圣胡安 — 联合会议：ICANN 董事会和技术专家小组
大西洋标准时间 (AST) 2018 年 3 月 14 日星期三 — 17:00 至 18:30
ICANN61 | 波多黎各圣胡安

凯西 • 彼得森
(CATHY PETERSEN)： 大家好。请技术专家小组 (TEG)、董事会和董事会技术委员会 (BTC) 的各位成员到主桌前就坐，谢谢。

拉姆 • 莫罕
(RAM MOHAN)： 我是拉姆，我想请董事会成员也到主桌前就坐，本次会议是 TEG 和董事会联合会议。

阿迪尔 • 阿科普罗根
(ADIEL AKPLOGAN)： 欢迎大家，欢迎 TEG 成员和董事会成员出席本次会议，由于戴维 (David) 现在没有时间，我将主持本次会议。今天的会议议程上有三个主要话题，分别是：域名系统 (DNS) 隐私，也就是 DNS 隐私工作的现状；还有 DNS 捕获分析，对 DNS 数据进行的监测有哪些，分析类型有哪些，这个主题将由迈特 (Matt) 和莫里西奥 (Mauricio) 从 ICANN 组织的角度来介绍；最后是杰伊 • 戴利 (Jay Daley) 就域名和网站分类做正式介绍。

现在我们没有[听不清]，但是如果你们还有其他任何话题，请把它们写下来，我们可以接受并适时讨论它们。

TEG 和董事会在两场 ICANN 会议上碰头，去年我们在政策论坛期间召开了一次会议，所以大约是一年两次，讨论 TEG 和董事会双方共同关心的一些话题。

在正式开始之前，我要感谢所有演讲人，因为他们自愿在很短的时间内筹备并递交了这些演示资料，所以非常感谢你们的努力。那么 -- 什么事，卡韦赫？

卡韦赫 • 兰杰巴尔 (KAVEH RANJBAR)： 我建议加一个“其他事务”，简短地讨论一下未来的 TEG 会议和董事会技术委员会的工作，谢谢。

阿迪尔 • 阿科普罗根： 好的，谢谢。那么加一项，TEG 和董事会技术社群；有关未来如何组织这方面的工作，人们一直都在讨论。 话不多说，首先我们就有请蒂姆 • 维森斯基 (Tim Wicinski) 就 DNS 隐私进行报告。蒂姆？

蒂姆 • 维森斯基： 好的，谢谢阿迪尔。我是蒂姆 • 维森斯基，你们当中有的人认识我，我是 ITF 的 DNS 隐私工作组联合主席，也是负责 DNS 运营的联合主席之一，同时也被指定为他们的一名技术联络人。首先对整个问题做一个概览，为什么 DNS 隐私很重要，我们的技术标准现状，实施状态，因为那一直是关键所在。另

外对我而言运营部署是一个大问题。我的正式工作是 Sales Force 的一名基础架构师，我们是一家非常庞大的企业，用 DNS 来做许多非常疯狂的事情，所以在运营方面，我非常关心运营部署之类的事情。另外还有未来的方向；我们认为 ITF 未来会怎么处理这方面，我们认为整个世界未来在这方面会何去何从。

众所周知，DNS 已经有 30 年的历史，有大量信息被泄露，比如，每次查找所得的完全合格域名都会发送到根域名服务器。当然，有的请求过分暴露，就像有的人放上自己的名字，我们公司给我的笔记本电脑安了个名字交给我，对此我别无选择，当然它就会泄露到互联网上。其次还有像 EDNS 客户端子网这样的东西，所有内容分发网络 (CDN) 和人们都用它来对我们进行更好的地理定位。那样会泄露数据，存在隐私担忧，所以在隐私方面，人们对此非常担忧。

从 ITF 角度，讲一点历史；2013 年 7 月被称为“斯诺登之夏”，当时 ITF 公布了 7258，我们在其中论述到，无处不在的监控是对互联网用户和组织的攻击。但是在这个雷达之下不久，到了 2016 年，欧盟通过了通用数据保护条例 (GDPR)，并在今年五月施行，所以遵守这些规范成为重中之重。

在我工作的地方，有许多人在为此做着大量工作，因为我们确实会在笔记本电脑里存储公司客户信息，这样一来我们就要尽力擦除从日志到数据库的一切信息，所以这不是件小事。

现在，有趣的是，我想 GDPR 编制人员还没有真正搞懂 DNS，所以我想他们还没有接触我们；他们还在担心网站一类的事情。这很可能是好的一面。

技术方面，在技术标准上，DNS 安全上，1999 年 3 月公布了域名系统安全扩展 (DNSSEC) 文件，它其实是要对 DNS 区进行签名并验证签名区，但是它始终缺乏一个必要条件，始终缺乏一个促使我们做这件事的“杀手锏”。

