PLAN POUR LE RENFORCEMENT DE LA SECURITE, DE LA STABILITE ET DE LA RESILIENCE DE L'INTERNET (FY 11)

Septembre 2010

Table des matières

Synthèse

L'Internet a prospéré en tant qu'écosystème réunissant plusieurs parties prenantes organisées à travers la collaboration pour privilégier la communication, la créativité et le commerce au sein d'un patrimoine commun. L'interopérabilité du patrimoine commun dépend du fonctionnement et de la coordination des systèmes d'identificateurs uniques de l'Internet.[1] L'ICANN et les opérateurs de ces systèmes admettent que maintenir et renforcer la sécurité, la stabilité et la résilience de ces systèmes constituent un élément fondamental de leur relation collective.

Ce document est une mise à jour du plan de l'ICANN pour le renforcement de la sécurité, de la stabilité et de la résilience publié le 16 mai 2009 (ci-après le plan SSR 2009, http://www.icann.org/en/topics/ssr/ssr-draft-plan-16may09-en.pdf). Pour l'exercice financier 2011 (FY 11), le plan SSR a été actualisé pour refléter les activités de l'ICANN en matière de sécurité de juin 2010 à juillet 2011. Les mises à jour du plan SSR 2009 seront notées en italique. Le plan SSR FY 11 est publié pour la consultation publique d'août à septembre 2010.

Le plan stratégique de l'ICANN 2010-2013 (http://www.icann.org/en/strategic-plan/strategic-plan-2010-2013-19feb10-en.pdf) spécifie « La stabilité et la sécurité du système de noms de domaine (DNS) sont des priorités importantes pour la communauté de l'ICANN et les internautes au niveau mondial. Elles constituent les éléments fondamentaux de la mission de l'ICANN. Le mauvais usage et les attaques contre le DNS et les autres infrastructures du DNS sont en croissance progressive. Pour garantir la sécurité, la stabilité et la résilience qui sont cruciales pour le DNS, l'ICANN doit oeuvrer en partenariat avec les autres parties impliquées dans les aspects plus vastes de ces problématiques ».

Le plan stratégique identifie la stabilité et la sécurité comme étant l'une des quatre zones principales de concentration stratégique de l'ICANN. Ceci s'aligne sur l'importance capitale accordée à la SSR dans l'affirmation d'engagements (http://www.icann.org/en/documents/affirmation-of-commitments-30sep09-en.htm) conclue le 30 septembre 2009 entre l'ICANN et l'administration nationale des

[1] Conformément aux statuts de l'ICANN, l'ICANN coordonne l'attribution et l'affectation des trois sets d'identificateurs uniques de l'Internet : les noms de domaine (formant un système nommé DNS) ; les adresses du protocole Internet (IP) et les numéros de système autonome (AS) ; et les numéros de port et paramètre du protocole.

télécommunications et de l'information des États-Unis (NTIA). Le plan stratégique répartit la vaste série de responsabilités de l'ICANN en matière de sécurité, de stabilité et de résilience, en objectifs stratégiques, travail communautaire, projets stratégiques et travail du personnel.

La sécurité, la stabilité et la résilience dans le fonctionnement des systèmes d'identificateurs uniques de l'Internet forment une partie fondamentale de la mission de l'ICANN. A mesure que la fréquence et la sophistication des attaques perturbatrices et des autres comportements malveillants augmentent, l'ICANN et sa communauté doivent continuer à collaborer pour améliorer la résilience du DNS et renforcer son aptitude à maîtriser ces évènements. A mesure que s'amplifie la nature des attaques et des comportements malveillants, l'ICANN doit collaborer avec les autres parties prenantes dans ce domaine afin de clarifier le rôle de l'ICANN et de trouver des solutions à des problèmes qui dépassent la mission d'une seule entité.

Objectifs stratégiques identifiés pour la sécurité et la stabilité du DNS :

1. *temps de disponibilité et bon fonctionnement 100% du DNS.*
2. *Abus du DNS plus réduit.*
3. *Exploitation plus sûre des noms de domaine de premier niveau (TLD).*
4. *Résilience améliorée du DNS aux attaques.*

Le 12 février 2010, l'ICANN a publié les initiatives stratégiques proposées pour une sécurité, une stabilité et une résilience (SSR) améliorées du DNS (http://www.icann.org/en/topics/ssr/strategic-ssr-initiatives-09feb10-en.pdf). Le document présente la logique, les attributs clés et les projections de coûts de deux initiatives stratégiques liées à la sécurité et à la stabilité du DNS.

Se basant sur les commentaires reçus lors de deux périodes de consultation publique, lors de la conférence de l'ICANN à Nairobi, de l'atelier sur la collaboration et les exigences opérationnelles d'une équipe de réponse aux urgences informatiques du système de noms de domaine (DNS-CERT) tenu en avril 2010 et de la conférence de l'ICANN à Bruxelles, l'ICANN ne prévoit pas la mise en place d'une DNS-CERT mais plutôt de poursuivre la collaboration avec les parties prenantes afin de définir des exigences opérationnelles pour une capacité de réponse collective

du DNS, une analyse des menaces et une évaluation des risques portant sur l'ensemble du DNS.

Le rôle de l'ICANN

L'ICANN agit conformément à ses statuts en mettant en place des processus, des politiques et des programmes multipartites et consensuels, y inclus ceux liés à la sécurité, la stabilité et la résilience.

- Le rôle de l'ICANN doit se concentrer sur ses missions primordiales liées aux systèmes d'identificateurs uniques.
- L'ICANN ne joue pas un rôle de surveillance ou de lutte opérationnelle contre les comportements malveillants.
- L'ICANN n'a pas de rôle en ce qui concerne l'utilisation de l'Internet liée à l'espionnage électronique et à la guerre de l'information.
- L'ICANN ne détient pas de rôle dans la détermination de ce qui constitue un contenu illicite sur Internet.
- Le rôle de l'ICANN inclut la participation à des activités avec la communauté élargie de l'Internet pour lutter contre l'abus des systèmes d'identificateurs uniques. Ces activités comprendront la collaboration avec les gouvernements luttant contre les activités malveillantes rendues possibles par l'utilisation frauduleuse des systèmes pour les aider à protéger ces systèmes.

Les programmes de sécurité, de stabilité et de résilience de l'ICANN

- L'ICANN est responsable des opérations de l'autorité pour les noms et numéros assignés (IANA). Garantir le fonctionnement sûr, stable et résilient de la fonction de zone racine du DNS a été et sera toujours la priorité absolue.
- L'ICANN est un facilitateur du système des noms de domaine (DNS) et coordonne les efforts de la communauté visant à renforcer les fondations du système en matière de sécurité, de stabilité et de résilience. De tels efforts comprendront le soutien à l'élaboration et au déploiement de protocoles et de technologies d'appoint pour authentifier les noms et les numéros sur Internet.
- L'ICANN favorise et facilite les activités menées par les registres DNS, les bureaux d'enregistrement et les autres membres de la communauté en matière de sécurité, de stabilité et de résilience.

- L'ICANN est responsable du fonctionnement sûr, stable et résilient de ses propres biens et services.
- L'ICANN prend part à des activités et débats publics plus élargis liés à la sécurité, la stabilité et la résilience des systèmes d'identificateurs uniques de l'Internet.

Plans pour renforcer la sécurité, la stabilité et la résilience

Au cours de l'année de fonctionnement FY 11, l'ICANN prévoit de mettre en œuvre les programmes et initiatives brièvement exposés dans ce document. L'annexe A présente en détail les objectifs de programmes et activités spécifiques, les partenaires, les produits livrables et les engagements en matière de ressources.

- ***Opérations de l'autorité pour les noms et numéros assignés (IANA)*** *- le 16 juillet 2010, l'ICANN, VeriSign et la NTIA ont mis en œuvre les extensions sécurité du DNS (DNSSEC) pour la zone racine faisant autorité. Il s'agissait d'une étape importante dans le cadre de l'amélioration de la sécurité et de la stabilité d'Internet. L'ICANN continuera à collaborer avec la communauté Internet pour éliminer les obstacles à l'adoption des DNSSEC. D'autres initiatives comprennent l'amélioration de la gestion de la zone racine par le biais de l'automatisation ; l'authentification améliorée des communications avec les gestionnaires de TLD.*
- ***Opérations du serveur racine du DNS*** *- l'ICANN poursuivra les efforts pour la mise en œuvre de plans et d'exercices avec les opérateurs de serveurs racine pour parer aux imprévus et pour l'amélioration de la résilience et de l'infrastructure de la racine L.*
- ***Registres gTLD*** – veiller à ce que l'évaluation des candidats aux nouveaux noms de domaine génériques de premier niveau (gTLD) et aux noms de domaine internationalisés (IDN) prenne toujours en compte la sécurité des opérations. *L'ICANN continuera à rechercher la mise en œuvre de mesures visant à combattre le potentiel de conduite malveillante émanant de la mise en place de nouveaux gTLD.* L'ICANN affinera le plan de continuité des registres gTLD et continuera à tester le système de sauvegarde des données.
- ***Registres ccTLD*** *- à mesure que les ccTLD IDN sont introduits via la procédure accélérée 'fast track', l'ICANN poursuit ses efforts visant à traiter les soucis de gestion des variantes et les préoccupations relatives à la sécurité.*

L'ICANN poursuivra sa collaboration avec les registres de noms de domaine de premier niveau de code de pays (ccTLD) à travers le programme conjoint de planification des réponses aux attaques et aux imprévus (ACRP) et la formation sur l'opération des registres (ROC) conjointement avec l'organisation de soutien aux politiques de codes de pays (ccNSO), les associations de noms de domaine de premier niveau (TLD) et la société Internet (ISOC).

- ***Conformité contractuelle*** – l'ICANN continuera à renforcer la portée des activités d'application contractuelle impliquant les gTLD pour inclure le lancement d'audits des parties contractantes en tant que partie de la mise en œuvre des amendements de mars 2009 à l'accord d'accréditation de bureau d'enregistrement (RAA) et identifier l'implication potentielle de parties contractantes dans des activités malveillantes pour agir en conséquence. L'ICANN continuera aussi à faciliter la considération de politiques sur les activités de conformité dans le cadre des amendements potentiels du RAA au cours du FY 11.
- ***Réponse à l'abus malveillant du DNS*** - l'ICANN tirera parti de ses efforts collectifs et facilitera le partage d'informations pour permettre une réaction efficace concernant la conduite malveillante favorisée par l'abus du DNS.
- ***Opérations de sécurité et continuité internes de l'ICANN*** – *l'ICANN veillera à ce que ses programmes de sécurité soient réalisés dans l'ensemble des programmes de gestion des risques d'entreprise, de gestion des crises, et de continuité des activités. Un accent spécial sera mis sur l'établissement d'une base solide de plans documentés et de procédures de soutien. Ces programmes comprennent :*
  - ***Plan de sécurité de l'information d'entreprise*** *- l'ICANN a mis au point un plan de sécurité de l'information d'entreprise en s'appuyant sur les normes ISO 27002. Le plan est mis en œuvre au cours du FY 11.*
  - ***Plan de sécurité des conférences*** *- tirant parti des efforts déployés pour une planification d'une sécurité améliorée des conférences mondiales de l'ICANN, un plan de sécurité des conférences a été élaboré et sera utilisé lors de la sélection et de la préparation des sites des conférences de l'ICANN à compter du FY 11.*
  - ***Plan de sécurité physique et du personnel*** *- dans le cadre des efforts déployés pour améliorer la sécurité du personnel et des installations, ces deux plans sont mis en œuvre au cours du FY 11.*
  - ***Plan de gestion des incidents et de continuité des affaires*** *- l'ICANN a effectué un exercice de continuité de*

l'IANA en 2010 et les efforts se poursuivront au cours du FY 11 avec, notamment, un exercice de communication en cas de crise de l'ICANN et la mise en œuvre du plan de gestion des incidents et de continuité des affaires de l'ICANN.

- ***Programme de gestion des risques d'entreprise*** *- l'ICANN a mis en œuvre des directives de gestion des risques d'entreprise (ERM) et a établi un programme ERM au cours du FY 10. L'ICANN continuera à renforcer ce programme au cours du FY 11 de par l'évaluation des risques et le soutien au comité des risques du Conseil d'administration de l'ICANN.*

- ***Assurer l'engagement et la coopération au niveau mondial*** – l'ICANN continuera à renforcer les partenariats avec le groupe de travail de l'ingénierie Internet (IETF), la société Internet (ISOC), les registres Internet régionaux (RIR), les groupes d'opérateurs de réseau (NOG), le centre d'opérations, d'analyse et de recherche du DNS (DNS-OARC) *et le forum des équipes de réaction aux incidents concernant la sécurité des systèmes d'information (FIRST).* L'ICANN prendra également part à des dialogues au niveau mondial afin de promouvoir la compréhension des défis liés à la sécurité, la stabilité et la résilience auxquels l'écosystème d'Internet est confronté et la manière de relever ses défis par le biais d'approches multipartites.

1. Objectif et vue d'ensemble

Le plan SSR actualisé présente dans ses grandes lignes et à une large variété de parties prenantes la manière selon laquelle l'ICANN, centrée sur sa mission liée aux identificateurs uniques de l'Internet, contribuera aux efforts mondiaux de maîtrise de la sécurité, stabilité et résilience en tant que défis pour l'Internet. Le plan explique les rôles de l'ICANN et les limites inhérentes à son implication dans ce domaine ; il brosse les programmes de l'ICANN existant dans ce domaine ; et présente en détail les activités programmées et les ressources y dédiées au cours de l'année de fonctionnement prochaine. Le plan se décline en sept sections et une annexe :

- Section 1 : Objectif et vue d'ensemble
- Section 2 : Défis et perspectives
- Section 3 : Le rôle de l'ICANN
- Section 4 : Les participants de l'ICANN aux efforts de sécurité, stabilité et résilience
- Section 5 : Les programmes en cours de l'ICANN liés à la sécurité, la stabilité et la résilience
- Section 6 : *Plans de l'exercice financier 2011 de l'ICANN pour renforcer la sécurité, la stabilité et la résilience*
- Section 7 : Conclusion
- *Annexe A : Les objectifs des programmes de l'exercice financier 2011 de l'ICANN en matière de sécurité, stabilité et résilience, les partenaires, les étapes importantes/produits livrables et les ressources humaines*

Tel que formulé dans la synthèse, ce plan actualisé tire parti du plan SSR 2009 et se base sur la vision et les objectifs définis dans le plan stratégique de l'ICANN pour 2010-2013. Cette version du plan vise à fournir des mises à jour supplémentaires sur les fondements de l'ICANN et de sa communauté concernant son rôle et à renforcer le cadre d'organisation de ses efforts en matière de sécurité, de stabilité et de résilience. Le plan a été mis à jour dans le cadre de la revue annuelle conjointement avec les cycles de planification opérationnelle et stratégique de l'ICANN.

2. Défis et perspectives

L'environnement plein de vie de l'Internet est menacé par les niveaux croissants d'activités malveillantes exercées par une variété d'intervenants y inclus les organisations criminelles profondément impliquées dans la fraude, l'extorsion et autres activités illicites en ligne et la hausse d'attaques par saturation ou par déni de service (DoS) et autres activités perturbatrices menées par le biais de l'Internet. 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. Mais l'ouverture a été également accompagnée de vulnérabilités. Par exemple, les activités qui profitent des occasions pour « usurper » ou « empoisonner » la résolution d'un DNS et mal orienter les connexions d'utilisateurs involontaires sont en croissance. De même, l'incidence de piratages de routage et enregistrements d'adresses et de piratage d'enregistrement de numéros de systèmes autonomes (ASN) est également en croissance. Les attaques par saturation ou déni de service (DoS) peuvent perturber les utilisateurs de tous types. Une préoccupation grandissante a été exprimée au cours des dernières années par l'ensemble des parties prenantes de l'Internet : utilisateurs, entreprises, états souverains et organisations impliquées dans les débats autour de l'Internet et de la société de l'information élargie. Les efforts déployés pour faire face à ces défis doivent également aborder la question des risques menaçant la sécurité et la stabilité pouvant provenir de l'établissement de nouveaux contrôles qui pourraient être utilisés à mauvais escient par des criminels ou de conceptions de réseau qui rendraient plus difficile l'accomplissement de la stabilité.

L'ICANN abordera la question des risques menaçant la sécurité, la stabilité et la résilience de l'Internet dans les limites de ses responsabilités. L'article I des règlements de l'ICANN définit la mission de l'ICANN qui est « de coordonner, à un niveau général, les systèmes mondiaux d'identificateurs uniques de l'Internet, et notamment d'en assurer la stabilité et la sécurité d'exploitation ». Les programmes et activités de l'ICANN dans ce domaine se concentrent sur l'accomplissement de trois caractéristiques principales au sein des systèmes d'identificateurs uniques de l'Internet : sécurité, stabilité et résilience. La sécurité est la capacité de protéger et d'empêcher l'usage impropre des systèmes d'identificateurs uniques de l'Internet. La stabilité est la capacité de garantir que le système fonctionne tel que prévu, et

que les utilisateurs des systèmes d'identificateurs uniques sont confiants dans le fait que le système fonctionne tel que prévu. La résilience est la capacité qu'ont les systèmes d'identificateurs uniques de répondre de manière efficace aux attaques malveillantes et autres activités perturbatrices, de réagir à ces activités et de récupérer. L'ICANN collabore avec les parties responsables dans la sphère des systèmes d'identificateurs uniques afin de garantir la responsabilité en matière de mise en œuvre appropriée de ses politiques et dispositions contractuelles. En tant qu'organisation de modèle multipartite, l'ICANN veille à ce que ses efforts tirent le meilleur parti des ressources de la communauté disponibles dans ce domaine, en collaborant étroitement avec ses parties prenantes principales et en identifiant de manière explicite les objectifs et critères de mesure de performance dans sa planification stratégique, opérationnelle et financière. Ce plan fournit à la communauté une feuille de route décrivant comment l'ICANN fait face à ses responsabilités. *L'annexe A du plan fournit des détails sur les activités programmées au cours de l'exercice financier 2011, les étapes importantes et les ressources y associées. Dans le cadre des objectifs du personnel de sécurité de l'ICANN pour l'exercice financier 2011, l'accent sera spécialement mis sur l'établissement de critères de mesure des programmes plus élargis visant à améliorer, à un niveau général, la stabilité, la sécurité et la résilience des systèmes d'identificateurs uniques.*

3. Le rôle de l'ICANN

L'ICANN agit conformément à ses règlements en mettant en place des processus, des politiques et des programmes multipartites et consensuels, y inclus ceux liés à la sécurité, la stabilité et la résilience. La mission principale de l'ICANN se concentre sur la favorisation d'une approche multipartite de l'opération efficace des fonctions de l'IANA ; l'établissement de politiques mondiales qui garantissent la coordination du DNS, des adresses de protocole Internet (IP) et des affectations d'IP ; et la promotion de la concurrence et du choix au sein de l'environnement des gTLD par le biais d'un système de contrats avec les registres gTLD et les bureaux d'enregistrement accrédités par l'ICANN.

Dans le cadre de sa mission, l'ICANN a joué un rôle au cours des dix dernières années, contribuant à la sécurité et à la stabilité des systèmes d'identificateurs uniques de l'Internet. L'ICANN et les opérateurs de systèmes d'identificateurs uniques associés ont reconnu et admis que maintenir et renforcer la sécurité et la stabilité des services représentait un élément vital de leur relation. Ce principe est souligné dans le système de contrats et d'accords existant entre l'ICANN et les opérateurs selon la nature distincte des relations, les rôles spécifiques et les responsabilités mutuelles. Cet effort collectif et sa mise en œuvre fournissent l'assurance essentielle que les identificateurs uniques et les organisations qui les procurent à travers le monde garantiront la sécurité, la stabilité et la résilience par le biais d'un système coordonné et coopératif.

