الخطة المعنية بتحسين أمان واستقرار ومرونة الإنترنت
(العام المالي 2011)

سبتمبر 2010

قائمة المحتويات

ملخص تنفيذي

إن الإنترنت بمثابة نظام بيئي يربط بين العديد من أصحاب المصالح الذين ينتظمون في إطار من التعاون لتعزيز سبل التواصل والابتكار والتجارة ضمن مجتمعات عالمية. ويتوقف تبادل المجالس العمومية العالمية على تشغيل وتنسيق أنظمة معرفات شبكة الإنترنت الفريدة.[1] وتُقر ICANN ومشغلو هذه النظم بأن صون وتعزيز الأمن والاستقرار ومرونة هذه الأنظمة يعد بمثابة عنصر أساسي للعلاقة التعاونية.

ويعتبر هذا المستند تحديثاً لخطة ICANN الخاصة بتحسين أمان الإنترنت والمرونة والاستقرار التي تم الإعلان عنها في 16 مايو 2009 (والمشار إليها فيما بعد بخطة SSR 2009 http://www.icann.org/en/topics/ssr/ssr-draft-plan-16may09-en.pdf). وبالنسبة للعام المالي 2011، فقد تم تحديث خطة SSR بحيث تعكس أنشطة الأمان الخاصة بـ ICANN اعتبارًا من يونيو 2010 إلى يوليو 2011. وسيتم الإشارة إلى التحديثات بالخطة من خطة SSR لعام 2009 بالخط المائل. كما يجري الإعلان عن خطة العام المالي 2011 لـ SSR في الوقت الحالي للتعليق عليها اعتبارًا من أغسطس حتى سبتمبر 2010.

تعلن الخطة الإستراتيجية لـ ICANN من العام 2010 حتى 2013 (http://www.icann.org/en/strategic-plan/strategic-plan-2010-2013-19feb10-en.pdf) بأن "استقرار وأمان نظام اسم النطاق (DNS) له أهمية قصوى بالنسبة لمجتمع ICANN بالإضافة لمستخدمي الإنترنت على مستوى العالم. كما أنهما يشكلان العناصر الرئيسية لمهمة ICANN. وأن إساءة استخدام الهجمات ضد DNS والبنية التحتية الأخرى للإنترنت تزيد بمعدل ثابت. ولضمان الأمان والاستقرار والمرونة الضرورية لـ DNS، يجب على ICANN التعاون مع الجهات الأخرى المعنيين بالنواحي الأوسع لتلك القضايا".

وتتعامل الخطة الإستراتيجية استقرار وأمان DNS باعتبار أنه إحدى النقاط الأربعة الرئيسية التي تركز عليها ICANN. وهذا الأمر يتواءم مع الأهمية العالية المولاة إلى SSR في تأكيد الالتزامات (http://www.icann.org/en/documents/affirmation-of-commitments-30sep09-en.htm) والتي تم تنفيذها في 30 سبتمبر 2009 بين ICANN وإدارة المعلومات والاتصالات الوطنية بالولايات المتحدة الأمريكية (NTIA). وتقسم الخطة الإستراتيجية النطاق العريض لأمان ICANN والاستقرار والمرونة إلى أهداف إستراتيجية وعمل مجتمعي وعمل خاص بفريق العمل.

ويعتبر التشغيل الآمن والمستقر لنظم المعرفات الفريدة للإنترنت جزءًا أساسياً من مهمة ICANN. فمع زيادة تكرار الهجمات والسلوكيات الضارة الأخرى وزيادة تعقيدها، يتعين على ICANN ومجتمعها مواصلة التعاون في تحسين مرونة DNS وتعزيز قدرتها على التعامل مع هذه الأحداث. ونظرًا لطبيعة الهجمات والسلوكيات الضارة التي تتسم بالتوسع، يجب أن تتعاون ICANN مع أصحاب المصالح الآخرين في هذا المجال لتوضيح الدور المنوط بـ ICANN والعثور على حلول للمشكلات التي تعتبر مهمة تفوق قدرات أي كيان فردي.

[1] وفقاً للوائح الداخلية لـ ICANN، تنسق ICANN تخصيص المجموعات الثلاث من المعرفات الفريدة للإنترنت وهي: أسماء النطاقات (تشكيل نظام يشار إليه بـ DNS)؛ وبروتوكول الإنترنت (IP) والعناوين ونظام التسمية (AS) والأرقام ومنفذ البروتوكول وأرقام المعلمات.

الأهداف الإستراتيجية المحددة لأمان واستقرار DNS:

1. *100% من جهوزية DNS.*
2. *إساءة DNS أقل.*
3. *عمليات تشغيل (TLD) أكثر أمانًا.*
4. *مرونة DNS أفضل تجاه الهجمات.*

في 12 فبراير 2010، أعلنت ICANN عن مقترح مبادرات إستراتيجية من شأنها تحسين الأمان والاستقرار والمرونة لـ DNS المعروف بـ (SSR) (http://www.icann.org/en/topics/ssr/strategic-ssr-initiatives-09feb10-en.pdf). ويوضح المقترح المزايا الرئيسية والموقف العقلاني والتكاليف المقترحة لمبادرتين إستراتيجيتين تتعلقان بالأمان والاستقرار لـ DNS.

واستنادًا إلى المقترحات الواردة في فترتي التعليق العامة خلال اجتماع ICANN في نيروبي وأبريل 2010 DNS-CERT للمتطلبات التشغيلية وورش العمل التعاونية واجتماع ICANN في بروكسل، فإن ICANN لا تخطط لتشغيل DNS-CERT بل إن ICANN تواصل المشاركة والتعاون مع أصحاب المصلحة لتحديد المتطلبات التشغيلية للاستجابة الجماعية لـ DNS وإمكانيتها مع اتساع النظام والمخاطر المحيطة به DNS والتقييم وتحليل التهديدات.

دور ICANN

تعمل ICANN بما يتفق مع اللوائح الداخلية لتنفيذ عمليات تضم عددًا من أصحاب المصالح وتقوم على الموافقة الجماعية بالإضافة إلى السياسات والبرامج والتي تشمل العمليات والسياسات والبرامج ذات الصلة بالأمن والاستقرار والمرونة.

- يجب أن يركز دور ICANN على مهامها الرئيسية المرتبطة بنظم المعرفات الفريدة.
- ولا تلعب ICANN دور الشرطي على الإنترنت أو في مكافحة السلوك الإجرامي من الناحية العملية.
- كما لا تلعب ICANN دوراً في استخدام الإنترنت المرتبط بجاسوسية وحرب الإنترنت.
- ولا تلعب ICANN أي دور في تحديد ما يعتبر محتوى غير قانوني على الإنترنت.
- بل إن دور ICANN يتضمن المشاركة في الأنشطة مع مجتمع الإنترنت الأوسع نطاقاً المعنية بمكافحة إساءة استخدام نظم المعرفات الفريدة. وتتضمن هذه الأنشطة التعاون مع الحكومات في مكافحة الأنشطة الضارة التي تحدث من خلال إساءة استخدام النظم سعيًا للمساعدة في حمايتها.

برامج الأمان والاستقرار والمرونة الخاصة بـ ICANN

- تعد ICANN مسئولة عن عمليات هيئة أرقام الإنترنت المُخصصة (IANA). ويعتبر ضمان استمرار التشغيل الآمن والمستقر والمرن لوظيفة منطقة جذر DNS على قمة أولوياتها.
- كما تعد ICANN عنصر تفعيل لنظام اسم النطاق (DNS) وهي تتناول جهود المجتمع المعنية بتعزيز أسس أمن واستقرار ومرونة النظام. وتتضمن هذه

الجهود دعم تطوير وتوزيع البروتوكولات ودعم تقنيات مصادقة أسماء وأرقام الإنترنت.

- كما تعد ICANN عنصر تفعيل وتسهيل لأنشطة تعزيز الأمن والاستقرار والمرونة التي تبذلها سجلات DNS والمسجلين وباقي أعضاء المجتمع.
- وتتحمل ICANN المسئولية عن عملية الأمن والاستقرار والمرونة فيما يخص أصولها والخدمات التي تقدمها.
- كما تعتبر ICANN أحد المشاركين في المنتديات والأنشطة الأوسع نطاقاً المرتبطة بأمن واستقرار ومرونة نظم المعرف الفريدة للإنترنت.

الخطط المعنية بتحسين الأمن والاستقرار والمرونة

خلال العام المالي 2011، تخطط ICANN لتنفيذ البرامج والمبادرات الموضحة هنا. ويستعرض الملحق "أ" تفاصيل خاصة حول أهداف الأنشطة ومساعي الشركاء والالتزامات بالموارد.

- ***عمليات IANA*** – *في 16 يوليو 2010 نفذت ICANN وVeriSign وNTIA عملية DNSSEC لمنطقة الجذر المرخصة. وكان ذلك بمثابة إنجاز كبير لتحسين الأمان والاستقرار بالإنترنت. وسوف تستمر جهود ICANN في العمل مع مجتمع الإنترنت على إزالة العقبات لتبني DNSSEC. وتتضمن المبادرات تحسين إدارة منطقة الجذر من خلال الأتمتة، وتحسين مصادقة الاتصالات مع مديري TLD .*
- ***عمليات تشغيل خادم جذر DNS*** – *سوف تستمر جهود ICANN في تبني تخطيط لحالة الطوارئ وتدريب مع مشغلي الجذر وتحسين مرونة وبنية الجذر L.*
- ***سجلات gTLD*** – ضمان تقييم مقدم الطلب لنطاق المستوى الأعلى الجديد (gTLD) وأسماء النطاق الدولية (IDN) والاستمرار في تقديمه لعمليات تشغيل آمنة. *سوف تستمر ICANN في التنفيذ الحثيث لإجراءات تقييد الاستخدام الضار للإساءة المحتملة التي تنتج عن تأسيس gTLDs الجديدة.* سوف تعمل ICANN على تطوير خطة استمرارية تسجيل gTLD واختبار نظام مستودع البيانات.
- ***سجلات ccTLD*** – نظرًا لأن *ccTLD IDN يتم طرحها من خلال عملية التتبع السريع، فسوف تستمر جهود ICANN في التصدي لمختلف الأمور الإدارية والأمور الأخرى الخاصة بالحد من مشكلات الأمان.*

  سوف تستمر جهود ICANN في جهدها الجماعي مع سجلات نطاق رموز البلدان (ccTLD) من خلال برنامج الهجمة المشتركة وخطط الاستجابة في حالة الطوارئ (ACRP) ودورة عمليات تشغيل السجل (ROC) بما يتوافق مع منظمة دعم أسماء رموز البلدان (ccNSO) واسم النطاق الإقليمي من المستوى الأعلى (TLD) وجمعياته وISOC.
- ***التوافق التعاقدي*** – ستواصل ICANN جهودها الرامية إلى تحسين نطاق أنشطة التنفيذ التعاقدي المشتملة على gTLDs بحيث تتضمن كذلك بدء عمليات تدقيق للأطراف المتعاقدة كجزء من تنفيذ تعديلات مارس 2009 لاتفاقية اعتماد المسجل (RAA) والوقوف على المشاركة المحتملة للأطراف المتعاقدة في النشاط الضار لاتخاذ إجراء للالتزام. وسوف تستمر جهود ICANN في تسهيل اعتبارات السياسة على أنشطة توافقية محسنة كجزء من التعديلات على RAA في العام المالي 2011.

- ***الاستجابة لإساءة الاستخدام الضار لـ DNS*** – سوف تزيد ICANN من جهودها الداعمة مع تسهيل مشاركة المعلومات لتمكين الاستجابة على نحو فعال فيما يخص السلوك الضار الذي يتيحه استخدام DNS.
- ***عمليات الاستمرار والأمان المشترك لـ ICANN*** – *سوف تعمل ICANN على ضمان البرامج الآمنة واتصالها مع المخاطر المشتركة من الإدارة وإدارة الأزمات وبرامج استمرار الأعمال التجارية. وسوف يقع ضمن بؤرة الاهتمام إنشاء أساس قوي من الخطط الموثقة والإجراءات الداعمة. وتتضمن تلك البرامج:*
  - ***خطة الأمان المعلوماتية المشتركة*** – *طورت ICANN خطة الأمان المعلوماتية المشتركة من معايير ISO 27002. وتم تنفيذ تلك الخطة في العام المالي 2011.*
  - ***خطة أمان الاجتماعات*** – *بناء على الجهود الرامية إلى دعم تخطيط الأمان المحسن لاجتماعات ICANN العالمية فسيتم استخدامها في تحديد الموقع والإعداد لاجتماعات ICANN في العام المالي 2011 وما بعده.*
  - ***خطة الأمان الشخصي والبدني*** – *كجزء من الجهود الرامية إلى تحسين الأمان الشخصي والبدني تم وضع خطتين يتم تنفيذها في العام المالي 2011.*
  - ***استمرار الأعمال التجارية وخطة الإدارة في حالة الحوادث*** – *عقدت ICANN تدريب استمرارية IANA في العام 2010 كما ستستمر تلك الجهود في العام المالي 2011 مع التدريب على اتصالات ICANN في حالة الأزمات وتنفيذ استمرار الأعمال التجارية لـ ICANN وخطة الإدارة في حالة الحوادث.*
  - ***برنامج إدارة مخاطر الشركات*** – *نفذت ICANN إرشادات خطة إدارة مخاطر الشركات (ERM) وقامت بتأسيس برنامج ERM في العام المالي 2010. وسوف تستمر ICANN في تحسين هذا البرنامج في العام المالي 2011 مع تقييم المخاطر ودعم لجنة مخاطر مجلس* ICANN.
- ***ضمان التعاون والاشتراك العالمي*** – سوف تستمر ICANN في تحسين التعاون والشراكة مع فريق مهمة هندسة الإنترنت (IETF) ومجتمع الإنترنت (ISOC) وسجلات الإنترنت الإقليمية(RIRs) ومشغلي الشبكة بالمجموعات (NOGs) وعمليات تشغيل DNS–والتحليل والاستجابة (DNS-OARC) ومنتدى *فرق الاستجابة في حالة الحوادث* (FIRST). كما تشارك ICANN في الحوارات العالمية الرامية إلى تعزيز فهم تحديات الأمن والاستقرار والمرونة التي تواجه النظام البيئي للإنترنت وكيفية مواجهة هذه التحديات بالاستعانة بالمناهج التي تضم العديد من أصحاب المصالح.

1. الغرض ونظرة عامة

ويحدد تحديث خطة SSR إلى نطاق كبير من أصحاب المصلحة كيفية إسهام ICANN في الجهود العالمية لتحديد أمان الإنترنت والاستقرار والمرونة والنظر بعين التحدي إلى لهذه الأمور مقابل الإنترنت والتركيز على المهمة المتعلقة بمعرفات الإنترنت الفريدة. وتوضح الخطة أدوار وحدود ICANN فيما يخص مشاركتها في هذا المجال، مع إلقاء الضوء على برامج ICANN الحالية المعنية بهذا الصدد وتوضح تفصيلاً الأنشطة المقررة والموارد المخصصة على مدار العام التشغيلي التالي. وقد قُسمت الخطة إلى سبعة أقسام وملحق:

- القسم 1: الغرض ونظرة عامة
- القسم 2: التحدي والفرص
- القسم 3: الدور المنوطة به ICANN
- القسم 4: مساهمو ICANN في جهود تحقيق الأمان والاستقرار والمرونة
- القسم 5: برامج ICANN المتواصلة المعنية بالأمان والاستقرار والمرونة
- القسم 6: *خطط ICANN للعام المالي 2011 المعنية بتحسين الأمن والاستقرار والمرونة*
- القسم 7: خاتمة
- *الملحق أ: كل ما يخص برنامج ICANN للعام المالي 2011 لتحقيق الأمن والاستقرار والمرونة من أهداف وشركاء وعناصر رئيسية لنتائج وموارد*

كما هو محدد في الملخص التنفيذي فإن هذا التحديث يستند إلى خطة SSR 2009 ورؤية الأهداف المحددة بالخطة الإستراتيجية لـ ICANN في الأعوام 2010-2013. وهذا الإصدار من الخطة مقصود به تقديم تحديثات إضافية حول تأسيس ICANN واستمرارها فيما يتعلق بدورها وتحسين إطار العمل لتنظيم جهود الاستقرار والأمان والمرونة. وقد تم تحديث الخطة كجزء من المراجعة السنوية بما يتوافق مع دوائر التخطيط الإستراتيجي والتشغيلي لـ ICANN.

2. التحدي والفرص

تتعرض بيئة الإنترنت الحيوية إلى التهديد من قبل المستويات المتزايدة من النشاط الضار لمجموعة متنوعة من الجهات حتى أصبح يضم مشاركة مكثفة من المنظمات الإجرامية في مجال الاحتيال والابتزاز وغير ذلك من الأنشطة غير القانونية التي تتم على الإنترنت، علاوة على زيادة حجم هجمات رفض الخدمة وغيرها من الأنشطة المشوشة التي تتم عبر الإنترنت. ولقد أصبح النشاط الممارس عبر الإنترنت يعكس على نحو متزايد النطاق الكامل لدوافع وسلوكيات الإنسان. فبصفة جزئية، يعكس هذا النشاط الطبيعة المنفتحة للإنترنت التي جعلت منه ابتكاراً ناجحاً وفعالاً وأتاحت الفرصة للتواصل والابتكار والمتاجرة ضمن مجتمعات عالمية. إلا أن هذا الانفتاح له مساوئه كذلك. فعلى سبيل المثال، لقد تزايد استغلال الفرص "لتزييف" أو "إفساد" نظام اسم النطاق (DNS) للتوجيه الخطأ لاتصالات الكمبيوتر الخاصة بالمستخدمين غير المهرة. وبالمثل، يتواصل تزايد حالات اختراق توجيه الاتصالات وعمليات اختراق تسجيل العناوين وتسجيل أرقام النظام المستقل (ASN). يمكن لهجمات DoS إزعاج كافة أنواع المستخدمين . ولقد تم خلال السنوات الأخيرة الإفصاح عن القلق المتزايد لكافة أصحاب المصالح ذات الصلة بالإنترنت المستخدمون والمؤسسات الدول ذات السيادة والمنظمات المشاركة في مناقشات بشأن الإنترنت ومجتمع المعلومات الأوسع نطاقاً. ويجب أن تتناول الجهود الرامية إلى مواجهة هذه التحديات كذلك العمل على معالجة المخاطر المحيطة بالأمن والاستقرار والتي قد تنشأ عن وضع عناصر تحكم جديدة قد يساء استخدامها من قبل المجرمين أو وضع تصميمات جديدة للشبكات تزيد من صعوبة تحقيق الاستقرار المنشود.

سوف تتناول ICANN المخاطر التي تواجه أمن واستقرار ومرونة الإنترنت ضمن نطاق مسئولياتها. تنص المادة 1 من اللائحة الداخلية لـ ICANN على أن مهمة ICANN تتمثل في "تنسيق نظام المعرفات الفريدة للإنترنت على نحو إجمالي، وضمان التشغيل الآمن والمستقر لنظم المعرفات الفريدة للإنترنت". وتركز برامج وأنشطة ICANN ضمن هذا السياق على تحقيق ثلاث خصائص أساسية في إطار نظم المعرف الفريد للإنترنت: الأمن والاستقرار والمرونة. يتمثل الأمن في القدرة على حماية نظم المعرفات الفريدة للإنترنت ومنع سوء استخدامها. ويتمثل الاستقرار في القدرة على ضمان عمل النظام على النحو المتوقع له، وفي ثقة مستخدمي نظم المعرف الفريد للإنترنت في عمل النظام على النحو المتوقع. أما المرونة فهي قدرة نظم المعرف الفريد للإنترنت على الاستجابة بفاعلية للهجمات الضارة وغيرها من الأنشطة المشوشة. تعمل ICANN بالتعاون مع أطراف مسئولة من مختلف مجالات نظم المعرف الفريد للإنترنت لضمان المسائلة عن التنفيذ الملائم لسياساتها وترتيباتها التعاقدية. وبصفتها منظمة تضم العديد من أصحاب المصالح، تحرص ICANN على أن تحقق من خلال جهودها الاستخدام الأمثل لمواد المجتمع المتوافرة في هذا المجال، وأن تعمل بالتعاون مع أصحاب المصالح الرئيسيين بها مع تحديد أهداف ومقاييس الأداء بوضوح في تخطيطها الإستراتيجي والتشغيلي والمالي. توفر هذه الخطة للمجتمع خارطة طريق توضح الكيفية التي تفي بها ICANN بما عليها من مسئوليات.

يستعرض الملحق أ للخطة بعض التفاصيل الخاصة بأنشطة العام المالي 2011 المقررة وأهم المعايير والموارد ذات الصلة. ومن أهم محاور اهتمام أهداف العام المالي 2011 لموظفي أمن الإنترنت بـ ICANN سيكون وضع مقاييس للبرامج الأوسع نطاقاً الرامية إلى تحسين المستوى الإجمالي لأمن واستقرار ومرونة نظم المعرفات الفريدة للإنترنت.

3. الدور المنوطة به ICANN

تعمل ICANN وفقاً للوائحها الداخلية لتنفيذ عمليات تضم عدد من أصحاب المصالح وتقوم على الموافقة الجماعية لوضع سياساتها وبرامجها، متضمنة تلك المرتبطة بالأمن والاستقرار والمرونة.وتتمثل المهمة الرئيسية لمنظمة ICANN في تمكين استخدام منهج يضم العديد من أصحاب المصالح لتشغيل بفاعلية وظائف هيئة الأرقام المعينة للإنترنت (IANA)؛ وإنشاء سياسات عالمية تضمن تحقيق التنسيق بين DNS وبروتوكول الإنترنت (IP) وتعيينات IP وتعزز من المنافسة والاختيار من ضمن بيئة نطاق المستوى الأعلى العام (gTLD) من خلال نظام قائم على العقود مع تسجيلات gTLD والمسجلين المعتمدين من قبل ICANN.

