Cadre de la sécurité, la stabilité et la résilience

L'ICANN est une organisation mondiale chargée de coordonner les systèmes d'identifiant unique d'Internet au profit de l'intérêt public du monde entier afin d'assurer que l'Internet reste unique et interopérable.

Mars 2013

Table des matières

Liste de schémas et d'illustrations

Résumé

L'Internet s'est développé comme un écosystème constitué par un grand nombre de parties prenantes qui collaborent entre elles dans un environnement ouvert et transparent. L'Internet encourage le partage de connaissances, la créativité et le commerce dans le cadre d'une ressource commune mondiale. L'interopérabilité des ressources communes mondiales dépend de l'opération et de la coordination des systèmes d'identifiant unique d'Internet ainsi que de la santé, la stabilité et la résilience d'Internet.[1]

L'ICANN et les opérateurs de ces systèmes reconnaissent que le maintien et l'amélioration de la sécurité, la stabilité et la résilience de ces systèmes est un élément clé de leur relation de collaboration.

Depuis 2009, l'ICANN publie annuellement un Cadre sur la sécurité, la stabilité et la résilience (SSR). Le Cadre est reconnu dans l'affirmation des engagements[2], et a été analysé favorablement par l'équipe de révision de la sécurité et la stabilité [3] lors du processus de révision de l'affirmation des engagements.

Le cadre SSR décrit le rôle de l'ICANN et les limites de sa mission de soutien à un Internet unique, mondial et interopérable, ainsi que les défis que doivent relever les systèmes d'identifiant unique d'Internet. Le présent document comporte deux parties. La partie A explique les fondements du rôle de l'ICANN en matière de sécurité, de stabilité et de résilience, ainsi que l'écosystème d'Internet et la communauté de l'ICANN. La partie B décrit les objectifs stratégiques de l'ICANN en matière de SSR, ainsi que les activités prévues pour l'exercice opérationnel 2014 (juillet 2013-juin 2014).

Les changements majeurs dans l'exercice fiscal 2014 par rapport à l'exercice fiscal 2013 concernent l'adoption des recommandations de l'équipe de révision SSR en octobre 2012[4] et les réactions concernant les changements intervenus dans l'écosystème Internet, étant donné que la version précédente datait de juin 2012 (voir Partie B). Les activités prévues pour l'exercice fiscal 2014 se focaliseront sur le soutien à un écosystème sain afin de jeter les bases pour un Internet plus stable, plus fiable et plus résilient au profit de la communauté mondiale.

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

[2] Affirmation des engagements conclue entre le Département de commerce des États-Unis et l'ICANN, http://www.icann.org/en/about/agreements/aoc/affirmation-of-commitments-30sep09-en.htm.

[3] Rapport final de l'équipe de révision de la sécurité, la stabilité et la résilience, 20 juin 2012, http://www.icann.org/en/about/aoc-review/ssr/final-report-20jun12-en.pdf.

[4] Adoption des recommandations de l'équipe de révision SSR par le Conseil d'administration de l'ICANN, le 18 octobre 2012, http://www.icann.org/en/about/aoc-review/ssr/board-action.

Le Cadre de l'exercice fiscal 2014 est disponible sous la forme d'un document unique pour faciliter sa traduction et son partage à l'occasion de la prochaine conférence de l'ICANN à Beijing, Chine, du 7 au 11 avril 2013.

Partie A – Fondements du rôle de l'ICANN

Mission et valeurs principales de l'ICANN

> « La mission principale de l'ICANN consiste à assurer la coordination générale des systèmes d'identifiants uniques d'Internet au niveau mondial, et en particulier, leur fonctionnement stable et sécurisé. »
>
> Statuts de l'ICANN, amendés le 20 décembre 2012 (http://www.icann.org/en/about/governance/bylaws#I)
>
> Valeur principale nº 1 – « Préserver et améliorer la stabilité opérationnelle, la fiabilité, la sécurité et l'interopérabilité mondiale d'Internet »

Cette valeur fondamentale est reconnue dans l'affirmation des engagements, lorsqu'il est dit que « la coordination technique mondiale de la structure sous-jacente d'Internet –le DNS- est nécessaire pour assurer l'interopérabilité » et que « la préservation de la sécurité, la stabilité et la résilience du DNS » est un engagement clé au profit des utilisateurs d'Internet du monde entier.

Rôle et attributions de l'ICANN en matière de SSR

Dans le cadre du processus de révision prévu par l'affirmation des engagements, l'équipe de révision de la sécurité, la stabilité et la résilience a recommandé à l'ICANN de « publier une déclaration unique, claire et cohérente de ses attributions en matière de SSR et de sa mission technique limitée ». (Recommandation nº 1, 20 juin 2012).

Une version préliminaire de la déclaration sur le rôle et les attributions de l'ICANN en matière de sécurité, stabilité et résilience des systèmes d'identifiant unique d'Internet a été publiée en mai 2012 (http://www.icann.org/en/news/public-comment/draft-ssr-role-remit-17may12-en.htm), et révisée suite aux commentaires publics et aux discussions qui ont eu lieu dans le cadre des conférences de l'ICANN à Prague (juin 2012) et à Toronto (octobre 2012, http://toronto45.icann.org/meetings/toronto2012/presentation-draft-ssr-role-remit-04oct12-en.pdf).

La description ci-dessous du rôle et des attributions de l'ICANN concerne la recommandation nº 1 :

> En sa qualité d'organisation multipartite, l'ICANN facilite la sécurité, la stabilité et la résilience des systèmes d'identifiant unique d'Internet grâce à ses activités de coordination et de collaboration.
>
> Compte tenu de son caractère mondial, la communauté attend de l'ICANN qu'elle s'acquitte de sa mission de manière ouverte, responsable et transparente, et qu'elle assure l'inclusion de la grande diversité de parties prenantes qui composent le vaste écosystème d'Internet.

Du point de vue de sa mission technique, le rôle de l'ICANN vis-à-vis de la sécurité, la stabilité et la résilience englobe trois catégories de responsabilités :

1. Les responsabilités opérationnelles de l'ICANN (gestion organisationnelle des risques liés aux opérations internes, y compris la racine L, les opérations du DNS, les opérations de signature de clé du DNSSEC, les fonctions IANA, les opérations des nouveaux TLD, la gestion de la base de données des zones horaires, etc.) ;
2. L'engagement de l'ICANN en tant que coordinateur, collaborateur et facilitateur des questions techniques et politiques de la communauté globale en matière d'identificateurs uniques d'Internet ;
3. L'engagement de l'ICANN auprès des autres membres de l'écosystème mondial d'Internet.

Schéma 1 – Mission technique de l'ICANN

Définitions pour ce Cadre

Sécurité - la capacité de protéger et d'empêcher l'usage impropre des identificateurs uniques d'Internet.

Stabilité - la capacité à garantir que le système fonctionne conformément aux prévisions et à faire en sorte que les utilisateurs des systèmes d'identificateurs uniques y fassent confiance.

Résilience – la capacité du système d'identificateurs uniques à supporter / tolérer / survivre de manière efficace aux attaques malveillantes et à d'autres éléments perturbateurs sans interrompre ou arrêter le service.

Remarque – Ces définitions restent inchangées depuis le Cadre SSR de l'exercice fiscal 2012, publié en 2011.

Sur la base du travail accompli dans le 2ème Symposium sur la sécurité du DNS (tenu à Kyoto, Japon, en 2010) et le 3ème Symposium sur la sécurité du DNS (tenu à Rome, Italie, en 2011), une définition initiale de la **santé de l'identifiant unique** a été incluse dans le Cadre SSR de l'exercice fiscal 2014. Ce concept est une adaptation de la définition de « santé du DNS » figurant sur le rapport du Symposium de Kyoto :

> Un état de fonctionnement général des identifiants uniques d'Internet qui s'inscrit dans les limites techniques nominales en termes de cohérence, d'intégrité, de vitesse, de disponibilité, de vulnérabilité et de résilience.

Une définition issue du domaine de l'économie écologique décrit la santé de l'écosystème comme étant « une mesure de la performance totale d'un système complexe, construite à partir du comportement de ses parties. »[5]

Responsabilités ne relevant pas du rôle de l'ICANN en matière de SSR :

- L'ICANN ne joue pas un rôle de gendarme ou un rôle opérationnel vis-à-vis des comportements malveillants sur Internet ;
- L'ICANN n'est pas responsable de l'utilisation d'Internet à des fins de cyber espionnage ou de cyber guerre ;
- L'ICANN ne joue aucun rôle dans la détermination de ce qui constitue un comportement illicite sur Internet ;

En tant qu'organisation, l'ICANN n'est pas un organisme d'application de la loi, un tribunal ou une agence gouvernementale. Les organismes d'application de la loi et les gouvernements participent en tant que parties prenantes aux processus et au développement de politiques de l'ICANN.

En outre, l'ICANN joue un rôle de soutien au travail des organismes d'application de la loi ou des agences gouvernementales dans la mesure où elle met en place des actions légitimes à leur demande. L'ICANN participe aux côtés de la communauté de la sécurité opérationnelle à l'étude, l'analyse et l'identification d'usages malveillants ou frauduleux du DNS.

[5] Ce concept est adapté de « What is a healthy ecosystem? » de Robert Costanza et Michael Mageau, University of Maryland Institute for Ecological Economics, 1999, publié dans Aquatic Ecology, http://geminis.dma.ulpgc.es/profesores/personal/jmpc/Master08%28PrimeraEdici%F3n%29/Homeostasis/Homeo03s.pdf, http://books.google.com/books?id=YTeCxF5gqMQC&dq=ecosystem+and+health. Le concept décrit a été aussi influencé par « A Framework to Analyze the Robustness of Social-ecological Systems from an Institutional Perspective » (2004), http://www.ecologyandsociety.org/vol9/iss1/art18/.

L'ICANN ne peut pas suspendre ou annuler les noms de domaine de manière unilatérale. L'ICANN a le droit de faire respecter ses contrats avec des tiers, y compris auprès des prestataires de services d'enregistrement de noms de domaine.

En ce qui concerne les protocoles d'Internet, l'ICANN joue le même rôle que tout autre partie prenante ; l'ICANN n'a pas de compétence sur l'évolution des protocoles Internet et les normes y afférentes. L'ICANN soutient le développement de standards ouverts par le biais de processus multipartites et collaboratifs.

Le défi à relever

L'usage impropre et les attaques contre le DNS ou contre d'autres infrastructures Internet compromettent la sécurité de l'identifiant unique. Les attaques au DNS visent le vaste éventail d'utilisateurs, d'individus, de commerces, la société civile et les gouvernements.

Face à l'accroissement de la fréquence et de la sophistication des événements perturbateurs et des autres comportements malveillants, l'ICANN et la communauté mondiale doivent poursuivre leur collaboration en vue d'un écosystème sain, en améliorant la résilience des systèmes d'identifiant unique et en renforçant leurs capacités.

L'activité sur Internet témoigne du vaste éventail de motivations et de comportements humains. En partie, une telle activité reflète le caractère ouvert qui a fait le succès d'Internet et qui a permis l'innovation, le partage des connaissances, la créativité et le commerce au sein de ce patrimoine commun.

Dans l'environnement actuel de gouvernance multipartite et collaborative d'Internet, avec un écosystème Internet de plus en plus vaste, la vision traditionnelle de la cyber sécurité pilotée par un secteur, que ce soit les gouvernements ou le secteur privé, n'est plus valable. Ni les gouvernements ni les acteurs du secteur privé à titre individuel ne possèdent les attributions administratives ou légales adéquates pour agir sur l'ensemble hétéroclite de systèmes et de réseaux interconnectés, si bien que l'opération et la sécurisation de ces ressources constitue une tâche qui reste hors de la portée de tout effort qui ne soit multipartite et collaboratif.

Toutes les parties investies dans la cyber sécurité doivent adopter une vision plus large. La sécurité dans le cadre des identifiants uniques d'Internet devrait être abordée par le biais d'un écosystème Internet sain. Cette approche se base sur un Internet durable ou sain, stable et résilient. Un système qui soit durable pour l'avenir. Nous devons collectivement nous concentrer sur la capacité de l'écosystème à « maintenir sa structure et sa fonction au fil du temps face à des perturbations externes »[6].

