新 gTLD 项目中防止 DNS 滥用的保护措施

ICANN 运营和政策研究 | 2016 年 3 月

目录

简介

根据 ICANN《义务确认书》(AoC) 第 9.3 节中关于促进域名系统 (DNS) 中竞争、消费者选择和消费者信任的要求，本报告旨在辅助竞争、消费者选择和信任审核小组 (CCT-RT) 开展工作。辅助的方式如下：

- 提供自 2012 年 1 月份新 gTLD 项目推出以来 DNS 滥用情况的综述
- 针对为缓和新 gTLD 中 DNS 滥用的情况而提出的九项保护措施，讨论衡量其有效性的选项
- 提出一个研究模型，帮助评估这九项保护措施对缓和新 gTLD 中 DNS 滥用情况的有效性

AoC 中陈述：

> ICANN 将组织一次审核工作，评估 gTLD 的…扩张对竞争、消费者信任和选择的促进程度如何，并审视…**在…扩张过程中所采用的缓和保护措施**的有效性…[着重强调]。审核将由社群成员中的志愿者来执行，并会组建审核小组且公布组建情况以征询公众意见…最后产生的审核建议将提供给董事会，并予以公布以征询公众意见。董事会将在收到建议后六个月内采取行动。

在为潜在 DNS 扩张进行准备的过程中，ICANN 向其专家选区征求了意见，以考察在扩张后的 DNS 中滥用、恶意及犯罪活动增加的可能性，并就如何通过一系列**保护措施先发制人地缓和**这些活动提出建议。[1]为确定缓和潜在滥用行为的一系列步骤，ICANN 首先向多个组织和领域的专家 — 包括反网络钓鱼工作组 (APWG)、注册管理机构互联网安全小组 (RISG)、安全与稳定咨询委员会 (SSAC)、计算机应急响应小组 (CERT) 和来自银行、金融、互联网安全业界的人士 — 提出了四个问题。这四个问题分别是：

1) 如何确保不会让不良行为者来运营注册管理机构？
2) 如何确保注册管理机构信息的完整性和实用性？
3) 如何确保更集中地打击已经确定的滥用行为？
4) 如何为本身容易引发恶意行为的 TLD 提供一个增强的控制框架？

[1]《恶意行为的缓和措施》，ICANN 新 gTLD 项目解释性备忘录，2009 年 10 月 3 日，https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf

在经过广泛协商后，专家组针对上述各方面的问题提出了以下**建议**：

问题	建议
1) 如何确保不会让不良行为者来运营注册管理机构？	1) **审查注册管理运行机构。**通过背景调查降低潜在注册管理运行机构曾是犯罪、恶意和/或失信行为参与方的风险。
2) 如何确保注册管理机构信息的完整性和实用性？	2) **要求进行域名系统安全扩展 (DNSSEC) 部署。**所有新注册管理机构都必须达到这一要求，从而最大程度地降低 DNS 记录造假的可能性。 3) **禁止使用“通配符”**，以便防止可导致到达恶意站点的 DNS 重定向和合成 DNS 响应。 4) **鼓励移除“孤立粘合”记录**，从而最大程度地减少对这些先前已从注册管理机构记录中删除的域残留信息的利用机会。作为 TLD 域文件中带有“避风港”性质的域名服务器条目，它们可能会被恶意行为者所利用。
3) 如何确保更集中地打击已经确定的滥用行为？	5) **要求提供“增强型”WHOIS 记录**，鼓励保持 WHOIS 数据的可用性和完整性。 6) **集中化域文件访问**，创建一个当在各个 TLD 域内新建了域时，能够更高效获取新域更新的方式。 7) **记录注册管理机构和注册服务机构级别的滥用问题联系人和政策**，提供单一联系人来解决滥用投诉。 8) **提供注册管理机构加急安全请求流程**，解决需要注册管理机构立即行动以及 ICANN 加速响应的安全威胁。
4) 如何为本身容易引发恶意行为的 TLD 提供一个增强的控制框架？	9) **创建一个高安全区域验证项目框架草案**，制定一套标准，通过加强运营和安全控制来保障对更易成为恶意行为者目标的 TLD — 例如银行和医药 TLD 等的信任。

衡量这些保护措施的有效性是 CCT-RT 工作的中心目标。为帮助开展这一工作，本报告将深入剖析其中每一项保护措施，提出衡量其有效性的潜在手段，并提出一个严谨、全面地分析其有效性的研究模型。请注意，本报告旨在作为 CCT-RT 的*辅助工具*。它旨在提供*可能的方法*，并激发组内对在新 gTLD 项目背景下，如何最好地开展对 DNS 滥用问题及其缓和保护措施的研究这一问题的讨论。

DNS 滥用：关键术语

“DNS 滥用”涵盖多种多样的活动。尽管对于该词没有一个举世公认的定义，但有一些定义性词语却得到广泛认可，包括“网络犯罪”、“骇客袭击”，以及 ICANN 曾经用过的“恶意行为”等。来自罗马大学和全球网络安全中心的研究人员将这些对 DNS 的威胁分为三类，即：数据损坏、拒绝服务和隐私。[2]

本报告中使用“DNS 滥用”一词，指代积极利用 DNS 和/或域名注册程序进行的蓄意欺骗、纵容或未经允许的活动。这一工作定义是建立在观察哪些活动在文献中常常被当作“恶意”或“滥用”活动来探讨的基础上，旨在为 CCT-RT 提供一个出发点，使他们能在工作中进一步优化自己对 DNS 滥用的定义。在下文探讨的活动中，有些属于“缺乏诚信”类的商业实践 — 但未必是非法的，还有的活动纯属欺诈，在全世界大多数司法辖区可能都是非法的。每种滥用活动（如下所述）在多大程度上符合此定义，从而可以从缓和新 gTLD 项目中 DNS 滥用问题的九项保护措施的角度出发来进行分析，这一问题仍有待于 CCT-RT 考虑。目标是提供一个有效的定义结构，来界定对哪些活动理应包含在其工作中的更多讨论。

DNS 滥用：伎俩和工具

恶意行为者通常会采用下列途径来实施其计划：[3]

- **被入侵域**：在此类域中，恶意行为者闯入了注册人的 Web 托管服务。
- **恶意注册**：恶意行为者为达到从事 DNS 滥用活动的明确目的而注册的域。

---

[2] Casalicchio、Caselli 和 Coletta，“Measuring the Global Domain Name System”（衡量全球域名系统），《IEEE Network》第 27 卷第 1 期（2013 年），第 25-31 页。DOI：10.1109/MNET.2013.6423188

[3] 注意，列表中前两个途径是恶意行为者采用的主要途径。参见 Illumintel 为 ICANN 董事会新 gTLD 项目委员会开展的“Potential for Phishing in Sensitive-String Top-Level Domains”（在敏感字符串顶级域中实施网络钓鱼的可能性）研究，2015 年 5 月 21 日，https://www.icann.org/resources/pages/new-gtld-program-committee-2014-03-21-en

- **子域中间商**：允许人们在服务提供商所拥有的二级域下的第三级注册的服务 — 其中有许多是免费服务，并提供 WHOIS 服务以外的匿名注册。这些中间商通常不会保留除用户帐户名以外的任何注册资料或联系人资料。[4]
- **IP 地址**：网络钓鱼攻击有时会使用网址中的 IP 地址而不是域名。
- **短网址**：一种压缩冗长域地址的技术，可能被恶意行为者用来混淆域名，将不知情的用户重定向到恶意站点。[5]

尽管 DNS 滥用的形式多种多样，但其典型目标在于散布**恶意软件**，以中断计算机运行、收集敏感信息，或者获取对私人计算机系统的访问权。[6]恶意软件自身可执行一系列有害活动，且形式多种多样。最常分发的程序包括：

- **病毒**：此类恶意程序执行一系列不必要的活动，包括创建、移动和/或擦除文件，和/或消耗计算机内存，致使计算机无法正常运行。它们通常会自我复制，并通过被感染的电子邮件扩散到多个网络。例如“蠕虫”和“木马”。[7]
- **间谍软件**：此类恶意软件可捕获诸如用户名、密码、信用卡资料、上网习惯和电子邮件等信息。[8]

恶意软件常通过**僵尸程序**分发，这些自动化程序经编码后可连续运行，执行恶意或滥用的功能。[9]**僵尸网络**是指这些僵尸程序所组成的网络，它利用被感染的计算机来散布恶意软件。[10]而被感染的用户往往不知道他们的设备正被用于此类目的。

---

[4] 反网络钓鱼工作组，“Making Waves in the Phisher’s Safest Harbor:Exposing the Dark Side of Subdomain Registries”（在网络钓鱼者的避风港掀起波澜：揭露子域注册管理机构的黑幕），2008 年 11 月，http://docs.apwg.org/reports/APWG_Advisory_on_Subdomain_Registries.pdf

[5] 参见 StopTheHacker.com，“The Curse of the URL Shorteners:How Safe Are They?”（短网址的诅咒：它们到底有多安全？），访问于 2016 年 2 月 26 日，https://www.stopthehacker.com/2010/02/19/analyzing-url-shorteners/

[6] “竞争、消费者信任和选择实施建议小组 (IAG-CCT)：CCT 审核关于度量指标的最终建议”，2014 年 9 月 26 日，https://newgtlds.icann.org/en/reviews/cct/iag-metrics-final-recs-26sep14-en.pdf

[7] 卡巴斯基实验室，“What is a Computer Virus or a Computer Worm?”（什么是计算机病毒或计算机蠕虫？），访问于 2016 年 2 月 26 日，http://www.kaspersky.com/internet-security-center/threats/viruses-worms

[8] 卡巴斯基实验室，“What is Spyware?”（什么是间谍软件？），访问于 2016 年 2 月 26 日，http://usa.kaspersky.com/internet-security-center/threats/spyware#.VtCsAJMrJTY

[9] 僵尸程序通常并非恶意，并会执行若干正当功能。但是本报告中仅指其恶意形式。请参见 Gabada、Usman 和 Sharma，“Techniques to Break the Botnet Attack”（打破僵尸网络攻击的技术），International Journal for Research in Emerging Science and Technology 第 2 卷第 1 期（2015 年 3 月），http://ijrest.net/downloads/volume-2/special-issue-1/pid-m15ug638.pdf

注册滥用政策工作组

2010 年，GNSO 的注册滥用政策工作组 (RAPWG) 撰写了一份报告，探讨了《注册管理机构-注册服务机构协议》中关于滥用的条款。在报告中，工作组对“滥用”下了一个统一定义，即：

> 滥用是一种：a) 导致实际和实质损害的行为，或可实质预见此类损害的行为；以及 b) 非法或不正当行为，或者被认为以其他形式违背所述正当目的的意图和企图（若此类目的已公开）的行为。”[11]

