Initiatives proposées pour une sécurité, une stabilité et une résilience améliorées du DNS

Présentées par

La Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN)

Publié pour consultation publique.

12 février 2010

Initiatives proposées pour une sécurité, une stabilité et une résilience améliorées du DNS

1. Vue d'ensemble

Ce document présente la logique, les attributs clés et les projections de coûts de deux initiatives stratégiques liées à la sécurité, la stabilité et la résilience du système de noms de domaine (DNS) que l'ICANN estime nécessaires afin de remplir ses obligations selon ses règlements, l'affirmation d'engagements de 2009 et le plan stratégique de l'ICANN pour 2010-2013. Ce document est une base à la discussion multi-parties prenantes des initiatives proposées, des responsabilités de l'ICANN en matière d'établissement des capacités proposées et de la manière selon laquelle la communauté pourrait procéder en organisant les efforts afin de soutenir de telles initiatives. L'encadrement de haut niveau et les implications relatives aux ressources sont identifiés, mais les alternatives de financement de ces initiatives ne sont pas analysées.

Note : Ces initiatives sont proposées en tant qu'efforts s'ajoutant à ceux identifiés dans le cadre du plan opérationnel et budget de l'ICANN pour l'exercice 2011, publié pour discussion à la conférence de Nairobi.

2. Hypothèses

2.1 Le système de noms de domaine est devenu un service sous-jacent essentiel alimentant l'Internet. Le DNS permet la résolution de nom pour les utilisateurs du Web et sous-tend la messagerie électronique, la messagerie textuelle, la communication vocale par Internet et d'autres services et protocoles Internet essentiels. En même temps, le DNS existe dans un environnement de menaces et de risques croissants. Les opérations techniques du système sont exposées à une variété d'attaques telles que les attaques par déni de service ou par saturation (DDoS) à l'encontre des serveurs et résolveurs de noms qui font autorité, à des niveaux allant jusqu'à et incluant les serveurs de noms racine ; les attaques par empoisonnement de cache qui affectent l'intégrité de la résolution du DNS tel que décrit par le chercheur en sécurité Dan Kaminsky ; et d'autres méthodes, le piratage psychologique inclus, qui permettent à des attaques malveillantes de mal orienter et d'abuser des services du DNS. De plus, scélérats et criminels exploitent la dépendance des utilisateurs vis-à-vis du DNS et utilisent le système de diverses façons pour mener toutes sortes d'activités malveillantes.

2.2 Actuellement, la communauté d'opérateurs qui fournissent des services DNS collabore activement avec les vendeurs, les chercheurs en sécurité, les équipes d'application de la loi et d'intervention, afin de réagir aux menaces naissantes d'une manière en grande partie ad hoc. Des initiatives existent au sein de la communauté DNS pour améliorer le partage d'informations, l'identification d'activités malveillantes et le renforcement de la collaboration en ce qui concerne les attaques DDoS et autres visant l'ensemble du système. Ces efforts collaboratifs impliquent en général des efforts déployés par les membres de la communauté DNS et sécurité qui se réunissent de manière bénévole pour traiter les situations naissantes. Plusieurs appels à action sur le traitement et la

réduction des risques systémiques pour le DNS ont été faits au cours de l'année passée.[1] La fréquence et la gravité de ces appels à action révèlent un besoin croissant pour une appréciation des risques dans tout le système, des plans d'urgence et des capacités de réaction permanente.

2.3 Les efforts actuels de traitement de la variété de menaces et de risques pour le DNS ne sont pas concentrés de manière systémique. A un niveau opérationnel, des opérateurs versés en matière de sécurité au sein du DNS et forts en ressources, ont développé des mécanismes puissants pour comprendre les menaces et prendre des mesures qui réduisent les risques pour eux et leurs clients. Toutefois, la collaboration dans ce domaine ne s'étend pas en général aux opérateurs de DNS moins capables et moins bien financés et aux autres parties prenantes qui ne sont pas conscientes des menaces et des risques et qui n'ont pas d'aptitude à réagir de manière appropriée lorsque de telles menaces à la sécurité, la stabilité et la résilience se présentent. De plus, les efforts existants ont prouvé qu'une concentration soutenue sur la surveillance, la réponse et la réparation, était nécessaire pour affronter des menaces non accessibles à des remèdes techniques faciles à localiser. A un niveau supérieur, le DNS manque de points centraux couvrant l'ensemble du système pour la reddition de comptes liée aux capacités clés en matière d'appréciation du risque, de plans et d'exercices d'urgence et de réponse soutenue et dédiée. De telles activités doivent considérer le DNS de manière holistique et répondre aux besoins des composantes et opérateurs individuels.

2.4 Au fond, ces types de capacités ne peuvent totalement dépendre des efforts de volontaires agissant sans soutien organisationnel dédié, approches opérationnelles très au point et engagements de finances à long terme. Les efforts pour assurer la stabilité et la résilience du DNS doivent atteindre des niveaux de performance et de responsabilisation en ligne avec d'autres aspects critiques de l'infrastructure des communications, nécessitant des niveaux similaires d'investissement en matière de personnel à temps plein et de soutien.

