GROUP	ACTION NEEDED: Complete your analysis of your reading list assignments. Follow instructions! Refer to http://mm.icann.org/pipermail/cctreview-safeguards/2016-June/000070.html - Indicate whether your article/source is relevant - highlight in green if it is!					
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
DNS Abuse	**Article:** APWG News Center **Volunteer:** Gao	This site collects information on phishing from across the world. It is a repository for all reports generated by the APWG.		The News Center is where APWG posts all summaries and links to the latest releases of their Phishing Trends Reports.	APWG is the global industry, law enforcement, and government coalition focused on unifying the global response to cybercrime through development of data resources, data standards and model response systems and protocols for private and public sectors.	A valuable resource for statistics on Phishing attacks in general. Drew/Gao: this might be a green We have a safeguard on that (Prohibition of abusive activities) and no good data.
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
DNS Abuse	**Article:** APWG Phishing Attacks Trends Reports **Volunteer:** Gao	A repository of all (now) Quarterly reports generated by the APWG.	Phishing incidents are decreasing over time as more safeguards are implemented	Analysis of phishing attacks over each quarter of the year, compared to year, compared to other prior quarters.	Phishing activities fluctuate over time, with varying industries taking it in turns to be the most targeted.	A valuable resource for the latest statistics on Phishing trends and reports. Drew/Gao: this might be a green We have a safeguard on that (Prohibition of abusive activities) and no good data.

	Article & Volunteer	Observations (Review Team's)	Hypothesis (posed by observation)	Research	Findings	Possible recommendations & Champion
DNS Abuse	**Article:** APWG- Global Phishing Survey: Trends and Domain Name Use in 1H2014 **Volunteer:** Gao	- Legacy TLDs and some free ccTLDs are more prone to phishing attacks than new gTLDs. - New gTLDs are either too expensive for phishers to register on or use more safeguards to deter phishing activity	- With the introduction of new gTLDs, there will be increased phishing activity. - The new gTLDs will be more prone to phishing attacks.	Various metrics measured: Phishing Domains per 10,000 Phishing Attacks per 10,000 (is a ratio of number of domain names used for phishing in a TLD to the number of registered domain names in that TLD). The metric "Phishing Attacks per 10,000" is another useful measure of the pervasiveness of phishing in a namespace. It especially highlights what TLDs are predominantly used by phishers who use subdomain services, and where high-volume phishers place multiple phish on one domain	New gTLDs are not any more prone to phishing than legacy TLDs and ccTLDs. ON the contrary, they experienced less targeted phishing in the first half of 2014. - Apple became the world's most-phished brand. (Page 7) - The introduction of new top-level domains did not have an immediate major impact on phishing. (Page 12) - Chinese phishers were responsible for 85% of the domain names that were registered for phishing. (Page 13) - Malicious domain and subdomain registrations continue at historically high levels, largely driven by Chinese phishers. (Page 13, Page 19) - he average uptimes of phishing attacks remain near historic	A useful resource to gauge whether new gTLDs have had more or less safeguards and thus how well they can be "trusted" in theory, by consumers.

					lows, pointing to some success by anti-phishing responders. (Page 8) ● The companies (brands) targeted by phishing targets varied a lot, with many new targets, showing that phishers are scouting for new places to phish. ● Mass hackings of vulnerable shared hosting providers led to 20% of all phishing attacks. (Page 15)	
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
DNS Abuse	**Article:** APWG-Making Waves in the Phisher's Harbor: Exposing the dark side of subdomain registries **Volunteer:** Gao	Subdomains provide an opportunity for phishing attacks because of the relaxed registration information needed to set them up, and the ease with with phishers can access them: they mostly require an email address and the subdomain desired				

	Article & Volunteer	Observations (Review Team's)	Hypothesis (posed by observation)	Research	Findings	Possible recommendations & Champion
DNS Abuse	**Article:** Measuring Perpertrators and Funders of Typosquatting **Volunteer:** Jonathan					
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
DNS Abuse	**Article:** Measuring the Global DNS **Volunteer:** Jonathan	Article discusses potential methodology for developing metrics around DNS health. More appropriate for SSRT and the Health Index effort.				
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
Procedures	**Source:** Compliance related metrics **Volunteer:** Laureen					TBD Need to confer with compliance to determine scope of their data and what would be useful for our efforts
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**

Consumer/End-User Behavior	Article: Consumer awareness summary Volunteer: Carlton & Jamie					
	Article & Volunteer	Observations (Review Team’s)	Hypothesis (posed by observation)	Research	Findings	Possible recommendations & Champion
DNS Abuse Procedures	Article: Notice and takedowns in everyday practice - Online takedowns study Volunteer: Calvin & David					
	Article & Volunteer	Observations (Review Team’s)	Hypothesis (posed by observation)	Research	Findings	Possible recommendations & Champion
DNS Abuse	Article: SAC 045 Invalid Top Level Domain Queries at the Root Level of the Domain Name System					

	Volunteer: Carlton & Carlos					
	Article & Volunteer	Observations (Review Team's)	Hypothesis (posed by observation)	Research	Findings	Possible recommendations & Champion
DNS Abuse	Article: SAC 062 SSAC Advisory Concerning the Mitigation of Name Collision Risk Volunteer: Carlton & Carlos					
	Article & Volunteer	Observations (Review Team's)	Hypothesis (posed by observation)	Research	Findings	Possible recommendations & Champion
DNS Abuse	Article: SAC 066 SSAC Comment Concerning JAS Phase One Report on Mitigating the Risk of DNS Namespace Collisions Volunteer: Carlton & Carlos					

	Article & Volunteer	Observations (Review Team’s)	Hypothesis (posed by observation)	Research	Findings	Possible recommendations & Champion
DNS Abuse	Article: SAC074 SSAC Advisory Registrant on Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle Volunteer: Carlton & Carlos					
	Article & Volunteer	Observations (Review Team’s)	Hypothesis (posed by observation)	Research	Findings	Possible recommendations & Champion
DNS Abuse & Procedures	Article: Knujon March 2016: Internet Limbo Report Volunteer: Fabro	Ad hoc data. Inspiring to discuss, but methodology is weak.				
	Article & Volunteer	Observations (Review Team’s)	Hypothesis (posed by observation)	Research	Findings	Possible recommendations & Champion
N/A	Article: WHOIS Accuracy Reporting System (ARS)					

	Volunteer: Calvin					
	Article & Volunteer	Observations (Review Team's)	Hypothesis (posed by observation)	Research	Findings	Possible recommendations & Champion
DNS Abuse	Article: SSAC Comment on Orphan Glue Records in the Draft Applicant Guidebook Volunteer: Calvin					
	Article & Volunteer	Observations (Review Team's)	Hypothesis (posed by observation)	Research	Findings	Possible recommendations & Champion
DNS Abuse	Article: High-security Zone Top-Level Domain Advocacy Group Volunteer: David					
	Article & Volunteer	Observations (Review Team's)	Hypothesis (posed by observation)	Research	Findings	Possible recommendations & Champion
Impact of Safeguards & PICs	Article: Mitigating the Risk of DNS Namespace Collisions					

