
DNS 滥用问题缓解

第 5.1 次会议

目录

| | |
|------------------------------------|----|
| 背景 | 2 |
| 问题 | 3 |
| 领导团队关于 GAC 行动的提议 | 4 |
| 相关工作进展 | 5 |
| DNS 滥用的定义：是否已就基础设施滥用达成共识？ | 5 |
| DNS 滥用的定义：消费者保护部对话 | 6 |
| 意识和透明度：GAC 主导的社群合作 | 7 |
| 意识和透明度：DNS 滥用问题研究 | 8 |
| 意识和透明度：域名滥用活动报告 (DAAR) | 8 |
| 有效性：注册管理机构和注册服务机构合同中的当前 DNS 滥用保护措施 | 9 |
| 有效性：注册管理机构回应安全威胁的非约束性框架 | 10 |
| 有效性：采取积极措施和防止系统性滥用 | 10 |
| 现状 | 11 |
| 主要参考文档 | 12 |

会议目标

- 回顾最近关于 DNS 滥用的定义、检测和缓解所开展的工作和所进行的讨论，以及为使 WHOIS 符合 GDPR 规定而采取的措施所产生的影响。
- 探讨 GAC 公共安全工作组 (PSWG) 和 GAC 就 DNS 滥用缓解问题所持的立场和可能的后续工作内容。

背景

互联网上的恶意活动通过利用互联网和 DNS 生态系统各个方面（包括协议、计算机系统、个人和商业交易、域名注册流程等）的漏洞，对域名注册人和最终用户造成威胁和不利影响。其中有些恶意活动可以威胁到 DNS 基础设施，乃至整个 DNS 的安全性、稳定性与弹性。

在 ICANN 社群内，这些威胁和恶意活动统称为“DNS 滥用”。一般而言，可以将“DNS 滥用”理解为包含所有或部分互联网恶意活动，例如，分布式拒绝服务攻击 (DDoS)、垃圾邮件、网络钓鱼、恶意软件、僵尸网络以及传播非法内容。虽然所有人似乎都认为滥用是一个问题并且应该予以解决，但是对于谁应该负责解决这些问题，仍存在许多意见分歧。注册管理机构和注册服务机构特别担心被要求承担更多责任，因为这会影响到他们的商业模式和盈亏底线。

应当指出的是，在本次讨论中，即使是“DNS 滥用”的确切定义，也将是一个争辩的主题¹。

不过，这项工作在过去几年中已经取得了一些进展。下面总结了 ICANN 社群以前为解决 DNS 滥用问题所采取的各项措施，其中有些措施得到了 GAC 的大力协助：

- ICANN 通用名称支持组织 (GNSO) 在 2008 年成立了[注册滥用政策工作组](#)。该工作组明确了一系列具体问题，但是未实现任何政策成果，后续也没有在相应场合（包括[ICANN 第 41 届会议](#)和[ICANN 第 42 届会议](#)期间举办的研讨会）讨论可供注册管理机构和注册服务机构借鉴的[非约束性最佳实践](#)。
- 在新通用顶级域项目中，ICANN 组织根据[《恶意行为的缓和措施》](#)备忘录（2009 年 10 月 3 日）实施了一系列新要求²。ICANN 最终在[《ICANN 关于新通用顶级域项目保护措施的报告》](#)（2016 年 7 月 18 日）中对这些要求的有效性进行了评估，以便为章程规定的审核（即 CCT 审核）做准备。
- 在 GAC 公共安全工作组 (PSWG) 成立之前，由[执法机构 \(LEA\) 代表](#)指导 2013 年《注册服务机构认证协议》的磋商事宜³，这些代表也在制定有关安全威胁的 GAC 建议的过程中发挥了指导作用，这项工作取得的成果是在明确了注册管理机构职责的《新通用顶级域注册管理机构基本协议》中新增了一些条款。随后又通过 ICANN 组织、注册管理机构和 PSWG 之间经过磋商确定的非约束性[注册管理运行机构应对安全威胁的框架](#)（2017 年 10 月 20 日）对这些条款进行了补充。
- 安全与稳定咨询委员会 (SSAC) 向 ICANN 社群提出了相关建议，特别是[SAC038: 注册服务机构滥用问题联系人](#)（2009 年 2 月 26 日）和[SAC040: 防止域名注册服务遭到非法利用或滥用的保护措施](#)（2009 年 8 月 19 日）

¹ [GDD 峰会](#)（2019 年 5 月 7 日 - 8 日）期间进行的[DNS 滥用和消费者保护](#)讨论即是如此

² 审查注册管理运行机构、要求展示 DNSSEC 部署计划、禁止使用通配符、在从区域中删除域名服务器条目的同时删除相应的孤立粘合记录、要求维护详尽 WHOIS 记录、对域文件访问进行集中管理、要求记录注册管理机构级别的滥用问题联系人和相关流程

