Deuxième révision de la sécurité, la stabilité et la résilience (SSR2)

Résumé analytique et contexte

Résumé analytique

Le présent rapport est une première version préliminaire des conclusions et recommandations de l'équipe de révision SSR2. Il y a plusieurs éléments sur lesquels l'équipe de révision SSR2 continue de se répéter, mais dans l'ensemble, l'équipe estime que le rapport est à un point où les commentaires du public fourniraient une contribution utile et critique pour informer le rapport final.

En particulier, la SSR2 RT apprécierait des commentaires sur :

- les résultats et les recommandations ;
- quelle partie de l'ICANN (par exemple, le Conseil d'administration, l'organisation ICANN ou la communauté de l'ICANN) devrait traiter chaque recommandation ;
- quelles mesures seraient les plus appropriées pour que chaque recommandation soit mesurable, tout en évitant de fabriquer la solution ;
- quelle serait la priorité à octroyer à chaque recommandation ;
- tout rapport supplémentaire ou autre document que vous pensez que l'équipe de révision devrait examiner avant de finir ses recommandations (veuillez consulter le wiki de la SSR2[1] , y compris les « documents de référence », les « documents d'information » et les « questions-réponses » pour les documents que l'équipe a examinés).

En vertu du processus de révision communautaire établi, la communauté aura également d'autres possibilités de contribuer au rapport final de la SSR2.

Aperçu

Introduction

[à inclure dans le rapport final]

Contexte

[à inclure dans le rapport final]

Objectifs

En vertu des statuts constitutifs de l'organisation ICANN[2] (article 4.6(c)), « Le Conseil d'administration effectuera une révision périodique du respect de l'engagement de l'ICANN vis-à-vis du renforcement de la stabilité opérationnelle, la fiabilité, la résilience, la sécurité et l'interopérabilité mondiale des systèmes et processus, internes et externes, qui affectent directement et/ou sont affectés par le système d'identificateurs uniques de l'Internet dont l'ICANN assure la coordination (la « révision SSR ») ».

Plus particulièrement :

[1] Wiki de l'équipe de révision SSR2 de l'ICANN, https://community.icann.org/display/SSR/SSR2+Review.
[2] « Statuts constitutifs de la Société pour l'attribution des noms de domaine et des numéros sur Internet », ICANN, modifiés le 28 novembre 2019, https://www.icann.org/resources/pages/governance/bylaws-en.

ii. L'équipe de révision SSR (« équipe de révision SSR ») pourra évaluer, mais sans s'y limiter, ce qui suit :

A. *des questions concernant la sécurité, la stabilité opérationnelle et la résilience, tant au niveau physique que du réseau, eu égard à la coordination du système d'identificateurs uniques de l'Internet ;*
B. *le respect d'un plan de mesures d'urgence approprié pour le système d'identificateurs uniques de l'Internet ;*
C. *le maintien de procédures de sécurité claires et interopérables à l'échelle mondiale pour les parties du système d'identificateurs uniques de l'Internet dont l'ICANN assure la coordination.*

iii. L'équipe de révision SSR évaluera également si l'ICANN a bien mis en œuvre ses actions en matière de sécurité, l'efficacité de ses actions pour répondre aux défis et aux menaces réels et potentiels liés à la sécurité et la stabilité du DNS, et jusqu'à quel point ses actions en matière de sécurité sont suffisamment robustes pour répondre aux menaces et aux défis futurs liés à la sécurité, la stabilité et la résilience du DNS, et ce conformément à la mission de l'ICANN.

iv. L'équipe de révision SSR examinera également la mesure dans laquelle les recommandations des révisions SSR précédentes ont été mises en œuvre et jusqu'à quel point leur mise en œuvre a eu l'effet souhaité.

v. La révision SSR sera menée au moins tous les cinq ans à compter de la date à laquelle s'est réunie l'équipe de révision SSR précédente ».

Recommandations de la SSR2 - Résumé

L'équipe de révision SSR2 a harmonisé toutes les recommandations de la SSR2 avec le plan stratégique 2021-2025 de l'ICANN[3], ses buts et objectifs. Le rapport précise les objectifs pertinents soutenus par les recommandations individuelles ; l'équipe de révision SSR2 a retiré de ce rapport toutes les recommandations n'étant pas clairement en ligne avec le plan stratégique.

Toutes les recommandations de l'équipe de révision SSR2 sont en ligne avec le plan stratégique de l'organisation ICANN et sont considérées comme prioritaires.

N°	Recommandation	Propriétaire	Priorité
1	**Terminer la mise en œuvre de toutes les recommandations de la SSR1 pertinentes**		Élevée

3 « Plan stratégique de l'ICANN pour les exercices fiscaux 2021 – 2025 », ICANN, dernière mise à jour le 29 mars 2019, , https://www.icann.org/public-comments/strategic-plan-2018-12-20-en.

