# Nouveau programme gTLD

# Mémorandum explicatif

# Limiter les conduites malveillantes

Date de publication : 12 novembre 2010

## Origines – Programme du nouveau gTLD

L'ICANN a été fondé il y a dix ans, sous la forme d'une organisation à but non-lucratif et à plusieurs acteurs, afin de coordonner le système d'attribution d'adresses d'Internet. L'un de ses principes fondateurs, reconnu par les États-Unis et d'autres gouvernements, fut de promouvoir la compétition dans le marché du nom de domaine, tout en garantissant la sécurité et de la stabilité d'Internet. Le développement du « Generic top-level domains » (gTLDs) va dans le sens d'une plate-forme permettant plus d'innovation, de choix et de changement dans le système d'attribution d'adresses d'Internet.

La décision d'introduire de nouveaux gTLDs fut l'aboutissement d'un processus, long et détaillé, de consultation de toutes les parties prenantes de la communauté global d'Internet représentée par un large éventail d'acteurs – gouvernements, individus, autorités issues de la société civile, de la propriété commerciale et intellectuelle, et communauté technologique. Ont aussi participé au projet le Comité consultatif gouvernemental de l'ICANN (GAC), le Comité consultatif At-Large (ALAC), Country Code Names Supporting Organization (ccNSO) et le Comité consultatif pour la sécurité et la stabilité (SSAC). Le processus consultatif a donné lieu à une politique d'introduction de nouveaux gTLDs, complété par le Generic Names Supporting Organization (GNSO) en 2007, et adopté par le conseil de l'ICANN en juin 2008.

Ce mémorandum explicatif appartient à une série de documents publiés par l'ICANN pour aider la communauté globale d'Internet à mieux comprendre les besoins et les processus présentés dans le Guide du candidat. Depuis la fin de l'année 2008, le personnel de l'ICANN partage l'évolution du développement du programme avec la communauté Internet, à travers un ensemble de forums de discussion publics concernant le Guide du candidat et les documents annexes. Tous les commentaires reçus sont attentivement évalués et utilisés pour affiner plus avant le programme.

Veuillez noter que ce document n'est qu'une ébauche à discuter. Les candidats potentiels ne doivent s'en remettre à aucun détail proposé concernant le programme du nouveau gTLD, celui-ci demeurant l'objet de consultations plus approfondies et de révisions.

## Résumé des points-clés de ce document

- Bien que neuf recommandations destinées à limiter les conduites malveillantes aient déjà été incorporées au Guide, un travail sur l'implémentation à proprement parler est en cours.
- Les solutions qui ont été détaillées dans ces mémorandums se traduiront par des améliorations significatives pour l'environnement DNS, en augmentant la protection pour les inscrits, en assurant un environnement plus sûr, et en développant et en implémentant des outils destinés à détecter et à lutter contre des comportements malveillants potentiels.

## Résumé

L'ICANN a précédemment publié deux versions de ce Mémorandum explicatif destiné à décrire neuf améliorations dans le Guide du candidat, pour traiter les conduites malveillantes potentielles. Le premier mémo a été publié le 3 octobre 2009, et le second, le 31 mai 2010.

Cette mise à jour a pour but de décrire les travaux d'implémentation complémentaires qui ont été menés dans ce domaine – même si les recommandations ont déjà été incorporées au Guide, un travail sur l'implémentation à proprement parler est en cours.

Les solutions qui ont été détaillées dans ces mémorandums se traduiront par des améliorations significatives pour l'environnement DNS, en augmentant la protection pour les inscrits, en assurant un environnement plus sûr, et en développant et en implémentant des outils destinés à détecter et à combattre des comportements malveillants potentiels. L'ICANN et la communauté poursuivra sa collaboration sur des mesures et des initiatives qui contribueront à un lancement stable du nouveau processus gTLD. Les problèmes de sécurité, de stabilité et de résistance demeureront des préoccupations de haute priorité pour l'ICANN, tant que le nouveau gTLD évolue vers son lancement et son implémentation.

Ce document met en lumière la quantité significative d'excellent travail qui a déjà été effectué, essentiellement par des volontaires de la communauté dans des commentaires de forums ou des groupes de travail. L'ICANN apprécie cela et exprime sa reconnaissance pour l'implication des volontaires, pour leur travail sur des initiatives qui vont améliorer de manière significative l'environnement DNS.

