New gTLD Program
Explanatory Memorandum

Harms Caused by NXDOMAIN Substitution in Top-level and Other Registry-class Domain Names

Date of Publication: 24 November 2009

Background - New gTLD Program

Since ICANN was founded ten years ago as a not-for-profit, multi-stakeholder organization dedicated to coordinating the Internet's addressing system, one of its foundational principles, recognized by the United States and other governments, has been to promote competition in the domain-name marketplace while ensuring Internet security and stability. The expansion of the generic top-level domains (gTLDs) will allow for more innovation, choice and change to the Internet's addressing system, now represented by 21 gTLDs.

The decision to introduce new gTLDs followed a detailed and lengthy consultation process with all constituencies of the global Internet community represented by a wide variety of stakeholders – governments, individuals, civil society, business and intellectual property constituencies, and the technology community. Also contributing were ICANN's Governmental Advisory Committee (GAC), At-Large Advisory Committee (ALAC), Country Code Names Supporting Organization (ccNSO), and Security and Stability Advisory Committee (SSAC). The consultation process resulted in a policy on the introduction of New gTLDs completed by the Generic Names Supporting Organization (GNSO) in 2007, and adopted by ICANN's Board in June, 2008. The program is expected to launch in calendar year 2010.

This explanatory memorandum is part of a series of documents published by ICANN to assist the global Internet community in understanding the requirements and processes presented in the Applicant Guidebook, currently in draft form. Since late 2008, ICANN staff has been sharing the program development progress with the Internet community through a series of public comment fora on the applicant guidebook drafts and supporting documents. To date, there have been over 250 consultation days on critical program materials. The comments received continue to be carefully evaluated and used to further refine the program and inform development of the final version of the Applicant Guidebook.

For current information, timelines and activities related to the New gTLD Program, please go to http://www.icann.org/en/topics/new-gtld-program.htm.

Please note that this is a discussion draft only. Potential applicants should not rely on any of the proposed details of the new gTLD program as the program remains subject to further consultation and revision.

Summary of Key Points in this Paper

- The Board directed ICANN staff to report on the harms and concerns posed by the use (at registry level) of redirection and synthesizing of DNS responses, and ultimately the need to ensure the integrity of error responses as well as name resolution; collectively, NXDOMAIN substitution.
- NXDOMAIN substitution harms and concerns may be categorized as follows:
  1. Architectural implications
  2. Impact on Internet protocols
  3. Single point of failure
  4. Reserved and blocked domains appearing alive
  5. Fragmentation of the DNS ecosystem
  6. Privacy concerns
  7. Lack of choice for Internet users
  8. Poor user experience
  9. Use of privileged position
- ICANN strongly discourages the use of DNS redirection, wildcards, synthesized responses and any other form of NXDOMAIN substitution in new and existing gTLDs and ccTLDs and any other level in the DNS tree for registry-class domain names.
- If a gTLD, ccTLD or registry-class domain manager intends to offer a service that depends on NXDOMAIN substitution, it should consult with technical experts (e.g., IAB/IETF, SSAC) on the possible effects of such implementation, and submit the proposal for global public scrutiny before implementing such a service, as appropriate.

Executive Summary

At its public meeting in Sydney in June 2009, the ICANN Board of Directors resolved that new top-level domains (TLDs) should not use DNS (Domain Name System) redirection and synthesizing of DNS responses. In response to the Board resolution, ICANN included a default prohibition for redirection and synthesizing of DNS responses in the draft Registry Agreement & Specifications[1] for new generic TLDs (gTLDs). ICANN also included a similar

[1] ICANN. (2009, October 4). *Draft Applicant Guidebook, v3, Module 5, Registry Agreement & Specifications.* Retrieved from http://icann.org/en/topics/new-gtlds/draft-agreement-specs-clean-04oct09-en.pdf

commitment as part of the request for new IDN[2] ccTLDs[3] in the proposed Terms and Conditions, and in the three proposed relationship options[4] between ICANN and the IDN ccTLD manager.