Une montée en puissance des menaces contre les systèmes d'identifiant unique d'Internet a pu être constatée l'année dernière. Les attaques contre les opérateurs de registre des domaines de premier niveau (voir la déclaration de l'IEDR de novembre 2012, https://www.iedr.ie/wp-content/uploads/2012/12/IEDR-Statement-D-issued-8Nov.pdf et un article de Techcrunch de novembre 2012 sur PKNIC, http://ta.gg/5uf), les bureaux d'enregistrement, le secteur bancaire, les organismes d'application de la loi, ainsi que les menaces adressées aux opérateurs du

[6] Costanza et Mageau, et al.

serveur racine ont été signalées par les médias en 2012. Voir le rapport d'Arbor Networks sur la sécurité de l'infrastructure mondiale, de janvier 2013, sur http://www.arbornetworks.com/research/infrastructure-security-report.

L'intervention du gouvernement a entraîné la déconnexion des utilisateurs du monde extérieur, par exemple en Syrie (voir http://www.renesys.com/blog/2012/11/syria-off-the-air.shtml). L'impact de l'ouragan Sandy sur la connectivité Internet de la région nord-est des États-Unis a montré le pouvoir des désastres naturels sur les réseaux mondiaux (voir une Analyse préliminaire des pannes de réseau pendant l'ouragan Sandy, Rapport technique ISI-TR-685b de l'USC/ISI, novembre 2012, ftp://ftp.isi.edu/isi-pubs/tr-685.pdf).

Le faible rythme d'adoption du DNSSEC par les bureaux d'enregistrement, les développeurs d'applications et de navigateurs et les registrants compte parmi les tendances qui ont contribué à inhiber l'amélioration de la santé des systèmes d'identifiant unique. La prise de conscience accrue sur l'utilisation malveillante du DNS a stimulé le développement de tactiques et d'outils pour répondre à ce problème.

D'autres tendances qui ont été constatées :

- L'accroissement continu de l'adoption du DNSSEC par les opérateurs TLD.
- L'expansion des instances du serveur racine dans le monde entier.
- De nouveaux ccTLD (IDN et non-IDN) lancés dans un nombre croissant de langues et de jeux de caractères.
- Le progrès dans l'évaluation des candidatures du programme des nouveaux gTLD et l'introduction anticipée des nouveaux gTLD en 2013.
- L'intérêt croissant porté au renforcement des capacités en matière de cyber sécurité, qui a stimulé la mise en place de formations en matière de DNS pour les communautés juridique et d'application de la loi, outre les communautés opérationnelles.

L'écosystème Internet et la communauté de l'ICANN

L'ICANN est chargée d'opérer au profit de la communauté Internet dans son ensemble. Le public concerné comprend un ensemble varié de communautés, liées entre elles par Internet et fonctionnant comme un écosystème complexe. L'Internet est maintenant un élément essentiel pour l'échange mondial de connaissances et d'informations, ainsi que pour le commerce et la gouvernance. Déclaration de Vancouver de l'UNESCO, septembre 2012 (http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/mow/unesco_ubc_vancouver_declaration_en.pdf) et déclaration finale de la SMSI+10, Vers des sociétés du savoir pour la paix et le développement durable, 27 février 2013 (http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/wsis/WSIS_10_Event/wsis10_final_statement_en.pdf).

L'Internet est reconnu comme un élément essentiel pour soutenir l'économie mondiale et le développement durable (voir Perspectives de l'économie Internet de l'OCDE 2012, http://www.oecd.org/sti/interneteconomy/ieoutlook.htm).

Le terme « écosystème » décrit le monde naturel qui nous entoure. Il peut être défini comme le réseau d'interactions entre les organismes eux-mêmes et entre les organismes et leur

environnement. Les écosystèmes sont des entités dynamiques. L'Internet est un écosystème et un réseau d'organisations et de communautés. Ces organisations et ces communautés travaillent ensemble et jouent chacune un rôle. La réussite et l'essor d'Internet tiennent au fait que son écosystème est ouvert, transparent et collaboratif.

L'écosystème d'Internet est constitué par un certain nombre d'organisations et de processus qui façonnent la coordination et la gestion de l'Internet mondial et permettent son fonctionnement général. Parmi ces organisations on retrouve : des organisations d'ingénieurs et à vocation technologique, des opérateurs de réseau, des organisations de gestion de ressources, des utilisateurs, la société civile, des entités commerciales et non commerciales, des éducateurs, des décideurs politiques, des organismes d'application de la loi et des gouvernements.

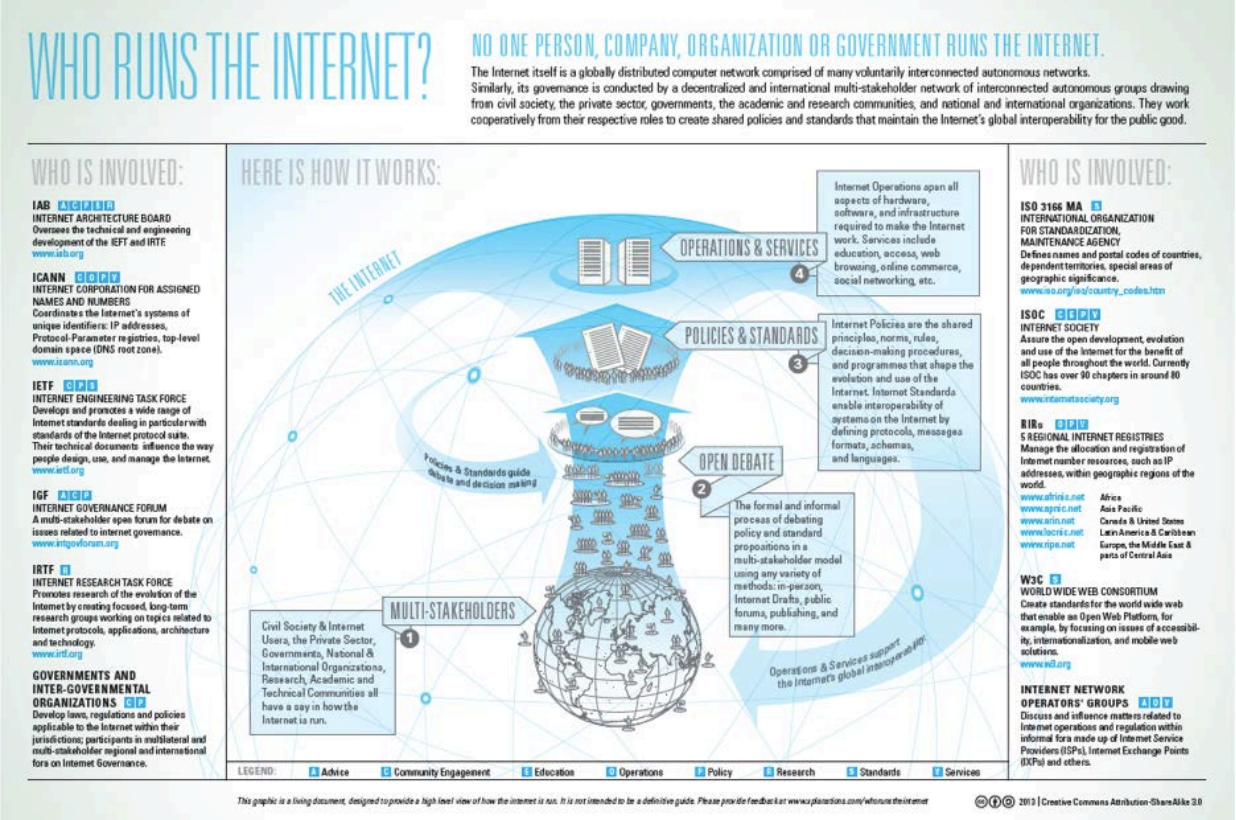


Schéma 2- Infographie de l'écosystème d'Internet

Du point de vue de l'ICANN, l'écosystème Internet peut être vu à trois niveaux :

- la communauté mondiale,
- la communauté de l'ICANN,
- et l'ICANN en tant qu'organisation.

La communauté mondiale est intégrée par ceux qui croient à un système d'identifiant unique sain, stable et fiable pour le partage de connaissances, le commerce et l'innovation, mais qui peuvent ne pas connaître ou participer à l'ICANN.

La communauté de l'ICANN est composée par la vaste communauté d'acteurs impliqués dans les programmes, les processus et les activités de l'ICANN, qui pilotent le modèle multipartite de développement de politiques au profit des utilisateurs mondiaux d'Internet.

L'ICANN en tant qu'organisation intègre les structures opérationnelles, les fonctions et le personnel chargés de soutenir la communauté de l'ICANN dans son ensemble et d'assurer la coordination multipartite des identifiants uniques d'Internet.

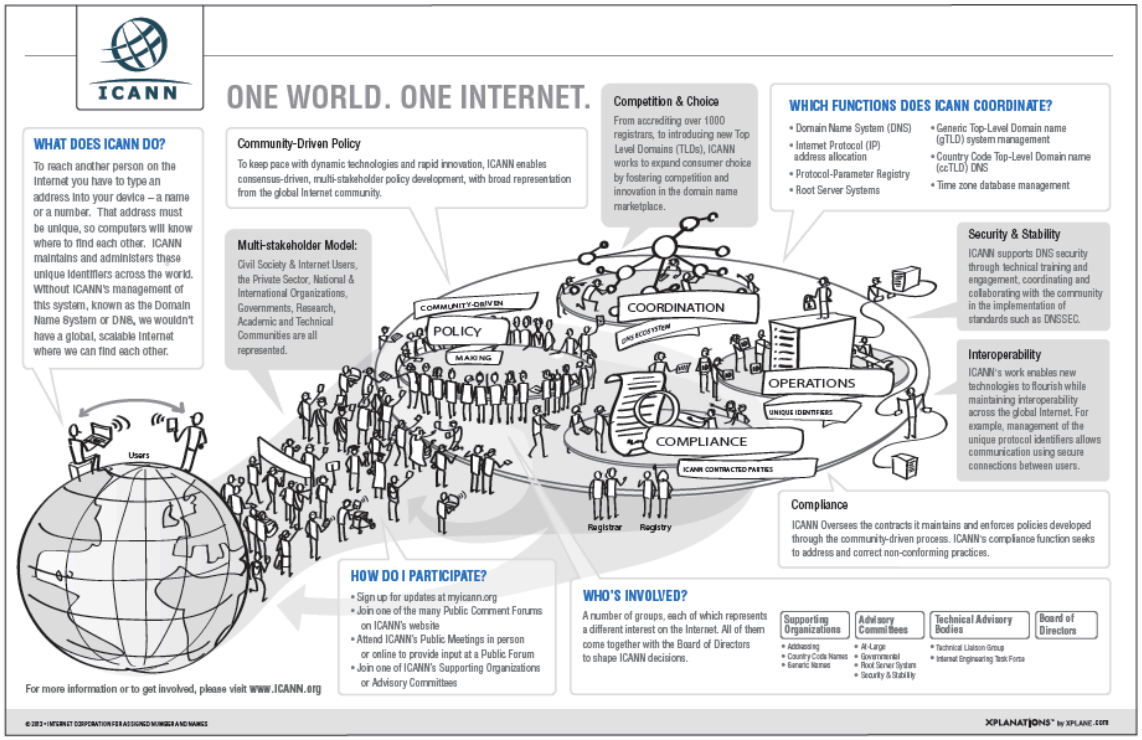


Schéma 3 – Infographie de l'ICANN

Une copie 11x17 de l'infographie ci-dessus est disponible en six langues sur https://community.icann.org/display/ISBM/Handouts+for+Speakers+Bureau.
La communauté participe aux activités de l'ICANN par le biais des groupes de parties prenantes, des regroupements, des organisations de soutien et des comités consultatifs. Des informations sur les comités consultatifs peuvent être trouvées en cliquant sur les pages ci-dessous :

1. Comité consultatif At-large - http://www.atlarge.icann.org/alac
2. Comité consultatif gouvernemental - https://gacweb.icann.org/
3. Comité consultatif sur le système de serveurs racine - http://www.icann.org/en/groups/rssac
4. Comité consultatif sur la sécurité et la stabilité - http://www.icann.org/en/groups/rssac

Ces comités fournissent des avis au Conseil d'administration de l'ICANN, participent aux processus de développement de politiques par le biais de leurs commentaires et encouragent la participation de la communauté.

Le développement de politiques concerne trois organisations de soutien :

1. Organisation de soutien aux politiques d'adressage (*Address Supporting Organization* - ASO) - http://aso.icann.org/ (adresses IP)
2. Organisation de soutien aux politiques de codes de pays (*Country Code Names Supporting Organization* - ccNSO) - http://ccnso.icann.org/ (ccTLD)
3. Organisation de soutien aux politiques des noms génériques– http://gnso.icann.org (gTLD)

Depuis la création de l'ICANN en 1998, il y a 15 ans, le DNS qui comptait à l'époque quelques centaines de milliers de noms de domaines, distribués dans sept domaines de premier niveau génériques et environ 250 000 TLD de code de pays, a fortement évolué et comporte maintenant plus de 250 millions de noms de domaine, utilisés par 2,5 milliards d'utilisateurs d'Internet, répartis dans 316 TLD. Cet espace connaîtra une croissance spectaculaire avec l'introduction des nouveaux TLD génériques en 2013.