	Volunteer: David					
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
DNS Abuse	**Article:** IETF-RFC List **Volunteer:** **Drew**	Still assessing				
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
DNS Abuse	**Article:** The NameSENTRY Abuse Report **Volunteer:** **Carlos**					
	ACTION NEEDED: 1) refine your findings based on instructions http://mm.icann.org/pipermail/cctreview-safeguards/2016-June/000070.html ; 2) highlight in green if relevant source and 3) Send Alice a note to confirm they have completed their review					
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
DNS Abuse	**Article:** Potential for Phishing in Sensitive-String Top-Level Domains **Volunteer:** **Laureen**	New gTLD policies impose more safeguards than legacy gTLDs. Certain practices (safeguards prohibiting domain abuse, restricted	More protective practices may reduce incidence of phishing in new gTLDs. Sensitive string gTLDS have a	Primarily relies on APWG Global Phishing surveys. Also looked at 300 most recent domains listed at Artists Against 419 (aa419.org) a repository of fraud	Article considers what needs to happen for a phishing attempt to succeed and when and how prevention and mitigation can be effective.	Phishing does not appear to be any more or less prevalent proportionally in new gTLDs. Pricing appeared to be a factor for attracting phishing in new xyz gTLD.

		registration policies, pricing) may decrease phishing.	lower incidence of phishing due to restricted registration policies.	sites, particularly advance fee frauds	Practical and easy to understand. Explains technical concepts in plain language. Most phishing takes place on compromised domains (phisher has broken into registrant's web hosting) so registration restrictions (including those for sensitive string domains) don't matter under this scenario. pp. 12-14, 26 Other methods: malicious registrations [84% to chinese targets]; subdomain resellers [registries often provide free services including P/P services] ; and IP addresses. Pp10-11 Phisher can get benefit of "trusted" sensitive domain by simply creating URL	Malicious registrations can be reduced by controlling access to domain registrations via more stringent registration requirements and higher pricing. gTLD operators should have and enforce terms of service and that allow suspension of the domain name for malicious actions, including phishing.

					string that appears to in the sensitive domain. Pp. 19-21 Phishing emails often hide their real destination domain name from user. Pp8-9. Phishing generally small compared to # of domains in the world (mostly concentrated in legacy gTLDs and cc TLDs. pp. 10-11, 19-20 .com contains 41.3% of domains and 58% of phishing domains (2H2014 data set). p.14 Expansion of gTLDs will likely not affect total amount of phishing. Will create new locations for phishing to take place. pp 15-16, 22, 26 New gTLD analysis: 26-29	

					Registration restrictions, pricing strategies (higher prices), and active mitigation deter phishing. Quick takedowns of phishing sites are essential. p.25	
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
N/A	**Article:** Verizon 2016 Data Breach Investigations Report **Volunteer: Laureen**	Data breaches continue to increase and evolve. Not a primary source for our work but likely a good source of data and background for prevalence of data breaches and phishing in particular	Are new gTLDs more or less apt to be involved in the data breaches discussed in this report?	Data set of over 100,000 incidents Many contributors (see p. 71)	Accommodation and Retail industries account for majority of data breaches (an incident that results in unauthorized disclosure of data) p.4 Actors in breaches primarily external p. 7 Primary motive is $$$ pp. 7-8 Phishing (w/attached malware) and point of sale attacks are common infiltration tools p.9 (Phishing focus pp. 17-19; PoS focus pp. 31-34)	Consider how Phishing and DoS attacks relate to consumer trust. If we opt to focus on these issues of domain abuse, the same person can include this report as a resource (perhaps Gao?)

					Denial of Service attacks (DoS) con't to evolve (pp. 56-59) Many different ways that bad actors can compromise credentials to infiltrate (figure 45 pg. 62)	
	Article & Volunteer	Observations (Review Team's)	Hypothesis (posed by observation)	Research	Findings	Possible recommendations & Champion
Procedures	**Source: ICANN Compliance web page** **Volunteer: Laureen**	New gTLDs impose more restrictive policies (in Registry and Registrar agreements).	Do the more restrictive policies for new gTLDs result in fewer complaints than legacy gTLDs? (would need to know whether ICANN Compliance compare complaint rates for legacy vs. new gTLDs?)		On-line resource displaying variety of data maintained by ICANN K Compliance. Data includes yearly reports on notices of breach, suspension, termination, or non-renewal; quarterly and annual reports; and summaries of outreach	Consider meeting with K compliance to ask about available data on new gTLDs.
	Article & Volunteer	Observations (Review Team's)	Hypothesis (posed by observation)	Research	Findings	Possible recommendations & Champion
Procedures	**Article:** ICANN Contract Compliance 2015 Annual Report	New gTLDs impose more restrictive policies (in Registry and Registrar agreements)	Has introduction of new gTLDs increased complaints?	ICANN Contract Compliance Data	Yearly report summarizing ICANN Contract Compliance Activity	WhoIS inaccuracy is the largest complaint category. Consider.

	Volunteer: Laureen	Notes huge increase from 2014 in gTLDs (+400 to +1100) and +1400 accredited registrars to 2100)			Complaint count increased by 20% from prior year (increase in new gTLDs and registrars likely a factor) Chief notes that while ICANN c/n be solution to problems of abuse and illegal activity, they can play a role in partnership with others in the Internet ecosystem. In addition to handling complaints, Compliance performs audits; conducts outreach; and seeks to improve processes. Re: audits, review of potential risk of K'ed parties' non-compliance with various K provisions. Launched initiative to improve knowledge of K compliance which included a video on how they can help	

					w/domain name registration issues and a chart on what is a contract compliance complaint (available in 8 languages) Registrars: Abuse complaints: 438 (1%); WHOIS inaccuracy (+75%); transfer (+14%) Chart p. 8; description p.11 Registry: Abuse contact data (61) (small percentage of 2180 total); Zone file access (+31%); Registry Data Escrow (+21%) Chart p. 8; description p.13 Formal notice activity included notices for publishing email POC for abuse reports;; maintain/publish records re: abuse reports; and publish on website procedure for receipt and	

					tracking of abuse reports (all at approx. +4%)	
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
Procedures	**Article:** ICANN Contract Compliance Dashboard Jan. 2016 **Volunteer: Laureen**	Monthly summary of ICANN Compliance complaint activity.	This report does not distinguish between legacy and new gTLDs (does Compliance have this data?)	Complaints filed with ICANN	For Registrars: top complaint topics involve WHOIS inaccuracy (68.2%) and transfers (20.5%) Abuse complaints relatively low (38 vs. +2000 for WHOIS inaccuracy and +600 for transfer) For Registries: Zone file Access (61.9%) and Registry Data Escrow (12.6%) Only 4 complaints re: Abuse Contact data	
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
Impact of Safeguards & PICs	**Source: GAC Safeguard Advice in Communiques (ICANN 53, ICANN54 Volunteer: Laureen**	Governmental Advisory Committee issues formal written advice after every ICANN meetings. In response to new gTLD program, GAC	Has GAC Safeguard advice enhanced consumer trust; had an impact on abuse?	GAC Communiques	Note: Although GAC issued many items of safeguard advice, ICANN did not accept all advice as given. Beijing advice highlights:	We should add review of PICs for strings corresponding to highly regulated sectors to our data requests.

		issued safeguard advice on a variety of issues			Advice for all gTLDs Reconsider decision to allow singular and plural versions of same string b/c could lead to consumer confusion Require Registry operators to conduct WHOIS Verification and checks Require Registry operators to ensure terms of use for registrants prohibit abusive activity (e.g. malware, botnets, phishing, piracy, infringement, fraud or deceptive activity, counterfeiting) Require Registry Operators to conduct technical analysis to to asses whether domains in its gTLDs are being used to perpetuate security threats (e.g. pharming; phishing malware botnets)	Brainstorm on how to measure impact of GAC safeguard advice. Complicated b/c n/all advice implemented and n/necess. implemented as advised. We should follow up on GAC gathered data on community applications and CPEs LK can champion these issues.