L'ICANN prévoit de continuer à contribuer par une variété d'activités pour permettre aux systèmes de nommage et d'adressage de l'Internet d'être sûrs, stables et résilients face aux risques et menaces en évolution. En même temps, elle veillera à ce que ses efforts se concentrent sur sa mission principale liée aux systèmes d'identificateurs uniques de l'Internet. Elle n'agira pas en tant que policier dans la lutte opérationnelle contre les comportements criminels et les parties malveillantes. L'ICANN ne se livre pas à des activités liées à l'utilisation de l'Internet pour l'espionnage électronique et la guerre de l'information. Par ailleurs, l'ICANN ne s'implique pas dans des activités liées à ce qui constitue un contenu illicite résidant dans l'internet ou passant par l'Internet. L'ICANN continuera à participer avec la communauté élargie responsable de la sécurité de l'Internet à des forums clés relatifs à la lutte contre les activités malveillantes (par ex. l'hameçonnage et la diffusion de programmes malveillants) qui utilisent le système d'identificateurs uniques de l'Internet.

L'ICANN organise ses activités de sécurité, stabilité et résilience à travers la considération de son rôle : en tant que directement responsable, en tant que facilitateur/favorisant, en tant que participant.

- L'ICANN est directement responsable des opérations de l'IANA et collabore dans la compilation et distribution de la zone racine avec le Ministère du commerce des E.U. et VeriSign. Garantir le fonctionnement sûr, stable et résilient de la fonction de zone racine du DNS a été et sera toujours la priorité absolue. De plus, l'ICANN est un favorisant primordial des efforts de la communauté d'adressage et DNS pour l'authentification des numéros et noms Internet. L'ICANN préconise la mise en œuvre des extensions de sécurité du système de noms de domaine (DNSSEC) comme étant une démarche essentielle pour la maîtrise de la sécurité du DNS (*l'ICANN, VeriSign et la NTIA ont mis en œuvre les DNSSEC dans la zone racine le 16 juillet 2010*). D'autres efforts capitaux porteront sur l'amélioration de la compréhension des risques, la facilitation de la mise en œuvre à ancre de confiance unique (TA) des clés publiques de ressources (rPKI), et la coopération avec des partenaires pour renforcer les pratiques de sécurité et de résilience au sein de la communauté des TLD.
- L'ICANN sert de facilitateur des activités menées par les registres DNS et les bureaux d'enregistrement en matière de sécurité, de stabilité et de résilience. La nature des rôles et des responsabilités de l'ICANN dépend des caractéristiques spécifiques de ses relations avec ces opérateurs fondamentaux. En plus des activités de collaboration, l'ICANN a conclu des accords avec tous les registres gTLD et les bureaux d'enregistrement accrédités par l'ICANN. Ces accords sont progressivement devenus des mécanismes d'amélioration de la sécurité, de la stabilité et de la résilience à travers le DNS. Les efforts de l'ICANN visant à garantir la conformité et la mise en œuvre des dispositions de ces accords constituent un point central des efforts de persévérance. Concernant les registres ccTLD, l'ICANN et les opérateurs de ccTLD ont exprimé leur engagement envers le renforcement de la stabilité, sécurité et interopérabilité du DNS dans l'intérêt de la communauté Internet locale et mondiale sur la base d'une relation d'appairage. Le partage d'informations, l'entraide et le renforcement des aptitudes seront le point central des activités poursuivies. L'ICANN se concentrera également sur le soutien des capacités de réaction collective au sein de la communauté afin de renforcer la sécurité du DNS.

- L'ICANN participe à des activités avec la NRO (Numbering Resource Organisation) et les RIR. Ces activités sont guidées par la compréhension primordiale que les RIR et l'ICANN doivent maintenir et renforcer la sécurité, la stabilité et la résilience de l'Internet au bénéfice des internautes locaux et mondiaux.
- L'ICANN est directement responsable du fonctionnement sûr, stable et résilient de ses propres biens et services lors de l'exécution des fonctions de l'IANA et autres fonctions de coordination, et en tant qu'opérateur du serveur racine L du DNS.
- Les organisations de soutien, les comités consultatifs et le personnel de l'ICANN sont des participants clés aux activités et débats publics plus élargis dont les objectifs varient entre l'amélioration de la résilience face aux attaques perturbatrices et les efforts collectifs centrés sur la lutte contre les activités malveillantes sur Internet telles que la propagation de programmes malveillants et l'hameçonnage qui utilisent les systèmes d'identificateurs uniques de l'Internet. Les exemples comprennent les séances dédiées à l'abus de DNS et aux DNSSEC lors des dernières conférences de l'ICANN.
- L'ICANN a une mission de fondation concernant son rôle dans la coordination des systèmes d'identificateurs uniques de l'Internet et remplira un rôle de leader face aux défis liés à la mise en place d'un écosystème Internet sûr, stable et résilient qui doit également demeurer un environnement plein de vie permettant le dialogue, le commerce et l'innovation au niveau mondial.

4. Les participants de l'ICANN aux efforts de sécurité, stabilité et résilience

L'engagement de l'ICANN en matière de sécurité, de stabilité et de résilience nécessite des activités impliquant l'ensemble du personnel de l'organisation, de ses organisations de soutien et comités consultatifs. Les principaux acteurs comprennent :

- ***Le personnel de l'IANA*** – chargé de l'exécution des fonctions de l'IANA y inclus la coordination de la zone racine du DNS, l'exploitation du registre .arpa, l'attribution de l'espace d'adresses IP, et l'enregistrement des paramètres de protocole. Les activités spécifiques liées à la sécurité, la stabilité et la résilience sont brièvement décrites ci-dessous.
- ***Personnel opérations DNS*** - chargé des opérations de la racine L, un des treize serveurs de noms racine, de l'infrastructure des DNSSEC pour les domaines gérés par l'ICANN et les TLD, la signature de la racine DNSSEC (KSK), les installations de clés de signature de clé, les cérémonies et l'hébergement des ccTLD, les serveurs DNS de l'ICANN faisant autorité et le portefeuille de domaines de l'ICANN. Les membres de l'équipe d'opérations DNS assistent régulièrement à des conférences telles que NANOG, RIPE, MENOG, LACNOG, NZNOG, SANOG, AFNOG, pour discuter entre autres des divers aspects concernant des projets liés aux activités d'opérations DNS de l'ICANN.
- ***Personnel services / conformité contractuelle*** – chargé d'assurer la coordination et la conformité avec les accords de la part des registres gTLD et des bureaux d'enregistrement accrédités par l'ICANN. Les activités spécifiques liées à la sécurité, la stabilité et la résilience sont brièvement décrites ci-dessous.
- ***Personnel chargé des politiques*** – chargé d'assister les organisations de soutien et les comités consultatifs dans le déroulement de leurs activités liées à l'élaboration de politiques, y inclus les activités des groupes de travail établis par les organisations de soutien. Les activités spécifiques liées à la sécurité, la stabilité et la résilience sont brièvement décrites ci-dessous.
- ***Personnel partenariats mondiaux*** – chargé des contacts au niveau local et régional avec les parties prenantes de l'ICANN pour garantir la pleine participation de l'ICANN aux opérations et à la mise en œuvre au niveau mondial. A cet égard, les activités de l'ICANN liées à la sécurité, la stabilité et

la résilience sont intégrées dans l'ensemble du travail du service de partenariats mondiaux pour l'organisation.

- ***Personnel relations d'entreprise / communications*** – chargé d'assurer la communication efficace des plans et programmes de l'ICANN et de représenter l'organisation et ses activités auprès de la communauté de l'ICANN. Les activités de l'ICANN liées à la sécurité, la stabilité et la résilience sont intégrées dans son programme général de communications d'entreprise.
- ***Personnel sécurité*** – chargé de la planification et de l'exécution quotidienne des efforts opérationnels de l'ICANN liés à la sécurité selon les instructions du Conseil d'administration et du chef de direction de l'ICANN réalisant ainsi les plans stratégiques et opérationnels de l'ICANN. L'équipe coordonne la variété des efforts de l'ICANN pour garantir une participation efficace aux thèmes liés à la sécurité, y compris la cybersécurité et autres débats publics sur la sécurité, stabilité et résilience.
- ***Le comité consultatif pour la sécurité et la stabilité (SSAC)*** – le SSAC, comité consultatif de l'ICANN, est chargé d'identifier et de communiquer au Conseil d'administration et à la communauté de l'ICANN, les problèmes clés et défis confrontés par l'ICANN dans le cadre de la garantie de sécurité et stabilité des systèmes d'identificateurs uniques de l'Internet. Le comité réalise des études sur les problèmes clés, requises par le Conseil d'administration de l'ICANN et lancées dans le cadre de son mandat décrit ci-dessous, et collabore avec d'autres organisations de l'ICANN telles que l'organisation de soutien aux politiques des noms génériques (GNSO).
- ***Le comité consultatif sur le système de serveurs racine (RSSAC)*** – le RSSAC, comité consultatif de l'ICANN, donne des conseils sur les exigences opérationnelles des serveurs de noms racine, examine et conseille sur les aspects du système de serveurs de noms racine liés à la sécurité, la performance globale du système, sa robustesse et sa fiabilité.

Plus globalement, les activités liées à la sécurité, la stabilité et la résilience se produisent dans toutes les organisations de soutien et autres comités consultatifs de l'ICANN tel que décrit ci-dessous.

Le personnel chargé de la sécurité de l'ICANN a la responsabilité globale de l'orchestration efficace dans toutes les activités de l'ICANN, de l'établissement d'un processus intégré de planification et de pistage de ces activités tout en assurant l'alignement et l'intégration dans tous les services et auprès de

toutes les parties prenantes. La figure 1 représente la relation organisationnelle de base au sein de la structure de l'ICANN.

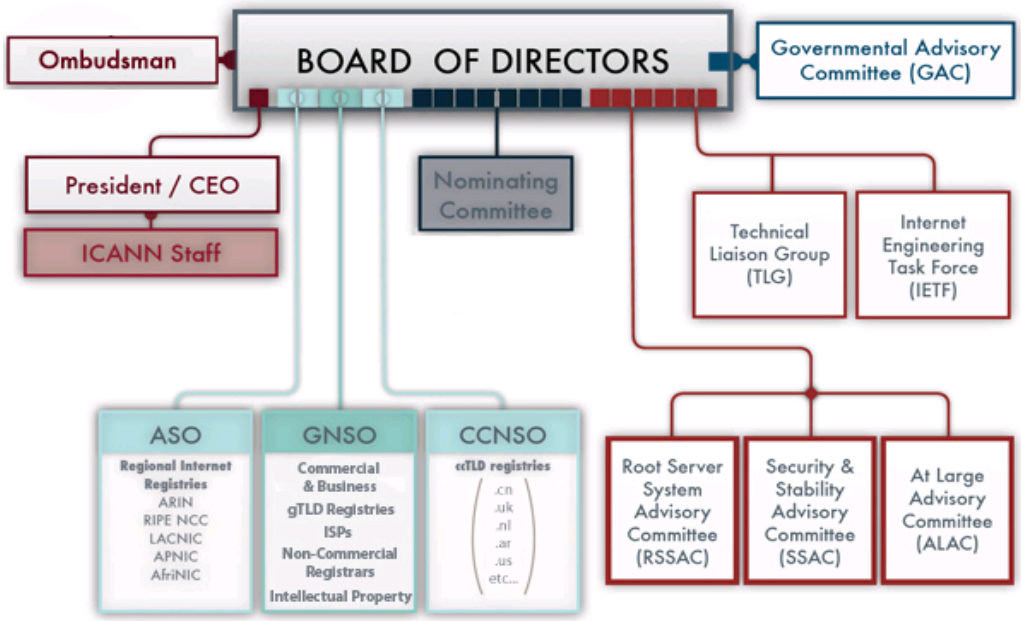


Figure 1 – Structure

5. Les programmes en cours de l'ICANN liés à la sécurité, la stabilité et la résilience

Cette section décrit les principaux programmes et activités réalisés par l'ICANN et qui contribuent à la sécurité, la stabilité et la résilience des systèmes d'identificateurs uniques de l'Internet, identifiant les partenaires opérationnels clés et fournissant des renseignements sur le contexte des efforts existants. L'objectif de cette section du plan est d'expliquer les fonctions de base de la grande variété d'activités de l'ICANN qui contribuent à la sécurité, la stabilité et la résilience des systèmes d'identificateurs uniques. Pour que l'ICANN remplisse efficacement ses responsabilités dans ce domaine, la majorité des cadres principaux du personnel ainsi que les organisations de soutien et les comités consultatifs sont impliqués. Cette section fournit le contexte et les explications portant sur la manière selon laquelle les programmes et les activités s'intègrent à la structure de l'ICANN et croisent les organisations externes.

La section est organisée autour du cadre établi dans la section 3, commençant par les fonctions principales de DNS/adressage ; le travail avec les communautés de registres et de bureaux d'enregistrement TLD ; la collaboration avec les registres Internet régionaux (RIR) à travers l'ASO ; les programmes de sécurité et de continuité d'entreprise ; les activités des organisations de soutien et des comités consultatifs, et la participation aux activités mondiales et régionales portant sur la sécurité, la stabilité et la résilience de l'Internet.

5.1 Sécurité, stabilité et résilience des fonctions principales de DNS/adressage

5.1.1 Opérations de l'IANA

L'ICANN dirige les fonctions de l'IANA en coordination avec le Ministère du commerce des E.U., VeriSign, le groupe de travail de l'ingénierie Internet (IETF), les registres Internet régionaux (RIR) et les opérateurs de domaines de premier niveau (TLD) tel que décrit ci-dessous. Mener ces activités à bien constitue la contribution essentielle de l'ICANN à la stabilité et à la résilience de l'Internet. A travers la gestion des fonctions de l'IANA, l'ICANN coordonne et gère les registres des identificateurs clés permettant un Internet mondial interopérable.

Bien que l'Internet soit connu pour être un réseau mondial exempt de toute coordination centralisée, les opérations des systèmes d'identificateurs uniques clés doivent être coordonnées au niveau mondial – et ce rôle de coordination est assumé par l'ICANN. Plus précisément, à travers les fonctions de l'IANA, l'ICANN affecte et gère des codes uniques et des systèmes de numérotation qui sont utilisés dans les normes techniques (protocoles) qui actionnent l'Internet. Les diverses activités des fonctions de l'IANA peuvent être classées en trois grandes catégories :

- ***Noms de domaine*** – A travers les fonctions de l'IANA, l'ICANN gère la zone racine, les domaines .int et .arpa et des ressources de pratiques de noms de domaine internationalisés (IDN). Les pratiques de gestion garantissent que tout changement dans ces zones soit évalué en matière d'impact sur la stabilité et la sécurité du domaine de premier niveau spécifique et de la zone racine dans son ensemble. La gestion des fonctions de l'IANA permet également à l'ICANN de jouer un rôle qui favorise la sécurité des systèmes d'adresses IP et DNS en déployant et en maintenant des ancres de confiance à la racine des systèmes d'adressage et DNS qui peuvent grandement renforcer l'intégrité des données des identificateurs uniques ainsi que l'intégrité des réponses au sein du système DNS.
- ***Adresses et numéros de systèmes autonomes (AS)*** - l'IANA gère la base mondiale des adresses IPv4 et IPv6 et des numéros de systèmes autonomes (ASN). L'IANA affecte ces ressources de numéros aux RIR conformément aux politiques ayant trait aux ressources de numéros mondiales élaborées par les communautés RIR à travers leurs processus d'élaboration de politiques et coordonnées au niveau mondial par l'ASO. Ce processus de politique participative permet d'obtenir le consensus mondial des destinataires finaux des ressources que l'IANA et les RIR agissent en toute équité, transparence et stabilité. *L'ICANN collabore avec les RIR (par le biais de l'ASO) et l'IETF pour le développement de la technologie RPKI afin d'introduire une certification des ressources de numéros.*
- ***Affectations de protocoles*** – Les registres de protocoles et paramètres de l'Internet sont gérés par l'ICANN, à travers les fonctions de l'IANA, conjointement avec l'IETF. L'ICANN met en œuvre et gère plus de 700 registres de protocoles et paramètres selon les normes développées à travers le processus consensuel de longue date de « demande de commentaires » (RFC). A travers une collaboration étroite avec l'IETF et les rédacteurs des RFC, le personnel chargé des

fonctions de l'IANA veille à ce que les registres soient établis selon des processus réguliers, et gérés de manière à être précis et disponibles. Les relations entre le personnel chargé des fonctions de l'IANA et l'IETF sont documentées dans le RFC 2860 et dans un accord de niveau de service.

Le personnel chargé des fonctions de l'IANA a collaboré avec la communauté TLD pour suivre la mise en œuvre de minimisation globale au sein du système TLD en réponse à la vulnérabilité à l'empoisonnement du cache DNS découverte en été 2008 (voir la présentation « 2008 DNS Cache Poisoning Vulnerability » à l'adresse http://www.iana.org/about/ presentations/davies-cairo-vulnerability-081103.pdf). L'ICANN veillera à ce que ses programmes et activités renforcent des processus sûrs, stables et résilients en matière de changements / ajouts de la zone racine et de fonctionnement d'ancres de confiances pour des demandes au sein du DNS tel que décrit en détail ci-dessous.

L'ICANN remet annuellement au Ministère du commerce des E.U. un plan de sécurité de l'information se rapportant à la gestion des fonctions de l'IANA en accord avec le contrat portant sur les fonctions de l'IANA conclu entre l'ICANN et le Ministère du commerce et dans le cadre de son propre plan d'entreprise de réponse aux attaques et aux imprévus. *En janvier 2010, l'ICANN a effectué un exercice de continuité de l'IANA réussi, voir le rapport post-action à l'adresse http://www.icann.org/en/security/iana-business-continuity-exercise-aar-23feb10-en.pdf.*

L'ICANN prévoit de procéder aux dernières attributions d'espace d'adressage unicast IPv4 aux registres Internet régionaux (RIR) au cours de l'année civile 2011. Les attributions seront faites conformément à la politique mondiale d'attribution de l'espace d'adressage restant IPv4[2], qui a été élaborée par les communautés RIR et ratifiée par le Conseil d'administration de l'ICANN en mars 2009.

Bien que cette attribution épuise la réserve d'espace d'adressage géré par le service IANA de l'ICANN, les RIR auront toujours des réserves d'adresses desquelles ils pourront attribuer et affecter des adresses aux FAI et autres opérateurs de réseaux. Les RIR travaillent sur l'établissement de politiques qui garantiront l'accès à de petits blocs d'adresses IPv4 pour les nouveaux venus sur le marché[3] au cours de la période suivant l'attribution des derniers

[2] http://www.icann.org/en/general/allocation-remaining-ipv4-space.htm

[3] http://www.nro.net/documents/comp-pol-201006.html#2-6

cinq /8 et avant que l'IPv6 ne soit adopté par la majorité des réseaux connectés sur Internet.

Les RIR ont également établi des politiques permettant le transfert d'espace d'adressage IPv4 d'un opérateur de réseau à un autre opérateur de réseau[4]. Ces politiques sont conçues pour permettre aux réseaux de déplacer des adresses de sorte à ce qu'elles fournissent la plus grande valeur possible, permettant une croissance de réseau continue.

Le comité des risques du Conseil d'administration de l'ICANN travaille sur l'évaluation des risques auxquels l'ICANN pourrait être confrontée comme conséquence de la disponibilité réduite d'espace d'adressage IPv4.

La solution à long terme est l'adoption généralisée d'IPv6. Bien que des progrès considérables aient été accomplis et que des FAI, tels que XS4all aux Pays-Bas, commencent à offrir des IPv6 comme service standard à tous leurs clients, il reste beaucoup à faire. L'ICANN a organisé un nombre de séances de sensibilisation lors des conférences de l'ICANN et les RIR ont mis en place des programmes de formation et de sensibilisation aux IPv6[5][6][7][8][9].

Ce qu'il est essentiel de ne pas oublier c'est que l'Internet existant continuera à fonctionner, même après que les RIR aient attribué leurs réserves d'IPv4. Il y aura une période au cours de laquelle certains réseaux seront accessibles sur IPv6 et d'autres pas mais les IPv6 permettront aux opérateurs de continuer à agrandir leurs réseaux au-delà des limites imposées par les IPv4.