The Board also directed ICANN staff to report on the harms and concerns posed by the use of such technologies and ultimately the need to ensure the integrity of error responses as well as name resolution. Those harms and concerns, as acknowledged in several documents referenced below, are collected here for public consideration.

In its review of previously published documentation on the effects of these technologies, ICANN staff summarizes the problems caused by NXDOMAIN substitution as follows:

1. Architectural implications
2. Impact on Internet protocols
3. Single point of failure
4. Reserved and blocked domains appearing alive
5. Fragmentation of the DNS ecosystem
6. Privacy concerns
7. Lack of choice for Internet users
8. Poor user experience (e-mail example)
9. Use of privileged position

Succinctly, a recommendation by the Security and Stability Advisory Committee (SSAC) summarizes the findings:

> *Synthesized responses should not be introduced into top-level domains (TLDs) or zones that serve the public, whose contents are primarily delegations and glue, and where delegations cross organizational boundaries over which the operator may have little control or influence. Although the wildcard mechanism for providing a default answer in response to DNS queries for uninstantiated names is documented in the defining RFCs (Requests for Comment), it was generally intended to be used only in narrow contexts (for example, MX records for e-mail applications), generally within a single enterprise...*[5]

Definitions

For the purposes of this document the following terms are defined as follows:

Wildcard: DNS wildcard Resource Record as described in Request for Comments (RFCs) 1034 and 4592.

---

[2] Internationalized Domain Name
[3] Country code top-level domain
[4] ICANN. (2009, September 30). *Proposed Final Implementation Plan for IDN ccTLD Fast Track Process* . Retrieved from http://www.icann.org/en/topics/idn/fast-track/idn-cctld-implementation-plan-30sep09-en.pdf
[5] SSAC. (2004, July 9). *SAC006: Redirection in the COM and NET Domains.* Retrieved from http://www.icann.org/en/committees/security/ssac-report-09jul04.pdf. pp. 5 - 6

NXDOMAIN: A "Name Error" response, RCODE 3 as described in RFC 1035 and related RFCs.

Registry-class domain names (RCDN): Refers to a top-level domain (TLD) or any other domain name at any level in the DNS tree for which a registry (or an affiliate engaged in providing Registration Services) provides registry services to other organizations or individuals, maintains data, arranges for such maintenance, or derives revenue from such maintenance.

NXDOMAIN substitution: The practice of sending DNS responses that include Resource Records (e.g., IP addresses, name servers names, etc.) in response to queries for uninstantiated domain names. Such responses may be the result of the use of DNS redirection, synthesizing of responses, wildcards or similar technology. The substitution may be for a subset or all uninstantiated domains, e.g., via a wildcard record in the zone or other means.

Uninstantiated domain names: Domain names that are either not registered, or the registrant has not supplied valid records such as NS records for listing in the DNS zone file, or their statuses do not allow them to be published in the DNS.

Preface

In June 2009, the ICANN Board of Directors resolved:

> *Resolved (2009.06.26.19,) that new TLDs, including ASCII and IDN gTLDs and IDN ccTLDs, should not use DNS redirection and synthesized DNS responses. Staff is directed to revise the relevant portions of the draft Applicant Guidebook to prohibit such redirection and synthesis at the top-level for new gTLDs, and to take all available steps with existing gTLDs to prohibit such use.*[6]

As a result of this resolution, ICANN included in the draft Registry Agreement & Specifications[7] for new gTLDs a default prohibition for redirection and synthesized DNS responses. It should be noted that this prohibition is default. If an applicant for a new gTLD believes there is a legitimate use of these technologies that will not have security or stability issues as described in Module 2 of the Applicant Guidebook (currently in draft version 3)[8], the applicant has the option to include the service in its application justifying its reasoning why security and stability issues will not arise.

In the same meeting the Board also resolved:

> *Resolved (2009.06.26.20), the Board further directs staff to communicate and disseminate in July 2009 the concerns regarding harm caused by the redirection and synthesizing of DNS responses with appropriate parties, including the ccNSO, ccTLD operators and the GAC, who might be able to ensure measures are taken*

---

[6] ICANN Board of Directors. (2009, June 26). *Adopted Board Resolutions, Sydney, Australia.* Retrieved from http://www.icann.org/en/minutes/resolutions-26jun09.htm#7

[7] ICANN. (2009, October 4). *Draft Applicant Guidebook, v3, Module 5, Registry Agreement & Specifications.* op. cit.