وكجزء من مهمتها، لعبت ICANN دوراً خلال الأعوام العشرة الأخيرة في الإسهام في تحقيق أمن واستقرار نظم المعرفات الفريدة للإنترنت. فلقد أدركت كل من ICANN ومشغلو نظم المعرفات الفريدة للإنترنت ذوي الصلة أن صيانة وتحسين أمن واستقرار الخدمات إنما يعد عنصراً جوهرياً في علاقتهم. ويبرز هذا المبدأ في نظام العقود والاتفاقيات التي تعقد بين ICANN والمشغلين وفقاً للطبيعة المتفردة للعلاقات بينهم والأدوار الخاصة بكل طرف والمسئوليات المتبادلة. إن هذا الجهد المتعاون وتنفيذه يوفران عنصر الثقة الضروري في أن المعرفات الفريدة والمنظمات التي توفرها عبر مختلف أرجاء العالم سوف تضمن الأمن والاستقرار والمرونة من خلال نظام منسق متعاون.

وتعتزم ICANN مواصلة المساهمة في مجموعة واسعة النطاق من الأنشطة لتمكين تحقيق الأمن والاستقرار والمرونة لأسماء الإنترنت ونظم المعالجة في مواجهة المخاطر والتهديدات المستجدة. وفي الوقت ذاته، سوف تضمن تركيز جهودها على مهمتها الرئيسية المرتبطة بنظم المعرفات الفريدة للإنترنت. ولن تتعامل مع موظف السياسة بالتعاون على تقليل السلوكيات الإجرامية والإجراءات الضارة وعواملها. فمنظمة ICANN لا تشارك في أنشطة أو حوارات ذات صلة باستخدام الإنترنت لغرض أعمال جاسوسية وحرب الإنترنت. كما أنها لن تقحم نفسها في مناقشات حول ما يمثل محتوى غير قانوني ينشر على أو ينتقل عبر مواقع الإنترنت. فسوف تواصل ICANN مشاركة مجتمع الإنترنت الأوسع نطاقاً في المنتديات الرئيسية المتعلقة بمكافحة بعض الأنشطة الضارة المحددة (مثل الاحتيال والبريد المزعج) التي تستخدم نظام المعرف الفريد للإنترنت.

تقوم ICANN بهيكلة أنشطتها المعنية بالأمن والاستقرار والمرونة من خلال مراعاة دورها باعتبارها: مسئولاً مباشرًا، وأحد عناصر التمكين/التسهيل، وكمشارك.

- وتتحمل ICANN المسئولية المباشرة عن عمليات IANA كما تساهم في جمع وتوزيع منطقة الجذر مع وزارة التجارة الأمريكية وVeriSign. وهو ما يضمن استمرار التشغيل الآمن والمستقر والمرن لوظيفة منطقة جذر DNS على قمة أولوياتها. علاوة على ذلك، تعد ICANN عنصر تفعيل رئيسي لـ DNS وهي تتناول جهود المجتمع المعنية بمصادقة أسماء وأرقام الإنترنت. وترى ICANN أن أحد الخطوات الرئيسية في معالجة أمن DNS هو تنفيذ امتدادات الأمان لنظام أسماء النطاقات (DNSSEC) (*ICANN، VeriSign وNTIA بحيث يتضمن توقيع منطقة الجذر في 16 يوليو 2010*). وتركز الجهود الرئيسية الأخرى على تحسين فهم المخاطر على جميع نواحي النظام، وتمكين التنفيذ على مستوى الجذر للبنية التحتية الرئيسية العامة للموارد (RPKI) فضلاً عن التعاون مع الشركاء لتحسين ممارسات الأمن والمرونة في مجتمع TLD.

- تعد ICANN جهة تفعيل وتسهيل لأنشطة تعزيز الأمن والاستقرار والمرونة المبذولة من قبل سجلات DNS والمسجلين وباقي أعضاء المجتمع. تعتمد طبيعة أدوار ومسئوليات ICANN على السمات الخاصة لعلاقتها بهؤلاء المشغلين الرئيسيين. وبالإضافة إلى أنشطة التعاون، قامت ICANN بإبرام عقود مع كافة تسجيلات gTLD والمسجلين المعتمدين من قبل ICANN. ولقد أخذت هذه الاتفاقيات في أن تمثل على نحو متزايد آليات لتحسين الأمن والاستقرار والمرونة عبر DNS. وتعد الجهود التي تبذلها ICANN في سبيل ضمان الالتزام وتنفيذ أحكام هذه الاتفاقيات من أهم العناصر التي تركز عليها في تقدمها للأمام. وفيما يتعلق بتسجيلات نطاقات المستوى الأعلى لرمز البلد (ccTLD)، فلقد أكدت ICANN ومشغلو ccTLD على التزامهما نحو تحسين مستوى استقرار وأمن وإمكانية تشغيل DNS لصالح مجتمع الإنترنت المحلي والعالمي على أساس العلاقة المناظرة. وتكون مشاركة المعلومات والدعم المتبادل وتعزيز القدرات هي محاور اهتمام الأنشطة الرامية إلى التقدم. ستركز ICANN كذلك على إمكانيات الاستجابة المشتركة بالمجتمع لتوفير الأمان المحسن لـ DNS.
- تشارك ICANN في بعض الأنشطة مع منظمة مصادر الأرقام (NRO) وتسجيلات الإنترنت الإقليمية (RIR) في ظل توجيه إدراك واسع النطاق بأنه يتعين على RIRs وICANN العمل على صيانة وتحسين أمن واستقرار ومرونة الإنترنت لصالح مستخدميه على المستوى المحلي والعالمي.
- تعد ICANN مسئولة على نحو مباشر عن عملية الأمن والاستقرار والمرونة فيما يخص أصولها وخدماتها إبان إجراءها لعمليات IANA وغيرها من وظائف التنسيق وبصفتها مشغل لخادم جذر L الخاص بـ DNS.
- تعتبر المنظمات الداعمة واللجان الاستشارية والموظفين بـ ICANN المشاركين الرئيسيين في المنتديات والأنشطة الأوسع نطاقاً والتي تتراوح أغراضها من تحسين المرونة في مواجهة الهجمات المشوشة إلى الجهود التعاونية التي تنصب على مكافحة نشاط الإنترنت الضار مثل نشر البرامج الضارة والاحتيال التي يستغل نظم المعرفات الفريدة للإنترنت. تتضمن الأمثلة جلسات مفصلة باجتماعات ICANN الأخيرة على إساءة DNS وDNSSEC.
- تحمل ICANN على عاتقها مهمة اكتساب ثقة العامة فيما يخص دورها في تنسيق نظم المعرف الفريد للإنترنت كما سوف تلعب دور قيادي فيما يخص تحديات تحقيق نظام بيئي للإنترنت يتسم بالأمن والاستقرار والمرونة والذي يجب أن يظل كذلك بيئة حيوية لدعم الحوار والتجارة والابتكار على مستوى العالم.

4. مساهمو ICANN في جهود تحقيق الأمان والاستقرار والمرونة

تتضمن مساهمات ICANN المتعلقة بتحقيق الأمن والاستقرار والمرونة عدة أنشطة تشمل العاملين في المنظمة ودعم المنظمات واللجان الاستشارية. تتضمن قائمة المشاركين الرئيسيين:

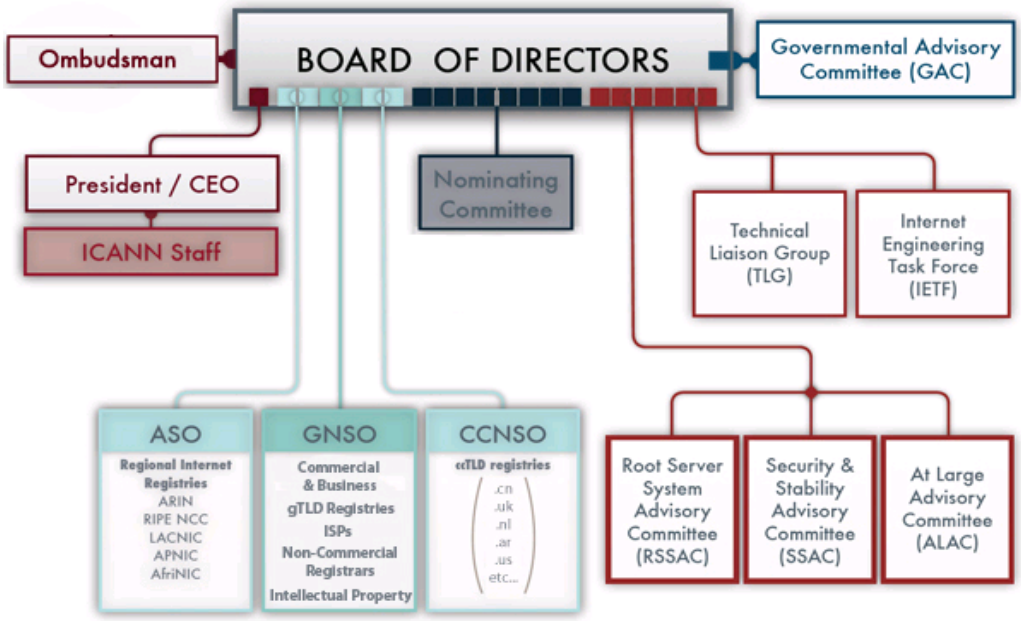
- ***فريق عمليات تشغيل IANA*** – هو المسئول عن تنفيذ وظائف IANA بحيث تتضمن تنسيق منطقة جذر DNS وتشغيل تسجيل arpa. وتخصيص مساحة عنوان IP وتسجيل معايير البروتوكول. نوضح أدناه بعض الأنشطة المحددة الخاصة بالأمن والاستقرار والمرونة.
- ***فريق عمليات تشغيل DNS*** – هو المسئول عن عمليات التشغيل للجذر L أحد خوادم الاسم الثلاثة عشر وبنية DNSSEC التحتية لـ ICANN-وإدارة النطاقات وTLDs وتوقيع DNSSEC بالجذر ROOT (KSK) و منشآت KSK والخطب وتسكين ccTLD وخوادم DNS المخولة لـ ICANN وملف تعريف ICANN. يحضر أعضاء فريق عمليات تشغيل DNS بانتظام الاجتماعات مثل NANOG وRIPE وMENOG وLACNOG وNZNOG وSANOG وAFNOG وآخرين للحديث عن المظاهر المختلفة المتعلقة بالمشروعات لأنشطة DNS لعمليات التشغيل.
- ***فريق الخدمات / التوافق التعاقدي*** – هو المسئول عن ضمان التنسيق والالتزام بالاتفاقيات المبرمة من قبل تسجيلات gTLD والمسجلين المعتمدين من قبل ICANN. نوضح أدناه بعض الأنشطة المحددة الخاصة بالأمن والاستقرار والمرونة.
- ***فريق السياسة*** – هو المسئول عن المساعدة في دعم المنظمات واللجان الاستشارية في تنفيذ الأنشطة الخاصة بهم المتعلقة بصياغة السياسة، متضمنة تلك الأنشطة المعنية بدعم مجموعات العمل المكونة من قبل المنظمة. نوضح أدناه بعض الأنشطة المحددة الخاصة بالأمن والاستقرار والمرونة.
- ***فريق الشراكة العالمية*** – متضمنة تلك الأنشطة المعنية بدعم مجموعات العمل المكونة من قبل المنظمة. وفي هذا الصدد، يتم تضمين أنشطة ICANN المرتبطة بالأمن والاستقرار والمرونة في العمل الإجمالي الخاص بالشراكات العالمية للمنظمة.
- ***فريق الاتصالات المشتركة*** – هو المسئول عن ضمان توصيل خطط وبرامج ICANN بفاعلية وتمثيل المنظمة وأنشطتها أمام مجتمع ICANN. تتكامل أنشطة ICANN المرتبطة بالأمن والاستقرار والمرونة مع البرنامج الكلي لاتصالات الشركة.
- ***فريق الأمان*** – هو المسئول عن التخطيط والتنفيذ اليومي لجهود ICANN التشغيلية المرتبطة بالأمن وفقاً لتوجيهات مجلس ICANN والمسئول التنفيذي الأول للمنظمة سعياً لتحقيق الخطط الإستراتيجية والتشغيلية لـ ICANN. يقوم الفريق بتنسيق كافة جهود ICANN لضمان المشاركة الفعالة في الموضوعات ذات الصلة بالأمن، متضمنة أمن الإنترنت وغير ذلك من المنتديات المرتبطة بالأمن والاستقرار والمرونة.
- ***اللجنة الاستشارية للأمان والاستقرار (SSAC)*** – تعتبر اللجنة الاستشارية لمنظمة ICANN وSSAC هي المسئولة عن تعريف مجلس ومجتمع ICANN بالقضايا والتحديات الرئيسية التي تواجهها ICANN في سبيل سعيها لتحقيق الأمن والاستقرار لنظم المعرفات الفريدة للإنترنت. تقوم اللجنة بإجراء دراسات على القضايا الرئيسية وفقاً لطلبات مجلس ICANN وحسبما تبادر به

المنظمة كجزء من التزامها الموصوف أدناه، علاوة على التعاون مع منظمات ICANN الأخرى مثل منظمة دعم الأسماء العامة (GNSO).

- ***اللجنة الاستشارية لنظام خادم الجذر*** – عبارة عن لجنة استشارية تابعة إلى ICANN، حيث توفر RSSAC الاستشارة فيما يخص المتطلبات التشغيلية لخوادم اسم الجذر علاوة على اختبار ومساندة العناصر الأمنية لنظام خادم اسم الجذر وأداء النظام بأكمله وفعاليته وكفاءته.

وعلى نحو أوسع نطاقاً، فإن الأنشطة المتعلقة بتحقيق الأمن والاستقرار والمرونة تتم عبر ICANN لدعم المنظمات واللجان الاستشارية الأخرى كما هو موصوف أدناه.

يتحمل فريق الأمن في ICANN مسئولية عامة حيال تحقيق تنظيم فعال عبر مختلف أنشطة ICANN ووضع عملية متكاملة للتخطيط والمتابعة لهذه الأنشطة مع ضمان المحاذاة والتكامل عبر مختلف الأقسام ولدى أصحاب المصالح. يصف الشكل 1 العلاقة التنظيمية الأساسية في هيكل ICANN.



الشكل 1 – هيكل ICANN التنظيمي

5. برامج ICANN المتواصلة المعنية بالأمان والاستقرار والمرونة

يوضح هذا القسم أكبر البرامج والأنشطة التي تجريها ICANN مساهمة منها في تحقيق أمن واستقرار ومرونة نظم المعرف الفريد للإنترنت، وكذلك للوقوف على الشركاء التشغيليين الرئيسيين وتوفير معلومات مرجعية حول الجهود الراهنة. إن الغرض من هذا القسم من الخطة هو توفير فهم أساسي للنطاق العريض من أنشطة ICANN المعنية بالمساهمة في تحقيق أمن واستقرار ومرونة نظم المعرفات الفريدة للإنترنت. وحتى يتسنى لمنظمة ICANN الإيفاء بما على كاهلها من مسئوليات في هذا المجال بفاعلية، يتم تضمين أغلب العناصر الكبرى من الموظفين وكذلك المنظمات الداعمة واللجان الاستشارية. ومن ثم، يطرح هذا القسم بعض المعلومات المرجعية والإيضاحية حول كيفية ملائمة البرامج والأنشطة ضمن هيكل ICANN وكذلك حول كيفية تفاعلهما مع المنظمات الخارجية.

يدور هذا القسم حول إطار العمل الذي تم وضعه في القسم 3، بدءًا من وظائف DNS/المعالجة الرئيسية؛ والعمل مع تسجيل TLD ومجتمعات المسجل المشاركة مع NRO وRIR؛ وأمن الشركة وبرامج الاستمرارية؛ وأنشطة المنظمات الداعمة واللجان الاستشارية، المشاركة في الأنشطة المعنية بأمن واستقرار ومرونة الإنترنت على المستوى المحلي والعالمي.

5.1 برامج الأمان والاستقرار والمرونة الخاصة بـ DNS/Addressing

5.1.1 عمليات تشغيل (IANA)

تعمل ICANN على تشغيل وظائف IANA بالتعاون مع كل من وزارة التجارة الأمريكية وVeriSign وفريق عمل هندسة الإنترنت (IEFT) وتسجيلات الإنترنت الإقليمية (RIRs) ومشغلي النطاق الأعلى مستوى (TLD) كما هو موصوف أدناه. ويعد الأداء الفعال لهذه الأنشطة هو المساهمة الأساسية التي تشارك بها ICANN في تحقيق أمن واستقرار ومرونة الإنترنت. ومن خلال تنفيذ وظائف IANA، تقوم ICANN بتنسيق وإدارة التسجيلات الخاصة بالمعرفات الرئيسية ممكنة بذلك توفير خدمة إنترنت عالمية وعالية الكفاءة.

بينما يشتهر الإنترنت بكونه شبكة عالمية تخلو من كافة صور التنسيق المركزي، يلزم تنسيق العمليات الرئيسية لنظام المعرف الفريد للإنترنت على مستوى عالمي - وتتولى ICANN هذا الدور التنسيقي. وعلى وجه الخصوص، تقوم IANA بتخصيص وصيانة الرموز الفريدة ونظم الترقيم المستخدمة في المعايير التقنية ("البرتوكولات") التي توجه الإنترنت. ويمكن تقسيم الأنشطة المتعددة التي تقوم بها ICANN إلى ثلاث فئات:

- ***أسماء النطاق*** – من خلال وظائف IANA، تقوم ICANN بإدارة جذر DND ونطاقات int. وarpa. علاوة على مصدر ممارسات اسم النطاق العالمي (IDN). تعمل ممارسات إدارة IANA على ضمان أن أي تغير يطرأ على أي من هذه المناطق يخضع لتقييم أثره على استقرار وآمان النطاق الأعلى مستوى وعلى منطقة الجذر إجمالاً. يتيح كذلك تنفيذ وظائف IANA إلى ICANN لعب دورا في توفير أمن DNS ونظم توجيه IP من خلال نشر وصيانة مراسي ثقة

عند جذر DNS ونظم التوجيه التي في مقدورها تحسين بدرجة كبيرة سلامة بيانات المعرف الفريد وكذلك سلامة الاستجابات ضمن نظام DNS.

- ***العناوين وأرقام AS*** – من خلال وظائف IANA، تقوم ICANN بتنسيق المجموعة العامة لعناوين IPv4 وIPv6 وASNs، حيث توفرهما إلى RIRS. تخصص IANA موارد الأرقام هذه بـ RIRs بما يتفق مع سياسات مصدر الأرقام العالمية المطورة من مجتمعات RIR من خلال عمليا تطوير السياسة والتنسيق العالمي من ASO. وتتيح عملية سياسة المشاركة هذه تحقيق إجماع عالمي من قبل متلقي المصادر التي توفرها ICANN وRIR على نحو عادل وقابل للتوقع ومستقر. *تعمل ICANN مع RIRs (من خلال ASO) وIETF على تطوير تقنية RPKI لتقديم شهادة موارد الرقم.*
- ***تعيينات البروتوكول*** – تتم إدارة بروتوكول الإنترنت وتسجيلات المعايير بواسطة ICANN، من خلال وظائف IANA بالتعاون مع IEFT. تقوم ICANN بتنفيذ وصيانة البروتوكولات وتسجيلات المعايير التي تزيد عن 700 بروتوكول وتسجيل وفقاً للمعايير الموضوعة من خلال عملية الإجماع طويلة الأجل الخاصة بنشر طلب تعليقات (RFC). ومع العمل عن قرب مع IEFT ومؤلفي RFCs، يضمن فريق عمل وظائف IANA إنشاء التسجيلات باستخدام عمليات متناسقة وصيانتها لتظل دقيقة ومتاحة. وقد تم توثيق العلاقة بين فريق عمل وظائف IANA وIETF في RFC 2860 وفي اتفاقية مستوى الخدمة.

كذا عمل فريق عمل IANA مع مجتمع TLD لتعقب التنفيذ الإجمالي للتسكين ضمن نظام TLD استجابةً للضعف الضار للذاكرة المؤقتة لـ DNA المكتشف في صيف 2008 (انظر العرض التقديمي "الضعف الضار للذاكرة المؤقتة لـ DNA" على http://www.iana.org/about/ presentations/davies-cairo-vulnerability-081103.pdf). سوف تحرص ICANN على أن تعمل برامجها وأنشطتها على تحسين العمليات الآمنة والمستقرة للتغيرات/الإضافات التي تطرأ على منطقة لجذر علاوة على تشغيل نقاط ائتمان المراسي للاستعلامات ضمن DNS كما هو موضح أدناه.

تقوم ICANN سنوياً بإمداد وزارة التجارة الأمريكية بخطة لأمن المعلومات ذات صلة بتنفيذ وظائف IANA بالالتزام بعقد IANA الذي أبرمته ICANN مع وزارة التجارة كجزء من تخطيطها الخاص بالأمان وحالات الطوارئ. *في يناير 2010، عقدت ICANN تدريب استمرارية ناجح مع IANA، انظر تقرير ما بعد الإجراء الموجود في* http://www.icann.org/en/security/iana-business-continuity-exercise-aar-23feb10-en.pdf.

تتوقع ICANN إعداد تحديدات أخيرة من مساحة IPv4 الموحدة لسجلات الإنترنت الإقليمية (RIRs) خلال العام 2011. وهذه التحديدات ستتم وفقا للسياسة العالمية لتحديد تجوال مساحة عناوين IPv4[2] والتي تم تطويرها من مجتمعات RIR وتصنيفها من مجلس ICANN في مارس 2009.

على الرغم من أن هذا التحديد سيفرغ حوض العناوين الذي تتم إدارته من قسم IANA بـ ICANN فإن RIRs لا تزال تحدد المساحات مما يتم تحديده وتعيين عناوينه لـ ISPs ومشغلي الشبكة الآخرين. ويعمل RIRs على تأسيس سياسات

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

تضمن الوصول إلى الأشياء الصغيرة لمساحة عنوان IPv4 لمداخل السوق الجديد[3] خلال فترة بعد آخر خمسة /8s والتي تم تحديدها قبل تبني IPv6 من أغلبية شبكات الإنترنت المتواصلة.

كما أسست RIRs كذلك سياسات تسمح بمساحة عناوين IPv4 لنقلها من شبكة إلى أخرى إلى مشغل آخر للشبكة[4]. وهذه السياسات مصممة للسماح للشبكات لنقل العناوين حيث تكون ذات قيمة أكبر وتسمح باستمرار نمو الشبكة.