5.1.2 Opérations DNS

L'ICANN a préconisé le besoin de mettre en œuvre des DNSSEC au niveau de la racine. *Depuis le plan SSR initial, l'ICANN, VeriSign et*

[4] http://www.nro.net/documents/comp-pol-201006.html#1-3-2

[5] http://www.afrinic.net/training/ipv6training.htm

[6] http://www.apnic.net/services/services-apnic-provides/training/courses/ipv6-essentials

[7] https://www.arin.net/knowledge/v4-v6.html

[8] http://lacnic.net/en/eventos/ipv6/

[9] http://www.ripe.net/training/ipv6/outline.html

la NTIA ont progressé dans le sens de la mise en œuvre des DNSSEC par le biais d'une introduction échelonnée qui conduira à une signature globale de la racine en juillet 2010. La première cérémonie de signature de clé de signature (KSK) pour les DNSSEC a eu lieu à Culpeper, en Virginie le 16 juin 2010 (voir http://www.icann.org/en/announcements/announcement-4-16jun10-en.htm), et une deuxième cérémonie KSK a eu lieu le 12 juillet 2010 à Los Angeles, en Californie pour permettre la signature de la zone racine. Le déploiement des DNSSEC dans la zone racine offre des avantages à ceux qui publient des informations dans le DNS, permet à la communauté Internet et aux utilisateurs finaux de localiser des « ancres de confiance » essentielles cryptographiques dans la zone racine et protège les résolveurs DNS des empoisonnements du cache.

L'ICANN a commencé par signer .arpa et un grand nombre des propres noms de domaine organisationnels de l'ICANN. Les préparatifs ont comporté un banc d'essai de la mise en œuvre de DNSSEC depuis juin 2007, une collaboration avec les opérateurs de TLD et autres opérateurs du DNS concernant les efforts de mise en œuvre des DNSSEC, permettant d'acquérir une maîtrise technique de la mise en œuvre d'approches cryptologiques conformément aux normes pertinentes et de veiller à ce que la mise en œuvre des efforts relatifs aux DNSSEC fasse partie des plans opérationnels et budgets. L'ICANN a établi un groupe de membres du personnel dédié à la gestion et sécurisation des applications des DNSSEC, y compris la signature de icann.org et iana.org. Enfin, afin de promouvoir la mise en œuvre générale des DNSSEC, l'ICANN a établi le référentiel d'ancres de confiance pour les domaines de premier niveau (ITAR) de l'IANA, en tant que moyen d'assurer la disponibilité, pour les TLD ayant mis en œuvre des DNSSEC, de clés DNSSEC à ceux qui les déploient.

L'ICANN collabore avec les opérateurs de serveurs de noms racine concernant la coordination sûre et stable de la zone racine, pour assurer une planification appropriée des imprévus et privilégier des processus clairs dans les changements de zone racine. L'ICANN continuera à collaborer avec les opérateurs de serveurs de noms racine et autres concernant la coordination sûre et stable du système de serveurs racine. Le RSSAC a été un conseiller clé sur la manière selon laquelle des changements de protocole tels que l'ajout d'enregistrements IPv6 à la racine, avaient un impact sur ce système.

De plus, l'ICANN gère le serveur de noms racine *l.root-servers.net.* De par ce rôle opérationnel, le personnel de l'ICANN interagit également au niveau opérationnel avec les autres opérateurs de serveurs racine. En tant qu'opérateur de la racine L, l'ICANN est

également active au sein de la communauté DNS contribuant, entre autres, aux efforts de la communauté comme dans le cadre du centre d'opérations, d'analyse et de recherche du DNS (DNS-OARC) et du projet de recherche de l'association coopérative pour l'analyse des données Internet (CAIDA) « Day in the Life of the Internet – un jour dans la vie de l'Internet » L'ICANN est engagée à utiliser ses opérations pour promouvoir la diversité et la compréhension des meilleures pratiques, et cherche à apprendre et à partager les leçons acquises. *L'équipe d'opérations DNS a également soutenu une étude d'extensibilité de la racine L, http://www.icann.org/en/announcements/announcement-17sep09-en.htm.*

En 2009, l'ICANN a amélioré la résilience de la racine L avec des instances à Prague en République Tchèque et à Istanbul en Turquie. Des améliorations supplémentaires sont prévues en 2010 et en cours du FY 11.

5.2 Sécurité, stabilité et résilience des registres et bureaux d'enregistrement de TLD

Une des responsabilités directes et essentielles de l'ICANN, liées à la sécurité, stabilité et résilience générales de l'Internet, consiste en la gestion des accords avec les registres gTLD et les bureaux d'enregistrement accrédités par l'ICANN et en la structure cadre des accords utilisée pour gérer les relations avec les registres de ccTLD. L'ICANN a des contrats avec 16 registres gTLD et plus de 900 bureaux d'enregistrement accrédités responsables de la coordination de l'enregistrement des noms de domaine et de leur résolution dans le DNS. Les responsabilités de ces parties contractantes sont décrites dans les accords de registres (RA) et les accords d'accréditation de bureaux d'enregistrement (RAA). L'ICANN cherche à protéger les titulaires de noms de domaine et à contribuer à la préservation de la sécurité, stabilité et résilience du DNS et de la sphère Internet à travers les dispositions de ces accords. Au cours des dix dernières années, l'ICANN a œuvré en vue de renforcer ces accords par l'introduction de dispositions qui améliorent la stabilité et la résilience tel que décrit ci-dessous.

5.2.1 Registres gTLD

L'ICANN collabore avec les opérateurs de gTLD en matière de coordination sûre et stable de ces TLD. Tous les registres gTLD ont des accords avec l'ICANN. Tandis que certains éléments de ces accords peuvent varier, les dispositions relatives à la sécurité, à la stabilité et à la résilience sont systématiques. Ces accords comportent une disposition exigeant des opérateurs de registres

qu'ils mettent en œuvre les spécifications provisoires ou politiques établies par l'ICANN et les politiques consensuelles élaborées par l'organisation de soutien aux politiques des noms génériques (GNSO) et adoptées et approuvées par l'ICANN. D'autres dispositions des accords qui contribuent au fonctionnement sûr et stable des registres comportent l'exigence d'établissement d'accords de niveau de service et sauvegarde des données de tiers concernant les services DNS, le système d'enregistrement partagé, et les opérations de serveurs de noms. Les contrats ICANN-gTLD définissent les niveaux de disponibilité et de performance ainsi que les exigences du centre de données. En 2007, l'ICANN a entamé l'effort de planification de continuité de registre gTLD qui a résulté en l'établissement d'un plan de travail ainsi qu'en un engagement envers une série d'exercices annuels du plan afin d'améliorer les aptitudes de la communauté de registres gTLD à traiter les problèmes ou défaillances au sein du système de registres/bureaux d'enregistrement.

En 2006, l'ICANN a introduit le processus d'évaluation des services des registres (RSEP) en tant que moyen de facilitation d'un processus opportun et prévisible pour l'introduction de nouveaux services de registres. Une des composantes clés du RSEP consiste en la détermination de la mesure dans laquelle un service proposé pourrait potentiellement poser un problème de sécurité ou de stabilité. S'il est établi que le service proposé pourrait poser un problème de sécurité ou de stabilité, la proposition est renvoyée à une commission indépendante d'experts techniques nommée la commission d'évaluation technique des services des registres (RSTEP). La RSTEP examine le service proposé et exprime ses recommandations au Conseil d'administration de l'ICANN concernant l'approbation ou le rejet du service.

Le processus de demande de sécurité accélérée de registre (ERSR) a été introduit en octobre 2009 (voir http://www.icann.org/en/registries/ersr/). L'ERSR a été élaboré pour fournir aux registres gTLD un processus d'information de l'ICANN d'un incident actuel ou imminent touchant la sécurité de leur TLD et/ou le DNS et de demande de levée contractuelle pour des actions que les registres pourraient entreprendre ou ont entrepris pour réduire ou éliminer un incident. Une levée contractuelle est une exemption de conformité à une disposition spécifique de l'accord de registre pendant la période de temps nécessaire pour réagir et répondre à l'incident. L'ERSR a été conçu pour permettre le maintien de la sécurité opérationnelle autour d'un incident tout en tenant les parties compétentes (soit l'ICANN, les autres fournisseurs touchés, etc.) informées en tant que de besoin.

5.2.2 Nouveaux gTLD et IDN

Tout au long de l'exercice financier 2010 et au cours de l'exercice financier 2011, l'ICANN a travaillé avec la communauté pour renforcer les approches visant à réduire la conduite malveillante dans les nouveaux TLD [voir note explicative sur la réduction de la conduite malveillante en date du 28 mai 2010, http://www.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-memo-update-28may10-en.pdf].

Avec le lancement de la procédure accélérée ccTLD IDN en novembre 2009 et les préparatifs pour que le processus relatif aux nouveaux TLD comprenne les IDN, l'ICANN reconnaît le besoin d'entreprendre des efforts pour garantir les opérations sûres, stables et résilientes des nouveaux entrants au DNS et au système en tant qu'ensemble. Le processus de candidature aux nouveaux gTLD et de révision comporte une évaluation technique de l'aptitude du candidat à exploiter un registre ainsi que de la conformité des chaînes aux exigences techniques définies dans les RFC, concernant le protocole des candidatures aux noms de domaine internationalisés (IDNA) et les directives IDN.

L'ICANN a lancé la procédure accélérée ccTLD IDN le 16 novembre 2009 (voir http://www.icann.org/en/topics/idn/fast-track/). Depuis son lancement, le programme a reçu 34 demandes en 22 langues différentes (voir http://www.icann.org/en/topics/idn/fast-track/string-evaluation-completion-en.htm). Ces chaînes passent actuellement par l'étape de délégation IANA et les premières chaînes ccTLD IDN ont été introduites dans la zone racine en mai 2010 pour l'Egypte, l'Arabie saoudite, les Émirats arabes unis et la Fédération de Russie. Le Conseil d'administration de l'ICANN a approuvé la délégation de chaînes à la Chine, à Hong Kong et à Taiwan lors de la conférence de l'ICANN à Bruxelles en juin 2010 et des chaînes pour le Sri Lanka, la Thaïlande, le Territoire palestinien occupé, la Jordanie et la Tunisie ont été approuvées en août 2010.

L'introduction initiale des ccTLD IDN dans la procédure accélérée est limitée aux chaînes non litigieuses qui représentent des noms de pays et de territoires correspondant aux ccTLD existants.

Dans la procédure accélérée, une équipe d'experts indépendants, la commission de stabilité du DNS, procède à une évaluation de la chaîne ccTLD IDN proposée en matière de 'confusabilité' et de conflits potentiels avec les exigences de sécurité et de stabilité pour les chaînes IDN. Il est prévu que le processus relatif aux nouveaux gTLD dispose d'une commission d'experts similaire qui serait chargée de l'évaluation technique des candidats et de leurs TLD proposés. De plus, le processus relatif aux nouveaux gTLD

offre une procédure préliminaire d'évaluation des services des registres (RSEP) permettant d'évaluer les problèmes de sécurité ou de stabilité potentiels liés aux nouveaux services de registre proposés dans la candidature aux gTLD.

En outre, tous les candidats devront passer un contrôle technique préliminaire à la délégation visant à vérifier leur conformité aux exigences techniques requises pour exploiter un registre.

L'ICANN a l'intention de lancer une révision de la mise en œuvre de la procédure accélérée ccTLD IDN au cours de l'exercice FY 11.

5.2.3 Bureaux d'enregistrement gTLD

L'ICANN collabore avec les bureaux d'enregistrement sur les questions relatives à la sécurité, la stabilité et la résilience. Du point de vue contractuel, un accord d'accréditation de bureau d'enregistrement (RAA) standard régit la relation de l'ICANN avec les bureaux d'enregistrement. Le RAA définit certaines normes relatives à la collecte, la conservation et la sauvegarde de données. Le RAA comporte également, par référence, des politiques consensuelles élaborées par la communauté de l'ICANN, telles que, entre autres, la politique sur le transfert entre bureaux d'enregistrement, la politique sur le rappel des données Whois, et la politique sur la précision des noms rétablis, qui soutiennent de diverses manières la sécurité, la stabilité et la résilience du DNS. *Un RAA amélioré a été introduit en 2009 et plus de 95% des enregistrements des gTLD sont actuellement couverts au titre du RAA 2009 de par son adoption librement consentie de la part des bureaux d'enregistrement. L'ICANN a également publié un guide du RAA 2009 à l'adresse de non juristes, en réponse à la demande d'un guide par le comité consultatif At-Large (http://www.icann.org/en/registrars/non-lawyers-guide-to-ra-agreement-15feb10-en.htm).*

Le personnel de l'ICANN chargé de la liaison avec les bureaux d'enregistrement agit au premier niveau, surveillant quotidiennement la conformité des bureaux d'enregistrement avec les exigences des RAA par le biais de la résolution officieuse des plaintes de titulaires de noms de domaine et des conflits entre registres, et par le biais de révisions périodiques d'accréditation (par ex. lors du renouvellement du RAA d'un bureau d'enregistrement).

Dans le cadre du soutien d'un système de noms de domaine plus stable, l'ICANN a élaboré des programmes et des procédures afin de traiter les défaillances éventuelles de bureaux d'enregistrement. Par exemple, l'ICANN a mis en œuvre son programme de sauvegarde des données des bureaux

d'enregistrement qui exige des bureaux d'enregistrement de déposer une sauvegarde des données d'enregistrement en main tierce, quotidiennement ou hebdomadairement. La procédure relative à la transition d'un bureau d'enregistrement désaccrédité facilite le transfert opportun des enregistrements d'un bureau d'enregistrement désaccrédité à un bureau d'enregistrement accrédité par l'ICANN. En outre, le personnel de l'ICANN utilise plusieurs processus opérationnels internes conçus pour aider à conserver un environnement d'enregistrement de domaines sain et à empêcher toute perturbation des titulaires de noms de domaine et des internautes en cas de défaillance d'un bureau d'enregistrement.

5.2.4 Whois

Les services Whois fournissent un accès public aux données relatives aux noms de domaine enregistrés qui comprennent actuellement les coordonnées de contact des titulaires des noms de domaine enregistrés. L'ICANN joue un rôle dans l'administration de règles développées par la communauté pour le système Whois au sein des gTLD. L'ampleur des données d'enregistrement recueillies au moment de l'enregistrement d'un nom de domaine et les modes d'accès à ces données, sont définis dans les accords établis par l'ICANN portant sur les noms de domaine enregistrés dans les gTLD. Par exemple, l'ICANN demande aux bureaux d'enregistrement accrédités de recueillir et de fournir un accès public libre au nom de domaine enregistré et à son serveur de nom et bureau d'enregistrement, à la date à laquelle le domaine a été créé et à la date d'expiration de l'enregistrement, ainsi qu'aux coordonnées de contact du titulaire du nom enregistré, et des responsables technique et administratif.

Le Whois est utilisé par diverses communautés pour nombre d'objectifs y compris la facilitation de la coordination technique et l'aide à la prestation de renseignements sur les organisations et les personnes éventuellement impliquées dans une utilisation frauduleuse potentielle du DNS. Les activités de l'ICANN se concentrent sur la veille à la conformité des registres gTLD et des bureaux d'enregistrement accrédités par l'ICANN à leurs obligations contractuelles. Dans la considération des changements de politiques relatifs au Whois, la communauté de l'ICANN reconnait l'utilisation légitime du système Whois dans le soutien à la lutte contre l'abus de DNS, tout en cherchant à équilibrer les intérêts de la grande variété de parties prenantes dans la façon de fonctionner du système Whois. L'ICANN reconnaît les soucis de confidentialité et de sécurité exprimés par diverses personnes

quant à la mise à disponibilité de leurs coordonnées via le Whois. L'ICANN poursuit ses efforts pour traiter ces préoccupations. Reconnaissant que la fiabilité et l'utilité du service Whois actuel pourraient s'affaiblir avec le temps et suivant les conseils du GNSO, le personnel de l'ICANN a établi une série détaillée d'exigences pour le WHOIS qui prend en compte les faiblesses connues du service actuel et comprend des exigences éventuelles qui pourraient être nécessaires pour soutenir des initiatives stratégiques futures. [Référence : Résolutions du conseil de l'organisation de soutien aux politiques des noms génériques de l'ICANN (GNSO), mai 2009. Marina Del Rey, Californie : ICANN. Extrait le 25 octobre 2009 de http://gnso.icann.org/resolutions/#200905]. Le rapport tente d'identifier les exigences techniques qu'il pourrait être nécessaire de mettre en œuvre pour corriger les défauts et mettre en œuvre des politiques Whois à venir. Un nombre d'attributs inclus dans cet inventaire proviennent des recommandations du SSAC au GNSO, démontrant que l'ICANN, à travers la considération par l'ensemble des organisations de soutien et des comités consultatifs de mesures visant à améliorer le WHOIS, est engagée à trouver des solutions qui maintiennent l'utilité du WHOIS tout en privilégiant la confidentialité et la sécurité des informations WHOIS.

5.2.5 Conformité contractuelle

Le service de conformité contractuelle veille à ce qu'aussi bien l'ICANN que ses parties contractantes remplissent les exigences stipulées dans les accords conclus entre les parties. Les activités du service comprennent la gestion du système de réception des plaintes de l'ICANN qui permet au public de communiquer les plaintes liées aux noms de domaine et pouvant se rapporter à des problèmes de sécurité, de stabilité et de résilience. Voir le site Web à l'adresse http://reports.internic.net/cgi/registrars/problem-report.cgi. Le personnel chargé de la conformité contractuelle examine les plaintes relatives à des violations éventuelles de RAA et une action de conformité est prise lorsque des violations de contrat sont découvertes. Bien que la majorité des plaintes reçues par le biais de ce système se rapporte à des questions ne dépendant pas de l'autorité de l'ICANN (par ex. pourriels, contenu de site Web, service clientèle d'un bureau d'enregistrement), l'ICANN transmet ces plaintes aux bureaux d'enregistrement pour traitement.

Le service de conformité contractuelle gère également le système de signalement de problèmes de données Whois (WDPRS) qui

peut être consulté à l'adresse http://wdprs.internic.net/. Le WDPRS est conçu pour aider les bureaux d'enregistrement à remplir leur obligation d'enquête sur les inexactitudes présumées de données Whois. Ce système, développé en 2002, permet au public d'enregistrer des plaintes pour inexactitude de données Whois et ces plaintes sont transmises aux bureaux d'enregistrement pour la prise de mesures appropriées. En consultation avec la communauté, le WDPRS a été transformé en 2008 pour aborder des préoccupations en matière de fonctionnalité, de capacité limitée et de manque de suivi de la conformité. Le WDPRS restructuré a été lancé en décembre 2008 et l'équipe de conformité poursuit ses efforts pour améliorer ce système avec pour objectif le renforcement de l'exactitude des données du Whois.

L'ICANN a chargé le centre national de recherche de l'opinion de l'université de Chicago de réaliser une étude sur l'exactitude des données Whois. Un rapport préliminaire a été publié le 15 février 2010, http://www.icann.org/en/announcements/announcement-3-15feb10-en.htm.

5.2.6 Protéger les titulaires de noms de domaine gTLD

L'ICANN fait également son possible pour que les titulaires de noms de domaine aient confiance dans la sécurité, la stabilité et la résilience du DNS. Les efforts se déclinent en une variété de moyens. Ces protections comprennent des dispositions dans les contrats, les accords et les programmes de mise en application de l'ICANN. L'ICANN fournit des informations aux titulaires de noms de domaine concernant les obligations des bureaux d'enregistrement au titre des RAA et des moyens de déposer leurs plaintes par le biais du site Web InterNIC http://www.internic.net/. L'ICANN a également réalisé une campagne de sensibilisation auprès de la communauté de bureaux d'enregistrement, encourageant le soutien aux IPv6 pour les titulaires des noms de domaine.

