ICANN69 | 虚拟年度大会 — DNS 滥用
中欧夏季时间 2020 年 10 月 20 日（星期四）— 10:30 至 12:00

发言者： 语言服务团队测试。

本次会议将同时使用 Zoom 和 Congress Rental Network 公司负责运营的远程同声传译服务平台。欢迎参会人员下载 Congress Rental Network 应用程序，遵循 Zoom 聊天中的指示，或者遵循会议网页上提供的会议详情文档中的指示。如果你想发言，请在 Zoom 会议室中举手示意，主持人叫到你的名字后，我们的技术支持团队将允许你开启麦克风。为方便记录，请报上名字，如果你不说英语，请说明你将使用的语言。发言时，请将所有其他设备和应用程序静音，包括 Congress Rental Network 应用程序。同时，请大家发言时口齿清晰并保持正常语速，以便口译人员能准确翻译，音频测试到此结束。

如果想让我重新读一遍，请提出来。谢谢。

发言者： 大家好，欢迎各位。我们将在一分钟后开始。谢谢。

发言者： 会议即将开始，请开始录音。

注：本文是一份由音频文件转录而成的 Word/文本文档。虽然转录内容大部分准确无误，但有时可能因无法听清段落内容和纠正语法错误而导致转录不完整或不准确。本文档旨在帮助理解原始音频文件，不应视为权威性的会议记录。

欧赞 • 萨辛 (OZAN SAHIN)： 大家好，欢迎来到 DNS 滥用全体会议，我是本次会议的远程参会经理欧赞 • 萨辛。请注意，本次会议正在录音，请遵循 ICANN 的预期行为标准。

在本次会议期间只有在问答窗格中用英语提交的问题或意见才会被大声读出来。该功能可以从 Zoom 工具栏访问。我会在本次会议的主席或主持人指定的时间大声读出这些问题和意见。

本次会议提供实时速记和口译服务。要查看实时速记，请单击 Zoom 工具栏中的隐藏字幕按钮。本次会议将提供阿拉伯语、中文、英语、法语、俄语和西班牙语同声传译服务，并将同时使用 Zoom 和 Congress Rental Network 公司负责运营的远程同声传译服务平台。我们鼓励与会者下载 Congress Rental Network 应用程序，遵循 Zoom 聊天中的指示，或者遵循会议网页上提供的会议详情文档中的指示。

如果你想发言，请在 Zoom 会议室中举手示意，会议主持人叫到你的名字后，我们的技术支持团队将允许你开启麦克风。为了方便记录，请说出你的姓名，如果你使用英语以外的其他语言，还要说明你要使用的语言。发言时，请务必关闭所有其他设备，包括 Congress Rental Network 应用程序，同时也请清楚地以合理的语速发言，以便准确地翻译。

我要强调一点，没有技术支持团队的协助，远程参会者在本次会议期间无法点击麦克风按钮打开声音。所有参会者都可以在聊天中发表意见，为此请使用聊天窗格中的下拉菜单，选择回

复所有专家组成员和与会人员，这样每个人都能读到你的意见。请注意，在 Zoom 网络研讨会形式下，私聊只能在专家组成员之间进行。标准参会者发送的消息将被主持人看到。联合主持人和其他专家组成员也会看到。接下来将由托马斯 • 李凯尔特 (Thomas Rickert) 发言。托马斯？

托马斯 • 李凯尔特： 非常感谢欧赞。大家上午好，下午好，晚上好，我是托马斯 • 李凯尔特。我是互联网行业协会 (ECO) 的名称与号码主管，ECO 实际上是 ICANN69 的联合主办方之一，我在我的家乡德国在线欢迎大家。我在波恩。我很想亲自去汉堡看你们，但遗憾的是，此时此刻是不可能的了。我希望我们在不久的将来有机会见面，希望大家都平安无事。请转到到下一张幻灯片。

正如欧赞已经提到的，本次会议和 DNS 滥用有关，实际上在 ICANN 的历史上，在波恩召开过很多关于 DNS 滥用的会议，我想这个问题之所以一直困扰着我们，是因为现实中有很多不法活动在互联网上不断发生。很多不法分子都在试图利用用户知识的匮乏，引导或误导他们使用一些非正当的产品或服务，最终造成经济和其他方面的损失。我想对于 ICANN 来说，由于根据 ICANN 章程 ICANN 的职权非常有限，所以这个话题是非常特殊的，这也是为什么我认为有必要继续就 DNS 滥用问题进行对话，了解这个问题是什么，了解互联网生态系统中不同参与者的角色和责任是什么，然后也要看看解决方案或潜在的前进方向是什么。

实际上在本次会议中，我希望可以讨论到以上所有问题，但我们还是要把重点放在解决方案和前进方向上。本次会议将持续 90 分钟，具体方式是先由演讲者进行演讲，我稍后会向大家介绍，然后我们将在每次演讲后暂停一下，看看大家是否在问答窗格中提出了任何问题。我们会尽量回答你们在那里输入的问题，请把这些问题限制在你刚才听到的演讲内容上，这样万一演讲者的介绍有什么不清楚的地方，我们会尽量解决。但在演讲者发言之后，我们将在 90 分钟的会议结束前有一个问答环节，此时你们有机会提出更多的一般性问题。你可以在问答窗格中提问，也可以通过举手提问，然后技术人员会打开你的麦克风，让你加入讨论，在 -- 你知道你也可以口头发言。我的开场白和介绍马上结束，我们很快就可以谈谈 -- 深入探讨一些实质性的原因。下面介绍今天谁将和我们交流 DNS 滥用的信息，第一位是戴维 • 康纳德 (David Conrad)，然后是杰夫 • 贝瑟 (Jeff Bedser)。接着我们将听取梅森 • 科尔 (Mason Cole) 和克里斯 • 路易斯-埃文斯 (Chris Lewis-Evans) 的发言。最后是詹姆斯 • 布雷德尔 (James Bladel)，然后进入讨论，希望大家各抒己见。在最后几分钟，我将试着总结概括会上的内容。请转到下一张幻灯片，简单地概括一下 -- 哦，这已经是戴维的部分了。到这里你们大致了解了今天的会议程序，接下来，话不多说，有请戴维 • 康纳德谈谈 ICANN 对 DNS 滥用的见解。戴维，交给你。

戴维 • 康纳德： 谢谢你，托马斯。请播放下一张幻灯片。在此次全体大会之前，我被要求整理出一套幻灯片，反映从 2019 年 9 月到 2020 年 9 月域名安全威胁的总体形势。如果你看一下 DARR 报告，也就是 ICANN 网站上提供的 DNS 活动报告，这些报告中公布的数据实际上可以追溯到 9 个月前，抱歉这里写错了。但要求是回顾过去一年的情况。所以我的团队整理了一些总体统计数据，在过去的一年里，我们看到网络钓鱼、恶意软件和僵尸网络的数量都减少了，但是垃圾邮件的数量增加了，而且由于垃圾邮件的普遍性，在查看 DNS 滥用的统计数据时，整体有点被歪曲的情况。这一歪曲在于，从 2019 年到 2020 年，这一年的滥用域名数量增加了 13% 左右，但是由于其他各种情况都减少了，所以整体的滥用率差不多保持不变。请播放下一张幻灯片。然而我们在 DARR 内的数据可以追溯到 2017 年 10 月，如果你再往前看，可以看到一些非常明显的趋势。这里的趋势线显示，你知道，gTLD 的数量很明显是上升的，你可以看到，尽管随着时间的推移增减不一，但趋势线是相当明显的。图 2 中显示的是总体安全威胁的数量，也就是我们在 DARR 项目中关注的所有事件，它们都是由僵尸网络社区控制的。网络钓鱼、恶意软件分发和垃圾邮件。可以看到，随着时间的推移，下降趋势十分明显。请看图 3，它基本上根据某个域内的域名数量进行了标准化处理，你会再次看到随着时间的推移呈下降趋势，尾部略有抬升。然后图 4 显示，红色的是垃圾邮件，它仍然占据主导。另外要注意一点，在这 4 张图中，不管是红线还是蓝线，都代表 GDPR 生效的时间。在这些图中

