

DNS 滥用问题缓解

第 6 次会议

目录

会议目标	第 1 页	领导层的 GAC 行动提案	第 1 页	当前状态和近期发展动态	第 2 页	主要参考文件	第 7 页
------	-------	---------------	-------	-------------	-------	--------	-------

会议目标

本次会议的目标是召集 GAC 成员继续审议 ICANN 组织和 ICANN 社群为防范和缓解 DNS 滥用问题而实施的计划，GAC 将听取相关工作进展情况的简要汇报，并继续讨论 GAC 与更广泛的 ICANN 社群可能做出的合作努力，以支持增强的合同条款和可能的政策制定流程，从而更好地缓解 DNS 滥用问题。

领导层的 GAC 行动提案

1. 审核 ICANN 组织围绕 DNS 滥用开展的各项活动的进展，这些活动通过 ICANN 的 DNS 安全威胁缓和项目（例如 DAAR、DNSTICR 及能力培养/培训）与合同合规项目开展，包括在最近的董事会与 GAC 互动小组电话会议上向 GAC 介绍的最新情况（8 月 31 日），以及 ICANN 组织预计应在 ICANN75 会前向 GAC 所做的简要汇报¹
2. 评估 ICANN 社群围绕 DNS 滥用开展的讨论和实施工作的进展，包括相关 GNSO 小组对 DNS 滥用的审议，该小组最近表示正在准备分享一份“有关 ICANN75”的报告草案²。

¹ 请参阅 <https://gac.icann.org/sessions/boardgac-interaction-group-bgig-call-31-august-2022>（2022 年 8 月 31 日）和 <https://gac.icann.org/sessions/icann-org-preicann75-oral-briefing-to-the-gac>（2022 年 9 月 6 日）[需要登录]

² 请参阅 2022 年 8 月 25 日 GNSO 理事会会议的[会议记录草稿](#)。

当前状态和近期发展动态

- 自 ICANN66 以来，GAC 公共安全工作组领导根据 [PSWG 2020-2021 年工作计划](#) 及其“战略目标 1：培养减少 DNS 滥用和网络犯罪的能力”，向 GAC 简要介绍了 DNS 滥用问题³。
 - GAC 对注册管理机构和注册服务机构可采取的 DNS 滥用防范措施进行了审核，特别是注册政策（包括身份验证）和定价策略作为主要因素，在确定任何给定 TLD 的滥用程度方面所起到的作用⁴。
 - GAC 还听取了正在实施或可能实施的计划的简要汇报，这些计划的目的是为了更有效地从 ICANN 董事会和 ICANN 组织层面解决 DNS 滥用问题，其中包括：修订 ICANN 与注册管理机构和注册服务机构签署的合同、执行现有的相关要求、实施相关的 CCT 和 SSR2 审核建议和隐私/代理服务提供商政策建议、提高注册数据准确度，以及公布更详细的域名滥用活动数据。
 - 在 [ICANN72 公报](#)（2021 年 11 月 1 日）中，GAC 着重指出：“为更加有效地解决 DNS 滥用问题，有必要对合同要求做出改进。在这方面，依照章程规定，ICANN 的职责是适当考量政府和公共权威机构提出的公共政策问题，并为公众利益行事。此外，章程还规定，ICANN 在履行其使命期间，有权协商协议条款，包括公共利益承诺。因此，根据 GAC 和其他倡导公共利益的利益相关方的意见，ICANN 特别适合就改进现有合同进行协商，从而更加有效地遏制 DNS 滥用。”
 - 在 ICANN73 会议期间，GAC 审议了由欧盟委员会发布的 DNS 滥用研究（请参阅[报告](#)及其[技术附录](#)，2022 年 1 月 31 日），并在 [ICANN73 GAC 公报](#)中指出该研究：“提供了许多有价值的案例研究，明确了互联网生态系统中的不同参与者，并就不同参与者（例如，注册管理机构、注册服务机构、分销商、托管服务提供商、注册人等）如何应对在 DNS 系统不同层面发生的 DNS 滥用情况提出了建议”。同一份公报还指出，“这项研究涵盖的所有有害或非法活动并非都属于 ICANN 的职权范围”，但 GAC 仍然可以是“各国政府讨论 DNS 滥用问题的重要场所”。
 - 在 ICANN74 会议期间，GAC 讨论了 ICANN 的报告《[回顾过去四年：DNS 滥用趋势简要回顾](#)》（2022 年 3 月 22 日）。报告指出，鉴于识别恶意软件分发、网络钓鱼和僵尸网络等重要威胁的实际趋势非常困难，因此在现阶段就相关趋势下结论还为时尚早。报告强调了有必要综合考虑这些因素以及 DNS 滥用在人员和经济方面造成的危害，目的是提供全面的趋势图景，支持更好地了解驱动因素，并为整个行业的有效运营设置适当的激励措施。在 [ICANN74 海牙公报](#)（2022 年 6 月 20 日）中，GAC 呼吁提供“对衡量的 DNS 滥用类型的更细致划分；以及可用的原始汇总数据。”
 - 在 ICANN74 会议期间，GAC 邀请 DNS 滥用协会展示其[最近推出的](#) Net Beacon（以前称为集中式滥用报告工具），表示开发此工具是为了响应 SAC115 和 SSR2 建议 13.1，并与 CCT-RT 建议 20 保持一致。

