阿布扎比 — 跨社群会议：DNS 滥用报告在政策制定和滥用缓解中的使用
格林威治恒星时 2017 年 10 月 30 日星期一 — 13:30 至 15:00
ICANN60 | 阿拉伯联合酋长国阿布扎比

伊朗嘉 • 卡函嘉玛
(IRANGA KAHANGAMA)： 大家下午好。请大家找位子坐好，我们很快就要开始了。

谢谢。

好的。感谢大家的到来，本次会议的主题是滥用报告，针对基于事实的政策制定和有效的 DNS 滥用缓解。我是伊朗嘉 • 卡函嘉玛，是本次公共安全工作组会议的联合发起人之一，代表美国联邦调查局，同时也是公共安全工作组的一员。

我的联合主席卡特琳，你要自我介绍一下吗？

卡特琳 • 鲍尔-布尔斯特
(CATHRIN BAUER-BULST)： 当然。我是卡特琳 • 鲍尔-布尔斯特。我是 GAC 公共安全工作组的联合主席之一，代表欧盟委员会。

伊朗嘉 • 卡函嘉玛： 谢谢卡特琳。

下面由我非常简单地介绍一下本次会议的历史和逻辑，以及期待取得的成果。之后卡特琳将进一步介绍本次会议的安排和细节。

从公共安全工作组的角度，我们想吸引 ICANN 社群聚焦 DNS 滥用和 DNS 滥用缓解的自然演进。这是我们所做的其他工作的自然进展，包括通过 GAC 关于 DNS 滥用问题的建议以及我们开展的一些其他讨论和活动，提出各种各样的问题。

当举行跨社群会议的要求提出来时，显然我们非常感兴趣。我想有一点非常清楚，社群内部对进一步讨论这个问题，继而讨论如何解决其中的一些问题十分感兴趣。

所以我简单介绍一下背景信息，我们召开了三次工作组电话会议，由来自不同利益相关方社群的志愿者参加，也就是你们在桌上看到的这些人。我们给自己布置了一个任务，就是决定本次会议的开展方式。

公共安全工作组起初围绕 DNS 滥用缓解整理了一些原则概念，并试着进行综合。

在提出一些原则后，很明显对于这些问题存在很多迥然不同的观点，结果这个会议的内容就自然变成了我们应该和广大的社群分部讨论这些问题，也就是你们今天在这里所看到的。

我们已经做的就是，组织好本次会议，而且我们已经将 DNS 滥用缓解问题分成了三类：DNS 滥用的识别、DNS 滥用的报告，以及统计数据及其应当如何使用。

会上我们将让观众加入这三个主题的讨论。我们希望在本次会议的成果基础上，以及公共安全工作组和其余社群的持续交流中，催生出一种基于原则的方法。

谢谢。

卡特琳 • 鲍尔-布尔斯特： 在翻到下一张幻灯片之前，让我简单介绍一下。我们将首先听到戴维 • 康纳德 (David Conrad) 和德瑞 • 巴格利 (Drew Bagley) 带来的两个简短演示，他们就坐在我的左边。之后我们有一个专家组，它是由不同团体的代表、不同团体的参与者组成，他们也为伊朗嘉介绍的本次会议的筹备工作做出了贡献。他们是来自注册管理机构利益相关方团体的艾伦 • 伍兹 (Alan Woods)，来自注册服务机构利益相关方团体的格雷姆 • 邦顿 (Graeme Bunton)，来自 NCUC 的塔妮娅 • 拓毕那 (Tania Tropina)，来自商业选区的丹尼斯 • 米歇尔 (Denise Michel)，来自 IPC 的乔纳森 • 马科夫斯基 (Jonathan Matkowsky)，即将就任的 SSAC 主席罗德 • 拉斯穆森 (Rod Rasmussen)，以及 ICANN 合规和消费者保护副总裁杰米 • 赫德兰 (Jamie Hedlund)。

请换到下一张幻灯片。

正如伊朗嘉所说，我们为本场讨论做了精心安排，以两个简短的演示开场，然后就将进入伊朗嘉提到的三个类别下的讨论。在先前的电话会议中，在对原则的讨论中，得出的结论是，虽然我们还不能就 DNS 滥用报告的数据收集以及之后的数据使用应当适用哪些原则达成一致，但有一点很清楚，用于这一流程的原则必须响应三个关键问题，也就是你们在这张幻灯片上看到的这些问题，在开场的两个演示之后我们会回过头来讨论。这些问题分别是，第一，我们如何以可靠的方式识别 DNS 滥用？在此基础上，我们如何创建有效和透明的滥用报告来提供这个数据？第三，然后我们如何继续使用这个数据？

这就是我们希望今天和大家探讨的三个部分。在这个主题上我们有一个由知名专家组成的大型专家组，我们非常希望你们加入进来，让本次会议成为一场互动积极的会议。

所以我们将要做的就是，首先我们将以两个简短的演示开场。然后我们就开始对各个部分进行讨论，每位专家组成员负责一个问题。在我们回应特定问题的同时，如果你们要加入，不管是对这个类别下一般问题的讨论，还是我们与专家组成员讨论的具体问题，都请先向麦克风附近的 ICANN 工作人员表明自己的身份。你们看到他们在这里举起的号码，所以请先举手。工作人员将走向你并向我们示意你要发言，我们将为你预留时间。

为了让尽可能多的人有机会发言，我们将把每个人的回答时间限制在两分钟以内。专家组也是一样。在这里我们要尽量做到公平。请踊跃发言，和我们分享你们的观点。

现在，话不多说，我们要请戴维 • 康纳德给我们做第一个演示，关于域名滥用活动报告系统。

戴维，交给你。

戴维 • 康纳德： 非常感谢。

我是戴维 • 康纳德，ICANN 的首席技术官。关于本次讨论，在我的小组内以及首席技术官办公室，开发了一个域名滥用活动报告系统。

请翻到下一张幻灯片。噢，那是我。哈！好了。

介绍一点背景。什么是域名滥用活动报告，我们喜欢简单地称之为 DAAR。它是一个可以跨 TLD 注册管理机构和注册服务机构，用来报告域名注册和滥用数据的系统。目前它主要关注 gTLD，因为这里有可以分析的数据，但是系统并非局限于此。如果 ccTLD 想要加入，我们也很乐意与他们讨论。

DAAR 与其他报告系统有何不同？相信很多人都知道，现在有大量的报告机制，它们实际上大都和某种商业产品或服务有关。

我们要做的就是研究所有我们可以收集到数据的 gTLD 注册管理机构和注册服务机构。与我们所做的大多数分析不同，我们试图使用海量的数据源，而且都是声誉数据源，也称为禁用清单或 RBL。

我们也会收集一个时期的数据，以保存足够的数据进行历史研究。

我们希望或者实际上是需要审视许多不同的威胁。我们所关注的这些威胁就是在北京 GAC 公报中所确定的威胁，包括网络钓鱼、僵尸网络要求和控制，以及恶意软件传播。而且在我们的分析中也争议性地纳入了垃圾邮件。我们纳入垃圾邮件主要是因为它是其他滥用形式的一个非常有效的风向标，给我们提供了一个指标和信息。因为通常当 TLD 受到这样或那样的恶意软件或恶意活动影响时，也会受到垃圾邮件的影响。