³ 请参阅[执法机构尽职调查建议](#)（2009 年 10 月）和[12 项执法机构建议](#)（2012 年 3 月 1 日）

- **ICANN 组织旗下的安全、稳定与弹性 (SSR) 小组**定期为公共安全社群提供[培训](#)，并协助其应对大规模的网络安全事故，包括采用[注册管理机构安全请求快速处理流程 \(ERSR\)](#)。最近，ICANN 首席技术官办公室发起了[域名滥用活动报告 \(DAAR\)](#) 项目，旨在编制月度滥用报告。这个工具得到了 GAC 和一些特定审核小组的大力支持，他们认为该工具可以帮助实现透明度和识别问题根源，进而便可以通过合规或制定新政策（如有需要）来解决问题。

问题

由于以前采取的措施尚未有效减少 DNS 滥用问题，因此，显然我们还有很多工作要做。虽然 DNS 滥用问题得到了 ICANN 社群的广泛关注，并且现在已经制定了用于缓解 DNS 滥用问题的行业最佳实践，但是由 GAC 主导的社群合作以及 CCT 对[通用顶级域 \(gTLD\) 中域名系统 \(DNS\) 滥用的统计数据](#)分析进行的审核（2017 年 8 月 9 日）仍然凸显了一些趋势，包括滥用问题居高不下、易引发滥用问题的商业行为屡禁不止，这些趋势表明“还可以进一步扩展和增强当前的缓解措施和保护措施”，同时也表明今后有可能需要制定新政策⁴。

此外，随着欧盟《通用数据保护条例》(GDPR) 的生效，以及为使 WHOIS 系统（一种重要的犯罪和滥用行为调查工具）符合 GDPR 规定而采取的种种措施的出台，执法机构、网络安全、消费者保护，以及知识产权保护等领域的相关人员愈加担心是否能够有效缓解 DNS 滥用问题⁵。

据 ICANN 合同合规部和消费者保护部的报告显示，在此背景下，ICANN 咨询委员会（尤其是 GAC、SSAC 和 ALAC）和众多受影响的第三方纷纷要求 ICANN 组织和 ICANN 社群采取进一步行动⁶。

为了采取进一步的行动，ICANN 社群需要就一些未解决的问题达成某种形式的共识。ICANN 社群通常围绕以下几方面展开有关滥用问题缓解和潜在政策工作的讨论：

- **DNS 滥用的定义：**
鉴于 ICANN 的职权范围，及其与注册管理机构和注册服务机构签署的合同，哪些行为可构成滥用？
- **DNS 滥用行为检测和举报（从意识和透明度角度）：**
如何确保能够检测出 DNS 滥用行为，并让利益相关方（包括消费者和互联网用户）知晓 DNS 滥用行为？
- **DNS 滥用行为预防和缓解措施（从有效性角度）：**
ICANN 组织、相关行业人员，以及其他利益相关方可以使用哪些工具和流程来减少滥

⁴ 请参阅 GAC 有关 [gTLD 中 DNS 滥用的统计数据](#) 最终报告的 [评议](#)（2017 年 9 月 19 日）。

⁵ 请参阅《GAC 巴塞罗那公报》（2018 年 10 月 25 日）第 III.2 节和 IV.2 节，其中援引了注册目录服务 (RDS) 审核小组 [报告草案](#)（2018 年 8 月 31 日）第 5.3.1 节，以及反网络钓鱼工作组与信息传递、恶意软件和移动反滥用工作组联合 [报告](#)（2018 年 10 月）中有关对执法机构的影响调查

⁶ 请参阅 [GDD 峰会](#)（2019 年 5 月 7 日 - 8 日）期间进行的 [DNS 滥用和消费者保护](#) 讨论

用行为并在滥用行为发生后有效应对？对于预防和缓解 DNS 滥用行为，应该由谁负责哪一方面的工作？各相关方如何开展最为有效的合作？

GAC 一直在为增强互联网的安全性和稳定性，进而保障所有互联网用户的利益而努力，为此，GAC 希望能够积极参与并推进有关上述问题的讨论，以便最终可以找到更行之有效的滥用行为预防和缓解措施。