你会注意到，域名滥用数量没有受到任何显著影响，至少从 DARR 的范围内来看是这样。请播放下一张幻灯片。如果我们再看一下从 2017 年 10 月到 2020 年 10 月个别威胁在同期内的表现，你会再次看到趋势线出现了一些有趣的假象。和我在第一页给出的统计数据相似，网络钓鱼、恶意软件和命令与控制都在下降。如果你看回到 2017 年 10 月 20 日，情况恰恰相反，网络钓鱼、恶意软件和命令与控制都在上升，只不过有些缓慢。而同一时间段内垃圾邮件其实是明显下降的。在这些图中，你需要注意务必要正确地比较 Y 轴。所有这些垃圾邮件都比其他所有事件高出一个数量级，所以这一点要警惕。下一张幻灯片。我们在 CTO 办公室收集的另一个数据集是标识符技术健康指标。那是从 2018 年 1 月开始的，我们监测了大量与标识符生态系统健康相关的衡量标准。在这组衡量标准中，有一组特定的衡量标准，M2 衡量标准，是专注于域名滥用的。它显示了自 2018 年 1 月以来，在 gTLD 和注册服务机构中，每 10000 个域名中的滥用数随时间变化的趋势，以及占安全威胁 50% 到 90% 的 gTLD 或注册服务机构的数量。如果你看 ITHI 网站上的表格，它的用户界面也许会让你想起 90 年代初，这里的滥用率显示，例如对于网络钓鱼，在可检测到的网络钓鱼安全威胁中，有 10% -- 10 个注册管理机构占据了 90%。而这一比例是每个注册管理机构 0.3% 和 0.1% 的 ... 这里注册服务机构的数据不可以全信。我们掌握的注册服务机构信息来自于我们的供应商 iThreat，长期以来这些信息被收集到一个数据库中，因为我们无法访问 DARR 系统内与个别域名相关的注册服

务机构信息。这些信息可能已经过时了，所以注册服务机构信息应该只作为一个索引，而不一定是完全准确的数值。另外我要指出的是，注册服务机构，这里的数据 -- ITHI 衡量标准是由 DARR 使用的相同的原始数据，加上一些与注册服务机构相关的信息推导出来的。请播放下一张幻灯片。我们在 OCTO 内开展的另一个与 DNS 滥用有关的项目名叫域名安全威胁识别、收集和报告，简称 DNSTICR。该项目大约从 2020 年 1 月开始，旨在收集与已注册的疫情相关域名有关的信息。在疫情爆发初期有多份报告表明存在大量与疫情相关的注册，并暗示这些注册被用于恶意目的。在 DNSTICR 内，我们只把网络钓鱼和恶意软件分发视为安全威胁。从 2020 年 5 月到 2020 年 9 月，我们一直在收集数据，并对数据进行分析。我们通过自身的系统发现，在检测到的 134,000 个注册中，大约有 1.7% 的注册有足够的可信度，我们称之为有滥用行为的迹象。实际上在 6 月份，我们已开始向注册服务机构报告这些高可信度域名。请播放下一张幻灯片。所以从 2020 年 6 月到 2020 年 9 月的报告期内，有 80,000 个疫情相关域名被注册。其中有 170 个导致有人向注册服务机构发送了报告，表明存在我们所认为的安全威胁行为。关于这一点再解释一下，它意味着该域名已经在域名系统中注册。它至少在一个提供商列表中发现了一个报告，当我们考察实际注册时，域名 -- 抱歉，是与域名相关联的网站，上面有内容表明存在某种安全威胁。我们要做的是尽量减少误报的数量，所以这 170 个报告中，截至 10 月 6 日，有 87 个在域名系统上不复存在。它们被删除了。56 个不再符合报告标

准。要么是域名不再解析，要么是网站上已经没有可用的安全威胁记录。其中有 20 个不解析域名，NS 记录指定的域名服务器不响应 DNS 查询。170 个中仍有 7 个显示为恶意。以上就是我要说的全部内容，我很乐意回答任何问题，如果现在有的话，托马斯。如果没有问题的话，就请你介绍下一位演讲人。

托马斯 • 李凯尔特： 非常感谢，戴维。[听不清]其实我们有几个问题。我不确定现在是否能全部处理，但我们还是试试看。伊丽莎白 • 苏蒂 (Elizabeth SZUDI) 问到了垃圾邮件。这是否表示 ... 非应邀电子邮件，还是说垃圾邮件也会含有和发送其他技术形式[听不清]和或网络钓鱼，垃圾邮件是否也含有或发送其他的滥用形式，不管是以什么方式分类的滥用。

戴维 • 康纳德： 我们掌握的信息源自于可信提供商列表。他们并没有区分垃圾邮件使用的机制是蓄意安全威胁。所以你看到的垃圾邮件相关信息是报告给不同可信提供商的信息。为了让你们了解我们所收集的信息，在我们的 DARR 报告和方法文件中，实际上列出了我们使用的可信提供商和这些可信提供商中的具体信息源。

托马斯 • 李凯尔特： 谢谢，还有两个问题。据我的成员描述，域名滥用增加暴露出的是品牌名称滥用的问题。我觉得这种增长也应该体现在网络

钓鱼上。大部分网络钓鱼都是通过垃圾邮件进行的。这些数字是如何处理这一点的？它们应该是并列的。接下来的问题是，对于十个最恶劣的注册管理机构，将会采取什么合规措施。他们到目前为止的状况如何，谢谢。

戴维 • 康纳德： 关于网络钓鱼和垃圾邮件之间的关系，我们收集到的信息具体来源于代表提供商。如果有人在垃圾邮件中列入了某个事件，而它是网络钓鱼，它是通过网络钓鱼分发，那么它就可能出现在两个不同的类别中，因为它在多个地方进行了报告。我们试图删除这种性质的冗余条目，但是你知道，它是有可能的，在某些情况下这些域名可能会重复。据我所知，这种情况不太可能。对于我们收集到的信息，我们不会以任何方式进行修正。这是我们通过一些不同的供应商汇总而来的信息，如果大家看到与 DNS 滥用和安全威胁有关的不同统计数据，我们将非常有兴趣了解他们是使用什么数据源来获取这些信息的。我们可以利用 DARR 系统，看看能否将这些数据集纳入 DARR 系统以及我们正在使用的其他系统中。关于第二个问题，请大家注意，对 90% 的滥用负责的注册管理机构或注册服务机构的绝对数量，需要放到非标准化数据的语境下理解。这也许并不奇怪，注册的总数量和这些注册中的滥用数量之间有很强的关联性。如果从非标准化数据来看，那么拥有注册量最多的注册管理机构和注册服务机构无疑将拥有最多的滥用域名。实际上最好是在标准化数据的语境下看待这些数据，它们是相对于

