devraient être régulièrement publiées de façon à pouvoir identifier les registres et bureaux d'enregistrement qui ont besoin d'un examen plus approfondi et pour lesquels le département de la conformité de l'ICANN doit en faire une priorité. En identifiant des phénomènes de malveillance, l'ICANN devrait mettre en place un plan d'action pour répondre à ces études, remédier aux problèmes identifiés, et définir une future collecte de données.

Fondements/Conclusions connexes : L'étude sur l'utilisation malveillante du DNS demandée par la CCT-RT a identifié des taux très élevés de malveillance associée à des registres et bureaux d'enregistrement spécifiques ainsi qu'à des caractéristiques d'enregistrement, comme les enregistrements de masse, qui semblent favoriser les comportements malveillants. De plus, l'étude a conclu que les prix et les restrictions d'enregistrement coïncident avec des malveillances, ce qui signifie qu'il existe de nombreux facteurs à prendre en compte afin d'extrapoler les tendances de malveillance à travers les TLD pour des opérateurs de registre et des bureaux d'enregistrement spécifiques. L'étude sur l'utilisation malveillante du DNS a mis en évidence certains comportements qui vont complètement à l'encontre de la confiance du consommateur dans le DNS. Certains registres et bureaux d'enregistrement semblent encourager ou au contraire ignorer délibérément la question de l'utilisation malveillante du DNS. Ces comportements doivent être identifiés rapidement et des mesures doivent être prises par le département de la conformité de l'ICANN.

À : Le Conseil d'administration de l'ICANN, le groupe des représentants des opérateurs de registre, le groupe des représentants des bureaux d'enregistrement, l'organisation de soutien aux extensions génériques et le groupe de travail PDP consacré aux procédures futures, la deuxième équipe de révision de la sécurité, la stabilité et la résilience du DNS.

Condition préalable ou niveau de priorité : élevée

Consensus au sein de l'équipe : oui

Détails : Des études supplémentaires doivent être réalisées en continue, collectant des données utiles concernant l'utilisation malveillante du DNS à la fois au niveau du bureau d'enregistrement et du registre. Les données devraient être régulièrement publiées, permettant ainsi à la communauté et au département de conformité de l'ICANN en particulier d'identifier les registres et bureaux d'enregistrement qui doivent être soumis à un examen de conformité plus approfondi et éradiquer ainsi de tels comportements.

Recommandation D : Une politique de règlement de litiges relatifs à l'utilisation malveillante du DNS (DADRP) doit être envisagée par la communauté afin de traiter les opérateurs de registre et bureaux d'enregistrement qui sont identifiés comme ayant des niveaux excessifs de malveillance (à définir, p.ex., plus de 10 % de leurs noms de domaine sont sur une liste noire). En premier lieu, il s'agirait de demander à ces opérateurs de registre et bureaux d'enregistrement de a) expliquer la situation au département de conformité de l'ICANN, b) s'engager à changer ces comportements dans un délai précis, et/ou d'adopter des politiques d'enregistrement strictes dans un délai précis. Une DADRP sera mise en place si l'ICANN ne prend pas elle-même les mesures nécessaires.

Fondements/Conclusions connexes : L'étude sur l'utilisation malveillante du DNS demandée par la CCT-RT a identifié des taux très élevés d'utilisations malveillantes associées à des registres spécifiques. Il est important d'avoir un mécanisme pour gérer ces cas d'utilisations malveillantes et en particulier s'ils sont courants chez certains registres. Les comportements malveillants doivent être éradiqués du DNS et cela donnerait une arme supplémentaire pour combattre ces abus.

À : Le Conseil d'administration de l'ICANN, le groupe des représentants des opérateurs de registre, le groupe des représentants des bureaux d'enregistrement, l'organisation de soutien aux extensions génériques et le groupe de travail PDP consacré aux procédures futures, la deuxième équipe de révision de la sécurité, la stabilité et la résilience du DNS.

Condition préalable ou niveau de priorité : élevée

Consensus au sein de l'équipe : Consensus à la majorité pas à l'unanimité (voir déclaration de la minorité en annexe 6.1 Déclarations des minorités)

Détails : Le département de la conformité de l'ICANN est un moyen de traiter les taux élevés d'utilisations malveillantes du DNS, en appliquant les amendements existants ainsi que tout autre amendement au contrat d'accréditation de bureau d'enregistrement afin d'empêcher l'utilisation systémique de bureaux d'enregistrement spécifiques pour une utilisation malveillante du DNS conformément à la recommandation 2. Cependant, une DADRP spécifique devrait être envisagée car elle pourrait aussi être très utile dans le traitement des cas d'utilisations malveillantes du DNS, servir également d'effet dissuasif significatif et aider à prévenir ou réduire ces taux élevés d'utilisations malveillantes du DNS. Les opérateurs de registre et les bureaux d'enregistrement qui sont identifiés comme ayant des taux élevés de malveillance (à définir, par exemple lorsqu'un opérateur de registre a plus de 10 % de noms de domaine sur liste noire plus ou moins hétérogène selon : StopBadware SDP, APWG, Spamhaus, Secure Domain Foundation, SURBL et CleanMX). Une DADRP devrait établir des sanctions spécifiques. Exemples provenant de l'étude sur l'utilisation malveillante du DNS de nouveaux gTLD ayant plus de 10 % de leurs noms de domaine sur liste noire, selon Spamhaus : .SCIENCE (51 %), .STREAM (47 %) .STUDY (33 %) .DOWNLOAD (20 %) .CLICK (18 %) .TOP (17 %) .GDN (16 %) .TRADE (15 %) .REVIEW (13 %) et .ACCOUNTANT (12 %). Par conséquent, ces registres devraient être obligés d'examiner leurs noms de domaine au second niveau utilisés dans des cas d'utilisations malveillantes du DNS et expliquer pourquoi, s'engager à rétablir tout ça dans

un délai précis, et adopter des politiques d'enregistrement plus strictes pour garantir qu'il existe des obligations contractuelles pertinentes pour gérer de manière efficace ces enregistrements. Si les noms de domaine en question ne sont pas rétablis de manière satisfaisante, et si l'ICANN ne prend pas des mesures immédiates, alors une partie affectée pourrait faire appel à une DADRP. Le processus devrait impliquer une plainte écrite au registre, un temps de réponse alloué au registre, et un entretien oral. La décision finale devrait être prise par un panel d'experts qui pourrait être en mesure de recommander un ou plusieurs mécanismes d'application à convenir avec la communauté.

Aux fins de cette recommandation, un bureau d'enregistrement agissant sous le contrôle d'un opérateur de registre serait couvert par une DADRP, il est donc important de s'assurer que « l'opérateur de registre » intègre des entités contrôlées directement ou indirectement par, ou sous le contrôle commun d'un opérateur de registre, que ce soit par une structure de propriété ou par le contrôle de titres comportant droit de vote, par contrat ou autrement où l'idée de 'contrôle' est rattachée à l'idée de possession, directement ou indirectement, ou par le pouvoir de diriger ou d'établir la direction de la gestion et des politiques d'un entité, que ce soit par le biais d'une structure de propriété ou par le contrôle de titres comportement droit de vote, par contrat ou de toute autre manière.

5.2 Mécanismes de protection des droits

De nouveaux mécanismes de protection des droits (RPM) ont été spécialement développés dans le cadre de l'introduction du programme des nouveaux gTLD parallèlement aux mécanismes existants de protection des droits. L'équipe de révision CCT a tenté de savoir si ces RPM permettent de promouvoir un environnement sûr et de favoriser la confiance des consommateurs dans le DNS ainsi que de mesurer l'impact des coûts du programme des nouveaux gTLD pour les titulaires de droits de propriété intellectuelle.

Les RMP sont en premier lieu décrits pour vérifier leur exhaustivité avant que nous les prenions en considération et avant de savoir s'ils ont aidé à atténuer les problèmes relatifs aux droits de marques déposées et des consommateurs dans le cadre de l'expansion des gTLD. Il est évident que l'équipe de révision CCT a fait face à des difficultés pour obtenir des données fiables pour faire cette évaluation, se tournant principalement vers les données obtenues par l'ICANN selon le rapport d'indicateurs CCT[111] et l'étude d'impact de l'INTA[112] ainsi que les données et commentaires existants provenant de la révision des mécanismes de protection des droits de l'ICANN et de la révision indépendante du rapport sur les services du centre d'échange d'information sur les marques (TMCH). [113]

L'équipe de révision CCT a également pris note des travaux réalisés en parallèle par les groupes de travail qui examinent actuellement les RPM et cherchent à ne pas faire double emploi ou compromettre ce travail, et attend donc avec impatience les rapports de ces groupes.

5.2.1 Contexte des RPM

[111] ICANN, « Rapport des indicateurs relatifs à la concurrence, confiance et choix du consommateur (CCT) , » consulté le 10 octobre 2017, https://www.icann.org/resources/reviews/cct/metrics
[112] Nielsen, enquête de l'INTA sur l'impact des coûts des nouveaux gTLD (avril 2017), consulté le 14 septembre 2017 : community.icann.org/download/attachments/56135378/INTA Cost Impact Report revised 4-13-17 v2.1.pdf
[113] Analysis Group, révision indépendante du rapport consacré aux services du centre d'échange d'information sur les marques (TMCH), (février 2017), consulté le 10 octobre 2017, https://newgtlds.icann.org/en/reviews/tmch/revised-services-review-22feb17-en.pdf

Avant l'augmentation du nombre des gTLD en 2012, en plus des mesures prises par les tribunaux, le principal mécanisme de protection des droits pour le système des noms de domaine était la politique uniforme de règlement de litiges relatifs aux noms de domaine (UDRP), une méthode alternative de règlement des litiges (adoptée par l'ICANN le 26 août 1999) qui s'appliquait à tous les domaines génériques de premier niveau. Toutefois, des problèmes liés à la protection des marques déposées ont été identifiés avant l'expansion des gTLD en 2012. La communauté des marques déposées craignait notamment que ce mécanisme ne permette pas de protéger convenablement les droits des marques déposées et les consommateurs dans un DNS en pleine expansion. Le Conseil de l'ICANN a donc pris la résolution (2009.03.06) qu'un groupe diversifié internationalement de personnes ayant les connaissances, l'expertise et l'expérience en matière de marques déposées, la protection des consommateurs, le droit de la concurrence et l'interaction des marques déposées avec le système des noms de domaine se réunisse pour proposer des solutions aux problèmes chapeautant la protection des marques dans le cadre de l'introduction de nouveaux gTLD[114]. Ce groupe a été baptisé équipe de mise en œuvre des recommandations (IRT).

Un ensemble de nouveaux mécanismes de protection des droits (RPM) a été proposé par l'IRT, à savoir : le système uniforme de suspension rapide (URS) ; la procédure de règlement de litiges après délégation (PDDRP) ; la procédure de règlement de litiges après délégation des marques déposées (TM-PDDRP) ; la procédure de règlement des litiges sur la restriction des registres (RRDRP) ; procédure de règlement de litiges relatifs aux engagements d'intérêt public (PICDRP) ; et le centre d'échange d'information sur les marques (pour les services avec période d'enregistrement prioritaire et de réclamations)[115].