À partir de mars 2013, il y aura 316 TLD délégués dans la zone racine. Le schéma ci-dessous explique la façon dont ces TLD sont catégorisés.

Schéma 4- TLD dans la zone racine (Crédit d'image : Kim Davies, IANA)

Relations en matière de SSR

L'ICANN entretient des relations avec des parties contractantes (registres et bureaux d'enregistrement de noms de domaines, fournisseurs de dépôt de données ou autres), met en place des partenariats, conclut des protocoles d'accord, établit des cadres de responsabilité et échange des lettres. D'autres relations moins formelles ou moins structurées peuvent exister entre l'ICANN et d'autres organisations internationales ou des parties prenantes de l'écosystème. https://www.icann.org/en/about/agreements.

Les parties impliquées dans le processus d'enregistrement de noms de domaine travaillent ensemble afin d'assurer que les décisions liées à la coordination technique mondiale des identifiants uniques d'Internet soient prises au profit de l'intérêt public, de façon responsable et transparente.

L'image ci-dessous décrit la nature des relations qui s'établissent dans le processus d'enregistrement de noms de domaine.

Suite aux recommandations 4 et 5 de l'équipe de révision de la SSR, l'ICANN est en train de documenter et de définir la nature de ses relations SSR avec la communauté de l'ICANN. Cela aidera à fournir une perspective simple pour comprendre les interdépendances entre les différentes organisations et entités dans le cadre de leurs différents rôles, et permettra à

l'ICANN de procéder à des arrangements de travail efficaces pour soutenir ses objectifs et ses buts stratégiques en matière de SSR.

Partie B - Module SSR pour l'exercice fiscal 2014

Cette section du Cadre sur la sécurité, la stabilité et la résilience se focalise sur les activités et les initiatives envisagées en matière de SSR pour l'exercice fiscal 2014, pour la période comprise entre le 1er juillet 2013 et le 30 juin 2014.

La sécurité dans le plan stratégique de l'ICANN

Le plan stratégique de l'ICANN identifie la stabilité et la sécurité comme étant l'un des quatre domaines d'intervention stratégique clés pour l'organisation. Cela va de pair avec la grande importance accordée à la SSR dans l'affirmation des engagements. Le plan stratégique répartit la vaste série de responsabilités de l'ICANN en matière de sécurité, de stabilité et de résilience en quatre domaines : les objectifs stratégiques, le travail communautaire, les projets stratégiques et le travail du personnel.

Le plan stratégique de l'ICANN 2012-2015 restera inchangé en 2013 (voir https://www.icann.org/en/news/announcements/announcement-28jan13-en.htm). Il s'agit du même plan stratégique publié avant le Cadre SSR de l'exercice fiscal 2013 (Juin 2012). À partir des commentaires reçus lors du cycle de planification 2013, il a été constaté qu'il existe une demande constante de formation et d'activités de renforcement des capacités de la part de la communauté. Cette demande témoigne du soutien au travail technique réalisé par l'équipe de sécurité de l'ICANN.

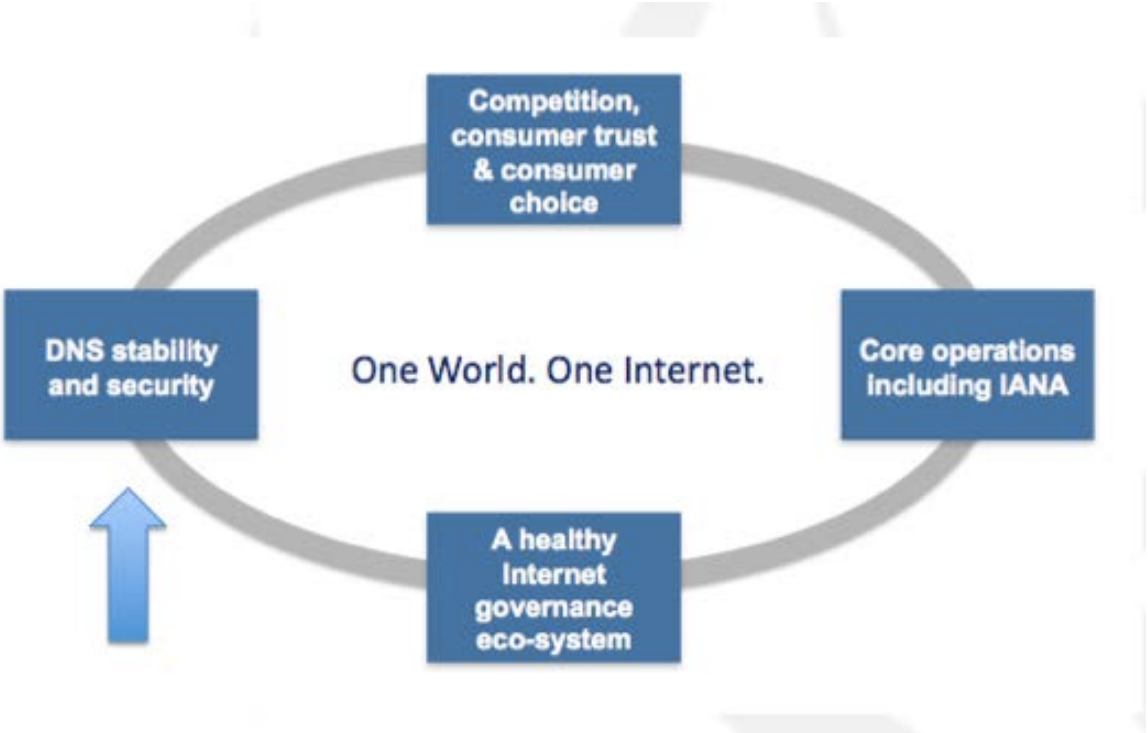


Schéma 5 – Plan stratégique de l'ICANN

Le plan stratégique 2012-2015 décrivait 5 objectifs stratégiques pour la sécurité et la stabilité du DNS :

1. Maintenir et gérer la disponibilité du DNS.
2. Améliorer la gestion de risques et résilience du DNS, les adresses IP et paramètres.
3. Promouvoir l'adoption généralisée du DNSSEC.
4. Améliorer la coopération internationale en matière de DNS.
5. Améliorer la réponse aux incidents de sécurité du DNS.

L'ICANN commencera un processus de planification stratégique en vue de l'élaboration d'un plan à long terme pour les cinq prochaines années, à partir de juin 2013. Des informations complémentaires seront disponibles sur cette nouvelle approche. Étant donné l'importance clé que revêt la sécurité pour l'organisation, la sécurité, la stabilité et la résilience des systèmes d'identifiant unique resteront des domaines stratégiques incontournables pour l'ICANN.

Révision de l'affirmation des engagements

L'affirmation des engagements conclue entre l'ICANN et le Département de commerce des États-Unis le 30 septembre 2009 (http://www.icann.org/en/documents/affirmation-of-commitments-30sep09-en.htm) reconnaît qu'un engagement clé est celui de préserver la sécurité, la stabilité et la résilience du DNS (Section 3b). L'affirmation des engagements a également « institutionnalisé et formalisé la coordination technique du système de noms et d'adressage d'Internet (DNS) au niveau mondial sous le leadership d'une organisation du secteur privé ».

Dans sa section 9.2, l'affirmation reconnaît que l'ICANN a adopté un plan de sécurité, stabilité et résilience (SSR) qui sera régulièrement mis à jour afin de refléter les menaces naissantes pour le DNS (y compris les identifiants uniques). Ce plan sera révisé au moins tous les trois ans.

La première révision du plan SSR, qui s'est achevée en juin 2012, « a trouvé des domaines où le travail de l'ICANN est satisfaisant, des domaines où des améliorations pourraient être introduites et d'autres domaines où des éléments clé en matière de SSR devraient être définis et mis en œuvre. » Rapport final de l'équipe de révision SSR, Juin 2012.

Le Conseil d'administration de l'ICANN a approuvé le rapport final et les recommandations en octobre 2012.[7] Depuis sa réunion à Toronto, l'ICANN a avancé dans la mise en œuvre des recommandations de l'équipe de révision SSR.

Une mise à jour sur les progrès de mise en œuvre de l'ICANN a été publiée le 19 décembre 2012 (http://blog.icann.org/2012/12/tracking-the-ssr-review-implementation/). Deux recommandations ont déjà été mises en œuvre (recommandations 18 et 24). Pendant la période comprise entre ce qui reste de l'exercice fiscal 2013, l'exercice fiscal 2015 et le début du prochain processus de révision SSR, l'ICANN fera le suivi de la mise en œuvre des

[7] http://www.icann.org/en/groups/board/documents/resolutions-18oct12-en.htm#1.e

recommandations ainsi que des autres révisions de l'affirmation des engagements (http://www.icann.org/en/news/in-focus/accountability).

Les vingt-huit recommandations sont conformes à la structure de gestion de l'ICANN présentée lors de la réunion de l'ICANN à Toronto. Il s'agit de :

- L'affirmation des objectifs [Recommandations 1, 2, 18, 24]
- L'excellence des opérations [Recommandations 7, 8, 17, 20, 21, 9, 10, 11, 22, 25, 26, 27, 15, 28]
- L'internationalisation [Recommandations 3, 4, 5, 14, 16]
- L'évolution du modèle multipartite [Recommandations 6, 12, 13, 19, 23]

Des détails supplémentaires sur la mise en œuvre de chacune des recommandations sont présentés dans l'Annexe A. Les plans et les cadres SSR de l'ICANN couvrant les exercices fiscaux 2010, 2011, 2012 et 2013 sont disponibles sur https://www.icann.org/en/about/staff/security/archive.

Une nouvelle saison – Vers une organisation matricielle

En octobre 2012, lors de la réunion de l'ICANN tenue à Toronto, le PDG de l'ICANN Fadi Chehadé a présenté la nouvelle structure de gestion de l'ICANN. Celle-ci applique une organisation matricielle aux fonctions de l'ICANN. La sécurité fait partie des fonctions techniques de l'ICANN, associée aux équipes opérationnelles IANA, IT et DNS de l'ICANN.

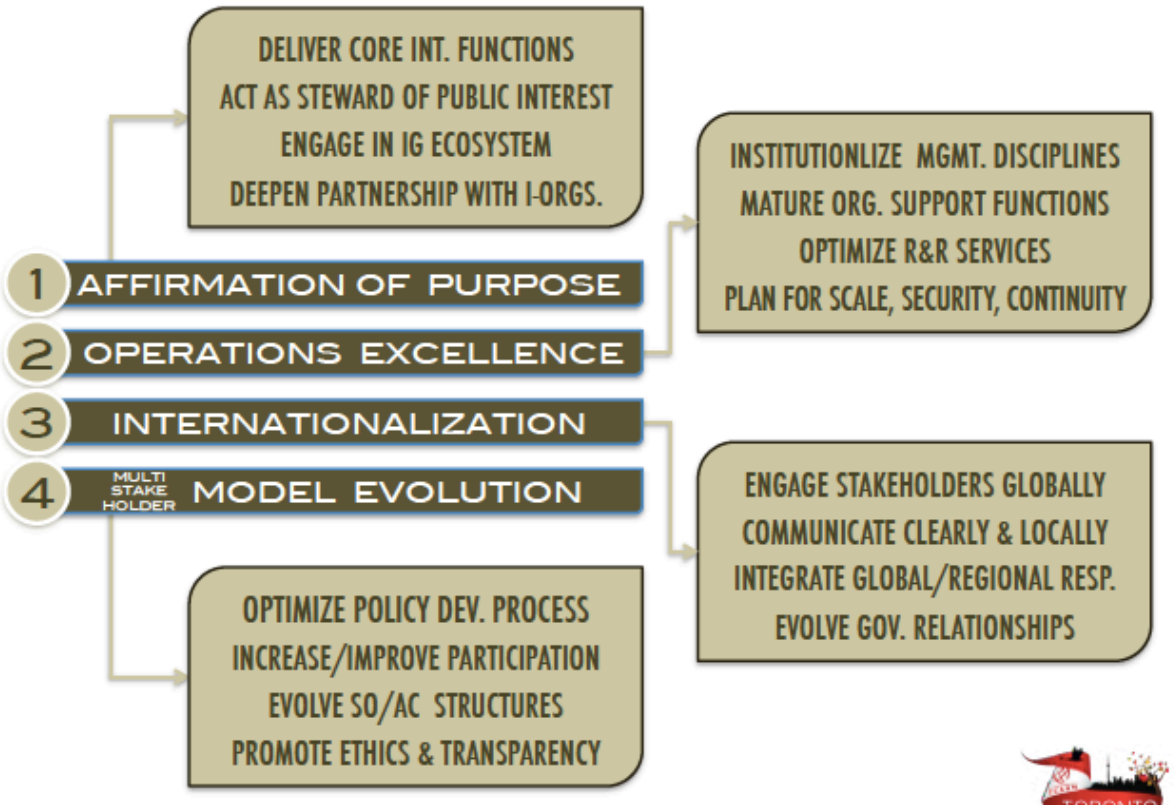


Schéma 6- Domaines de gestion de l'ICANN

L’activité de l’équipe de sécurité traverse l'organisation et apporte son soutien à chacun des domaines de gestion. Cela inclut le soutien à l'excellence des opérations et à l'équipe de l’engagement des parties prenantes mondiales de l’ICANN (*Global Stakeholder Engagement* - GSE) dans les domaines de l'internationalisation, l'évolution du modèle multipartite et les discussions avec la communauté sur la gouvernance d'Internet.