注册数量而言的，当你开始看那些数据时，就不太容易发现谁是真正的坏人。

托马斯 • 李凯尔特： 非常感谢。恐怕我们要请出下一位演讲人了。戴维，我建议在我们听取杰夫发言的同时，你也许试着可以在问答窗格里以书面形式回答一些问题。后面的演讲人也一样，对于那些可以解决的问题，我们会尽量在会议结束前回过头讨论。也就是问答环节。我希望大家可以接受这种方式。那么有请杰夫 • 贝瑟。他在 iThreat 工作。杰夫，交给你了。10 分钟。

杰夫 • 贝瑟： 大家早上好，晚上好，白天好。这是工作组于一年前由 SSAC 组建后开展的工作。它有一个非常全面的图表，里面纳入了许多我们还没有涉及到的关于 DNS 滥用的其他问题。这是我们拿出的第一个涵盖 DNS 滥用问题的工作成果。这是一份尚未公布的文件，这份 SSAC 文件有望在未来几周内发布。我们原本希望在 ICANN69 上发布，但是内部流程还没有完成，所以我们希望尽快将它发布出来。请播放下一张幻灯片。首先我想确认一下，SSAC 在这个特殊工作成果中所做的事情之一，就是我们邀请了 SSAC 的责任审计员嘉宾加入到工作组中。这些嘉宾来自注册管理机构利益相关方团体的 PSWG，有些嘉宾带来的技能和知识帮助我们更好地理解了一些政策问题以及一些滥用处理问题。抱歉，翻译应用刚刚才启动。所以这个小组是由

SSAC 的内外部人士共同组成的。这给我们带来了一群有政策背景的人。他们拥有处理 DNS 滥用的背景，还有的人来自像注册管理机构、注册服务机构和内容分发网络这样地方，因此给了我们一个很好的起点。你们听到戴维 • 康纳德讲到了一点，就是关于滥用数据的测量，这种测量的一个要点不仅仅在于它在现在或过去的某一天存在，而是在于 DNS 滥用问题究竟存在了多久。域名滥用存在的每一个小时和每一天，就有可能产生更多的受害者。更多的受害者意味着更多的损失等等，在后面的演讲中，你们将看到克里斯托弗 • 路易斯-埃文斯 (Christopher LewisEvans) 带来的关于 DNS 滥用造成损失的数据。但互联网本身的滥用就已经到了令人堪忧的程度。你们可以从董事会、媒体、内部或执法机构获得各种各样的报告，但毫无疑问，DNS 滥用是存在的。任何人都不应该指望 DNS 滥用会停止，因为它是 ... 网络犯罪将一直继续。只要有受害者，犯罪就会继续。我们正在解决的问题是信任被侵蚀，互联网最终用户，无论是商业、个人还是非商业性质，不管他们从事什么活动，都需要信任这个系统，他们需要信任系统和服务提供商，以及基础设施。即将公布的报告将概述一个减少 DNS 滥用的策略。这一努力是为了推出最佳实践，只有在大多数实体的合作和理解下才能实现。DMOOEP 提醒，那些签约方和 ICANN 只是被用来实施侵害的整个 DNS 系统的一小部分。他们是托管服务提供商。有电子邮件提供商。有内容分发系统。在这个结构中被利用的地方多种多样，而签约方只是整个生态系统的一小部分。请播放下一张幻灯片。所以文件的要点如下。

鼓励对滥用进行标准定义。文件没有试图重新定义或应用新的定义，而实际上是从现有定义出发，这些定义是用本地语言写成的较好的定义。它们描述了这个问题。当你在处理一个问题时，拥有一套标准定义当然是推进工作的最佳方式。其次是确定解决滥用问题的适当的首要责任方。每一类滥用都有其特殊性，适合解决它们的地方或许是在注册管理机构层面。或许是在托管层面。也可以是这个生态系统中的任何地方，但某些类型的滥用总是会有一个最适合解决它们的地方。确定最佳实践以便部署证据标准，这是一个十分棘手的问题。不同司法管辖区的法律标准对证明某个事件存在问题、属于欺诈或属于犯罪，有着不同的证据要求。但是，如果有证据标准表明该事件是命令与控制僵尸网络所为，这时你就需要向你要求对该僵尸网络域名采取行动的任何一方证明它是僵尸网络。建立标准化升级路径来解决滥用问题，在这里我们都要明白，每个域名都有生命周期 ... 在解析它的整个过程中有不同的参与者。现实情况也是，有些地方你会得到一个无响应的实体，而该实体是解析域名的首要责任方。因此，建立升级路径允许不同的实体进入生态系统，并指示它们去寻找一个它们无法联系上的托管服务提供商。它们没有可用的联系信息，或者对联系人无响应。适合下一方尝试前往已解析域名的升级路径在哪里。这也是为了减少受害状况，域名运营的时间越长，受害者就越多。确定合理的行动和滥用报告时间框架。按照现在的升级路径，大多数方面允许他们报告的对方有 24 小时进行响应。因此，如果一方报告滥用，表示我有域名进入了生态系统的错误部

分，而那要转介 3 次，就可能要 72 小时以上才能使一个域名得到解析。所以确定一个合理的行动时间框架也会减少域名运营的时间。我们也在研究制定通知人计划的建议，这些程序将加快并高效处理滥用系统的某些部分。现在有很多商业实体和非营利性实体确实会检测滥用并报告。但我们在工作组注意到另一个有趣的趋势，随着越来越多的消费者和品牌开始检测滥用行为并雇佣公司检测滥用行为，报告滥用行为的公司数量正在上升，而且有大量的新参与者正在报告滥用行为，以了解服务条款和 DNS 服务的运作方式。通知人计划将在这方面带来帮助。... 在 GDPR 内，它不是。这关系到实际处于不同域名控制点的实体。有时，滥用联系信息很容易找到，但有时则不然。机制，允许通知人轻松找到向谁报告域名问题并提供证据的信息，这将使生态系统如虎添翼，并最终建立一个合理保障联系信息质量的机制。保持这些信息最新并及时更新。保持信息的可用性。所以，再次说明，我希望这份报告在未来几周内由工作组主席向全体社群发布，并期待大家的反馈。现在，托马斯，交回给你。

托马斯 • 李凯尔特： 非常感谢杰夫，撇开内容不谈，你很好地把时间控制在了我们分配给你的十分钟之内。非常好。我看到问答窗格中的讨论主要是针对戴维的后续问题，所以如果你们有问题要问杰夫，请把问题输入问答窗格，我建议杰夫和戴维一样，如果问题是提给你的，请尽量在问答窗格中以书面形式回答，这样我们就可

以继续有请下一位演讲者。那就是梅森 • 科尔 (Mason Cole)。梅森是 CSG 的成员，他将代表商业利益相关方团体和博钦律师事务所，谈谈 CSG 的观点和 DNS 滥用。交给你，梅森。

