الخطة المعنية بتحسين حماية الإنترنت والاستقرار والمرونة

مسودة معتمدة – 16 مايو 2009

جدول المحتويات

الخطة المعنية بتحسين حماية الإنترنت والاستقرار والمرونة i
مسودة معتمدة – 16 مايو 2009 i
جدول المحتويات ii
الملخص التنفيذي 1
دور ICANN 2
برامج الأمان والاستقرار والمرونة الخاصة بـ ICANN 2
الخطط المعنية بتحسين الأمن والاستقرار والمرونة 3
1. الغرض ونظرة عامة 4
2: التحدي والفرص 5
3: دور ICANN 6
4: مساهمو ICANN في جهود تحقيق الأمان والاستقرار والمرونة 8
5: برامج ICANN المتواصلة المعنية بالأمان والاستقرار والمرونة 9
5.1 DNS الرئيسية/ معالجة الأمن والاستقرار والمرونة 10
5.1.1 عمليات IANA 10
5.1.2 عمليات خادم جذر DNS 11
5.2 أمن واستقرار ومرونة تسجيلات ومسجلي TLD 12
5.2.1 تسجيلات gTLD 12
5.2.2 gTLDs وIDNs الجديدة 13
5.2.3 مسجلي gTLD 13
5.2.4 Whois 14
5.2.5 التوافق التعاقدي 14
5.2.6 حماية مالكي أسماء نطاقات gTLD 15
5.2.7 ccTLDs 15
5.2.8 المتطلبات التقنية لـ IANA 16
5.2.9 الاستجابة المشتركة لإساءة الاستخدام الضارة لنظام اسم النطاق 16
5.2.10 توفير أمن واستقرار ومرونة DNS على نحو شامل 16
5.3 التعاون مع منظمة مصادر الأرقام (NRO) وتسجيلات الإنترنت الإقليمية (RIRs) 17

5.4.	**عمليات الأمن والاستمرارية التجارية لـ ICANN**	17
5.5	**أنشطة المنظمات الداعمة واللجان الاستشارية لـ ICANN**	18
5.6	**التعاون العالمي المعني بتحسين الأمن والاستقرار والمرونة**	19
5.6.1	الشركاء والأنشطة على المستوى العالمي	19
5.6.2	الشركاء والأنشطة على المستوى الإقليمي	20
5.6.3	العمل مع الحكومات	21
6.	خطط ICANN لفبراير 2010 المعنية بتحسين الأمن والاستقرار والمرونة	22
6.1.	**وظائف DNS/التوجيه الرئيسية**	23
6.1.1	عمليات IANA	23
6.1.2	عمليات خادم جذر DNS	23
6.2	**العلاقات مع تسجيلات ومسجلي TLD**	24
6.2.1	تسجيلات gTLD	24
6.2.2	gTLDs الجديدة	24
6.2.3	IDNs	24
6.2.4	ccTLDs	25
6.2.5	المُسجلون	25
6.2.6	الالتزام التعاقدي	25
6.2.7	الاستجابة المشتركة لإساءة الاستخدام الضارة لنظام اسم النطاق	26
6.2.8	توفير أمن DNS على نحو شامل	26
6.3	**التعاون مع NRO وRIRs**	26
6.4.	**عمليات الأمن والاستمرارية التجارية لـ ICANN**	27
6.5	**المنظمات الداعمة واللجان الاستشارية التابعة إلى ICANN**	27
6.6	**المشاركة العالمية**	28
6.6.1	تمديد الشراكات القائمة	28
6.6.2	المؤسسات التجارية	28

6.6.3 المشاركة في الحوار المعني بأمن الإنترنت العالمي 28

7. الخاتمة 29

الملحق أ 30

الملحق ب - قاموس مصطلحات واختصارات خطط SSR 38

الملخص التنفيذي

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. ويعتمد التعاون المشترك بين تلك المجتمعات العالمية على تشغيل وتنسيق نظم المعرفات الفريدة للإنترنت.[1] وتقر ICANN ومشغلو هذه النظم بأن صيانة وتحسين أمن واستقرار ومرونة هذه النظم إنما يعد عنصراً جوهرياً في علاقتهم القائمة على التعاون.

تنص خطة ICANN الاستراتيجية 2009 - 2012 (www.icann.org/en/strategic-plan/strategic-plan-2009-2012-09feb09-en.pdf) على أن "الأمن والاستقرار والمرونة ستظل في مقدمة أولوياتها وأن ICANN ستعمل بفاعلية مع أصحاب المصالح المتعلقة بالإنترنت لتعزيز وحماية أمن واستقرار الإنترنت، مع إعطاء اهتمام خاص لمهمة ICANN في حماية أمن واستقرار ومرونة أنظمة المعرفات الفريدة للإنترنت". وتحدد الخطة الاستراتيجية مجموعة من الأهداف خلال مجموعة كبيرة من مسئوليات ICANN المتعلقة بالأمن والاستقرار والمرونة. تعالج الخطة الاستراتيجية مخاوف الأمن والاستقرار والمرونة كأولوية ثانية - تعزز الأمن والاستقرار والمرونة في توزيع وتخصيص المعرفات الفريدة للإنترنت. وتنص الأولوية الثانية على: أن التشغيل الآمن والمستقر لنظم المعرفات الفريدة للإنترنت يعتبر جزءً أساسيًا من مهمة ICANN. ومع زيادة تكرار الهجمات والسلوكيات الضارة الأخرى وزيادة تعقيدها، يجب أن تستمر ICANN ومجتمعها في تحسين مرونة DNS وتعزيز قدرتها على التعامل مع هذه الأحداث. وحيث تتسع طبيعة الهجمات والسلوكيات الضارة، يجب أن تعمل ICANN مع أصحاب المصالح الآخرين في هذا المجال لتوضيح دور ANNIC والعثور على حلول للمشكلات التي هي أكبر من مهمة أي كيان واحد. والهدف الرئيسي لهذه الأولوية هو ضمان احتفاظ أنظمة المعرفات الفريدة للإنترنت بقوتها طوال فترة هذه الخطة.

وقد تم تحديد أهداف معينة في الأولوية الثانية من الخطة الاستراتيجية وهي:

أ. تقديم خطة للمشاورة تقوم بتحديد دور ICANN في أمن الإنترنت واستقراره ومرونته وتحديد الشركاء الملائمين وبدء العمل المشترك. تحديد دور ICANN بطريقة تسهل فهم مجال الجهود والتكاليف والعائدات وبدء عملية تؤدي إلى إبرام اتفاقية بين المجتمع ومجلس الإدارة في أوائل 2009. العمل بفاعلية مع الشركاء لمتابعة أساليب أصحاب المصلحة المتعددين وإجراء برامج تسهم في أمان واستقرار ومرونة الإنترنت بشكل عالمي. ويتم تحديد مقاييس هذه البرامج بنهاية 2009 ويتم وضع التقييمات الأولية للبرنامج بحلول منتصف 2010.

ب. تقديم آليات تسمح للمستخدمين بالتحقق من صحة معرفي الإنترنت التي تقوم ICANN بنشرهم، والمساهمة بشكل واسع في الجهود التقنية لتقديم نظم آمنة بشكل أكثر لأسماء وعناوين الإنترنت. وتسعى ICANN بصفة خاصة للعمل مع أصحاب المصالح لضمان توقيع DNSSEC لمنطقة جذر DNS بنهاية عام 2009 وتعزيز تنفيذ rPKI لتحسين معالجة قضية الأمن والاستقرار.

ج. إجراء برامج مركزة لتحسين فهم المخاطر وتحسين أمن ومرونة التنظيمات المرتبطة بمجتمع TLD وتتضمن البرامج العمل مع الشركاء لوضع أسلوب فعال لمشاركة

[1] ووفقًا للوائح الداخلية لـ ICANN، تنسق ICANN تخصيص المجموعات الثلاث من المعرفات الفريدة للإنترنت وهي: أسماء النطاق (تكوين نظام يشار إليه بمصطلح DNS)، وعناوين بروتوكول الإنترنت (IP) وأرقام النظام المستقل (AS) و ومنفذ البروتوكول وأرقام المعيار.

أفضل الممارسات عبر المجتمع بحلول نهاية 2009 وإجراء برامج تدريبية وبرامج اختبارات مستمرة على أساس إقليمي لهذا المجتمع خلال فترة هذه الخطة.

د. العمل مع أصحاب المصلحة عبر مجتمع ICANN لتنظيم التعاون المستمر لفهم المخاطر وتحسين أمن ومرونة DNS ضد سلسلة كاملة من التهديدات طوال فترة سريان الخطة. وستعمل ICANN مع شركائها لوضع مناهج لقياس المخاطر التشغيلية لـ DNS ومستخدميها بحلول منتصف 2010.

وتقدم خطة ICANN الخاصة بتحسين الأمن والاستقرار والمرونة المستند المطلوب في الهدف "أ"، كما أنها تصف بالتفصيل الدور الخاص بـ ICANN في معالجة الأمن والاستقرار والمرونة، كما أنها تقدم نظرة عامة على برامج ICANN في هذه المجال، بالإضافة إلى أنها توضح بالتفصيل أنشطة الخطة التي تحسن مساهماتها خلال العام التنفيذي التالي. وقد تم وضع الإصدار الأول من الخطة ليكون بمثابة أساس لـ ICANN ومجتمعاتها فيما يتعلق بدورها ومن أجل إنشاء إطار لتنظيم جهود الأمن والاستقرار والمرونة. ولا تقدم الخطة رؤية لأدوار جديدة رئيسية أو لبرامج جديدة لـ ICANN في هذا المجال.

دور 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.

- يجب أن يركز دور ICANN على مهامها الرئيسية المرتبطة بنظم المعرفات الفريدة.
- لا تلعب ICANN دور الشرطي على الإنترنت أو في مكافحة السلوك الإجرامي على نحو عملي.
- لا تلعب ICANN دوراً في استخدام الإنترنت المرتبط بجاسوسية وحرب الإنترنت.
- لا تلعب ICANN دوراً في تحديد ما يعتبر محتوى غير قانوني على الإنترنت.
- يتضمن دور ICANN المشاركة في الأنشطة مع مجتمع الإنترنت الأوسع نطاقاً المعنية بمكافحة إساءة استخدام نظم المعرفات الفريدة. تتضمن هذه الأنشطة التعاون مع الحكومات في مكافحة الأنشطة الضارة التي تحدث بإساءة استخدام النظم للمساعدة في حمايتها.