Suite à l'application du modèle matriciel, le travail de l’ICANN sera réparti en trois plateformes principales – Los Angeles, Singapour et Istanbul. L’ICANN gardera également des bureaux à Bruxelles, à Washington DC et dans d’autres sites, afin de rester proche de ses parties prenantes.

Visualisation de la sécurité de l'ICANN

Dans le cadre des explications sur le rôle et les attributions de l’ICANN, le schéma ci-dessous permet de visualiser les fonctions de l'ICANN dans le domaine de la sécurité, la stabilité et la résilience.

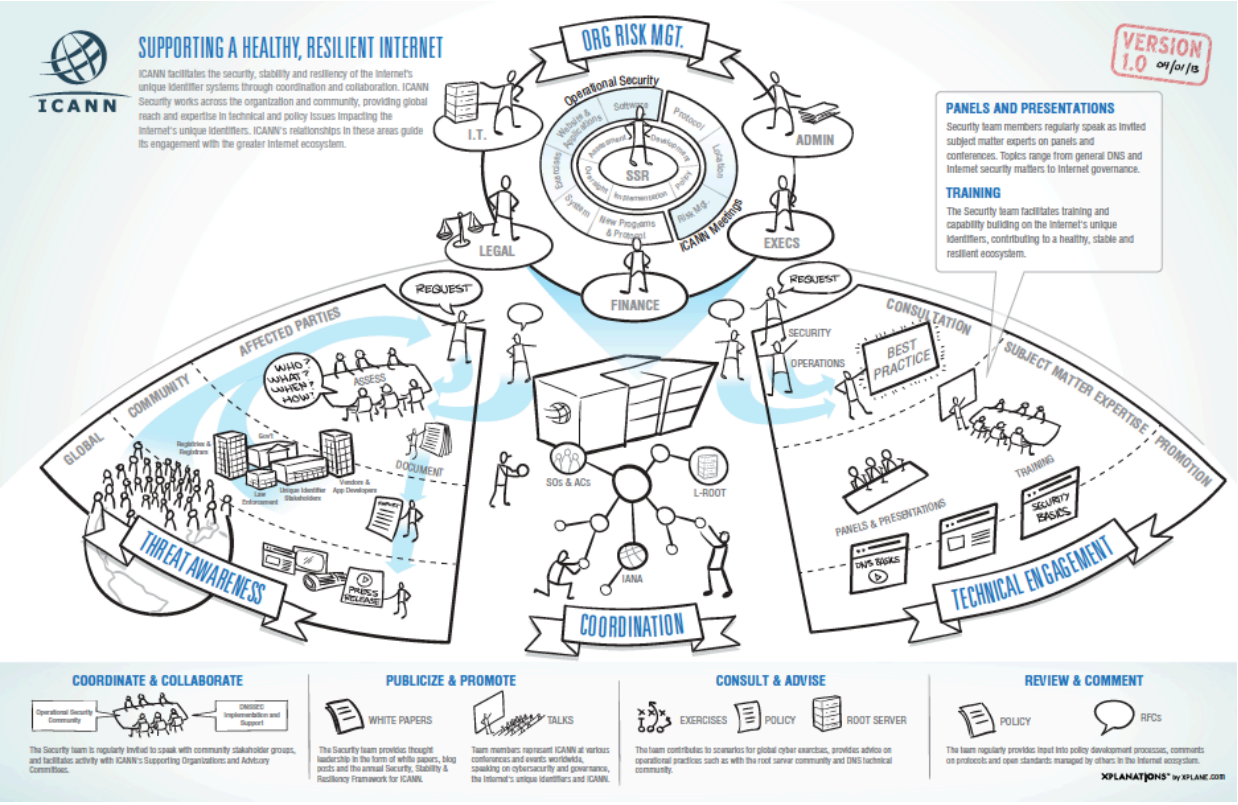


Schéma 7 – Infographie de la sécurité de l’ICANN

Ce schéma montre les fonctions primaires de l’ICANN en matière de sécurité, de soutien à la gestion du risque organisationnel, d'assistance à la prise de conscience sur les menaces qui pèsent sur les identifiants uniques d’internet, de collaboration et de coordination avec des partenaires de la communauté d’Internet et de mise à disposition d’expertises techniques, y compris par le biais de formations, de leadership et de consultation sur des questions techniques et politiques. (Remarque – ce travail est en cours et sera révisé avant la réunion de l’ICANN à Beijing)

Comment la sécurité, la stabilité et la résilience s'inscrivent dans les domaines fonctionnels de l'ICANN

La sécurité au sein de l'ICANN peut être considérée comme :

- une valeur fondamentale pour l'ICANN, dans l'affirmation des engagements
- un des quatre domaines d'intervention du plan stratégique
- un domaine thématique d'ordre général qui traverse l'organisation
- un département au sein de l'ICANN
- un élément essentiel dans les projets et les activités

La sécurité dans l'ICANN est assurée par une équipe décentralisée à envergure mondiale, ayant une expertise technique et politique qui lui permet de se pencher sur les problèmes susceptibles d'impacter sur les identifiants uniques d'Internet. L'équipe de sécurité joue un rôle interne et externe. Son travail, transversal à l'organisation et à la communauté, vise à soutenir la mission de l'ICANN consistant à préserver et à améliorer la stabilité opérationnelle, la fiabilité et l'interopérabilité mondiale d'Internet. Cette tâche peut ne pas toujours être visible ou publique, mais joue un rôle important pour l'ICANN et ses engagements. L'équipe sert de passerelle entre les opérateurs de DNS, la communauté technique, l'application de la loi, la communauté chargée de la sécurité opérationnelle et les groupes de parties prenantes.

Membres de l'équipe de sécurité de l'ICANN

Au moment de la publication du présent document, l'équipe de sécurité est intégré par :

- Jeff Moss – Vice-président et chef de la sécurité (chef d'équipe et membre de l'équipe exécutive de l'ICANN; collaborateur technique et intervenant fréquent sur des thèmes liés à Internet et aux problèmes de sécurité)
- Geoff Bickers – Directeur des opérations de sécurité (programmes de sécurité d'entreprise, sécurité des réunions, sécurité physique et personnelle de l'ICANN, liaison avec l'IT de l'ICANN)
- John Crain – Directeur principal, sécurité, stabilité et résilience (chef de l'engagement technique en matière d'identification et de surveillance de menaces, et représentant des serveurs racine auprès du Conseil du DNS-OARC.
- Patrick Jones – Directeur principal, Sécurité (coordonateur d'équipe, membre de l'équipe exécutive de l'ICANN, de l'équipe de mise en œuvre de la révision SSR, liaison auprès de l'ICANN GSE et collaborateur en matière de gouvernance Internet)
- Richard Lamb – Gestionnaire principal de projet, DNSSEC (collaborateur technique en matière de formation et d'adoption du DNSSEC ; collaboration avec la communauté en matière de DNSSEC ; gestion de politiques et de pratiques pour le déploiement du DNSSEC)
- Dave Piscitello – Technologue expert en sécurité (engagement technique, leader en formation et réflexion ; leader auprès de la communauté d'application de la loi et de la

sécurité opérationnelle ; membre du groupe de gestion exécutive de l'Initiative du Commonwealth sur la cybercriminalité).

- Sean Powell - ingénieur spécialiste en sécurité informatique (sécurité organisationnelle ; sécurité des réseaux et des informations ; collaboration avec l'IT de l'ICANN et soutien au Directeur des opérations de sécurité)

Photo 1 – Jeff Moss lors de l'IGF en Russie

Photo 2 – John Crain, Rick Lamb (ICANN) et Revil Wooding (PCH) à l'occasion du CaribNOG3

Photo 3 – Patrick Jones lors du Dialogue sur la cyber sécurité de l'OEA, décembre 2012


Photo 4 – Dave Piscitello intervenant à la Conférence du réseau droit pénal de la CPI, La Haye, décembre 2012.

Critères de participation

En février 2012, l'équipe de sécurité a formalisé ses critères en matière de sensibilisation et d'engagement. Les critères ont eu une influence sur d'autres parties de l'ICANN et visent à orienter l'équipe de sécurité de l'ICANN et la direction exécutive par rapport aux types d'activités collaboratives et communautaires soutenues par l'équipe de sécurité.

Tableau 1 – Critères de sécurité pour la sensibilisation et l'engagement

Types d'événements	Exemples
Réunions publiques de l'CANN	ICANN Beijing, Durban, Buenos Aires
Réunions internes de l'ICANN	Réunion exécutive, équipe de sécurité, atelier du Conseil d'administration, formation de personnel, budget, autres.
Réunions concernant des aspects opérationnels de l'ICANN/l'IANA/la racine-L/le DNSSEC, etc.	IETF, DNS-OARC, RIPE NCC, NOG, SSAC, RSSAC, entre autres
Réunions où l'ICANN collabore en matière de menaces mondiales/atténuation	APWG, MAAWG, Conférence de l'Interpol sur l'économie souterraine, exercices de cyber sécurité, OEA
Collaboration technique – Formations et renforcement des capacités	Formation sur la planification de réponses aux attaques et aux imprévus (ACRP), opérations de sécurisation des registres, DNSSEC, application de la loi et gouvernement, Initiative du Commonwealth sur la cybercriminalité.
Symposiums, interventions de PME invitées, éducation continue	SATIN, Symposium SSR, Security Confab, RSA, BlackHat, FIRST, ICLN
Collaboration dans l'écosystème, modèle multipartite	IGF et IGF régionaux, RANS, OCDE, Forum WSIS, Cyber sécurité panarabe, CTU

Critères de participation	✓
L'événement soutient-il un objectif stratégique de l'ICANN ?	1. Maintenir et faciliter la disponibilité du DNS 2. Améliorer la gestion des risques et résilience du DNS 3. Promouvoir l'adoption généralisée du DNSSEC. 4. Améliorer la coopération internationale en matière de DNS. 5. Améliorer la réponse aux incidents de sécurité du DNS.
L'événement s'inscrit-il dans un des domaines suivants ?	1. opérationnel / organisationnel 2. collaboration 3. engagement technique
L'événement soutient-il un partenariat, un protocole d'accord ou une relation avec des parties prenantes ?	
Contribue-t-il ou renforce-t-il la réputation de	

l'ICANN en tant qu'organisation?	
Quelle est la fréquence de l'événement ?	
Existe-t-il la possibilité de rencontrer d'autres parties prenantes à proximité ?	Qui d'autre y participe ?
Comment cet événement est-il pris en compte dans le budget ?	Le but est-il de soutenir une autre équipe?

