ICANN | GAC
Governmental Advisory Committee

ICANN 68
VIRTUAL POLICY FORUM
22–25 June 2020

DNS 滥用问题缓解

第 2 次会议和第 8 次会议

目录

会议目标

GAC 将讨论有关 DNS 滥用问题的最新情况，特别是在 COVID-19 疫情背景下，并介绍计划在 ICANN 第 68 届会议期间围绕该主题召开的跨社群全体会议。此次会议还将回顾和讨论在预防和缓解 DNS 滥用问题和安全威胁方面的相关工作进展。

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。这些恶意活动可能会威胁到 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 DNS 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个问题，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型和盈亏底线。

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 组织根据恶意行为缓和措施备忘录（2009 年 10 月 3 日）实施了一系列新要求[2]。ICANN 关于新通用顶级域项目保护措施的报告（2016 年 7 月 18 日）对这些要求的有效性进行了评估，以便为章程规定的竞争、消费者信任和消费者选择 (CCT) 审核做准备，CCT 审核小组于 2018 年 9 月 8 日针对 DNS 滥用问题提出了相关建议。

- 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 GAC PSWG** 之间一致同意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**开发出了 ICANN 的域名滥用活动报告 (DAAR) 工具，并编制了月度滥用报告。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[5]的相关人员愈加担心是否能够有效缓解 DNS 滥用问题。最近，COVID-19 这项全球公共卫生紧急事件证明了现有挑战仍然存在，因为与 COVID-19 相关的域名注册量激增，其中有少量相关域名[6]被投机者用于实施欺诈。

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[7]。

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 滥用的统计数据分析最终报告的 意见（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 18 日）中有关对执法机构的影响调查

[6]请参阅注册服务机构利益相关方团体领导层于 2020 年 4 月 9 日向 GAC 提交的报告

[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

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（本简报中详细记录了这些问题）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 在 ICANN 第 68 届会议期间的行动提议

1. 回顾迄今为止从相关方（包括公共权威机构、注册服务机构、ccTLD 运营商和 ICANN 组织）报告的**与 COVID-19 相关的 DNS 滥用问题**中汲取的**经验教训**，并从关于 COVID-19 疫情期间 DNS 滥用和恶意注册的跨社群全体会议（此次会议计划在 ICANN 第 68 届会议期间，于 2020 年 6 月 22 日召开）开始，**根据需要为促进 ICANN 社群的参与做好准备**。

2. 根据 GAC 蒙特利尔公报建议（2019 年 11 月 6 日），**商议接下来可以采取哪些措施来解决 GAC 之前确定的与 DNS 滥用相关的主要公共政策问题，特别是要**与 GNSO 理事会、ALAC、ccNSO 甚至是 ICANN 董事会就以下事宜共同商讨后续工作安排：**在启动新通用顶级域后续轮次之前可以采取哪些措施来解决 CCT 审核小组针对 DNS 滥用问题提出的建议**。

3. 根据以下两项中列出的 ICANN 董事会行动内容，**讨论**围绕 **CCT 审核小组和注册目录服务审核小组 (RDS/WHOIS2-RT) 提出的有关 DNS 滥用问题的建议**所开展的审议和实施工作的**进展情况**：
   a. 关于 CCT 审核建议的董事会行动平衡记分卡（2019 年 3 月 1 日）
   b. 关于 RDS/WHOIS2-RT 审核建议的董事会行动平衡记分卡（2020 年 2 月 25 日）

4. **审议在更广泛的 ICANN 社群内重点开展的 DNS 滥用问题缓解工作的进展**，特别是由签约方、ccTLD 运营商和 ICANN 组织开展的工作，包括为了提升实践标准和合同中所设标准所做的工作：
   a. **gTLD 注册服务机构和注册管理机构**根据行业领先的滥用应对框架**采取自愿措施**
   b. **ccTLD 运营商积极实施反滥用措施**，这能为 gTLD 注册管理机构提供实践经验
   c. **对注册服务机构开展 DNS 安全威胁方面的合同合规审计**，预计这项工作将在类似的注册管理机构审计结束之后开展
   d. 根据注册管理机构、GAC 和 SSAC 之前讨论的结果，**改进 ICANN 域名滥用活动报告 (DAAR)**