En outre, le travail des organisations de soutien et des comités consultatifs de l'ICANN s'est concentré sur le traitement des préoccupations des titulaires des noms de domaine concernant la sécurité, la stabilité et la résilience. Des documents consultatifs du SSAC ont identifié des pratiques que les bureaux d'enregistrement devraient prendre en considération pour protéger les noms de domaine et les comptes d'enregistrement de noms de domaine contre les accès non autorisés et pour protéger les informations de

configuration du DNS contre les abus.[10]*Les projets du SSAC pour 2010 comprennent un rapport complémentaire qui identifie les pratiques que les titulaires de noms de domaine peuvent directement mettre en œuvre pour surveiller et protéger de manière proactive leurs comptes d'enregistrement de domaines et leurs informations de configuration du DNS contre les abus. D'autres activités du SSAC comprennent la rédaction de documents sur l'interdiction de réacheminement par les TLD [SAC041, le déploiement des DNSSEC, les coordonnées de contact vérifiées en cas d'abus [SAC038] et le traitement des enregistrements orphelins du DNS.*

Le comité consultatif d'At-Large (ALAC) a soulevé plusieurs questions portant sur la protection des titulaires de noms de domaine. L'ALAC a d'abord soulevé la question du 'domaine tasting' ce qui a résulté en l'approbation de la part du Conseil du GNSO et du Conseil d'administration d'une nouvelle politique consensuelle visant à éliminer les abus de la période de grâce de cinq jours pour « goûter à un nom de domaine ». *Plus récemment, l'ALAC a communiqué au conseil du GNSO des préoccupations concernant la récupération de noms de domaine par les titulaires après leur expiration (PEDNR) et la responsabilité et transparence des enregistrements de noms de domaine [http://www.atlarge.icann.org/announcements/announcement-19jul10-en.htm].* Le GNSO est en train d'entreprendre un nombre d'initiatives supplémentaires susceptibles de résulter en une meilleure protection pour les titulaires de noms de domaine. Ces initiatives comprennent des améliorations de la politique de transfert entre bureaux d'enregistrement qui prennent en compte le besoin d'authentification électronique, et les élaborations de politiques portant sur l'hébergement 'fast flux' et les enregistrements frauduleux.

5.2.7 ccTLD

L'interaction de l'ICANN avec les registres ccTLD est dictée par la compréhension primordiale du fait que les registres ccTLD et l'ICANN sont appelés à préserver et à renforcer la sécurité, la stabilité et la résilience du DNS au bénéfice des internautes locaux et mondiaux. Ceci se reflète dans le programme de responsabilité cadre qui forme la base de la variété d'accords conclus entre les registres ccTLD individuels et l'ICANN. Le centre d'intérêt principal de l'ICANN en matière de favorisation de la sécurité, stabilité et résilience concernant les ccTLD est de fournir, en

[10] Voir le SAC 40, mesures pour protéger les services d'enregistrement de domaines contre l'exploitation ou les abus, 19 août 2009 (http://www.icann.org/en/committees/security/sac040.pdf).

s'associant avec les ccTLD et d'autres, une plateforme privilégiant le partage d'information, l'action commune, la formation technique de sensibilisation et le renforcement des aptitudes en termes de planification des réponses aux attaques et imprévus. Le personnel de l'ICANN collabore étroitement avec les opérateurs de TLD pour les instruire des problèmes de sécurité au travers des fonctions de l'IANA, du programme de planification des réponses aux attaques et imprévus (ACRP) et des efforts des chargés de liaison régionaux du service des partenariats mondiaux. L'IANA a développé une relation de confiance avec les opérateurs de TLD bâtie sur la performance améliorée et sur la sensibilisation de la communauté des opérateurs de TLD, qui apporte son soutien dans la mise en place d'une réponse collective aux situations liées au DNS et exigeant une coordination mondiale.

5.2.8 Exigences techniques de l'IANA

De par la gestion de la fonction IANA, l'ICANN aide aussi à garantir que les TLD remplissent les exigences techniques pour privilégier des opérations stables et sûres. Les exigences spécifiques de serveurs de noms garantissent la disponibilité de domaines du DNS, et le personnel chargé des fonctions de l'IANA collabore étroitement avec les gestionnaires des TLD pour résoudre les problèmes auxquels ces derniers pourraient être éventuellement confrontés dans la maintenance des normes techniques. L'ICANN ne s'implique pas dans les opérations des ccTLD, mais se tient prête à aider dans les situations où les changements de leurs données de zone racine doivent être réalisés rapidement et de manière fiable. L'objectif primordial de l'ICANN est d'assurer la stabilité et la sécurité de la zone des TLD et de la zone racine.

5.2.9 Réponse collective à l'abus malveillant du système de noms de domaine

L'ICANN collabore avec une variété d'organisations dans la recherche de tous les moyens permettant aux parties prenantes d'analyser les activités pouvant éventuellement impliquer un abus du DNS. Depuis la fin de 2008, une augmentation inquiétante de l'activité impliquant des programmes malveillants affectant le DNS s'est produite. Un de ces incidents les plus remarquables était le ver informatique Conficker [Sommaire et revue du Conficker, http://www.icann.org/en/security/conficker-summary-review-07may10-en.pdf] L'ICANN a pris part à une réaction collective mondiale pour endiguer le Conficker conjointement avec les opérateurs de registres TLD et les communautés chargées de la sécurité et de l'application de la loi. L'ICANN a publié un rapport, 'sommaire et revue du Conficker' qui relate la chronologie des évènements liés à la limitation de l'expansion du Conficker,

présente les leçons apprises et suggère des moyens visant à améliorer les efforts collectifs à venir (par ex. le processus ERSR de l'ICANN). L'ICANN continue à travailler avec les registres et les bureaux d'enregistrement pour assurer la prise de conscience et faciliter la diffusion d'informations lorsque se produisent des incidents sécuritaires d'échelle mondiale impliquant le DNS. Le mandat de l'ICANN est limité dans ce domaine. L'ICANN a donc participé en tant que pair aux débats sur la mise en place de réactions efficaces lorsque des situations opérationnelles spécifiques surviennent.

Pour faciliter et élargir la collaboration dans ce domaine, le personnel de l'ICANN a soutenu les efforts déployés au sein du ccNSO à l'adresse des ccTLD concernant la réaction aux incidents. En février 2010, l'ICANN a publié une analyse de rentabilité mondiale d'une fonction DNS-CERT (http://www.icann.org/en/topics/ssr/dns-cert-business-case-19mar10-en.pdf) dans la communauté Internet. L'analyse de rentabilité comporte une description des exigences et des coûts éventuels, y compris l'option de mise en pratique d'une telle fonction DNS-CERT par d'autres membres de la communauté. Depuis la publication de l'analyse de rentabilité DNS-CERT, la prise en considération des commentaires du public (http://www.icann.org/en/public-comment/summary-analysis-strategic-ssr-initiatives-and-dns-cert-business-case-24may10-en.pdf) et les discussions aux conférences de l'ICANN à Nairobi et à Bruxelles, l'ICANN travaille avec les parties prenantes concernées en vue d'identifier des approches d'une capacité de réaction collective DNS qui ne soit pas dirigée par l'ICANN mais qui soit élaborée en collaboration avec la communauté.

5.2.10 Faciliter la sécurité et la résilience dans l'ensemble du DNS

Alors que nulle entité seule n'a de responsabilité déterminante, le personnel, les organisations de soutien et les comités consultatifs de l'ICANN jouent un rôle de facilitateur dans l'amélioration de la stabilité, sécurité et résilience de l'ensemble du DNS. Depuis sa création, le SSAC a fourni des analyses et des recommandations à la communauté du DNS. Le document consultatif 004 du SSAC, *'sécuriser la périphérie'*, fournit une analyse fondamentale liée aux défis sécuritaires confrontant les systèmes d'identificateurs uniques.[11]Les efforts principaux ont consisté, entre autres, en une analyse et des recommandations portant sur les attaques par saturation avec déni de service distribué (DDoS), la mise en œuvre

[11] SAC 004, Securing the Edge, 17 octobre 2002, http://www.icann.org/en/committees/security/sac004.pdf.

des DNSSEC, l'ajout d'enregistrements IPv6 à la racine du DNS, le 'domain name front running' (pratique théorique qui consiste pour un bureau à enregistrer un domaine qui vient de faire l'objet d'une recherche de disponibilité), l'hébergement 'fast flux' et le piratage de nom de domaine. De plus, des membres du SSAC participent au comité sur les politiques Internet du groupe de travail anti-hameçonnage (APWG), ont co-rédigé des documents de présentation technique décrivant comment les hameçonneurs exploitent les noms de sous-domaine, comment les organisations devraient réagir à une attaque de site Web, et collaborent avec l'IPC pour étudier conjointement les vulnérabilités exploitées des sites Web.

L'ICANN poursuivra son rôle de facilitateur, en cherchant à identifier des possibilités de collaboration à l'échelle de la communauté et en identifiant et atténuant les risques menaçant les systèmes. L'ICANN a entamé les efforts visant à améliorer la compréhension des risques menaçant l'ensemble du système DNS et l'atténuation de ces risques, au cours du Symposium mondial sur la sécurité, la stabilité et la résilience du DNS, organisé en février 2009 en partenariat avec le centre technologique de la sécurité de l'information de Georgia (GTISC). Le symposium s'est concentré sur la compréhension des risques liés au DNS dans les grandes entreprises, les défis en matière d'opérations sûres, stables et résilientes du DNS dans des environnements à ressources limitées, et sur le traitement du mauvais usage du DNS à des fins malveillantes. Le rapport est disponible à l'adresse http://www.gtisc.gatech.edu/icann09. *Un deuxième symposium sur la sécurité, la stabilité et la résilience du DNS a eu lieu à Kyoto, au Japon en février 2010, voir http://dns-srr.e-side.co.jp/, et le rapport a été publié en avril 2010 à l'adresse http://www.icann.org/en/announcements/announcement-26apr10-en.htm.*

En outre, le personnel, les organisations de soutien et les comités consultatifs de l'ICANN ont démarré une collaboration de plus en plus intensive avec une variété de parties prenantes afin d'améliorer la capacité de l'ICANN en matière d'élaboration de politiques efficaces, de mise en application contractuelle et autres initiatives de manière à aborder les défis liés à la sécurité et à la résilience se présentant au DNS et présentés par ce dernier.

5.2.11 Validité, droit d'usage et caractère unique des ressources de numéros Internet.

A travers la gestion des fonctions IANA, l'ICANN acquiert la stratégie et la responsabilité de la stabilité, sécurité et résilience

du système d'attribution de numéros Internet et, en fin de compte, à travers l'application de l'infrastructure des clés publiques de ressources (rPKI), le système mondial de routage IP. Cette responsabilité se manifeste dans le besoin de mettre en œuvre une application techniquement idéale de l'ancre de confiance unique RPKI, tel que mentionné par le conseil pour l'organisation de l'Internet (IAB)[12] et le NRO[13], et résulte en la capacité de certifier pleinement la validité, le droit d'usage et le caractère unique des ressources de numéros Internet. L'ICANN et le personnel de l'ICANN ont déployé des efforts considérables, collaborant avec l'IETF et d'autres groupes dédiés, prenant part au processus de normalisation, communiquant avec les parties prenantes et mettant en place une mise en œuvre d'une RPKI à l'essai (maintenant interrompue).

L'ICANN s'engage à travailler avec toutes les parties prenantes RPKI et le personnel de l'ICANN a entamé des processus de manière à assurer la mise en œuvre technique la plus sensée et la mise à disponibilité de la communauté Internet en fonction des échéances et des considérations appropriées.

5.3 Portée mondiale de la sécurité (engagement, prise de conscience)

5.3.1 Activités et partenaires mondiaux

Le noyau de la stratégie d'engagement mondial de l'ICANN par rapport à la sécurité, la stabilité et la résilience repose sur des partenariats réels avec une variété d'organisations. Nombreux sont les efforts menés par l'équipe de partenariats mondiaux du personnel de l'ICANN. L'ICANN a été un participant actif à une grande variété de forums mondiaux relatifs à l'Internet, y inclus plusieurs traitant des questions de sécurité, de stabilité et de résilience. La variété de partenaires et d'activités énumérés ci-dessous n'est pas complète et l'ICANN cherchera à en considérer d'autres à mesure que les occasions se présenteront. Les partenaires mondiaux principaux comprennent :

- ***Le groupe de travail de l'ingénierie Internet (IETF)/le conseil pour l'organisation de l'Internet (IAB)*** - dirigent les efforts pour établir des approches technologiques visant à renforcer la sécurité de l'Internet concentrés sur l'élaboration de

[12] http://www.ietf.org/mail-archive/web/ietf-announce/current/msg07028.html

[13] http://www.nro.net/news/nro-declaration-rpki.html

pratiques opérationnelles et de protocoles plus puissants. L'ICANN collabore avec l'IETF dans le cadre de l'établissement de ces protocoles liés au nommage et à l'adressage et fait son possible pour assurer leur déploiement au sein du noyau de l'Internet afin d'aider à sécuriser l'ensemble de cet environnement. En particulier, l'ICANN participera aux efforts d'établissement de protocoles qui fournissent une base plus sécurisable pour l'Internet centrée sur des efforts tels que les DNSSEC et la rPKI.

- ***La société Internet (ISOC)*** - promeut la prise de conscience des préoccupations de cybersécurité et le besoin d'établir la confiance en l'Internet auprès de la base d'utilisateurs mondiaux, notamment dans le monde en développement ; en collaboration avec d'autres, fournit la formation technique visant à améliorer la sécurité et la résilience de l'Internet. L'ICANN collabore avec l'ISOC pour aider à assurer la prise de conscience et l'amélioration des aptitudes en matière de sécurité, stabilité et résilience. L'ICANN prévoit de collaborer dans la mise au point du programme commun en cours ISOC/ICANN pour fournir une formation aux opérateurs de TLD qui comporte une formation technique sur les moyens d'améliorer la sécurité et d'atténuer les attaques électroniques et les perturbations.
- ***Forum sur la gouvernance de l'Internet (IGF)*** - l'IGF sponsorise les dialogues multipartites sur la sécurité et la confiance électroniques. En outre, l'IGF a mis l'accent sur la gestion des ressources décisives de l'Internet et sur la cybercriminalité. L'ICANN continuera à participer à l'IGF, à sensibiliser sur son rôle en matière de sécurité, de stabilité et de résilience par rapport au système d'identificateurs uniques de l'Internet et à contribuer au dialogue mondial au sein de ce forum.
- ***Le centre -d'opérations, d'analyse et de recherche du DNS (DNS-OARC)*** - l'ICANN continuera à parrainer le DNS-OARC, et à participer activement à l'ensemble de ses activités.

5.3.2 Activités et partenaires régionaux

L'ICANN a établi des liens régionaux par le biais d'une variété de partenaires et d'activités. Les aspects principaux des activités régionales de l'ICANN sont soulignés ci-dessous :

- ***Associations régionales de ccTLD*** - en plus de la collaboration dans le cadre du programme ACRP tel que défini ci-dessous, l'ICANN continuera à offrir son aide et son expertise pour les activités sponsorisées par ces organisations.

- ***Centres d'information de réseaux (NIC)/groupes d'opérateurs de réseaux (NOG) régionaux*** - l'ICANN continuera à participer à ces forums pour veiller à ce que ses activités permettent de la meilleure façon possible des exploitations de réseaux sûres et résilientes, y compris la coordination des fonctions de l'IANA.
- ***Asie*** - l'ICANN a lancé le programme de formation sécurité et résilience des ccTLD dans le cadre des efforts de soutien du renforcement des capacités en matière de DNS, en collaboration avec l'association TLD Asie-Pacifique (APTLD) en mai 2008 à Kuala Lumpur et reçoit toujours un fort soutien de l'activité dans cette région. L'ICANN continuera à participer à des forums régionaux tels que l'Internet Resource Management Essentials pour offrir conseils opérationnels et formation en matière de sécurité et de résilience du DNS à mesure que les occasions se présentent.
- ***Europe*** - l'ICANN continuera à participer aux efforts de l'agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) liés aux DNSSEC et à l'amélioration de la résilience du DNS dans le cadre de l'effort général de la Commission européenne dans le domaine de la protection de l'infrastructure critique. L'ICANN collaborera avec le Conseil des registres européens nationaux de domaines de premier niveau (CENTR) pour réaliser des séances de formation sur la sécurité et résilience des ccTLD démarrées avec la conférence RIPE 58 de mai 2009 à Amsterdam. L'ICANN poursuivra son partenariat avec l'Institut pour la sécurité de l'information (IISI) de l'université d'état de Moscou dans le cadre de la promotion du dialogue mondial sur la cybersécurité. En particulier, l'ICANN et l'IISI ont organisé de 2008 à 2010 des ateliers communs à Garmisch, en Allemagne avec le soutien du Centre germano-américain Marshall pour les études stratégiques. Les deux parties prévoient de poursuivre leur collaboration en 2011.
- ***Afrique et Amérique latine*** - l'ICANN poursuivra les activités liées à la cybersécurité conjointement avec les organisations régionales de l'ISOC ainsi que dans le cadre d'autres forums appropriés. L'ICANN a organisé une formation sur la sécurité et la résilience aux ccTLD conjointement avec l'association LACTLD en 2009 et 2010. L'ICANN a également organisé une formation ccTLD conjointement avec l'association africaine des domaines de premier niveau (AfTLD) et l'ISOC-Afrique et avec l'APTLD en Asie.

5.3.3 Le travail avec les gouvernements

L'ICANN collabore avec des gouvernements de par le monde dans la recherche de la sécurité, stabilité et résilience des systèmes d'identificateurs uniques de l'Internet. L'ICANN continuera à apporter sa perspective technique et opérationnelle en matière d'amélioration de la sécurité, de la stabilité et de la résilience du système d'identificateurs uniques de l'Internet. L'ICANN comprend que ces systèmes doivent être traités comme étant des infrastructures essentielles. Au sein de la structure de l'ICANN, le comité consultatif gouvernemental (GAC) recevra des mises à jour régulières concernant les efforts de l'ICANN en matière de sécurité, stabilité et résilience et contribuera à ses programmes dans le cadre du processus de planification stratégique. L'ICANN restera active, définissant son rôle dans les débats mondiaux autour de la sécurité et des implications de gestion de la sécurité et de la résilience liées aux systèmes d'identificateurs uniques. L'ICANN communiquera avec les commissions des Nations Unies et les organisations internationales, intergouvernementales et régionales, orientant ses efforts vers la facilitation d'activités régionales conçues pour améliorer la sécurité et la résilience dans le DNS. Ces activités se baseront sur les protocoles d'entente que l'ICANN détient avec une variété de ces organisations. Par exemple, l'ICANN continuera à participer aux forums liés à la cybersécurité tels que les efforts continus de l'OCDE pour la lutte contre les programmes malveillants. L'ICANN continuera également à solliciter les efforts associés de l'APEC et d'autres organisations dans ce domaine.

Le GAC offre également ses conseils à l'ICANN sous forme de communiqués lors des conférences internationales de l'ICANN.

5.4 Communication avec les registres Internet régionaux

L'ICANN communique avec l'ASO de par son interaction avec la NRO (Number Resource Organisation). A travers cette interaction, l'ICANN travaille avec les RIR ce qui permet à l'ICANN et aux RIR de maintenir et de renforcer la sécurité, la stabilité et la résilience du DNS au bénéfice des internautes locaux et mondiaux. L'ICANN participe avec ces organisations à un certain nombre d'activités liées à la sécurité, la stabilité et la résilience de l'Internet. Plus particulièrement, l'ICANN a travaillé avec ces organisations pour les DNSSEC de sous-domaines dans .arpa y compris ip6.arpa et in-addr.arpa. Les RIR sont en train d'élaborer les moyens permettant la certification des adresses IP et des numéros de systèmes

autonomes (AS) à travers l'effort RPKI. Les RIR sont également responsables des affectations d'ASN et l'ICANN devrait rechercher un partenariat avec les RIR portant sur l'intégrité de ces affectations. A court terme, cet effort fournira une corrélation validée entre le titulaire de la ressource de numéro et cette dernière. Ce système de certification hiérarchique peut servir de base au développement d'un moyen d'authentification des protocoles d'échange de routes (Border Gateway Protocol). L'ICANN continuera à vouloir faire partie de ces efforts.

5.5 Opérations de sécurité et continuité d'entreprise de l'ICANN

L'ICANN veille à ce que ses propres opérations soient sûres, stables et résilientes dans la gestion de l'IANA et des autres fonctions essentielles qu'elle exécute, en tant que partie des systèmes d'adressage et DNS. L'ICANN veille également à remplir ses responsabilités d'entreprise et de contributeur de la communauté en matière de sécurité, stabilité et résilience globales des systèmes d'identificateurs uniques de l'Internet. L'ICANN aura la capacité de réagir et de collaborer efficacement avec les autorités appropriées si ses propres actifs faisaient l'objet d'activités malveillantes.

