ICANN82 | 社群论坛 – GAC：DNS 滥用问题讨论会议
2025 年 3 月 11 日（星期二） – 10:30 至 12:00（太平洋标准时间）

发言人（男，姓名不详） 大家上午好。请就坐。我们马上就要开始了。

谷尔顿 • 泰普 • 奥克苏佐格鲁 (GULTEN TEPE OKSUZOGLU) 大家好，欢迎参加于世界协调时 3 月 11 日星期二 17:30 举行的 ICANN82 政府咨询委员会 (GAC) 关于 DNS 滥用问题的专题讨论会议。请注意，本次会议正在录音，并受 ICANN 预期行为标准和 ICANN 社群反骚扰政策约束。

在本次会议中，如果要通过聊天窗口提交问题或评论，请注意形式要适当，我们会大声朗读您的问题或评论。请记得说出您的姓名，如果您使用的是英语以外的其他语言，还要说出您将使用的语言。请清楚表达并保持合理语速，以便翻译人员能够准确地进行翻译工作。同时，请确保在发言时其他所有设备均保持静音。您可以在 Zoom 工具栏中访问此次会议的所有可用功能。

我就说到这里，下面有请 GAC 主席尼古拉斯 • 卡瓦耶罗发言。交给你了，尼古拉斯。

尼古拉斯 • 卡瓦耶罗 (NICOLAS CABALLERO) 谢谢谷尔顿。谢谢。各位上午、下午和晚上好。欢迎大家参加本次 DNS 滥用问题缓和会议。我们邀请了阵容卓越的演讲嘉宾：ICANN 合规部的乐缇西亚 • 卡斯蒂罗 (Leticia Castillo)、西

昂 • 罗伊德 (Siôn Lloyd)，抱歉，我的发音正确吗？是读作西昂 (Siôn) 吗？他将稍后到达会场；NetBeacon Institute 的格雷姆 (Graeme)、来自 Tucows 的雷哲 • 莱维 (Reg Levy)、鲁克 (Luc) 以及杰夫 (Jeff)。欢迎各位。

我们的嘉宾还有 GAC 主题负责人、来自欧盟委员会的玛蒂娜 • 巴贝罗 (Martina Barbero) 以及来自日本的宫本 (TOMO)。我们将就 DNS 滥用的具体细节与各位展开深度探讨。我就介绍到这里。下面有请来自日本的同事宫本。交给你了，宫本。

宫本友纪 (TOMONORI MIYAMOTO)

谢谢主席先生，尼科。大家好！欢迎参加 GAC DNS 滥用问题讨论会议。我是来自日本的宫本友纪。本次会议由来自 [音频不清晰 00:02:16] 的玛蒂娜以及我本人主持。玛蒂娜在线上参会，我是来自日本的宫本。本次会议邀请到了许多演讲嘉宾。欢迎 ICANN 合规部门的乐缇西亚、ICANN 首席技术官办公室 (OCTO) 的西昂、安全与稳定咨询委员会 (SSAC) 的杰夫、签约方机构 (CPH) 的鲁克以及 NetBeacon 的格雷姆。非常感谢你们的参与。请切换到下一张幻灯片。

好的。以下是本次会议的议程安排。我们将分享和讨论 GAC 关于 DNS 滥用的调查结果、ICANN 合同合规最新进展、恶意域名注册的推断分析 (INFERMAL) 报告以及域名衡量项目 (Domain Metrica)。我们还将讨论缓解 DNS 滥用问题的后续步骤。请切换到下一张幻灯片。

请允许我简要介绍本次 DNS 滥用主题会议的背景。我们可以看到，处理 DNS 滥用问题是我们的重要事项。在上一次会议中，

我们已经在西雅图与 SSAC、非商业利益相关方团体 (NCSG) 和一般会员咨询委员会 (ALAC) 就 DNS 滥用问题进行过讨论。这与我们昨天谈到的数据准确度也有一些联系。根据 ICANN 合同、注册服务机构 (RA) 注册服务机构认证协议 (RAA)，通用顶级域 (gTLD) 的注册管理机构和注册服务机构必须对 DNS 滥用报告做出回应。

这些合同于去年 4 月修订，目前已经快一年了。对于 DNS 滥用的背景和方法有各种不同的理解。除技术性网络安全问题外，一些国家或地区还致力于解决儿童性虐待资料 (CSAM) 等线上危害问题，以及日本的漫画盗版等版权侵权问题。值得注意的是，ICANN 合同中对 DNS 滥用的定义是明确且有限制的，包括传播恶意软件、僵尸网络、网络钓鱼、网址嫁接和垃圾邮件。然而，DNS 滥用与各种滥用行为在路径上存在一定的关联性或相互作用。

为了应对 DNS 滥用的挑战，我们认为有必要介绍 ICANN 内部正在开展的工作，回顾一些相关数据，并分享 ICANN 外部工作的良好实践。请切换到下一张幻灯片。

谢谢。有些人可能还记得这张图表，它说明了相关社群的情况。其中绿色方块显示的是 ICANN 合同的范围，相当有限；为了有效地处理这个问题，我们需要考虑建立蓝色方块中的那些关系，如注册服务机构和分销商之间签订合同；此外，我们还可以在红色方块中的扩展社群之间寻求合作，如可信通知者项目。在 ICANN 合同的限制之外，我们还可以做很多工作。请切换到下一张幻灯片。

这是我们当前的道路，也是我们前进的方向。去年秋天，我们在伊斯坦布尔 ICANN81 会议上讨论了 ICANN 内部可以开展的工作。我们听取了 ICANN 合规方面的介绍，并与包括 SSAC 和 CPH 在内的利益相关方开展讨论。今年早些时候，在 1 月和 2 月，我们就 DNS 滥用问题开展了 GAC 调查。本次调查涵盖 GAC 成员对 DNS 滥用情况和案例的理解，包括方法、扩展社群合作、数据监测等。

我们将在本次会议回顾上述调查内容并展望未来的发展，我们将分享 GAC 调查的结果，并听取 ICANN 关于合规最新进展、INFERMAL 和域名衡量项目的介绍，随后将针对这些主题组织专家组讨论。最后将讨论后续步骤。我们将基于今天的讨论成果制定后续行动计划。我们将在布拉格讨论生态系统的全面合作。我们来看下一张幻灯片。玛蒂娜，交给你了。

玛蒂娜 • 巴贝罗

非常感谢，宫本。我很高兴能参与会议并发言，尽管距离很远。我是来自欧盟委员会的玛蒂娜 • 巴贝罗。我是 DNS 滥用主题 [音频不清晰 00:06:47]，和宫本一起负责该主题。在接下来的演讲中，我们将重点简要介绍 2025 年初启动的 GAC DNS 滥用调查结果。请切换到下一张幻灯片，我们将直接进入主题。

这是一项根据 GAC 关于 DNS 滥用的战略目标 4 而制定的调查。目的是对 GAC 成员开展调查，深入了解各政府对这一主题的期望和关切。同时，作为该主题的负责人，我们可以了解如何通过参与 ICANN 会议以及在闭会期间满足 GAC 员的期望。

我们于 1 月份开始调查，2 月份结束，共收到 21 份回复。幻灯片上展示了地理分布情况，各大洲均有代表参与，当然参与程度也各不相同。在此，请允许我暂停一下，衷心感谢所有回复了 GAC 调查问卷的 GAC 成员，这对我们收集观点确实很有帮助。虽然我们没有具有统计学代表性的样本，但我认为这为我们提供了非常丰富的信息，有助于规划 DNS 滥用缓解方面的工作，以及了解 GAC 成员在与 DNS 滥用缓解有关的具体讨论主题方面的兴趣。

