New gTLD Program Safeguards Against DNS Abuse

Revised Report

ICANN Operations and Policy Research | July 2016

Table of Contents

INTRODUCTION 1

DNS ABUSE: KEY TERMINOLOGY 3

THE REGISTRATION ABUSE POLICIES WORKING GROUP 5

DNS ABUSE: KEY STATS AND TRENDS 11

DNS ABUSE IN NEW GTLDS 12
A CASE STUDY IN DNS ABUSE: PHISHING IN NEW GTLDS 14

THE NINE SAFEGUARDS 16

QUESTION: HOW DO WE ENSURE THAT BAD ACTORS DO NOT RUN REGISTRIES? 16
SAFEGUARD: VET REGISTRY OPERATORS 17
QUESTION: HOW DO WE ENSURE INTEGRITY AND UTILITY OF REGISTRY INFORMATION? 19
SAFEGUARD: REQUIRE DEMONSTRATED PLAN FOR DNSSEC DEPLOYMENT 19
SAFEGUARD: PROHIBITION OF WILDCARDING 21
SAFEGUARD: REMOVAL OF ORPHAN GLUE RECORDS 23
QUESTION: HOW DO WE ENSURE MORE FOCUSED EFFORTS ON COMBATING IDENTIFIED ABUSE? 25
SAFEGUARD: REQUIREMENT FOR THICK WHOIS RECORDS 25
SAFEGUARD: CENTRALIZATION OF ZONE-FILE ACCESS 27
SAFEGUARD: DOCUMENTED REGISTRY- AND REGISTRAR- LEVEL ABUSE CONTACTS AND PROCEDURES 28
SAFEGUARD: PARTICIPATION IN AN EXPEDITED REGISTRY SECURITY REQUEST PROCESS (ERSR) 30
QUESTION: HOW DO WE PROVIDE AN ENHANCED CONTROL FRAMEWORK FOR TLDS WITH INTRINSIC POTENTIAL FOR MALICIOUS CONDUCT? 31
SAFEGUARD: CREATE A DRAFT FRAMEWORK FOR A HIGH SECURITY ZONE VERIFICATION PROGRAM 31

RESEARCH PROPOSAL AND MODELS 33

A POSSIBLE QUALITATIVE FRAMEWORK FOR TESTING THE EFFECTIVENESS OF SAFEGUARDS 34
RESEARCH DESIGN: KEY QUESTIONS AND CONSIDERATIONS 34
CAUSAL MODELS AND HYPOTHESES 36

CONCLUSION 38

APPENDIX: SURVEY OF ABUSE-RELATED ACTIVITIES AT ICANN 39

Introduction

In accordance with section 9.3 of ICANN's Affirmation of Commitments (AoC) to promote competition, consumer choice, and consumer trust in the Domain Name System (DNS), this report is intended to aid the work of the review team on Competition, Consumer Choice, and Consumer Trust (CCT-RT). It will do so by:

- Providing an overview of the state of DNS abuse following the roll-out of the New Generic Top-Level Domain (gTLD) Program in January 2012
- Discussing options for measuring the effectiveness of the nine safeguards put in place to mitigate DNS abuse in new gTLDs
- Proposing a research model to help assess the effectiveness of the nine safeguards in mitigating DNS abuse in new gTLDs

The AoC states:

> ICANN will organize a review that will examine the extent to which the… expansion of gTLDs has promoted competition, consumer trust and consumer choice, as well as effectiveness of…**safeguards put in place to mitigate issues involved in the…expansion**…[emphasis added]. The reviews will be performed by volunteer community members and the review team will be constituted and published for public comment…Resulting recommendations of the reviews will be provided to the Board and posted for public comment. The Board will take action within six months of receipt of the recommendations

In preparation for the potential expansion of the DNS, ICANN solicited advice from its expert constituencies to examine the potential for increases in abusive, malicious, and criminal activity in an expanded DNS and to make recommendations to **pre-emptively mitigate** those activities through a number of **safeguards**.[1] The effort to identify steps for mitigating potential abuse began with posing four questions to experts in a diverse array of groups including the Anti-Phishing Working Group (APWG), the Registry Internet Safety Group (RISG), the Security and Stability Advisory Committee (SSAC), Computer Emergency Response Teams (CERTs) and members from the banking, financial, and Internet security communities. Those questions were:

1) How do we ensure that bad actors do not run registries?
2) How do we ensure integrity and utility of registry information?
3) How do we ensure more focused efforts on combating identified abuse?

[1] "Mitigating Malicious Conduct," ICANN, New gTLD Program Explanatory Memorandum, 3 October 2009, https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf

4) How do we provide an enhanced control framework for TLDs with intrinsic potential for malicious conduct?

After extensive consultations, the expert groups arrived at the following **recommendations** to address each issue area:

Question	Recommendation(s)
1) How do we ensure that bad actors do not run registries?	1) **Vet registry operators** through background checks to reduce the risk that a potential registry operator has been party to criminal, malicious, and/or bad faith behavior.
2) How do we ensure integrity and utility of registry information?	2) **Require Domain Name System Security Extension (DNSSEC) deployment** on the part of all new registries to minimize the potential for spoofed DNS records. 3) **Prohibit "wildcarding"** to prevent DNS redirection and synthesized DNS responses that may result in arrival at malicious sites. 4) **Encourage removal of "orphan glue" records** to minimize use of these remnants of domains previously removed from registry records as "safe haven" name server entries in the TLD's zone file that malicious actors can exploit.
3) How do we ensure more focused efforts on combating identified abuse?	5) **Require "Thick" WHOIS records** to encourage availability and completeness of WHOIS data. 6) **Centralize Zone File access** to create a more efficient means of obtaining updates on new domains as they are created within each TLD zone. 7) **Document registry- and registrar-level abuse contacts and policies** to provide a single point of contact to address abuse complaints. 8) **Provide an expedited registry security request process** to address security threats that require immediate action by the registry and an expedited response from ICANN.

4) How do we provide an enhanced control framework for TLDs with intrinsic potential for malicious conduct?	9) **Create a draft framework for a high security zone verification program** to establish a set of criteria to assure trust in TLDs with higher risk of targeting by malicious actors—e.g. banking and pharmaceutical TLDs—through enhanced operational and security controls.

Measuring the effectiveness of these safeguards is a central aim of the work of the CCT-RT. To aid that work, this report will present an in-depth examination of each of these safeguards, propose potential means to measure their effectiveness where possible, and put forward a research model to analyze their effectiveness in a rigorous and comprehensive manner. Note that this report is meant as an *aid* to the CCT-RT. It is meant to offer *possible* methods and to provoke discussion within the team about how best to approach their study of DNS abuse and the safeguards put in place to mitigate it in the context of the New gTLD Program.

DNS Abuse: Key Terminology

"DNS abuse" covers a wide range of activities. While no globally accepted definition exists, definitional variants can include "cyber-crime," "hacking," and, as ICANN has used in the past, "malicious conduct". Researchers from the University of Rome and the Global Cyber Security Center classify such threats to the DNS as falling under three categories: data corruption, denial of service, and privacy.[2]

"DNS abuse" is the term used in this report, and refers to intentionally deceptive, conniving, or unsolicited activities that actively make use of the the DNS and/or the procedures used to register domain names. This is a working definition based on review of which activities are generally explored in the literature as malicious or abusive, and is intended to provide a point of departure for the CCT-RT to refine their own definition of DNS abuse in their work. As explored below, some activities tend to fall under "bad faith"—but not necessarily illegal—commercial practices while others are outright scams that are likely to be illegal in most jurisdictions around the world. The extent to which each abusive activity (described below) falls under this definition and can be analyzed from the standpoint of the nine safeguards to mitigate DNS abuse in the New gTLD Program will remain open for consideration by the CCT-RT. The goal is to provide a working definitional structure to frame additional discussion around which activities should be included in their work.

[2] Casalicchio, Caselli, and Coletta, "Measuring the Global Domain Name System," IEEE Network 27, no. 1, (2013) 25-31. doi: 10.1109/MNET.2013.6423188

DNS Abuse: Tactics and Instruments

Malicious actors typically carry out their schemes via the following avenues:[3]

- **Compromised domains**: domains in which a malicious actor has broken in to the web hosting of a registrant.
- **Malicious registrations**: domains registered by malicious actors for the express purpose of engaging in DNS abuse.
- **Subdomain resellers**: services—many of which are free and offer anonymous registration outside of a WHOIS service—that allow people to create registrations at the third level beneath a second-level domain that the service provider owns. These resellers often do not maintain any registration or point of contact data beyond user account names.[4]
- **IP addresses**: phishing attacks sometimes use IP addresses in their URLs rather than domain names.
- **Shortened URLs**: a technique to compact lengthy domain addresses that can be used by malicious actors to obfuscate a domain name and thus redirect unsuspecting users to malicious sites[5]

While DNS abuse can take a number of forms, its typical aim is to distribute **malware**—short for "malicious software"—which is used to disrupt computer operations, gather sensitive information, or gain access to private computer systems.[6] Malware itself can carry out a number of harmful activities and take a number of forms. The most commonly distributed programs include:

- **Viruses**: Malicious programs that carry out a number of unwanted activities and cause computers not to function properly, including creating, moving,

---

[3] Note the first two listed tend to be the primary avenues used by malicious actors. See Illumintel, "Potential for Phishing in Sensitive-String Top-Level Domains," study for the ICANN Board of Directors New gTLD Program Committee, 21 May 2015, https://www.icann.org/resources/pages/new-gtld-program-committee-2014-03-21-en

[4] Anti-Phishing Working Group, "Making Waves in the Phisher's Safest Harbor: Exposing the Dark Side of Subdomain Registries," November 2008, http://docs.apwg.org/reports/APWG_Advisory_on_Subdomain_Registries.pdf

[5] See StopTheHacker.com, "The Curse of the URL Shorteners: How Safe Are They?" accessed 26 February 2016, https://www.stopthehacker.com/2010/02/19/analyzing-url-shorteners/

[6] "Implementation Advisory Group for Competition, Consumer Choice, and Consumer Trust (IAG-CCT): Final Recommendations on Metrics for CCT Review," 26 September 2014, https://newgtlds.icann.org/en/reviews/cct/iag-metrics-final-recs-26sep14-en.pdf

and/or erasing files, and/or consuming computer memory. Often they duplicate themselves and travel across networks via infected emails. Examples include "worms" and "trojan horses".[7]

- **Spyware**: Malware that can capture information such as usernames, passwords, credit card info, web browsing habits, and e-mails.[8]

Malware is often distributed through the use of **bots**, which are automated programs that are coded to operate continuously to perform malicious or abusive functions.[9] **Botnets** are networks of these bots that utilize infected computers to distribute malware.[10] Those who are infected do not know their devices are being used for such purposes.