[8] ICANN. (2009, October 4). *Draft Applicant Guidebook, v3, Module 2: Evaluation Procedures.* Retrieved from http://icann.org/en/topics/new-gtlds/draft-evaluation-procedures-clean-04oct09-en.pdf

to assure the integrity of error responses as well as name resolution for ccTLDs.[9]

In response to this second Board resolution, this explanatory memorandum presents a summary of the numerous findings published on the subject.

The documents about the topic use different names for the same practice or slight variations of it, e.g., DNS redirection, synthesizing of responses, wildcard. The common factor is the practice of returning Resource Records e.g., IP address, MX records, etc. instead of a response at the DNS protocol level indicating the requested domain is not instantiated. In this document the term "NXDOMAIN substitution" (see *Definitions* section) will be used to refer to any of such practices.

The intended audience of this paper is current and potential RCDN managers, including both ccTLDs and gTLDs, and any other party interested in the management of RCDNs. This explanatory memo may also provide guidance for the community on the issues of NXDOMAIN substitution at the registry level.

NXDOMAIN substitution can happen at any level in the DNS resolution chain, from the authoritative DNS servers to the recursive resolver and the application level in the end-user computer. This memo focuses exclusively on the issue in authoritative DNS servers of RCDNs. For issues at other levels of the DNS resolution chain the interested reader is referred to SSAC's report SAC032[10].

Key Issues Identified

Several organizations and expert bodies such as the ICANN's SSAC and the Internet Architecture Board (IAB) have previously documented their opinions against the use of NXDOMAIN substitution. In particular it is worth noting the SSAC's recommendation SAC041:

> *SSAC advises ICANN that new TLDs, including both new gTLDs and new ccTLDs, should not use DNS redirection and synthesized DNS responses.*[11]

Further, in the same document this position is extended to sub-TLD levels:

> *SSAC reiterates its position that synthesized DNS responses at the TLD level (and subordinate levels) is a destabilizing practice.*[12]

The IAB also warned against using this technology in domains below the TLD level:

> *Note that these considerations apply to any wildcard deployment of this type. The list of problems encountered in this case clearly demonstrates that, although wildcard records are part of the base DNS protocol, there are situations in which it simply is not safe to use them. As noted in an earlier section, two warning flags suggesting that this type of wildcard deployment is dangerous were that*
>
> *1. it affected more than one protocol, and*

---

[9] ICANN Board of Directors. op. cit.
[10] SSAC. (June de 2008). *SAC032: Preliminary Report on DNS Response Modification.* From http://www.icann.org/en/committees/security/sac032.pdf
[11] SSAC. (2009, June 10). *SAC041: Recommendation to prohibit use of redirection and synthesized responses by new TLDs.* Retrieved from http://www.icann.org/en/committees/security/sac041.pdf
[12] Idem

2. it was done high enough up in the DNS hierarchy that its effects were not limited to the organization that chose to deploy these wildcard records.[13]

As shown above, DNS experts believe the effects of NXDOMAIN substitution are not just harmful at the TLD level, but in lower levels of the DNS hierarchy, provided that delegations in said zone are for organizations not related to the one managing the zone. In this document the term "RCDN" (as described in the *Definitions* section) is used to reference these domains regardless of their level in the DNS tree.

In reviewing the numerous documents that have been published about the harms and concerns caused by the use of NXDOMAIN substitution in RCDNs, the following categories of issues were identified. Each section below presents a category. References to the authoritative documents are also provided at the end.

1. Architectural implications

A common use for NXDOMAIN substitution is to return an IP address, with the aim of directing web site lookups to an information website or portal. Such use violates the layered protocol design of the Internet since the DNS query is protocol neutral, while the IP address given back is targeted for an application layer protocol: HTTP.