梅森 • 科尔： 谢谢，托马斯。你们能听清楚我说话吗？谢谢。好的，大家上午好，下午好，晚上好。我开始了。我想我不需要 10 分钟，但还是要看讨论的情况。请播放下一张幻灯片。所以我们在这里要再度讨论 DNS 滥用的问题。正如杰夫和其他人所指出的那样，这个问题并没有真正地消散，可能永远不会。我们看到它年复一年地定期发生。它被外部事件放大了，比如我们在今年春天 3、4 月份看到的 COVID 爆发。有时在国家灾难发生期间也会看到它。像内乱。还有其他世界性问题。当然，所有这一切的共同主题是，DNS 被用于非法目的。这是 ICANN 第 4 次 -- 我相信是连续第 4 次就 DNS 滥用召开全体会议。如果我们能够继续富有成效地讨论这个问题，同时也讨论我们能够带来哪些富有成效的解决方案，以便真正对 DNS 滥用做些什么，减少其发生，我想这对我们很多人来说都是有利的。请播放下一张幻灯片。好的，所以在统计领域，似乎人人都要做的就是，真正地去看和去分析 DNS 滥用，你会发现各种各样的统计数据。最近引起 SSAC 注意的是 Interisle 咨询集团在几天前公布的一组统计数据。研究期间，即今年的 5 月 1 日至 7 月 31 日，重点关注了网络钓鱼，但报告影响了超过 99,000 个唯一域名、439 个顶级域名和 414 个注册服务机构。而在这一总数中，Interisland 确

定了超过 60000 个恶意注册的域名，因此我们知道存在的网络钓鱼问题可能比报告的更为严重，尽管具体规模未知，并且 WHOIS 日期的编辑导致了对问题的检测不足。下一张幻灯片。因此，根据 SSAC 我们知道，DNS 滥用及其最终导致的网络犯罪继续造成每年数百万人深受其害，并降低了人们对互联网的信任度。我要强调杰夫之前谈到的。这涉及到对互联网基石的信任，即 DNS 能否成为一个值得信任的检索信息、开展业务和完成工作的地方。所以作为一个开展个人和非商业业务的地方，我们有这种信任很重要。请播放下一张幻灯片。谢谢。统计和我们应该一致同意的地方。我认为我们大家都可以带来不同的讨论角度，因为显然我们已经召开了 4 次会议。DNS 滥用可能在上升或下降，具体取决于你的数据来源。但我们可以也应该同意的是，当滥用确实发生时，会对我们讨论的互联网信任产生影响，因而它需要一个主动的、数据驱动的补救措施。这里我强调主动。我们有机会更主动、更坚决地去处理 DNS 滥用问题。而且我想避免在 ICANN 内部掀起一场争论，关于是否 -- 不是我们是否应该打击 DNS 滥用，而是我们如何谈论 DNS 滥用。这不是一场我们应该互相挑起的战争。我们应该一致对外，针对不法分子采取一些措施。请播放下一张幻灯片。因此，正如其他人所说，这方面已经取得了进展，我想再次特别表扬今年早些时候 — 我想也许是去年 — 开始实施的注册管理机构和注册服务机构自愿框架。它对 DNS 滥用产生了可衡量的影响，应该予以表扬。所以我想花一点时间认可签约方在这种情况下完成的出色工作。下一张幻灯片。有些地方还没有取得

进展，我们还有改进的空间。自愿框架很棒。但是它们并非完全包容。而且我们知道，仍然有那么 8 到 10 个经常被提及的不法分子，ICANN 说它知道他们一般会藏在哪里。你知道，从容易的做起，追踪已知的不法分子，在签约方已建立的框架之外对滥用采取一些措施，将是一项十分有用的工作。请播放下一张幻灯片。所以让我们回到蒙特利尔。去年的这个时候，我们举行了第一次关于 DNS 滥用的全体会议。我想提一下 Tucows 的 ... 的发言，我觉得很有用。我们需要处理我们面前的问题，如果合规团队 — 他指的是 ICANN 合规团队 — 能够有效识别合同中的一些具体要素，这些要素将有助于他们对我们都知道存在的、明显的不法行为采取强制措施，那么让我们展开讨论。合规团队处理的是我们一致同意应当处理的已知不法行为。我想提出这个观点，因为这又是一个我们可以在这里提出的主动解决方案，可以利用我们已有的一些工具来识别不法分子并追究他们的责任。请播放下一张幻灯片。好，这是我的最后一张幻灯片。所以，一个人当然不可能一步登上珠穆朗玛峰。而要一步一步来，分阶段进行。同样，我们也有机会分阶段处理 DNS 滥用问题。除了即将发布的 SSAC 建议，这里还有一些关于我们可以针对滥用采取什么措施的意见。一举清除在空间中制造最大问题的那 8 到 10 个不法分子，我们现在就可以利用手中的工具做到这一点。我们可以同时或以后讨论滥用的定义，以及是否需要工具。我们可以考虑为那些运行“干净”注册管理机构和注册服务机构的运营商提供激励，或许还可以提供经济奖励。ICANN 组织有机会 ... 合规职能。我希望 ICANN 和签约

方采取主动。... 不仅要在滥用事实发生后采取适当措施缓解，还要在发生前进行预防。然后，我个人希望看到，我们目前确定的节奏，即每届会议进行一次全体讨论，可以变成每届会议进行一次报告，报告我们在 DNS 滥用方面做了什么。以上就是一些关于我们明年可以如何继续推进打击 DNS 滥用的想法。托马斯交回给你。

托马斯 • 李凯尔特： 非常感谢梅森。非常感谢。我们有 2 个问题是问你的。我建议我们在继续之前先回答这两个问题，如果你可以简短地回答一下就太好了。... 谁赞助了。

杰夫 • 贝瑟： 我没有，抱歉。

托马斯 • 李凯尔特： 鲁克 (LUC) 问梅森，你能不能解释一下 WHOIS 的编辑是如何影响网络钓鱼检测的？我相信追踪网络钓鱼企图背后的相关人员可能会更难，但滥用域名的数量还是一样的。谢谢。

杰夫 • 贝瑟： 谢谢你的问题。鲁克允许我书面回答这个问题。这是一个 -- 其中涉及到很多复杂的问题，我想花点时间来正确回应一下。托马斯，这样可以吗？

托马斯 • 李凯尔特： 当然可以。还有几个问题没有回答。如果可以的话，我们希望全部以书面形式回应问答窗格里的问题。我知道这些问题已经同时公开了，大家都可以看到。所以如果你提出一个问题，请快速检查一下你的问题或者类似的问题之前是否已经问过，这样就可以避免回答者重复回答。下一位是克里斯托弗 • 路易斯-埃文斯，他将代表公共安全工作组谈谈滥用问题，克里斯是英国国家打击犯罪局的代表，交给你了。

克里斯 • 路易斯-埃文斯： 谢谢，托马斯，大家好。也感谢大家参加本次关于 DNS 滥用的全体会议。首先，请翻到下一张幻灯片。

首先是我们为什么要讨论 DNS 滥用问题？梅森和杰夫都已经谈到了一些不同的原因，其实我觉得这些主要原因就是滥用对互联网用户产生了实际影响。所以我提出了 5 个涵盖不同类型的统计数据。不同范围的滥用。FBI 的互联网犯罪投诉中心产生了很好的统计数据。他们显示了去年的投诉数量，得出的平均数是每天 1300 起。你知道，造成损失的数额相当巨大。而且那涵盖了所有互联网用户。也就是企业、个人，每一个参与其中的人。在我们的国家统计中，记录了报告的 85% 的欺诈是借助网络完成的，所以你可以看到 DNS 滥用对互联网个人用户造成的影响有多大。关于已经造成的损害的规模，勒索软件可能是目前最大的恶意软件形式，或者说产生了最大的影响，自去年以来同比增长了 715%。所以造成损害的金额真的