在看下一张幻灯片之前，在了解讨论细节之前，我们想非常简短地介绍一下调查要点，主要有三个要点。大家应该可以知道，调查证实了 DNS 滥用缓解是 GAC 成员的首要工作任务。这一点毋庸置疑。从调查中还可以看出，GAC 成员对这一问题的处理方法多种多样，大家的最佳实践和应对方法各有不同。GAC 成员处理 DNS 滥用问题的方式多种多样，这使得本次调查的结果更加有趣。

调查的第二个要点是，总体而言，GAC 成员对 ICANN 社群和 ICANN 组织为打击 DNS 滥用所做的努力表示赞赏。但同时也认识到，这是一个极其重要和紧迫的问题，需要做的还有更多。我们需要加大力度。调查的最后一个要点是，GAC 成员认为，作为 ICANN 社群的一部分，GAC 在推进 DNS 滥用缓解工作方面可以发挥重要作用。

我们稍后会详细介绍，但 GAC 可以做的工作有很多，包括监督合同修正案的遵守情况、讨论政策发展（这也是我们今天的一项议程）、制定指南、促进 ICANN 内部和外部的合作，以及应对新趋势和分享最佳实践。以上就是主要内容。如果要从今天

的演示中保留一张幻灯片，也许应该是这一张，最重要的一张。现在，我们来详细介绍一下调查的各个部分。请切换——好的，感谢！

调查的一部分内容包括：了解 GAC 成员对 DNS 滥用的定义、针对这一主题有哪些方法和最佳实践，以及他们是否参与了社群合作。正如幻灯片所示，GAC 成员对 DNS 滥用的定义基本上沿用了 ICANN 所做的定义：对调查做出回复的 GAC 成员中有 44% 采用了 ICANN 的定义；但也有少数成员 (25%) 采用了更宽泛的定义，将在线危害和 CSAM 等其他方面也纳入其中；部分受访者目前正在制定定义，但尚未通过。

正如我在前面的要点介绍中提到的，我们从调查回复中还看到，GAC 成员有不同的方法来处理 DNS 滥用问题，这些方法包括立法举措、政策框架、与计算机紧急事件响应小组 (CERT) 一起实施网络举措、与国家和地区顶级域 (ccTLD) 合作、与严格意义上的 DNS 相关 ICANN 社群以外的其他参与者合作。因此，GAC 成员手中掌握着各种各样的工具，这也产生了各种各样的最佳实践。

在收集到的最佳实践中，我们发现了一些解决 DNS 滥用问题的积极措施。公私合作伙伴关系，无论是与注册服务机构和注册管理机构等签约方，还是与来自公民社会等组织的其他方面合作；推动采用安全标准，包括实施经济激励措施、了解客户的举措，以及使用人工智能，这一发现很有趣。我想我们都听说过 AI 在冒名顶替方面的危险，及其在域名系统滥用方面带来的挑战。但调查结果显示，GAC 成员也将 AI 视为应对和减少 DNS 滥用的一种方式。

在社群合作方面，与 GAC 成员开展合作的参与者也非常广泛，包括互联网服务提供商、执法部门、机构、CERT、知识产权机构等。幻灯片上显示，实际上有 60% 的受访 GAC 成员表示他们参与了此类社群合作。我们来看下一张幻灯片。

第二部分内容——请返回前一页。谢谢。调查的第二部分内容是询问 GAC 成员“如何监控 DNS 滥用？”。我们向数据来源提问：GAC 成员从哪里找到有关 DNS 滥用的数据？从回答中我们发现了一些相同点。有些 GAC 成员确实有专门的网站供公众举报欺诈行为；大多数 GAC 成员使用外部来源；还有与政府和非政府机构共享信息；

当然，大部分选择与 CERT 合作；绝大多数 GAC 成员使用 ICANN 作为信息来源，无论是出版物还是我们今天稍后将讨论的 INFERMAL 报告等，这些都是来自 ICANN 社群的不同类型的信息来源。可以看出，大家收集数据的方法各有不同，但我们可以确定一些共同的数据来源。这一点非常重要，因为当我们讨论 DNS 滥用问题时，我们需要了解所使用的证据类型。请切换到下一张幻灯片。

这项调查的一个重要内容是了解 GAC 成员对 ICANN 社群在解决、预防和缓解 DNS 滥用方面所做努力的满意度和评价。我们设置了四个问题，每个问题在某种意义上都针对不同的利益相关方。其中一个要求 GAC 成员评价 ICANN 组织的工作成效；我们还要求他们评估注册管理机构和注册服务机构在承担合同修订义务方面所做的工作；

然后，我们要求 GAC 成员对签约方的工作进行评估。屏幕上显示了具体信息，我们将一一介绍，但可以说，评估结果存在一

定的一致性。对签约方工作的满意度稍低，我们稍后会看到原因。但总体而言，正如我在先前的要点介绍中所说，GAC 成员似乎对社群所做的努力表示赞赏，并对这些努力给予了相当高的评价。我们来看下一张幻灯片。

或许可以更具体地讲讲 GAC 成员如何看待 ICANN 组织在减少 DNS 滥用方面所做的努力。我认为大家普遍感到满意，但同时也认识到进展没有那么快，有效性还可以更高。总体而言，GAC 成员鼓励 ICANN 组织及其新任 CEO 在这一领域设定更加远大的目标。关于对签约方所做工作的赞赏，我认为大家普遍感到满意，大家再次认识到签约方做了哪些工作，而且认为其意义重大。

但我们也了解到，签约方之间仍然存在很多不一致：一些签约方仍然在做最基础的工作，而一些则致力于更有效地解决 DNS 滥用问题。如果想在整个行业取得进步，还有很大的进步空间。当被问及对注册协议和注册服务机构认证协议以及新规定的满意度时，大家强烈表示这是向前迈出的重要一步，但我们目前还没有足够的数据来衡量这些规定的有效性。

但同时，与 GAC 在这一问题上的立场相一致的是，我们认识到这些修订留下了一些空白领域，仍有一些尚未覆盖的领域。例如，修正案没有要求签约方采取积极措施，也没有要求签约方以透明的方式报告他们所做的工作；而且也没有覆盖所有价值链，例如，分销商没有包括在内。部分 GAC 成员还将这一点与准确度问题联系起来。这些都是合同修正案目前没有涵盖的方面，GAC 成员认为这些方面同样重要。请切换到下一张幻灯片。

我想这是我关于调查的最后一张幻灯片了。调查的最后一部分旨在询问 GAC 成员，他们希望 GAC 在处理 DNS 滥用问题时重点关注哪些方面？应优先采取哪些行动？应确立何种目标？尤其是在明年开始的新一轮工作的背景下。我们可以将 GAC 成员的答复归纳为四大类，大家可以在屏幕上看到。一方面，GAC 在跟进和监督合同修正案的执行方面发挥作用；要与 ICANN 合规部门联系；确保在下一轮次新的参与者进入之前，解决 DNS 滥用问题的标准有所提高。

第二，有针对性的政策发展也很重要。我想我们早些时候也与 ALAC 讨论过。在不同的领域，有针对性的政策发展可能有助于解决特定类型的 DNS 滥用问题，或在 INFERMAL 报告结论的基础上采取积极主动的措施。我们在考虑制定政策时，可以列出一系列相关主题。

第三大类或者说第三种回复关于 GAC 在制定指南和促进合作方面的作用。我所说的促进合作，指的不仅是要确保 GAC 与 ICANN 内部的其他社群进行交流，还有与 ICANN 外部建立的联系。部分 GAC 成员还认为，必须强调有必要就如何有效解决 DNS 滥用问题制定指南，并在新一轮工作开始前完成这项工作。

最后一类——我认为这也与我们昨天与 SSAC 的讨论有关——GAC 应在应对新趋势和分享最佳实践方面发挥作用。技术发展永无止境，技术创新持续演进。我们需要关注这些技术发展带来的新威胁，包括与量子有关的威胁、冒名顶替，AI 带来的威胁；还需要促进分享最佳实践，包括各 gTLD 和 ccTLD 之间的共享。这确实是一些 GAC 成员所强调的做法。

