

圣胡安 — 标识符技术健康指标
大西洋标准时间 2018 年 3 月 13 日星期二 — 17:00 至 18:30
ICANN61 | 波多黎各圣胡安

凯西·彼得森

(CATHY PETERSEN): 大家下午好。我们将在几分钟后开始标识符技术健康指标会议。请大家再稍等几分钟，我们的会议即将开始。谢谢。

阿兰·杜朗德

(ALAIN DURAND): 大家下午好。这里是标识符技术健康指标 (ITHI) 会议。这个项目已经开始了一段时间，今天我们将展示一些有意思的数据 [听不清]。你会发现这些数据非常有意思。我觉得它们挺有意思的。

此次会议中，我们共有三位发言人。第一位是保罗·威尔逊 (Paul Wilson)，现任 NRO 主席。他将为我们介绍 NRO 就此领域所开展工作的最新进展。

第二位和第三位将侧重说明该项目的主要部分，即由 ICANN 管理的事务。第二位发言人是克里斯蒂安·胡伊特马 (Christian Huitema)，他将就当前的衡量标准和当前衡量标准相关的数据发表演讲。

第三位发言人为杰夫·休斯顿 (Geoff Huston)，他将就拟定的一套 [某些] 新衡量标准发表演讲。

注意：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。

话不多说，现在有请保罗，他将为我们介绍数字领域开展的活动。保罗？

保罗·威尔逊：

谢谢阿兰，大家好。我们一共运行了五个地区互联网注册管理机构，并使用非常熟悉的 WHOIS 服务运行一个 WHOIS 注册管理机构。所以我们有五个不同的注册管理机构，它们分别由五个 RIR 管理。它们之间具有很强的协调性。从技术上看，它们可能有不一致的地方，当然还有错误和不完整等等缺陷。因此，RIR 在 NRO 的领导下相互协作，确保这些注册管理机构相互之间存在意义，并且正依据其存储的记录完成其目的。

此工作我们已经执行了很长一段时间，但我认为近年来情况有所变化，因为有更广泛的相关方对数据库、数据库的正确性和有效性产生了更大的兴趣。另外，更新的步伐也加快了很多。因此，在我们解决目前的 IPv4 地址短缺问题之前，地址分配状态相当稳定。它们被分配到保留和使用这些分配的各方。但是现在，有很多转移正在进行。在地区内和地区互联网注册管理机构之间有很多转移正在进行，显然我们需要更新数据库。这就是我们关注正确性和完整性等问题的另一个原因。

正如我所说的，自 RIR 成立以来，我们一直在用心关注注册管理机构的工作。我们尚未就健康问题发表评论，但有关标识符健康的想法非常新颖，我想这是 ICANN 项目带来的新议题。话虽如此，我们一直保持着关注。

另一方面，当然，我们与网络运营商建立了会员关系，他们是地址块和 ASN 的第一接收人。所以，他们有义务根据与每个 RIR 的关系不断更新其记录并保持最新状态。这里的政策问题在于究竟有哪些期望以及如果不遵守这些政策会有哪些处罚。

这些问题一般都是按区域进行处理。因此，五个 RIR 的确拥有独立的政策流程和会员资格，并将在不同时间讨论与 WHOIS 相关的政策。正如我所提到的，现在这些讨论的频率和强度也有所提高。我想可以说，围绕这五个地区，我们都在以不同的方式加强管理，但整体上都同样朝着更清晰、更严格地执行政策的方向迈进。

ICANN 执行 ITHI 项目确实不足为奇。它显然是我们所有注册管理机构职能执行者的共同利益，因此我们决定插手 ICANN 的 ITHI 项目。我认为这其实相当有用，因为虽然我们已经开展密切合作，但实际上并未确定一套一致的衡量标准，而我们现在已经通过 ITHI 项目往前迈进。

事实上，我们去年花了一段时间了解我们的注册服务协调小组的工作，该小组的工作人员由五个 RIR 中从事注册服务领域工作的人员组成。针对我们所提到的数字空间中的标识符健康问题，该小组完成了一些关于制定衡量标准草案的工作。他们还发起了关于草案的公共协商。

公共协商于去年年底进行，它为我们的社群提供了针对该流程提出反馈意见的机会。事实上，我们收到的反馈意见非常少，

所以我们现在正在准备文件，即将完成以供最终批准和发布。该文件基本上以 WHOIS 记录的形式说明了数字空间中的标识符健康状况。目前我们的进度是到了三个 C：全面 (comprehensive)、即时 (current) 和正确 (correct) 的数据，这也是我们的目标。