是大幅度增加。不仅仅是个人和企业的经济损失。还有个人数据在 ... 中被外泄，被不法分子利用。在英国国内，超过 60% 的网络事件记录的数据外泄是由于网络钓鱼或恶意软件所致，这显然是解释 DNS 滥用的两个关键点。这一点也得到了梅森前面提到的 DNS 滥用框架的认可。关于 -- 请翻到下一张幻灯片。我想我看到马克西姆 (Maxime) 在聊天中提到，我们有很多地方可以解决 DNS 滥用问题，在 ICANN 内部，我们显然集中在注册服务机构的注册上，以及 ICANN 本身和合同以及其他各种事情，但是要解决和减少造成的损害，我们需要整个系统的响应。也就是 ... 互联网服务电子邮件提供商，ISP，内容分发网络，等等等等。我们在一个非常庞大的环境下工作，而且我们确实需要一些工具，来帮助那些试图解决滥用问题的人找到对的地方。在这里我提到了一个共同的 -- 下一张幻灯片。ICANN 是我们共同的促进者，我们在这里讨论 DNS 滥用。我们正在产生一定影响，而且梅森强调的没错，需要主动开展一些工作。而且能够采取主动措施非常关键，因为它提高了通过门槛，真正使这种损害更加难以实现。所以对我们在这个环境中的利益相关方团体来说，我们有 ICANN 这个共同的促进者。但是我们确实没有一个机构能涵盖整个生态系统，包括内容方面和其他所有方面。请播放下一张幻灯片。那么我们能做什么？作为一个执法者，显然我很熟悉 ICANN 内部的情况。我和注册服务机构团体、注册管理机构团体和其他利益相关方召开了许许多多有效的会议，你可以利用其中的一些知识来指导你适当地处理滥用投诉。但这在整个执法机构，甚至在整个网络安全

部门，都是不一样的。你知道，有坊间证据表明，有人试图去找 ICANN 实现域名的暂停。那找错地方了。其实有一点没有弄清楚，要寻求做出改变，取决于 DNS 滥用的类型。... 内容，可能有恶意软件。取缔域名不一定是第一反应。不过，如果它意味着减少对互联网用户造成的损害，那就可能是正确的。如果我们没有任何行动会怎么样呢？我们又该如何升级？这其实就涉及到共同的促进者了。我们如何去要求网络发帖者删除内容。什么都没有发生。我们如何升级。注册服务机构不响应，这要花多长时间。建立这些机制是我们可以采取的提高门槛的另一个步骤，我认为它十分重要，可以真正使犯罪分子难以实现这一损害。采取主动无法解决一切的问题。遗憾的是，总是有办法绕过系统。我们必须有一个良好的系统，这样就能够做出反应，并且能够在合适的时间内做出反应。关键在于，我们的任何流程都要及时，并且能够以简洁的方式进行。我提到了数据共享协议。关键在于，我们不能直接出现在别人家门口，说你能给我们 IT 数据吗？凡事都要进行合理的检查与衡量，而数据共享协议可以做到这一点。以适当的方式。事实上，你知道，你并不希望在处理一个事件时，要第一时间和注册管理机构或注册服务机构或网络发帖者交谈。你知道，其实你可以做的是建立一个框架，并拥有一个协议，这样你就知道流程，知道需要哪些制衡，正如杰夫在之前的发言中提到的，你要知道需要满足哪些标准，需要提供哪些证据，才能真正有助于减少损害，这才是这方面真正的关键所在。所以对我来说，我觉得我们还有很多事情可以做，并且都是建立在很好的主动措施

基础上。但是我们现在谈论的是减少 DNS 滥用的影响所造成的损害。减少域名数量并不一定总是 … 犯罪分子利用域名的手段多种多样。只有认识到这一点才能阻止正在造成的损害，我就说到这里。我愿意回答任何问题。

托马斯 • 李凯尔特： 非常感谢克里斯。我要读马克西姆问你的一个问题。你有没有什么计划 … 进入这个流程？所有互联网滥用都是通过 IP 发生的。

克里斯 • 路易斯-埃文斯： 它其实 … 就在图中的注册管理机构下面。抱歉，它有点小。它在上一张幻灯片上。所以，是的，他们绝对是这个生态系统的一个关键组成部分。首先，我与他们合作得非常好。我在他们的地区内拥有非常良好的关系，所以这是关键。谢谢。

托马斯 • 李凯尔特： 马克西姆提出的另一个问题是，有很多人呼吁采取主动的方法。有没有人能解释一下，当相关域名还没有被用来做坏事的时候，如何预测未来的情况。

克里斯 • 路易斯-埃文斯： 显然，要预测犯罪的发生是非常困难的，而且你也无法真正做到。但是，如果我们有现成的系统来处理滥用问题，那么一旦

滥用发生，就可以采取主动的措施。所以拥有正确的系统，并能够及时采取行动，我认为是一个很好的步骤。签约方从事着大量的数据活动，你知道，在 DNS 滥用框架内和其中的一些细节以及可能的 -- 已经远远超出了我可以讨论的范围。因此我认为，为阻止滥用我们可以主动去做很多事，但是如你所说，我们无法预测。谢谢。

托马斯 • 李凯尔特： 非常感谢，我想这方面我们可能要在稍后的小组讨论中进行讨论。在请出最后一位演讲者之前，如果可以的话，我有一个问题。在你的一张幻灯片上提到，85% 的欺诈案件都是借助网络完成的。所有这些都是我们所说的 DNS 滥用吗？

克里斯 • 路易斯-埃文斯： 不是，它们不全是 DNS 滥用。其中包括直接的垃圾邮件，这取决于你对 DNS 滥用的定义，我想杰夫谈到了 DNS 滥用是什么？所以，对，那是其他机制，这就是为什么我也包括了 ICO 统计，它们只局限于通俗理解的 DNS 滥用类别。

托马斯 • 李凯尔特： 谢谢克里斯。虽然我想继续，但是我看到莫妮卡 (Monica) 提了一个问题，我至少要回答这个问题，因为一直以来都有人投诉性别多样性，所以我们先试着回答莫妮卡的问题，然后再继续。这个问题是问克里斯托弗 • 路易斯-埃文斯的，你能不能

详细说明一下为什么记录的 60% 的数据外泄要归因于网络钓鱼和恶意软件。你有任何数据来源的详细信息吗？你能否详细说明一下归因于它们是什么意思？也许你可以解释一下作案手法。

克里斯・路易斯-埃文斯： 那是 ICO 公布的数据，ICO 是英国的数据保护机构。由于时间关系，也许我可以在聊天中分享相关细节。

托马斯・李凯尔特： 谢谢克里斯，下面有请最后一位重要的演讲人，那就是来自 GoDaddy 的詹姆斯・布雷德尔，他将代表签约方发言。詹姆斯交给你了。

詹姆斯・布雷德尔： 谢谢，能听到我说话吗？

托马斯・李凯尔特： 可以。

詹姆斯・布雷德尔： 现在已经是半夜了，谢谢让我加入这次讨论。最后一个演讲的好处在于，我可以借鉴前几位演讲人的观点和意见，整场会议我都在认真听并做笔记。我要介绍签约方的观点，在我们浏览