³ 请参阅 [ICANN66](#)、[ICANN68](#)、[ICANN69](#)、[ICANN70](#)、[ICANN71](#)、[ICANN72](#)、[ICANN73](#) 和 [ICANN74](#) 期间举行的相关 GAC 全体会议的材料。

⁴ 具体请参阅 [ICANN66](#) 期间关于注册管理机构和注册服务机构可采取的预防措施的讨论，以及 [ICANN69](#) 期间在 .DK ccTLD 中实施身份验证的经验。

- 在 [ICANN74 海牙公报](#)（2022 年 6 月 20 日）中，GAC 表示“**任何关于 DNS 滥用的 PDP 都应严格制定，以便及时产生切实可行的效果**”，ICANN 董事会对此回应⁵表示同意这一观点，并准备支持 ICANN 社群的此类工作。
- **GNSO 理事会 DNS 滥用小组**[预计](#)将在 ICANN75 会议“前后”就以下内容报告其调查结果，即“**GNSO 理事会应考虑采取哪些政策措施（若有），以支持各社群团体为解决 DNS 滥用问题已经开展的工作**”。
 - 2022 年 1 月 31 日，GNSO 理事会[宣布](#)成立此 **GNSO 小组**，期望该小组“与社群中积极就该议题发表意见的其他团体（例如政府咨询委员会[...]）开展沟通交流，更好地了解其对 GNSO 抱有的期望以及其是否/如何期望后续政策工作为已经在实施的计划提供助力”。
 - 在 GAC 对 GNSO 请求社群就 DNS 滥用政策制定提供意见的[回复](#)（2022 年 4 月 4 日）中，GAC 主席重申了“GAC 关注的这个长期存在的问题”的重要性，以及 GAC 对“在启动未来的新 gTLD 之前，推进社群讨论、推动相关进展并汇集各种观点”的关注。鉴于“正在开展的社群工作可能会产生有益的举措和成果，这可能会消除对 PDP 的需求”这一事实，回复信函中建议“此时[...]开展 PDP 范围界定工作可能为时过早”。来自 ALAC、SSAC、BC、RySG 和 DNS 滥用协会的其他社群的回复，可在[GNSO 小组工作空间](#)的“关于 DNS 滥用的后续工作”部分中找到。
- **注册管理机构和注册服务机构为缓解 DNS 滥用问题采取的措施和计划**
 - 2020 年 3 月 27 日，ICANN 组织[实行了](#) [.COM 注册管理机构协议拟定修订案](#)，以将旨在促进 DNS 滥用行为检测和举报的合同条款的应用范围扩大到四分之三的 gTLD 域名空间⁶。此外，ICANN 组织与 Verisign 公司达成具有约束力的[意向书](#)，不仅提出了共同制定最佳实践和潜在的新合同义务的合作框架，还出台了一系列帮助衡量和缓解 DNS 安全威胁的措施。
 - 在 **2019 冠状病毒病 (COVID-19) 疫情背景下**，**签约方和公共安全利益相关方**报告⁷了其开展的协作，即通过采用标准化表单以及为相关权威机构建立单一联络点，促进举报滥用行为、对举报事件进行审核以及将举报事件转交给相关司法机构进行处理。执法机构与注册服务机构建立的合作关系以及**注册服务机构利益相关方团体**在 ICANN67 期间发布的[注册服务机构滥用报告指南](#)是开展这些工作的基础。该指南已进行了[更新](#)（2022 年 1 月），并获得了**注册管理机构利益相关方团体**的认可。
 - **公共利益注册管理机构 (PIR)**（.ORG 和若干新 gTLD 的注册管理运行机构）[发起成立](#)（2021 年 2 月 17 日）**DNS 滥用协会**。该计划已[呈交给 GAC PSWG](#)（2021 年 3 月 3