The Registration Abuse Policies Working Group

In 2010, the GNSO's Registration Abuse Policies Working Group (RAPWG) produced a report that explored abuse provisions in registry-registrar agreements.[11] In it, the group developed a consensus definition of abuse, which reads:

> Abuse is an action that: a) causes actual and substantial harm, or is a material predicate of harm, and b) Is illegal or illegitimate, or is otherwise contrary to the intention and design of a stated legitimate purpose, if such purpose is disclosed.[12]

They went further to distinguish between "**registration**" and "**use**" abuse, with the former referring to issues that arise during the registration of domains, while the latter

---

[7] Kaspersky Lab, "What is a Computer Virus or a Computer Worm?" accessed 26 February 2016, http://www.kaspersky.com/internet-security-center/threats/viruses-worms

[8] Kaspersky Lab, "What is Spyware?" accessed 26 February 2016, http://usa.kaspersky.com/internet-security-center/threats/spyware#.VtCsAJMrJTY

[9] Bots are often not malicious and carry out any number of legitimate functions. However, this report refers only to their malicious form. See Gabada, Usman, and Sharma, "Techniques to Break the Botnet Attack," International Journal for Research in Emerging Science and Technology 2, no. 1 (March 2015), http://ijrest.net/downloads/volume-2/special-issue-1/pid-m15ug638.pdf

[10] Ibid.

[11] In their public comments on this report, the Intellectual Property Constituency noted that the RAPWG "predated the development of the new gTLD registry agreement by some time, and some of [their] observations regarding 'use abuse' have been superseded by certain elements in the registry agreement, including such specified abuses as piracy and counterfeiting, which inherently involve issues concerning uses of domain names and not mere 'registration' issues" (p. 1).

[12] "Registration Abuse Policies Working Group Final Report," May 2010, http://gnso.icann.org/en/issues/rap/rap-wg-final-report-29may10-en.pdf

refers to how the domains are used post-registration. Their definitional framework is as follows:

> Registration issues are related to the core domain name-related activities performed by registrars and registries. These generally include (but are not limited to) the allocation of registered names; the maintenance of and access to registration (WHOIS) information; the transfer, deletion, and reallocation of domain names; and similar areas discussed in more detail below. These are generally within the scope of GNSO policy-making. Many of these are specifically listed in registration agreements as being subject to Consensus Policies, and the extant Consensus Policies have to do with these kinds of topics.

The group discussed the following activities as potential forms of registration abuse:

- **Cybersquatting** - the deliberate and bad-faith registration and use of a name that is a registered brand or mark of an unrelated entity, often for the purpose of profiting (typically, though not exclusively, through pay-per-click advertisements).
- **Front-running** – when a party obtains some form of insider information regarding an Internet user's preference for registering a domain name and uses this opportunity to pre-emptively register that domain name.
- **Gripe sites** – websites that complain about a company's or entity's products or services and uses a company's trademark in the domain name (e.g. companysucks.example). The concern expressed within the group was that these types of sites have the potential to infringe on trademark owners' rights. But the group also noted that in many cases such sites are avenues for legitimate complaints and are protected under free speech laws in many jurisdictions.
- **Deceptive and/or offensive domain names** – registration of domain names that direct unsuspecting consumers to obscenity or direct minors to harmful content—sometimes referred to as a form of "mousetrapping."
- **Fake renewal notices** – misleading correspondence sent to registrants from an individual or organization claiming to be or to represent the current registrar. These are sent for a variety of deceptive purposes.
- **Name spinning –** using automated tools used to create permutations of a given domain name string. While registrars regularly use such tools legitimately to suggest alternate strings to potential registrants when the string a registrant queries is not available, the group's concern here was that such tools could produce results that infringed upon trademarked strings.[13]

[13] In their public comment on this report, the Registry Stakeholder Group noted "the fact that Name Spinning could lead to suggestions which are trademarked names is

- **Pay-per-click** – an Internet advertising model used on websites, in which the advertiser pays the host only when their ad is clicked. The concern raised was use of a trademark in a domain name to draw traffic to a site containing paid placement advertising.[14]
- **Traffic diversion** – use of brand names in HTML visible text, hidden text, meta tags, or web page title to manipulate search engine rankings and divert traffic.
- **False affiliation** – falsely purporting to be an affiliate of a brand owner.
- **Cross-TLD registration scam** – a deceptive sales practice where an existing registrant is sent a notice that another party is interested in or is attempting to register the registrant's domain string in another TLD. The registrant is therefore pushed to make additional registrations via the party who sent the notice – often a reseller who would profit from the additional registrations, and is offering the new domain creates at a higher-than-average market price.
- **Domain kiting/tasting** – when registrants abuse the "Add Grace Period" through continual registration, deletion, and re- registration of the same names in order to avoid paying registration fees.

In contrast, the RAPWG defined "use" issues as follows:

> Domain name use issues concern what a registrant does with his or her domain name after the domain is created—the purpose the registrant puts the domain to, and/or the services that the registrant operates on it. These use issues are often independent of or do not involve any registration issues…[D]omain name use is an area in which ICANN's and the GNSO's policy-making authority is more limited.

The group discussed the following activities as potential forms of use abuse:

- **Phishing** – a website fraudulently presenting itself as a trusted site (often a bank) in order to deceive Internet users into divulging sensitive information (e.g. online banking credentials, email passwords). The goal of phishing is usually the theft of funds or other valuable assets.
- **Spam** – bulk unsolicited e-mail sent from domains, and used to advertise websites.

---

offset by the fact that the registrar intimates/informs the fact of the domain name being a trademark as a compliance measure to the registrant and even then, if the registrant registers such a domain name, the abuse would be covered under cybersquatting." (p. 1).

[14] Endurance International Group, who provided a public comment on this report, argued in those comments that pay-per-click advertising and traffic diversion are website content issues and are thus outside of ICANN's remit to address.

- **Malware/Botnet Command-and-Control** –using domain names as a way to control and update botnets, which are networks of thousands to millions of infected computers under the common control of a criminal. Botnets can be used to perpetrate many kinds of malicious activity, including **distributed denial-of-service attacks (DDoS)**, **spam**, and **fast-flux** hosting of phishing and spam sites [see below for further explanation of the practices and terminology used in this definition].
- **Use of stolen credentials** – e.g. identity, access, and financial credentials to register domain names for malicious purposes, steal from, and/or otherwise disrupt and individual's or organization's operations.

In the report, the RAPWG reiterates that ICANN and its various supporting organizations have some purview over *registration* issues through the policy-making and enforcement processes, while *use* issues are more difficult to confront given ICANN's limited authority over how registrants use their domain names. Note that the definitions and activities provided in this section were solely those discussed by members of the RAPWG for the purposes of their report, and do not constitute an endorsement by ICANN as to which activities are in fact DNS abuse. The definitions and activities noted here are provided to serve the work of the CCT-RT, and are for informational and discussion purposes only.

Specification 11 of the New gTLD Registry Agreement

Specification 11 of the New gTLD Registry Agreement mandates that registry operators commit to certain public interest commitments (PICs) as part of their contractual obligations with ICANN. Sub-sections 3a and 3b focus on registry operators' PICs as an aspect of DNS abuse, and describe activities that should be included in their efforts to mitigate and track abusive behavior in their TLDs. Specification 11 states:[15]

> 3a. Registry Operator will include a provision in its Registry-Registrar Agreement that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name.
>
> 3b. Registry Operator will periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. Registry Operator will maintain

[15] "Registry Agreements," accessed 4 February 2016, https://www.icann.org/resources/pages/registries/registries-agreements-en

statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. Registry Operator will maintain these reports for the term of the Agreement unless a shorter period is required by law or approved by ICANN, and will provide them to ICANN upon request.

The activities described within Specification 11 may provide an additional definitional framework for the CCT-RT as they refine the scope of their review.

DNS Abuse: Additional Terminology and Considerations

A number of other terms and considerations are worth noting in regard to the activities that constitute DNS abuse:

- **Phishing** uses both **social engineering** and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social engineering schemes use spoofed emails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers. **Spear-phishing** is a specific form of phishing email scam that targets specific individuals with high-value credentials within an organization to trick them into providing sensitive information.[16]
- **Fast-flux** is a technique carried out by botnets in phishing, spam, and other malware delivery activities in which attacks are sent from a constantly shifting set of IP addresses, rendering detection very difficult.[17]
- **Typo-squatting**—aka "URL hijacking"—is a form of **cyber-squatting** that relies on users making a typographical error when entering a website address into a web browser, and often directs users to malicious sites.[18]
- **Malvertising** is advertising on a website or ad network that is set up to infect viewers with malware either every time it is seen or at various intervals based on time or number of hits.[19]

---

[16] "SSAC Advisory on Registrant Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle," ICANN Security and Stability Advisory Committee, November 2015, https://www.icann.org/en/system/files/files/sac-074-en.pdf,

[17] "SSAC Advisory on Fast Flux Hosting and DNS," ICANN Security and Stability Advisory Committee, March 2008, https://www.icann.org/en/system/files/files/sac-025-en.pdf

[18] Moore and Edelman, "Measuring the Perpetrators and Funders of Typosquatting," paper presented at the 14th Intl. Conference on Financial Cryptography and Data Security, Tenerife, January 2010, http://www.benedelman.org/typosquatting/typosquatting.pdf,

- **Search engine poisoning** is an activity that manipulates search engines to display search results that link to malicious websites.[20]
- **Spoofing attacks** are when a malicious actor impersonates another device or user in order to launch attacks against network hosts, steal data, spread malware, or bypass access controls.[21]
- **(Distributed) Denial of Service (DDoS) attacks** are cyber-attacks that work to make one or more computer systems unavailable. A *distributed* attack—carried out through a botnet—is when multiple systems are coordinated to overwhelm victims' servers with requests. A new form of **"amplified" DDoS attack** has emerged that use DNS reflection and amplification to achieve extremely high attack data bit rates (reportedly exceeding 300 gigabits per second), which overwhelm a victim's network capacity and result in significant or complete service outages.[22]
- **Domain shadowing** is another emerging form of DNS abuse in which criminals, using stolen or phished credentials, create numerous subdomains associated with existing legitimate domains in a registrant's portfolio. The legitimate domains continue to function normally from the view of the registrant while these subdomains direct visitors to malicious sites.[23]
- **DNS cache poisoning** is an attack in which a malicious actor tricks a name server into adding or modifying cached DNS data with malicious data. **Pharming** is one form of this activity in which a malicious actor coaxes a victim into clicking on a link—usually sent via spam email—which in turn infects the