					Require registry operators to ensure a mechanism for making and handling complaints Ensure real and immediate consequences for false WHOIS information and violation of requirement that domains should not be used for illegal purpose (including suspension of domain name) For sensitive/regulated strings: Registry operators to include in acceptable use policy that registrants comply with all applicable laws (including privacy and consumer protection) Registry operators to require registrants that collect sensitive data (financial,	

					health) to implement reasonable security measures Registry Operators to require Registrants to have a single POC to report complaints or abuse. Further Targeted Safeguards for domains associated with market sectors with clear and/or regulated entry requirements (financial, gambling, professional services: environmental, health and fitness, corporate identifiers and charity) Registry operator to verify and validate credentials at time of registration; consult with authorities if in doubt; conduct post registration checks to ensure continued compliance	

					Restricted Registration Policies Registry operator should administer in transparent way; no undue preference to any registrar or registrants For strings representing generic terms, exclusive registry access should serve a public purpose Highlights of 2013 Buenos Aires Communique Consider whether Public Interest Commitments fully implement safeguard advice Recategorize .doctor as a highly regulated string to therefore ascribe these domains exclusively to legitimate medical practitioners (noting strong implications for consumer	

					protection and consumer trust) New Registry OPerators should be aware of importance of protecting children consistent with UN Convention on Rights of the Child Highlights of 2014 Singapore Communique Concerns about outcomes of community applications Reiterates advice that singular and plural of same string could cause consumer harm Poses lengthy list of questions in appendix aimed at whether NGPC has fully implemented GAC safeguard advice (particularly verification/validation requirement; security checks) and	

					concerns about proposed PIC Dispute Resolution Process Highlights of London Communique Asks for briefing on GAC concerns about implementation of safeguard advice re: verification of WHOIS information, verification/validation of credentials for regulated industries, security checks, PICDRP, and discrimination in restricted TLDs Annex includes detailed discussion of where GAC thinks that NGPC has failed to fully implement its advice Highlights of Los Angeles Communique Reiterates concerns with NGPC's failure to implement GAC advice on safeguards	

					related to WHOIS, Security Risks, PICDRP, verification/validation of highly regulated strings, ensuring nondiscriminatory registration policies Con’t concerns about consistency of Community Priority Evaluation process Subsequent Rounds GAC advises that reviews of first round should be completed and finalized before policy for further gTLD rounds is developed. Highlights of 2015 Singapore Communique Regrets NGPC failure to adopt verification/validation requirement for strings associated with highly regulated industries.	

					Reiterates concerns re: length, complexity, and ambiguity of PICDRP. Seeks “fast track” for Law enforcement and gov’t agencies. Highlights of 2015 Buenos Aires Communique Asks NGPC to create a list of commended PICs related to verification/validation of credentials for domains in highly regulated sectors Asks for method to assess number of abusive domain names within assessment of new gTLD program Clarify acceptance or rejection of GAC advice with a straightforward scorecard Highlights of Dublin Communique	

					Reiterates requests for 1) clear scorecard of accepted and rejected safeguard advice; 2) list of commended PICs re: verification/validation of credentials for domains in highly regulated sectors; and 3) harmonized methodology for reporting levels and persistence of abusive conduct (malware, botnets, phishing, piracy, infringement, fraud or deceptive activity, counterfeiting or other illegal activity) within new gTLDs Reiterates concerns about CPEs and assessing public policy related aspects of current gTLD program before launching new rounds Marrakech Communique Highlights Focus on ensuring existing GAC	

					safeguards maintained and improved. Encourages review of PICs for strings corresponding to highly regulated sectors Intends to gather data community applications and CPEs to contribute to CCT review.	
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
Impact of Safeguards & PICs	**Article:** [CZDS-ZFA Passwords Reports] **Volunteer: Jamie**	Monthly reports listing numbers of credentials with access to TLD zone files. TLD zone files contain the list of domain names that are registered and active for a given registry. Every new Registry is required to provide zone data files to approved requestors (e.g. law enforcement agents, IP attorneys,	N/A	Spreadsheet of alphabetized listing of TLDs and number of passwords issued for access to zone files	Number of TLDs in May report with credentialed ZFA users: 993 Top 20 TLDs by number of credentialed ZFA users: guru 1314 works 1312 technology 1311 voyage 1311 training 1309 today 1307 ventures 1307 vacations 1306	Consider whether this data has any intrinsic significance. Data doesn't show what users found in ZF; only that they got permission to look. May be of interest only in conjunction with other data (e.g., level of reported abuse on a TLD). FInally, might be interesting to compare with comparable data for legacy TLDs.

		researchers) upon technical delegation of its gTLD. The process used by many existing Registries is to create and execute a contract for every zone data request. By contrast, the process is streamlined by allowing requestors using the CZDS agree to standardized Terms and Conditions before submitting one or multiple requests, and Registries can simply approve or deny requests with one click. Registries can also save time by appointing ICANN to handle zone data file formatting and transfer (AXFR) instead of using internal resources.			watch 1306 tips 1305 villas 1305 vision 1305 support 1303 solutions 1302 systems 1302 viajes 1301 supplies 1300 tools 1300 supply 1299 solar 1295 Bottom 20: mls 93 xn--w4rs40l 92 pro 85 warman 68 ally 57 shop 45 mlb 36 anquan 35 shouji 35 xihuan 35 yun 35 bnpparibas 16 gdn 16 voting 9 unicom 8 htc 7 xn--8y0a063a 7 shaw 6 xn--mxtq1m 6 xn--5tzm5g 5	

	Article & Volunteer	Observations (Review Team's)	Hypothesis (posed by observation)	Research	Findings	Possible recommendations & Champion
DNS Abuse	**Article:** DNSSEC Deployment Report **Volunteer: Jamie**	Website with graphical and spreadsheet depiction of TLDs that are DNSSEC-signed in the root and that are signed allowing for signing of SLDs. While number of signed TLDs is high, number of signed SLDs remains low.	Contractual requirement on registries to sign TLDs has accelerated deployment of DNSSEC at top level but not at second level	Data set of signed TLDs and SLDs.	87% of TLDs (1160/1327) are signed; only 3% of SLDs are signed; number of signed TLDs on 10/13: <200; number of signed TLDs as of 3 June 2016: 1160	Consider why DNSSEC adoption by registrants is so low and whether higher adoption would have positive impact on trust.
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
DNS Abuse	**Article:** TLD DNSSEC Report	Similar to report above, graphical depiction of DNSSEC deployment and list of signed TLDs as of 4 June 2016. Also lists TLDs that have not been signed (mostly ccTLDs)	Contractual requirement on registries to sign TLDs has accelerated deployment of DNSSEC at top level but not at second level	Data set of signed TLDs	Summary: ● 1327 TLDs in the root zone in total ● 1169 TLDs are signed; ● 1160 TLDs have trust anchors published as DS records in the root zone	Contractual requirement to deploy DNSSEC has had or could have positive impact on consumer trust.
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**