这些目标划分为五个具体措施，即：与数据库完整性相关的数据库可衡量标准、唯一性、我们的数据库与其他外部官方记录的匹配、数据在实际覆盖注册管理机构中记录的人员方面的有效性以及数据的即时性。该文件还指出了与这些措施无法达成目标相关的各种风险，并分析了无法达成目标的可能原因。

这个文件很快就会发布。我们无法提供的资料是，由于衡量标准还处于草拟阶段，我们目前还无法提供有关我们的合规性的实际数据，关于这方面我想阿兰稍后将为大家演示。但显然，制定这些标准的目的是能够对一些指标进行衡量，从而设定我们希望遵守的目标并追踪某个时间段内的合规程度。

因此，我认为如果你对数字空间感兴趣，那就关注这个空间，我们将适时报告五个 RIR 数字空间中的互联网标识符健康状况。我想就这些了。谢谢阿兰。

阿兰·杜朗德：

谢谢保罗。我想借此机会感谢你和数字社群的其他成员与我们合作开展此项目。我认为这是一次非常有意思的合作，在此过程中我们学到了很多知识。

保罗·威尔逊： 是的，我同意。同样也感谢你，阿兰。谢谢。

阿兰·杜朗德： 现在我们正在进行同一流程，例如检查 [问题] 空间和确定衡量标准，然后进行实际的衡量，因此它实际上是正常状态。但是你目前还无法提供数据，那么不管什么时候能准备好，我们都期待将来看到第一批数据。

现在我们换个主题，谈谈域名空间。克里斯蒂安将为我们介绍此方面的进展。

克里斯蒂安·胡伊特马： 大家下午好。我是克里斯蒂安·胡伊特马。在与阿兰一起研究可以通过哪些工作制定 DNS 的实际衡量标准后，过去一年半里，我一直在研究 DNS 数据和 [状态] 的衡量问题。

正如保罗所说，在设定这些衡量标准时必须遵循一些原则。我们采用的原则基本上就是这张幻灯片上的这些。这是我们第一次真正希望在技术上实现衡量标准运营。我们不想涉及政策方面。制定衡量标准的目的是描述系统的状态，而不是以某种方式做基本判断。

我们一直在考虑确定我们想要跟踪的、可能存在问题的领域，确定这些领域的衡量标准以及衡量它们的方法。

另一个原则是我们不想使用快照。我们想要实现的是建立一个持续长期运行并本质上提供衡量标准的系统。我们的目标是每个月发布一个新的数值，当然也发布过去几个月的数值，以此估计趋势。因为我们认为趋势与实际数值几乎同等重要。

这就是我们要实现这个目标的原因。我们在自动化方面投入了大量资金和精力。我们在多个区域设置了探测器，并不断进行反馈和实现自动化。因此，发布数据的网站、每个月生成的衡量标准等等都是自动化的。

在展示的幻灯片中，我们将给出衡量结果。与不想涉及政策方面的原因相同，我们希望给出衡量结果的原始值。每次看到一个数字，你会说：“哦，X 轴坐标值现在达到了 29%。为什么会这样？”那么，我们的一般回答是：“我们不知道为什么会如此。”我的意思是，我们可以猜测，但你猜测的结果和我们的一样好。所以我们不想把这些猜测结果放在公布的衡量标准中。这些衡量标准就是直接的衡量结果。

还有一个原则是我们非常小心，避免隐私问题。所以我们发布的所有数据都是原原本本的统计数据。我们的所有工具均为开放资源，我们的所有结果都会公布，因此可以进行分析。

我们在之前的会议中做过几次演示。例如，我们已经在阿布扎比演示了 ITHI 衡量标准。在我们看来，衡量标准分为七类。首先，我们正在研究 WHOIS 数据的准确性。然后我们正在关注根服务器的行为以及它们在一定程度上导致的滥用的程度。

抱歉，是域名滥用、域名系统的滥用。我们正在查看 DNS 根流量。

针对这里列出的所有这些衡量标准，我们都有数据来源。例如，针对 WHOIS，我们正在从事 ICANN 合规部的工作。针对域名滥用，我们正在从事 DAAR 项目的工作。针对根流量、递归服务器、DNS 参数的 IANA 注册管理机构和 DNSSEC 部署的衡量，我们正在研究根流量或递归解析器流量的扫描值。我们正在与递归解析器协作进行有效的 [探测]，以获取这些统计数据。