还有一个关键点是，我们努力采用一种科学的方法，尽可能做到透明和可再现。DAAR 项目实际上起源于一家安全硬件供应商的报告，报告显示有多个 gTLD 百分之百与垃圾邮件或滥用有关。而其中有些报告颇为滑稽，事实上其中一个百分之百与垃圾邮件有关的区只包含一个域，它就是 NIC.顶级域，但是因为这个顶级域恰好匹配了该安全供应商所关注的某个字符串，我想其实是 .ZIP，结果就导致该顶级域内的所有域都被归入“恶意”一类。

当这个事情出来时，媒体实际上助长了它。实际上那给 ICANN 和一般会员社群都造成了很多问题。在那之后，多位社群成员找到我和 ICANN，并且提出“应该让某人保存一个权威的清单。应该有人正式提出一个人人都同意的方法，这样我们就不会收到这些商业利益驱使下的带有偏见性的报告了。”由此就触发了一些初步的想法，最终催生了 DAAR。

请翻到下一张幻灯片。

又是我。呀！算了。

发言人（姓名不详）： 要我来处理吗？

戴维 • 康纳德： 不用，我会解决。这是技术。我不怎么擅长那些东西。

[笑声]

我提到过，DAAR 使用很多威胁数据集。所以我们会收集向行业和互联网用户报告的相同的滥用数据。DAAR 的其中一个关键要求就是，我们通过这个项目所做的任何事都必须是任何人都可以再现的。我们不依赖任何机密数据。我们不会自己生成任何数据。我们基本上是使用公开数据，将它进行关联，并简单地生成庞大的电子数据表来记录各种各样的滥用。

我们收集的滥用数据由商业安全系统使用，这些系统每天都在保护着数亿用户和数十亿邮箱。学术和行业用户像我们一样使用这一信息，他们信赖这些数据集。学术研究和行业已经证实了这些数据集的准确性、可靠的全球覆盖和低误报率。

我们通过 DAAR 提出的结构是建立一个可扩展的框架，并且我们正在尝试对不同的数据子集进行分析，以期更好地了解实际情况。

这里的关键点是，DAAR 是一个工具，可以让 ICANN 社群了解外界对域名生态系统的感受。

看吧，我没有说“下一张幻灯片”，但它不听我的。很讨厌。在这里。

这是一个有关我们选择数据集的标准的问题。这张幻灯片显示了在当前版本的 DAAR 内我们所使用的标准。我们正在进行的工作之一，是就 DAAR 中所用数据源的选择标准征求 SSAC 的意见，此外目前我们也在筹备一个面向社群 — 抱歉，是面向独立专家的 RFP，希望他们就我们的方法提供意见。一旦收到反馈信息，我们就将撰写一份文件，描述我们提议采用的方法，然后提交这份文件进行公共评议。之后我们将在正常的 ICANN 流程内根据建议的标准修改数据源。

但是目前，对我们所用数据集的要求是，运营安全社群必须信任这些数据集的准确性和清晰性。特别是，我们使用的任何数据集都必须有一个非常明确的流程，通过这个流程可以在禁用清单中添加或删除域名。所选的禁用清单必须提供一个反映我们需求的威胁分类。主要是僵尸网络、恶意软件传播和网络钓鱼。

这些 RBL 在运营安全社群广为采用。这些数据源被纳入了网络运营商使用的商业安全系统，例如，在邮件服务器中等等，用于保护用户和设备。电子邮件和消息传送提供商也会利用它们来保护自己的用户。

说明一下，我们所使用的这些声誉禁用清单，实际上几乎到处都在用。不管是在浏览器中，还是在云和内容服务系统中，还是在你们的社交媒体工具中，此外还经常会在 DNS 中。它在哪里？实际上在哥本哈根，Farsight Security 的保罗 • 维克西 (Paul Vixie) 给技术专家小组做了一个演讲。他们开发了一个软件，可以利用响应策略区，通过策略阻止域名。

我们知道有一些互联网服务提供商和电子邮件服务提供商在阻止整个顶级域，因为他们相信这些域充斥着恶意域和 DNS 滥用。

此外，专用网络运营商使用 RBL 和商业防火墙，还有企业邮件和消息传送系统以及第三方电子邮件服务提供商。

这里列出了我们目前在 DAAR 系统中使用的清单 — 抱歉我有点超时了。所以我们基本上 — 那是什么？有七种主要的 RBL，其中一个实际上是复合清单，包含了许多其他清单。

那么为什么 DAAR 要报告垃圾邮件域？这个问题在多个场合上都有人提出来。

在海德拉巴公报中，GAC 表达了对垃圾邮件的关切，当然我们一直对我们的社群言听计从。更现实的是，垃圾邮件是安全威胁的主要传播途径之一，DAAR 系统会衡量在垃圾邮件正文中找到的域名，而不是垃圾邮件域本身。

我就讲到这里，接下来交给法比恩 (Fabien) 吗？还是伊朗嘉或卡特琳？

请继续。

卡特琳 • 鲍尔-布尔斯特： 非常感谢，戴维。德瑞。到你了。

德瑞 • 巴格利： 谢谢你卡特琳。我是德瑞 • 巴格利，来自安全域基金会 (Secure Domain Foundation) 和 CrowdStrike。接着戴维对这一数据的价值以及这类数据的可靠性的介绍，我要讨论的是我们可以如何利用这一数据来阻止 TLD，不仅仅是在运营层面，还要纳入到策略当中，以便切实帮助加大力度，维护一个自由开

放的互联网，同时不违背普遍适用性的理念，因为如果滥用愈演愈烈，就会与普遍适用性背道而驰。

正如戴维所提到的，社群内就某些滥用形式达成了共识，特别是网络钓鱼和恶意软件，它们是协议中明确禁止的行为，此外还有它们常用的传播机制即垃圾邮件。

所以在通过策略应对滥用时，社群要了解很重要的一点，就是不要卷入对滥用的五花八门的解释当中，否则我们就将无法切实解决滥用问题。对社群而言开始研究策略问题非常重要，特别是其中达成共识并且有可衡量标准的领域。正如戴维所说的，在网络钓鱼、恶意软件和垃圾邮件，以及僵尸网络命令与控制方面，有很多可衡量的可靠标准。

在竞争、消费者信任和消费者选择审核小组中，我们研究了由 DNS 滥用引申出的问题，即采取哪些保障措施来预防新 gTLD 中的滥用情况。作为代理，为衡量这一问题，我们关注了网络钓鱼、恶意软件和垃圾邮件，并委托开展了一项研究，观察类似于戴维在各种黑名单上呈现的数据，并在宏观层面对其进行分析，以便我们能够提出策略建议。

我以此为示例，说明可以如何利用这类数据来切实推进社群中以数据驱动的政策制定工作。

历经一年的数据分析，我们发现，事实上，滥用并非真的普遍存在于每个 TLD 当中。同样，它也不是完全无章可循。实际上我们可以确定一些因素，它们与某个区域或某些注册服务机

构的高滥用率存在较强关联性，或者与某些注册管理运行机构或注册服务机构的低滥用率较存在较强关联性。

所以在注册限制较多的情况下，注册域名的难度加大，滥用情况较少，这并不奇怪。

类似地也可以发现，滥用率很高的注册服务机构或注册管理运行机构往往开价非常低，通常还会提供各种批量注册选项，稍后我会详细介绍。

此外，在微观层面上对某些 TLD 进行分析时，我们发现被用作诱饵的商标词汇和网络钓鱼活动之间存在很强的关联性，这可能也不是什么新鲜事了。但是在这份报告中所阐述的特定示例牵涉到 76 个域名，它们使用苹果商标比如 iPhone 的不同排列形式，企图对用户进行有针对性的网络钓鱼活动。这 76 个域名，我想是由该 TLD 中的 83 个滥用实例组成，它们均发生在一个特定的部分中。