3. Le rôle et les responsabilités de l'ICANN

3.1 Le DNS doit fonctionner de manière sûre, stable et résiliente. L'ICANN a de nombreux engagement qui exigent qu'elle entreprenne des efforts afin de réaliser cet objectif. L'article I des règlements de l'ICANN stipule que « La mission de l'ICANN est de coordonner, à un niveau général, les systèmes mondiaux d'identificateurs uniques de l'Internet, et notamment d'assurer la stabilité et la sécurité d'exploitation des systèmes d'identificateurs uniques de l'Internet ». L'affirmation d'engagements de 2009 (http://icann.org/en/announcements/announcement-30sep09-en.htm) affirme que le DNS sert en tant que fonction critique au sein de l'environnement de l'Internet et de ce fait, les risques liés à l'exploitation doivent être judicieusement gérés. L'ICANN s'est engagée à « préserver la sécurité, la stabilité et la résilience du DNS ». L'affirmation

[1] Voir http://www.enisa.europa.eu/media/press-releases/improving-resilience-3-tips, et http://www.enisa.europa.eu/media/press-releases/guide-to-mitigate-vulnerabilities-threats-cyber-attacks, et http://www.it-scc.org/documents/itscc/IT-SCC_ITSRA_Release_08_21_09_clean_final2.pdf.

exige de plus de la part de l'ICANN qu'elle identifie les menaces actuelles et futures et mette en place une planification d'urgence appropriée.

3.2 L'implication de ces engagements pour l'ICANN est claire. L'affirmation d'engagements requiert que l'ICANN entreprenne des efforts collaboratifs afin d'identifier et de réduire les risques pour la sécurité et la résilience à travers un système de DNS réparti, qui comprend un vaste éventail de parties prenantes qui exploitent et utilisent les services de DNS.[2] Compte tenu de la nature du DNS, des opérations fiables et résilientes du système de serveurs racine et des noms de domaine de premier niveau doivent constituer une priorité de premier ordre. La croissance du DNS de par l'accroissement naturel de l'utilisation, et l'introduction de nouvelles technologies et propositions pour établir de nouveaux domaines de premier niveau (y compris ceux utilisant des noms de domaine internationalisés) exigent de plus que l'ICANN comprenne et cherche à réduire les risques menaçant le système. Il est important de noter que l'ICANN a cherché à améliorer la sécurité, la stabilité et la résilience du DNS depuis ses débuts. Le *Plan pour le renforcement de la sécurité, stabilité et résilience de l'Internet* de l'ICANN (http://www.icann.org/en/announcements/announcement-2-21may09-en.htm) aborde une large variété d'activités et de programmes existants. Les initiatives ébauchées dans ce document traitent des efforts supplémentaires que l'ICANN doit entreprendre afin de répondre à ces engagements.

3.3 Les impératifs consistant à améliorer la compréhension et la réduction systémiques des risques pour le DNS et à répondre à ses engagements nécessiteront de l'ICANN qu'elle collabore avec la communauté du DNS afin d'entamer un travail supplémentaire qui tire parti aussi bien des efforts passés que de la collaboration actuelle. A cette fin, le plan stratégique de l'ICANN pour 2010-2013 fait de l'amélioration de la stabilité, sécurité et résilience du DNS, l'une des quatre zones de concentration de l'ICANN au cours de ladite période. Le plan stratégique aborde en particulier l'exigence pour l'ICANN d'établir une approche pour une équipe de réponse aux urgences informatiques du système de noms de domaine (DNS-CERT) ainsi que pour une planification et des exercices d'urgence concernant le DNS. L'ICANN cherche à avancer pour assurer la mise en place d'approches qui concernent l'ensemble du système afin d'évaluer les risques, de mettre en place des plans d'urgence contre les menaces potentielles et d'orchestrer des capacités de réponse aux incidents en collaboration afin d'améliorer la sécurité, la stabilité et la résilience globales du système de DNS. L'ICANN prévoit également d'entamer des efforts visant à améliorer les critères de mesure couvrant l'ensemble du système afin que la communauté du DNS puisse jouir d'une meilleure compréhension de la sécurité, stabilité et résilience du DNS, prévoir les défis et répondre de manière effective.

[2] En programmant d'assumer son rôle dans la gestion des risques pour la sécurité, la stabilité et la résilience du DNS, l'ICANN n'aborde pas des problématiques liées à la compétition de sécurité nationale entre les états dans le domaine de la guerre de l'information ou de l'espionnage ou de gestion du contrôle de contenus hébergés sur Internet, tel que ceci est traité dans le plan de l'ICANN pour le renforcement de la sécurité, stabilité et résilience de l'Internet. Voir http://www.icann.org/en/topics/ssr/ssr-draft-plan-16may09-en.pdf).

3.4 L'utilité potentielle et le succès opérationnel des initiatives ébauchées ci-dessous nécessiteront le soutien et l'engagement de la communauté. La révision de la part de la communauté, les retours d'informations et la planification liés à la mise en œuvre de ces initiatives seront intégrés dans les processus de budgétisation et de planification opérationnelle de l'ICANN.

4. Risques pour l'opération du DNS

4.1 A l'aube de l'année 2010, l'écosystème de l'Internet demeure plein de vie. L'activité sur Internet reflète de plus en plus la gamme complète de motivations et comportements humains. En partie, une telle activité reflète le caractère ouvert qui a fait le succès d'Internet, qui a permis d'aiguiser l'innovation et de favoriser la communication, la créativité et le commerce au sein d'un patrimoine commun. L'écosystème est également menacé par les niveaux croissants d'activité malveillante menée par une variété d'acteurs et il existe de fortes indications que la participation d'organisations criminelles se trouve en expansion rapide. Le paysage des menaces comprend la fraude, l'extorsion et d'autres activités illicites en ligne, qui sapent la confiance de l'utilisateur dans les services basés sur Internet, les attaques par déni de service (DoS) et d'autres activités perturbatrices qui déstabilisent l'infrastructure de l'Internet. Notamment, la capacité de certains acteurs malveillants à mener des attaques contre le fonctionnement du DNS lui-même et la facilité et la fréquence avec laquelle ces acteurs utilisent autant les résolutions de noms que les services d'enregistrement pour faciliter une série d'activités malveillantes ou criminelles, présentent des risques croissants pour le fonctionnement correct de l'Internet et mettent en question l'intégrité et la fiabilité de l'Internet en tant que plateforme mondiale de communications.