最后一点虽然不属于其中任何一类，但出现在多个答复中，那就是 DNS 滥用与注册数据（例如数据准确度）之间的联系。这也是我们作为主题负责人在推进工作时需要考虑的一点。这张幻灯片基本上总结了我们作为主题负责人在 GAC 相关专题方面所做的工作，以及我们在讨论 DNS 滥用问题时应该解决的问题。现在，如果有人对上述内容有疑问，我们可以进行简短的问答。交给你了，尼科，请你管理发言队列。

尼古拉斯 • 卡瓦耶罗　非常感谢欧盟委员会代表。你的专业演讲总是令我们获益良多。在我请右边的日本代表宫本发言之前，请允许我先请会场或线上的各位提问或发表意见。大家可以畅所欲言。

玛蒂娜 • 巴贝罗　我想关于刚刚展示的其中一张幻灯片，可能会有关于评价标准的问题。我想问题会是，量表上的 1 究竟代表最好还是最差？答案是，1 表示对相关措施完全不满意，而 4 表示非常满意。这就是我们使用的评价标准量表。

尼古拉斯 • 卡瓦耶罗　感谢玛蒂娜的详细说明。大家可以畅所欲言。还有其他意见、想法或问题吗？我看没有人举手。那就这样，交给你了，宫本。请发言。

宫本友纪　非常感谢请切换到下一张幻灯片。

谢谢。接下来是 ICANN 合规部门的最新进展。我将邀请乐缇西亚进行说明。交给你了，谢谢。

乐缇西亚 • 卡斯蒂罗

谢谢。大家好！我叫乐缇西亚 • 卡斯蒂罗，我是 ICANN 合同合规部的高级主管。非常荣幸借此机会介绍 DNS 滥用缓解要求的最新执行情况。

我事先收到了一些问题，将尝试在后续演讲中回答这些问题。当然，我也很乐意回答任何其他问题。下一张幻灯片。请切换到下一张幻灯片。很抱歉。谢谢。

从 2024 年 4 月 5 日到 12 月 5 日，合规部通过非正式解决方案解决了 204 起 RAA 和 RA 中 DNS 滥用要求的调查。“非正式”指无正式通知。调查结果是暂停了 2,900 多个恶意域名，禁用了超过 365 个网络钓鱼网站。截至 2025 年 3 月 5 日，即上周，我们有 46 项 DNS 滥用调查正在进行中，目前已有 5,400 多个恶意域名被暂停。截止目前，我们处理的合规案件帮助 8000 多个滥用域名得到缓解。

此外，签约方还根据我们的合规案件要求实施了补救计划，以保持合规性。多个注册服务机构和注册管理机构在未收到 ICANN 合规部门的联系的情况下，还主动采取行动打击 DNS 滥用行为，并履行其合同义务。我们目前发出了三份与新的 DNS 滥用要求有关的正式违规通知。我们仅在使用了非正式程序但未得到解决的情况下，才会发出违规通知。非正式流程通常包括三次通知和两次电话，我们会在电话中联系签约方，提供有关事项的信息，以及要求提供合规证据。

但是，如果我们发现以前纠正过的违规行为屡次失效，那么将加快这个过程。在签约方执行补救计划的同时，发出三次违规通知，要求他们当前符合合规要求，未来还要继续。我们还将持续监督和审查。若签约方需要一定时间来实施补救计划，常见做法是延长最后期限，但有特定条件的规定，

例如，如已确认的滥用域名继续活跃，并且该 DNS 滥用持续危害潜在受害者，则不允许延期。下一张幻灯片。

如先前所述，目前有 46 项正在进行的调查。其中约 48% 是由自称信息安全研究人员的人提交的投诉；知识产权律师和品牌保护协会提交的投诉约占 15%；在表格中填写“其他投诉人”的类别占比 13%，这些通常是被冒名顶替的公司的代表；

此外，还有一部分是收到附带域名的钓鱼邮件或钓鱼短信并进行举报的用户；24% 的投诉人选择了其他占比较小的类别，例如，其他签约方、注册人等。下一张幻灯片。

从地域分布来看，大多数投诉人的举报来自于亚洲/澳大利亚/太平洋地区和北美地区，其次是欧洲和拉丁美洲，这些在这张幻灯片上有详细说明。请切换到下一张幻灯片。

除了通过处理投诉来执行所有合同要求外，我们每年还进行两轮审计，每轮审计持续约六个月。在毕马威会计师事务所 (KPMG) 的协助下，合规部审计小组会评估从签约方收集到的数据和关于签约方的数据，以评估合规情况。需要指出的是，审计后也会发出正式的违规通知，而且我们会在每轮审计结束时发布一份报告，其中包括主要审计结果和被审计方名单。

10 月份，我们启动了注册管理机构审计，其中提出了 DNS 滥用缓解要求。审计中提出的问题旨在确认和核实注册管理机构是否了解相关义务，是否制定了必要的流程来履行这些义务。鉴于此，我们在选择审计对象时参考了与 DNS 滥用相关的内部和外部排名。请注意，被选中并不意味着其 TLD 不合规，我们目前正在审查收集到的所有信息和记录，之后将做出是否合规的决定，并将在完成审计后发布报告，详细说明此次审计结果。下一张幻灯片。

最后一张幻灯片总结了我们目前开展的工作。我们计划发布一份记录一年以来执行情况的报告，与半年期的报告类似，其中包含我们从社群收到的有关该报告的一些反馈意见。报告内容还将包括更多有关投诉处理和结果、审计、投诉人培训材料以及我们当前主动执行工作进展的信息。我们正在编写这份报告，尚未确定发布日期，但已经在筹划中。其中还有更多关于执行情况的细节，例如我们最近根据收集到的网络钓鱼活动和其他活动信息主动发起了执行行动。

目前，新的主动执行工作和针对投诉者的培训材料也正在制作中。所有这些都是对我们目前通过投诉处理和审计而开展执行工作的补充。我们承诺遵守新的要求，并将继续报告进展情况。我就说到这里，下面是大家的提问时间。

尼古拉斯 • 卡瓦耶罗　非常感谢乐缇西亚的精彩演讲，为我们介绍了大量细节。我们现在暂停一下，看看会议现场或线上的大家有没有问题或意见。会场和线上都没有人举手。有请 [印度代表] 和加布 (Gabe)

发言。[印度代表]，请发言。请尽量说慢点，[印度代表]，我了解你。为了口译员顺利翻译，请尽量慢一点。

发言人（男，姓名不详） 谢谢主席。鉴于报告强调屡犯者和滥用集群属于少数几家注册服务机构，对吗？无论原因在于定价模式还是批量 API。是否考虑过根据审计结果对注册服务机构进行风险评分？我的意思是，为注册服务机构制定某种星级评定机制，以此区分谁做得好，谁做得不好。

乐缇西亚 • 卡斯蒂罗 感谢你提出的这个问题。请允许我复述一遍，确认我的理解准确。你指的是我在演讲中展示的图表还是总体来说？

发言人（男，姓名不详） 总的来说，我不是针对演示文稿。我的问题是，这些审计或所有非正式报告都明确指出，某些注册服务机构的 DNS 缓解措施非常少，对吗？我理解的对吗？

乐缇西亚 • 卡斯蒂罗 审计仍在进行中，所以我们还没有公布任何结果。

发言人（男，姓名不详） 非正式报告指出，某些注册服务机构——大部分 DNS 滥用屡犯者或滥用群组都是一些注册服务机构，这就是非正式报告的调查结果，我不确定具体是谁。我的意思是，我们是否打算推出某种星级评估指标？根据注册服务机构在 DNS 滥用缓解措施方