---

[19] Fourth Global DNS Stability, Security, and Resiliency Symposium, Meeting Report, October 2012, https://www.icann.org/en/system/files/files/dns-symposium-25oct12-en.pdf,

[20] "Search Engine Poisoning," Imperva, accessed 1 February 2016, https://www.imperva.com/resources/glossary?term=search_engine_poisoning_sep,

[21] Veracode, "Spoofing Attack: IP, DNS & ARP," accessed 4 February 2016, http://www.veracode.com/security/spoofing-attack

[22] "SSAC Advisory on DDoS Attacks Leveraging DNS Infrastructure," ICANN Security and Stability Advisory Committee, February 2014, https://www.icann.org/en/system/files/files/sac-065-en.pdf. See also Alvarez, Carlos, "Amplified DDoS Attacks: The Current Biggest Threat Against the Internet," ICANN Blog, 11 April 2014, https://www.icann.org/news/blog/amplified-ddos-attacks-the-current-biggest-threat-against-the-internet

[23] "SSAC Advisory on Registrant Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle," ICANN Security and Stability Advisory Committee, November 2015, https://www.icann.org/en/system/files/files/sac-074-en.pdf

victim's personal computer or server and redirects users to fraudulent websites where confidential personal information can be gathered.[24]

A key factor to remember when it comes to nearly all of these tactics is that they exploit **human weaknesses** in the forms of greed, carelessness, and/or naiveté. Thus, **end-users tend to be the weakest links in the cyber-security chain**.[25]

DNS Abuse: Key Stats and Trends

A recent ICANN-sponsored global survey of 6,144 consumers reported the following:

- 74% were aware of phishing
- 79% were aware of spamming
- 40% were aware of cybersquatting
- 67% were aware of stolen credentials
- 76% were aware of malware

Along with high awareness of malicious behavior in the DNS, consumer end-users also reported high levels of being "very/somewhat scared" of each abusive behavior, and indicated a belief that they were also "very/somewhat" common.[26]

Symantec, one of the world's largest cyber-security firms, produces a yearly report on the state of global Internet security.[27] Its latest provides a number of indicators to illustrate general trends in key DNS abuse-related activities. As such it can serve as one point of departure for more segmented analysis of DNS abuse in new and legacy gTLDs as the work of the CCT-RT progresses:

Indicator	Descriptive Stats	Trend
Websites found with malware	• 2014: 1 in 1126 • 2013: 1 in 566	

[24] See Piscitello, Dave, "DNS Pharming: Someone's poisoned the water hole!", WatchGuard Technologies Expert Editorial, 2005, http://www.corecom.com/external/livesecurity/dnsphishing.htm

[25] Khonji, Mahmoud and Youssef Iraqi, "Phishing Detection: A Literature Survey," IEEE Communications Surveys & Tutorials 15, no. 4 (Q4 2013), doi: 10.1109/SURV.2013.032213.00009.

[26] ICANN Global Consumer Research, conducted by Nielsen, April 2015, https://www.icann.org/news/announcement-2015-05-29-en

[27] Symantec, "Internet Security Threat Report 20," April 2015, https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf

Overall Spam Rate (percentage of all emails classified as spam)	• 2015: 54%[28] • 2014: 60% • 2013: 66%	
Global Spam Volume per Day (estimated)	• 2014: 28 billion • 2013: 29 billion	
Email Phishing Rate (proportion of emails that are phishing attempts)	• 2014: 1 in 965 • 2013: 1 in 392	
New Malware Variants Added Each Year	• 2014: 317 million • 2013: 252 million	
Email Malware Rate (proportion of emails containing malware)	• 2014: 1 in 244 • 2013: 1 in 196 • 2012: 1 in 291	
Number of Bots	• 2014: 1.9 million • 2013: 2.3 million • 2012: 3.4 million	

While these data generally indicate downward trends in the specific forms of DNS abuse analyzed, it is important to note that they present a snapshot of those trends. For example, while phishing attacks appear to be going down according to the table, **since 2008 the number of phishing attacks has nearly doubled**, indicating the downward trend shown may be nothing more than a slight downtick in the overall trend line.[29] Furthermore, the data presented cover the *entire* DNS; they do not specifically describe DNS abuse in *new* gTLDs

DNS Abuse in New gTLDs

Few systematic studies on DNS abuse in new gTLDs have been conducted, which is likely a function of their newness. The ICANN-sponsored survey referenced above

[28] Note this 2015 number taken from Symantec's November 2015 Intelligence Report at www.symantec.com/content/en/us/enterprise/other_resources/intelligence-report-11-2015-en-us.pdf. The figure listed is an annual figure minus reporting for December 2015. Symantec did not report annualized 2015 figures for the other metrics listed in this table.

[29] Illumintel, "Potential for Phishing in Sensitive-String Top-Level Domains," study for the ICANN Board of Directors New gTLD Program Committee, 21 May 2015, https://www.icann.org/resources/pages/new-gtld-program-committee-2014-03-21-en

reported that **consumer trust in new gTLDs is much lower than in legacy TLDs**, with approximately 50% of consumers reporting trust in new versus approximately 90% reporting trust in legacy TLDs.[30] Researchers from the University of California, San Diego found that **new TLD domains are more than twice as likely as legacy TLDs to appear on a domain blacklist**—a list of domains of known spammers— within their first month of registration. [31]

According to members of the APWG, it appears that **malicious actors are testing the new gTLD space** as a potential base for their activities.[32] They suggest this may be a result of increased competition in the new gTLD market, which drives down prices and in turn attracts malicious actors looking to capitalize on lower costs. However, they note the difficulty in drawing conclusions based on limited comparative evidence given that new gTLDs are in the early phases of their introduction. They suggest that future studies compare DNS abuse in new and legacy TLDs when enough data is available.[33]

Architelos, a TLD consulting and management firm, offers more segmented analysis of DNS abuse in new, legacy, and country-code TLDs (ccTLDs). Their latest report, released in June 2015, utilizes their Namespace Quality Index (NQI) measure, which is the **amount of abuse domains listed on their blocklist portfolio per million domains** under management in each registry, to analyze the state of abusive behavior in legacy and new gTLDs. The report offers a number of important findings:[34]

- According to the NQI from January 2014 to June 2015, the rate of **abusive activities** (phishing, malware, botnet command and control, and spam) in new gTLDs **has spiked dramatically** since the first abuse in new gTLDs was detected in February 2014, and is approaching the levels of legacy gTLDs.
- **Spam accounts for 99% of reported abuses in new gTLDs** during the timeframe of their analysis (spam comprised 90% in legacy gTLDs and in ccTLDs).

---

[30] ICANN Global Consumer Research, conducted by Nielsen, April 2015, https://www.icann.org/news/announcement-2015-05-29-en

[31] Note this was a "snapshot" measure taken at the time of their study and did not reflect any longer term analysis. See Der et al., "From .academy to .zone: An Analysis of the New TLD Land Rush," University of California, San Diego, Department of Computer Science and Engineering, October 2015, doi: 10.1145/2815675.2815696.

[32] Anti-Phishing Working Group, "Global Phishing Survey: Trends and Domain Name use in 1H2014," 25 September 2014, https://apwg.org/apwg-news-center/

[33] Ibid.

[34] Architelos, "The NameSentry℠ Abuse Report," June 2015, http://architelos.com/wp-content/uploads/2015/06/Architelos-StateOfAbuseReport2015-webc-FIN.pdf

- In May 2015, **the NQI score for new gTLDs was 11,654 per million domains** under management compared to approximately **16,500 per million in legacy** gTLDs
- **Phishing, malware, and botnet command-and-control rates in new gTLDs are still very low** compared to legacy gTLDs, although this is likely to increase as awareness and adoption of new gTLDs increases. From May 2014 to May 2015, **the amount of phishing domains spiked** from seven blocklisted domains detected to 143, a 20-fold increase (compared to a rise from approximately 7,300 to 14,000 in legacy gTLDs for the same period). However, **77% of those 143 new phishing reports were concentrated in just ten new gTLDs**.

A Case Study in DNS Abuse: Phishing in New gTLDs

The prevalence of phishing can serve as one indicator of the extent to which malicious actors are abusing new gTLDs. In a study co-authored by members of the APWG, the authors noted that **the expansion of the DNS through the New gTLD Program is unlikely to increase the total amount of phishing in the world,** but will create **new, different locations from which phishing attacks can occur**, as cyber-criminals tend to favor "hopping" from TLD to TLD over time.[35] Phishers will not usually register domains that have brand names, instead preferring nonsense strings or placing a brand name somewhere in a subdomain or subdirectory, as brand owners routinely scan for their names being used inappropriately. In the second half of 2014, only 1.9% of all domains used for phishing contained a brand name or variation (often they were misspellings).

In another analysis paper written by members of the APWG, the authors reached a similar conclusion, noting that new gTLDs have not caused a "bonanza" of new phishing. The authors of both papers utilize a measure, "phishing domains per 10,000", which is the ratio of the number of domain names used for phishing in a TLD to the number of registered domain names in that TLD, as a gauge for the health of new TLDs as it pertains to phishing.[36] In their analysis, they conclude that a score **between 3.4 and 4.7 phishing domains per 10,000 represents a "middle ground" phishing prevalence score.**[37] Any score above 4.7 would indicate a TLD with above average levels of phishing. The median phishing domains per 10,000 score for all TLDs in the second half of 2014 was 3.4. **Only nine of the 295 *new* gTLDs (in 2014) had**

---

[35] Illumintel, "Potential for Phishing in Sensitive-String Top-Level Domains," study for the ICANN Board of Directors New gTLD Program Committee, 21 May 2015, https://www.icann.org/resources/pages/new-gtld-program-committee-2014-03-21-en

[36] Anti-Phishing Working Group, "Global Phishing Survey: Trends and Domain Name use in 2H2014," 27 May 2015, https://apwg.org/apwg-news-center/

[37] Note the APWG's report from the first half of 2014 suggested a measure between 4.1 and 4.7. These measures change according to the "curve" of overall phishing activity.

scores above 3.4.[38] In addition, **the average "uptimes" of phishing attacks**—or how long those attacks are active and a key measure of the strength of phishers' efforts—**are at historic lows**, indicating some **success of anti-phishing efforts**.[39]