4.2 Il existe trois catégories principales de risques pour la sécurité, la stabilité et la résilience : les activités malveillantes (attaques contre le DNS ou attaques qui exploitent les résolutions de noms ou les systèmes d'enregistrement), les risques techniques menaçant la stabilité du DNS, et les risques organisationnels liés au DNS.

4.2.1 Risques d'activités malveillantes

4.2.1.1 A la base, le risque principal préoccupant l'ICANN est la disponibilité du DNS à résoudre les noms et à faciliter une grande variété de transactions à travers l'Internet. Une menace majeure à la disponibilité peut provenir sous forme d'attaques DoS contre les opérateurs de services DNS à divers niveaux des systèmes. L'impact des attaques DoS dépend autant des types de services ciblés que de la sophistication et du volume de trafic de l'attaque. Au cours de la dernière décennie, les opérations de serveurs racine ainsi que les domaines de premier niveau (TLD) ont été directement attaqués. Quatre cas sont remarquables : 1) le 21 octobre 2002, le premier cas documenté d'attaque coordonnée contre les treize serveurs racine du DNS a eu lieu (http://d.root-servers.org/october21.txt) ; 2) en février 2006, des attaques ont eu lieu contre des serveurs de noms gérés par un fournisseur clé de services de noms de domaine de premier niveau (http://www.icann.org/en/committees/security/dns-ddos-advisory-31mar06.pdf) ; 3) en février 2007, une attaque a eu lieu contre six des treize serveurs racine du DNS (http://www.icann.org/en/announcements/factsheet-dns-attack-

08mar07.pdf) ; 4) plus récemment, en décembre 2009, les attaques DoS contre des fournisseurs de DNS ont fait de nouveau la une lorsqu'une attaque contre le service UltraDNS de NeuStar a touché plusieurs sites de commerce électronique (http://www.cnn.com/2009/TECH/12/24/cnet.ddos.attack/index.html). Cette histoire d'attaques démontre l'accroissement continu en ressources à la disposition de ceux qui mènent les attaques ainsi que la sophistication des auteurs.

4.2.1.2 Des efforts considérables pour réduire ces risques sont en cours. Ils consistent en l'allocation automatique de bande passante afin de parer aux DDoS et la mise en place et le déploiement de technologies et de méthodologies telles que l'envoi à la cantonade, où les données sont acheminées vers la meilleure destination ou la destination la plus proche. Comme exemple de déploiement de solutions d'envoi à la cantonade, le système de serveurs racine du DNS a passé d'une présence en treize lieux (systèmes) à une présence en plus de deux cents lieux (voir les détails sur http://www.root-servers-org). Il existe également des niveaux croissants de planification et de collaboration parmi les opérateurs de DNS, avec la mise en place d'organisations telles que le centre de recherche et d'analyses de l'opération du DNS (DNS-OARC) (http://www.dns-oarc.org), le groupe de sécurité Internet des registres (RISG) (http://registrysafety.org/website/) ainsi que des efforts visant à comprendre les risques associés au DNS tels que le symposium mondial pour la sécurité, la stabilité et la résilience du DNS (http://www.gtisc.gatech.edu/pdf/DNS_SSR_Symposium_Summary_Report.pdf). Toutefois, les menaces sont elles aussi en croissance puisque des botnets de plus en plus larges contrôlés par des criminels et autres acteurs malveillants posent le risqué d'attaques très importantes en termes de sophistication et d'échelle. La planification visant à affronter de telles perturbations doit également parer à la possibilité de perturbation des services de DNS suite à des attaques malveillantes menées contre des systèmes desquels dépend le DNS et allant de l'alimentation en courant au routage Internet.

4.2.1.3 La nature ouverte et distribuée de l'exploitation du DNS, alliée à l'administration largement répartie des serveurs et résolveurs de noms, expose les utilisateurs à un nombre de risques supplémentaires. Le protocole DNS (sans utilisation d'extensions de sécurité) est vulnérable aux attaques qui utilisent le *détournement* des requêtes. En particulier, l'attaque renvoie de fausses informations en réponse à une requête DNS (usurpation ou détournement, *poisoning* ou *pharming*) ou des informations différentes de celles voulues par l'autorité du nom de domaine (redirection ou modification de réponse). De telles attaques trompent les utilisateurs du DNS d'une multitude de façons : en dirigeant les utilisateurs vers des sites Web à contenu frauduleux ou à code malveillant, en faisant en sorte que les courriels apparaissent provenir de sources pastiches et ainsi de suite. Les techniques mises en œuvre pour l'exécution d'attaques qui permettraient une usurpation systématique de caches DNS et ainsi, un détournement de trafic Internet, présentent des occasions aux activités malveillantes qui peuvent représenter des risques pour l'intégrité du DNS en tant qu'ensemble.

4.2.1.4 Les services d'enregistrement des noms de domaine fournissent un autre vecteur d'attaque aux scélérats. Les attaquants exploiteront les faiblesses techniques (vulnérabilités du site Web) ou opérationnelles d'un bureau d'enregistrement ou d'un titulaire de nom de domaine (personnel qui peut être victime de piratage psychologique) afin d'acquérir le contrôle non autorisé d'un compte d'enregistrement de nom de domaine (pour plus de détails, voir SAC040 http://www.icann.org/en/committees/security/sac040.pdf). Lorsqu'il a le contrôle du compte d'enregistrement piraté, l'attaquant modifie la configuration DNS de, potentiellement, tous les domaines dans un compte piraté pour les acheminer vers un serveur de nom contrôlé par l'attaquant. Ce dernier obtient ainsi le contrôle de la résolution de nom du Web du domaine fragilisé, de la messagerie électronique et des autres applications Internet. De telles attaques de piratage de noms de domaine ou de comptes sont utilisées pour le défacement de sites Web, la perturbation de services de messagerie électronique ou autres offerts par le titulaire, ou pour capturer des informations confidentielles ou personnelles.