L'ICANN se consacre à un programme de sécurité continuel visant à gérer les risques pour les actifs informationnels, humains et matériels de l'organisation. En automne 2008, l'ICANN a embauché un directeur des opérations sécurité chargé de ce programme. L'ICANN fournit des actifs informationnels, des services et une technologie pour soutenir l'IANA et d'autres opérations cruciales. Les efforts récents se sont concentrés sur la réévaluation, la documentation et le déploiement de processus et de politiques de sécurité plus robustes. *Le plan de sécurité de l'information de l'ICANN est testé conformément aux normes ISO 27002 et les améliorations visant au soutien des procédures et processus sont en cours. Le plan de sécurité de l'information de l'ICANN comprend également la remise du plan de sécurité de l'information de l'IANA au Ministère du commerce des E.U. et la gestion de la réalisation des audits indépendants de son programme. La planification de l'ICANN en matière de sécurité du personnel et des actifs se concentre sur la protection du personnel et des installations de l'ICANN telle que requise pour que l'ICANN mène à bien ses diverses activités mondiales. Ceci inclut l'assurance sécurité lors des conférences mondiales de l'ICANN. L'ICANN a établi un processus de planification pour gérer les risques liés à la sécurité de l'ensemble de l'entreprise et s'appuie*

sur sa propre équipe interne de sécurité ainsi que sur le soutien de ses conseillers en sécurité.

Les programmes de sécurité de l'ICANN s'intègrent au programme général de gestion des risques de l'entreprise supervisé par le Conseil d'administration de l'ICANN, ainsi qu'aux programmes réciproquement solidaires de continuité des affaires de l'entreprise. L'ICANN a affiné ses processus de gestion des risques en établissant des directives de gestion des risques pour l'organisation, en mettant en place une équipe chargée de superviser la gestion des risques et en effectuant des évaluations régulières des risques portant sur les principaux risques organisationnels et, enfin, en rédigeant des rapports de gestion des risques se rapportant aux initiatives essentielles de l'ICANN.

A mesure que l'ICANN se développe, les actifs de l'entreprise augmentent en parallèle à son activité mondiale et à son profil public. L'ICANN continue à souligner l'importance d'une saine gestion des risques, de la continuité des affaires et de la sécurité en tant que composantes principales de ses processus d'entreprise.

5.6 Activités des organisations de soutien et des comités consultatifs de l'ICANN

La communauté élargie de l'ICANN joue également un rôle essentiel dans la facilitation de la sécurité, stabilité et résilience des systèmes d'identificateurs uniques à travers un processus de politiques ascendant. Les trois organisations de soutien de l'ICANN – l'organisation de soutien aux politiques des noms génériques (GNSO), l'organisation de soutien aux politiques de codes de pays (ccNSO), et l'organisation de soutien aux politiques d'adressage (ASO) - sont responsables de l'élaboration des politiques de sorte à inclure les sujets liés à la sécurité et à la stabilité. Les détails concernant chacune des organisations de soutien et les processus respectifs peuvent être consultés aux adresses http://gnso.icann.org, http://ccnso.icann.org/, et http://aso.icann.org/. Ces organisations font des recommandations qui doivent être approuvées par le Conseil d'administration de l'ICANN afin d'être mises en œuvre à travers une variété de contrats, d'accords, de protocoles d'entente (MoU) et d'activités du personnel. Les domaines clés du ressort du GNSO comprennent les politiques liées aux accords de registres et bureaux d'enregistrement gTLD devant inclure, entre autres, la considération de tous changements de politiques relatifs au Whois des gTLD, l'examen des problèmes causés par

l'hébergement 'fast flux', les questions d'expiration des noms de domaine, les transferts de noms de domaine entre bureaux d'enregistrement et les politiques relatives aux enregistrements frauduleux.

L'ICANN est actuellement en train de collaborer avec la communauté pour réviser le processus d'élaboration de politiques (PDP) existant et relatif aux gTLD afin de le rendre plus efficace et plus proche des besoins d'élaboration de politiques de l'ICANN. Les nombreuses révisions envisagées des PDP actuels comprennent des changements orientés vers l'apport d'une plus grande expertise et recherche technique et vers un établissement des faits assez tôt dans le cadre du processus afin d'aider à définir et à cibler les défis difficiles d'une manière plus informée et mieux documentée ; et vers l'élaboration de meilleurs moyens d'évaluation de l'efficacité des nouvelles politiques.

Le ccNSO facilite la collaboration de l'ICANN avec les ccTLD visant, entre autres, à un partage des informations liées à la sécurité, la stabilité et la résilience.

L'ASO coordonne l'élaboration de politiques portant sur l'attribution par l'IANA d'adresses IP et de numéros SA aux RIR. Les différentes communautés RIR élaborent ces politiques mondiales. Il est du ressort de l'ASO de prendre ces politiques élaborées au niveau régional et de les coordonner en une politique mondiale unique. Cette dernière est ensuite transmise au Conseil d'administration de l'ICANN pour ratification.

En outre, l'ICANN a quatre comités consultatifs qui fournissent des conseils au Conseil d'administration et à la communauté de l'ICANN : le comité consultatif At-Large (ALAC), le comité consultatif gouvernemental (GAC), le comité consultatif sur le système de serveurs racine (RSSAC), et le comité consultatif pour la sécurité et la stabilité (SSAC). Les détails concernant les fonctions, les processus et les activités de ces comités peuvent être consultés à l'adresse http://www.icann.org/en/committees/. Ces comités consultatifs collaborent souvent à travers l'ensemble de la structure d'organisations de soutien / comités consultatifs dans le cadre de divers efforts et notamment avec le SSAC. Les comités sont assistés par le personnel de l'ICANN chargé des politiques dans la réalisation des études, l'organisation de débats et la formulation de recommandations.

Le SSAC conseille la communauté et le Conseil d'administration de l'ICANN sur des sujets liés à la sécurité et à la stabilité des systèmes de nommage et d'adressage de l'Internet. Ces sujets se rapportent entre autres au fonctionnement correct et fiable du système de nom racine, à l'attribution d'adresses et de numéros

Internet, et aux services de registres et bureaux d'enregistrement tels que le Whois. Le SSAC se livre à une évaluation continue des menaces et à une analyse des risques des services de nommage et d'attribution d'adresses Internet pour localiser les principales menaces à la sécurité et à la stabilité et conseiller la communauté de l'ICANN en conséquence. Les détails des activités du SSAC peuvent être consultés à l'adresse www.icann.org/en/committees/security.

A part les activités mentionnées plus haut, les autres activités en cours au sein des organisations de soutien et des comités consultatifs comprennent les discussions communes réunissant ces groupes lors des conférences de l'ICANN pour discuter des problèmes d'intérêt commun liés à la sécurité et à la stabilité, l'organisation d'ateliers et de séances d'information sur la sécurité et la stabilité, et la communication d'activités liées aux politiques à l'ensemble de la communauté au moyen de la mise à jour mensuelle des politiques (http://www.icann.org/en/topics/policy/).

Le travail stratégique pertinent du GNSO comprend :

Fast Flux : Un processus d'élaboration de politique (PDP) du GNSO sur l'hébergement 'fast flux' a été achevé en septembre 2009. Le rapport du groupe de travail a examiné qui profitait du 'fast flux' et qui était lésé, comment les internautes étaient-ils affectés par l'hébergement 'fast flux' et la mesure dans laquelle les changements techniques et de politiques relatifs au DNS réduisaient les effets négatifs de l'hébergement 'fast flux'. En septembre 2009, le GNSO a adopté une motion pour créer un groupe de rédaction chargé de rédiger un plan de travail pour mettre en œuvre les recommandations proposées par le groupe de travail.

Transferts :

Le conseil du GNSO a un groupe de travail qui se concentre sur le troisième des six efforts d'élaboration de politiques prévus pour traiter des divers aspects des transferts entre bureaux d'enregistrement. Le groupe de travail sur la partie B de l'IRTP traite cinq problématiques portant plus particulièrement sur le piratage de noms de domaine, l'annulation urgente d'un transfert non approprié et l'utilisation du 'statut de verrouillage'. Le groupe de travail sur la partie B de l'IRTP a publié son rapport initial le 29 mai (http://www.icann.org/en/announcements/announcement-05jul10-en.htm). Le rapport comprend, entre autres, la recommandation d'une politique accélérée d'annulation de

transfert et la recommandation de réalisation d'une étude sur les exigences d'un Whois substantiel pour tous les gTLD. Suite à la clôture de la période de consultation le 8 août, le groupe de travail passera en revue les commentaires reçus et entamera la finalisation de son rapport pour le soumettre ensuite au conseil du GNSO.

Enregistrements frauduleux :

Lancé en février 2009, le groupe de travail sur les politiques en matière d'enregistrements frauduleux (RAP) a été chargé d'examiner ces politiques de plus près. Le groupe de travail RAP a examiné des questions telles que la définition de la différence entre enregistrement frauduleux et utilisation frauduleuse de nom de domaine, la définition des fraudes existantes, l'identification des avantages ou désavantages éventuels de l'adoption d'une approche plus uniforme dans les contrats et quels domaines, le cas échéant, seraient appropriés pour une élaboration de politique du GNSO qui traite des enregistrements frauduleux. Le groupe de travail RAP a soumis son rapport final au conseil du GNSO le 29 mai 2010 [http://www.icann.org/en/announcements/announcement-29may10-en.htm]. Le rapport comporte des recommandations concrètes visant à traiter les enregistrements frauduleux de noms de domaine dans les gTLD. Les recommandations portent entre autres sur :

- *le cybersquattage : recommandant le lancement d'un processus d'élaboration de politique pour examiner l'état actuel de la politique de règlement uniforme des litiges (UDRP).*
- *les problèmes d'accès au WHOIS : recherchant des moyens permettant d'assurer l'accessibilité des données du WHOIS de manière adéquatement fiable, applicable et cohérente ; et demandant que le service de conformité de l'ICANN publie des données concernant l'accessibilité du WHOIS.*
- *l'usage malveillant de noms de domaine : recommandant la création de meilleures pratiques pour aider les bureaux d'enregistrement et les registres à traiter l'usage illicite de noms de domaine.*

- *les faux avis de renouvellement : recommandant des mesures d'exécution éventuelles de la part du service de conformité de l'ICANN*
- *les enregistrements frauduleux dans plusieurs TLD à la fois : recommandant la coordination de la surveillance et de la recherche avec la communauté*
- *l'uniformité des contrats : recommandant la création d'un rapport sur les problématiques afin d'évaluer l'éventualité d'établissement d'un minimum de dispositions de base relatives aux enregistrements frauduleux dans tous les accords pertinents de l'ICANN.*
- *les pratiques à l'échelle du GNSO pour rassembler et diffuser les meilleures pratiques et pour l'uniformité des rapports.*
- *le délit d'initié*
- *le 'domain kiting'*
- *les noms de domaine trompeurs et/ou injurieux*

Ayant examiné les recommandations, le conseil du GNSO a décidé d'établir une équipe de rédaction chargée de rédiger une proposition d'approche relative aux recommandations contenues dans le rapport. Cette proposition d'approche pourrait comprendre des échéances pour l'établissement de groupes qui seraient chargés d'examiner certaines des recommandations du rapport final et de la façon de traiter les recommandations qui n'ont pas obtenu de consensus unanime.

Récupération des noms de domaine après leur expiration : En mai 2009, le conseil du GNSO avait lancé un PDP sur la récupération des noms de domaine après leur expiration. Ce groupe de travail traite des questions relatives à la mesure dans laquelle les titulaires de noms de domaine devraient pouvoir réclamer leurs noms de domaine après leur expiration. La question est de savoir dans quelle mesure les politiques actuelles des bureaux d'enregistrement en matière de renouvellement, de transfert et de suppression de noms de domaine ayant expiré, sont-elles adéquates.

Améliorations du RAA : En mai 2009, le Conseil d'administration de l'ICANN a approuvé une révision de l'accord d'accréditation de bureaux d'enregistrements (RAA) (http://www.icann.org/en/topics/raa/). Le nouvel RAA comprend une obligation de vigilance accrue de la part des bureaux d'enregistrement et de leurs affiliés, l'identification de bureaux

d'enregistrement éventuellement impliqués dans des activités de cybersquattage et autres conduites malveillantes, des exigences et des obligations de données WHOIS renforcées concernant les fournisseurs de services d'anonymisation et d'intermédiation et des exigences d'identification des points de contact en cas d'abus pour pouvoir signaler les cas de conduite malveillante impliquant le DNS. *Des représentants des agences d'application de la loi, l'ALAC et d'autres groupes de parties prenantes participent à la recherche d'améliorations supplémentaires à apporter au RAA (voir http://www.icann.org/en/announcements/announcement-28may10-en.htm), et ont présenté des propositions de modifications lors de la conférence de l'ICANN à Bruxelles en juin 2010.*

Données d'enregistrement internationalisées : Actuellement, il n'existe pas de normes ou de directives qui définissent comment les données d'enregistrement de noms de domaine internationalisées devraient être composées et affichées. Un groupe de travail SSAC-GNSO commun a été réuni par le Conseil d'administration de l'ICANN afin d'étudier la faisabilité et l'à-propos de l'introduction de spécifications d'affichage pour les données d'enregistrement internationalisées. Le groupe sollicitera les opinions des regroupements intéressés y compris les opérateurs de ccTLD, le ccNSO, l'ASO, l'ALAC et le GAC au cours des discussions afin d'obtenir la plus grande contribution possible de la part de la communauté. La série initiale d'objectifs du groupe de travail sur l'IRD vise à comprendre et à s'accorder sur les types, les genres et les codages des données d'enregistrement que les parties contractantes rassembleraient, afficheraient et maintiendraient.

6. Plans de l'exercice financier 2011 de l'ICANN pour renforcer la sécurité, la stabilité et la résilience

Les activités de l'ICANN liées au renforcement de la sécurité, de la stabilité et de la résilience et les ressources attribuées à ces efforts, sont guidées par les processus de planification stratégique et opérationnelle. Pour l'exercice financier 2011, les activités de l'ICANN comprendront un nombre d'initiatives clés, telles que :

- ***Opérations de l'IANA*** – recommander, éduquer et compléter la mise en œuvre des DNSSEC au niveau racine tel que proposé dans le plan stratégique de l'ICANN pour 2010-2013 ainsi qu'améliorer la gestion de la zone racine par le biais de l'automatisation ; et authentification améliorée des communications avec les gestionnaires de TLD.
- ***Opérations du serveur racine du DNS –*** poursuivre la recherche de reconnaissance mutuelle des rôles et des responsabilités et entreprendre un effort bénévole pour la mise en œuvre de plans d'opérations en cas d'imprévus et d'exercices.
- ***Registres gTLD –*** veiller à ce que l'évaluation des candidats aux nouveaux gTLD et IDN prenne toujours en compte la sécurité des opérations. L'ICANN affinera le plan de continuité des registres gTLD et testera le système de sauvegarde des données.
- ***Registres ccTLD –*** l'ICANN renforcera sa collaboration sur l'affinage du programme de renforcement des capacités DNS, y compris le programme conjoint de planification des réponses aux attaques et aux imprévus (ACRP) et le programme de formation aux opérations de registre établi conjointement avec le ccNSO et les associations de TLD régionales.
- ***Conformité contractuelle –*** l'ICANN continuera à renforcer le champ des activités d'application contractuelle impliquant les gTLD pour inclure le lancement d'audits des parties contractantes dans le cadre de la mise en œuvre du RAA 2009 et identifier l'implication potentielle de parties contractantes dans des activités malveillantes pour agir en conséquence.
- ***Réponse à l'abus malveillant du système de noms de domaine*** - l'ICANN tirera parti de ses efforts collectifs portant sur la conduite malveillante favorisée par l'utilisation du DNS et facilitera le partage d'informations pour permettre une réaction efficace.

- ***Opérations de sécurité et continuité internes de l'ICANN*** – l'ICANN veillera à ce que ses programmes de sécurité soient réalisés dans l'ensemble des programmes de gestion des risques d'entreprise, de gestion des crises, et de continuité des activités. Un accent spécial sera mis sur la mise en œuvre des plans et procédures de soutien nécessaires.
- ***Assurer l'engagement et la coopération au niveau mondial*** – l'ICANN renforcera les partenariats pour inclure le groupe de travail de l'ingénierie Internet (IETF), la société Internet (ISOC), les registres Internet régionaux et les groupes d'opérateurs de réseaux, le centre d'opérations, d'analyse et de recherche du DNS (DNS-OARC) et le forum des équipes de réaction aux incidents concernant la sécurité des systèmes d'information (FIRST). L'ICANN prendra également part à des dialogues au niveau mondial afin de promouvoir la compréhension des défis liés à la sécurité, la stabilité et la résilience auxquels l'écosystème d'Internet est confronté et la manière de relever ses défis par le biais d'approches multipartites.

La série complète d'activités est expliquée ci-suit. L'annexe A fournit des détails sur les objectifs spécifiques, les partenaires, les produits livrables et les engagements en matière de ressources au cours de l'exercice financier 2011.

6.1 Fonctions essentielles DNS/adressage

6.1.1 Opérations de l'IANA

L'ICANN continuera à exécuter les fonctions de l'IANA et à œuvrer pour améliorer l'excellence opérationnelle de ces opérations en collaboration avec le Ministère du commerce des E.U., VeriSign, les RIR et les opérateurs de TLD.

Les initiatives spécifiques d'amélioration des fonctions de l'IANA comprennent :

- l'amélioration de la gestion de la zone racine par le biais de l'automatisation (logiciel eIANA/RZM) ; l'authentification améliorée des communications avec les gestionnaires de TLD ; et les révisions des processus et pratiques en vue des considérations de sécurité et d'optimisation.
- le soutien au développement et à la mise en œuvre d'attributions et d'affectations d'adresses IP sûres par le biais de rPKI ou d'autres mécanismes adoptés par les RIR et la communauté de routage Internet pour inclure une assistance

continue au groupe de travail du référentiel SIDR (Secure Intelligence Data Repository) de l'IETF.

- la collaboration avec les communautés techniques et opérationnelles pour identifier, analyser et éventuellement mettre en œuvre des exigences ou des normes techniques supplémentaires afin d'améliorer la sécurité, la stabilité et la résilience du DNS.

Dans le cadre des améliorations globales de la résilience, l'ICANN a effectué un exercice de continuité de l'IANA en janvier 2010, mettant ainsi à l'épreuve le basculement des services de l'IANA depuis Marina del Rey en Californie à Reston en Virginie. L'exercice a démontré les capacités de basculement et les mécanismes de communications pour garantir la disponibilité des services de l'IANA. L'ICANN améliorera la résilience des services de l'IANA en 2010-2011.

6.1.2 Opérations DNS

L'ICANN, le ministère du Commerce des E.U. et VeriSign ont réalisé une étape importante en 2010 quant à la mise en œuvre des DNSSEC dans la zone racine. Selon la priorité indiquée dans le plan stratégique pour 2010-2013, l'ICANN poursuivra ses efforts soutenant l'introduction des DNSSEC par les opérateurs de TLD et autres au cours de l'exercice FY 11.

L'ICANN poursuivra également une série d'activités permettant d'élargir la mise en œuvre des DNSSEC pour couvrir le DNS au niveau mondial, en collaborant avec des experts du DNS et des opérateurs expérimentés. L'ICANN veillera à ce que ses programmes y compris les transferts entre bureaux d'enregistrement et les sauvegardes de données prennent cette mise en œuvre en compte. Elle poursuivra par ailleurs les discussions avec les parties prenantes concernant la mise en œuvre. L'ICANN continuera à maintenir le référentiel d'ancres de confiance pour les domaines de premier niveau (ITAR) de l'IANA jusqu'à ce la zone racine soit signée. L'ICANN continuera à rechercher l'autorisation de signer les zones .int et .arpa. L'ICANN soutiendra la mise en œuvre des DNSSEC en signant les zones gérées par l'ICANN (y compris icann.org et iana.org), et en facilitant le partage des leçons acquises parmi les parties impliquées dans la mise en œuvre des DNSSEC.