这些数据总体表明，事实上存在一个政策空白。我想这就是为什么 DAAR 项目以及社群中的其他人通过收集和分析这些大型数据集，特别是依赖 WHOIS 数据所做的工作非常重要的原因。因为那样你就可以真正看到，事实上，我们现有的机制可能没有考虑到我们正面临的每一种情况，而这些情况正实实在在地影响着 DNS 的稳定性与弹性。

我要特别指出两家通过我们现有的工具集发现问题重大的注册服务机构，它们对我们后续的政策制定工作具有参考意义。

第一家注册服务机构已被叫停，但是在 2016 年的大部分时间里它都以非常高的滥用率在运营。而且实际上，它的叫停还不是因为居高不下的滥用率所致。而是因为当时他们停止支付账单，还有一些其他事情。但是基本上，如果你实施网络犯罪并且仍支付账单，那么就有可能在更长时间内侥幸逃脱惩罚，我想这是从中可以吸取的教训之一。

实际上它还凸显出一个问题，在一个以投诉驱动的模型中，我们要等待对 DNS 滥用做出反应，实际上我们可能会耽搁一段时间，直到收到这些投诉之后才能够采取应对之策。

然而，如果我们能够利用这些广泛的 DNS 数据集，例如 DAAR 举措将会为社群带来的突出数据集，那么我们就可以从中提前发现问题，而不必等到具体的违规事件发生，致使大量受害者受到影响之后。

这里是第二家注册服务机构 AlpNames，目前仍在运营。同样，它的滥用率也非常高。而且，在 CCT 进行研究的同时，这家注册服务机构还在提供批量注册服务。注册人可以找到 AlpNames 一次性注册 2,000 个域名，AlpNames 会很方便地创建这个域 — 他们可以为用户提供域生成算法。所以你可以随机生成 2,000 个域名，我相信它们的用途十分正当，因而可以注册你们的域。所以尽管这家注册服务机构滥用率非常高，却并没有遭到有效投诉，也不必面临暂停程序，也就不足为奇。

这就是利用这些批量数据和洞察我们可以收集到的信息，它为社群呈现出一个潜在的政策空白。

我在这里一直点错按钮，可能是我想一直强调这两家注册服务机构。

[笑声]

通过 CCT 审核小组的例子可以知道，我们能够利用这一数据并制定出具体的政策建议，这些建议将写进我们草案的 DNS 滥用一章，在下周或下下周应该就可以向社群发布。但是你们知道，它不应该终止于 CCT 审核小组。作为一个社群，在这类数据更多地公开提供给社群之后，不管是通过 DAAR 还是通过网络安全社群的成员提供的，比如 APWG、安全域基金会、Spamhaus、Stopbad 等等自告奋勇提供这类数据的成员，我们作为一个社群都不应该仅仅将它用于运营中，用来阻止某些活动，而且还应该用它来指导政策决定，发现这些空白，并切实确保我们能够从一个对滥用的被动反应模型转变为一个主动模型。在此模型中，注册服务机构和注册管理运行机构能够让反复违规者对自身服务的滥用更加难以为继。此外我们还可以利用这些数据来衡量工作取得的进展，看看我们是否真正全方位地缓解了滥用。所以我希望今天这个专家组能够真正地从不同角度出发讨论这个问题，因为很显然，它触及了社群中的很多领域，是我们要正确解决的问题。

现在既然我们有了可用的、可操作的数据，我们就应该真正拥抱它，利用它来制定政策，从而为我们大家创建一个更好的 DNS。下面我把接力棒传回给卡特琳。

伊朗嘉 • 卡函嘉玛： 谢谢戴维和德瑞的介绍。我要再强调一次，回答的时间限制在两分钟以内。虽然我们已经超时了几分钟，但是至少要确保大家充分地交流。

接下来要请专家组成员开始回答问题。之后观众可以自由发言，加入到这个讨论中。发言时请使用麦克风。

我想可以先从艾伦开始，如果他不介意第一个的话。但是可能要从链条的顶端开始。

我们刚刚听到德瑞谈了几个实例。当我们发现非常明显的滥用者时，注册管理机构拥有哪些可以自行支配的工具来帮助确认其中的一些问题，扭转观察到的反复违规或滥用的趋势？

艾伦 • 伍兹： 谢谢伊朗嘉。艾伦 • 伍兹。我先介绍一下自己。我来自 Donuts 注册管理机构。谈谈这个问题本身，当你说到“明显的滥用者”时我感到很心虚，因为很遗憾，你知道，我看到的这些数据和我们看到的这些数据都来自于像 DAAR 这样的机制。正是这些来源给我们提供了潜在滥用情况的绝佳清单。

但是目前我们实际上并不能断定说某人是明显的滥用者，因为很遗憾，我们依然缺乏证据来支持我们采取行动，或者支持我们将问题上报至注册服务机构或者有关方面来进行调查。

所以我们真正要问的第一个问题是，我们怎么知道这是一个明显的滥用行为？我的意思是，当我们获得信息和证据时，显然接下来就要利用这个证据。我们会对它进行审核，客观地审查，然后上报至有关方面，在这种情况下很可能是记录在案的注册服务机构。

如果注册服务机构不采取行动，那么显然注册管理机构自己就要考虑采取行动。

眼下，的确，我们会看一些通过 Spamhaus 或 SURBL 等清单收到的指标。但是之后，我们自己还要找到额外的信息、额外的证据，来跨越统计性证据和实质性证据之间的鸿沟。这个问题我就说到这里。

伊朗嘉 • 卡函嘉玛： 谢谢，艾伦。简单补充一下，可不可以说至少这些统计数据提供了一种很好的方式，可以指向某些问题，这些问题可能需要进一步调查，以便协助注册管理机构方面？

艾伦 • 伍兹： 是的。尽管可能有些争议，但是我认为的确，它可以为我们指引方向。但是很多时候，在我们进行审查时可以找到的唯一额外证据就是它被列入禁用清单这个事实。我们希望能够获得更多细节，或者找到额外的途径来查明它们为何被列入清单的原因，而不是仅仅给出一个它就在清单上的苍白陈述。

但是对我们而言那很困难。我们尽最大努力来处理这些情况。一旦发现某个引爆点，我们就会竭尽全力来确定出现这个引爆点背后的原因。但那并非总是清晰明了。而且要获取这个信息非常困难，特别是要从禁用清单提供商那里获取，他们不会给我们提供这些信息，因为他们无法提供或者没有这个信息，或者那是企业机密。

卡特琳 • 鲍尔-布尔斯特： 戴维，你要简单回答一下吗？

戴维 • 康纳德： 我想补充一点，DAAR 纳入历史信息的其中一个原因其实就是为了帮助识别长期趋势，包括某些长期的滥用信息。我完全同意“明显的滥用者”这个概念只存在于旁观者的眼里，我们必须获得额外的信息来确认真正的滥用者，而不是 — 你知道 — 某个喜欢用随机字符串作为域名的人。