这些幻灯片时，你们将会看到，这些观点和目前已经听到的观点大体一致。请播放下一张幻灯片。我想基本上，在线滥用就像托马斯在开场时说的，是我们行业的一个挑战。这是签约方的一个优先事项。到目前为止所有人力和系统的投入都表明了这一点，而且我认为，不管是戴维呈现的数据，还是 Interisle 报告中呈现的 ICANN 主要签约方的数据，都证明这些投入正在得到回报，一般滥用特别是 DNS 滥用正在被大规模地发现和缓解。但我认为我们确实需要认识到一般滥用、内容滥用和其他类型的滥用与 DNS 特定滥用之间的区别，这又回到了托马斯关于 ICANN 承担有限角色的言论，它根据其章程的限制，专注于 DNS 本身的滥用。

下一张幻灯片。所以在这个基础上，ICANN 的使命是确保 DNS 的安全性和稳定性。但是，我们讨论的很多滥用行为，特别是垃圾邮件，还有一些其他在线欺诈欺骗行为，在很大程度上依赖于内容，就是从这里开始我们偏离了 ICANN 的职权范围。同样，注册管理机构或注册服务机构减轻滥用或减少滥用内容的能力也受到限制。我们经常称之为“核选项”。作为注册管理机构或注册服务机构，我们只能借助一个杠杆，那就是取缔域名或暂停域名。而这对于内容滥用是不合适的。可以想象，如果某人在 Facebook 页面上精心策划了一个骗局，我们不可能取缔整个 Facebook.com。如果假冒产品被放到 eBay 上出售，那么暂停 eBay 是适当的反应。这时就是我们说的，只有一个杠杆，“核选项”。幸运的是，很多注册管理机构和注册服务

机构位于生态系统的其他部分。比如 GoDaddy 是一个注册机构和注册服务机构，也是一个虚拟主机。所以在检测滥用时，我们有更多渠道可以使用。因此我认为，这就是为什么你听到签约方说只有一部分在线滥用问题真正属于 ICANN 的职权范围的其中一个原因。但是，我们作为一个行业，已经围绕着 ICANN 之外的一些其他努力自我组织起来，解决各种各样的滥用问题。请播放下一张幻灯片。

因此，去年 9 月，也就是正好在我们大家最后一次齐聚蒙特利尔之前 -- 我们中有将近十二个注册管理机构和注册服务机构推出了一个关于 DNS 滥用的框架，目的就是前几位演讲人所说的，为滥用设置标准化定义。以及一些标准的行动期望。我想，杰夫引用的 SSAC 报告确定了各种情况下的责任方是谁以及典型的缓解措施是什么。

目前这个框架已经发展到超过 50 个签署方，我想就像梅森所指出的，它正在产生影响。它正在鼓舞着那些或许不得不容忍滥用的能力较低的注册管理机构和注册服务机构，帮助打造全行业的整体能力，并使这些滥用行为者日趋边缘化。就在昨天，所有原始参与者和一些新的签署方发布了第一年的更新。你可以在 abuse framework.org 上找到它，它解释了我们在框架下运营的经验和一些滥用趋势。因此，与其让本次会议充斥着图表和统计数据，我鼓励大家访问那个链接，并从这个框架的每个成员那里获得最新信息。此外，在 2019 年早些时候，我想大概是 4 月或 5 月份，互联网与管辖权政策网络公布了一

份白皮书，里面同样概述了发现和减轻 DNS 滥用的所有挑战，这些定义与你在 DNS 滥用框架中看到的内容高度一致，但是它们包括 ... 托管，而托管并不包括在框架中，所以这里存在一点差异。当我们查看内容时，还看到在 DNS 滥用之外有无数行业联盟、协会和同盟以及任务组。所有这些其他事情大家可能很熟悉，也可能不熟悉。但它们针对的是特定滥用类别，如垃圾邮件，如虐童。反恐。招募融资。药品。之所以列出这一点，是因为这些行动并不发生在 ICANN 之下，ICANN 下所涵盖的一个滥用类别并不意味着其他方面完全没有展开工作。而且，事实上，很多签约方会更换头衔参与到其他组织中，或许是作为一个网络 ... 其他公司。请换下一张幻灯片。这是目前的情况。我们看到，今年就像坐过山车一样。作为疫情之下的一个谋生手段，全世界竞相转向线上，特别是小企业。为了维持经营，大家熟悉且喜爱的餐厅正转向外卖或路边摊模式。对于那些有孩子的人来说，今天的学校已经完全转变了教学体验，政治、民间和宗教组织也都更多地走向虚拟世界而非现实世界，ICANN 也是如此。我这么说是因为我们的行业为这个大转折做出了贡献。这些趋势早已有之，但 COVID-19 加速了这个原本要几十年完成的进程，并将其压缩到几个月。当然，我们希望当这一切结束时，我们都能更灵活稳健地从这一转变中迅速恢复过来。

但是，我们不应该感到惊讶的是，所有犯罪分子、骗子、坏人和机会主义者也纷纷跟随这一转变。他们也在转型，他们改进

了方法和战术来跟随他们的受害者，如果受害者不再参与实体经济，他们也会进一步加强虚拟方面和网络方面的攻击。但是尽管说了这么多，没有数据表明天会塌下来，互联网会崩溃。事实远非如此。下一张幻灯片，回到戴维的一些统计数据，你知道，在我们的行业中，网络钓鱼报告曾多次小幅增加，我想戴维提供了一个趋势线图表。有几个离群值拉高了平均值，这与我们在春季看到的一些峰值相呼应，之后在夏季也有几个。总的来说，我认为我们看到了一个温和的增长。现在可能要更具体到 GoDaddy 而不是整个行业，因为我没有汇总的统计数据，但我们看到了 15% 的同比增长。活动方面似乎没有出现跳跃式增长，也没有数据表明出现了一些全新的或新颖的攻击类型。目前 GoDaddy 每天处理大约 2000 份网络钓鱼报告。那不是域名，也不是具体的事件，而只是报告。应当说明的是，其中有一些报告来自比如说互联网工具栏，发送了大量重复的信息。因此检查其中的每个报告并删除重复报告是一项重要的工作，而且即使我们只占这些报告的约 8%，有时不到 3%，也要注意，大部分报告是不可操作的。它们要么不再运行，要么缺乏关键信息。所以渠道中存在大量噪音。具体的合法事件很难处理，也许我们可以从运营上研究这个问题，并且也许要和 OCTO 乃至全行业进行协调，更好地重新聚焦在合法问题上。请播放下一张幻灯片。稍微讲一下。尽管不完全相关，但我认为聚焦与疫情相关的骗局和欺诈活动也是这个主题的一部分。这些骗局当然占据了今年年初的头条新闻，我想梅森提到了我们在 3 月和 4 月看到的峰值，当时几乎人人都处于某种封锁的