我认为有一件大事就是 ITF 目前正在进行的 DNS 的名称实体验证工作，基本上我们会将证书密钥嵌入到签名区中，以便用浏览器和服务器认证证书进行证实，但是现在 DNSSEC 并没有大量推出。ICANN 是推动它的一个主力军，在通用顶级域 (gTLD) 方面。美国政府提出了这一要求，德国和荷兰也是；而且正是因为美国政府的要求，我的雇主也提出了进行 DNSSEC 这个巨大需求。

我们即将面临这些紧要的并且正在升级的大问题，我的一位同事出席了上一次 DNS 会议或者几天前的一次会议，并且说到，不是每个人都会进行 DNSSEC，有很多云提供商就不在乎，而 DNS 供应商虽然对它表示支持，但他们告诉我们的是“我们支持客户想要的，但我们的客户并没有真正要求它。”在基础架构群体之外，唯一真正想要在企业范围内推行的就是 Cloudflare，我们很可能会是第二个，但实际上我们非常提心吊胆。

DNSSEC 验证基本上就是你如何对查找进行验证，这一切都在你的 DNS 解析器上进行，其用户人群的比例非常低。谷歌的“8 代 DNS”(DNS on the 8’s) — 我是这么称呼它的 — 这么做了，还有 quad-9 成员，也就是“现在的 9 代 DNS”(now DNS on the 9’s) 也这么做了，它们都会进行 DNSSEC 验证，它们也很可能是极少数大规模这么做的。

大约一个月前，我们大家都认识并喜爱的亚太互联网络信息中心 (APNIC) 的杰夫 • 休斯顿 (Jeff Houston) 写了一篇关于 DNSSEC 峰值的精彩博文，他看了它们的数据后感觉到验证数字在开始下降，他想知道我们是否达到了 DNSSEC 峰值，而且事情开始出现转机。

老实说，如果你们看到 ICANN 的企业选区，他们在完全回避这个问题。因为在每家公司的防火墙背后，都有太多的“脏衣服”。深陷其中难免会令人尴尬，我们也不能免罪。但是你可以到任何一家公司的防火墙背后去看看，他们都在使用自己创建的根区，所以他们完全不担心信息泄露。如果我们创建这个不在根顶级域 (TLD) 的根区，那就意味着任何泄露都会发生，因为他们假设了它会发生。人们不可能真正追根究底找到我们，所以这并不罕见，我在很多大公司都听说过，这一点有些可怕。

在域签名方面，它其实只限于我所认为的互联网基础架构公司，TLD 的基础架构，ICANN 的方法是在根区驱动它。一些

更大的供应商，比如谷歌，但是甚至连谷歌都不会对自身的域签名，这一点非常有趣，好像在挥手示意；他们会验证，但他们不对自己的域签名，挥挥手就算了。

基本上这就是目前的情况，我们已经在朝另一个方向走。抱歉，我用错了按钮。

在隐私领域进行的其他工作，当然，就是非标准，DNSCurve、DNSCrypt、DNC、.onion 等等。任何在 ICANN 世界的人肯定都记得 .onion，它被定义为一个只能在 IDF 内使用的名称，因为他们想要获得一个 L 证书，而那是可以做到的唯一方式。老实说可能还有其他一些种子文件 (torrent) 类型的东西想要做相同的事情，目前在 ITF 我们基本上忽略这些。

在标准方面，我们做了一些事情。查询名称最小化；停止发送全名到根域名服务器，实际上在 GDPR 的语境下这对我们有益，所以在这里我们有点儿超前。随着它慢慢推出，我们将开始看到受支持的工具。

接下来是 TLS 上的 DNS (DNS over TLS)，使用端口 853 取代 53，它基本上是基于 TCP 的，虽然它会使用 TLS，但从验证的角度来看，我们能否信任从这类客户那里看到的 TL 证书？[听不清]工作组基本上就是聚焦这个问题。

在[听不清]中，我们的焦点始终放在循序渐进的解决方案上，而不能好高骛远。DNS 已经很深地嵌入到我们的基础架构中，

完全从头开始建立某个事物这种想法注定会失败。我们聚焦到解析器这一站，这是技术性最强的；那是你的浏览器或笔记本电脑和你的内部递归服务器在对话，而这个对话会揭露最多信息。对我们来说，更难的问题是递归服务器和权威服务器的对话。