DNS Abuse	**Article::** Deployment Guide: DNSSEC for Internet Service Providers (ISPs) **Volunteer: Jamie**	Published as part of ISOC's Deploy360 Programme, this is a high level piece encouraging ISPs to deploy DNSSEC in their networks with short description of deployment requirements.	ISOC Deploy360 programme has had a positive impact on ISP adoption of DNSSEC	More of a blog than a research program	None; advocacy piece	Research whether third parties like ISOC have had a positive impact on DNSSEC deployment
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
DNS Abuse	**Article:** CloudFlare: How DNSSEC works **Volunteer: Jamie**	Vendor webpage describing how DNSSEC works.	Availability of DNSSEC products and services will increase deployment at second level.	Narrative on how DNSSEC works.	None. Narrative description on DNSSEC.	Research whether availability of vendor products and services have had a positive impact on DNSSEC deployment
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
DNS Abuse	**Article:** DNSSEC- What it is and why is it important? **Volunteer: Jamie**	ICANN staff created webpage describing DNSSEC in Q&A format. Page is archived as document was drafted before root was signed in 2010. Needs to be updated.	Does the availability of information on DNSSEC increase deployment	Q&A on how DNSSEC works. Out of date.	None. Q&A on DNSSEC.	
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**

Procedures	**Article:** [ICANN Registry Agreements] **Volunteer: Carlton**	The Base agreement formally covers in seven (7) articles the intentions and expectations from the delegation and operation of the gTLD, inclusive of the understandings, obligations and mutual covenants of ICANN and the registry operator. It also specifies and frames the process by which amendments to contract, the services and redress of grievances are addressed.	Where lies the responsibilities for safeguards, trust and consumer protections?	ICANN deems itself the capacity to execute and maintain the agreement; Registry Operator warrants it is competent to operate the registry per agreement; will only provide approved services and will follow all the rules and policies specified for provisioning registry services	The narrative is that by virtue of it being subject to public comment, the base agreement is developed by the community. Amendments are purely bilateral, between ICANN and the RySG. The community may comment but has no standing otherwise. The base contract is for ten (10) years, renewable. The burden of technical acceptance of tld - and the extent and possibility of use - is solely that of the registry operator. Services provisioned must be approved and in keeping with consensus policies. Any variation in service must be approved prior to launch or change.	Specification 6 & 7 outlines several safeguards pertinent to consumer trust and consumer confidence and protection; availability, abuse mitigation, name collision; minimum RPMs' Specification 11 frames the PICs for registry Maybe 3rd Party Liability for some actions might actually assist in enforcing the rules.

					Price changes must be notified to ICANN and registrars. [New policy will change that!] Registry fee consists of 2 parts; fixed and transaction level fee. Registry operator must escrow registration data and with approved provider. Registry operator must provide registration data publication services to specifications. Mediation and arbitration are preferred modes for dispute resolution and ICANN’s liability is strictly limited. Some aspects of the contract, notably SLAs, PICs and clauses derived of consensus policies,	

					are ring fenced from both arbitration or mediation. Registry operator is obliged to indemnify and defend ICANN “and its directors, officers, employees, and agents” from all third-party suits, liabilities, costs, damages. Registry is obliged to report specific data every month in a specified format The amendment process is well defined: It can only be initiated by ICANN or the RySG and may not be invoked more than once per year. If deadlocked or stalemated, mediation is invoked by either party. If mediation fails, then arbitration.	

					Assuming agreement, the proposed amendment is published for public comment and all registries notified. The public comment period must last a minimum of 30 days and is extensible. At the end of the public comment period, the working party consider and adjudicate comments. Thereafter a final proposal is provided all registry operators and it is put to the vote of the ICANN board. Assuming approval all around, the proposal[s] become effective 60 days after legal notice is served on all registry operators. [Specifications 6, 7, 10 and 11 refer	

					safeguards and trust matters.]	
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
DNS Abuse	**Article:** Afilias Anti Abuse Policy **Volunteer: Carlton**	Policy is pursuant to the Registry-Registrar Agreement (RRA) and is intended to address all matters that Afilias considers "creates security and stability issues for the registry, registrars and registrants, as well as for users of the Internet in general." Afilias recognizes a veritable smorgasbord of abuse factors, from spam thru fast flux hosting and child pornography to illegal access to computers and networks.	What is their experience in identifying domain abuse and how successful have they been in curbing them by the penalties exacted?	What has been the impact of new gTLDs on domain abuse and could any be traced to the new specs; Specs 6,7, 11.	TBD; Need domain abuse figures reported, action taken and impact.	Consider Afilias list of domain abuse factors as baseline and see what reporting mechanisms there are in their RRA for comparative analysis.
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**

DNS Abuse	**Article:** [.RICH Anti Abuse Policy] **Volunteer: Carlton**	i-REGISTRY is operator of the .rich TLD. The abuse policy is integral to their RRA. They broadly outline how the operator will respond to abuse which covers "general aspects of anti-abuse, acceptable use and rapid takedown and applies to registrars and registrants." It identifies and share as common with Afilias their listed abuse factors but in response will engage in proactive screening, inclusive of WHOIS records, expedited response to law enforcement requests. i-REGISTRY also enumerate the abuse reports by type they will generate.	Does the .rich domain abuse reports show any major comparable variations from that of Afilias and if so, in what specific areas? What is the impact of Spec 6,7, 11, if at all?	The .rich Domain Abuse Report & how the PICs have performed.	TBD	Are new gTLDs experiencing domain abuse at a higher level than legacy TLD? What is the nature of such abuse, if any? Are the Safeguards in Specs 6,7 and 11 of any impact?

	Article & Volunteer	Observations (Review Team's)	Hypothesis (posed by observation)	Research	Findings	Possible recommendations & Champion
Consumer & End User Behaviour	**Article:** ICANN Global Consumer Research Report 2015 **Volunteer: Carlton**	The survey commissioned by ICANN aims to measure consumer awareness, choice and trust in the DNS in general and the new gTLDs in particular. The methodology adopted makes a distinction between end users and registrants; end user experience is reported here. An update is expected soon. Visitation is the measure of awareness.	What is the level of awareness of consumers for the DNS and specifically, the new gTLDS? Is trust and confidence in the DNS impacting end user behaviour?	Sample size 6,144 18+ year-olds in 24 countries on all continents. Survey conducted online.	46 percent reported awareness of at least one new gTLD - 65 percent of those who are aware reporting they have also visited a new gTLD. - .EMAIL and .LINK led in awareness and visitation of new gTLDs. In comparison: - 79% were aware of the legacy domains COM, NET, and ORG especially. - 71% have visited those Domains with an implied purpose and functional associations were the ones most recalled.	Only those already online has opinions! 74% percent are familiar with malware, phishing or stolen credentials. Only 37% were aware of cybersquatting What is the level of awareness of the safeguards or any of the domain anti abuse policies embedded in RRAs
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
DNS Abuse	**Article:** SAC041- **Recommendation to prohibit**	SSAC asserts that DNS redirection and synthesized DNS responses erode the	Harmful and contrary messaging can be introduced in the	Several respected researchers have reported the possibility of	Wildcarding can spoof messages from authorized sources in a conversation. This	"Synthesized responses should not be introduced into top-level domains