Avec la création de la nouvelle structure matricielle, l'équipe de sécurité prête son concours à l'équipe de l'engagement des parties prenantes mondiales de l'ICANN (GSE) ainsi qu'à d'autres équipes au sein de l'organisation. Voici des exemples de types d'événements et d'activités soutenues par l'équipe de sécurité de l'ICANN :

- Réunions de l'IETF à Vancouver et à Atlanta
- Réunions de X-CON, CNNIC et CONAC en Chine
- BlackHat et DefCon à Las Vegas, Abu Dhabi et Amsterdam
- Groupe d'experts des Nations Unies sur les noms géographiques / Conférence des Nations Unies sur la normalisation des noms géographiques à New York
- Conférence de l'Interpol sur l'économie souterraine à Lyon, France
- Réunion des registres CIS à Budva, Monténégro
- Formation en matière de DNS avec l'Agence de lutte contre la grande criminalité organisée et l'*Office of Fair Trading* (l'autorité britannique de la concurrence) à Londres, Royaume-Uni
- Formation sur le DNSSEC en Colombie avec .CO ; au Pérou avec .PE et avec le *Network Startup Resource Center* à Hong Kong
- Formation sur le renforcement des capacités du DNS avec LACTLD à Saint Martin et au Paraguay
- Télécommunauté de l'Asie et du Pacifique, à Macao
- MENOG en Jordanie
- LACNIC/LACNOG en Uruguay
- Formation sur le DNS avec Europol
- MAAWG, APWG, RIPE NCC et DNS-OARC
- Lancement par l'OEA/CICTE d'un cyber laboratoire pour la réalisation d'exercices
- APNIC 34
- ION Mumbai et Interop
- Discussions et présentations à distance, dans le cadre de l'IGF Caraïbes à Sainte Lucie en août 2012 et de la Conférence sur les TIC à Népal, en février 2013

Un élément clé de la collaboration technique de l'équipe de sécurité concerne les formations en matière de DNS en réponse à des demandes de la communauté. L'équipe a développé un programme, qui comporte des modules sur :

- Les Bases du DNS (y compris un aperçu de la participation à l'ICANN)
- Le programme de réponse à des attaques et à des imprévus pour les opérateurs TLD
- La formation en matière de DNS adressée à la communauté de l'application de la loi et à la communauté de la sécurité opérationnelle
- La formation en matière de DNSSEC
- Un cours sur la sécurisation des opérations de registre

L'ICANN est souvent partenaire du *Network Startup Resource Center* (http://nsrc.org/), basé à l'Université d'Oregon, dans des activités de collaboration technique auprès d'organisations TLD régionales, des universités et des opérateurs du monde entier. L'ICANN est aussi partenaire d'AfTLD, APTLD, LACTLD pour ces formations.

Activité à l'échelle internationale

Sur la scène mondiale, des activités importantes ont été mises en place au cours de l'exercice fiscal 2013. L'ICANN a souscrit aux principes sur la cyber résilience du Forum économique mondial, http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf, et a participé aux réunions du Forum économique mondial à Davos, Suisse, et à Washington DC en 2012 et en 2013.

L'ICANN a accueilli l'Initiative du Commonwealth sur la cybercriminalité (CCI) à sa réunion de Prague, en République Tchèque, en juin 2012. Dave Piscitello, membre de l'équipe de sécurité de l'ICANN, a été nommé membre du groupe de gestion exécutive de la CCI en novembre 2012 (http://blog.icann.org/2012/11/icann-security-team-members-appointed-to-lead-roles-in-global-community-initiatives/).

L'ICANN a soutenu la formation DNSSEC en Amérique Latine et aux Caraïbes (Trinité, Colombie, Chili, Pérou et Paraguay).

En juillet, le Département du Commerce des États-Unis a annoncé l'attribution à l'ICANN du contrat des fonctions IANA, http://www.ntia.doc.gov/press-release/2012/commerce-department-awards-contract-management-key-internet-functions-icann. L'ICANN a publié une version publique de sa proposition de contrat pour les fonctions IANA le 9 juillet 2012 : https://www.icann.org/en/news/announcements/announcement-2-09jul12-en.htm. Le contrat concerne la période comprise entre le 1er octobre 2012 et le 30 septembre 2015, avec deux périodes optionnelles séparées, pour une durée totale du contrat de sept ans.

En juillet 2012, l'ICANN a participé à la réunion sur la cyber sécurité hémisphérique de l'OEA tenue en Uruguay et au Dialogue sur la cyber sécurité de l'OEA à Washington, le 13 décembre 2012, http://www.oas.org/en/media_center/press_release.asp?sCodigo=E-465/12.

En août 2012, l'IAB, l'IEEE-SA, l'IETF, l'ISOC et le W3C ont lancé *Open Stand* (http://open-stand.org/), un modèle ouvert pour le développement collaboratif et ascendant de standards

pour l'innovation et l'interopérabilité. Cette initiative est en ligne avec les principes de l'ICANN en matière de collaboration multipartite, ascendante et axée sur le consensus.

L'ICANN a participé au 3ème Conseil de la Commission fédérale américaine des communications (US FCC) sur la sécurité, la fiabilité et l'interopérabilité (CSRIC III). Le groupe de travail 4 a publié son rapport sur les meilleures pratiques en matière de sécurité du réseau en septembre 2012 (http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRICIII_9-12-12_WG4-FINAL-Report-DNS-Best-Practices.pdf). Des contributions ont été faites au Groupe de travail 3, au DNSSEC et groupe de travail 7, au Code de conduite Anti-Bot pour les ISP.

L'ICANN a participé à la Conférence de Budapest sur le cyberspace en octobre 2012 (http://www.cyberbudapest2012.hu/), qui a fait suite à la Conférence de Londres de 2011 (https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement).

L'ICANN a co-présidé son 4ème Symposium mondial DNS SSR avec son groupe de travail anti-hameçonnage (APWG) dans le cadre de la réunion eCOS à Las Croabas, Puerto Rico en octobre 2012 (http://docs.apwg.org/events/2012_ecrime.html).

L'OCDE a publié une analyse des stratégies nationales en matière de cyber sécurité en octobre 2012, identifiant dans plusieurs stratégies nationales le soutien à des dialogues multipartites sur la cyber sécurité. Le titre exact de cette publication : OCDE (2012), « *Cybersecurity Policy Making at a Turning Point : Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy* », OECD Digital Economy Papers, No. 211, Publications de l'OCDE. http://dx.doi.org/10.1787/5k8zq92vdgtl-en.

L'ICANN a été bien représentée au 7ème Forum sur la gouvernance d'Internet à Baku, Azerbaïdjan, en novembre 2012 (http://blog.icann.org/2012/10/icann-at-internet-governance-forum-2012-2/), où la sécurité d'Internet a été un des principaux sujets de discussion (http://www.intgovforum.org/cms/component/content/article/114-preparatory-process/927-igf-2012). L'ICANN a également participé à des événements régionaux de l'IGF en Amérique Latine et les Caraïbes, en Russie, aux Émirats arabes unis et aux États-Unis.

En décembre 2012, le PDG de l'ICANN Fadi Chehadé a fait une présentation à l'ouverture de la Conférence mondiale des télécommunications internationales à Dubaï (http://www.itu.int/en/wcit-12/Pages/speech-chehade.aspx). En février 2013, l'ICANN a participé au groupe informel d'experts chargé de la préparation de la prochaine édition du Forum mondial des politiques de télécommunications qui se tiendra à Genève, en mai 2013.

L'ICANN a participé à l'Observatoire panarabe pour la sûreté et la cyber sécurité à Tunis, Tunisie, en décembre 2012, où elle a partagé des informations avec les participants sur ses rôles et ses attributions dans les activités liées à la sécurité, la stabilité et la résilience. En décembre, l'ICANN a également participé à la Conférence du réseau droit pénal international à La Haye, Pays Bas, et a collaboré avec Europol afin de faciliter des formations en matière de DNS dans le cadre du lancement du nouveau Centre européen de lutte contre la cybercriminalité (EC3).

En janvier 2013, l'équipe de la sécurité de l'ICANN a publié un document de réflexion intitulé « l'importance d'évaluer les dommages collatéraux avant de demander la saisie d'un domaine », http://blog.icann.org/2013/01/the-value-of-assessing-collateral-damage-before-

requesting-a-domain-seizure/. Il s'agit de la suite du document de réflexion publié en mars 2012 sur les saisies et les suspensions de domaine, http://blog.icann.org/2012/03/thought-paper-on-domain-seizures-and-takedowns/. Ces documents sont en rapport avec le SAC 056, « Rapport consultatif du SSAC sur les impacts du blocage de contenus par le système de noms de domaine », http://www.icann.org/en/groups/ssac/documents/sac-056-en.pdf, publié en octobre 2012.

L'ICANN a suivi le développement de la stratégie de l'Union Européenne sur la cyber sécurité (janvier 2013), http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security et le décret présidentiel des États-Unis sur le renforcement de la lutte contre la cybercriminalité (février 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0. Les deux documents témoignent de l'intérêt croissant porté sur l'établissement de mécanismes de partage d'information et de collaboration pour répondre aux menaces qui pèsent sur la cyber sécurité.

Parmi les événements mondiaux saillants qui ont eu lieu dans le domaine d'Internet avant la publication du présent document, on retrouve :

- APRICOT 2013 (Conférence Internet régionale d'Asie-Pacifique sur les technologies opérationnelles), à Singapour, 19 février – 1er mars 2013, http://www.apricot2013.net/.
- SMSI+10, Vers des sociétés du savoir pour la paix et le développement durable (organisée par l'UNESCO), à Paris, 25-27 février 2013, http://www.unesco.org/new/en/communication-and-information/flagship-project-activities/wsis-10-review-event-25-27-february-2013/.
- La réunion des parties prenantes arabes sur la gouvernance d'Internet à Dubaï, la réunion des parties prenantes africaines et les parties prenantes des EAU sur la gouvernance d'internet à Addis Ababa, Ethiopie, http://www.icann.org/en/news/announcements/announcement-07feb13-en.htm.
- L'IETF 86, à Orlando, Floride, du 10 au 15 mars 2013, http://www.ietf.org/meeting/86/index.html.

Activités pour l'exercice fiscal 2014

Pour l'exercice fiscal 2014, les activités de l'ICANN visant à soutenir un écosystème sain, stable et résilient se focaliseront sur les domaines suivants :

- Soutenir l'excellence opérationnelle dans les activités menées par l'IANA, l'IT et les opérations DNS
- Assurer la collaboration technique (grâce à l'expertise dans des domaines précis et le leadership éclairé assurer la participation de la communauté, la mise en place d'activités de formation et de renforcement de capacités en matière de DNS avec des partenaires lorsque cela est demandé).

- Encourager l'adoption et la connaissance du DNSSEC par les entreprises, les utilisateurs et les opérateurs.
- Mettre en œuvre les recommandations de l'équipe de révision SSR
- Soutenir l'accroissement de la capacité de la racine-L, la publication de données et de mesures par l'équipe d'opérations du DNS de l'ICANN
- Élaborer un Cadre de gestion de risques du DNS et finaliser un cycle d'évaluation.
- Accroître l'expertise de l'ICANN en matière de gestion des risques d'entreprise afin de mieux soutenir le Comité des risques du Conseil d'administration et de mieux répondre à l'évolution des besoins de l'ICANN dans le domaine de la gestion des risques organisationnels.
- Soutenir l'établissement de nouveaux bureaux de liaison à Singapour et à Istanbul et élargir les capacités de l'équipe de sécurité dans ces sites afin de mieux servir la communauté.
- Agir en tant que spécialistes pour l'équipe de l'engagement des parties prenantes mondiales dans les discussions sur la gouvernance d'Internet et la cyber sécurité, en représentant l'ICANN dans des conférences et des réunions.
- Faciliter et encourager la participation dans l'ICANN des organismes d'application de la loi et de la communauté de la sécurité opérationnelle.
- Engager le dialogue avec la société civile sur les problèmes liés à la confidentialité et à la liberté d'expression, dans la mesure où ils ont trait à la sécurité des identifiants uniques et à la santé de l'écosystème d'Internet (en renforçant les activités de sensibilisation et la participation des membres de l'écosystème aux questions relatives à la SSR).
- Renforcer les réseaux internes de l'ICANN, les processus IT et la sécurité de l'information.
- Collaborer avec la communauté technique, les opérateurs des serveurs racine, les développeurs d'applications et de navigateurs sur toute question liée au DNS.
- Soutenir les équipes chargées de la politique de l'ICANN et des relations avec les parties prenantes lorsque cela sera nécessaire (SSAC, RSSAC et problèmes liés à la SSR lorsqu'ils sont discutés dans les SO et les AC).
- Contribuer au succès des réunions de l'ICANN à Durban, à Buenos Aires, à Singapour et à Londres.