2	**Recommandation 9 de la SSR1 - Systèmes de gestion de la sécurité de l'information et certifications de sécurité** 2.1. L'organisation ICANN devrait établir une feuille de route de ses audits de sécurité et de ses activités de certification conformes aux normes de l'industrie qui sont en cours d'exécution, y compris les dates spécifiques pour obtenir chaque certification et mettant l'accent sur les domaines d'amélioration continue. 2.2. L'organisation ICANN devrait élaborer un plan de certifications et de formation pour les rôles à remplir dans l'organisation, effectuer le suivi des taux d'achèvement, justifier leurs choix et documenter la manière dont les certifications s'intègrent aux stratégies de sécurité et de gestion des risques de l'organisation ICANN. 2.3. L'organisation ICANN devrait également justifier ses choix, tout en démontrant comment ils s'intègrent à ses stratégies de sécurité et de gestion des risques. 2.4. L'organisation ICANN devrait mettre en œuvre un système de gestion de la sécurité de l'information et se soumettre à l'audit d'un tiers. 2.5. Afin de bénéficier des avantages d'un régime de certification et d'audit, l'organisation ICANN devrait être auditée et certifiée par un tiers conformément aux normes de sécurité du secteur et devrait évaluer les options de certification de ses responsabilités opérationnelles avec des normes internationales généralement acceptées (par exemple ITIL, ISO 27001, SSAE-18).		Élevée
3	**Recommandations 12, 15 et 16 de la SSR1 - Stratégie et cadre de la sécurité, la stabilité et la résilience, indicateurs et divulgations de vulnérabilité** 3.1. L'organisation ICANN devrait aborder clairement et publiquement les questions relatives à la sécurité (en considérant la sécurité opérationnelle, par exemple, après un moratoire établi et l'anonymisation des informations, si cela s'avérait nécessaire), et promouvoir les meilleures pratiques en matière de sécurité chez toutes les parties contractantes. 3.2. L'organisation ICANN devrait également inclure les meilleures pratiques liées à la SSR dans un document consensuel, établir des objectifs clairs, mesurables et traçables, puis mettre en œuvre les pratiques dans les contrats, les accords et les MoU. 3.3. L'organisation ICANN devrait mettre en œuvre un rapport coordonné de divulgation de vulnérabilités. Les divulgations et les informations concernant les problèmes liés à la SSR devraient être communiquées rapidement aux parties concernées de confiance (par exemple, celles affectées ou requises pour résoudre le problème donné), comme dans les cas de violation de toute partie contractante et de vulnérabilités clés identifiées et informées à l'organisation ICANN. 3.4. L'organisation ICANN devrait établir un plan de communication clair pour les rapports à la communauté et produire des rapports réguliers (au moins annuels) et en temps opportun contenant des indicateurs anonymes du processus de divulgation des vulnérabilités. Ces communiqués devraient		Élevée

	contenir une divulgation responsable telle que définie par le processus convenu par la communauté et inclure des indicateurs anonymes.		
4	**Recommandations 20 et 22 de la SSR1 - Transparence budgétaire et budgétisation de la SSR dans les nouveaux gTLD** 4.1. Dans la mesure du possible (contractuellement) et du raisonnable en termes d'effort (c'est-à-dire plus de 10 % de l'activité décrite dans le poste budgétaire), l'ICANN devrait être plus transparente vis-à-vis du budget alloué aux secteurs de l'organisation ICANN liés à la mise en œuvre du cadre des systèmes d'identificateurs de sécurité, stabilité, et résilience (IS-SSR) et à l'exécution de fonctions liées à la SSR, y compris celles associées à l'introduction des nouveaux gTLD.		Moyenne
5	**Recommandation 27 de la SSR1 - Gestion des risques** 5.1. Le cadre de gestion des risques de l'ICANN devrait être centralisé et coordonné de manière stratégique. 5.2. L'organisation ICANN devrait articuler clairement son cadre de risques et l'aligner stratégiquement par rapport aux exigences et objectifs de l'organisation, en décrivant les mesures pertinentes de succès et la manière dont l'organisation ICANN évaluera ces mesures. 5.3. L'ICANN devrait mettre à la disposition de la communauté les informations relatives à la gestion des risques. Ces informations devraient être régulièrement mises à jour pour refléter le panorama actuel des risques (au moins une fois par an).		Élevée
6	**Créer un poste responsable de la sécurité stratégique et tactique et de la gestion des risques** 6.1. L'organisation ICANN devrait créer un poste responsable de la sécurité stratégique et tactique et de la gestion des risques dans le domaine de la sécurité interne de l'organisation, ainsi que du système d'identificateurs global externe. 6.2. L'organisation ICANN devrait embaucher une personne dûment qualifiée pour ce poste et allouer un budget spécifique suffisant pour exécuter les fonctions inhérentes à ce rôle. 6.3. Le responsable de ce poste devrait gérer la fonction de sécurité de l'organisation ICANN et superviser les interactions du personnel dans tous les domaines pertinents ayant un impact sur la sécurité. 6.4. Il devrait également fournir des rapports réguliers au Conseil d'administration et à la communauté de l'ICANN 6.5. et devenir un outil de recherche et de résolution de problèmes qui permettrait la mise en place de stratégies et l'exécution de programmes polyvalents pour obtenir des améliorations substantielles. 6.6. En outre, ce rôle devrait participer à toutes les négociations contractuelles relatives à la sécurité entreprises par		Élevée

	l'organisation ICANN (par exemple, les chaînes d'approvisionnement pour le matériel et les logiciels et les conventions de service y associés), et approuver toutes les dispositions contractuelles relatives à la sécurité.		
7	**Élaborer un cadre de gestion des risques de sécurité** 7.1. L'organisation ICANN devrait articuler clairement son cadre de gestion des risques de sécurité et s'assurer que ce dernier s'aligne stratégiquement avec les exigences et les objectifs de l'organisation. 7.2. L'organisation ICANN devrait décrire les mesures pertinentes de succès et la façon dont ces mesures doivent être évaluées. La SSR2 RT en a décrit les fondements en détail dans les commentaires supplémentaires concernant la recommandation 9 de la SSR1 (voir la ' Recommandation 9 de la SSR1 - Systèmes de gestion de la sécurité de l'information et certifications de sécurité' plus haut dans ce rapport). 7.3. L'organisation ICANN devrait : 7.3.1. Adopter et mettre en œuvre la norme ISO 31000 « Gestion des risques » et valider et certifier sa mise en œuvre par des audits indépendants appropriés.[4] Les efforts de gestion des risques devraient être déployés dans les plans de continuité des opérations et les plans et les dispositions de reprise des opérations après sinistre. 7.3.2. Mettre à jour régulièrement un registre des risques de sécurité et l'utiliser pour hiérarchiser et guider les activités de l'organisation ICANN. L'organisation ICANN devrait informer sur les mises à jour de sa méthodologie et du registre des risques de sécurité. Les conclusions devraient être intégrées aux plans de continuité des opérations et de reprise après sinistre (BC/DR) et au système de gestion de la sécurité de l'information (ISMS). 7.3.3. Nommer ou désigner une personne responsable et dédiée à la gestion des risques de sécurité qui informera le cadre supérieur chargé de la sécurité, comme décrit dans la recommandation « rôle de sécurité des cadres supérieurs ».		Élevée
8	**Établir un plan de continuité des opérations basé sur la norme ISO 22301** 8.1. L'organisation ICANN devrait établir un plan de continuité des opérations pour tous les systèmes appartenant à l'organisation ICANN, ou sous sa responsabilité, basé sur la norme ISO 22301 « gestion de la continuité des opérations ».[5] 8.2. L'ICANN devrait identifier l'importance de délais fonctionnels acceptables pour la continuité des opérations et la reprise		Élevée

4 Organisation internationale de normalisation, « ISO 31000, gestion des risques » , https://www.iso.org/iso-31000-risk-management.html.