5.2.2 Description des RPM

5.2.2.1 Politique uniforme de règlement de litiges relatifs aux noms de domaine (UDRP)

La procédure uniforme de résolution des litiges en matière de noms de domaine (UDRP) est une méthode alternative de règlement de litiges adoptée par l'ICANN le 26 août 1999 et qui s'applique à tous les domaines génériques de premier niveau (gTLD), y compris les gTLD historiques (tels que .com, .net, .info) et les nouveaux gTLD, et à certains domaines de premier niveau géographique (ccTLD) qui l'ont adoptée. Pour profiter de cette UDRP, le requérant doit démontrer, via la règle de la prépondérance de la preuve, que les trois conditions suivantes sont réunies : (i) le nom de domaine enregistré par le défendeur est identique ou similaire au point de créer une confusion à une marque déposée ou marque de services sur laquelle le requérant a des droits ; (ii) le défendeur n'a aucun droit ni intérêt légitime eu égard au nom de domaine ; et (iii) le nom de domaine a été enregistré et utilisé de mauvaise foi.

Une procédure mise en œuvre en vertu de l'UDRP dure environ 2 mois, du dépôt de la plainte à la décision. Le coût du dépôt d'une plainte en vertu de l'UDRP est compris entre

[114] ICANN, « Résolutions adoptées du Conseil d'administration : Mexico : Protections des marques déposées au sein des nouveaux gTLD, » 6 mars 2009, https://www.icann.org/resources/board-material/resolutions-2009-03-06-en#07.

[115] En outre, les processus de conflit de chaînes ont été introduits pour les candidatures pour les gTLD eux-mêmes, concernant la confusion de chaînes, l'intérêt public limité, les objections de la communauté et les objections pour atteinte aux droits. Ces éléments sont abordés plus en détail dans l'article sur les candidatures et l'évaluation.

1 500 USD pour 1 à 5 noms de domaine (panel d'un seul membre) et 4 000 USD pour 1 à 5 noms de domaine (panel de trois membres), à l'exclusion des frais d'avocats. Les recours disponibles en vertu de l'UDRP sont limités à l'annulation ou au transfert d'un nom de domaine. Aucun dommage-intérêt n'est accordé et il n'y a pas de mécanisme d'appel. Une décision est généralement mise en œuvre dans les 10 jours ouvrables suivant sa notification, à moins qu'une procédure judiciaire soit engagée devant un tribunal compétent.

Les plaintes UDRP sont déposées par voie électronique auprès d'un fournisseur de services de règlement de litiges approuvé par l'ICANN. À ce jour, les fournisseurs suivants ont été approuvés par l'ICANN : le Centre de règlement des litiges relatifs aux noms de domaines asiatiques (ADNDRC), le Forum (NAF), l'Organisation mondiale de la propriété intellectuelle (OMPI), le Centre d'arbitrage de la cour d'arbitrage tchèque pour les litiges liés à l'Internet (CAC) et le Centre arabe pour le règlement des litiges relatifs aux noms de domaine (ACDR).

5.2.2.2 Système uniforme de suspension rapide (URS)

Le système uniforme de suspension rapide (URS) est une procédure alternative de règlement des litiges, lancée en 2013 et qui a été initialement conçue pour des cas évidents de cybersquattage impliquant des nouveaux domaines génériques de premier niveau (gTLD), bien qu'elle ait été volontairement adoptée par une poignée de ccTLD et de TLD « parrainés » (comme .pw, .travel, .pro et .cat). Les exigences de fond de l'URS sont similaires à celles prévues pour l'UDRP, bien que la charge de la preuve soit plus lourde (« une preuve claire et convaincante », par opposition à « la prépondérance de la preuve »). Le requérant doit donc prouver que les 3 conditions suivantes sont réunies : (1) le nom de domaine est identique ou similaire au point de créer une confusion à une marque verbale : (a) pour laquelle le requérant détient un enregistrement national ou régional valide et qui est actuellement utilisée ; ou (b) qui a été validée par un tribunal ; ou (c) qui fait l'objet d'une protection spéciale par une loi ou un traité en vigueur au moment où la plainte URS est déposée (1.2.6.1 de l'URS) ; (2) le titulaire de nom de domaine n'a aucun droit ni intérêt légitime eu égard au nom de domaine (1.2.6.2 de l'URS) ; et (3) le nom de domaine a été enregistré et est utilisé de mauvaise foi (1.2.6.3 de l'URS). Les plaintes sont limitées à 500 mots. L'URS est destiné aux cas les plus évidents de cybersquattage et n'est donc généralement pas approprié pour les litiges relatifs aux noms de domaine portant sur des questions substantielles, plus complexes et contestables (comme la question de l'utilisation loyale).

Le seul recours disponible en vertu de l'URS est la suspension du nom de domaine (l'UDRP prévoyant le transfert ou l'annulation).

En vertu de l'URS, un nom de domaine peut rapidement être suspendu, dans un délai de 3 semaines après le dépôt d'une plainte. Dans le cas d'une décision favorable au requérant, le nom de domaine est suspendu pour le reste de la période d'enregistrement (qui peut être prolongée d'une année supplémentaire). Le site Web associé au nom de domaine en question affichera une bannière indiquant « Ce site est suspendu », mais le WHOIS du nom de domaine continuera d'afficher les renseignements du titulaire du nom de domaine initial (sauf pour la redirection des serveurs de noms). Si la décision en faveur du requérant a pris la forme d'un jugement par défaut, le titulaire de nom de domaine peut demander une révision de novo en déposant une réponse jusqu'à 6 mois après l'avis de défaut (qui peut être prolongé de six mois supplémentaires à la demande du titulaire de nom de domaine). En cas de contestation de la décision, l'URS prévoit un mécanisme d'appel se fondant sur le dossier existant.

Les frais de dépôt d'une plainte URS s'élèvent à environ 375 USD (pour 1 à 14 noms de domaine).

Seuls trois fournisseurs ont jusqu'ici été accrédités pour l'URS : le Centre de règlement des litiges relatifs aux noms de domaine asiatiques (ADNDRC), le Forum (NAF) et MSFD Srl (basée à Milan, Italie).

5.2.2.3 Procédures de règlement de litiges après délégation (PDDRP)

5.2.2.4 Les procédures de règlement de litiges après délégation sont des mécanismes de protection des droits qui ont été conçus pour protéger contre une conduite d'un opérateur de registre de nouveaux gTLD (par opposition à un titulaire de nom de domaine ou un bureau d'enregistrement). Il y a trois PDDRP :

La procédure de règlement de litiges relatifs aux marques déposées après délégation (TM-PDDRP) permet au propriétaire d'une marque déposée de porter plainte contre l'opérateur de registre pour son implication dans une affaire de contrefaçon de marques déposées, au premier ou au second niveau d'un nouveau gTLD.

Au premier niveau, le requérant doit démontrer via une « preuve claire et convaincante » que « la conduite affirmative de l'opérateur de registre dans l'exploitation et l'utilisation de son nouveau gTLD qui est identique à ou similaire au point de créer une confusion avec la marque du requérant, est à l'origine de ou contribue substantiellement à l'une des situations suivantes : (1) tire indûment profit du caractère distinctif ou de la renommée de la marque du requérant ; ou (2) porte atteinte au caractère distinctif ou à la renommée de la marque du requérant ; ou (3) crée un risque de confusion avec la marque du requérant (paragraphe 6.1 de la TM-PDDRP).

Au second niveau, les requérants sont tenus de démontrer via une « preuve claire et convaincante » que « la conduite affirmative de l'opérateur de registre correspond à : (a) un comportement ou une pratique caractéristique d'un opérateur de registre qui tente, de mauvaise foi, de tirer profit de la vente de noms de domaine portant atteinte à des marques déposées ; et (b) une tentative, de mauvaise foi, d'un opérateur de registre de tirer profit de l'enregistrement systématique de noms de domaine dans des gTLD qui sont identiques à ou similaires au point de créer une confusion avec la marque du requérant, qui : (i) tire indûment profit du caractère distinctif ou de la renommée de la marque du requérant ; ou (ii) porte atteinte au caractère distinctif ou à la renommée de la marque du requérant ; ou (iii) crée un risque de confusion avec la marque du requérant » (paragraphe 6.2 de la TM-PDDRP).

Si l'opérateur de registre est reconnu coupable par le panel d'experts, un certain nombre de recours peuvent être recommandés, y compris des mesures correctives visant à prévenir la contrefaçon d'enregistrements, la suspension de l'acceptation d'enregistrements de nouveaux noms de domaine dans les gTLD en jeu jusqu'à ce que l'infraction ait cessé ou pour une période prescrite par l'expert, ou la résiliation du contrat de registre, dans des circonstances extraordinaires où l'opérateur de registre a agi « avec malveillance »

(paragraphe 18 de la TM-PDDRP). Enfin, l'ICANN a le pouvoir d'imposer les mesures qu'elle juge appropriées, le cas échéant.

À ce jour, l'ICANN a désigné les fournisseurs de services de règlement de litiges suivants qui peuvent intervenir en vertu de la TM-PPDRP : le Centre de règlement des litiges relatifs aux noms de domaine asiatiques (ADNDRC), le Forum (NAF) et l'Organisation mondiale de la propriété intellectuelle (OMPI).

Procédure de règlement des litiges sur la restriction de registre (RRDRP), permet à une institution établie de déposer une plainte contre un des opérateurs de registre des nouveaux gTLD basés sur la communauté qui ne respecte pas les restrictions à l'enregistrement figurant dans son contrat de registre. Pour qu'une plainte soit recevable, le requérant doit démontrer via la règle de la « prépondérance de la preuve » que : « (i) la communauté invoquée par l'objecteur est une communauté définie ; (ii) il existe une forte association entre la communauté invoquée et la chaîne ou étiquette gTLD ; (iii) l'opérateur du TLD a violé les termes du programme de restrictions de la communauté dans son accord ; (iv) il y a un préjudice mesurable pour le requérant et la communauté citée par l'objecteur. » Les mesures correctives recommandées par le panel d'experts sont similaires à celles prescrites dans le cadre de la TM-PDDRP. Enfin, l'ICANN a le pouvoir de décider ou non d'imposer de telles mesures correctives.

La procédure de résolution des litiges relatifs aux engagements d'intérêt public (PICDRP) permet à toute personne ou entité (le « rapporteur ») de déposer une plainte contre un bureau d'enregistrement des nouveaux gTLD pour non-respect des engagements d'intérêt public dans la spécification 11 de son contrat de registre. Le rapporteur doit déposer un « rapport PIC » auprès de l'ICANN en remplissant un formulaire en ligne. Le « rapport PIC » doit (1) identifier les PIC formant la base de ce rapport (2) préciser les motifs du non-respect d'un ou plusieurs PIC et fournir des éléments de preuve et (3) définir la façon dont le rapporteur a été lésé par la non-conformité alléguée. L'ICANN peut mener une enquête sur la conformité ou invoquer un « panel permanent ». Si l'opérateur de registre est reconnu ne pas être en conformité avec son PIC, il aura 30 jours pour remédier à sa non-conformité. Si l'opérateur de registre ne parvient pas à résoudre les problèmes de non-conformité, l'ICANN déterminera les recours appropriés.