他们进一步区分了“**注册**”滥用和“**使用**”滥用，前者是指域名注册期间出现的问题，后者是指注册后如何使用这些域名。它们的定义框架如下：

> 注册问题涉及注册服务机构和注册管理机构开展的与域名相关的重要活动。这些活动一般包括（但不限于）注册域名的分配，注册 (WHOIS) 信息的维护和访问，域名的转让、删除和重新分配以及下文详细说明的相似方面。这些活动一般都属于 GNSO 政策制定的范畴。这些活动中有许多已明确列在注册协议中，但还是以共识性政策为准，现有的共识性政策需针对此类问题作出规定。

工作组将以下活动作为注册滥用的潜在形式进行了讨论：

- **域名抢注** — 通过非诚信方式故意注册和使用非相关实体的注册品牌或注册商标作为域名，通常是为了牟利（通常是通过按点击付费的广告牟利，但并非仅仅如此）。
- **域名抢先注册** — 某方获取互联网用户注册某个域名的偏好等内部信息，并趁机抢先注册该域名。
- **牢骚网站** — 抱怨某公司或某实体的产品或服务的网站，并且在域名中使用了该公司的商标（例如 companysucks.商标示例）。工作组内部表达了对这类网站可能会侵犯商标所有人权益的担忧。但工作组同时也指出，在很多情况下，此类网站是正当投诉的渠道，并且在很多司法辖区受到言论自由法保护。
- **欺骗性和/或攻击性域名** — 注册域名，将不知情的用户定向到淫秽内容，或将未成年人定向到有害内容 — 有时也称为某种形式的“鼠标陷阱”。
- **伪造续订通知** — 个人或组织以当前注册服务机构之名，向注册人发送的误导性函件。发送此类通知是为了达到各种各样的欺骗目的。
- **域名排列注册** — 使用自动化工具创建某个既定域名字符串的不同排列形式。虽然注册服务机构经常会在潜在注册人查询的字符串不可用时，合理使用此类工具为注册人推荐替代字符串，但是工作组担心此类工具生成的结果可能会对商标字符串构成侵权。

---

[10] 同上。

[11] 《注册滥用政策工作组最终报告》，2010 年 5 月，http://gnso.icann.org/en/issues/rap/rap-wg-final-report-29may10-en.pdf

- **按点击付费** – 网站上使用的一种互联网广告模式，广告主仅在其广告被点击时才向托管方付费。这里提出的担忧是，域名中使用的商标会将流量吸引到包含付费广告位的站点。
- **分食流量** – 在 HTML 可见文本、隐藏文本、元标签或网页标题中使用品牌名称，以操纵搜索引擎排名并分食流量。
- **虚假关联** – 谎称是品牌所有人的关联机构。
- **跨 TLD 注册诈骗** – 一种欺骗性销售手段，通知现有注册人某一方有意或试图在另一 TLD 中注册该注册人的域名字符串，由此迫使注册人通过通知发送方追加注册。该通知发送方通常是可以从追加注册中获利的中间商，并且将以高于市场平均价的价格提供新域名创建服务。
- **域名重复注册/体验** – 注册人频繁注册、删除和重新注册相同名称，滥用“追加宽限期”，以避免支付注册费。

另一方面，RAPWG 对“使用”问题定义如下：

> 域名使用问题则是域名注册人在域名创建后用域名做什么的问题，也就是域名注册人使用该域名的目的和/或域名注册人通过该域名提供何种服务的问题。这些使用问题通常独立于或者说不涉及任何注册问题…ICANN 和 GNSO 的政策制定权力在域名使用领域会受到更多限制。

工作组将以下活动作为使用滥用的潜在形式进行了讨论：

- **网络钓鱼** – 此类网站伪装成受信任站点（通常是银行），诱使上网用户泄露敏感信息（例如网上银行凭证、电子邮箱密码）。网络钓鱼的目的通常是盗取资金或其他有价值的资产。
- **垃圾邮件** – 从某些域发出的大量不请自来的电子邮件，用于推销网站。
- **恶意软件/僵尸网络指挥控制** – 使用域名作为一种方式，控制和更新受同一犯罪分子控制的成千上万台被感染计算机组成的僵尸网络。僵尸网络可用于从事各种各样的恶意活动，包括**分布式拒绝服务攻击 (DDoS)**、**垃圾邮件**以及托管网络钓鱼和垃圾邮件站点的**快速通量** [参见下文对本定义中所用手段和术语的进一步解释]。
- **使用被盗凭证** – 使用诸如身份、访问和财务凭证等来注册域名用于恶意目的，从个人或组织的运营过程中窃取信息，和/或以其他方式中断个人或组织的运营。

在报告中，RAPWG 再三说明 ICANN 及其下各支持组织通过政策制定和实施流程对*注册*问题有一定控制权，但是，鉴于 ICANN 对注册人如何使用其域名的管理权有限，*使用*问题将更难应付。注意，本部分中给出的定义和活动专指 RAPWG 成员为撰写报告所讨论的定义和活动，并不表示 ICANN 赞同这些活动就是事实上的 DNS 滥用。在此提出这些定义和活动旨在方便 CCT-RT 开展工作，仅供参考和讨论之用。

《新 gTLD 注册管理机构协议》规格 11

《新 gTLD 注册管理机构协议》规格 11 规定，作为对 ICANN 合同义务的一部分，注册管理运行机构须恪守某些公众利益承诺 (PIC)。第 3a 和 3b 小节作为涉及 DNS 滥用的内容强调了注册管理运行机构的公众利益承诺，并且描述了他们在工作中应进行哪些活动来缓和并跟踪自身 TLD 内的滥用行为。规格 11 陈述：[12]

> 3a. 注册管理运行机构将在其《注册管理机构-注册服务机构协议》中纳入如下规定，要求注册服务机构在其注册协议中禁止注册域名持有者散布恶意软件、滥用僵尸网络、网络钓鱼、盗版、商标或版权侵权、诈骗或欺骗、造假以及以其他方式从事违反适用法律的活动，并（依据适用法律和任何相关程序）注明这些行或活动会带来的后果，包括暂停域名的使用。
>
> 3b. 注册管理运行机构应定期进行技术分析，评估 TLD 中的域名是否被用于威胁网络安全的行为，例如网址嫁接、网络钓鱼、恶意软件和僵尸网络等。注册管理运行机构将编制统计报告作为定期安全检查的结果，并在报告中记录所发现的安全威胁的数量以及所采取的措施。注册管理运行机构将在协议期间保存这些报告（除非法律要求或 ICANN 批准保存更短时间）并根据要求提供给 ICANN。

规格 11 中所描述的活动可以为 CCT-RT 提供一个额外的定义框架，以便其进一步界定审核的范围。

DNS 滥用：其他专用术语和考虑因素

有关构成 DNS 滥用的活动，还有一些其他专用术语和考虑因素值得注意。

- **网络钓鱼**利用**社会工程**和技术手段来窃取消费者个人身份资料和财务帐户凭证。社会工程方案使用伪造电子邮件引诱消费者进入假冒网站，目的是欺骗收件人泄漏财务资料，例如信用卡卡号、帐户用户名、密码和社会保险号码等。**鱼叉式网络钓鱼**是一种有针对性的网络钓鱼邮件诈骗形式，它将目标对准组织内拥有高价值凭证的个人，并欺骗他们提供敏感信息。[13]
- **快速通量**是僵尸网络在网络钓鱼、垃圾邮件和其他恶意软件传送活动中使用的一项技术。此类攻击来自于一套经常变化的 IP 地址，因而大大增加了检测的难度。[14]

---

[12]《注册管理机构协议》，访问于 2016 年 2 月 4 日，https://www.icann.org/resources/pages/registries/registries-agreements-en

[13]《SSAC 注册人保护公告：凭证管理生命周期内安全性和稳定性维护的最佳实践》，ICANN 安全与稳定咨询委员会，2015 年 11 月，https://www.icann.org/en/system/files/files/sac-074-en.pdf

[14]《SSAC 关于快速通量托管和 DNS 的咨询报告》，ICANN 安全与稳定咨询委员会，2008 年 3 月，https://www.icann.org/en/system/files/files/sac-025-en.pdf

- **误植域名** — 又称“URL 劫持”— 是**域名抢注**的一种，通常是利用用户在 Web 浏览器中输入网址时所犯的书写错误，将用户定向到恶意站点。[15]
- **恶意广告**是指在某个网站或广告网络上做广告，目的是在每一次被观看时，或者每隔一定时间或一定的点击次数，使观看者的设备感染恶意软件。[16]
- **搜索引擎投毒**是一种操纵搜索引擎的活动，使其显示包含恶意网站链接的搜索结果。[17]
- **欺诈攻击**是指恶意行为者冒充另一设备或用户，对网络主机发动攻击，或者窃取数据、传播恶意软件或绕过访问控制。[18]
- **（分布式）拒绝服务 (DDoS) 攻击**是设法使一个或多个计算机系统不可用的网络攻击。*分布式*攻击 — 通过僵尸网络进行 — 是指多个系统经协调后发出大量请求来压垮受害人的服务器。一种新形式的**“放大”DDoS 攻击**，利用 DNS 反射和放大来达到极高的攻击数据比特率（据报告超过 300 吉比特/秒），从而吞噬受害人的网络容量，并造成重大或彻底的服务中断。[19]
- **域阴影**是另一种新型的 DNS 滥用形式，犯罪分子利用通过窃取或网络钓鱼得到的凭证，在注册人资产中创建无数个与现有合法域相关的子域。在注册人看来，其合法域仍在正常运行，但实际上这些子域正将访客定向到恶意站点。[20]

---

[15] Moore 和 Edelman，“Measuring the Perpetrators and Funders of Typosquatting”（衡量误植域名的作恶者和出资者），该论文于 2010 年 1 月在特内里费岛举行的第 14 届 International Conference on Financial Cryptography and Data Security（金融密码术与数据安全国际会议）上发布，http://www.benedelman.org/typosquatting/typosquatting.pdf

[16] 第四届全球 DNS 稳定性、安全性和灵活性研讨会，会议报告，2012 年 10 月，https://www.icann.org/en/system/files/files/dns-symposium-25oct12-en.pdf

[17] “Search Engine Poisoning”（搜索引擎投毒），Imperva，访问于 2016 年 2 月 1 日，https://www.imperva.com/resources/glossary?term=search_engine_poisoning_sep

[18] Veracode，“Spoofing Attack:IP, DNS & ARP”（欺诈攻击：IP、DNS 和 ARP），访问于 2016 年 2 月 4 日，http://www.veracode.com/security/spoofing-attack

[19] 《SSAC 有关利用 DNS 基础设施进行 DDoS 攻击的咨询报告》，ICANN 安全与稳定咨询委员会，2014 年 2 月，https://www.icann.org/en/system/files/files/sac-065-en.pdf。另请参见 Alvarez、Carlos，“放大 DDoS 攻击：当前互联网所面临的最大威胁”，ICANN 博客，2014 年 4 月 11 日，https://www.icann.org/news/blog/amplified-ddos-attacks-the-current-biggest-threat-against-the-internet