If a third party were to try to reverse the effects of the NXDOMAIN substitution, it would need to coordinate with and rely on the source of the synthesized responses (i.e., the RCDN registry) – an unworkable and unacceptable dependency. They would need to arrange a way to make specific application protocols able to operate as if there were no NXDOMAIN substitution for that RCDN. It may be the case that a workaround could be devised at the DNS level (e.g., by tagging specific strings such as "www" to receive special handling) or it could be necessary to develop a specific measure for every existing and future application protocol.

Moreover, if there were more than one RCDN implementing NXDOMAIN substitution, there would be the need to implement a solution for each one of them. Since the solution could be different for each RCDN, this workaround mechanism will not scale for many RCDNs.

Current DNSSEC[14] implementations do not resolve this problem. DNSSEC contains a provision (the label count in the signature records) that in theory would allow recognizing a DNS response as being product of a wildcard synthesis, one of the forms of NXDOMAIN substitution. However, typical deployment of DNSSEC to date uses a model where DNS recursive resolvers process the DNSSEC records. These servers are typically at Internet Service Providers (ISPs) and are therefore one step before the user in the DNS resolution chain. In practice this means the vast majority of end-users will still be unable to have a direct way to recognize synthesized wildcard records coming from authoritative DNS servers.

Further information on these issues can be found in (SSAC, 2004) and (RSTEP, 2006).

---

[13] IAB. (2003, September 19). *Architectural Concerns on the use of DNS Wildcards.* Retrieved from http://www.iab.org/documents/docs/2003-09-20-dns-wildcards.html

[14] DNS Security Extensions, see RFCs 4033, 4034, 4035 and related RFCs http://www.rfc-editor.org/rfcsearch.html

2. Impact on Internet protocols

It has been suggested that the size (number of registrations) in the RCDN makes a difference on the effects a NXDOMAIN substitution implementation has on the Internet. While the number of registrations is important, the RSTEP panel stated that, in its review of the "search.travel Wildcard Proposal," the apparent "small size" of a RCDN is not enough to ensure that the effects would also be small when NXDOMAIN substitution is implemented for a Resource Record type widely used such as the "A" (IPv4 address) type. In such cases, the effects will be felt in almost every application that uses the Internet for that RCDN:

> *Because the proposed wildcard changes the expected behavior of the DNS in such a fundamental way, it is impossible to anticipate all of its side effects without testing each and every mail server and agent, every instant message application and agent, every VOIP server, proxy, and user agent, every parental control system … basically every application on the Internet.*[15]

The main risk associated with NXDOMAIN substitution is that for the affected DNS type (e.g., A, AAAA, MX) it (fully or partially) eliminates NXDOMAIN responses, something on which an application may depend. Given the number of applications in the Internet, it is not feasible for an organization to provide a redirection service for every present and future Internet protocol.

Implementation of NXDOMAIN substitution for type "A" Resource Records in a RCDN produces another set of problems when combined with the search list functionality of many DNS clients.

A DNS search list works by appending each element of a list of domains to DNS queries made from a computer as an aid to complete domains typed. For example, if a search list contained "example.com" and "example2.com", and a user were to type "www" in a Web browser, the DNS client would first append "example.com" to give "www.example.com" and would return a result if that domain resolves. If it does not, it would append "example2.com" to give "www.example2.com" and so on if there were more domains in the search list.

For example, if the RCDN has a type "A" wildcard record, three potential issues may arise:

1. If the user configures said RCDN in the search list, the user will get redirected to the wildcard IP address if a typed domain does not exist. This is true even for a nonexistent domain in another RCDN since "www.non-existant.anotherRCDN.RCDN" would resolve to the wildcard in the latter RCDN.
2. This issue could be complicated further if using an operating system/resolver with a (once common) behavior described in RFC 1535[16] that would use parent domains of domains configured in the search list as if they were in the list. For example if the domain "division.example.RCDN" were configured in the list, the

---

[15] RSTEP. (2006, November 2). *Report on Internet Security and Stability Implications of the Tralliance Corporation search.travel Wildcard Proposal.* Retrieved from http://www.icann.org/en/registries/rsep/tralliance_report.pdf. p. 11

[16] Gavron, E. (1993, October). *RFC 1535: A Security problem and proposed correction with widely deployed DNS software.* Retrieved from RFC Editor: http://www.rfc-editor.org/rfc/rfc1535.txt

parent domain "example.RCDN" would be used in the search list as if also configured.