5.2.2.5 Centre d'échange d'information sur les marques (TMCH)

Le TMCH, établi en mars 2013, est une base de données centralisée des marques vérifiées du monde entier créée à l'initiative de l'ICANN afin de fournir une protection aux propriétaires de marque en vertu des nouveaux gTLD. Le TMCH remplit plusieurs fonctions importantes, y compris l'authentification et la vérification des enregistrements de marque, le stockage des enregistrements de marque dans une base de données et la fourniture de ces informations aux registres et bureaux d'enregistrement des nouveaux gTLD. Les données figurant dans le TMCH portent sur les mécanismes de protection des droits tels que les services de revendication prioritaire (qui offre la possibilité aux propriétaires de marque d'enregistrer des noms de domaine correspondant à leurs marques avant la mise à disposition générale) et les services de revendication de marques (un service informant les titulaires de noms de domaine et les propriétaires de marque de l'enregistrement de noms de domaine potentiellement illicite). L'enregistrement d'une marque auprès du TMCH est nécessaire pour être en mesure de participer non seulement à la période d'enregistrement prioritaire et aux services de revendication de marques, mais aussi aux mécanismes de protection des droits des registres tels que les mécanismes de blocage des noms de

domaine comme la liste de marques protégées pour les extensions de Donut (DPML) (bien que cela soit facultatif pour les autres RPM tels que l'URS). Le TMCH est donc un outil important de protection des droits des marques en vertu du programme des nouveaux gTLD.

5.2.3 Examen de ces mécanismes : ont-ils permis d'atténuer les problèmes relatifs à la protection des droits de marques déposées et des consommateurs dans le cadre de l'expansion des gTLD ?

L'équipe de révision CCT a examiné la capacité de ces mécanismes à atténuer les problèmes relatifs à la protection des droits de marques déposées et des consommateurs dans le cadre du développement des gTLD et a cherché à obtenir des données permettant d'aider à évaluer l'impact du programme des nouveaux gTLD de l'ICANN sur les coûts et les efforts requis pour protéger les marques déposées dans le système des noms de domaine.

L'équipe de révision CCT a tout d'abord analysé les données obtenues par l'ICANN en vertu du rapport sur les indicateurs CCT[116] mais également l'étude d'impact de l'INTA[117] pour laquelle on espérait obtenir des données supplémentaires sur l'impact du coût des nouveaux gTLD sur les propriétaires de marques ainsi qu'obtenir des données existantes et des commentaires de la révision des mécanismes de protection des droits. L'équipe de révision CCT a également pris note des travaux réalisés en parallèle par les groupes de travail qui examinent actuellement les RPM et cherchent à ne pas faire double emploi ou compromettre ce travail, et attend donc avec impatience les rapports de ces groupes.

5.2.3.1 Révision par l'ICANN des mécanismes de protection des droits (RPM)

Les conclusions préliminaires concernant la révision des mécanismes de protection des droits (RPM) de l'ICANN menée par l'organisation de l'ICANN et publiée le 11 septembre 2015, ont déterminé que l'URS a produit des résultats positifs dans certains cas limités. La vitesse et le faible coût font les affaires de ceux qui sont confrontés à des cas évidents et ne cherchent pas forcément à obtenir la suspension du nom de domaine. Cependant, certains détenteurs de droits n'ont pas opté pour l'utilisation de ce service parce qu'ils trouvent la norme « claire et convaincante » trop sévère et que le recours à l'URS est limité à la suspension seulement. Des craintes ont également été formulées quant à la possibilité que le nom de domaine soit de nouveau enregistré par un autre contrevenant potentiel une fois publié, c'est pourquoi certains détenteurs de droits se sentent plus à l'aise avec le nom de domaine dans leur portefeuille, ce qui est possible grâce à l'UDRP. En effet, la valeur d'un nom de domaine suspendu est remise en question.

5.2.3.2 Étude d'impact de l'INTA

[116] ICANN, « Rapport des indicateurs relatifs à la concurrence, confiance et choix du consommateur (CCT) , » consulté le 10 octobre 2017, https://www.icann.org/resources/reviews/cct/metrics
[117] Nielsen (avril 2017), enquête de l'INTA sur l'impact des coûts des nouveaux gTLD, consulté le 24 octobre 2017, community.icann.org/download/attachments/56135378/INTA Cost Impact Report revised 4-13-17 v2.1.pdf

Les résultats de l'étude d'impact de l'INTA contiennent des informations importantes qui permettent d'informer pleinement la communauté sur l'impact du programme des nouveaux gTLD de l'ICANN sur les coûts et efforts requis pour protéger les marques dans le DNS. Les membres de l'INTA et les titulaires de droits de propriété intellectuelle ont, à plusieurs reprises, fait part de leurs inquiétudes concernant le programme des nouveaux gTLD estimant qu'une telle expansion pourrait créer des coûts supplémentaires avec l'application de droits de propriété intellectuelle. L'enquête a cherché à évaluer les efforts et coûts supplémentaires requis pour protéger les marques déposées au sein du DNS.
L'INTA est une organisation mondiale composée de 6 600 propriétaires de marques déposées et professionnels de plus de 190 pays. Elle était donc bien placée pour répondre à une enquête de Nielsen basée sur les commentaires de la CCTRT, et il a été demandé aux membres de l'INTA de prendre en compte l'ensemble des coûts de ces 2 dernières années (2015 et 2016). Leur estimation des coûts comprend :

- les frais juridiques internes et externes,
- les frais de dépôt de plaintes,
- les frais de recherche,
- Les coûts totaux, dont les charges de personnel responsable de ces activités.

Les personnes ayant répondu à cette enquête ont affirmé que la compilation des données nécessaires pour répondre correctement à l'enquête avait été une tâche considérable. Au total, 33 personnes ont répondu dont une sans but lucratif. Bien que le taux de réponse à l'enquête soit supérieur à la norme pour un échantillon similaire [118] et si l'on considère le niveau d'effort requis pour compléter une enquête qui représente un certain coût financier, la taille de l'échantillon est relativement petite d'un point de vue statistique et exige une certaine prudence dans son interprétation. Néanmoins, les résultats donnent un aperçu des thèmes et tendances principaux[119].

Les points clés de l'étude d'impact :

1. Bien que l'un des objectifs du programme des nouveaux gTLD soit d'augmenter le choix pour les nouveaux propriétaires, ce choix ne semble pas être la préoccupation principale lorsqu'ils décident d'enregistrer un nouveau gTLD. La raison principale (90 %) expliquant pourquoi les propriétaires de marques déposées enregistrent des noms de domaine au sein de nouveaux gTLD est purement défensive : empêcher quelqu'un d'autre de l'enregistrer.

2. Les noms de domaine enregistrés par des propriétaires de marques au sein de nouveaux gTLD sont en général en parking et ne créent pas de valeur autre que d'empêcher une utilisation non autorisée par d'autres personnes.

3. Le programme des nouveaux gTLD a augmenté le coût global de la défense des marques déposées avec une surveillance Internet et des mesures de détournement représentant les plus grosses dépenses. Ces coûts ont eu le même impact sur les petites et grandes entreprises, le nombre de marques étant le facteur de coût le plus déterminant.

[118] Cette déclaration se base sur l'expérience générale de Nielsen avec des échantillons de clients ou de membres.
[119] Selon Nielsen,l 'échantillon total suffit à donner des informations directionnelles concernant ces tendances, mais les chiffres exacts comportent quand même une marge d'erreur élevée (le pourcentage +/- dont on entend souvent parler lors de sondages)

4. Les personnes interrogées ont déclaré que le coût total moyen de mise en application relatif aux TLD (anciens et nouveaux) par entreprise était de 150 000 $ par an. Ceci étant dit, le coût varie beaucoup selon les personnes interrogées.[120] Ce point mériterait une recherche plus approfondie lors de prochaines enquêtes.

5. Concernant les litiges, plus de 75 % des cas rapportés aujourd'hui impliquent des services d'anonymisation et d'enregistrement fiduciaire et près des 2/3 présentent un certain niveau d'inexactitude/d'informations WHOIS incomplètes.

6. Même si les nouveaux gTLD représentent 1/6 des dépenses d'application, ils ne représentent pas encore 1/6 des enregistrements de noms de domaine. Autrement dit, le coût des mesures d'application au sein des nouveaux gTLD représente environ 18 % des coûts d'application de l'ensemble des TLD alors que le nombre total d'enregistrements de nouveaux gTLD par rapport à l'ensemble des TLD est de 10 % au moment de l'étude d'impact. [121] Ces données indiquent donc qu'il y a un coût disproportionné en lien avec les mesures d'application des nouveaux gTLD par rapport aux coûts totaux de mise en application. Cela montre qu'il pourrait y avoir proportionnellement plus de cas d'atteintes aux marques au sein des nouveaux gTLD qu'au sein des anciens gTLD.[122]

7. On considère en général que les RPM aident à atténuer les risques anticipés avec les nouveaux gTLD. À la question : « Merci de nous dire dans quelle mesure vous avez le sentiment que les mécanismes de protection des droits listés ci-dessus ont ou n'ont pas permis d'atténuer les risques encourus avec les nouveaux gTLD ? », les réponses étaient variées mais elles donnaient un aperçu intéressant de l'état d'esprit des propriétaires de marques répondant à l'enquête[123]. Deux-tiers des personnes interrogées

[120] Les coûts totaux rapportés varient de zéro à 5,2 millions de dollars.
[121] Nielsen, enquête sur l'impact des coûts des nouveaux gTLD (2017). Coûts moyens pour l'ensemble des TLD pour 2 années = 292 000 $. Coûts moyens pour les nouveaux gTLD pour 2 années = 53 690 $ (environ 18 %).
[122] Nielsen, enquête sur l'impact des coûts des nouveaux gTLD (2017). « Nielsen explique que les chiffres de la surveillance Internet, principale dépense, devraient être précisés : ces coûts sont des coûts généraux et ne sont pas spécifiques aux nouveaux gTLD. Une entité aura des dépenses de surveillance dans tous les TLD. Il pourrait y avoir une augmentation graduelle des coûts de surveillance étant donné les nouveaux gTLD supplémentaires pris en compte, et en effet il existe une preuve anecdotique selon laquelle plus de marques ont commencé une activité de surveillance depuis l'introduction des nouveaux gTLD. Cependant, ces coûts n'étaient pas détaillés dans le questionnaire, la surveillance était considérée comme un coût irrécupérable. Il aurait donc été normal de supposer que ces coûts augmentent et non baissent « Par conséquent, ces coûts totaux devraient être supérieur à 18 % ».
[123] Période d'enregistrement prioritaire : souvent avec un coût important pour le propriétaire de marque. Réclamations : le nom est déjà enregistré avant que nous en soyons notifiés ; URS : le nom n'est pas transféré ; critère d'action restreint ; PDDRP : le critère est tellement restreint que les circonstances ne se produisent presque jamais ; UDRP : critère bien défini, il existe maintenant un organisme d'aide à la jurisprudence, le transfert du nom est une option. Cependant, le prix a un effet dissuasif dans les cas les plus évidents.
La période d'enregistrement prioritaire et la période de revendications de marques sont trop courtes. Les entreprises ont besoin de mettre en place des mesures supplémentaires pour observer leur portefeuille au sein de nombreux gTLD publiés semaine après semaine.
Nous en avons utilisé certaines qui fonctionnent. D'autres non.
URS : il est coûteux de suspendre (et non de transférer) un domaine litigieux ; après-délégation : très intéressant, mais compliqué et lourd à mettre en place (actions communes de divers propriétaires de marques souvent requises).
Les périodes d'enregistrement prioritaire n'ont qu'un effet mineur car beaucoup de registres ciblent les propriétaires de marques avec des prix discriminatoires alors qu'en même temps, beaucoup proposent le même nom de domaine à quelqu'un qui n'est pas propriétaire d'une marque et à un prix bien plus bas. Les avis de plaintes n'empêchent pas les cyber-squatteurs d'enregistrer des noms de domaine malgré la notification qu'il existe des droits, ce qui veut dire que le problème qui existe pour les TLD historiques persiste pour les nouveaux gTLD après qu'un enregistrement ait lieu. L'URS a une charge de la preuve assez lourde comparé au rapport coût-efficacité de l'UDRP. La PDDRP, la RRDRP et la PICDRP peuvent être efficaces, mais ne sont pas considérées comme des options valables, elles ont donc un impact mineur sur l'atténuation des risques.
Nous avons principalement réalisé des enregistrements défensifs.