According to the authors of both papers, **domain price appears to be a significant driver of phishing** in TLDs, and domains tend to be cheaper in legacy TLDs.[40] This sentiment was echoed by a number of representatives from registries and registrars at an ICANN-sponsored teleconference on measuring DNS abuse, who indicated that **higher prices for domains was a key factor in reducing abusive activities in general**.[41] The authors from the APWG predict that as new gTLDs become more prevalent and prices drop due to increased supply and competition, we will see more phishing in them compared to legacy and country-code TLDs (ccTLDs). A key piece of evidence for this trend is demonstrated by the case of the .xyz gTLD, which offered free domains for a period of time. In the second half of 2014, nearly 2/3 of phishing in new gTLDs was concentrated in the .xyz registry.[42] Keeping costs down appears to be a significant concern for phishers, as studies have shown it to be an increasingly "low-skill low-reward business."[43] While some stories show spectacular profits as a result of phishing, it appears as though the average phisher can net something on the order of a few hundred US dollars per week.[44]

---

[38] Anti-Phishing Working Group, "Global Phishing Survey: Trends and Domain Name use in 2H2014," 27 May 2015, https://apwg.org/apwg-news-center/

[39] The second half of 2014 did see a slight uptick in *median* uptimes, from 8 hours and 42 minutes to 10 hours and 6 minutes. See Anti-Phishing Working Group, "Global Phishing Survey: Trends and Domain Name use in 2H2014," 27 May 2015, https://apwg.org/apwg-news-center/

[40] Anti-Phishing Working Group, "Global Phishing Survey: Trends and Domain Name use in 2H2014," 27 May 2015, https://apwg.org/apwg-news-center/

[41] One participant anecdotally posited a threshold of greater than US$15 for a domain was generally when abuse rates began to decline. ICANN Operations and Policy Research, "Reviewing New gTLD Program Safeguards Against DNS Abuse," 28 January 2016, teleconference proceedings, recordings available at https://newgtlds.icann.org/en/reviews/dns-abuse

[42] The authors note that most of the .xyz phishing registrations were made through Chinese registrars and used to attack Chinese targets. See Anti-Phishing Working Group, "Global Phishing Survey: Trends and Domain Name use in 2H2014," 27 May 2015, https://apwg.org/apwg-news-center/

[43] Herley and Florencio, "A Profitless Endeavor: Phishing as Tragedy of the Commons," Microsoft Research, September 2008, http://research.microsoft.com/en-us/um/people/cormac/Papers/PhishingAsTragedy.pdf

[44] Ibid. Given its "underground" nature, data is difficult to obtain. Thus, there is still significant debate on the actual costs and benefits of phishing in general.

The Nine Safeguards

In the lead-up to the New gTLD Program, ICANN solicited advice from subject matter experts in DNS abuse and cyber-security to suggest what pre-emptive measures could be taken to mitigate the kinds of activities explored above. The expert community arrived at the following nine safeguards presented below. It now remains with the CCT-RT to determine the extent to which these safeguards were effective in achieving their intended aims.

In order to understand the "effectiveness" of the nine safeguards to mitigate DNS abuse, **"effectiveness" must first be defined as a measureable concept**. The following pages will discuss such definitions in the context of each question posed as part of initial efforts to establish what kinds of safeguards would be necessary for the New gTLD Program. Available data on proposed "effectiveness" measures will be presented. If data is unavailable, then a discussion of the reasons behind the lack of data and other potential means to assess a given safeguard's effectiveness will follow.

Question: How do we ensure that bad actors do not run Registries?

"Effectiveness" in the context of this question can be understood as preventing "bad actors," such as those who have been convicted of a felony or misdemeanor related to financial activities, from running registries. As early as 2001, the .COM Registry Agreement mandated that termination of the Registry Agreement would be possible if a registry operator was:

> "(a) convicted by a court of competent jurisdiction of a felony or other serious offense related to financial activities, or is the subject of a determination by a court of competent jurisdiction that ICANN reasonably deems as the substantive equivalent of those offenses; or (b) is disciplined by the government of its domicile for conduct involving dishonesty or misuse of funds of others."[45]

This clause also exists in the New gTLD Registry Agreement, along with additional provisions:

> (f) ICANN may, upon notice to Registry Operator, terminate this Agreement if (i) Registry Operator knowingly employs any officer who is convicted of a misdemeanor related to financial activities or of any felony, or is judged by a court of competent jurisdiction to have committed fraud or breach of fiduciary

[45] ".com Registry Agreement," 25 May 2001, https://www.icann.org/resources/unthemed-pages/registry-agmt-com-2001-05-25-en#II-16C.

duty, or is the subject of a judicial determination that ICANN reasonably deems as the substantive equivalent of any of the foregoing and such officer is not terminated within thirty (30) calendar days of Registry Operator's knowledge of the foregoing, or (ii) any member of Registry Operator's board of directors or similar governing body is convicted of a misdemeanor related to financial activities or of any felony, or is judged by a court of competent jurisdiction to have committed fraud or breach of fiduciary duty, or is the subject of a judicial determination that ICANN reasonably deems as the substantive equivalent of any of the foregoing and such member is not removed from Registry Operator's board of directors or similar governing body within thirty (30) calendar days of Registry Operator's knowledge of the foregoing.[46]

Safeguard: Vet Registry Operators

Background

Vetting registry operators prior to execution of a Registry Agreement and delegation of a TLD into the root zone was added as a safeguard to the gTLD Applicant Guidebook for the New gTLD Program in order to prevent applicants with a history of criminal or malicious behavior from running TLDs. The measure was developed as a means to create a defined process to screen registry operators prior to signing the Registry Agreement during the initial evaluation of applications.

ICANN engaged PricewaterhouseCoopers (PwC) to perform background screenings focused on two areas: 1) general business diligence and criminal history, and 2) history of cybersquatting behavior. The eligibility of a given application to proceed in the New gTLD Program was reported in Initial Evaluation and, sometimes, Extended Evaluation reports.

The background screening used in the New gTLD Program is conducted at a point in time during the Initial Evaluation process. In cases where an applicant reported changes to its application information in the course of the evaluation, an additional background screening occurred prior to signing the Registry Agreement. And in every case, ICANN reserved the right to conduct additional due diligence as necessary before signing an agreement.

Defining "Effectiveness"

For this safeguard, "effectiveness" can be conceived as preventing registry operators with a malicious or criminal history from signing a Registry Agreement with ICANN. However, as noted above, a vetting process occurs at a point in time, and changes can occur in the entity responsible for management of a TLD (e.g., a company may be sold, or an officer may be replaced). In the context of DNS abuse, it may also be important

[46] "Registry Agreements," 9 January 2014, https://www.icann.org/resources/pages/registries/registries-agreements-en

to consider whether there is evidence of bad actors running registries, or a risk of such, on an ongoing basis.

Current Context

According to the Program Implementation Review published in January 2016, the background screening process was "a review performed on all applying entities, and all individuals and organizations disclosed in questions 9-11 of the application, which included officers and directors of the applying entities, in addition to shareholders owning a significant stake in the entity."[47] According to the Review, ICANN conducted 1,150 background screenings on 1,930 applications (a number of entities submitted multiple applications). The background screening results for each application were reported following the completion of its Initial Evaluation procedures. In some cases clarifying questions were posed to the applicant by the background screening panel. Overall, the Program Implementation Review called the background screening a successful process as all applicants were able to be screened, but noted that the time between the application submission deadline and the signing of the Registry Agreements was longer than anticipated. This meant that many applicants had to be re-screened. The Review suggests that background screenings could be conducted at the contracting stage rather than during Initial Evaluation to minimize the need for re-screening.

Possible Methods of Data Collection and Measurement

It may be too soon to determine if *both* aspects of the safeguard have been effective as preventative measures. Any measure of "effectiveness" would have to take into account data on rejections based on the initial background screening as well as from terminations of Registry Agreements due to a registry's failure to eliminate bad actors from its officer staff or board of directors. And due to the personal information involved and sensitivity around the background screening process, reports indicating whether applications were eligible to proceed to the next step in the process are limited. However, overall numbers are available. Formal compliance complaints and/or terminations of Registry Agreements could provide a gauge of whether this safeguard continues to be effective.[48]

Additionally, the safeguard may have had a deterrent effect on prospective applicants with questionable staff backgrounds. However, measuring a deterrent effect—i.e. how many applicants *did not* apply—is near impossible given that such an effect does not generate measurable data.

---

[47] "Program Implementation Review," 29 January 2016, https://www.icann.org/en/system/files/files/program-review-29jan16-en.pdf

[48] The International Trademark Association supported these measures to gauge this safeguard's effectiveness in its public comments on this report.

Question: How do we ensure integrity and utility of registry information?

Defining "effectiveness" in terms of this question can be understood as the successful use of safeguards to aid in validating and securing registry information. The following three preventative safeguards were designed to accomplish this.

Safeguard: Require Demonstrated Plan for DNSSEC Deployment

Background

The Domain Name System Security Extension (DNSSEC) was developed to curtail attempts by malicious actors to hijack the DNS lookup process. Such actors can hack into a web user's lookups and, for example, direct them to their malicious websites to steal confidential information. DNSSEC protects against such attacks by digitally signing data so users can be assured the source is valid. It employs cryptographic signatures to existing DNS records to verify that a DNS record comes from its official name server and was not altered at any point.[49] Registries' deployment of DNSSEC allows registrants to assign specific domain name keys to their domains if they choose. Mandating DNSSEC via the Registry Agreement was aimed at ensuring its more widespread and rapid deployment.

The safeguard requires all new gTLD applicants to have a specific plan for DNSSEC deployment.[50] This is evaluated during the Initial Evaluation process, with the primary aim to reduce the risk of spoofed DNS records. Under the Registry Agreement, new gTLD registry operators are required to sign TLD zone files with DNSSEC, follow best practices as described in the Internet Engineering Task Force's (IETF) RFC 4641 and its successors, accept public-key material from child domain names in a secure manner, and publish the DNSSEC Practice Statements (DPS) according to the format in RFC 6841.[51] [52]

---

[49] "DNSSEC – What Is It and Why Is It Important?" accessed 1 February 2016, https://www.icann.org/resources/pages/dnssec-qaa-2014-01-29-en; "How DNSSEC Works," accessed 1 February 2016, https://www.cloudflare.com/dnssec/how-dnssec-works/

[50] In its public comment on this report, the Governmental Advisory Committee noted several background documents from ICANN's Security and Stability Advisory Committee (SSAC) on DNSSEC's development and deployment. See SAC 26, 29, 30, 35, 63 at www.icann.org/groups/ssac/documents.

[51] ICANN Registry Agreement, Specification 6: 1.2 DNSSEC, accessed 1 February 2016, https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm

[52] "RFC" is a "Request for Comments" series of documents produced by the IETF that contain technical and organizational briefs on computer networking, protocols, procedures, and concepts. See www.ietf.org/rfc.

