Rapport final de la deuxième équipe de révision de la sécurité, la stabilité et la résilience du DNS(SSR2) – Résumé analytique et recommandations

Extrait du rapport final de l’équipe de révision SSR2

25 janvier 2021

ICANN

TABLE DES MATIERES

A. Résumé analytique

En vertu de l'article 4.6(c) des statuts constitutifs de la Société pour l'attribution des noms de domaines et des numéros sur Internet :

« *Le Conseil d'administration effectuera une révision périodique du respect de l'engagement de l'ICANN à renforcer 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 d'Internet dont l'ICANN assure la coordination (« révision de la SSR »)* ».[1]

Les révisions de la SSR sont une partie critique du mandat de l'organisation ICANN [2]de « fonctionner autant que possible de manière ouverte et transparente, conformément aux procédures conçues pour assurer l'équité ». Il s'agit de la deuxième révision de la SSR qui, en vertu des statuts constitutifs, comprend une révision par l'organisation ICANN des recommandations de la première révision de la SSR ainsi que de nouvelles recommandations pour que l'organisation ICANN les prenne en considération.

L'équipe de révision SSR2 propose 24 groupes de recommandations, ce qui donne lieu à 63 recommandations spécifiques, à commencer par l'évaluation de la réponse de l'organisation ICANN aux recommandations de la SSR1. Nous avons adopté l'approche consistant à les diviser en recommandations très spécifiques en réponse au manque de spécificité des recommandations de la SSR1. Les recommandations sont ensuite structurées de manière à offrir un aperçu des opérations internes et de l'engagement de l'organisation ICANN (en particulier les contrats et le traitement des plaintes), et de la manière dont l'organisation ICANN peut prendre des mesures pour améliorer ses propres actions SSR et aider les autres à comprendre comment améliorer les leurs. Les recommandations contenues dans le document souvent dérivent des autres et incluent des dépendances entre elles. L'organisation ICANN et le Conseil d'administration doivent en tenir compte lors de l'élaboration des plans de mise en œuvre. L'équipe de révision est parvenue à un consensus complet sur chaque recommandation.

Pour aider les futures équipes de révision SSR à faire des évaluations plus efficaces, l'équipe de révision SSR2 s'est efforcée de formuler ses propres recommandations suivant les critères SMART : *spécifiques, mesurables, attribuables, pertinentes, et traçables*. Dans de nombreux cas, les détails requis pour rendre chaque recommandation pleinement SMART, y compris l'attribution des délais appropriés, nécessiteront une réflexion et des mesures de la part de l'équipe responsable de la mise en œuvre et devraient être inclus dans le plan final de mise en œuvre. L'équipe de révision a également proposé plusieurs suggestions concernant la façon dont les révisions futures pourraient être traitées, reconnaissant que ceci ne relève pas du mandat direct de la révision SSR elle-même. Des informations supplémentaires sur le processus et la méthodologie utilisés par cette première équipe de révision SSR2 pour s'acquitter de ses responsabilités sont disponibles dans l'annexe C : Processus et méthodologie.

[1] ICANN, « Statuts constitutifs de la société pour l'attribution des noms de domaine et des numéros sur Internet : Article 4.6(c) : Révisions spécifiques : révision de la sécurité, la stabilité et la résilience » modifiée le 28 novembre, https://www.icann.org/resources/pages/governance/bylaws-en/#article4.

[2] Article 3.1 des statuts constitutifs de l'ICANN : https://www.icann.org/resources/pages/governance/bylaws-en/.

1. Contexte

Comme indiqué à la section A.2., « Objectifs de la révision de la SSR », les statuts constitutifs de l'ICANN exigent une évaluation périodique de la sécurité, la stabilité et la résilience du système des noms de domaine (DNS). Le Conseil d'administration de l'ICANN a reçu le premier rapport formel de la révision SSR le 13 septembre 2012. Cinq ans plus tard, la deuxième révision a commencé avec la réunion initiale de l'équipe de révision SSR2, tenue le 2 mars 2017. Cependant, depuis sa création, l'équipe de révision SSR2 a rencontré plusieurs défis qui ont prolongé la durée de la révision bien au-delà de ce qui était prévu. L'équipe de révision SSR2 s'est réunie régulièrement jusqu'en octobre 2017, lorsque le Conseil d'administration a interrompu ses activités.[3] Les réunions ont repris avec de nouveaux membres le 19 juin 2018.[4]

Le paysage de l'écosystème global d'identificateurs uniques a continué d'évoluer au cours de la période prolongée du processus de révision. En dépit de la perturbation mondiale des activités et des déplacements résultant de la pandémie de COVID-19 qui a entraîné des retards supplémentaires dans le processus de révision SSR2, l'équipe de révision SSR2 a pu terminer son travail. Au cours de la dernière année du processus de révision, l'équipe a choisi de ne pas recommencer l'évaluation de ses recommandations initiales, mais plutôt de préserver leurs contributions fondamentales et historiques. L'équipe de révision estime que ces recommandations restent largement pertinentes pour l'organisation ICANN et pour soutenir la sécurité, la stabilité et la résilience du DNS mondial.

2. Objectifs de la révision SSR

En conformité avec l'article 4.6(c) des statuts constitutifs de l'ICANN : *« Le Conseil d'administration effectuera une révision périodique du respect de l'engagement de l'ICANN à renforcer 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 d'Internet dont l'ICANN assure la coordination (« révision SSR »)*[5].

Il indique en particulier que :

ii. L'équipe de révision SSR (« équipe de révision SSR ») pourra évaluer ce qui suit :

1. *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 ;*
2. *le respect d'un plan de mesures d'urgence approprié pour le système d'identificateurs uniques de l'Internet ;*

[3] Lettre du Dr Stephen D. Crocker, président du Conseil d'administration de l'ICANN, à l'équipe de révision SSR2, en date du 28 octobre 2017, https://www.icann.org/en/system/files/correspondence/crocker-to-ssr2-28oct17-en.pdf.

[4] ICANN, « La deuxième révision de la sécurité, la stabilité et la résilience du DNS (SSR2) recommence », blog du 7 juin 2018, https://www.icann.org/news/announcement-2-2018-06-07-en.

[5] Article 4.6(c) des statuts constitutifs de l'ICANN, https://www.icann.org/resources/pages/governance/bylaws-en.

3. *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'organisation ICANN a bien mis en œuvre ses actions en matière de sécurité, quelle a été l'efficacité de ses actions en matière de sécurité 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 enjeux 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 à quel point les recommandations formulées par les révisions SSR précédentes ont été mises en œuvre et dans quelle mesure la mise en œuvre de ces recommandations a abouti aux résultats escomptés.

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 ».

3. Influence des autres équipes de révision et des comités consultatifs

L'organisation ICANN devrait s'impliquer à plusieurs équipes de révision et comités consultatifs (AC), comme l'exigent les statuts constitutifs de l'ICANN. Bien que chacun de ces comités et équipes ait des mandats précis, les recommandations formulées par ces groupes peuvent se chevaucher sur les domaines de travail des autres équipes de révision et comités. L'équipe de révision SSR2 a évalué les recommandations d'autres équipes de révision et comités consultatifs afin de déterminer si leurs recommandations publiées ont eu un impact sur la sécurité, la stabilité et la résilience de l'organisation ICANN et du DNS mondial. Dans plusieurs cas, l'équipe de révision SSR2 a jugé nécessaire d'incorporer et de s'appuyer sur ces recommandations pour développer les directives relatives à la SSR pour l'organisation ICANN (voir en particulier la section E.1. Mesures de sauvegarde non atteintes pour le programme des nouveaux gTLD et la section E.3. Alternatives des PDP). L'équipe de révision SSR2 a considéré ces chevauchements sur les recommandations comme une corroboration tacite des mérites des questions correspondantes et a davantage considéré les accords entre les recommandations de l'équipe de révision et celles d'autres groupes comme un soutien empirique à leur nécessité. Les recommandations de la SSR2 sont destinées à compléter les recommandations de ces autres équipes de révision.

B. Recommandations de la SSR2

L'équipe de révision SSR2 est parvenue à un consensus complet sur chaque recommandation.

1. Tableau récapitulatif

Nº	Recommandation	Propriétaire	Priorité

Recommandation 1 de la SSR2 : révision des recommandations de la SSR1			
1.1	Le Conseil d'administration de l'ICANN et l'organisation ICANN doivent effectuer une révision plus approfondie des recommandations de la SSR1 et exécuter un nouveau plan pour achever la mise en œuvre de ces recommandations (voir l'annexe D : Conclusions relatives aux recommandations de la SSR1).	Conseil d'administration de l'ICANN et organisation ICANN	Faible
Recommandation 2 de la SSR2 : créer un poste de direction où le titulaire soit responsable de la sécurité stratégique et tactique et de la gestion des risques			
2.1	L'organisation ICANN devrait créer un poste responsable de la sécurité (CSO) ou responsable de la sécurité des informations (CISO) au niveau de la direction de l'organisation ICANN, embaucher une personne qualifiée pour ce poste et allouer un budget spécifique suffisant pour exécuter les fonctions liées à ce rôle.	Organisation ICANN	Moyenne - Élevée
2.2	L'organisation ICANN devrait inclure dans la description de ce rôle que le responsable gèrera la fonction de sécurité de l'organisation ICANN et supervisera les interactions du personnel dans tous les domaines pertinents ayant un impact sur la sécurité. Le responsable devrait être chargé de fournir des rapports réguliers au Conseil d'administration et à la communauté de l'ICANN sur toutes les activités liées à la sécurité, la stabilité et la résilience au sein de l'organisation ICANN. Les fonctions de sécurité existantes devraient être restructurées et réorganisées sur le plan organisationnel pour en informer ce nouveau directeur.	Organisation ICANN	Moyenne - Élevée
2.3	L'organisation ICANN devrait inclure dans la description de ce rôle que ce directeur sera responsable de la sécurité stratégique et tactique et de la gestion des risques. Ces domaines de responsabilité comprennent la responsabilité et la coordination stratégique d'une fonction centralisée d'évaluation des risques, la planification de la continuité des opérations (BC) et du plan de reprise après sinistre (DR) (voir également la recommandation 7 de la SSR2 : améliorer les processus et procédures de continuité des opérations et de reprise après sinistre) dans le domaine de la sécurité interne de l'organisation, y compris le serveur racine géré par l'ICANN (IMRS, communément dénommé racine-L), et coordonner avec d'autres parties prenantes impliquées dans le système	Organisation ICANN	Moyenne - Élevée

	d'identificateurs global externe, ainsi que publier une méthodologie et une approche d'évaluation des risques.		
2.4	L'organisation ICANN devrait inclure dans la description de ce rôle que ce cadre exécutif sera responsable de toutes les questions et responsabilités budgétaires liées à la sécurité et prendra part à toutes les négociations contractuelles relatives à la sécurité (par exemple, les contrats de registre et de bureau d'enregistrement, les chaînes d'approvisionnement pour le matériel et les logiciels, et les conventions de service y associées) entreprises par l'organisation ICANN, en signant toutes les conditions contractuelles liées à la sécurité.	Organisation ICANN	Moyenne - Élevée
Recommandation 3 de la SSR2 : améliorer la transparence budgétaire liée à la sécurité, la stabilité et la résilience			
3.1	Le cadre exécutif responsable de la sécurité (voir la recommandation 2 de la SSR2 : créer un poste de direction où le titulaire soit responsable de la sécurité stratégique et tactique et de la gestion des risques) devrait informer la communauté au nom de l'organisation ICANN au sujet de la stratégie, des projets et du budget SSR de l'organisation ICANN deux fois par an et mettre à jour et publier des aperçus de budget chaque année.	Organisation ICANN	Élevée
3.2	Le Conseil d'administration de l'ICANN et l'organisation ICANN devraient s'assurer que les éléments de budget spécifiques concernant la performance de l'organisation ICANN des fonctions liées à la SSR soient liés aux buts et objectifs spécifiques du plan stratégique de l'ICANN. L'organisation ICANN devrait mettre en œuvre ces mécanismes par le biais d'un processus de budgétisation et de rapport annuel cohérent et détaillé.	Conseil d'administration de l'ICANN et organisation ICANN	Élevée
3.3	Le Conseil d'administration de l'ICANN et l'organisation ICANN devraient créer, publier et demander des commentaires publics sur des rapports détaillés concernant les coûts et la budgétisation liés à la SSR dans le cadre du cycle du plan stratégique.	Conseil d'administration de l'ICANN et organisation ICANN	Élevée
Recommandation 4 de la SSR2 : améliorer les processus et les procédures de gestion des risques			
4.1	L'organisation ICANN devrait continuer à centraliser sa	Organisatio	Élevée

	gestion des risques, articuler clairement son cadre de gestion des risques de sécurité et s'assurer que cela s'aligne stratégiquement sur les exigences et les objectifs de l'organisation. L'organisation ICANN devrait décrire les mesures pertinentes de succès et la façon dont ces mesures doivent être évaluées.	n ICANN	
4.2	L'organisation ICANN devrait adopter et mettre en œuvre la norme ISO 31000 « Gestion des risques », valider et certifier sa mise en œuvre par des audits indépendants appropriés. L'organisation ICANN devrait mettre à la disposition de la communauté des rapports d'audit, potentiellement expurgés. Les efforts de gestion des risques devraient être inclus dans les plans et procédures de la BC et de la DR (voir la recommandation 7 de la SSR2 : améliorer les processus et procédures de continuité des opérations et de reprise après sinistre).	Organisation ICANN	Élevée
4.3	L'organisation ICANN devrait nommer ou désigner une personne responsable et dédiée à la gestion des risques de sécurité qui informera le cadre supérieur chargé de la sécurité (voir la recommandation 2 de la SSR2 : créer un poste de direction où le titulaire soit responsable de la sécurité stratégique et tactique et de la gestion des risques). Cette fonction devrait mettre à jour régulièrement, informer sur un registre des risques de sécurité et guider les activités de l'organisation ICANN. Les conclusions devraient être prises en compte dans les plans et les procédures de la continuité des opérations (BC) et la reprise après sinistre (DR) (voir la recommandation 7 de la SSR2 : améliorer les processus et procédures de continuité des opérations et de reprise après sinistre) et le système de gestion de la sécurité de l'information (ISMS) (voir la recommandation 6 de la SSR2 : se conformer aux systèmes de gestion de la sécurité de l'information et des certifications de sécurité).	Organisation ICANN	Élevée
Recommandation 5 de la SSR2 : se conformer aux systèmes de gestion de la sécurité de l'information et des certifications de sécurité			
5.1	L'organisation ICANN devrait mettre en œuvre un ISMS qui devrait être audité et certifié par un tiers selon les normes de sécurité de l'industrie (par exemple, ITIL, famille ISO 27000, SSAE-18) pour ses responsabilités opérationnelles. Le plan devrait inclure une feuille de route et des dates limites pour obtenir des certifications et noter les domaines qui seront la cible d'une amélioration continue.	Organisation ICANN	Élevée

5.2	Dans le cadre du ISMS, 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.	Organisation ICANN	Élevée
5.3	L'organisation ICANN devrait exiger que les parties externes qui fournissent des services à l'organisation ICANN soient conformes aux normes de sécurité pertinentes et documentent leur diligence raisonnable concernant les fournisseurs et les fournisseurs de services.	Organisation ICANN	Élevée
5.4	L'organisation ICANN devrait informer la communauté et au-delà en présentant des rapports clairs qui démontrent ce que l'organisation ICANN fait et réalise dans le domaine de la sécurité. Ces rapports seraient extrêmement utiles s'ils fournissaient des informations décrivant comment l'organisation ICANN suit les meilleures pratiques et établit des processus peaufinés et en constante amélioration pour gérer les risques, la sécurité et les vulnérabilités.	Organisation ICANN	Élevée
Recommandation 6 de la SSR2 : divulgation et transparence de la vulnérabilité de la SSR			
6.1	L'organisation ICANN devrait promouvoir de manière proactive l'adoption volontaire des meilleures pratiques et des objectifs de la SSR pour la divulgation de la vulnérabilité par les parties contractantes. Si les mesures volontaires s'avèrent insuffisantes pour atteindre l'adoption de telles meilleures pratiques et objectifs, l'organisation ICANN devrait mettre en œuvre les meilleures pratiques et objectifs dans les contrats, les accords et les protocoles d'accord.	Organisation ICANN	Élevée
6.2	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, tels que les violations au sein de toute partie contractante et les cas de vulnérabilités critiques découvertes et signalées à l'organisation ICANN, doivent être communiquées rapidement aux parties de confiance et concernées (par exemple, les personnes concernées ou requises pour résoudre le problème). L'organisation ICANN devrait faire régulièrement des rapports sur les vulnérabilités (au moins une fois par an), y compris les mesures	Organisation ICANN	Élevée

	anonymisées et en utilisant une divulgation responsable.		
Recommandation 7 de la SSR2 : améliorer les processus et procédures de continuité des opérations et de reprise après sinistre			
7.1	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 », identifiant des délais acceptables pour la continuité des opérations et la reprise après sinistre (BC/DR).	Organisation ICANN	Moyenne - Élevée
7.2	L'organisation ICANN devrait s'assurer que le plan de reprise après sinistre pour les opérations de l'entité Identificateurs techniques publics (PTI) (c'est-à-dire les 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 en conformité avec la norme ISO 27031. L'organisation ICANN devrait développer ce plan en étroite collaboration avec le Comité consultatif du système des serveurs racine (RSSAC) et les Opérateurs de serveur racine (RSO).	Organisation ICANN	Moyenne - Élevée
7.3	L'organisation ICANN devrait également établir un plan de reprise après sinistre pour tous les systèmes détenus par ou sous le mandat de l'organisation ICANN, toujours en conformité avec la norme ISO 27031.	Organisation ICANN	Moyenne - Élevée
7.4	L'organisation ICANN devrait établir un nouveau site pour la reprise après sinistre pour tous les systèmes appartenant à l'organisation ICANN ou sous son mandat, dans le but de remplacer les sites Los Angeles ou Culpeper ou d'ajouter un troisième site permanent. L'organisation ICANN devrait localiser ce site en dehors de la région de l'Amérique du nord et de tout territoire américain. Si l'organisation ICANN choisissait de remplacer l'un des sites existants, ce site ne devrait pas être fermé tant que l'organisation n'ait pas vérifié que le nouveau site soit entièrement opérationnel et capable de gérer la reprise après sinistre de ces systèmes pour l'organisation ICANN.	Organisation ICANN	Moyenne - Élevée
7.5	L'organisation ICANN devrait publier un résumé de ses plans et procédures pour la continuité des opérations et la reprise après sinistre à l'échelle mondiale. Cela améliorerait la transparence et la fiabilité au-delà des	Organisation ICANN	Moyenne - Élevée

	objectifs stratégiques de l'organisation ICANN. L'organisation ICANN devrait engager un auditeur externe pour vérifier les aspects liés à la conformité avec ces plans de continuité des opérations et de reprise après sinistre.		
Recommandation 8 de la SSR2 : permettre et démontrer la représentation de l'intérêt public dans les négociations avec les parties contractantes			
8.1	L'organisation ICANN devrait mettre en place une équipe de négociation comprenant des experts en matière d'abus et de sécurité non affiliés ou payés par des parties contractantes pour représenter les intérêts des entités non contractantes et travailler avec l'organisation ICANN pour renégocier les contrats des parties contractantes de bonne foi, avec transparence publique, et dans le but d'améliorer la SSR du DNS pour les utilisateurs finaux, les entreprises et les gouvernements.	Organisation ICANN	Moyenne
Recommandation 9 de la SSR2 : surveiller et appliquer la conformité			
9.1	Le Conseil d'administration de l'ICANN devrait demander à l'équipe chargée de la conformité de surveiller et d'appliquer strictement la conformité des parties contractantes aux obligations SSR actuelles et futures et aux obligations en matière d'abus dans les contrats, les accords de base, les spécifications temporaires et les politiques communautaires.	Conseil d'administration de l'ICANN	Élevée
9.2	L'organisation ICANN devrait surveiller et appliquer de manière proactive les obligations contractuelles des registres et des bureaux d'enregistrement afin d'améliorer l'exactitude des données d'enregistrement. Cette surveillance et cette application devraient inclure la validation des champs d'adresses et la réalisation de vérifications périodiques de l'exactitude des données d'enregistrement. L'organisation ICANN devrait concentrer ses efforts d'application sur les bureaux d'enregistrement et les opérateurs de registre ayant fait l'objet de plus de 50 plaintes ou rapports par an concernant la présentation de données auprès de l'organisation ICANN.	Organisation ICANN	Élevée
9.3	L'organisation ICANN devrait mener des activités de conformité auditées en externe au moins une fois par an et publier les rapports d'audit et la réponse de l'organisation ICANN aux recommandations d'audit, y compris les plans de mise en œuvre.	Organisation ICANN	Élevée

9.4	L'organisation ICANN devrait s'occuper de la fonction de conformité en publiant des rapports réguliers qui énumèrent les outils manquants qui aideraient à soutenir l'organisation ICANN dans son ensemble et à l'utilisation efficace des clauses contractuelles pour traiter les menaces de sécurité au DNS, y compris les mesures qui nécessiteraient des modifications aux contrats.	Organisation ICANN	Élevée
Recommandation 10 de la SSR2 : clarifier les définitions des termes relatifs à l'utilisation malveillante			
10.1	L'organisation ICANN devrait publier une page Web incluant sa définition pratique de l'utilisation malveillante du DNS, c'est-à-dire ce qu'elle utilise pour les projets, les documents et les contrats. La définition devrait signaler explicitement les types de menaces de sécurité que l'organisation ICANN, en vertu de son mandat, considère actuellement qu'il faut traiter par le biais de mécanismes contractuels et de conformité, ainsi que ceux qui, de l'avis de l'organisation ICANN, se trouvent en dehors de ses attributions. Si l'organisation ICANN utilisait une autre terminologie similaire, par exemple « une menace à la sécurité », « un comportement malveillant », elle devrait inclure à la fois sa définition de ces termes et la manière dont elle établit précisément une distinction entre ces termes et l'utilisation malveillante du DNS. Cette page devrait inclure des liens vers des extraits de toutes les obligations actuelles liées à l'utilisation malveillante dans les contrats avec les parties contractantes, y compris les procédures et protocoles pour répondre aux abus. L'organisation ICANN devrait mettre à jour cette page chaque année, inclure la date de la dernière version et fournir les liens vers des versions plus anciennes avec les dates de publication y associées.	Organisation ICANN	Élevée
10.2	Établir un groupe de travail intercommunautaire (CCWG) appuyé par le personnel afin d'établir un processus permettant de faire évoluer les définitions de l'interdiction de l'utilisation malveillante du DNS, au moins une fois tous les deux ans, selon un calendrier prévisible (par exemple, tous les mois de janvier), qui ne prendra pas plus de 30 jours ouvrables. Ce groupe devrait faire participer les parties prenantes de la protection des consommateurs, de la cybersécurité opérationnelle, de la recherche universitaire ou indépendante sur la cybersécurité, de l'application de la loi et du commerce électronique.	Organisation ICANN	Élevée

10.3	Le Conseil d'administration de l'ICANN et l'organisation ICANN devraient utiliser les définitions de consensus de manière cohérente dans les documents publics, les contrats, les plans de mise en œuvre de l'équipe de révision et d'autres activités, et faire en sorte que ces termes renvoient à cette page Web lorsqu'ils sont utilisés.	Organisation ICANN	Élevée
Recommandation 11 de la SSR2 : résoudre les problèmes d'accès aux données CZDS			
11.1	La communauté de l'ICANN et l'organisation ICANN devraient prendre des mesures pour assurer que l'accès au Service centralisé de données de zone (CZDS) soit disponible, en temps voulu, et qu'il n'y ait pas d'obstacles inutiles pour les demandeurs, par exemple le manque d'auto-renouvellement des informations d'identification d'accès.	Conseil d'administration de l'ICANN et organisation ICANN	Moyenne
Recommandation 12 de la SSR2 : réviser les efforts d'analyse et de signalement de l'utilisation malveillante du DNS pour permettre la transparence et la révision indépendante			
12.1	L'organisation ICANN devrait créer une équipe consultative d'analyse de l'utilisation malveillante du DNS composée d'experts indépendants (c'est-à-dire d'experts sans conflits d'intérêts financiers) pour recommander une refonte de l'activité de signalement d'abus du DNS avec des données exploitables, la validation, la transparence et la reproductibilité indépendante des analyses comme ses priorités les plus élevées.	Organisation ICANN	Moyenne
12.2	L'organisation ICANN devrait structurer ses accords avec les fournisseurs de données d'une manière qui permette le partage des données à des fins non commerciales, en particulier pour la validation ou la recherche scientifique examinée par des pairs. Cette licence non commerciale spéciale et gratuite pour utiliser les données peut impliquer un délai qui ne présente pas de conflit avec les opportunités de revenus commerciaux du fournisseur de données. L'organisation ICANN devrait publier tous les termes du contrat de partage de données sur le site Web de l'ICANN. L'organisation ICANN devrait mettre fin à tout contrat qui ne permette pas une vérification indépendante de la méthodologie derrière la liste de noms bloqués.	Organisation ICANN	Moyenne
12.3	L'organisation ICANN devrait publier des rapports qui	Organisatio	Moyenne

	identifient les opérateurs de registre et les bureaux d'enregistrement dont les domaines sont responsables de la plupart des cas d'abus L'organisation ICANN devrait inclure des formats de données lisibles par machine, en plus des données graphiques incluses dans les rapports actuels.	n ICANN	
12.4	L'organisation ICANN devrait rassembler et publier des rapports sur les actions prises par les opérateurs de registre et les bureaux d'enregistrement, soit volontaires, soit en réponse à des obligations juridiques, pour répondre à des plaintes pour conduite illégale et / ou malveillante basées sur les lois applicables en relation avec l'utilisation du DNS.	Organisation ICANN	Moyenne
Recommandation 13 de la SSR2 : accroître la transparence et la responsabilité du signalement des plaintes pour abus			
13.1	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 agirait purement comme un flux entrant, et l'organisation ICANN collecterait et traiterait uniquement le résumé et les métadonnées, y compris les horodatages et les types de plaintes (catégoriques). L'utilisation du système devrait devenir obligatoire pour tous les domaines génériques de premier niveau (gTLD) ; la participation de chaque domaine de premier niveau géographique (ccTLD) serait volontaire. En outre, l'organisation ICANN devrait partager les rapports d'abus (par exemple, par e-mail) avec tous les ccTLD.	Organisation ICANN	Élevée
13.2	L'organisation ICANN devrait publier le nombre de plaintes déposées sous une forme qui permette à des tiers indépendants d'analyser les types de plaintes concernant le DNS.	Organisation ICANN	Élevée
Recommandation 14 de la SSR2 : créer une spécification temporaire pour les améliorations de la sécurité fondées sur des données factuelles			
14.1	L'organisation ICANN devrait créer une spécification temporaire qui exige que toutes les parties contractantes maintiennent le pourcentage de domaines identifiés par l'activité de signalement d'abus DNS révisée (voir la recommandation 13.1 de la SSR2) comme abusive en dessous d'un seuil raisonnable et publié.	Organisation ICANN	Élevée

14.2	Pour permettre une action anti-abus, l'organisation ICANN devrait fournir aux parties contractantes des listes de domaines dans leurs portefeuilles identifiés comme abusifs, conformément à la recommandation 12.2 de la SSR2 concernant la révision indépendante des données et des méthodes pour la liste de domaines bloqués.	Organisation ICANN	Élevée
14.3	Si le nombre de domaines liés à une activité abusive atteignait le seuil publié décrit dans la recommandation 14.1 de la SSR2, l'organisation ICANN devrait mener une enquête pour confirmer la véracité des données et de l'analyse, puis émettre un avis à la partie concernée.	Organisation ICANN	Élevée
14.4	L'organisation ICANN devrait permettre aux parties contractantes un délai de 30 jours pour réduire la fraction de domaines abusifs en dessous du seuil ou pour démontrer que les conclusions ou les données de l'organisation ICANN sont erronées. Si une partie contractante ne parvenait pas à faire la rectification pendant 60 jours, le département de la conformité contractuelle de l'ICANN devrait passer au processus de désaccréditation.	Organisation ICANN	Élevée
14.5	L'organisation ICANN devrait envisager d'offrir des incitations financières : les parties contractantes avec des portefeuilles au-dessous d'un pourcentage donné de noms de domaine abusifs devraient recevoir une réduction des frais sur les transactions payantes jusqu'à un seuil approprié.	Organisation ICANN	Élevée
Recommandation 15 de la SSR2 : lancer un EPDP fondé sur des données factuelles pour améliorer la sécurité			
15.1	Après avoir créé la spécification temporaire (voir la recommandation 14 de la SSR2 : créer une spécification temporaire pour les améliorations de sécurité fondées sur des données factuelles), l'organisation ICANN devrait établir un processus accéléré d'élaboration de politiques (EPDP) soutenu par le personnel pour créer une politique anti-abus. Les volontaires de l'EPDP devraient représenter la communauté de l'ICANN, en utilisant les numéros et la distribution de la spécification temporaire pour les données d'enregistrement de gTLD comme modèle de charte de l'équipe responsable de l'EPDP.	Organisation ICANN	Élevée
15.2	L'EPDP devrait s'appuyer sur le fondement de la définition du CCWG proposée dans la recommandation 10.2 de la SSR2. Ce cadre de politique devrait définir	Organisation ICANN	Élevée

	des contre-mesures et des mesures correctives appropriées pour différents types d'abus, des délais pour les actions des parties contractantes tels que les délais des rapports d'abus/rapports de réponse et les actions d'application de la conformité contractuelle de l'ICANN en cas de violations de la politique. L'organisation ICANN devrait insister sur le pouvoir de résilier les contrats dans le cas de répétitions de conduites et de pratiques de protection des abus de la part de toute partie contractante. Le résultat devrait inclure un mécanisme de mise à jour des critères de référence et des obligations contractuelles liées aux abus tous les deux ans, en utilisant un processus qui ne prendrait pas plus de 45 jours ouvrables.		
Recommandation 16 de la SSR2 : exigences de confidentialité et RDS			
16.1	L'organisation ICANN devrait fournir des références croisées cohérentes sur son site Web afin de fournir des informations claires et faciles à trouver sur toutes les actions, passées, présentes et planifiées, prises au sujet de la confidentialité et de la gestion des données, en portant une attention particulière aux informations concernant le service d'annuaire de données d'enregistrement (RDS).	Organisation ICANN	Moyenne
16.2	L'organisation ICANN devrait créer des groupes spécialisés au sein de la fonction de conformité contractuelle qui comprennent les exigences et les principes de confidentialité (tels que la limitation de la collecte, la qualification des données, la spécification des objectifs, et des mesures de sécurité pour la divulgation) et qui puissent faciliter les besoins d'application de la loi dans le cadre du RDS, modifié et adopté par la communauté (voir également la recommandation 11 de la SSR2 : résoudre les problèmes d'accès aux données CZDS).	Organisation ICANN	Moyenne
16.3	L'organisation ICANN devrait effectuer des audits périodiques sur le respect des politiques de protection de la vie privée mises en œuvre par les bureaux d'enregistrement pour s'assurer que celles-ci aient mis en place des procédures pour traiter les atteintes à la vie privée.	Organisation ICANN	Moyenne
Recommandation 17 de la SSR2 : collision de noms			
17.1	L'organisation ICANN devrait créer un cadre qui caractérise la nature et la fréquence des collisions de	Organisation ICANN	Moyenne

	noms et des préoccupations y associées. Ce cadre devrait inclure des mesures et des mécanismes pour établir à quel point l'interruption contrôlée réussit à identifier et à éliminer les collisions de noms. Ceci peut être pris en charge par un mécanisme permettant d'activer la divulgation protégée des instances de collision de noms. Ce cadre devrait permettre le traitement approprié des données sensibles et des menaces à la sécurité.		
17.2	La communauté de l'ICANN devrait élaborer une politique claire pour éviter et gérer les collisions de noms liées à de nouveaux gTLD et mettre en œuvre cette politique avant la prochaine série de gTLD. L'organisation ICANN devrait s'assurer que l'évaluation de cette politique soit entreprise par les parties n'ayant aucun intérêt financier dans l'expansion des gTLD.	Conseil d'administration de l'ICANN et organisation ICANN	Moyenne
Recommandation 18 de la SSR2 : informer les débats sur les politiques			
18.1	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, le Symposium sur la sécurité et la vie privée de l'IEEE, ainsi que les conférences sur la sécurité opérationnelle 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.	Organisation ICANN	Faible
18.2	L'organisation ICANN devrait assurer que ces rapports comprennent des observations pertinentes pouvant avoir trait à des recommandations d'actions, y compris les changements aux contrats avec les opérateurs de registre 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.	Organisation ICANN	Faible
18.3	L'organisation ICANN devrait également recommander que ces rapports incluent des recommandations pour des études supplémentaires qui confirment les résultats révisés par les pairs, une description des données qui seraient nécessaires pour mener à bien d'autres études, et expliquer comment l'organisation ICANN peut offrir d'aider à garantir l'accès à de telles données,	Organisation ICANN	Faible

	par exemple, via le CZDS.		
Recommandation 19 de la SSR2 : développement complet d'un test de régression du DNS			
19.1	L'organisation ICANN devrait compléter la mise au point d'une suite de tests de comportement des résolveurs du DNS.	Organisation ICANN	Faible
19.2	L'organisation ICANN devrait garantir que la capacité de continuer à exécuter des tests fonctionnels des différentes configurations et versions de logiciel soit mise en œuvre et entretenue.	Organisation ICANN	Faible
Recommandation 20 de la SSR2 : procédures officielles pour les roulements de clé			
20.1	L'organisation ICANN devrait établir une procédure formelle, étayée sur un outil de modélisation et de langage qui suive un processus formel, pour spécifier les détails des roulements de clé futurs, y compris des points à décider, 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 (par exemple, le programme ou l'automate avec un nombre défini d'états (FSM)) pour consultation publique et l'organisation ICANN devrait 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'est-à-dire, avec la même périodicité) de sorte que l'organisation ICANN puisse utiliser les leçons apprises pour ajuster le processus.	Organisation ICANN	Moyenne
20.2	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.	Organisation ICANN	Moyenne
Recommandation 21 de la SSR2 : améliorer la sécurité des communications avec les opérateurs de TLD			
21.1	Les opérations de l'organisation ICANN et de la PTI devraient accélérer la mise en œuvre de nouvelles mesures de sécurité du système de gestion de la zone racine (RZMS) concernant l'authentification et l'autorisation des modifications demandées et offrir aux opérateurs de TLD la possibilité de tirer parti de ces	Organisation ICANN et Conseil d'administration de l'ICANN	Moyenne

	mesures de sécurité, en particulier l'authentification MFA et les e-mails chiffrés.		
Recommandation 22 de la SSR2 : mesures du service			
22.1	Pour chaque service qui relève de l'autorité de l'organisation ICANN, y compris les services liés à la zone racine et aux gTLD, ainsi que les registres IANA, l'organisation ICANN devrait créer une liste de statistiques et de mesures qui reflètent l'état opérationnel (comme la disponibilité et la réactivité) de ce service, et publier un répertoire de ces services, ensembles de données et mesures sur une seule page du site Web icann.org, par exemple sous la plateforme de données ouvertes (ODP). L'organisation ICANN devrait produire des mesures pour chacun de ces services sous forme de résumés à la fois au cours de l'année précédente et longitudinalement (pour illustrer le comportement de base).	Organisation ICANN	Faible
22.2	L'organisation ICANN devrait demander chaque année des commentaires de la communauté sur les mesures. Cette rétroaction devrait être prise en considération, résumée publiquement après chaque rapport et incorporée dans les rapports de suivi. Les données et les méthodologies associées utilisées pour mesurer les résultats de ces rapports devraient être archivées et rendues publiques afin de favoriser la reproductibilité.	Organisation ICANN	Faible
Recommandation 23 de la SSR2 : roulement de l'algorithme			
23.1	Les opérations de la PTI devraient mettre à jour la déclaration de pratiques DNSSEC (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 à d'autres algorithmes ou à des algorithmes après-quantiques futurs, ce qui créera une sécurité équivalente ou même supérieure et préservera ou améliorera la résilience du DNS.	PTI	Moyenne
23.2	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.	PTI	Moyenne

Recommandation 24 de la SSR2 : améliorer la transparence et les tests de bout en bout pour le processus EBERO			
24.1	L'organisation ICANN devrait coordonner les tests de bout en bout du processus EBERO complet à des intervalles prédéterminés (au moins une fois par an) en utilisant un plan de test qui inclue des ensembles de données utilisés pour les tests, les états de progression et les délais, et qui soit 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.	Organisation ICANN	Moyenne
24.2	L'organisation ICANN devrait faciliter la recherche du manuel du processus de transition commun en fournissant des liens sur le site Web de l'EBERO.	Organisation ICANN	Moyenne

2. Établissement des priorités

L'équipe de révision SSR2 a harmonisé toutes les recommandations de la SSR2 avec le plan stratégique pour les exercices fiscaux 2021 à 2025 de l'ICANN, ses buts et objectifs.[6] L'équipe de révision a retiré de ce rapport toute recommandation qui ne s'harmonise pas clairement 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 importantes.

L'équipe de révision SSR2 a utilisé un outil d'enquête en ligne (la solution Qualtrics, basée sur Internet) pour interroger tous les membres de l'équipe sur la priorité de chaque groupe de recommandations dans ce rapport.[7] Cette enquête a permis de classer chaque groupe sur une échelle de cinq points, à savoir : priorité très faible, priorité faible, priorité moyenne, priorité élevée et très haute priorité.