ont le sentiment que les UDRP et les périodes d'enregistrement prioritaire requises ont aidé à atténuer les risques, 90 % des personnes interrogées enregistrent un nouveau gTLD pendant une période d'enregistrement prioritaire. Parmi ceux qui pensent que les RPM sont efficaces, le classement est le suivant :

a. Enregistrement prioritaire 79 %
b. UDRP 73 %
c. Réclamations 66 %
d. URS 49 %
e. PDDRP/RRDRP/PICDRP 27 %

Il existe cependant une preuve anecdotique assez importante selon laquelle les propriétaires de marques sont des acquéreurs réticents face aux enregistrements prioritaires et beaucoup considèrent que c'est une dépense trop coûteuse :

> "« Les périodes d'enregistrement prioritaire sont vite devenues un produit de profit plus qu'un outil de protection »[124],
> « Les périodes d'enregistrement prioritaire n'ont qu'un effet mineur car beaucoup de registres ciblent les propriétaires de marques avec des prix discriminatoires alors qu'en même temps, beaucoup proposent le même nom de domaine à quelqu'un qui n'est pas propriétaire d'une marque et à un prix bien plus bas »[125]
> « Le registre .top a augmenté les frais d'enregistrement prioritaire de 30 000 $ pour [société].top. Nous avons refusé l'enregistrement »[126]

8. Les enregistrements du TMCH sont utilisés par une majorité des personnes interrogées. Si l'on observe les données, la majorité des personnes interrogées (environ 9 sur 10) a enregistré au moins 1 marque déposée auprès du TMCH, 6 personnes sur 10 en ayant enregistré entre 1 et 10. Concernant les coûts associés, ils varient nettement parmi les personnes interrogées allant de moins de 1 000 $ à 48 000 $, la moyenne étant à environ 7 700 $.

9. L'introduction du processus URS a apporté une alternative à l'UDRP mais il est moins utilisé. La raison principale mentionnée expliquant qu'il soit moins populaire est

---

C'est un bon mécanisme mais il est incomplet. L'URS est plus rapide que l'UDRP mais c'est plus qu'une question de jours, l'inefficacité ajouté à un programme malveillant et vous n'obtenez pas le nom de domaine. L'UDRP prend plusieurs mois. Les deux sont coûteux. Les professionnels ont toujours besoin d'enregistrements défensifs à un coût élevé pour protéger les clients des abus de leurs marques de confiance.
Nous préfèrerions avoir une procédure de blocage pour les marques déposées qui pourrait vraiment atténuer les risques, mais en l'absence de blocage, le TMCH apporte au moins un mécanisme pour que nous puissions enregistrer des noms de domaine avec nos marques avant qu'elles ne soient cyber-squattées. La procédure de plaintes du TMCH ne fonctionne que dans une mesure restreinte car elle ne prend en compte les dépôts que dans une période de temps très limitée. Nous estimons que l'URS a une valeur limitée étant donné les exigences requises pour plusieurs domaines. Nous utilisons l'UDRP mais seulement avec les TLD historiques car il y a un nombre accablant d'atteinte dans les domaines .com.
La période d'enregistrement prioritaire permet aux propriétaires de marques d'acheter un nom de domaine incorporant une marque déposée clé, avant tout le monde. Les autres mécanismes cependant, ne semblent pas autant efficaces et exigent des dépenses de ressources importantes de la part des propriétaires de marques déposées.
Nous n'avons pas eu l'occasion de les utiliser.
Les titulaires de noms de domaine sont prêts à payer de légers frais d'enregistrements pour utiliser un nom de domaine contenant une célèbre marque déposée. » (p. 59).

[124] Nielsen, enquête sur l'impact des coûts des nouveaux gTLD (2017), p.52.
[125] Ibid, p. 59
[126] Ibid, p. 50

l'impossibilité de transférer un nom de domaine après une prise de décision fructueuse et une charge de la preuve plus lourde.

10. En ce qui concerne la question des prix plus élevés, trois-quarts des personnes interrogées évaluent les prix des noms de domaine au cas par cas et deux-tiers des décisions d'enregistrement de noms de domaine ont été impactées par les prix plus élevés, .sucks étant le plus mentionné en tant que TLD pour lequel elles ont payé un prix plus élevé. Cependant, 15 % des personnes interrogées refusent de payer un prix plus élevé.

5.2.4 Rapport de l'ICANN sur les indicateurs relatifs à la concurrence, à la confiance et au choix du consommateur (CCT)

5.2.4.1 Nombre de plaintes déposés (UDRP et URS)

Il est évident au vue des données obtenues par l'ICANN auprès de l'ensemble des fournisseurs de services de règlements de litiges relatifs aux noms de domaine[127] que le nombre total de plaintes déposées (UDRP + URS) a nettement augmenté depuis l'introduction des nouveaux gTLD. Concernant l'UDRP, il y a eu une augmentation assez importante du nombre de plaintes UDRP déposées alors que l'utilisation de l'URS a été plus limitée et nous avons constaté une légère baisse des plaintes déposées depuis son introduction et la première utilisation au sein des nouveaux gTLD en 2014.
Les premiers nouveaux gTLD sont entrés dans la zone racine en 2013[128] mais ce n'est qu'en 2014 que nous avons vu la première UDRP impliquant un nouveau gTLD dans l'affaire « Canyon Bicycles GmbH c. Domains By Proxy, LLC / Rob van Eck » et qui concernait le nom de domaine <canyon.bike>[129] le 14 mars 2014. La première décision URS concernaitle nom de domaine <aeropostale.uno> le 28 avril 2014.[130] Nous avons pris pour point de départ l'année précédente sans litige lié à un nouveau gTLD, nous avons eu un total de 3 371 litiges, tous des UDRP et qui concernaient uniquement des anciens gTLD.

[127] ICANN, « Rapport sur les indicateurs relatifs à la concurrence, à la confiance et au choix du consommateur (CCT) : mécanismes de protection des droits », consulté le 10 octobre 2017, https://www.icann.org/resources/pages/cct-metrics-rpm-2016-06-27-en#1.12
[128] ICANN, « Les premiers registres de nouveaux gTLD reçoivent des jetons pour le système de gestion de la zone racine », consulté le 10 octobre 2017, https://newgtlds.icann.org/en/announcements-and-media/announcement-22oct13-en, premiers nouveaux gTLD à entrer dans la zone racine en octobre 2013.
[129] OMPI, « Décision du panel du centre administratif sur l'arbitrage et la médiation : Canyon Bicycles GmbH c. Domains By Proxy, LLC / Rob van Eck dossier No. D2014-0206, » consulté le 10 octobre 2017, http://www.wipo.int/amc/en/domains/search/text.jsp?case=D2014-0206, première décision UDRP impliquant un nouveau gTLD.
[130] ADR, « Décision d'appel URS du forum national d'arbitrage : Aeropostale Procurement Company, Inc. c. Michael Kinsey et al. Numéro de plainte : FA1403001550933," consulté le 10 octobre 2017, http://www.adrforum.com/Domaindecisions/1550933A.htm, première décision URS impliquant un nouveau gTLD.

Tableau 13 : Le nombre de plaintes déposées avec des fournisseurs de services UDRP et URS. [Mis à jour chaque trimestre] [Depuis : 3 août 2017]

Année	Répartition totale UDRP et URS	Total des cas combinés
2013	3 371 (UDRP)	3 371
2014	4 056 (UDRP) & 231 (URS)	4 287
2015	4 130 (UDRP) & 213 (URS)	4 343
2016	4 368 (UDRP) & 222 (URS)	4 590
2017 T1/T2	2 112 (UDRP) & 104 (URS)	2 216 (pour une demi-année)

Source : Bases de données du fournisseur d'arbitrage
Catégorie de la révision CCT : Confiance du consommateur

En 2014, nous avons vu le nombre total de plaintes (UDRP et URS combinées) passer à 4 287 soit une augmentation de 27 %. En 2015 le nombre total de plaintes a augmenté légèrement passant à 4 343 (1,3 % de plus qu'en 2014) et en 2016 une nouvelle augmentation de 5,7 % passant le nombre total de plaintes à 4 590. Par conséquent, en comparant le nombre total de plaintes en 2013 l'année précédant les premiers litiges de nouveaux gTLD et 2016, nous avons une nette augmentation de 36 % de plaintes déposées par l'ensemble des fournisseurs.

Si nous observons uniquement les plaintes UDRP, nous constatons une augmentation entre 2013 et 2014 de 20 %, une autre augmentation entre 2014 et 2015 d'environ 2 % et à nouveau entre 2015 et 2016 de 5,8 %. Si nous observons uniquement les cas URS, la première chose à noter est que sa popularité en tant que RPM est et reste faible avec 231 plaintes en 2014, 213 en 2015 et 222 en 2016. Donc environ 5 % du total des plaintes déposées sont des URS. De plus, il ne semble pas y avoir d'augmentation significative du nombre de plaintes déposées d'années en années. Nous remarquons une baisse de plaintes URS entre 2015 et 2014 et même en 2016 le total des plaintes URS déposées reste inférieur à 2014, première année d'exploitation des nouveaux gTLD. Cela nous amène à nous demander si l'URS réalise pleinement son potentiel en tant que RPM utile.

Il est important de noter que le nombre de plaintes UDRP et URS déposées ne reflète qu'une partie des coûts supportés par les propriétaires de marques déposées dans la défense de leurs marques et la majeure partie des coûts d'exécution peut avoir été engagée sous la forme d'enregistrements défensifs/blocage/surveillance/lettres de mise en demeure et action en justice, pour lesquels nous n'avons pas de données. Cependant, l'étude d'impact de l'INTA donne un aperçu de cela.

5.2.4.2 Plaintes soumises à l'ICANN concernant la mise en œuvre des décisions UDRP et URS

Le rôle de l'ICANN est de veiller à ce que les bureaux d'enregistrement soient conformes aux UDRP et aux règlements UDRP ainsi qu'aux règles et procédures de l'URS.

Par exemple, un fournisseur de services UDRP peut déposer une plainte UDRP signalant qu'un bureau d'enregistrement n'a pas bloqué un domaine soumis à une procédure UDRP ou répondu à la demande de vérification du fournisseur, dans un délai convenable. Le requérant peut ensuite déposer une plainte auprès de l'ICANN si le bureau d'enregistrement ne parvient pas à mettre en œuvre en temps opportun une décision UDRP.