[20] 《SSAC 注册人保护公告：凭证管理生命周期内安全性和稳定性维护的最佳实践》，ICANN 安全与稳定咨询委员会，2015 年 11 月，https://www.icann.org/en/system/files/files/sac-074-en.pdf

- **DNS 缓存投毒**攻击是指恶意行为者设法让域名服务器添加恶意数据，或者将缓存的 DNS 数据修改为恶意数据。**网址嫁接**是此类活动的一种形式，恶意行为者诱骗受害人点击一个链接（通常是通过垃圾邮件发送），由此感染受害人的个人计算机或服务器，并将用户重定向到欺诈性网站，收集机密个人信息。[21]

对于所有这些伎俩必须谨记一条：它们几乎都利用了诸如贪婪、粗心和/或天真等**人性的弱点**。因此，**最终用户往往是网络安全链条中最薄弱的一环**。[22]

DNS 滥用：主要统计和趋势

ICANN 近期发起的一项针对 6,144 名消费者的全球调查报告了如下结果：

- 74% 的消费者了解网络钓鱼
- 79% 的消费者了解垃圾邮件
- 40% 的消费者了解域名抢注
- 67% 的消费者了解窃取凭证
- 76% 的消费者了解恶意软件

除了对 DNS 中的恶意行为具有较高认知度以外，多数消费者和最终用户还表示对每一种滥用行为“非常/有点害怕”，并且相信这些行为也“非常/比较”常见。[23]

[21] 参见 Piscitello、Dave，“DNS Pharming:Someone’s poisoned the water hole!”（DNS 网址嫁接：有人在水里投毒！），WatchGuard Technologies 专家社论，2005 年，http://www.corecom.com/external/livesecurity/dnsphishing.htm

[22] Khonji、Mahmoud 和 Youssef Iraqi，“Phishing Detection:A Literature Survey”（网络钓鱼检测：文献调查），IEEE Communications Surveys & Tutorials（IEEE 通信调查和教程），第 15 卷第 4 期（2013 年第 4 季度），DOI：10.1109/SURV.2013.032213.00009

[23] ICANN 全球消费者调查，由尼尔森公司进行，2015 年 4 月，https://www.icann.org/news/announcement-2015-05-29-en

作为全世界最大的网络安全企业之一，赛门铁克公司 (Symantec) 编写了一份关于全球互联网安全状况的年度报告。[24]它在最新报告中提供了多个指标，表明主要 DNS 滥用活动的总体趋势。因此，随着 CCT-RT 工作不断推进，该报告可以作为对新旧 gTLD 中 DNS 滥用进行更多分段分析的一个出发点：

指标	描述性统计数据	趋势
发现带恶意软件的网站	• 2014 年：1/1126 • 2013 年：1/566	
垃圾邮件总体比例（所有被归类为垃圾邮件的电子邮件百分比）	• 2015 年：54%[25] • 2014 年：60% • 2013 年：66%	
全球每天的垃圾邮件数量（估计值）	• 2014 年：280 亿 • 2013 年：290 亿	
电子邮件网络钓鱼率（企图进行网络钓鱼的电子邮件占比）	• 2014 年：1/965 • 2013 年：1/392	
每年新增的恶意软件变体	• 2014 年：3.17 亿 • 2013 年：2.52 亿	
电子邮件含恶意软件率（含恶意软件的电子邮件比例）	• 2014 年：1/244 • 2013 年：1/196 • 2012 年：1/291	
僵尸程序数量	• 2014 年：190 万 • 2013 年：230 万 • 2012 年：340 万	

尽管在被分析的特定 DNS 滥用形式中，这些数据大体呈现下降趋势，但需要指出的是，它们仅代表这些趋势的一个片段。例如，尽管从表格来看，网络钓鱼攻击似乎在减少，但是**自 2008 年以来，网络钓鱼攻击数将近翻了一番**，这表明表格所示的下降趋势仅仅是整体趋势线上一个略低的点而已。[26]此外，表格所示的数据涵盖*整个* DNS；并未具体描述*新* gTLD 中的 DNS 滥用。

---

[24] Symantec，“Internet Security Threat Report 20”（互联网安全威胁报告 20），2015 年 4 月，https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf

[25] 注意，此 2015 年数据出自 Symantec 2015 年 11 月的信息报告：www.symantec.com/content/en/us/enterprise/other_resources/intelligence- report-11-2015-en-us.pdf。所列数字为除 2015 年 12 月外的年度数据。对于此表格中所列的其他指标，Symantec 未报告 2015 年数据

[26] Illumintel 为 ICANN 董事会新 gTLD 项目委员会开展的“Potential for Phishing in Sensitive-String Top-Level Domains”（在敏感字符串顶级域中实施网络钓鱼的可能

新 gTLD 中的 DNS 滥用

关于新 gTLD 中 DNS 滥用的系统性研究很少，可能是由于其新颖性所致。ICANN 发起的上述调查显示，**消费者对新 gTLD 的信任远低于传统 TLD**，其中信任新 TLD 的受访消费者约为 50%，而信任传统 TLD 的受访消费者达到近 90%。[27]加州大学圣地亚哥分校的研究人员发现，在注册后的第一个月内，**新 TLD 域名出现在域名黑名单上的概率是传统 TLD 的两倍多**（域名黑名单是指已知垃圾邮件发送人所在域名的名单）。[28]

据 APWG 成员称，**恶意行为者似乎在测试新 gTLD 空间**作为其活动基地的可能性。[29]他们认为这可能是新 gTLD 市场竞争加剧的结果，加剧的竞争压低了价格，进而吸引恶意行为者寻找以更低成本牟利的机会。但是他们同时指出，鉴于新 gTLD 尚处于早期引入阶段，可用于比较的证据有限，在此基础上很难得出结论。他们建议等到未来数据充足时再对新旧 TLD 中的 DNS 滥用进行比较研究。[30]

TLD 咨询管理公司 Architelos 提供了对新旧 TLD 以及国家和地区 TLD (ccTLD) 中 DNS 滥用的更为细致的分析。在 2015 年 6 月发布的最新报告中，他们运用自创的“域名空间质量指数”(NQI) 指标 — 即在各注册管理机构所管理的**每百万域名中，被列入其阻止列表的滥用域名数量** — 分析了新旧 gTLD 中的滥用行为情况。报告列出了许多重要发现：[31]

- 根据 2014 年 1 月到 2015 年 6 月的 NQI，新 gTLD 中的**滥用活动**（网络钓鱼、恶意软件、僵尸网络指挥控制和垃圾邮件）比例自 2014 年 2 月在新 gTLD 中发现第一起滥用案例以来**急剧上升**，并且正逼近传统 gTLD 的水平。
- 在被分析的时间区间内，**在新 gTLD 中报告的滥用中，垃圾邮件占 99%**（在传统 gTLD 和 ccTLD 中，垃圾邮件占 90%）。

性）研究，2015 年 5 月 21 日，https://www.icann.org/resources/pages/new-gtld-program-committee-2014-03-21-en

[27] ICANN 全球消费者调查，由尼尔森公司进行，2015 年 4 月，https://www.icann.org/news/announcement-2015-05-29-en

[28] 注意，这一指标是在研究时获取的一个“快照”，不反映任何更长期的分析结果。参见 Der 等人撰写的“From .academy to .zone:An Analysis of the New TLD Land Rush”（从 .academy 到 .zone：新 TLD 抢滩分析），加州大学圣地亚哥分校计算机科学与工程部，2015 年 10 月，DOI：10.1145/2815675.2815696。

[29] 反网络钓鱼工作组，“全球网络钓鱼调查：域名的使用和趋势（2014 年上半年）”，2014 年 9 月 25 日，https://apwg.org/apwg-news-center/

[30] 同上。

[31] Architelos，“The NameSentry™ Abuse Report”（NameSentry™ 滥用报告），2015 年 6 月，http://architelos.com/wp-content/uploads/2015/06/Architelos-StateOfAbuseReport2015-webc-FIN.pdf

- 2015 年 5 月，**新 gTLD 的 NQI 分数为 11,654/百万受管理域名**，而**传统 gTLD 的分数约为 16,500/百万受管理域名**。
- 与传统 gTLD 相比，**新 gTLD 中网络钓鱼、恶意软件和僵尸网络指挥控制占比依旧非常低**，但是随着新 gTLD 认知度和普及率的增加，这一比例可能会上升。从 2014 年 5 月到 2015 年 5 月，**从事网络钓鱼的域名数量飙升**，发现后被加入阻止列表的域名从 7 个增至 143 个，翻了 20 倍（同期传统 gTLD 中被阻止的域从约 7,300 个增至 14,000 个）。但是，**在这 143 个新网络钓鱼报告中，有 77% 仅集中在 10 个新 gTLD 上**。

DNS 滥用案例研究：新 gTLD 中的网络钓鱼

网络钓鱼的盛行率可作为恶意行为者对新 gTLD 滥用程度的一个指标。在由 APWG 成员共同撰写的一份研究报告中，作者指出 **DNS 通过新 gTLD 项目的扩张不太可能会推升全球网络钓鱼的总量，**但是可能催生出**新的、与以往不同的网络钓鱼攻击发生地**。因为随着时间推移，网络罪犯可能喜欢从一个 TLD“跳到”另一个 TLD。[32]网络钓鱼者通常不再注册包含品牌名称的域名，而是倾向于注册无意义字符串，或者将品牌名称放到子域或子目录中的某个位置，因为品牌所有人会定期查找其品牌名称使用不当的情况。2014 年下半年，在所有被用于网络钓鱼的域名中，仅有 1.9% 含有品牌名称或其变化形式（通常是错误拼写）。

在 APWG 成员撰写的另一篇分析文章中，作者得出了类似结论，指出新 gTLD 中尚未形成新网络钓鱼的“重灾区”。上述两篇文章的作者使用了一个指标 — “每 10,000 个域名中用于网络钓鱼的域名”，也就是一个 TLD 中用于网络钓鱼的域名数与该 TLD 中注册域名总数之比，作为衡量新 TLD 在网络钓鱼方面健康程度的标尺。[33] 在分析中，他们得出结论：**每 10,000 个域名中用于网络钓鱼的域名数量介于 3.4 和 4.7 之间为网络钓鱼盛行率的“中间”分数。**[34]分数超过 4.7 表示该 TLD 的网络钓鱼盛行率高于平均水平。2014 年下半年，对所有 TLD 而言，每 10,000 个域名中用于网络钓鱼的域名数量中值为 3.4。**在 295 个*新* gTLD（2014 年）中，只有 9 个分数超过 3.4**。[35]除此之外，**网络钓鱼攻击的平均“上线时间”** — 或者这些攻击的活跃时间，

---

[32] Illumintel 为 ICANN 董事会新 gTLD 项目委员会开展的“Potential for Phishing in Sensitive-String Top-Level Domains”（在敏感字符串顶级域中实施网络钓鱼的可能性）研究，2015 年 5 月 21 日，https://www.icann.org/resources/pages/new-gtld-program-committee-2014-03-21-en