برامج الأمان والاستقرار والمرونة الخاصة بـ ICANN

- تعد ICANN مسئولة عن عمليات هيئة أرقام الإنترنت المُخصصة (IANA). وهو ما يضمن أن يظل التشغيل الآمن والمستقر والمرن لوظيفة منطقة جذر DNS على قمة أولوياتها.
- 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.
- تعد ICANN عنصر تفعيل وتسهيل لأنشطة تعزيز الأمن والاستقرار والمرونة المبذولة من قبل سجلات DNS والمسجلين وباقي أعضاء المجتمع.
- تعد ICANN مسئولة عن عملية الأمن والاستقرار والمرونة فيما يخص أصولها وخدماتها.
- إن ICANN مشاركاً في المنتديات والأنشطة الأوسع نطاقاً المرتبطة بأمن واستقرار ومرونة نظم المعرف الفريدة للإنترنت.

الخطط المعنية بتحسين الأمن والاستقرار والمرونة

وخلال العام التشغيلي 2009 - 2010 تخطط ICANN لتنفيذ برامجها ومبادراتها الموضحة هنا. يستعرض الملحق أ تفاصيل حول الأهداف الخاصة بالبرنامج والنشاط والشركاء والنتائج ومخصصات الموارد.

- **عمليات IANA** - وفقًا للخطة الاستراتيجية لـ NICAN لأعوام 2009-2012، يجب أن تكون ICANN جاهزة لتنفيذ DNSSEC لمناطق الجذر المعتمدة، بالإضافة إلى العمل مع مجتمع الإنترنت لإزالة العقبات التي تعترض طريق اعتماد DNSSEC. تعتبر ICANN مستعدة وراغبة وقادرة على توقيع الجذر. ووفقًا لاقتراحها لعام 2008، يتم تناول الجهود الحالية والمخططة لـ ICANN في الأقسام 5-1-1-3 و6-1-1-1. تتضمن المبادرات تحسين إدارة منطقة الجذر من خلال الأتمتة، وتحسين مصادقة الاتصالات مع مديري TLD
- **عمليات خادم منطقة جذر DNS** - مواصلة السعي لتحقيق إقرار متبادل للأدوار والمسئوليات والمبادرة بجهود تطوعية لتنفيذ تخطيط وتدريبات الطوارئ.
- **تسجيلات gTLD** - ضمان تقييم مقدمي طلبات الحصول على gTLD وطلبات IDN من أجل تقديم عمليات آمنة. وسوف تعمل ICANN على تطوير خطة استمرارية تسجيل gTLD واختبار نظام مستودع البيانات.
- **تسجيلات ccTLD** - سوف تسعى ICANN لتحسين سبل تعاونها مع نطاق المستوى الأعلى لرمز البلد (ccTLD) على صعيد تطوير البرنامج المشترك للتخطيط للاستجابة للهجوم ولحالات الطوارئ (ACRP) الذي تم إنشاؤه بالاشتراك مع منظمة دعم أسماء رمز البلد (ccNSO) واتحادات TLD الإقليمية.
- **الالتزام 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.
- **الاستجابة لإساءة الاستخدام الضارة 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.
- **العمليات الداخلية لأمن واستمرارية ICANN** - تحرص ICANN على تنفيذ برامجها الأمنية ضمن الإطار الإجمالي لإدارة مخاطر الشركة وإدارة الأزمات وبرامج استمرارية العمل. وسوف يقع ضمن بؤرة الاهتمام إنشاء أساس قوي من الخطط الموثقة والإجراءات الداعمة.
- **ضمان المشاركة والتعاون العالمي** - 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 (OARC-DNS). 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

1.1 توضح هذه الخطة لنطاق كبير من أصحاب المصالح كيف تساهم ICANN في الجهود العالمية التي تتناول الأمن والاستقرار والمرونة بصفتها تحديات تواجه الإنترنت، مع التركيز في مهمتها على معرفات 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 FY10 المعنية بتحسين الأمن والاستقرار والمرونة
- القسم 7: خاتمة
- الملحق أ: كل ما يخص برنامج ICANN FY 10 لتحقيق الأمن والاستقرار والمرونة من أهداف وشركاء وعناصر رئيسية/نتائج وموارد

1.2 كما هو موضح في الملخص التنفيذي، تقدم هذه الخطة الرؤية والأهداف المنصوص عليها في خطة ICANN الاستراتيجية 2009-2012. وقد تم وضع الإصدار الأول من الخطة ليكون بمثابة أساس لـ ICANN ومجتمعاتها فيما يتعلق بدورها ومن أجل إنشاء إطار لتنظيم جهود الأمن والاستقرار والمرونة. ولا تقدم الخطة رؤية لأدوار جديدة رئيسية أو لبرامج جديدة لـ ICANN في هذا المجال. وسيتم تحديث الخطة سنويًا مع دورات التخطيط الاستراتيجية والتنفيذية لـ ICANN.

2: التحدي والفرص

2.1 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 ابتكارًا ناجحًا وفعالاً وأتاحت الفرصة للتواصل والابتكار والمتاجرة ضمن مجتمعات عالمية. إلا أن هذا الانفتاح له مساوءه 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). ويمكن لهجمات رفض الخدمة (DoS) إزعاج كافة أنواع المستخدمين. ولقد تم خلال السنوات الأخيرة الإفصاح عن القلق المتزايد لكافة أصحاب المصالح ذات الصلة بالإنترنت - المستخدمون، المؤسسات، 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.

2.2 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 FY10 المقررة وأهم المعايير والموارد ذات الصلة. ومن أهم محاور اهتمام أهداف FY10 لموظفي أمن الإنترنت بـ ICANN سيكون وضع مقاييس للبرامج الأوسع نطاقاً الرامية إلى تحسين المستوى الإجمالي لأمن واستقرار ومرونة نظم المعرفات الفريدة للإنترنت.

3: دور ICANN

3.1 تعمل ICANN بما يتفق مع لوائحها الداخلية فيما يتعلق بإجراء عمليات قائمة على الإجماع تضم العديد من أصحاب المصالح لوضع سياساتها وبرامجها لتتضمن تلك البرامج المعنية 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.

3.2 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.

3.3 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. وهي لن تلعب دور الشرطي في المكافحة العملية للسلوك الإجرامي ومرتكبي الأنشطة الضارة. 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.

3.4 تقوم ICANN بهيكلة أنشطتها المعنية بالأمن والاستقرار والمرونة من خلال مراعاة دورها باعتبارها: كمسئول مباشر، كعنصر تمكين/تسهيل، كمشارك.

- تعد ICANN مسئولة على نحو مباشر عن عمليات IANA كما تساهم في جمع وتوزيع منطقة الجذر مع وزارة التجارة الأمريكية وVeriSign. وهو ما يضمن أن يظل 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) بحيث يتضمن توقيع منطقة جذر DNS. وقد اقترحت ICANN منهجًا يتيح استمرار آلية توزيع جذر DNS دون انقطاع، وهي مهمة مشتركة بين ICANN وVeriSign وNTIA ومشغلي خادم الجذر الآخرين بـ DNSSEC. وقد قدمت ICANN حلول مرنة تمثل مناهج مؤقتة للوصول إلى حلول انتقالية قبل الوصول إلى حلول دائمة، وقد أجرت استعداداتها التشغيلية من أجل أن تلعب هذا الدور. 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.
- 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. 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.

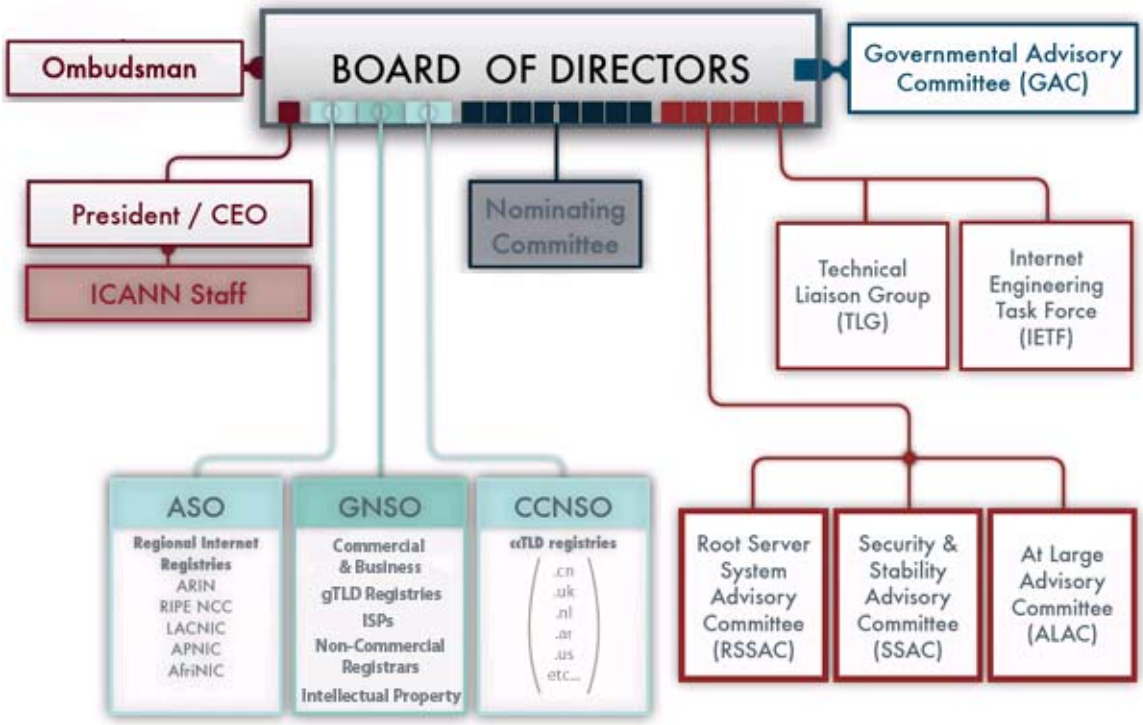
4: مساهمو ICANN في جهود تحقيق الأمان والاستقرار والمرونة