3. When using IPv4 addresses directly instead of domains, some applications and resolver libraries that will not initially recognize an IPv4 as such, will try to resolve it as if it were a domain (since syntactically IPv4 addresses are legal domains). When the DNS client uses the search list, a resolution attempt would be made for "<the IP address>.RCDN" having the user directed to the wildcard IP address instead of the intended IP address, regardless of whether or not the IP address provided by the user was correct.

Further information on these issues can be found in (IAB, 2003) and (RSTEP, 2006).

3. Single point of failure

A redirection service based on NXDOMAIN substitution can result in a centralized point being accessed for the traffic of uninstantiated domains in a RCDN. A failure in such a system could impact response time for end-users thus detrimentally affecting the user experience. An error in the redirection system could also potentially cause more traffic to go the DNS root-servers.

Redirection services are generally implemented to generate revenue. As a result, they are extremely attractive targets for attacks by those interested in thwarting the service or redirecting traffic to their own servers.

Further information on these issues can be found in (IAB, 2003).

4. Reserved and blocked domains appearing alive

A registry typically has domains that are not available for registration even though they are not registered. For example, a domain may be considered reserved for use by an entity (e.g., the registry, a regulator, etc.) or reserved by agreement without having the domain appear in the DNS. It may also be that certain domains are blocked (i.e., not available for registration) for a variety of policy reasons.

Notably, for IDNs there are often provisions for reserved/blocked domain variants that are never intended to appear in the DNS.

Under a RCDN implementing NXDOMAIN substitution reserved or blocked domains, otherwise not appearing in the DNS, when subject to NXDOMAIN substitution would look as if they were delegated/existent from an end-user point of view.

Further information on this issues can be found in (SSAC, 2004) and (IAB, 2003).

5. Fragmentation of the DNS ecosystem

Previous experiences with the introduction of NXDOMAIN substitution in RCDNs showed that actors who sought to reverse the effects of the changes took action to implement a series of workarounds, e.g., filters to the server redirection, patches to DNS resolvers, etc.

Those actions have resulted in an environment complicated for individuals or organizations trying to develop new applications or use existing ones (e.g., surfing the Web, sending e-mail, etc.) in the ways they were accustomed to.

Further information on these issues can be found in (Levien, 2005).

6. Privacy concerns

Depending on implementation details, some data from various Internet protocols may arrive at the redirection server's network against the intention of the sender. Portions of this data may be sensitive and the registry could be making itself the unintended recipient of such data by implementing NXDOMAIN substitution in its delegated RCDN.

It is also worth noting that by positioning itself as an unintended recipient of data, the registry implementing NXDOMAIN substitution is also changing the purported privacy requirements of the information being transmitted. For example, if party A intended to send information to party B under certain privacy legislation relevant to A and B and NXDOMAIN substitution causes the information transit through or be delivered to party C (the redirection service), which may bound to a different jurisdiction and local law, there may be consequences for the sender or the registry.

In the case of wildcard, although it is bounded at zone level, there is also the case of a perceived intrusion to a child domain zone. For example, suppose the zone "RCDN" has a wildcard record and "example.RCDN" is delegated containing only one child domain "www.example.RCDN". If a user typed the nonexistent domain "ftp.example.RCDN", the DNS servers from "example.RCDN" will get queried and the usual behavior as if there were no wildcard in RCDN will happen. However, if the user mistakenly typed the nonexistent domain "www.ezample.RCDN" (with "z" instead of "x"), the response will come from the RCDN DNS servers containing the wildcard record. From the user's point of view there would be leakage of the wildcard effects from the parent to the child. This should not be a problem if the registry and the registrant organizations are related someway. It becomes more problematic in cases where the interests of the organization managing the RCDN are not aligned with those of the organization who registered "example.RCDN".