过去一年，我们一直在努力确定这些衡量标准。现在我们已经可以对首批数据进行介绍。在过去两个月里，我们已经设定了取得的初始数据，而且已经能够获取 M1、M2、M3 和 M7 的数据。杰夫·休斯顿将在下个发言中展示 M5 的数据。我们还可以通过早期协作获取 M4 和 M6 衡量标准的初始数据，这些数据与客户端使用 DNS 有关。

所以我们整合了已经开发的 M5。我们将建立渠道并使用更多探测器，这样我们就可以获得比衡量标准 M4 和 M6 更多的数据。我们将丰富这些数据并在 ITHI ICANN 网站上发布。

第一个衡量标准，即 M1。M1 跟踪 WHOIS 数据的准确性。我们通过使用准确性的代用指标实现此目的，即投诉次数。我们不会使用投诉的 [实际] 次数。我们使用的是 ICANN 合规部已验证的投诉的次数。目前，该次数不到百万分之六。这是我

们的第一个数据，所以我们还无法确定趋势。但是随着时间的推移，我们会追踪这一趋势。

有了所有这些数据，我们就会发现平均值并不能说明问题。如果我告诉你，平均每注册的一百万域名 [数字] 中有 6 个投诉，这只是一个平均值而已。我们这里绘制了一条曲线，代表投诉的 [听不清] 频率。基本上，对于 Y 轴上以及 X 轴上的投诉总数，注册服务机构数量从投诉次数最多到最少排列。

我们可以看到，这个分布不是 [听不清]。如果每个注册服务机构的投诉次数相同，你会在斜线的位置看到一条直线。但事实却不是这样。你会看到这条线非常弯曲，大量向 Y 轴方向倾斜。实际上，其中的六个注册服务机构占总投诉的至少 50%。我的意思是，这不是一个偶数，六个注册服务机构占比超过了 50% 多一点。而其中 44 个注册服务机构占总投诉的 90%。这是从总共近 2,000 个注册服务机构中得来的数据。所以这里存在非常严重的 [偏态] 分布。

正如我所说的，这些是 [听不清] 数字，而不是对原因的判断或推理。但这就是我们研究的。

凯西·彼得森：

不好意思，克里斯蒂安。我们收到了一条线上问题。

克里斯蒂安·胡伊特马： 有请？

凯西·彼得森： 问题来自凯茜·克莱曼 (Kathy Kleimanin)：“你怎么知道 WHOIS 投诉是有效的？我们知道有些投诉是以骚扰为目的。”

阿兰·杜朗德： 我来回答这个问题。我们一直与 ICANN 合规部密切合作。我们研究的并非所有投诉。我们只研究与数据准确性有关的投诉。还有很多其他类型的投诉我们没有考虑在内。

ICANN 合规部有一个查看这些投诉并对其进行评估的流程。如果他们认为有足够的理由对这些投诉进行研究，就会发出他们所谓的“第一个通知”。如果没有得出结果，他们就会发出第二个通知，然后是第三个通知，然后可能一直发送直到 [数据外泄]。这是一个非常明确的流程，在 ICANN 合规部有详细记录。

因此，再次回答这个问题，我们只研究与 WHOIS 注册数据库的准确性有关的和已经过验证、通过第一个通知阶段的投诉。

克里斯蒂安·胡伊特马： 谢谢，阿兰。那么以上就是关于 WHOIS 准确性的衡量标准 M1 的内容。衡量标准 M2 系列涉及的是域名系统滥用问题，为此我们正在与 DAAR 项目合作。他们正在跟踪四种类型的滥用行为：网络钓鱼域使用的网站数量、恶意软件域使用的网站数

量、僵尸网络命令与控制的数量以及垃圾邮件域的数量。衡量标准定义为 10,000 个域名中滥用域的数量。

我们现在看到的是全球平均值，前三种滥用类型的平均值基本为 4 个或 3 个，对于垃圾邮件域来说平均值则大得多，因为垃圾邮件分布非常广泛。

现在我们像分析 M1 一样进行说明，我们同样可以看到，这些平均值并不能完全说明问题。看一下每个 TLD 的分布情况就知道了。例如，涉及网络钓鱼时，一个 gTLD 就占了所有网络钓鱼域的 50% 以上。仅 11 个 gTLD 就能占据所有网络钓鱼域。我们看到其他域也有同样类型的偏态分布。这显然表明了问题的结构。

我们一直在努力为各注册服务机构进行相同的衡量，但我们不希望花太多时间在注册服务机构数据上，因为我们的注册服务机构数据必须通过 WHOIS 流程进行评估，并且需要遵循所有使用 WHOIS 数据的限制条件，包括时间和其他所有方面的限制。因此，只有当我们获得的数据能够真正证实可以被信任时，我们才会认真对待，现在还只是初步尝试。