[33] 反网络钓鱼工作组，“全球网络钓鱼调查：域名的使用和趋势（2014 年下半年）”，2015 年 5 月 27 日，https://apwg.org/apwg-news-center/

[34] 注意，APWG 的 2014 年上半年报告表明该指标介于 4.1 和 4.7 之间。这些指标的变化符合网络钓鱼的整体活跃度“曲线”

[35] 反网络钓鱼工作组，“全球网络钓鱼调查：域名的使用和趋势（2014 年下半年）”，2015 年 5 月 27 日，https://apwg.org/apwg-news-center/

也是钓鱼者攻击强度的关键指标之一 — **处于历史低位**，表明**反网络钓鱼工作取得了一定成效**。[36]

两篇文章的作者称，**域名价格似乎是影响 TLD 中网络钓鱼的重要驱动因素**，在传统 TLD 中，域名往往更加便宜。[37]在 ICANN 发起的一个关于衡量 DNS 滥用的电话会议上，该观点在来自注册管理机构和注册服务机构的多名代表中引起了共鸣，他们表示，**较高的域名价格是滥用活动总体减少的关键因素**。[38]来自 APWG 的作者预测，随着新 gTLD 的普及以及伴随供应量增加和竞争加剧而来的降价，我们将在新 gTLD 中看到比传统 TLD 以及国家和地区 TLD (ccTLD) 更多的网络钓鱼。佐证这一趋势的一个主要证据来自 .xyz gTLD 的案例，该 gTLD 曾在一段时间内提供免费域名。2014 年下半年，新 gTLD 中近 2/3 的网络钓鱼集中在 .xyz 注册管理机构。[39]保持低成本似乎是网络钓鱼者的一个重要关注点，研究表明这是一项越来越趋于“低技术含量和低回报的业务”。[40]尽管有故事显示网络钓鱼带来了惊人的利润，但是普通网络钓鱼者似乎每周只能净赚几百美元左右。[41]

九项保护措施

在启动新 gTLD 项目之前，ICANN 咨询了 DNS 滥用和网络安全领域的主题问题专家，让他们就可以采取哪些先发制人的措施来缓和上文所述的各类活动提出建议。专家社群提出了下述九项保护措施。现在，CCT-RT 仍要负责确定这些保护措施在实现预期目标方面的有效性究竟如何。

---

[36] 事实上，2014 年下半年的上线时间*中值*略有上升，从 8 小时 42 分钟增至 10 小时 6 分钟。参见反网络钓鱼工作组，“全球网络钓鱼调查：域名的使用和趋势（2014 年下半年）”，2015 年 5 月 27 日，https://apwg.org/apwg-news-center/

[37] 反网络钓鱼工作组，“全球网络钓鱼调查：域名的使用和趋势（2014 年下半年）”，2015 年 5 月 27 日，https://apwg.org/apwg-news-center/

[38] 一位参与者非正式地假定了一个 15 美元的阈值，一般来说域名价格大于这一阈值时，滥用率开始下降。ICANN 运营和政策研究，“针对新 gTLD 项目中防 DNS 滥用的保护措施的审核工作”，2016 年 1 月 28 日，电话会议记录，相关录音位于 https://newgtlds.icann.org/en/reviews/dns-abuse

[39] 作者指出，大多数用于网络钓鱼的 .xyz 域名是通过中国注册服务机构注册的，并用于攻击中国目标。参见反网络钓鱼工作组，“全球网络钓鱼调查：域名的使用和趋势（2014 年下半年）”，2015 年 5 月 27 日，https://apwg.org/apwg-news-center/

[40] Herley 和 Florencio，“A Profitless Endeavor:Phishing as Tragedy of the Commons”（无利可图的事业：网络钓鱼的平民悲剧），Microsoft Research（微软研究院），2008 年 9 月，http://research.microsoft.com/en-us/um/people/cormac/Papers/PhishingAsTragedy.pdf

[41] 同上。鉴于其“地下”性质，相关数据很难获得。因此，对于网络钓鱼的实际总体成本和收益依然存在较大争议

为理解缓和 DNS 滥用的九项保护措施的“有效性”，**首先必须把“有效性”定义为一个可以衡量的概念**。下文将在已经提出的各问题的背景下讨论这一定义，以初步确定对于新 gTLD 项目而言，哪些保护措施势在必行。文中将提供关于所提出“有效性”措施的可用数据。如果没有数据可用，将讨论缺乏数据的原因，然后提供其他评估该保护措施有效性的潜在方法。

问题：如何确保不会让不良行为者来运营注册管理机构？

在这一问题的背景下，“有效性”可以理解为防止“不良行为者”— 即那些曾经犯下与经济活动有关的重罪或轻罪的行为人 — 运营注册管理机构。早在 2001 年，《.COM 注册管理机构协议》就规定，如果注册管理运行机构存在以下情况，则可以终止注册管理机构协议：

> “(a) 被管辖法院判处重罪或涉及金融活动的其他严重犯罪，或是管辖法院认定的处罚对象，或 ICANN 有理由相信此处罚在性质上与以上罪行同样严重；或者 (b) 因涉及不诚实行为或滥用他人资金被驻地政府处罚。”[42]

此条款也存在于新 gTLD 注册管理机构协议中，并附带其他规定：

> (f) 如发生以下情形，ICANN 可在通知注册管理运行机构后终止本协议：(i) 注册管理运行机构雇用的任何高管被判重罪或与经济活动相关的轻罪，或被具有有效管辖权的法院判定进行欺诈或违反诚信义务，或是某司法认定的处罚对象，且 ICANN 有理由相信此处罚在性质上与以上罪行同样严重，且注册管理运行机构获悉此情况后三十 (30) 天内未终止雇用该高管；或者 (ii) 注册管理运行机构董事会或类似主管团体的任何成员被判重罪或与经济活动相关的轻罪，或被具有有效管辖权的法院判定进行欺诈或违反诚信义务，或是某司法认定的处罚对象，且 ICANN 有理由相信此处罚在性质上与以上罪行同样严重，且注册管理运行机构在获悉此情况后三十 (30) 天内未将该成员从注册管理运行机构董事会或类似主管团体除名。[43]

[42]《.com 注册管理机构协议》，2001 年 5 月 25 日，https://www.icann.org/resources/unthemed-pages/registry-agmt-com-2001-05-25-en#II-16C。

[43]《注册管理机构协议》，2014 年 1 月 9 日，https://www.icann.org/resources/pages/registries/registries-agreements-en

保护措施：审查注册管理运行机构

背景

“在签署注册管理机构协议并在根区中授权 TLD 之前审查注册管理运行机构”已作为一项保护措施增加到新 gTLD 项目的《gTLD 申请人指导手册》中，旨在防止有犯罪史或恶意行为史的申请人运营 TLD。制定这一措施是为了创建一个固定流程，在签署注册管理机构协议之前的初始申请评估中筛查注册管理运行机构。

ICANN 已聘请普华永道 (PwC) 执行背景筛查，重点关注两个方面：1) 一般业务尽职调查和犯罪记录；以及 2) 域名抢注行为记录。特定申请是否有资格进入新 gTLD 项目一般会在初步评估中报告，有时也会在扩展评估中报告。

新 gTLD 项目中的背景筛查将在初步评估流程期间适时进行。如果申请人在评估过程中报告其申请信息变更，那么在签署注册管理机构协议之前将再一次开展背景筛查。无论是哪种情况，ICANN 均保留在签署协议之前根据需要再次开展尽职调查的权利。

定义“有效性”

对于此项保护措施，“有效性”可以理解为防止有恶意行为或犯罪史的注册管理运行机构与 ICANN 签署注册管理机构协议。但是，正如上文所指出的，审查流程将适时进行，而负责管理 TLD 的实体可能会产生变化（例如公司被出售，或者高级职员更迭）。在 DNS 滥用的背景下，长期持续考虑是否有证据表明不良行为者在运营注册管理机构或者是否有此类风险也很重要。

现状

根据 2016 年 1 月公布的《项目实施审核》，背景筛查流程是“针对所有申请实体，以及在申请问题 9-11 中披露的个人和组织进行的审核，其中包括申请实体的高级职员、董事以及大股东。”[44]根据《审核》，ICANN 对 1,930 个申请进行了 1,150 次背景筛查（有的实体递交了多个申请）。各申请的背景筛查结果在初步评估程序完成后公布。在某些情况下，背景筛查专家组向申请人提出了一些问题要求其做出说明。总体而言，《项目实施审核》将背景筛查称为一个成功的流程，因为所有申请人均可接受筛查。但同时也指出，申请提交截止日期和注册管理机构协议签署日期之间的间隔长于预期。这意味着许多申请人需要重新筛查。《审核》建议，背景筛查可在签约阶段进行，而不是初步评估期间，以便将重新筛查的必要性降至最低。

[44]《项目实施审核》，2016 年 1 月 29 日，https://www.icann.org/en/system/files/files/program-review-29jan16-en.pdf

数据收集与衡量的可用方法

要判断对于*两个*方面而言，该保护措施作为预防措施是否均有效可能为时过早。任何对“有效性”的衡量都必须考虑基于初步背景筛查而被拒绝的情况数据，以及由于注册管理机构未能从高级职员或董事会中清除不良行为者而导致注册管理机构协议终止的情况数据。而且由于背景筛查流程牵涉到个人信息和敏感信息，表明申请是否有资格进入流程下一步的报告有限。但是，总体数据可以提供。可用将正式合规投诉和/或注册管理机构协议终止用来衡量此项保护措施是否继续有效。

此外，对于员工背景有问题的潜在申请人而言，此项保护措施还具有震慑作用。但是，衡量震慑作用 — 即有*多少*申请人*没有*申请 — 几乎不可能做到，因为这一作用不会产生任何可以衡量的数据。

问题：如何确保注册管理机构信息的完整性和实用性？

在此问题下对“有效性”的定义可以理解为：保护措施可成功用于协助验证和确认注册管理机构信息。以下三种预防性保护措施的设计就是为了做到这一点。

保护措施：要求提供 DNSSEC 部署示范计划

背景

域名系统安全扩展 (DNSSEC) 的开发旨在遏制恶意行为者劫持 DNS 查找进程的企图。例如，此类行为人可能会侵入 Web 用户的查找表，并将他们定向到恶意网站，以窃取机密信息。DNSSEC 通过对数据进行数字签名防范此类攻击，这样用户就可以对来源的正当性放心。它对现有 DNS 记录采用加密签名，以确认 DNS 记录来自官方域名服务器并且未在任何一点篡改。[45]注册管理机构部署 DNSSEC 后，注册人如果愿意，可以将具体域名密钥分配到他们的域名中。通过注册管理机构协议对 DNSSEC 做出规定，目的是保障它能更加广泛和快速地实现部署。

此保护措施要求所有新 gTLD 申请人有一个具体的 DNSSEC 部署计划。该计划会在初步评估流程中进行评估，主要目的是减少 DNS 记录造假的风险。根据注册管理机构协议的规定，新 gTLD 注册管理运行机构必须签署含 DNSSEC 的 TLD 域文件，遵循互联网工程任务组 (IETF) RFC 4641 及其后续意见征询中所述的最佳实践，以安全方式从子域名接受公钥材料，并按照 RFC 6841 中的格式公布 DNSSEC 规范声明 (DPS)。[46] [47]