Defining "Effectiveness"

"Effectiveness" of this safeguard can be defined in a number of ways. It could be defined simply as a registry operator having a specific plan for DNSSEC deployment, and passing the evaluation at the application stage. It could also be defined according to the number of issues reported on registry compliance with DNSSEC requirements. In its public comment on this report, the Registry Stakeholder Group suggested that the average time in which DNSSEC compliance issues are resolved could provide a measure to gauge "the execution and implementation" of DNSSEC. Finally, it could be defined according to more broad dissemination of DNSSEC, such as the rate of signing done by registrants or the development of DNSSEC-validating DNS resolvers within networks run by Internet Service Providers (ISPs).[53]

Current Context

As of 23 February 2016, 1,073 of the 1,236 TLDs (including ccTLDs) in the root zone had signed DNSSEC keys.[54] In its public comment on this report, the Intellectual Property Constituency noted that DNSSEC is widely regarded as effective among the ICANN community.

Possible Methods of Data Collection and Measurement

Two measurements available now are the number of TLDs in the root zone and number of second-level domains in each that have signed keys.[55] More in-depth measures could focus on measuring DNSSEC issues that were discovered during pre-delegation testing, how many service-level agreement (SLA) monitoring issues have been reported, and the number of complaints have been received regarding DNSSEC compliance.

A comprehensive measure of "effectiveness" in this area would need to take into account the fact that registrars, registrants, DNS hosting providers, and ISPs all play a key role in full DNSSEC deployment and functionality. For example, while registry operators are required to demonstrate a plan for DNSSEC deployment, this does not mean that registrants will necessarily sign on. Preliminary data collected by ICANN Technical Services indicate that often only a small percentage of second-level domains have signed DNSSEC keys (although this varies significantly by TLD).[56] A

---

[53] "Deployment Guide: DNSSEC for Internet Service Providers (ISPs)," accessed 1 February 2016, http://www.internetsociety.org/deploy360/resources/deployment-guide-dnssec-for-isps/

[54] "TLD DNSSEC Report," accessed 23 February 2016, http://stats.research.icann.org/dns/tld_report/

[55] See "DNSSEC Deployment Report," accessed 23 February 2016, http://rick.eng.br/dnssecstat/

[56] Data collected by ICANN Technical Services from publicly available zone files for the purposes of this report.

potential case study to consider could be that of CloudFlare—a domain name server services and DNS content delivery company—who decided to let anyone on their network secure their traffic with DNSSEC in a single step. A case study approach that provides a cross-industry look at support for DNSSEC by registries, registrars, DNS hosting providers, and ISPs could allow for the identification of areas of weakness in the deployment of DNSSEC across gTLDs. A group already collecting this information is the DNSSEC Deployment Working Group, which provides reports at dnssec-deployment.org.

Safeguard: Prohibition of Wildcarding

Background

This recommendation requires appropriate controls to prevent DNS "wildcarding." This is when, rather than providing a "name error" response for non-existent DNS queries, registry operators instead use DNS redirection, wildcards, or synthesized responses.[57] ICANN has prohibited these actions due to findings that suggest they pose a danger to the security and stability of the DNS by creating new opportunities for malicious attacks.[58]

This safeguard is defined in section 2.2 of Specification 6 to the Registry Agreement:

> 2.2. Wildcard Prohibition. For domain names which 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 status does not allow them to be published in the DNS, the use of DNS wildcard Resource Records as described in RFCs 1034 and 4592 or any other method or technology for synthesizing DNS Resources Records or using redirection within the DNS by the Registry is prohibited. When queried for such domain names the authoritative name servers must return a "Name Error" response (also known as NXDOMAIN), RCODE 3 as described in RFC 1035 and related RFCs. This provision applies for all DNS zone files at all levels in the DNS tree for which the Registry Operator (or an affiliate engaged in providing Registration Services) maintains data, arranges for such maintenance, or derives revenue from such maintenance.

However, in 2014, as part of the Name Collision Occurrence Management Framework, wildcarding was deployed in some TLDs for a limited period immediately after the delegation of the TLD (the controlled interruption period) as a means to identify any

---

[57] "About Wildcard Prohibition (Domain Redirect)," accessed February 1, 2016, https://www.icann.org/resources/pages/wildcard-prohibition-2014-01-29-en

[58] ICANN Security and Stability Advisory Committee, "SAC041: Recommendation to prohibit use of redirection and synthesized responses by new TLDs," 10 June 2009, https://www.icann.org/en/system/files/files/sac-041-en.pdf

namespace collisions.[59] As stated in the JAS Phase 1 Report *Mitigating the Risk of DNS Namespace Collisions*:

> We recommend that the registry implement the controlled interruption period immediately upon delegation in the root zone and the prohibition on wildcard records be temporarily suspended during this period. Given the objective of controlled interruption and the reality that no registrant data will be in the zone at this point, we believe that temporarily permitting wildcard records for this purpose is not counter to established ICANN prohibitions on wildcard records and does not raise the concerns that lead ICANN to establish these prohibitions.[60]

Defining "Effectiveness"

For this measure, "effectiveness" could theoretically be defined in terms of the degree of compliance with the prohibition on wildcarding in new gTLDs. The assessment of this behavior as a means of ensuring the integrity and utility of registry information can also be considered. Input regarding the impact on the behaviors this safeguard sought to prevent could also be assessed.

Current Context

ICANN makes available a "Wildcard Prohibition (Domain Redirect) Complaint Form" to allow reports of noncompliance with contractual provisions.[61] To date, ICANN has not

---

[59] See "Frequently Asked Questions: Name Collision Occurrence Management Framework for Registries," accessed 11 February 2016, www.icann.org/resources/pages/name-collision-ro-faqs-2014-08-01-en, which states: "The prohibition against wildcards is waived for the controlled interruption period for applicable TLDs (i.e., where there are no active names under the TLD other than 'nic'). This waiver only applies while there are no names delegated (hence, operational) within that TLD, removing the risks that are traditionally associated with wildcard implementations. The reason for lifting the prohibition and specifying the use of the wildcard is to catch all evident name collision situations. The wildcard at the 'top' of the zone will match all of the queries that will ever be seen once the zone runs in full production. This approach maximizes the steps taken to protect Internet users that are currently leaking queries that are meant to be local."

[60] JAS Global Advisors, "Mitigating the Risk of DNS Namespace Collisions," 4 June 2014, https://www.icann.org/en/system/files/files/name-collision-mitigation-study-06jun14-en.pdf

[61] See "Wildcard Prohibition (Domain Redirect) Complaint Form," accessed 11 February 2016, https://forms.icann.org/en/resources/compliance/registries/wildcard-prohibition/form

received any complaints on wildcard prohibition through this tool.[62] In its public comment on this report, the Intellectual Property Constituency noted that the prohibition of wildcarding is widely regarded as effective among the ICANN community.

Possible Methods of Data Collection and Measurement

As noted above, no complaints have been received concerning wildcarding by new gTLD registries. Qualitative inquiry with subject matter experts on the effectiveness of this safeguard may be a means of circumventing this lack of quantitative data.

Another approach could include looking not only at complaints to ICANN about failures to prohibit wildcarding in specific TLDs, but also the current prevalence of the use of DNS redirection for "error traffic monetization," which is the practice of redirecting DNS users to advertisement-oriented web servers when their DNS lookups fail. The University of California, Berkeley's ICSI Netalyzr is a network diagnosis tool as well as part of a measurement study that is working to measure the health of the Internet. It has been used in previous studies examining issues of DNS redirection and may be a useful tool for understanding the implications of wildcarding in the DNS.[63]

Safeguard: Removal of Orphan Glue Records

Background

This safeguard was developed to reduce the risk of malicious actors sneaking links to malicious domains into the root zone via "orphan glue" records, which are name server records that can remain once a "parent" record is removed from the zone. Orphan glue records can allow malicious actors to gain control of name servers, which then gives them the ability to carry out malicious activities from seemingly "legitimate" domains. For example, "fast-flux" attacks are known to make use of orphan glue records to host malicious domains for short amounts of time.[64]

The safeguard requires registry operators to provide a plan in their application to remove orphan glue records once the parent record is removed. Once bound by the

---

[62] However, Compliance has received some complaints on "Reserved Names/Controlled Interruption." See "ICANN Contractual Compliance Dashboard for 2016," accessed 12 February 2016, https://features.icann.org/compliance/dashboard/0116/report

[63] Weaver, Kreibich, and Paxson, "Redirecting DNS for Ads and Profit," USENIX Workshop on Free and Open Communications on the Internet (FOCI), 2011, http://www.icir.org/christian/publications/2011-foci-dns.pdf

[64] See ICANN Security and Stability Advisory Committee, "SSAC Advisory on Fast Flux Hosting and DNS," March 2008, https://www.icann.org/en/system/files/files/sac-025-en.pdf

terms of the Registry Agreement, registry operators are required to take action to remove orphan glue records per specification 6, section 4.2 of the Agreement, which states: "Registry Operator shall take action to remove orphan glue records… when provided with evidence in written form that such records are present in connection with malicious conduct."[65]

Defining "Effectiveness"

For this measure, "effectiveness" can be understood as regularized practices on the part of registries to provide points of contact for end-users to report abuse and confirm the automatic removal of orphan glue records when a parent record is removed from the zone.

Current Context

Initial community feedback on this issue suggests that orphan glue records as a source of abuse has been largely neutralized through regular practice of removing them from zone files, although they remain a "low-level" issue in some cases.[66] In its public comment on this report, the Intellectual Property Constituency noted that the removal of orphan glue records is widely regarded as an effective safeguard among the ICANN community.

Possible Methods of Data Collection and Measurement

ICANN has received some initial feedback suggesting that this safeguard be measured by using zone files to track orphan glue record removal over time.

Discussing the prevalence and use of orphan glue records for malicious purposes with registry operators could provide a qualitative measure of whether registries, registrars, and registrants are effectively utilizing the required mechanisms for removal of orphan glue records. The "evidence in written form" required for a registry operator to remove orphan glue records as mandated by Specification 6 may also provide a useful source of data. It may also be useful to locate instances of recommendations for the removal of orphan glue records in registry anti-abuse policies. For example, the ".rich" TLD includes a section focusing on the removal of

---

[65] See ICANN Security and Stability Advisory Committee, "SSAC Comment on Orphan Glue Records in the Draft Applicant Guidebook," May 2011, https://www.icann.org/en/system/files/files/sac-048-en.pdf.

[66] ICANN Operations and Policy Research, "Reviewing New gTLD Program Safeguards Against DNS Abuse," 28 January 2016, teleconference proceedings, recordings available at https://newgtlds.icann.org/en/reviews/dns-abuse

orphan glue records in its anti-abuse policy,[67] while Afilias focuses on the issue as an element of fast flux hosting.[68]

Question: How do we ensure more focused efforts on combating identified abuse?