但是我们想用一些像这样的表格来呈现这种数据偏态分布，说明有多少 gTLD 占据至少 50% 的网络钓鱼域、恶意软件域等。然后说明有多少 gTLD 占据至少 90% 的这些域。正如我所说的，我们正在衡量一些东西。我们不会提供任何详细解释，也不会进行推理说明出现这种情况的原因。

M1 和 M2 数据来源于 ICANN 合规部和 DAAR 项目，且都与数据质量有关。我们稍后会看到的 M3 和 M4 数据则与实际 DNS 流量有关，就是这里展示的内容。M3 衡量根流量相关的问题。我们通过检测 L 根的方式衡量根流量。我们基本上每天会对每个 L 根服务器进行一次抽样。抽样方式为随机抽取，所以当我们将其聚集到一起进行统计时，这些样本就代表了所有时间的变化情况。然后，我们会获取所有这些样本并每个月进行总结，最后获得这些衡量标准。

大家现在看到的是第一个衡量标准：有多少根查询得到的是“未找到此域”响应？答案是非常多，几乎是根流量的三分之二。这些查询无法得到特定的值。然后我们看看在剩下的查询中有多少可以被解析器缓存。我们再次看到，这个比例比较合理，为近 30%。我们不知道是否能被缓存的查询大约占 6-6.5%，它们很可能不能被缓存。我们每个月都会跟踪这些情况。大家可以看到当前值和平均值，以及显示它们所占域的比例的饼状图。

对于得到“未找到此域”回答的查询，即饼状图中更大的这一部分，我们尝试将其拆分为几个小的组成部分。为什么呢？我们发现正在研究的问题分为四个组成部分：保留名称、IETF 保留的名称（例如 .local，共有 5 个或 6 个，约占流量的 3.4%）、频繁泄露的字符串（例如 .home，占流量的 9.3%）以及频繁出现的模式（我们发现数据中有一个模式）。它们不是频繁出现的字符串。每个域名只出现非常短的时间。虽然有

很多不同的域名，但它们都遵循一定的模式，于是我们试图弄清楚这些模式。然后探索所有其他问题。大约有 10% 的字符串无法直接通过这些流程解释。

对于 RFC 6761 中定义的特殊用途域名，我们发现大部分使用的都是 .local 域。它大约占现在根流量的 2.77%。我们还发现了其他保留域，但数量要小得多：.Localhost 有很多，.invalid 有很多，其他域则极少。

对于频繁泄露的字符串，我们所做的是获取根区中最常见的字符串，在当前实施的当前差异中，我们只研究至少发生了 0.01% 时间的字符串。

在这张幻灯片中，我只展示了至少发生 0.02% 时间的字符串，因为该数值越低，结果就越不确定。而且展示太多的话，大家读起 PowerPoint 来会非常费劲。

我们再次看到有一个域名占据了主要部分，它就是 .home，占据了根区中请求的 3.5%。然后我们还可以看到其他一系列域名。这里很重要的一点是，我们可以衡量根区中这些域名的泄漏情况，并且可以逐月跟踪，这样我们就知道哪些域名正在使用中以及哪些域名反复出现。我们可能会发现它每个月都会有所变化。有些域名将会消失，但我们可以看到有些一直出现的常用核心域名。

要告诉大家的是，我们在此根流量中看到的很多域名均为非特殊用途域，并且与经常使用的字符串不一致。这些都只是随机

的域名。事实上，如果你看到了这里的说明，就会发现我们按这些域名的长度对其分布情况进行了区分。我们看到这些域名的长度大部分都在 7 到 15 个字符之间。我们没有展示更长的域名，因为它们的数量非常非常少。

当我通过随机抽样查看这些域名时，很多长度在 7 到 15 个字符之间的域名都看似由计算机随机生成。并非所有都是如此。实际上，我们很难区分哪些是由计算机随机生成、哪些是通过某种命名计划产生，例如在 Wi-Fi 网络中的命名计划。但这是我们想跟踪的内容，我们希望更进一步研究和深入分析。

以上就是根流量相关的内容。去年我们在开展第一次研究时做了一些实验，我们很快得出结论：根不一定代表用户产生的所有流量。如果你了解 DNS 架构，就会知道在根已经过 DNS 解析器过滤的情况下能看到什么。实际上，如果 DNS 解析器应用了 IETF 定义的所有现代技术，你只能在根区看到极少的流量。它们会缓存好的结果，也会缓存 [不满意的] 结果。所以我们无法看到这些。所以很多根区的流量对应的是异常行为。