5 "ISO 22301:2019 Sécurité et résilience — Systèmes de gestion de la continuité des opérations — Exigences," https://www.iso.org/standard/75106.html.

	après sinistre (BC/DR) en fonction de l'urgence de restaurer l'ensemble des fonctionnalités. 8.3. Pour les opérations des Identificateurs techniques publics (PTI) (fonctions IANA, y compris tous les systèmes pertinents qui contribuent à la sécurité et à la stabilité du DNS et également à la gestion de la zone racine), l'organisation ICANN devrait développer une approche partagée de la continuité des services en étroite collaboration avec le Comité consultatif du système des serveurs racine (RSSAC) et les opérateurs de serveurs racine. 8.4. L'organisation ICANN devrait publier des preuves (par exemple, un résumé) de ses plans et dispositions relatifs à la continuité des opérations. Un auditeur externe devrait être engagé pour vérifier les aspects liés à la conformité de la mise en œuvre des plans de continuité des opérations qui en résultent.		
9	**Assurez-vous que le plan de reprise après sinistre soit approprié, fonctionnel et bien documenté** 9.1. L'organisation ICANN devrait s'assurer que le plan de reprise après sinistre pour les opérations de la PTI (fonctions IANA) inclue tous les systèmes pertinents qui contribuent à la sécurité et à la stabilité du DNS, qui comprennent également la gestion de la zone racine et soient conformes aux *directives* de la norme ISO 27031 *relatives à la disponibilité des technologies de l'information et de la communication pour la continuité des opérations.* L'organisation ICANN devrait élaborer ce plan en étroite collaboration avec le RSSAC et les opérateurs de serveurs racine. 9.2. L'organisation ICANN devrait également établir un plan de reprise après sinistre pour tous les systèmes qui appartiennent à ou qui relèvent de l'organisation ICANN, conformément aux *directives* de la norme ISO 27031 *relatives à la disponibilité des technologies de l'information et de la communication pour la continuité des opérations.* 9.3. L'organisation ICANN devrait avoir un plan de reprise après sinistre développé dans les douze mois suivant l'adoption par le Conseil d'administration de l'ICANN de ces recommandations concernant l'établissement d'au moins un troisième site pour la reprise après sinistre (en plus de Los Angeles et Culpeper), plus précisément en dehors des États-Unis, de ses territoires et de la région d'Amérique du Nord, y compris un plan de mise en œuvre. 9.4. L'organisation ICANN devrait publier un résumé de ses plans et dispositions pour la reprise après sinistre à l'échelle mondiale. L'organisation ICANN devrait engager un auditeur externe pour vérifier les aspects liés à la conformité de la mise en œuvre de ces plans de reprise après sinistre.		Élevée
10	**Améliorer le cadre pour définir et mesurer la conformité des bureaux d'enregistrement et des opérateurs de registre**		Élevée

	10.1. Établir un cadre pour les indicateurs de performance dans le but de guider le niveau de conformité des bureaux d'enregistrement et des opérateurs de registre vis-à-vis des obligations en matière de WHOIS (y compris l'inexactitude), ainsi que d'autres éléments qui affectent les abus, la sécurité et la résilience, comme indiqué dans les révisions du RDS/WHOIS2 et de la CCT.[6,7] 10.2. Allouer un poste budgétaire spécifique à une équipe d'agents chargés de la conformité pour entreprendre ou mettre en service activement le travail des tests/évaluations de gestion de la performance des indicateurs convenus dans la SLA. 10.3. Modifier la clause de renouvellement de la SLA de 'renouvellement automatique' à un renouvellement cyclique tous les quatre ans incluant une clause de révision (cette période de révision devrait considérer le niveau de conformité des indicateurs de performance du bureau d'enregistrement et de l'opérateur de registre et recommander l'inclusion d'exigences pour renforcer la sécurité et la résilience au cas où la non-conformité serait évidente). 10.4. En outre, le Conseil d'administration de l'ICANN devrait assumer la responsabilité de mettre fin à l'EPDP[8] et de mettre en œuvre une politique WHOIS dans l'année suivant la publication de ce rapport.		
11	**Diriger les efforts visant à faire évoluer les définitions relatives à l'abus et permettre la création de rapports concernant ces définitions** 11.1. Le Conseil d'administration de l'ICANN devrait encourager les efforts visant à minimiser le langage ambigu et à parvenir à un accord universellement acceptable sur les abus, la SSR et les menaces à la sécurité dans ses contrats avec les parties contractantes et les plans de mise en œuvre. 11.2. L'organisation ICANN et le Conseil d'administration devraient mettre en œuvre les engagements relatifs à la SSR (ainsi que les recommandations de la révision de la CCT et du RDS/WHOIS2) sur la base des définitions actuelles contrôlées par la communauté concernant les abus, sans s'attarder[9].		Élevée

6 Équipe de révision RDS-WHOIS de l'ICANN, « Service d'annuaire de données d'enregistrement (RDS)- Révision WHOIS2 : Rapport final », 3 septembre 2019, https://www.icann.org/en/system/files/files/rds-whois2-review-03sep19-en.pdf.

7 « Concurrence, confiance et choix du consommateur : Rapport final », ICANN, 8 septembre 2018, https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf.

8 Organisation de soutien aux extensions génériques de l'ICANN, « Processus accéléré d'élaboration de politiques (EPDP) de la GNSO sur les recommandations de politique de la spécification temporaire relative aux données d'enregistrement des gTLD pour la considération du Conseil d'administration de l'ICANN », 1er mai 2019, https://www.icann.org/public-comments/epdp-recs-2019-03-04-en.