---

[45] “DNSSEC – What Is It and Why Is It Important?”（DNSSEC — 这是什么？为什么重要？），访问于 2016 年 2 月 1 日，https://www.icann.org/resources/pages/dnssec-qaa-2014-01-29-en；“How DNSSEC Works”（DNSSEC 如何工作），访问于 2016 年 2 月 1 日，https://www.cloudflare.com/dnssec/how-dnssec-works/

[46] ICANN 注册管理机构协议，规格 6：1.2 DNSSEC，访问于 2016 年 2 月 1 日，https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm

定义“有效性”

此项保护措施的“有效性”可以从多个方面定义。它可以简单地定义为注册管理运行机构拥有具体的 DNSSEC 部署计划，并通过了申请阶段的评估。也可以根据在注册管理机构对 DNSSEC 要求的遵守方面报告的问题数来定义。最后，它还可以根据 DNSSEC 的更广泛分发来定义，例如注册人完成的签名率，或者 DNSSEC 验证的 DNS 解析器在互联网服务提供商 (ISP) 运行的网络内的部署情况。[48]

现状

截止到 2016 年 2 月 23 日，在根区的 1,236 个 TLD（含 ccTLD）中，有 1,073 个签署了 DNSSEC 密钥。[49]

数据收集与衡量的可用方法

现有的两个衡量指标分别是根区中的 TLD 数量，以及在每个 TLD 中拥有签名密钥的二级域数量。[50]更深入的指标可重点衡量在授权前测试阶段发现的 DNSSEC 问题、有多少服务水平协议 (SLA) 监督问题被报告，以及在 DNSSEC 合规方面收到的投诉数量。

综合衡量此方面“有效性”需考虑这样一个事实，即注册服务机构、注册人、DNS 托管提供商和 ISP 均在 DNSSEC 的全面部署和功能中扮演着重要角色。例如，尽管注册管理运行机构被要求展示一个 DNSSEC 部署计划，但这不代表注册人一定会在上面签字。ICANN 技术服务部收集的初步数据表明，通常只有一小部分二级域拥有签名的 DNSSEC 密钥（虽然不同 TLD 之间差异显著）。[51]CloudFlare 案例是一个可以考虑进行的案例研究。CloudFlare 是一家域名服务器服务和 DNS 内容交付公司，该公司决定让其网络上的任何人都可一步到位地通过 DNSSEC 来保障他们的流量安全。采用案例研究方法，从不同行业视角看待注册管理机构、注册服务机构、DNS 托管提供商和 ISP 对 DNSSEC 的支持，可以确定各 gTLD 中 DNSSEC 部署的薄弱环节。DNSSEC 部署工作组已经收集这一信息，其报告位于 dnssec-deployment.org。

---

[47] “RFC”为“意见征询”系列文件，由 IETF 撰写，内含对计算机联网、协议、程序和概念的技术和组织摘要。参见 www.ietf.org/rfc

[48] “Deployment Guide:DNSSEC for Internet Service Providers (ISPs)”（部署指南：针对互联网服务提供商 (ISP) 的 DNSSEC），访问于 2016 年 2 月 1 日，http://www.internetsociety.org/deploy360/resources/deployment-guide-dnssec-for-isps/

[49] “TLD DNSSEC Report”（TLD DNSSEC 报告），访问于 2016 年 2 月 23 日，http://stats.research.icann.org/dns/tld_report/

[50] 参见“DNSSEC Deployment Report”（DNSSEC 部署报告），访问于 2016 年 2 月 23 日，http://rick.eng.br/dnssecstat/

[51] ICANN 技术服务部为本报告用途从公开域文件中收集到的数据

保护措施：禁止使用通配符

背景

此建议要求采取恰当控制措施，防止在 DNS 中使用“通配符”。如果使用“通配符”，则对于不存在的 DNS 查询，注册管理运行机构不会提供“名称错误”响应，而是使用 DNS 重定向、通配符或合成响应。[52]ICANN 已禁止了这些操作，因为有研究结果表明它们创造了新的恶意攻击机会，会给 DNS 的安全性和稳定性带来风险。[53]

此项保护措施已在《注册管理机构协议》规格 6 中第 2.2 节定义：

> 2.2. 禁用通配符。对于未注册的域名、注册人未提供要在 DNS 域文件中列出的有效记录（如 NS 记录）的域名，或域名状态不允许在 DNS 中公布的域名，禁止注册管理机构使用 RFC 1034 和 4592 中所述的 DNS 通配符资源记录，或用于合成 DNS 资源记录和在 DNS 中使用重定向的何其他方法或技术。当查询此类域名时，权威性名称服务器必须返回“名称错误”响应（也称为 NXDOMAIN），如 RFC 1035 和相关 RFC 中所述的 RCODE 3。此规定适用于 DNS 树中所有级别的所有 DNS 域文件，注册管理运行机构（或参与提供注册管理机构服务的关联机构）将为这些文件维护数据、安排此类维护或通过此类维护获取收入。

然而，2014 年，作为域名冲突管理框架的一部分，在一些 TLD 授权后通配符被立即部署到这些 TLD 中一段有限的时间（控制性中断期），用以识别任何域名空间冲突。[54]如 JAS 第 1 阶段报告*《缓和 DNS 域名空间冲突风险》*所述：

> 我们建议注册管理机构在根区授权后立即实施一个控制性中断期，在此期间暂时解禁通配符记录。考虑到控制性中断的目标以及此时在区域中将没有注册人数据这个事实，我们相信为达到这一目的而暂时允许使用通配符记录与

---

[52] “About Wildcard Prohibition (Domain Redirect)”（关于通配符禁用[域名重定向]），访问于 2016 年 2 月 1 日，https://www.icann.org/resources/pages/wildcard-prohibition-2014-01-29-en

[53] ICANN 安全与稳定咨询委员会，《SAC041：禁止新 TLD 使用重定向及合成响应的建议》，2009 年 6 月 10 日，https://www.icann.org/en/system/files/files/sac-041-en.pdf

[54] 参见“常见问题与解答：针对注册管理机构的域名冲突管理框架”，访问于 2016 年 2 月 11 日，www.icann.org/resources/pages/name-collision-ro-faqs-2014-08-01-en，其中陈述：“对于适用的 TLD（即在该 TLD 下除了‘nic’外没有其他有效域名），在控制性中断期内可免于遵守禁用通配符的规定。此豁免权仅适用于在该 TLD 内没有任何名称被授权（因而也没有任何名称在运营）的情况，以便消除传统上与通配符实施有关的风险。暂时解禁并规定可以使用通配符是为了捕捉到所有明显的域名冲突情况。在区域‘顶级’使用的通配符将匹配所有查询 — 这些查询在该区域全面投入运行后将会看到。此方法最大限度地增加了为保护那些目前正在泄露查询（本意为本地查询）的互联网用户而采取的步骤。”

ICANN 禁止使用通配符记录的规定并不冲突，也不会引发担忧，导致 ICANN 确立这些禁用规定。[55]

定义“有效性”

这一措施的“有效性”理论上可定义为对新 gTLD 中禁用通配符这一规定的遵守程度。也可考虑将对这一行为的评估作为保障注册管理机构信息完整性和实用性的一种手段。在对这些行为（即，此保护措施设法防止的行为）的影响方面，相关意见也可以纳入评估。

现状

ICANN 提供了一个《通配符禁用（域名重定向）投诉表》，用于报告与合同规定不符的情况。[56]迄今为止，ICANN 尚未通过此工具收到任何对禁用通配符的投诉。[57]

数据收集与衡量的可用方法

正如上文所指出的，尚未收到新 gTLD 注册管理机构有关通配符的投诉。就这一保护措施的有效性咨询主题问题专家，要求其给出定性意见，这可能是弥补定量数据缺乏的途径之一。

其他途径可包括，不但要关注 ICANN 收到的有关特定 TLD 内未能禁用通配符的投诉，还要关注当前 DNS 重定向用于“错误流量货币化”（即，当 DNS 查找失败时，将 DNS 用户重定向到广告用 Web 服务器的做法）的频率。加州大学伯克利分校的 ICSI Netalyzr 是一个网络诊断工具，也是衡量互联网健康程度的研究的一部分。在以往的研究中，它一直被用来检查 DNS 重定向问题，可作为了解 DNS 中通配符影响的一个有用工具。[58]

---

[55] JAS Global Advisors，“Mitigating the Risk of DNS Namespace Collisions”（缓和 DNS 域名空间冲突风险），2014 年 6 月 4 日，https://www.icann.org/en/system/files/files/name-collision-mitigation-study-06jun14-en.pdf

[56] 参见《通配符禁用（域名重定向）投诉表》，访问于 2016 年 2 月 11 日，https://forms.icann.org/en/resources/compliance/registries/wildcard-prohibition/form

[57] 但是，合规部已收到一些对“保留名称/控制性中断”的投诉。参见“2016 年 ICANN 合同合规公告板”，访问于 2016 年 2 月 12 日，https://features.icann.org/compliance/dashboard/0116/report

[58] Weaver、Kreibich 和 Paxson，“Redirecting DNS for Ads and Profit”（为做广告和牟利重定向 DNS），USENIX 关于自由和开放的互联网通信 (FOCI) 的研讨会，2011 年，http://www.icir.org/christian/publications/2011-foci-dns.pdf

保护措施：移除孤立粘合记录

背景

此项保护措施的制定，旨在减少恶意行为者通过“孤立粘合”记录将恶意域链接偷偷加入根区的风险。孤立粘合记录是指“父”记录从区域中删除后，可能依然残留的域名服务器记录。孤立粘合记录可使恶意行为者获得对域名服务器的控制，进而能够在看似“正当”的域名中从事恶意活动。例如，“快速通量”攻击就是利用孤立粘合记录在短时间内托管恶意域名。[59]

此项保护措施要求注册管理运行机构在其申请中提供一个计划，用于在父记录移除后立刻移除孤立粘合记录。一旦受到注册管理机构协议的条款约束，注册管理运行机构就必须根据协议中规格 6 第 4.2 节的下述规定，采取措施移除孤立粘合记录：“有书面证据表明某些孤立粘合记录遭恶意使用时…注册管理运行机构应采取措施移除此类记录。。”[60]

定义“有效性”

此项措施的“有效性”可以理解为注册管理机构方面确立常规化做法，为最终用户提供联系人以便其报告滥用情况，并确认当父记录从区域中移除时孤立粘合记录也自动移除。

现状

社群对此问题的初步反馈表明，孤立粘合记录作为滥用来源的情况已通过将它们从域文件中移除的常规做法而大为缓解，尽管在某些情况下它们依然是一个“低级”问题。[61]