如果我们想要查看用户实际在做什么，就会希望接近客户端。正因如此，我们一直在研究递归解析器，对其进行探测，并尝试了解当中发生了什么。客户端发出的查询中有多少会出现已注册的 TLD，而不是我们在根区看到的所有这些字符串？有多少会出现这些 IETF 保留名称？有多少会出现我们在那里看到的常用字符串，以及其他内容？

大家应该记得刚刚我们在展示根流量时提到，我们发现这些结果为“TLD 不存在”的查询代表了近三分之二的流量。在我们的一项探测中 — 我必须对我们的数据进行限定，确保我们今天只有一个衡量点。我们渐渐在获取更多衡量点。在这一个衡量点中，这些不存在的 TLD 请求只占流量的 1%，非常低。

趋势也不一样。在保留名称中，我们看到了少量 `.localhost` 和 `.local` 流量，而其他名称几乎没有。

在经常使用的字符串中，我们发现了有点让人意外的情况。它实际上由本地名称支配，比如人们试图解析主机名，但他们执行查询的方式不正确，最终在发送 [查询] 时将主机名写成了一个 [标记] 名称，而该名称可能会被误认为是顶级域。我们不会公布这些名称的值，因为存在隐私问题。它们通常是探测器 [提供] 者的本地架构中的名称，所以我们将其全部放在了“本地主机名”的总类别中。

如果超出了这个范围，我们就会看到根区这类名称的流量很小。我们看到了一些使用频率高的名称（例如 `.home`）的流量，但我们也看到了 `.dns`、`.internal` 或 `.unifi` 这类名称的流量，在此情况下它们代表其使用的 Wi-Fi 网络。所以这是我们获得的教训之一。在这一点上，我们希望能够在拥有更多探测结果之后再作出决定性声明，但我们发现客户端流量与根流量之间存在差异。

你想说几句吗？

阿兰·杜朗德:

我想对克里斯蒂安刚刚说的内容稍作补充。到目前为止，我们一直在与一些小型机构合作，而且已经有两个机构同意参与并已经开始提供数据。在此我想指出这两个机构。

一个是位于加纳的海岸角大学，另一个是阿根廷的拉普拉塔大学。此外，我们现在还与第三个机构开展合作，即印度尼西亚 [或多或少] 服务提供商 **Nawala**。我们昨晚很晚还在努力帮助他们安装工具以完成所有这些衡量工作。

我们正在联系其他潜在合作伙伴，我们的目标是让更多机构参与其中。如果我们能够在今年年底前获得 5、6 或多达 10 个合作伙伴的话，将会相当满意。我们希望有不同类型的参与者，包括一些学术型的、一些更偏向工业性的、一些服务提供商、一些小型或大型或者非常庞大的机构。

但是我们是从核心 [听不清] 的方式开始。我们从小范围着手。这使我们能够理解事情的发展情况以调整我们拥有的工具。现在我们正在开发一个加强其自动化的流程。我们可以联系更大型的机构，甚至希望在某些时候能联系更大型的机构。

所以我想感谢克里斯蒂安 [编写] 工具并帮助大家进行部署。

克里斯蒂安·胡伊特马:

谢谢。其实，阿兰也花了很多时间来部署它们。这个全球基础设施的重点在于要由你在半夜花费大量时间打电话或者电脑聊天。但是，我认为这是我们所研究内容的一部分。

所以 M3 和 M4 对流量的两个部分进行了分析。我们在根区和客户端发现了哪种类型的 DNS 流量？通过 M4 数据，我们还希望看到我们为 IETF 所研究的所有这些 IANA 注册管理机构有多好、多有用。我们无法追踪所有 IANA 注册管理机构，因为我们只有 DNS [相关] 数据。但是我们所做的目的是获得 DNS [相关] 表格，查看注册管理机构所含的一部分参数，例如 [r] 类型或 [r 代码] 分类。此外还有 DNSSEC 或 DANE 使用的参数。

对于这些参数，我们想得到两个问题的答案。其一是，人们是否真的使用了已注册的数据？基本上我们做了什么，我们会说，“如果一个表格定义了十个值，那么这些值当中有多少个可以在数据集中至少看到一次？”对于某些表格来说，答案是零。有几个这样的表格是这样。

对于像 DNS 类或算法编号这样的经典表格，答案则在 20% 到 70% 之间。有些值很少使用。例如，在安全算法中，某些安全算法已经过时，人们不会再使用它们。但我们仍然可以看到。这让我们觉得 IANA 所做的事情是有用的，给我们带来了信心。