Les neuf recommandations qui ont été proposées pour implémentation dans le nouveau gTLD, et qui sont désormais comprises ou référencées dans la version finale du Guide du candidat proposé sont les suivantes :

1. ***Opérateurs de registre approuvés*** – Cette recommandation implique que les opérateurs d'enregistrement du candidat au nouveau gTLD fassent l'objet d'un examen adéquat, pour s'assurer que l'opérateur d'enregistrement n'a pas d'historique pénal ou malveillant.
2. ***Plan démontré pour le développement du DNSSEC*** – Cette recommandation implique qu'il soit obligatoire pour un candidat à un nouveau gTLD de faire la preuve d'un plan pour le développement du DNSSEC, afin de réduire le risque d'enregistrements DNS fictifs.
3. ***Interdiction du « wild carding »*** - Cette recommandation suppose que des contrôles appropriés dans le domaine du *wildcarding* DNS réduiraient les risques de redirection du DNS vers un site malveillant.
4. ***Suppression des « glue records » isolés*** – Cette recommandation implique que les gTLDs suppriment les enregistrements de noms de serveurs lorsqu'un système est supprimé du gTLD, afin de réduire le risque d'utilisation de ceux qui resteraient par une personne malveillante.
5. ***Condition pour un enregistrement WHOIS lourd*** - Cette recommandation suppose que les nouveaux gTLDs maintiennent et fournissent un accès aux enregistrements « WHOIS lourds », pour améliorer la précision et la complétude des données WHOIS. L'usage l'utilisation d'enregistrements WHOIS lourds constitue un mécanisme clé pour lutter contre les usages malveillants des nouveaux gTLDs, en offrant une chaîne contractuelle plus complète dans le cadre du TLD. Cela devrait permettre une recherche de données plus rapides et la résolution des activités malveillantes, puisqu'elles seraient identifiées.
6. ***Centralisation de l'accès à la zone-file*** – Cette recommandation implique que les certificats d'accès pour obtenir des données enregistrées de la zone-file soient disponibles via une source centralisée, permettant une identification plus précise et plus rapide des points de contact clés dans chaque TLD. Cela réduit le temps nécessaire à la mise en œuvre d'actions correctives dans le cadre de TLDs victimes d'activités malveillantes.
7. ***Niveau de registre documenté des abus de contacts et de procédures*** – Cette recommandation implique que les gTLDs établissent un point de contact unique responsable du traitement des plaintes pour abus, et que ces registres proposent une description des politiques qu'elles mettent en place pour combattre les abus. Ces conditions sont considérées comme des étapes fondamentales pour le succès des efforts de lutte contre les conduites malveillantes dans le cadre des nouveaux gTLDs.
8. ***Participation à un processus rapide d'enregistrement de la sécurité des requêtes*** – Cette recommandation implique que les nouveaux gTLDs puissent entreprendre des actions rapides et efficaces à la lumière des menaces systémiques qui pèsent sur le DNS en établissant un processus dédié pour examiner et approuver les requêtes de sécurité expédiées.
9. ***Ebauche de cadre pour la vérification de la zone de haute sécurité*** – Cette recommandation suggère la création d'un programme volontaire destiné à désigner les TLDs désireux d'établir et de démontrer un meilleur niveau de sécurité et de confiance. L'objectif général du programme est de proposer un mécanisme pour les TLDs qui souhaiteraient mettre en valeur leur niveau de sécurité et de fiabilité, pour les business models de TLD qui bénéficieraient d'une telle mise en valeur.

Le reste de ce mémorandum abordera le statut particulier du travail concernant chacune de ces recommandations.

## Statut des neuf recommandations à propos des conduites malveillantes

Cette section expose le statut actuel des neuf recommandations destinées à réduire les conduites malveillantes dans les nouveaux gTLDs.

### 1. Opérateurs de registre approuvés

- **Statut actuel**

  La recommandation consistant à exiger un « examen » ou une enquête sur les origines des opérateurs de registre est un principe directeur dans l'amélioration du processus de candidature au nouveau gTLD, pour les nouveaux candidats. Le processus de candidature au nouveau gTLD comprend des critères précis, pour lesquels les candidats au nouveau gTLD font l'objet d'une vérification, qui fait partie du processus de candidature. La version finale du Guide du candidat proposé a été amendée pour apporter plus de détail et de pertinence dans la réponse au commentaire. La référence précise au terrorisme a été supprimée (comme l'est la liste très simplifiée de domaines faisant l'objet de vérification). Le filtrage des origines ne sera mené que dans deux domaines : le zèle général dans le domaine des affaires et l'historique pénal ; et l'historique du comportement de « cybersquatting ».