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

- ***فريق IANA*** - مسئول عن تنفيذ وظائف IANA بحيث تتضمن تنسيق منطقة جذر DNS وتشغيل تسجيل .arpa وتخصيص مساحة عنوان IP وتسجيل معايير البروتوكول. وقد وضع فريق IANA خططًا لتنفيذ DNSSEC على مستوى الجذر ولمناطق DNS التي تديرها ICANN. نوضح أدناه بعض الأنشطة المحددة الخاصة بالأمن والاستقرار والمرونة.
- ***فريق الخدمات/الالتزام التعاقدي*** - مسئول 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*** - مسئول 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 الشراكات العالمية*** - مسئول عن التعاون على المستوى العالمي والإقليمي مع أصحاب المصالح في ICANN لضمان تحقيق ICANN لمشاركة عالمية كاملة في العمليات والتنفيذ. وفي هذا الصدد، يتم تضمين أنشطة ICANN المرتبطة بالأمن والاستقرار والمرونة في العمل الإجمالي الخاص بالشراكات العالمية للمنظمة.
- ***فريق علاقات/اتصالات الشركة*** - مسئول 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 الأمن*** - مسئول 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 للأمن والاستقرار (SSAC)*** - تعتبر اللجنة الاستشارية لمنظمة ICANN وSSAC مسئولتان 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 (RSSAC)*** - 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 تفاعلها مع المنظمات الخارجية.

يدور هذا القسم حول إطار العمل الذي تم وضعه في القسم 3.4، بدءً من وظائف DNS/المعالجة الرئيسية؛ العمل مع تسجيل TLD ومجتمعات المسجل؛ المشاركة مع NRO وRIR؛ أمن الشركة وبرامج الاستمرارية؛

أنشطة المنظمات الداعمة واللجان الاستشارية، المشاركة في الأنشطة المعنية بأمن واستقرار ومرونة الإنترنت على المستوى المحلي والعالمي.

5.1 DNS الرئيسية/ معالجة الأمن والاستقرار والمرونة

5.1.1 عمليات IANA

5.1.1.1 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.

5.1.1.2 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 النطاقات** - من خلال وظائف IANA، تقوم ICANN بإدارة جذر DNS 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 دوراً 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.
- **مصادر الأرقام** - من خلال وظائف IANA، تقوم ICANN بتنسيق المجموعة العامة لعناوين IPv4 وIPv6 وASNs، حيث توفرهما إلى RIRS. ومن خلال IANA، تشترك ICANN في نشاط التنسيق هذا إلى توجيه العمليات والإجراءات التي تنشأ عن مجتمعات RIR من خلال عمليات تطوير سياستها. وتتيح عملية سياسة المشاركة هذه تحقيق إجماع عالمي من قبل متلقي المصادر التي توفرها CANNI وRIR على نحو عادل وقابل للتوقع ومستقر.
- **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، ويضمن 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.

5.1.1.3 وقد أيدت ICANN الحاجة لتنفيذ DNSSEC على مستوى الجذر، وقدمت اقتراحًا لوزارة التجارة فيما يتعلق بدور وظائف IANA في توقيع اتفاقية مستوى الجذر في سبتمبر 2008، وقد أخذت استعداداتها للاضطلاع بهذا الدور

بالإضافة إلى توقيع نطاقات int. وarpa.. 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 وفقًا 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 org.icann وorg.iana. وأخيرًا، 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.

5.1.1.4 بالإضافة إلى ذلك، عملت ICANN مع (RIR's) وIEFT على تطوير تقنية rPKI لتقديم التصديق على مصادر الترقيم المعينة. كذا عمل فريق عمل IANA مع مجتمع TLD لتعقب التنفيذ الإجمالي للتسكين ضمن نظام TLD استجابة 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.

5.1.1.5 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.

5.1.2 عمليات خادم جذر DNS

5.1.2.1 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.

5.1.2.2 سوف تواصل ICANN العمل لإرساء دعائم علاقات رسمية مع مشغلي خادم اسم الجذر وفقاً لالتزامها في هذا الصدد المنصوص عليه في "البيان الصادر من مجلس ICANN عام 2006 لتأكيد المسئوليات الخاصة بإدارة القطاع الخاص في ICANN". وفي عام 2008، توصلت ICANN إلى اتفاقية خاصة بالمسئوليات المتبادلة مع اتحاد نظم الإنترنت فيما يتعلق بتشغيل جذر F وهو ما عزز من "الالتزام نحو تحسين أمن واستقرار وقابلية تشغيل نظام اسم النطاق (DNS) من منظور عالمي ولصالح مجتمع الإنترنت العالمي على نحو تطوري وعلى أساس من العلاقة المناظرة".

5.1.2.3 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.

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 (RAA). 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 تسجيلات gTLD

5.2.1.1 تتعاون ICANN مع مشغلي gTLD فيما يتعلق بالتنسيق الآمن والمستقر لـ TLDs. علاوة على ذلك، يوجد لدى كل من تسجيلات TLD عقداً 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 الأحكام 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 gTLD-ICANN 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.

5.2.1.2 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.

5.2.2 gTLDs وIDNs الجديدة

5.2.2.1 بينما تستعد ICANN لفتح عمليات إلى TLDs جديدة لتضمين أسماء النطاقات الدولية، تدرك ICANN الحاجة إلى بذل الجهود لضمان تحقيق عمليات آمنة ومستقرة ومرنة للداخلين الجدد في DNS وفي النظام 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. وسوف تتم عملية تقديم IDN ccTLDs عقب عملية مختلفة حيث أن هذا التقديم المبدئي يقتصر على السلاسل غير المتنافسة التي تمثل أسماء بلدان وأقاليم مناظرة إلى ccTLDs القائمة. في يوليو 2007، قدمت ACSS تعليقات على تأثير IDN على الأمن والاستقرار على مستوى الجذر بالنسبة إلى DNS مع توضيح عمليات التخطيط والاختبار.

5.2.2.2 سوف يقوم فريق مستقل من الخبراء بإجراء تقييم تقني لمقدمي الطلبات وTLDs المقدمة من جانبهم. علاوة على ذلك، توفر عملية gTLD الجديدة عملية RSEP مسبقة لتقييم المشكلات المحتملة على نطاق الأمن والاستقرار لخدمات التسجيل الجديدة المقترحة في طلب gTLD. وبالنسبة إلى IDN TLDs، فإن متطلبات السلسلة التقنية والتقييم المرتبط بها هي ذاتها الخاصة بكل من IDN gTLDs وIDN ccTLDs.

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

5.2.3 مسجلي gTLD

5.2.3.1 تتعاون ICANN كذلك مع المسجلين فيما يتعلق بالأمن والاستقرار والمرونة. وتخضع العلاقة القائمة بين ICANN والمسجلين تعاقدياً إلى اتفاقية اعتماد المسجلين القياسية (RAA). 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.

5.2.3.2 يعمل موظفو Liaison للمسجل الخاص بـ ICANN كخط دفاع أول لمراقبة 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).

5.2.3.3 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.

5.2.4 Whois

5.2.4.1 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.

5.2.4.2 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.

5.2.5 التوافق التعاقدي

5.2.5.1 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 الموقع الرسمي على http://reports.internic.net/cgi/registrars/problem-report.cgi. يتم التحقيق في الشكاوى المقدمة بشأن الانتهاكات المحتملة لـ RAA من قبل موظفي التوافق التعاقدي ويتم اتخاذ إجراء لضمان الالتزام عند اكتشاف أية انتهاكات للعقود المبرمة. 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.

5.2.5.2 يقوم قسم الالتزام التعاقدي كذلك بإدارة نظام الإبلاغ عن مشكلات بيانات Whois(WDPRS) والذي يمكن الوصول إليه من خلال موقع 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

ادعائاتهم بعدم دقة بيانات Whois، حيث يتم عقب ذلك نقل تلك الشكاوى إلى المسجلين لاتخاذ الإجراءات اللازمة. وبالتشاور مع المسجل واتحادات حقوق الملكية الفكرية (IPC)، تم إعادة تصميم WDPRS في عام 2008 ليكون قادراً على مواجهة عدة مشكلات أثارها مجتمع الإنترنت، والتي تضمنت الفعالية المحدودة والسعة المحدودة وعدم وجود سبل لمتابعة مدى الالتزام. ولقد تم تدشين WDPRS الجديد في ديسمبر 2008. ويواصل موظفو قسم الالتزام العمل على تحسين هذا النظام ساعين إلى زيادة دقة بيانات Whois.

5.2.6 حماية مالكي أسماء نطاقات gTLD

5.2.6.1 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 ANNIC 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 لـ InterNIC http://www.internic.net/. ولقد أجرت ICANN كذلك تعاوناً مع مجتمع المسجلين، لتشجيع دعم 6IPv لمالكي أسماء النطاقات.

5.2.6.2 علاوةً على ذلك، يتركز نشاط ICANN المعني بدعم المنظمات واللجان الاستشارية على مشكلات أمن واستقرار ومرونة مالكي أسماء النطاقات. ولقد قام مستشارو SSAC بتقديم توجيهات إلى المسجلين بخصوص الممارسات التي تساعد على تحسين مستوى حماية أسماء النطاقات والمشكلات المتعلقة بالتمويه السريع أو إساءة استخدام بيانات Whois والاستيلاء على الأسماء وكذلك حول مشكلات مالكي أسماء النطاقات الخاصة باعتبارات التجديد. وبعيداً عن SSAC، قامت اللجنة الاستشارية العامة (ALAC) بطرح 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. وقريباً، أخطرت ALAC مجلس GNSO بقلقها حيال استعادة أسماء النطاقات بعد انتهاء مدة صلاحيتها من قبل مالكي أسماء النطاقات. 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 LDccT وICANN بحفظ وتحسين أمن واستقرار ومرونة DNS لصالح مستخدمي الإنترنت على الصعيدين المحلي والعالمي. وهو ما ينعكس في برنامج إطار عمل المسائلة الذي يشكل الأساس الذي تقوم عليه مجموعة الاتفاقيات المبرمة بين تسجيلات 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. ولقد قامت IANA بتنمية علاقة

قائمة على الثقة 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 TLDs بالمتطلبات التقنية اللازمة لدعم تحقيق عمليات آمنة ومستقرة. إن المتطلبات الخاصة لخوادم الأسماء تضمن توافر النطاقات لدى 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 دائم للمساعدة في الحالات التي تستلزم إجراء تغيير سريع ودقيق في بيانات منطقة الجذر خاصتها. يتمثل الهدف الرئيسي لـ IANA في ضمان أمن واستقرار منطقة TLD ومنطقة الجذر.