L'équipe de révision a déterminé que sur les vingt-quatre groupes de recommandations, vingt-sept recommandations spécifiques dont la plupart concernent la gestion interne de la sécurité de l'organisation ICANN et les actions anti-abus devraient être considérées comme étant de priorité élevée. Neuf recommandations sont de priorité moyenne-élevée. Dix-huit recommandations, provenant principalement des sections mondiales du DNS, ont été classées en priorité moyenne, et les huit recommandations restantes ont été classées en priorité faible.

[6] Voir l'annexe G : Mappage des recommandations de la SSR2 pour le plan stratégique de l'ICANN des exercices fiscaux 2021 à 2025 et pour les statuts constitutifs de l'ICANN.

[7] Voir https://www.qualtrics.com/.

C. Mise en œuvre et effets escomptés des recommandations de la SSR1

En 2012, le Conseil d'administration de l'ICANN a constaté *« que les 28 recommandations du rapport final [SSR1] sont réalisables et applicables »*, et a unanimement accepté et demandé au personnel de mettre en œuvre les 28 recommandations de la SSR1.[8] Une des tâches de l'équipe de révision SSR2 était d'évaluer « *la mesure dans laquelle les recommandations des révisions précédentes de la SSR ont été mises en œuvre et à quel point leur mise en œuvre a eu l'effet souhaité* ».

Le processus et la méthodologie utilisés par l'équipe de révision SSR2 pour évaluer les mises en œuvre et leurs effets sont résumés à l'annexe C : Processus et méthodologie. Cette section décrit le processus d'évaluation, les types de preuves et de données utilisées, ainsi que la méthodologie adoptée pour parvenir à une conclusion sur le niveau de mise en œuvre des recommandations. Les conclusions et les fondements à l'appui de l'équipe de révision SSR2 pour chacune des recommandations de la SSR1 sont présentés à l'annexe D : Conclusions relatives aux recommandations de la SSR1.

Chaque révision est une occasion d'apprentissage et, après avoir évalué les recommandations de la SSR1, l'équipe de révision SSR2 signale l'importance et la nécessité de fournir des recommandations basées sur des indicateurs de performance mesurables, ce qui a souvent manqué dans les recommandations de la SSR1. Cette observation est étayée par la nécessité d'assurer une mise en œuvre et une évaluation efficaces des recommandations de toute future équipe de révision.

[8] ICANN, « Réunion ordinaire du Conseil d'administration de l'ICANN », dernière mise à jour le 18 octobre 2012, https://www.icann.org/resources/board-material/minutes-2012-10-18-en et « Rapport final de la sécurité, de la stabilité et de la résilience de l'équipe de révision du DNS », équipe de révision SSR, 20 juin 2012, https://www.icann.org/en/system/files/files/final-report-20jun12-en.pdf.

1. Résumé : révision de la SSR1

L'équipe de révision SSR2 a examiné les 28 recommandations de la SSR1 et a constaté qu'elles restent toutes pertinentes à la date de publication du présent rapport (voir le tableau 2).[9] L'équipe considère qu'aucune recommandation n'a été pleinement mise en œuvre, pour les raisons décrites à l'annexe D : Conclusions relatives aux recommandations de la SSR1.

Tableau 2 : aperçu de la recommandation de la SSR1

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Pertinent	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Mise en œuvre	P	P	P	P	P	N	P	P	-	P	P	P	N	N	P	P	-	N	-	P	P	P	P	P	P	P	P	P
Efficace	N	N	N	Y	-	N	N	N	-	N	-	N	N	N	-	N	-	-	N	N	N	N	-	N	N	-	N	N

Clé : Y = Oui ; N = Non ; P = Partielle ; - = Impossible à déterminer

L'équipe de révision SSR2 prend note des problèmes suivants qui sont réapparus :

1. Il y a généralement un manque d'indicateurs, de mesures et de règles du jeu dans les recommandations de la SSR1 et les plans de mise en œuvre associés qui permettraient à la communauté et à l'organisation ICANN de suivre et de comprendre l'espace de sécurité et leurs propres activités.

2. Il y a un manque de preuves, de définitions et de procédures accessibles au public, ce qui empêche l'observation indépendante des activités liées à la SSR. Cette pénurie d'informations entraîne un manque de clarté quant à la manière dont l'organisation ICANN a mis en œuvre les recommandations de la SSR1.

3. Il y a un manque de révision et de responsabilité de la communauté par rapport aux différents plans de mise en œuvre, ce qui empêche la communauté de l'ICANN d'avoir l'opportunité de fournir des commentaires sur les questions relatives à la SSR.

4. L'organisation ICANN ne dispose actuellement pas d'une stratégie globale, d'objectifs identifiables ou d'une politique claire et complète en matière de sécurité, stabilité et résilience. Sans une stratégie SSR fonctionnelle et une gestion intégrée de la sécurité et des risques (par exemple, politiques, procédures, normes, lignes de base, lignes directrices), les responsabilités liées à la SSR ne sont pas attribuées, mesurées et suivies, ce qui entraîne un manque de transparence, de responsabilité et des lacunes apparentes dans les responsabilités de l'organisation ICANN liées à la SSR.

L'équipe de révision SSR2 reconnaît que les directives initiales fournies par l'équipe de révision SSR1 n'étaient pas dans tous les cas suffisamment mesurables, et bien que l'organisation

[9] ICANN, Rapport de mise en œuvre de la révision de la SSR, juin 2015 https://www.icann.org/en/system/files/files/ssr-review-implementation-30jun15-en.pdf.

ICANN ait indiqué qu'elle croyait que toutes les recommandations ont été traitées, les plans de mise en œuvre de ces recommandations étaient souvent peu clairs et insuffisamment mesurables. L'équipe de révision SSR2 n'a donc pas pu confirmer que la mise en œuvre des recommandations de la SSR1 ait été terminée. L'organisation ICANN devrait effectuer une révision plus approfondie de la mise en œuvre des recommandations de la SSR1, en tenant compte des conclusions proposées par l'équipe de révision SSR2.

Ce rapport propose également des suggestions qui ne relèvent pas de la portée directe de la révision de la SSR2 (voir annexe A - Autres suggestions) pour permettre aux futures équipes de révision d'éviter certains des défis rencontrés par l'équipe de révision SSR2.

Recommandation 1 de la SSR2 : révision approfondie des recommandations de la SSR1

1.1. Le Conseil d'administration de l'ICANN et l'organisation ICANN doivent effectuer une révision plus approfondie des recommandations de la SSR1 et exécuter un nouveau plan pour achever la mise en œuvre de ces recommandations (voir l'annexe D : Conclusions relatives aux recommandations de la SSR1).

D. Questions clés liées à la stabilité au sein de l'ICANN.

Cette section est axée sur les domaines liés aux articles 4.6(c) (ii) A, 4.6(c) (ii) B et 4.6(c) (iii) des statuts constitutifs de l'ICANN.[10] Ces domaines comprennent les questions de sécurité, de stabilité opérationnelle et de résilience, tant physiques qu'au niveau du réseau, relatives à la coordination du système d'identificateurs uniques d'Internet ; le cadre de mesures d'urgence de sécurité pour le système d'identificateurs uniques d'Internet ; et l'exhaustivité et l'efficacité des processus de sécurité internes de l'organisation ICANN et du cadre de sécurité de l'ICANN.

La question fondamentale qui éclaire les recommandations de cette section est le manque de preuves vis-à-vis de la disposition de l'équipe de révision SSR2 qui démontrent un programme SSR efficace, complet et transparent pour l'organisation ICANN. Au cours de la révision par l'équipe de la sécurité interne de l'organisation ICANN, il était évident que l'organisation ICANN a entrepris divers projets et a pris des mesures de sécurité pertinentes. L'équipe de révision n'a toutefois pas vu de preuves suffisamment complètes d'un programme de gestion et de sécurité de l'information correctement géré et documenté (voir la section D.3. Gestion des risques et de la sécurité), des processus de continuité des opérations (BC) et de reprise après sinistre (DR) (voir la section D.4. Gestion de la continuité des opérations) ou d'une structure de sécurité largement indépendante adaptée à une organisation qui prenne en charge un système essentiel au fonctionnement de l'Internet (voir la section D.1. Améliorations de la structure organisationnelle).

[10] Consulter l'annexe H - Statuts constitutifs et les sections du plan stratégique les plus pertinentes pour les recommandations de la SSR2 qui apparaissent dans le présent rapport pour y voir repris les articles des statuts constitutifs de l'ICANN et du plan stratégique pour les exercices fiscaux 2021 à 2025 qui sont les plus pertinents pour la SSR.

Conformément à ses statuts constitutifs, l'organisation ICANN doit *« fonctionner autant que possible de manière ouverte et transparente, conformément aux procédures conçues pour assurer l'équité »*.[11] Les recommandations de cette section sont proposées pour aider l'organisation ICANN à améliorer la divulgation et la transparence de la SSR dans tous les aspects de l'organisation, dans la mesure du possible en tenant compte des objectifs de sécurité. En suivant ces recommandations, l'organisation ICANN résoudra avec efficience et efficacité la question fondamentale de la transparence des informations et du manque de direction et d'organisation en matière de sécurité claire et démontrable.

1. Améliorations de la structure organisationnelle - Rôle du cadre supérieur responsable de la sécurité.

Actuellement, l'organisation ICANN divise les activités liées à la SSR à travers l'organisation. L'équipe de révision SSR2 reconnaît les rôles du Bureau du directeur de la technologie (OCTO), qui a des responsabilités, notamment :

La recherche de questions liées au système d'identificateurs uniques d'Internet (noms de domaine, adresses IP/NUMÉROS AS, paramètres de protocole, etc.)

Le soutien à l'amélioration de la sécurité, de la stabilité et de la résilience de ces identificateurs.[12]

Et le directeur de l'information, qui est généralement responsable du *« suivi et de l'entretien des systèmes et des opérations techniques de l'ICANN, de la sécurité d'entreprise et de la technologie de l'information, et de l'équipe d'ingénierie du DNS de l'ICANN (http://www.dns.icann.org/), qui administre la racine L et les services de réseau du DNS de l'ICANN, »*[13] ainsi que la sécurisation, la surveillance, et la gestion des ressources de données, tels que les données privées des parties contractantes.

L'organisation ICANN devrait désigner un cadre responsable de toutes les questions liées à la sécurité, y compris la définition des objectifs stratégiques, la gestion de la conformité réglementaire et de la budgétisation et la sécurisation des actifs de l'organisation.[14]

Plusieurs des mandats établis dans les statuts constitutifs et les engagements de l'ICANN assumés dans son plan stratégique pour les exercices fiscaux 2021 à 2025 seraient du ressort de ce cadre supérieur. En outre, la recommandation 24 de la SSR1 prévoyait la création d'une équipe du service de sécurité.[15] La structure actuelle répartit ces responsabilités entre deux unités distinctes au sein de l'organisation ICANN. La gestion centralisée piloterait plus

[11] Article 3.1 des statuts constitutifs de l'ICANN, https://www.icann.org/resources/pages/governance/bylaws-en/#article3

[12] Bureau du directeur de la technologie (OCTO), ICANN, consulté le 27 décembre 2019, https://www.icann.org/octo.

[13] ICANN, « Systèmes d'information et innovation », consulté le 21 janvier 2020, https://www.icann.org/resources/pages/technical-functions-cio.

[14] L'Institut des sciences de l'éducation (IES) : Centre national de statistiques de l'éducation, « CHAPITRE 3 - Politique de sécurité : développement et mise en œuvre », consulté le 9 décembre 2020, https://nces.ed.gov/pubs98/safetech/chapter3.asp.

[15] Consulter l'annexe A : Conclusions relatives aux recommandations de la SSR1.

efficacement l'alignement stratégique de toutes les activités connexes en consolidant le travail sous un seul rôle, avec un budget adapté.[16] Cela appuiera les efforts visant à mettre à la disposition de la communauté et des futures équipes de révision une documentation cohérente et homogène.

Recommandation 2 de la SSR2 : désigner un cadre responsable de la sécurité stratégique et tactique et de la gestion des risques

L'équipe de révision SSR2 considère qu'il est nécessaire que l'organisation ICANN ait un responsable au niveau de la direction pour coordonner et gérer de manière stratégique les activités liées à la sécurité et aux risques de l'organisation ICANN et pour mettre en œuvre la mission et les objectifs stratégiques de sécurité de l'organisation ICANN.[17]

2.1. L'organisation ICANN devrait désigner un cadre responsable de la sécurité (CSO) ou responsable de la sécurité des informations (CISO) au niveau de la direction de l'organisation ICANN, embaucher une personne qualifiée pour ce poste et allouer un budget spécifique suffisant pour exécuter les fonctions liées à ce rôle.

2.2. L'organisation ICANN devrait inclure dans la description de ce rôle que le responsable gèrera la fonction de sécurité de l'organisation ICANN et supervisera les interactions du personnel dans tous les domaines pertinents ayant un impact sur la sécurité. Le responsable devrait être chargé de fournir des rapports réguliers au Conseil d'administration et à la communauté de l'ICANN sur toutes les activités liées à la sécurité, la stabilité et la résilience au sein de l'organisation ICANN. Les fonctions de sécurité existantes devraient être restructurées et réorganisées sur le plan organisationnel pour en informer ce nouveau directeur.

2.3. L'organisation ICANN devrait inclure dans la description de ce rôle que ce directeur sera responsable de la sécurité stratégique et tactique et de la gestion des risques. Ces domaines de responsabilité comprennent la responsabilité et la coordination stratégique d'une fonction centralisée d'évaluation des risques, la planification de la continuité des opérations (BC) et du plan de reprise après sinistre (DR) (voir la recommandation 7 de la SSR2 : améliorer les processus et procédures de continuité des opérations et de reprise après sinistre) dans le domaine de la sécurité interne de l'organisation, y compris le serveur racine géré par l'ICANN (IMRS, communément dénommé racine-L), et coordonner avec d'autres parties prenantes impliquées dans le système d'identificateurs global externe, ainsi que publier une méthodologie et une approche d'évaluation des risques.

[16] Voir la clause 5.1 dans les normes de l'Organisation internationale de normalisation et des normes ISO 27001, ISO/IEC 27001:2013 technologies de l'information — techniques de sécurité — systèmes de gestion de la sécurité de l'information — exigences, qui correspondent également au principe 3 CC1.3/COSO du SSAE18 2017 critères des services fiables, https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/othermapping/trust-services-map-to-iso-27001.xlsx.

[17] Le Conseil d'administration de l'ICANN peut être guidé par des ressources telles que le Manuel des risques de cybersécurité : Association nationale des directeurs d'entreprise, « Manuel du directeur de la NACD sur la surveillance des risques cybernétiques », 2017, http://boardleadership.nacdonline.org/Cyber-Risk-Handbook-GCNews.html.

2.4. L'organisation ICANN devrait inclure dans la description de ce rôle que ce cadre exécutif sera responsable de toutes les questions et responsabilités budgétaires liées à la sécurité et prendra part à toutes les négociations contractuelles relatives à la sécurité (par exemple, les contrats de registre et de bureau d'enregistrement, les chaînes d'approvisionnement pour le matériel et les logiciels, et les conventions de service y associées) entreprises par l'organisation ICANN, en signant toutes les conditions contractuelles liées à la sécurité.

Cette recommandation pourra être considérée comme mise en œuvre lorsque l'organisation ICANN aura créé et rempli le rôle de responsable de la sécurité avec les responsabilités définies dans les recommandations.

Cette recommandation pourra être considérée comme efficace lorsque l'organisation ICANN centralisera les responsabilités en matière de sécurité, de sorte que l'organisation ICANN puisse manifestement coordonner les activités et le budget de la SSR et aborder les questions de sécurité au niveau de gestion approprié.

2. Budgets et rapports liés à la SSR

Bien que l'organisation ICANN puisse couvrir les activités liées à la SSR sous différents postes de son budget annuel, la manière dont l'organisation ICANN alloue actuellement des fonds à des fonctions spécifiques liées à la SSR n'est toujours pas claire. Cette section du rapport de la SSR2 examine l'intention et les résultats (lorsqu'ils sont détectables et mesurables) des recommandations de la SSR1 relatives à la budgétisation et à la création de rapports SSR.

Les recommandations 20, 21 et 22 de la SSR1 ont abordé divers aspects de la nécessité d'un ensemble plus granulaire et transparent de processus de budgétisation et de rapports pour les postes budgétaires liés à la SSR. Par exemple, la recommandation 20 de la SSR1 prévoyait un degré plus élevé de granularité pour l'examen et la consultation publique sur les postes budgétaires liés à la SSR ainsi que pour la révision régulière.[18] [19] La recommandation 21 de la SSR1 indiquait que l'organisation ICANN devait établir un processus interne plus structuré permettant de montrer comment les décisions existantes au niveau organisationnel et budgétaire sont liées au cadre IS-SSR, y compris l'analyse coût/bénéfice sous-jacente. La recommandation 22 de la SSR1 conseillait à l'organisation ICANN de publier, surveiller et mettre à jour la documentation sur les ressources organisationnelles et budgétaires nécessaires pour gérer les aspects liés à la sécurité, la stabilité et la résilience conjointement avec l'introduction des nouveaux gTLD.

L'équipe de révision SSR2 a évalué l'étendue de la mise en œuvre de ces recommandations par l'organisation ICANN en explorant les documents accessibles au public, les documents mis à la disposition de l'équipe de révision par l'organisation ICANN, le rapport de mise en œuvre de la SSR1 et les réponses reçues concernant de nombreuses questions envoyées au

[18] Consulter l'annexe D - Recommandation 20 de la SSR1 et Recommandation 22 de la SSR1 pour plus de détails sur les résultats et les conclusions de l'équipe de révision SSR2 concernant ces recommandations.

[19] ICANN, « Cadre des systèmes d'identificateurs de sécurité, stabilité, et résilience (IS-SSR) – exercices fiscaux 2015 et 2016 », 15 septembre 2016, https://www.icann.org/en/system/files/files/ssr-framework-fy15-16-30sep16-en.pdf.

personnel de l'organisation ICANN.[20] L'organisation ICANN n'a pas fourni d'informations supplémentaires à l'équipe de révision SSR2 au-delà de la granularité de ce que le personnel a partagé avec la SSR1, ce qui a abouti à ces recommandations initiales (recommandations 20, 21 et 22 de la SSR1). L'équipe de révision a constaté que, bien que les rapports annuels sur les activités liées à la SSR aient été établis via les documents du cadre IS-SSR et les rapports annuels, la plupart des informations relatives aux questions budgétaires de la SSR étaient trop élevées, ce qui n'est pas conforme aux recommandations formulées par la révision de la SSR1. Le budget annuel de l'organisation ICANN ne fournit pas d'informations précises sur les activités liées à la SSR, et les documents du cadre IS-SSR ne sont plus produits.[21]

En examinant spécifiquement le programme des nouveaux gTLD de l'ICANN, la structure et le budget du nouveau programme reflétaient à un niveau élevé les questions SSR liées au programme de nouveaux gTLD (par exemple, le panel pour la stabilité du DNS, l'EBERO).[22] Toutefois, l'organisation ICANN n'a pas atteint les résultats escomptés de données plus détaillées et d'une meilleure clarté des informations concernant l'organisation et le budget pour la mise en œuvre du cadre IS-SSR et l'exécution des fonctions liées à la SSR concernant le programme des nouveaux gTLD. Notamment, dans les archives de documents de sécurité, de stabilité et de résilience des systèmes d'identificateurs de l'ICANN (IS-SSR), il n'existe aucun document spécifique au programme des nouveaux gTLD .[23] Lors de la révision des documents du cadre IS-SSR de 2016 et des rapports annuels, les gTLD sont mentionnés à deux reprises : une fois dans le module A comme une tendance dans l'écosystème Internet et une fois de plus dans le module B dans le cadre du plan stratégique global de l'ICANN.[24] Dans le cadre précédent, publié en mars 2013, l'organisation ICANN mentionne le programme des nouveaux gTLD comme une « tendance » et un moteur de politique pour l'Organisation de soutien aux extensions génériques (GNSO).[25] Les seules mentions restantes du programme des nouveaux gTLD se trouvent dans la section faisant état de la mise en œuvre des recommandations de la SSR1. Bien que l'organisation ICANN ait publié un rapport annuel qui inclut les coûts directs des ressources partagées et les coûts des fonctions de soutien allouées à la SSR, le présent rapport ne fournit pas une ventilation du financement, des ressources ou d'autres activités liées au programme de nouveaux gTLD.[26]

---

[20] Wiki de l'équipe de révision SSR2 de l'ICANN, documents d'information, consulté le 10 décembre 2020, https://community.icann.org/display/SSR/Background+Materials.

[21] ICANN, « Informations financières actuelles de l'ICANN (exercices fiscaux 2020 et 2021) », s.d., https://www.icann.org/resources/pages/governance/current-en, et ICANN, « Archive des documents de la IS-SSR », s.d., https://www.icann.org/ssr-document-archive. Note : le budget de l'ICANN ne fait état d'aucune dépense spécifique liée à la SSR. L'archive des documents de l'IS-SSR ne présente aucun cadre pour les documents IS-SSR après les exercices fiscaux 2015 et 2016.

[22] ICANN, « Adoption du budget de l'exercice fiscal 2021 de la Société pour l'attribution des noms de domaine et des numéros sur Internet », 7 mai 2020, 26 à 28, https://www.icann.org/en/system/files/files/adopted-budget-fy21-07may20-en.pdf.

[23] Archive des documents de l'IS-SSR, https://www.icann.org/ssr-document-archive

[24] ICANN, cadre de l'IS-SSR – exercices fiscaux 2015 et 2016, https://www.icann.org/en/system/files/files/ssr-framework-fy15-16-30sep16-en.pdf.

[25] ICANN, « Cadre de la sécurité, la stabilité et la résilience », 8 mars 2013 https://www.icann.org/en/system/files/files/ssr-plan-fy14-06mar13-en.pdf.

[26] ICANN, « Plan opérationnel des activités liées à la SSR pour l'exercice fiscal 2018 », s.d., https://community.icann.org/x/DqNYAw.

Pour résumer les préoccupations de l'équipe de révision dans ce domaine, bien que l'organisation ICANN puisse couvrir les activités liées à la SSR sous différents postes de son budget annuel, il n'est toujours pas clair la manière dont l'organisation ICANN alloue des fonds à des fonctions spécifiques liées à la SSR. L'équipe de révision n'a pas pu trouver de preuve d'un rapport sur le budget et les impacts des ressources associées aux événements de la SSR par l'organisation ICANN ; si ces documents existent, ils ne sont pas facilement accessibles.

Recommandation 3 de la SSR2 : améliorer la transparence budgétaire liée à la sécurité, la stabilité et la résilience

3.1. Le cadre exécutif responsable de la sécurité (voir la Recommandation 2 de la SSR2 : désigner un cadre responsable de la sécurité stratégique et tactique et de la gestion des risques) devrait informer la communauté au nom de l'organisation ICANN au sujet de la stratégie, des projets et du budget SSR de l'organisation ICANN deux fois par an et mettre à jour et publier des aperçus de budget chaque année.

3.2. Le Conseil d'administration de l'ICANN et l'organisation ICANN devraient s'assurer que les éléments de budget spécifiques concernant la performance de l'organisation ICANN au niveau des fonctions relatives à la SSR soient liés aux buts et objectifs spécifiques du plan stratégique de l'ICANN. L'organisation ICANN devrait mettre en œuvre ces mécanismes par le biais d'un processus de budgétisation et de rapport annuel cohérent et détaillé.

3.3. Le Conseil d'administration de l'ICANN et l'organisation ICANN devraient créer, publier et demander des commentaires publics sur des rapports détaillés concernant les coûts et la budgétisation liés à la SSR dans le cadre du cycle du plan stratégique.

Cette recommandation pourra être considérée comme mise en œuvre dès que l'organisation ICANN habilitera le nouveau cadre supérieur à prendre en charge toutes les fonctions et les éléments de budget pertinents.

Cette recommandation pourra être considérée comme efficace si la communauté de l'ICANN avait une vision transparente du budget lié à la SSR.

3. Gestion des risques et de la sécurité

La gestion des risques de sécurité est un processus continu qui permet à une organisation d'identifier les risques de sécurité et de mettre en œuvre des stratégies pour les atténuer. L'équipe de révision a constaté que bien que l'organisation ICANN ait lancé des activités détaillées et appropriées dans le domaine de la gestion des risques de sécurité, ce qui a abouti au rapport du groupe de travail sur le cadre de risques du DNS et le cadre IS-SSR pour les exercices fiscaux 2015 et 2016, les résultats de ces activités n'ont pas été tenus à jour.[27] Ce manque d'action remet en question l'efficacité des efforts de gestion des risques de sécurité, en particulier la répétitivité et la définition des processus en question.

[27] ICANN, « Rapport sur le cadre de gestion des risques du DNS », groupe de travail sur le cadre de gestion des risques du DNS, modifié le 4 octobre 2013, https://www.icann.org/public-comments/dns-rmf-final-2013-08-23-en et ICANN, Cadre IS-SSR pour les exercices fiscaux 2015 et 2016.

Sans la documentation actuelle disponible, l'équipe de révision n'a pas pu trouver des preuves démontrant la conformité de l'organisation ICANN aux normes et aux meilleures pratiques de l'industrie.[28] L'absence de documentation actuelle inclut un manque majeur d'audits de tiers sur l'approche et la mise en œuvre de l'organisation ICANN. En revanche, l'équipe de révision note que les différentes parties contractantes et les ccTLD sont conformes aux normes de sécurité et de l'industrie pertinentes, soulignant que ces normes sont applicables dans et pour l'espace du DNS.[29] Finalement, l'équipe de révision n'a pas été en mesure de déterminer si le travail entrepris par l'organisation ICANN dans le domaine de la gestion des risques de sécurité est suffisant ou non.

En l'absence d'informations à jour et publiquement disponibles, il est également peu probable que les membres de la communauté et d'autres parties (par exemple, les gouvernements, les titulaires de noms de domaine) soient en mesure d'évaluer le travail de l'organisation ICANN. Cette absence entraîne un manque de transparence qui a un impact sur les valeurs fondamentales de l'organisation ICANN et la confiance mondiale dans l'organisation ICANN et l'écosystème du DNS. Une gestion adéquate des risques et de la sécurité exige des processus clairs qui suivent les normes internationales connues et les directives des meilleures pratiques, ainsi que des responsabilités et des structures claires et accessibles au public. Les audits faits par des tiers, s'ils sont effectués conformément aux normes acceptées et suivis de rapports d'audit accessibles au public, fourniront une perspective différente, confirmeront que les mesures sont appropriées et renforceront la confiance entre la communauté et l'organisation ICANN. La création et le maintien de structures et de procédures de gestion de la sécurité aideront l'organisation ICANN à maintenir sa position en matière de sécurité plus complète et indépendante des membres individuels du personnel.

L'équipe de révision SSR2 est parfaitement consciente du fait que le partage excessif de certaines informations opérationnelles peut être problématique, notamment en matière de sécurité. Néanmoins, l'organisation ICANN gère un système critique ayant un impact mondial et devrait fournir des informations pertinentes en matière de sécurité et des données associées à la communauté. La surveillance des processus de divulgation (risques, sécurité et vulnérabilités), y compris la détermination du calendrier du moratoire et de la divulgation publique, devrait relever du mandat du cadre supérieur en fonction (voir la Recommandation 2 de la SSR2 : désigner un cadre responsable de la sécurité stratégique et tactique et de la gestion des risques).

Recommandation 4 de la SSR2 : améliorer les processus et les procédures de gestion des risques

4.1. L'organisation ICANN devrait continuer à centraliser sa gestion des risques, articuler clairement son cadre de gestion des risques de sécurité et s'assurer que cela s'aligne stratégiquement sur les exigences et les objectifs de l'organisation.

[28] Consulter la Recommandation 5 de la SSR2 : se conformer aux systèmes de gestion de la sécurité de l'information et des certifications de sécurité, Recommandation 6 de la SSR2 : divulgation et transparence de la vulnérabilité de la sécurité, la stabilité et la résilience, et la Recommandation 7 de la SSR2 : Recommandation 7 de la SSR2 : améliorer les processus et procédures de continuité des opérations et de reprise après sinistre.

[29] Exemples de divers ccTLD certifiés conformément à la norme ISO/IEC 27001:2013 et/ou ISO 22301:2012 : DENIC https://www.denic.de/en/content-pool/information-security-master/, IIS https://internetstiftelsen.se/docs/27001-eng-Certificate.pdf, nic.at https://www.nic.at/en/the-company/certificates-and-awards, Nominet https://www.nominet.uk/security-at-nominet/.

L'organisation ICANN devrait décrire les mesures pertinentes de succès et la façon dont ces mesures doivent être évaluées.

4.2. L'organisation ICANN devrait adopter et mettre en œuvre la norme ISO 31000 « Gestion des risques », valider et certifier sa mise en œuvre par des audits indépendants appropriés.[30] L'organisation ICANN devrait mettre à la disposition de la communauté des rapports d'audit, potentiellement expurgés. Les efforts de gestion des risques devraient être inclus dans les plans et procédures de la BC et de la DR (voir la recommandation 7 de la SSR2 : améliorer les processus et procédures de continuité des opérations et de reprise après sinistre).

4.3. L'organisation ICANN devrait nommer ou désigner une personne responsable et dédiée à la gestion des risques de sécurité qui informera le cadre supérieur chargé de la sécurité (voir la recommandation 2 de la SSR2 : désigner un cadre responsable de la sécurité stratégique et tactique et de la gestion des risques). Cette fonction devrait publier des mises à jour régulières, informer sur un registre des risques de sécurité et guider les activités de l'organisation ICANN. Les conclusions devraient être prises en compte dans les plans et les procédures de la continuité des opérations (BC) et la reprise après sinistre (DR) (voir la recommandation 7 de la SSR2 : améliorer les processus et procédures de continuité des opérations et de reprise après sinistre) et le système de gestion de la sécurité de l'information (ISMS) (voir la recommandation 6 de la SSR2 : se conformer aux systèmes de gestion de la sécurité de l'information et des certifications de sécurité).

Cette recommandation pourra être considérée comme ayant été mise en œuvre lorsque les processus de gestion des risques de l'organisation ICANN seront suffisamment documentés conformément aux normes internationales (par exemple, ISO 31000), et que l'organisation ait établi un cycle d'audits réguliers pour ce programme, y compris la publication de rapports sommaires d'audit.

Cette recommandation pourra être considérée comme efficace lorsque l'organisation ICANN disposera d'un programme de gestion des risques fort et clairement documenté.

Recommandation 5 de la SSR2 : se conformer aux systèmes de gestion de la sécurité de l'information et des certifications de sécurité

5.1. L'organisation ICANN devrait mettre en œuvre un ISMS qui devrait être audité et certifié par un tiers selon les normes de sécurité de l'industrie (par exemple, ITIL, famille ISO 27000, SSAE-18) pour ses responsabilités opérationnelles. Le plan devrait inclure une feuille de route et des dates limites pour obtenir des certifications et noter les domaines qui seront la cible d'une amélioration continue.

5.2. Dans le cadre de l'ISMS, 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

[30] Organisation internationale de normalisation, *ISO 31000 « Gestion des risques »*, https://www.iso.org/iso-31000-risk-management.html.

certifications s'intègrent aux stratégies de sécurité et de gestion des risques de l'organisation ICANN.

5.3. L'organisation ICANN devrait exiger que les parties externes qui lui fournissent des services soient conformes aux normes de sécurité pertinentes et documentent leur diligence raisonnable concernant les fournisseurs et les fournisseurs de services.

5.4. L'organisation ICANN devrait informer la communauté et au-delà en présentant des rapports clairs qui démontrent ce que l'organisation ICANN fait et réalise dans le domaine de la sécurité. Ces rapports seraient extrêmement utiles s'ils fournissaient des informations décrivant comment l'organisation ICANN suit les meilleures pratiques et établit des processus peaufinés et en constante amélioration pour gérer les risques, la sécurité et les vulnérabilités.

Cette recommandation pourra être considérée comme mise en œuvre lorsque l'organisation ICANN disposera d'un ISMS orienté parallèlement aux normes acceptées (par exemple, ITIL, famille ISO 27000, SSAE-18), avec des audits réguliers qui valident les procédures de gestion de la sécurité appropriées.

Cette recommandation pourra être considérée comme efficace lorsque l'organisation ICANN disposera d'un système de gestion de la sécurité des informations entièrement documenté, qui traite de manière adéquate les menaces de sécurité actuelles et offre des plans pour traiter les menaces de sécurité futures potentielles.

Recommandation 6 de la SSR2 : divulgation et transparence de la vulnérabilité de la SSR

L'équipe de révision SSR2 recommande à l'organisation ICANN d'améliorer ses processus internes afin de soutenir la gestion et la création de rapports sur les vulnérabilités liées aux SSR par les actions suivantes :

6.1. L'organisation ICANN devrait promouvoir de manière proactive l'adoption volontaire des meilleures pratiques et des objectifs de la SSR pour la divulgation de la vulnérabilité par les parties contractantes. Si les mesures volontaires s'avèrent insuffisantes pour atteindre l'adoption de telles meilleures pratiques et objectifs, l'organisation ICANN devrait mettre en œuvre les meilleures pratiques et objectifs dans les contrats, les accords et les protocoles d'accord.

6.2. 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, tels que les violations au sein de toute partie contractante et les cas de vulnérabilités critiques découvertes et signalées à l'organisation ICANN, doivent être communiquées rapidement aux parties de confiance et concernées (par exemple, les personnes concernées ou requises pour résoudre le problème). L'organisation ICANN devrait publier régulièrement des rapports sur les vulnérabilités (au moins une fois par an), y compris les mesures anonymisées et en utilisant une divulgation responsable.

Cette recommandation pourra être considérée comme mise en œuvre lorsque l'organisation ICANN encouragera l'adoption volontaire des meilleures pratiques SSR pour les divulgations de

vulnérabilité par les parties contractantes et mettra en œuvre les rapports de divulgation de vulnérabilité y associés.

Ces recommandations pourront être considérées comme efficaces lorsque l'organisation ICANN et les parties contractantes auront adopté les meilleures pratiques et objectifs SSR pour la divulgation de la vulnérabilité.

4. Gestion de la continuité des opérations et plan de reprise après sinistre

Compte tenu de la criticité des fonctions exercées par l'organisation ICANN, allant du DNS aux registres IANA (y compris la gestion et la maintenance des registres critiques comme la zone racine, les numéros IP et AS et les registres de protocole), l'organisation ICANN devra s'engager dans des registres bien planifiés, exécutés, et une gestion documentée tant de la continuité des opérations que de la planification de la reprise après sinistre. Sur la base de ce rôle critique, l'équipe de révision SSR2 estime que l'organisation ICANN devrait avoir des programmes de continuité des opérations (BC) et de reprise après sinistre (DR) plus robustes et mieux organisés. L'ICANN bénéficierait de suivre les meilleures pratiques de l'industrie, en particulier la mise en œuvre et la documentation de la conformité aux normes internationales applicables (par exemple, ISO/IEC 27001, NIST 800-53). Des audits indépendants devraient suivre ces mesures afin de confirmer la pertinence des procédures.

L'équipe a examiné la documentation disponible concernant la BC et la DR. La documentation la plus récente date de 2017.[31] Conformément aux normes ISO 22301 et 22730, les meilleures pratiques exigent des révisions annuelles de ces politiques et procédures. Des audits indépendants sont nécessaires pour s'assurer que les plans de BC et DR soient à jour et conformes aux meilleures pratiques appropriées pour la criticité du DNS. En général, l'équipe de révision SSR2 et les membres du personnel de l'organisation ICANN n'ont pas été en mesure de trouver et de présenter une documentation suffisamment détaillée qui permettrait une évaluation appropriée de la mise en œuvre par l'organisation ICANN de leurs plans de BC et DR. L'organisation ICANN peut apporter des modifications à la façon dont elle gère la BC et la DR qui résulteraient dans des améliorations significatives pour les fonctions essentielles qu'elle fournit.[32]

La conformité aux normes internationales bien établies, confirmée par des audits externes tiers, est essentielle pour toute organisation qui gère une infrastructure critique pour l'Internet, même si cette conformité n'est pas exigée par la loi. Des experts externes contribueraient à la transparence et à la légitimité des plans et procédures de la BC et la DR de l'organisation

[31] Wiki SSR2, documents et versions préliminaires de l'équipe de révision, « questions et réponses de la SSR2 », s.d., 2, https://community.icann.org/pages/viewpage.action?pageId=64076120. Note : selon les entretiens avec le personnel de l'ICANN, « ces documents sont confidentiels et ne sont pas publiquement disponibles pour des raisons de sécurité. Il existe un plan de reprise après sinistre pour les systèmes, un plan de continuité pour les fonctions IANA et un plan de continuité plus large en cours d'élaboration pour l'ensemble de l'organisation ICANN qui devrait être mis en œuvre en 2019 ».

[32] L'équipe est consciente du fait que le système de gestion de la sécurité de l'information (ISMS), la continuité des opérations (BC), la reprise après sinistre (DR) et la gestion des risques conforme aux normes ISO interagissent et sont interdépendants. Néanmoins, l'équipe a jugé approprié de donner des détails sur les besoins identifiés, la mise en œuvre et les étapes nécessaires.