L'ICANN cherche également à favoriser l'établissement de mécanismes plus robustes pour la coordination en tant que membre de la communauté d'opérateurs de serveurs racine concernant les mesures qui pourraient contribuer à la sécurité, la stabilité et la résilience. En sa qualité d'opérateur L, l'ICANN

prévoit de collaborer avec d'autres opérateurs de serveurs racine pour démarrer un effort bénévole de réalisation de plans et d'exercices visant à améliorer la résilience des systèmes de serveurs racine contre une variété d'imprévus significatifs.

L'ICANN prévoit de poursuivre les améliorations de l'exploitation de la racine L. En outre, l'ICANN a chargé le DNS-OARC d'étudier l'impact des changements y compris de la mise en œuvre des nouveaux gTLD et IDN, de la mise en œuvre de l'IPv6, et de la mise en œuvre éventuelle de la signature DNSSEC de la zone racine, sur l'exploitation d'un seul serveur racine basée sur le modèle racine L. Plus généralement, le RSSAC et le SSAC sont en train de réaliser une étude conjointe de la sécurité et stabilité des serveurs racine à la lumière des changements prévus et décrits en détail à la section 6.6.

6.2 Relations avec les registres et les bureaux d'enregistrement TLD

6.2.1 Registres gTLD

L'ICANN poursuivra la coordination contractuelle liée aux opérations de gTLD pour inclure la revue des candidatures aux nouveaux services via RSEP. Lorsque le processus de nouveaux gTLD sera opérationnel, l'ICANN s'attend à ce que les revues comportent des propositions qui requièrent l'activation du RSTEP pour évaluer les questions de sécurité, de stabilité et de résilience. L'ICANN poursuivra ses efforts pour encourager la collaboration de la communauté et l'utilisation des meilleures pratiques liées à la sécurité, la stabilité et la résilience à travers la réalisation par l'ICANN d'ateliers réunissant registres et bureaux d'enregistrement au niveau régional, la participation à une variété de forums de la communauté, et le partage d'informations sur son propre site Web. En 2010, l'ICANN a introduit à son tableau de bord à l'adresse de la communauté, des signalements améliorés des données relatives aux registres gTLD (http://www.icann.org/idashboard/public/).

6.2.2 Nouveaux gTLD

La mise en place potentielle de processus liés à l'établissement des nouveaux gTLD représentera le centre d'intérêt principal de la sécurité, stabilité et résilience au cours de l'année prochaine. En février 2009, le Conseil d'administration de l'ICANN a chargé le RSSAC et le SSAC de réaliser conjointement une étude des implications potentielles en matière de sécurité, stabilité et

résilience sur le système de serveurs racine en tant qu'ensemble, en ce qui concerne une série de changements potentiels au sein du DNS y inclus la mise en œuvre des nouveaux gTLD et IDN, en même temps que la mise en œuvre éventuelle de la signature DNSSEC de la zone racine. Leurs rapports sont attendus en 2010. Dans le cadre du processus relatif aux nouveaux gTLD, l'ICANN établira également les dispositions relatives à l'évaluation des candidats pour s'assurer qu'ils sont en mesure de mettre en œuvre des opérations techniquement sûres, conformes aux dispositions Whois, qu'ils peuvent mettre en place un plan d'opérations solide et garantir la protection des titulaires de noms de domaine. L'ICANN continuera à affiner le plan de continuité des registres gTLD et le programme d'exercices. L'ICANN veillera également à ce que le système de candidature automatisée aux TLD soit mis en place et géré de manière sûre.

6.2.3 IDN

Dans le même esprit, les efforts de l'ICANN visant à faciliter la mise en œuvre des TLD IDN (ccTLD et gTLD) veilleront à ce que ces nouveaux noms de domaine représentés par des caractères de langues locaux soient sûrs, stables et résilients. L'ICANN soutient le travail de mise à jour des directives IDN devant être suivies par les opérateurs de TLD IDN et l'exploitation des IDN de deuxième niveau. L'ICANN continuera à faciliter les efforts des registres en collaborant avec les distributeurs pour veiller à ce que des tableaux IDN soient établis, ce qui limite dans la mesure du possible les conflits et confusions de chaînes, et réduit les possibilités de mauvais usage du système à des fins malveillantes. Une fonction de soutien centrée sur les IDN sera mise à la disposition des parties intéressées à devenir des opérateurs de TLD IDN et en quête d'assistance et d'expertise dans ce domaine.

L'ICANN communique également avec des experts pour garantir une introduction stable de TLD IDN dans les pays et territoires qui ont plus d'une langue ou d'une écriture et auront besoin de mise en œuvre synchronisée. Ceci comprend également la collaboration avec les parties prenantes, à savoir les développeurs de navigateurs et d'applications, les opérateurs de registres IDN et autres afin de soutenir l'introduction des IDN.

6.2.4 ccTLD

L'ICANN poursuivra ses efforts visant à renforcer la sécurité, stabilité et résilience des ccTLD par le biais de sa collaboration avec les opérateurs de ccTLD. Ces activités se concentreront au cours de l'année prochaine sur l'affinage du programme de renforcement des capacités DNS, y compris le programme d'ateliers sur la planification des réponses aux attaques et aux

imprévus (ACRP), établi conjointement avec le ccNSO et les associations de TLD régionales. Le programme de renforcement de capacités DNS se concentre sur la sécurité et la résilience améliorées à travers une planification proactive et des aptitudes de réponse renforcées face à une gamme complète de menaces et de risques perturbateurs. Le programmes se prolongera au cours de l'année prochaine pour inclure une formation technique sur l'amélioration de la sécurité et de la résilience face aux menaces grandissantes et pour fournir une aide au développement de programmes d'exercices et d'évaluation du plan d'opérations et de sécurité des ccTLD.

6.2.5 Bureaux d'enregistrement

La communauté examine de plus près les améliorations relatives aux exigences d'accréditation des bureaux d'enregistrement et de sauvegarde des données, introduites dans les améliorations du RAA. En plus de l'assistance à ces efforts, le personnel de l'ICANN continuera à élaborer des procédures et des processus au sein des cadres contractuels et de politiques existants pour protéger les bureaux d'enregistrement et renforcer, en fin de compte, la sécurité, la stabilité et la résilience du DNS. En particulier, le travail est déjà entamé pour durcir les procédures de candidature à l'accréditation, établir des RAA aux exigences d'éligibilité et aux règles de disqualification accrues, et développer des procédures qui permettent aux bureaux d'enregistrement de se retirer du marché des bureaux d'enregistrement de manière responsable. Le travail précédent sur le développement des procédures de sauvegarde des données et de résiliation des bureaux d'enregistrement renforcera également les efforts actuels et futurs de l'ICANN en matière de mise en application de la conformité, permettant ainsi une résiliation d'accréditation de bureau d'enregistrement dans les cas où les actes dudit bureau d'enregistrement menaceraient la sécurité et la stabilité du DNS. L'ICANN continuera à bâtir une communauté de bureaux d'enregistrement puissante par le biais de manifestations de sensibilisation qui permettent le partage des meilleures pratiques dans le domaine. L'ICANN commencera à établir de nouveaux réseaux de communication pour aider les bureaux d'enregistrement dans le signalement opportun et la réponse aux menaces cruciales contre la sécurité.

6.2.6 Conformité contractuelle

L'ICANN continuera à élargir le champ des activités d'application contractuelle. Les activités comporteront des audits des parties contractantes dans le cadre de la mise en œuvre du RAA 2009. De plus, le personnel chargé de la conformité contractuelle

collaborera avec l'équipe sécurité de l'ICANN pour identifier les parties contractantes qui prennent possiblement part à des activités malveillantes. Dans les cas où les parties contractantes ont pris part à des activités malveillantes, des mesures de mise en application du contrat peuvent être prises. Dans tous les autres cas, les organismes d'application de la loi et autres agences compétentes seront informés afin de traiter ces sujets comme il se doit.

Le service de conformité contractuelle a réalisé des études d'évaluation de l'exactitude des coordonnées de contact Whois au sein du système gTLD et d'évaluation de la mesure dans laquelle les titulaires de noms de domaine utilisent les services de confidentialité et d'anonymisation pour abriter leur identité. Dans un effort visant à encourager la conformité contractuelle et à assurer la confiance du public, le service de conformité contractuelle développe un système d'identification publique des parties conformes. Ce système se trouve à son premier stade de développement. Les commentaires des communautés de bureaux d'enregistrement et de registres seront sollicités avant qu'il ne soit mis en œuvre.

6.2.7 Réponse collective à l'abus malveillant du système de noms de domaine

Le personnel de l'ICANN continuera à tirer parti des efforts collectifs nés en réponse aux évènements récents associés au système de noms de domaine depuis la fin de 2008 tels que les activités déployées autour du réseau de zombies Szirbi et du ver Conficker fin 2008/début 2009. L'ICANN envisage que cette collaboration implique les registres et bureaux d'enregistrement du DNS, la communauté active dans la recherche sécurité et les distributeurs de logiciels et de logiciels antivirus. En particulier, l'ICANN prévoit de collaborer avec les communautés de registres et de bureaux d'enregistrement pour renforcer les approches collectives dans la lutte contre la propagation des programmes malveillants, des vers et des réseaux de zombies qui utilisent le DNS pour la propagation et le contrôle. L'ICANN cherchera à déterminer des procédures pour la communication et la validation des activités de registres et de bureaux d'enregistrement ainsi que pour examiner la manière de participer au partage d'informations avec les chercheurs de la sécurité, les distributeurs de technologie et les organismes d'application de la loi, le cas échéant. L'ICANN sollicitera les commentaires du public sur les procédures relatives au démarrage d'activités de réaction collective. Ces procédures seront soumises à l'approbation du Conseil d'administration. Ces approches permettront à l'ICANN d'être plus proche de la variété de parties prenantes qui

pourraient rechercher son engagement et sa collaboration au niveau mondial.

6.2.8 Faciliter la sécurité dans l'ensemble du DNS

Le personnel de l'ICANN cherchera à tirer parti des symposiums sur la sécurité, la stabilité et la résilience du DNS de février 2009 et de février 2010, en facilitant les efforts collectifs majeurs liés à la réduction des risques opérationnels pour les opérateurs et les utilisateurs du DNS. Les plans comprennent l'organisation d'un symposium annuel qui examinerait les risques partout dans le DNS et le renforcement des occasions de collaboration dans le but permanent de relever les défis liés à l'assurance de la sécurité et de la stabilité du DNS dans le monde en développement. L'ICANN prévoit également de collaborer avec le DNS-OARC et les équipes du FIRST (Forum of Incident Response and Security) en mettant l'accent sur le mode d'orchestration de réponses efficaces aux évènements et imprévus significatifs au sein de la communauté du DNS. De plus, le personnel de l'ICANN continuera à suivre la progression des plans pour la mise en place d'un système de nommage d'objet (ONS) et la mesure dans laquelle de tels plans pourraient impliquer le DNS pour veiller à ce que les problèmes potentiels liés à la sécurité, la stabilité et la résilience soient identifiés au plus tôt.

6.3 Sensibilisation sur la sécurité au niveau mondial

6.3.1 Élargir les partenariats existants

L'essentiel de la stratégie d'engagement mondial de l'ICANN en matière de sécurité, de stabilité et de résilience est de se baser sur et d'utiliser le travail existant réalisé par l'équipe de partenariats mondiaux et d'élargir les partenariats puissants. Les activités spécifiques prévues avec ces partenaires au cours de l'exercice 2011 comprennent :

- ***Société Internet (ISOC)*** - l'ICANN prévoit de collaborer dans la mise au point du programme commun en cours ISOC/ICANN pour fournir une formation aux opérateurs de TLD avec des plans supplémentaires portant sur la prestation d'une formation technique sur les moyens d'améliorer la sécurité et d'atténuer les attaques électroniques et les perturbations.
- ***DNS-OARC*** – l'ICANN poursuivra sa collaboration avec le DNS-OARC et d'autres parties prenantes intéressées en soutenant les initiatives stratégiques dans le domaine SSR et le concept

DNS-CERT. L'ICANN a aussi communiqué avec les organisations pour réaliser des programmes éducationnels et de formation en partenariat avec d'autres afin d'améliorer la compréhension du fonctionnement des systèmes d'identificateurs uniques, du rôle de l'ICANN et des défis inhérents à la gestion des risques de ces systèmes.

6.3.2 Entreprise commerciale

L'ICANN tirera parti des symposiums de février 2009 et 2010 sur la sécurité, la stabilité et la résilience du DNS pour comprendre la dépendance de l'entreprise vis-à-vis du DNS et les risques y associés. Au cours de l'année prochaine, les efforts déployés pour la sécurité, la stabilité et la résilience seront incorporés au programme de sensibilisation du chef de la direction de l'ICANN dans le but d'assurer l'incorporation d'un large éventail de perspectives d'entreprise.

6.3.3 Participation au dialogue cybersécurité mondial

L'ICANN prendra part à ces dialogues pour veiller à une compréhension claire de son rôle et de ses contributions spécifiques. Les activités spécifiques envisagées par l'ICANN dans ce domaine au cours de l'année à venir comprennent :

- ***Forum des équipes de réaction aux incidents concernant la sécurité des systèmes d'information (FIRST)*** - l'ICANN et FIRST ont organisé en mars 2010 un atelier commun sur la sécurité Internet à Nairobi au Kenya destiné aux équipes africaines de réaction aux incidents. L'ICANN collabore avec FIRST dans le cadre d'un sondage des équipes de réponse aux urgences informatiques au cours de l'exercice FY 11 et participe aux programmes de FIRST.
- ***Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)*** - l'ICANN prévoit une collaboration avec l'ENISA dans le cadre d'un exercice électronique européen et d'activités de réponse aux incidents informatiques.
- ***Forum sur la gouvernance de l'Internet (IGF)*** - l'ICANN participera à la conférence de l'IGF à Vilnius en Lituanie en septembre 2010 et appuiera la continuation de l'IGF par l'assemblée générale des N.U.

L'ICANN poursuivra activement les possibilités de collaboration avec d'autres groupes de réflexion et institutions académiques sur le leadership éclairé dans l'identification des défis liés à la sécurité, la stabilité et la résilience.

L'ICANN prévoit de poursuivre sa collaboration avec l'ASO (et par le biais de l'ASO, avec la NRO et les RIR) et de participer à des activités d'intérêt réciproque liées à la sécurité, la stabilité et la résilience. Le personnel de l'ICANN cherchera à communiquer avec la NRO concernant les activités collectives qui renforceraient l'assurance de sécurité, stabilité et résilience du DNS. Ces discussions comporteront la compréhension des vues de la NRO concernant le mauvais usage éventuel de l'espace d'adresses Ipv4 patrimonial et le besoin éventuel d'une politique mondiale qui aborderait les préoccupations identifiées.

6.4 Opérations de sécurité et continuité d'entreprise de l'ICANN

Le personnel de l'ICANN veillera à ce que ses programmes de sécurité soient réalisés dans l'ensemble des programmes de gestion des risques d'entreprise, de gestion des crises, et de continuité des activités. Un accent spécial continuera à être mis sur l'établissement d'un fondement solide de politiques et processus documentés et de procédures de soutien. Les initiatives récentes se sont concentrées sur les améliorations de la gestion du risque et le maintien de la continuité de l'ICANN en tant qu'entreprise, y compris la formalisation des plans de continuité des affaires/gestion des crises de l'ICANN et la réalisation d'exercices internes à l'ICANN conjointement avec d'autres activités pour inclure les exercices de continuité et préparations des rencontres gTLD. L'ICANN a commencé à utiliser des sites d'exploitation alternatifs physiquement répartis pour renforcer la continuité des affaires et la capacité de reprise sur sinistre de l'infrastructure TI de l'ICANN.

Dans le cadre de ses activités en cours en 2010, le personnel de l'ICANN continuera à améliorer la gamme complète de processus d'entreprise relatifs à l'information, au personnel et à la sécurité. Quant à la planification de la gestion des risques et de la continuité, l'accent sera spécialement mis sur l'établissement d'une base solide de plans documentés et de procédures de soutien. Les initiatives spécifiques mises en route en 2010 pour améliorer le maintien de la sécurité de l'ICANN comprennent des améliorations des contrôles d'accès physiques et logiques, de la gestion des changements, des procédures de secours informatique, d'audit et de journalisation, de la formation du personnel en matière de sensibilisation à la sécurité, de renforcement des capacités de réponse aux incidents et des améliorations de la sécurité des postes mobiles. Des plans de sécurité documentés pour le personnel et les conférences mondiales de l'ICANN ont été préparés. La validation et révision

externe de ces plans est programmée pour fin 2010. L'ICANN veillera au développement d'outils TI performants de collaboration et de sensibilisation de la communauté et à leur déploiement accompagné des procédures de sécurité appropriées.

L'ICANN prévoit la réalisation d'une révision et d'un audit indépendants de ses programmes de sécurité et de continuité au cours de la deuxième moitié de 2010.

6.5 Organismes de soutien et comités consultatifs de l'ICANN

Le SSAC prévoit de concentrer ses efforts futurs sur le déploiement des DNSSEC, la protection de l'enregistrement de domaines, la réduction du mauvais usage des noms de domaines et la stabilité du système d'adresses.

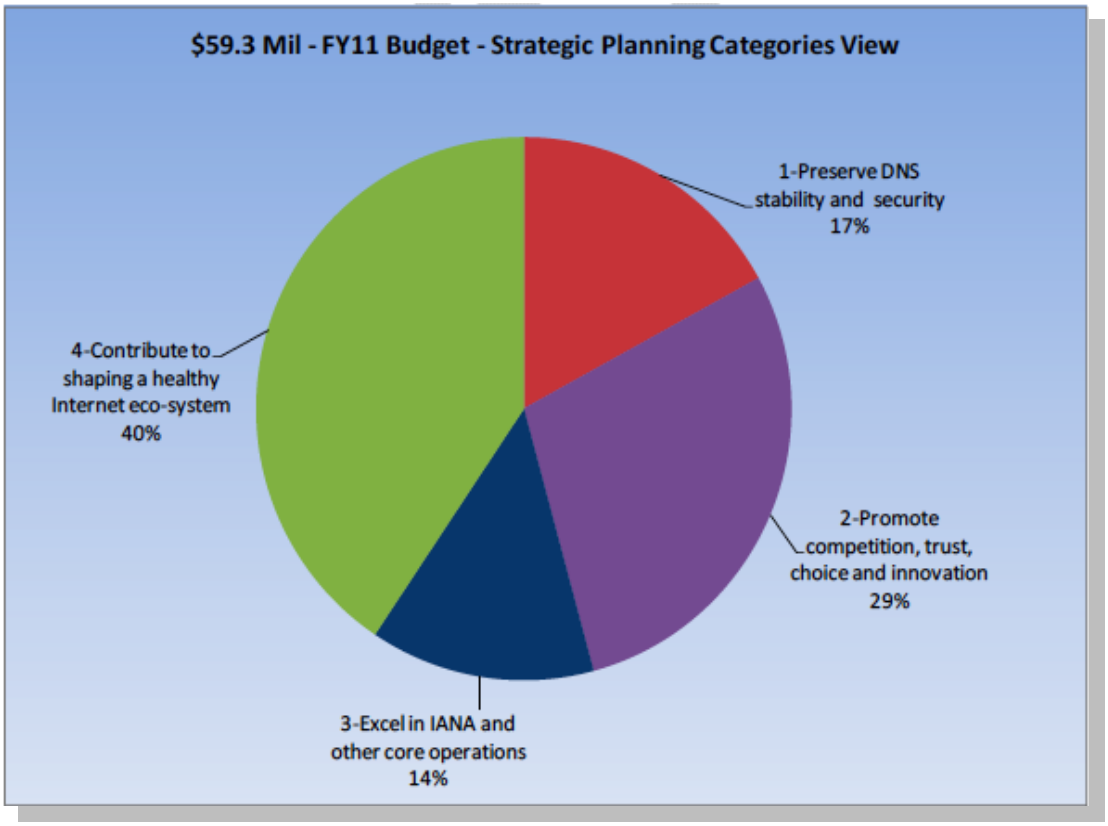
En janvier 2009, le Conseil du GNSO a présenté un rapport initial sur l'hébergement 'fast flux' proposé à la consultation publique et à l'attention du Conseil d'administration pour prise de mesures subséquentes. Il considère également un grand nombre d'études possibles des Whois relatifs. Le Conseil du GNSO a un groupe de travail qui se concentre sur le deuxième des six efforts d'élaboration de politiques prévus pour traiter des divers aspects des transferts entre bureaux d'enregistrement. Le GNSO a établi un groupe de travail sur les enregistrements frauduleux et envisage une initiative liée à la récupération de noms de domaine après leur expiration. Afin de réunir la grande variété de parties prenantes de l'ICANN ayant des intérêts dans ces sujets, plusieurs conférences internationales de l'ICANN ont comporté un atelier élargi sur la cybercriminalité et les enregistrements frauduleux (à Mexico, à Séoul, à Nairobi et à Bruxelles).