4.2.1.5 Alors que le DNS est conçu pour servir les utilisateurs d'Internet, il est malheureusement également exploité par des scélérats pour faciliter une grande variété de comportements criminels et frauduleux. La conséquence non voulue est parfaitement illustrée par la manière selon laquelle le DNS est exploité pour faciliter une activité malveillante communément appelée *hameçonnage.* Les hameçonneurs enregistrent des noms de domaine dans le but spécifique de soutenir des attaques lancées à partir de réseaux d'ordinateurs fragilisés ou infectés par un *bot*, appelés « réseaux de bots » ou « *botnets* ». L'attaquant utilise souvent certains de ces noms de domaine malveillants pour opérer un *DNS de crime*, une collection de résolveurs de DNS qui sont spécifiquement programmés et déployés pour résoudre des requêtes DNS émises par des victimes d'hameçonnage. D'autres noms de domaine malveillants sont utilisés pour héberger des sites Web dont l'identité a été usurpée. Les réponses à la requête DNS d'une victime pour le nom de domaine apparemment légitime d'une institution financière, d'un site de commerce électronique, d'une agence gouvernementale ou d'une entité similaire dirigent cette victime vers un site Web trompeur ou à identité usurpée. De manière tout à fait innocente, la victime interagit avec ce site trompeur comme elle l'aurait fait normalement avec les sites légitimes des institutions financières, des sites de commerce électronique, des organisations caritatives ou des agences gouvernementales. Ces sites malveillants sont toutefois conçus pour voler des identités, des informations de comptes bancaires et de cartes de crédit et pour vendre des produits illégaux ou factices à la victime, pour escroquer les organisations caritatives et autres activités malveillantes. [3]

4.2.1.6 De plus en plus, le DNS joue également un rôle prédominant dans la favorisation des « réseaux de bots à louer », à savoir des réseaux d'attaque offerts au service dans une économie clandestine florissante. Des botnets composés de centaines de milliers ou

[3] Conseil gouvernemental de coordination des technologies de l'information, Ministère de la sécurité publique des Etats-Unis. 2009. Évaluation des risques de référence du secteur des technologies de l'information. Washington, DC : Imprimerie du gouvernement, pp 32-33.

même de millions d'ordinateurs infectés (bots) sont contrôlés à distance pour exécuter beaucoup de types d'attaques malveillantes (par ex. des DDoS) ou soutenir des activités criminelles (traite d'êtres humains, distribution de médicaments illégaux, pourriels, et activités similaires). Pour contrôler les bots de manière efficace et avec une résilience considérable contre les contremesures mises en place par les praticiens de la sécurité et les agents d'application de la loi, les attaquants programment les bots de sorte que ces derniers utilisent le DNS pour identifier l'adresse de commande centralisée ou les points de rendez-vous qui émettent les commandes à l'adresse des bots. Récemment, certains programmes malveillants tels que les variantes du programme malveillant Conficker, ont utilisé des approches qui cherchaient à dépendre de séries de noms de domaine prédéterminés comme aspect clé du contrôle des bots.

4.2.2 Risques techniques

4.2.2.1 L'opération ou l'intégrité du DNS peut être défavorablement influencée si l'utilisation répandue de pratiques opérationnelles douteuses résultait en une perturbation de service, ou si un changement technique résultait en une vulnérabilité non prévue que les scélérats ou criminels exploiteraient pour faciliter des activités malveillantes. Des cas illustrant ce dernier type de problèmes et la manière grandement réactive selon laquelle de tels problèmes sont actuellement gérés, ont eu lieu en 2008. L'expert en sécurité Daniel Kaminsky a découvert une vulnérabilité sérieuse dans le protocole DNS, et a par la suite publiquement démontré qu'une pratique appelée modification de réponse du DNS pouvait être exploitée par les attaquants pour pirater des sites Web de grandes sociétés en utilisant des services d'hébergement Web totalement hors de la portée administrative de ces organisations. Le comité consultatif pour la sécurité et la stabilité de l'ICANN (SSAC) a ensuite publié un document consultatif d'avertissement contre la menace potentielle d'une modification de réponse du DNS à l'adresse de la communauté (http://www.icann.org/en/committees/security/ sac032.pdf). Des systèmes ad hoc ont été mis en place pour que les opérateurs et les utilisateurs du DNS puissent tester leurs systèmes en matière de vulnérabilité et prendre des mesures préventives ou correctives. La communauté de l'ICANN a démarré et poursuit plusieurs initiatives qui pourraient contribuer à une divulgation plus coordonnée des menaces de la sorte liées au DNS et à une réponse plus organisée à ces menaces. Ceci inclut la coopération de l'ICANN avec des partenaires pour réaliser des symposiums annuels qui rassemblent des experts afin d'étudier le paysage des menaces, d'évaluer conjointement les risques et de faire des recommandations visant à gérer ces risques. Le premier symposium a eu lieu en février 2009 en collaboration avec le *Georgia Tech Information* Security *Center* (*GTISC*).

