PLAN POUR LE RENFORCEMENT DE LA SECURITE, DE LA STABILITE ET DE LA RESILIENCE DE L'INTERNET

Projet approuvé – 16 mai 2009

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 collaborative.

Le plan stratégique de l'ICANN pour 2009-2012 (www.icann.org/en/strategic-plan/strategic-plan-2009-2012-09feb09-en.pdf) spécifie « La sécurité, la stabilité et la résilience resteront nos priorités absolues et l'ICANN travaillera efficacement en collaboration avec d'autres parties prenantes de l'Internet afin de renforcer et de protéger la sécurité et la stabilité de l'Internet, en accordant une attention particulière à la mission de l'ICANN qui consiste à protéger la sécurité, la stabilité et la résilience des systèmes d'identificateurs uniques de l'Internet ». Le plan stratégique identifie un nombre d'objectifs à travers le large éventail de responsabilités de l'ICANN en matière de sécurité, de stabilité et de résilience. Le plan stratégique aborde les préoccupations de sécurité, stabilité et résilience sous la priorité 2 – Renforcer la sécurité, la stabilité et la résilience dans l'allocation et l'attribution des identificateurs uniques de l'Internet. La priorité 2 spécifie : 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 améliorer la résilience du DNS et à 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. L'objectif principal de cette priorité est de veiller à ce que les systèmes d'identificateurs uniques de l'Internet restent viables et à ce que leur fonctionnement reste solide pendant la durée de ce plan.

[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.

Les objectifs spécifiques identifiés dans le cadre de la priorité 2 du plan stratégique sont :

A. Soumettre à la consultation un plan qui définisse le rôle de l'ICANN en matière de sécurité, stabilité et résilience de l'Internet ; identifier les partenaires appropriés et démarrer une action conjointe. Définir le rôle de l'ICANN de sorte que la portée de ses efforts, les coûts et les résultats soient bien compris et mettre en œuvre un processus qui mène à un accord de la part de la communauté et du Conseil d'administration en 2009. Collaborer de façon efficace avec les partenaires afin de poursuivre des approches multipartites et de réaliser des programmes qui contribuent à la sécurité, la stabilité et la résilience de l'Internet à l'échelle mondiale. Des critères de mesure de ces programmes seront établis d'ici la fin de 2009 et les premières évaluations auront lieu d'ici la mi-2010.

B. Fournir les mécanismes qui permettront aux utilisateurs de valider l'authenticité des identificateurs de l'Internet que l'ICANN publie et contribuer largement aux efforts techniques visant à offrir des systèmes de nommage et d'adressage Internet plus sécurisables. En particulier, l'ICANN fera tout son possible pour collaborer avec les parties prenantes principales, assurer la signature du DNSSEC de la zone racine DNS d'ici la fin de 2009 et encourager la mise en œuvre de rPKI pour renforcer la maîtrise de la sécurité et la stabilité.

C. Réaliser des programmes ciblés pour renforcer la compréhension des risques et renforcer la sécurité et la résilience des organismes associés à la communauté TLD. Les programmes comprendront le travail en partenariat afin d'établir une approche efficace en matière de partage des meilleures pratiques à travers la communauté d'ici la fin de 2009 et mettre en place des programmes continus de formation et d'exercices régionaux pour cette communauté durant toute la période couverte par le plan.

D. Collaborer avec les parties prenantes à l'échelle de la communauté de l'ICANN pour établir les modalités d'une collaboration continue visant à comprendre les risques et à renforcer la sécurité et la résilience du DNS vis-à-vis d'une gamme complète de menaces et ce, durant toute la période couverte par le plan. L'ICANN collaborera avec des partenaires pour établir les approches permettant de mesurer les risques opérationnels encourus par le DNS et ses utilisateurs, d'ici la mi-2010.

Le plan de l'ICANN pour le renforcement de la sécurité, stabilité et résilience correspond au document requis sous l'objectif A et délimite, de plus, le rôle spécifique de l'ICANN en matière de sécurité, de stabilité et de résilience. Il présente une vue d'ensemble des

programmes de l'ICANN dans ce domaine, et expose en détail les activités programmées qui renforceront ses apports tout au long de l'exercice financier prochain. La première version du plan a pour objet de servir de base à l'ICANN et à sa communauté concernant le rôle de l'ICANN et d'établir le cadre pour l'organisation des efforts de sécurité, stabilité et résilience de l'ICANN. Le plan n'envisage pas de nouveaux rôles ou programmes majeurs pour l'ICANN dans ce domaine.

Le rôle de l'ICANN

L'ICANN agit conformément à ses statuts en mettant en place des processus multipartites consensuels pour établir ses politiques et ses programmes, 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'exercice 2009-2010, 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'IANA*** – Conformément au plan stratégique de l'ICANN pour 2009-2012, l'ICANN devrait être opérationnellement prête à mettre en œuvre les extensions sécurité du DNS (DNSSEC) pour la zone racine faisant autorité, et collaborer avec la communauté Internet pour lever les obstacles à l'adoption des DNSSEC. L'ICANN est prête, disposée à et en mesure de signer la racine. Selon sa proposition de septembre 2008, les efforts actuels et prévus de l'ICANN sont abordés aux sections 5.1.1.3 et 6.1.1.1. 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 gérants 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 et d'exercices.***
- ***Registres gTLD – veiller à ce que l'évaluation des candidats aux nouveaux noms de domaine générique de premier niveau (gTLD) et aux noms de domaine internationalisés (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 avec les registres de noms de domaine de premier niveau de code pays (ccTLD) sur l'affinage du programme conjoint de planification des réponses aux attaques et aux imprévus (ACRP) établi conjointement avec l'organisation de soutien aux politiques de codes de pays (ccNSO) et les associations de domaines de premier niveau (TLD) régionales.***
- ***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.

- ***Réponse à l'abus malveillant du DNS*** - l'ICANN tirera parti de ses efforts collaboratifs 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.
- ***Assurer l'engagement et la coopération au niveau mondial –*** l'ICANN continuera à renforcer les partenariats en vue d'inclure le groupe de travail de l'ingénierie Internet (IETF), la société Internet (ISOC), les groupes de registres Internet régionaux (RIR) et les groupes d'opérateurs de réseau (NOG), le centre d'opérations, d'analyse et de recherche du DNS (DNS-OARC). 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

1.1 Ce plan 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'exercice prochain. 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 2010 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 2010 de l'ICANN en matière de sécurité, stabilité et résilience, les partenaires, les étapes importantes/produits livrables et les ressources y consacrées

1.2 Tel que formulé dans la synthèse, ce plan se base sur la vision et les objectifs définis dans le plan stratégique de l'ICANN pour 2009-2012. La première version du plan a pour objet de servir de base à l'ICANN et à sa communauté concernant le rôle de l'ICANN et d'établir le cadre pour l'organisation de ses efforts de sécurité, stabilité et résilience. Le plan n'envisage pas de nouveaux rôles ou programmes majeurs pour l'ICANN dans ce domaine. Le plan sera mis à jour annuellement conjointement avec les cycles de planification stratégique et opérationnelle de l'ICANN

2. Défis et perspectives

2.1 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 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.