### 2. Demande de développement du DNSSEC

- **Statut actuel**

  Présenter un plan de développement du DNSSEC est une composante obligatoire du processus de candidature au nouveau gTLD. La spécification 6 de l'Accord de registre contient une disposition stipulant que : « L'opérateur de registre signera ses zone-files de TLD en implémentant des Domain Name System Security Extensions (« DNSSEC »). » Depuis que la zone d'origine a été signée pour le DNSSEC, le 15 juillet 2010, 64 TLDs (à la date du 11 novembre 2010) ont signé leur zone.

### 3. Interdiction du « wild carding »

- **Statut actuel**

  La terminologie liée à l'interdiction des « wildcards » fait toujours partie de la Spécification 6 de l'Accord de registre. Aucun changement n'a affecté cette interdiction depuis que le Conseil directorial de l'ICANN a décidé, lors de sa réunion publique à Sidney en juin 2009, que les nouveaux domaines de haut niveau ne devaient pas utiliser la redirection DNS, en en synthétisant les réponses.

### 4. « Glue records » isolés

- **Statut actuel**

  Le SSAC a réuni un groupe de travail pour étudier cette question, et une quantité considérable d'analyses de zones TLD et d'enregistrements ont été effectués pour obtenir une image plus claire de la prévalence de ces « orphelins » dans les principaux TLDs. Le groupe de travail a examiné des zone-files pour tous les gTLD actuels et a analysé la fréquence de l'utilisation des « orphelins » dans le cadre de conduites malveillantes. Le SSAC a développé un projet de rapport du groupe de travail qui est actuellement en cours de finalisation par le groupe. Ces recommandations générées par le groupe de travail du SSAC

pourraient offrir des informations complémentaires pour les registres, concernant la manière de gérer les enregistrements isolés, et feront l'objet d'une évaluation pour leur éventuel ajout aux processus clés du gTLD. Comme le précise la Résolution 2.8 du 25 septembre 2010 du Conseil de l'ICANN, « les dispositions actuelles du Guide exigent de chaque candidat qu'il décrive les mesures qu'il propose pour la gestion et la suppression des glue records isolés pour les noms supprimés dans la zone. Cette condition doit être maintenue et sera ajustée si le SSAC émet de nouvelles recommandations dans ce rapport concernant cette question. »

## 5. Condition pour WHOIS lourd

- **Statut actuel**

Le statut de cette recommandation reste inchangé et le « WHOIS lourd » est une condition pour tous les nouveaux gTLDs. Tous les nouveaux gTLDs devront implémenter des conditions de WHOIS lourd, selon la Spécification 4 de l'Accord de registre. On trouvera plus d'informations concernant cette recommandation dans le Mémorandum explicatif sur le WHOIS publié le 30 mai 2010.

## 6. Centralisation de l'accès à la zone-file

- **Statut actuel**

L'ICANN a accepté la recommandation concernant la création d'un mécanisme destiné à soutenir la centralisation de l'accès aux enregistrements de zone-file, et un Groupe de conseil appelé « Zone-File Access Advisory Group » (« ZFA AG ») a été créé, avec la mission de travailler avec la communauté, d'élaborer une proposition pour un mécanisme d'assistance à la centralisation de l'accès à la zone-file. Le ZFA AG a terminé son travail, dont les détails sont disponibles dans la Proposition stratégique publiée le 13 mai 2010.
En résumé, le ZFA AG préconise un Modèle hybride (le « Modèle ») qui est un mélange des modèles bilatéral amélioré et de chambre de compensation décrits dans sa proposition. Le Modèle offre un point de contact unique pour les candidats à la recherche d'accès à la zone-file, et préserve largement les rôles existants et les fonctions opérationnelles des fournisseurs de données. Le Modèle introduit deux changements au système d'accès actuel à la zone-file. D'abord, il standardise la relation entre les fournisseurs de données de la zone-file (par exemple les opérateurs de registre) et les consommateurs (par exemple les organisations anti-abus ou de protection des marques déposées, les chercheurs, l'Université, etc.) en établissant trois catégories : critères de candidature, critères d'accès, et critères de format de dossiers/enregistrements. Ensuite, il introduit une chambre de compensation légère pour la gestion de l'identité dans le système d'accès à la zone-file, auquel elle apportera un point de contact unique pour les consommateurs cherchant un accès à la zone-file.
L'ICANN développe actuellement un plan afin d'identifier un fournisseur de service adéquat pour implémenter la recommandation esquissée dans cette proposition.
Les références à l'accès à la zone-file se trouvent dans la Section 2 de la Spécification 4 de l'Accord de registre.