但是在社群内部我们想要极力促成信息的提供，特别是长期信息，以便在政策讨论中参考，帮助清楚地辨别某些域名空间内的滥用趋势。

伊朗嘉 • 卡函嘉玛： 谢谢。

接下来罗德要发言，之后我们看到 2 号麦克风那里有人要发言。

罗德 • 拉斯穆森： 你好。我是罗德 • 拉斯穆森。在这里我是以个人的名义发言，而不是代表 SSAC。

我要直接回答这个问题，因为我认为之前我们听到的内容回答的是“某个实体如何以可靠的方式识别滥用”这个问题，而不是“你们如何以可靠的方式识别滥用”。后者需要有政策、信任等等。

这个行业已存在 15 年之久，目前已经发展出了极其可靠的方法，能够以系统的方式识别被滥用的对象。

之后这些对象会被注入到诸如 Internet Explorer、Google Safe Browsing 等服务中，如果你们使用像 Gmail 或 Hotmail 之类的电子邮件服务的话。今天，它们全都会在识别后的几秒钟内以数以百万计的规模自动地放入到这些工具中。

所以识别部分，技术是高度可靠的。目前已经有许多方法可以将对象加入白名单，并将误报率降低至接近零的水平。所以这个技术是存在的。

实际上关键在于将信息转化为行动。那需要签订合同。需要建立信任。需要各种各样的条件来围绕此建立一个框架，让人们能够在不同的地方采取行动，不管是域注册管理机构、域注册服务机构、电子邮件提供商，还是某个提供 Web 软件的人。

所以，我只想回答“从技术的角度而言这个问题已经解决”。但是从政策的角度而言却不一定如此。谢谢。

伊朗嘉 • 卡函嘉玛： 谢谢，罗德。

我们可以用麦克风了吗？

戴夫 • 匹斯特洛 (DAVE PISCITELLO)： 戴夫 • 匹斯特洛，来自 ICANN。我不喜欢“明显的滥用者”这个词。DAAR 当然不是用来衡量它的。我们要用 DAAR 来衡量基于禁用清单、声誉清单的安全威胁以及我们所认为的滥用。而且我认为这和注册管理机构、注册服务机构、DNS 托管公司或 ISP 的义务截然不同，它们必须去了解向他们提交的申诉材料，然后进行调查并加以证实。

如果我处在那个位置，那么我会尝试获取包含 URL 的电子邮件 — 你知道，获取包含 URL 的附件，然后访问网站，执行 WebGet 或者 curl，这些都是良性的。大量程序有望纳入到注册服务机构-注册管理机构层面的尽职调查中。我不是说那是零成本。

但是 DAAR 不是为了成为一个你们可以寻求获得全部答案的地方。DAAR 旨在成为一个针对整个域名空间、整个滥用威胁形势的统计调查机制，并尽量提供一些数字来帮助我们确认哪方面的策略卓有成效，哪方面的策略可能缺失，以及综合情况如何。

卡特琳 • 鲍尔-布尔斯特： 谢谢戴夫。

格雷姆，请允许我把问题抛给注册服务机构。现在，我们已经谈到我们所拥有的一系列不同指标。我们有 DAAR 提供评估基础，我们也了解到注册管理机构和注册服务机构方面还需要做更多工作来将这些信息转化为可操作的工具，以便针对可能违反你们条款和条件的客户采取行动。

现在，当然就要把焦点放到这些条款和条件上来，以及根据这些条款和条件你们需要哪些条件才能够采取行动，以及在制定策略方面你们可以产生怎样的影响。可以请你来谈谈吗？

格雷姆 • 邦顿： 当然。谢谢你卡特琳。我是格雷姆 • 邦顿，来自 Tucows。

我认为有几点需要注意，尽管艾伦提出的观点很好。正如你刚才所说的，将禁用清单联系到可操作的实质性证据不是小事。

而且我认为戴夫刚才的发言，也就是你们可以在你们的平台上用来打击滥用的方法，有一个先决条件，那就是你们的一线滥用队列监督人员达到了一定的熟练水平，但是老实说，这种水平并非全球所有注册服务机构都具备。当然，在你们优化流量以缩短滥用队列时，你们不一定有太多时间来开展深入的调查。

我还想说一点，因为我听到有人谈到了。我们已经看到算法生成的域名被用于网络管理。它们不一定就不好。在一些地方，人们可以用它们来运营业务。

基于滥用队列中的情况和你们的监督方法，要跟踪惯犯尤其困难。

我们没有做出一个简单的、肯定的回答，那是我们非常感兴趣的事情，因为它减少了我们平台上的滥用，而这正是我们渴望去做的。但是它要求对滥用队列中的情况有一个非常广阔的视野，要达到这一点绝非易事。

卡特琳 • 鲍尔-布尔斯特： 谢谢格雷姆。我想艾伦也要发言。

艾伦 • 伍兹： 还是艾伦 • 伍兹。对于戴夫 • 匹斯特洛刚刚的发言，我想说如果他离我近一点，我一定会站起来握住他的手，因为理解这一点非常重要。也就是说，DAAR 是一个展示统计数据的项目，但是在 DAAR 和实际行动之间，注册服务机构、注册管理机构或者其他有关方面还必须开展工作。所以谢谢你，戴夫。

伊朗嘉 • 卡函嘉玛： 谢谢，艾伦。

我想更具体一点，罗德，你提到在这方面已经做了大量工作。你能不能具体地讲讲需要哪种类型的数据才能切实促进这类行动？

罗德 • 拉斯穆森： 当然。有各种各样的方法。当然，它取决于滥用的类型。举个例子，真正容易检测的是域生成算法所生成的内容。域生成算法会被恶意软件用来创建一系列域名，这些域名未来可能会被注册。如果对恶意软件进行反向工程，就会获得将来可能会被使用的域的列表。然后就可以观察这些域的注册情况并采取相应的行动，因为它可能是安全研究人员的字符串，而不是坏人。那是一种方式。

垃圾邮件是一种明显的方式，已经存在 10 年、15 年、20 年以上，可能和基本的初步分析一样久远。它的分析方法现在已经非常成熟。

各种各样的平台、Facebook、社交网络都在使用它。所有电邮程序或电邮平台都会在用户允许的情况下查看内容，观察一些大规模发生的事件，然后再看看这些域是否恰好是他们要找的域。

这些信息将很有可能派上用场，也许是关联到一些元数据，比方说 WHOIS 查询或 DNS 查询，或者调查你们自己的已知或未知对象的数据库。为此你们可以使用一系列的公式。

此外还有附加到浏览器上的工具，有网络安全设备用来监视网络上进进出出的数据流，有非常复杂的机器学习算法来查找诸如隧道等行为，以及其他各种各样守护和监督你们网络的活动。丰富多样的技术可以结合到一起，形成这些不同类型的滥用领域的清单。

伊朗嘉 • 卡函嘉玛： 谢谢。感觉一整天都说不完。我想有一点很清楚，在这个领域，可用数据的多样性是关键。我想我们有一个远程问题。我们将稍后解答。卡特琳，你要问下一个问题吗？

卡特琳 • 鲍尔-布尔斯特： 是的。实际上，我想要回到策略制定所需要参考的不同类型的数据上，德瑞对其做了非常精彩的陈述。这个审视总体趋势和发展的想法可以为策略制定提供信息，由此到更具体的信息，注册管理机构和注册服务机构都需要了解，以便能够根据具体情况采取具体行动，那可能需要有另一种标准的证据。当然，它不是特别依赖犯罪调查之类。它可能也会受到特定提供商条款和条件的影响。