	use of redirection and synthesized responses by new TLDs **Volunteer: Carlton**	trust relationships and present opportunities for malicious attacks, thusly undermining the stability and security of the DNS	error resolution process via an iterative resolver with capability to modify a response from an authoritative source	harmful outcomes from so-called wildcarding processes. Coming on a service request by an operator, this was further studied by a [RTS] Evaluation Panel and affirmed.	could be exploited for cause, resulting in instability in the DNS resulting in an erosion of trust and decrease in the security of the system. Existing services, such as email and spam filters are adversely affected and can fail, resulting in economic harm to consumers and users of these systems.	(TLDs) or zones that serve the public, whose contents are primarily delegations and glue, and where delegations cross organizational boundaries over which the operator may have little control or influence."
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
DNS Abuse	**Article:** SSAC Advisory on Registrant Protection - Best Practices for Securing Security and Stability in the Credential Management Lifecycle **Volunteer: Carlton**	Credential management has been tapped as the source of many recent breaches of security. SSAC outlines the best practice for registries and registrars to enhance the security of domain names and the operating support systems pertaining	The security of domain names and the systems that are used to provision them is maintained if certain practices are adopted and adhered to.		Reporting of security breaches at registries and registrars must be instituted and established as part of ICANN compliance framework The notice is contractually obliged and must include detailed description of the type of unauthorized access, how it occurred, the	Determine the status of implementation, if any of SSAC Advisory.

		with improved credential management.			number of registrants affected, and any action taken by Registrar in response Stronger authentication practices must be encouraged in future Registrar - Registry Accreditation Agreements, inclusive of multi-factor authentication ICANN should facilitate training of registries and registrar personnel in the best practices enumerated in collaboration with other interested parties in the Internet ecosystem and with coverage of specific topics.	
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
Consumer & End User	**Article:** Trust in the Internet Survey 2016 by	(Not a primary source for our work). This discussion paper gives a snapshot of	Regardless of the domain, most consumers are not highly confident	Survey was fielded by IDG Research Services from Oct 16 2015 to Oct 22 2015. The results	Last year's survey suggested that there was a strong appetite for verification amid	=> the ball is currently in businesses' court: The new gTLDs provide a significant opportunity for

Behavio r	nccgroup and IDG Research Services **Volunteer: Carlos**	consumers' current attitudes to the new gTLDs. research suggests that online security is an increasingly important part of "brand perception"	with the new names. But there is variation between the trust levels of different names. '.brand' – domains that are brand specific such as .hsbc – and '.bank' engender the most trust.	were collected through an online questionnaire. 5,000 people from the US and 5,000 people from the UK were surveyed.	the flurry of new gTLDs. This year's survey reinforces this view. Over 40% said that they don't feel enough is currently being done to protect their data.	businesses to use them to differentiate and protect their brand – to secure the way their customers see them.
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
DNS Abuse	**Article:** Techniques to Break the Botnet Attack **Volunteer: Carlos**	Technical Paper about Internet Relay Chat (IRC) protocol	A bot is a program that runs on an end-system performing tasks automatically. A botnet is typically seen as a network of bots that use computing resources for a malicious end. The botnet is generally controlled by a single entity called as botmaster. Botnets infect new machines using techniques		Denial of Service (DoS) and then Distributed Denial of Service (DDoS) were implemented in these bots. A survey shows 90.4% of total emails were spam in June 2009. Among all spam, 83.2% was sent through botnets.	DNS Based Detection Technique The bots use DNS queries in order to locate the C&C server hosted by the Dynamic DNS provider. Monitoring the traffic and the DNS makes it pretty easy to detect the botnet and DNS traffic irregularity. This is most famous and easy technique to botnet detection but it will be tough to detect recent advanced botnet through this technique. DNS Failure Graph

			common to most classes of malware, they are distinguished by their use of command and control (C&C) server. The master computer sends instruction to its bots through a command and control (C&C) server, which passes commands from the botmaster to bots, and sends stolen information from bots to their master.			DNS Failures method is the simplest and yet efficient method for detecting the attackers network.DNS failure are rare to occure in any network,but in attackers network the graph of DNS failure rises while generating new malicious websites. This become a way through which the attackers network can be traced. This method studies the DNS faliure graph to detect the attackers network.
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
DNS Abuse	**Article:** **ISTR 20: Internet Security Threat Report** **Volunteer: Carlos**	Symantec´s yearly report	All type of threats. Relevance of DNS specific threats: Section on WEB THREATS (pp.31-45) Poodle,		The total number of sites found with malware has virtually halved since 2013.	

			ShellShock, and Heartbleed			
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
DNS Abuse	**Article:** Secure Domain Foundation, The Cost of Doing Nothing: The Business Case for Proactive Anti-Abuse **Volunteer: Drew**	Survey of registrars about their anti-abuse practices and costs Can potentially use as a primary source to illustrate wide interpretation of 2013 RAA as well as business/legal incentives for anti-abuse efforts connected to consumer safeguards and trust	Whether there is a business case for proactive anti-abuse	Surveyed registrars comprising a cumulative total of 35 million registered domain names.	Registrars differ from one another in how they interpret their responsibilities under 3.18 and 3.7.8 of the RAA 2013. Increased abuse complaints drive up costs for registrars. Proactive anti-abuse, detecting abuse before a complaint has been filed, can save money. Reputation matters for some registrars because of increased competition. Therefore, resources are spent responding to publicized complaints.	Look into how divergent methods of WHOIS verification and reasonable investigation requirements vary for new gTLD registrars. Determine if there is a direct correlation between varying interpretations of safeguards and prevalence of abuse as well as effect on public trust.
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
N/A	**Article:** Amplified DDoS Attacks: The current biggest threat	Brief overview of recent distributed denial of service attacks and interview with experts on how to	DDoS is a big threat that can be mitigated if ISPs adopted BCP38, thereby validating IP address sources	Interview cybersecurity experts	There is no valid reason for network operators to accept traffic from spoofed IP addresses (IP addresses that do not	Determine whether new gTLD operators (registries) have been affected by DDoS attacks

	against the Internet **Volunteer: Drew**	mitigate future attacks Likely not a primary resource for purposes of the CCT Review			match up with the numbers in their source range).	
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
N/A	**Article: DNS Pharming: Someone's poisoned the water hole!** **Volunteer: Drew**	Article written in 2005, providing an overview of DNS cache poisoning Likely not a primary resource for purposes of the CCT Review	Techniques for efficient DNS querying lead to reliance on DNS cache which can be corrupted to route users to malicious IP addresses.		DNS cache poisoning on a local machine or DNS resolver can lead an Internet user to navigate to an attacker's website instead of the website to which the user intended to navigate. This may be done through pharming, by luring a user to click on a link in an email that leads the victim's machine to query the attacker's name server which then overwrites the local DNS cache with false IP addresses for legitimate domain names.	Determine whether there are any DNS cache poisoning issues unique to new gTLDs. Determine whether DNSSEC adopted has mitigated this.
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**