面的表现进行排名。就是这样。我不确定你能否回答这个问题或者 [音频不清晰 00:33:34]。

乐缇西亚 • 卡斯蒂罗 我不确定我是否是合适的人选，但我可以从合规的角度给你一个答案，仅限于我们在执行协议中的角色。在合规方面，我们收集了大量数据，并对所有数据进行审查。我之前提到过，我们正在研究这项计划，目前的进度是正在设计这项主动监测、主动执行计划。我们在投诉中收集到的数据，包括模式、多次违规、违规次数多于其他人的签约方等等，所有这些都是我们在设计主动执行工作时要考虑的数据。

我们在通过现有程序开始执行时，总会考虑到各种模式。但我不确定我是否是具体回答你所提问题的合适人选。

尼古拉斯 • 卡瓦耶罗 谢谢 [印度代表]。谢谢乐缇西亚。请安德鲁斯先生发言。

加布里埃尔 • 安德鲁斯 (GABRIEL ANDREWS) 大家好。非常感谢你的演讲，乐缇西亚。我很好奇，你谈到了为这些调查收集和研究的数据量，你提到今年已经有 46 个了。数量很庞大。我想知道贵部门通常要求注册服务机构提供什么样的数据。例如，这些数据是否涉及这 5,400 项恶意要求背后所涉人员的注册信息、注册人信息或账户持有人信息。

乐缇西亚 • 卡斯蒂罗 谢谢提出这个问题。我是乐缇西亚 • 卡斯蒂罗。当我们发起合规调查时，会根据正在调查的投诉的具体义务进行调整。例

如，在处理所谓的数据准确度不足问题时，会调查与数据相关的问题。涉及 DNS 滥用义务时，一般来说，这也取决于具体的投诉内容，我们通常要求——我们提供投诉的副本，我们提供收到的证据的副本，还会提出我们认为注册服务机构或注册管理机构需要解决的任何其他重要问题，然后我们要求他们解释，详细解释合同方对此事所做的审查。了解采取了哪些行动、行动是否恰当、能否缓解、阻止或干扰、为什么选择这些行动，以及如果没有采取任何行动，则需要解释原因并提供所有相关记录。

有时，注册服务机构在解释调查情况时，会根据具体情况解释他们正在采取的所有步骤，其中一些可能设计账户内部检查，作为审查的一部分，他们会向我们解释这一点。要求提供的证明确实要根据调查内容而定。

尼古拉斯 • 卡瓦耶罗　　谢谢。下面请多米尼加共和国代表发言。

发言人（女，姓名不详）　　谢谢主席先生。我想用西班牙语发言。非常感谢乐缇西亚。我有一个简短的评论，还有一个问题。我感觉非常放心。因为在上一届会议上，关于 DNS 滥用的讨论太多了，我们发现并没有解决什么问题。但事实上，根据你们的发言，我可以理解你们要做的工作非常艰巨。正如前一位演讲者所说，你们有大量的请求或投诉需要调查。各国家和地区当然会对你们的工作更加放心。

这些审计和报告是否在网上公布？我们可否查阅？就我们国家而言，基于我们的网络安全战略，基于我们的努力跟踪与监测结果，基于与系统和性别暴力相关的内容，这次审计报告会非常有用。它会是一个很好的材料，可以让我们更多地了解正在发生的事情和趋势。非常感谢

乐缇西亚 • 卡斯蒂罗

谢谢。我是乐缇西亚 • 卡斯蒂罗，将使用西班牙语回答。非常感谢你的评论，也非常感谢提问。我们收集了所有投诉的数据和信息，内容很多；我们接收所有案件，然后着手处理。我们每月都会发布一些报告。这些报告不仅包括与 DNS 滥用有关的义务，还包括 ICANN 合同中规定的其他一些义务。

关于 DNS 滥用，有一份针对性报告涉及我们根据要求采取的行动。该报告每月发布一次，其中包含大量数据，并根据 DNS 滥用类型进行了分类。我们还会发布包含案例或更多背景信息的报告，因为有时如果大家只看到数据，那么会需要更多背景信息或示例。

这份报告已于 11 月 8 日发布在我们的页面上，我们正努力发布另一份包含更多背景信息和示例的报告。我们的想法是将社群从上一份报告中收到的反馈意见纳入其中，我们将在一年后发布该报告，审计部门也将发布各自的报告。以上是对多米尼加共和国代表的回答，非常感谢。

尼古拉斯 • 卡瓦耶罗 请瑞士代表发言。然后为了节省时间，我必须结束发言队列，因为后续还有嘉宾要演讲。瑞士代表，有请。

发言人（男，姓名不详） 谢谢尼古拉斯，谢谢组织本次会议。特别感谢乐缇西亚提供的详实的信息。我只想与大家分享一些与瑞士联邦警察的交流。他们认为合同修订产生了积极影响，这是一个好迹象。与此同时，他们也发现一些注册服务机构并没有真正进行应有的合作，因此，我们对如何才能提高这些似乎不愿合作或似乎想不担风险但获利的注册服务机构的积极性持怀疑态度。是否也有一些直接的方式将这种现象通知给你们，根据这些数据做到合同合规，这将是一个重要的方面。

另外，我们收到的反馈是，来自执法机构的滥用投诉显然并不总能得到应有的重视。这也引起了一些担忧，因为有时即使很清楚这些投诉来自合法来源，但其合法性显然会被讨论。我想和大家分享的就是这些。谢谢。

乐缇西亚 • 卡斯蒂罗 谢谢你的意见。我是合规部门的乐缇西亚。希望我还记得我想说的所有内容。我们鼓励他们向我们提交投诉。我们有一个公开的网络论坛，每年都会收到成千上万的投诉，那里设置了一些问题，目的是收集重要信息，如果投诉是由执法部门提交的，也会在系统内进行监测。因此，我们会收到这类报告，并在系统内进行监测。我们鼓励认为签约方没有履行义务的各方向我们提交投诉。

我们有完善的程序，当非正式阶段的程序 [音频不清晰 00:43:04] 变为正式违规时，我们将通过该程序履行义务，正如我们之前所说的那样，正式违规之后仍未纠正的结果是暂停或终止注册 [音频不清晰 00:43:15]，或者是终止注册协议。我们确实有相应的执行方法。

至于执法部门，我当然鼓励他们与我们联系。我们不希望他们认为我们不重视他们的投诉。我们关注每个人的投诉。我不确定我的推测是否正确，但他们可能指的是，提交投诉时，需要说明他们是否是注册服务机构所在辖区内的执法部门。如果不清楚他们是否在该辖区内，我们可能会要求提供更多信息。这并不意味着我们不会处理投诉，我们一定会处理。但我们需要知道该管辖权是否适用，以确定我们的执行适用于协议中哪个部分，我不确定这是不是你所说的意思。我很乐意在线下与您交流。

尼古拉斯 • 卡瓦耶罗　非常感谢，乐缇西亚。谢谢瑞士代表。现在交给宫本，继续演讲环节。宫本，交给你了。

宫本友纪　非常感谢，非常感谢各位介绍有关 ICANN 合规部门的最新工作进展。我非常期待看到报告发布和后续工作。非常感谢，接下来有请来自 ICANN OCTO 的西昂 • 罗伊德发言，请他介绍 INFERMAL 报告和域名衡量项目。谢谢。

西昂 • 罗伊德

非常感谢，好的。大家好，我在这里。我是西昂 • 罗伊德，我在 ICANN 首席技术官办公室工作。我要介绍的是两项截然不同的工作，一项是域名衡量项目，另一项是 INFERMAL。请切换到下一个幻灯片。谢谢。

首先是域名衡量项目，它是什么？这是一个收集域名数据的系统，并使这些数据以尽可能多的格式供尽可能多的用户搜索、使用和下载。下一张幻灯片。

我们有域级别的数据，然后可以将其汇总到 gTLD 级别和注册服务机构级别，这些是可以搜索的。无论搜索的是实体、域名、gTLD 还是注册服务机构，都可以获得相关的元数据和背景。我们还有一些可共享的域名级数据。稍后我们将看到这方面的示例。还可以在网络用户界面上使用其他一些可视化和图表，以及一些不同的应用程序编程接口 (API)，这些接口支持通过脚本和代码与数据交互，如果这样做更适用于你的用例的话。下一张幻灯片。