ICANN par le biais d'un appel d'offres public pour les auditeurs, ainsi que par la publication ultérieure du rapport final d'audit (et, si nécessaire, expurgé). En particulier, la norme ISO 31000 « Gestion des risques », la famille ISO/IEC 27000 « Systèmes de gestion de la sécurité de l'information » et la norme ISO 22301 « Gestion de la continuité des opérations » seraient utiles comme orientation, et plus important encore, serviraient de normes cibles pour les audits indépendants faits par des tiers.[33] Bien que l'organisation ICANN soit unique dans sa structure organisationnelle et sa mission, les normes ISO sont flexibles et applicables à l'organisation ICANN, en particulier lorsqu'il s'agit de l'organisation ICANN et des fonctions IANA. L'équipe de révision considère également que l'utilisation des normes NIST est appropriée, à condition que l'organisation ICANN documente minutieusement le processus et qu'elle soit auditée indépendamment par un tiers respecté.[34]

L'évaluation des processus et procédures appropriés en matière de BS et DR est un travail qui s'appuie sur des activités d'évaluation des risques plus générales, comme décrit ci-dessus à la section D.3. Gestion des risques et de la sécurité. L'ICANN soutient un système critique pour le fonctionnement de l'Internet et est donc à un niveau supérieur aux exigences normales en matière de BC et de DR. Un compromis présumé des procédures liées à la clé de signature de clé (KSK), en particulier pendant une crise, constituerait un problème considérable et doit être évité. Les problèmes mondiaux turbulents de 2020, de la pandémie de COVID-19 à d'importants troubles sociaux, ont démontré comment le fait d'avoir deux sites dans le même pays (dans ce cas, les États-Unis) est insuffisant et a entraîné des niveaux de risque inopinément élevés pour la fonction de continuité des opérations et de reprise après sinistre au sein de l'organisation ICANN. Les interdictions de voyager affectent également différents sites aux États-Unis, et des événements violents se sont également produits dans la plupart des grandes villes du pays en même temps. En outre, bien qu'extrêmement improbable, les deux sites pourraient être affectés par d'autres événements indésirables, tels que des tremblements de terre, des incendies ou d'autres catastrophes naturelles. Les types de risques qui peuvent avoir un impact sur les opérations de l'organisation ICANN évolueront et l'organisation ICANN devra répondre en conséquence par le biais d'une évaluation régulière et documentée des plans de BC et DR, y compris une planification et une exécution appropriées et opportunes lorsque des changements s'avèrent nécessaires.

Recommandation 7 de la SSR2 : améliorer les processus et procédures de continuité des opérations et de reprise après sinistre

7.1. L'organisation ICANN devrait établir un plan de continuité des opérations pour tous les systèmes appartenant à l'organisation ICANN, ou sous sa responsabilité, basée sur

[33] Normes et séries de normes de l'Organisation internationale de normalisation *ISO 31000, ISO/IEC 27000:2018 « Technologies de l'information — techniques de sécurité — systèmes de gestion de la sécurité de l'information — vue d'ensemble et vocabulaire »,* et *ISO 22301:2019 « Sécurité et résilience — systèmes de gestion de la continuité des opérations— exigences ».*

[34] Département du commerce des États-Unis, Institut national des normes et de la technologie des États-Unis (NIST). *Publication spéciale NIST (SP) 800-30 Rév. 1, Guide pour la gestion de l'évaluation des risques*. Gaithersburg, MD : Département du commerce des États-Unis, 2012. https://doi.org/10.6028/NIST.SP.800-30r1 et Département du commerce des États-Unis, Institut national des normes et de la technologie des États-Unis (NIST), Centre des ressources de sécurité informatique. *SP 800-53 - révision 5 - Contrôles de la sécurité et de la protection des données à caractère personnel pour les systèmes et organisations de l'information*. Gaithersburg, MD : XXX Département du commerce des États-Unis, 2020. https://doi.org/10.6028/NIST.SP.800-53r5.

la norme ISO 22301 « Gestion de la continuité des opérations », identifiant des délais acceptables pour la continuité des opérations et la reprise après sinistre (BC/DR).[35]

7.2. L'organisation ICANN devrait s'assurer que le plan de reprise après sinistre pour les opérations de l'entité Identificateurs techniques publics (PTI) (c'est-à-dire les 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 en conformité avec la norme ISO 27031.[36] L'organisation ICANN devrait développer ce plan en étroite collaboration avec le Comité consultatif du système des serveurs racine (RSSAC) et les Opérateurs de serveur racine (RSO).

7.3. L'organisation ICANN devrait également établir un plan de reprise après sinistre pour tous les systèmes détenus par ou sous le mandat de l'organisation ICANN, toujours en conformité avec la norme ISO 27031.

7.4. L'organisation ICANN devrait établir un nouveau site pour la reprise après sinistre pour tous les systèmes appartenant à l'organisation ICANN ou sous son mandat, dans le but de remplacer les sites de Los Angeles ou Culpeper ou d'ajouter un troisième site permanent. L'organisation ICANN devrait installer ce site en dehors de la région de l'Amérique du Nord et de tout territoire américain. Si l'organisation ICANN choisissait de remplacer l'un des sites existants, ce dernier ne devrait pas être fermé tant que l'organisation n'ait pas vérifié que le nouveau site soit entièrement opérationnel et capable de gérer la reprise après sinistre de ces systèmes pour l'organisation ICANN.

7.5. L'organisation ICANN devrait publier un résumé de ses plans et procédures pour la continuité des opérations et la reprise après sinistre à l'échelle mondiale. Cela améliorerait la transparence et la fiabilité au-delà de ses objectifs stratégiques. L'organisation ICANN devrait engager un auditeur externe pour vérifier les aspects liés à la conformité avec ces plans de continuité des opérations et de reprise après sinistre.

Cette recommandation pourra être considérée comme mise en œuvre lorsque les plans et processus de BC et DR de l'organisation ICANN seront entièrement documentés conformément aux normes acceptées dans l'industrie, y compris des audits réguliers sur le suivi de ces processus, et lorsqu'un site situé en dehors des États-Unis ou en dehors de l'Amérique du Nord sera opérationnel.

Cette recommandation pourra être considérée comme efficace lorsque l'organisation ICANN pourra démontrer comment elle peut gérer les incidents qui ont un impact sur l'ensemble des États-Unis ou de l'Amérique du Nord.

[35] ISO 22301:2019

[36] Normes et suites de normes de l'Organisation internationale de normalisation *ISO 27031, ISO/IEC 27031:2011 « Technologies de l'information — techniques de sécurité — lignes directrices pour la préparation des technologies de l'information et de la communication à la continuité des opérations ».*

E. Contrats, conformité et transparence en matière d'utilisation malveillante du DNS

Depuis sa fondation, la mission de l'ICANN a été de *« coordonner le développement et la mise en œuvre de politiques élaborées via un processus multipartite ascendant basé sur le consensus et conçues pour assurer le fonctionnement sûr et stable des systèmes d'identificateurs uniques de l'Internet »*.[37] L'équipe de révision SSR2 conclut que, malgré l'engagement ci-dessus, le système actuel coordonné par l'ICANN ne traite pas suffisamment l'utilisation malveillante du DNS et les préjudices y associés. Des groupes au sein et en dehors de la communauté de l'ICANN ont noté cette lacune pendant plusieurs années.[38] Certaines des communications les plus pointues sur ce sujet proviennent de représentants des gouvernements du monde entier via le Comité consultatif gouvernemental (GAC), qui affirme depuis plus de dix ans qu'ils ne trouvent pas que les processus et procédures de l'ICANN soient suffisants pour répondre aux intérêts de sécurité publique.[39]

L'utilisation malveillante du DNS à des fins frauduleuses ou criminelles a existé avant l'organisation ICANN.[40] Le panorama des menaces, qui tournait autrefois autour du spam, de l'hameçonnage et de la fraude, s'est élargi pour inclure des attaques plus sophistiquées, par exemple, les logiciels malveillants, les rançonlogiciels et le piratage de la messagerie en entreprise (BEC), qui ciblent les entreprises, les gouvernements et l'Internet des objets (IoT).[41] Les acteurs malveillants comprennent désormais des acteurs commerciaux et parrainés par l'État, qui développent des plateformes industrielles pour soutenir les abus. La pandémie de COVID-19 et les quarantaines y associées ont fourni une surface d'attaque élargie aux criminels opportunistes.[42]

Comme indiqué ci-dessous à la section E.1. Mesures de sauvegarde non atteintes pour le programme des nouveaux gTLD, l'utilisation malveillante du DNS a été une préoccupation clé de toutes les parties prenantes à l'époque, et l'organisation ICANN a eu plusieurs occasions d'élaborer des politiques conçues pour assurer le fonctionnement stable et sécurisé du système de noms uniques d'Internet pendant l'expansion de l'espace de noms mondial. L'organisation

[37] Article 1.1 (a) des statuts constitutifs de l'ICANN, https://www.icann.org/resources/pages/governance/bylaws-en/#article1.

[38] Exemples : « Lettre ouverte à la communauté de l'ICANN du Groupe des représentants des opérateurs de registre », 19 août 2020, https://docs.wixstatic.com/ugd/ec8e4c_00d2dbac27b24330b8342686e9c2e53a.pdf, et lettre de l'unité constitutive des utilisateurs commerciaux au Conseil d'administration de l'ICANN, Göran Marby, Président-directeur général de l'ICANN, Keith Drazek, président du conseil de la GNSO et la communauté de l'ICANN, 28 octobre 2019, https://www.bizconst.org/assets/docs/positions-statements/2019/2019_10October_28%20BC%20Statement%20on%20DNS%20Abuse.pdf.

[39] Comité consultatif gouvernemental de l'ICANN, « Déclaration du GAC sur l'utilisation malveillante du DNS », 18 septembre 2019, 1, https://gac.icann.org/file-asset/public/gac-statement-dns-abuse-final-18sep19.pdf.

[40] Consulter l'annexe F : « Données de recherche sur les rapports des tendances de l'utilisation malveillante du DNS » pour plus d'information sur les tendances historiques dans ce domaine.

[41] Comité consultatif sur la sécurité et la stabilité (SSAC) de l'ICANN, « SAC105 : le DNS et l'Internet des objets : opportunités, risques et défis », 28 mai 2019 https://www.icann.org/en/system/files/files/sac-105-en.pdf.

[42] Interpol, « Panorama mondial de la cybermenace liée au COVID-19 », avril 2020 https://www.interpol.int/en/content/download/15217/file/Global%20landscape%20on%20COVID-19%20cyberthreat.pdf.

ICANN a également eu l'occasion de servir de chef de file pour guider l'ensemble des communautés DNS et de sécurité vers un ensemble commun de termes, de définitions et de données qui faciliterait la communication et la collaboration, comme indiqué dans la section E.2. Enjeux : définitions et données.

Ces opportunités existent toujours pour l'organisation ICANN. Les recommandations de cette section proposent à l'organisation ICANN des suggestions spécifiques sur où et comment améliorer le respect de sa propre mission et la manière de diriger plus fermement les communautés du DNS et de la sécurité.

1. Mesures de sauvegarde non atteintes pour le programme des nouveaux gTLD

L'utilisation malveillante du DNS a été une préoccupation majeure lors du lancement du programme des nouveaux gTLD en 2010. Les organismes d'application de la loi, les gouvernements, les communautés qui s'occupent de la sécurité et les groupes d'intérêts commerciaux et d'utilisateurs ont tous plaidé pour des obligations contractuelles d'atténuation de l'utilisation malveillante dans le contrat de registre des nouveaux gTLD de base et du contrat d'accréditation de bureaux d'enregistrement (RAA) de 2013. Dans le cadre de ces délibérations, la communauté de l'ICANN a préparé, en 2009, une note explicative proposant des mesures visant à atténuer les comportements malveillants dans le programme des nouveaux gTLD.[43] La note explicative comprenait des recommandations pour vérifier les opérateurs de registre, définir les contacts et les procédures d'utilisation malveillante au niveau du registre et centraliser l'accès aux fichiers de zone. Malheureusement, il y avait un écart entre les mesures décrites dans cette note explicative et ce qui est ressorti des négociations closes entre l'organisation ICANN et les opérateurs de registre. Les tentatives ultérieures d'améliorer les pratiques de sécurité par le biais de modifications contractuelles ont reçu des critiques pour manque de transparence et d'engagement de la communauté dans le processus.[44]

En 2013, l'équipe de révision de la concurrence, la confiance et le choix des consommateurs (CCT) de l'ICANN a examiné l'efficacité de ces mesures de protection visant explicitement à atténuer les taux d'activités abusives, malveillantes et criminelles dans ces nouveaux gTLD. L'équipe CCT a commandé une étude indépendante (ci-après, le rapport SADAG) qui a utilisé des sources de données publiques pour montrer que les taux d'abus dans les nouveaux gTLD étaient plus élevés que dans les gTLD historiques, ce qui implique que les mesures de protection ont été inefficaces.[45] Le rapport final de la CCT a conclu :

[43] ICANN, « Atténuation des conduites malveillantes », note explicative des nouveaux gTLD, 3 octobre 2009, https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf.

[44] Unité constitutive des utilisateurs commerciaux de la GNSO de l'ICANN, « Commentaire sur les modifications proposées au contrat de registre de base des nouveaux gTLD », , présentation de l'unité constitutive des utilisateurs commerciaux, version 3, 20 juillet 2016, https://www.bizconst.org/assets/docs/positions-statements/2016/2016_07july_20%20bc%20comment%20on%20proposed%20gtld%20base%20registry%20agreement%20final.pdf.

[45] Korczyński, Maciej , Maarten Wullink, Samaneh Tajalizadehkhoob, Giovane C.M. Moura et Cristian Hesselman, « Rapport final sur l'analyse statistique de l'utilisation malveillante du DNS » (Statistical Analysis of DNS Abuse in gTLDs Final Report), SIDN Labs et The Delft University of Technology, août 2017, consulté le 3 août 2018, https://www.icann.org/public-comments/sadag-final-2017-08-09-en.

« Bien que l'utilisation malveillante ne soit pas universellement persistante dans tous les nouveaux gTLD, elle est endémique dans de nombreux cas. Plus inquiétant encore, à l'heure actuelle il existe peu de recours pour que la communauté arrête les opérateurs de registre et les bureaux d'enregistrement des nouveaux gTLD ayant de niveaux élevés d'abus. Cela encourage les opérateurs de réseau à bloquer unilatéralement tout le trafic de certains TLD ou de bureaux d'enregistrement spécifiques, ce qui va à l'encontre des objectifs de la communauté en matière d'acceptation universelle pour les nouveaux gTLD.

Le manque de prévision à propos de la propagation de certaines activités abusives vis-à-vis des nouveaux gTLD précédemment identifiées par la communauté est important. L'équipe de révision de la CCT reconnaît le rôle que jouent les noms de domaine pour l'infrastructure en permettant les activités abusives qui ont des conséquences sur la sécurité, la stabilité et la résilience du DNS, sur la confiance du consommateur, et, en définitive, un impact chez les utilisateurs finaux du monde entier. En conséquence, il s'agit d'un thème prioritaire qui doit être abordé avant toute nouvelle expansion du DNS, et l'équipe de révision propose plusieurs recommandations pour remédier aux lacunes du statu quo et améliorer la sécurité du DNS ».[46]

La révision de la CCT et le rapport SADAG y associé, ainsi que d'autres rapports de tiers, ont également constaté qu'après le lancement du programme des nouveaux gTLD, certains opérateurs de registre et bureaux d'enregistrement ont rapidement établi des pratiques pour augmenter promptement et sensiblement les enregistrements de domaine, par exemple, les enregistrements en masse, dont un bon nombre sont utilisés pour perpétrer des abus et des activités criminelles.[47] Spamhaus (entre autres) publie également ce qu'ils estiment être les TLD et les bureaux d'enregistrement étant la cible d'un plus grand nombre d'abus, et certaines entités figurent sur ces listes tous les ans.[48] Alpnames, mis en évidence dans le rapport SADAG comme l'un des bureaux d'enregistrement dont l'utilisation malveillante du DNS est la plus flagrante, a offert des enregistrements en masse bon marché et « *a agi comme bureau d'enregistrement parrain pour 53,97 % (59,044) des nouveaux domaines gTLD qui ont été mis sur la liste noire par Spamhaus* ».[49] Le département de la conformité contractuelle de l'ICANN n'a pas suffisamment répondu à ces abus systémiques en cours, même après que de nombreuses organisations les leur aient signalés à maintes reprises.[50] Le département de la

[46] Équipe de révision de la concurrence, la confiance et le choix du consommateur, « Rapport final de l'équipe de révision de la concurrence, la confiance et le choix du consommateur » ICANN, 8 septembre 2018, https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf, et Piscitello, Dave, « Armer les noms de domaine : comment l'enregistrement en masse facilite les campagnes de spam mondiales », Spamhaus, 21 mars 2020, https://www.spamhaus.org/news/article/795/weaponizing-domain-names-how-bulk-registration-aids-global-spam-campaigns.

[47] Ibid., et, Piscitello, Dave, « Armer les noms de domaine : comment l'enregistrement en masse facilite les campagnes de spam mondiales », Spamhaus, 21 mars 2020, https://www.spamhaus.org/news/article/795/weaponizing-domain-names-how-bulk-registration-aids-global-spam-campaigns.

[48] Spamhaus, « Les TLD faisant l'objet de plus d'abus au monde », consulté le 5 décembre 2020, https://www.spamhaus.org/statistics/tlds/, et Spamhaus, « Les bureaux d'enregistrement de domaine faisant l'objet de plus d'abus au monde », consulté le 5 décembre 2020, https://www.spamhaus.org/statistics/registrars/. Note : les documents de soutien sur les pages de Spamhaus offrent un aperçu de la façon dont ils déterminent les domaines et les bureaux d'enregistrement « malveillants ».

[49] Rapport SADG, 19, https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf.

[50] Lettre d'Adobe Systems, DomainTools, eBay, Facebook, Microsoft et Time Warner (également appelé équipe de travail indépendante sur la conformité) à Jamie Hedlund, vice-président sénior du département de la conformité

conformité contractuelle de l'ICANN n'a désaccrédité Alpnames qu'après avoir remarqué qu'Alphanames avait cessé ses activités.[51] Nous espérons que l'organisation ICANN et l'industrie du DNS puissent démontrer des progrès mesurables sur la prévention et l'atténuation de l'utilisation malveillante du DNS. Autrement, les gouvernements concluront probablement que le modèle d'autogouvernance de l'industrie de l'ICANN n'est plus adapté à l'objectif.

Comme indiqué dans la révision WHOIS2/RDS, le département de la conformité contractuelle de l'ICANN a l'occasion d'être proactif dans la résolution des « *problèmes systémiques présumés, des plaintes d'inexactitude signalées, des études ou révisions de l'exactitude du RDS ou rapports DAAR, de la recherche, l'analyse et l'application contre l'inexactitude des données d'enregistrement* ».[52]

Recommandation 8 de la SSR2 : permettre et démontrer la représentation de l'intérêt public dans les négociations avec les parties contractantes

> 8.1. L'organisation ICANN devrait mettre en place une équipe de négociation comprenant des experts en matière d'abus et de sécurité non affiliés ou payés par des parties contractantes pour représenter les intérêts des entités non contractantes et travailler avec l'organisation ICANN pour renégocier les contrats des parties contractantes de bonne foi, avec transparence publique, et dans le but d'améliorer la SSR du système des noms de domaine pour les utilisateurs finaux, les entreprises et les gouvernements.

Cette recommandation pourra être considérée comme mise en œuvre lorsque l'organisation ICANN aura inclus des spécialistes en matière d'utilisation malveillante et de sécurité dans ces négociations et que la gestion du système de noms de domaine soit conforme à la sécurité publique et aux intérêts des consommateurs, et pas seulement à ceux de l'industrie des noms de domaine.

Cette recommandation pourra être considérée comme efficace lorsqu'un ensemble plus large et plus équilibré de parties prenantes sera en mesure de participer directement aux contrats négociés avec les parties contractantes.

---

contractuelle de l'ICANN et des sauvegardes des consommateurs et directeur général du, bureau de Washington D.C., 27 février 2018, https://www.icann.org/en/system/files/correspondence/vayra-to-hedlund-27feb18-en.pdf.

[51] Lettre de Jamie Hedlund, vice-président sénior du département de la conformité contractuelle de l'ICANN et des sauvegardes des consommateurs et directeur général du bureau de Washington D.C, à Iain Roache, Alpnames Limited, « RE: AVIS DE RÉSILIATION DU CONTRAT D'ACCRÉDITATION DE BUREAU D'ENREGISTREMENT», 15 mars 2019 https://www.icann.org/uploads/compliance_notice/attachment/1113/hedlund-to-roache-15mar19.pdf.

[52] Équipe de révision RDS-WHOIS2, « Rapport final de la révision du Service d'annuaire de données d'enregistrement (RDS)-WHOIS2 », 3 septembre 2019, https://www.icann.org/en/system/files/files/rds-whois2-review-03sep19-en.pdf, 46. Note: consulter la Recommandation R4.1 : « *le Conseil d'administration de l'ICANN devrait prendre des mesures pour s'assurer que le département de la conformité contractuelle de l'ICANN soit dirigé de manière proactive pour surveiller et appliquer les obligations des bureaux d'enregistrement en ce qui concerne l'exactitude des données RDS (WHOIS) à l'aide des données provenant des plaintes pour inexactitude entrantes et des études ou des révisions de l'exactitude du RDS afin de rechercher et de résoudre les problèmes systémiques. Une approche basée sur les risques devrait être mise en œuvre pour évaluer et comprendre les problèmes liés à l'inexactitude et puis prendre les mesures appropriées pour les atténuer ».*

Recommandation 9 de la SSR2 : surveiller et appliquer la conformité

9.1. Le Conseil d'administration de l'ICANN devrait demander à l'équipe chargée de la conformité de surveiller et d'appliquer strictement la conformité des parties contractantes aux obligations SSR actuelles et futures et aux obligations en matière d'abus dans les contrats, les accords de base, les spécifications temporaires et les politiques communautaires.

9.2. L'organisation ICANN devrait surveiller et appliquer de manière proactive les obligations contractuelles des registres et des bureaux d'enregistrement afin d'améliorer l'exactitude des données d'enregistrement. Cette surveillance et cette application devraient inclure la validation des champs d'adresses et la réalisation de vérifications périodiques de l'exactitude des données d'enregistrement. L'organisation ICANN devrait concentrer ses efforts d'application sur les bureaux d'enregistrement et les opérateurs de registre ayant fait l'objet de plus de 50 plaintes ou rapports par an concernant la présentation de données auprès de l'organisation ICANN.

9.3. L'organisation ICANN devrait mener des activités de conformité auditées en externe au moins une fois par an et publier les rapports d'audit et la réponse de l'organisation ICANN aux recommandations d'audit, y compris les plans de mise en œuvre.

9.4. L'organisation ICANN devrait s'occuper de la fonction de conformité en publiant des rapports réguliers qui énumèrent les outils manquants qui aideraient à soutenir l'organisation ICANN dans son ensemble à utiliser efficacement des clauses contractuelles pour traiter les menaces de sécurité au DNS, y compris les mesures qui nécessiteraient des modifications aux contrats.

Cette recommandation pourra être considérée comme mise en œuvre lorsque des vérifications se produiront régulièrement et que des résumés seront publiés.

Cette recommandation pourra être considérée comme efficace lorsque l'organisation ICANN aura terminé un audit avec succès et en ait informé la communauté.

Cette recommandation requiert une action du Conseil d'administration de l'ICANN et de l'organisation ICANN. Le Conseil d'administration pourrait avoir à mettre à jour sa position et ses instructions après avoir terminé le processus accéléré d'élaboration de politiques (EPDP) sur la lutte contre l'utilisation malveillante (voir la recommandation 15 de la SSR2 : lancer un EPDP fondé sur des données factuelles pour améliorer la sécurité

2. Enjeux : définitions et accès aux données

L'équipe de révision SSR2 a trouvé deux catégories de défis persistants : l'une a trait aux définitions et à la portée des abus que les obligations contractuelles de l'ICANN peuvent gérer et l'autre, à l'accès aux données qui peuvent éclairer la détection, l'atténuation, la prévention et la réponse aux abus. Les recommandations 11 à 14 de la SSR2 visent à améliorer la transparence et la responsabilité dans les deux domaines.

A. Définitions d'utilisation malveillante / abus

Lors d'un dialogue tenu en avril 2018 avec l'équipe de révision SSR2, le département de la conformité contractuelle de l'ICANN a affirmé que les contrats actuels avec les opérateurs de registre et les bureaux d'enregistrement n'autorisent pas l'ICANN à exiger aux opérateurs de registre de suspendre ou de supprimer les noms de domaine potentiellement abusifs et qu'ils sont donc inefficaces, car ils permettent la poursuite des activités à ceux qui sont impliqués dans l'utilisation malveillante systémique du DNS.[53] Ce point a également été publiquement affirmé dans la lettre du département de la conformité contractuelle de l'ICANN adressée au groupe de travail indépendant sur la conformité.[54]

Un an plus tard, en avril 2019, le département de la conformité contractuelle de l'ICANN a signalé à l'équipe de révision SSR2 que l'absence d'une interdiction contractuelle sur « l'utilisation malveillante systématique du DNS » empêche le département de la conformité contractuelle de l'ICANN de s'y attaquer efficacement jusqu'à ce qu'il existe une politique de consensus communautaire la définissant et l'interdisant.[55] De plus, le Conseil d'administration de l'ICANN a récemment annoncé qu'il retarderait la mise en place des Recommandations 14 et 15 de la révision de la CCT qui conseillent des modifications aux contrats en vigueur pour aider à prévenir l'utilisation malveillante du DNS. Le Conseil d'administration a souligné que ce retard est dû au fait que « *des discussions communautaires sont toujours en cours pour parvenir à une compréhension commune de l'utilisation malveillante du DNS et des termes connexes* ».[56] L'équipe de révision SSR2 observe que la nature non structurée et illimitée de ces discussions complique la recherche d'une résolution et que l'organisation ICANN et les parties contractantes sont encouragées à reporter indéfiniment la résolution de ce problème. Nous recommandons une approche de ce problème à trois volets, y compris une spécification temporaire pour un CCWG à court terme et limité dans le temps pour le moyen terme, et un EPDP structuré pour l'horizon à long terme.

L'organisation ICANN a intégré depuis plus d'une décennie des descriptions et des définitions de travail de « l'utilisation malveillante du DNS » et des termes connexes, y compris (mais sans s'y limiter) la sécurité, la stabilité de l'organisation ICANN, et les cadres de résilience de 2009 à 2017,[57] les conclusions consensuelles de la communauté de l'ICANN relatives au programme des nouveaux gTLD ainsi que le consensus subséquent sur les sauvegardes, l'obligation

[53] Documents d'information : discussion avec le département de la conformité de l'ICANN - terminée le 14 mai 2019, réponse du département de la conformité de l'ICANN aux questions de la SSR2 au 26 avril 2019, https://community.icann.org/display/SSR/Briefing+Materials.

[54] Lettre de Jamie Hedlund, vice-président sénior du département de la conformité contractuelle de l'ICANN et des sauvegardes des consommateurs et directeur général du bureau de Washington D.C, au groupe de travail indépendant sur la conformité, « RE: Lettre du 27 février 2018 du groupe de travail indépendant sur la conformité », 4 avril 2018 https://www.icann.org/en/system/files/correspondence/hedlund-to-vayra-04apr18-en.pdf. Voir aussi la note en bas de page 44 relative à : la lettre du 27 février 2018 de l'équipe de travail indépendante sur la conformité.

[55] Documents d'information, https://community.icann.org/display/SSR/Briefing+Materials, 4. Remarque : consulter la réponse à la question 6.

[56] Conseil d'administration de l'ICANN, « Résolutions approuvées | Réunion régulière du Conseil d'administration de l'ICANN », ordre du jour principal, concurrence, confiance des consommateurs, recommandations en attente de l'équipe de révision de la concurrence, la confiance et le choix du consommateur (CCT-RT), 22 octobre 2020, https://www.icann.org/resources/board-material/resolutions-2020-10-22-en#2.a.

[57] Archive des documents de l'IS-SSR, https://www.icann.org/ssr-document-archive

contractuelle 11b de la Spécification de [58]2013 énumérant les activités malveillantes, [59]et le projet DAAR (signalement des cas d'utilisation malveillante des noms de domaine) de l'ICANN .[60]

Le conseil de la GNSO a également demandé au groupe de travail sur les politiques en matière d'enregistrements frauduleux (RAPWG) d'examiner les questions entourant les utilisations illicites des noms de domaine. Le rapport final a établi que :

« *Le RAPWG reconnaît que la cybercriminalité est une question importante pour la communauté de l'ICANN. Fréquemment, la communauté Internet communique à l'ICANN ses inquiétudes vis-à-vis des comportements malveillants, et en particulier, la mesure dans laquelle les délinquants tirent profit des services d'enregistrement de noms de domaine et de résolution de noms. De nombreuses parties, y compris des entreprises, des consommateurs, des gouvernements et des agents des forces de l'ordre, demandent à l'ICANN et à ses parties contractantes de surveiller les conduites malveillantes et, le cas échéant, de prendre les mesures appropriées pour détecter, bloquer et réduire ces comportements* ».[61]

Le RAPWG a recommandé un processus communautaire supporté par les ressources de l'ICANN, pour créer une liste non obligatoire des bonnes pratiques afin d'aider les bureaux d'enregistrement et les opérateurs de registre à aborder l'utilisation illicite des noms de domaine. Dix ans plus tard, l'organisation ICANN n'a toujours pas fait de progrès significatifs sur ces questions. [62] (Consulter aussi la Recommandation 9 de la SSR2 : surveiller et appliquer la conformité).

---

[58] Groupe de travail sur les politiques en matière d'enregistrements frauduleux de la GNSO de l'ICANN, « Rapport final du Groupe de travail sur les politiques en matière d'enregistrements frauduleux », 29 mai 2010. https://gnso.icann.org/sites/default/files/filefield_12530/rap-wg-final-report-29may10-en.pdf, 3. Note : le présent rapport a défini l'utilisation malveillante comme « *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* ». Consulter aussi, opérations et recherche sur les politiques de l'ICANN, « Sauvegardes du programme des nouveaux gTLD contre l'utilisation malveillante du DNS », juillet 2016 https://newgtlds.icann.org/en/reviews/dns-abuse/safeguards-against-dns-abuse-18jul16-en.pdf, 3. Note : le présent rapport a également utilisé la distinction faite par le RAPWG à propos des *enregistrements abusifs* et *de l'utilisation abusive*, notant que les enregistrements abusifs se trouvent plus clairement dans le champ d'application de la politique de l'ICANN et de la GNSO. Le RAPWG a identifié des exemples d'enregistrements abusifs tels que : le cybersquattage, la réservation préventive, les sites diffamatoires, les noms de domaine trompeurs et/ou injurieux, les faux avis de renouvellement, la permutation de noms, le paiement au clic, les détournements de trafic, la fausse affiliation, les escroqueries d'enregistrement par TLD croisés, le *domain kiting/tasting.* Ce RAPWG a également identifié des formes d'utilisation malveillante : hameçonnage, spam, commande et contrôle de logiciels malveillants/réseaux zombies, DDoS et fast flux.

[59] ICANN, « Spécification 11 (3)(a) et spécification 11 (3) (b) du contrat de registre de base - Mise à jour le 31 juillet 2017 », https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf et ICANN, « Avertissement, spécification 11.(3)(b) du contrat de registre des nouveaux gTLD », 8 juin 2017, https://www.icann.org/resources/pages/advisory-registry-agreement-spec-11-3b-2017-06-08-en.

[60] Voir la question « De quels types de menaces de sécurité s'occupe le DAAR ? » FAQ sur le DAAR de l'ICANN, https://www.icann.org/octo-ssr/daar-faqs/#security-threats. Plus particulièrement : hameçonnage, logiciels malveillants, commande et contrôle de réseaux zombies et spam.

[61] Rapport final du RAPWG, 6, https://gnso.icann.org/sites/default/files/filefield_12530/rap-wg-final-report-29may10-en.pdf.

[62] Lettre de Claudia Selli, présidente de l'unité constitutive des utilisateurs commerciaux de l'ICANN, à Maarten Botterman, président du Conseil d'administration de la Société pour l'attribution des noms de domaine et des

B. Accès aux données

Le deuxième défi majeur concerne l'accès aux données sur les noms de domaine qui informent les opérations de sécurité et la recherche. Les quatre types de données ayant reçu une plus grande attention sont les données d'enregistrement, qui facilitent le suivi des activités abusives au propriétaire et à l'opérateur du domaine associé, les données du fichier de zone du TLD (via le service centralisé de données de zone (CZDS)), qui soutient la recherche sur la sécurité, les données concernant le signalement d'abus utilisées pour éclairer l'analyse de l'ICANN sur l'utilisation malveillante du DNS, et les données de mise en conformité contractuelle pour soutenir l'analyse des tendances et l'évaluation des approches opérationnelles pour atténuer les abus.

i. Données d'enregistrement

Depuis au moins 2003, l'organisation ICANN a reconnu la nécessité d'équilibrer le besoin de transparence et de responsabilité des métadonnées d'enregistrement de noms de domaine, c'est-à-dire les coordonnées des propriétaires de noms, et les exigences légales dans le monde entier qui interdisent ou compliquent parfois le partage de telles informations.[63] Le RAPWG a découvert que l'accessibilité de base au service d'annuaire de données d'enregistrement (RDS, avant connu comme le WHOIS) est intimement liée aux enregistrements frauduleux de domaine et qu'il s'agit d'un élément lié à l'utilisation malveillante des noms de domaine.[64] Ils ont également constaté que les données RDS ne sont pas toujours accessibles et pas toujours fournies par les bureaux d'enregistrement de façon fiable, régulière ou prévisible, et que les utilisateurs reçoivent parfois des résultats RDS différents selon le lieu et la manière dont ils effectuent la vérification. Cela a conduit à deux recommandations du RAPWG :

« La GNSO devrait demander au département de la conformité de l'ICANN de publier davantage d'informations au sujet de l'accessibilité au WHOIS, au moins une fois par an. Ces données devraient inclure a) le nombre de bureaux d'enregistrement qui présentent un schéma peu raisonnable de restriction d'accès au port 43 des serveurs WHOIS, et b) les résultats d'un audit annuel de conformité comprenant toutes les obligations d'accès au WHOIS ».

Et

« La GNSO devrait déterminer quels sont la recherche et les processus supplémentaires qui pourraient être nécessaires pour s'assurer que les données WHOIS soient accessibles de manière pertinemment fiable, exécutoire et cohérente ».[65]

En juin 2018, en réponse aux nouvelles difficultés d'accès aux données d'enregistrement liées au RGPD, le Comité consultatif sur la sécurité et la stabilité (SSAC) de l'ICANN a conseillé de toute urgence au Conseil d'administration de l'ICANN de travailler à la modification des contrats afin de résoudre les problèmes persistants d'accès aux données. Aucune de ces

numéros sur Internet (ICANN), 9 décembre 2019, p. 1 et 3, https://www.icann.org/en/system/files/correspondence/selli-to-botterman-09dec19-en.pdf.

[63] ICANN, « Procédure révisée de l'ICANN pour gérer les conflits relatifs au WHOIS et les lois en matière de vie privée », 18 avril 2017, https://whois.icann.org/en/revised-icann-procedure-handling-whois-conflicts-privacy-law.

[64] Rapport final du RAPWG, 71- 80, https://gnso.icann.org/sites/default/files/filefield_12530/rap-wg-final-report-29may10-en.pdf.

[65] Ibid, 79 et 80.

recommandations n'a encore été mise en œuvre.[66] Selon le rapport de situation de l'organisation ICANN adressé à l'équipe de révision SSR2 (le 2 juillet 2020), l'organisation ICANN a délégué ces recommandations SSAC101 à la GNSO pour son plan de travail de l'étape 2 de l'EPDP sur l'accès aux données d'enregistrement.[67] Aucune de ces recommandations n'a jamais fait partie du plan de travail de l'étape 2 de l'EPDP, les sujets n'ont pas été abordés dans l'EPDP et la GNSO n'a entrepris aucun travail connexe. Le SSAC a également fait d'autres tentatives, sans un impact observable.[68] Certains chercheurs en matière de sécurité ont noté que la spécification temporaire pour les données d'enregistrement des gTLD permet désormais aux bureaux d'enregistrement de domaines gTLD d'expurger toutes les données de contact de domaine de la publication dans le RDS, même les enregistrements qui ne sont pas couverts par une loi sur la protection de la vie privée telle que le RGPD.[69]

Ce dernier EPDP est la version la plus récente et la plus amplifiée du débat sur l'accès aux données d'enregistrement.[70] Les déclarations minoritaires ont invariablement manifesté que les recommandations du rapport n'attachaient pas la même importance aux droits des personnes fournissant des données aux opérateurs de registre et aux bureaux d'enregistrement et à l'intérêt public pour prévenir les préjudices associés aux activités malveillantes qui pourraient tirer parti du DNS.[71] La dissidence considérable apparue dans le rapport final implique que ce processus n'a pas permis de dégager un consensus communautaire au sujet de l'accès aux

[66] Comité consultatif sur la sécurité et la stabilité de l'ICANN, « SAC101 : avis du SSAC concernant l'accès aux données d'enregistrement des noms de domaine », avis du Comité, 14 juin 2018, https://www.icann.org/en/system/files/files/sac-101-en.pdf. Note : Le SSAC a publié une « deuxième version » du document, ce qui a considérablement affaibli les recommandations de la première version pour que le Conseil d'administration de l'ICANN travaille dans la modification des contrats afin de résoudre les problèmes persistants d'accès aux données. https://www.icann.org/en/system/files/files/sac-101-v2-en.pdf. Voir les pages 4 et 5 pour le texte intégral des recommandations du document SSAC101v2.