N/A	**Article: WHOIS Accuracy Reporting System (ARS)** **Volunteer: Drew**	Website for the WHOIS Accuracy Reporting System reports New report coming out in June 2016 - could be used as a primary source	Whether WHOIS data of registered domain names used valid syntax and whether information was operationally valid		Phase 2 report indicates that, as of 2015, 97% of domain names were operating under the rules of the 2009 RAA due in part to grandfathering of already-registered domain names or already-accredited registrars. There does not appear to be a significant different in the 2009 RAA-based accuracy of new gTLD WHOIS data over legacy new gTLD data.	Should determine if there is any correlation between WHOIS accuracy and DNS abuse and consumer trust
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
DNS Abuse	**Article: DNS Stability, Security, and Resiliency** **Volunteer: Drew**	Could be used as a primary source Excellent overview of threats to the DNS system but mostly applicable to DNSSEC adoption issues for purposes of the CCT Review				https://www.icann.org/en/system/files/files/dns-symposium-25oct12-en.pdf

	Article & Volunteer	Observations (Review Team's)	Hypothesis (posed by observation)	Research	Findings	Possible recommendations & Champion
DNS Abuse	**Article:** Registration Abuse Policies Working Group Final Report **Volunteer: Drew**	Could be used as source article Analysis of variations in registration abuse policies				Research on registrar abuse policies should be informed by this report
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
N/A	**Article:** SAC 025: SSAC Advisory on Fast Flux Hosting and DNS **Volunteer: Drew**				There are patterns of fast flux hosting related domain names	Is fast flux hosting more or less prevalent in new gTLDs?
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
DNS ABuse	**Article:** Search Engine Poisoning (SEP) **Volunteer: David**	SEP is common practice amongst hackers. The goal is to make use of search engine results to draw users to sites that contain malware.	Are new gTLDs more subject to SEP as the TLD may in itself be a keyword?		The hacker selects URLs taken from domains that rank high in search engine. The bad actor creates a huge number of URLs	Assess whether new gTLDs are more vulnerable to SEP attacks than legacy ones? Assess whether specific new gTLDs being targeted?

		Popular Search Engine results are manipulated or the malicious site may appear as a sponsored link. The popular sites are infected by XXS (Cross Site Scripting) They become intermediaries that redirect unsuspecting users to malicious sites. It is a DNS abuse though not sure how easy to quantify..			containing targeted keywords. The target keywords become associated with these URLs. These are then included in forums, user comments or reviews and leading a server delivering the malware. This is XXS (Cross Site Scripting). The attacker is not taking over the website. The poisoned results get high ranking for the target keywords given the high ranking domains in the first place + large amount of references in these URLs. Significant economic consequences on targeted companies: brand damage, loss of customers, decreased rankings.	What solutions have been offered if any by new gTLD registries? Are search engines "avoiding" certain TLDs? Consider the improvements which can be made by search engines to return more sanitized references to consumers.
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
DNS Abuse	**Article:** Spoofing Attack : IP, DNS & ARP	Spoofing attacks are when a malicious party impersonates another device or	Are new gTLDs any more subject to Spoofing		3 of the most common types of Spoofing attacks are :	Consider the vulnerability of new gTLDs regarding Spoofing attacks and

	Volunteer: David	user on a network in order to launch attacks (malware and viruses) It is a DNS abuse though not sure how easy to quantify..	attacks than legacy gTLDs? Can a user trust the domain name has not had its underlying DNS spoofed? Internet Users want to be assured that when they type in a certain domain name that they go to the right domain name and that the DNS has not been hijacked.		- Via IP - Via ARP - Via DNS DNS Servers Spoofing attacks are executed by modifying the DNS server in order to reroute a specific domain name to a different IP address	the impact on companies and on consumers. Which new gTLD registries are offering additional protection and if so how? If so to what extent successful?
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
DNS Abuse & Safeguards & PICS	**Article:** fTLD Enhanced Security **Volunteer: David**	fTLD Registry Services offer for .bank and .insurance enhanced trust Should such enhanced trust, it it works, not be extended across all new gTLDs?	Are the security requirements listed by fTLD enough to limit DNS abuse? Would it be feasible to oblige all (which?) Registries to ensure a higher level of security?	fTLD Registry Services, LLC provides a detailed list of Security Requirements. Consider these and other TLDs that may provide (eg .TRUST)	fTLD Registry Services, LLC offers solution to protect Domain Names and the servers associated against different types of attack including spoofing, phishing and other malicious activities. p.2	Study if it is feasible to implement mandatory higher security requirements to prevent more DNS abuse? Identify and review other new gTLD registries that have put in place enhanced security.

						Consider the tenability of a position of prohibiting Proxy/Privacy Registration Services. Consider the recommendations of the WHOIS Review Team.
	Article & Volunteer	**Observations (Review Team’s)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
Safeguards & PICs	**Article :** Frequently Asked Questions: Name Collision Occurrence Management Framework for Registries **Volunteer: David**	This occurs when a TLD is being used in an internal network. A query for that internal TLD could end up in the public DNS	Did the Name Collision Occurrence Management Framework work? What examples can be identified showing name collisions were avoided?	Review Report on effectiveness from ICANN? Review reports on effectiveness of not or other comments from Registries	No findings from the ICANN FAQs, need to assess usefulness from objective sources.	Identify any ICANN or Registry reports on effectiveness of the Framework and issues avoided as well as what could be improved in the future.
	Article & Volunteer	**Observations (Review Team’s)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
DNS Abuse	**Article:** The Curse of the URL Shorteners: How Safe Are They?	URL Shortening services like bit.ly Google and Microsoft are popular.	identify the effectiveness of security measures put in place by the various URL shortening services	we attempt to create shortened URLs to create a shortened link to any infected domain(stage 1) or malicious full URL	This limited experiment shows that URL shortening services have a long way to go before Internet users can trust them to deliver	URL shortening services Are a threat. They can improve and provide a safer web experience for their users. Can we measure how well they are doing?

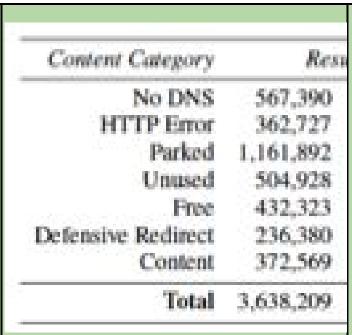
	Volunteer: Fabro Stiebel	Credible sources, like ISC SANS, show that URL shortening services, when compromised, can provide a mechanism for malicious hackers to infect unsuspecting visitors. Criminals use these services to bypass Google's Safe Browsing service, which is used by popular browsers. URL shortening services have partnered with security companies to identify malicious URLs and websites. Some of them even use the SURBL blacklists to identify if someone has tried to link to a malicious website.	Do URL shortening services have any kind of security measures in place? How effective are these security measures?	(stage 2). Data, feb/2010	safe links. About half of the most popular URL shortening services seem to be somewhat effective at blocking access to well known malicious URLs that can be found on blacklists. It seems that popular services like bit.ly, which do try to use blacklists in order to prevent malicious hackers from using their services and pointing to bad websites, can still be easily fooled by chaining together shortened URLs created by another service.	Note: research was from 2010. We probably would need to repeat the test to consider the results valid,
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**