数据收集与衡量的可用方法

ICANN 已收到一些初步反馈，建议通过使用域文件长期跟踪孤立粘合记录的删除情况来衡量这一保护措施。

与注册管理运行机构讨论孤立粘合记录用于恶意目的的频率和情况可以提供一个定性指标，用于衡量注册管理机构、注册服务机构和注册人是否有效运用要求的机制来移除孤立粘合记录。要求注册管理运行机构提供“书面证据”，证明其按照规格 6 的要求移除孤立粘合记录，也可提供一个有用的数据来源。此外也可以在注册管理机构的反滥用政策中查找移除孤立粘合记录的建议实例。例如，“.rich”TLD 在

---

[59] 参见 ICANN 安全与稳定咨询委员会《SSAC 关于快速通量托管和 DNS 的咨询报告》，2008 年 3 月，https://www.icann.org/en/system/files/files/sac-025-en.pdf

[60] 参见 ICANN 安全与稳定咨询委员会《SSAC 关于申请人指导手册草案中孤立粘合记录的意见》，2011 年 5 月，https://www.icann.org/en/system/files/files/sac-048-en.pdf

[61] ICANN 运营和政策研究，“针对新 gTLD 项目中防 DNS 滥用的保护措施的审核工作”，2016 年 1 月 28 日，电话会议记录，相关录音位于 https://newgtlds.icann.org/en/reviews/dns-abuse

其反滥用政策中包含专门的一节，阐述孤立粘合记录的移除，[62]而 Afilias 则将这一问题作为快速通量托管的一个要素进行了阐述。[63]

问题：如何确保更集中地打击已经确定的滥用行为？

这个问题从信息的可用性着眼，旨在抑制 DNS 中的滥用活动，并帮助定位 DNS 中已经确定的滥用者。

保护措施：增强型 WHOIS 记录的要求

背景

此项保护措施要求新 gTLD 维护并提供对“增强型 WHOIS”记录的访问权限，以帮助提高 WHOIS 数据的可用性和完整性。增强型 WHOIS 记录是由注册管理机构保管的记录，它“除了包含所属注册服务机构信息和注册状态信息以外，还包含注册人联系信息以及指定管理和技术联系人的信息。”[64]而“减弱型 WHOIS”记录仅存储足以识别所属注册服务机构的信息和注册状态信息，不提供关于注册人的信息。在识别 DNS 中活动的恶意行为者的过程中，使用增强型 WHOIS 记录可进行更加完整和快速的数据搜索。

定义“有效性”

此措施的“有效性”可通过一套增强型 WHOIS 记录的开发来定义，这些记录经常被管理部门用于跟踪、识别和制止恶意行为者在 DNS 中的活动。

现状

每一个新 gTLD 注册管理运行机构，只要其 TLD 已获得授权进入根区，就必须创建和维护增强型 WHOIS 记录，这是其合同义务的一部分。

数据收集与衡量的可用方法

规定新 gTLD 注册管理机构维护增强型 WHOIS 记录背后的意图是创建一套更全面的联系记录，以便于管理部门跟踪和阻止恶意活动。获取 DNS 滥用响应人关于增强型和减弱型 WHOIS 记录在抑制 DNS 滥用中效用的反馈，可以作为评估此项保护措施有效性的一个方法。

其他潜在措施可源自 WHOIS 准确度报告体系 (ARS) 生成的数据，该体系是目前在开发中的一个项目，目标是“以系统性的方式识别和报告准确度，改善 WHOIS 中合

---

[62] “.RICH Anti-Abuse Policy”（.RICH 反滥用政策），访问于 2016 年 2 月 11 日，http://nic.rich/files/policies/rich-anti-abuse-policy.pdf

[63] “Afilias Anti-Abuse Policy”（Afilias 反滥用政策），访问于 2016 年 2 月 11 日，http://dotblue.blue/about/afilias-anti-abuse-policy

[64] ICANN WHOIS，“WHOIS 快速入门”，访问于 2016 年 2 月 11 日，https://whois.icann.org/en/primer

同数据的质量”。[65]下列图表出自 2015 年 12 月公布的第 2 阶段报告，表中按联系方式分别总结了 gTLD 对 2009 注册服务机构认证协议 (RAA) 语法要求的整体准确度，以及 gTLD 对 2009 RAA 可操作性要求的整体准确度：[66]

gTLD 对 2009 RAA 语法要求的整体准确度（按联系方式划分）

	电子邮件地址	电话号码	邮政地址	3 项均准确
3 种联系人类型均准确	99.1% ± 0.2%	83.3% ± 0.7%	79.4% ± 0.8%	67.2% ± 0.9%

gTLD 对 2009 RAA 可操作性要求的整体准确度（按联系方式划分）

	电子邮件地址	电话号码	邮政地址	3 项均准确
3 种联系人类型均准确	87.1% ± 0.7%	74.0% ± 0.9%	98.0% ± 0.3%	64.7% ± 0.9%

WHOIS ARS 研究的三个阶段分别关注语法、准确度和效用，可以为衡量此保护措施的有效性提供一系列间接指标。理论上，更准确的 WHOIS 记录将给反滥用社群提供一个更有用的打击 DNS 滥用的工具。但是，恶意行为者不大可能主动给出“准确的”联系信息。CCT-RT 仍要决定“语法、准确度和效用”是否是衡量此方面有效性的恰当指标。

保护措施：域文件访问的集中化

背景

此项保护措施要求访问凭证可通过一个集中化来源获取注册管理机构域文件数据，这样当在各个 TLD 域内新建了域名时，反滥用社群就能更高效地获取新域名更新。其目的是在 TLD 遭受恶意行为时，减少采取纠正措施所需的时间。

定义“有效性”

此项保护措施的“有效性”可以定义为：集中化域资料服务 (CZDS) 及时高效处理注册管理机构域文件数据请求，从而最大限度地缩短打击恶意活动时的响应时间的能力。

---

[65] 注意，研究的第 3 阶段尚未展开，但预计会关注“身份要求”，测试提供的联系人是否就是实际上负责该域名的个人或实体。“语法要求”定义为 WHOIS 条目的格式。“可操作性要求”定义为通过这些联系人信息能否解析并连接到用户。注意，虽然联系人信息或许可以操作并连接到用户，但 ARS 不会测试该用户是否就是在 WHOIS 记录中所表示的那一个。参见《WHOIS ARS 第 2 阶段第 1 期报告：语法和可操作性准确度》，访问于 2016 年 2 月 1 日，https://whois.icann.org/en/file/whois-ars-phase-2-cycle-1-report-syntax-and-operability-accuracy 和“WHOIS 准确度报告体系 (ARS)”，访问于 2016 年 2 月 11 日，https://whois.icann.org/en/whoisars

[66] 同上。

现状

根据《注册管理机构协议》规格 4 第 2 节，新 gTLD 注册管理机构必须向提出请求的最终用户提供域资料。ICANN 的公开报告显示，仅 2015 年一年就批准了超过 300 万个域文件访问 (ZFA) 密码。[67]为撰写本报告而与安全研究人员进行的交流表明，CZDS 为 DNS 滥用响应人以及那些寻求知识产权保护的用户提供了一个宝贵的服务。然而，尽管 CZDS 的开发是为了使提供域文件访问的流程更加高效，但注册管理机构自身普遍表示对这一服务感到失望。[68]注册管理运行机构仍要对最终用户进行验证，而注册管理机构协议并未规定注册管理运行机构必须在多长时间内响应访问请求。这就导致对注册管理运行机构的请求常常“堆积如山”，难以应付，而在他们方面又对及时响应请求无能为力。一位注册管理机构代表表示，其*每天*都会收到 7,000-10,000 个域文件访问请求。[69]这可能会导致使用条款的履行大打折扣，以及草草验证请求人的凭证。[70]ICANN 合规部指出，第三方通过 CZDS 提出的域文件访问请求是 2015 年注册管理机构合规方面的最大问题之一，其中大多数投诉都和注册管理运行机构不响应域文件访问请求，以及因注册管理机构协议不允许的原因导致注册管理运行机构被拒绝访问有关。[71]

数据收集与衡量的可用方法

“有效性”的一个潜在指标可通过 CZDS 密码报告来衡量，这些报告会显示 CZDS 内的 ZFA 密码（给予请求批量访问域文件的用户）数量以及特定 TLD 和所有 TLD 内每个月批准的密码数量。[72]用户对服务的反馈可能会给这样一个指标提供额外的深度，因为许多用户报告了 CZDS 请求处理的问题（至少是非正式报告）。

---

[67] CZDS ZFA 密码月度报告，访问于 2016 年 2 月 1 日，https://czds.icann.org/en/reports
[68] ICANN 运营和政策研究，“针对新 gTLD 项目中防 DNS 滥用的保护措施的审核工作”，2016 年 1 月 28 日，电话会议记录，相关录音位于 https://newgtlds.icann.org/en/reviews/dns-abuse
[69] 同上。
[70] 同上。
[71] 《ICANN 合同合规性 2015 年度报告》，2016 年 1 月，https://www.icann.org/en/system/files/files/annual-2015-27jan16-en.pdf
[72] CZDS ZFA 密码月度报告，访问于 2016 年 2 月 1 日，https://czds.icann.org/en/reports

保护措施：记录注册管理机构级别的滥用问题联系人和程序

背景

此项保护措施要求注册管理运行机构确立单一联系人负责处理滥用投诉。《申请人指导手册》指示申请人制定一个“在其网站上提供并公布滥用问题单一联系人信息的实施计划，该联系人负责处理需要立即引起注意的问题，并及时回应滥用投诉…”。[73]《注册管理机构协议》规格 6 第 4.1 节陈述：“注册管理运行机构应向 ICANN 提供并在其网站上发布准确详细的联系人信息，包括有效的电子邮件地址、邮寄地址以及处理与 TLD 中恶意行为有关的质询的主要联系人，并应在此类联系人信息发生任何变更时及时通知 ICANN。”[74]

定义“有效性”

此措施的“有效性”可通过这一信息对前端用户的可用性来衡量，并找到一种方式衡量用户举报 DNS 滥用的相对轻松程度。还可采用另一种辅助方法，即，与执法部门和注册管理运行机构面谈，了解他们对此项措施有效性的反馈。

现状

ICANN 合规部对注册管理机构被要求在其网站上发布的滥用问题联系人信息进行了监查，并在其最后一次“合同合规更新”中对此问题的审查做了如下陈述：

> ICANN 一直主动监查注册管理机构根据新注册管理机构协议必须在其网站上公布的滥用问题联系人信息。通过监查，ICANN 确保最终用户（包括但不限于执法机构）能够找到一个联系人来报告 TLD 中存在的恶意活动…ICANN 审查了 64 个索赔期开始日期介于 2015 年 1 月 1 日至 2015 年 3 月 31 日之间的顶级域网站。针对注册管理机构的不合规问询或通知数低于前一轮监查。其中所指出的部分不足如下：完全不显示要求的信息、主要联系人缺失，或者用于举报滥用的邮寄地址缺失。ICANN 将与注册管理机构合作，一起纠正发现的不合规问题。[75]