2.2 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 statuts 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 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 prennent 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 2010, les étapes clés et les ressources y associées. Dans le cadre des objectifs du personnel de sécurité de l'ICANN pour l'exercice financier 2010, l'accent sera mis spécialement 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

3.1 L'ICANN agit conformément à ses statuts en mettant en place des processus multipartites consensuels pour établir ses politiques et ses programmes, 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 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.

3.2 En tant que partie 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 collaboratif 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.

3.3 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 n'engagera pas des activités ou des débats liés à l'utilisation de l'Internet pour l'espionnage électronique et la guerre de l'information. Par ailleurs, l'ICANN ne s'impliquera pas dans des discussions relatives 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 les pourriels) qui utilisent le système d'identificateurs uniques de l'Internet.

3.4 L'ICANN organise ses activités de sécurité, stabilité et résilience à travers la considération de son rôle : d'entité directement responsable, de facilitateur/favorisant, de 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 recommande la mise en œuvre des extensions de sécurité du système de noms de domaine (DNSSEC) y compris la signature de la zone racine du DNS représente une étape essentielle dans la maîtrise de la sécurité du DNS. L'ICANN a proposé une approche qui permet la continuation ininterrompue du mécanisme de distribution racine du DNS, une tâche partagée entre l'ICANN, VeriSign, le NTIA et les opérateurs de serveurs racine dans le cadre de la mise en œuvre des DNSSEC. L'ICANN a présenté des solutions flexibles qui satisfont une approche intermédiaire pouvant mener à une solution permanente, et a procédé à des préparatifs opérationnels afin de remplir son rôle. D'autres efforts capitaux porteront sur l'amélioration de la compréhension des risques, la facilitation de la mise en œuvre des clés publiques de ressources (rPKI) au niveau racine, 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 collaboratives, l'ICANN a conclu des contrats avec tous les registres gTLD et les bureaux d'enregistrement accrédités par l'ICANN. Ces accords sont de plus en plus 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 de l'avancement de ses efforts. 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 au bénéfice 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 participe à des activités avec la NRO (Numbering Resource Organisation) et les RIR 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 la réalisation 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 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 collaboratifs 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. 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 :

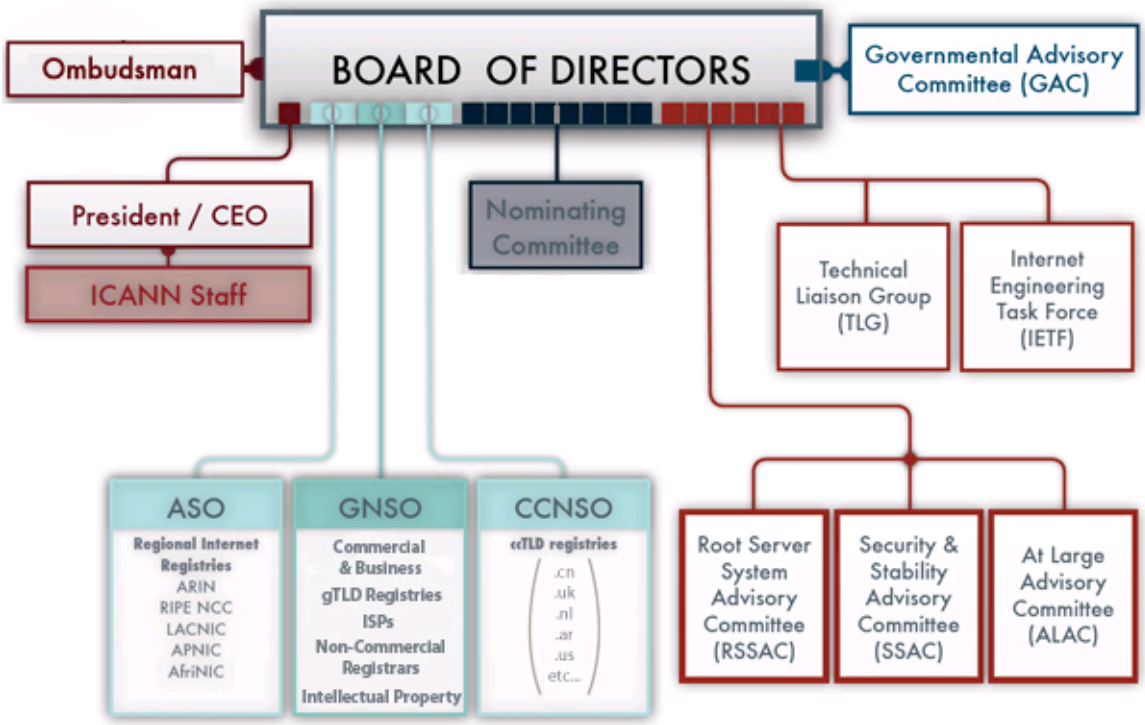
- ***Le personnel de l'IANA*** – chargé de la réalisation des fonctions de l'IANA y inclus la coordination de la zone racine du DNS, l'exploitation du registre .arpa, l'attribution de l'espace adresse IP, et l'enregistrement des paramètres de protocole. Le personnel affecté aux fonctions de l'IANA a établi des plans de mise en œuvre des DNSSEC au niveau racine et pour les zones DNS gérées par l'ICANN. Les activités spécifiques liées à la sécurité, la stabilité et la résilience sont brièvement décrites ci-dessous.
- ***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 à 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 à 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 au regard des sujets 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)*** – ce 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 tel que requis par le Conseil d'administration de l'ICANN et tel que lancé 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) –*** ce comité consultatif de l'ICANN donne des conseils sur les exigences opérationnelles des serveurs de noms racine, examine les aspects liés à la sécurité du système de serveurs de noms racine ainsi que la performance globale du système, sa robustesse et sa fiabilité et donne des conseils en la matière.
- 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 organisationnelle de l'ICANN



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 en cours. 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 3.4, commençant par les fonctions principales de DNS/adressage ; le travail avec les communautés de registres et de bureaux d'enregistrement

TLD ; la communication avec la NRO et les RIR ; les programmes de sécurité et 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

5.1.1.1 L'ICANN assume 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.

5.1.1.2 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 racine du DNS, les domaines .int et .arpa et des ressources de pratiques de noms de domaine internationalisés (IDN). Les pratiques de gestion garantissent que tout changement à 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.

- ***Ressources de numéros*** – A travers les fonctions de l'IANA, l'ICANN coordonne la réserve mondiale d'adresses IPv4 et IPv6, et les ASN, les fournissant aux RIR. Dans cette activité de coordination, par le biais des fonctions de l'IANA, l'ICANN est guidée par les processus et les procédures provenant des communautés de RIR, à travers leurs processus d'élaboration de politiques. Ce processus de politique participative permet d'obtenir le consensus mondial des destinataires finaux des ressources que l'ICANN et les RIR agissent en toute équité, transparence et stabilité.
- ***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). Au travers d'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.