[67] Jennifer Bryce à la liste de diffusion de l'équipe de révision SSR2, 2 juillet 2020, objet : État des documents SAC097 et SAC102v2, https://mm.icann.org/pipermail/ssr2-review/2020-July/002280.html. Veuillez consulter la page 2 du message :

[68] Lettre du Comité consultatif sur la sécurité et la stabilité de l'ICANN à Russ Weinstein, directeur des services d'enregistrement et d'engagement, et à Jamie Hedlund, vice-président sénior du département de la conformité contractuelle et de la protection des consommateurs, « objet : SSAC2019-02 : Rapport sur la demande des services de données d'enregistrement, 3 mai 2019, https://www.icann.org/en/system/files/files/ssac2019-02-03may19-en.pdf. Note : le SSAC a publié le document SSAC 2019-2 en informant que l'organisation ICANN donne des orientations à tous les opérateurs de registre, en clarifiant les objectifs, les attentes et les obligations contractuelles pour signaler les requêtes de port 43 et les requêtes RDAP. Il n'y a aucune preuve que cela ait eu lieu.

[69] Greg Aaron, Lyman Chapin, David Piscitello et Colin Strutt, « Panorama de l'hameçonnage en 2020 : une étude de la portée et la distribution de l'hameçonnage », Interisle Consulting Group, LLC, 13 octobre 2020, http://www.interisle.net/PhishingLandscape2020.pdf.

[70] Organisation de soutien aux extensions génériques de l'ICANN, Rapport final portant sur l'étape 2 du processus accéléré d'élaboration de politiques (EPDP) consacré à la spécification temporaire relative aux données d'enregistrement des gTLD, 31 juillet 2020, https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf.

[71] Ibid., annexe F - Déclaration minoritaire, p. 151 à 154. Comprend les déclarations minoritaires de : Comité consultatif At-Large (ALAC), Unité constitutive des utilisateurs commerciaux (BC) / Unité constitutive des représentants de la propriété intellectuelle (IPC), Comité consultatif gouvernemental (GAC), Groupe des représentants des entités non commerciales (NCSG), Groupe des représentants des bureaux d'enregistrement (RrSG), Groupe des représentants des opérateurs de registre (RySG), Comité consultatif sur la sécurité et la stabilité (SSAC).

données. Notant que le « *système actuellement fragmenté pour les divulgations* » combiné à un cadre juridique relativement incertain fait partie du problème, le PDG de l'ICANN a récemment demandé à la Commission européenne des précisions juridiques sur les dispositions de contrôle du RGPD.[72]

Le RAA 2013 comprenait une exigence de validation croisée d'adresses pour les données d'adresses des enregistrements de domaine.[73] La validation croisée d'adresses est un contrôle de validité commun et automatisé (par exemple, si le numéro de la maison existe dans la rue, qui existe dans la ville et la province, et si le code postal est correct). À la date de ce rapport, l'organisation ICANN n'a pas appliqué cette exigence de validation. En ce qui concerne les enregistrements à travers des services d'anonymisation et d'enregistrement fiduciaire, le conseil de la GNSO de l'organisation ICANN a unanimement soutenu une politique d'accréditation pour les fournisseurs de services d'anonymisation et d'enregistrement fiduciaire, qui pourrait inclure l'amélioration des pratiques opérationnelles impliquant des réponses aux agents des forces de l'ordre et aux détenteurs de propriété intellectuelle.[74] Le Conseil d'administration de l'ICANN a approuvé la politique en août 2016.[75] En octobre 2020, l'ICANN n'a pas mis en œuvre ces exigences et le site Web dédié à ce travail n'a pas été mis à jour depuis mars 2018.[76]

ii. Service centralisé de données de zone (CZDS)

L'accès aux dossiers de zone a toujours été un aspect important des opérations et de la recherche liées à la sécurité. Dans le cadre du programme des gTLD, la communauté a accordé que les nouveaux opérateurs de registre gTLD acceptent des obligations contractuelles de « *fournir des données de zone aux demandeurs approuvés (par exemple, les agents des forces de l'ordre, les avocats experts en propriété intellectuelle, les chercheurs) lors de la délégation technique de leurs gTLD ».*[77] Toutefois, l'accès complet et utilisable à ces données a été problématique, par exemple lorsqu'il s'agit de demander et de renouveler l'accès et d'acquérir les fichiers réels.[78] À l'heure actuelle, les opérateurs de registre n'accordent pas

[72] Lettre de Göran Marby, Président-directeur général de la Société pour l'attribution de noms de domaine et de numéros sur Internet (ICANN) , à M. Roberto Viola, directeur général du groupe de discussion sur les réseaux de communication de contenu et de technologie de la Commission européenne, Mme Monique Pariat, directrice générale du groupe de discussion sur l'immigration et les affaires intérieures de la Commission européenne, et Mme Salla Saastamoinen, directrice générale par intérim du groupe de discussion sur la justice et les consommateurs de la Commission européenne, 2 octobre 2020, https://www.icann.org/en/system/files/correspondence/marby-to-viola-et-al-02oct20-en.pdf.

[73] ICANN, « Contrat d'accréditation de bureau d'enregistrement de 2013 », consulté le 8 décembre 2020, https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en. Note : consulter la section 1(e) de la spécification relative au programme d'exactitude du Whois, https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#whois-accuracy.

[74] ICANN, « Services d'anonymisation et d'enregistrement fiduciaire », consulté le 8 décembre 2020, https://whois.icann.org/en/privacy-and-proxy-services. Note : consulter la section 2, « Processus d'adoption des recommandations de politique ».

[75] Ibid.

[76] Groupe de travail des bureaux d'enregistrement chargé de la validation du WHOIS, « Documents », dernière mise à jour le 21 mars 2018 https://community.icann.org/display/AFAV/Documents.

[77] ICANN, « Service centralisé de données de zone CZDS », consulté le 7 décembre 2020, https://czds.icann.org/home.

[78] Piscitello, Dave, « Le langage contractuel CZDS non spécifique rend les approbations d'accès aux données de zone un jeu de dés », blog, The Security Skeptic, 13 août 2019,

l'accès comme prévu et le révoquent périodiquement, avec de longs processus de renouvellement.[79] Ces données sont régulièrement utilisées pour étudier l'utilisation malveillante du DNS.[80] Le SSAC a rédigé un avis sur ce sujet en juin 2017 (SAC097), il y a plus de trois ans.[81] Le Conseil d'administration de l'ICANN a accepté les recommandations, mais ne les a toujours pas exécutées.[82] L'équipe de révision SSR2 reconnaît que certains TLD (comme les TLD de marque) peuvent nécessiter des accommodements en ce qui concerne le CZDS en raison de problèmes de protection de la marque ou de sécurité, mais en général, l'accès aux données critiques via le CZDS reste problématique.[83]

Après la résolution du Conseil d'administration de juin 2018, le nombre de plaintes relatives à l'accès aux dossiers de zone a augmenté et demeure plus élevé que vers la mi-2018. Ils constituent désormais la plus grande catégorie de plaintes concernant les opérateurs de registre.[84] Le département de la conformité contractuelle de l'ICANN n'a parfois pas traité les plaintes ZFA pendant des mois après leur soumission.[85] En 2018, l'organisation ICANN a demandé au groupe de travail chargé des procédures pour des séries ultérieures de nouveaux gTLD (communément appelé le groupe de travail SubPro) de résoudre ce problème.[86] Le groupe de travail SubPro n'en a pas mentionné le contenu dans son récent rapport préliminaire

https://www.securityskeptic.com/2019/08/unspecific-contract-language-makes-zone-data-access-approvals-a-dice-roll.html.

[79] Piscitello, Dave, « Le langage contractuel CZDS non spécifique rend les approbations d'accès aux données de zone un jeu de dés », blog The Security Skeptic, 14 août 2019, https://www.securityskeptic.com/2019/08/unspecific-contract-language-makes-zone-data-access-approvals-a-dice-roll.html, et le document du SSAC de l'ICANN, « SAC 096 : rapport consultatif du SSAC concernant le service centralisé de données de zone (CZDS) et les rapports mensuels d'activité des opérateurs de registre », 16 juin 2017, https://www.icann.org/en/system/files/files/sac-097-en.pdf.

[80] KC Claffy, et David Clark, « Rapport de l'atelier sur l'économie de l'Internet) (WIE 2019) », avril 2020 https://ccronline.sigcomm.org/2020/ccr-april-2020/workshop-on-internet-economics-wie-2019-report%EF%BB%BF/.

[81] 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.

[82] Comité consultatif sur la sécurité et la stabilité de l'ICANN, « Statut des conseils du Comité consultatif sur la sécurité et la stabilité (SSAC) », dernière mise à jour le 31 octobre 2020 https://features.icann.org/board-advice/ssac. Consulter le document « SAC097 : rapport consultatif du SSAC concernant le service centralisé de données de zone (CZDS) et les rapports mensuels d'activité de l'opérateur de registre, R-1 (12Jun2017) ».

[83] Mark VB Partridge et Jordan A. Arnot. « Expansion du système des noms de domaine : Avantages, objections et conflits ». DePaul J. Art Tech. et Intell. Prop. L 22 (2011) : 317 (voir la page 5 de l'article), et « Plateforme d'essai CZDS-API -- liste de diffusion pour les utilisateurs du CZDS-API qui s'abonnent aux sujets de discussion de l'API et y participent », https://mm.icann.org/mailman/listinfo/czds-api-testbed. Voir les fils de discussion au sujet des plaintes dans l'archive (notez que l'accès est limité aux abonnés, mais que l'abonnement est ouvert).

[84] ICANN, « Mesure de la performance du département de conformité contractuelle », consulté le 7 décembre 2020, https://features.icann.org/compliance/dashboard/report-list. À noter que les plaintes au titre de l'accès au fichier de zone représentaient 85,5 % des plaintes en mars 2020, comparativement à 31,9 % en mars 2018.

[85] « Plateforme d'essai CZDS-API -- liste de diffusion pour les utilisateurs du CZDS-API qui s'abonnent aux sujets de discussion de l'API et y participent », https://mm.icann.org/mailman/listinfo/czds-api-testbed. Voir les fils de discussion au sujet des plaintes dans l'archive (notez que l'accès est limité aux abonnés, mais que l'abonnement est ouvert).

[86] ICANN, « Charte du groupe chargé des procédures pour des séries ultérieures de nouveaux gTLD », 21 janvier 2016, https://gnso.icann.org/sites/default/files/filefield_48475/subsequent-procedures-charter-21jan16-en.pdf.

de 363 pages.[87] Il n'existe aucune preuve que l'organisation ICANN, le Conseil d'administration de l'ICANN ou la communauté des opérateurs de registre aient pris des mesures suffisantes pour résoudre les problèmes d'accès au CZDS. La Recommandation 11 de la SSR2 « Résoudre les problèmes d'accès aux données CZDS » se concentre sur ce problème.

iii. Rapport d'activités sur l'utilisation malveillante du DNS

Le projet DAAR (Signalement des cas d'utilisation malveillante des noms de domaine) de l'ICANN est une « *plateforme pour étudier le comportement relatif à l'enregistrement de noms de domaine et les menaces à la sécurité (abus) des opérateurs de registre de domaines de premier niveau (TLD) et des bureaux d'enregistrement de TLD* » avec l'objectif général « *de signaler l'activité des menaces de sécurité à la communauté de l'ICANN, qui peut utiliser les données pour prendre des décisions éclairées* ».[88] L'organisation ICANN a commencé son programme DAAR en 2017. L'organisation ICANN a affirmé que le DAAR était destiné à fournir à la communauté une approche scientifique transparente et reproductible pour signaler l'utilisation malveillante du DNS.[89] Depuis janvier 2018, l'OCTO de l'ICANN publie un rapport mensuel de haut niveau basé sur l'analyse des données du DAAR, mais à une granularité qui ne permet pas d'arriver à des conclusions sur les bureaux d'enregistrement et les opérateurs de registre qui présentent des abus significatifs. L'organisation ICANN ne partage pas non plus de données complètes (brutes) avec des chercheurs qui pourraient aider à améliorer la méthodologie ou à confirmer les résultats. Le personnel de l'OCTO a signalé à l'équipe de révision SSR2 que ces objectifs (données exploitables, validation) n'étaient pas des objectifs conceptuels du DAAR.[90] L'équipe de révision SSR2 considère que la façon dont l'organisation ICANN structure apparemment les accords avec les fournisseurs de données agit comme un inhibiteur significatif de ces objectifs et propose une révision de son programme d'analyse de l'utilisation malveillante du DNS où la transparence, la reproductibilité et les produits de données exploitables soient les objectifs principaux.

L'identification des opérateurs de registre et des bureaux d'enregistrement présentant des niveaux disproportionnés d'utilisation malveillante faciliterait la prise de décisions éclairées et ajouterait une mesure de transparence et de responsabilité au système d'enregistrement de noms de domaine qui n'existe pas aujourd'hui. En effet, l'équipe de révision n'est pas sûre de l'intérêt de l'implication de l'ICANN dans ce domaine si les données et les analyses ne sont ni exploitables ni partagées aux fins de la reproductibilité et de la validation. L'équipe de révision SSR2 estime qu'il serait approprié de mettre fin au programme DAAR si la communauté et l'organisation ICANN ne pouvaient pas réformer le DAAR pour atteindre ces objectifs. Recommandation 12 de la SSR2 : Réviser les efforts d'analyse et de signalement de l'utilisation malveillante du DNS pour permettre que les responsables de la transparence et la révision indépendante se centrent sur ce problème.

---

[87] Groupe de travail chargé des procédures pour des séries ultérieures de nouveaux gTLD de l'ICANN, « Rapport final sur les procédures pour des séries ultérieures de nouveaux gTLD de la GNSO », consulté le 7 décembre 2020, https://www.icann.org/public-comments/gnso-new-gtld-subsequent-draft-final-report-2020-08-20-en.

[88] FAQ du DAAR, https://www.icann.org/octo-ssr/daar-faqs/#security-threats.

[89] Piscitello, Dave, « Le système de signalement des cas d'utilisation malveillante des noms de domaine (DAAR) », rapport de l'APWG EU de l'ICANN, 2017 octobre https://www.icann.org/en/system/files/files/presentation-daar-31oct17-en.pdf.

[90] Transcription de l'appel, « Appel de la SSR2 sur le DAAR - 24 juin 2020 à 15h00 UTC » , https://community.icann.org/x/WIJIC.

iv. Plaintes

Le rapport de la CCT a noté la difficulté d'évaluer l'impact des sauvegardes étant donné le manque de transparence de la part du département de la conformité contractuelle de l'ICANN concernant les plaintes et le manque d'application des engagements d'intérêt public dans les contrats.[91] L'équipe de révision SSR2 a constaté qu'un problème clé pour ceux qui signalent des domaines malveillants est la nature compliquée du dépôt de plaintes, les différentes exigences entre les parties contractantes, et souvent le manque de réponse ou d'action (en temps opportun). L'équipe de révision SSR2 croit qu'un système centralisé de dépôt de plaintes pour abus simplifierait le processus de traitement des plaintes pour abus tant pour les auteurs que pour les parties contractantes et réduirait le nombre de plaintes mal redirigées.

L'équipe de révision SSR2 croit qu'un programme révisé d'analyse de l'utilisation malveillante du DNS permettrait au département de la conformité contractuelle de l'ICANN d'établir des attentes standard concernant la prévalence des abus. Étant donné que les noms bloqués peuvent ne pas être précis à 100 % et peuvent être manipulés, l'ICANN devra s'efforcer de valider les résultats de l'analyse et les parties contractantes devront avoir la possibilité de réfuter l'avis de l'ICANN.

Recommandation 10 de la SSR2 : clarifier les définitions des termes relatifs à l'utilisation malveillante

10.1. L'organisation ICANN devrait publier une page Web incluant sa définition pratique de l'utilisation malveillante du DNS, c'est-à-dire ce qu'elle utilise pour les projets, les documents et les contrats. La définition devrait signaler explicitement les types de menaces de sécurité que l'organisation ICANN, en vertu de son mandat, considère actuellement qu'il faut traiter par le biais de mécanismes contractuels et de conformité, ainsi que ceux qui, de l'avis de l'organisation ICANN, se trouvent en dehors de ses attributions. Si l'organisation ICANN utilisait une autre terminologie similaire, par exemple « une menace à la sécurité », « un comportement malveillant », elle devrait inclure à la fois sa définition de ces termes et la manière dont elle établit précisément une distinction entre ces termes et l'utilisation malveillante du DNS. Cette page devrait inclure des liens vers des extraits de toutes les obligations actuelles liées à l'utilisation malveillante dans les contrats avec les parties contractantes, y compris les procédures et protocoles pour répondre aux abus. L'organisation ICANN devrait mettre à jour cette page chaque année, inclure la date de la dernière version et fournir les liens vers des versions plus anciennes avec les dates de publication y associées.

10.2. Établir un groupe de travail intercommunautaire (CCWG) appuyé par le personnel afin d'établir un processus permettant de faire évoluer les définitions de l'interdiction de l'utilisation malveillante du DNS, au moins une fois tous les deux ans, selon un calendrier prévisible (par exemple, tous les mois de janvier), qui ne prendra pas plus de 30 jours ouvrables. Ce groupe devrait faire participer les parties prenantes de la protection des consommateurs, de la cybersécurité opérationnelle, de la recherche universitaire ou indépendante sur la cybersécurité, de l'application de la loi et du commerce électronique.

[91] Rapport de la CCT, 9 et 10, https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf.

10.3. Le Conseil d'administration de l'ICANN et l'organisation ICANN devraient utiliser les définitions consensuelles de manière cohérente dans les documents publics, les contrats, les plans de mise en œuvre de l'équipe de révision et d'autres activités, et faire en sorte que ces termes renvoient à cette page Web lorsqu'ils sont utilisés.

Cette recommandation pourra être considérée comme mise en œuvre lorsque l'organisation ICANN publiera la page Web qui inclut le premier résultat du CCWG ainsi que le processus de mise à jour de la page Web.

Cette recommandation pourra être considérée comme efficace lorsque l'organisation ICANN sera capable d'offrir une transparence et une responsabilité accrues en ce qui concerne les descriptions acceptées et approuvées par la communauté, la clarté des discussions communautaires et l'interprétation des documents de politique, permettant ainsi aux autres parties prenantes de définir des codes de conduite concernant l'utilisation malveillante du DNS.

Recommandation 11 de la SSR2 : résoudre les problèmes d'accès aux données CZDS

11.1. La communauté de l'ICANN et l'organisation ICANN devraient prendre des mesures pour assurer que l'accès aux données CZDS soit disponible, en temps voulu, et qu'il n'y ait pas d'obstacles inutiles pour les demandeurs, par exemple le manque d'auto-renouvellement des informations d'identification pour l'accès.

Cette recommandation pourra être considérée comme mise en œuvre lorsque l'organisation ICANN et la communauté mettront à disposition des demandeurs les données CZDS en temps opportun et sans obstacles inutiles.

Cette recommandation pourra être considérée comme efficace lorsque l'organisation ICANN signalera une diminution du nombre de plaintes concernant l'accès aux fichiers de zone et améliorera la capacité des chercheurs à étudier les opérations liées à la sécurité du DNS.

Cette recommandation vise à établir un accès approprié aux données des fichiers de zone de sécurité utilisées par les universitaires et les spécialistes en sécurité. Cette recommandation requiert une action du Conseil d'administration de l'ICANN, de l'organisation ICANN et de la GNSO.

Recommandation 12 de la SSR2 : réviser les efforts d'analyse et de signalement de l'utilisation malveillante du DNS pour permettre la transparence et la révision indépendante

12.1. L'organisation ICANN devrait créer une équipe consultative d'analyse de l'utilisation malveillante du DNS composée d'experts indépendants (c'est-à-dire d'experts sans conflits d'intérêts financiers) pour recommander une refonte de l'activité de signalement d'abus du DNS avec des données exploitables, la validation, la transparence et la reproductibilité indépendante des analyses comme ses priorités les plus élevées.

12.2. L'organisation ICANN devrait structurer ses accords avec les fournisseurs de données d'une manière qui permette le partage des données à des fins non commerciales, en particulier pour la validation ou la recherche scientifique examinée par des pairs. Cette licence non commerciale spéciale et gratuite pour

utiliser les données peut impliquer un délai qui ne présente pas de conflit avec les opportunités de revenus commerciaux du fournisseur de données. L'organisation ICANN devrait publier tous les termes du contrat de partage de données sur le site Web de l'ICANN. L'organisation ICANN devrait mettre fin à tout contrat qui ne permette pas une vérification indépendante de la méthodologie derrière la liste de noms bloqués.

12.3. L'organisation ICANN devrait publier des rapports qui identifient les opérateurs de registre et les bureaux d'enregistrement dont les domaines sont responsables de la plupart des cas d'abus L'organisation ICANN devrait inclure des formats de données lisibles par machine, en plus des données graphiques incluses dans les rapports actuels.

12.4. L'organisation ICANN devrait rassembler et publier des rapports sur les actions prises par les opérateurs de registre et les bureaux d'enregistrement, soit volontaires, soit en réponse à des obligations juridiques, pour répondre à des plaintes pour conduite illégale et / ou malveillante basées sur les lois applicables en relation avec l'utilisation du DNS.

Cette recommandation pourra être considérée comme mise en œuvre lorsque les efforts de l'organisation ICANN pour analyser l'utilisation malveillante du DNS introduisent des mesures qui produisent des données exploitables, précises et fiables.

Cette recommandation pourra être considérée comme efficace lorsque toutes les données disponibles pour l'organisation ICANN seront également disponibles pour la communauté et les chercheurs indépendants, peut-être avec un délai, pour fournir la validation et le retour.

Recommandation 13 de la SSR2 : accroître la transparence et la responsabilité du signalement des plaintes pour abus

13.1. 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 agirait purement comme un flux entrant, et l'organisation ICANN collecterait et traiterait uniquement le résumé et les métadonnées, y compris les horodatages et les types de plaintes (catégoriques). L'utilisation du système devrait devenir obligatoire pour tous les gTLD ; la participation de chaque ccTLD devrait être volontaire. En outre, l'organisation ICANN devrait partager les rapports d'abus (par exemple, par e-mail) avec tous les ccTLD.

13.2. L'organisation ICANN devrait publier le nombre de plaintes déposées sous une forme qui permette à des tiers indépendants d'analyser les types de plaintes concernant le DNS.

Cette recommandation pourra être considérée comme mise en œuvre lorsque l'organisation ICANN simplifiera le processus de dépôt et de réception des plaintes pour abus et offrira un aperçu du nombre de plaintes et de certaines métadonnées (par exemple, type d'abus signalé, dates, délai de résolution) pour les chercheurs et les membres de la communauté. Cette recommandation pourra être considérée comme terminée lorsque le portail sera opérationnel.

Cette recommandation pourra être considérée comme efficace lorsque les parties contractantes passeront moins de temps sur les plaintes mal dirigées, et tant la communauté de recherche

que la communauté élargie de l'ICANN pourront voir et étudier les données associées à ces plaintes.

En raison de la complexité de cette entreprise, cette recommandation devrait prendre plusieurs années (au moins trois) une fois que le Conseil d'administration de l'ICANN aura approuvé sa mise en œuvre.

3. Alternatives au processus d'élaboration de politiques (PDP)

Il est important de répondre aux allégations selon lesquelles une politique de consensus élaborée par un processus d'élaboration des politiques (PDP) est la seule voie pour mettre en œuvre plusieurs de nos recommandations. Il existe de nombreuses façons pour le Conseil d'administration de l'ICANN de mettre en œuvre nos recommandations. Le Conseil pourrait choisir des négociations contractuelles, émettre des avis aux parties contractantes ou utiliser un groupe de travail intercommunautaire à durée limitée et soutenu par des experts.[92] L'organisation ICANN pourrait même émettre une spécification temporaire basée sur une conviction du Conseil d'administration que l'utilisation malveillante du DNS est une grave préoccupation en matière de sécurité publique qui nécessite une attention urgente. L'utilisation récente par le Conseil de la spécification temporaire en réponse aux incohérences entre le RGPD de l'UE et les propres statuts constitutifs de l'organisation ICANN est une étude de cas utile. La communauté de l'ICANN a pris des années pour élaborer une politique d'accès aux données d'enregistrement qui serait compatible avec le RGPD, mais qui a effectivement remis le problème. Nous voyons un schéma similaire en ce qui concerne l'utilisation malveillante du DNS et l'accès aux données d'enregistrement pour lutter contre l'abus.

L'organisation ICANN peut mener des négociations contractuelles bilatérales et le fait. Des changements aux contrats de registre et de bureau d'enregistrement de l'organisation ICANN ont eu lieu sans une politique de consensus créée par un PDP. Lorsque l'organisation ICANN est passée au RAA 2013 et au contrat de registre de base de 2017, l'organisation ICANN et une équipe de négociation représentant l'industrie respective ont géré le processus, sans aucun PDP. La communauté a eu l'occasion de formuler des commentaires sur le texte préliminaire, mais seule l'équipe de négociation a participé aux discussions et aux décisions.[93] Ces négociations à porte fermée entre l'organisation ICANN et les parties contractantes sont un véhicule précieux pour le progrès, mais sont limitées en matière d'utilisation malveillante du DNS parce qu'elles excluent toutes les autres parties prenantes, y compris les gouvernements, les entreprises et le public, qui ont tous un intérêt à réduire les enregistrements abusifs. Recommandation 12 de la SSR2 : réviser les efforts d'analyse et de signalement de l'utilisation malveillante du DNS pour permettre la transparence et la révision indépendante de surmonter cet écueil.

---

[92] Des exemples antérieurs d'avis aux parties contractantes sont disponibles sur le site Web des bulletins d'information à l'intention des bureaux d'enregistrement (https://whois.icann.org/en/registrar-advisories).

[93] Contrat d'accréditation de bureau d'enregistrement de 2013, https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en. Note : l'ICANN peut modifier les contrats soit par le biais d'une politique de consensus, soit par la négociation entre l'organisation ICANN et les autres parties concernées, conformément à l'article 1.2 du RAA, aux politiques de consensus et à la spécification des politiques temporaires, https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#consensus-temporary.

Surtout à la suite de l'incapacité de l'EPDP à résoudre l'accès aux données d'enregistrement, les conflits d'intérêts énormes qui pèsent sur le processus d'élaboration de politiques et la lenteur des progrès dans la lutte contre l'utilisation malveillante du DNS, l'équipe de révision estime qu'un processus EPDP concernant les abus ne permettra pas d'apporter, à lui seul, une solution efficace. La finalisation de l'EPDP sur l'accès aux données d'enregistrement a pris des années et le produit final a fait l'objet de la dissidence d'une majorité de la communauté de l'ICANN. Il y a eu des déclarations minoritaires substantielles du Comité consultatif At-Large (ALAC), de l'Unité constitutive des utilisateurs commerciaux (BC), de l'Unité constitutive des représentants de la propriété intellectuelle (IPC), du Groupe des représentants des entités non commerciales (NSCG), du Groupe des représentants des bureaux d'enregistrement (RrSG) et du Groupe des représentants des opérateurs de registre (RySG). Le rapport minoritaire de la BC et de l'IPC a signalé que : « Les régulateurs et les législateurs devraient prendre bonne note du fait que le modèle multipartite de l'ICANN s'est avéré incapable de répondre aux besoins en matière de protection des consommateurs, de cybersécurité et d'application de la loi ».[94] Le rapport minoritaire du SSAC a également mis en garde contre le fait que le processus d'élaboration de politiques de l'ICANN *« n'a pas fourni de résultats raisonnablement adaptés à la sécurité et à la stabilité ».*[95]

En résumé, l'atténuation, la prévention et l'arrêt de l'utilisation malveillante du DNS existants sont contestés par l'ambiguïté de la terminologie et des exigences contractuelles existantes, les conflits d'intérêts entre toutes les parties qui auraient besoin d'agir, et les engagements variés des gouvernements du monde entier pour traiter également l'utilisation malveillante du DNS par le biais d'autres procédures juridiques. Certaines politiques et obligations contractuelles liées à l'utilisation malveillante du DNS existent déjà, mais l'organisation ICANN et les parties contractantes doivent les mettre en œuvre et les appliquer plus efficacement ; et la communauté doit élaborer des politiques, des obligations contractuelles et des activités supplémentaires pour suivre le rythme de l'utilisation malveillante du DNS. L'équipe de révision SSR2 considère l'utilisation malveillante du DNS comme un besoin critique qui mérite de et justifie un contrôle strict de l'ICANN dans ce domaine. La spécification temporaire du RGPD a démontré que le Conseil d'administration de l'ICANN maintient son autorité en matière d'élaboration de politiques en réponse à divers besoins. En outre, le Conseil a des devoirs fiduciaires pour s'assurer que les politiques organisationnelles de l'ICANN et les contrats dérivés soient adaptés à l'objectif de l'organisation ICANN en tant que société californienne d'utilité publique à but non lucratif chargée de surveiller la sécurité, la stabilité du DNS et l'élaboration de politiques dans l'intérêt public. Une nouvelle spécification temporaire combinée à un nouvel EPDP pourrait s'avérer la meilleure approche.[96]

Recommandation 14 de la SSR2 : créer une spécification temporaire pour les améliorations de la sécurité fondées sur des données factuelles

[94] Rapport de l'étape 2 de l'EPDP de la GNSO, Déclaration minoritaire des BC/IPC, 114 à 121, https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf.

[95] Ibid., 145 à 162, Déclaration minoritaire du SSAC.

[96] L'équipe de révision SSR2 croit que l'organisation ICANN a compilé un ensemble suffisant de connaissances, y compris celles qui ont conduit au programme DAAR et les rapports DAAR eux-mêmes, pour compiler un rapport thématique, justifiant ainsi le démarrage d'un EPDP plutôt qu'un PDP.

14.1. L'organisation ICANN devrait créer une spécification temporaire qui exige que toutes les parties contractantes contrôlent le pourcentage de domaines identifiés par l'activité de signalement d'abus DNS révisée (voir la recommandation 13.1 de la SSR2) identifiés comme abusifs et le maintiennent en dessous d'un seuil raisonnable et publié.

14.2. Pour permettre une action anti-abus, l'organisation ICANN devrait fournir aux parties contractantes des listes de domaines dans leurs portefeuilles identifiés comme abusifs, conformément à la recommandation 12.2 de la SSR2 concernant la révision indépendante des données et des méthodes pour la liste de domaines bloqués.

14.3. Si le nombre de domaines liés à une activité abusive atteignait le seuil publié décrit dans la Recommandation 14.1 de la SSR2, l'organisation ICANN devrait mener une enquête pour confirmer la véracité des données et de l'analyse, puis émettre un avis à la partie concernée.

14.4. L'organisation ICANN devrait permettre aux parties contractantes un délai de 30 jours pour réduire la fraction de domaines abusifs en dessous du seuil ou pour démontrer que les conclusions ou les données de l'organisation ICANN sont erronées. Si une partie contractante ne parvenait pas à compléter la rectification pendant 60 jours, le département de la conformité contractuelle de l'ICANN devrait passer au processus de désaccréditation.

14.5. L'organisation ICANN devrait envisager d'offrir des incitations financières : les parties contractantes avec des portefeuilles au-dessous d'un pourcentage donné de noms de domaine abusifs devraient recevoir une réduction des frais sur les transactions payantes jusqu'à un seuil approprié.

Recommandation 15 de la SSR2 : lancer un EPDP fondé sur des données factuelles pour améliorer la sécurité

15.1. Après avoir créé la spécification temporaire (voir la Recommandation 14 de la SSR2 : créer une spécification temporaire pour les améliorations de sécurité fondées sur des données factuelles), l'organisation ICANN devrait établir un EPDP soutenu par le personnel pour créer une politique anti-abus. Les volontaires de l'EPDP devraient représenter la communauté de l'ICANN, en utilisant les numéros et la distribution de la spécification temporaire pour les données d'enregistrement de gTLD comme modèle de charte de l'équipe responsable de l'EPDP.[97]

15.2. L'EPDP devrait s'appuyer sur le fondement de la définition du CCWG proposée dans la recommandation 10.2 de la SSR2. Ce cadre de politique devrait définir des contre-mesures et des mesures correctives appropriées pour différents types d'abus, des délais pour les actions des parties contractantes tels que les délais des rapports d'abus/rapports de réponse et les actions d'application de la conformité contractuelle de l'ICANN en cas de violations de la politique. L'organisation ICANN devrait insister sur le pouvoir de résilier les contrats dans le cas de répétitions de conduites et de pratiques de protection des abus de la part de toute partie contractante. Le résultat devrait inclure un mécanisme de mise à jour des critères de référence et des obligations contractuelles

[97] ICANN, « Charte de l'équipe du PDP », page modifiée le 23 juillet 2018, 12 à 14, https://community.icann.org/display/EOTSFGRD/EPDP+Team+Charter.

liées aux abus tous les deux ans, en utilisant un processus qui ne prendrait pas plus de 45 jours ouvrables.

Les recommandations 14 et 15 de la SSR2 pourront être considérées comme mises en œuvre lorsque le département de la conformité contractuelle de l'ICANN disposera des outils nécessaires pour répondre de manière appropriée aux parties contractantes qui ne répondent pas à l'utilisation malveillante du DNS, en particulier l'existence d'obligations liées à l'abus dans tous les contrats et accords pertinents.

Les Recommandations 14 et 15 de la SSR2 pourront être considérées comme efficaces lorsque le département de la conformité contractuelle de l'ICANN utilisera ces outils pour traiter les violations flagrantes des politiques de la part des parties contractantes.

Le résultat prévu des Recommandations 14 et 15 de la SSR2 est d'habiliter le département de la conformité contractuelle de l'ICANN à s'occuper des pires contrevenants en matière d'utilisation malveillante du DNS, l'équipe de la conformité contractuelle de l'ICANN ayant déclaré ne pas avoir suffisamment d'outils pour y faire face.

Ces recommandations nécessitent une action de l'organisation ICANN et de la communauté de l'ICANN et sont destinées à guider la création de politiques. Ces recommandations sont réalisables, mais l'organisation ICANN ne pourra les compléter qu'au fil du temps.

4. Vie privée et supervision des données

La protection de la vie privée est un problème en constante évolution en raison de la quantité croissante de données collectées et analysées par des tiers (en plus des entités gouvernementales traditionnelles) ainsi que du panorama de la législation sur la protection de la vie privée. L'équipe de révision SSR2 conclut que l'organisation ICANN n'a pas été aussi proactive qu'elle aurait dû l'être étant donné le paysage changeant, comme en témoignent ses incohérences dans les données disponibles dans et à propos du RDS.[98]

Il y a une prolifération de pages Web sans dates associées à ces pages dans l'ensemble du site Web de l'ICANN qui traitent de divers aspects de l'anonymisation des données d'enregistrement. Ce manque d'horodatages a rendu impossible pour l'équipe de révision de faire des recherches raisonnables sur l'historique de l'organisation ICANN à cet égard.[99] Depuis octobre 2020, le site Web du RDS et la documentation connexe sont également obsolètes et ne contiennent pas de documents communautaires pertinents. Il existe quelques pages Web de l'ICANN sur le RDS, mais celles-ci ne font pas de références croisées. La dernière mise à jour de la page Web du RDS de l'ICANN en 2017 ne fait donc pas référence aux mesures actuelles de la spécification temporaire ou au statut de l'EPDP.[100] L'équipe de révision considère que le

[98] Consulter la section E.2.b.i « Données d'enregistrement » et la section E.2.b.ii « Service centralisé de données de zone » (CZDS) du présent rapport.

[99] Exemples : https://whois.icann.org/en/privacy-and-proxy-services, https://whois.icann.org/en/privacy, https://whois.icann.org/en/revised-icann-procedure-handling-whois-conflicts-privacy-lawet https://www.icann.org/rdap. Note : ces pages semblent toutes avoir de nombreuses années, et plusieurs incluent une note en bas de la page : « Le 17 mai 2018, le Conseil d'administration de l'ICANN a adopté une spécification temporaire pour les données d'enregistrement des gTLD. Cette page est en cours de révision et sera mise à jour pour répondre à la Spécification temporaire ».

[100] ICANN, « À propos du WHOIS », dernière mise à jour en juillet 2017https://whois.icann.org/en/about-whois.

manque d'information et de cohérence sur le site Web reflète le manque de clarté et de cohérence de l'ICANN sur les questions entourant la confidentialité.

Dans la section E.2.b.i. « Données d'enregistrement », l'équipe de révision a également souligné la nécessité d'équilibrer la transparence et la responsabilité des métadonnées d'enregistrement des noms de domaine à la lumière de divers règlements sur la protection de la vie privée comme le RGPD. En assurant la cohérence de son propre site Web ainsi que de ses politiques de consensus et ses contrats avec les opérateurs de registre et les bureaux d'enregistrement, l'organisation ICANN aidera à assurer la gestion sécurisée et la protection de la collecte, la conservation, l'entiercement, le transfert et l'affichage des données d'enregistrement, ce qui inclut les coordonnées du titulaire du nom de domaine, les informations administratives, et les contacts techniques ainsi que les informations techniques associées à un nom de domaine.

Recommandation 16 de la SSR2 : exigences de confidentialité et RDS

16.1. L'organisation ICANN devrait fournir des références croisées cohérentes sur son site Web afin de fournir des informations claires et faciles à trouver sur toutes les actions (passées, présentes et planifiées) prises au sujet de la confidentialité et de la gestion des données, en portant une attention particulière aux informations concernant le RDS.

16.2. L'organisation ICANN devrait créer des groupes spécialisés au sein de la fonction de conformité contractuelle qui comprennent les exigences et les principes de confidentialité (tels que la limitation de la collecte, la qualification des données, la spécification des objectifs, et des mesures de sécurité pour la divulgation) et qui puissent faciliter les besoins d'application de la loi dans le cadre du RDS, modifié et adopté par la communauté (voir également la recommandation 11 de la SSR2 : résoudre les problèmes d'accès aux données CZDS).

16.3. L'organisation ICANN devrait effectuer des audits périodiques sur le respect des politiques de protection de la vie privée mises en œuvre par les bureaux d'enregistrement pour s'assurer que celles-ci aient mis en place des procédures pour traiter les atteintes à la vie privée.