5.2.9 الاستجابة المشتركة لإساءة الاستخدام الضارة لنظام 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. وتعمل ICANN بنشاط شديد مع التسجيلات والمسجلين لضمان توافر الوعي اللازم ولتيسير نشر المعلومات. إن تفويض ICANN يعد محدوداً في هذا المجال، ولهذا شاركت كنظير في المناقشات الخاصة بكيفية تمكين استجابات فعالة عند ظهور مواقف تشغيلية محددة.

5.2.10 توفير أمن واستقرار ومرونة DNS على نحو شامل

5.2.10.1 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. 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. علاوةً على ذلك، يشارك أعضاء SSAC في لجنة سياسة الإنترنت التابعة إلى مجموعة عمل مكافحة الخداع (APWG) وقامت بالمشاركة في إصدار تقارير رسمية حول كيفية قيام المخادعون باستغلال أسماء النطاقات والنطاقات الفرعية.

5.2.10.2 وتخطط ICANN إلى 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 بلدان العالم النامي ومواجهة إساءة استخدام DNS للأنشطة الضارة. يتوافر التقرير على الموقع التالي: http://www.gtisc.gatech.edu/icann09.

5.2.10.3 فضلاً عما سبق، قام موظفو ICANN والمنظمات المساندة واللجان الاستشارية بالمبادرة بزيادة حجم التعاون مع جهود مجموعة كبيرة من اصحاب 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.

5.3 التعاون مع منظمة مصادر الأرقام (NRO) وتسجيلات الإنترنت الإقليمية (RIRs)

يتم التفاعل بين ICANN وNRO وRIRs في ظل فهم عميق لضرورة قيام كل من RIRs وICANN بحفظ وتحسين أمن واستقرار ومرونة الإنترنت لصالح مستخدمي الإنترنت على الصعيدين المحلي والعالمي. ولقد شاركت ICANN مع هذه المنظمات في عدد من الأنشطة ذات الصلة بأمن واستقرار ومرونة الإنترنت. وعلى وجه الخصوص، تتعاون ICANN مع هذه المنظمات لتوقيع DNSSEC للأجزاء العكسية من شجرة DNS. إن RIRs، بصفتها تسجيلات عناوين IP، مشاركة على نحو مباشر في الجهود المعنية بتمكين التصديق على العناوين ووجهات بروتوكول البوابة الحدودية من خلال جهود rPKI، وسوف تواصل ICANN سعيها للمشاركة معهم في هذه الجهود.

5.4. عمليات الأمن والاستمرارية التجارية لـ ICANN

5.4.1 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، وكذلك للإيفاء بمسئوليات الشركة وكمساهم من المجتمع في تحقيق أمن واستقرار ومرونة نظم المعرفات الفريدة للإنترنت.

5.4.2 تعمل ICANN نحو تحقيق برنامج أمني شامل يقوم بإدارة المخاطر عبر كافة أصولها من معلومات وعاملين وأصول مادية. وفي خريف 2008، قامت ICANN بتعيين مدير لعمليات الأمن والذي تولى مسئولية هذا البرنامج. توفر ICANN المعلومات وبيانات العمليات الحساسة وتعتمد على استخدام تقنية المعلومات (IT) لتنفيذ تلك العمليات. 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. يتركز تخطيط أمن العاملين على حماية موظفي ICANN في مواقع العمل الرئيسية خاصتها وفي الأماكن التي يقومون فيها بتنفيذ أنشطة ICANN العامة، بحيث تتضمن توفير الأمن لهم خلال اجتماعات ICANN. ولقد قامت ICANN بوضع عملية تخطيط لإدارة المخاطر المرتبطة بأمن العاملين مع تعزيز فريق الأمن الداخلي الخاص بها فضلاً عن توفير الدعم من مستشاري الأمن. قامت ICANN كذلك بوضع عملية تخطيط لإدارة المخاطر المرتبطة بمرافقها المادية بحيث تتضمن موقعها الرئيسي في مارينا ديل راي بكاليفورنيا في الولايات المتحدة الأمريكية وكذلك مكاتبها الفرعية ومرافقها الاحتياطية.

5.4.3 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. ومع نمو ICANN، ينمو أساس أصول الشركة إلى جانب نشاطها العالمي وحضورها العام. هذا ومن المتوقع أن تصبح بيئة الأمن التجاري لـ ICANN مثيرة للتحديات على نحو

متزايد مع مواصلة ICANN التأكيد على أهمية توافر إدارة فعالة للمخاطر واستمرارية العمل والأمن كأجزاء جوهرية من عملياتها التجارية.

5.5 أنشطة المنظمات الداعمة واللجان الاستشارية لـ ICANN

5.5.1 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 تحت عناية 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.

5.5.2 تعمل ICANN حالياً مع المجتمع لمراجعة عملية تطوير سياسة gTLD (PDP) الحالية لجعلها أكثر فاعلية ومقدرة على الاستجابة لاحتياجات تطوير سياسة ICANN. من بين التنقيحات العديدة المتصورة 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.

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

5.5.4 تعمل ASO على وضع سياسة ترتبط بتخصيص مجموعات عناوين IPv4 وIPv6 ومجموعات رقم AS إلى RIRs.

5.5.5 علاوةً على ماسبق، يوجد لدى ICANN أربع لجان استشارية تقدم توصياتها إلى مجلس الإدارة وإلى مجتمع ICANN - اللجنة الاستشارية العامة (ALAC) واللجنة الاستشارية الحكومية (GAC) واللجنة الاستشارية المعنية بنظام خادم الجذر (RSSAC) واللجنة الاستشارية للأمن والاستقرار (CSSA). يمكن الإطلاع على معلومات تفصيلية حول وظائف تلك اللجان وعملياتها وأنشطتها على موقع http://www.icann.org/en/committees/gac/. عادة ما تتعاون هذه اللجان الاستشارية من خلال هيكل المنظمات الداعمة/اللجان الاستشارية فيما تبذله من مجهودات، وعلى الأخص مع SSAC. تلقى هذه اللجان الدعم من فريق سياسة ICANN في إجراء الدراسات وحضور المداولات وتقديم التوصيات.

5.5.6 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 الإطلاع على معلومات تفصيلية حول أنشطة SSAC على موقع www.icann.org/en/committees/security.

5.5.7 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 نبذات حول الموضوعات المتعلقة بالأمن والاستقرار، ونشر الأنشطة المرتبطة بالسياسة بين أعضاء المجتمع من خلال التحديث الشهري للسياسة (http://www.icann.org/en/topics/policy/).

5.6 التعاون العالمي المعني بتحسين الأمن والاستقرار والمرونة

5.6.1 الشركاء والأنشطة على المستوى العالمي

إن الهدف الرئيسي لإستراتيجة التعاون العالمي لمنظمة ICANN فيما يتعلق بموضوعات الأمن والاستقرار والمرونة يتمثل في دعم واستخدام العمل القائم الذي يتم على يد فريق الشراكات العالمية. لقد كانت ANNIC شريكاً نشطاً في مجموعة كبيرة من المنتديات العالمية المرتبطة بالإنترنت، والتي يتناول العديد منها قضايا أمن واستقرار ومرونة الإنترنت. إن مجموعة الشركاء والأنشطة الواردة أدناة غير شاملة ولسوف تسعى ICANN إلى التعاون مع آخرين عند إتاحة الفرصة لذلك. ومن بين الشركاء العالميين الرئيسيين:

- فريق عمل 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 في 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.
- جمعية الإنترنت (ISOC): تعمل 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 الازم 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 وتشوشها.
- منتدى إدارة الإنترنت: يقوم منتدى IGF برعاية عدداً من الحوارات التي تضم عدداً من أصحاب المصالح والخاصة بأمن الإنترنت والثقة به. كما قام 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 - مركز العمليات والتحليل والاستجابة (DNS-OARC): سوف تواصل ICANN دورها كراعي داعم ومشارك نشط في كافة أنشطة OARC-DNS.

5.6.2 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 موضحاً أدناه، سوف تواصل ICANN تقديم المساعدة والخبرة للأنشطة التي تخضع لرعاية هذه المنظمات.
- ***مراكز معلومات الشبكات (NICs)/مجموعات مشغلي الشبكات (NOGs)*** - سوف تواصل ICANN مشاركتها في هذه المنتديات لضمان نجاح أنشطتها في توفير عمليات آمنة ومستقرة على الشبكة على أفضل نحو ممكن، متضمناً تنسيق أنشطة IANA.
- ***آسيا*** - قامت ICANN بالمبادرة ببرنامج التدريب على أمن ومرونة ccTLD بالتعاون مع اتحاد TLD لدول أسيا المطلة على المحيط الهادئ (APTLD) في مايو 2008 في كوالا لامبور. وهي تواصل تلقي دعم قوي للأنشطة التي تتم في هذه المنطقة. ولسوف 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 (CENTR) 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 عامي 2008 و2009 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 قبل عقد الاجتماع العام الدولي الرابع والثلاثين لـ ICANN والذي عقد في مارس 2009، ولقد خطط لعقد جلسات مستقبلية مع LACTLD. وتعتزم ICANN كذلك تقديم تدريب ccTLD بالتعاون مع الاتحاد الأفريقي لنطاقات المستوى الأعلى (AfTLD) وAfrica-ISOC. وقد تم البدء في هذه الأنشطة في إبريل 2009 إبان اجتماع المنظمة الأفريقية لنطاقات المستوى الأعلى (AFTLD) في أروشا بتنزانيا.