⁵ 请参阅 <https://gac.icann.org/sessions/boardgac-interaction-group-bgig-call-31-august-2022>（2022 年 8 月 31 日）[需要登录]

⁶ 这些条款包含[规范 11.3b](#)，此规范目前仅适用于新 gTLD。截至 2022 年 3 月，.COM 共有 1.613 亿个注册域名，其中不包括所有 TLD 的 3.505 亿个域名中的 1.334 亿个 ccTLD 域名，占有 gTLD 注册域名的 74%（请参阅 2022 年 6 月的[Verisign 域名行业简报](#)）

⁷ 请参阅签约方在[ICANN68 会议之前](#)和[ICANN68 会议期间](#)所做的汇报，以及在 ICANN68 会议期间[PSWG 向 GAC 所做的简要汇报](#)。

日)。在 [ICANN70 公报](#) 中，GAC 对发起成立 DNS 滥用协会表示欢迎，同时“鼓励社群积极参与合作，全面解决 DNS 滥用问题”。

- 此后，DNS 滥用协会 [发布了路线图](#)（2021 年 6 月 14 日），讨论了 [如何减轻互联网基础设施各个层面上的危害](#)（2021 年 8 月 24 日），并发布了 [关于识别恶意注册的最佳实践](#)（2021 年 12 月 2 日）。在 ICANN74 会议期间，DNS 滥用协会受邀展示了其 [最近推出的 Net Beacon](#)（以前称为 [集中式滥用报告工具](#)），开发此工具是为了响应 SAC115 和 SSR2 建议 13.1，并与 CCT-RT 建议 20 保持一致。