相关工作进展

最新工作进展概述

- **面对 COVID-19 疫情，GAC 和受影响的利益相关方积极合作，在相互协调的基础上共同开展了多项工作来应对**各种欺诈和犯罪活动：
  - **GAC 领导层**在由注册服务机构利益相关方团体 (RrSG) 要求开展的讨论会（4 月 9 日）上做了报告，并在一次领导层联合电话会议（2020 年 6 月 3 日）上进一步讨论了相关事项，以便为 ICANN 第 68 届会议做好准备。
  - 在应对涉及 COVID-19 的潜在欺诈活动的过程中，**注册服务机构**报告了在相关辖区内评估欺诈活动时所面临的挑战，并寻求公共权威机构的协助。为帮助其成员处理相关问题，RrSG 编制并共享了注册服务机构应对 COVID-19 疫情的方案。
  - **GAC 成员已受邀共享**由各公共权威机构提供的**相关资源**，例如，由执法机构（美国联邦调查局、英国国家打击犯罪调查局 (UK NCA)、欧洲刑警组织）和消费者保护机构（美国联邦贸易委员会 (US FTC)）共享的资源
  - **欧盟委员会**汇报了与欧盟成员国、欧洲刑警组织、ccTLD 和注册服务机构合作开展的工作，包括采用标准化的表单以及为成员国的相关权威机构建立单一联系点，这些工作旨在促进报告涉及 COVID-19 相关域名/内容的滥用事件、对报告事件进行审查以及向相关司法机构提交报告。
  - 世界各地的 **ccTLD 运营商**预计将于 2020 年 6 月 4 日至 5 日向 GAC 汇报他们从此次疫情期间的运营工作中所汲取的经验教训。
  - 在 ICANN 第 68 届会议召开之前，计划由 **ICANN 首席技术官办公室** (OCTO) 向 GAC 进行汇报，汇报内容预计包括 ICANN 为支持签约方采取的应对行动而专门实施的举措和投入的资源

- 与此同时，**签约方、ICANN 安全与稳定咨询委员会 (SSAC) 和 ICANN 组织为应对安全威胁开展了新工作：**
  - 如 GAC 公共安全工作组在 ICANN 第 67 届会议期间所做的报告所述，**注册服务机构利益相关方团体**发布了《注册服务机构滥用报告指南》
  - **DNS 行业的主要利益相关方提出了** DNS 滥用应对框架（2019 年 10 月 17 日）作为一项**自愿措施**，截至 2020 年 3 月 29 日，已有 56 个机构签署了该框架。
  - **SSAC** 成立了一个 DNS 滥用问题工作组，并邀请了 PSWG 的一名代表加入该工作组。
  - 在实施 2021-2025 财年战略规划期间，**ICANN 组织**宣布成立 DNS 安全协调计划技术研究小组（2020 年 5 月 6 日），旨在 *“探寻各类方案，明确 ICANN 可以和应该采取哪些措施来加强与 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”*。预计将于 2021 年 5 月提出相关建议。