4.2.2.2 L'opération du DNS peut être aussi défavorablement influencée si des changements techniques du DNS modifient le comportement du système ou résultent en des charges de trafic qui nécessitent des changements considérables en matière de capacité courante ou prévue. Afin de réduire le potentiel d'adoption de pratiques opérationnelles qui puissent perturber la sécurité et la stabilité du DNS au niveau des domaines de premier niveau, le Conseil d'administration de l'ICANN a mis en œuvre en 2009, des démarches visant à interdire l'utilisation de redirection compte tenu des

risques que cette pratique pose pour la stabilité du DNS tel qu'identifié par le comité consultatif pour la sécurité et la stabilité (SAC041 http://www.icann.org/en/committees/security/sac041.pdf).[4] En 2010, la communauté du DNS poursuivra la révision complète des impacts potentiels qui pourraient résulter d'une série de changements proposés au niveau de la racine du DNS : la mise en œuvre des extensions de sécurité du système de noms de domaine (DNSSEC), la mise en œuvre des IPv6 et le besoin d'enregistrements glue des IPv6 à ajouter au fichier de zone racine, l'introduction de la procédure accélérée pour permettre l'utilisation de labels de noms de domaine internationalisés (IDN) au premier niveau du DNS et l'introduction de nouveaux domaines de premier niveau.

4.2.3 Défaillances en matière d'organisation

4.2.3.1 L'incapacité potentielle d'organisations qui accomplissent des rôles clés dans l'opération du DNS à fonctionner de manière effective constitue également une catégorie de risques importante. Au cœur du DNS, la capacité de l'ICANN, des opérateurs de serveurs racine, des registres de TLD et des bureaux d'enregistrement à fournir des services sans interruption, est essentielle à la sécurité et la stabilité globales du DNS. Chacune de ces entités est individuellement responsable de sa propre viabilité financière, continuité d'entreprise et gestion du risque. Mais au niveau du système, des dispositions doivent être prises pour parer aux imprévus lorsqu'une organisation ne peut plus exécuter sa fonction de manière appropriée et pour faire en sorte que les services soient rétablis, perpétués ou reconstitués afin d'assurer des opérations continues et efficaces du DNS et afin de protéger les titulaires de noms de domaine.

4.2.4. Mesurer le risque et la sécurité, stabilité et résilience.

4.2.4.1 Actuellement, il n'existe pas de consensus réel quant aux mesures correctes et aux niveaux de performance acceptables du système en tant qu'ensemble, en ce qui concerne les risques et la sécurité, stabilité et résilience. Des opérateurs individuels et des chercheurs indépendants ont mesuré divers aspects du DNS mais à ce jour, peu de progrès ont été réalisés dans la définition et la mise en œuvre de critères de mesure standard de l'ensemble du système ou de niveaux de service acceptables. Les efforts visant à améliorer la gestion des risques liés à la sécurité, la stabilité et la résilience du DNS doivent être guidés par une capacité améliorée de mesurer ces caractéristiques et d'évaluer l'utilité des programmes et des investissements de ressources.

4.2.4.2 Un élément clé qui favoriserait l'amélioration de cette situation sera de garantir que les diverses parties des opérations du DNS sont correctement orchestrées et mesurées. Le rapport de 2009 de l'équipe d'étude des serveurs racine (RSST) sur l'extensibilité de la racine (http://www.icann.org/en/committees/dns-root/root-scaling-study-report-31aug09-en.pdf) réclame « la mise en place de mécanismes efficaces pour la détection et la réduction des risques à mesure que ces derniers deviennent visibles » liés au système de serveurs racine. La mise en place de critères de mesure et d'équipement

[4] Conseil gouvernemental de coordination des technologies de l'information, Ministère de la sécurité publique des Etats-Unis. 2009. Évaluation des risques de référence du secteur des technologies de l'information. Washington, DC : Imprimerie du gouvernement, pp 32-33.

donne lieu à certains défis intéressants. Notamment, la nature distribuée du DNS réclame un modèle de mesure conjoint, nécessitant la participation d'acteurs et d'organisations multiples. Le thème des systèmes d'alerte précoce de l'Internet est en cours d'étude au sein de forums variés, y compris l'agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), qui organise son premier atelier sur l'alerte précoce de l'Internet et l'intelligence des réseaux en mars 2010 (http://www.enisa.europa.eu/events/ee/ EWNI2010). L'ICANN conjointement avec l'université de Kyoto, a tenu son deuxième symposium mondial sur la sécurité, la stabilité et la résilience du DNS en février 2010, avec un accent particulier sur la mesure. L'ICANN prévoit d'encourager et de participer à des activités qui amélioreront l'état de compréhension de la manière de mesurer les risques pour le DNS et la santé, la sécurité, la stabilité et la résilience du système en tant qu'élément fondamental favorisant la mise en place d'une évaluation des risques efficace, d'exercices et de plans d'urgence et de capacités de réponse.

5. Initiatives stratégiques

5.1 Les deux initiatives présentées dans ce document abordent les besoins critiques en mettant en place les capacités nécessaires pour que l'ICANN remplisse les engagements de sécurité, de stabilité et de résilience identifiés plus tôt. Tel que mentionné au début, ce document a pour intention de fournir une base à la discussion multi-parties prenantes de ces initiatives proposées, des responsabilités de l'ICANN en matière d'établissement des capacités proposées et de la manière selon laquelle la communauté pourrait procéder en organisant les efforts afin de soutenir de telles initiatives. L'encadrement de haut niveau et les implications relatives aux ressources sont identifiées, mais les alternatives de financement de ces initiatives ne sont pas analysées. Ce document ne présuppose pas que l'ICANN financera ou disposera de personnel pour ces initiatives.