我不会一一阅读所有功能，只举几个非常简单的例子。如果你收到一封电子邮件或一条短信，其中包含一个你不熟悉的域名，你可以将其输入。然后会得到一些背景信息，如为其提供支持的注册服务机构和创建日期等，这样你就能知道该域名的存在时间及其 DNS 设置。下一张幻灯片。

大家可以看到，我们是否知道该域名有任何滥用报告，以及我们的哪些信息提供商曾报告过该域名被滥用，同时还附有显示该域名受欢迎程度的趋势图。我们使用 Tranco 的排名，可以帮

助大家了解某个域名的使用情况和受欢迎程度。下一张幻灯片。

还可以在这里进行类似的搜索，但搜索的是 TLD 级别。这时同样可以获得一些背景信息：注册管理机构、该 TLD 的规模以及自上次衡量以来的净变化。此外还可以获取一些统计数据，了解我们检查过的所报告的滥用数量，包括唯一计数和在总数中的占比。下一张幻灯片。

同时还能获得一些其他信息，比如这些滥用报告的趋势，以及我们对相关域名的地理位置定位，这样我们就能看到这些域名的托管地。下一张幻灯片。

接下来是谈到过的共享域名级数据。作为该系统的注册管理机构或注册服务机构，可以访问自己管理的域名列表。在你的 TLD 中，你就是该域名的支持注册服务机构。同样，我们会告知谁举报了该域名，以及举报的滥用形式。在这里我们可以看到一些域名被报告用于僵尸网络、命令和控制、恶意软件，但绝大多数域名被举报的原因是被用于网络钓鱼。下一张幻灯片。

域名衡量项目目前还不是一个成品。我们认为它将在整个生命周期中不断发展，将根据所做的研究，添加新的指标和新的数据源。在这个平台上，我们不仅可以发布研究成果，还可以发布我们从社群收到的反馈。现在任何拥有 ICANN 账户的人都可以使用该平台。现在使用注册 ICANN 会议的账户，就可以访问所有域名衡量项目数据。这里有几个链接，其中有一个次级页面，那里提供了更多细节；还有一些链接是常见问题解答以及提供文档等其他内容；还有一个链接指向我们的网络研讨会，

提供了更多具体信息，并展示该平台的更多功能。下一张幻灯片。

下面谈谈去年末发布的 INFERMAL 研究报告。此前已多次提及。下一张幻灯片。

该项目由 ICANN 资助，是由 KOR 实验室的马切伊 • 科尔琴斯基 (Maciej Korczyński) 教授领导的一个小组与格勒诺布尔大学合作完成的。项目研究了注册政策和实践，以找出攻击者通常选择去攻击的特定 TLD 注册服务机构组合模式。我之前提到过，最终报告已于去年年底发布。如需了解更多详细信息，请点击这一链接，这同样是一个次级页面，其中有实际报告的链接，内容详实且全面。此外，今年早些时候举办了一场扩展网络研讨会。下一张幻灯片。

INFERMAL 的工作方式是研究注册的不同特征。例如，关于定价，当时是否有折扣？可能有。比如说需要注册大量域名，那么每次注册的费用是否会降低？有哪些批量注册设施？再如，是否存在应用程序编程接口？从根本上说，这要看用户与注册流程之间的交互自动化程度如何。支持哪些支付方式？是否接受加密货币支付？是否支持 PayPal 等第三方支付？此外，注册费中还包含哪些其他服务？是否提供虚拟主机服务？是否提供证书？在注册过程中为你提供多少服务？下一张幻灯片。

另一组检查功能可被视为验证或安全实践。其中有些是主动的，例如，在接受注册付款之前验证联系方式。存在哪些限制？是否需要在注册地所在的国家、地区或司法管辖区有当地

机构？需要哪些文件？为了防止注册明显会遭到滥用或明显可能遭到滥用的域名，可能会采取哪些主动措施？

例如，包含 Office 365 或 Facebook 类似字符串的域名更有可能成为网络钓鱼的目标。是否在购买域名之前对此类情况进行过检查？在采取主动措施的同时，我们还研究了一些被动措施，如正常运行时间——在滥用内容以某种方式得到缓解之前，被报告的域名还能活跃多长时间？下一张幻灯片。

研究中使用了各种不同的数据集。我就不一一介绍了，主要使用了多种第三方数据。有些是人工收集的数据，这些只通过程序查看哪些可用；有些是主动衡量数据，如 DNS 衡量数据、WHOIS 衡量数据等。下一张幻灯片。

报告本身非常详细，所有数据都给出了具体信息和来龙去脉。我无法在五张幻灯片中将其展现出来，这只是对报告内容的粗略介绍。与滥用增加相关性最强的是 API 的可用性，即自动化；提供的额外服务，如 DNS 托管或网站托管；以及注册折扣。从另一个方向看，与滥用缓解最相关的是主动措施，如在购买域名前验证联系方式，以及注册限制。

最后，作者在介绍这项工作时还特别指出了两点，即域名对攻击者的吸引力很可能是多种因素共同作用的结果。没有任何单一因素会单独成为滥用程度的决定性因素。此外，根据这些数据做出的任何决定都必须考虑其他影响。举例来说，某项决定可能会降低攻击者对特定 TLD 和注册服务机构的攻击，但会对合法用户造成影响。任何措施都会同时影响合法用户和攻击者，而且任何攻击者都有可能对所采取的措施做出反应。

最后，我想对科尔琴斯基教授和他的团队表示感谢，感谢他们所做的庞大的工作量，感谢他们编写的这份非常全面的报告。现在请大家提问。谢谢。

尼古拉斯 • 卡瓦耶罗 非常感谢你的讲解，罗伊德先生，确实非常有趣，尤其是关于电话号码和电子邮件地址要求这些常见因素如何缓解 DNS 滥用现象的解释。看看大家有没有什么问题。下面我们有五分钟的简短问答环节。大家可以畅所欲言。我看到会议室后排有人举手。请使用麦克风进行提问。

亚历山大 • 乌贝里斯 (ALEX URBELIS) 好的。我是来自以太坊域名服务的亚历山大 • 乌贝里斯。我有一个关于域名衡量项目以及跟踪的威胁主体体统计数据的问题。你提到正在跟踪主机的实际位置。根据我跟踪众多威胁行为者的经验，主机往往隐藏在 Cloudflare 之后。那么，你们是否有任何方法从 Cloudflare 获取实际主机信息，或者你们只是跟踪指向 Cloudflare 的 NS 记录并将其视为主机。

西昂 • 罗伊德 只是对被举报滥用域名的已解析 IP 地址进行地理定位。是的，我们知道数据中会有不准确、不一致的地方，但有可能会显示出一些出乎意料或令相关方感兴趣的结果。

亚历山大 • 乌贝里斯 好的。那么这些数据是在项目中实时更新还是事后更新？

西昂 • 罗伊德	每天更新。
亚历山大 • 乌贝里斯	明白了。
西昂 • 罗伊德	每天都会更新。
亚历山大 • 乌贝里斯	如果我理解正确的话，我们可以举报一个域名，ICANN 会进行调查，并每天更新域名衡量项目数据？
西昂 • 罗伊德	数据输入队列是我们向系统输入的信誉拦截列表。
亚历山大 • 乌贝里斯	我明白了，谢谢。
西昂 • 罗伊德	不客气。
尼古拉斯 • 卡瓦耶罗	感谢你提出这个问题。接下来请万国邮政联盟 (UPU) 代表发言。有请特雷西。