Cette recommandation pourra être considérée comme mise en œuvre lorsque les actions de l'organisation ICANN concernant la confidentialité et leur gestion du RDS seront correctement documentées, et que des ressources spécifiquement affectées au sein de l'organisation ICANN maintiennent l'organisation en conformité avec les meilleures pratiques et les exigences juridiques actuelles dans cet espace.

Cette recommandation pourra être considérée comme efficace lorsque l'organisation ICANN pourra démontrer une conformité continue avec les meilleures pratiques et les exigences légales en matière de traitement des données et de protection de la vie privée.

F. Autres problèmes liés à la SSR concernant le DNS mondial

L'équipe de révision SSR2 reconnaît que l'organisation ICANN n'est qu'une des nombreuses entités de l'écosystème du DNS. Cela dit, l'organisation ICANN fait partie de ceux qui sont dans une position unique pour influencer et guider les actions liées à la SSR dans l'ensemble de l'écosystème. Cette section propose des recommandations spécifiques pour savoir où l'organisation ICANN peut améliorer ses politiques et pratiques pour elle-même et pour l'ensemble du DNS mondial. En modélisant les meilleures pratiques dans la gestion de l'IMSR, en partageant la contribution consolidée des chercheurs, en offrant des outils de test et d'analyse et d'autres actions possibles discutées dans cette section, l'organisation ICANN peut prendre des mesures pour améliorer ses propres actions en matière de SSR et aider les autres à comprendre comment améliorer les leurs.

1. Collision de noms

Bien que l'organisation ICANN fournisse des informations détaillées et une formation sur la collision de noms, il n'existe aucune restriction pour les titulaires de noms de domaine utilisant un identifiant unique pour une zone privée qui entre en collision avec une zone publique. L'équipe de révision SSR2 croit que l'étude récemment terminée et publiée (ci-après appelée étude NCAP de 2019) est un pas dans la bonne direction pour gérer les collisions de noms indésirables.[101] Toutefois, cette étude n'a pas abordé le besoin continu de mécanismes pour découvrir les collisions de noms non déclarées, à la fois malveillantes et accidentelles. L'étude a également conclu qu'il n'y avait pas de recherche récente sur les collisions de noms (depuis 2017) et a pris la diminution des collisions de noms signalées comme indicateur du bon fonctionnement des mécanismes actuels.[102] D'autre part, des recherches examinées par des pairs en 2016 ont révélé que la dernière série de gTLD exacerbait de manière mesurable le problème de la collision de noms.[103] La diminution des collisions de noms signalées, comme l'indiquent les mécanismes traditionnels de signalement, peut ne pas impliquer l'absence de collisions de noms. Plutôt, la nature des collisions de noms peut avoir changé de manière à échapper à ces mécanismes traditionnels. Il y a également eu une diminution de la délégation de nouveaux gTLD au cours des dernières années, ce qui pourrait avoir une incidence supplémentaire sur le nombre absolu de collisions de noms signalées.[104]

Même si un cadre d'interruption contrôlée a été proposé pour éviter une éventuelle collision de noms de domaine dans un rapport commandé par l'ICANN en 2014 (ci-après appelé « Rapport de la première étape »), ce cadre d'interruption contrôlée n'a jamais été testé contre des

[101] Scarfone, Karen, « Gestion des risques des collisions de noms au premier niveau : Résultats du projet d'analyse de la collision de noms (NCAP), OCTO de l'ICANN, 27 mai 2020, https://www.icann.org/en/system/files/files/managing-risks-tld-2-name-collision-07may20-en.pdf.

[102] Ibid, 43.

[103] Chen, Qi Alfred, Eric Osterweil, Matthew Thomas et Z. Morley Mao. « Attaque MitM par collision de noms : Analyse des causes et évaluation de la vulnérabilité à l'ère des nouveaux gTLD ». Symposium de l'IEEE sur la sécurité et la protection de la vie privée (SP) de 2016 (mai 2016), 675 à 690. doi:10.1109/sp.2016.46.

[104] ICANN, site Web des nouveaux gTLD, https://newgtlds.icann.org/en/program-status/statistics. Note : au 12 décembre 2020, seulement 9 gTLD restent en cours de traitement par rapport aux 1930 gTLD disponibles au début.

scénarios d'attaque de collision de noms en évolution.[105] Par exemple, le SSAC a indiqué que « *au lieu d'une seule période d'interruption contrôlée, l'ICANN devrait introduire des périodes d'interruption continues, interrompues par des périodes de fonctionnement normal, pour permettre aux systèmes des utilisateurs finaux concernés de continuer à fonctionner pendant la période de test de 120 jours avec moins de risque d'impact commercial catastrophique* ».[106] Dans le rapport de la première étape, les auteurs ont fondé certaines de leurs conclusions sur le manque de courriers électroniques et d'appels téléphoniques de la part des titulaires des domaines de second niveau, ce qui ne reflète pas adéquatement la complexité du problème.[107] Le rapport de la première étape a également discuté de plusieurs approches alternatives au cadre d'interruption contrôlée, y compris l'utilisation du système pot de miel, de DNAME et d'approches chaîne à chaîne, mais ces approches n'ont jamais été envisagées pour la mise en œuvre.[108] L'équipe de révision SSR2 conclut, contrairement au rapport de la première étape, que la collision de noms demeure un défi qui mérite d'être étudié et atténué.

Recommandation 17 de la SSR2 : mesure des collisions de noms

17.1. L'organisation ICANN devrait créer un cadre qui caractérise la nature et la fréquence des collisions de noms et des préoccupations y associées. Ce cadre devrait inclure des mesures et des mécanismes pour établir à quel point l'interruption contrôlée réussit à identifier et à éliminer les collisions de noms. Ceci peut être pris en charge par un mécanisme permettant d'activer la divulgation protégée des instances de collision de noms. Ce cadre devrait permettre le traitement approprié des données sensibles et des menaces à la sécurité.

17.2. La communauté de l'ICANN devrait élaborer une politique claire pour éviter et gérer les collisions de noms liées à de nouveaux gTLD et mettre en œuvre cette politique avant la prochaine série de gTLD. L'organisation ICANN devrait s'assurer que l'évaluation de cette politique soit entreprise par les parties n'ayant aucun intérêt financier dans l'expansion des gTLD.

Cette recommandation pourra être considérée comme mise en œuvre lorsque l'organisation ICANN élaborera un cadre pour produire des résultats qui caractérisent la nature et la fréquence des collisions de noms et les préoccupations qui en résultent en identifiant des mesures et en concevant des mécanismes pour établir la mesure dans laquelle le mécanisme d'interruption contrôlée est réussi.

La recommandation pourra être considérée comme efficace lorsque l'organisation ICANN et la communauté seront capables de détecter, d'agir et, en fin de compte, de minimiser l'existence de collisions de noms et de répondre à l'évolution des scénarios de collision de noms.

---

[105] ICANN, rapport « Atténuation des risques de collision dans l'espace de noms du DNS, première étape », 6 juillet 2014, 6, https://www.icann.org/en/system/files/files/name-collision-mitigation-study-06jun14-en.pdf, et ICANN, « Cadre de gestion de l'occurrence de collisions de noms de domaine », 30 juillet 2014, 2 et 3, https://www.icann.org/en/system/files/files/name-collision-framework-30jul14-en.pdf.

[106] ICANN SSAC, « SAC066 : commentaire du SSAC relatif au rapport sur la première étape du JAS concernant l'atténuation du risque de collisions dans l'espace de noms du DNS, 6 juin 2014, 4 https://www.icann.org/en/system/files/files/sac-066-en.pdf.

[107] Rapport « Atténuer les risques de collision dans l'espace de noms du DNS, première étape », 22, https://www.icann.org/en/system/files/files/name-collision-mitigation-study-06jun14-en.pdf.

[108] Ibid.

Cette recommandation devra être complétée avant la prochaine série de gTLD.

2. Recherche et séances d'information

La communauté de recherche universitaire mène actuellement un grand nombre d'activités concernant les questions liées à la sécurité, la stabilité et la résilience dans les couches de nommage, de routage et d'adressage. La communauté de l'ICANN a l'occasion de tirer parti de cette activité et de cette expertise pour éclairer les politiques et le développement technologique qui réduiront de manière mesurable les préjudices liés à la SSR dans l'écosystème. Mais il n'existe aucune fonction pour s'assurer que l'organisation ICANN elle-même et la communauté qu'elle sert restent au courant de ces développements.

Recommandation 18 de la SSR2 : informer les débats sur les politiques

18.1. 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, le Symposium sur la sécurité et la vie privée de l'IEEE, ainsi que les conférences sur la sécurité opérationnelle 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.[109]

18.2. L'organisation ICANN devrait assurer que ces rapports comprennent des observations pertinentes pouvant avoir trait à des recommandations d'actions, y compris les changements aux contrats avec les opérateurs de registre 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.

18.3. L'organisation ICANN devrait également recommander que ces rapports incluent des recommandations pour des études supplémentaires qui confirment les résultats révisés par les pairs, une description des données qui seraient nécessaires pour mener à bien d'autres études, et expliquer comment l'organisation ICANN peut offrir d'aider à garantir l'accès à de telles données, par exemple, via le CZDS.

[109] Liens vers les conférences : ACM CCS <https://dl.acm.org/conference/ccs>, ACM Internet Measurement Conference <https://www.sigcomm.org/events/imc-conference>, Usenix Security <https://www.usenix.org/conferences>, CCR <https://www.ccrsummit.com/>, SIGCOMM <https://www.sigcomm.org/>, Symposium de l'IEEE sur la sécurité et la vie privée <https://www.ieee-security.org/index.html>, FIRST <https://www.first.org/>. Note : la mise en œuvre suggérée pourrait être de contacter les organisateurs (présidents du comité de programme technique, organisateurs de groupe de pilotage, etc.) et de demander des résumés des délibérations et/ou d'inviter les membres du comité de ces sites à présenter chaque année des résumés pertinents de leurs délibérations, lors de l'un des événements communautaires de l'ICANN. Dans une telle mise en œuvre, l'organisation ICANN conserverait les réunions d'information dans un rapport archivé.

Cette recommandation pourra être considérée comme mise en œuvre lorsque l'organisation ICANN créera et maintiendra une archive publique de résumés ou de réunions d'information de diverses conférences de recherche en matière de réseautage et de sécurité.

Cette recommandation pourra être considérée comme efficace lorsque l'information provenant de la communauté de recherche sur les questions liées à la SSR deviendra plus accessible aux personnes qui prennent des décisions stratégiques.

3. Banc d'essai du DNS

Comme l'écosystème du DNS est déjà vaste et en pleine croissance, il est essentiel de maintenir et de surveiller une suite de tests de régression et un banc d'essai pour analyser les comportements et les interactions du DNS. L'équipe de révision SSR2 a conclu que les activités de test du DNS menées actuellement par l'OCTO répondront convenablement à ce problème une fois qu'elles seront terminées.[110] L'équipe de révision croit en outre que le soutien et la maintenance de ce banc d'essai (ainsi que la considération de ses résultats et constats) sont une exigence de l'organisation ICANN.

L'achèvement et la maintenance en temps opportun de ce banc d'essai permettraient à la communauté de l'ICANN de tester et de rechercher le comportement du résolveur, ce qui est essentiel pour assurer l'intégrité et la disponibilité mondiale du DNS.

Recommandation 19 de la SSR2 : développement complet d'un test de régression du DNS

19.1. L'organisation ICANN devrait compléter la mise au point d'une suite de tests de comportement des résolveurs du DNS.

19.2. L'organisation ICANN devrait garantir que la capacité de continuer à exécuter des tests fonctionnels des différentes configurations et versions de logiciel soit mise en œuvre et entretenue.

Cette recommandation pourra être considérée comme mise en œuvre lorsque l'organisation ICANN terminera l'élaboration d'une suite de tests accessible au public pour les tests communautaires et la recherche sur le comportement du résolveur.

Cette recommandation pourra être considérée comme efficace lorsqu'une suite de tests sera disponible avec un cycle de mise à jour annuel qui permette de garantir l'intégrité et la disponibilité mondiale du DNS.

4. Problèmes liés à la zone racine et au registre

A. Roulement de la clé

La clé de signature de clé des DNSSEC (KSK) de la zone racine a été reprise le 11 octobre 2018 pour la première fois depuis l'établissement de la clé de la zone racine délibérément non

[110] « Plateforme d'essai du résolveur », référentiel GitHub de l'ICANN, https://github.com/icann/resolver-testbed.

validable (DURZ).[111] Au cours du processus de roulement, il y a eu beaucoup de débats et de nombreux appels à des analyses des détails du roulement.[112] L'un des résultats de l'analyse de l'équipe de révision SSR2 a été de comprendre que les étapes d'exception qui fonctionnent correctement dans la procédure sont nécessaires pour un roulement de clé sûr et réussi.[113] L'organisation ICANN a retardé le transfert pendant un an et a pris des mesures pour apaiser les inquiétudes. Les discussions sur le calendrier et la procédure pour les futurs transferts au sein de la communauté de l'ICANN ont déjà commencé, y compris la prise en compte de nouvelles complexités potentielles, par exemple, les roulements de l'algorithme.[114] L'organisation ICANN a par la suite organisé un appel à commentaires ouvert sur le prochain processus de clé de signature de clé (KSK) prévu.[115]

En raison de la criticité des protections de sécurité qui sont (et seront) dérivées de la zone racine signée par les DNSSEC, des analyses de processus officiellement vérifiables sont essentielles pour assurer la sécurité, la stabilité et la résilience du processus par lequel les protections des DNSSEC sont maintenues pendant les roulements de la KSK de la zone racine.[116] La modélisation formelle des processus utilise une méthodologie et/ou un environnement de programmation pour spécifier chaque tâche dans un processus, évaluer son exécution (réussite, échec, autre, etc.) et spécifier les actions de suivi sous différents résultats. Les spécifications de processus comme celle-ci ont montré l'utilité dans les processus interhumains complexes qui incluent la sécurité électorale, la sécurité des processus médicaux, et plus encore.[117] Dans ces cas, les tâches des individus (dans l'espace humain) sont complexes et modélisées dans des langages formels de spécification des processus, et les choix et conséquences critiques (et critiques à la vie) sont symboliquement modélisés et officiellement suivis. Cette modélisation permet des prescriptions quantitatives et des

[111] ICANN, « Le premier roulement de la KSK de la racine a été complété avec succès », 15 octobre 2018, https://www.icann.org/news/announcement-2018-10-15-en.

[112] ICANN, « Le roulement récent de la KSK : résumé et prochaines étapes », blog de l'ICANN, 30 janvier 2018, https://www.icann.org/news/blog/the-recent-ksk-rollover-summary-and-next-steps, et Moritz Müller, Matthew Thomas, Duane Wessels, Wes Hardaker, Taejoong Chung, Willem Toorop, et Roland van Rijswijk-Deij, « Roulez, roulez Taejon votre racine : une analyse exhaustive du plus grand roulement de la racine de la KSK des DNSSEC » 2019 octobre https://dl.acm.org/doi/10.1145/3355369.3355570.

[113] Transcription de la plénière de la SSR2 nº 97 - séance du matin, 17 janvier 2020, p. 35, https://community.icann.org/x/HJkzBw.

[114] Rapport du personnel relatif à la procédure de consultation publique : proposition pour les roulements futurs de la clé de signature de clé de la zone racine, 7 août 2020 https://www.icann.org/en/system/files/files/report-comments-proposal-future-rz-ksk-rollovers-07aug20-en.pdf. Note : les Services de registre japonais, l'Unité constitutive des utilisateurs commerciaux, le Groupe des représentants des entités non commerciales, le Comité consultatif du système des serveurs racine, le Comité consultatif sur la sécurité et la stabilité de l'ICANN et plusieurs personnes ont soumis des commentaires.

[115] « Proposition pour les futurs roulements de clé de signature de clé (KSK) de la zone racine », 1er novembre 2019, https://www.icann.org/public-comments/proposal-future-rz-ksk-rollovers-2019-11-01-en.

[116] Osterweil, Eric. « Le dernier de sa nature cybersécuritaire : : utilisez-le avant de le perdre ». *IEEE sécurité et vie privée* 18, nº 4 (2020) : 67 à 70.

[117] Osterweil, Leon J., Matt Bishop, Heather Conboy, Huong Phan, Borislava I. Simidchieva, George Avrunin, Lori A. Clarke et Sean Peisert, « Analyse itérative pour améliorer les propriétés clés des processus essentiels dépendant de l'activité humaine : un exemple de sécurité pendant les élections », Transactions ACM sur la confidentialité et la sécurité (TOPS), vol. 20, nº 2, mai 2017, p. 5:1 à 31. (UM-CS-2016-012) et Clarke, Lori A., Yao Chen, George S. Avrunin, Bin Chen, Rachel Cobleigh, Kim Frederick, Elizabeth A. Henneman et Leon J. Osterweil. « Programmation de processus pour assurer la sécurité médicale : une étude de cas sur la transfusion sanguine ». Atelier sur les processus logiciels, p. 347 à 359. Springer, Berlin, Heidelberg, 2005.

prédictions sur ce qui devrait être fait et ce qui peut être attendu et peut résulter des choix, des exceptions et des exécutions réussies.[118] Par rapport aux élections et aux processus médicaux, le roulement de la KSK de la zone racine du DNS se présente comme un événement convivial dont la sécurité et l'exactitude sont critiques à l'échelle mondiale.

Recommandation 20 de la SSR2 : procédures officielles pour les roulements de clé

20.1. L'organisation ICANN devrait établir une procédure formelle, étayée sur un outil de modélisation et de langage qui suive un processus formel, pour spécifier les détails des roulements de clé futurs, y compris des points à décider, 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 (par exemple, le programme ou l'automate avec un nombre défini d'états (FSM)) pour consultation publique et l'organisation ICANN devrait 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'est-à-dire, avec la même périodicité) de sorte que l'organisation ICANN puisse utiliser les leçons apprises pour ajuster le processus.

20.2. 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.

Cette recommandation pourra être considérée comme mise en œuvre lorsque l'organisation ICANN développera un processus et une vérification formels qui offrent une vérification du processus de roulement de la clé après chaque roulement de la clé, et lorsque l'organisation ICANN commencera à exécuter des exercices de simulation sur table réguliers pour tester et familiariser les participants avec le processus de roulement de la clé.

Cette recommandation pourra être considérée comme efficace lorsque la SSR du processus par lequel les protections DNSSEC sont maintenues pendant les roulements de la KSK de la zone racine soient formellement vérifiables.

Cette recommandation devra être effectuée en simultané avec chaque roulement de la clé.

B. Gestion des changements de la zone racine

L'équipe de révision SSR2 a observé que la PTI a bien réussi à mettre en œuvre des mécanismes qui réduisent la possibilité de manipuler les données TLD et la zone racine.[119] La gestion de la zone racine suit un système de flux de travail pour la gestion des étiquettes TLD dans la zone racine appelé Système de gestion de la zone racine (RZMS). Ce flux de travail suit

[118] 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. 5:131. (UM-CS-2016-012)

[119] Jennifer Bryce à la liste de diffusion de l'équipe de révision SSR2, 2 juillet 2020, objet : Réponses SSR sur le DNS, https://mm.icann.org/pipermail/ssr2-review/2019-March/001569.html.

une approche prudente de la gestion du changement, car chaque changement nécessite une révision de la part de plusieurs parties.[120]

Bien qu'aucun problème de sécurité et de stabilité ne soit connu et ne soit lié à une utilisation abusive du RZMS, il existe un risque de cyberattaques insignifiantes au cours du processus d'authentification pour toutes les parties impliquées dans le flux de travail du RZMS. La communication avec les opérateurs TLD se fait désormais en envoyant des e-mails en texte clair et en accédant au système à l'aide d'une simple combinaison utilisateur/mot de passe. L'authentification des demandes de changement doit être plus stricte et impliquer une authentification multi-facteurs (MFA) et une communication sécurisée (par exemple, le chiffrement) lors de l'utilisation de la messagerie.

L'équipe chargée des fonctions IANA est en train de développer sa nouvelle génération de RZMS, ce qui implique une réécriture substantielle du modèle d'autorisation.[121] La nouvelle génération de RZMS devrait comporter un modèle d'authentification et d'autorisation robuste et sécurisé pour la soumission et l'approbation des demandes, ainsi que des fonctionnalités supplémentaires qui améliorent la sécurité et la stabilité du système DNS mondial, notamment :

- Garantir l'intégrité et l'authenticité des demandes de modification des données TLD.
- Imposer des communications sécurisées à tous les niveaux impliquant la gestion des demandes.
- Être résilient aux activités frauduleuses possibles qui impliquent des serveurs DNS faisant autorité pour les zones racine et TLD.
- Répondre rapidement aux demandes de suppression (suppression des enregistrements NS ou DS).
- Examen (impliquant l'évaluation du SSAC et du RSSAC et le processus d'approbation publique) de contrôles techniques et de procédures supplémentaires automatisés pour la résolution rapide des problèmes pouvant affecter le fonctionnement continu du DNS pour les TLD.
- Examen par le SSAC et le RSSAC de la mise en œuvre du RFC 8078 et des mises à jour connexes pour la gestion automatisée du maintien de l'ancre de confiance de la délégation des DNSSEC (CDS/CDNSKEY).122

Bien que l'organisation ICANN ait déjà annoncé le développement et la mise en œuvre du nouveau système RZMS avec des exigences de sécurité plus strictes en matière de communication, l'équipe de révision SSR2 n'a trouvé aucune indication quant au moment auquel l'organisation ICANN prévoit de mettre le nouveau système en service.

Recommandation 21 de la SSR2 : améliorer la sécurité des communications avec les opérateurs de TLD

[120] Noms et numéros de l'Internet (IANA), « processus de demande de changement dans la zone racine », consulté le 8 décembre 2020, https://www.iana.org/help/root-zone-process.
[121] PTI, « Réunion des membres de la ccNSO - Mise à jour de la fonction de nommage de l'IANA », ICANN60, 31 octobre 2017, diapositives 11 à 14, https://ccnso.icann.org/sites/default/files/field-attached/presentation-pti-members-31oct17-en.pdf.
[122] Gudmundsson, O. et P. Wouters, « Gestion des enregistrements du parent via le CDS/CDNSKEY », RFC 8078, DOI 10.17487/RFC8078, mars 2017, <https://www.rfc-editor.org/info/rfc8078>.

21.1. Les opérations de l'organisation ICANN et de la PTI devraient accélérer la mise en œuvre de nouvelles mesures de sécurité du RZMS concernant l'authentification et l'autorisation des modifications demandées et offrir aux opérateurs de TLD la possibilité de tirer parti de ces mesures de sécurité, en particulier l'authentification multi-facteurs (MFA) et les e-mails chiffrés.

Cette recommandation pourra être considérée comme mise en œuvre lorsque l'organisation ICANN et la PTI disposeront d'un RZMS de nouvelle génération qui implique un modèle d'authentification et d'autorisation robuste et sécurisé pour la soumission et l'approbation des demandes, ainsi que des fonctionnalités supplémentaires qui améliorent la sécurité et la stabilité du système DNS global.

Cette recommandation pourra être considérée comme efficace lorsque l'organisation ICANN atténuera le potentiel de problèmes de sécurité et de stabilité qui impliquent l'utilisation abusive du RZMS par le biais de procédures de gestion de l'identité améliorées.

C. Données de la zone racine et registres de l'IANA

Les registres de l'IANA comprennent des paramètres critiques qui sont spécifiés par les RFC dans le Groupe de travail de génie Internet (IETF), le Groupe de travail de la recherche Internet (IRTF) et la filière de soumission indépendante.[123] La disponibilité et l'intégrité de ces registres de paramètres sont primordiales et doivent être clairement informées à la communauté au moyen d'indicateurs clés de performance (KPI) officiels. Actuellement, les indicateurs de la disponibilité des services fournis par l'organisation ICANN ne sont pas accessibles à la communauté. Les parties prenantes ont besoin de cette information pour évaluer les aspects touchant à la sécurité, la stabilité et la résilience de ces services au fil du temps.

L'organisation ICANN peut également trouver la création de KPI pour la zone racine du DNS (y compris les DNSSEC, la disponibilité, l'intégrité, les abus, etc.) comme le moyen le plus efficace de mesurer, suivre et communiquer à la communauté les tendances des données concernant la zone racine.

Des KPI utiles comprennent, entre autres :

- Le délai de propagation des changements de la zone racine vers des instances.
- Zone racine du DNS (y compris les DNSSEC, la disponibilité, l'intégrité, etc.), afin que les tiers puissent suivre les aspects liés à la SSR.
- Mesures démontrant la taille, la croissance et la composition des registres IANA et la disponibilité de ces registres sur le réseau mondial.

Recommandation 22 de la SSR2 : mesures du service

22.1. Pour chaque service qui relève de l'autorité de l'organisation ICANN, y compris les services liés à la zone racine et aux gTLD, ainsi que les registres IANA, l'organisation ICANN devrait créer une liste de statistiques et de mesures qui reflètent l'état opérationnel (comme la disponibilité et la réactivité) de ce service, et publier un répertoire de ces services, ensembles de données et mesures sur une seule page du site Web icann.org, par exemple sous la plateforme de données ouvertes (ODP). L'organisation ICANN devrait produire des mesures pour chacun de ces services sous

[123] IANA, « Procédures d'enregistrement du protocole », 3 janvier 2020, https://www.iana.org/help/protocol-registration.

forme de résumés à la fois au cours de l'année précédente et longitudinalement (pour illustrer le comportement de base).

22.2. L'organisation ICANN devrait demander chaque année des commentaires de la communauté sur les mesures. Cette rétroaction devrait être prise en considération, résumée publiquement après chaque rapport et incorporée dans les rapports de suivi. Les données et les méthodologies associées utilisées pour mesurer les résultats de ces rapports devraient être archivées et rendues publiques afin de favoriser la reproductibilité.

Cette recommandation pourra être considérée comme mise en œuvre lorsque l'organisation ICANN mettra à la disposition de la communauté les mesures du statut opérationnel sur les services de soutien de l'organisation ICANN.

Cette recommandation pourra être considérée comme efficace lorsque la communauté constatera une augmentation de la transparence des opérations de l'organisation ICANN liées à la SSR.

D. Cryptographie du DNS

L'équipe de révision SSR2 a étudié deux volets dans le domaine de la cryptographie du DNS. En premier lieu, l'équipe a étudié la transition de l'algorithme RSA vers un algorithme de courbe elliptique pour les signatures DNSSEC. Deuxièmement, l'équipe a étudié la nécessité de passer à un algorithme de signature numérique post-quantique.[124] Pour rester à jour avec les progrès des technologies informatiques traditionnelles, la taille des clés RSA doit augmenter au fil du temps. Par ailleurs, les DNSSEC pourraient passer de RSA à la cryptographie à courbe elliptique (ECC), qui offre la même sécurité avec des clés publiques plus petites et des signatures plus petites. En outre, il y a une préoccupation que l'invention d'un ordinateur quantique à grande échelle pourrait fracturer à la fois le RSA et l'ECC. Avant qu'un ordinateur quantique à grande échelle ne passe, les DNSSEC doivent passer à un algorithme de sécurité quantique. L'organisation ICANN et la PTI n'ont pas de dispositions dans la déclaration de pratiques DNSSEC (DPS) pour permettre un tel changement.

L'organisation ICANN n'est pas la seule organisation à avoir besoin de tenir compte des progrès attendus dans le domaine de la cryptographie. Les groupes de normalisation de l'industrie se préparent également à un avenir post-quantique. L'activité la plus connue est le projet de cryptographie post-quantique du NIST, qui travaille avec des chercheurs du monde entier pour développer de nouvelles primitives cryptographiques qui ne soient pas susceptibles d'être attaquées par des ordinateurs quantiques.[125] On peut s'attendre à ce que ce projet prenne encore plusieurs années avant que les algorithmes qui en résultent ne soient prêts pour la normalisation, mais il est certainement bien avancé.

Entre-temps, les chercheurs s'accordent à dire que les signatures basées sur le hachage n'ont pas de danger post-quantique. Le Groupe de travail de la recherche Internet (IRTF) a spécifié ces algorithmes de signature dans son Groupe de recherche sur le Forum Crypto (CRFC), en

[124] Consulter l'« annexe G : Cryptographie » pour plus de détails sur les recherches de l'équipe.

[125] Institut national des normes et de la technologie (NIST), Laboratoire des technologies de l'information, Centre de ressources pour la sécurité informatique, « Cryptographie post-quantique », créé le 03 janvier 2017, mis à jour le 23 novembre 2020, https://csrc.nist.gov/projects/post-quantum-cryptography.

utilisant de petites clés privées et publiques à faible coût de calcul.[126] Cependant, les signatures sont assez grandes et une clé privée ne peut produire qu'un nombre limité de signatures. Ces deux propriétés rendent les signatures basées sur le hachage indésirables dans l'environnement des DNSSEC.

La documentation de l'organisation ICANN ne tient pas compte de la nécessité de passer de l'algorithme actuel à un autre. Cela laisse l'organisation ICANN mal préparée pour les progrès attendus dans les algorithmes de signature de clés cryptographiques.

Recommandation 23 de la SSR2 : roulement de l'algorithme

> 23.1. Les opérations de la PTI devraient mettre à jour la déclaration de pratiques DNSSEC (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 à d'autres algorithmes ou à des algorithmes après-quantiques futurs, ce qui créera une sécurité équivalente ou même supérieure et préservera ou améliorera la résilience du DNS.
>
> 23.2. 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.

Cette recommandation pourra être considérée comme mise en œuvre lorsque **la** PTI mettra à jour le DPS pour permettre la transition d'un algorithme de signature numérique à un autre et développera un plan de consensus pour les roulements futurs de l'algorithme DNSKEY de la racine.

Cette recommandation pourra être considérée comme efficace lorsque l'organisation ICANN sera prête à utiliser des algorithmes plus avancés pour la signature des clés, y compris toute augmentation de la longueur des clés et de la durée du transfert des clés.

5. Opérateur de registre de secours (EBERO)

Un fournisseur EBERO sert de composant spécifique d'infrastructure de reprise après sinistre et représente un rôle important dans l'offre de systèmes et de capacités opérationnelles nécessaires pour prendre en charge toutes les fonctions critiques d'un registre gTLD défaillant.

Un fournisseur EBERO est activé temporairement lorsqu'un opérateur de registre TLD risque de ne pas pouvoir assurer les fonctions de registre critiques.[127] Ce processus assure la disponibilité de ces fonctions de l'opérateur de gTLD, protège les titulaires de noms de domaine et fournit une couche supplémentaire de protection au DNS. Comme l'indiquent les diverses normes bien connues telles que la norme ISO 22301, les meilleures pratiques exigent que les

[126] IRTF, Groupe de recherche du Forum Crypto, https://irtf.org/cfrg.

[127] ICANN, « Opérateur de registre de secours », s.d., https://www.icann.org/resources/pages/ebero-2013-04-02-en.

processus DR soient testés régulièrement (voir la Recommandation 7 de la SSR2 : améliorer les processus et procédures de continuité des opérations et de reprise après sinistre).

L'équipe de révision SSR2 n'a pas pu vérifier que l'organisation ICANN ait coordonné les tests de bout en bout nécessaires de l'ensemble du processus EBERO décrit dans le « Manuel du processus de transition commun - version 3 ».[128] L'organisation ICANN et les fournisseurs EBERO ont testé les parties du processus (un test a été réalisé avec .doosan, et un autre test a été réalisé avec .mtpc), le test le plus récent ayant été réalisé en 2017.[129] L'équipe de révision SSR2 a trouvé les résultats de ces tests dans les débats lors de réunions plutôt que sur n'importe quelle page Web dédiée de l'ICANN.[130] L'équipe de révision reconnaît que les détails de la façon dont un processus EBERO de bout en bout est testé ne sont pas inclus dans le cadre d'une révision SSR. Toutefois, il est essentiel de pouvoir vérifier que les tests aient été effectués et en examiner les résultats pour assurer la transparence vis-à-vis de la communauté.

Il convient également de noter que, bien que les processus de l'EBERO soient documentés dans le Manuel du processus de transition commun, ce document a été extrêmement difficile à trouver, car il est intégré au contrat de l'EBERO.

Recommandation 24 de la SSR2 : améliorer la transparence et les tests de bout en bout pour le processus EBERO

24.1. L'organisation ICANN devrait coordonner les tests de bout en bout du processus EBERO complet à des intervalles prédéterminés (au moins une fois par an) en utilisant un plan de test qui inclue des ensembles de données utilisés pour les tests, les états de progression et les délais, et qui soit 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.

24.2. L'organisation ICANN devrait faciliter la recherche du manuel du processus de transition commun en fournissant des liens sur le site Web de l'EBERO.

Cette recommandation pourra être considérée comme mise en œuvre lorsque l'organisation ICANN coordonnera les tests annuels de bout en bout du processus EBERO complet avec la documentation publique pour le résultat.

Cette recommandation pourra être considérée comme efficace lorsque l'organisation ICANN sera en mesure de valider que le processus EBERO fonctionne comme prévu, protégeant les titulaires de noms de domaine et fournissant une couche supplémentaire de protection au DNS.

[128] ICANN, « Contrat de l'opérateur de registre de secours », août 2019 https://www.icann.org/en/system/files/files/cira-ebero-15aug19-en.pdf. Note : consulter l'annexe B - Processus de transition communs.
[129] ICANN, rapport d'exercice EBERO, présentation à la Journée technique de l'ICANN55, 7 mars 2016, https://meetings.icann.org/en/marrakech55/schedule/mon-tech/presentation-ebero-07mar16-en.pdf, et Murphy, Kevin, « Second registre d'urgence testé avec Dead dot-brand », Domain Incite, 27 avril 2017, http://domainincite.com/21724-second-emergency-registry-tested-with-dead-dot-brand.
[130] Arias, Francisco, « Exercices EBERO », présentation à la Journée technique de l'ICANN60, 30 octobre 2017, https://ccnso.icann.org/sites/default/files/field-attached/presentation-ebero-exercises-30oct17-en.pdf.

Annexe A : autres suggestions

Tout au long du processus de révision, la deuxième équipe de révision de la sécurité, la stabilité et la résilience du DNS (SSR2) a noté plusieurs domaines où des changements permettraient d'améliorer l'efficacité et les capacités des futures équipes de révision. Bien que ces éléments ne relèvent pas du mandat de l'équipe de révision, nous espérons que l'organisation ICANN considèrera les suggestions suivantes comme des apports aux révisions futures. Ils sont répertoriés par ordre de priorité.

Suggestion 1

L'organisation ICANN devrait mettre en œuvre une fonction de suivi des progrès en ligne pour chaque recommandation de chaque équipe de révision. En permettant que les progrès accomplis tout au long de la mise en œuvre soient visibles en ligne, l'ensemble de la communauté pourra observer les détails de la mise en œuvre et fournir des commentaires sur les défauts éventuels. Pour atteindre la transparence et la visibilité souhaitées, il est nécessaire que la communauté ait une plus grande granularité concernant les plans de mise en œuvre et les progrès que celle que l'on peut voir sur les pages Web de mise en œuvre de la CCT à présent.[131] L'équipe de révision SSR2 considère que la recommandation 1 ne s'aurait pas avéré nécessaire si une telle fonction avait été en vigueur lors de la mise en œuvre des recommandations de l'équipe de révision SSR1. En outre, pour reprendre le concept d'un responsable de la mise en œuvre de la CCT, l'organisation ICANN devrait fournir des rapports trimestriels aux membres de l'équipe de révision qui a produit les recommandations, leur permettant de partager périodiquement leurs retours sur la question de savoir si la mise en œuvre produit l'effet prévu et éviter les questions de la prochaine équipe de révision lorsqu'elle évaluera la mise en œuvre. L'équipe de révision SSR2 croit que l'évaluation des recommandations de l'équipe de révision SSR1 aurait été plus simple si une telle fonction avait été mise en place avant que l'équipe de révision SSR2 n'ait été réunie.

Suggestion 2

Pour éviter tout malentendu et des attentes non satisfaites, l'organisation ICANN devrait rédiger clairement par écrit le processus d'obtention de ressources sous-traitées pour les équipes de révision, y compris les jalons et les points que l'équipe de révision devrait approuver. Chaque équipe de révision aura besoin d'un rédacteur technique, de sorte que l'organisation ICANN devrait fournir à l'équipe de révision un rédacteur technique dès la toute première réunion de l'équipe.

Suggestion 3

Pour faciliter l'enquête, peu après la fin de la période de consultation publique, et pour « *répondre aux besoins croissants d'inclusion, de responsabilité et de transparence* », comme indiqué par l'objectif stratégique 2.1, l'équipe de révision SSR2 suggère que l'organisation ICANN crée une liste de diffusion par courrier électronique pour divulguer les annonces concernant les périodes de consultation publique. Aujourd'hui, il peut être très difficile de trouver des informations sur les consultations publiques. La mise en œuvre de cette suggestion permettra d'accroître la sensibilisation des abonnés aux listes de diffusion vis-à-vis des

[131] ICANN, « Recommandations approuvées de l'équipe de révision de la concurrence, la confiance et le choix du consommateur (CCT-RT) : plan de mise en œuvre et prochaines étapes », consulté le 19 décembre 2020, https://www.icann.org/public-comments/cct-rt-implementation-plan-2019-09-11-en.

périodes de consultation publique, sans nécessiter d'efforts supplémentaires. L'existence de ces messages permettra aux membres des futures équipes de révision et aux autres parties concernées de trouver de l'information grâce aux outils de recherche facilement disponibles dans les archives de courrier.