我想或许可以请丹尼斯分享一下你在为社群设定标准和为客户设定标准方面的特殊经验。根据你的经验，在如何起草条款和条件才能高效和有效应对滥用这个问题上，有没有要吸取的教训？

丹尼斯 • 米歇尔： 我是丹尼斯。

在我们的所有平台上，有一个广阔的全球安全和滥用缓解系统，一直处于监控和更新当中。

我们广泛协调各个行业和领域，分享最佳实践，不仅是在服务方面，还有安全数据分享方面。

我认为，在比较我们做什么和一些注册服务机构及注册管理机构做什么的过程中，有一个要素尚未真正解决，那就是这么做的动机和意愿。

商业选区就 CCT 审核所进行的滥用研究提出了大量意见，并提供了一些非常具体的方法，该研究可以以此为起点，提升我们合力缓解滥用的能力，并从总体上改进我们的工作。譬如：将处理滥用的动机和良好实践相联系；研究注册管理机构和注册服务机构必须支付的费用并将它们与最佳实践和结果相联系；确保这是首次滥用研究，今后还将持续开展，并且能够获得严谨和可操作的趋势数据；增加对高滥用率的注册管理机构的合规审查。

为应对滥用，目前可以做的事情有很多。我们能够越早在开放域中实施这个开放数据举措，越早在网站上看到 DAAR 报告的测试形式，就能越早地采取行动。谢谢。

卡特琳 • 鲍尔-布尔斯特： 下面是观众发言。一号。

雷格 • 利维 (REG LEVY)： 谢谢。我是 Tucows 和 ENOM 的雷格 • 利维。我想谈谈最近有人谈到的条款和条件问题。有一点千真万确，那就是我们大多数人都在条款和条件中规定了，我们可以出于任何原因或者没有原因地撤销域名，哪怕只是心血来潮。但这些条款和条件是为了保护我们，它们不是为了监督互联网或者进行任何类型的监管。它们适用于我们没有对某事做出决定，但是之后却又绝对必须做出决定的情况，在这种情况下我们就有采取行动的合法权利。它实际上并非只是为了满足我们心血来潮的想法。

卡特琳 • 鲍尔-布尔斯特： 我想我们很快要进入下一部分。但是我还要问乔纳森最后一个问题，就是发言中提到的特定指标的概念。

德瑞谈到，我们要寻找特定类型的滥用，而后还列举了一些工具。他指出垃圾邮件是其中之一。他认为另一个就是，侵犯知识产权有时可以联系到滥用，或者可以作为潜在滥用的指标。你能不能谈谈这些指标，以及它们在滥用识别方面起到的辅助作用？

乔纳森 • 马特考夫斯基： 当然。我是乔纳森 • 马特考夫斯基，来自 RiskIQ 和 IPCM，以下发言仅代表我个人。

首先，关于注册服务机构依据注册服务机构认证协议所承担的处理滥用投诉并适当开展调查的义务，这对社群有利。我鼓励各位好好利用它，并以此为契机来保护社群，防止滥用。这包括所有非法活动。

我们一致认为，窃取个人信息的网络钓鱼和内容密切相关。

我们都听到了 SADAG 报告是如何论述被恶意使用的误植域名的。从很多方面来说这都是真的，内容与安全威胁有关。特别是包含不止一个互联网地址的复杂威胁。

我相信大家都从新闻中了解到 Adobe Flash 弹窗是如何被利用来哄骗人们下载恶意软件，或者窃取电脑上的 CPU 的。

所以存在确定的关系。另外我也要说，注册管理运行机构并非总是能够了解到对滥用投诉无动于衷的注册服务机构。所以，当注册服务机构未履行义务时必须通知它们，以便它们能采取行动。

这一信息应该包含在技术统计分析中，也就是向 ICANN 报告的数据集中。并且 ICANN 也可以随时要求提供。

所以我想说，DAAR 项目应该在内部使用。我鼓励 ICANN 合规部在内部将它用于临时审核。回顾一些数据集 — 至少是 SADAG 报告 — 就会发现，相对于滥用投诉的总量而言，提交的合规报告比较少，但还是存在像南京这家公司一样的公司。

比如看看 Dynamic Dolphins 发生的事情。看看 ICANN 在 2013 年发生的事情。

所以谢谢。

伊朗嘉 • 卡函嘉玛： 谢谢乔纳森。接下来继续翻到下一张幻灯片。谢谢。那么，如何创建有效和透明的滥用报告。

我想我们首先请泰蒂娅娜来谈谈戴维 • 康纳德的演示，其中提到了一些不同的实例，在这些实例中禁用清单被用于不同的互联网浏览器和电子邮件，最终非商业用户也会使用。

所以我想问你的就是，最终用户的利益与其中一些统计分析的交集在哪里？能不能有效利用 DNS 滥用数据来创建某种用户友好型工具，能够向公众提示风险和潜在的滥用网点？

泰蒂娅娜？

泰蒂娅娜 • 拓毕那： 非常感谢。我是泰蒂娅娜 • 拓毕那。

首先，我要理清一个混淆的概念。我认为我们不代表最终用户。我们代表非商业用户。二者存在很大的差别，因为最终用户包括商业用户和非商业用户。

但是我要说的是，在整个滥用报告工具和滥用报告系统的问题上，我们确实占了一席之地。

我要再次强调我们是 NCUC。所以要知道，我们实际上并不收集统计数据。我们不会叫停网址。那么我们要使用哪种工具？

我个人可以肯定地说，我支持收集统计数据。我支持共享数据并通报给全行业。

但是在 ICANN 这里，属于 ICANN 使命范畴的技术性的 DNS 滥用，和仅仅关乎内容的滥用，二者是泾渭分明的。因为不是所有违反适用法律的非法活动都属于 DNS 技术滥用。

而且我们相信，ICANN 和 ICANN 所使用的工具应当和 ICANN 的使命紧密相关。我知道，有的人可能会提出他们的 RAA。但是 RAA 源自于 2013 年，而 ICANN 的使命确立于移交期间。所以我相信后者优先。

第二，我们必须小心谨慎。关于预防方法，我分享了很多。这里有一个主动行动、被动反应和先发制人的界线。那么预防是什么意思？行业参与者在什么时候必须采取行动？你知道吗？预防意味着什么？我想我们必须明确这一点。我已经说过，我们必须从狭义上定义 DNS 滥用。而且作为非商业用户我们也相信，我们不应该忘记打击滥用的主要方法不仅仅是暂停网址，而且还要抓住那些违法者和真正的滥用者。这是执法部门的工作。抱歉。我们还要 20 秒。

所以我们不希望中介机构或行业来充当内容警察或任何意义上的监督者。

这就是为什么当我们听到行业应该自我监督时感到害怕的原因。不应该那样。他们无论如何都应该处理 DNS 滥用。谢谢。

卡特琳 • 鲍尔-布尔斯特： 谢谢，泰蒂娅娜。

接下来要请德瑞从安全研究人员的角度，谈谈你们对这个数据应该多久公布一次的看法。在你们看来，有没有某种对安全社群有用的最低频率或理想频率？

德瑞 • 巴格利： 谢谢。回到我先前提到的 CCT 委托进行的研究，我认为有一点非常重要，这不仅仅是每五年开展一次的工作 — 每次都会有一个或者多个审核小组来调查这个问题，因为据我所知，它会在多个审核小组之间进行。而且我认为，鉴于 DAAR 产生的统计数据对社群公开透明，那么只要它作为一个数据集以某种形式持续存在，可能就会很有用。接下来你们应该做的就是，定期分析这些数据的实际含义。所以你们有数据提供给社群进行解构和分析。然后或许可以进行一些综合分析，就像 CCT 委托的研究所做的那样。也许可以一年两次，我认为那样将很有帮助。