Following the example above, it could be argued that the same problem would occur if "ezample.RCDN" were registered by another organization. The difference is the scale of the issue; without wildcard the problem would happen with a few (registered) domains that are type-variants of "example.RCDN", while for a RCDN with wildcard the problem would happen with all the variants of "example.RCDN".

Further information on these issues can be found in (SSAC, 2004); (RSTEP, 2006) and (IAB, 2003).

7. Lack of choice for Internet users

Applications such as Web browsers may have functionality based on local options set by the user (e.g., language, directories, etc.) that is executed when a DNS lookup gets an NXDOMAIN response. Such functionality is cancelled in a RCDN by the implementation of NXDOMAIN substitution, leaving the user without any possibility of accepting the loss of functionality, rejecting it, or substituting it with an alternative offer. The user may not be a client of said RCDN but rather a casual Internet user who has absolutely no influence over the registry in order to modify the described behavior.

Further information on these issues can be found in (RSTEP, 2006); (SSAC, 2006); (SSAC, 2004); (IAB, 2003) and (Levien, 2005).

8. Poor user experience (e-mail example)

In normal scenarios (i.e., without NXDOMAIN substitution), any application that checks for domain existence will receive an immediate negative response (in case of nonexistent domains) it can communicate back to the user, in the form of "Host not found" or similar message.

For a RCDN with NXDOMAIN substitution, the user will not be able to identify the nonexistence of domains subject to this substitution and the problem will not be noticed until later by the user in the form of its inability to do the intended task, e.g., print, send e-mail, etc. For example, with e-mail transmission, the message is likely to be queued and retried for several days before it comes back as undeliverable. The error message, when it finally appears, will likely not adequately explain the problem (e.g., a timeout error saying the recipient is temporarily offline, rather than explaining the domain does not exist).

Further information on these issues can be found in (IAB, 2003).

9. Use of privileged position

Normally if someone wants to make use of a domain, they have to register it (and pay a fee for the right to use it). In the case of NXDOMAIN substitution in a RCDN, the registry would be making use (and perhaps profit) from all or a subset of the uninstantiated domains without having registered or paid for them. If another organization (e.g., ISP, search engine, etc.) wished to compete with such a registry service, it would have to invest a considerable amount of money in order to achieve similar results.

In the case of wildcard implementation, the number of domain permutations a registry would be taking advantage is extremely large (a number on the order of 99 digits), considering a domain label has 63 characters in length with 37 possible characters. Even considering a shorter domain (e.g., 13 characters), something closer to the range likely to be used by an end-user[17], the total number of domains has 21 digits (excluding considerations of child domains).

Further information on these issues can be found in (Levien, 2005).

Recommendations from expert groups

Many well-known DNS experts have written about and published papers on NXDOMAIN substitution at RCDNs in its different forms, and they frequently shared a common view: approach the issue with caution and preferably avoid the use of these technologies.

Below are recommendations from three groups of such experts.

Internet Architecture Board:

> *Given these issues, it seems clear that the use of wildcards with record types that affect more than one protocol should be approached with caution, that the use of wildcards in situations where their effects cross organizational boundaries should also be approached with caution, and that the use of wildcards with*

[17] The average length of the leftmost label (i.e., not counting ".TLD") of domains under COM, NET, ORG, INFO and BIZ TLDs is 13.09, calculated with zone files of 11 October 2009.

record types that affect more than one protocol in situations where the effects cross organizational boundaries should be approached with extreme caution, if at all.[18]

Committee on Internet Navigation and the DNS from *Signposts in Cyberspace*:

Recommendation: TLDs and other DNS operators that do not have agreements with ICANN should voluntarily agree to adhere to published technical standards and to consult the technical community and conduct public review processes before introducing new services that could have a detrimental effect on the DNS or on other services that depend on the DNS.[19]

Security and Stability Advisory Committee:

Synthesized responses should not be introduced into top-level domains (TLDs) or zones that serve the public, whose contents are primarily delegations and glue, and where delegations cross organizational boundaries over which the operator may have little control or influence. Although the wildcard mechanism for providing a default answer in response to DNS queries for uninstantiated names is documented in the defining RFCs (Requests for Comment), it was generally intended to be used only in narrow contexts (for example, MX records for e-mail applications), generally within a single enterprise...[20]