我们希望了解的另一个问题是，人们是否绕过 IANA 注册，直接自行设定值。在这一集合中，我们只看到了 DNS 选项代码（即 EDNS0 DNS 选项代码）的情况，尽管我们在自然环境下看到了某些实验值的使用。这就是目前的总体情况。

现在我想在此对 TLSA 证书使用情况和生成的 DANE 证书进行说明。我的数据中没有关于它们的信息。所以我和维克多·杜霍夫内 (Victor Dukhovny) 就此谈了很久。他说这很正常，因为 DANE 大部分用于邮件服务器和权威服务器之间。邮件服务器将直接查询权威服务器。所以我们的探测点无法捕获到流量。我正在与他合作直接提取他自己的 DANE 衡量标准中的流量，这样我们就可以真正适当地评估 DANE 表的使用情况。

这基本上就是我们可以使用这些衡量标准来跟踪 IANA 的方式。我们跟踪的不只是一张表。我在上一张幻灯片中展示了四个或五个表格的数据。这里是我们一起完成的整个列表，在弄清楚如何解析数据并进行提取时，我们最终可能还会添加更多表格。

最后一个衡量标准 M7 与 DNSSEC 部署有关。我们对 DNSSEC 部署的评估始于解析根区以了解有多少 TLD 正在提供 DNS 密钥。该数值相当稳定，保持在 90% 左右。我们希望它会随着时间的推移产生变化并达到 100%，但它的变化非常缓慢。

现在，通过分析 M4 数据，我们意识到当时看到的很大一部分流量实际上是 DNS 安全流量。我们会看到是因为当客户端使用 DNS 安全时我们就能够发现，他们会在查询中加入 DO 位，其在响应中 [听不清]。因此，我们可以衡量一小部分包含此位的查询，并且说：“嘿，如果我们能找到执行这个操作的客户端，我们就知道有如此多的客户端在使用 DNSSEC。”

因此，我们可以在 M7.2 中将想要执行的操作添加到此数据中，即：使用 DNSSEC 的客户端执行的 DNSSEC 查询的百分比。如果我们真的有雄心壮志，那么我们肯定也会查看使用 DNSSEC 的递归解析器执行的查询百分比，以及提供 DNSSEC 响应的权威服务器的响应百分比。我认为这样我们就将掌握 DNSSEC 的实际使用情况，并且能够回答这个问题：今天使用了多少 DNSSEC？我想这对社群来说会很有意思。

那么我已经展示了七项衡量标准中的六项。杰夫·休斯顿将在我之后展示衡量标准 5。正如我所说的，M7 非常稳定，所以现在这张图表无法给我们提供很多信息。

谢谢大家。如果大家有任何疑问，请提出，我现在将为你解答。

鲁本斯·库尔

(RUBENS KUHL):

鲁本斯·库尔，.br。我只是想说明一下，递归服务器、递归 DNS、递归衡量标准共基于三个递归服务器。目前我们在互联网上有 50,000 个 [听不清] 系统，所以也许我们不应该在获得至少 5,000 个 DNS 递归服务器之后才发布这些结果，因为其不具有任何统计相关性。这就像是在显微镜上放置一个 [听不清] 然后在此基础上推导出世界上所有的纺织品一样。

[所以我觉得可笑的是] ICANN 会发布这样一个衡量标准，特别是在一个 ICANN 没有获得与权威根数据不同的直接数据的领域，而且是在运行其中一个最全面的根服务器系统的情况下，因为它是 [听不清] 实例。所以根在根查询中具有非常好的统计显著性。但对于递归查询，在其跨过一个非常好的、具有统计相关性的阈值之前，我们根本就不应该发布。

克里斯蒂安·胡伊特马： 这是一个非常好的观点。我们在这次演示中一直在使用各种警告来解释我们现在只有一个衡量点，并说明我们想要做的 [听不清]。显然，我们想实现的不仅仅是衡量点。我不知道我们需要获得 5,000 个。如果能获得 5,000 个，我会非常乐意，但我不知道我们需要有 5,000 个。

我的计划是比较多个网站在登录时的数据，了解它们的不同点和共同点。会产生这种想法是因为我们知道存在差异。它们的时间上有差异，比如早上和晚上有所不同。周末和工作日也不同。我们知道在地理上有差异。中国和美国的人们所要求的流量有所不同。我们知道在职业类型上存在差异。在学术和政府部门、企业、专用网络或移动网络中，人们不会执行同一个查询。很清楚的一点是，我们希望能够代表所有这些标准。