تعمل لجنة تقييم مخاطر مجلس ICANN على تقييم المخاطر التي قد تواجهها ICANN نتيجة لتقليل التوفر لمساحة عناوين IPv4.

الحل طويل الأمد للتبني المنتشر لـ IPv6. في حين ينظر للتقدم الكبير الحادث مع ISPs مثل XS4all في نيوزيلندا وهي تبدأ بعرض IPv6 كخدمة قياسية لكافة العملاء، وهناك طريقة أخرى للتنفيذ. تجري ICANN عددا من جلسات التوعية الجديدة باجتماعات ICANN في حين تجري RIRs جلسات عن IPv6 فيما يتعلق بالتدريب والتوعية بهذا البرنامج[5][6][7][8][9].

ولعل الحدث الرئيسي للتذكير يتمثل في استمرار الإنترنت الحالي في العمل حتى بعد تحديد RIRs لخوادم IPv4. وستكون هناك فترة حيث يمكن الوصول لبضع الشبكات عبر IPv6 وبعضها لن يكون متمتعا بتلك الميزة إلاّ أن IPv6 سيسمح للمشغلين بالاستمرار في زيادة شبكاتهم إلى أبعد مدى من IPv4.

5.1.2 عمليات DNS

أوعزت ICANN بالحاجة إلى تنفيذ DNSSEC بالمستوى الجذري. ونظرا لبدء خطة SSR فإن ICANN وVeriSign وNTIA قد تقدمت في اتجاه تنفيذ DNSSEC من خلال التقديم المتوازن للجذر الإجمالي وتوقيعه في 2010. ولعل الخطة الرئيسية الأولى للتوقيع (KSK) تتمثل في عقد DNSSEC في Culpeper وVirginia في 16 يونيو 2010 (انظر http://www.icann.org/en/announcements/announcement-4-16jun10-en.htm) وخطبة KSK الثانية عقدت في 12 يوليو 2010 في لوس أنجلوس كاليفورنيا لتمكين الاشتراك في منطقة الجذر. ويقدم توظيف DNSSEC بمنطقة الجذر فوائد كثيرة لمن تم الإعلان عن معلومات متعلقة بـ DNS وتسمح

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

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

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

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

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

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

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

لمجتمع الإنترنت والمستخدمين بتحديد المادة الرئيسية بمنطقة الجذر وحماية قرارات DNS من الإهمال المؤقت.

وقد بدأت ICANN في الاشتراك في arpa. والعديد من النطاقات التنظيمية المملوكة لـ ICANN. وقد تضمنت هذه الاستعدادات تنفيذ اختبار DNSSEC منذ يونيو 2007، بالتعاون مع TLD ومشغلي DNS الآخرين فيما يتعلق بجهود تنفيذ DNSSEC، والحصول على الكفاءة الفنية في تنفيذ مناهج التشفير وفقاً للمعايير ذات الصلة وضمان تنفيذ جهود DNSSEC كجزء من إدارة الخطط والموازنات. وقد أنشئت ICANN فريق عمل مكرس مسئول عن إدارة وتأمين عمليات تنفيذ DNSSEC، والتي تضمنت توقيع icann.org وiana.org. وأخيراً، من أجل التنفيذ العام لـ DNSSEC، أنشأت ICANN مستودع ائتمان IANA لنطاقات المستوى الأعلى (ITAR) كطريقة لضمان مفاتيح DNSSEC لـ TLDs التي نفذت DNSSEC لتكون متاحة لمن يوزعون DNSSEC في هذا الوقت.

تتعاون ICANN مع مشغلي خوادم اسم الجذر فيما يتعلق بالتنسيق الآمن والمستقر لمنطقة الجذر، لضمان التخطيط الملائم لحالات الطوارئ وللحفاظ على عمليات واضحة في تغيرات منطقة الجذر. وستواصل ICANN تعاونها مع مشغلي خوادم اسم الجذر وغيرهم فيما يتعلق بالتنسيق الآمن والمستقر لنظام خادم الجذر. لقد كانت RSSAC مستشاراً رئيسياً فيما يخص كيفية تغير البروتوكولات، مثل إضافة تسجيلات IPv6 إلى الجذر، وهو ما من شأنه التأثير على النظام.

علاوةً على ذلك، تقوم ICANN *بتشغيل خادم اسم* الجذر المعروف بـ *l.root-servers.net*. ومن خلال هذا الدور التشغيلي، يتفاعل موظفو ICANN كذلك على المستوى التشغيلي مع مشغلي خادم الجذر الآخرين. وبصفتها مشغل جذر L، تلعب ICANN دوراً نشطاً في مجتمع DNS متضمناً المساهمة في جهود المجتمع مثل مركز العمليات والتحليل والبحث المعني بنظام اسم الجذر (DNS-OARC) وكذلك في المشروع البحثي "يوم في حياة الإنترنت" التابع للاتحاد التعاوني لتحليل بيانات الإنترنت (CAIDA). وتلتزم ICANN باستخدام عملياتها لتعزيز التنوع والفهم لأفضل الممارسات وهي تسعى لتعلم الدروس المستفادة ونشرها. *يدعم فريق عمليات تشغيل DNS كذلك دراسة موازنة الجذر L،* http://www.icann.org/en/announcements/announcement-17sep09-en.htm.

في 2009 حسنت ICANN مرونة الجذر L مع مدن مثل براغ، جمهورية التشيك واسطنبول،تركيا. وتم الإعداد لمزيد من التحسينات في العام 2010 وإلى العام المالي 2011.

5.2 أمن واستقرار ومرونة تسجيلات ومسجلي TLD

من المسئوليات الرئيسية والمباشرة الواقعة على كاهل ICANN فيما يخص أمن واستقرار ومرونة الإنترنت هو إدارة الاتفاقيات مع تسجيلات gTLD والمسجلين المعتمدين من قبل ICANN وكذلك إدارة هيكل اتفاقية إطار العمل المستخدمة لإدارة العلاقات مع تسجيلات ccTLD. لقد أبرمت ICANN عقوداً مع 16 تسجيل gTLD ومع ما يزيد عن 900 مسجل معتمد من المسئولين عن تنسيق تسجيل أسماء النطاقات والتأكد من توافقها مع DNS. ويتم تفصيل مسئوليات هؤلاء الأطراف المتعاقدة من خلال اتفاقيات التسجيل (RA) واتفاقيات اعتماد المسجلين (RAAs). وتسعى ICANN من جانبها إلى حماية مالكي أسماء النطاقات والمساهمة في الحفاظ على أمن واستقرار ومرونة DNS والإنترنت الأوسع نطاقاً من خلال الأحكام التي تتضمنها هذه الاتفاقيات. وعلى مدار العقد المنصرم، سعت ICANN جاهدة نحو تعزيز تلك

الاتفاقيات بحيث تتضمن أحكاماً من شانها تحسين الاستقرار والمرونة كما هو موضحاً أدناه.

5.2.1 سجلات gTLD

تتعاون ICANN مع مشغلي gTLD فيما يتعلق بتنسيق الأمان والاستقرار لتلك TLDs. تحافظ كل سجلات gTLD على اتفاقيات مع ICANN. وعلى الرغم من أنه قد يكون هناك تفاوت في بعض عناصر هذه العقود، إلا أن الأحكام المتعلقة بالأمن والاستقرار والمرونة ثابتة فيها جميعاً. تتضمن هذه الاتفاقيات حكماً يلزم مشغلي التسجيلات بتنفيذ المواصفات أو السياسات المؤقتة الموضوعة من قبل ICANN وسياسات الإجماع الموضوعة من قبل GNSO والمعمول بها في ICANN. وتشتمل الفقرات الأخرى التي تسهم في تحقيق تشغيل آمن ومستقر للتسجيل على متطلب بتوفير مستودع بيانات لطرف ثالث واتفاقيات على مستوى الخدمة خاصة بخدمات DNS ونظام التسجيل المشترك وعمليات خادم الاسم. تحدد عقود ICANN-gTLD متطلبات التوافر ومستويات الأداء ومركز البيانات. وفي عام 2007، بادرت ICANN بجهود على صعيد التخطيط لاستمرارية gTLD والتي تمخضت عن وضع خطة عمل علاوة على الالتزام بسلسلة من التدريبات السنوية للخطة لتحسين قدرة مجتمع تسجيل gTLD على التعامل مع المشكلات أو حالات الفشل التي تواجه نظام السجل/المسجل.

في عام 2006، قدمت ICANN عملية تقييم خدمات التسجيل (RSEP) كوسيلة لتسهيل توفير عملية دقيقة وقابلة للتوقع لتقديم خدمات تسجيل جديدة. ومن العناصر الرئيسية لـ RSEP هو تحديد ما إذا كانت الخدمة المقترحة يمكن أن تمثل مشكلة على صعيد الأمن أو الاستقرار. فإذا تم البت بأن الخدمة الجديدة قد تمثل مشكلة فيما يخص الأمن والاستقرار، يتم إحالة العرض إلى لجنة مستقلة من الخبراء التقنيين تسمى لجنة التقييم التقني لخدمات التسجيل (RSTEP). تقوم لجنة RSTEP بمراجعة الخدمة المقترحة وتقدم توصياتها إلى مجلس ICANN حول ما إذا كان يجب اعتماد أو رفض الخدمة.

تم تقديم طلب أمان السجل المرسل (ERSR) في أكتوبر 2009 (انظر http://www.icann.org/en/registries/ersr/). قامت ERSR بتطوير العملية لاتخاذ إجراء سريع في الحالات التي تقوم فيها سجلات gTLD بإبلاغ ICANN بدرجة الأمان الحالية أو الوشيكة لـ TLD و/أو DNS وطلب التنازل التعاقدي عن الإجراءات التي قد يقومون باتخاذها أو اتخذوها بالفعل للتخلص من الحوادث أو التقليل منها. والتنازل التعاقدي هو استثناء من التوافق مع فقرة محددة لاتفاقية السجل لفترة من الوقت ضرورية لاستجابة للحوادث. وقد صممت ERSR للسماح بالأمان التشغيلي للحفاظ عليه بمستوى الحوادث مع الحفاظ على الأطراف ذات الصلة (مثل ICANN أو المزودين المتأثرين الآخرين وما إلى ذلك) وإبلاغهم ما أمكن.

5.2.2 gTLDs الجديدة وIDNs

خلال العام المالي 2010 وإلى العام المالي 2011، عملت ICANN مع المجتمع على تحسين طرق الحد من الإجراءات الخبيثة لـ TLDs الجديدة [انظر مذكرة الحد من الإجراءات الخبيثة والضارة 28 مايو 2010، http://www.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-memo-update-28may10-en.pdf].

ومع إطلاق عملية التتبع السريع لـ IDN ccTLD في نوفمبر 2009 والاستعدادات لعملية gTLD الجديدة لتضمين IDNs وتعمل ICANN على إدراك الحاجة إلى توحيد الجهود لضمان الأمن والاستقرار ومرونة عمليات التشغيل للمداخل الجديدة بنظام DNS والنظام ككل. يتضمن طلب gTLD الجديد وعملية المراجعة تقييم تقني لقدرة مقدم الطلب على تشغيل تسجيل وكذلك لتوافق السلاسل مع المتطلبات التقنية المنصوص عليها في RFCs وفقاً لبرتوكول أسماء النطاقات الدولية في الطلبات (IDNA) وتوجيهات IDN.

أطلقت ICANN عملية التتبع السريع IDN ccTLD في 16 نوفمبر 2009 (انظر http://www.icann.org/en/topics/idn/fast-track/). تلقى البرنامج 34 طلبا بعدد من اللغات 22 مختلفة منذ الانطلاق (انظر http://www.icann.org/en/topics/idn/fast-track/string-evaluation-completion-en.htm). تتنقل هذه السلاسل في الوقت الحالي من خطوة تفويض IANA وسلاسل IDN ccTLD الأولى التي أدخلت إلى منطقة الجذر في مايو 2010 لبلاد مصر والمملكة العربية السعودية والإمارات العربية المتحدة وروسيا الاتحادية. وافق مجلس إدارة ICANN على تفويض سلاسل إلى الصين وهونج كونج وتايوان في اجتماع ICANN في بروكسل في يونيو 2010 والسلاسل لبلاد سيريلانكا وتايلاند وفلسطين المحتلة والأردن وتونس حيث تمت الموافقة عليها في أغسطس 2010.

والتمهيد الأولي لعملية التتبع السريع لـ IDN ccTLDs مقصور على-السلاسل غير المستمرة التي تمثل البلدان وأسماء المناطق المطابقة لـ ccTLDs الحالية.

في عملية التتبع السريع يوجد فريق مستقل من الخبراء ومجلس استقرار DNS وقد عقدت تقييم لمقترح IDN ccTLD والصراع المحتمل مع متطلبات الأمان والاستقرار لسلاسل IDN. ويتوقع وجود لجنة خبراء مماثلة لعملية gTLD الجديدة على أن تتوفر وتعقد التقييم التقني لمقدمي الطلبات ومقترح TLDs. علاوة على ذلك، توفر عملية gTLD الجديدة عملية RSEP (تقييم خدمة السجل) مسبقة لتقييم المشكلات المحتملة على نطاق الأمن والاستقرار لخدمات التسجيل الجديدة المقترحة في طلب gTLD.

فضلاً عما سبق، سوف يتعين على جميع مقدمي الطلبات اجتياز فحص تقني سابق للتفويض للتحقق من استيفاءهم للمتطلبات التقنية اللازمة لتشغيل تسجيل.

تنوي ICANN بدء مراجعة تنفيذ عملية التتبع السريع لـ IDN ccTLD في العام المالي 2011.

5.2.3 مسجلي gTLD

تتعاون ICANN كذلك مع المسجلين فيما يتعلق بالأمن والاستقرار والمرونة. وعلى نحو تعاقدي فإن اتفاقية اعتماد المسجل القياسية (RAA) تحكم علاقات ICANN مع المسجلين. هذا وتنص RAA على بعض المعايير الخاصة بجمع البيانات والاحتفاظ بها وإيداعها في مستودع بيانات. كما تضم RAA كذلك، بالإشارة، سياسات الإجماع الموضوعة من قبل مجتمع ICANN، مثل سياسة الانتقال الداخلي ما بين المسجلين وسياسة التذكير ببيانات Whois وسياسة دقة الأسماء المستعادة، إضافة إلى سياسات أخرى، والتي تدعم بسبل مختلفة أمن واستقرار ومرونة DNS. *تم تقديم RAA المحسنة في 2009 وأكثر من 95% من سجلات gTLD يتم تناولها حاليا في اتفاقية RAA 2009 من خلال تبني سجل طوعي. أعلنت ICANN عن دليل غير المحامين لاتفاقية RAA لعام 2009 استجابة لطلب لجنة At-Large الاستشارية لعمل دليل (http://www.icann.org/en/registrars/non-lawyers-guide-to-ra-agreement-15feb10-en.htm).*

يعمل موظفو سجل Registrar Liaison التابع لـ ICANN كخط دفاع أول في مراقبة توافق التسجيل مع متطلبات RAA بصفة يومية من خلال العمل بصفة غير رسمية على حل شكاوى مالكي أسماء النطاقات والمنازعات الداخلية التي تنشأ فيما بين المسجلين، وكذلك من خلال مراجعات الاعتماد الدورية (مثل عند تجديد RAA للمسجل).

دعماً لتحقيق نظام اسم نطاق أكثر استقراراً، قامت ICANN بتطوير برامج وإجراءات لمواجهة الفشل المحتمل للمسجل. على سبيل المثال، قامت ICANN بتنفيذ برنامجها لمستودع بيانات المسجل، والذي يلزم المسجلين بإيداع نسخة احتياطية من بيانات التسجيل في مستودع بيانات على أساس يومي أو أسبوعي. يعمل إجراء انتقال المسجلين غير المعتمدين على تسهيل الانتقال السريع للتسجيلات من مسجل غير معتمد إلى مسجل معتمد من قبل ICANN. علاوةً على ذلك، يستخدم موظفو ICANN العديد من عمليات تشغيل الإنترنت التي تهدف إلى المساعدة على الحفاظ على بيئة تسجيل نطاق صحية ومنع إزعاج مالكي أسماء النطاقات ومستخدمي الإنترنت في حالة فشل التسجيل.

Whois 5.2.4

توفر خدمات Whois الوصول العام إلى البيانات الخاصة بأسماء النطاقات المسجلة، والتي تتضمن حالياً معلومات الاتصال الخاصة بمالك الاسم المسجل. تلعب ICANN دوراً في إدارة القواعد الموضوعة من قبل المجتمع لنظام Whois ضمن gTLDs. إن حجم بيانات التسجيل التي يتم جمعها إبان تسجيل اسم نطاق، والسبل التي يمكن من خلالها الوصول إلى تلك البيانات، يتم تحديدها في الاتفاقيات التي تبرم مع ICANN حول أسماء النطاقات المسجلة في gTLDs. على سبيل المثال، تطلب ICANN من المسجلين المعتمدين القيام بجمع وتقديم وصول عام مجاني إلى اسم النطاق المسجل وخوادم الاسم الخاصة به والمسجل والتاريخ الذي تم فيه إنشاء النطاق وتاريخ انتهاء صلاحيته، ومعلومات الاتصال الخاصة بمالك الاسم المسجل وجهة الاتصال الخاصة بالأمور التقنية وجهة الاتصال الخاصة بالأمور الإدارية.

يتم استخدام Whois من قبل مجتمعات مختلفة لأغراض متعددة من بينها تيسير التنسيق التقني والمساعدة على توفير المعلومات الخاصة بالمنظمات والأفراد الذين قد يكونوا مشاركين في إساءة استخدام DNS. تتركز أنشطة ICANN على ضمان التزام سجلات gTLD والمسجلين المعتمدين من قبل ICANN بالتزاماتهم التعاقدية. وفيما يخص تغيرات السياسة المرتبطة بـ Whois، يدرك مجتمع ICANN الاستخدام الشرعي لنظام Whois لمساعدة هؤلاء العاملين على مكافحة إساءة استخدام DNS، مع السعي لتحقيق التوازن للنطاق العريض من اهتمامات أصحاب المصالح في كيفية تشغيل نظام Whois. كما تدرك ICANN أمور الخصوصية والسرية التي عبر الأفراد عن قلقهم حيالها فيما يخص إتاحة الوصول إلى معلوماتهم عبر Whois. تستمر ICANN في جهودها الرامية إلى تحديد هذه المشكلات. إدراك خدمة Whois الحالية أمر قد يقلل من الوثوقية والنفعية بمرور الوقت واتجاه GNSO، أكمل فريق عمل ICANN مجموعة كاملة من المتطلبات لـ WHOIS التي تتضمن عيوبا معروفة بالخدمة الحالية والمتطلبات المحتملة اللازمة لدعم مبادرات السياسة المستقبلية. [مرجع: منظمة دعم الأسماء العامة لـ ICANN على (GNSO) قرارات المجلس في مايو 2009. Marina Del Rey, CA: ICANN. استرجاع المعلومات في 25 أكتوبر 2009 من http://gnso.icann.org/resolutions/#200905].

يحاول التقرير تحديد المتطلبات التقنية الضرورية لتنفيذ وتصحيح العيوب وتنفيذ سياسات Whois المستقبلية. عدد من المزايا بهذا المخزون لها مناطق نشأة في توصيات SSAC لـ GNSO وتوضح أن ICANN ومن خلال اعتبار AC/SO

داخليا لإجراءات تحسين WHOIS هي ملتزمة بتمويل الحلول التي تحافظ على فائدة واستخدام WHOIS مع اعتبار الخصوصية والأمان لمعلومات WHOIS.

5.2.5 التوافق التعاقدي

يعمل قسم الالتزام التعاقدي على ضمان قيام كلا من ICANN والأطراف المتعاقدة معها على استيفاء المتطلبات الخاصة بكل منهما والمنصوص عليها في الاتفاقيات المبرمة فيما بينهما. تتضمن أنشطة هذا القسم إدارة نظام تلقي الشكاوى في ICANN والذي يسمح للعامة بتسجيل الشكاوى المرتبطة بأسماء النطاقات والتي قد تكون ذات صلة بشئون الأمن والاستقرار والمرونة. انظر موقع الويب على http://reports.internic.net/cgi/registrars/problem-report.cgi.
يبحث فريق عمل التوافق التعاقدي الشكاوى المتعلقة بمحاولات انتهاك RAA المحتملة واتخاذ إجراءات التوافق عند اكتشاف انتهاك التعاقد. وعلى الرغم من أن أغلب الشكاوى التي يتم تلقيها عبر هذا النظام تكون بخصوص أمور خارجة عن نطاق سلطة ICANN (مثل البريد المزعج ومحتوى مواقع الإنترنت وخدمة العملاء لدى المسجل)، تقوم ICANN جانبها بتحويل تلك الشكاوى إلى المسجلين للتعامل معها.

يقوم قسم التوافق التعاقدي كذلك بإدارة نظام تقرير مشكلات بيانات Whois (WDPRS) والذي يمكن الوصول إليه من خلال الرابط http://wdprs.internic.net/. وقد تم تصميم WDPRS لمساعدة المسجلين على الإيفاء بالتزامهم بالتحقيق في أي مزاعم بعدم دقة بيانات Whois. ويسمح هذا النظام، الذي تم وضعه في عام 2002، للعامة بتسجيل ادعاءاتهم بعدم دقة بيانات Whois، حيث يتم عقب ذلك نقل تلك الشكاوى إلى المسجلين لاتخاذ الإجراءات اللازمة. وبالتشاور مع المجتمع، فإن WDPRS أعادت التصميم في العام 2008 لتحديد المشكلات في الأداء الوظيفي والسعة المحدودة والافتقار إلى متابعة التوافق. ولقد تم تدشين WDPRS الجديد في ديسمبر 2008. ويواصل موظفو قسم الالتزام العمل على تحسين هذا النظام ساعين إلى زيادة دقة بيانات Whois.

فوضت ICANN مركز الرأي الوطني للأبحاث بجامعة شيكاغو من أجل إجراء دراسة على دقة بيانات Whois. تم نشر مسودة التقرير في 15 فبراير 2010، http://www.icann.org/en/announcements/announcement-3-15feb10-en.htm.