对此项保护措施的一些初步社群反馈表明，使用滥用问题联系人信息的大多是垃圾邮件发送人。[76]

---

[73]《gTLD 申请人指导手册》，2012 年 6 月 4 日，
https://newgtlds.icann.org/en/applicants/agb
[74]《注册管理机构协议》，2014 年 1 月 9 日，
https://www.icann.org/resources/pages/registries/registries-agreements-en
[75] 参见《ICANN 合同合规信息更新 2015 年 1 月 — 3 月》，
https://www.icann.org/en/system/files/files/compliance-update-mar15-en.pdf
[76] ICANN 运营和政策研究，“针对新 gTLD 项目中防 DNS 滥用的保护措施的审核工作”，2016 年 1 月 28 日，电话会议记录，相关录音位于
https://newgtlds.icann.org/en/reviews/dns-abuse

数据收集与衡量的可用方法

衡量此项保护措施有效性可以采用的一种方法是，分析 ICANN 合规报告和来自使用这些联系信息的用户的证言。还有一种方法可以是，收集注册管理机构滥用问题联系人的信息，并测试其作用。

保护措施：参与注册管理机构加急安全请求流程 (ERSR)

背景

此项保护措施为注册管理运行机构提供了一个机制，使其能够通过建立专门的流程来审查和批准加急安全请求，从而根据对 DNS 的系统性威胁情况采取快速果断的措施。事实上，注册管理机构可以申请合同豁免权，以便在应对某个安全威胁所需的时间内，免受注册管理机构协议中某一规定的限制。这一设计是为了避开威胁，提供运营安全，同时使相关各方始终了解威胁的状态。请注意，这一流程是为应对 Conficker 病毒而确立，因而在为新 gTLD 项目制定保护措施的工作开展之前就已经存在。尽管它没有包含在最新的注册管理机构协议中，但是作为一个流程，可以对当下有明确需求的注册管理机构采用。[77]

定义“有效性”

“有效性”可以定义为采用 ERSR 后，能否快速识别和缓解安全威胁。

现状

鉴于所涉数据的敏感性，ICANN 未公开报告这一流程的细节。但是，为撰写本报告而从安全研究人员处获得的初步意见表明，自 Conficker 病毒出现以来，此保护措施一直被有效用于瓦解后续僵尸网络。

数据收集与衡量的可用方法

为理解此项措施的有效性，可以收集那些申请过 ERSR 流程的用户的反馈，以便了解其处理安全威胁的效能。考虑到对 ERSR 的申请数量有限和流程内部安全数据的敏感性，可将分析重点放在该流程的执行*方式*上，例如采用 ERSR 后威胁解决的速度和相对轻松程度，而不是放在申请 ERSR 的实例数，或者有关如何应对安全威胁的细节上。

[77] 《注册滥用政策工作组最终报告》，2010 年 5 月，http://gnso.icann.org/en/issues/rap/rap-wg-final-report-29may10-en.pdf

问题：如何为本身容易引发恶意行为的 TLD 提供一个增强的控制框架？

保护措施：创建一个高安全区域验证项目框架草案

背景

此*建议* — 它既没有在注册管理机构协议中正式确立为一项保护措施要求，也没有构建成官方的、ICANN 支持的举措 — 提议为那些有意向的注册管理运行机构创建一个自愿参与项目，让它们能够确立并证明其 TLD 具有较高的安全性和可信度。该项目的总体目标是为那些希望脱颖而出的注册管理机构提供一套标准化的做法。[78]

定义“有效性”

此措施的“有效性”可以视为在恶意活动发生概率较高的 TLD（例如代表银行/金融和医药行业的 TLD）中，对高安全区域 (HSZ) 的成功采用、实施和验证。

现状

尽管对于这样一个项目，尚未通过 ICANN 的各种政策制定和实施机制正式形成一个综合的框架草案，但是已经有一些工作把目标放在满足对某些字符串日益高涨的安全需求上。

根据申请人指导手册问题 30 的指导原则，在新 gTLD 的申请流程中会评估申请人在敏感字符串方面的安全策略。该指导原则要求申请人

> …为计划建立的注册管理机构提供一份安全策略摘要，其内容包括但不限于…描述与所申请的 gTLD 字符串性质相适应的任何扩增的安全级别或功能，其中包括认同申请人承诺遵守的任何当前的国际或行业相关安全标准…[79]

此外，ICANN 的政府咨询委员会已建议创建一个模型，用于验证和确认作为严格监管行业中公众利益承诺 (PIC) 的注册管理运行机构凭证，以便建立和维护这些域的可信度。[80]

---

[78] icann.org，“公众意见：高安全区域顶级域最终报告”，2011 年 3 月 11 日 https://www.icann.org/news/announcement-2011-03-11-en

[79]《gTLD 申请人指导手册》，2012 年 6 月 4 日，https://newgtlds.icann.org/en/applicants/agb

[80] 参见“GAC 公报 — 阿根廷布宜诺斯艾利斯”，2015 年 6 月 24 日，https://www.icann.org/news/announcement-2-2015-06-24-en 和“GAC 公报 — 爱尔兰都柏林”，2015 年 10 月 21 日，https://www.icann.org/news/announcement-2015-10-22-en

此外，行业协会和注册管理机构方面也采取了一些独立的行动来提高新 gTLD 的安全性和诚信度。例如，fTLD Service, LLC 注册管理机构自行为其 TLD“.bank”和“.insurance”建立了一个高安全区域。[81]“DNS Seal 项目”力求通过自我规范和确定最佳实践在域名行业中树立诚信，帮助互联网用户识别可信赖的网站。[82]

数据收集与衡量的可用方法

通过收集注册管理运行机构的反馈，了解它们为何不愿进行 HSZ 验证，可以透视出这一建议保护措施乏人问津的深层原因。此外，与 fTLD Service, LLC 注册管理机构对话，了解他们选择自行建立 HSZ 的原因，也可提供一个额外的信息来源。

研究方案及模型

在考虑 DNS 通过新 gTLD 项目出现的扩张与 DNS 中滥用和犯罪行为的盛行率之间的关系时，出现了一些重要的**实证性谜题**。一些重大疑问依然存在，包括：新 gTLD 项目是否造成了 DNS 滥用增加，且该增加*与该项目促成的 DNS 规模扩大成正比*，以及至关重要的一个问题 — **提出的缓和保护措施是否能有效实现预期目标**。但是，目前专注于 DNS 滥用的文献几乎全都出自依赖描述性统计数据和集中探索具体 DNS 滥用活动的研究，都明显缺乏视野开阔的、采用多元化推理统计分析方法的纵向研究做支撑。

为了对新 gTLD 中的 DNS 滥用情况得出一个全面的认识，并评估缓和保护措施的有效性，本报告提出了一个**由假设驱动**的因果分析，将保护措施作为干预变量运用到一系列假设模型中。这些假设模型建立在合理推测新 gTLD 项目保护措施和 DNS 中滥用行为盛行率之间关系的基础上。模型集中回答一个中心研究问题：

> 为缓和新 gTLD 中的 DNS 滥用情况而提出的保护措施可以在多大程度上影响 DNS 中滥用行为的比例？

要全面地、科学合理地回答这个问题，需要建立一个可以测试的假设模型并分段进行调查，适当地专注于传统和/或新 TLD，和/或整个 DNS 空间。它要求建立一个**基线指标**作为出发点，回答新 gTLD 项目是否造成了 DNS 滥用增加，且该增加*与 DNS 本身的扩张成正比*这一根本问题。一旦确定了这一指标，我们就可以开始提出**一些问题，把重点放在 DNS 扩张的“前保护措施”时代与“后保护措施”时代的滥用率比较上。**这样，研究人员就能够结合大背景，来研究这九项保护措施与当前 DNS 滥用率之间的潜在关系。[83]

---

[81] 参见 fTLD Registry Services，“Enhanced Security”（加强安全），访问于 2016 年 2 月 11 日，www.ftld.com/enhanced-security/

[82]“About the DNS Seal Project”（关于 DNS Seal 项目），访问于 2016 年 2 月 12 日，http://dnsseal.wiki/About_the_DNS_Seal_Project

[83] 注意，这一将目前和“前-新 gTLD 时代”传统 TLD 的滥用率与新 gTLD 中的滥用率进行比较的方法是单独提出的，并且在关于衡量 DNS 滥用和九项保护措施有效

以下模型同时适合定性和定量测试方法。不过，正如上文所述，许多保护措施不会产生进行可靠统计分析所需的足够定量数据。有两种途径可解决此问题，即：挖掘衡量保护措施有效性的潜在间接指标，以及采用定性分析方法 — 例如用户反馈访谈、焦点小组、回顾相关出版物 — 以便增加实证深度，在更广的范围内探寻在采用保护措施的背景下可用的定量分析方法。

测试保护措施有效性的可用定性框架

本提案以及下列模型阐述了为促进对最有效测试方法（用于测试缓和 DNS 滥用的保护措施的有效性）的讨论，首先应采取的步骤。CCT-RT 仍要决定其 DNS 滥用缓和措施调查工作的范围和方法。

研究设计：关键问题和考量

有大量潜在数据 — 不管是定性数据还是定量数据 — 可能可以用于研究缓和 DNS 滥用的九项保护措施的有效性。但是，在决定采用哪些数据之前，必须敲定一个组织数据并实现审核目标的研究设计。任何研究设计都必须回答以下问题：[84]

1. 明确研究问题。我们试图解决的实证性谜题是什么？
2. 回顾并综合曾经出版的与此问题相关的文献。
3. 清楚明确地说明研究问题和/或研究问题的中心假设。
4. 有效描述充分回答研究问题和/或测试假设所需的数据，并解释如何获取这些数据。
5. 描述有待用于分析数据以判定假设真假的方法。

下面结合 DNS 滥用审核的背景一一回答这些问题：

1. 明确研究问题。我们试图解决的实证性谜题是什么？

   研究问题：尚不清楚这些保护措施对缓和新 gTLD 中 DNS 滥用问题的有效性如何。
   实证性谜题：一些指标表明整个 TLD（传统和新）中 DNS 滥用问题减少，还有一些指标表明在某些 TLD 中滥用数量增加。用于缓和 DNS 滥用的保护措施在这一差异出现的过程中发挥了多大作用尚不清楚。

性的电话会议上受到了许多参与者青睐。参见 ICANN 运营和政策研究，“针对新 gTLD 项目中防 DNS 滥用的保护措施的审核工作”，2016 年 1 月 28 日，电话会议记录，相关录音位于 https://newgtlds.icann.org/en/reviews/dns-abuse

[84] 摘自南加州大学的研究问题简明清单：http://libguides.usc.edu/writingguide/researchdesigns（访问于 2016 年 2 月 26 日）。