9 Le rapport de la CCT lui-même définit à la fois l'utilisation malveillante du DNS et l'utilisation malveillante de la sécurité du DNS, et invoque à la page 8, note en pied de page 11 des définitions approuvées contenues dans un

	11.3. Parallèlement, le Conseil d'administration de l'ICANN devrait encourager la communauté à faire évoluer la définition (et l'application) de l'utilisation malveillante du DNS et adopter le terme supplémentaire et la définition externe en évolution de la « menace à la sécurité »— terme utilisé par le projet de signalement des cas d'utilisation malveillante des noms de domaine (DAAR) de l'ICANN et par le GAC (dans son communiqué de Beijing[10] et pour la spécification 11[11]), et traité dans des conventions internationales telles que la Convention sur la cybercriminalité et ses « Notes explicatives » connexes — [12] à utiliser conjointement avec la définition de utilisation malveillante du DNS de l'organisation ICANN.[13] 11.4. Le Conseil d'administration de l'ICANN devrait confier au SSAC et au PSWG le travail avec des experts en matière de cybercriminalité et de fraude pour faire évoluer la définition de l'utilisation malveillante du DNS, compte tenu des processus et des définitions décrits dans la Convention sur la cybercriminalité.		
12	**Créer des mécanismes juridiques appropriés pour accéder aux données WHOIS** 12.1. Le Conseil d'administration de l'ICANN devrait créer des mécanismes juridiques d'accès aux données WHOIS appropriés pour des parties ayant fait l'objet d'un veto, telles que les agences d'application de la loi. 12.2. Le Conseil d'administration de l'ICANN devrait assumer la responsabilité et s'assurer que l'organisation ICANN arrive immédiatement à la fin de la mise en œuvre de la spécification temporaire relative aux données d'enregistrement des gTLD.		Élevée
13	**Améliorer l'exhaustivité et l'utilité du programme de signalement des cas d'utilisation malveillante des noms de domaine** 13.1. Le Conseil d'administration de l'ICANN et l'organisation ICANN devraient travailler avec les entités à l'intérieur et à l'extérieur de la communauté de l'ICANN qui atténuent les abus pour améliorer l'exhaustivité et l'utilité du DAAR dans le but		Élevée

document du personnel de l'ICANN intitulé « Sauvegardes contre l'utilisation malveillante du DNS du 18 juin 2016 ». En 2010, le groupe de travail sur les politiques en matière d'enregistrements frauduleux (RAP) a 'élaboré une définition consensuelle de la fraude', à savoir : « La fraude est une action qui : a) cause un préjudice réel et considérable, ou est le prédicat matériel d'un tel préjudice, et b) est illégale ou illégitime, ou est contraire à l'intention et au dessein d'un objectif légitime formulé, si un tel objectif est rendu public ». (Cette définition est citée avec approbation dans la page 88, note en bas de page 287 du rapport final de la CCT)

10 Comité consultatif gouvernemental de l'ICANN, « Avis du GAC : communiqué de Beijing de l'ICANN46 », dernière modification effectuée le 11 avril 2013, https://gac.icann.org/contentMigrated/icann46-beijing-communique.

11 ICANN, « Contrat de registre » , https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm.

12 Conseil de l'Europe, « Convention sur la cybercriminalité », ETS n° 185, p. 7, 23 novembre 2001, https://www.coe.int/en/web/cybercrime/the-budapest-convention.

13 Voir la note 50

	d'améliorer à la fois la mesure et l'information sur l'utilisation malveillante des domaines. 13.1.1. L'organisation ICANN devrait publier des rapports de DAAR qui identifient les opérateurs de registre et les bureaux d'enregistrement dont les domaines contribuent le plus aux abus selon la méthodologie DAAR. 13.1.2. L'organisation ICANN devrait rendre disponibles les données sources pour le DAAR par le biais de l'initiative d'ouverture des données de l'ICANN et hiérarchiser les éléments *« daar »* et « *daar-summarized* » de l'inventaire d'actifs de données de l'ODI[14] pour l'accès immédiat de la communauté. 13.1.3. L'organisation ICANN devrait publier des rapports qui incluent des formats de données lisibles par machine, en plus des données graphiques incluses dans les rapports actuels. 13.1.4. L'organisation ICANN devrait venir en aide au Conseil d'administration et à toutes les unités constitutives, groupes de parties prenantes et comités consultatifs, aux groupes d'intervenants et aux comités consultatifs pour l'interprétation du DAAR, y compris l'aide pour identifier les activités de politique et de conseil qui pourraient améliorer la prévention et l'atténuation de l'utilisation malveillante des noms de domaine.		
14	**Activer l'analyse quantitative rigoureuse de la relation entre les paiements pour les enregistrements de domaine et les preuves de menaces à la sécurité et d'utilisation malveillante du DNS** 14.1. L'organisation ICANN devrait recueillir, analyser et publier des données sur les prix afin de permettre des études indépendantes plus poussées et le suivi de la relation entre l'établissement des prix et les cas d'abus.		Élevée
15	**Améliorer les contrats avec les bureaux d'enregistrement et les opérateurs de registre dans le but d'encourager l'atténuation de l'utilisation malveillante du DNS** 15.1. L'organisation ICANN devrait rendre obligatoires les exigences en matière de SSR dans les contrats ou aux fins du renouvellement des contrats avec les parties contractantes, y compris les contrats de registre (contrats de base et contrats individuels) et le RAA. De telles exigences contractuelles devraient comprendre des dispositions qui établissent des seuils d'utilisation malveillante (p. ex., 3 % de tous les enregistrements) qui entraîneraient automatiquement des requêtes par rapport à la conformité, avec un seuil plus élevé (p. ex., 10 % de tous les enregistrements) au-dessus desquels l'organisation ICANN considère que les bureaux d'enregistrement et les opérateurs de registre manqueraient à		Élevée

[14] Voir : https://www.icann.org/en/system/files/files/odi-data-asset-inventory-spreadsheet-11jun18-en.csv tel que publié par le Bureau du CTO, disponible ici : https://www.icann.org/public-comments/odi-datasets-metadata-2018-06-11-en.