This question focuses on the availability of information to curtail the activities of and aid in locating identified abusers in the DNS.

Safeguard: Requirement for Thick WHOIS records

Background

This safeguard requires that new gTLDs maintain and provide access to "thick WHOIS" records to help improve the availability and completeness of WHOIS data. Thick WHOIS records are records held by registries that "contain the registrant's contact information and designated administrative and technical contact information, in addition to the sponsoring registrar and registration status."[69] This is in contrast to "thin WHOIS" records, which only store information sufficient to identify the sponsoring registrar and status of the registration, and provide no information on the registrant. The use of thick WHOIS records may allow for more complete and rapid data search during efforts to identify malicious actors operating in the DNS.

Defining "Effectiveness"

For this measure, "effectiveness" can be defined by the development of a set of thick WHOIS records that are regularly used by authorities to track, identify, and curtail the activities of malicious actors in the DNS. In their public comments on this report, the Intellectual Property Constituency and DotMusic noted the effectiveness of thick WHOIS records in helping to curtail intellectual property infringement and taking action against online piracy. DotMusic additionally noted that the emergence of proxy registration services has "effectively hidden the needed contact details for quarter or more of all registrations in the generic Top Level Domains" (p. 13)

---

[67] ".RICH Anti-Abuse Policy," accessed 11 February 2016, http://nic.rich/files/policies/rich-anti-abuse-policy.pdf,
[68] "Afilias Anti-Abuse Policy," accessed 11 February 2016, http://dotblue.blue/about/afilias-anti-abuse-policy
[69] ICANN WHOIS, "WHOIS Primer," accessed 11 February 2016, https://whois.icann.org/en/primer

Current Context

Every new gTLD registry operator who has had their TLD(s) delegated into the root zone is required to create and maintain thick WHOIS records as part of their contractual obligations.

Possible Methods of Data Collection and Measurement

The intention behind mandating that new gTLD registries maintain thick WHOIS records was to create a more comprehensive set of contact records to enable authorities to track down and stop malicious activity. Obtaining feedback from DNS abuse responders regarding the utility of thick versus thin WHOIS records in curtailing DNS abuse could be one means of assessing this safeguard's effectiveness. Along these lines, the International Trademark Association suggested a survey of abuse responders and law enforcement on the effectiveness of this safeguard in combatting abusive activities.

Other potential measures could stem from data generated by the WHOIS Accuracy Reporting System (ARS), which is a project currently in development whose goal is to "identify and report on accuracy in a systematic way to improve quality of contact data in the WHOIS".[70] The following charts from the Phase 2 Report published December 2015 summarize overall gTLD accuracy to 2009 Registrar Accreditation Agreement (RAA) Syntax Requirements by mode and overall gTLD accuracy to 2009 RAA operability requirements by mode:[71]

Overall gTLD Accuracy to 2009 RAA Syntax Requirements by Contact Mode

	Email	Telephone	Postal Address	ALL 3 Accurate
All 3 Contacts Accurate	99.1% ± 0.2%	83.3% ± 0.7%	79.4% ± 0.8%	67.2% ±0.9%

Overall gTLD Accuracy to 2009 RAA Operability Requirements by Contact Mode

	Email	Telephone	Postal Address	ALL 3 Accurate

[70] Note that Phase 3 of the study has yet to be carried out, but intends to focus on "Identity Requirements," which test whether the contact provided is actually the individual or entity responsible for the domain. "Syntax Requirements" are defined as the format of the WHOIS entry. "Operability Requirements" are defined as the ability for contacts to resolve and connect to a user. Note that while contacts may be operable and connect to a user, the ARS does not test whether that user is the one indicated in the WHOIS record. See "WHOIS ARS Phase 2 Cycle 1 Report: Syntax and Operability Accuracy," accessed February 1, 2016, https://whois.icann.org/en/file/whois-ars-phase-2-cycle-1-report-syntax-and-operability-accuracy and "WHOIS Accuracy Reporting System (ARS)," accessed 11 February 2016, https://whois.icann.org/en/whoisars

[71] Ibid.

All 3 Contacts Accurate	87.1% ± 0.7%	74.0% ± 0.9%	98.0% ± 0.3%	64.7% ±0.9%

The three phases of the WHOIS ARS study—which focus on syntax, accuracy, and validity, respectively—may provide a set of proxy measures for this safeguard's effectiveness. In theory, more accurate WHOIS records would provide the anti-abuse community with a useful tool to combat DNS abuse. However, it is unlikely that malicious actors would proactively give out "accurate" contact details. In their public comment on this report, the Intellectual Property Constituency noted that the WHOIS ARS does not take into account privacy and proxy services, which may result in a skewed impression of actual accuracy. It remains with the CCT-RT to decide whether "syntax, accuracy, and validity" are adequate proxies for effectiveness in this area.

Safeguard: Centralization of Zone-File Access

Background

This safeguard requires that access credentials to obtain registry zone file data be made available through a centralized source, which allows the anti-abuse community to more efficiently obtain updates on new domains as they are created within each TLD zone. This was intended to reduce the time necessary to take corrective action within TLDs experiencing malicious activity.

Defining "Effectiveness"

For this safeguard, "effectiveness" could be defined by the capacity of the Centralized Zone Data Service (CZDS) to handle requests for registry zone file data in a timely and efficient manner in order to minimize response times in countering malicious activity.

Current Context

New gTLD registries are required under Specification 4, Section 2 of the Registry Agreement to provide zone data to end users who request it. ICANN's publicly available reports show more than 3 million zone file access (ZFA) passwords approved for 2015 alone.[72] Conversations with security researchers for the purposes of this report indicate that the CZDS provides a valuable service to DNS abuse responders and to those seeking to protect their intellectual property. The Intellectual Property Constituency echoed this sentiment in their public comments on this report. However, while the CZDS was developed with the intention to make the process for providing access to zone files more efficient, registries themselves have reported widespread

[72] CZDS ZFA- Password Monthly Reports, accessed 1 February 2016, https://czds.icann.org/en/reports

frustration with the service.[73] Registry operators still have to verify an end-user, and the Registry Agreement does not delimit the time in which registry operators must respond to access requests. This results in an often unmanageable amount of requests "piling up" for registry operators and a lack of capacity on their part to respond to requests in a timely manner. One registry representative reported receiving 7,000-10,000 requests for zone file access *per day.*[74] This can result in less than full enforcement of the terms of use and cursory verification of the requestor's credentials.[75] ICANN Compliance identified requests for zone file access by third parties via the CZDS as one of the top issues in registry compliance for 2015, with most complaints pertaining to registry operators not responding to requests for zone file access and registry operators being denied access for reasons not permitted in the Registry Agreement.[76]

Possible Methods of Data Collection and Measurement

A potential proxy for "effectiveness" could be gauged through CZDS password reports, which show the number of ZFA-passwords (given to users who have requested access to zone files in bulk) within the CZDS and the number of passwords approved each month within specific TLDs and as a whole.[77] User feedback on the service may provide additional depth to such a measure as many users report problems with handling CZDS requests, at least anecdotally.

Safeguard: Documented Registry- and Registrar- Level Abuse Contacts and Procedures

Background

This safeguard requires that registry operators establish a single point of contact responsible for handling abuse complaints. The Applicant Guidebook directs applicants to develop an "implementation plan to establish and publish on its website a single abuse point of contact responsible for addressing matters requiring expedited attention and providing a timely response to abuse complaints…".[78] Specification 6,

---

[73] ICANN Operations and Policy Research, "Reviewing New gTLD Program Safeguards Against DNS Abuse," 28 January 2016, teleconference proceedings, recordings available at https://newgtlds.icann.org/en/reviews/dns-abuse

[74] Ibid.

[75] Ibid.

[76] "ICANN Contractual Compliance 2015 Annual Report,"January 2016, https://www.icann.org/en/system/files/files/annual-2015-27jan16-en.pdf

[77] CZDS ZFA- Password Monthly Reports, accessed 1 February 2016, https://czds.icann.org/en/reports

[78] "gTLD Applicant Guidebook," 4 June 2012, https://newgtlds.icann.org/en/applicants/agb

section 4.1 of the Registry Agreement states: "Registry Operator shall provide to ICANN and publish on its website its accurate contact details including a valid email and mailing address as well as a primary contact for handling inquiries related to malicious conduct in the TLD, and will provide ICANN with prompt notice of any changes to such contact details."[79]

Defining "Effectiveness"

For this measure, "effectiveness" could be measured by the availability of this information to front-end users, and finding a way to measure the relative ease with which users can report DNS abuse. A complementary approach could be to interview law enforcement and registry operators themselves for their feedback on the effectiveness of this measure.

Current Context

ICANN Compliance has monitored abuse contact information that registries are required to post on their websites, and stated the following in the last Contractual Compliance Update to review the issue:

> ICANN continued its proactive monitoring of the abuse contact information that registries under the New Registry Agreement must publish on their websites. By doing so, ICANN ensures that end-users, including but not limited to law enforcement agencies, find a point of contact to report malicious activities in the TLDs…ICANN reviewed the websites of 64 top-level domains that started the Claims Period between 1 January 2015 and 31 March 2015. The number of non-compliance inquiries or notices to registries was lower than in the previous round of monitoring. Some of the deficiencies noted were the following: not displaying the required information at all, missing primary contact, or missing mailing address for abuse reports. ICANN is collaborating with the registries to remediate the non-compliance found.[80]

Some initial community feedback on this safeguard indicates that the points of contact for abuse were used mostly by spammers.[81]

---

[79] "Registry Agreements," 9 January 2014, https://www.icann.org/resources/pages/registries/registries-agreements-en

[80] See "ICANN Contractual Compliance Update January – March 2015," https://www.icann.org/en/system/files/files/compliance-update-mar15-en.pdf.

[81] ICANN Operations and Policy Research, "Reviewing New gTLD Program Safeguards Against DNS Abuse," 28 January 2016, teleconference proceedings, recordings available at https://newgtlds.icann.org/en/reviews/dns-abuse

Possible Methods of Data Collection and Measurement

Analyzing ICANN Compliance reports and testimonials from those who use these contacts could be an approach to measuring the effectiveness of this safeguard. Another method could entail collecting registry abuse contact information and testing its functionality. The International Trademark Association and Intellectual Property Constituency suggested assessing registry operators' responsiveness to abuse claims received via this channel in their public comments on this report.