Pour accomplir ces tâches, l'ICANN doit faire évoluer son équipe de sécurité pendant l'exercice fiscal 2014 avec des expertises et des compétences supplémentaires. Il s'agit d'une action incontournable pour répondre aux besoins de la communauté et de la structure matricielle mise en œuvre pendant cet exercice fiscal. Des explications à l'appui des activités SSR prévues pour l'année fiscale 2014 seront fournies dans le plan opérationnel et le budget de l'exercice fiscal 2014, qui seront publiés après la réunion de l'ICANN à Beijing. Cette action fait suite aux orientations fournies dans les recommandations 20 et 21 en matière de SSR, où il est demandé à l'ICANN d'accroître la transparence des informations sur l'organisation et le budget liés au

Cadre SSR et de prévoir des processus plus structurés pour montrer la relation entre les décisions budgétaires et organisationnelles et le Cadre SSR.

Annexes

Annexe A – Suivi des recommandations de l'équipe de révision SSR (SSR RT)

Cette section fournit des détails sur les approches utilisées pour la mise en œuvre des 28 recommandations de l'équipe de révision SSR, conformément aux 4 domaines de gestion établis.

Affirmation de l'objectif – Attributions et mission de l'ICANN

Recommandation SSR RT	Mise en œuvre et État
Nº 1 - L'ICANN devrait publier une déclaration unique, claire et cohérente concernant ses attributions et sa mission technique limitée en matière de SSR.	Une consultation publique a été lancée sur une version préliminaire de la déclaration entre mai et septembre 2012 [lien : http://www.icann.org/en/news/public-comment/draft-ssr-role-remit-17may12-en.htm]. La version préliminaire de la déclaration a été révisée le 4 octobre 2012 [http://toronto45.icann.org/meetings/toronto2012/presentation-draft-ssr-role-remit-04oct2012-en.pdf]. Une version mise à jour est incluse dans le Cadre SSR de l'exercice fiscal 2014.
Nº 2- La définition et la mise en œuvre des attributions de l'ICANN et de sa mission technique limitée en matière de SSR devraient être révisées afin de garder le consensus et obtenir l'avis de la communauté.	La déclaration mise à jour sur le rôle et les attributions sera révisée par la prochaine équipe de révision SSR en 2015.
Nº 24 - L'ICANN doit définir clairement la charte, les rôles et les responsabilités de l'équipe du service de sécurité.	**Réalisé,** avec mise à jour de la page de l'équipe de sécurité [lien : https://www.icann.org/security] le 4 octobre 2012 et publication du Cadre SSR de l'année fiscale 2013. La description des rôles et des responsabilités sera encore peaufinée suite à la mise en œuvre de la nouvelle structure de gestion en 2013.
Nº 18 - L'ICANN devrait mener une révision opérationnelle annuelle de ses progrès dans la mise en place du cadre SSR et inclure cette évaluation dans le cadre SSR de l'année suivante.	**Réalisé** dans le Cadre SSR de l'exercice fiscale 2013 et répété avec une fréquence annuelle. Un suivi du progrès sera incorporé par le biais d'un nouveau tableau de bord dans la page de l'équipe de sécurité sur le site Web de l'ICANN.

Excellence dans les opérations - Objectifs

Recommandation SSR RT	Mise en œuvre et État
Nº 7- Sur la base de son cadre SSR actuel, l'ICANN devrait établir un ensemble clair d'objectifs, et conformément à ceux-ci établir les priorités pour ses initiatives et ses activités.	La nouvelle structure de gestion sera utilisée pour harmoniser les objectifs et les initiatives de l'ICANN avec le Cadre SSR annuel, et pour orienter l'élaboration du budget, du plan opérationnel et du prochain plan stratégique de l'ICANN pour l'exercice fiscal 2014. L'ICANN travaille pour aligner ses objectifs et ses activités avec cette structure.

Nº 8 - L'ICANN devrait continuer à peaufiner les objectifs de son plan stratégique, notamment l'objectif de maintenir et de gérer la disponibilité du DNS. Alignement clair entre le Cadre et le plan stratégique.	Ce point est lié au prochain plan stratégique. Une harmonisation des objectifs et des activités du plan stratégique avec le Cadre SSR et les recommandations de l'équipe de révision SSR s'avère nécessaire.

Excellence dans les opérations - Transparence

Recommandation SSR RT	Mise en œuvre et État
Nº 17 - L'ICANN devrait élaborer un processus interne plus structuré permettant de mieux comprendre le rapport existant entre certaines activités et initiatives et les buts, objectifs et priorités spécifiques du cadre SSR.	La structure de gestion a été utile pour appliquer cette recommandation et créer un mécanisme au niveau des processus internes capable de montrer le rapport existant entre certaines activités et initiatives SSR et les buts, les objectifs et les priorités de l'ICANN. Des informations supplémentaires sur ce processus seront disponibles pour la communauté sur MyICANN et sur la page Web de l'ICANN entre la conférence de Beijing et celle de Durban en 2013.
Nº 20 - L'ICANN devrait accroître la transparence des informations concernant l'organisation et le budget lié à la mise en place du cadre SSR et aux fonctions en matière de SSR.	Cette recommandation sera mise en œuvre dans le Cadre SSR et le processus d'élaboration du plan opérationnel et du budget de l'exercice fiscal 2014. Le nouveau tableau de bord incorporé à la page de l'équipe de sécurité sera aussi utilisé pour appliquer cette recommandation.

Excellence dans les opérations - Structure

Recommandation SSR RT	Mise en œuvre et État
Nº 21 - L'ICANN devrait élaborer un processus interne plus structuré permettant de mieux montrer le rapport existant entre le cadre SSR et certaines décisions concernant l'organisation et le budget, y compris l'analyse coût/bénéfice sous-jacente.	L'ICANN se servira du processus utilisé pour parvenir à la nouvelle structure de gestion pour identifier les décisions budgétaires et organisationnelles et les aligner avec les activités SSR du Cadre annuel. Cette action sera mise en œuvre dans le Plan opérationnel et le budget de l'exercice fiscal 2014.

Excellence des opérations – Standards et conformité

Recommandation SSR RT	Mise en œuvre et État
Nº 9 - L'ICANN devrait évaluer les options de certification sous les standards internationaux normalement acceptés (par ex. ITIL, ISO et SAS-70) pour ses responsabilités opérationnelles. L'ICANN devrait publier une feuille	La mise en place du DNSSEC dans la racine a obtenu la certification SysTrust [lien : https://www.iana.org/dnssec/systrust et https://cert.webtrust.org/icann.html]. D'autres processus de certification sont menés par les équipes de l'ICANN chargées de la fonction IANA, des IT et des opérations DNS, avec le soutien de l'équipe de la sécurité.

de route claire vers la certification.	
Nº 10 - L'ICANN devrait poursuivre ses efforts visant à assurer le respect de la conformité contractuelle et fournir des ressources adéquates pour remplir cette fonction. L'ICANN devrait également élaborer et mettre en place un processus plus structuré de suivi des dossiers et des recherches en matière de conformité.	La mise en œuvre de cette recommandation est actuellement prise en charge par l'équipe de l'ICANN chargée de la conformité à travers l'application des recommandations de l'équipe de révision du WHOIS.

Excellence dans les opérations - nTLD

Recommandation SSR RT	Mise en œuvre et État
Nº 11 - L'ICANN devrait établir et mettre en place des actions visant à mesurer le succès des nouveaux gTLD et des procédures accélérées IDN qui soient expressément en rapport avec les objectifs en matière de SSR, y compris des mesures de l'efficacité des mécanismes destinés à réduire l'utilisation frauduleuse des noms de domaine.	Le personnel examine toutes les implications de cette recommandation. L'équipe de la sécurité aura besoin de la collaboration de la communauté et du personnel pour la mise en œuvre complète de cette recommandation. La participation des parties prenantes de la communauté sera nécessaire dans la mesure où cette recommandation concerne la révision de la concurrence, la confiance du consommateur et le choix du consommateur, ainsi que les mesures des nouveaux gTLD et des ccTLD IDN délégués via la procédure accélérée ccTLD IDN. Cette recommandation se focalise sur des mécanismes liés à l'atténuation de l'utilisation malveillante des noms de domaine. Le personnel soutient les efforts des comités consultatifs et de la communauté en matière d'indicateurs pour mesurer les abus.
Nº 22- L'ICANN devrait publier, surveiller et mettre à jour la documentation sur les ressources organisationnelles et budgétaires nécessaires pour gérer les aspects liés à la sécurité, la stabilité et la résilience conjointement avec l'introduction des nouveaux gTLD.	Ces aspects sont liés à la recommandation nº 21 (décisions budgétaires et organisationnelles) ainsi qu'au développement d'une surveillance suite à l'introduction des nouveaux gTLD.

Excellence des opérations - Gestion des risques et Atténuation des menaces

Recommandation SSR RT	Mise en œuvre et État
Nº 25 - L'ICANN devrait mettre en place des mécanismes permettant d'identifier à la fois les risques à court terme et à long terme ainsi que des facteurs stratégiques dans son cadre de gestion des risques.	En cours de réalisation et dépendant de l'élaboration d'un cadre de gestion de risques conformément à la recommandation 26.
Nº 26 - L'ICANN devrait considérer	En cours de réalisation. L'ICANN a eu recours à *Westlake*

comme prioritaire l'achèvement dans les délais du travail d'élaboration d'un cadre de gestion des risques.	*Governance* pour l'aider dans son projet de cadre sur la gestion de risques du DNS. Westlake a mené une séance ouverte à Toronto, fournira une version préliminaire de cadre dans un futur proche et fera une brève présentation du concept du cadre à l'occasion de la réunion de l'ICANN à Beijing.
Nº 27 - Le cadre de gestion des risques de l'ICANN doit être exhaustif tout en respectant le champ d'application de ses attributions et de sa mission technique limitée en matière de SSR.	Le Cadre de gestion des risques sera aligné avec les activités de l'ICANN destinées à soutenir sa mission technique et la communauté. Il s'agira d'un travail exhaustif dans cette perspective, qui sera réalisé avec la mise en œuvre du Cadre prévu dans la recommandation 26.
Nº 15 - L'ICANN devrait agir en tant que facilitateur pour la divulgation et la diffusion des menaces à la sécurité du DNS et des techniques de réduction des risques.	La version préliminaire d'un document d'information coordonné est en cours d'élaboration par l'équipe de sécurité de l'ICANN. Le personnel collabore avec les opérateurs et les entités communautaires de confiance chargées de la sécurité pour identifier les menaces à la sécurité du DNS et mettre en place des techniques d'atténuation. Ces aspects sont lies à la recommandation 28.
Nº 28 - L'ICANN devrait poursuivre sa participation active dans la détection et la réduction de risques, ainsi que dans les efforts de communication visant à diffuser des informations liées aux menaces et aux incidents.	Cette recommandation soutient la poursuite des efforts de l'ICANN, y compris la surveillance de la zone racine, l'identification et l'atténuation de menaces liées aux opérations DNS de l'ICANN et de manière générale, aux menaces et aux incidents portant sur le DNS.

Internationalisation – Terminologie et relations

Recommandation SSR RT	Mise en œuvre et État
Nº 3 - Après avoir publié une déclaration consensuelle sur ses attributions et sa mission technique limitée en matière de SSR, l'ICANN devrait utiliser une terminologie cohérente et inclure des descriptions de cette déclaration dans tous ses documents.	L'équipe de sécurité travaillera au sein de l'organisation afin d'utiliser dans les documents de l'ICANN une terminologie cohérente, avec des descriptions du rôle et des attributions de l'ICANN en matière de SSR. Une première étape consiste à mettre un place une formation auprès du personnel de l'ICANN, suivie d'un séminaire Web pour permettre la participation de la communauté. Nous utiliserons aussi cette terminologie et ces descriptions pour les présentations et les engagements de l'ICANN.
Nº 4- L'ICANN devrait documenter et définir clairement la nature des relations en matière de SSR au sein de sa communauté afin de fournir une référence qui puisse contribuer à une meilleure compréhension des interdépendances entre les	Un travail est en cours pour documenter et définir ces relations. La visualisation des fonctions de sécurité de l'ICANN sera utilisée pour cartographier les relations entre les fonctions de coordination et de collaboration, l'identification de menaces et les domaines de collaboration technique.

organisations.	
Nº 5 - L'ICANN devrait utiliser la définition de ses relations en matière de sécurité, stabilité et résilience afin de maintenir des arrangements de travail efficaces et de démontrer la manière dont ces relations sont utilisées pour atteindre chacun des objectifs en matière de SSR.	L'équipe de sécurité travaillera avec l'équipe de l'engagement des parties prenantes mondiales de l'ICANN pour maintenir et améliorer l'efficacité des relations et des arrangements de travail. L'équipe de sécurité a établi des relations avec la communauté d'application de la loi et la communauté chargée de la sécurité opérationnelle au niveau mondial, et a assuré des formations en République Tchèque, en France, aux Pays Bas, au Royaume-Uni, aux États-Unis, entre autres.