- 自 ICANN 第 66 届会议以来，一些 **ICANN 社群工作组便开始对与 DNS 滥用有关的新建议进行审议**，其中一些工作组已经收到了 GAC 提供的意见，一些流程可能会成为 GAC 后续工作的主题：
    - 在 **RDS/WHOIS2-RT** 于 2019 年 9 月 3 日发布最终建议（这些建议对于缓解 DNS 滥用问题的重要性已在一份 GAC 意见（2019 年 12 月 23 日）中予以强调）之后，ICANN 董事会按照董事会行动平衡记分卡（2020 年 2 月 25 日）及其 2020.02.25.01 - 2020.02.25.06 号决议对这些建议进行了审议：其中 15 项建议被接受、4 项建议处于待定状态、2 项建议被转交给 GNSO、2 项建议被拒绝。
    - **第二轮 DNS 安全、稳定和弹性 (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 意见（2020 年 4 月 3 日）认可了其中的许多建议，尤其是与改进域名滥用活动报告 (DAAR) 和加强合规机制相关的建议。根据最近的审议，SSR2 审核小组预计将于 2020 年 10 月发布最终建议。
    - **GNSO 新通用顶级域后续流程政策制定流程工作组**最近发布了一份报告（2020 年 4 月 29 日），报告中称“*除了声明今后采取的任何措施都必须适用于现有和新通用顶级域（以及潜在的 ccTLD）之外，不打算就缓解域名滥用问题提出任何建议*”。尽管 CCT 审核小组向该工作组提出了相关建议，且这些建议得到了 ICANN 董事会的支持，此外，还有 GAC 蒙特利尔公报建议（2019 年 11 月 6 日）和 GAC ICANN 第 67 届会议公报（2020 年 3 月 16 日）中记录的更多 GAC 意见，但该工作组还是发表了此声明。最近召开的 GNSO 理事会会议（2020 年 3 月 21 日）讨论了成立跨社群工作组 (CCWG) 的可能性，并讨论了在需要制定新合同要求时，是否可以启动新的 GNSO PDP。该会议没有讨论由 GAC 领导层提出的非正式提案（2020 年 5 月 12 日），该提案建议在相关领域的专家（包括 ccTLD 运营商）中成立专题讨论组以确定今后政策工作的范围。

问题 - DNS 滥用的定义

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。[8]

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。[9]

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”和“安全威胁”**，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*”[10]，以及《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。*”[11]，并要求促进 ICANN 组织消费者保护部开展相关活动，**在 ICANN 第 66 届蒙特利尔会议召开之前和期间围绕滥用的定义展开更多讨论**。

特别值得注意的是，在 ICANN 第 66 届会议前的网络研讨会（2019 年 10 月 15 日）期间，**PSWG 和签约方讨论了当前问题和行业惯例**。为准备此次网络研讨会，注册管理机构利益相关方团体发布了一封公开信（2019 年 8 月 19 日），其中讨论了注册管理机构对 DNS 滥用定义的看法，注册管理机构为应对安全威胁而必须采取的有限措施，以及他们对 ICANN 的域名滥用活动报告的顾虑。作为回应，GAC 发布了关于 DNS 滥用问题的声明（9 月 18 日），而且企业选区也做出了回应（10 月 28 日）。

---

[8] “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。

[9] 请参阅 CCT 审核最终报告（2018 年 9 月 8 日）第 88 页；最近发表的关于 DNS 滥用的 GAC 声明（2019 年 9 月 18 日）中也着重提到了此问题

[10] 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*”。

[11] 请参阅董事会就 CCT 审核最终建议所采取的行动平衡记分卡第 5 页

问题 - 意识和透明度：社群参与缓解 DNS 滥用问题相关工作

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**。最近，ICANN 支持组织和咨询委员会 (SO/AC) 以及 ALAC 的领导人围绕此问题开展了很多活动，这些活动吸引了大量社群成员参与。

- 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型、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，并采取基于实事的政策制定流程。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[12]。

- 在 ICANN 第 66 届蒙特利尔会议期间（2019 年 11 月 6 日），ICANN 社群召开了一次关于 DNS 滥用问题的跨社群全体会议

- 在 ICANN 第 67 届虚拟会议期间（2020 年 3 月 9 日），ALAC 召开了两场会议，一场会议旨在介绍 DNS 滥用（包括提供教育性视频），另一场会议旨在审议应对一般 DNS 滥用案例时的合同合规实践，许多 ICANN 社群成员远程参与了这两场会议。

[12] 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）

问题 - 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 提出的关于安全检查的保护措施建议[13]，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意见）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 滥用的统计数据分析（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 在其意见（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 应继续使用统计数据分析方法，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。

2019 年 10 月 17 日，一家咨询公司 (Interisle Consulting Group) 发布了一项关于域名批量注册和联系信息访问权限非法滥用的研究，该研究与正在进行的社群讨论直接相关，其中探讨了以下问题：

- 网络犯罪分子如何利用批量注册服务使大量域名成为攻击“武器”。
- ICANN 为实现 GDPR 合规而制定的有关编辑 WHOIS 联系信息点的临时政策对网络犯罪调查的影响
- 需要 ICANN 组织和社群进行审议的政策建议