状态。我认为，这里的底线是，这些都是以内容为中心的。而且不是特别新。他们采用了一个新的包装，你知道，他们试图利用疫情下的日常景象，或抓住疫情早期阶段人们恐惧和焦虑的心理。但在这之下，依然是网络钓鱼和欺诈攻击这些我们多年甚至更长时间以来一直在应对的惯用伎俩。所以在我们的案例中，例如在 GoDaddy 中，我们认为不必争先恐后地制定新的服务条款或新的政策，或者开发新的功能。我们发现，我们现有的工具包很好地抵御了今年的 COVID-19 相关骗局，而且很多缓解措施依然是在虚拟主机上采取，而不一定是通过 DNS 上的攻击。我应该指出 -- 关于采取主动防范措施，有问题来回抛给克里斯和梅森 -- 早前我们收到了很多建议，甚至是来自政治人物的压力，你知道，要求在 DNS 中阻止 COVID。不要让任何人注册有该字符串的域名。不要让任何人注册“coronavirus”（冠状病毒），他们只会用它来做坏事，这是一个非常 -- 我注意到这类解决方案具有诱惑性。但我认为需要指出一点，在这个领域，情况比这要复杂得多。我们看到的大多数有害和滥用的域名并没有明确引用 COVID 或“coronavirus”，所以它们不会被类似这样的方法检测到。相反，我们找到了很多公共卫生机构、地方新闻机构和地方政府使用带有这些字符串的域名，用于发布官方新闻、信息通报和说明。因此，我认为我们需要 -- 或许 ICANN 社群的复杂性在于，当我们看到在 ICANN 外部有人呼吁在 DNS 中阻止某些字符串以解决某个问题时，我想我们所有人都认识到，虽然这很诱人，但不一定是一种有效或可接受的方法，比如从误报和附

带损害的角度来看。请放下一张幻灯片。我想这是我的最后一张。底线是，显然滥用是一个重要的问题。我们不是避而不谈，而是 ICANN 的角色和我们作为与 ICANN 签约的注册管理机构和注册服务机构的角色决定了我们受到相当多的限制。我们有更多工具可以在我们的工作场所中利用。我们认为，在 ICANN 讨论这些主题，促进讨论，从社群的其他层面获得更多观点，这些都是有价值的。而且我认为 OCTO 和 SSAC 正在进行的研究至关重要，收集和汇总一些行业范围的统计数据也很有帮助。但是我想，任何人都不会对此感到惊讶。你们将会看到，对于在这方面发起新的政策制定工作或进行合同修订，签约方会有一些犹豫。首先，我认为我们需要非常非常严格地界定问题，使其明确地落入 ICANN 的职权范围内。其次，我们必须 -- 我认为这又回到了梅森的幻灯片中引用的艾略特的话 -- 确保我们用尽所有现有的合同机制，对集中存在所有这些问题的少数坏人施加影响，而不是撰写针对这些问题的新政策，这一政策可能经过或没有经过检验。如果我们知道有一些方法被证明是有效的，我们如何才能自动推行它们，使它们得到更广泛的采用和实施？以上就是我的介绍，托马斯，谢谢你让我加入进来。也感谢大家听我说完。

托马斯 • 李凯尔特： 非常谢谢詹姆斯。詹姆斯，其实问答窗格里有一个问题是问你的。我想是马库斯 (Marcus V) 对詹姆斯的问题。受信任的通知人安排是不是一个好办法，可以减少你提到的所有噪音。

詹姆斯 • 布雷德尔： 我想是的。我认为受信任的通知人是一个很好的方式，可以过滤掉那些误报和重复报告。任何能让我们的团队和工具专注于实际威胁并疏通管道的方法都值得支持。当然。

托马斯 • 李凯尔特： 非常感谢。现在距离会议结束还有 17 分钟左右。我看到专家组成员正在回答问答窗格中的问题，我希望大家继续在问答窗格中交流。只是有一点，杰夫 • 纽曼 (Jeff Neumann) 围绕这些全体会议的讨论形式提了一个问题，认为它们应该产生具体的建议或结果。所以我想，尽管我们都听取了相同的介绍，但我不确定我们是否接收到了相同的讯息，所以我会试着梳理一些要点，希望我们能就这几点达成一致，这样我们就有了一些实实在在的东西，可以作为后续工作的基础。第一点，关于 DNS 滥用的定义，我想从专家组成员那里得到一些反馈，因为各种 ... 承担的角色和采取的行动，不管是主动的还是被动的，都取决于这个定义。在克里斯托弗 • 路易斯-埃文斯的演讲以及詹姆斯 • 布雷德尔的演讲中，都提到了 DNS 滥用框架，实际上突出了几个重点，那就是恶意软件、僵尸网络、网络钓鱼、网址嫁接、垃圾邮件，并对垃圾邮件主题做了一些定性。这是不是一个意见 -- 这是杰夫提出的一个问题 -- 你和你的 SSAC 的报告可能就建立在这个基础上，因为你提到你们研究了定义？所以我想，如果我们对什么是 DNS 滥用、什么不是有一个共同的理解，可能对每个人都很有帮助。如果有人想要提出自己的问题，请把它们写到问答窗格里。ICANN 工作人员

告诉我，鉴于我们的时间有限，最好不要打开个人的麦克风让他们发言，所以我会确保在时间允许的情况下读出你们的问题并进行讨论。杰夫，你可以回应一下吗？

杰夫 • 贝瑟： 当然，托马斯，谢谢。一个共同的定义框架是解决问题的核心，因为有了这个框架后，当出现核心定义未能涵盖的新型网络犯罪时，我们就能够定义它，围绕它设置一些参数，并解决它。所以我认为这是任何类型的 DNS 滥用解决方案的一个非常关键的组成部分，作为一个企业定义库，当试图对某个欺诈或域名事件进行归类时，人人都可以调用它。

托马斯 • 李凯尔特： SSAC 有没有查看 DNS 滥用框架文件所提供的定义，它基本上是建立在 ... 管辖权工作的基础上？

杰夫 • 贝瑟： 谢谢托马斯。有，它实际上在定义部分特别突出了这 2 个工作。

托马斯 • 李凯尔特： 非常好。专家组还有其他成员愿意回答 -- 不是同意，而是表示反对定义 -- 或者我们能不能保持沉默。如果对这个问题保持沉默，是不是表示默认 DNS 滥用框架可能是 DNS 滥用统一定义

的一个良好起点？我不会询问特定的专家组成员，因为我们只有几个专家组成员。如果你认为这些定义不恰当 -- 或者漏掉了什么，请打开你的麦克风发言。

詹姆斯： 我可以说一下。我认为这是一个很好的起点。我想杰夫提到了 SSAC 报告呼吁开展一些额外的工作来明确一个定义。我想，在聊天中有人问到在这之后怎么办？下一步是什么？我们如何防止出现专家组在 ICANN 第 70、71 和 72 届会议上不断重复这些演讲的情况？也许摆脱这个循环的方法是，从基于 SSAC 报告的框架内容开始，启动一些关于定义的讨论。然后在分析中包括为什么它适合或不适合 ICANN 的有限角色和有限机制，是否注册管理机构和注册服务机构要采用这一特定定义，还是 -- 我想这也是一个 SSAC 报告 -- 第二点是，它是否属于另一个责任方，如何把它交给责任方，也许我们可以给出这个提议，我可以从这些 -- 我只想回应[听不清]专家组不断重复地工作。

托马斯 • 李凯尔特： 谢谢詹姆斯。梅森，请。

梅森 • 科尔： 我想接着詹姆斯的话说几句。总体上我同意他的看法 -- 框架和即将发布的 SSAC 报告是定义的良好起点。我只想重申我在演讲部分所说的话，即，我不希望看到在滥用层出不穷的同时，