领导团队关于 GAC 行动的提议

在 ICANN 第 65 届马拉喀什会议期间，GAC 希望：

1. 制定相应流程以明确哪些情况构成 DNS 滥用（在符合 ICANN 使命的前提下），并确定自己对于此问题的立场。这将有助于推进 ICANN 社群内正在进行的多个方面的讨论，包括 DNS 滥用的定义、CCT 审核小组关于 DNS 滥用的建议和 ICANN 董事会对这些建议的审议，以及 ICANN 消费者保护部当前正在推行的相关举措。
2. 考虑是否存在制定政策的需求和机会，在考虑这一问题时会考量近期在 GDD 峰会期间开展的有关政策制定可能性的讨论⁷，并指明 GAC 之前在此问题上所持有的立场⁸。
3. 审议针对与 DNS 滥用有关的 CCT 审核建议（建议 14 至 19）所采取的行动，包括 ICANN 董事会对这些建议的审议和 ICANN 董事会指示 ICANN 组织开展的相应工作，以及由相关 ICANN 选区和流程进一步开展的审议工作。
4. 考虑展示 ccTLD 域名空间的行业最佳实践（例如，在 ICANN 第 64 届会议期间展示的 .DK 域名空间行业最佳实践⁹），并思考如何将其应用到 gTLD 领域。

⁷ 请参阅 [GDD 峰会](#)（2019 年 5 月 7 日 - 8 日）期间进行的 [DNS 滥用和消费者保护](#) 讨论

⁸ 尤其需要注意的是，GAC 在针对 [gTLD 中 DNS 滥用的统计分析](#) 最终报告的 [评议](#)（2017 年 9 月 19 日）中，表示

- “这项 DNS 滥用调查简要说明了一项调查结果，即，在传播虐童材料方面，某些 URL 被更为广泛的使用[...]如果该报告能够为这项调查结果提供更加清晰详尽的解释和/或相应的量化分析，这会有助于利益相关方更好地了解该调查对此问题的调查详尽程度，并为今后可能需要开展的政策工作提供指导信息”
- “制定更加严格的注册政策与减少滥用数量这两者之间存在的相互关联表明今后可能需要制定政策的方面。”
- “统计分析应该为今后制定 DNS 滥用应对政策提供有用信息，而且应该进一步分析并考虑统计分析信息可以如何促进 ICANN 组织及其合同合规部和安全部门采取有效措施来应对 DNS 滥用，并更好地预防滥用行为，避免在今后反复出现。”

⁹ 请参阅 [经验分享会：.DK 如何成功减少域名滥用](#)（2019 年 3 月 13 日），以及随后 [由 PSWG 开展的讨论](#)（2019 年 4 月 17 日）

相关工作进展

DNS 滥用的定义：是否已就基础设施滥用达成共识？

正如在最近的 [GDD 峰会](#)（2019 年 5 月 7 日 - 9 日）中着重指出的那样，社群范围内还未就哪些情况构成“DNS 滥用”达成共识，其中部分原因在于有些利益相关方担心 ICANN 可能会逾越其职责范围，并且担心这会对用户权利和签约方的盈亏底线造成影响¹⁰。

但是，CCT 审核小组表示，社群已经就哪些情况可构成“DNS 安全性滥用”或“DNS 基础设施安全性滥用”达成了共识，统一将其理解为包含“更具有技术含量的恶意活动形式”，例如恶意软件、网络钓鱼、僵尸网络，以及“用作其他滥用形式的传递方法”的垃圾邮件¹¹。

最近，在有关注册管理机构和注册服务机构合同条款实施审核的函件中，ICANN 合同合规部使用了“DNS 基础设施滥用”，其中，该部门使用了[《新 gTLD 注册管理机构协议》](#)（规范 11 3b）中提到的“诸如网址嫁接、网络钓鱼、恶意软件和僵尸网络等安全威胁”¹²，和[《注册服务机构认证协议》](#)（第 3.18 节）中提到的“滥用问题联系人”和“滥用报告”（该协议并未明确规定“滥用”的定义，但是将“非法活动”归属为滥用）。

在 GAC 看来，《新 gTLD 注册管理机构协议》中给出的“安全威胁”定义实际上与[《北京公报》](#)（2013 年 4 月 11 日）中适用于所有新通用顶级域 (NgTLD) 的 GAC 保护建议“安全检查”中的定义别无二致。

董事会于 2019 年 3 月 1 日通过了一项[决议](#)，该决议要求 ICANN 组织“促进社群确定‘滥用’的定义，进而确定针对此建议的后续行动。”¹³，并要求促进 ICANN 组织消费者保护部开展相关活动，继此之后，预计将在 ICANN 第 66 届蒙特利尔会议（2019 年 11 月 2 日 - 7 日）召开之前围绕滥用的定义展开更多讨论。