5.1.1.3 L'ICANN a prôné le besoin de mettre en œuvre des DNSSEC au niveau racine, a remis en au Ministère du commerce en septembre 2008 une proposition concernant le rôle des fonctions de l'IANA dans la mise en place d'une signature au niveau racine, et a réalisé les préparatifs pour remplir ce rôle ainsi que pour signer les domaines .int et .arpa. Ces 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.

5.1.1.4 De plus, l'ICANN a collaboré avec les RIR et l'IETF dans le cadre du développement de la technologie rPKI pour introduire l'authentification des ressources de numérotation attribuées. 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.

5.1.1.5 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 conclu entre l'ICANN et le Ministère du commerce et en tant que partie de son propre plan d'entreprise de réponse aux attaques et aux imprévus.

5.1.2 Opérations des serveurs racine du DNS

5.1.2.1 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.

5.1.2.2 L'ICANN continuera à travailler dans le but de formaliser ses relations avec les opérateurs de serveurs de noms racine conformément à son engagement exprimé dans « l'affirmation des responsabilités du Conseil d'administration de l'ICANN envers une gestion par le secteur privé » de 2006. En 2008, l'ICANN a conclu un accord de responsabilités mutuelles avec Internet Systems Consortium concernant l'exploitation de la racine F. Ceci a renforcé son

« engagement envers un renforcement croissant de la stabilité, Sécurité et interopérabilité du Système de noms de domaine (DNS) de l'Internet dans une perspective mondiale et au bénéfice de la communauté mondiale de l'Internet d'une manière évolutionniste basée sur une relation d'appairage ».

5.1.2.3 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 partager les leçons acquises.

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

5.2.1.1 L'ICANN collabore avec les opérateurs de gTLD en matière de coordination sûre et stable de ces TLD. De plus, les registres

de gTLD ont chacun un contrat avec l'ICANN. Tandis que certains éléments de ces contrats 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 par l'ICANN. D'autres dispositions de l'accord 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 un effort de planification de continuité 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.

5.2.1.2 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.

5.2.2 Nouveaux gTLD et IDN

5.2.2.1 Se préparant à engager les processus relatifs aux nouveaux TLD afin d'inclure les noms de domaine internationalisés, 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 revue comprend 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. Le processus d'introduction des ccTLD IDN suivra un parcours différent, cette introduction initiale étant limitée aux chaînes non litigieuses qui représentent des noms de pays et de territoires correspondant aux ccTLD existants. Le SSAC a remis ses commentaires sur l'impact des IDN sur la sécurité et la stabilité au niveau racine du DNS en juillet 2007 pris en compte dans les processus de planification de mise en œuvre et d'essai.

5.2.2.2 Une équipe d'experts indépendants réalisera l'évaluation technique des candidats et de leurs TLD proposés. De plus, le processus relatif aux nouveaux gTLD offre une procédure préliminaire RSEP permettant d'évaluer les problèmes de sécurité ou de stabilité potentiels liés aux nouveaux services des registres proposés dans la candidature aux gTLD. Pour les TLD des IDN, les exigences techniques relatives à la chaîne et l'évaluation associée sont les mêmes que pour les gTLD des IDN et les ccTLD des IDN.

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

5.2.3 Bureaux d'enregistrement gTLD

5.2.3.1 L'ICANN collabore également avec les bureaux d'enregistrement sur les questions relatives à la sécurité, la stabilité et la résilience. Du point de vue contractuel, la relation de l'ICANN avec les bureaux d'enregistrement est régie par l'accord d'accréditation de bureau d'enregistrement (RAA) standard. 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.

5.2.3.2 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 revues périodiques d'accréditation (par ex. lors du renouvellement du RAA d'un bureau d'enregistrement).

5.2.3.3 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

5.2.4.1 Les services Whois fournissent un accès public aux données relatives aux noms de domaine enregistrés et 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.

5.2.4.2 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.

5.2.5 Conformité contractuelle

5.2.5.1 Le service de conformité contractuelle veille à ce qu'autant 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. Consultez le site Web à l'adresse http://reports.internic.net/cgi/registrars/problem-report.cgi. Les plaintes relatives à des violations éventuelles de RAA sont examinées par le personnel chargé de la conformité contractuelle. 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.

5.2.5.2 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 le regroupements de bureaux d'enregistrement et le regroupement sur la propriété intellectuelle (IPC), le WDPRS a été transformé en 2008 pour pallier à diverses préoccupations soulevées par la communauté de l'Internet

notamment en matière de fonctionnalité limitée, de capacité limitée et de manque de suivi de la conformité. Le WDPRS transformé a été lancé en décembre 2008. L'équipe de conformité poursuit ses efforts pour améliorer ce système avec pour objectif le renforcement de l'exactitude des données du Whois.

5.2.6 Protéger les titulaires de noms de domaine gTLD

5.2.6.1 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.

5.2.6.2 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. Les membres du SSAC ont donné des conseils aux bureaux d'enregistrement en matière de pratiques à adopter pour améliorer la protection des noms de domaine et pour s'occuper des questions liées au 'fast flux', au mauvais usage des données Whois et au piratage de noms ainsi que pour traiter des préoccupations des titulaires portant sur des problèmes tels que les renouvellements. A part le SSAC, 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 conseillé le Conseil du GNSO concernant la récupération de noms de domaine par les titulaires après leur expiration. Le GNSO est en train d'entreprendre un nombre d'initiatives supplémentaires ayant la capacité de résulter en une meilleure protection pour les titulaires de noms de domaine. Ces initiatives

comprennent les renforcements 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 avec les ccTLD est de fournir, en s'associant avec les 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'ICANN, à travers les fonctions de 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. Elle apporte ainsi son soutien dans la mise en place d'une réponse collaborative 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 collaborative à l'abus malveillant du DNS

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. L'ICANN collabore activement avec les registres et les bureaux d'enregistrement pour assurer la prise de conscience et faciliter la diffusion des informations. 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.

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

5.2.10.1 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. Les efforts capitaux ont consisté, entre autres, en une analyse et des recommandations portant sur les attaques par saturation avec déni de service distribué (DDoS) du DNS, la mise en œuvre des DNSSEC ajoutant les 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. En outre, des membres du SSAC participent au comité sur les politiques Internet du groupe de travail anti-hameçonnage (APWG) et ont conjointement rédigé des documents de présentation technique de la manière selon laquelle les hameçonneurs exploitent des noms de domaine et de sous-domaine.

5.2.10.2 L'ICANN a l'intention de poursuivre ce rôle, 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 les risques 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 le monde en développement, 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.

5.2.10.3 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.