因为从长远角度出发理解有哪些趋势非常重要。某些网络钓鱼活动和其他类型的恶意活动可能会在某些方面歪曲结果。所以持续不断进行评估，看看作为社群我们的境况如何，这非常重要。

如果你们不介意，我想回应一下泰蒂娅娜的意见。因为在我觉得泰蒂娅娜说得非常精彩，真正反映出了社群的多样性以及对这个话题的不同视角。

这就是为什么我认为我在前面的一张幻灯片中强调的一点非常重要，那就是，与其花数年时间反复争论各种因国家而异的不同的滥用情况，倒不如我们作为一个社群，着手开始解决一些已达成共识并且实际上有权处理的事项 — 通过在协议中禁止行为的形式，就从这些非常技术性的事项入手，而不是迷失在一片杂草丛中。

所以我确实认为，我们的工作要建立在泰蒂娅娜所发表的这些意见的基础上。我也非常认同艾伦提到的一点，我们作为反应方要调查问题并追踪滥用者是非常困难的。因为显然，那需要证据。

而且正如泰蒂娅娜所指出的，提供商不是执法部门。所以，从暂停违反服务条款的某项服务，到采取行动应对潜在的犯罪方面，中间有不同的梯度。

这就是为什么我确实认为转换到一个主动模型非常重要，在这个模型中我们可以采用一些明显的指标，以便在注册本身存疑的情况下，可以在域启用之前等待一段时间。也许它在五分钟内不会启用。也许你可以进行人工审核，并在 24 小时后再允许或不允许域运行。我的意思是，虽然不同的提供商会采用不同的模型，但是我认为转换到这个模型对我们非常重要。

伊朗嘉 • 卡函嘉玛： 谢谢德瑞。

戴维，你要补充吗？

戴维 • 康纳德： 是的。目前与 DAAR 系统内生成的数据有关的公布计划是生成月度报告，里面基本上是记录我们看到的各个注册管理机构、注册服务机构的汇总统计数据。

之后实际上还计划通过开放数据举措长期提供这些数据，这样人们就可以基于我们收集到的数据进行历史趋势分析和时间序列分析。

不过这是暂定的计划。事实上我们非常希望听到社群对数据发布频率或者数据发布方法的建议。

伊朗嘉 • 卡函嘉玛： 抱歉再问一下，你们也确定了第一份报告的可能发布日期吗？

戴维 • 康纳德： 目前我们实际上还在对我们提供或者接收数据的各种数据源的许可要求进行评估。

所以其实我还不能给出一个具体的日期。因为...律师的原因。

[笑声]

伊朗嘉 • 卡函嘉玛： 有道理。现在请拿到麦克风的人发言。3 号，有请。

米尔顿 • 穆勒

(MILTON MUELLER)： 我是米尔顿 • 穆勒，来自佐治亚理工学院。谈到 DAAR，似乎存在两种不同的看法。我听到戴维说的是，我们会收集大量数据，发布报告，然后可以用这些报告来指导策略。但是我听到注册服务机构和注册管理机构的观点是，在看到数据和采取行动之间，还有大量工作要做。

另一方面，我听到有人谈到更先发制人的行动，这些数据实际上可以指导某些先发制人的行动。

所有我有一个问题，DAAR 究竟是什么或者将会成为什么。它有多大的扩展性，戴维？威胁在变化。现在你们完全依赖第三方 RBL。实际上你们并不生成它对吗？ICANN 实际上并不会收集这些基础数据。你们只是汇编整理，并使它成为一个 DNS 行业资源，这一点我认为无可厚非。

但是威胁在变化。罪犯在变化。他们的手法也在变化。

将来你们如何应对这些创新？你们要发展出一个职能部门来做，还是继续依赖第三方实体获取这些数据？

戴维 • 康纳德： 简单的回答就是，社群告诉我们做什么，我们就做什么。

在 DAAR 的语境中，我们追踪的威胁是北京 GAC 公报中所指明的威胁。如果有一天，社群建议我们追踪其他的滥用形式，那么我们将会看看我们可以做些什么来将它纳入到 DAAR 框架中。它是可以扩展的。

至于数据来源，对我们使用的数据来源的首要要求就是，它们必须公开。例如，如果 ICANN 生成的一个数据来源提供给了 ODI 或者其他机制，那么我们可能就会把它纳入到 DAAR 系统中。但是那同样也取决于社群的要求。

我想对于这个话题，我的同事匹斯特洛先生可能也有话要说。

戴夫 • 匹斯特洛： 是的，有一点。我非常高兴你问这个问题，因为我相信一年后我们将可以做一些事，而这些事是以前我们在本行业中无法做到的。我们将用一年时间创造一半历史。在这期间你们可以看到聚集和迁移行为。你们可以看到某个注册管理机构或注册服务机构的注册突然激增的延迟或时间，以及这些域名如何使用。如果我可以给你们展示一幅图表，那么里面就会显示某个注册服务机构出现约一千个注册的激增，以及在一个管理期后这些注册随时间的实际分发情况。现在，这和 SADAG 分析损害和恶意注册的域所基于的一些衡量指标非常不同。那会给我们呈现一些新的信息。

至于威胁的不断演变，你知道，我们和系统开发人员讨论过添加引导或黑名单的事。引导或黑名单是一些作为服务站点的分布式拒绝服务的列表。那是一个新出现的威胁。如果我们认为这个数据库中的数据是可信的、可靠的、准确的、公开的，满足我们的所有标准，那么我们就要坐下来好好考虑要不要把它加入我们的系统中，以便社群了解到这又是一个威胁。但还是像戴维说的，我们已经建立了一个平台，这个平台我认为在很多方面都具有极大的可扩展性，只要我们了解我们要衡量哪些威胁以及我们要使用哪些衡量指标，那么我想你建议的很多事情我们就都可以做。

戴维 • 康纳德： 谢谢戴夫。我想我们有两个远程问题。请把它们读出来，我们将一一解答。之后我想我们就要讨论第三个也是最后一个要点。

詹姆士 • 科尔 (JAMES COLE)： FAITID 的马克西姆 • 艾尔佐巴 (Maxim Alzoba) 提了一个问题。“ICANN 的首席技术官办公室有没有计划，有没有和社群中的 RySG 和 RrSG 部分就 DAAR 工具进行过交流，以使这个资源对注册管理机构和注册服务机构有用？”

伊朗嘉 • 卡函嘉玛： 能不能也读一下第二个？抱歉。

詹姆士 • 科尔： 第二个问题是，“为什么要把一家做法有问题的公司 Spamhaus 用作一个受信任的来源？该公司的升级程序包括切断注册人和注册服务机构、互联网，阻止注册服务机构 SAR 系统 DNS 服务器的邮件服务器，对社群毫无责任和透明度可言。”