¹⁰ “滥用缓解”的定义确实可能会对 ICANN 政策和合约所涵盖的活动范围造成影响。政府和其他利益相关方关注的是 DNS 滥用对公共利益造成的不利影响，包括公共安全和知识产权侵犯，而注册管理机构和注册服务机构更关心的是 DNS 滥用的定义是否会限制其商业活动和竞争力，提高其运营成本，并加大注册人对滥用域名采取行动后所需承担的责任。而非商业利益相关方团体关心的是是否会侵犯注册人和互联网用户的言论自由权和隐私权，与此同时，与签约方相同，该团体也担心 ICANN 会僭越其使命所涵盖的职责范围。

¹¹ 请参阅 [CCT 审核最终报告](#)（2018 年 9 月 8 日）第 88 页

¹² [公告：《新 gTLD 注册管理机构协议》规范 11 \(3\)\(b\)](#)（2017 年 6 月 8 日）将“安全威胁”定义为包含“网址嫁接、网络钓鱼、恶意软件、僵尸网络及其他形式的安全威胁”。

¹³ 请参阅[董事会就 CCT 审核最终建议所采取的行动](#)记分卡第 5 页

DNS 滥用的定义：消费者保护部对话

2017 年，ICANN 合同合规部职能扩张，将消费者保护部纳入其职能范围¹⁴，在此之后，GAC 参与了多项相关发展工作：

- ICANN 消费者保护主管的[介绍会](#)（2017 年 6 月 27 日），该会议的讨论事项为：在社群范围内建立非正式讨论机制，以提高意识，增强了解，并找到有助于 ICANN 组织改善合同合规部和消费者保护部部门绩效的方法。
- 由合同合规部和消费者保护部举办的[网络研讨会](#)（2017 年 9 月 25 日），近 100 位社群成员出席了此次会议，会议讨论了 [ICANN 职权范围内的保护措施汇总报告](#)（2017 年 9 月 11 日），之后与会者提交了问题以征询社群意见，相关内容随后发布在一篇[博客文章](#)（2017 年 10 月 11 日）中：
 - ICANN 在解决 DNS 滥用问题中应发挥怎样的作用？
 - DNS 滥用的涵盖范围与 ICANN 在解决此问题上所具有的职权范围之间是否存在差距？
 - 还有哪些工具或数据可以帮助评估 DNS 滥用？
 - 自愿措施可以在哪些领域发挥作用？
 - 为解决滥用问题，ICANN 应如何与其他利益相关方展开合作？
 - 如果 ICANN 社群无法圆满地解决 DNS 滥用问题，是否会引发政府介入的风险？
- [在华盛顿哥伦比亚特区召开的社群代表会议](#)（2019 年 1 月 11 日），会议旨在进一步讨论相关问题，以帮助社群在今后的 ICANN 会议期间广泛参与相关讨论。

最近，在 [GDD 峰会](#)（2019 年 5 月 9 日）期间，合同合规部和消费者保护部主持了一场[会议](#)，目的在于推进目前正在进行的对话：

- 一些签约方认为他们采取的自愿反滥用措施并无任何不当之处，并反对强制要求其**采取措施**，部分原因在于 ICANN 职权范围存在的限制，以及由不具操作可行性的滥用报告所带来的负担（这些报告的提交者通常并不了解注册管理机构¹⁵和注册服务机构只能采取有限的缓解措施）。
- 其他代表表示，**ICANN 有责任制定规则和适当的奖惩机制**，以便在不伤害遵纪守法的行动主体的前提下阻止不法分子实施不当行为（“**污染者支付**”原则），而且 ICANN 应当在相关报告中**指明滥用行为的责任方**。
- **ICANN 组织提出了 GNSO 政策制定流程的想法**，目的在于让合约内容符合咨询委员会和第三方的期望，并阻止相关方今后采取用于取代 ICANN 政策的不同法规。

¹⁴ [聘用 ICANN 消费者保护主管](#)（2017 年 5 月 23 日），该职位的职责是“提高利益相关方对 ICANN 当前采取的保护措施的认识，并促进各利益相关方讨论能够帮助 ICANN 改善其保护机制的更多方法”

¹⁵ 有关示例，请参阅自愿性的[《注册管理运行机构安全威胁回应框架》](#)中所包含的“注册管理机构为应对安全威胁可采取的措施类别”

- 上述观点遭到了强烈反对，为此，有人提议寻找解决此问题的其他方法，包括协调社群中各利益相关方当前所采用的不同定义，或者启动《注册管理机构协议》磋商（曾为 2013 年《注册服务机构认证协议》启动过类似的磋商）。
- 签约方请求 ICANN 组织在 ICANN 第 66 届蒙特利尔会议期间作为签约方代表对 ICANN 社群进行指导，包括展示最佳实践，并提供相应数据以展示普遍存在的不具操作可行性的投诉。