5.3 Communication avec la Number Resource Organisation (NRO) et les registres Internet régionaux (RIR)

L'interaction de l'ICANN avec la NRO et les RIR est dictée par la compréhension primordiale du fait que les RIR 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. L'ICANN participe avec ces organisations à un certain nombre d'activités liées à la sécurité, la stabilité et la résilience de l'Internet. Notamment, l'ICANN a travaillé avec ces organisations pour la signature sécurisée DNSSEC des zones inverses de l'arbre DNS. Les RIR, en tant que registres d'adresses IP, sont directement impliqués dans les efforts visant à l'authentification des adresses et les protocoles d'échange de routes (Border Gateway Protocol) par le biais de l'effort rPKI, et l'ICANN continuera à compter sur leur partenariat dans le cadre de ces efforts.

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

5.4.1 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 de l'ensemble des systèmes d'identificateurs uniques de l'Internet.

5.4.2 L'ICANN a œuvré pour un programme de sécurité global qui gère le risque à travers ses ressources informatiques,

humaines et matérielles. En automne 2008, l'ICANN a embauché un directeur des opérations sécurité chargé de ce programme. L'ICANN fournit l'information, les données sensibles des processus, et compte sur l'utilisation de la technologie de l'information (IT) pour mener ses opérations à bien. 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 /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. Le personnel chargé de la planification sécurité se concentre sur la protection du personnel de l'ICANN aux deux lieux de travail principaux, et dans la réalisation de la variété d'activités mondiales de l'ICANN, sur la garantie de la sécurité au cours des conférences de l'ICANN. L'ICANN a établi un processus de planification pour gérer les risques liés à la sécurité du personnel et s'appuie sur sa propre équipe interne de sécurité ainsi que sur le soutien de ses conseillers en sécurité. L'ICANN a établi un processus de planification pour gérer les risques liés aux installations matérielles y compris le siège principal de Marina del Rey, en Californie, aux Etats-Unis ainsi que les bureaux centraux et centres de sauvegarde.

5.4.3 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. Tandis que l'ICANN se développe, les actifs de l'entreprise augmentent en parallèle à son activité mondiale et à son profil public. L'environnement de sécurité d'entreprise de l'ICANN deviendra de plus en plus motivant et l'ICANN continuera à souligner l'importance d'une saine gestion, de la continuité des affaires et de la sécurité en tant que composantes principales de ses processus d'entreprise.

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

5.5.1 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. L'ICANN a trois

organisations de soutien – 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) lesquelles sont responsables de l'élaboration des politiques de sorte à inclure les sujets liés à la sécurité et à la stabilité. Les éléments spécifiques se rapportant à chaque organisation de soutien et à ses processus sont disponibles aux adresses suivantes 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, entre autres, 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.

5.5.2 L'ICANN est actuellement en train de collaborer avec la communauté pour réviser le processus d'élaboration de politiques (PDP) 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 d'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 à élaborer de meilleurs moyens d'évaluation de l'efficacité des nouvelles politiques.

5.5.3 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.

5.5.4 L'ASO élabore les politiques liées à l'attribution des blocs d'adresses IPv4 et IPv6, et de blocs de numéros de l'AS aux RIR.

5.5.5 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 éléments spécifiques liés aux fonctions, processus et activités de ces comités sont disponibles à l'adresse http://www.icann.org/en/committees/gac/. 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.

5.5.6 Le SSCA 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.

5.5.7 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/).

5.6 Engagement mondial pour renforcer la sécurité, la stabilité et la résilience

5.6.1 Activités et partenaires mondiaux

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. 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 clés comprennent :

- Le groupe de travail de l'ingénierie Internet (IETF)/l'Internet Architecture Board (IAB) : Dirige les efforts pour établir des approches technologiques visant à renforcer la sécurité de l'Internet concentrés sur l'élaboration de 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 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.

5.6.2 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 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 en tant que partie de l'effort plus large 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 en 2008 et 2009 des ateliers communs à Garmisch, en Allemagne avec le soutien du Centre germanoaméricain Marshall pour les études stratégiques. Les deux parties prévoient de poursuivre leur collaboration.
- ***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 fourni une formation sur la sécurité et la résilience des ccTLD conjointement avec l'association LACTLD avant la 34ème conférence internationale de l'ICANN tenue en mars 2009 et a programmé des séances futures avec la LACTLD. L'ICANN a également organisé une formation ccTLD conjointement avec l'association africaine des domaines de premier niveau (AfTLD) et l'ISOC-Afrique. Ces activités ont démarré en avril 2009 lors de la conférence de l'organisation africaine des domaines de premier niveau (AFTLD) à Arusha en Tanzanie.

5.6.3 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. Au niveau des organisations intergouvernementales, 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. Les aspects essentiels de l'engagement comprennent :

- ***Union internationale des télécommunications (ITU)*** - l'ITU mène un programme mondial cybersécurité (GCA) défini comme « un cadre pour la coopération internationale ayant pour objet d'accroître la confiance et la sécurité dans la société de l'information ». Dans le cadre de cet effort élargi, le bureau de développement des télécommunications de l'IUT, soit le IUT-D, a établi un programme de grande envergure pour collaborer avec les pays en développement et promouvoir les programmes nationaux de prise de conscience et de développement des compétences liés au renforcement de la cybersécurité. L'ICANN examinera toutes les possibilités de partenariat avec l'ITU dans ses efforts de cybersécurité, dans la sensibilisation, l'alerte et le développement des compétences, toujours consciente de son rôle technique pour le renforcement de la sécurité et de la résilience du DNS.
- ***Organisation de coopération et de développement économiques (OCDE)*** - 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 dans ce domaine.
- ***Autres organisations internationales et commissions économiques régionales des Nations Unies*** - L'ICANN communiquera avec d'autres organisations internationales et avec les commissions économiques des Nations Unies, orientant ses efforts vers la facilitation d'activités régionales conçues pour améliorer la sécurité et la résilience du DNS. Ces activités se

baseront sur les protocoles d'entente que l'ICANN a établis avec une variété d'organisations.

6. Plans de l'exercice financier 2010 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. Se projetant dans l'exercice 2009-2010, les plans de l'ICANN font appel à la réalisation d'un certain nombre d'initiatives clés comprenant :

- ***Opérations de l'IANA*** – recommander, éduquer et préparer pour la mise en œuvre des DNSSEC au niveau racine tel que proposé dans le plan stratégique de l'ICANN pour 2009-2012 ; ainsi qu'améliorer la gestion de la zone racine par le biais de l'automatisation ; et authentification améliorée des communications avec les gérants 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 et d'exercices.
- ***Registres gTLD*** – veiller à ce que l'évaluation des candidats aux nouveaux gTLD et des candidats aux 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 conjoint de planification des réponses aux attaques et aux imprévus (ACRP) établi conjointement avec le ccNSO et les associations de TLD régionales.
- ***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.
- ***Réponse à l'abus malveillant du système de noms de domaine*** - l'ICANN tirera parti de ses efforts collaboratifs 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. L'accent sera mis spécialement sur l'établissement d'une base solide de plans documentés et de procédures de soutien.