L'équipe de révision SSR2 suggère que l'organisation ICANN envoie au moins trois messages par période de consultation publique à cette liste de diffusion. Le premier message devrait être envoyé lors du début de la période de consultation publique et inclure une URL stable vers le document préliminaire pertinent. Le deuxième message devrait être envoyé à la fin de la période de consultation publique et devrait inclure une URL stable à l'ensemble de commentaires soumis. Le troisième message devrait indiquer si un consensus a été atteint et, dans l'affirmative, il devrait inclure une URL stable vers le document final. D'autres messages pourraient également être utiles, tel que la communication d'un prolongement de la période de consultation publique. En outre, l'équipe de révision SSR2 suggère que l'organisation ICANN crée une page Web dédiée à la liste de tous les appels publics à commentaires, qui serait alors liée à la page des documents pertinents.

Suggestion 4

Pour permettre des discussions transparentes sur la sécurité, l'organisation ICANN devrait envisager d'établir une plateforme d'assurance de l'ouverture des informations pour partager les informations de sécurité et d'utilisation malveillante afin de rendre les informations plus fluides et plus rapides à divulguer.

Annexe B : définitions et acronymes

Définitions

Une évaluation de ce type implique de s'accorder sur la définition des termes principaux associés à la révision. Initialement, la deuxième équipe de révision de la sécurité, la stabilité et la résilience du DNS (équipe de révision SSR2) fonctionnait selon les définitions suivantes :[132]

- Abus : Voir « utilisation malveillante du DNS » ci-dessous
- Piratage de la messagerie en entreprise (BEC) : type d'escroquerie visant les entreprises où les comptes de messagerie électronique des employés sont soit usurpés, soit compromis pour effectuer des virements frauduleux.
- Réseau zombie : un réseau d'ordinateurs infectés par des logiciels malveillants et contrôlés en tant que groupe sans la connaissance des propriétaires des ordinateurs.
- Fraude par certificat numérique : un attaquant enfreint une autorité de certification (CA) pour générer et obtenir des certificats frauduleux dans le but de lancer d'autres attaques ; un attaquant peut également utiliser des certificats frauduleux pour s'authentifier en tant qu'autre individu ou système, ou pour fausser des signatures numériques.
- Attaque par déni de service distribué (DDoS) : tentative malveillante de perturber un serveur, un service ou un réseau ciblé en écrasant la cible ou son infrastructure environnante par un flot de trafic Internet provenant de sources multiples (distribuées).
- Utilisation malveillante du DNS : utilisation malveillante intentionnelle des identificateurs universels fournis par le DNS au service de l'infrastructure de la cybercriminalité et pour diriger les utilisateurs vers des sites Web permettant d'autres formes de délits, comme l'exploitation d'enfants, l'atteinte à la propriété intellectuelle et la fraude.
- Système des noms de domaine (DNS) : le DNS est un service de base de données en ligne distribué qui traduit des noms de domaine faciles à mémoriser en adresses numériques de protocole Internet (IP) ; par exemple, le DNS convertit www.icann.org en 192.0.34.65 (spécifié dans les RFC 1034 et 1035).
- Cadre de systèmes identificateurs de la sécurité, la stabilité et la résilience (IS-SSR) : il s'agit d'un document, mis à jour périodiquement, qui décrit le rôle de l'ICANN et les limites de sa mission de soutien à un Internet unique, mondial et interopérable, ainsi que les défis que doivent relever les systèmes d'identificateurs uniques d'Internet ».
- Logiciel malveillant : logiciel spécialement conçu pour perturber, endommager ou obtenir un accès non autorisé à un système informatique.
- Hameçonnage : tentative frauduleuse d'obtenir des informations sensibles en se déguisant en une entité digne de confiance dans une communication électronique.
- Rançonlogiciel : logiciel malveillant conçu pour bloquer l'accès à un système informatique jusqu'à ce qu'une somme d'argent ne soit payée.
- Résilience : capacité du système d'identificateurs de l'Internet à résister, tolérer ou survivre de manière efficace à des attaques malveillantes et à d'autres éléments perturbateurs sans interrompre ou arrêter le service.
- Escroquerie : type de fraude conçue pour ressembler à une vraie activité commerciale ou une occasion d'investissement permettant de gagner de l'argent.
- Sécurité : capacité de protéger et d'empêcher l'usage impropre des identificateurs uniques d'Internet.

[132] ICANN, « Rôle et attributions des SSR », consulté le 27 décembre 2019, https://www.icann.org/resources/pages/ssr-role-remit-2015-01-19-en.

- Menace de sécurité : l'hammeçonnage, l'escroquerie, les logiciels malveillants, les rançonlogiciels, le spam, les attaques DDoS, la fraude par certificat numérique et les réseaux zombies sont parmi les menaces de sécurité les plus critiques.
- Spam : courrier électronique de masse non sollicité.
- Stabilité : capacité à garantir que le système des identificateurs fonctionne comme prévu et à faire en sorte que les utilisateurs des systèmes d'identificateurs uniques y fassent confiance.
- Identificateurs uniques : la mission technique de l'ICANN consiste à aider à coordonner, au niveau global, l'attribution des identificateurs uniques de l'Internet : plus précisément, les noms de domaine de premier niveau, les blocs d'adresses de protocole Internet (IP) et les numéros du système autonome (AS) attribués aux registres Internet régionaux, ainsi que les paramètres de protocole selon les directives de l'IETF.

Acronymes

- AS : système autonome
- BC : continuité des opérations
- CISO : directeur de l'information
- CSO : directeur de la sécurité
- CZDS : service centralisé de données de zone
- DAAR : signalement des cas d'utilisation malveillante des noms de domaine
- DNS : système des noms de domaine
- DNSSEC : extensions de sécurité du système des noms de domaine (tel que spécifié dans les RFC 4033, 4034 et 4035)
- DoH : DNS sur HTTPS
- DoT : DNS sur TLS
- DPS : déclaration de pratiques DNSSEC
- DR : reprise après sinistre
- DURZ : zone racine délibérément invalide
- EBERO : opérateur de registre de secours
- EPDP : processus accéléré d'élaboration de politiques
- FSM : automate avec un nombre fini d'états
- gTLD : domaine générique de premier niveau
- GNSO : Organisation de soutien aux extensions génériques
- HTTP : protocole de transfert hypertexte
- HTTPS : protocole de transfert hypertexte sécurisé
- IANA : Autorité chargée de la gestion de l'adressage sur Internet
- IETF : Groupe de travail de génie Internet
- IMRS : serveur racine géré par l'ICANN
- IP : Protocole Internet
- IRTF : Groupe de travail de la recherche Internet
- Cadre IS-SSR : cadre de systèmes d'identificateurs de la sécurité, la stabilité et la résilience de l'Internet
- ISMS : système de gestion de la sécurité des informations
- ISO : Organisation internationale de normalisation
- ITIL : bibliothèque de l'infrastructure IT
- KSK : clé de signature de clé
- NCAP : projet d'analyse de la collision de noms
- NIST : Institut national des normes et de la technologie
- OCTO : Bureau du directeur de la technologie
- PII : données personnelles identifiables

- PTI : Identificateurs techniques publics
- RDS : service d'annuaire de données d'enregistrement
- RAA : contrat d'accréditation de bureau d'enregistrement
- RAPWG : Groupe de travail sur les politiques en matière d'enregistrements frauduleux
- RDAP : protocole d'accès aux données d'enregistrement des noms de domaine
- RSSAC : Comité consultatif du système des serveurs racine
- SADAG : analyse statistique de l'utilisation malveillante du DNS dans les gTLD
- SMART : spécifique, mesurable, affectable, pertinent et traçable
- SOP : plans stratégiques et opérationnels
- SSAC : Comité consultatif sur la sécurité et la stabilité
- SSAE : déclaration sur les normes relatives aux missions d'attestation
- SSR : sécurité, stabilité et résilience
- SSR1 : premier processus de révision de la SSR
- SSR2 : deuxième processus de révision de la SSR
- TLS : sécurité de la couche transport

Annexe C : processus et méthodologie

Processus et méthodologie pour la révision des recommandations de la SSR1

Le processus d'évaluation de l'équipe de révision SSR2 décrit ci-dessous est basé sur des réunions d'information et des discussions avec le personnel de l'organisation ICANN responsable de la mise en œuvre ; sur la révision systématique d'une quantité importante de documents pertinents de l'ICANN et de rapports de mise en œuvre créés par l'organisation ICANN ; et sur des recherches et des entretiens supplémentaires.[133] L'équipe a également utilisé des séances de sensibilisation lors des réunions publiques de l'ICANN à Barcelone et Kobe pour assurer la liaison avec les parties prenantes pertinentes de la communauté. L'évaluation était à la fois quantitative et qualitative, dans la mesure du possible, selon la recommandation spécifique.

De nombreuses recommandations de la SSR1 étaient de haut niveau et manquaient de spécificité. L'équipe de révision SSR2 n'avait pas le pouvoir d'accéder et d'analyser le fonctionnement interne de l'ICANN et a donc demandé à l'organisation ICANN de fournir ses plans de mise en œuvre et des preuves de la correcte mise en œuvre aux membres de l'équipe de révision SSR2. Les recommandations elles-mêmes et la documentation fournie par l'organisation ICANN manquaient de KPI et de cibles définis, d'objectifs mesurables et de plans de mise en œuvre. Cela rajoutait un défi à la difficulté de mesurer ou de suivre les mises en œuvre. En outre, le libellé de certaines recommandations laisse une marge d'interprétation. Cela a parfois conduit à une compréhension différente de la recommandation de l'équipe SSR2 par rapport à celle utilisée par le personnel de l'organisation ICANN.

Pour chaque recommandation, le personnel de l'organisation ICANN a fourni des réponses initiales sur la mise en œuvre à l'équipe en 2017, en faisant rapport sur la manière dont ils ont mis en œuvre les recommandations de la SSR1. Le personnel de l'ICANN a cité des pages Web ou des documents, organisé des présentations de divers départements au sein de l'organisation ICANN et a également fourni à l'équipe des informations sur les recommandations pendant neuf mois. L'équipe a également examiné un nombre important de documents de référence pertinents à cette révision. L'équipe a mené des entretiens avec le personnel de l'organisation ICANN, a demandé des informations supplémentaires et a utilisé la contribution des parties prenantes concernées et de ses propres recherches pour effectuer d'autres analyses, le cas échéant.

Après avoir reçu des réponses de l'organisation ICANN aux questions soumises et terminé ses recherches et sa diligence raisonnable au meilleur de ses capacités, l'équipe a rédigé des évaluations préliminaires pour chaque recommandation entre la mi-2018 et la fin de l'année. Ces dernières ont été discutées en ligne, lors des appels hebdomadaires de l'équipe et lors de réunions en personne. L'équipe a modifié le texte au besoin et approuvé les conclusions et les constats relatifs à chaque recommandation de la SSR1 en vue de son inclusion dans le rapport préliminaire de l'équipe SSR2, avec les protocoles de consensus approuvés par l'équipe, et en notant les objections des minorités, le cas échéant.

[133] Wiki de l'équipe de révision SSR2 de l'ICANN, https://community.icann.org/display/SSR/SSR2+Review. Voir en particulier les documents de contexte et les documents d'information.

Après avoir discuté en ligne et en téléconférence, et après de multiples itérations, l'équipe a décidé de structurer son évaluation préliminaire selon la méthodologie suivante, qui se concentre sur l'achèvement des tâches, la pertinence et le travail supplémentaire requis :

1. Qu'est-ce qui a été fait pour mettre en œuvre la recommandation ?
2. La recommandation a-t-elle été pleinement mise en œuvre ?
3. La mise en œuvre a-t-elle eu l'effet escompté ?
4. Comment l'évaluation a-t-elle été effectuée ?
5. La recommandation est-elle toujours pertinente aujourd'hui ?
6. Si oui, quel autre travail s'avère-t-il nécessaire ? Si non, pourquoi pas ?

La première question vise ce que l'organisation ICANN a fait pour mettre en œuvre la recommandation. La deuxième question offre l'évaluation de l'équipe vis-à-vis du niveau de mise en œuvre à la « date de mise en œuvre complète » fournie par le personnel. L'équipe a rencontré de nombreuses recommandations qui semblent n'avoir été mises en œuvre que partiellement ou le/les plan/s de mise en œuvre étaient manquants. Dans ces cas, l'équipe a identifié des domaines spécifiques à améliorer. Dans certains cas, il était difficile d'établir des conditions préalables et des objectifs clairs nécessaires à une mise en œuvre réussie en raison de l'absence de plans de mise en œuvre, de documentation et d'indicateurs de performance manquants. La troisième question reprend la question de savoir si et dans quelle mesure la mise en œuvre a eu l'effet escompté. La quatrième question détaille la façon dont l'équipe SSR2 a mené l'évaluation. Les lecteurs peuvent associer chacun des documents et des autres preuves utilisés par l'équipe aux différentes recommandations. Sur la base de la question cinq, l'équipe a également évalué si chaque recommandation était toujours pertinente en 2018. Enfin, l'équipe a ensuite décidé si les circonstances actuelles justifiaient un travail supplémentaire pour mettre en œuvre exactement ou partiellement chaque recommandation, ce qui informerait alors la série de recommandations propres à l'équipe de révision SSR2.

Processus et méthodologie pour les SSR, les SSR du DNS et les défis futurs de l'ICANN

L'équipe de révision SSR2 a mené une série d'entretiens avec le personnel de l'organisation ICANN.[134] Les questions portaient sur l'exhaustivité et l'efficacité des processus de sécurité et sur l'efficacité du cadre de sécurité de l'organisation ICANN.

L'équipe de révision SSR2 s'est organisée autour d'un processus spécifique pour confirmer les conclusions et élaborer des recommandations pour leur examen par l'ICANN, notamment :

- Examiner, analyser et résumer la documentation pertinente.
- Mener des enquêtes dans les domaines de préoccupation identifiés.
- Mener des entretiens pertinents, le cas échéant.
- Rédiger un résumé des fondements, des constats et des recommandations.

La piste de travail 2 s'est concentrée sur les questions liées à la SSR de l'organisation ICANN elle-même, tandis que la piste de travail 3 s'est concentrée sur la SSR des systèmes d'identificateurs mondiaux : le DNS global, les bases de données de numéros de l'IANA (allocations d'IP et d'ASN) et les registres de protocole IANA. L'équipe de révision a

[134] Wiki de l'équipe de révision SSR2 de l'ICANN, https://community.icann.org/display/SSR/SSR2+Review. Voir en particulier les documents d'information.

spécifiquement examiné des rapports et d'autres données sur les risques, les menaces et l'utilisation malveillante du DNS, puis a mis en rapport les données résultantes avec les composantes, procédures et politiques pertinentes de l'ICANN.
Au sein de la piste de travail 4 concernant les défis futurs pour la SSR, l'équipe de révision SSR2 a examiné les recherches actuelles sur l'utilisation malveillante du DNS, l'impact de l'évolution continue des types et du volume de dispositifs connectés au DNS, les technologies émergentes, les domaines de préoccupation identifiés dans d'autres pistes de travail qui pourraient avoir des implications futures et les méthodologies institutionnelles de l'ICANN pour l'analyse et l'atténuation des menaces.
L'équipe de révision SSR2 a reconnu que cette piste de travail dépendait des thèmes émergents des autres secteurs dépendants. Plus précisément, en plus des défis généralement identifiés, la stabilité et la résilience du DNS pourrait être confrontée à d'autres défis spécifiques de la piste de travail en matière de la SSR de l'ICANN et du DNS.

Annexe D : conclusions relatives aux recommandations de la SSR1

Cette section comprend une évaluation détaillée de chacune des recommandations de la SSR1. Les constats présentés ici traitent des mises en œuvre spécifiques, de leurs problèmes et des idées de l'équipe pour poursuivre le travail. L'équipe de révision SSR2 a noté les questions suivantes qui réapparaissent :

1. Il y a un manque d'indicateurs, de mesures et de jalons qui permettraient à la communauté et à l'organisation ICANN de suivre et de comprendre l'espace de sécurité et leurs propres activités.

2. Il y a un manque de preuves, de définitions et de procédures accessibles au public, ce qui entrave l'observation des activités liées à la SSR et conduit à un manque de clarté quant à ce qui est fait, quand, par qui et comment.

3. La communauté manque d'opportunités de révision et de responsabilité, ce qui l'empêche de formuler des commentaires sur les questions liées à la SSR.

4. L'organisation ICANN ne dispose actuellement pas d'une stratégie globale, d'objectifs identifiables ou d'une politique claire et complète en matière de sécurité, stabilité et résilience. Sans une stratégie SSR fonctionnelle et une gestion intégrée de la sécurité et des risques (par exemple, politique, procédures, normes, références, lignes directrices), les responsabilités liées à la SSR ne sont pas attribuées, mesurées et suivies, ce qui entraîne un manque de transparence et de responsabilité.

Recommandation 1 de la SSR1

« L'ICANN devrait publier une déclaration unique, claire et cohérente concernant ses attributions et sa mission technique limitée en matière de SSR. L'ICANN devrait encourager et obtenir l'avis du public afin de parvenir à une déclaration consensuelle ».

Conclusion de la SSR2 : cette recommandation reste pertinente puisqu'elle a été partiellement mise en œuvre, mais n'a pas pleinement atteint l'effet escompté d'avoir une déclaration consensuelle, claire et cohérente décrivant les attributions de l'organisation ICANN en matière de SSR et sa mission technique.

Fondements :

- L'équipe a observé qu'il existe une déclaration et que l'organisation ICANN a mis à jour (mais ne maintient plus) cette déclaration à la suite de sa révision par la communauté.[135] Malgré l'existence de cette déclaration et ses définitions claires de « sécurité, stabilité et résilience », l'utilisation de ces définitions reste incohérente. Les conversations parallèles avec les membres de l'équipe qui ont accès au texte des contrats de l'organisation ICANN

[135] Rôle et attributions de la SSR, https://www.icann.org/resources/pages/ssr-role-remit-2015-01-19-en, et « Sécurité, stabilité et résilience de l'équipe de révision du DNS – Rapport préliminaire : rapport des commentaires publics », modifié le 18 mai 2012, http://www.icann.org/en/system/files/files/report-comments-ssr-rt-draft-report-18may12-en.pdf.

avec diverses parties contractantes ont indiqué que les définitions de « sécurité » et de « stabilité » utilisées dans les contrats de l'organisation ICANN avec les parties contractantes varient.[136]
- Aucune mesure n'a été fournie pour évaluer si la mise en œuvre avait pour effet de fournir des informations claires et cohérentes sur ses attributions SSR et les limites de sa mission technique. Au vu des différents sens attribués au terme « SSR » à l'ICANN, il n'a pas été possible d'adopter une définition commune, comme prévu par l'équipe de révision SSR1.

Recommandation 2 de la SSR1

« La définition et la mise en œuvre des attributions de l'ICANN et de sa mission technique limitée en matière de SSR devrait être révisée afin de garder le consensus et obtenir l'avis de la communauté. Le processus devrait se répéter de façon régulière, peut-être de manière conjointe avec le cycle des futures révisions de la SSR ».

Conclusion de la SSR2 : cette recommandation reste pertinente et n'a pas été pleinement mise en œuvre. L'effet prévu d'un processus de révision publique régulière pour les attributions SSR de l'organisation ICANN et la mission technique y associée n'a pas été accompli.

Fondements :
- L'équipe de révision SSR2 n'a pas trouvé de preuve que des révisions régulières de la mission SSR aient eu lieu. Il n'y a pas eu d'occasion de commenter spécifiquement le mandat et l'énoncé de la mission depuis 2013.

Recommandation 3 de la SSR1

« Après avoir publié une déclaration consensuelle sur ses attributions et sa mission technique limitée en matière de SSR, l'ICANN devrait utiliser une terminologie cohérente et inclure des descriptions de cette déclaration dans tous ses documents ».

Conclusion de la SSR2 : cette recommandation reste pertinente mais n'a pas été pleinement mise en œuvre. L'objectif de travailler à partir d'une terminologie et d'un ensemble de descriptions cohérents pour les documents relatifs à la SSR n'a pas été atteint.

Voir la Recommandation 13 de la SSR2 : accroître la transparence et la responsabilité en matière de signalement des plaintes pour utilisation abusive suivant la recommandation de la SSR2 qui s'ajoute à la recommandation originale de la SSR1.

Fondements :
- Un blog datant de juillet 2013 répertorie la terminologie que l'organisation ICANN utilise pour parler de la sécurité et qui est disponible pour la communauté ; cependant, ces définitions ne semblent pas être intégrées de manière cohérente dans d'autres documents liés à la SSR.[137]
- Le rapport du personnel de l'organisation ICANN sur cette recommandation semble indiquer que le personnel ajoute constamment des termes clés au glossaire public de l'organisation

[136] Consulter également la section 7.3 du contrat de base des nouveaux gTLD https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.html par rapport aux définitions de la sécurité et la stabilité de l'organisation ICANN https://www.icann.org/groups/ssac

[137] ICANN, « Terminologie de sécurité de l'ICANN », blog, modifié pour la dernière fois le 8 juillet 2013, https://www.icann.org/news/blog/icann-s-security-terminology.

ICANN dans le cadre du Plan stratégique et opérationnel (SOP) ; à mesure que les activités liées à la SSR évoluent, la terminologie et les descriptions seront mises à jour dans le cadre du SOP. Toutefois, le glossaire (disponible dans le blog évoqué ci-dessus) n'a pas été mis à jour depuis février 2014.

Recommandation 4 de la SSR1

« L'ICANN devrait documenter et définir clairement la nature des relations en matière de SSR au sein de la communauté de l'ICANN afin de fournir une référence qui puisse contribuer à une meilleure compréhension des interdépendances entre les organisations ».

Conclusion de la SSR2 : cette recommandation reste pertinente mais n'a pas été pleinement mise en œuvre. L'objectif de fournir une ressource ouverte et transparente qui décrive les relations de l'organisation ICANN en matière de SSR n'a pas été atteint.

Voir la Recommandation 2 de la SSR2 : désigner un cadre responsable de la sécurité stratégique et tactique et de la gestion des risques pour la recommandation de la SSR2 qui s'ajoute à la recommandation originale de la SSR1.

Fondements :

- Le personnel de l'organisation ICANN a créé un document adressé à l'équipe de révision SSR2 présentant les rôles et les responsabilités de l'ICANN en matière de SSR et répertoriant toutes les organisations avec lesquelles l'organisation ICANN a jamais eu une relation formelle.138 Le document contient des références spécifiques aux documents qui sous-tendent chacune de ces relations, ainsi qu'une description de la dimension SSR de ces relations. Cependant, bon nombre des références répertoriées dans ce document ne sont pas disponibles en ligne. Le document montre souvent que les composantes SSR des relations sont « inconnues ».

Recommandation 5 de la SSR1

« L'ICANN devrait utiliser la définition de ses relations en matière de sécurité, stabilité et résilience afin de maintenir des arrangements de travail efficaces et de démontrer la manière dont ces relations sont utilisées pour atteindre chacun des objectifs en matière de SSR ».

Conclusion de la SSR2 : cette recommandation reste pertinente mais n'a pas été pleinement mise en œuvre. L'équipe de révision n'a pas pu déterminer si l'organisation ICANN a atteint l'objectif d'adopter des méthodes de travail efficaces à l'appui de chacun des objectifs en matière de SSR.

Voir la Recommandation 3 de la SSR2 : améliorer la transparence budgétaire liée à la SSR pour la recommandation de la SSR2 qui s'ajoute à la recommandation originale de la SSR1.

Fondements :

[138] « Relations SSR », ICANN, 23 janvier 2017, https://www.icann.org/en/system/files/files/ssr-relationships-fy17-23jan17-en.pdf.

- L'équipe s'attendait à ce que le cadre IS-SSR inclue des informations sur la façon dont les relations clés prévues dans la recommandation 4 de la SSR1 sont utilisées pour atteindre les objectifs de la SSR ; toutefois, ces informations ne sont pas facilement disponibles.[139]
- L'équipe SSR2 n'avait pas suffisamment d'informations pour évaluer si les relations de travail sont fonctionnelles.

Recommandation 6 de la SSR1

« L'ICANN devrait publier un document où soient clairement établis les rôles et les responsabilités du SSAC et du RSSAC afin de bien encadrer les activités des deux groupes. Pour ce faire, L'ICANN devrait chercher à obtenir un consensus auprès des deux groupes, tout en reconnaissant l'histoire et les circonstances autour de leur constitution. L'ICANN devrait envisager la mise en place d'une gestion appropriée des ressources pour les deux groupes, cohérente avec les exigences qui lui sont imposées ».

Conclusion de la SSR2 : cette recommandation reste pertinente mais n'a pas été mise en œuvre. L'organisation ICANN n'a pas atteint l'objectif prévu de rendre les rôles du SSAC et du RSSAC clairs pour toutes les parties intéressées.

Fondements :

- Les rôles et responsabilités du SSAC et du RSSAC sont consignés dans un document.[140] Cependant, ce document public est toujours marqué comme « VERSION PRÉLIMINAIRE EN COURS DE RÉVISION ». Il semble que les travaux ont commencé sur cette recommandation, mais qu'ils ont pris fin sans refléter les révisions organisationnelles du SSAC et du RSSAC. Si un consensus a été atteint, l'équipe de révision SSR2 n'a pas pu trouver le document final.
- Le document se fonde sur les statuts constitutifs de l'ICANN avant la transition de l'IANA. Les parties des statuts qui décrivent le SSAC et le RSSAC sont en grande partie les mêmes, mais le RSSAC est maintenant explicitement chargé de répondre « aux demandes de renseignements ou aux opinions du Conseil d'administration ». La mise à jour n'a pas permis de résoudre le risque de chevauchement des rôles et des responsabilités entre le SSAC et le RSSAC dans les statuts de l'ICANN :

  > *« La mission du SSAC est de conseiller la communauté et le Conseil d'administration de l'ICANN sur des questions liées à la sécurité et à l'intégrité des systèmes de nommage et d'allocation d'adresses Internet ;*
  >
  > *Le RSSAC a pour fonction de conseiller la communauté et le Conseil d'administration de l'ICANN sur des questions liées au fonctionnement, à la gestion, à la sécurité et à l'intégrité du système des serveurs racine de l'Internet ».*

Recommandation 7 de la SSR1

« Sur la base de son cadre SSR actuel, l'ICANN devrait établir un ensemble clair d'objectifs, et conformément à ceux-ci établir les priorités pour ses initiatives et ses activités.

[139] Ibid.

[140] ICANN, « VERSION PRÉLIMINAIRE EN COURS DE RÉVISION : les rôles et les responsabilités du Comité consultatif sur la sécurité et la stabilité de l'ICANN et du Comité consultatif sur le système des serveurs racine », 5 mars 2015, https://www.icann.org/en/system/files/files/draft-rssac-ssac-roles-responsibilities-05mar15-en.pdf.

Conclusion de la SSR2 : la recommandation reste pertinente et a été partiellement mise en œuvre. L'objectif d'avoir des objectifs SSR clairs et révisés publiquement et l'effort d'établissement des priorités y associé n'a pas été atteint.

Voir la Recommandation 2 de la SSR2 : désigner un cadre responsable de la sécurité stratégique et tactique et de la gestion des risques, et la Recommandation 3 de la SSR2 : Améliorer la transparence budgétaire liée à la SSR pour les recommandations de la SSR2 qui s'ajoutent à la recommandation originale de la SSR1.

Fondements :

- Les activités liées à la SSR sont régulièrement présentées dans le cadre des plans stratégiques et opérationnels (SOP), y compris dans les rapports réguliers de gestion de portefeuille de l'ICANN et ses rapports trimestriels sur la SSR.[141] Les SOP ont été informés par le cadre IS-SSR, qui comprenait les priorités, les objectifs et les activités en matière de SSR. Ce cadre n'est cependant plus produit, laissant un vide concernant la façon dont le SOP prend en compte les actions liées à la SSR. Le processus de mise à jour des documents relatifs à la SSR n'est pas clair depuis la dernière publication du cadre IS-SSR en 2016.[142]
- Le cadre IS-SSR offrait à la communauté l'occasion d'éclairer la stratégie en matière de SSR. L'organisation ICANN ne produit plus ce cadre, ce qui implique un manque d'opportunités pour recueillir les commentaires de la communauté de l'ensemble des groupes de parties prenantes de l'ICANN sur la façon dont l'organisation ICANN aborde les activités en matière de SSR.
- La planification stratégique des questions de sécurité, de stabilité et de résilience semble être centrée sur le bureau du directeur de la technologie (OCTO) et, compte tenu de l'existence du SOP, l'équipe de révision a reconnu qu'il existe un niveau de planification pour les activités liées à la SSR au sein de l'OCTO. Toutefois, le niveau de détail et de planification prévu dans la recommandation ne comprend pas de discussions publiques de la même manière entre toutes les parties prenantes de l'organisation ICANN.

Recommandation 8 de la SSR1

« L'ICANN devrait continuer à peaufiner les objectifs de son plan stratégique, notamment l'objectif de maintenir et de gérer la disponibilité du DNS. Alignement clair entre le cadre et le plan stratégique ».

Conclusion de la SSR2 : bien que cette recommandation demeure pertinente aujourd'hui et ait été partiellement mise en œuvre, la mise en œuvre de cette recommandation n'a pas eu l'effet escompté de fournir un lien plus clair entre la stratégie relative à la SSR et le travail opérationnel.

Voir la Recommandation 2 de la SSR2 : désigner un cadre responsable de la sécurité stratégique et tactique et de la gestion des risques, et la Recommandation 3 de la SSR2 :

[141] ICANN, « Plan stratégique de l'ICANN pour les exercices 2021 à 2025 », s.d., https://www.icann.org/en/system/files/files/strategic-plan-2021-2025-24jun19-en.pdf, et Dave Piscitello, « Rapport des activités des systèmes d'identificateurs dans le domaine de la SSR », blog de l'ICANN, modifié pour la dernière fois le 21 janvier 2015, https://www.icann.org/news/blog/identifier-systems-ssr-activities-reporting-en.

[142] ICANN, cadre IS-SSR – Exercices fiscaux 2015 et 2016, https://www.icann.org/en/system/files/files/ssr-framework-fy15-16-30sep16-en.pdf.

Améliorer la transparence budgétaire liée à la SSR pour les recommandations de la SSR2 qui s'ajoutent à la recommandation originale de la SSR1.

Fondements :

- Les documents disponibles sur la page d'accueil de la mise en œuvre de la révision SSR1 indiquent que les directives portant sur la SSR sont incluses et traitées dans les rapports, les stratégies et les procédures pertinents.[143] Toutefois, les rapports disponibles ne fournissent pas suffisamment d'informations sur les activités de la SSR et manquent de détails quant à la mise en œuvre et à l'exécution des activités liées à la SSR.
- Le SOP n'indique pas quelles activités, priorités et dépenses du SOP sont liées à la SSR. Il est essentiel de signaler que les mécanismes envisagés par la SSR1 ont été remplacés par d'autres outils organisationnels et procéduraux, ce qui complique à la fois l'évaluation et la mise en œuvre.

Recommandation 9 de la SSR1

« L'ICANN devrait évaluer les options de certification des normes internationales normalement acceptées (par ex. ITIL, ISO et SAS-70) pour ses responsabilités opérationnelles. L'ICANN devrait publier une feuille de route claire vers la certification ».

Conclusion de la SSR2 : cette recommandation reste pertinente. L'équipe de révision SSR2 n'a pas pu déterminer si cette recommandation a été pleinement mise en œuvre et a eu l'effet prévu, car la recommandation initiale n'avait pas la spécificité nécessaire concernant la certification ou les certifications que devrait cibler l'organisation ICANN, ni quels sont les objectifs poursuivis.

Voir la Recommandation 4 de la SSR2 : améliorer les processus et les procédures de gestion des risques et la Recommandation 5 de la SSR2 : se conformer aux certifications appropriées en matière de sécurité et des systèmes de gestion de la sécurité des informations pour les recommandations de la SSR2 qui s'ajoutent à la recommandation originale de la SSR1.

Fondements :

- Suivant des entretiens avec le personnel de l'organisation ICANN, l'organisation ICANN a poursuivi certaines certifications axées sur l'IANA, par exemple, la certification SOC2/3 du système KSK de la zone racine, la certification SOC2 pour les systèmes d'attribution et d'entretien du registre et SysTrust pour la mise en œuvre des DNSSEC au niveau de la racine.144 En dehors des fonctions IANA, l'organisation ICANN génère des rapports de TI et de cybersécurité à l'aide de cadres d'amélioration continue, dispose d'un audit financier annuel, effectue annuellement une auto-évaluation et une évaluation de la documentation suivant les normes de l'EFQM et obtient des conseils professionnels pour aider à mesurer les performances et favoriser l'amélioration.145
- L'organisation ICANN signale également que tous les membres du personnel de sécurité des informations sont formés à l'aide des offres SANS.146

[143] Page d'accueil de la mise en œuvre de la révision SSR1, wiki, dernière mise à jour le 22 août 2017, https://community.icann.org/display/SSR/SSR1+Review+Implementation+Home.
[144] Voir le document de travail « Questions et réponses de la SSR2 », s.d., 6, https://community.icann.org/pages/viewpage.action?pageId=64076120.
[145] Ibid., 24.
[146] Ibid., 11.

- L'organisation ICANN signale que les résultats des audits internes sont communiqués uniquement au Conseil d'administration de l'ICANN.147
- L'équipe de révision SSR2 n'a pas pu trouver de documents pouvant servir de feuille de route pour la certification du processus SSR, ce qui rend impossible la révision communautaire.

Recommandation 10 de la SSR1

« L'ICANN devrait poursuivre ses efforts visant à assurer le respect de la conformité contractuelle et fournir des ressources adéquates pour remplir cette fonction. L'ICANN devrait également élaborer et mettre en place un processus plus structuré de suivi des dossiers et des recherches en matière de conformité ».

Conclusion de la SSR2 : cette recommandation reste pertinente et n'a pas été pleinement mise en œuvre. L'effet prévu d'avoir des ressources adéquates à appliquer pour faire valoir l'application de la conformité contractuelle et développer un processus structuré permanent de surveillance de la conformité n'a pas été atteint.

Voir la Recommandation 8 de la SSR2 : permettre et démontrer la représentation de l'intérêt public dans les négociations avec les parties contractantes, et la Recommandation 9 de la SSR2 : surveiller et appliquer la conformité dans le cas des recommandations de la SSR2 qui s'ajoutent à une recommandation originale de la SSR1.

Fondements :

- L'évaluation est basée sur des informations accessibles au public (par exemple, la page « Rapports de conformité contractuelle ») ainsi que sur un rapport du personnel de l'ICANN qui fournissait des preuves concernant la mise en œuvre de la recommandation.[148] Le rapport publique régulier des activités de conformité fait partie du plan stratégique et opérationnel (SOP) de l'organisation ICANN. L'organisation ICANN dispose d'une page publique dédiée aux rapports de conformité contractuelle, comprenant des données mensuelles, trimestrielles et annuelles, dix rapports différents pouvant être demandés sur une période de 13 mois, ainsi que des mesures et des données explicitement demandées par différents groupes de travail. Certains programmes contractuels de vérification de la conformité et de sensibilisation sont désormais en place. L'organisation ICANN a créé de nouveaux postes après la révision SSR1 afin d'assurer la réalisation des buts et des objectifs dans ce domaine.
- Les mécanismes de plainte ont été mis à jour en migrant au site Web de l'organisation ICANN, en automatisant et en lançant un outil de réclamation en masse. En outre, le personnel de l'ICANN a indiqué qu'une enquête Pulse avait été menée.[149] L'organisation ICANN a lancé un contrôle de qualité pour les inexactitudes dans les données RDS. Les rapports concernant l'exactitude du RDS existent depuis que l'équipe de révision du WHOIS de 2012 a recommandé leur création.

---

147 Ibid., 6.

148 Le rapport de mise en œuvre de la SSR1 est disponible à l'adresse https://community.icann.org/download/attachments/54691765/SSR%20Recs%201-28.pdf?api=v2 (diapositives 28 à 30) et le briefing de l'équipe de révision SSR2 sur cette recommandation est disponible à l'adresse https://community.icann.org/download/attachments/66085372/SSR1%20Compliance%20Briefing%20June%202017%20v3.pdf?version=2&modificationDate=1499814488000&api=v2.

149 Voir « Mise en œuvre de la recommandation 10 de la SSR » dans le Rapport consolidé sur la mise en œuvre de la SSR1, https://community.icann.org/download/attachments/54691765/SSR%20Recs%201-28.pdf?api=v2.

- Les rapports d'application de la conformité pour 2017 et 2016 contiennent peu de preuves des mesures d'application de la SSR, malgré le nouveau modèle de contrat de registre gTLD (juillet 2017) qui contient des obligations spécifiques sur les parties contractantes en matière de sécurité et de stabilité, et qui peut aider à poursuivre la mise en œuvre.150 Il n'est pas clair pour l'équipe de révision SSR2 en quoi l'objectif de l'organisation ICANN de réduire l'incidence et l'impact de l'utilisation malveillante des enregistrements et des comportements malveillants est lié aux actions de conformité ou à d'autres initiatives. La plupart des questions du rapport de mise en œuvre de la SSR1 du personnel mettent en lumière des questions relatives au WHOIS. En outre, le contrat d'accréditation de bureau d'enregistrement (RAA 2013) contient des droits d'application vagues pour l'organisation ICANN en relation avec les bureaux d'enregistrement dont les activités mettent en danger les services des bureaux d'enregistrement et des opérateurs de registre, le DNS, ou l'Internet.
- L'organisation ICANN produit des rapports mensuels sur son travail d'application de la conformité, mais il n'est pas clair dans quelle mesure la dimension de la SSR est abordée dans le cadre du processus de conformité.151

Recommandation 11 de la SSR1

« L'ICANN devrait définir et mettre en place des actions visant à mesurer le succès des nouveaux gTLD et des procédures accélérées IDN qui soient expressément en rapport avec les objectifs en matière de SSR, y compris des mesures de l'efficacité des mécanismes destinés à atténuer l'utilisation malveillante des noms de domaine ».