意识和透明度：GAC 主导的社群合作

在过去几年中，GAC 及其公共安全工作组 (PSWG) 在 ICANN 会议期间主办了多次跨社群合作活动，旨在增强参与意识并与相关专家共同探索解决方案，其中最主要的活动包括：

- 在海得拉巴举行的 ICANN 第 57 届会议（2016 年 11 月 5 日）期间，GAC PSWG 召开了一次关于 [gTLD 滥用问题缓解](#) 的高关注度主题会议，旨在促进 ICANN 社群之间的意见交流，此外，这次会议还强调了以下几点：
 - 对哪些行为构成 DNS 滥用缺乏共识；
 - 影响滥用问题缓解方法的商业模式、实践和技能具有多样性；以及
 - 需要加强行业范围的合作，通过共享安全威胁相关数据提供支持。
- 在哥本哈根举行的 ICANN 第 58 届会议（2017 年 3 月 13 日）期间，GAC PSWG 召开了一次内容为[有效缓解 DNS 滥用：预防、缓解和应对](#)的跨社群会议，在这次会议中，讨论了 DNS 滥用的最新趋势，尤其是网络钓鱼，以及跨注册服务机构和顶级域的域名跳跃等行为。要抵制这些行为，需要行业内部对这些行为做出更为协调一致、更精确的响应。此外，此次会议还强调了：
 - 最近发起的[域名滥用活动报告 \(DAAR\)](#) 项目；
 - ICANN 组织合同合规部与 SSR 职能之间应持续开展合作；以及
 - 利用[新 gTLD 拍卖收益](#)，为滥用问题缓解工作提供所需资金
- 在阿布扎比举行的 ICANN 第 60 届会议（2017 年 10 月 30 日）期间，PSWG 举办了一次关于 [DNS 滥用问题基于事实的政策制定和有效缓解工作报告](#) 的跨社群会议，讨论了以下事宜：制定一个公开可靠和切实可行的 DNS 滥用问题报告机制，以便用于滥用预防和缓解，并采取基于事实的政策制定流程。这次会议还确认了需要将[域名滥用活动报告 \(DAAR\)](#) 工具中包含的关于 DNS 滥用问题的详细可靠数据公之于众。除此之外，PSWG 还考虑制定更多切实可行的 GAC 原则¹⁶。

¹⁶ 请参阅附件 1: [ICANN60 关于 DNS 滥用问题的 GAC 简报](#) 中的滥用问题缓解原则，以及 [GAC 阿布扎比公报](#) 中的会议报告（第 3 页）

意识和透明度：DNS 滥用问题研究

根据 ICANN 组织在其关于[缓解恶意行为](#)的备忘录（2009 年 10 月 3 日）中纳入的新要求，以及 GAC 提出的关于安全保护的[保护措施建议](#)¹⁷，该工作组在新通用顶级域项目中加入了许多 DNS 滥用预防保护措施。

根据 ICANN 组织对这些[新通用顶级域项目保护措施](#)（2016 年 7 月 18 日，GAC 于 2016 年 5 月 20 日对这些保护措施提出了[评议](#)）有效性进行的评估，CCT 审核小组对新旧 gTLD 中的滥用率进行了更全面的比较分析，其中包括对假设情况进行的统计数据推理分析，例如，域名零售价和滥用率之间的关联。

已提交此[gTLD 中 DNS 滥用的统计分析](#)（2017 年 8 月 9 日）的结果以[征询公众意见](#)。据[报告](#)（2017 年 10 月 13 日）所述，社群提出的意见和建议具有建设性，因此，欢迎对这些研究进行科学严谨的分析，并呼吁开展更多此类研究。

GAC 在其[评议](#)（2017 年 9 月 19 日）中除了做出一些总结之外，还强调了以下几点：

- 该研究表明 DNS 中存在严重的滥用问题：
 - 在某些 NgTLD 中，注册域名滥用现象超过 50%
 - 在 NgTLD 中所有列入黑名单的网络钓鱼域中，有 5 个 NgTLD 占 58.7%
- 滥用与注册管理运行机构的政策有关：
 - 滥用率最高的 NgTLD 的注册管理运行机构在价格上具有竞争力；
 - 不法分子喜欢注册标准 NgTLD（可公开注册）域名，而不愿注册社群 NgTLD 域名（对谁能注册域名具有限制）
- 未来可能会围绕以下方面制定政策：
 - 后续 NgTLD 轮次、风险因 TLD 类别而异的证据，以及注册政策的严格性
 - 如此类统计分析结果所示，加强目前针对滥用问题的缓解措施和防御机制
- ICANN 应继续使用统计分析方法，扩大数据收集范围，来评估 DNS 滥用程度，并与社群共享相关信息。