5.2 L'initiative 2, concernant le besoin d'établir un DNS-CERT, est présentée plus en détail dans le dossier DNS-CERT qui accompagne ce document.

5.1 Initiative 1 – Analyse des risques, planification d'urgence et exercices couvrant l'ensemble du DNS

5.1.1 L'ICANN collaborera avec la communauté du DNS pour comprendre de manière proactive les risques clés menaçant le DNS. Ceci comprend l'analyse des menaces et risques naissants tels que requis dans l'affirmation d'engagements. Lorsque ces risques auront été analysés, la communauté du DNS doit identifier les imprévus préoccupant le plus la sécurité, la stabilité et la résilience de l'ensemble du DNS et garantir que des efforts sont mis en place pour réduire les risques identifiés. L'ICANN estime avoir un rôle important dans la favorisation de plans et d'exercices d'urgence couvrant l'ensemble du système, dans le cadre de ses responsabilités selon l'affirmation d'engagements. Un tel programme proactif complètera les capacités de réponse qui pourraient être fournies par un DNS-CERT en plus du renforcement de l'organisation en tant que centre naturel de soutien à la planification et aux exercices d'urgence.

5.1.2 Le premier aspect de cette initiative serait d'adopter une approche de l'analyse des risques fondée sur la communauté. Ceci inclut un cadre des risques pour le DNS accepté et des approches d'affinement pour mesurer ces risques. Cet effort comprendra l'établissement d'une approche propre à la réalisation régulière d'évaluations des risques pour le DNS et à proposition de mesures de réduction de ces risques. Cet effort tirera parti du travail réalisé dans le cadre du symposium 2010 sur la sécurité, la stabilité et la résilience du DNS ainsi que des efforts déployés par le DNS-OARC, l'ENISA et autres.

5.1.3 Un autre aspect de cette initiative consiste à renforcer la collaboration à l'échelle de la communauté concernant les plans d'urgence et leur utilisation comme base d'orientation des efforts visant à la mise en place de capacités de réponse. Le fondement de la planification d'urgence devrait commencer par un consensus concernant le cadre des risques pour l'ensemble du DNS qui identifierait les risques majeurs pour le DNS ainsi que les scénarios clés. Cet effort tirerait parti des efforts existants tels que ceux déployés à travers les partenariats public—privé préoccupés par la protection d'infrastructures critiques tels que le conseil de coordination du secteur des technologies de l'information des Etats-Unis et l'ENISA, ainsi que ceux menés dans le cadre de la communauté opérationnelle du DNS tels que par le DNS-OARC et les laboratoires NL Net. Cette initiative proposée envisage également une coordination étroite avec un mécanisme naissant de partage d'information des systèmes de serveurs racine et avec les opérateurs de registres TLD. L'analyse des risques et des imprévus clés serait utilisée pour évaluer la pertinence des mécanismes de réponse actuels, pour identifier les déficits nécessitant des actions et pour produire des plans d'urgence permettant de parer aux urgences identifiées. L'effort serait soutenu par un groupe de travail / consultatif permanent composé d'experts à l'échelle de la communauté. L'ICANN assumerait la responsabilité de soutenir le groupe et d'élaborer un plan d'action pour révision de la part de la communauté qui constituerait une contribution au cycle annuel de l'ICANN pour la budgétisation de sa planification opérationnelle relative à la sécurité, la stabilité et la résilience.

5.1.4 Une fois la planification d'urgence établie, un programme d'exercices couvrant l'ensemble du DNS est nécessaire afin de garantir l'évaluation des capacités de réponse et l'identification des déficits.[5] Comme pour les efforts de DNS-CERT et de planification d'urgence, l'élaboration d'un programme d'exercices devrait tirer parti des activités existantes et incorporer en tant que sous-éléments d'un programme plus vaste, des efforts tels que des efforts d'exercices d'urgence pour les TLD existants. Le but devrait être le lancement d'un programme d'activités qui serait couronné par un exercice biannuel couvrant l'ensemble du système DNS, concentré sur la réponse aux imprévus clés. De plus, le programme devrait inclure l'intégration avec d'autres programmes d'exercices tels que les séries d'exercices multinationaux *cyber storm* et autres exercices internationaux auxquels participent plusieurs parties prenantes. Tel qu'identifié dans l'affirmation d'engagements, l'ICANN a la responsabilité de soutenir une approche

[5] L'exigence d'un tel programme pour le DNS est spécifiquement identifiée dans le rapport du Ministère de la sécurité publique sur l'évaluation des risques dans le secteur des technologies de l'information.

communautaire à l'égard d'un tel programme, facilitant les sous-éléments d'un programme en tant que de besoin et orchestrant l'exercice biannuel sur l'ensemble du système DNS.

5.1.1 Démarches proposées spécifiques

5.1.1.1 Établir un groupe consultatif d'experts pour l'évaluation des risques pour le DNS et la planification d'urgence. Ce groupe serait composé d'experts provenant des communautés d'opérateurs du DNS et de cybersécurité. L'ICANN soutiendrait le groupe en mettant du personnel à sa disposition. Le point de concentration initial du groupe serait d'établir un cadre accepté par la communauté concernant les risques systémiques pour le DNS et l'identification des risques clés existants, ce d'ici le 3ème trimestre 2010. De plus, le groupe tirerait parti du travail accompli lors du symposium 2010 DNS SSR afin d'établir un cadre accepté par la communauté pour la mesure de la santé, de la sécurité, de la stabilité et de la résilience du DNS d'ici les débuts de 2011. Le groupe serait également chargé d'établir des scénarios de plans d'urgence de référence d'ici le 2ème trimestre 2011. Le groupe réaliserait un rapport annuel des risques et de réduction des risques pour le DNS, le premier rapport devant être remis le 3ème trimestre 2011.