	leurs contrats. La révision de la CCT a également recommandé cette approche.[15] 15.2. L'organisation ICANN devrait incorporer une clause contractuelle soutenant la résiliation des contrats dans le cas d'une « pratique et recours systématique » à l'utilisation malveillante (comme dans l'article 5.5.2.4, « Durée, résiliation et résolution de conflits » du Contrat d'accréditation de bureaux d'enregistrement de 2013[16]. 15.3. Afin de soutenir la révision de ces modifications aux contrats, l'organisation ICANN devrait : 15.3.1. Garantir l'accès aux données d'enregistrement pour les parties ayant des fins légitimes à travers des obligations contractuelles et à travers des mécanismes de conformité rigoureux. 15.3.2. Établir et appliquer les exigences du service centralisé de données de zone afin d'assurer un accès continu aux fins de recherche en matière de SSR. 15.3.3. Attirer les ccTLD et la ccNSO et travailler en collaboration pour aider à résoudre l'utilisation malveillante du DNS et les menaces à la sécurité dans les ccTLD. 15.3.4. Le Conseil d'administration de l'ICANN, la communauté et l'organisation ICANN devraient travailler avec la ccNSO pour avancer dans le domaine du suivi et du rapport des données ainsi que dans celui de l'évaluation de l'utilisation malveillante du DNS et des menaces a la sécurité dans les ccTLD, et pour élaborer un plan de la ccNSO qui soutienne le travail des ccTLD afin d'atténuer davantage l'utilisation malveillante du DNS et les menaces à la sécurité. 15.3.5. Mettre immédiatement en place une exigence pour que les services RDAP des parties contractantes approuvent préalablement l'espace d'adresses de l'organisation ICANN et établissent un processus de contrôle d'autres entités que les services RDAP des parties contractantes pré-approuveront pour leur accorder un taux d'enregistrement illimité. 15.4. À plus long terme, le Conseil d'administration de l'ICANN devrait demander à la GNSO de lancer le processus d'adoption de nouvelles politiques et de conclusion de nouveaux contrats avec les parties contractantes qui améliorent de façon mesurable l'atténuation de l'utilisation malveillante du DNS et les menaces à la sécurité, y compris les modifications aux informations du RDAP et des titulaires de noms de domaine, qui incitent les parties contractantes à atténuer l'utilisation malveillante et les menaces à la sécurité, qui établissent un cadre de mesure de la performance et qui institutionnalisent la formation et les certifications pour les parties contractantes et les parties prenantes clés.		
16	**Encourager en termes de prix pour que les parties contractantes atténuent l'utilisation malveillante et les menaces à la sécurité**		Élevée

[15] Voir les recommandations 14, 15 et 16 dans le document « Concurrence, confiance et choix du consommateur : rapport final », https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf.

[16] « Contrat d'accréditation de bureaux d'enregistrement », ICANN, https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en.

	16.1. L'organisation ICANN devrait encourager l'atténuation de l'utilisation malveillante et des menaces à la sécurité à travers les modifications suivantes aux contrats : 16.1.1. Les parties contractantes avec des portefeuilles de moins d'un pourcentage spécifique (p. ex., 1 %) de noms de domaine malveillants (tels qu'identifiés par les fournisseurs commerciaux ou par le DAAR) devraient recevoir une réduction des frais (p. ex., une réduction des frais applicables ou une augmentation du frais de transaction applicable par nom de domaine, et offrir une remise au bureau d'enregistrement). 16.1.2. Les bureaux d'enregistrement devraient bénéficier d'une réduction des frais pour chaque nom de domaine enregistré au nom d'un titulaire de nom de domaine jusqu'à un seuil approprié. 16.1.3. Renoncer à des frais de RSEP lorsque les dépôts en raison de la RSEP indiquent clairement que la partie contractante a l'intention d'atténuer l'utilisation malveillante du DNS et qu'aucun registre RSEP ne reçoit l'approbation préalable si elle permet qu'un champ EPP au niveau du registre désigne les noms de domaine gérés par un titulaire de nom de domaine vérifié. 16.1.4. Les frais remboursables versés par les bureaux d'enregistrement et les opérateurs de registre pour des domaines qui sont identifiés comme malveillants et des menaces à la sécurité et qui sont suspendus dans un délai approprié après l'enregistrement (p. ex., 30 jours après l'enregistrement du domaine). 16.2. Compte tenu du fait que toutes les parties (l'organisation ICANN, les parties contractantes et d'autres parties prenantes essentielles telles que les opérateurs de registre, les bureaux d'enregistrement, les fournisseurs de services d'anonymisation et d'enregistrement fiduciaire, les fournisseurs de services Internet et les parties contractantes) doivent comprendre comment mesurer, surveiller, dépister et identifier avec précision l'utilisation malveillante du DNS, l'organisation ICANN devrait institutionnaliser la formation et les certifications de toutes les parties dans les domaines identifiés par le DAAR et d'autres sources comme des méthodes communes d'utilisation malveillante **[citation à ajouter]** et la façon de mettre en place des efforts d'atténuation appropriés. La formation devrait inclure comme point de départ : Le suivi automatique des numéros des plaintes et de leur traitement ; les rapports publics annuels/trimestriels sur les plaintes et les actions ; et l'analyse.		
17	**Établir un portail centralisé des rapports d'utilisation malveillante** 17.1. L'organisation ICANN devrait établir et entretenir un portail centralisé des plaintes sur l'utilisation malveillante du DNS qui envoie automatiquement tous les rapports d'utilisation malveillante aux parties concernées. Le système ne pourrait agir que comme un affluent, dans lequel les métadonnées et les récapitulatifs seraient envoyés en amont. L'utilisation du		Élevée