意识和透明度：域名滥用活动报告 (DAAR)

在 ICANN 第 57 届会议（2016 年 11 月）和 ICANN 第 60 届会议（2017 年 11 月）期间，ICANN 组织发起了[域名滥用活动报告](#)研究项目，在这个项目中，GAC 和 PSWG 与 ICANN 董事会与社群积极展开合作，就 DNS 滥用问题缓解工作的有效性进行了探讨。¹⁸

制定 DAAR 的[目的](#)在于“[向 ICANN 社群报告安全威胁活动，社群利用这些数据帮助做出明智的政策决定](#)”。从 2018 年 1 月起，社群根据收集的 TLD 注册数据以及[高度可信数据源和安](#)

¹⁷ 审查注册管理运行机构、要求展示 DNSSEC 部署计划、禁止使用通配符、在从区域中删除域名服务器条目的同时删除相应的孤立粘合记录、要求维护详尽 WHOIS 记录、对域文件访问进行集中管理、要求记录注册管理机构级别的滥用问题联系人和相关流程

¹⁸ 请参阅：GAC PSWG 在[ICANN 第 57 届会议](#)（2016 年 11 月）、[ICANN 第 58 届会议](#)（2017 年 3 月）和[ICANN 第 60 届会议](#)（2017 年 10 月）期间召开的跨社群会议；[海德拉巴公报](#)（2016 年 11 月 8 日）中向 ICANN 董事会提出的有关 DNS 滥用保护措施有效性的问题；[GAC 哥本哈根公报](#)（2017 年 3 月 15 日）中提出的后续问题，以及 ICANN 组织提出的一系列[回复草案](#)。

[全威胁数据源](#)提供的大量信息¹⁹发布了[月度报告](#)，进而实现了这一目的。

因此，DAAR 有助于 GAC 确定发布[GAC 阿布扎比公报](#)（2017 年 11 月 1 日）中“*详细可靠的 DNS 滥用数据*”内容需满足的要求。但是，正如 M3AAWG 最近致 ICANN 组织的[信函](#)（2019 年 4 月 5 日）²⁰中所强调的那样，由于缺少 TLD 对应的注册服务机构的相关安全威胁信息，因此，DAAR 将仍无法满足 GAC PSWG 成员及其网络安全合作伙伴的期望，无法提供切实可行的信息。

有效性：注册管理机构和注册服务机构合同中的当前 DNS 滥用保护措施

根据[执法机构尽职调查建议](#)（2009 年 10 月），GAC 要求在 ICANN 与注册管理机构和注册服务机构签订的合同中包含 **DNS 滥用缓解保护措施**内容：

- 2013 年 [《注册服务机构认证协议》](#)（2013 年 9 月 17 日）纳入了针对 [12 项执法机构建议](#)（2012 年 3 月 1 日）的[评议](#)条款，并已获得 ICANN 董事会的批准（2013 年 6 月 27 日）
- 在[北京公报](#)（2013 年 4 月 11 日）中纳入符合 GAC 保护措施建议和 ICANN 董事会关于[实施适用于所有 NgTLD 的 GAC 保护措施的提案](#)（2013 年 6 月 19 日）的条款后，[《新 gTLD 注册管理机构协议》](#)已获得 ICANN 董事会的批准（2013 年 7 月 2 日）

在 NgTLD 最初几年的运营之后，在 ICANN 第 57 届会议（2016 年 11 月）期间，GAC 确定了一些条款和相关保护措施，但无法对这些措施的有效性进行评估。因此，在[海得拉巴公报](#)（2016 年 11 月 8 日）中，GAC 要求 ICANN 董事会对这些条款和措施的实施情况予以说明。为此，GAC 与 ICANN 组织之间开展了一次对话。GAC 与 ICANN 首席执行官召开了一次电话会议（2017 年 6 月 15 日），双方在会议上讨论了[GAC 哥本哈根公报](#)（2017 年 3 月 15 日）中提出的后续问题，以及一系列[回复草案](#)。尽管如此，仍存在大量悬而未决的问题，而且，GAC 还提出了一些新问题，这些问题将会记录在后续[工作文件](#)（2017 年 7 月 17 日）中。

GAC 针对所关注的尚未解决的问题，于 2017 年 6 月 8 日发布了一份[公告：《新 gTLD 注册管理机构协议》规范 11\(3\)\(b\)](#)，以回应一些注册管理运行机构提出的问题，寻求关于如何确保遵守[《新 gTLD 注册管理机构协议》规范 11](#) 第 3b 节的指导意见。本公告采取**自愿执行措施**，即注册管理运行机构可自愿按照规范 11(3)(b) 的要求执行这类技术分析，评估安全威胁并编制统计报告。