- **ICANN 组织的全方位应对⁸（现在是 DNS 安全威胁缓和项目的一部分）和合同执行方案**

- ICANN 组织 [介绍](#)（2021 年 7 月 22 日）了 [DNS 安全威胁缓和项目](#)，该项目旨在清晰展示与 DNS 安全威胁相关的各种计划和项目，并促进制定和执行统一战略。
- **ICANN 首席技术官办公室 (OCTO) 及其安全、稳定和弹性小组 (SSR)** 开展研究并保持 ICANN 在 DNS 安全领域的专业知识以造福社群。OCTO 广泛参与各种网络威胁情报和事件响应论坛，并积极开发系统和工具，以协助识别、分析和报告 DNS 滥用⁹。
 - 为应对 COVID-19 疫情，OCTO 开发了 [域名安全威胁信息搜集和报告 \(DNSTICR\)](#) 工具，帮助识别用于开展 COVID-19 相关滥用行为的域名并与相关方共享数据。在 ICANN68 之前已就这一问题向 GAC 做出初步 [简要汇报](#)（2020 年 6 月 12 日），并邀请 GAC 成员为提高这项工具的语言多样性尽一份力。
 - 自 2018 年 1 月以来，ICANN 一直通过 [域名滥用活动报告 \(DAAR\) 平台](#) [每月报告](#) 在 DNS 中观察到的域名注册和安全威胁行为¹⁰。2021 年 10 月，ICANN 组织与注册管理机构利益相关方团体宣布达成共识¹¹，根据达成的共识，双方在原则上同意利用注册管理机构持有的注册数据在 DAAR 中提供注册服务机构级别的信息，这一点在 [GAC 近期致 ICANN 的信函](#)（2022 年 2 月 21 日）中也有所提及。ICANN 董事会确认，这将反映在预计将在 ICANN75 前后不久发布的合同修订中¹²。ICANN 组织 [2022 年 7 月的 DAAR 报告](#) 指出：“关于注册服务机构资产组合的报告需要域名注册数据来确定哪些域名由哪些注册服务机构赞助。可以每天搜集和分析必要注册服务机构数据的系统正处在开发过程中。我们希望在未来的报告中添加关于注册服务机构的内容”。
 - 在实施 [2021-2025 财年战略规划](#) 期间，OCTO 支持 **DNS 安全协调计划技术研究组**（于 2020 年 5 月 [成立](#)）“[探寻各类方案，明确 ICANN 可以和应该采取](#)

⁸ 2020 年 4 月 20 日，ICANN CEO 发表了一篇博文，详细介绍 ICANN 组织 [多管齐下应对 DNS 滥用](#)

⁹ 在 [GAC 关于 DNS 滥用问题的电话会议](#)（2021 年 2 月 24 日）期间，ICANN 组织介绍了 OCTO DNS 滥用相关活动的最新动态，其中包括针对 DNS 安全威胁和 DNS 滥用的定义、签约方的义务、域名滥用活动报告 (DAAR)、域名安全威胁信息搜集和报告 (DNSTICR)、域安全协调计划 (DSFI) 的状况、新的域名安全知识共享和实例规范 (KINDNS) 倡议的讨论情况，以及回顾 OCTO 在全球的培训和能力建设领域所开展的工作

¹⁰ 迄今已有多个利益相关方和 ICANN 工作组就 DAAR 的局限性发表意见，特别是 M3AAWG 致 ICANN 组织的 [信函](#)（2019 年 4 月 5 日）和 SSR2 审核小组编制的 [报告草案](#)（2020 年 1 月 24 日）。注册管理机构利益相关方团体也表达了对 DAAR 的关注，并在至 ICANN CTO 的 [信函](#)（2020 年 9 月 9 日）中提出建议。

¹¹ 请参阅 RySG 致 ICANN 的信函（2021 年 10 月 22 日）和相应的 ICANN 博文（2021 年 10 月 28 日）

¹² 请参阅 <https://gac.icann.org/sessions/boardgac-interaction-group-bgig-call-31-august-2022>（2022 年 8 月 31 日）[需要登录]

哪些措施来加强与 DNS 生态系统利益相关方之间的合作与交流，以提高 DNS 的安全性”。经过 18 个月的审议，该研究组的[最终报告](#)（2021 年 10 月 15 日）得以[发布](#)。ICANN 组织[向 GAC 表示](#)（2022 年 2 月 16 日），正在制定相应的行动计划。2022 年 4 月 20 日，向社群介绍了[实施流程](#)和用于跟踪进度的[维基页面](#)。在 ICANN74 会议期间，GAC 讨论了优先考虑建议 E5 的价值，以便在 ICANN 社群的利益相关方之间建立一个[威胁和事件信息共享平台](#)¹³。