问题 - 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

[13]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

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。[14]

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全威胁数据源提供的大量信息发布了月度报告，进而实现了这一目的。[15]

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[16] 致 ICANN 组织的信函（2019 年 4 月 5 日）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。

最近，注册管理机构在致 ICANN 首席技术官办公室的一封公开信（2019 年 8 月 19 日）中称，“*将分析 DAAR，以期向 OCTO 提出改进建议，进而确保 DAAR 能够更好地实现其预期目标，并为 ICANN 社群提供宝贵的资源*”。虽然注册管理机构认识到“*一些社群成员可能会使用 ICANN 域名滥用活动报告 (DAAR) 中提供的数据来支持存在系统性或广泛 DNS 滥用的主张*”，但他们认为“*该工具有很大的局限性，无法准确可靠地提供安全威胁证据，并且尚未实现其目标*”。

问题 - 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）的意见条款，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 届会议期间，**GAC 确定了一些条款和相关保护措施，但无法对这些条款和保护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

[14]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；海得拉巴公报（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。

[15]如需了解更多信息，请参阅：https://www.icann.org/octo-ssr/daar-faqs

[16]信息传递、恶意软件和移动反滥用工作组

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”*。[17] 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”*。在最近一次审计（2019 年 9 月 17 日）的报告中，ICANN 得出了以下结论：

- 绝大多数注册管理运行机构都在努力解决 DNS 安全威胁。
- DNS 安全威胁主要集中在少数注册管理运行机构。
- 一些注册管理运行机构对合同规范 11 3(b) 做出了不同的解释，因此难以判断他们为减轻 DNS 安全威胁所做的努力是否合规和有效。

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。[18]ICANN 组织表示，将对注册服务机构开展 DNS 安全威胁审计。

[17] 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

[18] 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”*

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“*国家执法机构或相应管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）。

根据第 19 项建议，CCT 审核小组推迟了评估该框架有效性的任务[19]，因为该框架投入使用的时间还不够长，无法评估其有效性。

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[20]，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）
- 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。*”[21]

现状

GAC 的现状如下（按时间倒序列出）：

- 关于 SSR2 审核小组报告草案的 GAC 意见（2020 年 4 月 3 日）

---

[19] 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*

[20] 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）

[21] 请参阅董事会就 CCT 审核最终建议所采取的行动平衡记分卡第 5 页

- 关于 RDS/WHOIS2-RT 最终建议的 GAC 意见（2019 年 12 月 23 日）
- 关于 DNS 滥用的 GAC 声明（2019 年 9 月 18 日）
- 关于 CCT 审核最终建议的 GAC 意见（2018 年 12 月 11 日）
- 关于 CCT 审核小组报告草案新章节（2017 年 11 月 27 日）的 GAC 意见（2018 年 1 月 16 日）
- 关于 gTLD 中 DNS 滥用的统计分析的 GAC 意见（2017 年 9 月 19 日）
- 关于 SADAG 初步报告的 GAC 意见（2016 年 5 月 21 日）
- 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）
- 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 后续平衡记分卡”（第 11-32 页）做出回应
- 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 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 达喀尔公报（2011 年 10 月 27 日）第 III 节。执法机构 (LEA) 建议
- 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
- 关于注册服务机构协议修订的 LEA 建议（2012 年 3 月 1 日）
- 执法机构尽职调查建议（2009 年 10 月）

主要参考文档

- 关于 RDS/WHOIS2-RT 最终建议的 ICANN 董事会行动平衡记分卡（2020 年 2 月 25 日）
- 关于 CCT 审核最终建议的 ICANN 董事会行动平衡记分卡（2019 年 3 月 1 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 gTLD 中 DNS 滥用的统计分析（2017 年 8 月 9 日）
- 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）

文档管理

会议	ICANN68 虚拟政策论坛，2020 年 6 月 22 - 25 日
标题	DNS 滥用问题缓解
发布	GAC 成员（会前），公开发布（会后）
发布日期	第 1 版：2020 年 6 月 3 日