	système devrait être obligatoire pour tous les gTLD. Les ccTLD devraient être invités à s'y joindre. Les réponses doivent être accessibles publiquement et incluses dans les rapports annuels (en forme complète ou par référence). En outre, les rapports devraient être disponibles (p. ex., par e-mail) aux ccTLD qui ne participent pas.		
18	**S'assurer que les activités de conformité de l'ICANN soient neutres et efficaces** 18.1. L'organisation ICANN devrait faire vérifier ses activités de conformité à l'externe par un audit et suivre des normes exigeantes. 18.2. Le Conseil d'administration de l'ICANN devrait habiliter le Bureau de la conformité à réagir aux plaintes et à exiger à ce service de lancer des enquêtes et de faire respecter les obligations contractuelles à l'encontre de ceux qui aident et permettent l'utilisation malveillante systématique telle que définie par la SLA. Ce pouvoir supplémentaire pourrait inclure le soutien des actions progressives autour de l'escalade des mesures d'exécution et de mesures réalisables appropriées que l'organisation ICANN peut utiliser en réponse à tout manque de correction des manquements à la conformité dans les délais prescrits. 18.3. Le Bureau de la conformité de l'ICANN devrait, par défaut, inclure les SLA parmi ses exigences et ses rapports, des procédures claires et efficaces, un requérant pleinement informé, des mesures du niveau de satisfaction et un maximum de divulgation publique.		Élevée
19	**Mettre à jour la gestion des cas de nommage malveillant** 19.1. L'organisation ICANN devrait étayer son travail sur les activités actuelles pour enquêter sur les noms qui portent typiquement à confusion, en collaboration avec des chercheurs et des parties prenantes, le cas échéant. 19.2. Lorsque le nommage portant à confusion s'élève au niveau de nommage malveillant, l'organisation ICANN devrait inclure ce type d'abus dans ses rapports DAAR et élaborer des politiques et des meilleures pratiques d'atténuation. 19.3. L'organisation ICANN devrait publier le nombre de plaintes de nommage malveillant envoyées à travers le portail dans un format qui permette à des tiers indépendants d'analyser, atténuer et prévenir les dommages liés à l'utilisation de tels noms de domaine. 19.4. L'organisation ICANN devrait mettre à jour les « Lignes directrices pour la mise en œuvre des IDN » **[citation à ajouter]** pour inclure une section sur les noms contenant des marques déposées, des TLD en chaîne et l'utilisation d'erreurs de frappe (difficiles à identifier). En outre, l'ICANN devrait faire respecter par contrat les « Lignes directrices pour la mise en œuvre des IDN » dans le cas des gTLD et recommander que les ccTLD procèdent de la même façon.		Élevée

20	**Développement complet d'un test de régression du DNS** 20.1. L'organisation ICANN devrait compléter la mise au point d'une suite de tests de régression du DNS.[17] 20.2. L'organisation ICANN devrait garantir que la capacité d'exécuter des tests fonctionnels des différentes configurations et versions de logiciel soit mise en œuvre et entretenue.		Élevée
21	**Mettre en œuvre les recommandations des documents SAC063 et SAC073 et établir des procédures formelles pour les roulements de clés** 21.1. L'organisation ICANN devrait mettre en œuvre les recommandations des documents SAC063 et SAC073 afin de garantir la sécurité, la stabilité et la résilience du processus de roulement de la KSK. 21.2. L'organisation ICANN devrait établir une procédure formelle, étayée sur un outil de modélisation et de langage qui suive un processus formel, [18] pour spécifier les détails des roulements de clé futurs, y compris des points de décision, à l'exception de certains extraits, le plein contrôle du débit, etc. La vérification du processus de roulement de clé devrait inclure la publication de la procédure de programmation (p. ex., le programme ou le FSM) pour consultation publique, et intégrer les commentaires de la communauté. Le processus devrait remplir des critères d'acceptation vérifiables empiriquement à chaque étape pour que le processus continue. Ce processus devrait être réévalué au moins aussi souvent que le roulement lui-même (c.-à-d., avec la même périodicité) de sorte que les leçons tirées puissent être utilisées pour ajuster le processus. 21.3. L'organisation ICANN devrait créer un groupe de parties prenantes qui implique le personnel de l'ICANN (l'organisation ou la communauté) pour exécuter régulièrement des exercices de simulation qui suivent le processus de roulement de la KSK de la racine.		Élevée
22	**Établir des pratiques de sécurité de base pour les opérateurs de serveurs racine et les opérations** 22.1. L'organisation ICANN, en étroite collaboration avec le RSSAC et d'autres parties prenantes pertinentes, devrait s'assurer que le modèle de gouvernance du RSS tel que proposé par le RSSAC037 comprenne les meilleures pratiques de sécurité de base pour les opérateurs de serveurs racine et les opérations		Élevée

17 « Plateforme d'essai », référentiel GitHub de l'ICANN, https://github.com/icann/resolver-testbed.

18 Analyse itérative pour améliorer les propriétés clés des processus essentiels dépendant de l'activité humaine : un exemple de sécurité pendant les élections, Leon J. Osterweil, Matt Bishop, Heather Conboy, Huong Phan, Borislava I. Simidchieva, George Avrunin, Lori A. Clarke, Sean Peisert, Transactions ACM sur la confidentialité et la sécurité (TOPS), Vol. 20, n° 2, mai 2017, p. 5:1-31. (UM-CS-2016-012)

	afin de minimiser les risques affectant la sécurité, la stabilité et la résilience associés à l'exploitation du serveur racine. Ces meilleures pratiques devraient inclure la gestion des changements, les procédures de vérification et les procédures de contrôle de l'état de santé. 22.2. L'organisation ICANN devrait également mettre sur pied des indicateurs clés de performance (KPI) pertinents pour mesurer la mise en œuvre de ces meilleures pratiques et exigences, et garantir la publication de rapports publics annuels sur la façon dont les opérateurs de serveurs racine (RSO) et les autres parties pertinentes, y compris l'organisation ICANN, peuvent se conformer à ces KPI. 22.3. L'organisation ICANN devrait documenter les stratégies de renforcement du serveur racine exploité par l'ICANN (IMRS), communément connu sous le nom de « racine L », et encourager d'autres opérateurs de serveur racine à faire de même. 22.4. L'organisation ICANN devrait s'assurer que l'IMRS utilise un processus de divulgation des vulnérabilités (pas nécessairement public), qu'il publie des rapports de sécurité et de renseignements, qu'il communique avec les chercheurs et reçoive les conseils ou recommandations du RSSAC, le cas échéant.		
23	**Accélérer la mise en œuvre du RZMS de nouvelle génération** 23.1. Les équipes opérationnelles de l'ICANN et de la PTI devraient accélérer la mise en œuvre de nouvelles mesures de sécurité associées au RZMS liées à l'authentification et l'autorisation des modifications demandées. 23.2. L'organisation ICANN devrait lancer une consultation publique au plus tôt possible sur les changements concernant des révisions aux politiques du RZMS.		Élevée
24	**Créer une liste de statistiques et de mesures associées à l'état opérationnel du système d'identificateurs uniques** 24.1. L'organisation ICANN devrait créer une liste de statistiques et d'indicateurs qui reflètent le statut opérationnel (tel que la disponibilité et la réactivité) de chaque type d'information associée à un identificateur unique, tel que le service lié à la zone racine, les registres IANA et tout service gTLD qui soit dans la portée de l'autorité de l'organisation ICANN. 24.2. L'organisation ICANN devrait publier un répertoire de ces services, ensembles de données et mesures sur une seule page du site Web de l'organisation ICANN, par exemple dans la plateforme de données ouvertes. 24.3. L'ICANN devrait publier chaque année des récapitulatifs longitudinaux de ces données et demander les commentaires du public sur les récapitulatifs et les intégrer pour améliorer les rapports futurs. 24.4. Pour les deux séries de KPI, l'organisation ICANN devrait élaborer des récapitulatifs de l'année précédente et		Moyenne