5.6.3 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. أما على المستوى الداخلي فيما بين المنظمات الحكومية، سوف تظل ICANN تعمل بنشاط لتحديد دورها في المناقشات العالمية الدائرة حول الأمن والمشاركات المعنية بإدارة الأمن والمرونة المرتبطة بنظم المعرفات الفريدة للإنترنت. وتتضمن العناصر الرئيسية للمشاركة ما يلي:

- ***الاتحاد الدولي للاتصالات السلكية واللاسلكية (ITU)*** - يسعى ITU إلى أجندة عالمية لأمن الإنترنت (GCA) والمعرّفة "كإطار عمل للتعاون الدولي الرامي إلى تحسين الثقة والأمن في مجتمع المعلومات". وضمن سياق الجهد الأوسع نطاقاً، قام قطاع تطوير الاتصالات السلكية واللاسلكية التابع إلى ITU، والذي يشار إليه بالاختصار D-ITU، بإنشاء برنامج واسع المدى للعمل مع الدول النامية لتعزيز الوعي القومي وبرامج دعم القدرات المرتبطة بتحسين مستوى أمن الإنترنت. سوف تعزز ICANN من مشاركتها مع ITU في جهوده المعنية بأمن الإنترنت من خلال العمل على رفع مستوى الوعي وتعزيز الإمكانيات استناداص على دورها التقني في ضمان أمن ومرونة DNS.
- ***منظمة التعاون والتنمية الاقتصادية (OECD)*** - سوف تواصل ICANN مشاركتها في المنتديات المتعلقة بأمن الإنترنت مثل الجهود المتواصلة التي تبذلها لمكافحة البرامج الضارة OECD. كذا ستواصل ICANN المشاركة في جهود APEC في هذا الصدد.
- ***المنظمات الدولية الأخرى واللجان الاقتصادية الإقليمية التابعة للأمم المتحدة*** - سوف تتعاون ICANN مع المنظمات الدولية الأخرى واللجان الاقتصادية التابعة للأمم المتحدة، مستهدفة جهودها الرامية إلى تفعيل الأنشطة الإقليمية المصممة خصيصاً لتحسين الأمن والمرونة في DNS. وستقوم هذه الأنشطة على مذكرات التفاهم الموقعة بين ICANN وعدداً من المنظمات.

6. خطط ICANN لفبراير 2010 المعنية بتحسين الأمن والاستقرار والمرونة

إن أنشطة ICANN المرتبطة بتحسين الأمن والاستقرار والمرونة، والموارد المخصصة لهذه الجهود، تتم تحت توجيه عمليات التخطيط الإستراتيجية والتشغيلية. ومع التقدم قدماً في العام التشغيلي 2009-2010، تعتزم ICANN المطالبة بتدشين عدداً من المبادرات الرئيسية مثل:

- ***عمليات IANA*** - الدعم والتعليم والإعداد لتنفيذ DNSSEC على مستوى الجذر كما دعت إليه خطة ICANN الاستراتيجية 2009-2012 بالإضافة إلى تحسين إدارة منطقة الجذر من خلال الأتمتة، وتحسين مصادقة الاتصالات مع مديري TLD
- ***عمليات خادم منطقة جذر DNS*** – مواصلة السعي لتحقيق إقرار متبادل للأدوار والمسئوليات والمبادرة بجهود تطوعية لتنفيذ تخطيط وتدريبات الطوارئ.
- ***تسجيلات gTLD*** – ضمان تقييم مقدمي طلبات الحصول على gTLD وIDN ومواصلة تقديم عمليات آمنة. سوف تعمل ICANN على تطوير خطة استمرارية تسجيل gTLD واختبار نظام مستودع البيانات.
- ***تسجيلات 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
- ***الالتزام 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.
- ***الاستجابة لإساءة الاستخدام الضارة لاسم النطاق*** – سوف تزيد ICANN من جهودها الحثيثة فيما يخص السلوك الضار الذي يتيحه استخدام DNS مع تسهيل مشاركة المعلومات لتمكين الاستجابة على نحو فعال.
- ***العمليات الداخلية لأمن واستمرارية ICANN*** - تحرص ICANN على تنفيذ برامجها الأمنية ضمن الإطار الإجمالي لإدارة مخاطر الشركة وإدارة الأزمات وبرامج استمرارية العمل. وسوف يقع ضمن بؤرة الاهتمام إنشاء أساس قوي من الخطط الموثقة والإجراءات الداعمة
- ***ضمان المشاركة والتعاون العالمي*** – سوف تعمل ICANN على تحسين الشراكات لتضم فريق عمل هندسة الإنترنت (IETF) ومجتمع الإنترنت (ISOC) وتسجيلات الإنترنت الإقليمية ومجموعات مشغلي الشبكات ومركز عمليات وتحليل واستجابة DNS الذي يطلق عليه (DNS-OARC). 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 FY10.

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.

6.1.1.1 العمل مع شركاء إدارة منطقة الجذر ووزارة التجارة الأمريكية وVeriSign وبالتشاور مع مجتمع الإنترنت العالمي لتنفيذ عملية توقيع DNSSEC لمنطقة الجذر. وستواصل ICANN متابعة تنفيذ العملية الموضحة في اقتراح سبتمبر 2008. ووفقًا للأولوية الموضحة في الخطة الاستراتيجية 2009-2012، ستكون ICANN جاهزة تشغيليًا لنشر DNSSEC في منطقة الجذر بنهاية عام 2009. وقد اقترحت ICANN منهجًا يتيح استمرارية، غير متقطعة، لآلية توزيع جذر DNS، وهي مهمة مشتركة بين ICANN وVeriSign وNTIA ومشغلي خادم الجذر في تشغيل DNSSEC. وقد قدمت ICANN حلول مرنة تمثل مناهج مؤقتة للوصول إلى حلول انتقالية قبل الوصول إلى حلول دائمة، وقد أجرت استعداداتها التشغيلية من أجل أن تلعب هذا الدور.

سوف تواصل ICANN السعي نحو تحقيق العديد من الأنشطة لتمكين تنفيذ DNSSEC خلال DNS عالميًا. 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 و.arpa. 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.

6.1.1.2 تتضمن مبادرات تحسين وظائف IANA الأخرى:

- تحسين إدارة منطقة الجذر من خلال الأتمتة (برنامج eIANA/RZM)، 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 المتبناه 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

6.1.2 عمليات خادم جذر DNS

6.1.2.1 سوف تواصل ICANN السعي لتحقيق إقرار متبادل للأدوار والمسئوليات مع مشغلي الجذر كجزء من مجمل دورها في تنسيق DNS. 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.

6.1.2.3 تخطط ICANN لمواصلة تحسين تشغيل الجذر L. ولقد تعاقدت ICANN مع OARC-DNS لدراسة تأثير التغيرات متضمنة تنفيذ gTLDs وIDNs جديدة وتنفيذ 6IPv والتنفيذ المحتمل لتعيين DNSSEC 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 TLD

6.2.1 تسجيلات gTLD

سوف تواصل ICANN التنسيق التعاقدي المرتبط بعمليات gTLD ليتضمن تطبيقات فحص الخدمات الجديدة عبر RSEP. هذا وتتوقع ICANN أن تتضمن عمليات المراجعة الاقتراحات التي تطالب بتنشيط RSTEP لتقييم اعتبارات الأمن 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. علاوةً على ذلك، تخطط ICANN للعمل مع DNS-OARC لإنشاء بوابة لمشاركة المعلومات ذات الصلة بأفضل الممارسات والجهود المشتركة المعنية بالأمن والاستقرار والمرونة ليتم استخدامها من قبل مجتمع التسجيلات بالكامل.

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، وكل 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 خلال مدة 18 شهراً القادمة. هذا ومن المتوقع استلام تقريرهما بشأن هذه الدراسة في سبتمبر 2009.سوف تعمل ICANN كذلك على وضع أحكام تقييم مقدمي الطلبات لضمان قدرتهم على تنفيذ عمليات أمنة تقنياً والتحقق من التزامهم بأحكام Whois ومن قدرتها على توفير تخطيط سليم لحالات الطوارئ وضمان حماية مالكي أسماء النطاقات. ولسوف تواصل ICANN تطوير خطة استمرارية تسجيل gTLD وبرنامج التدريبات، بحيث يتضمن اختبار مباشر لنظام مستودع البيانات. 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. ستواصل ICANN عملها مع IEFT في دورها العام في وضع بروتوكولات الإنترنت لإتمام مراجعة، ومن ثم اعتماد، بروتوكول IDNA آمن ومستقر. في حالة عدم اعتما البروتوكول الموضوع من قبل IEFT على نحو تام، قد تقوم ICANN بموجب توصيات من المجتمع التقني بوضع متطلبات خاصة إضافية على IDN TLDs

بهدف ضمان عملها لأجل طويل حتى يتم الانتهاء من مراجعة البروتوكول. 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.

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 ccTLD. تخطيط الأمان وحالات الطوارئ. وتعتزم ICANN خلال العام التالي توفير القدرة على تقديم برنامج ACRP بلغات غير الإنجليزية وبأن تعمل مع معهد هندسة البرمجيات في جامعة كارنيج-ميلون للاستفادة من إطار عمل هندسة المرونة (REF) الخاص بها من خلال برنامج تطوعي لتقييم مدى نضج جهود أمن واستقرار ومرونة TLD.

6.2.5 المُسجلون

ستواصل ICANN تطوير سياساتها بهدف تحسين متطلبات اعتماد المسجلين ومستودعات البيانات من خلال التحسينات التي تضفيها 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 الالتزام التعاقدي

6.2.6.1 ستواصل ICANN زيادة نطاق أنشطة فرض الالتزام التعاقدي لتتضمن زيادة حجم فريق الالتزام التعاقدي. هذا وسوف تشتمل المجالات الرئيسية الجديدة على بدء عمليات تدقيق للأطراف المتعاقدة كجزء من تنفيذ تعديلات اتفاقية اعتماد المسجلين الصادرة في مارس 2009 (RAA). علاوةً على ذلك، سوف يعمل فريق الالتزام التعاقدي خلال عام 2009 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.