Internationalisation – Sensibilisation et engagement

Recommandation SSR RT	Mise en œuvre et État
Nº 14 - L'ICANN devrait veiller à ce que ses activités de communication en matière de SSR ne cessent d'évoluer afin qu'elles restent à tout moment opportunes, pertinentes et appropriées.	Les activités de sensibilisation ont été élargies et seront révisées annuellement. L'équipe de sécurité remplit une fonction de service expert auprès de l'équipe des parties prenantes mondiales et une fonction communautaire, par le biais des activités de sensibilisation et de collaboration en matière de SSR.
Nº 16 - L'ICANN devrait poursuivre ses efforts de communication afin d'accroître la participation de la communauté au processus de développement du cadre SSR. L'ICANN devrait également établir un processus pour obtenir des avis plus systématiques d'autres membres de l'écosystème.	Les activités de sensibilisation et les processus ont été élargis et seront révisés annuellement. Le travail permanent accompli par l'équipe de sécurité auprès des communautés chargées de la sécurité telles que APWG, MAAWG, a encouragé la participation au SSAC des membres de ces communautés. La participation de l'équipe de sécurité à l'ICLN et à la CCI met l'accent sur l'importance des approches multipartites pour faire face aux problèmes liés à la cyber sécurité. Ces aspects sont liés aux recommandations 4, 5 et 14. L'équipe de sécurité soutient un éventail d'initiatives de renforcement de capacités à la demande des parties prenantes, parmi lesquelles on retrouve des formations en matière de DNSSEC, des formations concernant la réponse aux attaques et incidents pour les ccTLD, des formations dans le domaine de l'application de la loi, ainsi que des activités de sensibilisation dans des réunions de groupes d'opérateurs de réseau telles que CaribNOG et MENOG, entre autres.

Evolution du modèle multipartite

Recommandation SSR RT	Mise en œuvre et État
Nº 6 - L'ICANN devrait publier un document où soient clairement établis les rôles et les responsabilités du SSAC et du RSSAC afin de bien encadrer les	Cette recommandation nécessitera la collaboration de la communauté et du personnel. Pour faciliter le suivi de la mise en œuvre de cette recommandation, elle a été divisée en deux : 6A [SSAC] et 6B [RSSAC].

activités des deux groupes.	6A – Les rôles et les responsabilités du SSAC sont définis dans ses procédures opérationnelles. Le SSAC mène un travail de révision de ses procédures opérationnelles pour l'année 2013 et est intéressé à aligner ces rôles et ses responsabilités avec ceux et celles du RSSAC. 6B – Les rôles et les responsabilités du RSSAC sont en cours de développement, suite à la fin de la consultation publique sur les amendements proposés aux statuts de l'ICANN concernant les objectifs du RSSAC. Voir http://www.icann.org/en/news/public-comment/bylaws-03jan13-en.htm.
Nº 12 - L'ICANN devrait travailler avec la communauté afin d'identifier les meilleures pratiques en matière de SSR et de donner son soutien à ces pratiques par le biais de contrats, d'accords, de protocoles d'accord (*MOU*) et d'autres mécanismes.	La mise en œuvre de la recommandation 12 impliquera la collaboration de la communauté et du personnel. Des discussions supplémentaires à ce propos auront lieu à l'occasion de la conférence de l'ICANN à Beijing dans un panel d'experts sur la sécurité DNS et avec le groupe de travail technique de la ccNSO sur les meilleures pratiques non contractuelles. L'équipe de sécurité a travaillé avec le groupe de travail anti-hameçonnage (APWG) du Comité sur les politiques d'Internet sur la protection des applications Web et a participé au développement de ressources destinées à renforcer la prise de conscience en matière de sécurité (à travers les activités de SANS Securethehuman.org et NCA Stop.Think.Connect). La consultation publique actuelle sur les accords de registre révisés pour les nouveaux gTLD (voir http://www.icann.org/en/news/public-comment/base-agreement-05feb13-en.htm) apporte des informations supplémentaires sur les meilleures pratiques.
Nº 13 - L'ICANN devrait encourager toutes les organisations de soutien à élaborer et à publier des meilleures pratiques en matière de SSR pour leurs membres.	Cette recommandation demandera la collaboration de la communauté et du personnel à travers l'ASO, la ccNSO et la GNSO dans leurs rôles respectifs, afin d'identifier les meilleures pratiques liées aux identifiants uniques.
Nº 19 - L'ICANN devrait élaborer un processus permettant à la communauté de faire un suivi de la mise en place du cadre SSR. L'information fournie devrait être suffisamment claire pour permettre à la communauté de suivre l'exécution des responsabilités de l'ICANN en matière de SSR.	L'équipe de sécurité publiera prochainement un tableau de bord sur sa page Web afin de montrer le suivi du Cadre SSR et des initiatives de l'ICANN en matière de SSR.
Nº 23 - L'ICANN doit fournir des ressources appropriées aux	Le personnel travaille à l'établissement d'un inventaire [23A] des activités en matière de SSR des groupes de travail et des comités

groupes de travail et comités consultatifs travaillant sur des questions liées à la sécurité, la stabilité et la résilience, cohérentes avec les exigences qui leur sont imposées. L'ICANN doit également veiller à ce que les décisions issues des groupes de travail et des comités consultatifs aient été prises de façon objective et n'aient pas été influencées par des pressions internes ou externes.	consultatifs existants (SSAC et RSSAC). Cet inventaire sera suivi de la description ou de la documentation des processus budgétaires pour qu'ils soient commentés par les SO/AC [23B]. Le point 23C décrit la démarche d'un processus opérationnel standard afin de montrer que les décisions des groupes de travail / SO/ AC sont prises de manière objective.

SSR RT Recommendations Tracking – February 2013

Recommendation	FY 13 T1	T2	T3	FY 14 T1	T2	T3	FY 15 T1	T2	T3
Rec 1 – Clear statement of ICANN's SSR role and remit	Published	Revise	Update						
Rec 2 – Role & remit review in 2015								Review	Publish
Rec 3 – Use consistent terminology	Develop	Ongoing							
Rec 4 – Document & define SSR relationships		Develop	Publish						
Rec 5 – Use SSR relationships for effective working	Ongoing	Ongoing	Ongoing						
Rec 6 – Roles for SSAC (6A) & RSSAC (6B)		Publish							
Rec 7 – Build from SSR Framework, clear objectives & priorities	Develop	Publish	Expected Complete	Reporting					
Rec 8 - Strategic Plan & SSR Framework alignment		Publish	Refine						
Rec 9 – Assess certification options, publish roadmap		Develop	Publish						
Rec 10 – Process for monitoring compliance & investigations (see Whois RT Implementation)		Whois RT Recs							
Rec 11 – Measures for success in nTLD & IDN FT re SSR			Develop	Publish			AoC CCR		
Rec 12 – w/Community, SSR-related best practices	Engage	Discuss							
Rec 13 – Encourage SOs/SGs to develop & publish SSR-related best practices			Expected Complete						
Rec 14 – Evolving SSR outreach		Publish	ongoing	ongoing	review	publish	ongoing	ongoing	
Rec 15 – Facilitate responsible disclosure of threats		Draft	Ongoing	X					
Rec 16 – Outreach w community; process for input		Publish	ongoing	ongoing	review	publish	ongoing	ongoing	
Rec 17 – Mapping activities to SSR Framework		Publish	X	Reporting					
Rec 18 (Implemented w FY 13 SSR Framework) – Annual review of SSR Framework	Complete								
Rec 19 – Dashboard for SSR Framework			Publish	Reporting					
Rec 20 – Transparency on SSR budget			Publish	ongoing					
Rec 21 – Show how budget & op decisions relate to SSR			Publish						
Rec 22 – Documenting mgmt. of SSR issues with operational readiness from introduction of nTLDs		Develop	Publish						
Rec 23 – Appropriate resources for SSR-related WGs & ACs		FY 14 Budget	Budget approx						
Rec 24 (Implemented w FY 13 SSR Framework) – Define Security team roles	Complete								
Rec 25 – DNS Risk Management Framework	Consultant	Draft	Publish	Assess	work	work	Review		
Rec 26 – Prioritizing completion of DNS RMF		Publish	Approv						
Rec 27 – DNS RMF covers IANA, L-root, other functions				Assess	work	work	Review		
Rec 28 – Active engagement in threat detection & mitigation	Underway	X							

Schéma 8 – Suivi des recommandations de l'équipe de révision SSR (SSR RT)

Annexe B – Rapport sur l'état des lieux de l'exercice fiscal 2013.

Domaine général	Programme / Initiative	Situation
Engagement en matière de sécurité mondiale	Collaboration avec la communauté au sens large, le secteur commercial, la communauté universitaire, la communauté technique et les organismes d'application de la loi sur les problèmes en matière de sécurité du DNS.	Participation au 4ème Symposium mondial sur la sécurité, la stabilité et la résilience du DNS, en partenariat avec l'APWG à eCOS, Puerto Rico, en octobre 2012.
		Participation aux ateliers de travail de l'Initiative du Commonwealth sur la cybercriminalité (CCI) à l'occasion des conférences de l'ICANN au Costa Rica et à Prague, ainsi qu'aux réunions de l'EMG et du groupe de pilotage de la CCI.
		BlackHat/Defcon en juillet 2012
		Forum de gouvernance d'Internet et événements régionaux de l'IGF
		Présentation faite au regroupement commercial (BC) à Washington DC et participation à l'élaboration du bulletin d'information du BC pour ICANN Toronto.
Collaboration	Soutien supplémentaire aux mesures du DNS et aux outils et indicateurs tels qu'ATLAS, du RIPE NCC	Soutien au RIPE NCC pour le déploiement supplémentaire de nœuds ATLAS et pour l'analyse de données. https://atlas.ripe.net/
	Automatisation de la zone racine	Le système de gestion de la zone racine (RZM) utilisé par IANA avec NTIA et Verisign a fêté sa première année de vie en août 2012 (voir http://blog.icann.org/2012/08/rzm-is-one-year-old/). L'équipe IANA travaille sur des processus supplémentaires de sécurisation, tels que le système de notification sécurisée. Voir http://www.icann.org/en/news/public-comment/iana-secure-notification-12dec12-en.htm.
	Formations techniques auprès des communautés d'application de la loi et des communautés chargées de la sécurité opérationnelle.	L'équipe de sécurité a accueilli les représentants de l'application de la loi à l'occasion de la conférence de l'ICANN à Prague et à Toronto. Elle a aussi assuré des formations en matière de DNS à Europol aux Pays Bas, et à SOCA, OFT et la police métropolitaine au Royaume-Uni.
	Sécurité et Stabilité Comité consultatif	Collaboration avec le SSAC dans le cadre des ateliers de travail sur le DNSSEC organisés lors des conférences de l'ICANN, participation à des groupes de travail et aux rapports consultatifs du SSAC. Le travail du SSAC a été important pendant l'exercice fiscal 2013.