5.2.6 حماية مسجلي gTLD

تسعى ICANN كذلك إلى ضمان تمتع مالكي أسماء النطاقات بالثقة في أمن واستقرار ومرونة DNS بعدة سبل مختلفة. تتضمن سبل الحماية تلك بعض الأحكام فيما تبرمه ICANN من عقود واتفاقيات وبرامج تنفيذ. تقوم ICANN بإمداد مالكي أسماء النطاقات بمعلومات حول التزامات المسجلين بموجب RAA وبالطريقة التي يمكنهم بها تقديم شكواهم من خلال الموقع الإلكتروني http://www.internic.net/.
وعقدت ICANN كذلك جلسة توعية مع مجتمع المسجلين للتشجيع على دعم IPv6 لمسجلي النطاق.

علاوةً على ذلك، يتركز نشاط ICANN المعني بدعم المنظمات واللجان الاستشارية على مشكلات أمن واستقرار ومرونة مالكي أسماء النطاقات. حدد استشاري SSAC السابقين ممارسات المسجلين التي يجب وضعها في الاعتبار لحماية حسابات اسم النطاق مقابل الوصول غير المرخص وحماية معلومات تكوين DNS من إساءة

الاستخدام[10]. تتضمن مشروعات SSAC في العام 2010 تقرير تعقيبي يحدد ممارسات المسجلين التي يمكن أن تنفذ مباشرة المراقبة الاحتياطية وحماية حسابات تسجيل النطاق ومعلومات تكوين DNS من إساءة الاستخدام. تتضمن أنشطة SSAC الأخرى أوراقا عن حظر إعادة التوجيه من TLDs [SAC041] وتوظيف DNSSEC وجهات اتصالا إساءة المستند [SAC038] ومعالجة سجلات DNS التي لا أصل لها.

لجنة At-Large الاستشارية (ALAC) طرحت عدة موضوعات خاصة بحماية مالكي أسماء النطاقات. ولقد كان أول موضوع تطرحه ALAC هو اختبار اسم النطاق والذي أدى بمجلس ولجنة GNSO إلى اعتماد سياسة جديدة للإجماع تهدف إلى القضاء نهائياً على إساءة استخدام فترة السماح لاختبار النطاق. *وأقرب من ذلك فإن ALAC حددت مشكلات مجلس GNSO حول التعافي بعد الانقضاء لأسماء النطاق من المسجلين (PEDNR) وتسجيل اسم النطاق والمسئولية والشفافية [http://www.atlarge.icann.org/announcements/announcement-19jul10-en.htm]. ويتخذ مجلس GNSO عدداً من المبادرات الإضافية الرامية إلى توفير قدر أكبر من الحماية لمالكي أسماء النطاقات مثل التعديلات التي أدخلت على سياسة الانتقال الداخلي فيما بين المسجلين والتي تضمنت وضع في الاعتبار الحاجة إلى تصديق إلكتروني وتحسينات سياسية في مجالات سياسات إساءة استخدام استضافة التمويه السريع والتسجيل.*

5.2.7 ccTLDs

يتم التفاعل بين ICANN وccTLD في ظل فهم عميق لضرورة قيام كل من ccTLD وICANN بحفظ وتحسين أمن واستقرار ومرونة DNS لصالح مستخدمي الإنترنت على الصعيدين المحلي والعالمي. وتعكس هذه برنامج إطار عمل المسئولية الذي يشكل أساسا لتوثيق العلاقة بين سجلات ccTLD الفردية وICANN. ويعد الهدف الرئيسي الذي تسعى إليه ICANN من خلال تعزيز الأمن والاستقرار والمرونة مع ccTLD، من خلال التعاون مع الآخرين، هو توفير برنامج لمشاركة المعلومات والعمل المشترك إضافة إلى توفير تدريب تقني يعمل على رفع مستوى الوعي وتعزيز القدرات اعتماداً على تخطيط الاستجابة للهجمات والحالات الطارئة. ويعمل موظفو ICANN عن قرب مع مشغلي TLD لإعلامهم بالقضايا الخاصة بالأمن من خلال IANA وبرنامج تخطيط الاستجابة للهجمات والحالات الطارئة (ACRP) والجهود المبذولة من خلال الاتصالات المتبادلة الإقليمية للشراكات العالمية. طورت ICANN علاقة ثقة مع مشغلي TLD من خلال تحسين الأداء والاتصال بمجتمع مشغلي TLD الأمر الذي يساعد على تمكين تحقيق استجابة مشتركة في المواقف التي تطلب التنسيق على المستوى العالمي لمعالجة القضايا المرتبطة بـ DNS.

5.2.8 المتطلبات التقنية لـ IANA

إن ICANN، من خلال إدارة وظيفة IANA، إنما تساعد كذلك على ضمان إيفاء TLD بالمتطلبات التقنية اللازمة لدعم تحقيق عمليات آمنة ومستقرة. إن المتطلبات الخاصة لخوادم الأسماء تضمن توافر نطاقات DNS، كما يعمل موظفو IANA عن كثب مع مديري TLD لحل أي مشكلة قد تواجههم بخصوص الحفاظ على تلك المعايير التقنية. لا تقوم ICANN بالتدخل في عمليات ccTLDs، إلا إنها تكون على استعداد

[10] انظر SAC 40، إجراءات لحماية خدمات تسجيل النطاق من الانتهاك أو إساءة الاستخدام كما في 19 أغسطس 2009 (http://www.icann.org/en/committees/security/sac040.pdf).

دائم للمساعدة في الحالات التي تستلزم إجراء تغيير سريع ودقيق في بيانات منطقة الجذر خاصتها. ويتمثل الهدف الرئيسي لـ IANA في ضمان أمن واستقرار منطقة TLD ومنطقة الجذر.

5.2.9 الاستجابة الجماعية لحالات الإساءة الضارة بنظام اسم النطاق

تتعاون ICANN مع مجموعة من المنظمات في محاولة لضمان قدرة أصحاب المصالح على تحليل النشاط لذي قد يتضمن إساءة استخدام DNS. منذ أواخر 2009، حدثت طفرة كبيرة في النشاط المتضمن لبرامج ضارة تستهدف DNS. أحد أهم تلك الحوادث كانت في حادثة Conficker Worm [ملخص عن حادثة Conficker ومراجعة لها، http://www.icann.org/en/security/conficker-summary-review-07may10-en.pdf]. شاركت ICANN في الاستجابة العالمية والمشتركة لاحتواء Conficker بالأمان ومشغلي سجلات TLD وجمعيات تعزيز القانون. أعلنت ICANN عن تقرير وملخص لهجمة Conficker ومراجعة لها وتوثيق لتسلسل الأحداث ذات الصلة بهجمة Conficker ومناقشة الدروس المستفادة واقتراح طرق لتحسين الجهود المشتركة المستقبلية (مثل عملية ERSR الخاصة بـ ICANN). تستمر ICANN في العمل مع السجلات والمسجلين على ضمان التوعية وتسهيل المعلومات عند الحوادث المتعلقة بالأمان للتوازن العالمي بما يتضمن حدوث DNS. إن تفويض ICANN يعد محدوداً في هذا المجال، ولهذا شاركت كنظير في المناقشات الخاصة بكيفية تمكين استجابات فعالة عند ظهور مواقف تشغيلية محددة.

لتسهيل التعاون في هذا المجال دعم فريق ICANN الجهود داخل ccNSO حول الاستجابة في حالة الحوادث لـ ccTLDs. في فبراير من العام 2010، أعلنت ICANN عن حالة توعية عالمية عن وظائف DNS-CERT (http://www.icann.org/en/topics/ssr/dns-cert-business-case-19mar10-en.pdf) في مجتمع الإنترنت. وتضمن الحالة التجارية وصفا للمتطلبات والتكاليف المحتملة بما يتضمن خيار تشغيل أعضاء المجتمع مثل وظيفة DNS-CERT. منذ نشر الحالة التجارية لـ DNS-CERT والنظر بعين الاعتبار لتعليقات العامة (http://www.icann.org/en/public-comment/summary-analysis-strategic-ssr-initiatives-and-dns-cert-business-case-24may10-en.pdf) ومناقشات اجتماعات ICANN في نيروبي وبروكسل فإن ICANN تعمل مع الأطراف المهتمة على تحديد طرق إمكانية الاستجابة التعاونية لـ DNS التي لا تعمل من ICANN ولكن تتطور بالتعاون مع المجتمع.

5.2.10 تمكين الأمان والمرونة الإجمالية لـ DNS

بينما لا توجد هيئة واحدة تحمل على عاتقها مسئولية كبيرة، فإن موظفي ICANN والمنظمات المساندة واللجان الاستشارية يلعبون دوراً فعالاً في تحسين استقرار وأمن ومرونة DNS على نحو شامل. فمنذ نشأتها، قامت SSAC بتوفير التحليلات والتوصيات إلى مجتمع DNS. SSAC الاستشارية 004 *وتأمين الحافة* قد قدمت تحليل تأسيس ذو صلة بتحديات الأمان لأنظمة معرفات الإنترنت الفريدة[11]. ولقد تضمنت الجهود الرئيسية التحليلات والتوصيات المتعلقة بالهجمات الموزعة لرفض الخدمة (DDoS) الموجهة ضد DNS وتنفيذ DNSSEC الذي أدى إلى إضافة سجلات IPv6 إلى جذر DNS والتشغيل الأولي لاسم النطاق واستضافة التمويه السريع والاستيلاء على اسم النطاق. إضافة إلى ذلك شارك أعضاء SSAC في

[11] SAC 004 *وتأمين الحافة* في تاريخ 17 أكتوبر 2002، http://www.icann.org/en/committees/security/sac004.pdf.

ممارسات مجموعات المضادة للاحتيال (APWG) بلجنة سياسة الإنترنت وقد اتفقوا بشكل مشترك على تخويل العمليات الصحيحة وعلى كيفية استخدام المحتالين لأسماء النطاق الفرعية وكيفية إجراء التنظيم استجابة لهجمات الويب والتعاون مع IPC على دراسة هجمات موقع الويب الخبيثة.

سوف تستمر ICANN في تعزيز هذا الدور من خلال السعي إلى تحديد فرص التعاون على مستوى المجتمع بأكمله والوقوف على المخاطر التي تهدد النظام والعمل على الحد من فداحتها. ولقد بادرت ICANN بجهودها الرامية إلى تحسين مستوى فهم المخاطر التي تهدد DNS على مستوى النظام والعمل على الحد من فداحتها من خلال ندوة المخاطر العالمية التي تواجه DNS التي أقامتها في فبراير 2009 بالتعاون مع مركز جورجيا لأمن المعلومات التقنية (GTISC). ولقد قامت هذه الندوة بتسليط الضوء على فهم المخاطر المرتبطة بـ DNS في المؤسسات الكبرى والتحديات التي تواجه تحقيق عمليات DNS آمنة ومستقرة ومرنة في بيئات الموارد ومواجهة إساءة استخدام DNS للأنشطة الضارة. يتوفر التقرير على موقع الويب http://www.gtisc.gatech.edu/icann09. *عقدت جلسة ثانية عن أمان واستقرار ومرونة DNS في كيوتو في اليابان في تاريخ فبراير 2010، انظر http://dns-srr.e-side.co.jp/ وإعلان التقرير في أبريل 2010 على موقع الويب http://www.icann.org/en/announcements/announcement-26apr10-en.htm.*

فضلاً عما سبق، قام موظفو ICANN والمنظمات المساندة واللجان الاستشارية بالمبادرة بزيادة حجم التعاون مع جهود مجموعة كبيرة من أصحاب المصالح بهدف تحسين قدرة ICANN على إجراء تعديلات فعالة على سياساتها والقيام بمهام التنفيذ التعاقدي وغير ذلك من المبادرات على نحو يتناول تحديات الأمن والمرونة التي يواجهها DNS وتنشأ من خلاله.

5.2.11 صلاحية وحق استخدام وتفرد موارد أرقام الإنترنت.

إن ICANN، من خلال إدارة وظيفة IANA،تطلب الخطة الإستراتيجية ومسئولية أمان واستقرار ومرونة الإنترنت ونظام تحديد العدد من خلال مقدم الطلب والانطلاق ومورد البنية التحتية الرئيسية (RPKI) ونظام توجيه الإنترنت العالمي. وتتغير المسئولية وفق احتياجات تنفيذ الطلب النموذجي من الناحية التقنية لمجال RPKI الفردي الموثوق كما هو ملاحظ من IAB[12] وNRO[13] ويؤدي إلى القدرة على الشهادة بشكل كامل بالصلاحية وحق الاستخدام وتفرد موارد أرقام الإنترنت. وقد أعدت ICANN وفريق عمل ICANN تأثيرات فعلية واقعية للتعامل مع IETF والتركيز على المجموعات الأخرى عبر إشراكها في عملية قياسية والتواصل مع أصحاب المصلحة وتوظيف (الخارج حديثا) في تجربة تنفيذ RPKI.

وتلتزم ICANN بالتعامل مع كل أصحاب المصلحة لـ RPKI وفريق عمل ICANN الذي بدأ العمليات بطريقة تضمن المتطلبات التنفيذية الأكثر مصداقية المعمول بها والمتوفرة لمجتمع الإنترنت في الأوقات الزمنية المناسبة وفق الطلب المعتبر لذلك.

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

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

5.3. التوعية العالمية بالأمان (الاشتراك والتوعية)

5.3.1 الشركاء والأنشطة على المستوى العالمي.

وتعتبر خطة ICANN الإستراتيجية العالمية فيما يتعلق بالأمان والاستقرار والمرونة تستند إلى الشراكة الفعالة مع مجموعة المنظمات. والعديد من تلك الجهود يقودها فريق عمل ICANN وفريق الشراكة. لقد كانت ICANN شريكاً نشطاً في مجموعة كبيرة من المنتديات العالمية المرتبطة بالإنترنت، والتي يتناول العديد منها قضايا أمن واستقرار ومرونة الإنترنت. إن مجموعة الشركاء والأنشطة الواردة أدناه غير شاملة ولسوف تسعى ICANN إلى التعاون مع آخرين عند إتاحة الفرصة لذلك. ومن بين الشركاء العالميين الرئيسيين:

- ***فريق مهمة هندسة الإنترنت (IETF) لجنة الهندسة المعمارية للإنترنت (IAB)*** – تقود الجهود الرامية إلى وضع مناهج تقنية للدفع قدماً بأمن الإنترنت استناداً على تطوير بروتوكولات وإجراءات تشغيلية أكثر فاعلية. تعمل ICANN مع IETF على تأسيس تلك البروتوكولات المرتبطة بالتسمية والتوجيه، وهي تسعى إلى ضمان استخدامها ضمن جوهر عمليات الإنترنت للمساعدة في تأمين بيئة الإنترنت برمتها. وعلى وجه الخصوص، سوف تشارك ICANN في الجهود المبذولة الهادفة إلى وضع بروتوكولات توفر أساس أكثر أمناً للإنترنت استناداً على جهود مثل DNSSEC وRPKI.
- ***مجتمع الإنترنت (ISOC)*** – يعمل هذا المنتدى على تعزيز الوعي بمشكلات أمن الإنترنت والحاجة إلى إرساء الثقة في الإنترنت للقاعدة العامة من المستخدمين، وعلى الأخص في بلدان العالم النامي؛ كما تسعى، بالتعاون مع آخرين، إلى توفير التدريب التقني لتحسين أمن ومرونة الإنترنت. تعمل ICANN مع ISOC للمساعدة في توفير الوعي اللازم وتحسين إمكانيات الأمن والاستقرار والمرونة. تخطط ICANN للتعاون في تطوير برنامج ICANN/ISOC الجاري المشترك لتوفير التدريب لمشغلي TLD لتضمين التدريب التقني حول كيفية تحسين الأمن وتعزيز مقاومة هجمات الإنترنت وتشويشها.
- ***منتدى حوكمة الإنترنت (IGF)*** – يقوم منتدى حوكمة الإنترنت برعاية عدد من الحوارات التي تضم عدداً من أصحاب المصالح والخاصة بأمن الإنترنت والثقة به. كما قام منتدى IGF بتسليط الضوء على إدارة مصادر الإنترنت الحيوية وعلى جرائم الإنترنت. وسوف تواصل ICANN تعاونها مع IGF وذلك من خلال نشر الوعي بدوره في دعم الأمن والاستقرار والمرونة فيما يتعلق بنظام المعرف الفريد للإنترنت والمشاركة في الحوار العالمي الذي يتبناه هذا المنتدى.
- ***DNS–عمليات التشغيل والتحليل ومركز الاستجابة (DNS–OARC)*** – سوف تواصل ICANN دورها كراعٍ داعم ومشارك نشط في كافة أنشطة DNS-OARC.

5.3.2 الشركاء والأنشطة على المستوى الإقليمي

قامت ICANN بعقد روابط إقليمية من خلال مجموعة من الشركاء والأنشطة. وفيما يلي توضيحاً لأهم عناصر الأنشطة الإقليمية لـ ICANN:

- ***اتحادات ccTLD الإقليمية*** – علاوة على المشاركة في برنامج ACRP كما هو موضح أدناه، سوف تواصل ICANN تقديم المساعدة والخبرة للأنشطة التي تخضع لرعاية هذه المنظمات.
- ***مراكز معلومات الشبكات (NICs) لمجموعات مشغلي الشبكات*** – سوف تواصل ICANN مشاركتها في هذه المنتديات لضمان نجاح أنشطتها في توفير

عمليات آمنة ومستقرة على الشبكة على أفضل نحو ممكن، متضمناً ذلك تنسيق أنشطة IANA.

- ***أسيا*** – قامت ICANN بالمبادرة ببرنامج التدريب على أمن ومرونة ccTLD بالتعاون مع اتحاد TLD لدول أسيا المطلة على المحيط الهادئ (APTLD) في مايو 2008 في كوالالامبور. وهي تواصل تلقي دعم قوي للأنشطة التي تتم في هذه المنطقة. وسوف تواصل ICANN المشاركة في المنتديات الإقليمية مثل منتدى العناصر الرئيسية في إدارة مصادر الإنترنت بهدف توفير الاستشارات والتدريب العملي فيما يتعلق بأمن ومرونة DNS مع توافر الفرص السانحة.
- ***أوروبا*** – سوف تستمر ICANN في المشاركة في جهود الهيئة الأوروبية لأمن الشبكة والمعلومات (ENISA) ذات الصلة بـ DNSSEC وبتحسين مرونة DNS كجزء من الجهد الأكبر للمفوضية الأوروبية على صعيد حماية البنية التحتية. سوف تتعاون ICANN كذلك مع مجلس تسجيلات النطاقات الأعلى مستوى القومية الأوروبية لتقديم جلسات تدريبية حول أمن ومرونة ccTLD، والتي تم المبادرة بها بالتعاون مع الاجتماع الثامن والخمسين لـ RIPE في أمستردام والذي عقد في مايو 2009. وسوف تعمل ICANN كذلك على مواصلة شراكتها مع معهد جامعة موسكو لقضايا أمن المعلومات (IISI) بهدف تعزيز الحوار العالمي حول أمن الإنترنت. ولقد قامت ICANN وIISI على وجه الخصوص بعقد ورش عمل في جارميش بألمانيا في الأعوام 2008-2010 بدعم من مركز مارشال الألماني/الأمريكي للدراسات الإستراتيجية ويعتزم الطرفان مواصلة التعاون القائم بينهما.
- ***أفريقيا وأمريكا اللاتينية*** – سوف تواصل ICANN الأنشطة المرتبطة بأمن الإنترنت بالاشتراك مع المنظمات الإقليمية لـ ISOC وكذلك من خلال المنتديات الأخرى المناسبة. وقد قدمت ICANN التدريب على أمن ومرونة ccTLD بالتعاون مع اتحاد LACTLD في الأعوام 2009 و2010.وتعتزم ICANN كذلك تقديم تدريب ccTLD بالتعاون مع الاتحاد الأفريقي لنطاقات المستوى الأعلى (AfTLD) وISOC-Africa. وAPTLD فيأسيا.

5.3.3 العمل مع الحكومات

تتعاون ICANN مع الحكومات في مختلف دول العالم لتحقيق أمن واستقرار ومرونة نظم المعرفات الفريدة للإنترنت. سوف تواصل ICANN توفير منظورها الفني والتشغيلي فيما يتعلق بتحسين أمن واستقرار ومرونة نظم المعرفات الفريدة للإنترنت. وتدرك ICANN إنه يلزم التعامل مع هذه النظم باعتبارها بنية تحتية هامة. ضمن هيكل ICANN، تقوم اللجنة الاستشارية الحكومية (GAC) بتلقي تحديثات منتظمة حول جهود ICANN على صعيد الأمن والاستقرار والمرونة وتقدم معطياتها إلى تلك البرامج كجزء من عملية التخطيط الإستراتيجية. وسوف تظل ICANN تعمل بنشاط لتحديد دورها في المناقشات العالمية الدائرة حول الأمن والمشاركات المعنية بإدارة الأمن والمرونة المرتبطة بنظم المعرفات الفريدة للإنترنت. سوف تتعاون ICANN مع الأمم المتحدة والمنظمات الدولية الأخرى والإقليمية وهي تهدف إلى توحيد الجهود تجاه تمكين الأنشطة الإقليمية المخصصة لتحسين الأمان والمرونة بـ DNS. وسوف تستند تلك الأنشطة إلى المذكرات الإضافية مذكرات التفاهم الموقعة بين ICANN وعدداً من المنظمات. على سبيل المثال سوف تستمر ICANN في المشاركة في المنتديات ذات الصلة بالهجوم الإلكتروني مثل جهود OECD المستمرة للحد من الاستخدام الضار. وسوف تستمر ICANN كذلك في الاشتراك في جهود APEC المشتركة وجهود المنظمات الأخرى بهذه المنطقة.

تقدم GAC كذلك إرشادات إلى ICANN في شكل عواقب باجتماعات ICANN الدولية العامة.