Conclusion de la SSR2 : cette recommandation reste pertinente mais n'est pas mesurable. Bien que des mesures aient été prises pour atténuer l'utilisation malveillante des noms de domaine, il n'a pas été possible de déterminer si ou dans quelle mesure cela ait une incidence sur l'atténuation de l'utilisation malveillante des noms de domaine.

Le paysage DNS a changé depuis que la première équipe de révision SSR a formulé ses recommandations à la suite de l'expansion des nouveaux gTLD, en particulier. Toutefois, la recommandation d'intégrer les considérations SSR comme mesure clé du succès dans la gestion de l'espace DNS reste tout aussi pertinente, sinon plus, aujourd'hui qu'en 2011.

Voir la Recommandation 8 de la SSR2 : permettre et démontrer la représentation de l'intérêt public dans les négociations avec les parties contractantes, et la Recommandation 12 de la SSR2 : réviser les efforts d'analyse et de rapport de l'utilisation malveillante du DNS pour permettre la transparence et la révision indépendante, et la Recommandation 13 de la SSR2 : accroître la transparence et la responsabilité en matière de signalement des plaintes pour utilisation malveillante, dans le cas des recommandations de la SSR2 qui s'ajoutent à la recommandation originale de la SSR1.

Fondements :
- L'équipe de révision SSR2 n'a pas pu trouver de document décrivant les mesures de réussite, y compris les mesures de l'efficacité des mécanismes visant à atténuer l'utilisation malveillante des noms de domaine, qui fait l'objet d'un consensus communautaire. Ce

[150] ICANN, 31 juillet 2017, https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf.
[151] Voir les rapports de l'ICANN sur la « Mesure des performances de la conformité contractuelle », https://features.icann.org/compliance/dashboard/report-list.

manque de critères mesurables a également été noté dans le récent rapport et les recommandations de la CCT.[152]

- La spécification 11 du nouveau contrat de registre contient des obligations substantielles pour les registres en matière de SSR, y compris l'obligation d'effectuer périodiquement des analyses techniques et de tenir à jour des rapports statistiques pour évaluer si les domaines des TLD sont utilisés pour perpétrer des menaces de sécurité, telles que le dévoiement, l'hameçonnage, les logiciels malveillants et les réseaux zombies. Ces obligations exactes font partie du contrat de registre des nouveaux gTLD depuis l'ouverture des candidatures en 2012. L'organisation ICANN dispose d'un graphique de conformité, mais mesure le nombre de plaintes et les catégories.[153] Cela reste difficile à suivre étant donné que ses rapports sont répartis sur plusieurs pages.

Recommandation 12 de la SSR1

« L'ICANN devrait travailler avec la communauté afin d'identifier les meilleures pratiques en matière de SSR et de donner son soutien à ces pratiques par le biais de contrats, d'accords, de protocoles d'accord (MOU) et d'autres mécanismes ».

Conclusion de la SSR2 : la recommandation 12 de la SSR1 n'a pas été pleinement mise en œuvre et reste particulièrement pertinente aujourd'hui. L'objectif de définir et mettre en œuvre des meilleures pratiques en matière de SSR n'a pas été atteint.

Voir la Recommandation 8 de la SSR2 : permettre et démontrer la représentation de l'intérêt public dans les négociations avec les parties contractantes, et la Recommandation 9 de la SSR2 : surveiller et appliquer la conformité dans le cas des recommandations de la SSR2 qui s'ajoutent à une recommandation originale de la SSR1.

Fondements :

- La Spécification 11 du nouveau contrat de registre (RA) contient des obligations importantes en matière de SSR qui s'imposent aux opérateurs de registre. Les obligations de ce RA font partie du contrat de registre des nouveaux gTLD ordinaire depuis l'acceptation des candidatures en 2012. Cependant, l'organisation ICANN n'a apparemment pas utilisé ces dispositions comme base de référence pour évaluer leur efficacité dans la réalisation des objectifs de la recommandation 12 de la SSR1.
- Le rapport intitulé « Méthodologie d'atténuation des attaques du système d'identificateurs » est daté de février 2017. Le document présente des suggestions qui auraient été générées « *au sein de l'ICANN et par les experts de la communauté en matière de sécurité du système d'identificateurs* ».[154] Toutefois, il n'est pas clair quel processus a été suivi pour arriver aux meilleures pratiques énoncées dans le document. Rien dans le document de référence ne fait preuve d'aucune intégration de ces meilleures pratiques dans les contrats dans lesquels s'engage l'organisation ICANN. Le rapport ne contient aucune preuve de travail avant 2017.

[152] Rapport de la CCT, 9, https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf.

[153] Voir les « Rapports sur les performances de conformité contractuelle de l'ICANN », https://features.icann.org/compliance et les rapports sur la « Mesure des performances de conformité contractuelle », https://features.icann.org/compliance/dashboard/report-list.

[154] Phifer, Lisa et David Piscitello, « Méthodologie d'atténuation des attaques au système d'identificateurs », livre blanc de l'ICANN, 13 février 2017, https://www.icann.org/en/system/files/files/identifier-system-attack-mitigation-methodology-13feb17-en.pdf.

- Le rapport sur la méthodologie d'atténuation des attaques au système d'identificateurs présente une liste non exhaustive des attaques contre le système d'identificateurs. Bien qu'il y ait eu des accords, des renouvellements, des spécifications et des protocoles d'accord depuis février 2017, rien dans ce document n'a jamais été inclus dans les contrats avec les parties contractantes.
- La page de localisation des ressources de sensibilisation à la sécurité de l'ICANN n'a pas été mise à jour depuis 2014.[155]
- La révision SSR2 n'a trouvé aucune preuve que le personnel informe périodiquement les SO et AC des meilleures pratiques ou les invite à identifier d'autres meilleures pratiques.
- Le rapport du personnel sur cette recommandation de la SSR1 indique que le travail de publication de recommandations pour la protection des applications Web et le développement de ressources de sensibilisation à la sécurité avec le Groupe de travail anti-hameçonnage (APWG) du Comité consacré à la politique Internet est terminé. Il y avait un document consultatif de l'APWG sur « Que faire si votre site Web a été piraté par des spécialistes en hameçonnage », mais il a été publié avant la SSR1. Bien qu'il y ait un rapport du 4e Symposium mondial sur la stabilité, la sécurité et la résilience du DNS tenu à Porto Rico en 2012, le site Web de l'ICANN ne semble pas avoir un ensemble de recommandations pour la protection des applications Web et le développement de ressources pour la sensibilisation à la sécurité.[156]

Recommandation 13 de la SSR1

« L'ICANN devrait encourager toutes les organisations de soutien à élaborer et à publier des meilleures pratiques en matière de SSR pour leurs membres ».

Conclusion de la SSR2 : cette recommandation reste pertinente mais n'a pas été mise en œuvre. L'effet prévu d'instaurer un processus régulier permettant aux organisations de soutien (SO) de publier leurs meilleures pratiques liées à la SSR pour leurs membres n'a pas été atteint.

Voir la Recommandation 8 de la SSR2 : permettre et démontrer la représentation de l'intérêt public dans les négociations avec les parties contractantes, et la Recommandation 9 de la SSR2 : surveiller et appliquer la conformité dans le cas des recommandations de la SSR2 qui s'ajoutent à une recommandation originale de la SSR1.

Fondements :

- L'organisation ICANN considère que le travail sur cette recommandation est permanent et signale que, dans le cadre du SOP, le personnel de l'ICANN contacte toutes les SO et AC pour encourager l'identification et la publication d'une page de référentiel des meilleures pratiques. L'organisation ICANN signale en outre que, dans le cadre du SOP, son personnel s'engage dans une variété d'activités en cours pour encourager l'utilisation mondiale des meilleures pratiques en matière de SSR. L'équipe de révision SSR2 n'a pas pu trouver de preuve que l'organisation ICANN ait mené cette sensibilisation, ni de preuve que les SO aient publié des directives des meilleures pratiques liées à la SSR pour leurs membres.
- Le personnel de l'organisation ICANN a indiqué qu'il n'était pas au courant des mesures récentes qui ont été prises pour encourager les SO et les AC à produire et à publier des

[155] Localisateur des ressources de sensibilisation à la sécurité de l'ICANN, dernière mise à jour le 8 août 2014, https://www.icann.org/resources/pages/security-awareness-resource-2014-12-04-en.

[156] « Stabilité, sécurité et résilience du DNS », rapport de réunion du 4e Symposium mondial, ICANN et APWG, 25 octobre 2012, https://www.icann.org/en/system/files/files/dns-symposium-25oct12-en.pdf.

référentiels de meilleures pratiques pour les informations relatives à la SSR, déclarant que « *il est probable qu'il n'existe pas de publication d'informations relatives à la SSR par une organisation de soutien depuis les informations publiées sur le site des ccTLD en 2012 ».*[157] De plus, le personnel a indiqué que seule la ccNSO publie actuellement les meilleures pratiques en matière de SSR pour ses membres.

Recommandation 14 de la SSR1

« L'ICANN devrait veiller à ce que ses activités de communication en matière de SSR ne cessent d'évoluer afin qu'elles restent à tout moment opportunes, pertinentes et appropriées ».

Conclusion de la SSR2 : cette recommandation reste pertinente mais n'a pas été mise en œuvre et n'a donc pas atteint son effet prévu d'améliorer la rapidité, l'intérêt et la pertinence des activités de sensibilisation de l'ICANN liées à la SSR.

Voir la Recommandation 18 de la SSR2 : informer les débats de politique pour les recommandations de la SSR2 qui s'ajoutent à une recommandation originale de la SSR1.

Fondements :

- L'interface de participation n'a pas pris en compte directement la façon dont les activités de sensibilisation « évoluent » pour rester pertinentes.[158] La mise en œuvre s'est plutôt concentrée sur le signalement de ce qui est fait à un moment donné. Comme l'accent n'est pas mis sur l'évolution des activités, la recommandation n'a pas été mise en œuvre.

Recommandation 15 de la SSR1

« L'ICANN devrait agir en tant que facilitateur pour la divulgation et la diffusion des menaces à la sécurité du DNS et des techniques d'atténuation des risques ».

Conclusion de la SSR2 : cette recommandation reste pertinente et n'a pas été pleinement mise en œuvre. Bien qu'il existe un processus « sur les papiers », il n'est pas possible d'évaluer si ce processus est fonctionnel et efficace.

Voir la Recommandation 8 de la SSR2 : permettre et démontrer la représentation de l'intérêt public dans les négociations avec les parties contractantes, et la Recommandation 12 de la SSR2 : réviser les efforts d'analyse et de rapport de l'utilisation malveillante du DNS pour permettre la transparence et la révision indépendante, et la Recommandation 13 de la SSR2 : accroître la transparence et la responsabilité en matière de signalement des plaintes pour utilisation malveillante, dans le cas des recommandations de la SSR2 qui s'ajoutent à une recommandation originale de la SSR1.

Fondements :

- Bien que l'organisation ICANN ait mis en œuvre un processus de divulgation de vulnérabilités, il n'existe aucune statistique publique ni aucune autre information sur la fréquence à laquelle un tel processus a été invoqué.

[157] Wiki de la SSR2, documents finaux et préliminaires de l'équipe de révision, « Tableau des recommandations de la SSR1 » s.d., 26, https://community.icann.org/pages/viewpage.action?pageId=64076120.
[158] ICANN, interface de participation, consultée le 13 décembre 2020, https://features.icann.org/events-near-you.

- L'organisation ICANN a mis en œuvre un programme de divulgation de vulnérabilités pour les actifs publics de l'ICANN.159 Lorsque des vulnérabilités pour l'infrastructure du DNS sont signalées à l'organisation ICANN, l'organisation ICANN (lorsque cela est possible) diffusera cette information aux tiers externes responsables. Toutefois, il relève de la responsabilité du tiers de remédier à toute vulnérabilité au sein de sa ou de ses plateformes.
- Depuis 2013, aucun des rapports IS-SSR ne contient des statistiques ou des mesures liées à la communication de l'information. Il est impossible de savoir à partir des documents publiés si la méthodologie de divulgation de vulnérabilités a déjà été invoquée, ou si elle est fonctionnelle. Aucune donnée, même anonyme, n'indique que l'organisation ICANN coordonne les vulnérabilités, ou travaille pour coordonner les urgences et gérer les crises liées à la SSR.

Recommandation 16 de la SSR1

« L'ICANN devrait poursuivre ses efforts de communication afin d'accroître la participation de la communauté au processus de développement du cadre SSR. L'ICANN devrait également établir un processus pour obtenir des avis plus systématiques d'autres membres de l'écosystème ».

Conclusion de la SSR2 : cette recommandation reste pertinente et n'a été appliquée que partiellement. Étant donné le manque de preuves que les activités actuelles de sensibilisation ont entraîné une participation accrue de la communauté, cette recommandation ne peut pas être considérée comme ayant atteint l'effet escompté.

Voir la Recommandation 8 de la SSR2 : permettre et démontrer la représentation de l'intérêt public dans les négociations avec les parties contractantes, et la Recommandation 12 de la SSR2 : réviser les efforts d'analyse et de rapport de l'utilisation malveillante du DNS pour permettre la transparence et la révision indépendante, et la Recommandation 13 de la SSR2 : accroître la transparence et la responsabilité en matière de rapports de signalement des plaintes pour utilisation malveillante et la Recommandation 18 de la SSR2 : éclairer les débats sur les politiques, dans le cas des recommandations de la SSR2 qui s'ajoutent à une recommandation originale de la SSR1.

Fondements :

- La participation continue dans les communautés apparentées a atteint l'objectif de « participation » mais n'a pas pu déterminer comment l'information est intégrée « [de façon] systématique ». Cette recommandation prévoit une participation accrue du public à l'égard des initiatives de SSR, y compris les cadres et les rapports annuels. Cette recommandation n'a pas entraîné de changements évidents dans la façon dont le cadre IS-SSR et les rapports annuels sont créés.
- Il y a une sensibilisation continue aux communautés associées ayant des relations existantes avec l'organisation ICANN, ce qui accomplit l'objectif de « participation ». Toutefois, la recommandation demande la sensibilisation auprès d'autres communautés de SSR.
- Rien ne fait preuve que les activités actuelles de sensibilisation aient entraîné une participation accrue de la communauté.

[159] ICANN, « Processus de rapport des vulnérabilités des services en ligne de l'organisation ICANN », consulté le 13 décembre 2020, https://www.icann.org/vulnerabilities.

- La recommandation demande spécifiquement un processus plus systématique pour obtenir les commentaires des autres participants à l'écosystème. Le résultat final du rapport sur l'état de mise en œuvre de la SSR1 ne semble donc pas approprié.160
- Le rapport de mise en œuvre indique que le personnel « soutiendrait diverses initiatives de renforcement des capacités de l'équipe de sécurité ».161 L'équipe de révision SSR2 n'a pas été en mesure de déterminer si et comment ces initiatives de renforcement des capacités affecteraient un plus grand engagement dans le développement des cadres IS-SSR parce que l'organisation ICANN ne met plus à jour les cadres IS-SSR.
- L'équipe de révision SSR2 n'a pas trouvé des preuves publiques sur la tenue des initiatives de renforcement des capacités ou du moment auquel elles ont été menées.

Recommandation 17 de la SSR1

« L'ICANN devrait élaborer un processus interne plus structuré permettant de mieux comprendre le rapport existant entre certaines activités et initiatives et les buts, objectifs et priorités spécifiques du cadre SSR ».

Conclusion de la SSR2 : cette recommandation reste pertinente. En raison de l'absence d'indicateurs traçables, il est impossible de déterminer l'état d'avancement de la mise en œuvre à partir de documents disponibles au public. La recommandation n'a pas atteint son effet prévu car l'organisation ICANN n'entretient plus le cadre SSR.

Voir la Recommandation 2 de la SSR2 : désigner un cadre responsable de la sécurité stratégique et tactique et de la gestion des risques pour la recommandation SSR2 qui s'ajoute à la recommandation originale de la SSR1.

Fondements :

- Le rapport de mise en œuvre fait référence aux livrables de la Recommandation 2 de la SSR1 comme guide de la façon dont la Recommandation 17 de la SSR1 a été mise en œuvre. Toutefois, les Recommandations 2 et 17 de la SSR1 visent des objectifs différents. La Recommandation 2 de la SSR1 demande que les activités et les attributions liées à la SSR passent par une consultation publique régulière, tandis que la Recommandation 17 de la SSR1 suggère que les initiatives liées à la SSR se rapportent à des buts, des objectifs et des priorités stratégiques spécifiques. Les livrables de la Recommandation 2 de la SSR1 ne répondent pas aux exigences de la Recommandation 17 de la SSR1.
- Le rapport annuel le plus récent examiné par la SSR2 (exercice fiscal 2018) répertorie dix-huit initiatives distinctes pour l'exercice fiscal, puis décrit comment ces initiatives sont liées à la mission globale du bureau du directeur de la technologie et au plan stratégique global de l'ICANN. Le plan annuel est ensuite lié aux rapports d'activités qui décrivent le travail accompli au cours d'une période de rapport (six mois).
- Le lien entre le rapport annuel de la SSR et le plan stratégique de l'ICANN n'est pas clair. En outre, le plan stratégique ne mentionne pas les rapports annuels de la SSR et évoque à peine les activités liées à la SSR. S'il existait un processus interne plus structuré pour montrer comment les activités et les initiatives sont liées à des buts, objectifs et priorités stratégiques spécifiques dans le cadre IS-SSR, il n'est pas disponible au public ni à l'équipe

[160] ICANN, Rapport de mise en œuvre de la révision de la SSR, juin 2015 https://www.icann.org/en/system/files/files/ssr-review-implementation-30jun15-en.pdf.
[161] Ibid., 7.

de révision SSR2. Toutefois, la section du rapport annuel le plus récent qui identifie les initiatives annuelles tente de les relier au Plan stratégique de l'ICANN.
- D'autres recommandations de la SSR1 tentent d'aligner et d'intégrer les activités de l'ICANN en matière de SSR avec le Plan stratégique global. La mise en œuvre de la recommandation 17 de la SSR1 est loin de fournir un processus interne structuré et facile à examiner.

Recommandation 18 de la SSR1

« L'ICANN devrait mener une révision opérationnelle annuelle de ses progrès dans la mise en place du cadre SSR et inclure cette évaluation dans le cadre SSR de l'année suivante ».

Conclusion de la SSR2 : cette recommandation reste pertinente. L'équipe de révision SSR2 n'a pas pu trouver de preuve d'un processus de révision interne ou d'un processus de révision publique qui ait donné lieu à des mises à jour régulières du cadre IS-SSR et ne peut donc pas déterminer si cette recommandation a atteint les résultats escomptés.

Voir la Recommandation 2 de la SSR2 : désigner un cadre responsable de la sécurité stratégique et tactique et de la gestion des risques pour la recommandation SSR2 qui s'ajoute à la recommandation originale de la SSR1.

Fondements :
- La Recommandation 18 de la SSR1 suggère une approche récursive où l'examen d'une activité de l'année précédente influencera les décisions concernant les initiatives à l'avenir. L'équipe de révision SSR2 n'a pas trouvé de preuve d'un processus interne informel ou non documenté, ni n'a trouvé une révision publique, annuelle et opérationnelle de la mise en œuvre du cadre IS-SSR.

Recommandation 19 de la SSR1

« L'ICANN devrait élaborer un processus permettant à la communauté de faire un suivi de la mise en place du cadre SSR. L'information fournie devrait être suffisamment claire pour permettre à la communauté de suivre l'exécution des responsabilités de l'ICANN en matière de SSR ».

Conclusion de la SSR2 : cette recommandation reste pertinente. En raison d'un manque de spécificité de la phrase « clarté suffisante », cette recommandation n'est pas mesurable dans son intégralité. Cette recommandation n'a pas atteint l'effet escompté, car la communauté reste incapable de suivre les activités liées à la SSR dans un délai raisonnable et de manière ouverte et transparente.

Voir la Recommandation 2 de la SSR2 : désigner un cadre responsable de la sécurité stratégique et tactique et de la gestion des risques pour la recommandation SSR2 qui s'ajoute à la recommandation originale de la SSR1.

Fondements :
- L'organisation ICANN signale que la publication du cadre annuel IS-SSR162 suit les progrès réalisés par rapport aux activités engagées dans le cadre correspondant à l'année précédente. En outre, les rapports réguliers de gestion de projets, les plans opérationnels et

[162] Archive de documents de l'IS-SSR, https://www.icann.org/ssr-document-archive.

les budgets sont considérés comme des outils qui fournissent des détails sur les activités en matière de SSR. Toutefois, la publication d'un cadre annuel IS-SSR sur le site Web ne semble pas servir à informer la communauté et à lui permettre de suivre la mise en œuvre du cadre. La documentation de la mise en œuvre est très en retard sur la mise en œuvre et n'offre donc pas à la communauté un moyen de suivre les activités liées à la SSR.
- En outre, il semble que l'équipe de révision SSR1 a fourni un exemple de tableau de bord public pour le suivi des activités liées à la SSR, comme cela a été fait pour mettre en œuvre l'une des recommandations de l'ATRT. Toutefois, il n'y a aucune preuve qu'un tel tableau de bord soit disponible pour la communauté ou le public dans le cas des activités liées à la SSR.

Recommandation 20 de la SSR1

« L'ICANN devrait accroître la transparence des informations concernant l'organisation et le budget lié à la mise en place du cadre SSR et aux fonctions en matière de SSR ».

Conclusion de la SSR2 : cette recommandation reste pertinente et a été partiellement mise en œuvre. L'effet prévu d'améliorer la transparence des détails relatifs à la SSR, en ce qui concerne l'organisation et le budget, n'a pas été atteint.

Voir la Recommandation 3 de la SSR2 : améliorer la transparence budgétaire liée à la SSR dans le cas des recommandations de la SSR2 qui s'ajoutent à une recommandation originale de la SSR1.

Fondements :
- Le cycle de planification de l'ICANN est basé sur une approche qui comporte trois volets : un plan stratégique, un plan opérationnel quinquennal, et un plan opérationnel et un budget annuels.[163] Le cycle se termine par des rapports de réalisation et de progrès. L'étape I, telle que décrite dans les Rapports de mise en œuvre sur le Wiki de mise en œuvre de la SSR1, est maintenant en place pour fournir des informations publiques sur les plans, les budgets et les activités liés à la SSR (comme indiqué dans la Recommandation 2 de la SSR1) ; elle est intégrée au cadre IS-SSR de l'ICANN et aux rapports sur les activités et les dépenses liées à la SSR.[164] Les rapports périodiques des activités liées à la SSR augmentent cette information publique.[165] L'étape II s'occupe actuellement d'identifier les mécanismes qui fournissent des informations publiques plus détaillées sur les budgets et les dépenses liés à la SSR dans plusieurs départements de l'ICANN. Actuellement, des informations publiques sur ce sujet pour l'exercice fiscal 2018 peuvent être trouvées sur la page wiki consacrée à la Recommandation 20.[166]
- Le personnel a également élaboré un rapport a posteriori qui comprend les impacts sur le budget et les ressources liés à la gestion d'un événement.[167] Aucun rapport a posteriori n'a

[163] « Processus de planification de l'ICANN », https://www.icann.org/resources/pages/governance/planning-en.
[164] Page d'accueil de la mise en œuvre de la révision de la SSR1, https://community.icann.org/display/SSR/SSR1+Review+Implementation+Home.
[165] Rapport des activités concernant la SSR des systèmes d'identificateurs, https://www.icann.org/news/blog/identifier-systems-ssr-activities-reporting-en.
[166] Mise en œuvre de la révision de la SSR1, Recommandation 20, dernière mise à jour le 18 septembre 2018, https://community.icann.org/display/SSR/Rec+%2320.
[167] Rapports des activités concernant la SSR des systèmes d'identificateurs, https://www.icann.org/news/blog/identifier-systems-ssr-activities-reporting-en.

été publié depuis mars 2020. Un modèle de version publique de ces rapports est disponible sur la page wiki de la Recommandation 20.

- Les rapports annuels sur les activités liées à la SSR sont présentés dans les documents-cadres et les rapports annuels. Les documents budgétaires comportent très peu de détail au sujet des activités liées à la SSR. Ces mêmes activités ne semblent pas faire l'objet d'un rapport régulier de l'ICANN sur la gestion de projet. Le rapport de mise en œuvre indique que l'ICANN « *intégrera le cadre SSR et les rapports sur les activités et les dépenses liées à la SSR dans le cadre et le processus de planification afin de fournir des informations publiques sur les plans, les budgets et les activités liés à la SSR* ».[168] Toutefois, comme indiqué pour la Recommandation 19 de la SSR1, le système de gestion du portefeuille de l'ICANN et le tableau de bord du projet KPI disposent de quantités très limitées d'informations que la communauté peut utiliser pour suivre les efforts liés à la SSR.
- Le budget approuvé pour l'exercice fiscal 2018 comprend trois domaines de portefeuille liés à la SSR : évolution des identificateurs ; sécurité, stabilité et résilience des identificateurs de l'Internet ; réputation technique. Seuls les deux premiers (Évolution des identificateurs et SSR des identificateurs de l'Internet) ont des budgets dédiés au niveau du portefeuille ; aucun détail de ces budgets n'est fourni. Le rapport de mise en œuvre du personnel indique également que l'ICANN « *identifiera des mécanismes qui fournissent des informations publiques plus détaillées sur les budgets et les dépenses liés aux SSR dans plusieurs départements de l'ICANN* », suggérant que des travaux supplémentaires sont attendus sur cet aspect de la mise en œuvre.

Recommandation 21 de la SSR1

« L'ICANN devrait élaborer un processus interne plus structuré permettant de mieux montrer le rapport existant entre le cadre SSR et certaines décisions concernant l'organisation et le budget, y compris l'analyse coût/bénéfice sous-jacente ».

Conclusion de la SSR2 : cette recommandation reste pertinente et a été partiellement mise en œuvre. Elle n'a pas eu l'effet escompté de générer un processus ouvert et transparent concernant les décisions budgétaires liées à la SSR.

Voir la Recommandation 3 de la SSR2 : améliorer la transparence budgétaire liée à la SSR pour la recommandation de la SSR2 qui s'ajoute à la recommandation originale de la SSR1.

Fondements :

- Dans le rapport de mise en œuvre du personnel, trois livrables sont mentionnés :
  - Intégration du cadre IS-SSR et des rapports dans le cadre et le processus de planification afin de fournir au public des renseignements sur les plans, les budgets et les activités liés à la SSR.
  - Identification de mécanismes qui fournissent des informations publiques plus détaillées sur les budgets et les dépenses liés à la SSR dans plusieurs départements de l'ICANN.
  - Rapports d'exploration a posteriori incluant l'impact de la gestion de l'événement sur le budget et les ressources.
- Le rapport du personnel mentionne spécifiquement un modèle de rapport pour la publication d'informations relatives aux budgets et aux ressources affectés par les événements de

[168] Voir les mises à jour du rapport de mise en œuvre de la SSR1 pour la Recommandation 20, https://community.icann.org/download/attachments/54691765/SSR%20Recs%201-28.pdf?api=v2.

sécurité.[169] Le rapport du personnel suggère qu'il sera publié chaque année à compter de l'exercice fiscal 2018. Un examen des pages relatives à la SSR sur le site Web de l'ICANN indique qu'aucun rapport n'a été publié. Les rapports annuels sur les activités liées à la SSR sont présentés dans les documents-cadres et les rapports annuels. Le document du budget comporte des généralités sur les activités liées à la SSR. Toutefois, ces mêmes activités ne semblent pas faire l'objet d'un rapport régulier de l'ICANN sur la gestion de projets. Cette observation coïncide avec les constats de la SSR1 pour la Recommandation 20 de la SSR1. De plus, les rapports relatifs aux impacts des événements SSR sur le budget et les ressources semblent n'avoir jamais été effectués, et le modèle pour appuyer ces rapports ne semble pas être disponible pour examen ou consultation publique.

- Le processus de planification de l'ICANN garantit que les activités prévues et budgétisées, y compris celles liées à la SSR, soient identifiées par des objectifs spécifiques. Il n'a pas été prévu de demander des commentaires au public sur le modèle utilisé pour publier des renseignements plus détaillés sur les budgets et les dépenses liés à la SSR. Le modèle semble maintenant avoir été remplacé par le rapport annuel de l'exercice fiscal.

Recommandation 22 de la SSR1

« L'ICANN devrait publier, surveiller et mettre à jour la documentation sur les ressources organisationnelles et budgétaires nécessaires pour gérer les aspects liés à la sécurité, la stabilité et la résilience conjointement avec l'introduction des nouveaux gTLD ».

Conclusion de la SSR2 : cette recommandation reste pertinente et a été partiellement mise en œuvre. La mise en œuvre n'a pas eu l'effet total escompté.

Voir la Recommandation 3 de la SSR2 : améliorer la transparence budgétaire liée à la SSR dans le cas des recommandations de la SSR2 qui s'ajoutent à une recommandation originale de la SSR1.

Fondements :

- Des informations publiques sur le budget et les dépenses liés à la SSR dans plusieurs départements de l'ICANN ont été publiées pour l'exercice 2018 et sont disponibles ici : https://community.icann.org/x/DqNYAw. Ce rapport est mis à jour chaque année et couvre les coûts directs résultant des activités requises pour exécuter les fonctions SSR, les coûts directs des ressources partagées et les coûts des fonctions de soutien allouées à la SSR. Ce rapport ne fournit pas de ventilation du financement, des ressources ou d'autres activités liées au programme des nouveaux gTLD.
- L'organisation ICANN a également exploré les mécanismes qui fournissent davantage d'informations publiques sur les budgets et les dépenses liés à la SSR dans plusieurs services de l'ICANN. Toutefois, un modèle pour cette information publique ne comprend pas les activités ou les budgets associés à la dimension SSR du programme des nouveaux gTLD.
- Il est clair que l'organisation et le budget liés à la dimension SSR de l'équipe des nouveaux gTLD ont été fournis par l'intermédiaire de l'équipe de sécurité, mais également reflétés dans le budget et l'organisation du programme des nouveaux gTLD (par exemple, le Panel pour la stabilité du DNS, EBERO, d'autres étapes du processus, etc.). Il semble que le résultat souhaité de la mise en œuvre de cette recommandation ait été d'améliorer la quantité et la clarté des informations sur l'organisation et le budget pour la mise en œuvre

[169] Mise en œuvre de la révision SSR1, Recommandation 20, https://community.icann.org/display/SSR/Rec+%2320.

du cadre IS-SSR et l'exécution des fonctions liées à la dimension SSR du programme des nouveaux gTLD.

- Dans l'archive de documents sur l'IS-SSR de l'ICANN, il n'existe aucun document spécifique au programme des nouveaux gTLD. Dans le cadre daté du 30 septembre 2016, les gTLD sont mentionnés à deux reprises : une fois dans le module A comme une tendance dans l'écosystème Internet et une fois de plus dans le module B dans le cadre du plan stratégique global de l'ICANN. Dans le cadre de la SSR pour l'exercice fiscal 2014, publié en mars 2013, le programme des nouveaux gTLD est de nouveau mentionné comme une « tendance » et comme un moteur de politique pour la GNSO. Les seules mentions restantes du programme des nouveaux gTLD se trouvent dans la section faisant état de la mise en œuvre des recommandations de la SSR1.

Recommandation 23 de la SSR1

« L'ICANN doit fournir des ressources appropriées aux groupes de travail et comités consultatifs travaillant sur des questions liées à la sécurité, la stabilité et la résilience, cohérentes avec les exigences qui leur sont imposées. L'ICANN doit également veiller à ce que les décisions issues des groupes de travail et des comités consultatifs aient été prises de façon objective et n'aient pas été influencées par des pressions internes ou externes ».

Conclusion de la SSR2 : cette recommandation reste pertinente et a été partiellement mise en œuvre. L'effet escompté était de permettre aux groupes de travail et aux comités consultatifs de s'acquitter de leurs mandats d'une manière non mesurable, objective et libre de pressions externes ou internes.

Voir la Recommandation 3 de la SSR2 : améliorer la transparence budgétaire liée à la SSR dans le cas des recommandations de la SSR2 qui s'ajoutent à une recommandation originale de la SSR1.

Fondements :

- L'organisation ICANN fournit du personnel de soutien technique de l'ICANN au SSAC et au RSSAC pour aider à la rédaction de documents. Le budget de l'organisation ICANN inclut un certain financement pour soutenir la conduite de réunions du SSAC et du RSSAC (en particulier les frais de déplacement, d'hôtel, de restauration) ; l'organisation ICANN a signalé le budget de 2015 comme exemple à l'équipe de révision SSR2.[170] Le financement du soutien n'a jamais été lié ou conditionné par une évaluation formelle du rendement, de la production ou du contenu. L'ICANN estime que cela permet une indépendance adéquate. Dans la pratique, il n'est pas clair comment les priorités de travail du RSSAC ou du SSAC sont déterminées ou évaluées par l'ICANN ou par la communauté, ce qui crée un écart de responsabilité, en plus de rendre impossible l'évaluation de leurs ressources « compatibles avec les exigences qui leur sont imposées ». Le rapport original de la SSR1 comprenait le texte suivant associé à cette recommandation :
  « À partir des discussions avec le SSAC, il est apparu qu'une grande pression est parfois exercée sur ce comité pour qu'il apporte des réponses à des problèmes spécifiques dans des délais très courts. Cette contrainte au niveau des délais les amène à raccourcir les temps d'évaluation du problème, ce qui a pour résultat des recommandations plus ciblées. Manifestement, lorsqu'il s'agit d'analyser des risques immédiats, il arrive parfois que le délai fixé permette à peine de finir le travail de recherche. C'est inévitable. Or, il serait prudent

[170] ICANN, « Plan opérationnel et budget adopté pour l'exercice fiscal 2015 », 1er décembre 2014, 77-78, https://www.icann.org/en/system/files/files/adopted-opplan-budget-fy15-01dec14-en.pdf.

d'améliorer les plannings de façon à accorder au SSAC et au RSSAC autant de temps que possible pour mettre en place des recherches qui puissent donner lieu à des résultats de grande qualité ».

Cette observation fait écho aux circonstances et aux préoccupations des deux dernières années, en particulier dans le contexte du roulement de la KSK en octobre 2018, lorsque le SSAC a eu du mal à répondre aux demandes de conseil sur des délais courts, avec une disponibilité insuffisante de données/recherches pour éclairer le débat.[171] La fraction du budget de l'ICANN destinée au SSAC est probablement insuffisante, au vu des nombreuses questions existantes et émergentes liées à la SSR et des attentes que le SSAC fournisse des conseils qui nécessitent une recherche ou une synthèse des recherches antérieures. La structure actuelle du SSAC n'est pas non plus compatible avec un « travail de recherche de haute qualité », puisqu'il est composé d'un ensemble de « bénévoles » principalement issus de l'industrie, subventionnés par leurs employeurs pour le temps qu'ils consacrent à leur participation, et donc « exempts de toute pression extérieure ».

- Le manque de mesures et de surveillance du succès ou de l'échec du programme des nouveaux gTLD indique que cette approche multipartite n'est pas « exempte de pressions externes ». Il est impossible de conclure, grâce à des mesures du rapport de la CCT RT sur l'utilisation malveillante du DNS dans les nouveaux gTLD, que le programme des nouveaux gTLD ait été couronné de succès du point de vue de la CCT. De telles recherches relèvent bien des rôles et des responsabilités de l'équipe de sécurité de l'ICANN (voir la Recommandation 24 de la SSR1). L'ICANN n'a pas entrepris ou financé ce type d'exercice elle-même, probablement parce que les pressions externes contre ce type d'activité de recherche de la SSR ont prévalu.
- Rien dans le document sur les procédures opérationnelles du SSAC ne concerne la gestion des pressions externes et internes, à l'exception de l'article 2.1.2, Retraits et dissensions, ce qui signifie que chaque membre, et le comité lui-même, gère ses propres conflits d'intérêts, et que toutes les délibérations sont confidentielles pour des raisons de sécurité.[172] Il en va de même pour le RSSAC et le RZERC, mais dans ces deux cas, les comités sont structurés de manière à ce que chaque personne représente une partie prenante.
- Certains de ces comités consultatifs liés à la SSR manquent en permanence de certains types de parties prenantes (par exemple, victimes d'abus d'identificateurs, chercheurs universitaires, forces de l'ordre, décideurs).

Recommandation 24 de la SSR1

« L'ICANN doit définir clairement la charte, les rôles et les responsabilités de l'équipe du service de sécurité ».

Conclusion de la SSR2 : la recommandation reste pertinente et a été partiellement mise en œuvre. Elle n'a pas eu l'effet escompté d'avoir une charte claire, des rôles définis et des responsabilités définies pour l'équipe du Bureau principal de la sécurité.

Voir la Recommandation 2 de la SSR2 : désigner un cadre responsable de la sécurité stratégique et tactique et de la gestion des risques pour la recommandation SSR2 qui s'ajoute à la recommandation originale de la SSR1.

[171] ICANN, « Premier roulement de la KSK de la racine complété avec succès », annonces de l'ICANN, 15 octobre 2018, https://www.icann.org/news/announcement-2018-10-15-en.

[172] Comité consultatif sur la sécurité et la stabilité de l'ICANN, « Procédures opérationnelles du SSAC version 5.1 », 27 février 2019, 10, https://www.icann.org/en/system/files/files/operational-procedures-27feb18-en.pdf.