- ***Assurer l'engagement et la coopération au niveau mondial*** – l'ICANN renforcera les partenariats en vue d'inclure le groupe de travail de l'ingénierie Internet (IETF), la société Internet (ISOC), les groupes de registres Internet régionaux et opérateurs de réseau, et le centre d'opérations, d'analyse et de recherche du DNS (DNS-OARC). 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 présente en détail les objectifs spécifiques, les partenaires, les produits livrables et les engagements en matière de ressources au cours de l'exercice financier 2010.

6.1 Fonctions essentielles DNS/adressage

6.1.1 Opérations de l'IANA

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

6.1.1.1 La collaboration avec les partenaires de gestion de la zone racine, le Ministère du commerce des E.U. et VeriSign, en consultation avec la communauté Internet mondiale pour mettre en œuvre un processus de signature DNSSEC pour la zone racine. L'ICANN poursuivra ses efforts pour la mise en œuvre d'un processus tel que brièvement décrit dans sa proposition de septembre 2008. Selon la priorité définie dans le plan stratégique 2099-2012, l'ICANN sera prête, du point de vue opérationnel, à déployer les DNSSEC dans la zone racine d'ici la fin de 2009. L'ICANN a proposé une approche qui permet la continuation ininterrompue du mécanisme de distribution racine du DNS, une tâche partagée entre l'ICANN, VeriSign, le NTIA et les opérateurs de serveurs racine dans le cadre de l'exploitation des DNSSEC. L'ICANN a présenté des solutions flexibles qui satisfont une approche intermédiaire pouvant mener à une solution permanente, et a procédé à des préparatifs opérationnels afin de remplir son rôle.

L'ICANN poursuivra également une série d'activités permettant d'élargir la mise en œuvre des DNSSEC pour couvrir le DNS au niveau mondial. L'ICANN veillera à ce que ses programmes y compris les transferts entre registres 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) 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), en menant son propre banc d'essais et en facilitant le partage des leçons acquises parmi les parties impliquées dans la mise en œuvre des DNSSEC.

6.1.1.2 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 revues 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.

6.1.2 Opérations des serveurs racine du DNS

6.1.2.1 L'ICANN continuera à rechercher la reconnaissance mutuelle des rôles et des responsabilités des opérateurs de serveurs racine dans le cadre de son rôle général en matière de coordination du DNS. L'ICANN cherche également à favoriser l'établissement de mécanismes plus robustes pour la coordination en sa qualité de 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.

6.1.2.3 L'ICANN prévoit de poursuivre le renforcement 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. 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 outre, l'ICANN prévoit de collaborer avec le DNS-OARC pour établir un portail destiné au partage d'informations sur les meilleures pratiques de sécurité, stabilité et résilience et aux efforts collaboratifs à l'intention de l'ensemble de la communauté des registres.

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 au cours des 18 mois à venir. Leur rapport sur cette étude est attendu en septembre 2009. 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, qu'ils sont 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 pour y inclure un test réel du système de sauvegarde des données. 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 la même veine, 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 poursuivra sa collaboration avec l'IETF dans le cadre de son rôle général, établissant des protocoles Internet pour qu'une finalisation de la révision et donc, une validation d'un protocole IDNA sûr et stable s'ensuivent. Dans le cas où le protocole développé par l'IETF ne serait pas pleinement approuvé, l'ICANN pourra, suite aux recommandations de la communauté technique, établir des exigences supplémentaires spécifiques en termes de TLD IDN pour garantir qu'ils fonctionneront aussi bien à long terme lorsque la révision du protocole sera finalisée. L'ICANN continuera à faciliter les efforts des registres en collaborant avec les distributeurs pour veiller à ce que les tables IDN soient établies, 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 d'IDN et en quête d'assistance et d'expertise dans ce domaine.

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 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 ACRP met l'accent 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. Les programmes se prolongeront 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 sur l'aide au développement de programmes d'exercices et d'évaluation du plan d'opérations et de sécurité des ccTLD. Au cours de l'année prochaine, l'ICANN prévoit de mettre en place une livraison du programme ACRP dans des langues autres que l'anglais et de collaborer avec l'Institut d'ingénierie de logiciels de l'université de Carnegie-Mellon afin d'utiliser son Resiliency Engineering Framework (REF) dans le cadre d'un programme bénévole d'évaluation de la maturité des efforts portant sur la sécurité, la stabilité et la résilience des TLD.

6.2.5 Bureaux d'enregistrement

L'ICANN poursuivra l'élaboration des politiques pour renforcer les exigences d'accréditation des bureaux d'enregistrement et de sauvegarde des données à travers des améliorations des 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 des 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

6.2.6.1 L'ICANN continuera à élargir la portée de ses activités de mise en application contractuelle. Ceci inclut l'augmentation des effectifs chargés de la conformité contractuelle. Les nouveaux domaines d'activité principaux comprendront la mise en

place d'audits des parties contractantes dans le cadre de la mise en œuvre des amendements de mars 09 à l'accord d'accréditation de bureau d'enregistrement (RAA). De plus, en 2009, 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.

6.2.6.2 Le service de conformité contractuelle réalise actuellement 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 de mandataires 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 collaborative à l'abus malveillant du DNS

Le personnel de l'ICANN continuera à tirer parti des efforts collaboratifs 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 collaboratives 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'information 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 collaborative. 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 Facilitation de la sécurité dans l'ensemble du DNS

Le personnel de l'ICANN cherchera à tirer parti du symposium sur la sécurité, la stabilité et la résilience du DNS organisé en février 2009, en facilitant les efforts collaboratifs capitaux 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 Communication avec la NRO et les RIR

L'ICANN prévoit de poursuivre sa collaboration 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 les RIR concernant les activités collaboratives qui renforceraient l'assurance de sécurité, stabilité et résilience du DNS. Ces discussions comporteront la compréhension de l'intention des RIR 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

6.4.1 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 sera mis sur l'établissement d'une base solide de plans documentés et de procédures de soutien. Les initiatives spécifiques qui seront entreprises d'ici la mi 2010 pour améliorer la gestion du risque et le maintien de la continuité de l'ICANN comprendront 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 améliorera son utilisation de sites alternatifs dans le cadre de la mise en œuvre de la continuité TI. Un effort majeur établira un centre TI sûr et des centres de sauvegarde pour soutenir les programmes de continuité de l'ICANN. L'ICANN prévoit de réaliser une évaluation des risques de sécurité d'entreprise d'ici la mi 2009.