5.4 الاشتراك مع سجلات الإنترنت الإقليمية

اشتراك ICANN مع ASO بالتفاعل على منظمة موارد الأرقام (NRO). ومن خلال التفاعل فإن ICANN تعمل مع RIRs على تمكين ICANN وRIRs للحفاظ وتحسين الأمان والاستقرار والمرونة بالإنترنت لصالح لمستخدمين المحليين والعالميين للإنترنت. ولقد شاركت ICANN مع هذه المنظمات في عدد من الأنشطة ذات الصلة بأمن واستقرار ومرونة الإنترنت. تعمل ICANN بشكل خاص مع تلك المنظمات على توقيع DNSSEC النطاقات الفرعية arpa. بما يتضمن ip6.arpa وin-addr.arpa. وتعمل RIRs على تطوير وسائل لتمكين شهادة عناوين IP وأرقام AS من خلال جهود RPKI. كما أن RIRs مسئولة عن تحديدات ASN وتطلب ICANN الشراكة مع RIRs لتكامل هذه التحديدات. خلال الفترة القريبة القادمة ستقود تلك الجهود تصحيح صالح بين حاملي موارد الأرقام وموارد الأرقام. وهذا النظام التخطيطي يساعد على تحديد أساس تطوير الوسائل لتحييد مسارات بروتوكول مدخل الحدود. وسوف تستمر ICANN في طلب أن تكون شريكا في تلك الجهود.

5.5 عمليات تشغيل ICANN الجماعية للأمان والاستمرار

تحرص ICANN على أن تتسم عملياتها الخاصة بالأمن والاستقرار والمرونة عند تنفيذ IANA وغيرها من الوظائف الرئيسية التي تقوم بها، بصفتها جزء من DNS ونظم المعالجة، وكذاك للإيفاء بمسئوليات الشركة وكمساهم من المجتمع في تحقيق أمن واستقرار ومرونة نظم المعرفات الفريدة للإنترنت. وستمتع ICANN بالأهلية للإجابة بفعالية والعمل بشكل مناسب مع السلطات المناسبة على التقييم الأنشطة التي تخضع للإجراءات الضارة.

وتلتزم ICANN ببرنامج الأمان المستمر للحد من المخاطر بالمعلومات التنظيمية والشخصية والتقييم البدني. في خريف العام 2008 وظفت ICANN مدير علميات الأمن وهو مسئول عن تل ك البرامج. وتقدم ICANN أصول المعلومات والخدمات والتقنية التي تدعم IANA والعمليات الهامة الأخرى. ولعل الجهود الأخيرة التي تركز على إعادة التقييم والتوثيق قد تلعب دورا في عمليات الأمان والسياسات الأخرى. *تم وضع خطة أمن لمعلومات ICANN اعتماداً على معايير ISO 27002 ويتم حالياً إجراء التحسينات على إجراءات/عمليات الدعم. وتتضمن خطة أمن معلومات ICANN كذلك إمداد وزارة التجارة الأمريكية بخطة أمن معلومات IANA وإدارة عمليات التدقيق الخارجية لبرنامجها. يركز تخطيط ICANN البدني والشخصي على حماية منشآت ICANN الشخصية المطلوبة لإجراء مجموعة أنشطة عالمية لـ ICANN لتضمين عملية ضمان الأمان لاجتماعات ICANN العالمية. ولقد قامت ICANN بوضع عملية تخطيط لإدارة المخاطر المرتبطة بالأمان الشخصي مع تعزيز فريق الأمن الداخلي الخاص بها فضلاً عن توفير الدعم من مستشاري الأمن.*

إن البرامج الأمنية الخاصة بـ ICANN تأتي ضمن برنامج شامل لإدارة المخاطر التجارية تم تصميمه من قبل مجلس إدارة ICANN، علاوة على توفير الدعم المتبادل لبرامج استمرارية الأعمال التجارية. تتمتع ICANN بخطة جيدة لإدارة المخاطر مع تأسيس إرشادات إدارة المخاطر للمنظمة وفريق إدارة المخاطر وإجراء تقييمات لإدارة المخاطر بالمخاطر التنظيمية الرئيسية وإدارة المخاطر بمبادرات ICANN الرئيسية.

ومع نمو ICANN، ينمو أساس أصول الشركة إلى جانب نشاطها العالمي وحضورها العام. تستمر ICANN في التأكيد على إدارة المخاطر بشكل جيد والاستمرار التجاري والأمان كأجزاء أساسية للعمليات الرئيسية.

5.6 أنشطة المنظمات الداعمة واللجان الاستشارية لـ ICANN

يلعب مجتمع ICANN الأوسع نطاقاً هو الآخر دوراً رئيسياً في تمكين تحقيق أمن واستقرار ومرونة نظم المعرفات الفريدة للإنترنت من خلال عملية سياسية شاملة. يوجد لدى ICANN ثلاث منظمات داعمة - منظمة دعم الأسماء العامة (GNSO)، المنظمة الداعمة لأسماء رموز البلدان (ccNSO)، منظمة دعم العناوين (ASO)، وهي مسئولة عن تطوير السياسات بحيث تتضمن الموضوعات المرتبطة بالأمن والاستقرار. يمكن الوصول إلى معلومات تفصيلية حول كل منظمة داعمة وعملياتها على مواقع http://gnso.icann.org و http://ccnso.icann.org/ و http://aso.icann.org/. تقدم هذه المنظمات توصياتها والتي يلزم اعتمادها من قبل مجلس إدارة ICANN حتى يتم تنفيذها من خلال عدد كبير من العقود والاتفاقيات ومذكرات التفاهم (MoUs) وأنشطة الموظفين. ومن بين المجالات الرئيسية التي تقع في نطاق سلطة GNSO السياسة المرتبطة بسجل gTLD واتفاقيات المسجلين للتأكد من تضمنها لأي تغيرات تطرأ على السياسة الموضوعة فيما يخص gTLD Whois وفحص القضايا التي تنشأ عن استضافة التمويه السريع وانتهاء صلاحية أسماء النطاقات وعمليات انتقال أسماء النطاقات التي تتم فيما بين المسجلين والسياسات المعنية بإساءة استخدام التسجيل إضافة إلى موضوعات أخرى.

تعمل ICANN حالياً مع المجتمع لمراجعة عملية تطوير سياسة gTLD الحالية (PDP) لجعلها أكثر فاعلية ومقدرة على الاستجابة لاحتياجات تطوير سياسة ICANN. من بين المراجعات العديدة المقترحة لـ PDP الحالية نجد بعض التغييرات التي تهدف إلى جلب المزيد من الخبرة التقنية والبحث وعمليات تقصي الحقائق ضمن العملية للمساعدة في تحديد واستهداف التحديات الصعبة التي تواجه السياسة بطريقة أكثر خبرة؛ علاوة على تطوير سبل أفضل لتقييم مدى فعالية السياسات الجديدة.

تعمل منظمة ccNSO على تيسير تعاون ICANN مع ccTLDs لتضمين مشاركة المعلومات المرتبطة بالأمن والاستقرار والمرونة.

تنسق ASO عملية تطوير السياسة ذات الصلة بالتحديد من جانب IANA لعناوين IP وأرقام AS لـ RIRs. وتطور مجتمعات RIR المنفصلة هذه السياسات العالمية. وهي وظيفة ASO لتطوير تلك السياسات الإقليمية والتنسيق معهم بسياسة عالمية واحدة والتي يتم نقلها فيما بعد إلى مجلس ICANN للتصديق عليها.

إضافة إلى ذلك، فإن ICANN لديها أربعة لجان استشارية لتقديم النصيحة لمجلس الإدارة ومجتمع ICANN: اللجنة الاستشارية لـ At-Large (ALAC) واللجنة الاستشارية الحكومية (GAC) واللجنة الاستشارية للخادم الجذر (RSSAC) واللجنة الاستشارية لشئون الأمان والاستقرار (SSAC). ويمكن الوصول إلى الوظائف المحددة بكل عملية والأنشطة الخاصة بتلك اللجان على موقع الويب http://www.icann.org/en/committees/. عادة ما تتعاون هذه اللجان الاستشارية من خلال هيكل المنظمات الداعمة/اللجان الاستشارية فيما تبذله من مجهود، وعلى الأخص مع SSAC. تلقى هذه اللجان الدعم من فريق سياسة ICANN في إجراء الدراسات وحضور المداولات وتقديم التوصيات.

تقوم SSAC بنصح مجتمع ومجلس إدارة ICANN في الشئون الخاصة بأمن واستقرار نظم التسمية وتخصيص عناوين الإنترنت. وهو ما يتضمن أمور تتعلق بالتشغيل الصحيح والكفء لنظام اسم الجذر وتخصيص العناوين وتعيين أرقام الإنترنت وخدمات تسجيل gTLD والمسجلين مثل Whois. تشترك SSAC في نشاط متواصل لتقييم التهديدات وتحليل مخاطر خدمات التسمية وتخصيص عناوين

الإنترنت للوقوف على مكمن التهديد الرئيسي الذي يواجه الاستقرار والأمن، وبناء عليه تقدم توصياتها إلى مجتمع ICANN. يمكن الوصول إلى تفاصيل حول أنشطة SSAC على موقع الويب www.icann.org/en/committees/security.

علاوة على تلك الأنشطة المذكورة آنفاً، هناك أنشطة أخرى تتم داخل المنظمات الداعمة واللجان الاستشارية والتي تشتمل على مناقشات مشتركة بين هذه المجموعات خلال اجتماعات ICANN حيث يتم طرح موضوعات محل اهتمام مشترك ذات علاقة بالأمن والاستقرار وتنظيم ورش العمل وعرض نبذة حول الموضوعات المتعلقة بالأمن والاستقرار، ونشر الأنشطة المرتبطة بالسياسة بين أعضاء المجتمع من خلال التحديث الشهري للسياسة (http://www.icann.org/en/topics/policy/).

يتضمن عمل سياسة GNSO ما يلي:

Fast Flux (التمويه السريع): وقد اكتملت عملية استضافة تطوير سياسة GNSO (PDP) على التمويه السريع في سبتمبر 2009. وقد استكشف تقرير مجموعة العمل عن المستفيد من التمويه السريع ومن المتضرر وكيفية تأثر مستخدمي الإنترنت بعلمية استضافة الإنترنت السريع والتغييرات التقنية وتغييرات سياسة DNS لتقليل التأثيرات السلبية لعملية استضافة التمويه السريع. تبنى مجلس GNSO التحرك في سبتمبر 2009 لإنشاء فريق يقوم على عمل مسودة لتطوير خطة عمل لتنفيذ التوصيات المقترحة من مجموعة العمل.

عمليات النقل:

يمتلك مجلس GNSO "مجموعة عمل" تركز على جهود تطوير النهج الثاني من الست نُهج المخططة لتناول العناصر المختلفة لعمليات الانتقال الداخلية فيما بين المسجلين. يحدد الجزء ب من مجموعة العمل مهمة تحديد المشكلات الخمس المتعلقة بقرصنة النطاق والعودة الإجبارية للاسم المحول غير المناسب وحالة الغلق. أعلن الجزء ب من مجموعة العمل IRTP عن التقرير الأولي في 29 مايو (http://www.icann.org/en/announcements/announcement-05jul10-en.htm). وتضمن التقرير غير النقاط الأخرى مقترح سياسة حجز نقل النفقات ومقترح لطلب تقرير بالمشكلة على متطلبات Whois لكل gTLDs. وبعد إغلاق فترة التعليق العامة في 8 أغسطس ستراجع مجموعة العمل التعليقات العامة المستلمة وستبدأ العمل على إنهاء التقرير لاعتباره من مجلس GNSO تماما.

إساءة استخدام التسجيل:

مجموعة العمل على سياسة إساءة التسجيل والتي بدأت عملها في فبراير 2009 وكانت مهمتها التدقيق في سياسات الإساءة. وقد نظرت مجموعة العمل على RAP بعين الاعتبار إلى مشكلات مثل تحديد الاختلاف بين الإساءة للتسجيل وإساءة استخدام اسم النطاق وتحديد الإساءة الموجودة وتحديد الفوائد المحتملة أو العوائق لوجود أكثر من طريقة موحدة بالعقد والمناطق المناسبة إن وجدت لتطوير سياسة GNSO لتحديد الإساءة. سلمت مجموعة العمل على RAP تقريرها النهائي إلى مجلس GNSO في 29 مايو 2010 [http://www.icann.org/en/announcements/announcement-29may10-en.htm]. وتضمن التقرير توصيات محددة لتحديد إساءة التسجيل لاسم النطاق في gTLDs. وتضمين عدد من التوصيات ذات الصلة بها:

- *الاحتلال الإلكتروني: التوصية ببدء عملية تطوير السياسة للتحقق من الحالة الحالية لـ UDRP.*

- *مشكلات الوصول إلى WHOIS: البحث عن طرق تضمن إمكانية الوصول إلى بيانات WHOIS بالطرق المناسبة والموثوقة والمتسقة وطلب قسم توافق ICANN لنشر البيانات المتعلقة بإمكانية الوصول إلى WHOIS.*
- *الاستخدام الضار لأسماء النطاق: التوصية بإنشاء الممارسات الفضلى لمساعدة المسجلين والسجلات على تحديد الاستخدام المحظور لأسماء النطاق.*
- *إشعارات التجديد الزائفة: التوصية بإجراءات تعزيزيه من جانب لجنة توافق ICANN.*
- *نظام تسجيل TLD البيني: التوصية بتنسيق مراقبة وبحث مع المجتمع.*
- *توحد العقود: التوصية بإنشاء تقرير للمشكلات لتقييم الحد الأدنى للخط الأساسي لفقرات إساءة التسجيل التي يجب العمل على إنشائها لكافة نطاقات اتفاقيات ICANN.*
- *ممارسات GNSO-الواسعة لتجميع وتمييز الممارسات الأفضل وتوحيد التقارير.*
- *التشغيل التمهيدي*
- *قنص النطاق*
- *أسماء النطاق المخادعة و/أو المسيئة*

وفي ظل اعتبار التوصيات قرر مجلس GNSO أن يشكل فريقا لصياغة واقتراح منهجية للتوصيات المتضمنة بالتقرير والتي تتضمن توقيت تشكيل المجموعات لاعتبار عدد من التوصيات بالتقرير النهائي إلى جانب كيفية التعامل مع تلك التوصيات التي لم تحقق التوافق الجماعي.

استرداد اسم المجال بعد الانتهاء: بدأ مجلس GNSO استعادة اسم النطاق بعد الانقضاء في مايو 2009. وحددت مجموعة العمل تلك الأسئلة ذات الصلة بالمدى الذي يكون فيه المسجلون قادرون على الإدعاء بأسماء النطاق بعد الانقضاء. موضع المناقشة ما إذا كانت السياسات الحالية للمسجلين والمتعلقة بتجديد ونقل وحذف أسماء النطاقات منتهية الصلاحية تُعتبر كافية.

التحسينات على RAA: وافق مجلس إدارة ICANN على اتفاقية الاعتماد المراجعة (RAA) في مايو 2009 (http://www.icann.org/en/topics/raa/). وتتضمن اتفاقية RAA الجديدة استحقاق زائد على المسجلين ومنشآتهم لتحديد المسجلين ممن قد يكونوا متضمنين في الهجمات الإلكترونية والإجراءات الضارة إلى جانب إجراء متطلبات WHOIS المحسنة والالتزامات الخصوصية/البروكسي للمزودين لها ومتطلبات أخرى لتحديد نقاط الإساءة بالعقد لحالات الاستخدام الضار والمتضمنة لـ DNS. *اشتراك كل من ممثلين تعزيز القانون ALAC ومجموعات أصحاب المصلحة الآخرين في طلب التحسينات على RAA (انظر http://www.icann.org/en/announcements/announcement-28may10-en.htm) وتقديم اقتراح بالتعديلات في اجتماع ICANN في بروكسل في يونيو 2010.*

بيانات التسجيل الدولية: في الوقت الحالي لا توجد معايير أو إرشادات تحدد كيفية فرض بيانات التسجيل الدولية للنطاق وعرضها. تم حث مجموعة العمل المشتركة لـ SSAC-GNSO على العمل مع مجلس إدارة ICANN على دراسة مناسبة

وإمكانية تقديم مواصفات العرض للتعامل مع بيانات التسجيل الدولية. وستدعم المجموعة إدراج الإدخالات من الأطراف المهتمة بما يتضمن مشغلي ccTLD وCCNSO وASO وALAC وGAC خلال المناقشات لضمان الإدخال المجتمعي الموسع. ومجموعة الهداف الأولية لمجموعة عمل IRD لنيل التفاهم وتحقيق التوافق على الأنواع والأشكال وحالات التشفير لبيانات التسجيل للأطراف المتعاقدة للتجميع والعرض والحفاظ على المحتوى.

6. خطط ICANN للعام المالي 2011 المعنية بتحسين الأمن والاستقرار والمرونة

دليل عمليات التخطيط الإستراتيجي والتشغيلي لأنشطة ICANN ذات الصلة بتحسين الأمان والاستقرار والموارد اللازمة لتحديد تلك التأثيرات. في العام المالي 2011، ستتضمن أنشطة ICANN عددا من المبادرات الرئيسية مثل:

- ***عمليات تشغيل IANA*** – الدعم والتعليم والإعداد لتنفيذ CDNSSE على مستوى الجذر كما دعت إليه خطة ICANN الإستراتيجية 2010-2013 بالإضافة إلى تحسين إدارة منطقة الجذر من خلال العمل الآلي التام وتحسين مصادقة الاتصالات مع مديري TLD.
- ***عمليات خادم جذر DNS*** – مواصلة السعي لتحقيق إقرار متبادل للأدوار والمسئوليات والمبادرة بجهود تطوعية لتنفيذ تخطيط وتدريبات الطوارئ.
- ***سجلات gTLD*** – ضمان تقييم مقدمي الطلبات لـ gTLD الجديدة وIDN مع الاستمرار في تقديم عمليات آمنة. وسوف تعمل ICANN على تطوير خطة استمرارية تسجيل gTLD واختبار نظام مستودع البيانات.
- ***سجلات ccTLD*** – سوف تسعى ICANN لتحسين سبل تعاونها على صعيد تطوير البرنامج المشترك للتخطيط للاستجابة للهجوم ولحالات الطوارئ (ACRP) الذي تم إنشاؤه بالاشتراك مع ccNSO واتحادات TLD الإقليمية.
- ***التوافق التعاقدي Contractual Compliance*** – ستواصل ICANN جهودها الرامية إلى تحسين نطاق أنشطة التنفيذ التعاقدي المشتملة على gTLDs بحيث تتضمن كذلك بدء عمليات تدقيق للأطراف المتعاقدة كجزء من تنفيذ تعديلات مارس 2009 لاتفاقية اعتماد المسجل (RAA) والوقوف على المشاركة المحتملة للأطراف المتعاقدة في النشاط الضار لاتخاذ إجراء للالتزام.
- ***الاستجابة للاستخدام الضار لنظام اسم النطاق*** – سوف تزيد ICANN من جهودها الحثيثة فيما يخص السلوك الضار الذي يتيحه استخدام DNS مع تسهيل مشاركة المعلومات لتمكين الاستجابة على نحو فعال.
- ***عمليات الاستمرار والأمان المشترك لـ ICANN*** – سوف تعمل ICANN على ضمان البرامج الآمنة واتصالها مع المخاطر المشتركة من الإدارة وإدارة الأزمات وبرامج استمرار الأعمال التجارية. وسوف يقع ضمن بؤرة الاهتمام تنفيذ أساس قوي من الخطط الموثقة والإجراءات الداعمة.
- ***ضمان التعاون والمشاركة العالمية*** – سوف تستمر ICANN في العمل على تحسين الشراكات لتضم فريق عمل *هندسة الإنترنت* (IETF) ومجتمع الإنترنت (ISOC) وتسجيلات الإنترنت الإقليمية ومجموعات مشغلي الشبكات ومركز عمليات وتحليل واستجابة DNS والذي يشار إليه بـ (DNS-OARC) ومنتدى فريق الاستجابة للحوادث (FIRST). كما تشارك ICANN في الحوارات العالمية الرامية إلى تعزيز فهم تحديات الأمن والاستقرار والمرونة التي تواجه النظام البيئي للإنترنت وكيفية مواجهة هذه التحديات بالاستعانة بالمناهج التي تضم العديد من أصحاب المصالح.

يتم فيما يلي توضيح المجموعة الكاملة من الأنشطة. يستعرض الملحق أ تفاصيل حول الأهداف الخاصة والشركاء والنتائج ومخصصات الموارد خلال العام المالي 2011.

6.1 وظائف DNS/التوجيه الرئيسية

6.1.1 عمليات IANA

سوف تواصل ICANN تنفيذ وظائف IANA والعمل على تحسين التفوق التشغيلي لهذه العمليات بالتعاون مع وزارة التجارة الأمريكية وVeriSign وRIRs ومشغلي TLD.

تتضمن مبادرات تحسين وظائف IANA الأخرى المحددة:

- تحسين إدارة منطقة الجذر من خلال الأتمتة (برنامج RZM/eIANA)، وتحسين مصادقة الاتصالات مع مديري TLD؛ ومراجعة العمليات والإجراءات الخاصة باعتبارات الأمن والتحسين.
- دعم تطوير وتنفيذ تخصيصات وتعيينات عنوان IP آمن من خلال RPKI أو غيرها من الآليات المتبناة من قبل RIRs ومجتمع توجيه الإنترنت بحيث تتضمن الدعم المتواصل لمجموعة عمل مستودع بيانات مخابرات الأمن (SIDR) الخاصة بـ IETF.
- العمل مع المجتمعات التقنية والتشغيلية لتحديد وتحليل وتنفيذ المتطلبات أو المعايير التقنية الإضافية اللازمة لتحسين أمن واستقرار ومرونة DNS.

كجزء من التحسينات على المرونة الإجمالية عقدت ICANN تدريب لمجتمع IANA في يناير 2010 واختبرت خدمات IANA من مارينا ديل راي في كاليفورنيا إلى روسترفي فرجينيا. ووضح التدريب الأخير إمكانيات وقدرات IANA وآليات التواصل لضمان توفر خدمات IANA. سوف تعمل ICANN على تحسين مرونة خدمات IANA في الأعوام 2010-2011.

6.1.2 عمليات DNS

حققت ICANN ووزارة التجارة بالولايات المتحدة الأمريكية وVeriSign تقدما كبيرا في 2010 بشأن تنفيذ DNSSEC بمنطقة الجذر. لكل أولوية محددة في الأعوام 2010–2013 والتخطيط الإستراتيجي حيث تستمر ICANN في جهودها لدعم تقديم DNSSEC من مشغلي TLD والآخرين في العام المالي 2011.