	longitudinalement, demander et publier un résumé des commentaires de la communauté sur chaque rapport et incorporer ces commentaires pour améliorer les rapports de suivi ultérieurs.		
25	**Garantir la disponibilité continue de l'accès centralisé aux données contenues dans le fichier de zone** 25.1. La communauté de l'ICANN et l'organisation ICANN devraient prendre des mesures pour assurer que tant l'accès au CZDS que d'autres données soient disponibles, en temps voulu, et sans des obstacles inutiles pour les demandeurs. 25.2. L'organisation ICANN devrait mettre en œuvre les quatre recommandations du document SSAC 97 :[19] *« Recommandation 1 : Le SSAC recommande que le Conseil d'administration de l'ICANN suggère au personnel de l'ICANN d'envisager la révision du système CZDS pour résoudre le problème des abonnements résilies automatiquement par défaut, par exemple en permettant le renouvellement automatique par défaut des abonnements. Cela pourrait inclure une option permettant à un opérateur de registre de s'écarter de l'évaluation du cas par cas par défaut, obligeant ainsi l'abonné choisi à présenter une nouvelle demande à la fin de la période en cours. Le CZDS devrait continuer à donner aux opérateurs de registre la possibilité de résilier explicitement l'accès d'un abonné problématique à tout moment.* *Recommandation 2 : Le SSAC recommande que le Conseil d'administration de l'ICANN suggère au personnel de l'ICANN de s'assurer que dans les séries ultérieures de nouveaux gTLD, la convention d'abonnement au CZDS soit en ligne avec les changements exécutés à la suite de la mise en œuvre de la recommandation 1.* *Recommandation 3 : Le SSAC recommande que le Conseil d'administration de l'ICANN suggère au personnel de l'ICANN de chercher des moyens pour réduire le nombre de plaintes pour l'accès aux fichiers de zone, et de chercher des moyens pour résoudre les plaintes en temps opportun.* *Recommandation 4 : Le SSAC recommande que le Conseil d'administration de l'ICANN suggère au personnel de l'ICANN de s'assurer que l'accès au fichier de zone et les statistiques liées aux requêtes du WHOIS basé sur le web soient informés*		Élevée

19 Comité consultatif sur la sécurité et la stabilité de l'ICANN, « SAC097: rapport consultatif du SSAC concernant le service centralisé de données de zone (CZDS) et les rapports mensuels d'activité des opérateurs de registre ». 12 juin 2017, https://www.icann.org/en/system/files/files/sac-097-en.pdf.

	publiquement de manière précise, suivant des normes bien définies qui puissent être uniformément respectées par tous les opérateurs de registres gTLD. L'indicateur correspondant à l'accès au fichier de zone (ZFA) devrait être précisé dès que possible.		
26	**Documenter, améliorer et tester les processus de l'EBERO** 26.1. L'organisation ICANN devrait documenter publiquement les processus de l'EBERO, y compris les points de décision, les actions et les exceptions. Le document devrait décrire les dépendances de toute décision, action et exception. 26.2. Dans la mesure du possible, l'organisation ICANN devrait automatiser ces processus et les tester chaque année. 26.3. L'organisation ICANN devrait mener des tests de simulation publics de l'EBERO à des intervalles déterminés à l'aide d'un plan de test coordonné à l'avance avec les parties contractantes de l'ICANN afin de garantir que toutes les exceptions soient exercées et en publier les résultats. 26.4. L'organisation ICANN devrait améliorer le processus en permettant aux fournisseurs des services d'entiercement de données gTLD d'envoyer l'entiercement de données directement au fournisseur de l'EBERO.		Élevée
27	**Mise à jour de la DPS et création de consensus autour des futurs roulements de l'algorithme DNSKEY** 27.1. Les opérations de la PTI devraient mettre à jour la DPS pour faciliter la transition d'un algorithme de signature numérique à l'autre, y compris une transition précoce de l'algorithme de signature numérique RSA au ECDSA ou à des algorithmes après-quantiques futurs, ce qui créera un DNS plus résilient tout en offrant le même niveau de sécurité, voire davantage. 27.2. Étant donné que le roulement de l'algorithme DNSKEY de la racine est très complexe et délicat, l'équipe opérationnelle de la PTI devrait travailler avec les autres partenaires de la zone racine et la communauté internationale à l'élaboration d'un plan de consensus pour les roulements futurs de l'algorithme DNSKEY de la racine, compte tenu des leçons tirées du premier roulement de la KSK de la racine en 2018.		Moyenne
28	**Élaborer un rapport sur la fréquence de mesure des collisions de noms et proposer une solution** 28.1. L'organisation ICANN devrait parvenir à des résultats qui caractérisent la nature et la fréquence des collisions des noms et des préoccupations y associées. La communauté de l'ICANN devrait mettre en œuvre une solution avant la prochaine série de gTLD. 28.2. L'organisation ICANN devrait faciliter ce processus en lançant une étude indépendante des collisions de noms jusqu'à leur		Moyenne