DNS Abuse	**Article:** Symantec Intelligence Report November 2015 **Volunteer: Fabro**	Symantec report on Targeted Attacks & Phishing, Vulnerabilities, Malware, Mobile & Social Media, and Spam Ps: read with https://www.symantec.com/security-center/threat-report	None. It is a descriptive analysis of evolution of Internet threats, with no mention to gTLDs	comprehensive source of Internet, which is made up of more than 57.6 million attack sensors and records in over 157 countries	Public Administration was the most targeted sector Organizations with 251-500 employees were most likely to be targeted by malicious email In terms of targeted attacks in general, the Finance, Insurance, & Real Estate sector was the most targeted	Probably, the most targeted gTLD threats are public administration, large organizations, finance, insurance and real state.
	Article & Volunteer	**Observations (Review Team’s)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
DNS Abuse	**Article:** Redirecting DNS for Ads and Profit **Volunteer: Fabro Steibel**	Error traffic monetization solutions leverage the context provided by ISP customer traffic in order to rewrite protocol error messages to valid responses, redirecting users toWeb servers that show advertisements or search results hopefully of interest to the user.	We also observe a more aggressive form of DNSdriven traffic manipulation, search-engine proxying.	analysis of the redirection pages collected between Jan/2010 and May/11, the location and content of the ad servers, and the marketing material provided by the companies involved.	One monetization vendor reroutes all user search queries to Bing, Yahoo, and (sometimes) Google via proxy servers controlled or rovided by Paxfire. profits of 1–3 USD per customer per year Most monetization occurs in Italy (40%), the US (33%), Brazil (33%),	It suggest that ICANN wants to fight redirecting DNS. There , is a possibility of end user threats in redirecting DNS, that is not document in the article. However, considering that up to 1/3 of traffic is redirected In some major countries, there is a possible urge to tackle the issue. Note: this is not a gTLD particular

		Security researchers have exploited cross-site scripting vulnerabilities in two providers’ ad servers to demonstrate fairly sophisticated phishing and cookie theft attacks			Argentina (27%), Germany (25%), and Austria (20%). The UK (18%), Canada (15%), and Spain (12%) occupy the medium range. ISPs in Australia, Belgium, Finland, France, Israel, Lithuania, New Zealand, Norway, Poland, Russia, Sweden, and Switzerland do not commonly use DNS error monetization: these countries have wildcarding adoption rates below 10%.	issue, it refers to all web traffic

	Article & Volunteer	Observations (Review Team’s)	Hypothesis (posed by observation)	Research	Findings	Possible recommendations & Champion
N/A (Competition related)	**Article:** From .academy to .zone: An Analysis of the New TLD Land Rush **Volunteer: Fabro**	new TLDs have resulted in a burst of defensive registrations as companies aggressively defend their trademarks to avoid consumer confusion.	This paper analyzes the types of domain registrations in the new TLDs to determine registrant behavior in the brave new world of naming abundance. We also examine	We gather DNS, Web, and WHOIS data for each new domain, and combine this with cost structure data from ICANN, the registries, and domain registrars to	We find that only 15% of domains in the new TLDs show characteristics consistent with primary registrations, while the rest are promotional, speculative,	The paper concludes that the new gTLDs have yet to provide value to the Internet community in the same way as legacy TLDs.

		Data from latest monthly registry reports on January 31, 2015, which altogether totals 502 new TLDs. We have focused our analysis on why registrants spend money on domains in the new TLD program. We differentiate public and private TLDs by checking public information about the start of general availability we focus on domains that reached general availability (GA) before our February 3, 2015 We gathered pricing data for domains in the new gTLDs from a wide range of registrars We also compare new domain registrations	the cost structures and monetization models for the new TLDs to identify which registries are profitable.	estimate the total cost of the new TLD program	or defensive in nature; indeed, 16% of domains with NS records do not even resolve yet, and 32% are parked. Our financial analysis suggests only half of the registries have earned enough to cover their application fees, and 10% of current registries likely never will solely from registration revenue. 351,457 xyz domains (46% of xyz) remain unused and display a standard Network Solutions registration page when visited in a Web browser. Overall, the introduction of the new TLDs had only minimal impact in the rate of registration of the old TLDs	

		with URIBL, a publicly available domain blacklist, to see how the blacklist rate compares between old and new TLDs			 Content Category Resu No DNS 567,390 HTTP Error 362,727 Parked 1,161,892 Unused 504,928 Free 432,323 Defensive Redirect 236,380 Content 372,569 Total 3,638,209 Registrants purchase domain names from a registrar and pay a yearly fee to keep them, yet a large fraction of domains in the new gTLDs do not even resolve.	
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
DNS Abuse	**Article: Best Practices to Address Online and Mobile Threats** **Volunteer: Fabro**	This report provides readers with a plain language description of the threats facing businesses, network providers and consumers in the online and mobile threat environment, and suggest best practices for industry and governments to	This is a descriptive study, with general best practices	none	Domain name registries in both the generic Top Level Domain (gTLD) and country code Top Level Domain (ccTLD) spaces, as well as the registrars they do business with, should implement and closely oversee 'Know Your Customer' programs to prevent abuse of	They suggest registrars to implement accreditation programs

		address these threats Malware and Botnets, Phishing and Social Engineering, Internet Protocol and Domain Name System Exploits, Mobile, VoIP, and Telephony Threats, Hosting & Cloud			domain assignment. That will allow them to determine if and when they should avoid conducting business with a registry, a registrar, a reseller or a privacy/proxy service provider. For privacy/proxy services, there is an urgent need for accreditation programs to be implemented and enforced. This will clarify the rules and processes for handling requests to relay, pass communications to the underlying customer, and reveal, disclosing the customer’s identity. This applies to all privacy and proxy services, regardless of whether they operate in the gTLD space or the ccTLD space and regardless of whether they are owned, managed or	

					operated by a registry or a registrar.	
	Article & Volunteer	**Observations (Review Team's)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
DNS Abuse	**Article: A Profitless Endeavor: Phishing as Tragedy of the Commons** **Volunteer: Gao**	The Articles discusses that phishing as a pointless endeavour. It considers a few studies done on phishing by various methodologies and researchers, and the fact that each of these comes up varying results.	The Article hypothesises that the more effort phishers exert on their *Activity*, the less resources are available to all of them collectively. Therefore Phishing is pointless for all of them anyway. Another hypothesis is that the phishers make as much or as little as they would have made elsewhere, i.e. they only make the Opportunity Cost of another occupation, for all that risk they take.	Microsoft Research	Phishing is a classic example of **tragedy of the commons,** where there is open access to a resource that has limited ability to regenerate. Since each phisher independently seeks to maximize his return, the resource is over-grazed and yields far less than it is capable of. The situation stabilizes only when the average phisher is making only as much as he gives up in opportunity cost. Pg 1. Phishing is therefore a low skill, low reward business. The easier phishing gets, the worse the economic picture for phishers. As **more** phishers put **more** effort into this	Phishing is not only (or perhaps even mainly) a problem of how much money has been stolen or how much phishers are making. The main issue **is the reality the erosion of trust in email and web commerce is more significant than the lost dollars.**

					endeavor, the total revenue available for them falls rather than rises, as more awareness is raised among victims, and victims warn would-be victims. However, phishers do not stop. This can be likened to those with emotional ties to the profession, gambling tendencies, or they just simply do not have enough information. The article challenges what is commonly accepted views about Phishing: (a) Far from being an easy money proposition we claim that phishing is a low skill, low reward business, where the average phisher makes about as much as if he did something	

					legal with his time. (b) The absence of data documenting large phishing gains suggests that this view has merit. (c) It is difficult to obtain good enough data or estimates, and even the widely cited victim surveys are exaggerations of the truth and more biased than is generally realized.	