特雷西 • 哈克肖 (TRACY HACKSHAW)	谢谢尼科。我是特雷西 • 哈克肖。我刚刚查看了一下项目网站，不知道是否有机会进行比较，似乎一次只能做一个。有没有可能对 TLD 进行比较，例如比较两个 TLD？会推出这个功能吗？
西昂 • 罗伊德	如果与图表互动，当前就能实现这一点。你可以在会后找到我，我来进行演示，我很乐意为你演示。
尼古拉斯 • 卡瓦耶罗	谢谢 UPU 代表。在我们继续之前有没有其他的问题或意见？特雷西，你是之前举的手吗？噢，好的。谢谢。再次感谢大家！交给你了，宫本。抱歉，非常抱歉。请柬埔寨代表发言。
发言人（男，姓名不详）	大家上午好。我叫 [音频不清晰 00:59:48]，来自柬埔寨。我想向 GAC 主席提问。我想问的是，GAC 或 ICANN，目前是否有任何规定或指南来打击 DNS 滥用，或是否有任何法规性决定可以防止 DNS 滥用？因为今天上午谈论了调查、合规性和缓解措施，但没有提到关于防止 DNS 滥用的规定。这就是我的问题。谢谢。
尼古拉斯 • 卡瓦耶罗	感谢柬埔寨代表的提问。我不确定是否理解了你的问题。请你重复一遍，可以吗？

发言人（男，姓名不详） 我的问题是，GAC 或 ICANN 是否有类似防止 DNS 滥用或打击 DNS 滥用的规定或指南？

尼古拉斯 • 卡瓦耶罗 简言之，没有。GAC 没有任何具体的规定。ICANN 和 NetBeacon Institute 以及许多其他机构都提出了许多建议。当然，我们可以为你指出正确的方向，包括域名系统安全协议 (DNSSEC) 的实施，我们在 ICANN 内部有一个非常出色的团队，可以在这方面为你提供帮助。不仅有 DNSSEC 的实施，还有资源公钥基础设施 (RPKI) 和许多其他措施，例如《路由安全相互协议规范》(MANRS)，这些都可以在你的国家实施。没问题。但 GAC 本身并没有任何针对性指南。不过预先准备一系列措施也不失为一个好主意。再次感谢柬埔寨代表的提问。由于时间关系，再次交给宫本。请继续。

宫本友纪 非常感谢你提供来自 ICANN 的信息。非常感谢，现在进入专家组讨论环节。欢迎特邀专家：NetBeacon 代表格雷姆、CPH 代表雷哲与鲁克、SSAC 代表杰夫。请切换到下一张幻灯片。谢谢。

幻灯片上展示了今天的讨论主题。我们询问了专家组成员对 INFERMAL 和域名衡量项目的反馈。ICANN 社群考虑如何进一步解决 DNS 滥用问题，以及所需的其他数据和该领域的趋势等。专家组成员格雷姆、雷哲和杰夫将首先就这些主题进行演讲或简短评论，然后我们开始讨论，之后是问答环节。首先有请格雷姆。

格雷姆 • 本顿 (GRAEME BUNTON)

谢谢。我是格雷姆，是 NetBeacon Institute 的执行董事。我们致力于通过减少恶意域名来提升网络空间安全性。我汇总了几张幻灯片。为了节省时间，我尽量快一些，因为我知道在座的同事们都希望有时间提问。下一张幻灯片。

首先是对科尔琴斯基教授、ICANN、莎曼内 (Samaneh) 和整个 OCTO 团队为 INFERMAL 所做的工作表示敬意。这是一份非常出色的报告。它很有趣。它很重要。如果说我对报告有什么意见的话，那就是他们比我先完成了报告。这是我们非常想做的工作，他们却抢在了前面，这很棒。该报告的一大亮点是，它真正凸显了 DNS 滥用所涉及的复杂性。INFERMAL 确定了 73 个不同的特征，都是 DNS 滥用的重要因素。想象一下，注册服务机构可以调整其中任何一个因素，各调整一次都会引起相互作用。因此，这就是我们思考这个问题时需要考虑的背景。下一张幻灯片。

INFERMAL 提供了有关 DNS 滥用率问题的具体数据，而作为社群，我们长期以来一直认为这些问题与 DNS 滥用率有关。我们现在有了一些可以借鉴的数据。不用说价格问题，不受限的 API 肯定是一大惊喜，这些是我们从数据中获得的惊喜。出乎意料的是，注册服务机构的缓解速度与滥用率之间的关系竟然很低。我一直以为，如果注册服务机构能够快速、积极地缓解滥用域名的问题，那么他们对恶意行为者的吸引力就会降低。而 INFERMAL 报告指出二者并没有很强的关系，我认为该报告对这个社群也很有参考价值。下一张幻灯片。

那么，作为一个社群，我们应该做些什么呢？我认为，大家非常关注关于滥用的政策制定流程 (PDP)。我认为在启动之前，需

要制定一些原则。我刚刚听到 GAC 关于 DNS 滥用的调查，调查中发现的问题之一是如何更快地取得更多进展。该怎么做呢？首先要确定一个可以逐步取得进展的具体问题。我们不能单单就滥用问题启动一个 PDP，这个问题太大了，它不会有效果，而且将耗时数年，最终会让大家失望。

我们需要做的是找出一个具体的问题，在极具针对性的范围内来解决，范围应该非常非常小。小到几乎要让大家感到不适，因为会认为结果似乎是注定的，原因在于我们把范围缩小到可以在短时间内取得有意义的进展，然后继续下去。我们不断地把球往场上推进。抱歉，我用了一个体育方面的比喻。这样我们就能改善每个滥用情况，然后无论确定何种 PDP，如果我们达到了目标，就需要确保它与技术和商业模型无关。这样才能适用于整个生态系统。下一张幻灯片。

在我们具体规划这项工作时，还要考虑几点。必须清醒地认识到：犯罪分子更快、更聪明、更不受限。在这方面，他们往往比我们有更多的资源，他们不会按我们的规则办事。因此，我们不能制定具体规定，类似于限制特定服务等。犯罪分子会在数小时内自动适应，而我们制定政策却需要数年。我们知道，他们已经在针对不提供免费 API 等服务的注册服务机构编写脚本并实现自动化。技术发展日新月异，更容易使用。那我们该怎么做呢？

我认为，我们需要确定潜在的政策变化，激励注册服务机构根据具体情况调整现有因素——73 项功能。他们要找到实施摩擦的方法，以此影响犯罪分子，但不会影响良性注册人。我们需要确保这些措施是可执行和可审计的。看看能否把这一点说得

更具体一些。如果你读过 INFERMAL 报告，并且认为免费 API 访问的确会提高滥用率，那么请不要再考虑这些 API 的具体限制。但实际上，我们该如何让注册服务机构在选择允许谁访问这些功能时更加谨慎呢？

我认为，这正是我们可以制定有效应对政策的领域，这些政策可以适应市场，不仅可以缓解现有的滥用现象，还可以应对未来可能出现的滥用。最后，我想就数据和滥用报告谈几点看法。[音频不清晰 01:08:46] 可以全天候向注册服务机构和注册管理机构发布滥用报告。我们通过名为“MAP”的数据项目进行监测，该项目与域名衡量项目非常相似。该数据项目目前还处于初期阶段，还不能下定论。虽未经过严格实证，但我们开始看到合同修订后的缓解率在上升。因此，我们将继续仔细研究。我们也会继续向社群发布内容，鼓励大家每个人都去查看。以上就是我的意见。谢谢。

宫本友纪　　非常感谢你的意见。请雷哲发言。

雷哲 • 莱维 (REG LEVY)　　谢谢你，也谢谢格雷姆。我是来自域名注册服务机构 Tucows 的雷哲 • 莱维。我想说，关于欧盟代表在发言中提出的一些问题，欧盟代表要求建立一个网站，供大家集中提交举报。这就是格雷姆所做的工作。NetBeacon 是一个向所有注册服务机构举报域名滥用的集中门户，不必专门寻找特定的注册服务机构。我只想强调这一点，因为我知道这是欧盟代表刚刚提出的一个具体要求。