现在，TLD 的当然是一套权威服务器，大多数公司的域名服务器是另一套。我们感觉到这里涉及一个非技术性解决方案，类似于第 9 层类型的事物。我们认为如果不开展其他工作，要完成所有这些绝非易事。而且我们也试着跟踪实施和使用，因为有一件很重要的事情就是，我们要看到事情在部署，我们要看到人们在使用它，我们要看到它是不是真的有用。

所以，这里有几个不同的 TLS 上的 DNS 客户端，实际上有一些值得信赖的 TLS 上的 DNS 递归服务器，人们喜欢无拘无束，喜欢别人为他们切实做一些工作，实际上在移动空间已经做了一些有趣的工作。安卓的技术人员实际上在系统中有这个代码，它已经提交但没有推出，基本上支持了这个 TLS 上的 DNS。我在 iPhone 端也看到了这方面的例子，但不是来自苹果公司。

此外还有其他几个不同的客户端和转发器，在服务器方面一个很大的就是 Stubby，它是 GetDNS 的一个变形，此外还有 Knot 和 Unbound，所以这方面做了很出色的工作。我讲到了移动方面，它已经提交但没有发布，我看到了它的一些演示以

及图表，如果你们感到好奇的话，DNSprivacy.org 实际上提供了一些清楚的细节。

对我而言很重要的一件事就是运营部署；我要看到东西，我们要看到有一些东西被部署，我要看到人们在使用它，我相信这是件大事。ITF 标准没有人使用，这一点是 ITF 中的大多数人所深恶痛绝的，因为我们要推出真正能得到部署和使用的标准，如果不是这样，那么对我来说一切都是 0。关键在于用户意识，提高用户意识是一个难题，因为这里的问题有点儿复杂。但是我觉得移动端将会推动这方面，就像移动端目前正在推动互联网上的一切进展一样。所有流量都在移动端，一切都在走向移动端。

我们确实看到了，至少我看到了这种共享互联网服务器基础架构给企业选区带来的实实在在的好处，他们可能还没有看到。有很多公司在 AWS 中，在 Google Cloud 中，在 Rackspace 中，在 OVH 中，它们都在这类空间中，共享相同的服务器、解析器。它们看到了共享的网络基础架构，肯定还没有开始思考拥有像这样的架构。但是安全人员开始思考了，所以那将成为一个让技术人员拥有这个更大工具地方。我看到在部署 TLS 上的 DNS 的人就是 Quad-9 技术人员，他们实际上在大规模部署。这让我感到担忧，因为如果它不能真正发挥作用，那么我们就必须对此做些什么。

未来的方向；GDPR 实施在即，当然牵涉到很多领域，客户端子网、DNS 日志，还有正在进行的具体透明度流程。这些领域存在一点泄露问题。还有一项工作也在 ITF 进行，那就是 HTTP 上的 DNS (DNS over HTTP) 流程，也就是设法通过 443 端口来处理 DNS。实际上我觉得它很可能会比 TLS 上的 DNS 更加成功，因为人人都会在 Web 上做一些事情，对吧？每个人都会，而且在 Asia-PAC 已经有人那么做了，因为它会绕过所有防火墙；每个人都要通过 443 端口对话，每个人都要安全地对话，这就是我们将如何解决这个问题的方法。

所以我觉得在隐私方面，那将会成为这么一个地方，或者未来还有什么会带来更大影响呢？它将会是 Web 门户上的 DNS，Web 套接字上的 DNS。我提到了 HTTPS 上的 DNS，解析中间设备，解析 China，实际上我看到了活动代码，并且和技术人员讨论了很久。当然，还有人在看 QUIC 上的 DNS (DNS over QUIC)，也就是谷歌的 Web 部署，基本上是 Web 流量。

此外，我们正开始研究 TLS 上的 DNS 的解析器到权威部分，但是我想大多数人都害怕我们会接触 ICANN 并谈到根服务器，那是一个问题，但是还有很多其他权威服务器。我们怎么谈 .com？我们怎么去谈任何 TLD，对吧？

我相信他们想要看到，任何 TLD 运营商我想都会回头找我们说，“我要看到部署，运营数字，我要看到这个东西的表现如何。”我们不能把它打开，如果它会毁掉我们既有的东西，所

以这就是为什么我觉得拥有良好的运营数字实际上将有助于部署 TLS 上的 DNS。但是，如果是你们赌马的话，我觉得你们会选择 HTTPS 上的 DNS。我确实认为隐私问题目前还没有得到充分理解，那么我们能不能在减少的操作系统中进行更好的集成呢？