Safeguard: Participation in an Expedited Registry Security Request Process (ERSR)

Background

This safeguard provides a mechanism for registry operators to take quick and decisive action in light of systemic threats to the DNS by establishing a dedicated process to review and approve expedited security requests. In practice, registries are allowed to request a contractual waiver that exempts them from a specific provision in the Registry Agreement for the time period required to respond to a security threat. It was designed to provide for operational security around a threat while keeping relevant parties informed of the threat's status. Note that this process was established in response to the Conficker virus and thus before the work to define safeguards for the New gTLD Program. It is not included in the latest Registry Agreement, but as a process is available to registries with a clear and present need for it.[82]

Defining "Effectiveness"

"Effectiveness" could be conceptualized as the rapidity with which a security threat was identified and neutralized as a result of the ERSR.

Current Context

Given the sensitive nature of the data involved, ICANN does not report publicly on the details of this process. However, initial input from security researchers for the purposes of this report indicate that the safeguard has been used effectively since the emergence of the Conficker virus to dismantle subsequent botnets.

Possible Methods of Data Collection and Measurement

To understand the effectiveness of this measure, feedback from those who have requested the ERSR process could be collected to understand its capacity to handle security threats. Given the limited quantity of requests for the ERSR and the sensitivity of the security-oriented data inherent to the process, analytical focus could be placed on *how* the process was carried out—such as the speed and relative ease of

[82] "Registration Abuse Policies Working Group Final Report," May 2010, http://gnso.icann.org/en/issues/rap/rap-wg-final-report-29may10-en.pdf

addressing the threat as a result of the ERSR—rather than the number of instances the ERSR has been requested or the specifics of how the security threat was confronted.[83]

Question: How do we provide an enhanced control framework for TLDs with intrinsic potential for malicious conduct?

Safeguard: Create a Draft Framework for a High Security Zone Verification Program

Background

This *recommendation*—it was never formally established in the Registry Agreement as a required safeguard nor instituted as an official, ICANN-backed initiative—suggested the creation of a voluntary program for registry operators who wanted to establish and prove an enhanced level of security and trust in their TLDs. The overall goal of the program was to provide a standardized set of practices for registries seeking to distinguish themselves along these lines.[84]

Defining "Effectiveness"

For this measure, "effectiveness" could be seen as the successful adoption, implementation, and verification of a high security zone (HSZ) in a TLD with a high potential for malicious activity (e.g. those representing the banking/financial and pharmaceutical sectors).

Current Context

While no comprehensive draft framework for such a program has been formalized through ICANN's various policy development and implementation mechanisms, a number of efforts have been aimed at addressing the increased security needs of certain strings.

During the application process for a new gTLD, applicants' security policies as they relate to sensitive strings were assessed under the guidelines of question 30 of the Applicant Guidebook, which requires applicants to

> …provide a summary of the security policy for the proposed registry, including but not limited to…[a] description of any augmented security levels or capabilities commensurate with the nature of the applied for TLD string,

---

[83] The International Trademark Association and Dot Music supported "response time" to address identified threats as a means to measure the effectiveness of this safeguard in their public comments on this report.

[84] icann.org, "Public Comment: High Security Zone TLD Final Report," 11 March 2011, https://www.icann.org/news/announcement-2011-03-11-en

> including the identification of any existing international or industry relevant security standards the applicant commits to following…[85]

Additionally, ICANN's Governmental Advisory Committee has recommended a model be created for the verification and validation of registry operator credentials as public interest commitments (PICs) in highly regulated sectors in order to establish and maintain the trustworthiness of those domains.[86]

A number of independent efforts to increase security and trust in new gTLDs on the part of industry associations and registries have also emerged. For example, the fTLD Service, LLC registry is independently working to establish a high security zone for their ".bank" and ".insurance" TLDs.[87] The "DNS Seal Project" is working to build trust in the domain name industry through self-regulation and identification of best practices to help internet users identify trustworthy websites.[88]

Possible Methods of Data Collection and Measurement

Collecting feedback from registry operators on why they chose not to pursue HSZ verification could provide insight into this recommended safeguard's lack of adoption. Also, speaking with the fTLD Service, LLC registry on why they chose to pursue their own HSZ could provide an additional source of data. In their public comments on this report, the Registry Stakeholder Group and International Trademark Association suggested that abuse rates be compared in TLDs with HSZ protocols in place to those without such protocols. The Governmental Advisory Committee noted that future research in this area should account for the different "risk profiles" of TLDs operating in different sectors. For example, TLDs related to banking and pharmaceuticals carry a higher risk of user harm should their security be compromised when compared to TLDs related to the entertainment industry. The Intellectual Property Constituency recommended that the CCT-RT focus on why the HSZ framework was never adopted in order to make recommendations for any potential working groups focused on this area in the future.

---

[85] "gTLD Applicant Guidebook," 4 June 2012, https://newgtlds.icann.org/en/applicants/agb

[86] See "GAC Communiqué – Buenos Aires, Argentina," 24 June 2015, https://www.icann.org/news/announcement-2-2015-06-24-en and "GAC Communiqué - Dublin, Ireland," 21 October 2015, https://www.icann.org/news/announcement-2015-10-22-en

[87] See fTLD Registry Services, "Enhanced Security," accessed 11 February 2016, www.ftld.com/enhanced-security/

[88] "About the DNS Seal Project," accessed 12 February 2016, http://dnsseal.wiki/About_the_DNS_Seal_Project

Research Proposal and Models

Significant **empirical puzzles** present themselves with regard to the relationship between the expansion of the DNS through the New gTLD Program and the prevalence of abusive, criminal behavior in the DNS. Important questions remain as to whether the New gTLD Program has contributed to an increase in DNS abuse *that is proportional to the increase in the size of the DNS as a result of the Program*, and—crucially—**whether the safeguards put in place to mitigate it have been effective in achieving their intended objectives**. However, the current body of literature focused on DNS abuse is populated almost exclusively by studies reliant on descriptive statistics and focused probes of specific DNS abuse activities, and suffers from a distinct lack of broadly-focused longitudinal studies employing multivariate, inferential statistical analyses.

In order to arrive at a comprehensive picture of the state of DNS abuse in New gTLDs and to assess the effectiveness of safeguards to mitigate it, this report proposes a **hypothesis-driven** causal analysis utilizing safeguards as intervening variables in a set of hypothetical models built on reasoned assumptions regarding the relationship between the New gTLD Program safeguards and the prevalence of abusive behavior in the DNS. The model focuses on answering a central research question:

> To what extent can the safeguards put in place to mitigate DNS abuse in new gTLDs account for the rate of abusive behavior in the DNS?

Answering this question in a comprehensive, scientifically sound manner necessitates building a testable hypothetical model and segmenting inquiry to focus on legacy and/or new TLDs, and/or the entire DNS space as appropriate. It requires establishing a **baseline measure** as a point of departure in answering the foundational question of whether there has been an increase in DNS abuse as a result of the New gTLD Program that is *proportional to the expansion of the DNS* itself. Once this measure has been established, we can begin to ask **questions focused on rates of abuse in the "pre-safeguard" era compared to the "safeguarded" era of DNS expansion.** This enables researchers to contextualize the potential relationship between the nine safeguards and the current rate of DNS abuse.[89]

---

[89] Note that this approach to compare the rate of abuse in legacy TLDs both currently and during the "pre-New gTLD era" with abuse in new gTLDs was one independently brought up and favored by a number of participants at the teleconference session on measuring DNS abuse and the effectiveness of the nine safeguards. See ICANN Operations and Policy Research, "Reviewing New gTLD Program Safeguards Against DNS Abuse," 28 January 2016, teleconference proceedings, recordings available at https://newgtlds.icann.org/en/reviews/dns-abuse

The models below lend themselves to both qualitative and quantitative testing methods. However, as alluded to above, many of the safeguard measures do not generate quantitative data in the quantities needed to conduct a robust statistical analysis. Two approaches can address this: exploring potential proxy measures for safeguard effectiveness, and employing qualitative methods—e.g. user feedback interviews, focus groups, review of relevant publications—in order to add empirical depth to the wider scope of what quantitative methods are possible in the context of the safeguards.

A Possible Qualitative Framework for Testing the Effectiveness of Safeguards

This proposal and models below represent first steps to inform discussion on the most effective means to test the effectiveness of safeguards to mitigate DNS abuse. It remains to the CCT-RT to decide the scope and method of their inquiry into DNS abuse mitigation efforts.

Research Design: Key Questions and Considerations

An abundance of potential data exists—be they in qualitative and quantitative form—that could potentially be applied to investigate the effectiveness of the nine safeguards to mitigate DNS abuse. However, before deciding on which data to use, a research design to structure the data and achieve the review's objectives must be determined. Any research design must answer the following:[90]

1. Identify the research problem clearly. What is the empirical puzzle we're trying to solve?
2. Review and synthesize previously published literature associated with the problem.
3. Clearly and explicitly specify research questions and/or hypotheses central to the research problem.
4. Effectively describe the data necessary to adequately answer the research questions and/or test the hypotheses, and explain how such data will be obtained.
5. Describe the methods of analysis to be applied to the data in determining whether or not the hypotheses are true or false.

The Q&A below contextualizes these research tasks in terms of the DNS Abuse Review:

1. Identify the research problem clearly. What is the empirical puzzle we're trying to solve?

[90] This has been taken from the University of Southern California's succinct list of research questions at http://libguides.usc.edu/writingguide/researchdesigns (accessed 26 February 2016).

Research problem: It is unclear how effective the safeguards to mitigate DNS abuse in new gTLDs have been.
Empirical puzzle: Some indicators point to reduced amounts of DNS abuse in TLDs in general (legacy and new), while others point to increasing rates in particular TLDs. The extent to which the safeguards to mitigate DNS abuse have played a role in this variation remains unclear.

2. Review and synthesize previously published literature associated with the problem.

   This report is geared toward providing such a review and synthesis.

3. Clearly and explicitly specify research questions and/or hypotheses central to the research problem.

   Research question(s): What explains the variation in the rates of abuse in different TLDs? To what extent have the safeguards put in place to mitigate them been effective?

   Hypothesis examples (see models below for in-depth exploration of defining hypothetical relationships):
   - High-level (to guide overall or significant portion of review):
     - The expansion of the DNS has caused an *increase* in the amount of DNS Abuse that is not proportional to the expansion itself.
   - Low-level (to guide specific portions of inquiry within the review):
     - X safeguard intended to prevent Y form of DNS abuse has been ineffective in its intended aims

   Research questions and hypotheses should also indicate how each term is defined and/or measured. For example, as explored above, how do we measure "effectiveness" of a safeguard?

4. Effectively describe the data necessary to adequately answer the research questions and/or test the hypotheses, and explain how such data will be obtained.

   For example, "effectiveness" of safeguards may be measured qualitatively via interviews with experts and users of the safeguards. The extent to which the New gTLD Program has contributed to DNS Abuse may possibly be measured quantitatively by examining statistical correlations between the number of new domains and a DNS abuse proxy, such as phishing rate.