En ce qui concerne l'URS, par exemple, l'opérateur de registre doit également bloquer en temps opportun, et, s'il y a lieu, suspendre le nom de domaine en cause conformément à la décision URS et aux règles et procédures URS. Le requérant ayant obtenu gain de cause dans la procédure URS et le fournisseur URS peuvent soumettre une plainte URS à l'ICANN concernant des violations présumées via le formulaire web de conformité URS.

Si l'on observe le nombre de plaintes soumises à l'ICANN concernant la mise en œuvre de décisions UDRP et URS,[131] le nombre de plaintes concernant l'UDRP a baissé entre 2012 et 2014 d'environ 65 % et est assez stable depuis cette date à environ 250-227 plaintes annuelles. Les plaintes URS étaient assez élevées en 2014, première année où l'URS était disponible pour les nouveaux gTLD, mais ces deux dernières années (2015 et 2016) le nombre de plaintes a presque diminué de moitié.

Tableau 14 : Total des réclamations UDRP/URS à l'ICANN[132]

Année	Réclamations UDRP	Réclamations URS
2012	658	
2013	408	
2014	227	19
2015	250	11
2016	235	9
2017 T1/T2	122	10

Tableau 15 : Comparer le % de plaintes auprès de l'ICANN dans chaque RPM par rapport au nombre total de décisions de noms de domaine dans chaque RPM

Année	URS	UDRP
2014	8%	5,5%
2015	5,1%	6%
2016	4%	5,4%

En 2014, année où l'URS a été introduit, il y avait un nombre assez élevé de plaintes auprès de l'ICANN. Par rapport au nombre total de plaintes URS cette année-là, le pourcentage était de 8 %. En comparaison avec le niveau de plaintes pour l'UDRP en 2014 qui était de 5,5 %. Le niveau plus élevé de plaintes concernant l'URS par rapport à l'UDRP peut s'expliquer par un certain nombre de facteurs dont sa relative nouveauté, la complexité de son processus et son adoption récente par les bureaux d'enregistrement.
Si nous analysons les années 2015 et 2016, nous observons que le nombre de plaintes baisse pour l'URS et en 2016 le nombre de plaintes URS par rapport à l'UDRP était en fait inférieur et représentait 4 % et il était de 5,4 % pour l'UDRP. Il se peut qu'au fil du temps, les difficultés de l'URS aient été maîtrisées à la fois par les bureaux d'enregistrement, les registres et les utilisateurs finaux.[133]

5.2.4.3 Centre d'échange d'information sur les marques (TMCH)

[131] Il convient de noter que les plaintes concernant le bien-fondé de la décision sont en dehors du cadre contractuel de l'ICANN.
[132] ICANN, « Rapport sur les indicateurs relatifs à la concurrence, à la confiance et au choix du consommateur (CCT) : mécanismes de protection des droits », consulté le 18 octobre 2017, https://www.icann.org/resources/pages/cct-metrics-rpm-2016-06-27-en#1.9.b
[133] ICANN, « Rapport sur les indicateurs relatifs à la concurrence, à la confiance et au choix du consommateur (CCT) : mécanismes de protection des droits », consulté le 4 mars 2017, https://www.icann.org/resources/pages/cct-metrics-rpm-2016-06-27-en

L'ICANN a demandé à Analysis Group d'entreprendre une révision indépendante des services du TMCH à partir de la recommandation du GAC de mai 2011 selon laquelle une révision complète suite au lancement devait être réalisée.[134] La révision cherchait à évaluer les forces et faiblesses des services du TMCH à la lumière de cette recommandation et elle se basait sur une analyse du TMCH et des sources de données de tiers, ainsi que sur des entretiens et des enquêtes des parties prenantes du TMCH. Le rapport révisé[135] intégrait les commentaires publics au rapport original et des analyses publiées le 25 juillet 2016.[136] Selon le rapport, les données obtenues ont permis de faire des observations significatives concernant l'utilisation des services du TMCH étudiés. La recherche n'a pas permis de fournir des informations quantifiables sur les coûts et bénéfices liés à l'état actuel des services du TMCH. En effet, les coûts et bénéfices potentiels de l'expansion ou de la modification du fonctionnement des services nécessitaient une analyse concrète coût-bénéfice qui était hors du cadre du rapport d'Analysis Group.

Résumé des conclusions

En ce qui concerne la possibilité de prolonger la période de revendication ou d'élargir les critères de correspondance utilisés pour le déclenchement de notifications du service des plaintes, le rapport a montré que cela pourrait n'avoir qu'un intérêt limité pour les propriétaires de marques déposées. Une telle prolongation pourrait en effet entraîner des coûts pour les autres groupes de parties prenantes, tels que les registres, les bureaux d'enregistrement et les titulaires de noms de domaine non propriétaires de marques. L'insuffisance des données empêche toute conclusion définitive.

Selon le rapport, étant donné qu'une analyse coût-bénéfice n'a pas été réalisée, une éventuelle prolongation des services de revendication ou un élargissement des critères de correspondance doivent prendre en considération les compromis inévitables ressentis par les différents groupes de parties prenantes. En effet, le rapport a souligné que lors de l'évaluation de la prolongation de la période de revendication, le nombre d'enregistrements éventuels affectés par la prolongation doit être évalué. L'efficacité des notifications du service de revendication dépend du nombre de tentatives d'enregistrements réalisées ; s'il y a peu de tentatives d'enregistrements, alors il y a moins d'enregistrements potentiellement illicites réalisés.

Le rapport a soulevé que les enregistrements ont baissé après la période de revendication de 90 jours, ainsi, tout mois supplémentaire ajouté à cette période sera susceptible de diminuer le nombre.

Le rapport a également soulevé que selon les données, les propriétaires de marques déposées semblent avoir moins d'inquiétudes concernant les variations de chaînes et estiment ainsi qu'un élargissement des critères de correspondance peut en réalité être bénéfique pour les propriétaires de marques déposées. Inversement, le préjudice potentiel des enregistrements de noms de domaine des non propriétaires de marques pourrait augmenter. Ces derniers pourraient se sentir décourager d'enregistrer des variations de chaînes de marques déposées qui ne seraient pas considérées comme une atteinte aux marques.

[134] ICANN (26 mai 2011), commentaires du GAC sur le guide de candidature (version du 15 avril 2011), consulté le 15 octobre 2017, https://archive.icann.org/en/topics/new-gtlds/gac-comments-new-gtlds-26may11-en.pdf
[135] Analysis Group, révision indépendante du rapport consacré aux services du centre d'échange d'information sur les marques (TMCH) (2017).
[136] Analysis Group, révision indépendante du rapport préliminaire consacré aux services du Centre d'échange d'information sur les marques (TMCH) (juillet 2016), consulté le 10 octobre 2017, https://newgtlds.icann.org/en/reviews/tmch/ draft-services-review-25jul16-en.pdf

Le rapport a finalement pris en considération la période d'enregistrement prioritaire et les commentaires suite au questionnaire. Il semble que, bien que les propriétaires de marques déposées ont le sentiment que la période d'enregistrement prioritaire est utile, et que beaucoup ne l'utilisent pas, en ayant enregistré leurs marques au sein du TMCH, de nombreux propriétaires de marques déposées n'utilisent en réalité pas la période d'enregistrement prioritaire. Le rapport a conclu que ceci pourrait être dû au fait que les dépenses des enregistrements de noms de domaine prioritaires ou les autres protections des services du TMCH comme les services de revendication, réduisent le besoin pour les propriétaires de marques déposées d'utiliser les enregistrements prioritaires. L'équipe de révision CCT a le sentiment que c'est également dû au très grand nombre de nouveaux gTLD. Les enregistrements défensifs lorsqu'ils se multiplient au sein de nombreux nouveaux gTLD occasionnent des dépenses prohibitives et peu de propriétaires de marques sont prêts à s'engager de la même manière avec des enregistrements de noms de domaine défensifs à grande échelle. L'équipe de révision CCT a cherché à savoir si les dépenses supplémentaires du TMCH ont véritablement apporté de la valeur et n'ont pas agi comme un élément dissuasif, ne représentant qu'un coût supplémentaire pour les propriétaires de marques.

5.2.4.4 La procédure de règlement de litiges relatifs aux marques déposées après délégation (TM-PDDRP)

La conformité contractuelle de l'ICANN n'a reçu aucune plainte concernant la non-conformité d'un opérateur de registre avec la PDDRP. Toutefois, il convient de noter qu'il y a actuellement un groupe de travail de la GNSO qui travaille sur un processus de développement des politiques (PDP) pour examiner tous les mécanismes de protection des droits (RPM) dans tous les gTLD, qui explore les obstacles possibles à la mise en œuvre de la procédure PDDRP étant donné qu'il n'y a pas de dépôts PDDRP avec ces fournisseurs à ce jour.

5.2.4.5 Décisions sur la procédure de règlement de litiges relatifs à la restriction des registres (RRDRP)

La RRDRP est censée examiner les circonstances dans lesquelles un opérateur de registre d'un nouveau gTLD basé sur la communauté s'écarte des restrictions à l'enregistrement prévues dans son contrat de registre. Au 3 août 2017, aucun cas RRDRP n'était recensé.

5.2.4.6 Part des enregistrements prioritaires et des blocages de domaines sur le nombre total d'enregistrements dans chaque TLD

Au 3 août 2017, les seules données disponibles sur le nombre d'enregistrements prioritaires par rapport au nombre total d'enregistrements dans les nouveaux gTLD proviennent de l'ICANN. Selon l'ICANN, il n'y a pas de données consolidées disponibles concernant les services de blocages commerciaux offerts par les registres. La CCT-RT reste disposée à recevoir de telles données.

Conclusion

Les données que nous avons montrent une augmentation du nombre de litiges depuis l'introduction des nouveaux gTLD avec des litiges en hausse d'années en années depuis cette introduction. En effet, en 2016 le nombre total de plaintes déposées (UDRP et URS

combinées) était de 36 % supérieur à 2013, année où le premier nouveau gTLD a été introduit. (25 % si nous utilisons comme référence le taux moyen pour 2012 et 2013)

Cependant, l'augmentation du nombre de litiges relatifs aux noms de domaine n'est pas en soi surprenant au vue du nombre grandissant d'enregistrements de noms de domaine à travers le monde depuis que les nouveaux gTLD ont été introduits dans la zone racine et que les enregistrements ont lieu.
Il serait plus pertinent de se demander s'il y a proportionnellement plus d'atteintes aux marques dans les nouveaux gTLD ou les TLD historiques ? C'est une question plus complexe car il y a de nombreux facteurs pris en compte dans l'évaluation d'une atteinte aux marques pour lesquels nous n'avons pas de données. L'étude d'impact de l'INTA est un bon exemple de ce que représente la difficulté d'obtenir de telles informations.