	Soutien au groupe de travail sur la sécurité et la stabilité du DNS	Le DSSA a finalisé l'étape 1 de son rapport en août 2012. http://www.icann.org/en/news/public-comment/dssa-phase-1-report-14aug12-en.htm. Le DSSA se réunira à nouveau lors de la conférence de l'ICANN à Beijing. L'ICANN a également fait appel à Westlake Governance pour l'élaboration du cadre de gestions de risques du DNS.
	Évolution technique du Whois	L'ICANN a annoncé la création d'un groupe d'experts sur les services d'annuaire des gTLD en février 2013 (https://www.icann.org/en/news/announcements/announcement-14feb13-en.htm). En octobre 2012, l'ICANN a annoncé son partenariat avec CNNIC pour mettre en place un serveur Whois RESTful « open-source », http://blog.icann.org/2012/10/cnnic-selected-to-implement-an-open-source-restful-whois-server/.
	Développement de politiques – enregistrement frauduleux ; accords d'accréditation des bureaux d'enregistrement	L'ICANN a lancé une consultation publique à propos du rapport préliminaire sur l'uniformité des rapports, https://www.icann.org/en/news/public-comment/uofr-20feb13-en.htm. Ce rapport faisait suite à l'initiative lancée par le Conseil de la GNSO en réponse au travail accompli par le groupe de travail sur les politiques en matière d'enregistrement frauduleux. En ce qui concerne les accords d'accréditation des bureaux d'enregistrement, les négociations se poursuivent. Le PDG Fadi Chehadé a fait un point sur cette question le 7 Février 2013, http://blog.icann.org/2013/02/registrar-accreditation-agreement-negotiation-session/.
	Groupe de travail du SSAC sur le roulement de clés du DNSSEC	Le groupe de travail du SSAC sur le roulement des clés de la racine poursuit ses activités en 2013. Des informations supplémentaires seront disponibles lors de la conférence de l'ICANN à Beijing. Des cérémonies de clé réussies ont eu lieu à Culpeper, en Virginie, et à El Segundo, en Californie.
	DNSSEC – audit SysTrust	La certification SysTrust du DNSSEC est disponible sur : https://www.iana.org/dnssec/systrust.
	Formation en matière de DNSSEC auprès de la communauté	L'ICANN a participé à des formations en matière de DNSSEC en Colombie, au Pérou, au Paraguay, à Hong Kong, au Chili et en prévoit d'autres au Liban (mars 2013) et en Tunisie (avril 2013).
	Résilience de la racine-L	L'ICANN a soutenu la croissance et la distribution d'instances de la racine-L dans tout le monde. En particulier, des partenariats ont été annoncés pour fournir des instances de la racine-L en Afrique, avec AfriNIC, en Amérique Latine et les Caraïbes avec LACNIC, au Brésil avec CGI.Br, en Corée avec KISA, et ailleurs.
Programmes de sécurité d'entreprise	Améliorer les processus et la sécurité des réseaux internes à l'ICANN	L'équipe de sécurité a travaillé avec l'équipe IT de l'ICANN afin de renforcer les réseaux internes de l'ICANN. L'équipe a assuré une formation SANS pour tout le personnel IT et des formations de base en matière de sécurité pour le personnel de l'ICANN à Los Angeles et à Bruxelles.
	Améliorer la continuité du business et mettre en place des exercices en interne.	L'équipe de sécurité a soutenu des exercices portant sur la résilience de la racine et les processus de communication internes.

	Sécurité des réunions - évaluation de risques, sécurité des voyageurs	Mise en place d'évaluations sur les sites où auront lieu les conférences de l'ICANN ; mise à disposition de services de santé et d'urgences de terrain lors des conférences de l'ICANN (ISOS).
Activités inter organisations	Soutien aux opérations des nouveaux gTLD	Soutien à l'équipe des nouveaux gTLD pour le tirage au sort destiné à établir les priorités ainsi que pour les processus de révision.
		Soutien à la révision du système de vérification pré-délégation avec .SE, http://www.icann.org/en/news/announcements/announcement-21dec12-en.htm.
	Conformité contractuelle	L'équipe chargée de la conformité a poursuivi sa croissance en 2013 et a publié son plan d'audit (Voir http://www.icann.org/en/resources/compliance/audits)
	Programme IDN	Participation aux réunions du GENUNG et de l'UNCSGN à New York en juillet et août 2012 au siège des Nations Unies, et soutien au travail continu du programme sur les variantes d'IDN.
	Gestions des risques d'entreprises	L'ICANN a fait appel à Westlake Governance pour élaborer le cadre de gestion de risques du DNS. Des nouvelles par rapport aux progrès de Westlake seront communiquées lors de la conférence de l'ICANN à Beijing.

Le travail accompli par l'équipe de sécurité de l'ICANN dans le domaine technique est de nature collaborative. Il s'agit d'une tâche que nous menons à bien au service de la communauté dans son ensemble. Si nous apprécions fortement les lettres de soutien que nous avons reçues, il faut préciser que les félicitations et les déclarations de reconnaissance ne sont pas le but recherché par notre travail. Les lettres ci-après sont un exemple du soutien dont a bénéficié l'ICANN au cours de l'exercice fiscal 2013 pour son engagement en matière de sécurité auprès de la communauté.

COMNET
Foundation for ICT Development

www.comnet.org.mt

ICANN Security Team

12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536
USA

2nd July 2012

Re: Commonwealth Cybercrime Initiative

Dear ICANN Security Team,

We would like to express our gratitude and thanks for providing the Commonwealth Cybercrime Initiative the opportunity to host another workshop at the ICANN Meeting in Prague. The Event in Costa Rica was a big success and to follow with another space in Prague was excellent as it provided continuity. We sincerely appreciate the time and resources that ICANN has invested to provide a platform for the Initiative to raise its profile amongst the ICANN community.

Our Prague workshop resulted in two expressions of interest in the CCI from two governments in Africa and we also had excellent additions to our expert resource repository. We are already working on translating these expressions of interest into meaningful activity on the ground.

We are especially grateful of Mr Dave Piscitello's contributions in his capacity as ICANN representative on the CCI Steering Group. Mr Piscitello's involvement, in a very short time resulted in very tangible achievements for the Initiative.

ICANN's support of the Commonwealth Cybercrime Initiative has proven invaluable and we look forward to the opportunity to present the CCI at the next ICANN meeting in Canada if scheduling allows.

Thank you once again, and we look forward to our continued collaboration.

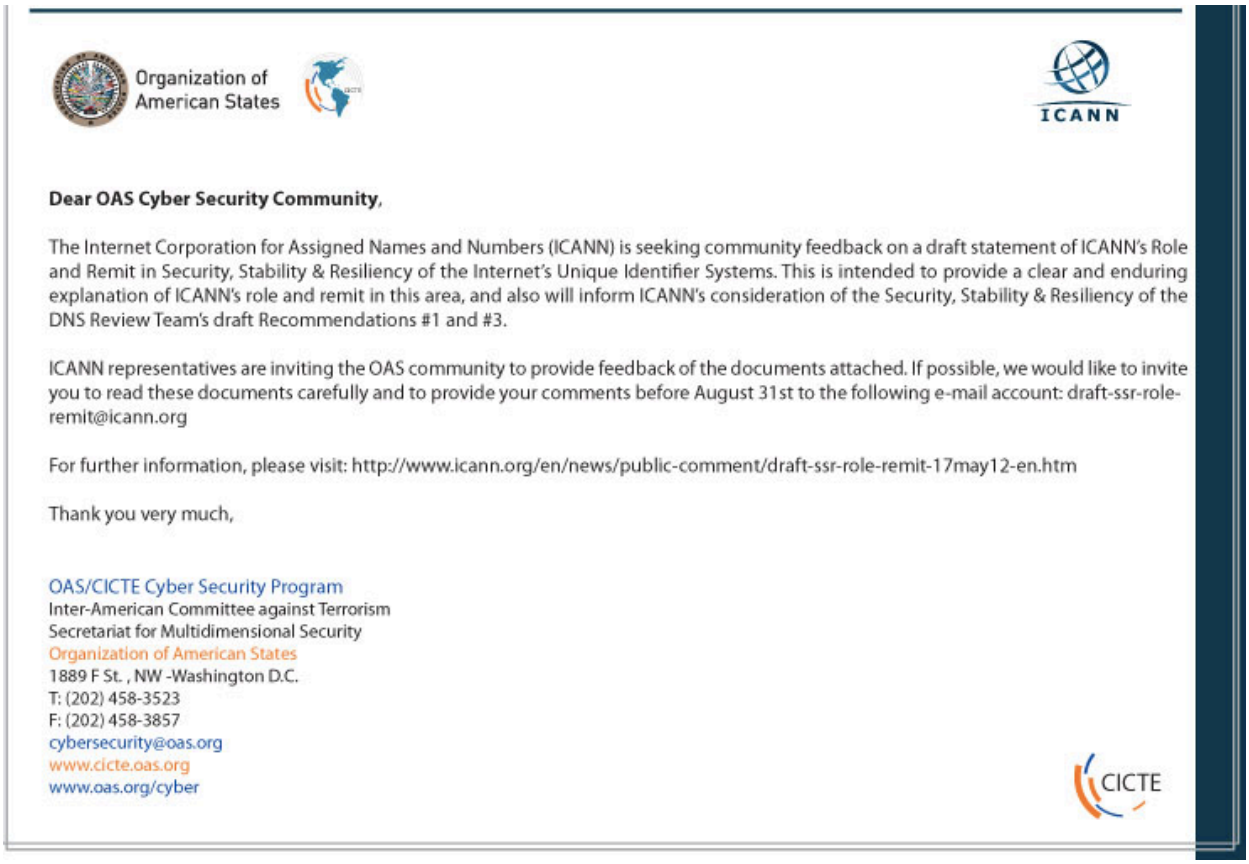
Yours,

Joseph V. Tabone

Chairman CCI Secretariat

Alfir, Reggie Miller Street, Gzira, GZR 1541, Malta | t: (356) 2132 3393 | f: (356) 2132 3390 | e: info@comnet.org.mt

Annexe C – Lettre adressée à l'ICANN par COMNET



Organization of American States

ICANN

Dear OAS Cyber Security Community,

The Internet Corporation for Assigned Names and Numbers (ICANN) is seeking community feedback on a draft statement of ICANN's Role and Remit in Security, Stability & Resiliency of the Internet's Unique Identifier Systems. This is intended to provide a clear and enduring explanation of ICANN's role and remit in this area, and also will inform ICANN's consideration of the Security, Stability & Resiliency of the DNS Review Team's draft Recommendations #1 and #3.

ICANN representatives are inviting the OAS community to provide feedback of the documents attached. If possible, we would like to invite you to read these documents carefully and to provide your comments before August 31st to the following e-mail account: draft-ssr-role-remit@icann.org

For further information, please visit: http://www.icann.org/en/news/public-comment/draft-ssr-role-remit-17may12-en.htm

Thank you very much,

OAS/CICTE Cyber Security Program
Inter-American Committee against Terrorism
Secretariat for Multidimensional Security
Organization of American States
1889 F St. , NW -Washington D.C.
T: (202) 458-3523
F: (202) 458-3857
cybersecurity@oas.org
www.cicte.oas.org
www.oas.org/cyber

CICTE

Annexe D – Avis de consultation publique lancé à la communauté de l'OEA

CARIBBEAN TELECOMMUNICATIONS UNION
3rd Floor, Victoria Park Suites, 14-17 Victoria Square, Port of Spain, Trinidad & Tobago, W.I.
Tel: (868)627 0281/0347 Fax: (868) 623 1623 E-Mail: otunion@otu.int Website: www.otu.int

7th September, 2012

Mr. Patrick Jones
Senior Manager, Security
Internet Corporation for Assigned Names and Numbers (ICANN)
1101 New York Ave
New York Avenue
Washington DC 20005
USA

Dear Mr. Jones,

Expression of Appreciation

On behalf of the Caribbean Telecommunications Union (CTU), I would like to express our sincere appreciation to you for participating in the CTU's 8th Caribbean Internet Governance Forum, which took place from the 29th to 30th August, 2012 at the Bay Gardens Hotel, Castries, St. Lucia.

Thank you for your presentation on "DNSSEC, Collaboration and Training" which was well received by the audience.

I take this opportunity to re-affirm the CTU's commitment to Caribbean ICT development and look forward to an ongoing partnership with ICANN in supporting Caribbean countries as they seek to leverage the power of ICT for social and economic development.

Sincerely,

Bernadette Lewis
SECRETARY GENERAL

Annexe E – Lettre adressée à l'ICANN par l'Union des télécommunications des Caraïbes.

Europol Unclassified – Basic Protection Level

The Hague, 3 January 2013

Ref: 647233

Dr Stephen D. Crocker
Internet Corporation for Assigned Names
and Numbers (ICANN)
12025 Waterfront Drive, Suite 300
Los Angeles CA 90094-2536
USA

Dear Dr Crocker, Dear Steve !

Dave Piscitello of ICANN visited us in The Hague on 12 December. The purpose of this meeting was for Dave to be informed on the development of the new European Cybercrime Centre (EC3), ourselves to be aware of ICANN cooperation with law enforcement and all of us to see how this could specifically work between ICANN and the EC3.

We were all pleased by the constructive dialogue and positive outcomes of the meeting. There appear clear opportunities for the EC3 to play the role of facilitator with ICANN for MS law enforcement, both with respect to their views on internet governance and in training to improve investigative capabilities. We will be in contact with Dave over the specifics concerning this in the coming weeks.

The EC3 is very appreciative of this initiative between our two organisations and hope that you can lend your full support to it. Thank you very much.

Yours sincerely,

Troels Oerting
Assistant Director
Head of European Cybercrime Centre (EC3)

EDOC#647233

Eisenhowerlaan 73
2517 KK The Hague
The Netherlands

P.O. Box 908 50
2509 LW The Hague
The Netherlands

Phone: +31(0)70 302 50 00
Fax: +31(0)70 345 58 96
www.europol.europa.eu

Annexe F – Lettre adressée à l'ICANN par EC3