格雷姆 • 本顿 感谢雷哲。

宫本友纪 谢谢。接下来有请杰夫。

杰夫 • 贝瑟 (JEFF BEDSER) 谢谢。本周早些时候，我已经与 SSAC 以及 GAC 沟通过，我只想强调几点。INFERMAL 研究报告非常宝贵。再次赞扬 OCTO 的研究人员受委托编写的这份报告。但正如我刚才所说，这不是一份建议性报告，而是一份研究结果报告，它向我们证实了一些我们长期以来一直怀疑的事情。可以确定的是存在经济考量。人们总是购买最便宜的资源，总是使用最容易获得的资源，无论是用于犯罪还是其他用途。

当我们审视网络犯罪时，我们看到的是每年 1 到 10 万亿美元的生意，而其中大部分是使用域名实现的。犯罪分子利用域名从事犯罪活动，从各国公民手中窃取钱财，其诱因很简单，他们总是会选择最便宜的域名。如果将最便宜的域名定价为 1000 美元，而他们从每个域名获取的利润高达数十万美元，那么对他们的收入不会有太大影响。但你会让世界上的所有人都买不起域名。

因此，在我看来，真正的解决方案不是如何阻止域名被滥用或出售，因为网络犯罪的经济规模高达 10 万亿美元，我们几乎无法阻止域名的出售。不过，我们能做的是努力改进检测和举报工作。在当前环境中，看看大多数举报和用于衡量这一问题的

RBL，有五到七个，有时是八个。他们关注的只是冰山一角，在座各位几乎都能拿到这些公开数据。

每家注册服务机构和注册管理机构每年都会收到成千上万份举报，这些举报从未出现在域名列表中，他们会据此采取相应行动。另一个现实情况是，在座的每一个人都曾收到过网络钓鱼或网络诈骗，但没有举报，只是删除了它，如果你否认，请举手。今天大概就有五次。大量滥用未被举报，我们不知道具体数量。但我们知道这个问题非常严重，打击滥用的最好办法就是作为一个社群来建立更好的检测模型。检测和报告的速度越快，缓解的速度就越快。在社群内开发技术，快速衡量证据，这也是新合同义务中的一项内容，即举报必须附有证据。

这是为什么呢？因为签约方和 ccTLD 在获得有据可依的举报后，可以更快地开展工作，不必重新调查举报，不必核实内容。他们可以根据举报证据，迅速确定能否解决，然后据此采取相应措施。所以，这就是我们需要前进的方向。我认为，INFERMAL 报告做得非常出色，它明确指出，在经济领域，网络犯罪现实经济考量是，其规模是广泛的，而解决方案将基于更完善的举报体系和更有效的滥用检测。谢谢。

宫本友纪　非常感谢你的意见。现在进入问答环节。有没有任何问题或意见？雷哲？

雷哲 • 莱维　谢谢。注册服务机构利益相关方团体代表雷哲 • 莱维。我还想强调杰夫和他的团队所做的出色工作，他的技术为 NetBeacon

的许多产品提供了支持。他们与 CleanDNS 密切合作。来自欧洲的代表提出了使用 AI 模型来帮助打击 DNS 滥用。作为注册服务机构，我们发现，LLM 带来了更多 DNS 滥用。这很有趣。但杰夫的团队确实有 LLM 工具，可以帮助我们获得更多信息，从而更好更快地采取行动。

尼古拉斯 • 卡瓦耶罗　感谢雷哲。大家可以自由提问或发表意见。是的，请讲。请拿起任何一个麦克风，提出您的问题。

迪恩 • 马克斯 (Dean Marks)　非常感谢，我是来自知识产权选区的迪恩 • 马克斯。我有一个问题想问杰夫，你强调了举报和检测。我想问的是，基于你的工作经验，这些似乎都是被动的。你有什么关于主动预防 DNS 滥用的建议或想法吗？你说定价并不重要：如果最低价格为 1,000 美元，网络犯罪分子仍然会迅速购买域名。这意味着定价对网络犯罪并不重要。你能介绍一些主动预防措施吗？了解你的客户是一种有用的预防方法吗？以上是我的问题。关于预防措施以及你对它们的看法。

杰夫 • 贝瑟　感谢迪恩。这个问题问得很好。根据历史经验，通过身份验证和认证来更好地了解客户是个不错的流程。我想我在本周之前的一次演讲中提到过。我认为，生成式人工智能的现实意义，就是可以利用它来创建看似与你所需身份一模一样的身份，使用一个真实的人名，但是其他人的照片，就是这样，而且现在

已经实现了。因此，如果每个人都进行身份验证，那么你将不会看到这种问题。

犯罪分子会找到那些尚未实现身份验证的地方，他们已经有了解决这个问题的办法。如果他们真的想要一个带有特定扩展名的域名，因为这个扩展名可以帮助他们说服别人相信自己，从而达到危害的目的，他们就会通过这个过程来获得该域名。事实证明已经有这种现象了。

我认为关键在于，我已经看到了注册服务机构和注册管理机构在这方面的努力，期待看到更多的合作。每家机构每年都要处理数十万甚至数百万份举报，而与每份举报相关的底层基础设施都可以成为一种模式，能够用于检测更多的举报。因此，当不良运营商注册了一个域名，而 Tucows 发现并在共享中关闭了这种模式时，其他注册商都可以看到这种模式，并表示，不，这给系统带来了一些摩擦，我们不允许这种情况继续发生。

社群开始合作，就会发生此类事件，因为域名存在时间很短，对吗？他们注册，又在一年内放弃使用。基础架构的维护和信誉保持的成本要高得多。因此，这里存在一个摩擦点，我认为还有一些其他值得关注的工作。关于支付处理商，很多支付处理商的网站，无论是假冒商店还是网络钓鱼，如果他们以任何方式使用信用卡设施，其商家账户都可能成为攻击目标，因为他们也很难被发现并遭到关闭。

因此不仅仅要关闭用作前端的域名，如果你能在支付处理方面也对它们进行攻击，就既能够夺走它们持续不断获取域名的工具，又能够让它们更难处理窃取的资金。

尼古拉斯 • 卡瓦耶罗 谢谢杰夫。在交给英国代表发言之前，格雷姆，关于这个问题，你有没有什么要补充的内容？

格雷姆 • 本顿 谢谢尼科。我是 NetBeacon Institute 格雷姆。我会尽量简明扼要。杰夫在这个问题上已经说得很好了，我只想强调，INFERMAL 报告中涉及的一点是，它强调增加 KYC 似乎也会导致身份窃取的增加。我们也看到人工智能越来越熟练于生成令人信服的假身份。因此，我自己有点不太相信这可以成为解决办法，它可能是大解决方案的一部分，但我不知道它能解决多少我们希望解决的问题。

我认为在 ICANN 外部还有其他一些有趣的机会有待探索，探索欺诈与滥用之间的关系，以及看看我们是否可以拥有相关技术和工具。但是，本周我与某方面交谈时，他们说自己所有的滥用行为都是使用合法信用卡购买的，这让我大吃一惊。由此可见，现有治理手段的交叉覆盖范围，尚未达到我们期望的状态。谢谢。

尼古拉斯 • 卡瓦耶罗 谢谢格雷姆。很抱歉让你久等了，英国代表。有请奈杰尔发言。

奈杰尔 • 希克森 (NIGEL HICKSON) 没关系。非常感谢大家为这次会议献言献策。我在想，这是一个极其复杂的领域，显然有很多事情正在发生。但是，我们的对手在钻研如何进行外国欺诈行为和网络犯罪等新问题。我认为 INFERMAL 报告非常有用。我记得在几年前关于批量注册的讨论中，当时还没有真正的证据，但现在我们有了。显然，我们