Les propriétaires de marques déposées utilisent également divers moyens pour gérer les enregistrements abusifs de noms de domaine, pas seulement l'UDRP ou l'URS, mais également des actions en justice, des lettres de mise en demeure pour lesquels il n'existe pas de suivi centralisé. Il en est de même pour les coûts engendrés par de telles mesures. Ce n'est pas non plus le rôle de l'ICANN de suivre ou d'essayer de suivre ces données. Cependant, l'ICANN collecte en effet des données sur l'utilisation des mécanismes de règlement de litiges, l'UDRP et l'URS via tous les fournisseurs de litiges relatifs aux noms de domaine. Les données montrent que les litiges relatifs aux noms de domaine augmentent. Nous avons également des données provenant de l'ICANN sur le nombre d'enregistrements de nouveaux gTLD par rapport au total des enregistrements gTLD (anciens et nouveaux gTLD). Ces données montrent également que les enregistrements de noms de domaine gTLD augmentent. Cependant, nous n'avons pas, dans les indicateurs de l'ICANN, la répartition de l'utilisation des UDRP, c'est-à-dire l'utilisation des UDRP dans les nouveaux gTLD par rapport à l'utilisation pour les TLD historiques.

Ainsi, pour tenter de répondre à la question visant à savoir s'il y a plus d'atteintes aux marques dans les nouveaux gTLD par rapport aux TLD historiques, nous pouvons examiner les données du principal fournisseur de règlement de litiges, l'OMPI, car ses données sont disponibles au public.
Les données de l'OMPI pour 2016 ont démontré que les litiges relatifs au cybersquattage concernant les nouveaux gTLD représentent 16 % des dossiers 2016 de l'OMPI. Parmi ceux-ci, les nouveaux gTLD .XYZ, .TOP et .CLUB ont été les nouveaux gTLD les plus impliqués dans les litiges relatifs aux noms de domaine. Les anciens gTLD représentent 70 % des cas de l'OMPI. Si l'on observe l'OMPI seule, 18,6 % de ses dossiers gTLD concernent des nouveaux gTLD. Si l'on se tourne vers les statistiques de l'ICANN pour les enregistrements de noms de domaine pour la fin de l'année 2016, nous avons 196 493 430 enregistrements gTLD et 27 659 702 enregistrements de nouveaux gTLD Ainsi, les nouveaux gTLD représentent donc 14 % du nombre total d'enregistrements de gTLD. Ces données nous indiquent qu'il y a proportionnellement plus de cas d'atteintes aux marques dans les nouveaux gTLD par rapport aux TLD historiques.

La question à se poser est de savoir si l'URS est un RPM valable étant donné sa faible utilisation par rapport à l'UDRP.
Le fait que la TM-PDDRP et la RRDRP n'ont pas été utilisées jusqu'à présent peut également remettre en question leur existence, mais peut tout autant souligner le fait que leur simple existence ait un effet dissuasif.[137]

5.2.5 Recommandations

Recommandation 40 : Une étude de l'impact visant à déterminer l'impact du programme des nouveaux gTLD sur le coût et les efforts requis pour protéger les marques déposées dans le DNS devrait être répétée à intervalles réguliers afin d'observer l'évolution du programme des nouveaux gTLD au fil du temps et l'augmentation des enregistrements de nouveaux gTLD. Nous recommandons en particulier que la prochaine étude d'impact soit achevée dans les 18 mois suivant la publication du rapport final de la CCT-RT et que d'autres études soient effectuées tous les 18 à 24 mois. La CCTRT reconnaît qu'elle a été réalisée en 2017 par Nielsen concernant les membres de l'INTA et nous encourageons à poursuivre cela en notant que les études doivent être plus accessibles.

Fondements/conclusions connexes : Il est probable que les coûts varient considérablement dans le temps à mesure que les nouveaux gTLD sont délégués et que les niveaux d'enregistrement évoluent. La répétition de l'étude d'impact permettra de réaliser une comparaison dans le temps.

À : Organisation de l'ICANN.

Condition préalable ou niveau de priorité : élevée

Consensus au sein de l'équipe : oui

---

[137] Sources :
Recueil des sources liées aux procédures :
wiki de la communauté de l'équipe de révision de la concurrence, de la confiance et du choix du consommateur, « Procédures », consulté le 5 mars 2017, https://community.icann.org/display/CCT/Procedures
ICANN, « Révision des mécanismes de protection des droits ».
GNSO de l'ICANN, « Révision PDP de tous les mécanismes de protection des droits dans tous les gTLD », consultée le 5 mars 2017, https://gnso.icann.org/en/group-activities/active/rpm
Analysis Group, révision indépendante du rapport préliminaire consacré aux services du Centre d'échange d'information sur les marques (TMCH) (juillet 2016), consulté le 5 mars 2017, https://newgtlds.icann.org/en/reviews/tmch/ draft-services-review-25jul16-en.pdf

wiki de la communauté de l'équipe de révision de la concurrence, de la confiance et du choix du consommateur, « Procédures », consulté le 5 mars 2017, https://community.icann.org/display/CCT/Procedures.

Recueil des sources liées à l'impact des sauvegardes et aux PIC :
ICANN, « Rapport sur les indicateurs relatifs à la concurrence, à la confiance et au choix du consommateur (CCT) : mécanismes de protection des droits », consulté le 5 mars 2017, https://www.icann.org/resources/pages/cct-metrics-rpm-2016-06-27-en

Détails : L'évolution au fil du temps fournira une image plus précise des coûts et permettra d'assurer le suivi de l'efficacité des RPM en général dans le DNS.

Mesures de réussite : Les résultats de ces études d'impact fourniront beaucoup plus de données pour les groupes de travail concernés qui examinent actuellement les RPM et le TMCH ainsi que les futurs groupes, au bénéfice de la communauté dans son ensemble. Les recommandations seront alors également en mesure d'évoluer de manière appropriée au sein des équipes de révision CCT.

Recommandation 41 : Une révision complète de l'URS devrait être effectuée et il conviendrait de tenir compte de la façon dont il devrait fonctionner avec l'UDRP. Toutefois, compte tenu de la révision PDP de tous les mécanismes de protection des droits dans tous les gTLD, actuellement en cours, une telle révision doit prendre en considération ce rapport lors de sa publication et pourrait même ne pas être nécessaire si ce rapport pose des conclusions substantielles et examine pleinement les modifications éventuelles.

Fondements/conclusions connexes : L'intérêt suscité par l'URS semble être inférieur aux attentes, il serait donc utile d'en comprendre les raisons et de savoir si l'URS est considéré comme un mécanisme efficace de prévention des abus. Il est également important que tous les gTLD soient traités sur un pied d'égalité. En effet, la révision PDP de tous les mécanismes de protection des droits dans tous les gTLD, effectuée parallèlement aux travaux de cette équipe de révision CCT, contribuera à cette réflexion avec son rapport prévu en 2018. Ce rapport du groupe de travail doit être pris en considération pour définir la portée d'une quelconque révision et des potentielles modifications.

À : Organisation de soutien aux extensions génériques

Condition préalable ou niveau de priorité : condition préalable

Consensus au sein de l'équipe : oui

Détails : Une révision de l'URS devrait examiner, entre autres, (1) le recours à l'option de transfert avec l'URS en plus de la suspension ; (2) le maintien de deux systèmes complets (à savoir l'UDPR et l'URS en parallèle) compte tenu de leurs mérites respectifs, (3) l'application potentielle de l'URS à tous les gTLD et (4) la disponibilité des différents mécanismes applicables dans les différents gTLD comme source de confusion pour les consommateurs et les titulaires de droits.

Mesures de réussite : Sur la base des résultats, une vue d'ensemble claire de la pertinence de l'URS et de l'efficacité du fonctionnement de l'URS de la façon prévue au départ.

Recommandation 42 : Une analyse coût-bénéfice et une révision du TMCH et de sa portée devraient être réalisées afin de fournir des informations quantifiables sur les coûts et bénéfices liés à l'état actuel des services du TMCH et permettre ainsi une révision des politiques efficace.

Fondements/conclusions connexes : Il semble probable qu'une révision complète du TMCH soit nécessaire, y compris une analyse coût-bénéfice. L'efficacité du TMCH semble être remise en question. La révision indépendante du rapport consacré aux services du centre d'échange d'information sur les marques (TMCH)[138] n'a pas permis d'établir des

[138] Analysis Group, révision indépendante du rapport consacré aux services du centre d'échange d'information sur les marques (TMCH) (2017).

conclusions définitives à cause des limites de données et a en effet conclu qu'il avait été impossible de réaliser une analyse coût-bénéfice de l'extension du service de revendication ou de l'élargissement des critères de correspondance. En effet, la révision PDP de tous les mécanismes de protection des droits dans tous les gTLD, effectuée parallèlement aux travaux de cette équipe de révision CCT, contribuera à cette réflexion avec son rapport prévu en janvier 2018. Ce rapport du groupe de travail doit être pris en considération pour définir la portée d'une quelconque révision et des potentielles modifications.

À : Organisation de soutien aux extensions génériques

Condition préalable ou niveau de priorité : condition préalable

Consensus au sein de l'équipe : oui

Détails : Il semble y avoir beaucoup de discussions et de commentaires sur la question visant à savoir si les fonctions du TMCH devraient s'étendre, en plus des correspondances identiques, aux « marques+mots clés » ou erreurs typographiques communes de la marque en question. Si une extension de ces fonctions est jugée utile, la base d'une telle extension doit alors être claire.

Mesures de réussite : La disponibilité de données suffisantes pour formuler des recommandations et permettre une révision efficace de la politique du TMCH.

6 Annexes

6.1 Opinions minoritaires sur le document relatif à l'utilisation malveillante du DNS, rec. 4

Alors que la CCT-RT a pu obtenir un soutien unanime pour la plupart de nos recommandations, certains membres de l'équipe de révision s'opposent à la création d'une procédure de règlement des litiges relatifs à l'utilisation malveillante du DNS (DADRP). Cette déclaration présente le raisonnement expliquant ce désaccord :

1. la CCT-RT a adopté, en tant que principe directeur, le fait que nos analyses et recommandations seraient basées sur les données. Cependant, aucune donnée ne soutient l'idée d'une DADRP. Rien n'indique que les opérateurs de registre sont responsables (directement ou indirectement) pour les malveillances au sein de leurs TLD ; aucune donnée n'indique que le département de la conformité de l'ICANN est incapable d'appliquer les obligations contractuelles ; et aucune donnée n'indique qu'une utilisation malveillante du DNS de certains TLD vise des tierces parties spécifiques qui pourraient initier une DADRP. Cette recommandation n'est alors pas conforme au modèle basé sur les données de la CCT-RT.

2. Le rapport sur l'utilisation malveillante du DNS précise clairement que d'essayer de réduire les cas d'utilisations malveillantes du DNS par le biais des registres du DNS est peu judicieux et inefficace. Aucune des sauvegardes requises des opérateurs de nouveaux gTLD ne semblent avoir permis de réduire la prévalence des malveillances, et l'une d'entre elles (l'adoption du DNSSEC) semble en réalité avoir un lien avec l'augmentation de ces malveillances. Le fait que la prévention des malveillances via les registres du DNS soit inefficace ne devrait pas être surprenant puisque les registres n'ont pas de lien direct avec les titulaires de noms de domaine et qu'il n'y a aucun mécanisme autre que la suspension d'un domaine (qui dans tous les cas n'est pas une approche appropriée) pour répondre à ce problème. Une DADRP qui cherche à punir les registres pour des comportements qu'ont des titulaires de noms de domaine sur lesquels ils n'ont pas de contrôle et avec lesquels ils n'ont pas de lien est fondamentalement peu judicieuse et ne répondra pas au problème de l'utilisation malveillante du DNS.