5.1.1.2 Établir un mécanisme de partage d'informations des systèmes racine du DNS qui serait un effort conjoint avec la communauté des opérateurs de serveurs racine et d'autres parties impliquées au sein de la communauté des serveurs racine, fondé sur les recommandations de l'étude d'extensibilité de la racine de 2009. Un groupe de travail assisté par le personnel de l'ICANN sera mis en place pour identifier les exigences de surveillance fonctionnelle et de performance. Les capacités clés comprendraient l'affinement de la modélisation du système racine du DNS, un partage d'informations amélioré entre les organisations impliquées dans le système racine, le déploiement potentiel des détecteurs nécessaires, et un soutien analytique dédié pour évaluer l'état de santé actuel du système racine du DNS et fournir les alertes relatives aux problèmes naissants. Des efforts seront déployés pour travailler avec la communauté dans le but de mettre en œuvre et de déployer des détecteurs et de mesurer les critères qui permettront d'obtenir une vue d'ensemble du système de serveurs racine et TLD et de sa manière de se comporter. Cet effort nécessitera la collaboration avec les opérateurs de TLD, les opérateurs de serveurs racine, l'administration nationale des télécommunications et de l'information (NTIA), l'ICANN et les autres parties impliquées dans l'opération et la gestion de l'infrastructure essentielle du DNS. Nous envisageons que ce système sera établi dans un soutien mutuel avec le développement du DNS-CERT.

5.1.1.3 Le soutien continu de la planification et des exercices d'urgence des opérateurs de serveurs racine. Suite aux exercices de communications réussis et à l'exercice de simulation initial qui aura lieu d'ici la deuxième moitié de 2010, l'ICANN prévoira de collaborer avec les opérateurs pour instaurer une approche programmatique à la planification d'urgence et aux exercices basés sur des scénarios. L'ICANN déploiera des capacités de communications qui complèteront et renforceront les systèmes existants utilisés dans ses propres opérations de serveurs racine.

5.1.1.4 Affinement continu de la planification et des exercices de continuité des TLD. L'ICANN et les opérateurs de registres TLD réaliseront des tests de sauvegarde des données tout au long de l'année 2010 et en 2011, fondés sur l'élaboration des spécifications de sauvegarde des données pour le processus des nouveaux noms de domaine génériques de premier niveau (gTLD). Des exercices supplémentaires sont programmés. Ils se concentreront sur les communications et sur les éléments de réponse aux crises entre l'ICANN et les opérateurs de registres TLD.

5.1.1.5 Lancer le développement d'un programme d'exercice et d'évaluation de l'ensemble du DNS. Un tel programme comprendrait le renforcement des efforts existants et nécessiterait la participation d'une grande variété de parties prenantes y compris celles impliquées dans les opérations DNS, les vendeurs du DNS et les communautés d'utilisateurs ainsi que la communauté plus élargie des experts en cybersécurité. Ce programme impliquerait également la compréhension et le renforcement de l'intersection avec d'autres programmes de cybersécurité et les évaluations et exercices y associés. D'ici la fin de 2010, cet effort évaluerait la nature et la pertinence des efforts existants et identifierait les lacunes clés. D'ici la moitié de 2011, une note conceptuelle sur une proposition de programme d'exercices DNS serait élaborée et proposée à la révision de la part de la communauté. De plus, l'ICANN parrainera un exercice limité portant sur l'ensemble du système au cours de la deuxième moitié de 2011. Il s'agira d'un prototype avec participation bénévole de la variété de parties prenantes, dans le but d'établir des processus de planification et d'exécution à long terme. La planification de cet exercice prototype commencerait en 2010. Le personnel de l'ICANN et d'autres membres de la communauté du DNS participeront à l'exercice multilatéral Cyber Storm III et, éventuellement, à d'autres exercices internationaux.

5.1.2 Projection des ressources

5.1.2.1 Projeter le besoin de cinq postes à plein temps :

- Coordinateur en chef, évaluation des risques, planification d'urgence et programme d'exercices
- Coordinateur de la planification d'urgence
- Coordinateur du programme d'exercices et d'évaluation
- Planificateur d'exercices
- Analyste de systèmes/expert en modélisation, système de partage des informations du système racine

5.1.2.2 Les exigences de soutien comprendraient la définition des exigences pour le partage d'informations des systèmes de serveurs racine ; le soutien aux efforts d'analyse des risques et de partage des informations des serveurs racine ; l'infrastructure et les coûts associés pour inclure l'octroi de licence et le soutien en logiciel et équipement pour la modélisation, un système de communications et de partage des informations des systèmes de serveurs racine et un système de déploiement prototype de détecteurs ; les coûts relatifs aux déplacements et aux réunions des groupes de travail et du personnel ; et les installations physiques et le soutien TI au personnel supplémentaire.

5.1.2.3 Nous prévoyons que les coûts pour soutenir cet effort de juillet 2010 à juin 2011 s'élèveront à approximativement 1,25 million de dollars US pour le personnel et 850 000 dollars US pour le soutien. La projection de coût annuel total pour la première année de cette initiative serait de 2,1 millions de dollars US.

5.1.2.4 **Hypothèses :** L'analyse des risques renforcerait les informations relatives aux menaces et l'analyse du DNS-CERT. Le système de partage d'informations des serveurs racine renforcerait le portail Web 2.0 développé par le DNS-CERT pour soutenir le partage d'informations.