在 ICANN 合同合规部进行的定期审计中，该部门于 2018 年 3 月至 9 月期间对 20 个 gTLD 的“*流程、程序和 DNS 基础设施的处理*”进行了[有针对性的审计](#)，审计结果显示存在以下几个问题：“*有 13 个顶级域(TLD) 的分析和安全报告不完整；缺乏标准化的滥用处理程序记录；未对已确定的威胁采取任何措施*”²¹。

¹⁹ 如需了解更多信息，请参阅：<https://www.icann.org/octo-ssr/daar-faqs>

²⁰ 信息传递、恶意软件和移动反滥用工作组

²¹ 请参阅 2018 年 11 月 8 日发布的博客文章 - 合同合规部：解决 DNS 基础设施滥用问题：<https://www.icann.org/news/blog/contractual-compliance-addressing-domain-name-system-dns-infrastructure-abuse>

就在不久后的 2018 年 11 月，合同合规部对几乎所有 gTLD 发起了 [DNS 基础设施滥用审计](#)，目的在于“[确保签约方履行其在 DNS 基础设施滥用和安全威胁方面的合同义务](#)”。根据 GDD 峰会期间发布的[报告](#)（2019 年 5 月 9 日），ICANN 组织将发布本次审计的最终报告（[原本](#)计划于 2019 年 5 月发布），此外，该组织目前正在计划对注册服务机构发起类似的审计，开始时间为 2019 年 7 月。

签约方对此持有异议，他们认为这些审计工作已超出其合同义务范围²²。他们认为，注册管理机构和注册服务机构利益相关方团体应与 ICANN 组织的合同合规部合作，确保本次注册管理机构 DNS 基础设施审计的最终报告中对 ICANN 的职权范围做出了明确规定（考虑到社群可能会要求启动政策制定流程），此外，还应确保在审计开始之前考虑对注册服务机构的关切。

有效性：注册管理机构回应安全威胁的非约束性框架

在新通用顶级域项目中，ICANN 董事会[通过决议](#)（2013 年 6 月 25 日），同意将所谓的“安全检查”（[北京公报](#) GAC 保护措施建议）纳入《新 gTLD 注册管理机构协议》的[规范 11](#) 中。但是，由于这些条款缺乏实施细节，因此董事会[决定](#)邀请社群参与，共同为“[注册管理运行机构回应已确定的会造成实际危害的安全风险（……）](#)”制定框架。

2015 年 7 月，ICANN 成立了一个[起草小组](#)，这个小组由来自注册管理机构、注册服务机构和 GAC（包括 PSWG 成员）的志愿者组成。在征询[公众意见](#)后，这个小组于 2017 年 10 月 20 日制定了[《注册管理运行机构安全威胁回应框架》](#)。

此框架是自愿性质的非约束性文件，旨在详细说明注册管理机构在面对发现的安全威胁时可以采取的应对方法，其中包括执法机构制定的报告。该框架推出了一个 24 小时回应平台，用于响应合法和可信来源（例如政府执法机构或相应辖区的公共安全机构）提出的高优先级请求（危及人类生命、破坏重要基础设施或儿童剥削等紧急情况）。

根据其建议 19，[CCT 审核小组](#)将对该框架有效性进行评估的工作推迟到后续审核中执行²³。

有效性：采取积极措施和防止系统性滥用

根据[对 DNS 滥用情况的分析](#)²⁴，包括审议 [ICANN 关于新通用顶级域项目保护措施的报告](#)（2016 年 3 月 15 日）和单独发布的 [DNS 滥用统计分析](#)（2017 年 8 月 9 日），CCT 审核小组针对 DNS 滥用提出了以下[建议](#)：

- 在《注册管理机构协议》中纳入鼓励采取积极的反滥用措施的内容（建议 14）

²² 请参阅 RySG 致 ICANN 组织合同合规部的[信函](#)（2019 年 11 月 2 日），ICANN 组织已对此信函作出[回复](#)（11 月 8 日），以及[公告](#)（11 月 15 日）中发布的意见：注册管理机构认为[审计问题](#)不利于开展超出其合同义务 [尤其是[规范 11.3b](#)] 规定的执法行动，并表示他们不愿“与 ICANN 组织和社群分享我们为打击 DNS 滥用行为所开展的工作的相关信息 [...]，因为这属于 ICANN 合规部的职责，不在《注册管理机构协议》范畴之内”