وسوف تعمل ICANN على دفع نطاق كبير من الأنشطة لتمكين التنفيذ الموسع لـ DNSSEC في كل أرجاء DNS على مستوى العالم وتجميع خبرات DNS ومشغليهم ذوي الخبرة. ستعمل ICANN على التأكد من أن برامجها التي تتضمن عمليات الانتقال الداخلية فيما بين المسجلين ومستودع البيانات تؤدي إلى عمليات التنفيذ واستمرار مناقشات أصحاب المصالح حول التنفيذ. وستواصل ICANN متابعة مستودعات الائتمان لنطاقات المستوى الأعلى (ITAR) حتى يتم توقيع منطقة الجذر. وستستمر ICANN في السعي للحصول على تخويل لتوقيع مناطق int. وarpa. ستواصل ICANN دعم تنفيذ DNSSEC من خلال تعيين المناطق المدارة من قبل ICANN (متضمنة icann.org وiana.org)؛ وإدارة الاختبارات وتسهيل جهود استنباط الدروس المستفادة بين هؤلاء المشتركين في تنفيذ DNSSEC.

كذلك تسعى ICANN إلى تمكين وضع آليات أكثر فاعلية للتنسيق باعتبارها جزء من مجتمع مشغلي الجذر فيما يتعلق بالتدابير التي من شأنها المساهمة في تحقيق الأمن والاستقرار والمرونة. هذا وتعتزم ICANN، من خلال دورها كمشغل L، التعاون مع مشغلي الجذر الآخرين في المبادرة بجهود تطوعية لإجراء التخطيط والتدريبات

اللازمة لتحسين مرونة نظم خادم الجذر في مواجهة مجموعة من الحالات الطارئة الحرجة.

تخطط ICANN لمواصلة تحسين تشغيل الجذر L. ولقد تعاقدت ICANN مع DNS-OARC لدراسة تأثير التغيرات متضمنة تنفيذ gTLDs وIDNs جديدة وتنفيذ IPv6 والتنفيذ المحتمل لتعيين NSSECD لمنطقة الجذر عند تشغيل عملية خادم جذر واحدة بناء على نموذج الجذر L. وعلى نحو أوسع نطاقاً، تقوم كل من RSSAC وSSAC بإجراء دراسة مشتركة حول أمن واستقرار خادم الجذر في ضوء التغيرات المتصورة والمفصلة في القسم 6.6 أدناه.

6.2 العلاقات مع تسجيلات ومسجلي DTL

6.2.1 سجلات gTLD

سوف تواصل ICANN التنسيق التعاقدي المرتبط بعمليات gTLD ليتضمن تطبيقات فحص الخدمات الجديدة عبر RSEP. بمجرد أن تصبح عملية gTLD قابلة للتشغيل فإن ICANN تتوقع المراجعات لتضمين المقترحات التي تطالب بتنشيط RSTEP لتقييم الأمان والاستقرار والمرونة. ولسوف تواصل ICANN جهودها الرامية إلى تشجيع تعاون المجتمع واستخدام أفضل الممارسات المرتبطة بالأمن والاستقرار والمرونة من خلال عقد ورش عمل التسجيل/المسجل الإقليمية التابعة لـ ICANN والمشاركة في مجموعة من منتديات المجتمع ومشاركة المعلومات على موقعها الخاص. في عام 2010، قدمت ICANN الإعلام عن البيانات حول سجلات gTLD بلوحة البيانات لاستخدام المجتمع (http://www.icann.org/idashboard/public/).

6.2.2 gTLDs الجديدة

إن التنفيذ المحتمل للعمليات المرتبطة بإنشاء gTLDs جديدة إنما من شأنه توفير عناصر الأمن والاستقرار والمرونة الأولية خلال العام القادم. وفي فبراير 2009، أوكل مجلس إدارة ICANN إلى RSSAC وSSAC مهمة المشاركة في دراسة المقتضيات المحتملة للأمن والاستقرار والمرونة بالنسبة لنظام خادم الجذر على نحو مجمل، مع النظر إلى سلسلة من التغيرات المحتملة داخل DNS، والتي تتضمن تنفيذ gTLDs وIDNs جديدة، علاوة على التنفيذ المحتمل لتعيين DNSSEC لمنطقة الجذر. ويُتوقع الإطلاع على التقارير الخاصة بهم في 2010. كجزء من عملية gTLD الجديدة سوف تقوم ICANN كذلك بتأسيس فقرات لتقييم مقدمي الطلبات لضمان إمكانية تنفيذهم للعمليات المؤمنة تقنيا والمتوافقة مع فقرات Whois والتي يمكن أن تقدم تخطيط طوارئ جيد وسليم مع ضمان حماية المسجلين. وسوف تواصل ICANN جهدها في خطة استمرار سجل gTLD وبرنامج التدريب. سوف تضمن ICANN كذلك الوضع والتشغيل الآمن لنظام مقدمي طلبات TLD الآلي.

6.2.3 IDNs

وفي اتجاه مماثل، سوف تعمل جهود ICANN المعنية بتمكين تنفيذ IDN TLDs (ccTLDs وgTLDs) على ضمان أمن واستقرار ومرونة تمثيل أسماء النطاقات الجديدة بحروف اللغة المحلية. تدعم ICANN العمل على تحديث إرشادات IDN ليتم إتباعها من مشغلي IDN TLDs وتشغيل IDNs من المستوى الثاني. وستواصل ICANN تسهيل جهود التسجيلات في العمل مع الموردين بهدف ضمان وضع جداول

IDN تعمل على الحد بقدر المستطاع من حالات التعارض والتشويش بين السلاسل والحد من فرص إساءة استخدام النظام للأغراض الضارة. كذا سوف يتم توفير وظيفة دعم قائمة على IDN لهؤلاء الأطراف المهتمين في أن يكونوا مشغلي IDN TLD وفي حاجة إلى المساعدة والخبرة في هذا المجال.

تشترك ICANN كذلك مع الخبراء على ضمان تقديم IDN TLDs للدول والمناطق التي لها أكثر من لغة أو حروف وتحتاج إلى تنفيذ متزامن. وتتضمن كذلك التعاون مع أصحاب المصلحة مثل برامج المتصفح ومطوري البرامج والطلبات ومشغلي سجل IDN وآخرين على دعم تقديم IDNs.

6.2.4 ccTLDs

ستواصل ICANN جهودها الرامية إلى تحسين أمن واستقرار ومرونة ccTLD من خلال التعاون مع مشغلي ccTLD. وسوف تركز هذه الأنشطة خلال العام المقبل على تطوير برنامج ورشة عمل التخطيط للاستجابة للهجمات ولحالات الطوارئ (ACRP) الذي تم وضعه بالتعاون مع ccNSO واتحادات TLD الإقليمية. ويركز البرنامج على تحسين الأمن والمرونة من خلال التخطيط التقدمي وتوفير إمكانيات قوية للاستجابة لمجموعة كاملة من التهديدات والمخاطر المشوشة. ولسوف يمتد هذا البرنامج حتى العام المقبل لتتضمن تدريب تقني لتحسين مستويات الأمن والمرونة في الاستجابة للتهديدات المتقدمة ولتقديم المساعدة في تطوير برامج التدريب *والتقييم* لصالح التخطيط لأمن وطوارئ تخطيط الأمان وحالات الطوارئ.

6.2.5 المسجلون

ينظر المجتمع بعين الاعتبار إلى التحسينات على اعتماد المسجل لمستودع البيانات والمتطلبات الخاصة به من خلال التحسينات على RAA. وإضافةً إلى دعم هذه الجهود، سيواصل موظفو ICANN تطوير إجراءات وعمليات أخرى داخل نطاق أطر العمل التعاقدية والسياسية لحماية مالكي أسماء النطاقات وتحسين أمن واستقرار ومرونة DNS بشكل مطلق. وتجدر الإشارة على وجه الخصوص إلى إنه جاري العمل حالياً على إحكام إجراءات طلب الاعتماد ووضع متطلبات صارمة لأهلية RAA وقواعد الاستبعاد، إلى جانب وضع إجراءات تسمح للمسجلين بالخروج من سوق التسجيل بطريقة مسئولة. كما أن العمل السابق في تطوير إجراءات إنهاء مستودعات البيانات والمسجلين سوف يؤدي هو الآخر إلى تعزيز جهود ICANN المتواصلة والمستقبلية لفرض الالتزام، مما يسمح بإنهاء اعتماد المسجلين في الحالات التي تمثل فيها أعمال المسجل تهديداً لأمن واستقرار DNS. ستواصل ICANN إنشاء مجتمع مسجلين قوي من خلال الأحداث الهامة التي تتيح مشاركة أفضل ممارسات الصناعة، كما ستبدأ في إنشاء قنوات اتصال جديدة لمساعدة المسجلين على الإبلاغ عن التهديدات الأمنية الحرجة والاستجابة لها في الوقت المناسب.

6.2.6 التوافق التعاقدي

سوف تستمر ICANN في زيادة نطاق أنشطة تعزيز التوافق التعاقدي. وستتضمن الأنشطة مراجعات للأطراف المتعاقدة كجزء من عملية تنفيذ RAA لعام 2009. علاوةً على ذلك، سوف يعمل فريق الالتزام التعاقدي بالتعاون مع فريق أمن ICANN لتحديد الأطراف المتعاقدة الذين قد يكونوا مشاركين في أنشطة ضارة. في تلك الحالات التي يثبت فيها مشاركة الأطراف المتعاقدة في أنشطة ضارة، قد يتم اتخاذ إجراءات لفرض تنفيذ العقد. وفي جميع الحالات الأخرى، سوف يتم إخطار هيئات تطبيق القانون أو الهيئات الأخرى المعنية لتتخذ من جانبها الإجراءات اللازمة.

لقد قام قسم التوافق التعاقدي بدراسة سبل تقييم دقة معلومات الاتصال في بيانات Whois ضمن نظام gTLD وقام بتقييم حدود استخدام أصحاب أسماء النطاقات لخدمات الخصوصية والبروكسي لإخفاء هويتهم. وسعياً منها للتشجيع على التوافق التعاقدي واكتساب الثقة العامة، يقوم قسم الالتزام التعاقدي بتطوير نظام لتحديد الأطراف الشاكية علنياً. ولازال هذا النظام في مراحل التطوير الأولى، سوف تتم استشارة مجتمعات المسجلين والتسجيلات قبل الشروع في تطبيقه.

6.2.7 الاستجابة الجماعية لحالات الإساءة الضارة بنظام اسم النطاق

سوف يواصل موظفو ICANN كذلك تعزيز الجهود المشتركة التي نشأت استجابة للأحداث الأخيرة التي تضمنت نظام اسم النطاق منذ أواخر عام 2008، مثل الأنشطة المحيطة بشبكة سزيربي الإلكترونية للاختلاس ودودة كونفيكر التي ظهرت في أواخر عام 2008/ومطلع عام 2009. هذا وترى ICANN ضرورة أن يتضمن هذا التعاون مشاركة تسجيلات ومسجلي DNS، ومجتمع أبحاث الأمن ومزودي البرامج وتقنيات مكافحة الفيروسات. وعلى نحو خاص، تعتزم ICANN التعاون مع مجتمعات التسجيلات والمسجلين لتعزيز المناهج التعاونية لمكافحة انتشار البرامج الضارة والديدان وشبكات الاختلاس الإلكترونية التي تستغل DNS للانتشار وفرض سيطرتها. ولسوف تسعى ICANN إلى وضع إجراءات محددة لتوصيل واعتماد أنشطة التسجيلات والمسجلين وكذلك لتحدد كيفية إسهامها في مشاركة المعلومات مع الباحثين في مجال أمن الإنترنت ومزودي التقنيات وجهات تطبيق القانون حسبما يستلزم الأمر. وستقدم ICANN تعليقاً عاماً على هذه الإجراءات لإجراء أنشطة استجابة تعاونية. سيتم تقديم هذه الإجراءات للمجلس بغرض الموافقة عليها. إن هذه المناهج من شأنها ضمان قدرة ICANN على الاستجابة لكافة أصحاب المصالح على المستوى العالمي الذين قد يطلبون مشاركتها وتعاونها.

6.2.8 تمكين الأمان الإجمالي لـ DNS

سيسعى فريق عمل ICANN إلى التركيز على الندوات المنعقدة في فبراير 2009 وفبراير 2010 حول أمن واستقرار ومرونة DNS وذلك من خلال مؤازرة الجهود المشتركة الرئيسية المرتبطة بالحد من المخاطر التي يواجهها مشغلو ومستخدمو DNS. هذا وتشتمل الخطط على عقد ندوة سنوية لمراجعة المخاطر التي تواجه DNS على وجه العموم وتحسين فرص التعاون مع التركيز المتواصل على مواجهة تحديات ضمان أمن واستقرار DNS في العالم النامي. كما تخطط ICANN إلى التعاون مع DNS-OARC ومع منتدى الاستجابة للحالات الطارئة والأمن (FIRST) مع التركيز على سبل صياغة استجابات فعالة للحالات الطارئة والأحداث الهامة داخل مجتمع DNS. علاوةً على ذلك، سوف يواصل موظفو ICANN تعقب تطور خطط وضع نظام لتسمية الموضوعات (ONS) وكيف يمكن لهذه الخطط أن تتضمن DNS لضمان سرعة تحديد المشكلات المحتملة المرتبطة بالأمن والاستقرار والمرونة.

6.3 التوعية بالأمان على المستوى العالمي

6.3.1 تمديد الشراكات القائمة

يعتبر جوهر إستراتيجية المشاركة العالمية لـ ICANN فيما يتعلق بالأمن والاستقرار والمرونة هو بناء واستخدام العمل القائم بواسطة الشراكة العالمية والتوسيع الإضافي

القوي للشراكة. وتتضمن الأنشطة المحددة المخططة للعام المالي 2011 مع الشركاء ما يلي:

- ***مجتمع الإنترنت:*** تخطط ICANN للتعاون في تطوير برنامج ICANN/ISOC الجاري المشترك لتوفير التدريب لمشغلي TLD لتوفير التدريب الفني حول كيفية تحسين الأمن وتعزيز مقاومة هجمات الإنترنت وتشويشها.
- ***DNS-OARC*** – سوف تستمر ICANN في التعاون مع DNS-OARC وأصحاب المصلحة الآخرين المهتمين بالأمر لدعم مبادرات SSR ومفهوم DNS-CERT. كما اشتركت ICANN أيضاً مع منظمات من أجل التدريب والتثقيف حول الشراكة مع الآخرين لتحسين فهم وظائف نظم المعرف الفريد ودور ICANN والتحديات الخاصة بإدارة المخاطر التي تواجه هذه النظم.

6.3.2 المؤسسات التجارية

ستقوم ICANN بمتابعة الندوة المنعقدة في فبراير 2009 و2010 حول أمن واستقرار ومرونة DNS حول فهم مرونة المؤسسة والمخاطر المقترنة بـ DNS. وخلال العام القادم، سيتم تضمين الجهود المبذولة للأمن والاستقرار والمرونة كجزء من برنامج ICANN CEO الذي يسعى نحو مشاركة نطاق واسع من الشركاء المحتملين.

6.3.3 المشاركة في الحوار عن الأمان الإلكتروني على مستوى العالم

ستشترك ICANN في هذه الحوارات سعياً وراء ضمان وجود فهم واضح لدورها الأساسي ومساهماتها. وتتضمن الأنشطة الخاصة التي تتوقعها ICANN خلال العام القادم:

- ***منتدى فرق الاستجابة للحالات الطارئة والأمن (FIRST)*** – عقدت ICANN وFIRST ورشة علم مشتركة في نيروبي cحول الهجمات الإلكترونية في دولة كينيا في مارس 2010 لفرق الاستجابة للحالات الطارئة في أفريقيا. وتتعاون ICANN مع FIRST في استبيان حول فرق الاستجابة لحالات الطوارئ في العام المالي 2011 مع المشاركة في برامج FIRST.
- ***الشبكة الأوروبية ووكالة أمن المعلومات (ENISA)*** – تخطط ICANN للتعاون مع ENISA في أوروبا بشأن الهجمات الإلكترونية وأنشطة الاستجابة للحوادث في حالة الطوارئ.
- ***منتدى حوكمة الإنترنت (IGF)*** – سوف تشارك ICANN في اجتماع IGF في فيلنيوس في ليتوانيا في سبتمبر 2010 كما ستدعم استمرار IGF من الجمعية العامة للأمم المتحدة.

وستقوم ICANN بالسعي الحثيث وراء الفرص المتاحة مع مفكرين آخرين ومؤسسات أكاديمية أخرى للتعاون من أجل زيادة تحديد المخاطر المتعلقة بالأمن والاستقرار والمرونة.

تخطط ICANN للاستمرار في التعاون مع ASO (ومن خلال ASO وNRO و RIRs) وللمشاركة في الأنشطة ذات الاهتمام المشترك المتعلقة بالأمان والاستقرار والمرونة. وسوف يسعى موظفو ICANN نحو إشراك NRO في تحديد أي الأنشطة المشتركة يلزم تحسينها حتى يتسنى ضمان أمن واستقرار ومرونة DNS. سوف تشتمل هذه المناقشات على فهم نوايا NRO فيما يتعلق بما هو محتمل من إساءة

استخدام مساحة عنوان IPv4 وإمكانية الحاجة إلى وجود سياسة عالمية لمواجهة المشكلات التي يتم تحديدها.

6.4 عمليات تشغيل ICANN الجماعية للأمان والاستمرار

سوف يحرص موظفو ICANN على أن يتم تنفيذ برامجها الأمنية ضمن إطار إدارة المخاطر التجارية الشاملة وإدارة الأزمات وبرامج الاستمرارية التجارية. ويستمر التركيز الأكبر على تأسيس أساس سليم من السياسات الموثقة والعمليات ودعم الإجراءات. تركز المبادرات الحديثة على التحسينات على إدارة مستوى المخاطر ICANN وإجراء الاستمرار بما يتضمن إنشاء خطط إدارة الأزمات التجارية الرسمية لـ ICANN وإجراء ممارسات ICANN الخارجية بالتوافق مع الأنشطة الأخرى لتضمين ممارسات استمرار gTLD وحالات الإعداد للاجتماعات. وقد بدأت CANNI استخدام مواقع عمليات التشغيل البديلة الموزعة ماديا لتحسين استمرار الممارسات التجارية وإمكانيات التعافي من الأزمات للبنية التحتية لـ ICANN.

وكجزء من عمليات التشغيل المستمرة في العام 2010، يستمر فريق عمل ICANN في العمل على تحسين التوازن الكامل للبنية المعلوماتية والعمليات الشخصية وعمليات الأمان كذلك. وكما هو الحال مع إدارة المخاطر والتخطيط للاستمرارية، سيكون التركيز الأكبر على وضع أساس سليم للخطط الموثقة وإجراءات الدعم. وتتضمن المبادرات المحددة لتحسين أمن ICANN خلال منتصف عام 2010- وجود تحسينات على عناصر التحكم وتغيير ومراجعة حالات تسجيل الدخول وإجراءات نسخ البيانات احتياطيا والتدريب والتوعية لفريق العمل واستمرار عمليات الاستجابة لحالات الطوارئ وإمكانيات الاستجابة والتحسينات على خدمة المحمول بأمان. خطط الأمان الموثقة لاجتماعات ICANN العالمية والشخصية التي تم الإعداد لها والتحقق من الخارج وجدولة مراجعة الخطط وكل ذلك تم تحديد مواعيده في آخر العام 2010. ستضمن ICANN تطوير تعاون المجتمع الناشئ والتوعية بأدوات تكنولوجيا المعلومات وتوزيعها باستخدام عناصر تحكم الأمن المناسبة في مكانها.

كما تخطط ICANN أيضاً للحصول على مراجعة خارجية وتدقيق لبرامج الأمن والمتابعة الخاصة بها خلال النصف الثاني من 2010.

6.5 دعم ICANN للمنظمات واللجان الاستشارية

تخطط SSAC إلى تركيز جهودها القادمة حول توزيع DNSSEC وحماية تسجيل النطاق والحد من إساءة استخدام أسماء النطاقات واستقرار نظام العناوين.

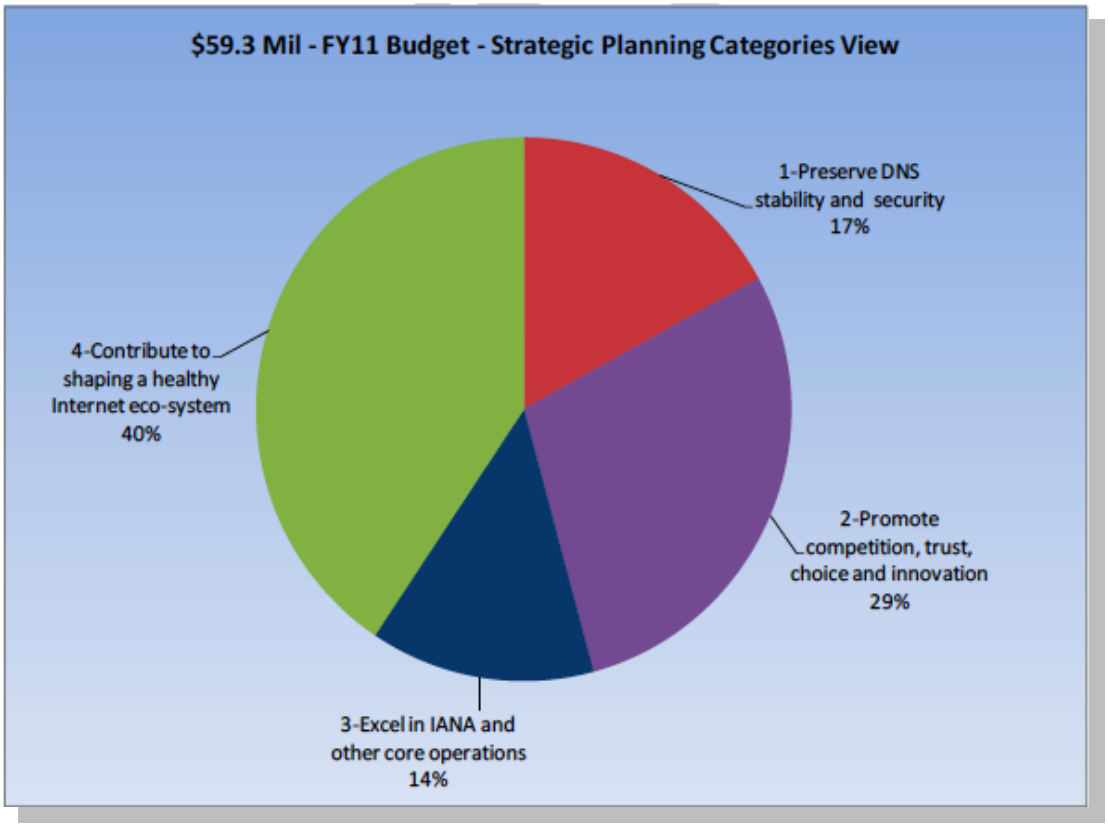
في يناير 2009 أصدر مجلس GNSO تقريرا أوليا خاص باستضافة التمويه السريع للتعليق العام وإجراءات المجلس الإضافية واعتبار الدراسات المحتملة الهائلة لدراسات Whois ذات الصلة. يمتلك مجلس GNSO "مجموعة عمل" تركز على جهود تطوير النهج الثاني من الست نُهج المخططة لتناول العناصر المختلفة لعمليات الانتقال الداخلية فيما بين المسجلين. ولقد اجتمعت GNSO "مجموعة عمل" لمواجهة إساءة استخدام التسجيل وهي تقوم حالياً بدراسة مبادرة ذات صلة باستعادة اسم النطاق بعد انتهاء صلاحيته. ومن أجل الجمع بين ذلك العدد الكبير من أصحاب المصالح في ICANN المهتمين بهذه الموضوعات، تضمنت الاجتماعات العامة العالمية لـ ICANN التي انعقدت سابقا وامتدت موضوعاتها لتشمل عدد من ورش العمل تناولت الجرائم الإلكترونية وسوء استخدام التسجيل (مكسيكو سيتي وسول ونيروبي وبروكسل).