5.2 Initiative 2 – DNS-CERT

5.2.1 En plus de l'évaluation proactive des risques, de la planification et des exercices d'urgence, la communauté du DNS a besoin de capacités de réponses efficaces, opérationnelles couvrant l'ensemble du système afin de traiter de manière opportune les défis de sécurité, stabilité et résilience. Une attaque coordonnée de grande échelle menée contre le DNS pourrait résulter en des retombées économiques et politiques considérables. Pourtant, il n'existe pas pour le DNS de point central de contact de gestion des incidents pour la coordination technique et stratégique liée à l'identification et à la coordination de la réponse à un tel incident. En 2009, le symposium mondial sur la sécurité, la stabilité et la résilience du DNS a mis l'accent sur la lacune en matière de réponse aux incidents de sécurité liés au DNS et a recommandé que des mesures soient prises pour résoudre ce manque. De plus, un grand nombre d'opérateurs du DNS ne disposent pas des ressources appropriées ce qui résulte en des limitations du point de vue déploiement d'efforts énergiques en matière de sécurité et de résilience. De telles organisations ne savent peut-être pas où s'adresser pour trouver de l'aide ou font face à des obstacles linguistiques ou géographiques entravant l'accès à l'aide recherchée. De telles organisations risquent d'être des points vulnérables ou exploitables au sein du DNS en tant qu'ensemble. L'ICANN estime qu'un point de contact central, un DNS-CERT, est requis pour fournir une coordination technique et stratégique pour le DNS et collaborer avec la communauté du DNS en vue d'identifier et de coordonner les réponses aux incidents de DNS mondiaux.

5.2.2 Un DNS-CERT coordonnerait les efforts existants au sein de la communauté du DNS pour maintenir une conscience de la situation afin que l'ensemble de la communauté puisse avoir accès à l'expertise pertinente à tout moment. Les parties prenantes clés d'un tel effort seraient les opérateurs et utilisateurs du DNS, les vendeurs, les chercheurs en sécurité et les répondeurs aux incidents. Un DNS-CERT renforcerait un nombre d'efforts existants qui cherchent à identifier les menaces, à partager les informations et à faciliter la réponse à travers le DNS. Les activités du DNS-CERT pourraient aider la collaboration et la coordination de ces efforts et la fourniture de services dans des domaines qui ne sont pas actuellement couverts ou avec des parties prenantes qui ne sont pas engagées dans ces efforts. Un DNS-CERT pourrait être lancé avec le soutien de l'ICANN, mais la structure d'organisation spécifique et le modèle de resourcement seront déterminés par le biais d'un dialogue avec la communauté. A cet égard, la supervision du DNS-CERT serait réalisée par un Conseil au niveau du commanditaire qui garantirait la reddition de

comptes au regroupement du CERT et évaluerait également les activités du DNS-CERT selon les besoins des parties prenantes desservies par l'organisation. Les opérations du DNS CERT seraient supervisées par une équipe centrale composée par des membres du personnel administratif et technique qui serait assistée par une équipe élargie de spécialistes en expertise virtuelle qui fourniraient une assistance tangible au DNS-CERT tout en étant géographiquement disséminés.

5.2.3 Un DNS-CERT fournirait des services aussi proactifs (à savoir, analyse des menaces, surveillance de la sécurité et de la santé du DNS, conscience de la situation et partage des informations) que réactifs (à savoir, un point de contact de 7 jours sur 7, 24 heures sur 24 et 365 jours par an, la coordination de la gestion des incidents, l'assistance à la gestion de la vulnérabilité et des services consultatifs en matière de sécurité) à son regroupement. Cette approche est importance pour deux raisons : (1) des informations proactives sur le paysage des menaces peuvent aider la communauté du DNS à établir un plan de gestion des menaces à travers la formation et les exercices ; et (2) des services de gestion réactive des incidents peuvent aider les parties qui ont des contraintes en matière de ressources, telles que les bureaux d'enregistrement situés dans des régions moins développées de la planète. Les informations et les analyses des menaces alimenteraient également la mise en place prévue de capacités d'analyse et d'identification des risques systémiques pour le DNS, décrite dans l'initiative 1. La définition des exigences fonctionnelles pour les capacités essentielles qu'un DNS-CERT fournira, se fera par le biais de l'analyse au niveau communautaire avec la participation des parties prenantes et des collaborateurs potentiels pour un DNS-CERT.

5.2.2 Projection des ressources

5.2.2.1 Selon l'évaluation des équipes nationales CERT de taille et de niveau de responsabilité similaires, nous estimons que le DNS-CERT peut initialement fonctionner avec un budget annuel d'un personnel d'environ 15 personnes qui comprendraient un directeur, deux chefs, une équipe de gestion des incidents formée de 10 personnes et un personnel d'assistance administrative/juridique. La projection de coût du personnel s'élève à 2,6 millions de dollars US. Les frais de soutien au déplacement du personnel, les coûts relatifs aux outils d'analyse et de communication, aux installations physiques et au soutien informatique sont estimés à 1,6 million de dollars US. L'estimation de coût totale pour la première année de cette initiative correspond à 4,2 millions de dollars US. Plus de détails sont fournis dans le dossier DNS-CERT qui accompagne ce document.

6. Conclusion

Les défis de sécurité, stabilité et résilience confrontés par le DNS sont en croissance. L'ICANN a des responsabilités considérables selon ses règlements et l'affirmation d'engagements quant au travail avec la communauté du DNS pour traiter ces défis. Notamment, l'établissement pour l'ensemble du système DNS d'une planification et d'exercices d'urgence ainsi que la mise en place de capacités de réponse en collaboration sont requis. Cette note conceptuelle fournit une base à une discussion multi-parties prenantes des initiatives proposées afin de traiter ces exigences.