我们将解决统计显著性方面的问题。我们肯定想要完成这个目标，但是必须有一个着手点，因此我们正在有效地收集数据。我们将对比数据来源，这样就可以真正回答你的问题。

鲁本斯·库尔：

没错，不过我想对此作出回应。虽然有这些警告的描述，但使用的字体都太小了。所以，所有阅读了报告内容的人都会重复并在新闻媒体和社交媒体上公布这些信息，而不会说明“此数据实际上没有意义”这一警告。所以实际上公布这些内容会对社群造成伤害。这是我对此的看法。

我对另一个问题的说明是，有人提到，有些注册服务机构的查询受到了 WHOIS 及其他限制条件的影响。这里有我从所有 [详尽] 注册，即 BRDA、批量简略注册数据中收集到的数据。该简略注册数据已经包含哪个注册商与该域相关联。所以不需要进行 WHOIS 查询。ICANN 内部已经有数据提供了这些信息，且精确度为 100%，所以你们也可以查一下。

克里斯蒂安·胡伊特马：

这是一个有趣的意见。事实上，这个意见很好。在解答这个问题时，我首先想说的是，ITHI 项目是 DAAR 项目的客户。我们会从 DAAR 获取数据，所以无论 DAAR 做出什么决定，我们都要继承。所以首先我想建议你将问题重定向到运行 DAAR 的人。

第二点是 [我会稍微] 尝试引导他们。我的理解是，他们希望该研究能够被复制，这意味着外部人员（非 ICANN 人员）实际上可以复制完全相同的研究、开放的方法和可访问的数据。你提到的数据可能可以或不可以从外部访问，这将使 ICANN 处于独特的位置，成为唯一能够完成此项研究的机构。他们的

选择是不往这个方向发展。他们可能会在某个时候改变方法，也许约翰·克莱恩 (John Crain) 可以对此进行说明，但到目前为止，这是我们已经采取和前进的方向。作为他们的客户，我们继承了这一决定。

所以问题是，为什么我们非得依赖 WHOIS 来对注册服务机构进行归因，而不是使用 ICANN 内部的数据？

约翰·克莱恩：

如果我们内部有可用的所有这些数据，那就太棒了。但我没有在内部找到。不过，我们努力在做的其中一件事是让其他人可以复制，这就意味着使用外部来源。我们唯一需要从 WHOIS 中获得的就注册服务机构 ID。实际上，我们早就讨论了内部可能存在来源的情况，因此我们可能需要转换思路，因为我认为 WHOIS 可能不太现实。

鲁本斯·库尔：

该来源叫做 BRDA，所以你可能需要进行调查或者破解这些服务器，然后从中获取数据。但即便是使用这些数据，它们也还是可以再现，只会让其他人在实际使用 WHOIS 查询时变得更加复杂。但是他们可以使用 WHOIS 查询再现，因为信息是相同的。所以这无论如何都不能保证是机密信息。

约翰·克莱恩： 好的，明白了。在开始这个项目时，我们的一切操作都应
与外部人员的操作完全一致。关于再现性的问题，你说对了，所以我们将重新考虑。

鲁本斯·库尔： 好的。

阿兰·杜朗德： 好的。凯西，聊天室有问题吗？

凯西·彼得森： 没有。

阿兰·杜朗德： 没有吗？好的。那么谢谢你，克里斯蒂安。

克里斯蒂安·胡伊特马： 谢谢。

阿兰·杜朗德： 非常感谢你在这里第一次展示这些数据。现在让我们有请杰夫·休斯顿。杰夫在吗？

凯西·彼得森： 这里有一个问题。

阿兰·杜朗德： 哦，我们有一个问题。

塞巴斯蒂安·巴肖莱

(SEBASTIEN BACHOLLET): 杰夫现在不在会议室，那么我想问一个问题，这个问题来自一个没有任何技术背景的人。你现在进行的工作和一些与密钥轮转及他们为了解正在发生的事情所需的数据相关的问题有关联吗？真的很抱歉，这是来自 [听不清] 的 [听不清] 问题。谢谢。

克里斯蒂安·胡伊特马： 截止到今天，答案是没有。它们之间没有关联。这不是我们最初考虑的衡量标准。现在和未来可能会有更多的轮转，而且可能会比较频繁，这可能会成为我们想要跟踪的问题。所以今天我们谈的是七个衡量标准。我们认为我们足够理解它们，能够进行衡量。我们现在正在考虑第二阶段，其中将添加更多衡量标准，届时我们会研究其他类型的问题。这个问题可能是我们需要关注并添加到工作内容的领域之一。[用法语回复]