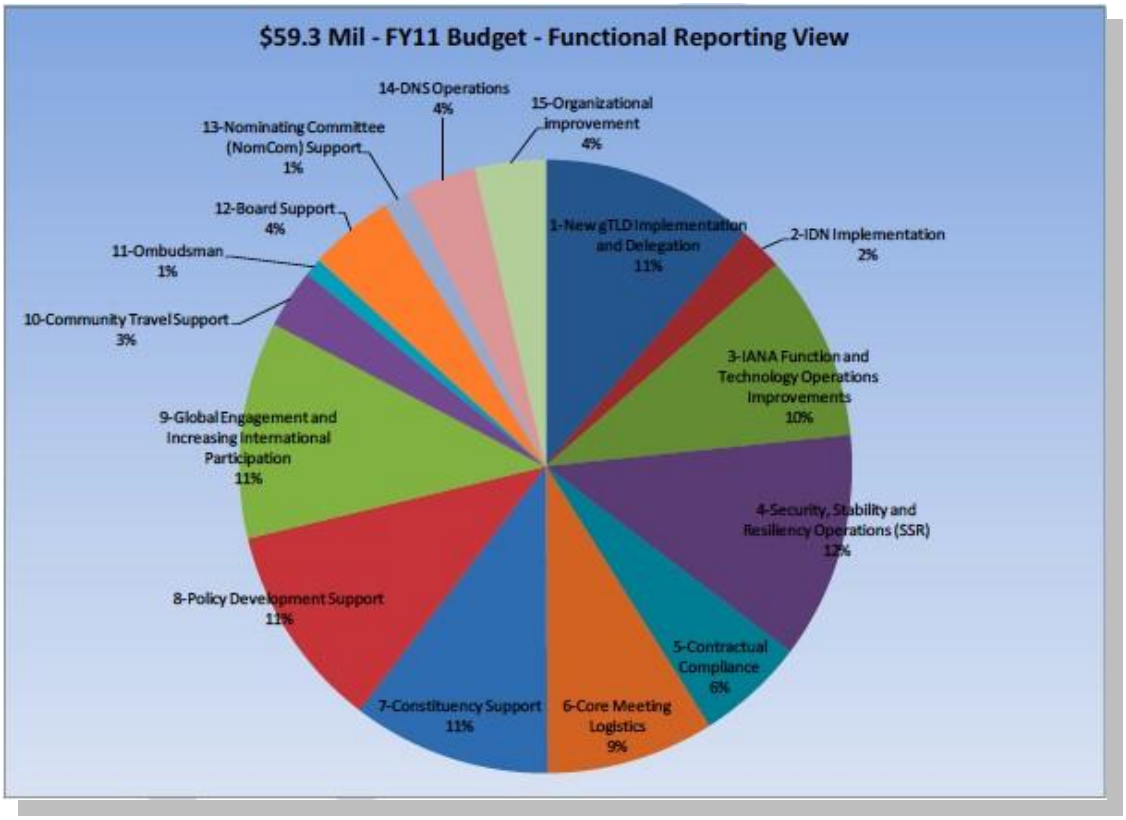
7. الخاتمة

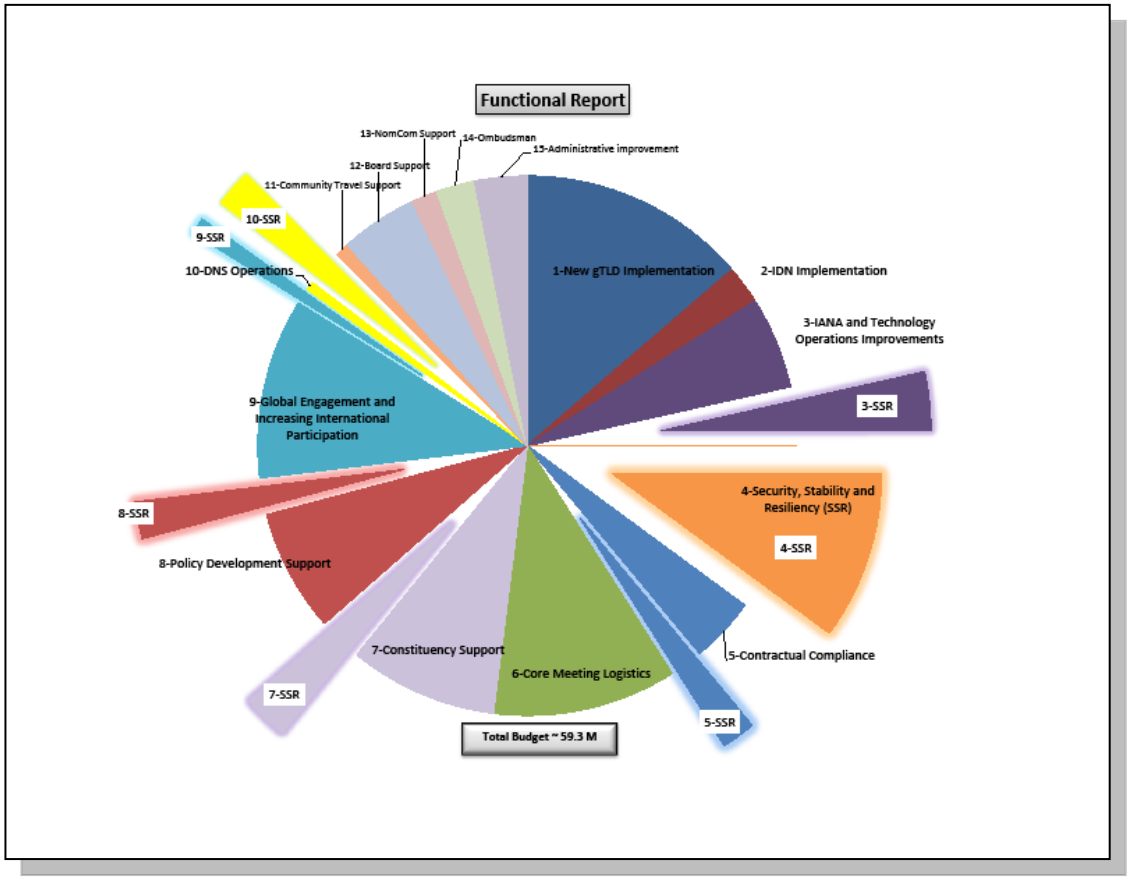
تفهم ICANN، كناحية هامة من مهمتها في كسب ثقة العامة، أن برامجها وأنشطتها يجب أن تساهم في جعل نظم التعريف الفريدة من الأهداف الفريدة للحصول على بيئة إنترنت أكثر أماناً واستقراراً ومرونة. ومع تزايد التحديات، أصبحت جهود ICANN في هذا المجال أصبحت أكثر خشونة. كما تعترف ICANN أيضاً بحدود دورها ومواردها وتضع خطة لإستراتيجيتها في هذه المجال للاعتماد بشدة على لاعب واحي للتعاون. ولقد تم التعرف بالإنترنت كبيئة عالمية تنمي الابتكار وتعتمد على تعاون أصحاب المصالح المتعددين. تساهم ICANN في تحسين أمن واستقرار ومرونة نظم المعرف الفريد الخاصة بها بالاعتماد على نفس المنهج.

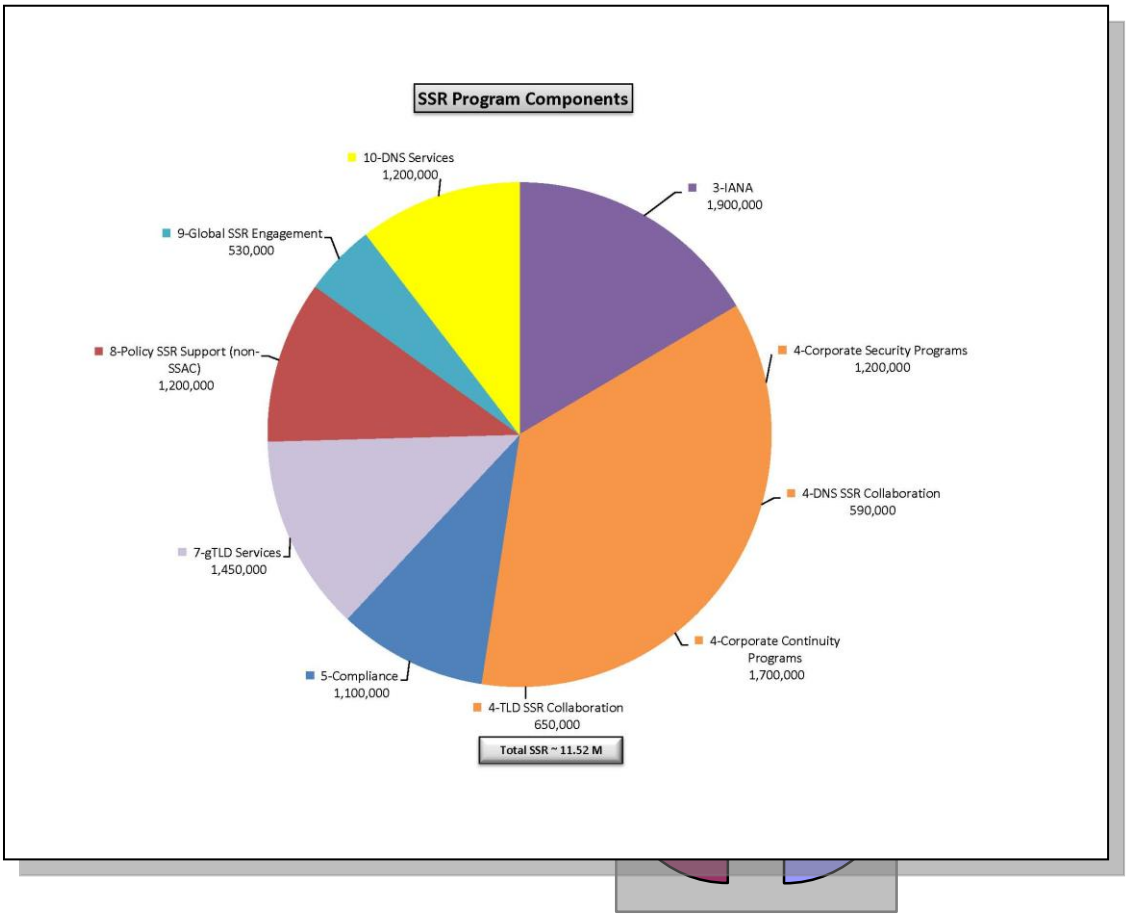
قامت ICANN منذ تأسيسها بتوفير الكثير من البرامج والأنشطة الخاصة بتحسين أمن واستقرار ومرونة الإنترنت والتي تتضمن الكثير من الجهود المرتبطة بوظائف التوجيه الرئيسية؛ والعمل مع ومجتمعات تسجيلات ومسجلي TLD؛ والاشتراك مع NRO وRIR؛ برامج الأمن التجاري وبرامج الاستمرارية؛ الأنشطة الخاصة بالمنظمات الداعمة واللجان الاستشارية؛ والمشاركة في الأنشطة المعنية بأمن واستقرار الإنترنت على المستوى الإقليمي والعالمي. ويهدف الجزء الأول من هذا الإصدار إلى الخطة إلى توفير أساس لصياغة دور ICANN وإطار العمل الذي تقوم ICANN من خلاله بتنظيم جهودها المتعلقة بالآمن والاستقرار والمرونة. وستتطور الخطة مع مرور الوقت كجزء من عملية التخطيط الإستراتيجي والتشغيلي لـ ICANN مما يسمح لجهود ICANN بالبقاء ذات صلة وشيكة ولضمان تركيز الموارد على أهم المسئوليات والمساهمات الخاصة بها.

الملحق أ – موارد العام المالي 2011 لـ SSR




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


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
5-Contractual Compliance
7-Constituency Support
6-Core Meeting Logistics
7-SSR
5-SSR
Total Budget ~ 59.3 M


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

نظرة عامة على المكونات الرئيسية لبرنامج الأمان والاستقرار والمرونة (SSR) الخاص بـ ICANN

- IANA - 1.9 مليون دولار
- خدمات DNS - 1.2 مليون دولار
- تصمين DNS في برنامج SSR– 590 ألف دولار
- خدمات gTLD - 1.45 مليون دولار
- التوافق - 1.1 مليون دولار
- تضمين TLD في برنامج SSR – 650 ألف دولار

إجمالي تكلفة RSS - 11.52 مليون دولار

- اشتراك SSR عالمياً - 530 ألف دولار
- برامج أمن الشركات - 1.2 مليون دولار
- برامج الاستمرار المشتركة - 1.7 مليون دولار
- دعم SSR للسياسة (خلاف - SSAC) - 550 ألف دولار
- دعم SSAC – 650 ألف دولار

أمان واستقرار ومرونة IANA

الأهداف

- التشغيل الآلي للعناصر الأساسية في عملية تغيير منطقة الجذر
- إدارة DNSSEC
- تنفيذ اختبار rPKI
- استمرار الأعمال التجارية

مواد التسليم (مراحل التنفيذ)

- تنفيذ RZM الآلية (يعتمد على أطراف NTIA & VeriSign)
- تنفيذ توقيع DNSSEC لـ ARPA. (يعتمد التاريخ على التعاون مع IAB & NTIA)
- التعاون مع مختبري rPKI
- خطة استمرار IANA (تم التدريب عليها في يناير 2010 والتدريب المستمر للخطة في العام المالي 2011)

أصحاب المصالح الرئيسيين

- IANA وشعلة الأمان وتقنية المعلومات
- DOC/USG وVerisign
- SSAC وRSSAC
- IETF والمجتمع المشغل لـ DNS
- RIRs والمجتمع العامل بالتوجيه

الموارد

- البشرية – 6.5 لدوام عمل كامل (يتضمن 2.5 دوام عمل كامل لشعبة تقنية المعلومات ودعم فرق العمل الأخرى)
- المالية – 1.9 مليون دولار لدعم طاقم العمل بدوام كامل وشعبة الدعم ودعم الانتقالات للفريق والخدمات المهنية وتطوير التطبيقات

عمليات DNS الخاصة بـ ICANN

الأهداف

- أنشطة DNSSEC والتدوير الرئيسي الدوري
- تنفيذ توقيع ICANN لكل من arpa. وzones
- تطبيق مستودع الأمان (TAR)
- عملية جذر L الآمنة والمرنة

أصحاب المصالح الرئيسيين

- عمليات DNS الخاصة بـ ICANN وفرق تقنية المعلومات
- طاقم عمل IANA الخاص بـ ICANN وDoC وVeriSign
- فريق أمان ICANN

النتائج (المعالم الرئيسية)

- التدوير الرئيسي في العام المالي 2011 في منشآت Culpeper وLAX
- توقيع DNSSEC لمناطق ICANN
- المستودع الموثوق بالعملية
- تحسين الجذر L

الموارد (العام المالي 2011)

البشرية – 7.0 لدوام عمل كامل (يتضمن تقنية المعلومات ذات الصلة ودعم الطاقم الآخر)

المالية – 1.2 مليون دولار لدعم طاقم العمل بدوام كامل والاستثمارات الكبيرة المخطط لها للخدمات الاحتياطية وDNSSec والجذر L والتحسينات والمنشآت الاحتياطية والخدمات المهنية والانتقالات

خدمات سجل/المسجل gTLD التابعة لـ ICANN (الخدمات)

الأهداف

- ضمان أن تنفيذ عناوين gTLD/IDN الجديدة تتعامل مع مشكلات SSR
- استمرار إكمال عملية مستودع البيانات وخطة استمرار gTLD
- إجراء عمليات RSEP/RSTEP

أصحاب المصالح الرئيسيين

- السجلات/المسجلون
- طاقم خدمات ICANN
- طاقم الأمان واستمرار ICANN
- GNSO/SSAC

النتائج

- تحسين عملية تنفيذ gTLD من منظور SSR
- اكتمال توازن الجذر (في العام المالي 2011)
- دليل مقدم الطلب المحسن (نوفمبر 2010)
- تدريبات مستودع البيانات (أغسطس - نوفمبر 2010)
- HSTLD RFI (سبتمبر - نوفمبر 2010)
- التحوط من الإجراءات الخبيثة

الموارد (العام المالي 2011)

البشرية – 2.75 لتمويل دوام العمل الكامل

المالية – ميزانية gTLD الجديدة لـ TBD - تتضمن قسمًا من فريق التقييم /دعم أنشطة IDN/gTLD الجديدة لتشتمل على أمان TAS وتمويل RSTEP/RSEP المخصص ودعم تدريبات الاختبار/الاستمرار وانتقالات فريق العمل / الدعم

التوافق التعاقدي (خدمات)

الأهداف
- تحسين عملية توافق ICANN
- نظام متوافق وWDPRS محسن
- تحسين مستوى دقة بيانات WHOIS

النتائج
- إجراء مراجعات كجزء من تنفيذ RAA لعام 2009
- التحسينات على WDPRS (أغسطس - نوفمبر 2010)
- دراسات WHOIS إضافية تعتمد على توصية مجلس GNSO

أصحاب المصالح الرئيسيين
- سجل/مسجل gTLD
- طاقم التوافق في ICANN
- فريق الأمان واستمرار ICANN

الموارد (العام المالي 2011)

البشرية – 3 لدوام عمل كامل

المالية – 1.1 مليون دولار لدعم طاقم العمل بدوام كامل، ودعم فريق العمل/الانتقالات والخدمات المهنية لإجراء الدراسات وعمليات التحسين لدعم الأنظمة؛

التعاون على تحقيق الأمان والاستقرار والمرونة لـ TLD (خدمات)

الأهداف
- برنامج لبناء سعة DNS كاملة
- تحديد برنامج تدريب تقني مشترك بين كل من ISOC وICANN
- إجراء ورش عمل لتخطيط تدريب TLD
- تحديد مقاييس البرنامج

النتائج (المعالم الرئيسية)
- إجراء جلسات تدريب ACRP في العام 2010
- التدريب التقني المشترك مع خطة ISOC والانتقال في 2010
- إجراء ورش عمل لتخطيط التدريب
- قياسات Prototype من مناقشة DNS

أصحاب المصالح الرئيسيين
- مشغلو ccTLD
- ccNSO ومشغلي TLD الإقليميين
- ISOC/NSRC
- طاقم عمل ICANN

الموارد (العام المالي 2011)

البشرية – 1 دوام عمل كامل

المالية – 650 ألف دولار لطاقم العمل لدوام كامل ودعم الفريق/الانتقالات والخدمات المهنية لتطوير وإجراء برامج التدريب

التعاون على تحقيق الأمان والاستقرار والمرونة لـ DNS (الأمان)

الأهداف
- إنشاء آليات استجابة مشتركة للإساءة إلى DNS
- مشاركة ممارسات SSR الرئيسية
- إجراء مخاطر DNS المستندة إلى المجتمع والتعاون
- تحسين تعاون SSR فيما يخص خادم الجذر

النتائج (المعالم الرئيسية)
- بناء التعاون والاستجابة المستمرة مع الشركاء
- الممارسة والإبلاغ عن المناقشات (فبراير ومارس 2011)
- الإبلاغ عن تدريب عمليات الجذر (TBA 2010)

أصحاب المصالح الرئيسيين
- ISOC وDNS-OARC وFIRST
- مجتمع خادم الجذر
- مجتمع تشغيل DNS الأوسع نطاقاً
- طاقم عمل ICANN
- RSSAC/SSAC

الموارد (العام المالي 2011)
البشرية – 1.25 لطاقم العمل بدوام كامل
المالية – 590 ألف دولار لطاقم العمل بدوام كامل والخدمات المهنية للدعم الجزئي والمشترك والانتقالات لدعم الأنشطة

برنامج الأمن المشترك (الأمن وتقنية المعلومات وغير ذلك في سائر قطاعات فريق العمل)

الأهداف
- تحسين وتنفيذ برامج الأمان الشخصي والمنشآت وتقنية المعلومات
  - **تنفيذ الخطط الرسمية**
  - تشكيل التدريب على الأمان
- تنفيذ خطط أمن وطوارئ المسافر والاجتماعات

النتائج
- إجراء برامج التدريب على الأمان (الجزء المدمج من ICANN على مستوى موسع اعتبارًا من سبتمبر 2009)
- تقنية المعلومات المحسنة وأنظمة التحكم في الوصول المادي (مصادقة تقنية المعلومات المحسنة بالأنظمة الرئيسية – خريف عام 2009)
- التدريب على أمن المسافر والاجتماعات (تدريب واحد في كل فصل)