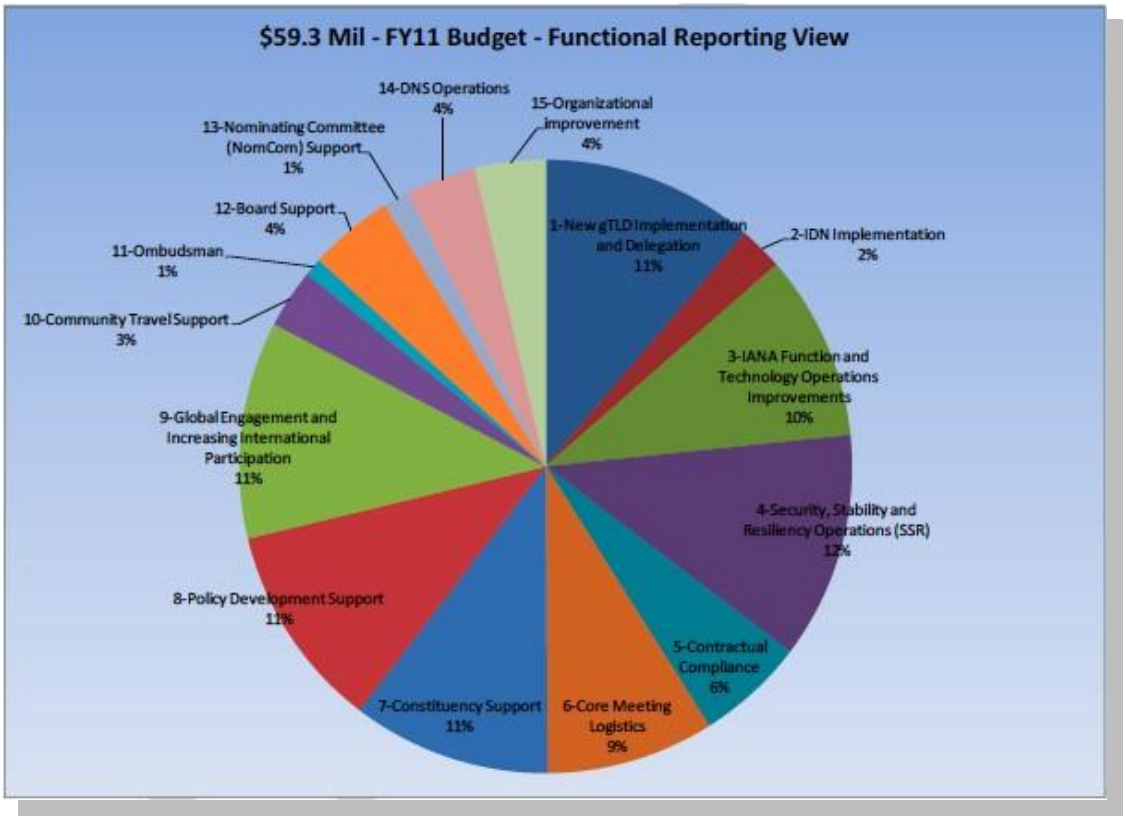
7. Conclusion

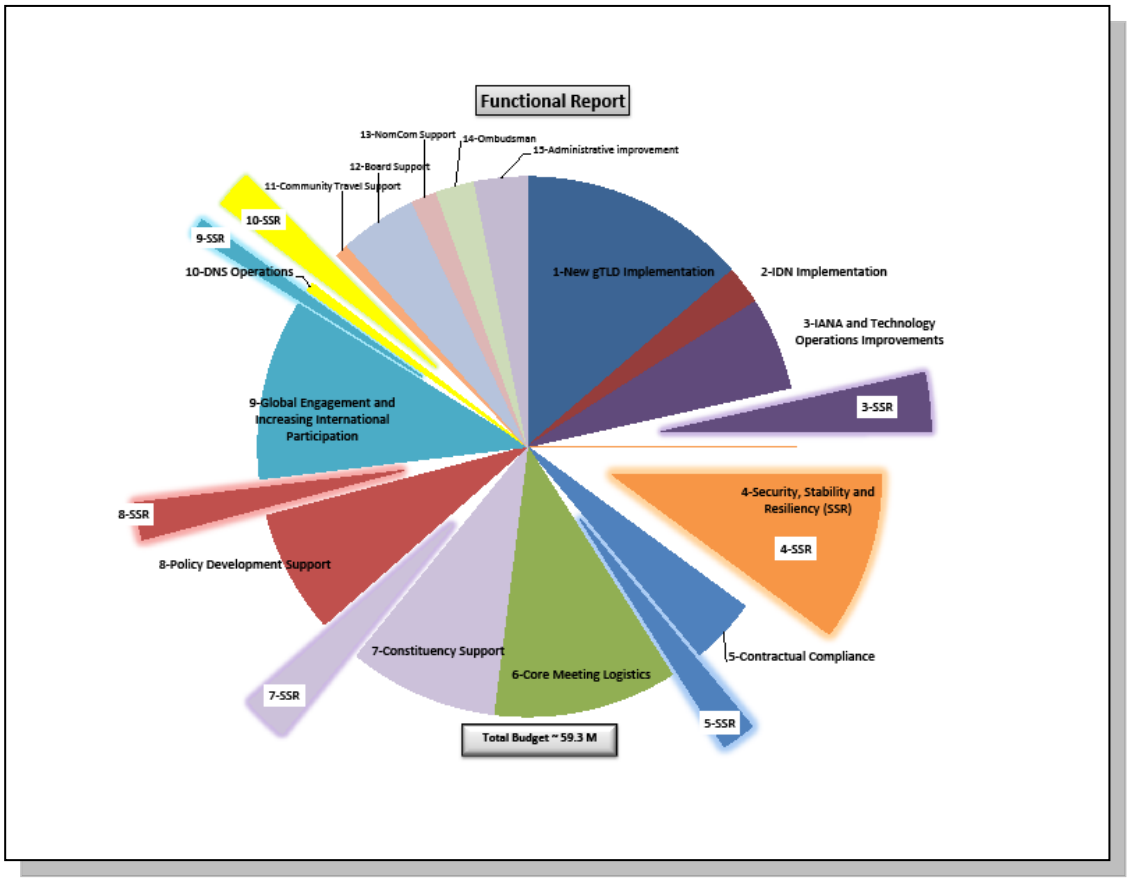
L'ICANN comprend qu'en tant qu'aspect fondamental de sa mission de fondation, ses programmes et activités doivent contribuer à faire des systèmes d'identificateurs uniques un aspect essentiel d'un environnement Internet plus sûr, stable et résilient. Les défis se développent et les efforts de l'ICANN dans ce domaine deviennent de plus en plus énergiques. L'ICANN reconnaît également les limites de son rôle et de ses ressources et planifie sa stratégie dans le domaine sur une base de collaboration intense. L'Internet s'est épanoui en tant qu'environnement mondial, encourageant l'innovation et se basant sur une coordination multipartite. La contribution de l'ICANN à l'amélioration de la sécurité, de la stabilité et de la résilience de ses systèmes d'identificateurs uniques se basera sur la même approche.

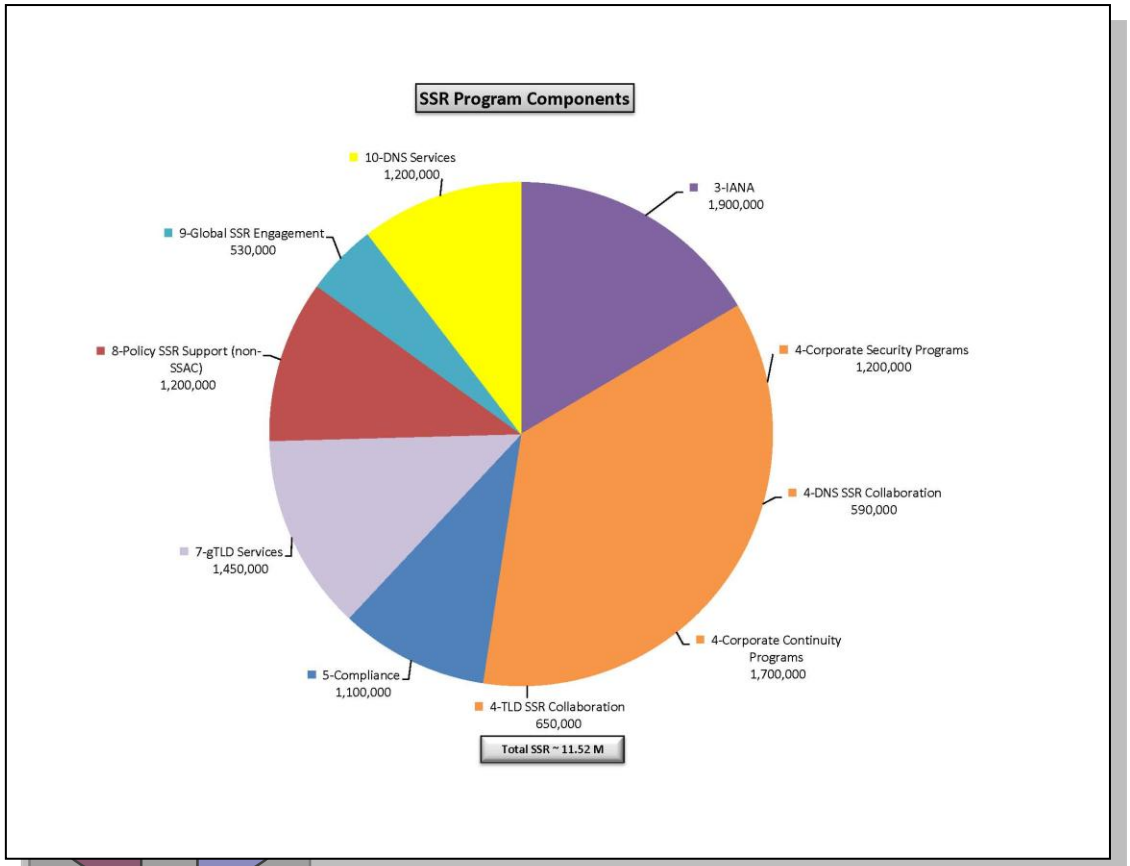
Depuis sa création, l'ICANN a réalisé des programmes et des activités visant à améliorer la sécurité, la stabilité et la résilience de l'Internet. Ceux-ci comprennent des efforts liés aux fonctions essentielles DNS/adressage ; à la collaboration avec les communautés de registres et de bureaux d'enregistrement TLD ; à la communication avec la NRO et les RIR ; aux programmes de sécurité et de continuité d'entreprise ; aux activités des organisations de soutien et des comités consultatifs, et à la participation aux activités mondiales et régionales portant sur la sécurité et la stabilité de l'Internet. L'intention de cette première version du plan est de fournir une base au développement du rôle de l'ICANN et du cadre autour duquel l'ICANN organise ses efforts de sécurité, de stabilité et de résilience. Le plan évoluera avec le temps, faisant partie du processus de planification stratégique et opérationnelle de l'ICANN, lui permettant de déployer des efforts toujours pertinents et de veiller à ce que ses ressources soient concentrées sur ses responsabilités et contributions les plus importantes.

Annexe A - Ressources SSR dans l'exercice financier 2011




$59.3 Mil - FY11 Budget - Functional Reporting View
14-DNS Operations 4%
15-Organizational improvement 4%
13-Nominating Committee (NomCom) Support 1%
12-Board Support 4%
11-Ombudsman 1%
10-Community Travel Support 3%
1-New gTLD Implementation and Delegation 11%
2-IDN Implementation 2%
3-IANA Function and Technology Operations Improvements 10%
4-Security, Stability and Resiliency Operations (SSR) 12%
5-Contractual Compliance 6%
6-Core Meeting Logistics 9%
7-Constituency Support 11%
8-Policy Development Support 11%
9-Global Engagement and Increasing International Participation 11%


Functional Report
13-NomCom Support
14-Ombudsman
15-Administrative improvement
12-Board Support
11-Community Travel Support
10-SSR
9-SSR
10-DNS Operations
1-New gTLD Implementation
2-IDN Implementation
3-IANA and Technology Operations Improvements
3-SSR
9-Global Engagement and Increasing International Participation
4-Security, Stability and Resiliency (SSR)
4-SSR
8-SSR
8-Policy Development Support
7-Constituency Support
6-Core Meeting Logistics
5-Contractual Compliance
7-SSR
5-SSR
Total Budget ~ 59.3 M


SSR Program Components
10-DNS Services
1,200,000
3-IANA
1,900,000
9-Global SSR Engagement
530,000
8-Policy SSR Support (non-SSAC)
1,200,000
4-Corporate Security Programs
1,200,000
4-DNS SSR Collaboration
590,000
7-gTLD Services
1,450,000
4-Corporate Continuity Programs
1,700,000
5-Compliance
1,100,000
4-TLD SSR Collaboration
650,000
Total SSR ~ 11.52 M

Exposé général des composantes principales du programme de sécurité, stabilité et résilience (SSR) de l'ICANN

- IANA - $1,9 M
- Services DNS - $1,2 M
- Collaboration SSR DNS - $590 mille
- Services gTLD - $1,45 M
- Conformité - $1,1 M
- Collaboration SSR TLD - $650 mille
- Engagement mondial SSR - $530 mille
- Programmes de sécurité d'entreprise - $1,2 M
- Programmes de continuité d'entreprise - $1,7 M
- Soutien aux politiques SSR (SSAC exclus) - $550 mille
- Soutien SSAC - $650 mille

TOTAL SSR - $11,52 M

Sécurité, stabilité et résilience de l'IANA (IANA)

Objectifs	Produits livrables (étapes importantes)
- Automatisation des éléments clés dans le processus de changement de la zone racine - Gestion des DNSSEC - Mise en œuvre rPKI à l'essai - Continuité des affaires	- Mise en œuvre de gestion zone racine automatisée (dépend des partenaires NTIA et VeriSign) - Mise en œuvre de la signature des DNSSEC de .arpa (la date dépend de la coordination avec l'IAB et la NTIA) - Coordination avec les évaluateurs rPKI - Plan de continuité de l'IANA (mis en place en janvier 2010, mise en place continue au cours de l'exercice financier 2011)
Parties prenantes principales	**Ressources**
- IANA, sécurité, TI - DOC/USG ; VeriSign - SSAC ; RSSAC - IETF ; communauté des opérateurs de DNS - RIR ; communauté des opérateurs de routage	- Humaines - 6,5 ETC (y compris 2,5 ETC pour le soutien TI et autre soutien de la part du personnel) - Financières - $1,9 M pour soutenir les ETC ; déplacement/soutien personnel ; services professionnels; développement d'applications

Opérations DNS de l'ICANN

Objectifs	Produits livrables (étapes importantes)
- Activités DNSSEC et roulement périodique clé - Mise en œuvre de signature .arpa de l'ICANN et zones - Référentiel d'ancres de confiance (TAR) - Exploitation sûre, résiliente de la racine L	- Déploiement clé au cours de l'exercice 2011 aux installations de Culpeper et LAX - DNSSEC signées dans les zones ICANN - Référentiel de confiance opérationnel - Amélioration de la racine L
Parties prenantes principales - Services DNS de l'ICANN, équipes TI - Personnel IANA de l'ICANN, DoC, VeriSign - Équipe sécurité de l'ICANN	**Ressources (FY 11)** Humaines - 7,0 ETC (y compris soutien TI et autre soutien de la part du personnel) Financières - $1,2 M pour soutenir les ETC ; investissements prévus pour services de renfort ; DNSSec, racine L, améliorations, installations de sauvegarde ; services professionnels et déplacements

Services de registres/bureaux d'enregistrement gTLD de l'ICANN (Services)

Objectifs	Produits livrables

- Garantir que la mise en œuvre des nouveaux gTLD/IDN prenne en compte les questions de SSR
- Continuer à affiner le processus de sauvegarde des données et le plan de continuité des gTLD
- Mettre en place les processus RSEP/RSTEP
	- Processus de mise en œuvre des gTLD amélioré du point de vue SSR
	  - Extensibilité de la racine achevée (au cours de l'exercice 2011)
	  - Guide de candidature amélioré (novembre 2010)
	- Exercices de sauvegarde des données (août-novembre 2010)
	- Demande d'informations concernant le programme HSTLD (septembre-novembre 2010)
	- Dispositions concernant la conduite malveillante

Parties prenantes principales - Registres/bureaux d'enregistrement - Personnel services de l'ICANN - Personnel sécurité et continuité de l'ICANN - GNSO/SSAC	**Ressources (FY 11)** Humaines - 2,75 ETC Financières – reste à déterminer, budget nouveaux gTLD - comporte une partie personnel d'évaluation/de soutien aux activités des nouveaux gTLD/IDN devant inclure la sécurité TAS ; des fonds dédiés aux RSEP/RSTEP ; soutien aux exercices d'essai/de secours ; déplacement/soutien au personnel

Conformité contractuelle (Services)

Objectifs	Produits livrables
- Processus de conformité de l'ICANN amélioré - Système de conformité et WDPRS améliorés - Exactitude améliorée des données WHOIS	- Exécution d'audits dans le cadre de la mise en œuvre du RAA 2009 - Améliorations du WDPRS (août-novembre 2010) - Études WHOIS supplémentaires selon la recommandation du conseil du GNSO
Parties prenantes principales - Registres/bureaux d'enregistrement gTLD - Personnel de l'ICANN chargé de la conformité - Personnel sécurité et continuité de l'ICANN	**Ressources (FY 11)** Humaines - 3 ETC Financières – $1,1M soutien aux ETC, soutien au personnel/aux déplacements ; services professionnels pour réaliser les études et soutenir les améliorations des systèmes ;

Collaboration pour la sécurité, stabilité et résilience des TLD (Sécurité)

Objectifs	Produits livrables (étapes importantes)
- Affiner le programme de renforcement des capacités DNS - Établir un programme commun de formation technique ISOC/ICANN - Organiser des ateliers de planification d'exercices TLD - Établir des critères d'évaluation des programmes	- Réaliser les séances de formation ACRP restantes en 2010 - Formation technique commune avec plan ISOC, transition en 2010 - Organiser des ateliers de planification d'exercices - Établir les critères d'évaluation sur la base du symposium DNS
Parties prenantes principales - Opérateurs ccTLD - ccNSO, opérateurs TLD régionaux - ISOC/NSRC - Personnel de l'ICANN	**Ressources (FY 11)** Humaines - 1 ETC Financières – $650 mille pour l'ETC, soutien personnel/déplacement ; services professionnels pour l'élaboration et la mise en place de programmes de formation

Collaboration pour la sécurité, stabilité et résilience du DNS (Sécurité)

Objectifs	Produits livrables (étapes importantes)
- Établir des mécanismes de réaction collective aux abus du DNS - Partager les pratiques clés en matière de SSR - Collaborer avec la communauté concernant les risques pour le DNS - Renforcer la collaboration SSR des serveurs racine	- Privilégier la collaboration et la capacité de réponse continuelle avec les partenaires - Réaliser le symposium et établir son compte-rendu (février et mars 2011) - Compte rendu sur l'exercice relatif aux opérations racine (à compléter en 2010)
Parties prenantes principales	**Ressources (FY 11)**
- ISOC, DNS-OARC, FIRST - Communauté des serveurs racine - Communauté élargie des opérateurs DNS - Personnel de l'ICANN - RSSAC/SSAC	Humaines - 1,25 ETC Financières – $590 mille pour les ETC, services professionnels pour le soutien du portail et de la collaboration, déplacement pour le soutien des activités