	achèvement éventuel et adopter ou être responsable de l'application ou de la non-adoption de toute recommandation qui en découle. Par « étude indépendante », l'équipe de révision SSR2 veut dire que l'organisation ICANN devrait s'assurer que les résultats de l'équipe d'évaluation du rapport et de la recherche de l'équipe de travail en charge du projet d'analyse de la collision de noms du SSAC (NCAP) soient approuvés par les parties n'ayant aucun intérêt financier associé à l'expansion des TLD. 28.3. L'organisation ICANN devrait accepter les rapports communautaires sur les cas de collision de noms. Ces rapports devraient permettre le traitement approprié des données sensibles et des menaces à la sécurité et devraient être intégrés aux indicateurs de rapport communautaire.		
29	**Se focaliser sur la vie privée et les mesures de la sécurité, la stabilité et la résilience et améliorer les politiques basées sur ces mesures** 29.1. L'organisation ICANN devrait surveiller et informer périodiquement sur l'impact des technologies telles que DoT (DNS sur TLS) et DoH (DNS sur HTTPS) sur la vie privée. 29.2. Les politiques de consensus et les accords de l'organisation ICANN avec des opérateurs de registre et des bureaux d'enregistrement devraient, par conséquent, comporter des dispositions qui tiennent compte de la conformité avec ces premiers, tout en veillant à ce que le DNS ne soit pas fragmenté en raison de la nécessité de maintenir ou de mettre en place des exigences minimales applicables à la collecte, la conservation, l'entiercement, le transfert et l'affichage de données d'enregistrement, qui comprend les coordonnées du titulaire, ses informations administratives, ses informations de contact technique, ainsi que des informations techniques associées à un nom de domaine. 29.3. L'organisation ICANN devrait : 29.3.1. Créer des unités spécialisées au sein de la fonction de conformité contractuelle qui mettent l'accent sur la vie privée et les principes (tel que la limitation de la collecte, la qualification des données, la spécification des finalités et les mesures de sécurité pour la divulgation) et qui puissent faciliter l'application de la loi en vertu du cadre RDAP changeant. 29.3.2. Assurer le suivi et l'évolution de la législation pertinente concernant la vie privée (p. ex., du CCPA et de la législation qui protège les informations personnelles identifiables (PII)) et assurer que les politiques et les procédures de l'organisation ICANN soient alignées et en conformité avec les exigences relatives à la vie privée et la protection des informations personnelles identifiables, tel que requis par la législation et la réglementation pertinentes.[20]		Élevée

[20] L'équipe de révision est consciente que la charte de l'organisation ICANN définit une approche pour la participation gouvernementale

	29.3.3. Élaborer et tenir à jour une politique de protection des informations personnelles identifiables. La politique devrait être communiquée à toutes les personnes impliquées dans le traitement d'informations personnelles identifiables. Il s'avérerait convenable de mettre en œuvre des mesures techniques et organisationnelles qui protègent de façon appropriée les PII. 29.3.4. Effectuer des audits périodiques de la conformité aux politiques relatives à la vie privée mises en œuvre par les bureaux d'enregistrement pour s'assurer que celles-ci aient, à tout le moins, des procédures pour traiter les atteintes à la vie privée. 29.4. Le délégué à la protection des données (DPO) de l'organisation ICANN devrait également être responsable des PII des DNS externes. Le DPO devrait orienter les gestionnaires et les parties concernées au sujet des responsabilités et des procédures, et surveiller et informer des développements techniques pertinents.		
30	**Rester informé sur la recherche académique au sujet des questions liées à la sécurité, la stabilité et la résilience et utiliser ces informations pour enrichir les débats de politique** 30.1. L'organisation ICANN devrait suivre les avancées de la communauté de chercheurs évalués par les pairs, en se concentrant sur le réseautage et les conférences de recherche sur la sécurité, y compris au moins, ACM CCS, ACM Internet Measurement Conference, Usenix Security, CCR, SIGCOMM, IEEE S&P, ainsi que les conférences sur la sécurité opérationnelle APWG, M3AAWG et FIRST, et publier un rapport pour la communauté de l'ICANN qui résume les implications des publications qui ont trait au comportement de l'organisation ICANN ou des parties contractantes. 30.1.1. Ces rapports devraient comprendre des recommandations d'actions, y compris les changements aux contrats avec les registres et les bureaux d'enregistrement, qui pourraient atténuer, prévenir ou réparer les préjudices en matière de SSR pour les consommateurs et les infrastructures identifiées dans la documentation révisée par des pairs. 30.1.2. Ces rapports devraient également recommander une étude supplémentaire qui confirme les résultats révisés par les pairs, inclure une description des données qui seraient nécessaires pour mener à bien d'autres études recommandées, et expliquer comment l'ICANN peut offrir d'aider à garantir l'accès à de telles données, p. ex., CZDS.		Moyenne
31	**Clarifier les implications en matière de SSR du DNS-sur-HTTP** 31.1. L'organisation ICANN devrait commander une enquête indépendante des implications des tendances de déploiement		Élevée

https://www.icann.org/en/system/files/files/proposed-org-engagement-govt-standards-charter-25feb19-en.pdf et le rapport législatif (*the Tracker*) https://www.icann.org/legislative-report-2019. Cependant, nous aimerions mettre l'accent plus spécifiquement sur la vie privée et la protection des données.

	du DoH en matière de SSR, ainsi que leurs conséquences sur le rôle futur de l'IANA dans l'écosystème de l'Internet. L'objectif est de garantir que toutes les parties prenantes aient la possibilité de comprendre les implications de ces développements en matière de SSR et l'éventail d'alternatives (ou leur absence) qu'ont les diverses parties prenantes pour influencer l'avenir.		

Directrices pour les équipes de révisions SSR futures - Leçons clés

Afin de permettre des évaluations plus simples par les équipes de révision SSR futures, l'équipe de révision SSR2 s'efforcera de formuler ses propres recommandations suivant les critères SMART : dans la mesure du possible, les recommandations seront *spécifiques, mesurables, attribuables, pertinentes, et traçables*. L'équipe de révision SSR2 estime que des recommandations plus claires et des axées sur des mesures permettront de simplifier les processus de mise en œuvre, suivi et évaluation qui devra être entrepris par la prochaine révision SSR. L'équipe de révision SSR2 a inclus des informations supplémentaires sur le processus et la méthodologie utilisés par cette première pour s'acquitter de ses responsabilités dans l'Annexe C : Processus et méthodologie.'