²³ CCT 审核建议 19：下一个 CCT 应审核《注册管理运行机构安全威胁回应框架》，并评估该框架是否可以作为一项足够清晰、有效的机制，能够针对安全威胁，提供系统化的指定措施，从而减少滥用行为

²⁴ 请参阅 [CCT 审核最终报告](#)（2018 年 9 月 8 日）第 9 节 - 关于保护措施的分析（第 88 页）

- 纳入旨在防止某些注册服务机构或注册管理机构通过系统性使用域名进行 DNS 安全滥用的合同条款，具体包括设定一个会自动触发合规性查询的滥用阈值，以及考虑制定一项可行的 DNS 滥用争议解决政策 (DADRP)，以应对社群认为 ICANN 组织本身不适合或不能执行这些规定的情况（建议 15）

ICANN 董事会已[通过决议](#)（2019 年 3 月 1 日），同意将这些建议标记为“待定”状态。另外，按照董事会的指示，ICANN 组织需要“协助社群尽快明确‘滥用’的定义，以便为此建议的下一步工作提供依据。”²⁵

现状

- [GAC 内罗毕公报](#)（2010 年 3 月 10 日）第 VI 节。执法机构尽职调查建议
- [GAC 达喀尔公报](#)（2011 年 10 月 27 日）第 III 节。执法机构 (LEA) 建议
- [GAC 北京公报](#)（2013 年 4 月 11 日），尤其是适用于所有 NgTLD 的“安全检查”保护措施部分（第 7 页）
- [GAC 海得拉巴公报](#)（2016 年 11 月 8 日），包括[滥用缓解建议](#)，该建议要求对“附录 1 - 向 ICANN 董事会提出的关于 ICANN 和签约方缓解 DNS 滥用的问题”（第 14-17 页）做出回应
- [GAC 哥本哈根公报](#)（2017 年 3 月 15 日），包括[滥用缓解建议](#)，该建议要求对 GAC 海得拉巴公报附录 1 中的“GAC 后续记分卡”（第 11-32 页）做出回应
- [GAC 巴塞罗那公报](#)（2018 年 10 月 25 日），特别是第 III.2 节 - GAC 公共安全工作组（第 3 页）和第 IV.2 节 - WHOIS 和数据保护立法部分（第 5 页）
- 关于 SADAG 初步报告的[GAC 评议](#)（2016 年 5 月 21 日）
- 关于 gTLD 中 DNS 滥用的统计分析的[GAC 评议](#)（2017 年 9 月 19 日）
- 关于 CCT 审核最终报告和建议的[GAC 评议](#)（2018 年 12 月 11 日）

²⁵ 请参阅[董事会就 CCT 审核最终建议所采取的行动](#)记分卡第 5 页

主要参考文档

- [执法机构尽职调查建议](#)（2009年10月）
- [关于注册服务机构协议修订的 LEA 建议](#)（2012年3月1日）
- GAC [北京公报](#)（2013年4月11日）中提出的适用于所有 NgTLD 的“安全检查”保护措施建议（第7页）
- 根据 [GAC 海得拉巴公报](#)（2016年11月8日）中的建议，以及 [GAC 哥本哈根公报](#)中的后续建议（2017年3月15日），[GAC 提出的关于滥用缓解的问题和 ICANN 答复草案](#)（2017年5月30日）
- [关于 gTLD 中 DNS 滥用的统计分析](#)（2017年8月9日）
- 关于 gTLD 中 DNS 滥用的统计分析的 [GAC 评议](#)（2017年9月19日）
- 关于 [CCT 审核小组报告草案新章节](#)（2017年11月27日）的 [GAC 评议](#)（2018年1月16日）
- [CCT 审核最终报告和建议](#)（2018年9月8日），特别是关于保护措施的第9节（第88页）
- 关于 CCT 审核最终报告和建议的 [GAC 评议](#)（2018年12月11日）
- ICANN 董事会 [就 CCT 审核最终建议所采取的行动记分卡](#)（2019年3月1日）

相关信息

- [ICANN65 GAC 第 11.1 次会议 - ICANN 审核最新工作进展](#)（包括关于 CCT 审核建议实施情况的相关简报）
- [ICANN65 GAC 第 8.1 次会议 - 关于 WHOIS 和数据保护政策的会议](#)
- [ICANN65 GAC 第 4.1 次会议 - 关于 NgTLD 后续流程政策制定流程的会议](#)

文档管理

| | |
|------|-------------------------------|
| 会议 | ICANN65 马拉喀什，2019年6月24日 - 27日 |
| 标题 | DNS 滥用问题缓解 |
| 发布 | GAC 成员，公开发布（会后） |
| 发布日期 | 第1版：2019年6月6日 |