	Article & Volunteer	**Observations (Review Team’s)**	**Hypothesis (posed by observation)**	**Research**	**Findings**	**Possible recommendations & Champion**
DNS Abuse	**Article:** What is SpyWare? **Volunteer: Gao**	The article describes what SpyWare is and how it affects consumers.			- Spyware generally refers to as software that is designed to “spy on” or gather data from a computer or other devices and forward it to a third party without the consent or	The best way to control spyware is by preventing it from getting on your computer in the first place, but not downloading programs and never clicking on

					knowledge of the user. ● This often means collecting confidential data such as passwords, PINs and credit card numbers, monitoring keyword strokes, tracking browsing habits and harvesting email addresses. ● Spyware activities also affect network performance, slowing down the system and affecting the whole business process. ● Generally classified into 4main categories: Trojans, adware, tracking cookies and system monitors. ● How spyware sneaks into a user’s computer: ● This software normally gets onto a computer by pegging itself onto some other program that the user intentionally	email attachments isn't always an option. Sometimes, even a trusted website can become compromised and infect your computer — even if you've done nothing wrong. internet security solutions with reliable antivirus detection capabilities and proactive protection can help. If your computer is already infected, many security providers offer spyware removal utilities to assist in identifying and removing spyware. There are a number of free antivirus solutions available, but it is recommended that users use good antivirus software with features such as virtual encrypted keyboard for entering in financial information or a

					downloads and installs. Sometimes this is done completely discreetly, but other times the desired software will include information in the license agreement describing the spyware — without using that term — and forcing the user to agree to install it in order to install the desired program. ● Spyware can also enter a computer when the user visits a compromised website or opens a malicious attachment in an email. ●	strong anti-spam filter and cloud-based detection system, which help reduce the risk. The choice of a reliable ISP is also key.. Spyware, and its associated malicious programs like malware and viruses, will always be a danger as long as users log onto an Internet connected device. Protecting finances and identity needs to be a top priority, and actions taken towards it at all times.
DNS Abuse - Safeguards & PICs	**Article:** About the DNS Seal Project	Project seems stale (last mention in 2011) Wiki last updated in Aug 2014 no google	An industry Led Project for self regulation would lead to more consumer trust.	None.	Two Goals: - To spread awareness in the broader Internet community about the different	Not Useful to use.

	Volunteer: Calvin	mention outside of it's own wiki.			types of behavior that affect both the DNS as a whole and individual users' online experiences - To publicly recognize actors within the DNS industry that adhere to industry best practices in order to promote responsibility, self-regulation, and a proactive approach to stopping DNS abuse	Maybe a recommendation we want to make, to increase Consumer Trust?
N/A	**Article WHOIS Primer** **Volunteer: Calvin**	Succinct and eloquent exposition of WHOIS	None	Recommended reading	Recommended reading for those looking to understand WHOIS better	
DNS Abuse	**Article: SSAC Advisory on DDoS Attacks Leveraging DNS Infrastructure** **Volunteer: Calvin**	Advisory postdates Applicant Guide Book and nGTLD program	A standard set of security implementations by Authoritative Name Server operators would make us safer.	Various papers citing DDOS attacks etc`	Concrete recommendations: 1. ICANN should help facilitate an Internet-wide community effort to reduce the number of open resolvers and networks that allow network spoofing. This effort should involve measurement efforts and outreach.	

					2. All network operators should take immediate steps to prevent network address spoofing. 3. Recursive DNS server operators should take immediate steps to secure open recursive DNS servers. 4. Authoritative DNS server operators should support efforts to investigate authoritative response rate limiting. 5. DNS server operators should put in place operational processes to ensure that their DNS software is regularly updated and communicate with their software vendors to keep abreast of the latest developments. 6. Manufacturers and/or configurators of	

					customer premise networking equipment, including home networking equipment, should take immediate steps to secure these devices and ensure that they are field upgradable when new software is available to fix security vulnerabilities, and aggressively replace the installed base of non-upgradeable devices with upgradeable devices.	
DNS Abuse	**Article:** SSAC Advisory on DDoS Attacks Leveraging DNS Infrastructure **Volunteer:** Calvin	Advisory issued post new GTLD program. Various recommendations are issued with regards to Internet infrastructure operators, parts of it pertaining to nGTLD operators.	What steps could be taken by nGTLD operators to enhance security.	Various papers, studies and RFC's are referenced.	1: ICANN should help facilitate an Internet-wide community effort to reduce the number of open resolvers and networks that allow network spoofing. 2: All types of network operators should take immediate steps to prevent network address spoofing. 3: Recursive DNS server operators	In as much as findings 2, 4, 5 apply to nGTLD registry operators, we should maybe re-interate that these steps should be carried out by ICANN contracted parties, specifically Registry and Registrar operators.

					should take immediate steps to secure open recursive DNS servers. 4: Authoritative DNS server operators should investigate deploying authoritative response rate limiting. 5: DNS operators should put in place operational processes to ensure that their DNS software is regularly updated and communicate with their software vendors to keep abreast of latest developments. 6: Manufacturers and/or configurators of customer premise networking equipment, including home networking equipment, should take immediate steps to secure these devices and ensure that they are field upgradable	

					when new software is available to fix security vulnerabilities, and aggressively replacing the installed base of non-upgradeable devices with upgradeable devices.	
DNS Abuse	**Article: SSAC Advisory on DDoS Attacks Leveraging DNS Infrastructure** **Volunteer:** Calvin	Advisory issued post new GTLD program. Various recommendations are issued with regards to Internet infrastructure operators, parts of it pertaining to nGTLD operators.	What steps could be taken by nGTLD operators to enhance security.	Various papers, studies and RFC's are referenced.	1: ICANN should help facilitate an Internet-wide community effort to reduce the number of open resolvers and networks that allow network spoofing. 2: All types of network operators should take immediate steps to prevent network address spoofing. 3: Recursive DNS server operators should take immediate steps to secure open recursive DNS servers.	In as much as findings 2, 4, 5 apply to nGTLD registry operators, we should maybe re-interate that these steps should be carried out by ICANN contracted parties, specifically Registry and Registrar operators.

					4: Authoritative DNS server operators should investigate deploying authoritative response rate limiting. 5: DNS operators should put in place operational processes to ensure that their DNS software is regularly updated and communicate with their software vendors to keep abreast of latest developments. 6: Manufacturers and/or configurators of customer premise networking equipment, including home networking equipment, should take immediate steps to secure these devices and ensure that they are field upgradable when new software is available to fix security vulnerabilities, and aggressively	

					replacing the installed base of non-upgradeable devices with upgradeable devices.	