6.2.6.2 لقد قام قسم الالتزام التعاقدي بدراسة سبل تقييم دقة معلومات الاتصال في بيانات Whois ضمن نظام gTLD وقام بتقييم حدود استخدام مالكو أسماء النطاقات لخدمات الخصوصية والبروكسي لإخفاء هويتهم. وسعياً منها للتشجيع على الالتزام 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 المشتركة لإساءة الاستخدام الضارة لنظام اسم النطاق

سوف يواصل موظفو ICANN كذلك تعزيز الجهود المتعاونة 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 تعليقًا عامًا 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 توفير أمن DNS على نحو شامل

سيسعى فريق عمل ICANN إلى تعزيز الندوة الخاصة بأمن واستقرار ومرونة DNS التي أقيمت في فبراير من عام 2009 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 OARC-DNS 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 التعاون مع NRO وRIRs

تعتزم ICANN مواصلة التعاون مع NRO وRIRs والمشاركة في الأنشطة ذات الاهتمامات المشتركة المرتبطة بالأمن والاستقرار والمرونة. وسوف يسعى موظفو ICANN نحو إشراك RIRs في تحديد أي الأنشطة المشتركة يلزم تحسينها حتى يتسنى ضمان أمن واستقرار ومرونة DNS. سوف تشتمل هذه المناقشات على فهم نوايا RIRs

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 الأمن والاستمرارية التجارية لـ ICANN

6.4.1 سوف يحرص موظفو ICANN على أن يتم تنفيذ برامجها الأمنية ضمن إطار إدارة المخاطر التجارية الشاملة وإدارة الأزمات وبرامج الاستمرارية التجارية. وسوف يقع ضمن بؤرة الاهتمام إنشاء أساس قوي من الخطط الموثقة والإجراءات الداعمة. وسوف تشتمل المبادرات الخاصة الرامية إلى تحسين إدارة المخاطر في NNICA ووضع الاستمرارية بها حتى منتصف عام 2010 على وضع خطط لاستمرارية أعمال ICANN / إدارة المخاطر وإجراء التدريبات الداخلية لـ ICANN بالاشتراك مع الأنشطة الأخرى بحيث تتضمن تدريبات استمرارية gTLD والإعدادات للاجتماعات. وسوف تعمل ICANN كذلك على تحسين استخدامها للمواقع البديلة كجزء من تنفيذ استمرارية تقنية المعلومات. ومن الجهود الكبرى المبذولة هناك السعي لإنشاء مركز آمن لتقنية المعلومات ومرافق احتياطية لدعم برامج استمرارية ICANN. وتخطط ICANN لإجراء تقييم لمخاطر المؤسسة بحلول منتصف 2009.

6.4.2 خلال العام القادم، سوف يعمل موظفو ICANN على ضمان تواجد نطاق كامل من المعلومات والأفراد وعمليات الأمان في أماكنها عبر جميع عملياتها. 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 في الوصول المنطقي والفعلي، ورفع وعي العاملين والتدريب على الاستجابة للحوادث وخطة لأمن المسافر والتخطيط لأمن الاجتماعات والاستجابة لها. ستضمن ICANN تطوير تعاون المجتمع الناشئ والتوعية بأدوات تكنولوجيا المعلومات وتوزيعها باستخدام عناصر تحكم الأمن المناسبة في مكانها.

6.4.3 يخطط موظفو ICANN للعمل مع معهد هندسة البرمجيات (SEI) في جامعة كارنيج ميلون لتعزيز إطار عمل هندسة مرونة SEI (REF) لضمان اشتمال برامجها المعنية بأمن الإنترنت والاستمرارية وإدراة المخاطر على أفضل الممارسات، ولقياس التحسينات عبر فترة من الزمن. وبحلول نهاية 2009، تخطط ICANN لتقييم عملياتها الأساسية بما يتوافق مع منهج REF. كما تخطط ICANN أيضًا للحصول على مراجعة خارجية وتدقيق لبرامج الأمن والمتابعة الخاصة بها خلال النصف الأول من 2010.

6.5 المنظمات الداعمة واللجان الاستشارية التابعة إلى ICANN

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

6.5.2 في يناير 2009، أصدر مجلس GNSO تقرير مبدئي حول استضافة التمويه السريع للتعليق العام والمزيد من الإجراءات الاستشارية، كما تضع المنظمة أيضًا في الاعتبار الكثير من الدراسات المحتملة الخاصة بـ 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 أسست GNSO "مجموعة عمل" لمواجهة إساءة استخدام

التسجيل وهي تقوم حالياً بدراسة مبادرة ذات صلة باستعادة اسم النطاق بعد انتهاء صلاحيته. ومن أجل الجمع بين اذلك العدد الكبير من اصحاب المصالح في ICANN المهتمين بهذه الموضعات، تضمن الاجتماع العام العالمي الـ 34 لـ ICANN الذي انعقد في مدينة مكسيكو سيتي، في مارس 2009، وجود ورشة عمل موسعة حول الجرائم الإلكترونية وورشة عمل أخرى حصرية للتركيز على سوء استخدام التسجيل.

6.6 المشاركة العالمية

6.6.1 تمديد الشراكات القائمة

يعتبر جوهر استراتيجية 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 لـ FY10 مع هذه الشراكات:

- ***مجتمع الإنترنت (ISOC)*** - 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 وتشوشها.
- ***DNS-OARC*** - ستقوم ICANN بدعم تشكيل المنفذ المضيف DNS-OARC لتبادل المعلومات ومشاركة أفضل ممارسات الأمن والاستقرار والمرونة داخل مجتمع TLD. كما اشتركت ICANN أيضًا 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.
- ***آسيا*** – تخطط NNICA لاستكشاف علاقة مع مركز أمن إنترنت عالمي تدعمه حكومة ماليزيا مع التركيز على كيف يمكن لـ ICANN المساهمة في الجهود العالمية لمكافحة أنشطة الإنترنت الضارة التي يمكن أن تهدد نظم المعرفات الفريدة للإنترنت.

6.6.2 المؤسسات التجارية

ستقوم ICANN بمتابعة الندوة المنعقدة في فبراير 2009 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.

6.6.3 المشاركة في الحوار المعني بأمن الإنترنت العالمي

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

- ***مركز الدراسات الاستراتيجية والدولية (CSIS)*** - تخطط ICANN لدعم سلسلة من ورش العمل خلال 2009-2010 لتتضمين تناول موضوع دور المنظمات متعددة اصحاب المصالح في تحقيق أمن الإنترنت العالمي. وستتضمن هذه الجهود المشتركة ورش عمل مع المؤسسات الشريكة لـ CSIS من خارج الولايات المتحدة.
- ***المجلس الأطلنطي*** - تخطط ICANN للتعاون مع "المجلس الأطلنطي" في الأنشطة ذات الصلة بمقابلة نقاط الضعف المتزايدة للدول والمنظمات الأصغر في مواجهة هجمات واعتراضات الإنترنت المتنامية. وستركز ICANN على دورها في تميكن مرون DNS في مواجهة هذه النشاط.

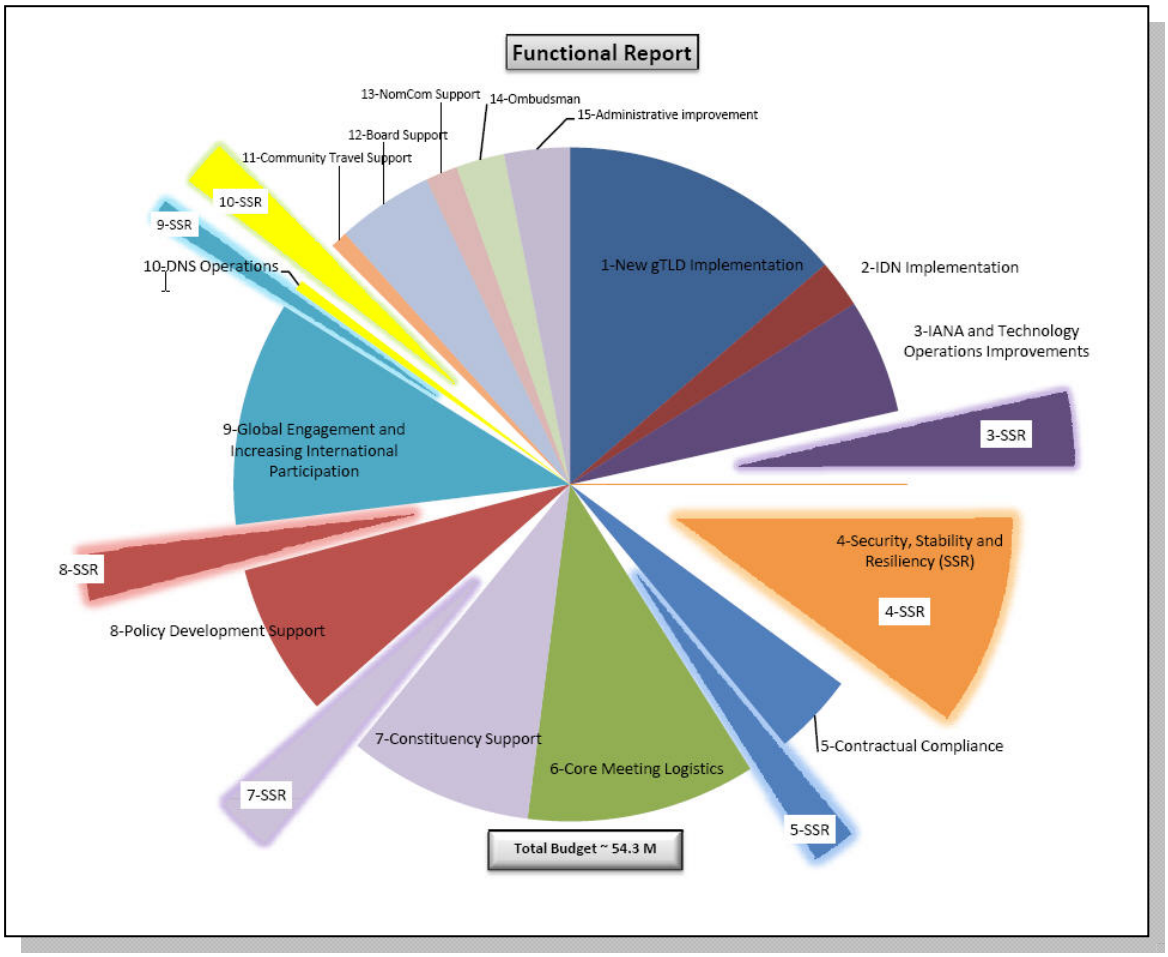
وستقوم ICANN بالسعي الحثيث وراء الفرص المتاحة مع مفكرين أخرين ومؤسسات أكاديمية أخرى للتعاون من أجل ريادة تحديد المخاطر المتعلقة بالأمن والاستقرار والمرونة.