6.4.2 Au cours de l'année prochaine, le personnel de l'ICANN veillera à ce qu'un éventail complet de processus liés à l'information, au personnel et à la sécurité soit mis en place dans toutes ses opérations. 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 qui seront entreprises d'ici la mi 2010 pour améliorer le maintien de la sécurité de l'ICANN comprendront des améliorations des contrôles d'accès physiques et logiques, la sensibilisation des employés et la formation à la réaction aux incidents, le plan de sécurité du voyageur, les plans et réponses sécurité des réunions. 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.

6.4.3 Le personnel de l'ICANN prévoit de collaborer avec l'Institut d'ingénierie de logiciels (SEI) de l'université de Carnegie-Mellon afin de stimuler son Resiliency Engineering Framework (REF) pour s'assurer que ses programmes de sécurité, de continuité et gestion des risques incorporent les meilleures pratiques, et pour mesurer les améliorations vers un perfectionnement dans le temps. D'ici la fin de 2009, l'ICANN prévoit d'avoir évalué la maturité de son processus de base en ligne en accord avec l'approche REF. En outre, l'ICANN prévoit la réalisation d'une revue et d'un audit indépendants de ses programmes de sécurité et de continuité au cours de la première moitié de 2010.

6.5 Organismes de soutien et comités consultatifs de l'ICANN

6.5.1 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.

6.5.2 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 ciblé sur le deuxième des six efforts d'élaboration de politiques prévus pour traiter des divers aspects des transferts entre registres. 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, la 34ème conférence internationale de l'ICANN réalisée à Mexico en mars 2009 a comporté un atelier élargi sur la cybercriminalité et un deuxième atelier exclusivement consacré aux enregistrements frauduleux.

6.6 Engagement mondial

6.6.1 Accroître 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'accroître les partenariats puissants. Les activités spécifiques prévues avec ces partenaires au cours de l'exercice 2010 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. Des plans supplémentaires portent 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 sponsorisera la formation d'un portail hébergé par le DNS-OARC pour l'échange d'informations et le partage des meilleures pratiques en matière de sécurité, de stabilité et de résilience au sein de la communauté TLD. 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.

- ***Asie*** - L'ICANN prévoit d'examiner une relation possible avec le nouveau centre international de cybersécurité soutenu par le gouvernement malaisien, centrée sur les moyens selon lesquels l'ICANN peut contribuer aux efforts mondiaux pour lutter contre les cyberactivités malveillantes qui peuvent menacer les systèmes d'identificateurs uniques de l'Internet.

6.6.2 Entreprise commerciale

L'ICANN tirera parti du symposium de février 2009 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.

6.6.3 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 :

- ***Centre d'études stratégiques et internationales (CSIS)*** - L'ICANN prévoit une sponsorisation conjointe d'une série d'ateliers au cours de 2009-2010 pour inclure l'examen du rôle des organisations multipartites dans la cybersécurité mondiale. Ces efforts collaboratifs comprendront des ateliers avec les institutions partenaires du CSIS en dehors des États-Unis.
- ***Conseil Atlantique*** - L'ICANN prévoit de collaborer avec le conseil atlantique dans le cadre d'activités abordant les vulnérabilités croissantes des plus petits pays et organisations face aux cyberattaques et aux protestations grandissantes. L'ICANN se concentrera sur son rôle de facilitateur de la résilience du DNS face à une telle activité.

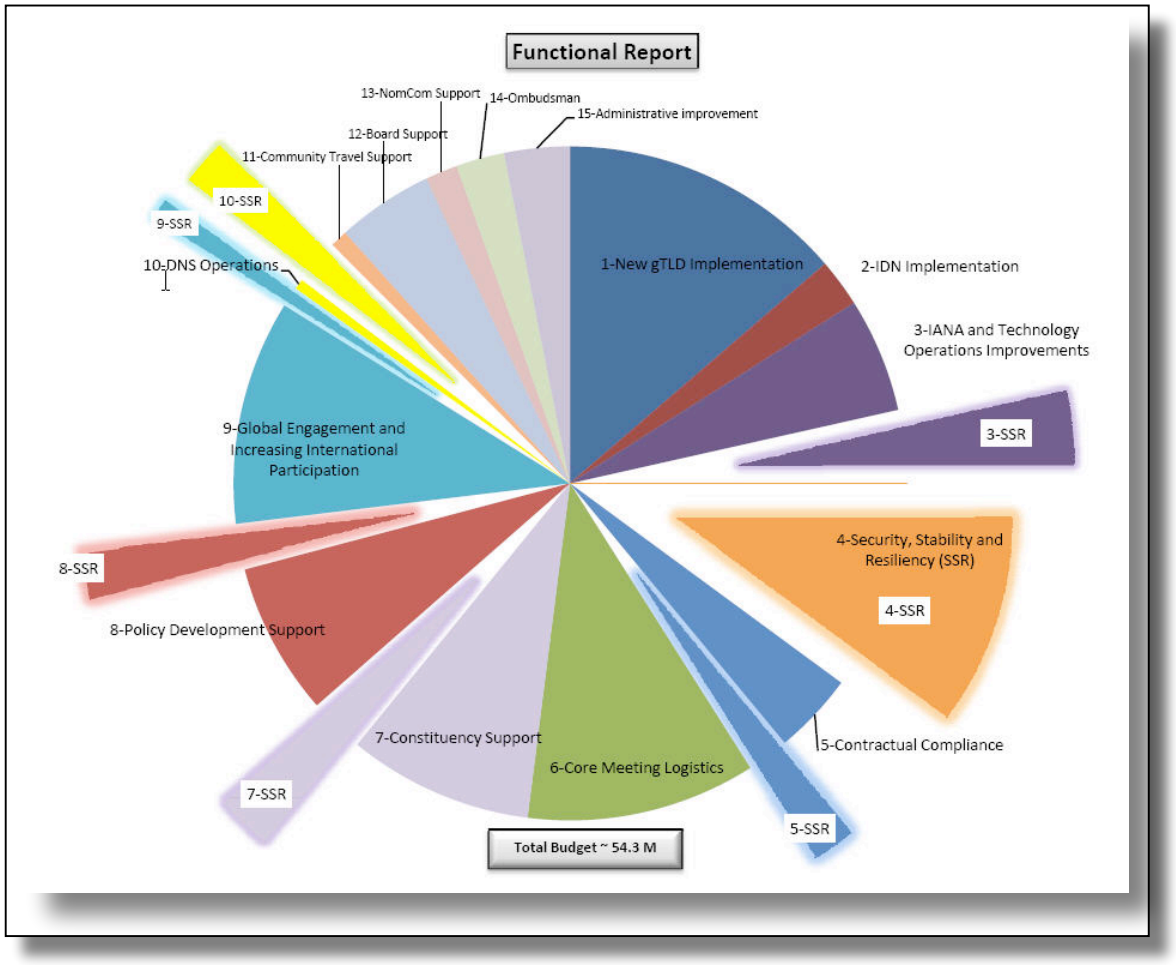
L'ICANN poursuivra activement les possibilités de collaboration avec d'autres groupes de réflexion et institutions académiques sur le leadership éclairé dans l'indentification des défis liés à la sécurité, la stabilité et la résilience.