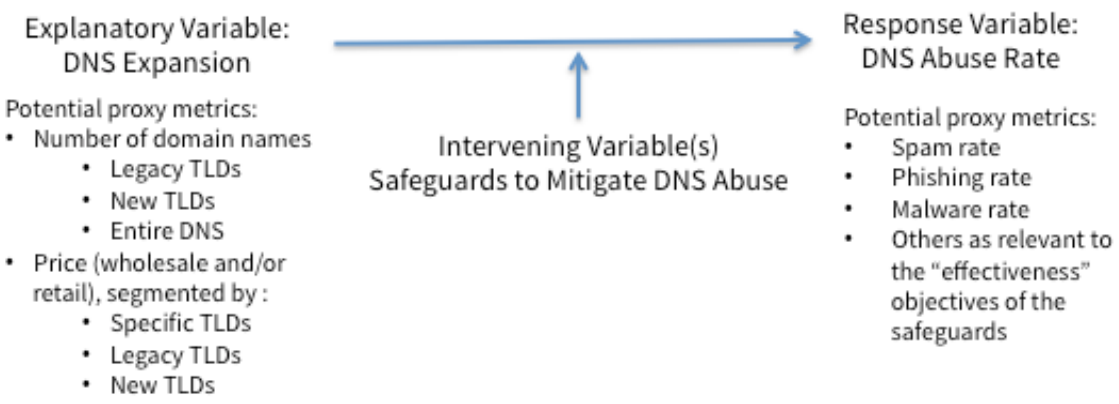
5. Describe the methods of analysis to be applied to the data in determining whether or not the hypotheses are true or false.

To be determined by the work of the CCT-RT, in addition to defining the research questions and hypotheses as explored above.

Causal Models and Hypotheses

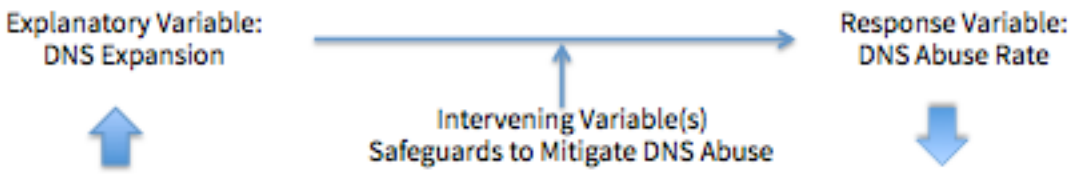
The models below derive from a simple central hypothesis that—theoretically at least—the introduction of safeguards to prevent DNS abuse in new gTLDs should result in a "cleaner" (i.e. fewer malicious activities) DNS space compared to the "legacy" TLD era when such safeguards did not exist.

Base Model



Three testable hypothetical scenarios derive from this base model:

Model 1: The expansion of the DNS has resulted in a proportional *decrease* in DNS abuse
(Effective Safeguard Hypothesis)

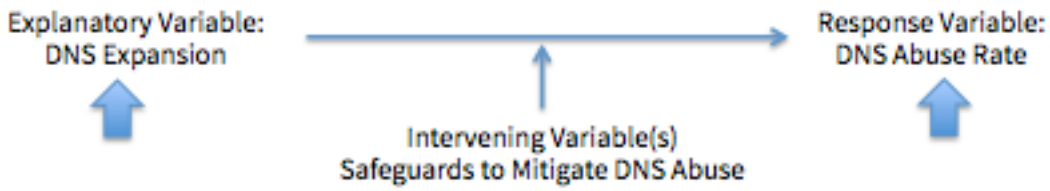


Research Question: To what extent are effective safeguards causal factors explaining the proportional *decrease* in DNS abuse?

Hypothesis 1: The "safeguarded" expansion of the DNS is a causal factor explaining the proportional **decrease** in DNS abuse in new and/or legacy TLDs, and/or the entire DNS (segment analysis by new and/or legacy, and/or entire DNS as appropriate).

Hypothesis 1.1: The safeguards put in place to mitigate DNS abuse have been **effective** in achieving their intended objectives, and are causal factors explaining the proportional decrease in DNS abuse (target individual safeguards for analysis as appropriate).

Model 2: The expansion of the DNS via the New gTLD Program has resulted in a proportional *increase* in DNS abuse
(Ineffective Safeguard Hypothesis)

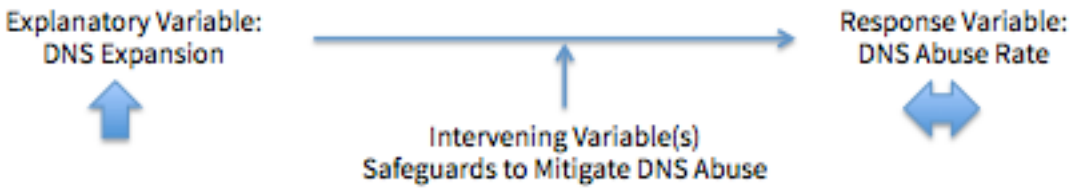


Research Question: To what extent are ineffective safeguards causal factors explaining the proportional *increase* in DNS abuse?

Hypothesis 2: The "safeguarded" expansion of the DNS is a causal factor explaining the proportional **increase** in DNS abuse in new and/or legacy TLDs, and/or the entire DNS (segment analysis by new and/or legacy, and/or entire DNS as appropriate).

Hypothesis 2.1: The safeguards put in place to mitigate DNS abuse have been **ineffective** in achieving their intended objectives (target individual safeguards for analysis as appropriate).

Model 3: The expansion of the DNS has had a *null effect* on DNS abuse
(Ineffective Safeguard Hypothesis)



Research Question: To what extent are ineffective safeguards causal factors explaining the *lack of change* in DNS abuse?

Hypothesis 3: The "safeguarded" expansion of the DNS has had no effect on the proportion of abusive behavior occurring within new and/or legacy TLDs, and/or the

entire DNS (segment analysis by new and/or legacy, and/or entire DNS as appropriate).

Hypothesis 3.1: The safeguards put in place to mitigate DNS abuse have been **ineffective** in achieving their intended objectives of providing a new gTLD space that is "safer" compared to the legacy space (target individual safeguards for analysis as appropriate).

Insofar as the work of the CCT-RT is concerned, this research proposal represents a possible approach to structuring their inquiry into the effectiveness of the nine safeguards to mitigate DNS abuse. Such an approach will likely necessitate hiring outside vendors with statistical and qualitative data collection and analysis expertise to build and conduct the actual study. It remains with the CCT-RT to decide the scope and method of any analysis. If nothing else, this research proposal can serve as a point of departure for discussing other possible approaches.

Conclusion

This report has aimed to provide a preliminary research framework for the CCT-RT to assess the effectiveness of the nine safeguards to mitigate DNS abuse that were developed by security and abuse experts and described in the 2009 New gTLD Program Explanatory Memorandum, "Mitigating Malicious Conduct."[91] In public comments received on this report, five of the nine submitted— from the GAC, DotMusic, IPC, INTA, and the BC—suggested expanding the scope of this report to include examination of additional types of safeguards, especially as they pertain to Rights Protection Mechanisms and associated issues related to copyright/trademark infringement, piracy, and counterfeiting. These issues are in the scope of the CCT-RT's efforts and have been examined in the "Revised Staff Report: Rights Protection Mechanisms Review".[92] However, they are not in scope for the particular purposes of this report, which focuses specifically on the nine safeguards explored above.

At the time of publishing the final version of this report, the CCT-RT is in the process of defining the scope and methodology of their review of New gTLD Program safeguards, including those examined in this report as well as those recommended by the five groups noted above.

---

[91] "Mitigating Malicious Conduct," ICANN, New gTLD Program Explanatory Memorandum, 3 October 2009, https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf

[92] "Rights Protection Mechanisms Review," ICANN, Revised Report, 11 September 2015, http://newgtlds.icann.org/en/reviews/rpm/rpm-review-11sep15-en.pdf

Appendix: Survey of Abuse-Related Activities at ICANN

Project	Scope	Source and Links
Registry Agreement Specification 11	Section 3a: "Registry Operator will include a provision in its Registry-Registrar Agreement that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name." Section 3b: "Registry Operator will periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. Registry Operator will maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. Registry Operator will maintain these reports for the term of the Agreement unless a shorter period is required by law or approved by ICANN, and will provide them to ICANN upon request."	Source: Registry Agreement Link: Registry Agreements Link: FAQs: Specification 11 of the Revised New gTLD Registry Agreement
SSR Review Team Recommendation 11	Recommendation 11: "ICANN should finalize and implement measures of success for new gTLDs and IDN fast track that expressly relate to its SSR-related program objectives, including measurements for the effectiveness of mechanisms to mitigate domain name abuse."	Source: Security, Stability and Resiliency of the DNS Review Team Link: Final Report of the Security, Stability and Resiliency of the DNS Review Team
GAC Advice: ICANN53 and ICANN54	ICANN53 Buenos Aires Communiqué: "The GAC…recommends…that the ICANN community creates a harmonised methodology to assess the number of abusive domain names within the current exercise of assessment of the new gTLD program."	Source: ICANN Governmental Advisory Committee Link: ICANN53 GAC

	ICANN54 Dublin Communiqué: "The GAC advises and urges the Board to…develop and adopt a harmonized methodology for reporting to the ICANN community the levels and persistence of abusive conduct (e.g., malware, botnets, phishing, pharming, piracy, trademark and/or copyright infringement, counterfeiting, fraudulent or deceptive practices and other illegal conduct) that have occurred in the rollout of the new gTLD program."	Communiqué, Buenos Aires Link: ICANN54 GAC Communique, Dublin
SSAC Advisory on Registrant Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle	Recommendation 1: "As part of regular reports, the ICANN Compliance Department should publish data about the security breaches that registrars have reported in accordance with the 2013 Registrar Accreditation Agreement (RAA) paragraph 3.20." Recommendation 2: "A provision similar to 2013 RAA paragraph 3.20 should be incorporated into all future registry contracts, with similar statistics published as per Recommendation 1 above."	Source: Security and Stability Advisory Committee Link: SAC074 Advisory
gTLD Marketplace Health Index	ICANN has developed a set of candidate concepts for community discussion to inform its creation of the gTLD Marketplace Health Index, which focus on (i) robust competition, (ii) consumer trust, and (iii) non-technical stability. These proposed concepts are intended to facilitate community discussion about what it means for the global gTLD marketplace to be "healthy." This community discussion is expected to produce measurable factors to serve as key performance indicators for the gTLD marketplace. A number of the concepts focus on DNS abuse as described herein.	Source: ICANN Staff Link: gTLD Marketplace Health Index Proposal: Call for Comments and Volunteers