塞巴斯蒂安·巴肖莱： 我明白你的意思。我只是想确保将我的问题解释清楚，抱歉。看来我们今天缺少数据来确定现在是否是进行密钥轮转的恰当时间。并不是说，只有每年能够收集数据的时候才能来确定何时进行密钥轮转，事实上，只要你的项目数据中包含可供有需

要的人用来确定何时进行密钥轮转的数据，就可以确定密钥轮转的时间。

克里斯蒂安·胡伊特马： 截止到今天，我们没有可以帮助他们的数据。

塞巴斯蒂安·巴肖莱： 谢谢。

帕特·凯恩 (PAT KANE)： 大家好。我是帕特·凯恩，来自 VeriSign。我还有一个针对塞巴斯蒂安所提问题的后续问题。今天早些时候，ICANN CTO 称 DNSSEC 查询的减少与去年秋季至明年 10 月的 KSK 轮转有关。所以我认为很重要的一点是，我们要从 DNSSEC 的使用情况中了解轮转与它之间有怎样的关联来指导决策，因为就拥有解析器但不具备密钥对的人而言，他们获得的很多数据比去年底获得的数据质量更差。因此，尽早将这些信息提供给戴维比较好。谢谢。

阿兰·杜朗德： 谢谢。这是一个很好的问题。正如我们所看到的，克里斯蒂安正在研究新的衡量标准 M7.2，它将实际跟踪设置了 DO 位的查询数量。这可能有助于在此方向上开发我们尝试在该特定领域

设计的其他衡量标准。所以，如果你对我们应该跟踪的内容有具体的想法，也许我们可以进行线下对话。

杰夫回来了吗？好的，很抱歉。我们的一位发言人掉线了。我简单地说一下我们打算做些什么。

衡量标准 M5 最初也是研究解析器的衡量标准之一，但更多地是从客户角度来看。我们已经请杰夫研究了这个问题，他拥有一个基于著名的谷歌广告的衡量系统，我们一直将其用于其他情况。我们请他使用该系统探索可以从客户端、根解析器的角度做些什么。

我们希望了解的其中一个问题是：解析器真的会缓存东西吗？有时我们认为它们会。有时我们认为它们可能不会，或者可能会缓存更短的时间或者更长的时间。所以我们认为可以对此进行一定的衡量。

我们也可以研究一些 DNSSEC 和 IPv6 的分布情况，了解解析器是否配置了 DNSSEC 或者是否能够使用 IPv6。我们也可能会找到最常用的解析器。最常用的解析器应能一目了然，因为该系统依赖于谷歌广告，因此使用解析器的是实际用户而非机器。所以它不会捕获机器到机器的通信，而是用户到机器的通信。

捕获到的内容可能是一些衡量 [听不清] 项目，可以让我们了解解密匙轮转以及实际需要多少解析器来覆盖 95% 或任何我们想要实现的百分比的人群。

这项工作还在进行当中。[那些] 是杰夫想提议的新衡量标准。秉承克里斯蒂安之前描述的精神，我们希望实现其自动化，如此就可以收集衡量标准并随时进行跟踪。

简而言之，这就是我们想和杰夫一起完成的项目。

很遗憾他不在线，但肯定是因为出现了一些外部情况。

如果没有其他问题，那么我们将提前结束本次会议。哦，问题来了。

鲁本斯·库尔：

其实，我的问题更多的是对帕特·凯恩所作评论的回应。为什么报告 DNSSEC 解析器的人数增加了 [听不清] 2010 KSK 的报告人数？我们还不知道这些人是否正在验证解析器。所以报告人可能是一个只有根密钥但未进行验证的人。所以在进行钥匙轮转时这可能并不是问题。因此，如果我们在衡量标准中做这样的研究，就可能应该考虑使用旧密钥验证解析器，而不仅仅是报告旧密钥的解析器。因为这并不能衡量所有东西，无法预测在进行根密钥轮转时会发生什么。

阿兰·杜朗德：

说得非常好，但我想补充一下。我们应该通过解析器背后的用户数量进行衡量。如果这只是有人在地下室使用的东西，还只打开五分钟，那么它可能没有为数百万用户提供服务的解析器来得重要。

鲁本斯·库尔： 同意。

阿兰·杜朗德： 如果没有其他问题，那么我们将关闭本届会议。ICANN 的下一场会议为政策会议，所以不会召开任何技术会议，我们暂时不会再见。但我们将在巴塞罗那见。

[文稿完毕]