Programme de sécurité d'entreprise (Sécurité, TI, autres sur l'ensemble du personnel)

Objectifs	Produits livrables

- Améliorer et mettre en œuvre des programmes de sécurité TI / Installations / Personnel
  - Mettre en œuvre des plans officiels
  - Instaurer la formation sécurité
- Mettre en œuvre des plans de sécurité et d'urgence pour les déplacements et les conférences
	- Réaliser des programmes de formation sécurité (incorporés dans les embauches de l'ICANN depuis septembre 2009)
	- Systèmes de contrôle de l'accès physique et TI mis en œuvre (authentification TI améliorée sur les systèmes clés - automne 2009)
	- Exercices de sécurité voyageurs et conférences (un exercice par trimestre)

Parties prenantes principales	**Ressources**
- Équipe de sécurité et résilience de l'ICANN - Opérateurs TI ICANN/IANA/DNS - Ressources humaines de l'ICANN - Équipe conférences mondiales de l'ICANN - Autre personnel de l'ICANN	Humaines - 2 ETC (comprend le soutien TI pour la sécurité) Financières – $1,1 M y compris les ETC, les contrôles d'accès physique et TI, les services professionnels pour réaliser la formation et les audits

Programme de continuité d'entreprise (Sécurité, TI, autres sur l'ensemble du personnel)

Objectifs

- Améliorer le programme de continuité des affaires
  - Établir un plan structuré
  - Établir un centre de données sécurisé
  - Établir des programmes d'exercices structurés

Produits livrables

- Plan interne de continuité des affaires de l'ICANN (octobre 2010)
- Améliorer la résilience du centre de données
- Appliquer la gestion de crise/continuité des affaires (octobre 2010-mars 2011)

Parties prenantes principales

- Équipe sécurité de l'ICANN
- Opérateurs TI ICANN/IANA/DNS
- Ressources humaines de l'ICANN
- Équipe conférences mondiales de l'ICANN
- Personnel de l'ICANN

Ressources

Humaines – 5 ETC (y compris la planification et la TI pour le centre de données)

Financières – $1,7M y compris les ETC, le soutien financier du centre de données, les services professionnels pour la réalisation de la formation et des audits

Engagement mondial sécurité, stabilité et résilience

(Partenariats mondiaux et sécurité)

Objectifs

- Maintenir les partenariats avec les organisations clés (ISOC; IISI; IMPACT; EC/ENISA; CSIS; Atlantic Council)
- Continuer à participer aux dialogues sur la sécurité Internet parrainés IGO, ECDE, IGF et autres)
- Collaborer avec les autres pour une réponse mondiale en matière de sécurité Internet

Produits livrables

- Réaliser des activités communes avec les organisations partenaires (une par trimestre)
- Participer à des forums dans toutes les régions principales (en cours)
- Adhérer au forum des équipes de réponses aux incidents et de sécurité (FIRST)

Parties prenantes principales

- Organisations mondiales/internationales
  - ISOC; IETF; ITU; IGF
- Forums sur la sécurité Internet
- Gouvernements/parties prenantes commerciales
- Personnel sécurité et équipe partenariats mondiaux de l'ICANN

Ressources (FY 11)

Humaines - 1,5 ETC

Financières – $530 mille pour les ETC ; soutien personnel/déplacements ; soutien aux forums menés ou soutenus par l'ICANN ; services professionnels pour l'élaboration de critères d'évaluation

Soutien des politiques pour les efforts liés à la SSR

(Politique)

Objectifs	Produits livrables
Établis par les SO/AC menant des activités SSR - GNSO ; ccNSO - GAC - RSSAC ; ALAC	- Dérivent des plans de travail de l'exercice financier 2011 tels qu'établis
Parties prenantes principales - SO/AC nommés - Personnel de l'ICANN chargé des politiques - Personnel sécurité de l'ICANN	**Ressources (FY 11)** Humaines - 2 ETC Financières – $550 mille pour les ETC et financement supplémentaire limité pour le soutien des activités liées à la SSR

Comité consultatif pour la sécurité et la stabilité (SSAC)

Objectifs	Produits livrables
- Favoriser le déploiement des DNSSEC - Garantir la stabilité de la zone racine en parallèle à la croissance et à la complexité - Protection des enregistrements de noms de domaine - Réduction des abus de noms de domaine - Traitement de la stabilité du système	- Rapports, documents consultatifs, commentaires - Études d'extensibilité de la racine - Étude de protection des noms de domaine - Étude des données d'enregistrement : affichage, accès, exactitude
Parties prenantes principales - Communauté sécurité Internet externe - Communauté des serveurs racine et IANA - GNSO et ccNSO - ALAC - ASO - Personnel de l'ICANN - GAC et Conseil d'administration	**Ressources (FY 11)** Humaines - 1,5 ETC Financières – $650 mille pour les ETC et financement limité pour le soutien au déplacement et publications ; soutien à l'achèvement des études d'extensibilité de la racine

Annexe B - Glossaire des termes et acronymes du plan SSR

ACRP (Attack and Contingency Response Planning) – Planification des réponses aux attaques et aux imprévus

Add Grace Period – Délai de renoncement ou période d'essai de cinq jours au début de l'enregistrement d'un nom de domaine de deuxième niveau régulé par l'ICANN. Les titulaires du nom de domaine ont la possibilité d'annuler leur enregistrement dans ce délai de cinq jours, au cours duquel les frais d'enregistrement doivent être totalement remboursés par le registre du nom de domaine.

APWG (Anti-Phishing Working Group) – Groupe de travail anti-hameçonnage

ASN (Autonomous System Numbers) - Numéros de systèmes autonomes : au sein de l'Internet, un système autonome (AS) est un ensemble de réseaux IP connectés qui présentent une politique de routage commune clairement définie vers l'Internet. Les fournisseurs de services Internet (ISP) doivent avoir un numéro de système autonome (ASN) officiellement enregistré par le biais de l'IANA.

ccNSO (country code Names Supporting Organization) – Organisation de soutien aux politiques de codes de pays de l'ICANN qui est l'entité chargée de l'élaboration de politiques pour un ensemble restreint de questions de domaines de premier niveau de codes pays au sein de la structure de l'ICANN.

ccTLD (country code Top-Level Domain) – Nom de domaine de premier niveau de code pays

CENTR (Council of European National Top Level Domain Registries) – Le conseil des registres européens nationaux de domaines de premier niveau est une association des registres de domaines de premier niveau de codes pays tels que .uk au Royaume-Uni et .es en Espagne. La pleine adhésion est ouverte aux organisations, personnes morales ou individus administrant un registre de noms de domaine de premier niveau de code pays.

CSIS (Center for Strategic and International Studies) – Le centre d'études stratégiques et internationales offre un aperçu stratégique et des solutions de politiques aux preneurs de décisions au sein des gouvernements, des institutions internationales, du secteur privé et de la société civile.

FIRST (Forum of Incident Response and Security Teams) – Forum des équipes de réponses aux incidents et de sécurité

gTLD (generic Top-Level Domain) – Nom de domaine générique de premier niveau

IANA (Internet Assigned Numbers Authority) – Autorité pour les noms et numéros assignés

IDN (Internationalized Domain Name) – Nom de domaine internationalisé

IETF (Internet Engineering Task Force) – Groupe de travail de l'ingénierie Internet

IP (Internet Protocol) – Protocole Internet de communication qui définit le format des données transmises et l'adressage des machines connectées. La majorité des réseaux combinent l'IP à un protocole de plus haut niveau nommé protocole de contrôle de transmission (TCP), qui établit une connexion virtuelle entre une destination et une source. L'IP en soi est une sorte de système postal. Il vous permet d'adresser et d'envoyer un paquet de données en utilisant le système, mais il n'existe pas de lien direct entre votre paquet et le destinataire. Le TCP/IP crée la connexion entre deux hôtes afin qu'ils puissent envoyer et recevoir des messages.

IPv4 - L'Internet Protocol version 4 est la quatrième révision du protocole Internet (IP) et la première version à avoir été largement déployée. Avec l'IPv6, il forme la base des méthodes d'inter-réseautage de l'Internet, et constitue encore et de loin le protocole de couches Internet le plus largement déployé.

IPv6 - L'Internet Protocol version 6 est la nouvelle génération de protocole de couches Internet destiné aux réseaux interconnectés à commutation de paquets et Internet. En décembre 1998, le groupe de travail de l'ingénierie d'Internet (IETF) a désigné l'IPv6 comme le successeur de la version 4, en publiant la spécification de normes, RFC 2460.

ISOC (Internet Society) - Société Internet

IT (Information Technology) - Technologie de l'information

Botnets - plus communément créés en dupant les utilisateurs ordinaires et les amenant à ouvrir une pièce jointe sur leur ordinateur apparemment inoffensive mais contenant en réalité un logiciel masqué destiné à être plus tard utilisé pour une attaque. Les logiciels désormais compromis, ou « bots » (abréviation de robot), sont combinés en réseaux qui peuvent alors être dirigés

tel que souhaité, le plus souvent à des fins d'attaques malveillantes.

Cache Poisoning - **Empoisonnement du cache** - exploitation d'une vulnérabilité du logiciel du serveur DNS qui accepte alors des informations incorrectes qui stocke dans son cache les informations erronées et envoie ainsi toutes les requêtes de serveur subséquentes vers le nouveau domaine faussement vérifié.

Denial of Service attack (DoS) - **Attaque par déni de service** - il s'agit d'un code malveillant qui provoque une surcharge en messages entrants, obligeant essentiellement le système ciblé à fermer, refusant donc l'accès à des utilisateurs légitimes.

Distributed Denial-of-Service attack (DDoS) – type d'attaque par déni de service au cours de laquelle l'attaquant utilise un code malveillant installé sur plusieurs systèmes pour en attaquer un seul. Cette méthode a un plus grand effet sur la cible que si elle provenait à partir d'une seule machine d'attaque. Sur Internet, dans l'attaque appelée distributed denial-of-service, une multitude de systèmes compromis attaque une seule cible, résultant en un déni de service aux utilisateurs du système ciblé. Le flot de messages entrants au système ciblé l'oblige en fait à s'arrêter, et à refuser de servir les utilisateurs légitimes. Les attaques DDoS sont plus efficaces lorsqu'elles sont lancées par un grand nombre de serveurs récursifs ouverts : la distribution augmente le trafic et réduit la concentration sur les sources de l'attaque. L'impact sur les serveurs récursifs ouverts mal utilisés est généralement réduit mais l'effet sur la cible est significatif. Le facteur d'amplification est estimé à 1:73. Les attaques basées sur cette méthode ont dépassé les 7 Gigabits par seconde.

DNS (Domain Name System) - Système de noms de domaine qui traduit un nom de domaine (alpha) en une adresse IP (numérique). Étant plus faciles à mémoriser, les noms de domaine sont alphabétiques. L'Internet est toutefois basé sur des adresses IP numériques (par ex. 198.123.456.0). Lorsque vous utilisez un nom de domaine (www.examplir.gratis.com), un service DNS traduit le nom alphabétique en l'adresse IP numérique correspondante.

DNSSEC – Extensions de sécurité du système de noms de domaine qui fournissent aux logiciels un moyen de valider que les données du système de noms de domaine n'ont pas été modifiées au cours du passage par l'Internet. Ceci est réalisé par l'incorporation à l'hiérarchie du DNS de paires de signatures clés publiques-privées qui forment une chaîne de confiance émanant de la zone racine. A noter que les DNSSEC ne sont pas une forme de cryptage. Elles

sont rétrocompatibles avec le DNS existant, n'intervenant pas dans les enregistrements précédents et les laissant tels quels – non cryptés. Les DNSSEC garantissent l'intégrité des enregistrements par l'utilisation de signatures numériques qui attestent leur authenticité.

Le concept de chaîne de confiance constitue le noyau des DNSSEC. La proposition de l'ICANN concernant la signature du fichier de zone racine en utilisant les DNSSEC (datant d'octobre 2008) repose sur cette notion et, basée sur les conseils de sécurité, recommande que l'entité responsable de changements, ajouts ou suppressions d'un fichier de zone racine et confirmant que ces changements sont valides, produise une signature numérique de la mise à jour du fichier de zone racine résultant des changements. Ce fichier signé devrait alors être transmis à une autre organisation (actuellement la société VeriSign) pour distribution. En d'autres termes, l'organisation responsable de la base de confiance initiale – validation des changements de zone racine avec les opérateurs de domaines de premier niveau – devrait également authentifier la validité du produit final avant sa distribution.

Domain Name Front Running – pratique douteuse utilisée par certains bureaux d'enregistrement de noms de domaine de mettre à profit des informations privilégiées et d'enregistrer à l'avance des noms de domaine faisant l'objet d'une recherche de disponibilité dans l'intention de vendre le nom, contre un droit de garantie, à des titulaires qui bénéficieraient logiquement de l'obtention de ce nom pour leur propre usage

Domain tasting – pratique qui consiste à enregistrer des noms de domaine en utilisant le délai de renoncement de cinq jours au début de l'enregistrement d'un nom de domaine de deuxième niveau régulé par l'ICANN pour tester l'attrait commercial d'un nom de domaine. Une analyse coûts-avantages est réalisée au cours de cette période par le titulaire l'informant ainsi sur la viabilité des revenus générés par les publicités placées sur le site Web du domaine.

Le 'domain tasting' ne devrait pas être confondu avec le '**domain kiting'**, pratique qui consiste à enregistrer des noms de domaine, les utiliser pendant le délai de renoncement de cinq jours, les laisser expirer et renouveler immédiatement l'opération pour une autre période de cinq jours. Ce processus est réitéré plusieurs fois de manière à obtenir ainsi l'enregistrement d'un nom de domaine sans réellement payer.

Double flux - variante du 'fast flux' qui préoccupe l'ICANN particulièrement. Dans cette technique, l'attaquant ne se

contente pas de changer les adresses qui dirigent vers des sites Web frauduleux, mais il incorpore les adresses des serveurs de noms DNS qu'il utilise pour les noms « conviviaux » dans des courriels hameçons. Dans les deux cas, les changements sont très rapides, de l'ordre de 3 minutes, et ne laissent pratiquement pas le temps aux enquêteurs de réagir. Le SSAC de l'ICANN collabore étroitement avec les défenseurs de marques, les organismes d'application de la loi, les registres et les bureaux d'enregistrement pour identifier des contre-mesures, notamment celles qui retireraient le DNS de l'équation 'fast flux'.

Fast flux - technique frauduleuse utilisée par les hameçonneurs, les usurpateurs d'identité et autres cybercriminels pour entraver les efforts des équipes de réponse aux incidents et des organismes d'application de la loi dans le dépistage et le démontage de sites Web illégaux. La technique 'fast flux' ressemble beaucoup au bonneteau, un jeu qui se fait généralement avec les rois de trèfle et de pique et la dame de cœur, où le "maître du jeu" manipule les trois cartes et demande au joueur de miser et de découvrir la carte rouge (le jeu est dénommé « trouver la dame » par les britanniques). Le manipulateur bouge les cartes à très grande vitesse tout en distrayant l'attention de la victime par la conversation, les plaisanteries et les tours de passe-passe. Le 'fast flux' est cependant un tour à enjeux élevés et est devenu une technique d'attaque préoccupante et omniprésente. Dans l'hébergement 'fast flux', le manipulateur change rapidement les adresses qui pointent vers des sites Web illégaux.

Malware – terme désignant un logiciel malveillant et provenant de la contraction de 'malicious' et 'software' souvent utilisé comme expression passe-partout pour inclure les virus, vers, chevaux de Troie, 'rootkits', logiciel espions, publiciels, les logiciels d'usurpation d'identité et autres logiciels indésirables introduits dans l'ordinateur d'un utilisateur avec ou sans son consentement Un logiciel est considéré malveillant en fonction de l'intention de nuire de son créateur plutôt qu'en fonction de caractéristiques particulières du logiciel.

NOC (Network Operations Center) - Un centre d'opérations de réseaux est un lieu physique à partir duquel un réseau habituellement important est géré, surveillé et dirigé. Les NOC offrent également un accès aux utilisateurs se connectant au réseau à partir d'un lieu externe à l'espace physique du réseau.

NOG (Network Operations Group) – Groupe d'opérateurs de réseau

NRO (Number Resource Organisation) – Organisation de ressources de numéros

Patches – correctifs conçus pour réparer les défauts d'un logiciel, souvent automatiquement installés pour réduire le besoin de participation de l'utilisateur final et augmenter la facilité d'utilisation.

Phishing – Hameçonnage - technique utilisée par des fraudeurs pour obtenir des renseignements précieux tells numéros de cartes de crédit, de sécurité sociale, noms d'utilisateurs et mots de passe en créant un site Web similaire à celui d'une organisation légitime et en dirigeant ensuite le courrier électronique vers le site frauduleux afin de soutirer des renseignements personnels à des fins financières ou politiques.

RAA (Registrar Accreditation Agreements) – Accords d'accréditation de bureaux d'enregistrement

Registry – Registre - une organisation qui gère l'enregistrement de noms de domaine Internet de premier niveau

Registrar – Bureau d'enregistrement - une société autorisée à enregistrer des noms de domaine Internet

RIR (Regional Internet Registry) – Registre Internet régional

rPKI (Resource Public Key Infrastructure) – Infrastructure des clés publiques de ressources

RSEP (Registry Services Evaluation Process) – Processus d'évaluation des services de registres

RSTEP (Registry Services Technical Evaluation Panel) – Commission d'évaluation technique des services de registres

Spam – Pourriel - tout courrier électronique non sollicité par le destinataire. Message généralement considéré comme un désagrément coûteux, le pourriel contient souvent maintenant un malware. Le malware est une classe de logiciel malveillant - virus, vers, chevaux de Troie, et logiciel espions – conçu pour infecter les ordinateurs et systèmes et usurper des renseignements importants, supprimer des applications, des lecteurs et des fichiers, ou convertir des ordinateurs en un atout pour une personne de l'extérieur ou un attaquant.

Spoofing – Mystification - une situation d'attaque dans laquelle une personne ou un programme se fait passer pour quelqu'un ou quelque chose d'autre en falsifiant des données. Les données falsifiées sont à leur tour considérées comme valides par le

système individuel qui essaie de se connecter avec le système ou programme légitime.

TLD (Top Level Domain) - Domaine de premier niveau

Trojan – Cheval de Troie - une classe de logiciel malveillant (malware) d'apparence légitime, mais conçu pour exécuter des fonctions malveillantes à l'insu de l'utilisateur, permettant un accès non autorisé à l'ordinateur hôte, donnant aux utilisateurs du logiciel la possibilité de sauvegarder leurs fichiers sur l'ordinateur de l'utilisateur involontaire ou même de visualiser l'écran de l'utilisateur et de prendre le contrôle de l'ordinateur.

Virus – Virus informatique - un programme ou une chaîne de code qui s'insère dans un ordinateur à l'insu de l'utilisateur et active un logiciel malveillant (malware). Un virus, même simple, peut se reproduire par réplication et devenir encore plus nuisible parce qu'il utilise rapidement toute la mémoire disponible d'un ordinateur infecté.

Worm – Ver – similaire à un virus dans sa conception, le ver est considéré comme une variante du virus, mais il est plus dangereux vue sa capacité de se propager par ses propres moyens à travers les réseaux. Les vers se propagent d'ordinateur à ordinateur, mais contrairement aux virus, ils sont capables de se propager sans aucun recours à une action humaine intentionnelle ou non. Un ver profite des caractéristiques de transport d'un fichier ou d'une information sur un système informatique et ceci lui permet de se déplacer sans aide. Par exemple, un ver peut envoyer sa propre reproduction en utilisant le carnet d'adresses d'un utilisateur à l'insu de ce dernier. Il se reproduit ainsi sur les ordinateurs nouvellement infectés et se propage à nouveau par le biais de leurs carnets d'adresses ainsi de suite jusqu'à avoir consommé tellement de mémoire et de largeur de bande qu'il provoquera l'interruption de réseaux entiers.