Fondements :

- Depuis 2018, le bureau principal de la sécurité n'existe pas. Cependant, l'équipe de l'OCTO (Bureau du directeur de la technologie) consacrée à la SSR travaille sur des questions externes liées à la SSR de l'ICANN, le CIO et son équipe travaillent sur des questions de sécurité internes, et l'équipe de recherche de l'OCTO se penche sur les risques et les opportunités futurs liés à la SSR dans le cadre de la portée et des attributions limitées de l'ICANN.173 La page Web de cette équipe décrit très vaguement sa mission et renvoie vers une page d'activités liées à la SSR.174 Il n'y a pas de langage faisant référence à la « charte », aux « rôles » ou aux « responsabilités » de cette équipe. L'équipe de la SSR2 suppose que les activités énumérées sur cette page sont ce que l'ICANN entend comme les rôles et responsabilités liés à la SSR de l'OCTO :
  - Échanger activement avec les communautés de la sécurité, des opérations et de la sécurité publique afin de recueillir et de traiter les données de renseignement qui indiquent des menaces (imminentes) aux opérations du DNS ou du service d'enregistrement de domaines (l'« écosystème DNS »).
  - Faciliter ou participer avec ces mêmes communautés à des activités de préparation aux menaces contre l'écosystème DNS afin de les protéger ou d'atténuer les risques.
  - Effectuer des études ou analyser des données pour mieux comprendre la santé et le bien-être de l'écosystème du DNS.
  - Coordonner les rapports de divulgation de vulnérabilités du DNS (https://www.icann.org/vulnerability-disclosure.pdf).
  - Prêter une expertise dans le domaine pour renforcer les capacités des ccTLD et des communautés de la sécurité publique dans des sujets pertinents pour l'écosystème DNS, y compris les DNSSEC, l'utilisation malveillante ou abusive des infrastructures ou des opérations du DNS.
  - Participer aux activités de gestion des risques de l'écosystème DNS.
  - En collaboration avec l'équipe en charge de la relation avec les parties prenantes mondiales de l'ICANN, participer à un effort mondial multipartite visant à améliorer la cybersécurité et à atténuer la cybercriminalité.
- L'OCTO ne semble pas avoir produit beaucoup en termes d'analyse de la SSR qui est à la disposition du public. L'initiative d'ouverture des données, le rapport DAAR et le projet de mesures Internet semblent tous être des projets avec des données associées qui sont internes à l'organisation ICANN. Il n'est pas clair à quel point tout ce travail a été utile jusqu'à présent à la communauté élargie que l'organisation ICANN est destinée à servir.

Recommandation 25 de la SSR1

« L'ICANN devrait mettre en place des mécanismes permettant d'identifier à la fois les risques à court terme et à long terme ainsi que des facteurs stratégiques dans son cadre de gestion des risques ».

Conclusion de la SSR2 : cette recommandation reste pertinente et a été partiellement mise en œuvre. La mise en œuvre n'a pas eu l'effet escompté.

[173] OCTO de l'ICANN, « Bureau du directeur de la technologie (OCTO) », consulté le 27 décembre 2019, https://www.icann.org/octo..

[174] OCTO de l'ICANN, « Sécurité, stabilité et résilience du système d'identificateurs de l'Internet », consulté le 27 décembre 2019, https://www.icann.org/octo-ssr.

Voir la Recommandation 4 de la SSR2 : améliorer les processus et les procédures de gestion des risques dans le cas des recommandations de la SSR2 qui s'ajoutent à une recommandation originale de la SSR1.

Fondements :

- Un cadre de gestion des risques a été accepté par le Conseil d'administration de l'ICANN en 2013, après avoir reçu les contributions de la communauté au cours des réunions ICANN50 et ICANN51. L'organisation ICANN gère un tableau de bord de gestion des risques de l'entreprise (ERM) qui répertorie les risques à surveiller et à traiter et suit un cadre de gestion des risques de l'entreprise. Cependant, bien qu'un mécanisme ait été mis en place, il y a un manque de clarté quant à la manière dont l'identification des risques alimente les processus et les politiques pertinents associés à la SSR.

Recommandation 26 de la SSR1

« L'ICANN devrait considérer comme prioritaire l'achèvement dans les délais du travail d'élaboration d'un cadre de gestion des risques ».

Conclusion de la SSR2 : cette recommandation reste pertinente et a été partiellement mise en œuvre. Étant donné que l'expression « dans les délais » n'offre aucune spécificité dans ce qui était prévu ou acceptable, il est impossible d'évaluer si l'effet prévu a été atteint.

Voir la Recommandation 4 de la SSR2 : améliorer les processus et les procédures de gestion des risques dans le cas des recommandations de la SSR2 qui s'ajoutent à une recommandation originale de la SSR1.

Fondements :

- Un cadre de gestion des risques a été accepté par le Conseil d'administration de l'ICANN en 2013,175 après avoir reçu les contributions de la communauté au cours des réunions ICANN50 et ICANN51. Une réponse plus détaillée à cette recommandation est traitée dans le cadre de l'évaluation de la Recommandation 27.

Recommandation 27 de la SSR1

« Le cadre de gestion des risques de l'ICANN doit être exhaustif tout en respectant le champ d'application de ses attributions et de sa mission technique limitée en matière de SSR ».

Conclusion de la SSR2 : cette recommandation reste pertinente. Étant donnée l'absence d'une définition du terme « exhaustif » par la SSR1 ou des mesures pour l'évaluer, l'équipe de révision SSR2 n'a pas été en mesure d'évaluer si cette recommandation a été pleinement mise en œuvre. L'organisation ICANN n'a pas atteint l'effet prévu de fournir des informations complètes et faciles à trouver sur le cadre de gestion des risques utilisé par l'ICANN.

Voir la Recommandation 4 de la SSR2 : améliorer les processus et les procédures de gestion des risques dans le cas des recommandations de la SSR2 qui s'ajoutent à une recommandation originale de la SSR1.

Fondements :

[175] ICANN, « Rapport sur le cadre de gestion des risques pour le DNS », modifié pour la dernière fois le 4 octobre 2013, https://www.icann.org/public-comments/dns-rmf-final-2013-08-23-en.

- L'équipe de révision de la SSR2 a discuté de la question de savoir si la Recommandation 27 de la SSR1 avait été mise en œuvre en fonction des références faites par le personnel lors de divers échanges de questions et de réponses liés à la Recommandation 25 de la SSR1. L'équipe de révision de la SSR2 a toutefois conclu que cette recommandation, bien qu'elle soit corrélée aux Recommandations 25 et 26 de la SSR1, est distincte parce qu'elle demande que le cadre soit « exhaustif ». L'équipe de révision SSR2 était d'avis que si la Recommandation 27 de la SSR1 était mise en œuvre conformément aux intentions de l'équipe de révision SSR1, elle aurait répondu aux mêmes préoccupations que les Recommandations 25 et 26 de la SSR1 cherchaient probablement à aborder.
- La SSR1 ne définissait point les éléments du cadre qui constitueraient un « ensemble » ou la façon dont il devrait être évalué. Au cours de la révision, il a été noté que cette recommandation aurait été mise en œuvre par des membres du personnel de l'ICANN qui ne font plus partie de l'organisation ICANN. À cet égard, la mémoire institutionnelle et un historique complet de la façon dont ils ont évalué « l'exhaustivité » du cadre de gestion des risques n'étaient pas disponibles.
- L'information disponible au public concernant la façon de traiter la gestion des risques a été trouvée fragmentée çà et là. À titre d'exemple, le personnel a indiqué que le Comité de gestion des risques du Conseil d'administration était intégré par l'équipe de direction de l'organisation ICANN, qui assure la surveillance. De plus, il était indiqué qu'il existe des agents de liaison liés au risque qui sont des membres du personnel représentant chaque fonction pour la mise en œuvre du cadre de risques, et que tout le personnel de l'organisation responsable des risques inhérents à sa fonction se concentre sur les questions de gestion des risques. Cela démontre que la fonction de risque pour l'organisation ICANN n'a pas été centralisée et coordonnée de manière stratégique.

Recommandation 28 de la SSR1

« L'ICANN devrait poursuivre sa participation active dans la détection et la réduction de risques, ainsi que dans les efforts de communication visant à diffuser des informations liées aux menaces et aux incidents ».

Conclusion de la SSR2 : cette recommandation reste pertinente et n'a pas été pleinement mise en œuvre. Bien que l'organisation ICANN ait échangé avec divers groupes pour aider à détecter, atténuer et partager des informations sur les menaces et les incidents, l'effet prévu de la mise à disposition de ces informations en dehors de ces groupes désignés n'a pas été atteint.

Voir la Recommandation 2 de la SSR2 : désigner un cadre responsable de la sécurité stratégique et tactique et de la gestion des risques, la Recommandation 8 de la SSR2 : permettre et démontrer la représentation de l'intérêt public dans les négociations avec les parties contractantes, et la Recommandation 12 de la SSR2 : réviser les efforts d'analyse et de rapport de l'utilisation malveillante du DNS pour permettre la transparence et la révision indépendante, et la Recommandation 13 de la SSR2 : accroître la transparence et la responsabilité en matière de signalement des plaintes pour utilisation malveillante, dans le cas des recommandations de la SSR2 qui s'ajoutent à la recommandation originale de la SSR1.

Fondements :

- L'équipe de révision SSR2 n'a trouvé aucune donnée publiquement disponible qui montre que l'organisation ICANN s'engage dans la détection et l'atténuation des menaces. L'organisation ICANN, lorsque cela est possible, diffuse les rapports des vulnérabilités signalées aux tiers externes responsables. Toutefois, il incombe au tiers d'agir en fonction des informations diffusées sur les menaces et les incidents.

- Il n’y a aucune preuve publique que l’organisation ICANN procède à une détection continue des menaces ni que quiconque soit chargé de cette fonction. La communauté de l’ICANN, cependant, dispose d’un certain nombre de groupes (ouverts et fermés) qui effectuent activement la détection des menaces, y compris le SSAC, le RSSAC, TLDOPS, le Groupe de travail sur la réponse aux incidents de la ccNSO et le Groupe de travail sur la sécurité publique. L’équipe SSR de l’OCTO coordonne avec ces groupes.

Annexe E : données de recherche sur les rapports des tendances d'utilisation malveillante du DNS

Quelques exemples connectés au DNS à divers degrés comprennent :

- Logiciel malveillant : de 2016 à 2018, le nombre d'URL uniques reconnus comme malveillants par les logiciels antivirus a plus que doublé à 554.159.6213[176], et les attaques de logiciels malveillants mobiles ont presque doublé de 2017 à 2018, atteignant plus de 116 millions[177].
- Fraude par certificat numérique : L'APWG rapporte que les responsables d'attaques d'hameçonnage utilisent de plus en plus les certificats numériques pour rendre les attaques légitimes et pour vaincre les avertissements de détection de fraude des navigateurs.[178] En raison de la suppression par l'ICANN de l'accès au WHOIS, l'administration du certificat SSL n'a plus accès aux données d'enregistrement des noms de domaine et ne peut pas utiliser les registres de propriété des noms de domaine que l'organisation ICANN est chargée de coordonner pour valider la propriété des noms de domaine. PhishLabs a déterminé que la moitié de tous les sites d'hameçonnage utilise le chiffrement SSL, qui peut induire les utilisateurs à penser faussement qu'un site est sûr à utiliser, par exemple, en raison du symbole de verrou vert qui apparaît dans la barre d'adresse du navigateur lorsque le chiffrement SSL est activé. Une partie de cette augmentation provient de l'ajout du chiffrement HTTP aux sites d'hameçonnage, une technique qui utilise une fonction de sécurité pour transformer les utilisateurs en victimes.[179]
- Hameçonnage : L'APWG a indiqué que les responsables d'attaques d'hameçonnage enregistrent les noms de domaine directement pour perpétrer la fraude et que les méthodes d'attaques d'hameçonnage sont devenues plus efficaces et plus difficiles à détecter.

  > « *Les responsables d'attaques d'hameçonnage utilisent de plus en plus les redirections de pages Web pour cacher leurs sites d'hameçonnage de la détection. Lorsque les victimes cliquent sur les liens dans les mails d'hameçonnage, les redirections emmènent l'utilisateur inattentif à d'autres sites avant d'arriver au site d'hameçonnage lui-même. Et puis, une fois que la victime aura soumis ses informations d'identification, d'autres redirections pourraient amener la victime vers un autre domaine* ».[180]

- Piratage de la messagerie en entreprise : le Centre consacré à la cybercriminalité du FBI, aux États-Unis, a signalé une augmentation de 136 % des pertes mondiales identifiées de 2016 à 2018 dues au piratage de la messagerie en entreprise, affectant les 50 états

[176] AMR, « Bulletin de sécurité de Kaspersky de 2018 : Statistiques », 4 décembre 2018, https://securelist.com/kaspersky-security-bulletin-2018-statistics/89145/.
[177] Victor Chebyshev, « Évolution du logiciel malveillant mobile en 2018 », 5 mars 2019, https://securelist.com/mobile-malware-evolution-2018/89689/.
[178] APWG, « Rapport des tendances des activités d'hameçonnage de l'APWG, 3e trimestre de 2018 », 11 décembre 2018, https://docs.apwg.org/reports/apwg_trends_report_q3_2018.pdf.
[179] Elliot Volkman, « 49 pour cent des sites d'hameçonnage utilisent désormais le HTTPS », blog de PhishLabs, 6 décembre 2018, https://info.phishlabs.com/blog/49-percent-of-phishing-sites-now-use-https.
[180] Rapport sur les tendances de l'activité d'hameçonnage de l'APWG, https://docs.apwg.org/reports/apwg_trends_report_q3_2018.pdf.

américains et 150 pays dans le monde entier. Entre octobre 2013 et mai 2018, le FBI a documenté une croissance de plusieurs milliards de dollars de BEC, qui implique souvent l'enregistrement frauduleux de noms de domaine qui sont trompeusement similaires à l'une des parties ciblées.[181]

- Escroquerie : la Commission australienne de la concurrence et de la consommation (ACCC) « ScamWatch » a signalé pratiquement le double en pertes dues aux escroqueries au cours des trois dernières années, passant à 11,8 millions d'AUD en pertes en 2019.[182] Les noms de domaine utilisés pour perpétrer des escroqueries en ligne enfreignent très typiquement les noms de marques ou d'entreprises. Les escrocs enregistrent ces noms avec peu ou pas de contrôle sur les volumes de noms similaires qu'il peut enregistrer et avec un accès limité à l'information que les enquêteurs peuvent utiliser pour identifier les délinquants.
- Réseaux zombies : en 2017, Spamhaus DBL a répertorié 50 000 noms de domaine correspondant à des contrôleurs de réseaux zombies enregistrés et configurés par des cyber-délinquants dans le seul but d'héberger un contrôleur de réseau zombie. Plus de 25 % de ces noms de domaine de réseaux zombies enregistrés ont été enregistrés par un seul bureau d'enregistrement, Namecheap.[183] En 2018, Spamhaus a répertorié 103 503 noms de domaine de contrôleurs de réseaux zombies, soit une augmentation de 106 %. Namecheap est resté le bureau d'enregistrement avec le plus d'enregistrements malveillants, avec une augmentation de 220 % des noms de domaine de contrôleurs de réseaux zombies enregistrés.[184]
- Spam : le spam est l'infrastructure de diffusion préférée pour l'hameçonnage, les logiciels malveillants et d'autres menaces liées au DNS. En août 2019, le volume moyen de spam par jour était de 416,04 milliards.[185]

> *« Quelle que soit l'évolution du paysage des menaces, les courriers électroniques malveillants et les spams restent des outils essentiels pour que les adversaires distribuent les logiciels malveillants, car ils envoient les menaces directement à la cible. En appliquant la bonne combinaison de techniques d'ingénierie sociale, comme l'hameçonnage, ou les liens et les pièces jointes malveillants, les adversaires n'ont qu'à s'asseoir et à attendre que les utilisateurs insouciants activent leurs exploits ».*[186]

- Attaque DDoS : les attaques par déni de service distribué (DDoS) ont augmenté de 40 % entre la mi-2017 et la mi-2018.[187] La taille maximale des attaques de DDoS a augmenté globalement de 174 % au premier semestre de 2018 par rapport à la même période de

[181] « Le piratage de la messagerie en entreprise. Une escroquerie de 12 milliards de dollars », annonce du service public du Bureau fédéral des enquêtes, 12 juillet 2018, https://www.ic3.gov/media/2018/180712.aspx.
[182] ScamWatch, Commission australienne de la concurrence et de la consommation, https://www.scamwatch.gov.au/about-scamwatch/scam-statistics.
[183] « Rapport sur les menaces des réseaux zombies de Spamhaus », Spamhaus Malware Labs, dernière modification le 8 janvier 2018, https://www.spamhaus.org/news/article/772/spamhaus-botnet-threat-report-2017.
[184] « Rapport sur les menaces des réseaux zombies de Spamhaus de 2019 », Spamhaus Malware Labs, s.d., https://www.spamhaustech.com/botnet-threat-report-2019/
[185] « Données relatives aux e-mails et au Spam », Cisco Talos Intelligence Group, https://www.talosintelligence.com/reputation_center/email_rep.
[186] « Rapport annuel de cybersécurité de Cisco de 2018 », Cisco Systems, février 2018, https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf.
[187] « Rapport des tendances d'attaques de DDoS pour la balise H1 de 2018 », Corero Network Security, s.d., https://info.corero.com/report-2018-half-year-ddos-trends-report-download.html.

2017, et la plus grande attaque jamais enregistrée (1,7 Tbit/s) a frappé un grand fournisseur de services nord-américain en février 2018.[188] Dans la mesure où tout, des entreprises aux organismes publics en passant par l'infrastructure physique des travaux publics, dépend de services ininterrompus liés au DNS, les attaques de DDoS non atténuées sont de plus en plus dangereuses. Les attaques de DDoS sont également devenues plus complexes et les attaques multivecteurs sont désormais les plus utilisées. Verisign a indiqué que 52 % de leurs attaques enregistrées au deuxième trimestre de 2018 étaient des attaques multivecteurs.[189] En outre, l'Internet des objets (IoT) est une préoccupation croissante pour les attaques de DDoS car ces appareils connectés sont des cibles faciles et continuent de proliférer. Le nombre d'appareils connectés était de 27 milliards en 2017 et devrait atteindre les 125 milliards en 2020.[190]

[188] Kevin Whalen, « Entrer dans l'ère du Terabit : préparez-vous à de plus grandes attaques de DDoS », 5 septembre 2018, https://www.netscout.com/blog/entering-terabit-era-get-ready-bigger-ddos-attacks.

[189] « Rapport sur les tendances de DDOS du 2e trimestre de 2018 : 52 pour cent des attaques ont employé plusieurs types d'attaque », blog de Verisign, modifié pour la dernière fois le 27 septembre 2018, https://blog.verisign.com/security/ddos-protection/q2-2018-ddos-trends-report-52-percent-of-attacks-employed-multiple-attack-types/.

[190] John English, « Préparation du réseau pour être à la hauteur des attentes de l'IoT », blog de NETSCOUT, modifié pour la dernière fois le 28 février 2018, https://www.netscout.com/blog/getting-network-ready-meet-iot-expectations.

Annexe F : données de recherche sur la cryptographie

Courbes elliptiques et cryptographie

La cryptographie à courbe elliptique (ECC) offre une alternative à la cryptographie à clé publique RSA utilisée actuellement pour les DNSSEC. La technique est basée sur la théorie de la courbe elliptique, qui peut être utilisée pour créer des clés cryptographiques plus rapides, plus petites et plus efficaces.[191]

La déclaration de pratiques DNSSEC (DPS) de la KSK de la racine fournit des conseils sur la longueur de la clé et son roulement. Cependant, la DPS ne dit rien sur les procédures de modification de l'algorithme de signature numérique. Des recommandations récentes de l'Agence de sécurité nationale des États-Unis recommandent l'utilisation de 3072 bits pour le RSA. L'algorithme EdDSA (Algorithme de sécurité numérique à courbe d'Edwards) semble offrir une meilleure alternative que les clés RSA de très grande taille.[192]

Cryptographie post-quantique

Il y a dix ans, la plupart des gens n'avaient jamais entendu parler de l'informatique quantique mais, ces dernières années, elle a captivé l'imagination du public. Une partie de cet intérêt vient de la puissance de calcul unique d'un ordinateur quantique. L'Académie nationale des sciences des États-Unis a récemment publié un rapport sur [l']« Informatique quantique : progrès et perspectives », où la conclusion générale est qu'il est temps de commencer à se préparer à un avenir quantique sûr.[193]

DigiCert a estimé qu'il faut plusieurs quadrillions d'années pour calculer une clé RSA de 2048 bits à l'aide de la technologie informatique classique.[194] À l'avenir, si un ordinateur quantique à grande échelle était inventé, il pourrait briser la même clé beaucoup plus rapidement, peut-être dans quelques mois seulement. Il reste encore de nombreuses difficultés techniques à surmonter avant de pouvoir construire un ordinateur quantique qui menace le RSA et l'ECC, les deux principaux algorithmes cryptographiques asymétriques utilisés pour sécuriser l'Internet.

Les progrès vers un ordinateur quantique à grande échelle doivent suivre le taux d'évolutivité du nombre de bits quantiques physiques ou de « qubits » dont disposent les ordinateurs et leurs

---

[191] Voir les RFC suivants pour de plus amples informations sur les nouveaux algorithmes potentiels pour les signatures des DNSSEC : P. Hoffman et W. Wijngaards, « Algorithme de signature numérique utilisant des courbes elliptiques (DSA) pour les DNSSEC », RFC 6605, DOI 10.17487/RFC6605, avril 2012, <https://www.rfc-editor.org/info/rfc6605>, O. Sury et R. Edmonds, « Algorithme de sécurité numérique à courbe d'Edwards (EdDSA) pour les DNSSEC », RFC 8080, DOI 10.17487/RFC8080, février 2017, , <https://www.rfc-editor.org/info/rfc8080> et P. Wouters et O. Sury, « Exigences de mise en œuvre de l'algorithme et orientation pour l'utilisation des DNSSEC », RFC 8624, DOI 10.17487/RFC8624, juin 2019, <https://www.rfc-editor.org/info/rfc8624>.

[192] Wouters et Sury, RFC 8624, https://www.rfc-editor.org/info/rfc8624.

[193] Académies nationales des sciences, de l'ingénierie et de la médecine. 2019. Informatique quantique : Progrès et perspectives. Washington, DC : Presse des académies nationales. https://doi.org/10.17226/25196.

[194] Hollebeek, Timothy, « DigiCert sur le quantique : rapport de l'Académie nationale des sciences », blog de DigiCert, 9 janvier 2019, https://www.digicert.com/blog/digicert-on-quantum-national-academy-of-sciences-report/.

taux d'erreur. Les taux d'erreur sont importants car ils ont un impact significatif sur le nombre de qubits physiques nécessaires pour créer un qubit logique. Les qubits physiques sont les systèmes quantiques individuels représentant un zéro ou un un ; cependant, les qubits physiques sont sujets à des erreurs par des interactions inévitables avec leur environnement, même à des températures proches de zéro absolu. Beaucoup de nombreux qubits physiques peuvent être combinés en un qubit logique unique, et les qubits supplémentaires sont utilisés pour détecter et corriger ces erreurs. Les chercheurs n'ont pas encore pu produire même un seul qubit logique, bien que des progrès soient rapidement réalisés vers cet objectif. Une fois les qubits logiques disponibles, le suivi du nombre de qubits logiques sera la mesure à surveiller.

Les groupes de normalisation de l'industrie se préparent également à un avenir post-quantique. L'activité la plus connue est le projet de cryptographie post-quantique du NIST, qui travaille avec des chercheurs du monde entier pour développer de nouvelles primitives cryptographiques qui ne soient pas susceptibles d'être attaquées par des ordinateurs quantiques.[195] On peut s'attendre à ce que ce projet prenne encore plusieurs années avant que les algorithmes qui en résultent ne soient prêts pour la normalisation.

Entre-temps, les chercheurs s'accordent à dire que les signatures basées sur le hachage n'ont pas de danger post-quantique. Le Groupe de travail de la recherche Internet (IRTF) a spécifié ces algorithmes de signature dans son Groupe de recherche sur le Forum Crypto (CRFC), en utilisant de petites clés privées et publiques à faible coût de calcul.[196] Cependant, les signatures sont assez grandes et une clé privée ne peut produire qu'un nombre limité de signatures. Bien que ces algorithmes soient disponibles aujourd'hui, ces deux dernières propriétés rendent les signatures basées sur le hachage indésirables dans l'environnement des DNSSEC.

[195] Institut national des normes et de la technologie (NIST), Laboratoire des technologies de l'information, Centre de ressources pour la sécurité informatique, « Cryptographie post-quantique », créé le 03 janvier 2017, mis à jour le 23 novembre 2020, https://csrc.nist.gov/projects/post-quantum-cryptography.
[196] IRTF, Groupe de recherche sur le Forum Crypto, https://irtf.org/cfrg.

Annexe G : schématisation des recommandations de la SSR2 pour le plan stratégique de l'ICANN des exercices fiscaux 2021 à 2025 et pour les statuts constitutifs de l'ICANN.

Statuts constitutifs de l'ICANN pertinents :

Articles 1.2(a)(i), 1.2(a)(ii) et 27.1(c)(i)(B) des statuts constitutifs sur la préservation et le renforcement de « l'administration du DNS ainsi que la stabilité opérationnelle, la fiabilité, la sécurité, l'interopérabilité mondiale, la résilience et le caractère ouvert du DNS et de l'Internet »,

Article 3.6(a) des statuts constitutifs : aider le Conseil à examiner et à faire rapport sur « les effets matériels possibles, le cas échéant, de sa décision sur l'intérêt public mondial, y compris une discussion des impacts importants sur la sécurité, la stabilité et la résilience du DNS ».

Articles 12.2(b) et 12.2(c) des statuts constitutifs : travailler en étroite collaboration avec le Comité consultatif sur la sécurité et la stabilité et le Comité consultatif sur le système de serveur racine en particulier, et s'assurer que le Conseil d'administration de l'ICANN et l'organisation ICANN exécutent pleinement leurs conseils acceptés.

Annexe G-1 des statuts constitutifs : les sujets, les problématiques, les politiques, les procédures et les principes évoqués à l'article 1.1(a)(i) en ce qui concerne les bureaux d'enregistrement et opérateurs de registre de gTLD sont : « les problèmes pour lesquels une résolution uniforme ou coordonnée serait raisonnablement requise pour faciliter l'interopérabilité, la sécurité et / ou la stabilité de l'Internet, des services de bureau d'enregistrement, des services de registre, ou du DNS » et « la sécurité et la stabilité de la base de donnée de l'opérateur de registre pour un TLD ».

Buts et objectifs pertinents du plan stratégique

Tiré du plan stratégique de l'ICANN pour les exercices fiscaux 2021 à 2025.[197]

1. Renforcer la sécurité du système des noms de domaine et du système de serveurs racine du DNS.

1.1 Améliorer la responsabilité commune de maintien de la sécurité et la stabilité du DNS en renforçant la coordination du DNS en partenariat avec les parties prenantes concernées.
1.2 Renforcer la gouvernance des opérations des serveurs racine du DNS en coordination avec les opérateurs des serveurs racine du DNS.
1.3 Identifier et atténuer les menaces à la sécurité du DNS via le renforcement des relations avec les fournisseurs de matériel, de logiciels et de services concernés.

[197] Plan stratégique de l'ICANN pour les exercices fiscaux 2021 à 2025, https://www.icann.org/en/system/files/files/strategic-plan-2021-2025-24jun19-en.pdf.

1.4 Renforcer la solidité des services et processus de signature et de distribution de la clé de la zone racine du DNS.

2. Objectif stratégique : renforcer l'efficacité du modèle de gouvernance multipartite de l'ICANN

2.1. Renforcer le processus ascendant et multipartite de prise de décision de l'ICANN et s'assurer que le travail soit accompli et que les politiques soient élaborées de manière efficace et en temps opportun.
2.2 Soutenir et renforcer la participation active, éclairée et efficace des parties prenantes.
2.3 Maintenir et améliorer l'ouverture, l'inclusion, la responsabilité et la transparence.

3. Objectif stratégique : faire évoluer les systèmes d'identificateurs uniques en coordination et en collaboration avec les parties concernées afin de répondre aux besoins des internautes du monde entier.

3.1 Stimuler la concurrence, le choix du consommateur et l'innovation dans l'espace Internet en renforçant la sensibilisation à l'acceptation universelle, aux IDN et à l'IPV6, et en encourageant leur utilisation et mise en œuvre.
3.2 Améliorer l'évaluation et la réactivité face à des nouvelles technologies qui ont un impact sur la sécurité, la stabilité et la résilience des systèmes d'identificateurs uniques de l'Internet grâce à un plus grand engagement auprès des parties concernées.
3.3 Continuer à assurer et à améliorer les fonctions IANA dans un souci d'excellence opérationnelle.
3.4 Soutenir l'évolution continue des systèmes d'identificateurs uniques de l'Internet par le biais du lancement d'une nouvelle série de gTLD financée et gérée de manière raisonnable, avec des risques évalués et conforme aux processus de l'ICANN.

4. Objectif stratégique : résoudre des problèmes géopolitiques ayant un impact sur la mission de l'ICANN visant à garantir un Internet unique et interopérable à l'échelle mondiale.

4.1 Identifier les défis et opportunités qui se présentent à l'échelle mondiale et y répondre dans le cadre de sa mission, en développant de nouveaux systèmes d'alerte précoce, tels que les rapports sur l'évolution des lois et réglementations à l'échelle mondiale préparés par l'ICANN.
4.2 Continuer d'établir des alliances au sein de l'écosystème de l'Internet et au-delà afin d'échanger avec les parties prenantes mondiales et les sensibiliser à la mission et au travail d'élaboration de politiques de l'ICANN.

5. Objectif stratégique : assurer la durabilité financière à long terme de l'ICANN.

5.1 Mettre en œuvre un plan financier quinquennal en appui au plan opérationnel quinquennal.
5.2 Développer des projections financières fiables et prévisibles.
5.3 Gérer les opérations et leurs coûts de façon à optimiser l'efficacité et l'efficience des activités de l'ICANN.
5.4 Veiller à ce que les réserves de l'ICANN soient en permanence constituées, atteintes et tiennent compte de la complexité et des risques de l'environnement de l'ICANN.

Nº	Recommandation	Objectif et buts stratégiques
1	Compléter la mise en œuvre de toutes les recommandations de la SSR1 pertinentes	Objectifs stratégiques 1, 2 et 3
2	Recommandation 2 de la SSR2 : désigner un cadre responsable de la sécurité stratégique et tactique et de la gestion des risques	Objectifs stratégiques 1, 3 et 4
3	Recommandation 3 de la SSR2 : améliorer la transparence budgétaire liée à la sécurité, la stabilité et la résilience	Objectifs stratégiques 1, 2, 3 et 5 ; et buts stratégiques 2.1 et 3.4
4	Recommandation 4 de la SSR2 : améliorer les processus et les procédures de gestion des risques	Objectifs stratégiques 1, 2, 3, 4 et 5
5	Recommandation 5 de la SSR2 : se conformer aux systèmes de gestion de la sécurité de l'information et des certifications de sécurité	Objectif stratégique 1 :
6	Recommandation 6 de la SSR2 : divulgation et transparence de la vulnérabilité de la SSR	Objectifs stratégiques 1, 2, 3 et 4 ; et buts stratégiques 1.1, 1.2, 1.3 et 4.1
7	Recommandation 7 de la SSR2 : améliorer les processus et procédures de continuité des opérations et de reprise après sinistre	Objectifs stratégiques 1, 3 et 4 ; et buts stratégiques 1.1, 1.4 et 3.3
8	Recommandation 8 de la SSR2 : permettre et démontrer la représentation de l'intérêt public dans les négociations avec les parties contractantes	Objectifs stratégiques 1 et 3 ; et buts stratégiques 1.1, 1.2, 1.3 et 1.4
9	Recommandation 9 de la SSR2 : surveiller et appliquer la conformité	Objectifs stratégiques 1, 2 et 3 ; et but stratégique 2.1
10	Recommandation 10 de la SSR2 : clarifier les définitions des termes relatifs à l'utilisation malveillante	Objectif stratégique 1 :
11	Recommandation 11 de la SSR2 : résoudre les problèmes d'accès aux données CZDS	Objectif stratégique 3 ; et but stratégique 3.2
12	Recommandation 12 de la SSR2 : réviser les efforts d'analyse et de signalement de l'utilisation malveillante du DNS pour permettre la transparence et la révision indépendante	Objectifs stratégiques 1, 2, 3, 4 et 5
13	Recommandation 13 de la SSR2 : accroître la transparence et la responsabilité du signalement des plaintes pour abus	Objectifs stratégiques 1 et 3 ; et but stratégique 2.1
14	Recommandation 14 de la SSR2 : créer une spécification temporaire pour les améliorations	Objectif stratégique 1 ; et but stratégique 1.1

	de la sécurité fondées sur des données factuelles	
15	Recommandation 15 de la SSR2 : lancer un EPDP fondé sur des données factuelles pour améliorer la sécurité	Objectif stratégique 1 ; et but stratégique 1.1
16	Recommandation 16 de la SSR2 : exigences de confidentialité et RDS	Objectifs stratégiques 1, 3 et 5
17	Recommandation 17 de la SSR2 : mesure des collisions de noms	Objectifs stratégiques 1, 3 et 4 ; et but stratégique 3.4
18	Recommandation 18 de la SSR2 : informer les débats sur les politiques	Objectifs stratégiques 1, 3 et 4 ; et but stratégique 3.2
19	Recommandation 19 de la SSR2 : développement complet d'un test de régression du DNS	Objectif stratégique 1 ; et buts stratégiques 1.1, 1.2, 1.3 et 1.4
20	Recommandation 20 de la SSR2 : procédures officielles pour les roulements de clé	Objectifs stratégiques 1, 2 et 4 ; et but stratégique 1.4
21	Recommandation 21 de la SSR2 : améliorer la sécurité des communications avec les opérateurs de TLD	Objectif stratégique 1 et but stratégique 3.3
22	Recommandation 22 de la SSR2 : mesures du service	Objectifs stratégiques 1, 2, 3, 4 et 5 ; et buts stratégiques 1.1, 1.2, 2.1, 3.2, 3.4 et 4.1
23	Recommandation 23 de la SSR2 : roulement de l'algorithme	Objectifs stratégiques 1 et 3
24	Recommandation 24 de la SSR2 : améliorer la transparence et les tests de bout en bout pour le processus EBERO	Objectif stratégique 1 ; et but stratégique 1.2

Annexe H : analyse des commentaires publics

L'équipe de révision SSR2 a créé une feuille de calcul pour enregistrer sa réponse aux commentaires publics et aux changements résultant des commentaires publics. Le fichier est disponible sur la page du wiki de la SSR2 consacrée aux documents et aux brouillons de l'équipe de révision ou peut être téléchargé directement suivant les liens ci-dessous.

Excel :
https://community.icann.org/pages/viewpage.action?pageId=64076120&preview=/64076120/155191048/Public%20Comment%20Feedback%20-%20March%202020.xlsx

PDF :
https://community.icann.org/pages/viewpage.action?pageId=64076120&preview=/64076120/155191042/Public%20Comment%20Feedback%20-%20March%202020.pdf

Annexe I : fiches d'information

L'organisation ICANN publie des fiches d'information et de frais trimestrielles, ainsi que des mises à jour mensuelles relatives à la participation et aux jalons. Ces documents témoignent de la transparence et la responsabilité face à la communauté sur la manière dont sont utilisés le temps et les ressources de l'équipe de révision.

La fiche d'information présente l'assistance des membres de l'équipe de révision, les coûts associés aux services professionnels et aux déplacements pour assister à des réunions en personne, les jalons et la participation.

En voici les définitions :

Services professionnels : budget approuvé pour que l'équipe de révision utilise les services d'experts indépendants, tel qu'établi dans l'article 4.6(a)(iv) des statuts constitutifs. Les équipes de révision pourront solliciter et sélectionner des experts indépendants afin qu'ils fournissent des conseils si elles les demandaient. L'ICANN prendra en charge les frais et dépenses raisonnables liés au recours à de tels experts pour chaque révision prévue par cet article 4.6 à condition que ces frais et dépenses ne dépassent pas le budget alloué à cette révision. Les directives relatives à la façon dont les équipes de révision doivent collaborer avec les experts indépendants et à la manière dont elles doivent traiter les conseils fournis sont établies dans les Normes opérationnelles.

Services de voyage : montant approuvé pour les déplacements de l'équipe de révision pour les réunions en personne. Les exemples des dépenses liées aux déplacements incluent - mais sans y être limitées - les frais des billets d'avion, l'hôtel, le remboursement de l'indemnité journalière, les coûts des installations pour les réunions, l'équipement technique et audiovisuel et le service de restauration. Ces dépenses comprennent le déplacement de l'équipe de révision et de soutien de l'organisation ICANN.

Soutien de l'organisation ICANN : montant approuvé dans le budget pour que l'organisation ICANN externalise des services pour soutenir le travail de l'équipe de révision.

Dépenses à ce jour : les montants comprennent les états financiers trimestriels depuis que l'équipe de révision commence le travail jusqu'à la fin du trimestre le plus récent.

Services engagés :
1. Services de voyage : dépenses estimées pour des réunions en personne approuvées.
2. Services professionnels : services concernant des contrats signés et devant être fournis ou facturés.

Il s'agit typiquement de services de soutien fournis non pas par des employés mais par des sous-traitants. Total

Dépensé et engagé à ce jour : il s'agit de la somme des « dépenses à ce jour » et des « services engagés » jusqu'à la fin du dernier trimestre Le montant des services engagés ne comprend pas les sommes dépensées à ce jour. Budget restant : Il s'agit de la différence entre les montants du « budget approuvé » et celui du « total dépensé et engagé à ce jour ».

Les archives des fiches d’information peuvent être consultées à l’adresse suivante : https://community.icann.org/x/S7zRAw.