我们却纠结或过度纠结于定义。现在是时候真正采取纠正行动了，而不是在试图界定问题的同时等待主动行动。所以我只想向社群明确一点，CSG 和其他对这个问题感兴趣的各方希望看到 ICANN 在这方面采取一些行动。回答米基拉 (Michaela) 的问题，我认为重点不在于我们一次、两次、三次还是四次开会讨论 DNS 滥用，我们需要做的是采取一些具体的措施，所以我希望事情朝这个方向发展，而不是过度纠结于定义部分。

托马斯 • 李凯尔特： 谢谢，梅森。

詹姆斯 • 布雷德尔： 也许我应该告诉你们专家组成员一直在翻来覆去地讨论这个问题，也许不应该，我不知道。但是你知道，梅森，我认为我们的分歧点在于，这就好比是射击中的“预备、开火、瞄准”，有了一个定义并理解这个定义后，我们就能界定一个明确的职权范围。你知道，要采取后续步骤，这是必需的。我只想强调，因为我想确保它是 -- 也许我描述得不是很好，或者传达得不好，但是工作从来都没有缺席。他们也许没有现身 ICANN，那是因为他们恰好在其他场合和不同的团体和公司交流，但我们并不是纠结在这个问题上裹足不前。我们只是在其他地方进行着工作。

梅森 • 科尔： 我赞成，詹姆斯。我也不想在专家组翻来覆去地讨论，但是你知道，我确实认为我们已经围绕这 8 到 10 个害群之马讨论好几个月了。也许你们还在做着其他一些事情，你知道，签约方在我们看不到的地方处理其他事情，但是你知道，我并不想采用“预备、开火、瞄准”的方法。我想通过一个正确的方法来解决 DNS 滥用问题，我认为我们还没有做到这一点。托马斯，我会让步，谢谢。

托马斯 • 李凯尔特： 谢谢梅森和詹姆斯。我想，大家都在等待专家组成员之间的互动。对此我很高兴。我想没有人应该把政策工作作为不采取行动的借口，而且你知道，至少根据我与签约方的讨论来看，我认为很多人 -- 所有人，至少是出席本次会议的人，做了相当多的工作。但我认为，定义部分仍然是把事情做对的关键。我们需要确保注册管理机构和注册服务机构在生态系统中占有一席之地，并能根据自己的能力采取适当的行动。ICANN 也一样。例如 ICO 协会，也在处理 … 来自公众的投诉，主要是针对 CASM 的。詹姆斯在他的发言中以及专家组面前提到，我联系了他们的负责人，并询问他们更愿意去找注册管理机构和注册服务机构还是托管提供商取缔域名，他们说更愿意去找托管公司，因为他们要确保非法材料 — 这些材料在很多案例中是持续滥用的证据 — 不会进一步从源头分发。好的，所以我想我们要把事情做对。下一点，我想简要地谈谈，统计数据中似乎有一些差异。有些人说数量正大幅下降，还有人说问题并没有

变小，而是或多或少维持原状。戴维，你听了专家组成员的发言，也跟进了聊天和问答窗格中的讨论。你能不能谈谈在统计数据方面对我们听到的不同讯息的理解。

戴维 • 康纳德： 我认为我们在看大象的不同部位，对。有一个问题是，到底什么是 DNS 滥用。人们衡量的到底是什么？我在聊天中提出的一个意见是，针对某些小组看到的数字与在我们的数据集内看到的数字相去甚远的情况，我们非常有兴趣看到其他人的数据集。我们正在努力收集尽可能多的数据，以便向社群提供信息，帮助促进这些讨论。我们能提供给社群的数据越多，就有望引导大家更好地了解 DNS 滥用背后的实际情况，而不是传闻。所以从我的角度来看，你知道，我们所拥有的数据表明，随着时间的推移，DNS 滥用一直在减少。还有人则认为 DNS 滥用正在增加。而我感兴趣的是，人们看到了什么样的数据集导致了这些不同的统计结果。

詹姆斯 • 布雷德尔： 托马斯，你知道，我认为这只是在一定程度上表明了这个问题在整个 DNS 和整个互联网的分布有多么的不均匀。我注意到在戴维的幻灯片上有一些离群值，而这些离群值对应着一些峰值，我想这在我们的数据集内也看到了。这就好比海平面不会变化，但每年会发几次洪水。也许这就是区别，并不是说我们看到的数字不一样，而是我们看待它的角度和时间周期不一样。

托马斯 • 李凯尔特： 谢谢詹姆斯。我还有一个问题要问克里斯。现在，我们已经听到詹姆斯和戴维都表示，获得统计数据或尽可能多的数据，试图理解不同的数据存储并从中找出传闻和事实之间的差异，这将会非常有用。据你所知，执法社群有没有进行一些讨论，来与行业在记录的格式或定义上保持一致，这样我们的政策或响应就有了相同的事实基础。

克里斯 • 路易斯-埃文斯： 好的，谢谢托马斯。执法机构在过去几年进行了一项重大变革，为的是对报告的犯罪、它们是如何记录的、导致这些犯罪的根本原因是什么做到更加公开透明，FEI 的 IC3 报告很好地说明了这些问题。我们如何在全球范围内协调，这一直是个有趣的问题。我认为，为了在数据记录的一套标准上达成一致，我们在 ICANN 内部的争论已经够多了。所以我认为这当然是需要进行的工作，但是，我认为更重要的是把数据公布出来，并且尽可能对会引起什么后果保持透明，这样我们才能在整个生态系统中更紧密地合作并发挥影响。

托马斯 • 李凯尔特： 非常感谢克里斯。本次会议还剩下 2 分钟，在结束之前请允许我试着总结一下。我想，我们听到了很多很棒的意见。我认为，专家组内外都一致认为，对于这个问题最好要有共同的定义、共同的统计数据或共同的数据点。我想有一点也很明确，任何说问题变大了、变小了或不一样的建议，都应当和证据一

起提供，以便其他数据整理者能联系到我们所拥有的数据或者申请或请求采取其他行动，以确保了解真正的事实而不仅仅是传闻，这将带来很大帮助。我还想回到杰夫在演讲中提到的一点，那就是教育。我们需要的用户是 ... 对于网络钓鱼或 ... 其他正在发生的坏事。因此，我认为它需要结合不同的事情，各个参与者可以在其各自的角色中采取不同的补救行动，不管是 ICANN 签约方、执法机构还是其他方面。但是我认为，如果我们能够研究这些问题，那将是一个很好的起点。我没有参与创建 DNS 滥用框架文件，但看起来很多人实际都指向了这份文件，因此或许可以建议把这份文件包括进来，作为讨论定义、受信任的通知人系统等等的参考依据。所以我认为我们不应该重新发明工具，而是要建立在以前工作的基础上。最后，我要感谢各位专家组成员。我要感谢 ICANN 工作人员，特别是技术团队，感谢你们确保会议顺利举行，中间没有出现任何技术问题。我还要感谢你们，... 连续几小时远程参加会议，也没有茶歇时间私下见面交流，这很不容易，所以感谢大家对我们的支持。谢谢大家的关注，再次感谢所有人，本次会议到此结束。

[会议记录结束]