戴维 • 康纳德： 谢谢你们的问题。先回答最后一个问题，使用 Spamhaus 是因为在反滥用社群中，Spamhaus 被认为是一个受信任的可靠来源，并且符合我们在最初构建草案时所指定的禁用清单选择的全部标准。另外值得一提的是，无论我们对某个禁用清单的感觉如何，事实上这些禁用清单都得到了业界、学术界、商业和非商业提供商的使用，影响着互联网上的流量。而且你知道，假装某个禁用清单不重要，因为你对它们的策略不敢苟同，并不能改变其他人依赖这个禁用清单来阻止特定域或 IP 地址的流量这个事实。如果标准发生变化，使得 Spamhaus 不能再被视作一个可行的选项或可行的数据贡献者，那么显然我们就可以做一些必要的调整。而且你知道，如果有明显的证据表明他们在处理请求时不遵循自己的规范，那么这又是一个我们可以审视的方面。根据我们以往的经验，很多时候人们之所以会投诉某个禁用清单，就是因为他们自己由于这样或那样的原因被

列在了禁用清单上，而在要求删除的过程中又遇到了挑战。任何时候只要我们有证据证明某个禁用清单没有兑现它们的承诺，那么这就会成为我们重新考虑是否将它们包含在数据源中的一个理由。

至于向社群提供数据，正如之前所说，我们目前的计划是通过开放数据举措提供这些数据。目前的计划是每月提供一次，但是还要取决于社群的要求。我们可以调整。我们可能会根据他们的任何需求做出调整。

伊朗嘉・卡函嘉玛： 谢谢，戴维。我想我们还漏掉了一个远程问题。我想很快来看一下这个问题。

詹姆士・科尔： 这个问题来自 Amazon 注册管理机构的克里斯蒂娜・罗塞特 (Kristina Rosette)。“ICANN 打算实施哪些机制和流程，以便在公开 DAAR 数据之前避免误报和潜在责任？”

戴维・康纳德： 我猜又是问我的。前面说到，我们不会自己生成这些数据。我们要依赖一些人人都可以接触到的外部实体，不管是通过支付许可费还是公开提供。如果某个报告被认定为有误，就会影响到这些 RBL 的数百万用户与相关资源的交互，不管这个资源是域名还是 IP 地址。有误报是事实。坊间经常传闻惊人的

误报情况。但是我们看重的事实和选择禁用清单的标准是，它们受到业界和学术界的审查，它们有添加和删除域名的文件化流程并遵守这些流程，并且这些禁用清单有一个清楚的运行机制。

关于责任的问题，你知道，我既不是律师，也不会在互联网上扮演律师的角色。

卡特琳 • 鲍尔-布尔斯特： 非常感谢，戴维。下面进入讨论的第三部分。我们要用最后这 12 到 15 分钟时间，来看看滥用报告如何支持注册管理机构和注册服务机构的滥用预防和缓解工作。在合同合规和执行、以及策略制定中，可以如何使用它？我们已经谈到了其中的一些问题。我们还没有过多谈到的是它在 ICANN 内部可以如何使用。或许我可以请教杰米，在这个流程中你们有没有提出自己的需求，以及你们怎么看未来合规部可能会如何使用它。

杰米 • 赫德伦
(JAMIE HEDLUND)： 谢谢。我从来都是毫不犹豫地表达我的需求。但是我们一直和 OCTO 密切合作，我想合同合规部基本上对 DAAR 非常兴奋，原因有几个。第一，它确实帮助提供了有数据支撑的证据，让我们聚焦应该在哪里部署资源。第二，如果组成 DAAR 的这些清单真的被商业企业、其他方面用来就电子邮件服务和网络访问之类的事项作出决定，那么我们的工作就会轻松许多，因

为这些注册管理机构或注册服务机构可能会发现自己的地位提高了，从而就有了内在的动力。

明确一点，DAAR 输出的是汇总结果，正如戴维所说的。我们不能将汇总的结果用于合同合规工作中。我们必须从更低的层面出发，寻找有望可以用于清理一些注册管理机构和注册服务机构区域的实质性证据。

最后一点我要说的是，我看到的输出结果显示，极少数的缔约方要为绝大多数的滥用负责。而且这些实体往往都不是 ICANN 的积极参与者，至少我看到的情况是这样。所以我想，如果我们可以利用这一数据并取得进展，不仅对用户和整个互联网有益，而且还将对 ICANN 和多利益相关方模型的可信度和合法性有益，要知道，移交后这个模型愈发受到关注。

伊朗嘉 • 卡函嘉玛： 谢谢杰米。哦，艾伦。请讲。

艾伦 • 伍兹： 感谢杰米的说明。听到你这样说很好。我还要指出一点，不法分子确实存在，除此之外还有许许多多注册管理机构正竭尽全力阻止滥用，他们还主动出席 ICANN 会议，并积极参与到这些讨论中。我的意思是，在我看来，从 Donuts 的角度，我们完全赞成执法。一旦我们获得这些证据，并且能够以那种方式决定和测试这些证据，那么我们绝对非常乐意这么做。

伊朗嘉 • 卡函嘉玛： 谢谢。格雷姆，你举手了吗？没有。

格雷姆 • 邦顿： 抱歉。不是，举了。我是格雷姆。你们知道，注册服务机构非常赞成将不法分子从平台上清除。那样会减轻我们其余人的负担，我们一直在非常努力地保持平台干净。那样也会减少很多策略影响，因为我们在努力寻求适用于所有缔约方或所有注册服务机构的策略解决方案，而如果是一个特定的行为者，那么这个解决方案就必须非常有针对性，适用范围非常窄。而且我认为，做到这一步会使很多问题迎刃而解，我们大家的日子也会轻松很多。谢谢。

伊朗嘉 • 卡函嘉玛： 一号麦克风。

格雷格 • 莫尼耶
(GREG MOUNIER)： 大家好。我是来自欧洲刑警组织 (Europol) 的格雷格 • 莫尼耶。我有一个问题要问格雷姆和艾伦。域名行业是一个利益驱动的行业，在我看来，主动的 NTWS（音）措施在行业眼中通常意味着额外的成本。所以我的问题是，如何才能扭转这个逻辑，确保主动的 NTWS 措施成为行业中的一项竞争优势。换句话说，比如，在 Tucows 的营销战略中说，“在 Tucows，我

们有着最低的滥用率，所以和我们在一起是安全的”。这样，你们就可以赚更多钱。

[鼓掌]

格雷姆 • 邦顿： 谢谢，格雷格。我是格雷姆。这是一个很好的问题。我也不确定。我想，采取主动也会带来一定的责任，在我们追求盈利时也要把这个责任考虑进去。所以技术只需要做到我们可以以某种方式对自己的注册采取主动这一步就可以了，但是我认为目前还没有达到这一步，或者至少我个人没有看到这一点。

伊朗嘉 • 卡函嘉玛： 罗德，你还有补充吗？

艾伦 • 伍兹： 我是艾伦 • 伍兹。来自 Donuts。我要说，我们非常重视这个问题。而且，这本身就是我们处理 DNS 滥用的方法的重要组成部分。但是，我们是 DNA 和健康域举措等活动的成员，并且尽力实施行业举措，正是这些自愿性举措将我们与不法分子区分开来。所以还是要这么做。

另外你也知道，每当我们撤下一个域时，事实上，也相当于告诉滥用者到别的地方去。这是我们要思考的另一个问题。我们可以将它们踢出我们的平台，但是它们会找到其他平台，不法分子的平台。所以我们也要着力清除不法分子。