o 关于合同合规实践，ICANN CEO 在一篇[博文](#)（2020 年 4 月 20 日）中回忆称：

“ICANN 合规部负责按照 ICANN 的政策和协议履行合同义务，这包括《注册管理机构协议》(RA) 和《注册服务机构认证协议》(RAA)。ICANN 合规部还与 OCTO 紧密合作，识别 DNS 安全威胁[...]，并将这些威胁告知相应的签约方机构。ICANN 合规部使用审计工作中搜集的数据[...]，用以评估注册管理机构和注册服务机构是否遵守了其 DNS 安全威胁义务。除了审计工作以外，ICANN 合规部还利用 OCTO 和其他部门搜集的数据，积极地与 DNS 安全威胁比例失当的注册管理机构和注册服务机构进行接触。若建设性的接触以失败告终，则 ICANN 合规部将立即针对拒绝遵守 DNS 安全威胁义务的相关方采取强制措施。”

- 在 2019 年 6 月完成之前对注册管理运行机构就 DNS 基础设施滥用执行的合同合规审计后¹⁴，ICANN [报告](#)（2021 年 8 月 24 日）了关于注册服务机构遵守 DNS 滥用义务情况的审计结果：
 - 共审计了 126 家注册服务机构（这些注册服务机构管理着 90% 以上的已注册 gTLD 域名）
 - 有 111 家注册服务机构没有完全遵守关于接收和处理 DNS 滥用报告的要求（即 RAA 第 3.18.1 节至第 3.18.3 节）
 - 有 92 家注册服务机构采取了行动以实现完全合规，而有 19 家注册服务机构正在实施调整
- 2022 年 4 月 13 日[宣布](#)针对选定注册管理机构开展新一轮审计工作。本轮审计将涉及 28 家运营 gTLD 的 gTLD 注册管理运行机构，这些注册管理运行机构以前没有在标准的全面审计中进行过审计，并且根据公开的信誉阻止名单（不包括垃圾邮件）报告，具有最高滥用得分。本次审计工作预计在 2022 年第 3 季度之前完成。
- 在 [ICANN 首席执行官在 ICANN73 会前向 GAC 所做的简要汇报](#)（2022 年 2 月 16 日）中，ICANN 合同合规部审核了 ICANN 协议中 DNS 滥用相关义务的履行情况，并展示了抽样的 3378 起关于注册服务机构不当处理滥用报告的投诉案例的结果，这些投诉导致了 456 次合规调查和 1 次违规通知。
- 2022 年 3 月 9 日，ICANN [宣布](#)推出新报告，以增强对投诉量和投诉趋势的了

¹³ [DSFI-TSG 最终报告](#)（2021 年 10 月 13 日）中的建议 E5 事件响应：“ICANN 组织应与相关方一起，鼓励在整个 DNS 行业开发和部署一个正式的事件响应流程，以便与生态系统中的其他机构进行互动。这类工作应包含事件响应处理，以及受保护的威胁和事件信息共享”

¹⁴ 请参阅 ICANN 博文[合同合规：解决域名系统 \(DNS\) 基础设施滥用问题](#)（2018 年 11 月 8 日）和[合同合规部针对注册管理运行机构应对 DNS 安全威胁审计工作的报告](#)（2019 年 9 月 17 日）

解。

- 在 ICANN75 筹备周期间，[合同合规部预计将向社群汇报最新工作进展](#)（2022 年 9 月 6 日），可能还会介绍上述最新一轮注册管理机构审计的进展情况。