أصحاب المصالح الرئيسيين
- فريق أمان ومرونة ICANN
- عمليات تقنية المعلومات الخاصة بكل من ICANN/IANA/DNS
- الموارد البشرية بـ ICANN
- فريق الاجتماعات العالمية لـ ICANN
- طاقم ICANN الآخر

الموارد

البشرية – 2 طاقم بدوام عمل كامل (يتضمن دعم تقنية المعلومات للأمن)

المالية – 1.1 مليون دولار يتضمن طاقم العمل بدوام كامل والتحكم في الوصول المادي وتقنية المعلومات والخدمات المهنية وإجراء التدريب والمراجعات

برنامج استمرار الشركات (الأمن وتقنية المعلومات وغير ذلك في سائر قطاعات فريق العمل)

الأهداف
- تحسين برنامج استمرارية الشركات
- وضع خطة رسمية
- إنشاء مركز آمن للبيانات
- إنشاء برامج رسمية للتدريب/الممارسة

النتائج
- خطة استمرار أعمال ICANN الداخلية (10 أكتوبر)
- تحسين مرونة مركز البيانات
- ممارسة إدارة الأزمات واستمرار الأعمال التجارية (أكتوبر 2010 - مارس 2011)

أصحاب المصالح الرئيسيين
- فريق أمان ICANN
- عمليات تقنية المعلومات لـ ICANN/IANA/DNS
- الموارد البشرية بـ ICANN
- فريق الاجتماعات العالمية لـ ICANN
- فريق عمل ICANN

الموارد

البشرية – 5 فرق عمل بدوام عمل كامل (يتضمن التخطيط وتقنية المعلومات لمركز البيانات)

المالية – 1.7 مليون دولار لطاقم العمل بدوام كامل والدعم الرئيسي لمركز البيانات والخدمات المهنية لإجراء التدريب والمراجعات

الأمن العام، والاستقرار والمشاركة الأمنية (الشراكات العالمية والأمان)

الأهداف
- الحفاظ على الشراكة مع المنظمات الرئيسية (مثل ISOC وIISI وIMPACT وEC/ENISA وCSIS؛ Atlantic Council)
- مواصلة المشاركة في حوارات حماية الإنترنت القائمة تحت رعاية IGO، مثل OECD، IGF، أخرى)
- التعاون مع الآخرين على الاستجابة لمتطلبات الأمان الإلكتروني العالمية

النتائج
- إجراء أنشطة مشتركة مع المنظمات المشاركة (واحدة في كل فصل)
- المشاركة في منتديات في كافة المناطق الكبرى (مستمر)
- العضوية في منتديات الاستجابة للحوادث وفرق الأمان (FIRST)

أصحاب المصالح الرئيسيين
- المنظمات العالمية/الدولية - ISOC وIETF وITU وIGF
- منتديات الحماية الإلكترونية
- أصحاب المصالح الرئيسيين من الحكومة / التجاريين
- فريق شراكة ICANN العالمية وفريق الأمان

الموارد (العام المالي 2011)

البشرية – 1.5 فريق عمل بدوام كامل

المالية – 530 ألف دولار لفريق العمل بدوام كامل ودعم الانتقالات / الفريق ودعم منتديات ICANN أو المنتديات المدعومة ودعم الخدمات المهنية لتطوير القياسات

دعم السياسة للجهود ذات الصلة بـ SSR (السياسة)

الأهداف
- يتم تحديدها من خلال SO/ACs المدعومة لإجراء نشاط SSR
- GNSO وccNSO
- GAC
- RSSAC وALAC

أصحاب المصالح الرئيسيين
- SO/ACs المسماة
- فريق سياسة ICANN
- فريق أمان ICANN

النتائج
- تشتق من خطط العمل للعام المالي 2011 كما تم تحديدها

الموارد (العام المالي 2011)
البشرية – 2 فريق عمل بدوام كامل

المالية – 550 ألف دولار لفرق العمل بدوام كامل ودعم التمويل الإضافي المحدود للأنشطة ذات الصلة بـ SSR

اللجنة الاستشارية للأمان والاستقرار (SSAC)

الأهداف
- دعم توظيف ونشر DNSSEC
- ضمان استقرار منطقة الجذر مع ما تحققه من نمو وتطور
- حماية حالات تسجيل النطاق
- تقليل الإساءة باسم النطاق
- التعامل مع استقرار النظام

أصحاب المصالح الرئيسيين
- مجتمع أمان الإنترنت الخارجي
- مجتمع خام الجذر وIANA
- GNSO وCCNSO
- ALAC
- ASO
- طاقم عمل ICANN
- GAC والمجلس

النتائج
- التقارير واللجان الاستشارية والتعليقات
- دراسات موازنة الجذر
- دراسة حماية اسم النطاق
- دراسة بيانات التسجيل: العرض والوصول والدقة

الموارد (العام المالي 2011)
البشرية – 1.5 فريق عمل بدوام كامل

المالية – 650 ألف دولار لطاقم العمل بدوام كامل ودعم التمويل الإضافي المحدود للمنشورات والانتقالات ودعم الدراسات المنافسة حول موازنة الجذر

الملحق ب - قاموس مصطلحات واختصارات خطط SSR

ACRP – تخطيط الاستجابة للهجمات وحالات الطوارئ

إضافة فترة سماح – فترة-اختيارية لمدة خمسة أيام في بداية تسجيل نطاق المستوى الثاني الذي تنظمه ICANN. قد يختار المسجلون حذف تسجيلهم خلال فترة اختيارية لمدة خمسة أيام، حينما يجب استرداد رسوم التسجيل بالكامل من قِبل تسجيلات أسماء النطاقات.

APWG – مجموعة عمل مكافحة الخداع

ASN – أرقام نظام الحكم الذاتي: في الإنترنت، يعتبر النظام المستقل (AS) مجموعة من بادئات توجيه IP المرتبطة التي تقدم سياسة توجيه شائعة ومحددة بوضوح للإنترنت. يجب أن يكون لدى مزودو خدمة الإنترنت (ISPs) أرقام نظام مستقل مسجل رسمياً من خلال IANA.

ccNSO – منظمة دعم أسماء رموز الدول الخاصة بـ ICANN هي هيئة وضع السياسات لنطاق ضيق من مشكلات نطاق المستوى الأعلى لرمز البلد العالمي داخل هيكل ICANN.

ccTLD – نطاق المستوى الأعلى لرمز البلد

CENTR – مجلس تسجيلات النطاقات الأعلى مستوى القومية الأوروبية هو مؤسسة تسجيلات نطاق المستوى الأعلى لرمز البلد مثل الرمز uk. في المملكة المتحدة والرمز es. في إسبانيا. تعتبر العضوية الكاملة مفتوحة للمنظمات والشركات والأشخاص الذين يديرون تسجيلات نطاق مستوى أعلى لرمز البلد.

CSIS – مركز الدراسات الإستراتيجية والدولية يقدم رؤى إستراتيجية ويبرز حلول السياسات لصانعي القرار في الحكومة والمؤسسات الدولية والقطاع الخاص والمجتمع المدني.

FIRST – منتدى الاستجابة للحالات الطارئة والأمن

gTLD – مزودو نطاقات المستوى الأعلى

IANA – هيئة أرقام الإنترنت المُخصصة

IDN – اسم النطاق الدولي

IETF – فريق عمل هندسة الإنترنت

IP – بروتوكول الإنترنت الذي يحدد شكل وتنسيق المحتوى ويحدد النظام كذلك. وتجمع معظم الشبكات بين بروتوكول الإنترنت مع بروتوكول مستوى أعلى يُدعى بروتوكول التحكم في الإرسال،وهو ما ينشئ ارتباطاً ظاهرياً بين الوجهة والمصدر. فبروتوكول الإنترنت في حد ذاته هو شيء يشبه نظام البريد. فهو يتيح وضع عنوان لعبوة وإرسالها باستخدام النظام، لكن لا يوجد رابط مباشر بين عبوتك والمستقبلين. تنشئ IP/TCP اتصالا بين مضيفين بحيث يمكنك إرسال رسائل للأمام والخلف.

IPv4 – بروتوكول الإنترنت الإصدار الرابع، هو التنقيح الرابع في تطوير بروتوكول الإنترنت وهو أول إصدار من البروتوكول يتم نشره بصورة واسعة. إلى جانب IPv6 يعتبر أساس المعايير استنادا إلى طرق الشبكة الداخلية للإنترنت ولا يزال بعيدا الانتشار على نطاق واسع بطبقة الإنترنت الخاصة بالبروتوكول.

IPv6 – بروتوكول الإنترنت الإصدار 6 وهو الجيل التالي من طبقة بروتوكول الإنترنت المخصص لمحتوى البيانات المحولة بين الشبكات الداخلية والإنترنت. في ديسمبر 1998، فريق عمل هندسة الإنترنت (IETF) صمم IPv6 كخليفة للإصدار 4 من خلال نشر مسار قياسي بالمواصفات الخاصة به RFC 2460.

ISOC – مجتمع الإنترنت

IT – تقنية المعلومات

Botnets (**شبكات الاختلاس الإلكترونية**) – يتم إنشاؤها عادةً بخداع المستخدمين العاديين بفتح مرفق على أجهزة الكمبيوتر الخاصة بهم والذي يبدو أنه لا يفعل شيئاً ولكنه في الواقع يثبت برنامجاً ليتم استخدامها لاحقاً في الهجوم. وهذه الأجهزة المصابة يتم تجميعها لتكون شبكات يمكن بعد ذلك استهدافها، بالهجمات الضارة عادةً، بكل سهولة.

Cache Poisoning (**الضعف الضار للذاكرة المؤقتة**) – استغلال تدفق في برنامج NSD لجعله يقبل معلومات غير الصحيحة التي تتسبب في أن يخزن الخادم مؤقتاً إدخالات خاطئة يرسل بها كل طلبات الخادم اللاحقة إلى النطاق الجديد الذي تم التحقق منه بصورة خاطئة.

هجمات رفض الخدمة (DoS) – رمز ضار يتسبب في فيضان من الرسائل الواردة، والتي تجبر بصورة أساسية النظام المستهدف على الإغلاق، وبالتالي تمنع استخدام المستخدمين الشرعيين.

هجوم رفض الخدمة الموزع (DDoS) – نوع من أنواع هجمات رفض الخدمة والتي يقوم فيها المهاجم باستخدام رمز ضار مثبت على أنظمة متعددة من أجل الهجوم على هدف مفرد. ويكون لهذه الطريقة تأثيراً أكبر على الهدف أكثر منه حينما يتم استخدام جهاز واحد للهجوم. ويعتبر هجوم رفض الخدمة الموزع أحد أنواع الهجوم الذي يتم فيه الهجوم من قِبل عدة أنظمة على هدف واحد، وبالتالي يمنع الخدمة عن مستخدمي النظام الهدف. وتجبر سيول الرسائل القادمة إلى النظام الهدف على الإغلاق وبالتالي تمنع المستخدمين الشرعيين من الاستفادة بالخدمة. وتعتبر هجمات DDoS الأكثر فاعلية حينما يتم شنها من خلال عدد كبير من خوادم متعددة مفتوحة: حيث يزيد التوزيع من المرور ويقلل من التركيز على مصادر الهجوم. ويكون عادة التأثير على الخوادم المتعددة المفتوحة سيئة الاستخدام منخفضاً، لكن التأثير على الهدف يكون كبيراً. ويقدر عامل التضخيم بنسبة 1:73 من الهجمات، ووفقاً لهذه الطريقة تتجاوز 7 جيجا بايت في الثانية.

DNS – نظام اسم النطاق الذي يترجم أسماء النطاق (حروف) إلى عناوين IP (أرقام). لأنها أسهل في الحفظ حينما تكون أسماء النطاقات أبجدية. ويستند الإنترنت مع ذلك إلى عناوين رقمية لـ IP (مثل 198.123.456.0). حينما تستخدم اسم نطاق (www.examplir.gratis.com)، تترجم خدمة DNS الاسم الأبجدي إلى عنوان IP الرقمي المقابل.

DNSSEC – نظام اسم النطاق يقدم امتدادات الأمان بطريقة للبرامج للتحقق من بيانات نظام اسم النطاق (DNS) المعدلة خلال نقل الإنترنت. يتم هذا عن طريق دمج أزواج مفاتيح التوقيع العامة ذات الطابع الخاص في التسلسل الهرمي لـ DNS لتشكيل سلسلة ثقة ناشئة في منطقة الجذر. في الأساس، لا يعد DNSSEC أحد أشكال التشفير. وهو يتوافق ارتجاعياً مع DNS الموجود، وبذلك تظل السجلات كما هي – غير مشفرة. يضمن DNSSEC تكامل السجلات من خلال استخدام التوقيعات الرقمية التي تُصَدِّق على موثوقيتها.

ويعد مفهوم "سلسلة الثقة" جزءاً صميماً من DNSSEC. ويوصي اقتراح منظمة ICANN بتوقيع ملف منطقة الجذر بـ DNSSEC (في أكتوبر 2008) المبني على هذا المفهوم والقائم على النصح الأمني بأن الجهة المسئولة عن إحداث عمليات التغيير والإضافة والحذف في ملف منطقة الجذر والتأكيد على صلاحية هذه التغييرات، يجب عليها إنشاء ملف محدث لمنطقة الجذر الناشئ وتوقيعه رقمياً. عندئذٍ يجب إرسال هذا الملف المُوَقع إلى منظمة أخرى (حالياً شركة VeriSign) للتوزيع. بمعنى آخر، يجب أن تكون المنظمة المسئولة عن القواعد--الأساسية للثقة والتي تقوم بالتأكيد على صلاحية التغييرات في منطقة الجذر مع مشغلي نطاقات المستوى الأعلى --بالتصديق أيضاً على صلاحية المنتج النهائي قبل توزيعه.

التشغيل الأولي لاسم النطاق – الممارسات المشكوك فيها التي يستخدمها بعض مسجلي أسماء النطاق من استخدام معلومات خاصة لتسجيل أسماء النطاقات مقدماً من أجل بيع الاسم، برسوم إضافية، للمسجِّلين الذي يرغبون في الاستفادة بشكل منطقي من الحصول على الاسم لاستخدامهم الخاص

اختبار النطاق – ممارسة مسجل اسم النطاق باستخدام فترة سماح بالإضافة لمدة خمسة أيام في بداية التسجيل لنطاق مستوى ثاني تنظمه ICANN لاختبار قابلية تسويق اسم النطاق. أثناء فترة تحليل التكاليف - الفوائد الذي يجريه المسجل حول بقاء الدخل المشتق من الإعلانات التي يتم وضعها على موقع الويب.

يجب عدم الخلط بين اختبار النطاق وقنص النطاق، وهي عملية حذف اسم النطاق أثناء فترة السماح الإضافية التي تستمر لمدة خمسة أيام وإعادة التسجيل على الفور لفترة خمسة أيام أخرى. ويتم تكرار هذه العملية أي عدد من المرات وتكون النتيجة النهائية تسجيل النطاق بدون دفع مال فعلياً له.

التمويه المزدوج – تهتم ICANN بنوع مختلف من التمويه السريع يدعى التمويه المزدوج والت لا يغير فيها المهاجم فقط العناوين التي تشير إلى مواقع الويب غير القانونية، لكن عناوين خوادم أسماء DNS التي يستخدمها المهاجم للأسماء "المحببة للمستخدم" التي يضمنها في رسائل البريد الإلكتروني المخادع. وفي كلتا الحالتين، تحدث التغييرات سريعاً جداً، في حوالي ثلاث دقائق، وهو ما لا يترك ظاهرياً للباحثين وقتاً للاستجابة. وتعمل اللجنة الاستشارية للأمان والاستقرار (SSAC) التابعة لـ ICANN عن قرب مع المدافعين عن العلامات التجارية وعن مطبقي القوانين بالإضافة إلى السجلات والمسجلين لتحديد الإجراءات المضادة، وبخاصة تلك التي تأخذ DNS خارج معادلة التمويه السريع.

التمويه السريع – أسلوب خداعي يستخدمه المخادعون ولصوص الهوية وغيرهم من مجرمي الإنترنت لإحباط جهود فريق الاستجابة للحوادث وجهود وكالات تطبيق القوانين في تتبع وإسقاط المواقع الإلكترونية غير القانونية. ويشبه أسلوب التمويه السريع بشدة لعبة الثلاث ورقات، حينما يقوم اللاعب بتطبيق الثلاث ورقات على منضدة ويتم إغراء الضحية بالمراهنة على قدرته على "متابعة البنت الحمراء" (ويطلق البريطانيون على هذه اللعبة "البحث عن السيدة"). ويحرك اللاعب الثلاث ورقات بسرعة يصعب متابعتها وفي الوقت ذاته يشتت انتباه ضحيته بالحوار والمزح الذكية وتجاهل اليد. ومع ذلك، فإن التمويه السريع لعبة شديدة المخاطرة وقد أصبح أسلوب هجوم مقلق وبغيض. وعند استضافة التمويه السريع، يقوم المهاجم بسرعة بتغيير العناوين التي تشير إلى المواقع الإلكترونية غير القانونية.

البرامج الخبيثة الضارة – هو دمج بين كلمتي "ضار" و"برامج" ويتم استخدامها في الأغلب كعبارة شاملة تتضمن فيروسات الكمبيوتر والديدان وأحصنة طروادة وبرامج أدوات الجذر وبرامج التجسس والبرامج الإعلانية وبرامج جريمة وأي برامج أخرى

غير مرغوب بها يتم إدخالها إلى أجهزة كمبيوتر المستخدم سواءً بموافقته أو بغير موافقته. وتعتمد البرامج الضارة على نية مبتكر الفيروس منه أكثر من أي سمة أخرى للبرامج.

NOC – مركز عمليات الشبكة هنا وهو مكان مادي يتم منه في الأغلب إدارة الشبكات الكبيرة ومراقبتها والإشراف عليها. كما يتيح مركز عمليات الشبكة (NOC) كذلك إمكانية الدخول على الشبكة من خارج المكان المادي.

NOG – مجموعة عمليات الشبكة

NRO – منظمة موارد الأرقام

الدفعات – برامج مصممة لتثبيت عيوب البرامج، ويتم تثبيتها في الأغلب تلقائياً لتقليل الحاجة لمشاركة المستخدم النهائي وزيادة سهولة الاستخدام.

الاحتيال والخداع – نوع من الاحتيال على الإنترنت يهدف إلى سرقة المعلومات القيمة مثل بطاقات الائتمان وأرقام الضمان الاجتماعي وهويات المستخدمين وكلمات السر عن طريق إنشاء موقع إلكتروني مشابه لموقع المنظمة القانونية، ثم توجيه حركة مرور البريد الإلكتروني للموقع الاحتيالي للحصول على المعلومات الخاصة للحصول على مكاسب مالية أو سياسية.

RAA – اتفاقيات اعتماد المسجل

السجل – منظمة تعمل على إدارة تسجيل أسماء النطاق من المستوى الأعلى للإنترنت.

مسجل النطاق – شركة مخولة بتسجيل أسماء نطاق الإنترنت

RIR – سجل الإنترنت الإقليمي.

RPKI – البنية التحتية الرئيسية العامة للموارد

RSEP – عملية تقييم خدمات السجل

RSTEP – هيئة التقييم التقني لخدمات السجل

Spam – أي بريد غير موثوق. يتم اعتبارها عادةً إزعاجاً مكلفاً، ويتضمن البريد العشوائي في الأغلب برامج ضارة. تعتبر البرامج الضارة فئة من البرامج المضرة مثل الفيروسات والديدان وأحصنة طروادة وبرامج التجسس - المصممة لإصابة أجهزة وأنظمة الكمبيوتر وسرقة المعلومات الهامة وحذف التطبيقات والمحركات والملفات أو تحويل أجهزة الكمبيوتر إلى أصول للمهاجم.

Spoofing – موقف هجومي يهجم فيه شخص أو برنامج عن طريق تزييف البيانات. ويثق النظام الفردي بالبيانات الزائفة باعتبارها صحيحة محاولاً الاتصال بالبرنامج أو النظام القانوني.

TLD – نطاق المستوى الأعلى

Trojan – فئة من فئات البرامج الضارة التي يبدو أنها تقوم بوظيفة مرغوب فيها لكنها بدلاً من ذلك تقوم بوظائف ضارة سرية تتيح وصولاً غير مصرح به إلى الجهاز المضيف، وهو ما يعطي لمستخدمي أحصنة طروادة القدرة على حفظ ملفاتهم على أجهزة كمبيوتر المستخدمين الجهلاء أو حتى مراقبة شاشة المستخدم والتحكم في أجهزة الكمبيوتر.

الفيروس – برنامج أو سلسلة من الرموز المحملة على جهاز كمبيوتر دون معرفة المستخدم ويشغل بعض البرامج الخبيثة الضارة المعروفة بـ (malware). وحتى الفيروس البسيط يمكن أن يكرر نفسه ليجعل نفسه أكثر تدميراً لأنه يستخدم بسرعة كل الذاكرة المتاحة على نظام جهاز الكمبيوتر المصاب.

الدودة – مشابهة للفيروس في تصميمها وتعتبر أحد أنواع الفيروسات، لكنها أخطر نظراً لقدرتها على إرسال نفسها عبر الشبكات. وتنتقل الديدان من كمبيوتر إلى آخر، لكنها على عكس الفيروسات، لديها القدرة على الانتقال بدون أي عمل من البشر سواءً كان مقصوداً أو غير مقصود. وتستفيد الدودة من سمات نقل الملف أو المعلومات على نظام الكمبيوتر، والذي يتيح لها التنقل دون الاحتياج لمساعدة. فعلى سبيل المثال، يمكن للدودة أن تنسخ نفسها باستخدام دفتر عناوين البريد الخاص بالمستخدم الذي لا يعلم عن ذلك شيئاً. ثم تقوم بنسخ نفسها على أجهزة الكمبيوتر الجديدة المصابة ثم تنتشر مرة أخرى من خلال دفاتر عناوين أنظمة الكمبيوتر المصابة الجديدة ثم تستهلك في النهاية قدراً كبيراً من الذاكرة وعرض النطاق وتتسبب في النهاية في أن تصيب الشبكة بأكملها بالتوقف.