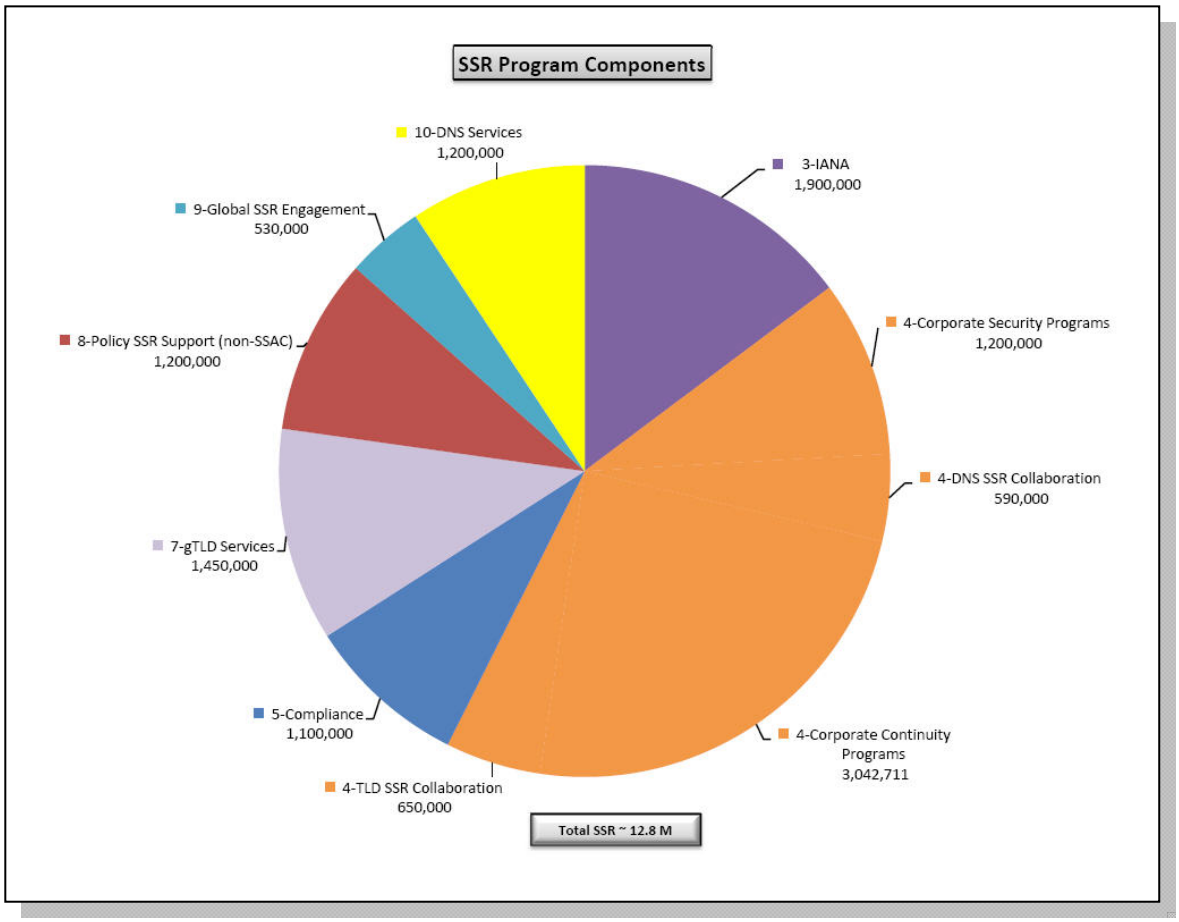
7. الخاتمة

تفهم ICANN، كناحية هامة من مهمتها في كسب ثقة العامة، أن برامجها وأنشطتها يجب أن تساهم في جعل نظم التعريف الفريدة من الأهاف الفريدة للحصول على بيئة إنترنت أكثر أماناً واستقراراً ومرونة. ومع تزايد التحديات، أصبحت جهود ICANN في هذا المجال أصبحت أكثر خشونة. كما تعترف ICANN أيضًا بحدود دورها ومواردها وتضع خطة لاستراتيجيتها 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.

منذ تأسيسها، قامت ICANN بتوفير الكثير من البرامج والأنشطة الخاصة بتحسين أمن واستقرار ومرونة الإنترنت والتي تتضمن الكثير من الجهود المرتبطة بوظائف DNS/التوجيه الرئيسية؛ والعمل مع ومجتمعات تسجيلات ومسجلي TLD؛ والاشتراك مع NRO وRIR؛ برامج الأمن التجاري وبرامج الاستمرارية؛ الأنشطة الخاصة بالمننظمات 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 الاستراتيجي والتشغيلي لـ ICANN مما يسمح لجهود ICANN بالبقاء ذات صلة وشيكة ولضمان تركيز الموارد على أهم المسئوليات والمساهمات الخاصة بها.

الملحق أ


Functional Report
13-NomCom Support
14-Ombudsman
15-Administrative improvement
12-Board Support
11-Community Travel Support
10-SSR
9-SSR
10-DNS Operations
1-New gTLD Implementation
2-IDN Implementation
3-IANA and Technology Operations Improvements
3-SSR
9-Global Engagement and Increasing International Participation
4-Security, Stability and Resiliency (SSR)
4-SSR
8-SSR
8-Policy Development Support
7-Constituency Support
6-Core Meeting Logistics
5-Contractual Compliance
7-SSR
5-SSR
Total Budget ~ 54.3 M


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

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

- IANA - $1.9 M
- DNS Services - $1.2 M
- DNS SSR Collaboration - $590 K
- gTLD Services - $1.45 M
- Compliance - $1.1 M
- TLD SSR Collaboration - $650K

OVERALL SSR – $12.8 M

- Global SSR Engagement - $530K
- Corporate Security Programs - $1.2 M
- Corporate Continuity Programs - $3.0 M
- Policy SSR Support (incl SSAC) - $1.2M

IANA Security, Stability and Resiliency (IANA)

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

ICANN DNS Services (IT Services)

Objectives	Deliverables (milestones)
- Prepare for DNSSEC zone signing for ICANN zones, ARPA-related zones and the root - Implement Trust Anchor Repository (TAR) - Secure, resilient L-root operation	- Trust Anchor Repository in full production: June 09 - L-root improvement (new design deployed at LA and Miami, 3rd node deployed at Prague): June 09 - Production infrastructure in place for signing root zone: Oct 09 - DNSSec signed ICANN zones: Oct 09
Key Stakeholders - ICANN IT Services Team - ICANN IANA staff, DoC, VeriSign - ICANN Security & Resiliency Team	**Resources (FY 10)** Human – 7.0 FTE (including related IT and other staff support) Financial – $1.2M to support FTEs; planned capital investments for back-up services; DNSSec, L-root, improvements; backup facilities; professional services and travel

ICANN gTLD Registry/Registrar Services (Services)

Objectives	Deliverables

- Ensure implementation new gTLD/IDNs addresses SSR issues
- Continue maturing data escrow process & gTLD continuity procedures
- Conduct RSEP/RSTEP processes on registry services proposals
	- Enhanced gTLD implementation process from SSR perspective
	  - SSAC/RSSAC study complete (Fall 09)
	  - Improved applicant guidebook (Aug 09)
	- Conduct data escrow test (Aug-Sep 09 or Jan 10)
	- Community failover exercise (Jan 10)
	- RSEP/RSTEP studies as required

Key Stakeholders - Registries/Registrars - ICANN Services staff - ICANN Security & Continuity staff - GNSO/SSAC	**Resources (FY 10)** Human – 2.75 FTE Financial – $1.45M includes portion of evaluation staff/support for new gTLD/IDN activities to include TAS security; dedicated RSEP/RSTEP funds; support for testing/contingency exercise; staff travel/support

Contractual Compliance (Services)

Objectives	Deliverables

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

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

TLD Security, Stability & Resiliency Collaboration

(Security)

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

DNS Security, Stability & Resiliency Collaboration

(Security)

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

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

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

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

Objectives	Deliverables

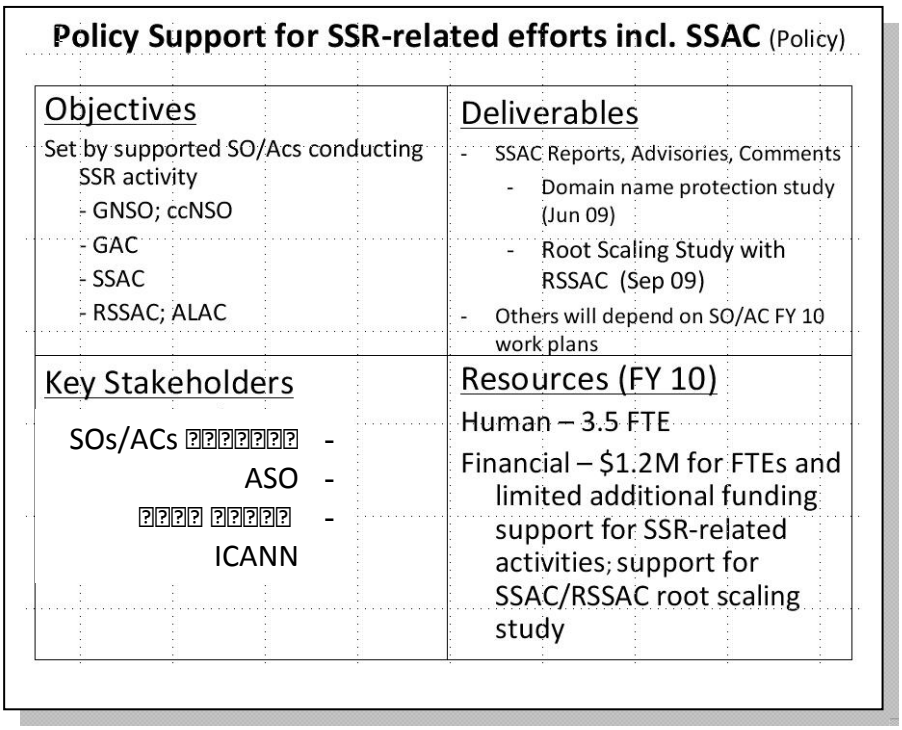
- Improve Business Continuity program
  - Establish formal plan
  - Establish secure data center
  - Establish formal drill/exercise programs
	- Initial ICANN Business Continuity plan (Oct 09)
	  - Improved Crisis Management plan (Aug 09)
	- Establish Secure IT Data Center (Sep 09)
	- Exercise Business Continuity/Crisis Management (Spring 10)