关于未来工作的社群建议

● SSR2 审核建议

- SSR2 审核小组提交了一份[报告草案](#)（2020 年 1 月 24 日），其中重点介绍了 DNS 滥用问题的预防和缓解措施。[GAC 评议](#)（2020 年 4 月 3 日）认可了其中的许多建议，包括与改进域名滥用活动报告 (DAAR) 和加强合规机制相关的建议。
- 在 ICANN70 会议期间，GAC 对[最终报告](#)（2021 年 1 月 25 日）进行了审议，准备在[公众意见征询程序](#)中最终提交 [GAC 评议](#)（2021 年 4 月 8 日）。
- ICANN 董事会就该审核小组制定的 63 项最终建议（2021 年 1 月 25 日）[采取了行动](#)（2021 年 7 月 22 日）。ICANN 组织发布了一篇[博文](#)，对董事会采取的行动进行了如下总结：
 - 13 项建议获得了批准（实施规划有待制定）；
 - 16 项建议被拒绝（其中包括无法完全获得批准的 6 项建议）；
 - 34 项建议处于未决状态，等待收集更多信息和进一步分析。
- 在 [ICANN72 公报](#)（2021 年 11 月 1 日）中，GAC 建议 ICANN 董事会：
 - *作为优先事项，采取必要的后续行动以支持快速实施董事会平衡记分卡 [...]*
 - *提供更多信息，以说明董事会和 SSR2 审核小组关于某些建议的实施程度持有的不同看法。*
- ICANN 董事会在其对 ICANN72 公报的[回复](#)（2022 年 1 月 16 日）中提供了更多信息。这是 GAC 和 ICANN 董事会在 ICANN73 会议期间开展了进一步讨论的议题¹⁵，相关情况以 ICANN 组织随后通过[信函](#)（2022 年 3 月 18 日）和[跟进电子邮件](#)（2022 年 4 月 12 日）与 GAC 进行的沟通为准。

- **安全与稳定咨询委员会 (SSAC) DNS 滥用问题工作组**发布了 [SAC115](#) 报告（2021 年 3 月 19 日），拟定了解决 DNS 滥用处理的互操作方法。
 - **SSAC 提出了一般最佳实践和流程框架**，以简化 DNS 滥用和常规互联网滥用举报流程，其中讨论了以下几个问题：解决滥用问题的主要责任人、证据标准、上报途径、合理行动期限以及联系信息可用性和质量。
 - **关键提案**（SSAC 建议 ICANN 社群应与更广泛的 DNS 基础设施社群建立合作，共同审查并进一步完善提案）是设立“**常见滥用应对协调人**”，作为完全独立的非营利性非政府组织，来担任整个 DNS 生态系统（包括 ICANN 签约方、托管服务提供商、

¹⁵ 请参阅 [ICANN73 GAC 会议记录](#) 第 13 页

互联网服务提供商 (ISP) 和内容分发网络 (CDN) 的调解人，简化滥用问题举报流程，并最大程度地减轻滥用问题危害。

- 如上所述，自 SAC115 以来，DNS 滥用协会已采取措施创建了一个通用滥用报告平台，即 [Net Beacon 报告工具](#)（2022 年 6 月）。在 ICANN74 会议期间，DNS 滥用协会向 GAC 介绍了 NetBeacon 的功能。

主要参考文件

- GAC 对 GNSO 请求社群就 DNS 滥用政策制定提供意见的[回复](#)（2022 年 4 月 4 日）
- [《回顾过去四年：DNS 滥用简要回顾》](#)（2022 年 3 月 22 日）
- 欧盟委员会发布的 [DNS 滥用调查报告](#) 及其中的[技术附录](#)（2022 年 1 月 31 日）
- SSR2 审核[最终报告](#)（2021 年 1 月 25 日）和[董事会行动平衡记分卡](#)（2021 年 7 月 22 日）
- ICANN [公告](#)和关于注册服务机构遵守 DNS 滥用义务情况的审计[报告](#)（2021 年 8 月 24 日）。
- SSAC [SAC115 报告](#)（2021 年 3 月 19 日），其中拟定了解决 DNS 滥用处理的互操作方法

更多信息

GAC 关于 DNS 滥用问题缓解的政策背景文件：

<https://gac.icann.org/briefing-materials/public/gac-policy-background-dns-abuse-mitigation.pdf>

文件管理

标题	ICANN75 GAC 会议简报 - DNS 滥用问题缓解
发布	GAC 成员（会前）和公众（会后）
发布日期	第 1 版：2022 年 9 月 2 日