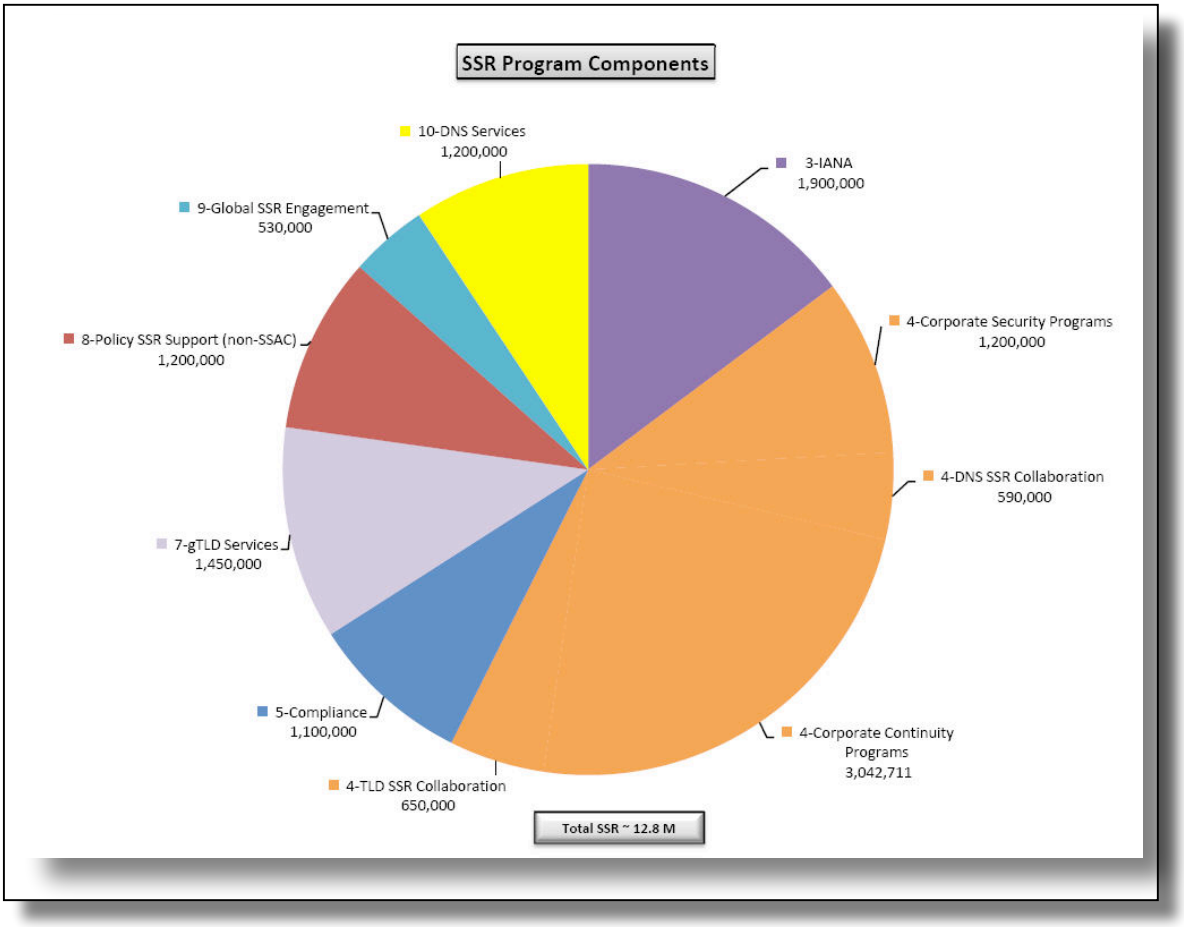
7. Conclusion

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 ; la collaboration avec les communautés de registres et de bureaux d'enregistrement TLD ; la communication avec la NRO et les RIR ; 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 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, en tant que 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


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 ~ 54.3 M


SSR Program Components
10-DNS Services
1,200,000
3-IANA
1,900,000
9-Global SSR Engagement
530,000
4-Corporate Security Programs
1,200,000
8-Policy SSR Support (non-SSAC)
1,200,000
4-DNS SSR Collaboration
590,000
7-gTLD Services
1,450,000
5-Compliance
1,100,000
4-Corporate Continuity
Programs
3,042,711
4-TLD SSR Collaboration
650,000
Total SSR ~ 12.8 M

Overview of Major Components of ICANN Security, Stability, Resiliency (SSR) Program

- IANA - $1.9 M
- DNS Services - $1.2 M
- DNS SSR Collaboration - $590 K
- gTLD Services - $1.45 M
- Compliance - $1.1 M
- TLD SSR Collaboration - $650K
- Global SSR Engagement - $530K
- Corporate Security Programs - $1.2 M
- Corporate Continuity Programs - $3.0 M
- Policy SSR Support (incl SSAC) - $1.2M

OVERALL SSR – $12.8 M

IANA Security, Stability and Resiliency (IANA)

Objectives	Deliverables (milestones)
- Automation of key elements in root zone change process - DNSSec operational readiness - Test rPKI implementation - Business continuity	- Implementation of automated RZM (date depends DOC approval; plan to have ready prior to implementation of new gTLDs) - Implement DNSSec signing of .ARPA (date depends on coordination with IAB and DOC) - Coordination with rPKI testers (currently underway) - IANA Continuity & Disaster Recovery Plan (approved by August 2009)
Key Stakeholders	**Resources**
- IANA, Security, IT - DOC/USG; Verisign - SSAC; RSSAC - IETF; DNS operator community, RIR communities; NRO	- Staffing – 6.5 FTE (including 2.5 FTE for related IT and other staff support) - Financial – $1.9M to support FTEs; staff support/travel; professional services; application development

ICANN DNS Services (IT Services)

Objectives
- Prepare for DNSSEC zone signing for ICANN zones, ARPA-related zones and the root
- Implement Trust Anchor Repository (TAR)
- Secure, resilient L-root operation

Deliverables (milestones)
- Trust Anchor Repository in full production: June 09
- L-root improvement (new design deployed at LA and Miami, 3rd node deployed at Prague): June 09
- Production infrastructure in place for signing root zone: Oct 09
- DNSSec signed ICANN zones: Oct 09

Key Stakeholders
- ICANN IT Services Team
- ICANN IANA staff, DoC, VeriSign
- ICANN Security & Resiliency Team

Resources (FY 10)
Human – 7.0 FTE (including related IT and other staff support)

Financial – $1.2M to support FTEs; planned capital investments for back-up services; DNSSec, L-root, improvements; backup facilities; professional services and travel

ICANN gTLD Registry/Registrar Services (Services)

Objectives
- Ensure implementation new gTLD/IDNs addresses SSR issues
- Continue maturing data escrow process & gTLD continuity procedures
- Conduct RSEP/RSTEP processes on registry services proposals