Key Stakeholders - ICANN Security & Resiliency Team - ICANN IT/IANA/DNS Ops - ICANN Human Resources - ICANN Global Meetings Team - ICANN Staff	**Resources** Human – 5 FTEs (includes planning and IT for data center) Financial – $3.0M including FTEs, capital support for data center, professional services for conducting training and audits

Global Security, Stability and Security Engagement

(Global Partnerships & Security)

Objectives	Deliverables
- Sustain partnerships with key organizations (ISOC; IISI; IMPACT; EC/ENISA; CSIS; Atlantic Council) - Continue participation in IGO sponsored cyber security dialogues OECD, IGF, others) - Collaborate with others on global cyber security response	- Conduct joint activities with partner organizations (One per trimester) - Engagement in forums across all major regions (On-going) - Engage with Forum of Incident Response and Security Teams regarding ICANN role in response (initial findings Jan 2010)
Key Stakeholders - Global/international organizations - ISOC; IETF; ITU; IGF - Cyber security forums - Governments/Commercial Stakeholders - ICANN Global Partnerships Team & Security Staff	**Resources (FY 10)** Human – 1.5 FTE Financial – $530K for FTEs; staff/travel support; support to ICANN-led or supported forums; professional services support for metrics development


Policy Support for SSR-related efforts incl. SSAC (Policy)
Objectives
Set by supported SO/Acs conducting SSR activity
- GNSO; ccNSO
- GAC
- SSAC
- RSSAC; ALAC
Deliverables
- SSAC Reports, Advisories, Comments
- Domain name protection study (Jun 09)
- Root Scaling Study with RSSAC (Sep 09)
- Others will depend on SO/AC FY 10 work plans
Key Stakeholders
SOs/ACs
ASO
ICANN
Resources (FY 10)
Human – 3.5 FTE
Financial – $1.2M for FTEs and limited additional funding support for SSR-related activities; support for SSAC/RSSAC root scaling study

الملحق ب - قاموس مصطلحات واختصارات خطط SSR

ACRP - الاستجابة للهجوم ولحالات الطوارئ (ACRP)

فترة السماح بالإضافة - 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 النظام المستقل: 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 رسميًا 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 الاستراتيجية والدولية يقدم رؤى استراتيجية 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 – يحدد بروتوكول الإنترنت تنسيق العبوات ومخطط العنونة. وتجمع معظم الشبكات بين بروتوكول الإنترنت مع بروتوكول مستوى أعلى يُدعى بروتوكول التحكم في الإرسال (TCP)، وهو ما ينشئ ارتباطًا ظاهريًا 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. ويصنع IP/TCP ارتباطًا بين مضيفين بحيث يمكنك إرسال رسائل للأمام والخلف.

IPv4 - بروتوكول الإنترنت الإصدار الرابع، هو التنقيح الرابع في تطوير بروتوكول الإنترنت (IP) وهو أول إصدار من البروتوكول يتم نشره بصورة واسعة. ويشكل مع 6IPv مركز أساليب تكوين الشبكات القائمة على المعايير الخاصة بالإنترنت، وهو مازال حتى الآن أوسع بروتوكولات طبقات الإنترنتانتشارًا.

IPv6 - بروتوكول الإنترنت الإصدار السادس هو بروتوكول الجيل التالي من طبقة الإنترنت لأعمال الإنترنت التي تغيرهاالعبوات والإنترنت. وفي ديسمبر 1998، عينت فريق عمل هندسة الإنترنت (IETF) الإصدار السادس من بروتوكول الإنترنت IPv6 كالنسخة التي خلفت الإصدار الرابع بإصدار مواصفات Standards-Track (تتبع المعايير)، RFC 2460.

ISOC – جمعية الإنترنت

IT – تكنولوجيا المعلومات

شبكات الاختلاس الإلكترونية - يتم إنشاؤها عادةً بخداع المستخدمين العاديين بفتح مرفق على أجهزة الكمبيوتر الخاصة بهم والذي يبدو أنه لا يفعل شيئًا ولكنه في الواقع يثبت برنامجًا ليتم استخدامها لاحقًا في الهجوم. وهذه الأجهزة المصابة يتم تجميعها لتكون شبكات يمكن بعد ذلك استهدافها، بالهجمات الضارة عادةً، بكل سهولة.

الضعف الضار للذاكرة المؤقتة - استغلال تدفق في برنامج DNS لجعله يقبل معلومات غير الصحيحة التي تتسبب في أن يخزن الخادم مؤقتًا 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 إساسية النظام المستهدف على الإغلاق، وبالتالي تمنع استخدام المستخدمين الشرعيين.

الهجمات الموزعة لرفض الخدمة (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 تأثيرًا 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 مساءة الاستخدام منخفضًا، لكن التأثير على الهدف يكون كبيرًا. ويقدر عامل التكبير بنسبة 1:73 من الهجمات، ووفقًا لهذه الطريقة تتتجاوز 7 جيجا بايت في الثانية.

DNS – نظام اسم النطاق الذي يقوم بترجمة أسماء النطاقات (الأبجدية) إلى عناوين IP (رقمية). لأنها أسهل في الحفظ حينما تكون أسماء النطاقات أبجدية. ومع ذلك فإن الإنترنت معتمد على عناوين IP الرقمية، على سبيل المثال (198.123.456.0). حينما تستخدم اسم نطاق (www.examplir.gratis.com)، تترجم خدمة DNS الاسم الأبجدي إلى عنوان IP الرقمي المقابل.

DNSSEC - امتدادات أمان نظام اسم النطاق تقدم طريقة للبرامج للتأكد من أن بيانات نظام أسماء النطاقات (DNS) لم يتم تعديلها أثناء مسارها عبر 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 ارتجاعيًا مع NSD 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" جزءًا صميمًا 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 المسؤولة عن إحداث عمليات التغيير والإضافة والحذف في ملف منطقة الجذر والتأكيد على صلاحية هذه التغييرات، يجب عليها إنشاء ملف محدث لمنطقة الجذر الناشئ وتوقيعه رقميًا. عندئذٍ يجب إرسال هذا الملف المُوَقع إلى منظمة أخرى (حاليًا شركة VeriSign) للتوزيع. بمعنى آخر، يجب أن تكون المنظمة المسؤولة عن القواعد الأساسية للثقة – والتي تقوم بالتأكيد على صلاحية التغييرات في منطقة الجذر مع مشغلي نطاقات المستوى الأعلى – بالتصديق أيضًا على صلاحية المنتج النهائي قبل توزيعه.

التشغيل الأولي لاسم النطاق - الممارسات المشكوك فيها والتي يستخدمها بعض مسجلي أسماء النطاقات من استخدام معلومات خاصة لتسجيل أسماء النطاقات مقدمًا 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 بالإضافة التي هي 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 فعليًا 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 البريد الإلكتروني المخادع. وفي كلتا الحالتين، تحدث التغييرات سريعًا جدًا، في حوالي ثلاث دقائق، وهو ما لا يترك ظاهريًا للباحثين وقتًا 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 الضارة – هو دمج بين كلمتي "ضار" و"برامج" ويتم استخدامها في الأغلب كعبارة شاملة تتضمن فيروسات الكمبيوتر والديدان وأحصنة طروادة وبرامج أدوات الجذر (rootkits) 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 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 مشغلي الشبكات

NRO – منظمة مصادر الأرقام

دفعات - برامج مصممة لتثبيت عيوب البرامج، ويتم تثبيتها في الأغلب تلقائيًا لتقليل الحاجة لمشاركة المستخدم النهائي وزيادة سهولة الاستخدام.

الخداع - نوع من الاحتيال على الإنترنت يهدف إلى سرقة المعلومات القيمة مثل بطاقات الائتمان وارقام 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 المُسجل

السجل – منظمة تدير تسجيل أسماء نطاقات المستوى الأعلى للإنترنت

المسجِّل - شركة مخولة لتسجيل أسماء نطاقات الإنترنت

RIR – مزود امتداد إنترنت إقليمي

rPKI – البنية التحتية الرئيسية العامة للموارد

RSEP – عملية تقييم خدمات السجل

RSEP – هيئة التقييم التقني لخدمات السجل

البريد العشوائي - أي بريد غير مرغوب فيه. يتم اعتبارها عادةً إزعاجًا مكلفًا، 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.

التزييف - 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

أحصنة طروادة - 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 التي يتم تحميلها على جهاز الكمبيوتر بدون علم المستخدم ويشغل برنامجًا ضارًا. وحتى الفيروس البسيط يمكن أن يكرر نفسه ليجعل نفسه أكثر تدميرًا لأنه يستخدم بسرعة كل الذاكرة المتاحة على نظام جهاز الكمبيوتر المصاب.

الدودة - تكون مشابهة للفيروس في تصميمها وتعتبر أحد أنواع الفيروسات، لكنها أخطر نظرًا 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 مقصودًا 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 شيئًا. 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 قدرًا كبيرًا من الذاكرة وعرض النطاق وتتسبب في النهاية في أن تصيب الشبكة بأكملها بالتوقف.