伊朗嘉 • 卡函嘉玛： 谢谢。（姓名）在排队，所以我要给他一个机会发言。

罗德 • 拉斯穆森： 谢谢。还是罗德 • 拉斯穆森。我参加的第一场 ICANN 会议，就是讨论这里的第一点。当时我代表反滥用行业，和注册服务机构进行讨论。遗憾的是，那场温哥华会议和会议期间发生的一些其他事情阻碍了这一讨论的扩大。你们可以查询一下历史。无论如何，那是十多年前的事了。现在，在这方面已经做了许多工作，而且非常成功。有很多例子。比如，反网络钓鱼工作组、我本人以及你们很多人都认识的格雷格 • 亚伦 (Greg Aaron) 自 2007 年至今一直在定期编写关于用于网络钓鱼的域注册的趋势报告。我们会和注册管理机构和注册服务机构一起，使用这些报告来识别问题和趋势，并且这些报告改变了他们处理问题的策略。那既是在 ICANN 空间，又是在 ccTLD 空间。特别是，ccTLD 曾经有过一些重大问题，通过找出其中的模式后已经得到解决。

此外，许多注册管理机构和注册服务机构还设立了各种自动报告机制，以及各种类型的后端框架。其中一个框架就是合同。过去我曾拥有一家公司，与这类实体签订了合同，作为它们的代理来确定某个对象算不算滥用，并代表他们做出决定将其撤下。还有一个例子是受信任的干预者计划，实际上你们可以从中获得认证，然后就能将这一信任转移给其他真正拥有专业知识从而能够胜任的人。所以，你们可以自动化并转移这些事项，模型确实存在。它更多的是提取出这个信息让人们可以使用的问题。谢谢。

卡特琳 • 鲍尔-布尔斯特： 时间刚刚好，罗德。一号麦克风。

大卫 • 泰勒

(DAVID TAYLOR)： 谢谢。我是大卫 • 泰勒，来自 Hogan Lovells。我是一名律师，你们可能会发出嘘声，但我还是 CCT 审核小组的一员，你们可能又要欢呼了，我想。也就是说，我和那个大胡子是一伙的。我的问题其实在于滥用报告，它显然是一个关键问题。有很多好的注册服务机构，也有很多坏的注册服务机构。有很多好的注册管理机构，也有一些坏的注册管理机构。我们知道，当我们追踪某人时，有时单个注册服务机构要花大量的时间才能撤下某个域名，即使非法滥用和非法活动非常明显也是如此。我是说非常明显。在法庭上很容易胜诉。即便如此你可

能还是要潜伏三到四周，才能让他们把它撤下。所以我们可以去找 ICANN 合规部，在某些情况下我们会去。

但是当我们撤下了一个注册服务机构时，正如德瑞之前所展示的 — 杰米，我们谈论过这个，但是你提到了 AlpNames 这家注册服务机构 — 尽管你看到滥用率很高，比如 .SCIENCE 区域文件的 51% 都是滥用域名，但你还是可以看到它仍然在运行，这家注册服务机构经过一年或半年之后仍然没有得到认证。但是外行就会很好奇，为什么要花这么长的时间来处理一个如此明显的问题？显然这是有原因的，你不能做自己能力范围以外的事，但我还是不能理解，也很难向委托人解释。

杰米 • 赫德伦：

所以基本上可以归结为两件事。一是对于任何高滥用率的特定缔约方，可操作证据和汇总报告都还不够。你还需要实质性证据才能够让我们推进工作。

二是合同本身有一些限制。比如，我们不能自己命令暂停或者撤销某个域。

我认为使用 DAAR 输出和一些潜在域名有望可以做到的一件事就是，它将表明我们在哪些地方做得成功，哪些地方做得失败。在我们失败的地方，长期存在一些不法分子，即便使用我们手中的工具仍无济于事，但这个信息将会提供给社群，以供社群在制定策略时使用。

所以即使我们不能成功地帮助清理注册管理机构/注册服务机构空间，但社群和人们 — 比如你们自己 — 还是会拥有证明哪里无效的证据，这一证据有望成为更改策略或合同的信息来源。

伊朗嘉 • 卡函嘉玛： 谢谢杰米。你的回应相当迅速。在本次会议结束之前，我再讲最后一点。我想让丹尼斯作为另一个受影响方发言，谈谈所有这些报告以及如何将它用到决策制定中。

丹尼斯 • 米歇尔： 当然。SADAG 报告，CCT 滥用报告表明，新 gTLD 遭遇的滥用率几乎比传统 gTLD 高十倍。该报告和相关资料中提供的滥用数据非常有用，并且和比方说目前正在运行的权利保护机制 PDP 以及目前正在运行的、旨在为下一轮新 gTLD 创建政策的后续程序 PDP 密切相关。

这只是一个例子。还有很多其他数据适用于像隐私/代理实施之类的事项以及 ICANN 内部的其他工作。

但是最终确实需要获取滥用数据和信息以及趋势信息，以便能够指导 ICANN 内的各项活动。我们理应成为一个以事实和真实数据为基础来制定政策的社群。这么做绝对是关键所在。而且戴维，如果说我们可以做些什么来请走律师的话，那就是我们可以将 DAAR 报告纳入到公共领域，并且可以再次启用 ODI

举措及其中的数据，我想它已经荒废大约四个月了，这么做将会大有帮助。我们非常期待在未来支持这些工作。

谢谢。

戴维 • 康纳德： 澄清一下。我所说的律师碍手碍脚的话当然是开玩笑的。我们必须理清许可协议，那需要一点时间。我们非常有信心，在不久的将来我们就能够推进一些（听不清）统计报告，可以想见，在那之后不久，应该就能以电子数据表的形式提供更丰富和更全面的信息。

卡特琳 • 鲍尔-布尔斯特： 好的。谢谢，戴维。由于时间关系，我们不能再回答任何问题了。抱歉。我想本场讨论证明了一点，那就是更多的讨论势在必行。讨论中提出了对缓解滥用的一些不同观点，我认为这一点非常好，因为它突出了社群各个部分从政策制定到采取单独行动的不同需求，不管是在预防上还是在反应上，而且还帮助确定了使用数据进而指导 DAAR 的方法。

此外我认为在戴维和杰米的发言中提出了一个非常有趣的视角，那就是，滥用集中在少数缔约方身上。在我们看来，这里的汇总数据符合特定数据，因为当然对此可以采取行动。即使在德瑞提到的 76 个例子中有两个属于误报，仍然还有其他充足的数据可以支持采取某种形式的行动。

未来我们可能要关注，如何才能缩小汇总数据和可操作数据之间的差距。对此，我想我们可以回到伊朗嘉在开头提到的这个原则的概念，下面我将交给他来继续谈谈这部分。

伊朗嘉 • 卡函嘉玛： 谢谢。

我想说，感谢所有专家组成员的参与。的确，我认为继续推进这个对话非常重要，而且我想主动为 PSWG 报名，来继续引导这个讨论。但是我认为，社群理应获得适当的跨社群机制，来切实组织和汇总这些问题，以便切实推进这项工作。所以我想，我们还会回来继续思考如何最好地推动解决其中的一些问题，并为社群提供合适的机制来继续为缓解 DNS 滥用而努力。我们有望以此作为一个论坛，让社群时刻掌握最新动态，同时也使社群保持足够的开放和透明，以期推进这方面的工作取得进展。

感谢大家的到来，也希望大家未来参与到此类活动当中。

谢谢。

[鼓掌]

[会议记录结束]