Deliverables
- Enhanced gTLD implementation process from SSR perspective
  - SSAC/RSSAC study complete (Fall 09)
  - Improved applicant guidebook (Aug 09)
- Conduct data escrow test (Aug-Sep 09 or Jan 10)
- Community failover exercise (Jan 10)
- RSEP/RSTEP studies as required

Key Stakeholders
- Registries/Registrars
- ICANN Services staff
- ICANN Security & Continuity staff
- GNSO/SSAC

Resources (FY 10)
Human – 2.75 FTE

Financial – $1.45M includes portion of evaluation staff/support for new gTLD/IDN activities to include TAS security; dedicated RSEP/RSTEP funds; support for testing/contingency exercise; staff travel/support

Contractual Compliance (Services)

Objectives	Deliverables

- Improved ICANN compliance process
- Improved compliant and WDPRS system
- Improved WHOIS data accuracy
	- Conduct audits as part of revised RAA implementation (50-100 by summer 2010)
	- Reporting improvements to WDPRS (by June 2010)
	- Conduct WHOIS related studies to further understanding of systems
	  - Proxy usage (Oct 2009)
	  - Data accuracy (Dec 2009)

Key Stakeholders - gTLD registry/registrars - ICANN Compliance staff - ICANN Security/Continuity staff	**Resources (FY 10)** Human – 3 FTE Financial – $1.1M support for FTEs, staff/travel support; professional services to conduct studies and support systems improvements

TLD Security, Stability & Resiliency Collaboration

(Security)

Objectives	Deliverables (milestones)
- Mature Attack & Contingency Response Program - Establish joint ISOC/ICANN tech training program - Establish TLD exercise planning workshops - Establish program metrics	- Conduct ACRP training sessions (5 in 2009); automate planning tool by Aug 09) - Joint technical training with ISOC plan (approve summer 09); first full program conducted fall 2009; two more by 2009) - Conduct exercise planning workshops (initial implementation Oct 2009) - Prototype metrics based on Resiliency Engineering Framework (fall 2009)
Key Stakeholders - ccTLD operators - ccNSO, regional TLD operators - ISOC/NSRC - ICANN staff	**Resources (FY 10)** Human – 1 FTE Financial – $650K for FTE, staff/travel to support; professional services for developing and conducting training programs

DNS Security, Stability & Resiliency Collaboration

(Security)

Objectives	Deliverables (milestones)
- Establish collaborative response mechanisms to DNS abuse - Share key SSR practices - Conduct community-based DNS risks & collaboration symposium - Enhance root server SSR collaboration	- Collaboration construct and on-going responses w/ partners (construct in place summer 2009) - Info Sharing Portal (Dec 09) - Conduct & report on symposium (Feb & Mar 2010) - Co-sponsor joint root community communications exercise (Fall 2009)
Key Stakeholders	**Resources (FY 10)**
- ISOC, DNS-OARC, FIRST - Root Server community - Broader DNS ops community - ICANN staff - RSSAC/SSAC	Human – 1.25 FTE Financial – $590K for FTE, professional services for portal and collaboration support, travel to support activities

Corporate Security Program (Security, IT, others across staff)

Objectives	Deliverables
- Improve and implement IT/Facilities/ Personnel Security Programs - Establish Formal Plans - Institute Security Training - Implement Traveler and Meetings Security & Contingency Plans	- Conduct Security Training Programs (embedded part of ICANN on-boarding by Sep 2009) - Improved IT & Physical Access Control Systems implemented (improved IT authentication on key systems – Fall 09) - Exercise Traveler and Meetings Security (one drill per trimester)
Key Stakeholders	**Resources**
- ICANN Security & Resiliency Team - ICANN IT/IANA/DNS Ops - ICANN Human Resources - ICANN Global Meetings Team - Other ICANN Staff	Human – 2 FTEs (includes IT support for security) Financial – $1.1 M including FTEs, physical & IT access controls, professional services for conducting training and audits

Corporate Continuity Program (Security, IT, others across staff)

Objectives

- Improve Business Continuity program
  - Establish formal plan
  - Establish secure data center
  - Establish formal drill/exercise programs

Deliverables

- Initial ICANN Business Continuity plan (Oct 09)
  - Improved Crisis Management plan (Aug 09)
- Establish Secure IT Data Center (Sep 09)
- Exercise Business Continuity/Crisis Management (Spring 10)

Key Stakeholders

- ICANN Security & Resiliency Team
- ICANN IT/IANA/DNS Ops
- ICANN Human Resources
- ICANN Global Meetings Team
- ICANN Staff

Resources

Human – 5 FTEs (includes planning and IT for data center)

Financial – $3.0M including FTEs, capital support for data center, professional services for conducting training and audits

Global Security, Stability and Security Engagement

(Global Partnerships & Security)

Objectives

- Sustain partnerships with key organizations (ISOC; IISI; IMPACT; EC/ENISA; CSIS; Atlantic Council)
- Continue participation in IGO sponsored cyber security dialogues OECD, IGF, others)
- Collaborate with others on global cyber security response

Deliverables

- Conduct joint activities with partner organizations (One per trimester)
- Engagement in forums across all major regions (On-going)
- Engage with Forum of Incident Response and Security Teams regarding ICANN role in response (initial findings Jan 2010)

Key Stakeholders

- Global/international organizations
  - ISOC; IETF; ITU; IGF
- Cyber security forums
- Governments/Commercial Stakeholders
- ICANN Global Partnerships Team & Security Staff

Resources (FY 10)

Human – 1.5 FTE

Financial – $530K for FTEs; staff/travel support; support to ICANN-led or supported forums; professional services support for metrics development

Policy Support for SSR-related efforts incl. SSAC (Policy)

Objectives	Deliverables

Set by supported SO/Acs conducting SSR activity
- GNSO; ccNSO
- GAC
- SSAC
- RSSAC; ALAC
	- SSAC Reports, Advisories, Comments
	  - Domain name protection study (Jun 09)
	  - Root Scaling Study with RSSAC (Sep 09)
	- Others will depend on SO/AC FY 10 work plans

Key Stakeholders	**Resources (FY 10)**
- Named SOs/ACs - ASO - ICANN policy staff - ICANN security	Human – 3.5 FTE Financial – $1.2M for FTEs and limited additional funding support for SSR-related activities; support for SSAC/RSSAC root scaling study

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 terme duquel les frais d'enregistrement doivent être totalement versés au 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 physiques 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 (Internationalised 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 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 protocole 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, elle forme la base des méthodes d'inter-réseautage de l'Internet, et constitue encore le protocole de couches Internet.

IPv6 – L'Internet Protocol version 6 est le successeur du protocole IPv4, pour la commutation de paquets et l'Internet. En décembre 1998, le groupe de travail de l'ingénierie Internet 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 Organization) **–** Organisation de ressources de numéros formée par les RIR.

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*, 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.