## 7. Niveau de registre documenté des abus de contacts et de procédures

- **Statut actuel**

La recommandation consistant à demander à ce qu'ils documentent un registre spécifique de contacts abusifs et qu'ils fournissent une description de leurs politiques particulières anti-abus est une obligation pour tous les nouveaux gTLDs. Cela n'a pas changé depuis le mémorandum d'origine concernant les conduites malveillantes. La disposition se trouve dans la Section 5.4.1 du Module 5.

## 8. Participation à un processus rapide d'enregistrement de la sécurité des requêtes (ERSR)

- **Statut actuel**

Le 1er octobre 2009, l'ICANN a annoncé que le Processus rapide d'enregistrement de la sécurité des requêtes (ERSR) était disponible. Le processus doit être utilisé exclusivement dans le cadre des incidents qui requièrent une action immédiate du registre afin d'éviter des effets délétères sur la stabilité ou la sécurité du DSN.

Le ERSR, une procédure de soumission en ligne, constitue le résultat d'un effort collaboratif entre l'ICANN et les registres du gTLD pour développer un processus d'action rapide, dans les cas où ces derniers :

- Informeraient l'ICANN d'un incident présent ou imminent menaçant la sécurité de leurs TLD et/ou du DNS ; et,
- Demanderaient une renonciation contractuelle pour des actions qu'ils pourraient entreprendre pour réduire ou éliminer l'incident.

Une renonciation contractuelle est une exemption destinée à se conformer à une disposition particulière dans un accord de registre pour la période de temps nécessaire pour répondre à l'incident.

## 9. Ebauche de cadre pour la vérification de la zone de haute sécurité

- **Statut actuel**

La recommandation proposant de créer une ébauche de cadre pour la vérification de la zone de haute sécurité émane des groupes de services bancaires et financiers tels que BITS (un consortium d'institutions de service financier américain), et une initiative baptisée High Security Zone Top Level Domain Program (« Programme HSTLD ») a été créée. L'idée consiste à esquisser un cadre de modes de contrôles proposés pour la vérification de la zone de haute sécurité. Afin d'analyser une possible approche d'un tel cadre, et avancer en direction d'une proposition d'un rapport communautaire, l'ICANN a formé le High Security Zone Top Level Domain Advisory Group (« Groupe HSTLD »). Le mandat du Groupe HSTLD a consisté à travailler avec la communauté à travers un modèle de développement partant de la base, afin de propose une ou plusieurs approche(s) de programme volontaire, consistant en des critères de contrôle et en des incitations à renforcer la sécurité et la confiance en les TLDs qui choisissent de participer à un tel programme. Un programme HSTLD ne sera pas piloté par l'ICANN, mais par une entité tierce indépendante qui établira les critères et certifiera les TLDs en fonction de ceux-ci.

Le 16 juin 2010, l'ICANN a posté le Snapshot de l'HSTLD #2 du Groupe HSTLD pour commentaires publics. Le Snapshot présente un cadre commun de principes, de critères et de standards de contrôle qui permettraient aux opérateurs de registre désireux d'effectuer un classement en tant que Domaine de haute sécurité top niveau de maintenir et de

démonter des pratiques et des politiques améliorées dans un esprit sécuritaires. Le cadre actuel constitue la base des conditions essentielles du programme HSTLD, et peut être référencé à l'Annexe A du Snapshot.

La période de commentaire public sur le Snapshot s'est conclue le 21 juillet 2010, et le résumé et les analyses des commentaires seront publiés en même temps que la version finale du Guide du candidat proposé. En outre, l'ICANN et le Groupe HSTLD se sont accordés sur l'intérêt de conduire une Requête pour information (RFI) sur le programme. L'objectif de la RFI est d'aider la communauté ICANN à mieux comprendre les cadres potentiels et les approches pour l'évaluation des registres TLD au regard des critères HSTLD, de déterminer où des améliorations à l'ébauche des critères et à l'ensemble du programme pourraient être apportées pour assurer son succès, et pour estimer la viabilité du programme HSTLD proposé.

L'ICANN a annoncé la publication de la RFI le 22 septembre 2010, et les réponses sont attendues le 23 novembre 2010.

La décision sera prise concernant les étapes ultérieures après la clôture de la période de la RFI, le 23 novembre 2010, et quand le Groupe HSTLD aura eu le temps nécessaire pour répondre aux questions et résumer et analyser les réponses.

L'ICANN poursuit sont engagement à faire réduire les conduites malveillantes dans les nouveaux gTLDs et soutient le développement du HSTLD comme concept volontaire, et mené de façon indépendante.