Conclusions

Following its core value number one "*Preserving and enhancing the operational stability, reliability, security, and global interoperability of the Internet*"[21], at the direction of the ICANN Board and given the arguments from the DNS experts previously cited:

1. ICANN included a default prohibition for DNS redirection, wildcards, synthesized responses and any other form of NXDOMAIN substitution in the draft Registry Agreement & Specifications[22] for new gTLDs.
2. ICANN notes that if an applicant for a new gTLD believes there is a legitimate use of these technologies that will not have security or stability issues as described in Module 2 of the draft Applicant Guidebook[23], the applicant has the option to include the registry service in its application justifying its reasoning why security or stability issues will not arise.
3. ICANN included a commitment to not implement DNS redirection and synthesized DNS responses as part of the request for new IDN ccTLDs in the proposed Terms and Conditions, and in the three proposed relationship options

---

[18] IAB. op. cit.
[19] (2005). 4.4 Responding to Domain Name Errors. In R. Levien, S. R. Austein, B. M. Stanley, B. L. Christine, C. Timothy, D. Hugh, et al., & T. N. Press (Ed.), *Signposts in Cyberspace. The Domain Name System and Internet Navigation* (pp. 173 - 186). Washington, DC, US.
[20] SSAC. (2004, July 9). op. cit. pp. 5 - 6
[21] ICANN. (2009, March 20). *ICANN Bylaws.* Retrieved from http://www.icann.org/en/general/bylaws.htm#I
[22] ICANN. (2009, October 4). *Draft Applicant Guidebook, v3, Module 5, Registry Agreement & Specifications.* op. cit.
[23] ICANN. (2009, October 4). *Draft Applicant Guidebook, v3, Module 2: Evaluation Procedures.* op. cit.

between ICANN and the IDN ccTLD manager: Documentation of Responsibility, Exchange of Letters, and Standard Agreement.[24]

4. ICANN strongly discourages the use of DNS redirection, wildcards, synthesized responses and any other form of NXDOMAIN substitution in existing gTLDs, ccTLDs and any other level in the DNS tree for registry-class domain names. If an existing gTLD operator intends to offer a service that depends on NXDOMAIN substitution, it must submit that request through the Registry Services Evaluation Process[25].
5. ICANN further recommends that if ccTLD or registry-class domain managers intend to offer a service that depends on NXDOMAIN substitution, they should consult with technical experts (e.g., IAB/IETF, SSAC) on the possible effects of such implementation, and submit the proposal for global public scrutiny before implementing such a service.

References

[1] IAB. (2003, September 19). *Architectural Concerns on the use of DNS Wildcards.* Retrieved from http://www.iab.org/documents/docs/2003-09-20-dns-wildcards.html

[2] RSTEP. (2006, November 2). *Report on Internet Security and Stability Implications of the Tralliance Corporation search.travel Wildcard Proposal.* Retrieved from http://www.icann.org/en/registries/rsep/tralliance_report.pdf

[3] SSAC. (2004, July 9). *SAC006: Redirection in the COM and NET Domains.* Retrieved from http://www.icann.org/en/committees/security/ssac-report-09jul04.pdf

[4] SSAC. (2006, November 10). *SAC015: Why Top Level Domains Should Not Use Wildcard Resource Records.* Retrieved from http://www.icann.org/en/committees/security/sac015.htm

[5] R. Levien, S. R. Austein, B. M. Stanley, B. L. Christine, C. Timothy, D. Hugh, et al. *Signposts in Cyberspace. The Domain Name System and Internet Navigation*. National Research Council of the National Academies. Section 4.4 Responding to Domain Name Errors. The National Academies Press. Washington, D.C., US. 2005.

[24] ICANN. (2009, September 30). *Proposed Final Implementation Plan for IDN ccTLD Fast Track Process.* op. cit.

[25] ICANN. (2006, August 15). *Registry Services Evaluation Policy.* Retrieved from ICANN: http://www.icann.org/en/registries/rsep/rsep.html