不会——至少今天下午不会通过一项建议——GAC 要求所有域名定价必须达到 100 美元或类似标准。这些都涉及市场竞争维度，难以解决。

但我记得，我们早些时候与 ALAC 讨论过这个问题，在某些领域，特别是在进行批量注册时，可能会有一些关于批量注册政策制定过程的空间，也许注册完全可以是免费的，也许注册服务机构为某个域名提供免费注册。这样一来，也许会有额外问题。这样做的原因可能是要举办某项体育赛事或建立一所新学校等等，这些过程中需要获得新域名。当然，有很多合法用途。但我认为，我们需要在前端做更多的工作，以了解发生了什么。谢谢。

雷哲 • 莱维 注册服务机构利益相关方团体代表雷哲 • 莱维。非常感谢奈杰尔。我们正在与编写发布 INFERMAL 的团队一起研究批量注册的问题，在这份报告中，我记得它的定义是一次注册 50 个域名。如果我们决定禁止同时注册 50 个域名，那么犯罪分子就会一次性注册 49 个。因此，我们接下来要做的是，他们想知道 INFERMAL 的数据是否以某种方式变为不良数据，他们——我指的是参与 INFERMAL 的一些域名注册服务机构——会提出一些假设；然后我们将检查我们看到的数据，并向他们提供是否存在相关性的信息。他们会向我们发送域名列表并提出一些假设。所以，这就是我们现在正在研究的事项。谢谢。

尼古拉斯 • 卡瓦耶罗 感谢雷哲。大家现在可以自由发言。玛蒂娜，趁你还在线上，你有什么想补充的吗？抱歉，杰夫。请讲。

杰夫 • 贝瑟 本周早些时候，我在一次演讲中打了个比方，谈到批量注册，可以将其视为许可模式，对吗？在大多数国家或地区，如果你驾驶一辆小型摩托车，相关要求是临近成年的年轻人可以取得驾驶该车型的驾照。但要驾驶半挂式卡车，我就不在这里把英制换算成公制了，如果是一辆大型半挂卡车，驾照要求要高很多。为什么？因为驾驶这种大型车辆对生命造成的风险要高得多，而任何想要拥有批量注册模式的注册服务机构都必须符合更高的使用和许可标准。

也许，这甚至是像一定数量的资金存置。如果使用不当，就会损失资金。有各种类型的方法，你可以提供针对滥用工具行为的保险，而一旦出现滥用，就会造成巨大损失。我认为这可能是讨论的方向。

宫本友纪 非常感谢专家组的讨论。非常感谢各位专家组成员。最后一项议程是 GAC 讨论。GAC 的讨论其实已经开始了，但我想请玛蒂娜介绍一下，你能为大家解释一下吗？

玛蒂娜 • 巴贝罗 非常感谢，宫本。我们期待本次会议取得丰硕成果。我认为本次会议非常精彩。不过，最后我们还是想向 GAC 提出一些问题，收集 GAC 成员关于以下各项的意见：今天的会议讨论；演

讲嘉宾的演讲要点；本次会议涉及的各项主题；以及本次会议如何影响 DNS 滥用问题的后续缓解工作。

一些参会人员已经特别指出了一些方向。我们非常希望在接下来的五分钟内听到大家对理想的后续步骤的设想。最后，根据 GAC 领导层的要求，我们还可以交流一些考量因素，关于本次讨论后想纳入公报的任何其他考量，以及对未来工作的期望和对新一轮工作的思考。简要回顾一下，正如你们中的一些人提到的，GAC 内部已经就可能的 PDP 进行过讨论，还与其他社群进行了讨论。我听到 ALAC 希望就该事项上与我们开展进一步合作。那么，交给你了，尼科。让我们用最后三分钟的时间看看是否希望在公报中添加任何其他想法。

尼古拉斯 • 卡瓦耶罗　非常感谢玛蒂娜。英国代表希望发言。我看到你举手了。有请。

发言人（男，姓名不详）　是之前举的手，抱歉。

尼古拉斯 • 卡瓦耶罗　哦，抱歉。我们还有三分钟的时间，线上或会场上的各位可以简单提问或发表意见。请大家畅所欲言。请使用麦克风发言。

戴维 • 休斯 (DAVID HUGHES)　知识产权选区代表戴维 • 休斯。我想问杰夫和格雷姆一个问题——比如说，我们发现有一些 ccTLD 的 DNS 滥用率极低，但实际不一定有，那么我们能向它们学习到什么？

杰夫 • 贝瑟　回答这个问题的最大难点是，gTLD 有一套相同的运营规则，而 ccTLD 却没有，而且差别很大。很多时候，低滥用率也对应着低增长率，即它们的处理量并不多，增长速度也没有特别快。但是，在元数据级别上有两种不同类型的滥用，一种是出于滥用目的而注册域名，另一种是主机被入侵然后遭到滥用。在大多数研究中，我们确实可以发现，由于模式不同，ccTLD 中的被入侵域比 gTLD 中的更多。

因此，我认为，在继续关注某些领域的低水平的同时，也要注意某个 ccTLD 的高滥用率，我不想在这里指名道姓，但覆盖了从 G 到 C 的全范围，它们的比例各不相同，其中有很多 gTLD 的滥用率相当低。我不确定我在这方面有什么建设性的意见。

格雷姆 • 本顿　谢谢提出这个问题。这很难回答。回到 INFERMAL 报告，其中处理和研究了 73 种不同的特征。因此，很难说会有一种解决方案，我不认为有。我还认为，只看滥用率是不正确的，因为网络犯罪分子在实施网络犯罪时，有时会出于某种原因选择一个 TLD，而注册管理机构或注册服务机构可能并不确定或没有能力进行相应调整。

因此，我们需要意识到这种复杂性，然后不仅要看比例，还要看缓解率，以及缓解时间的中位数，对整个滥用链进行更全面的审视。谢谢。

尼古拉斯 • 卡瓦耶罗 最后有请雷哲发言。雷哲，请讲。

雷哲 • 莱维 非常感谢。注册服务机构利益相关方团体代表雷哲 • 莱维。这个问题非常有意思，ccTLD 小组和台上的一些人明天将深入讨论。请大家查看日程表，了解更多相关会议信息。但是，各 ccTLD 的政策不同，面对的市场也不同。有些类型的滥用实际上会针对特定的 ccTLD，因为这正是他们获得点击量的途径。因此，正如格雷姆所说，其中涉及各种不同的因素，希望大家参与 ccTLD 会议进行深入探讨。

尼古拉斯 • 卡瓦耶罗 非常感谢。抱歉，丹麦代表，请尽量简短。我们已经超时了。请发言。

芬恩 • 彼得森 (FINN PETERSEN) 感谢，我是丹麦代表芬恩 • 彼得森。感谢最后给我发言的机会。我认为对某些 ccTLD 进行调查是个好方法。我知道至少在一个国家，批量注册被限制在 5 个域名以内，如果超过了这个数量，就需要对申请人的身份进行深入调查。这样会知道很多信息。但从我们今天听到的情况来看，也许 GAC 应该进一步研究，看看能否制订出关于批量注册的 PDP。如果我理解正确的

	话，若通过并实施该 PDP，那么它的范围会相当有限，我们就可以有——可以说——这对 GAC 而言并非难事，是容易实现的。谢谢。
尼古拉斯 • 卡瓦耶罗	非常感谢丹麦代表提出的意见。好想法。我想说的是，范围要小，时间要短。只要不超过五年，我们都非常欢迎。非常感谢你的建议。感谢雷哲、格雷姆、杰夫、宫本、乐缇西亚与西昂的精彩演讲。非常感谢大家！我们即将暂停会议，随后是午餐时间。请大家在下午 1 点 15 分回到会议室。非常感谢大家。本次会议到此结束。
格雷姆 • 本顿	谢谢大家。

[听写文稿结束]