3. Dans la mesure où il existe une inquiétude selon laquelle le département de la conformité de l'ICANN n'applique pas correctement les obligations contractuelles des registres, la solution serait d'améliorer la conformité de l'ICANN plutôt que de créer une nouvelle procédure de règlement des litiges. Améliorer la conformité de l'ICANN a l'avantage de répondre aux problèmes dans la totalité des contrats de registres et bureaux d'enregistrement, alors que la création de cette DADRP permet, au mieux, d'améliorer la mise en application pour un domaine en particulier. Créer des procédures de règlement de litiges uniques pour différentes parties du contrat n'est par nature pas évolutif car il n'est pas possible de le faire pour chaque composante majeure du contrat. Tout aussi important, cette approche créé une grande incertitude pour les parties contractantes qui peuvent penser que même si l'ICANN a examiné cette question et estime être en conformité avec le contrat, une tierce partie est désormais en désaccord avec cette évaluation et est en mesure de lancer, de son propre fait, une procédure coûteuse et complexe.

4. Alors que l'utilisation malveillante du DNS est un sujet important, la charte de la CCT-RT est d' « examiner (A) la mesure dans laquelle l'expansion des gTLD a favorisé la

concurrence, la confiance et le choix du consommateur et (B) l'efficacité du processus de candidature et d'évaluation des séries de nouveaux gTLD et des sauvegardes mises en place pour réduire les problèmes découlant des séries de nouveaux gTLD. » Il est donc de notre ressort d'examiner les sauvegardes existantes mises en place dans la série de 2012, mais pas de développer de nouveaux mécanismes complexes pour traiter l'utilisation malveillante du DNS.

Jordyn Buchanan, Carlos Raul Gutierrez, Carlton Samuels, Waudo Siganga

6.2 Déclaration individuelle

Jonathan Zuck
Président, CCT-RT

Drew Bagley
Équipe de direction , CCT-RT

25 octobre 2017
Objet : soumission de recommandations préliminaires pour la période de consultation publique

Cher M. Zuck, président de la CCT-RT,

J'apporte à la connaissance et à la réflexion de l'équipe de révision de la concurrence, la confiance et le choix du consommateur (CCT-RT) et de la communauté, une recommandation préliminaire (ci-après Recommandation 5), en lien avec les conclusions de la CCTRT, intégrée dans le présent chapitre préliminaire sur l'utilisation malveillante du DNS. La recommandation 5 n'était pas comprise dans le chapitre préparé pour commentaire public car la CCT-RT n'a pas eu le temps de suffisamment discuter, analyser ou déterminer la question de l'adoption de la recommandation avant la période de consultation publique. Néanmoins, je vous demande de présenter la recommandation 5 en tant qu'ajout au rapport préliminaire pour que la communauté ait connaissance de cette éventuelle recommandation et ait une chance d'apporter des commentaires qui pourront guider les analyses futures de la CCT-RT concernant cette proposition.

Sincères salutations,

Drew Bagley

Recommandation 5 : L'ICANN devrait collecter des données et diffuser la chaîne des parties responsables de l'ensemble des enregistrements de noms de domaine gTLD.

Fondements/Conclusions connexes : À l'heure actuelle, il n'existe pas de mécanisme cohérent pour déterminer tous les opérateurs qui sont sous contrat ou non avec l'ICANN et associés à des enregistrements de noms de domaine gTLD. Souvent, les enregistrements WHOIS ne font pas la distinction entre un bureau d'enregistrement et un revendeur. L'étude sur l'utilisation malveillante du DNS demandée par la CCT-RT, par exemple, n'a pas su distinguer les revendeurs et les bureaux d'enregistrement pour déterminer dans quelle mesure les taux d'utilisations malveillantes du DNS peuvent être dus à des revendeurs spécifiques et avoir un impact sur les niveaux d'utilisations malveillantes du DNS. Ces données devraient être disponibles pour améliorer les décisions basées sur les données nécessaires pour les recommandations proposées par la CCT-RT, pour compléter les

sauvegardes du programme des nouveaux gTLD, et améliorer les décisions du département de la conformité contractuelle de l'ICANN.

À: Le Conseil d'administration de l'ICANN, le groupe des représentants des opérateurs de registre, le groupe des représentants des bureaux d'enregistrement, l'organisation de soutien aux extensions génériques et le groupe de travail PDP consacré aux procédures futures, la deuxième équipe de révision de la sécurité, la stabilité et la résilience du DNS, l'équipe de révision du service d'annuaire de données d'enregistrement.
Condition préalable ou niveau de priorité : élevée
Consensus au sein de l'équipe : ???

Détails : Les informations WHOIS sont une source importante de données pour l'analyse de l'utilisation malveillante du DNS. Les sauvegardes, comme les exigences du WHOIS détaillé, n'obligent pas que les revendeurs soient listés dans les enregistrements WHOIS. En conséquence, la chaîne complète des parties impliquées dans une transaction d'enregistrement ne peut être facilement obtenue. Sans de telles informations, il est difficile de déterminer la mesure dans laquelle l'utilisation malveillante technique est liée à des revendeurs individuels plutôt qu'à des bureaux d'enregistrement. Par exemple, avec de telles données imprécises, il serait possible pour un revendeur associé à des taux de malveillances très élevés de rester opérationnel auprès d'un bureau d'enregistrement avec des taux de malveillances techniques relativement normaux. Cela permettrait en effet, une utilisation malveillante technique systémique par une partie non contractante, pourtant tenue par des exigences, à un rythme soutenu. Attendu que, collecter et publier ces informations permettraient à un utilisateur final de facilement déterminer le registre, le bureau d'enregistrement ou le revendeur associé à un enregistrement et ainsi supprimer l'opacité des parties responsables de l'atténuation des cas d'utilisations malveillantes du DNS. Cela permettrait une analyse plus précise de l'utilisation malveillante du DNS et de la transparence pour les utilisateurs Internet, renforçant ainsi les efforts de responsabilité de la communauté, et l'application de la conformité contractuelle.

6.3 Annexe C : enquêtes et études

Plusieurs enquêtes et études ont été commandées avant la formation de la CCT-RT afin de guider ses travaux :

- un groupe consultatif sur la mise en œuvre a été convoqué par le Conseil d'administration de l'ICANN en 2013 pour examiner une série d'indicateurs possibles qui ont été proposés par l'Organisation de soutien aux extensions génériques (GNSO) et le Comité consultatif At-Large (ALAC). Cette équipe, dénommée l'IAG-CCT, a évalué la faisabilité, l'utilité et la rentabilité d'adopter plusieurs indicateurs recommandés par ces deux groupes et a publié un ensemble de 66 indicateurs, que le Conseil d'administration de l'ICANN a adoptés pour les soumettre à la considération de la CCTRT.[139] L'ICANN a collecté des données concernant un grand nombre de ces indicateurs.[140] Sur les 66 indicateurs recommandés, plusieurs comprenaient des chiffres de référence montrant un aperçu des comportements et des activités dans le marché des noms de domaine avant la saturation des nouveaux gTLD. En fonction de l'indicateur en question, la période de référence pourrait couvrir entre une et plusieurs années avant la délégation des nouveaux gTLD.
    - L'IAG-CCT a déterminé qu'un sous-ensemble des indicateurs pourrait être mieux évalué à travers une enquête sur les consommateurs et les titulaires de noms de domaine. Les résultats de la deuxième partie de l'enquête sur les consommateurs menée par Nielsen ont été publiés en juin 2016.[141] L'étude a mesuré les attitudes actuelles des utilisateurs de l'Internet dans l'environnement des gTLD et du système des noms de domaine (DNS) ainsi que les changements dans les attitudes de ces consommateurs par rapport à la première partie de l'enquête, menée par Nielsen en 2015.[142] Les internautes ont répondu à des questions concernant la sensibilisation des consommateurs et leur perception en termes de choix, d'expérience et de confiance. L'enquête sur les consommateurs comprenait un univers qui était un échantillon représentatif des internautes des cinq régions de l'ICANN et a été menée dans la langue de chaque pays faisant l'objet de l'enquête. Les résultats de l'étape 2 de l'étude ont révélé que plus de la moitié des personnes interrogées (52 %) connaissait au moins un nouveau gTLD et que, dans l'ensemble, la confiance accordée à l'industrie des noms de domaine par rapport à d'autres industries liées aux technologies a été améliorée.
    - De même, Nielsen a mené une enquête mondiale sur les titulaires de noms de domaine qui ciblait ceux ayant au moins un nom de domaine enregistré. Les participants à l'enquête ont été interrogés sur leur connaissance des nouveaux gTLD ainsi que sur leur sentiment vis-à-vis du choix, de la confiance et de l'expérience eu égard à l'environnement actuel des gTLD. Les résultats de la première partie de l'enquête sur les titulaires de noms de domaine menée par Nielsen

[139] Groupe consultatif sur la mise en œuvre de la concurrence, la confiance et le choix du consommateur (26 septembre 2014), *Recommandations finales axées sur les mesures de la révision CCT,* consulté le 20 janvier 2017, https://community.icann.org/display/IAG/IAG-CCT+report

[140] ICANN, « Rapport des indicateurs relatifs à la concurrence, confiance et choix du consommateurs (CCT) », consulté le 25 janvier 2017, https://www.icann.org/resources/pages/cct-metrics-rpm-2016-06-27-en

[141] Nielsen, *enquête mondiale de l'ICANN sur les consommateurs partie 2*, (juin 2016) consultée le 30 janvier 2017, https://www.icann.org/news/announcement-2-2016-06-23-en

[142] Nielsen, *Enquête mondiale sur les consommateurs de l'ICANN* (avril 2015), consulté le 30 janvier 2017, https://www.icann.org/news/announcement-2015-05-29-en

ont été publiés en septembre 2015.[143] La CCTRT a reçu les résultats de la deuxième étape de l'enquête sur les titulaires de noms de domaine le 15 septembre 2016.[144] Les résultats ont révélé que les nouveaux gTLD inclus dans les deux étapes de l'enquête présentaient des niveaux de sensibilisation similaires, avec des niveaux de connaissance plus élevés en Amérique du Sud et en Asie-Pacifique, et que la confiance accordée à l'industrie demeure en général élevée, en particulier en Asie.

- Un deuxième sous-ensemble d'indicateurs de l'IAG-CCT vise à mesurer la concurrence dans l'espace des nouveaux gTLD à partir d'une analyse des données sur les prix et d'autres indices non liés aux prix. L'ICANN a engagé Analysis Group pour réaliser une étude économique qui avait deux objectifs principaux : d'une part, mesurer les pratiques de tarification relatives aux domaines dans les nouveaux gTLD et les comparer à celles des domaines dans l'espace des anciens gTLD ; et d'autre part, fournir une analyse qualitative des autres indicateurs de concurrence non liés aux prix, tel que les innovations techniques ou autres. Les résultats de l'évaluation de l'étape 1 d'Analysis Group ont été présentés en septembre 2015.[145] L'évaluation de l'étape 2 d'Analysis Group décrit comment les indicateurs relatifs à la concurrence établis dans l'étape 1 de l'évaluation ont changé (ou pas) à mesure que le programme des nouveaux gTLD s'est élargi au cours d'une année.[146] Les résultats de l'étude économique de l'étape 2, qui ont été présentés en octobre 2016, ont révélé une baisse du pourcentage des enregistrements de nouveaux gTLD attribuables aux quatre et huit registres avec la plupart des enregistrements, ainsi qu'une certaine volatilité dans le pourcentage d'enregistrements détenus par les opérateurs de registre. Les membres de la CCT-RT ont fourni à Analysis Group leurs commentaires au sujet de la méthode et l'approche utilisées avant de commencer la deuxième partie de l'analyse.