2. 回顾并综合曾经出版的与此问题相关的文献。

   本报告旨在提供这一回顾与综合。

3. 清楚明确地说明研究问题和/或研究问题的中心假设。

   研究问题：什么原因可以解释不同 TLD 中滥用率的差异？为缓和它们而提出的保护措施在多大程度上有效？

   假设示例（参见下文的模型，深入探究决定性假设关系）：
   - 高级别（指导整个审核或绝大部分审核）：
     - DNS 的扩张已造成 DNS 滥用数量*增加*，但与扩张本身不成正比。
   - 低级别（指导审核中调查的特定部分）：
     - 旨在防止 Y 形式的 DNS 滥用的 X 保护措施不能有效实现预期目标。

   研究问题和假设也应表明每个术语如何定义和/或衡量。例如，如上文所述，我们如何衡量保护措施的“有效性”？

4. 有效描述充分回答研究问题和/或测试假设所需的数据，并解释如何获取这些数据。

   例如，保护措施的“有效性”可以通过与专家和保护措施的使用者交谈来进行定性衡量。新 gTLD 项目在多大程度上造成了 DNS 滥用则可通过考察新域数和 DNS 滥用间接指标（例如网络钓鱼率）之间的统计相关性来量化。

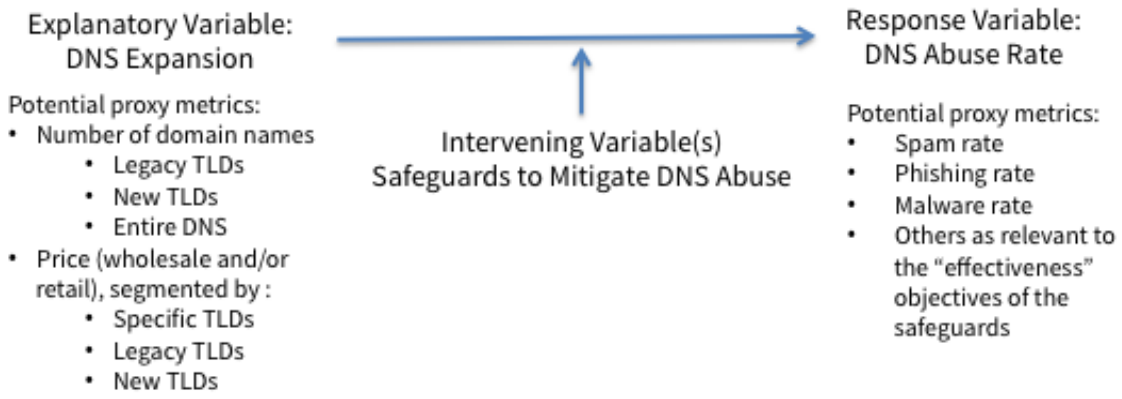
5. 描述有待用于分析数据以判定假设真假的方法。

   这个问题除了取决于上述研究问题和假设的定义外，还取决于 CCT-RT 的工作。

因果模型和假设

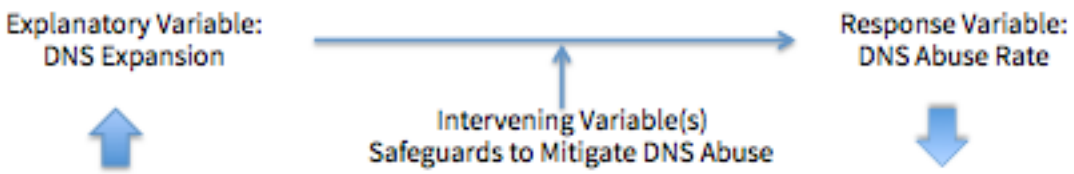
以下模型源于一个简单的中心假设，即：为防止新 gTLD 中的 DNS 滥用问题而引入保护措施，将带来一个比没有采用这些保护措施的“传统”TLD 时代“更洁净”（即更少恶意活动）的 DNS 空间（至少理论上是如此）。

基础模型



从这一基础模型衍生出三个可测试的假设情景：

模型 1：DNS 扩张导致 DNS 滥用比例*减少*
（有效保护措施假设）

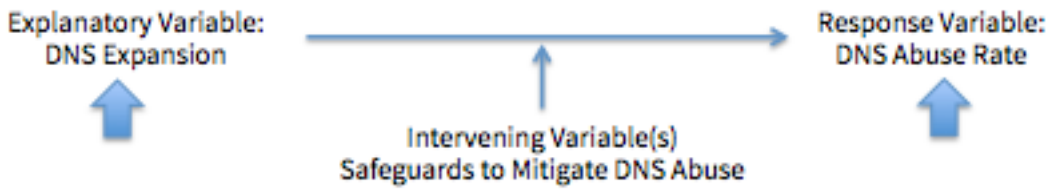


研究问题：DNS 滥用比例*减少*在多大程度上可以用有效保护措施来解释？

假设 1：DNS 扩张“采取了保护措施”可以作为一个成因，用来解释 DNS 滥用在新 TLD 和/或传统 TLD、和/或整个 DNS 中比例**减少**这个结果（适当按新 TLD 和/或传统 TLD、和/或整个 DNS 进行分段分析）。

假设 1.1：为缓和 DNS 滥用而提出的保护措施**有效**实现了其预期目标，并且可以作为成因，用来解释 DNS 滥用比例减少这个结果（适当对个别保护措施进行分析）。

模型 2：通过新 gTLD 项目实现的 DNS 扩张导致 DNS 滥用比例*增加*
（无效保护措施假设）

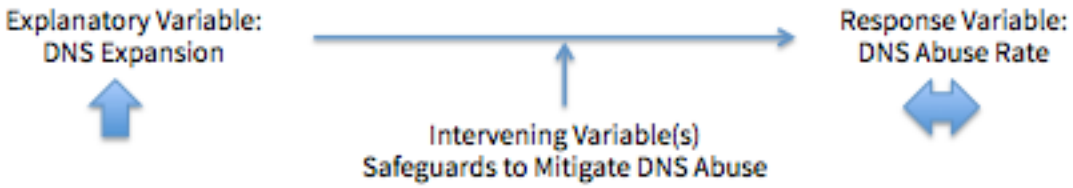


研究问题：DNS 滥用比例*增加*在多大程度上可以用无效保护措施来解释？

假设 2：DNS 扩张“采取了保护措施”可以作为一个成因，用来解释 DNS 滥用在新 TLD 和/或传统 TLD、和/或整个 DNS 中比例**增加**这个结果（适当按新 TLD 和/或传统 TLD、和/或整个 DNS 进行分段分析）。

假设 2.1：为缓和 DNS 滥用而提出的保护措施**未能有效**实现其预期目标（适当对个别保护措施进行分析）。

模型 3：DNS 扩张对 DNS 滥用*没有影响*
（无效保护措施假设）



研究问题：DNS 滥用*缺乏变化*在多大程度上可以用无效保护措施来解释？

假设 3：DNS 扩张“采取保护措施”对滥用行为在新 TLD 和/或传统 TLD、和/或整个 DNS 中的比例没有影响（适当按新 TLD 和/或传统 TLD、和/或整个 DNS 进行分段分析）。

假设 3.1：为缓和 DNS 滥用而提出的保护措施**未能有效**实现其预期目标，提供一个比传统空间“更安全”的新 gTLD 空间（适当对个别保护措施进行分析）。

就 CCT-RT 的工作而言，此研究方案提供了一个可用的方法，来组织对缓和 DNS 滥用的九项保护措施的有效性调查。采用这一方法可能需要聘请具有统计和定性数据收集分析专长，能够建立和开展实际研究的外部供应商。CCT-RT 仍要决定所有分析的范围和方法。在没有其他材料的情况下，可以从本研究方案出发，讨论其他可用的方法。

附录：对在 ICANN 进行的滥用相关活动的调查

项目	范围	资料来源和链接
注册管理机构协议规格 11	第 3a 节：“注册管理运行机构将在其注册管理机构-注册服务机构协议中纳入如下规定，要求注册服务机构在其注册协议中禁止注册域名持有者散布恶意软件、滥用僵尸网络、网络钓鱼、盗版、商标或版权侵权、诈骗或欺骗、造假以及以其他方式从事违反适用法律的活动，并（依据适用法律和任何相关程序）注明这些行或活动会带来的后果，包括暂停域名的使用。” 第 3b 节：“注册管理运行机构应定期进行技术分析，评估 TLD 中的域是否被用于威胁网络安全的行为，例如网址嫁接、网络钓鱼、恶意软件和僵尸网络等。注册管理运行机构将编制统计报告作为定期安全检查的结果，并在报告中记录所发现的安全威胁的数量以及所采取的措施。注册管理运行机构将在协议期间保存这些报告（除非法律要求或 ICANN 批准保存更短时间）并根据要求提供给 ICANN。”	资料来源：注册管理机构协议 链接：注册管理机构协议 链接：常见问题与解答：新 gTLD 注册管理机构协议（修订后）规格 11
SSR 审核小组建议 11	建议 11：“ICANN 应该最终落实并执行对以下方面所取得成绩的衡量，即与 SSR 相关计划目标明确关联的新 gTLD 和 IDN 快速通道，其中包括对减少域名滥用的机制的有效性衡量。”	资料来源：DNS 安全、稳定与弹性审核小组 链接：DNS 安全、稳定与弹性审核小组的最终报告
政府咨询委员会 (GAC) 建议：ICANN53 和 ICANN54	ICANN53 布宜诺斯艾利斯公报：“GAC…建议…ICANN 社群可制定一种协调的方法，在评估新 gTLD 项目时，同时评估遭到滥用的域名数量。” ICANN54 都柏林公报：“GAC 建议并敦促董事会…制定并采纳一种协调的方法，向 ICANN 社群报告新 gTLD 项目开展过程中出现的滥用行为（例如，恶意软件、僵尸网络、网络钓鱼、网域嫁接、盗版、商标和/或版权侵权、伪造、欺诈行为和其他非法行为）的程度和持续性。”	资料来源：ICANN 政府咨询委员会 链接：ICANN53 GAC 公报，布宜诺斯艾利斯 链接：ICANN54 GAC 公报，都柏林
SSAC 注册人保护公告：凭证管理生命周期内安全性和稳定性维护的最佳实践	建议 1：“作为常规报告的一部分，ICANN 合规部应公布注册服务机构按照 2013 注册服务机构认证协议 (RAA) 第 3.20 段的规定所报告的安全违规的相关数据。” 建议 2：“与 2013 RAA 第 3.20 段类似的规定应纳入到未来所有的注册管理机构合同中，并要参照上述建议 1 公布类似的统计结果。”	资料来源：安全与稳定咨询委员会 链接：SAC074 公告

gTLD 市场健康指数	ICANN 开发了一套候选概念供社群讨论，以助其创建一个专注于 (i) 良性竞争 (ii) 消费者信任和 (iii) 非技术型稳定性的 gTLD 市场健康指数。 这些概念的提出旨在促使社群就全球 gTLD 市场“健康”的含义展开讨论。预计在这一社群讨论中会产生一些可衡量因素，可以用作 gTLD 市场的关键绩效指标。 其中有几个概念是针对此处所述的 DNS 滥用。	资料来源：ICANN 员工 链接：gTLD 市场健康指数提案：征求意见并征召志愿者