- pour aider la CCTRT à évaluer l'efficacité des processus de candidature et d'évaluation du programme des nouveaux gTLD, ainsi que les sauvegardes mises en œuvre pour limiter leur utilisation malveillante, l'ICANN a collaboré avec la communauté afin de générer les rapports suivants :
  - la « révision de la mise en œuvre du programme révisé » publiée en janvier 2016 aborde l'efficacité et l'efficience de la mise en œuvre du programme des nouveaux par l'ICANN du point de vue du personnel ;[147]

[143] Nielsen, *enquête mondiale sur les titulaires de noms de domaine* (septembre 2015), consultée le 30 janvier 2017 https://www.icann.org/news/announcement-2015-05-29-en
[144] Nielsen, *enquête mondiale sur les titulaires de noms de domaine partie 2* (août 2016), consultée le 30 janvier 2017 https://www.icann.org/news/announcement-2015-05-29-en
[145] Analysis Group, *Première partie de l'évaluation des effets du programme des nouveaux gTLD sur la concurrence (*septembre 2015), consulté le 30 janvier 2017, https://www.icann.org/news/announcement-2-2015-09-28-en
[146] Analysis Group, *Deuxième partie de l'évaluation des effets du Programme des nouveaux gTLD sur la concurrence* (octobre 2016), consulté le 30 janvier 2017, https://www.icann.org/news/announcement-2016-10-11-en
[147] ICANN, *Révision de la mise en œuvre du programme* (janvier 2016), consulté le 30 janvier 2017, https://www.icann.org/en/system/files/files/program-review-29jan16-en.pdf

- Le « rapport révisé : les sauvegardes du programme des nouveaux gTLD contre l'utilisation malveillante du DNS » examine des méthodes pour mesurer l'efficacité des sauvegardes dans le but de limiter l'utilisation malveillante du DNS qui ont été mises en œuvre dans le cadre du programme des nouveaux gTLD. Il explique quelles sont les activités qui pourraient constituer une utilisation malveillante du DNS et fournit une révision préliminaire des documents disponibles qui examinent les taux de malveillances des nouveaux gTLD et du DNS dans son ensemble.[148]

- Le « rapport révisé : la révision du mécanisme de protection des droits » analyse les données relatives aux principaux mécanismes de protection tels que le Centre d'échange d'information sur les marques, le système uniforme de suspension rapide et le règlement de litiges après délégation. L'interaction entre les mécanismes de protection des droits et d'autres éléments du programme des nouveaux gTLD sont également considérés.[149]

- Afin de compléter les données existantes et de mieux orienter ses travaux, la CCT-RT a demandé de mener des enquêtes et études supplémentaires :
  - la sous-équipe consacrée à la concurrence et au choix du consommateur a demandé à Analysis Group et à l'organisation de l'ICANN des données supplémentaires concernant les analyses de tarification et d'enregistrement pour l'aider à répondre aux questions concernant l'efficacité de l'expansion des nouveaux gTLD comme promoteur de la concurrence au niveau des prix entre les opérateurs de gTLD, ainsi qu'entre les bureaux d'enregistrement et les revendeurs.

  - La sous-équipe Concurrence et choix du consommateur a demandé des données relatives au parking des gTLD historiques afin de compléter les données relatives au parking des nouveaux gTLD disponibles sur ntldstats.com. Ces données ont permis à la sous-équipe d'obtenir une image plus exacte des enregistrements dans chaque registre en supprimant les enregistrements qui ne reflètent pas les enregistrements « actifs ». D'autre part, la sous-équipe Concurrence et choix du consommateur a obtenu des données d'enregistrement de ccTLD de CENTR et Zooknic.

  - À la demande de l'équipe de révision, l'ICANN a passé un contrat avec SIDN afin d'effectuer une étude analysant les taux d'activité abusive, malveillante et criminelle dans les gTLD, soient-ils nouveaux ou anciens. L'étude sur « l'analyse statistique de l'utilisation malveillante du DNS dans les gTLD » compare les taux de ces activités entre les nouveaux et les anciens gTLD, et elle utilise des analyses statistiques inférentielles pour mesurer les effets des domaines en parking sur le DNSSEC, ainsi que les restrictions d'enregistrement sur les taux de malveillances en utilisant des

[148] Opérations et recherches en matière de politique de l'ICANN, *Sauvegardes du programme des nouveaux gTLD visant à lutter contre l'utilisation malveillante du DNS* : *rapport révisé* (juillet 2016), consulté le 30 janvier 2017, https://www.icann.org/news/announcement-2016-07-18-en

[149] ICANN, *Révision des mécanismes de protection des droits : rapport révisé* (septembre 2015), consulté le 30 janvier 2017, https://newgtlds.icann.org/en/reviews/rpm/rpm-review-11sep15-en.pdf

données historiques couvrant les trois premières années complètes du programme des nouveaux gTLD (2014-2016).[150]

- Lors de sa troisième réunion en personne tenue en juin 2016, la CCT-RT a demandé à ce qu'une enquête sur les candidats soit commandée. En plus d'aborder des sujets liés à la concurrence, au choix et à la confiance du consommateur, l'enquête visait également à examiner l'efficacité des processus de candidature et d'évaluation du programme des nouveaux gTLD. La CCT-RT a cherché à obtenir des réponses, pour mieux comprendre ce que les candidats pensent du processus de candidature, auprès de ceux ayant complété le processus, ceux dont la candidature est en cours et ceux ayant retiré leur candidature.

- Pour aider dans son évaluation du processus de candidature et d'évaluation, la CCTRT a demandé à AMGlobal de mener des recherches et des entretiens avec des entreprises, des organisations et d'autres institutions n'ayant pas présenté des candidatures pour les nouveaux gTLD mais qui pourraient avoir été considérés comme de bons candidats pour le programme en tant que cohortes d'entités similaires de pays développés ayant présenté leur candidature.[151] Le but de cette recherche était de comprendre plus profondément la sensibilisation des consommateurs du programme des nouveaux gTLD et la raison pour laquelle il n'y avait pas davantage de candidatures de sociétés venant des pays développés. Le rapport a été présenté en novembre 2016 et contenait des recommandations telles que la création d'outils de sensibilisation destinés au grand public répondant aux questions clés concernant les coûts, le processus de candidature, les délais et l'ICANN elle-même. D'autres recommandations proposaient de fournir à la communauté une explication complète des différents usages des nouveaux gTLD et de répondre aux questions potentielles de la communauté sur le modèle commercial et la pratique. Eu égard aux futures séries de candidature, le rapport proposait d'effectuer des recherches supplémentaires sur les meilleures manières de sensibiliser le grand public dans les pays du sud et de susciter un dialogue relatif aux nouveaux gTLD dans le domaine public-privé, et, dans la mesure du possible, de commencer à préparer le public pour la prochaine série dans les plus brefs délais.

- En outre, la CCT-RT a utilisé les résultats de l'enquête demandée par l'association internationale des marques de commerce (INTA). Cette enquête menée entre janvier et février 2017 a recueilli des informations auprès de 33 membres de l'INTA, des membres commerciaux et non commerciaux de l'INTA ainsi que des propriétaires d'IP qui ont répondu à des questions relatives aux coûts encourus par leurs clients dans le cadre du développement de l'espace TLD. L'enquête, qui a été envoyée à 1 096 participants

[150] *SIDN Labs et Delft University of Technology (août 2017), Rapport final de l'analyse statistique de l'utilisation malveillante du DNS dans les gTLD, consulté le 23 octobre 2017,* https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf

[151] AMGlobal Consulting, Nouveaux gTLD et pays du Sud : comprendre la demande limitée des pays du Sud lors de la dernière série de nouveaux gTLD et les options pour l'avenir (octobre 2016), consulté le 25 janvier 2017, https://community.icann.org/pages/viewpage.action?pageId=56135383

potentiels, donnait un aperçu de l'expérience de ces propriétaires de marques face à ce programme.[152]

[152] Nielsen (avril 2017), enquête de l'INTA sur l'impact des coûts des nouveaux gTLD, consulté le 24 octobre 2017, community.icann.org/download/attachments/56135378/INTA Cost Impact Report revised 4-13-17 v2.1.pdf

6.4 Annexe E : Résumé de la participation

Nom	Affiliation	Présence aux réunions (Nombre total de réunions plénières et de réunions en personnes : 65, jusqu'à septembre 2017)
Calvin Browne	GNSO	52
Carlos Raúl Gutierrez	GNSO	46
Carlton Samuels	ALAC	48
David Taylor	GNSO	47
Dejan Djukic	ccN	51
Drew Bagley	Expert indépendant	61
Fabro Steibel	Expert indépendant	28
Gao Mosweu	ccN	49
Jonathan Zuck	GNSO	55
Jordyn Buchanan	GNSO	61
Kaili Kan	ALAC	59
Laureen Kapin	Représentant du président du GAC	58
Megan Richards	GAC	48
N.Ravi Shanker (démissionné 18/10/17)	Expert indépendant	2
Stanley Besen (démissionné 25/06/2017)	Expert indépendant	33
Waudo Siganga	GNSO	53
Jamie Hedlund	Représentant du Président-directeur général de l'ICANN	49

Nom	Affiliation	Sous-équipe de la concurrence et du choix du consommateur (22 réunions jusqu'à septembre 2017)	Sous-équipe chargée des sauvegardes et de la confiance (26 réunions jusqu'à septembre 2017)	Réunions de la sous-équipe Nielsen (4 réunions jusqu'à septembre 2017)	Processus de candidature et d'évaluation (3 réunions jusqu'à septembre 2017)	Réunions de la sous-équipe de l'INTA (3 réunions jusqu'à septembre 2017)
Calvin Browne	GNSO	2	14			
Carlos Raúl Gutierrez	GNSO	5	13	2		0
Carlton Samuels	ALAC		17			2
David Taylor	GNSO	1	14			3
Dejan Djukic	ccN	19			1	2
Drew Bagley	Expert indépendant	2	23		0	
Fabro Steibel	Expert indépendant		11	3		
Gao Mosweu	ccN		22		1	
Jonathan Zuck	GNSO	18	18	3	2	
Jordyn Buchanan	GNSO	22		3	1	3
Kaili Kan	ALAC	16				
Laureen Kapin	Représentant du président du GAC		22	2	2	
Megan Richards	GAC	12			0	
N.Ravi Shanker (démissioné 18/10/2017)	Expert indépendant					
Stanley Besen (démissionné 25/06/17)	Expert indépendant	13	1	1		

Waudo Siganga	GNSO	16		2	1	1
Jamie Hedlund	Représentant du Président-directeur général de l'ICANN	6	13		0	

Les déclarations d'intérêt des membres de l'équipe de révision peuvent être consultées sur https://community.icann.org/display/CCT/Composition+of+Review+Team.
Les archives contenant les courriers électroniques peuvent être consultées sur https://community.icann.org/display/CCT/Email+Archives.