手机和笔记本能不能默认支持 TLS 上的 DNS？我们能不能建立真正有用的东西，我想我们大家都心知肚明了；这个东西已经打开并且在工作；它是现成的，但我们没有考虑它。我从公司的 IT 人员那里得到了笔记本电脑软件，他们部署了很多东西，我只要运行就可以了，对吧？我不必思考它 -- 所以，我想有很多人都获得了这些。我认为那会是这类事情的驱动因素。但是，在那之前，它肯定是零散的，或者进展会很缓慢。

而且你们在其中的范围有限。我想你们可以在 TLD 和 gTLD 方面提供帮助，但是很难；你们需要更大的“胡萝卜”，对吧？在这个世界上你们不能强迫人们去做事情。我们要如何找出最好的办法，来说服人们这是他们应该去做的正确的事情？我想有一个办法是展示大规模部署，并努力避开这些陷阱。但是，我看到 IPv6 部署；我是说，我们公司，我为一家大型企业工作，我们仍然没有部署 IPv6。因为对我们来说，到市场上购买大量的 IPv4 地址段更加便宜，因为我们有一本厚厚的支票簿，对吧？

人们不喜欢听到这些，而且我们还在和 AWS 之类的对手竞价。IPv6 很可能还要 20 或 30 年才能完成这个过程，所以事情的进展十分缓慢。我对此很沮丧，因为我认为我们应该加快速度，但是要有一些助推的因素，我想移动客户端将会推动整个这方面的发展。如果我们能够让巨大的移动平台部署默认立即可用的 TLS 上的 DNS，那就获得了一个巨大的用户基础，它的规模确实十分庞大。所以这就是我们面临的现状，希望我谈到了所有要点。如果大家有任何问题，如果我漏掉了什么…

阿迪尔 • 阿科普罗根： 蒂姆，非常感谢。很有意思。哦，实际上我想 —

蒂姆 • 维森斯基： 有问题吗？好的。

阿迪尔 • 阿科普罗根： 你好，谢林。请讲。

谢林 • 查拉比 (CHERINE CHALABY)： 非常感谢。你可以倒退几张幻灯片吗？继续…继续，对，就是这张。在最下面，你说“根服务器仅仅是解决方案的一部分。”你能否对此说得再详细一点呢？

蒂姆 • 维森斯基： 当然可以。谈到解析器和权威服务器的对话，当然链条的顶端是根服务器，对吧？但是它们和 TLD 对话，TLD 和二级服务器对话，所以我们可以研究解析器到权威段，我们可以和运行权威服务器的各方进行互动。

我觉得基本上我们要在链条上自下而上努力，首先从域名服务器的运行者开始，然后和 TLD 方面对话。因为我想随着你们收集到越来越多运营数据，证明它可以大规模运行，而不会破坏你们的基础架构之后，会让 TLD 人员更加放心，让他们知道“我可以部署这个东西，它不会崩溃。”

之后，我想根运营商，我和他们很多人都谈过，但是我认为他们都在同一条船上；他们想要看到“如果我们把它打开，它会怎么工作？对我们的基础架构会有怎样的影响？我们如何支持它，支持这一类事物？”

所以我感觉到，基本上我们就是要自下而上努力，从域名所有人开始到 TLD，再到根服务器的人员。你们可以给出很好的指导，就像 gTLD 流程和材料那样，但是你们可能没法让所有人来做特定的事情，对吧？我知道在 gTLD 方面，你们可以接触他们说，“哦，我们可以进行 DNSSEC”。也许对于下一轮，我们可以推出某种 TLS 上的 DNS，或者这种性质的东西，但那不会影响所有 ccTLD，不会影响一些既有的东西。所以我认为，你们要做的就是证明它不会破坏他们的基础架构。

谢林 • 查拉比： 追加一个小问题，你所说的“我们”是指谁。

蒂姆 • 维森斯基： 我们是指 ITF。在我们构建这些工具的时候，像我一样的人会去和人们交谈，并且说“这是一个很好的可以运行的东西”。然后我去和迈特 • 拉森 (Matt Larson) 说“迈特，我想 ICANN 需要在这方面做一些事情”。他可能会很理智地说，“我们要确保不会造成任何破坏”，这很可能是他要说的第一件事。

当我和人们交谈之后，而且我们还和一些 DNS 供应商交谈过，这些人是第三方，他们有的员工就坐在这里的圆桌旁，他们很理智地说到“我们愿意这么做，我们不反对，但我们要确保部署像这样的东西不会破坏我们自身的、为现有客户提供的基础架构。”这是一个非常有用的问题。而且对，我想根服务器一直是一个很好的榜样，但它不意味着人们总是会听，对吧？

阿迪尔 • 阿科普罗根： 谢谢，还有其他问题吗？虽然本次会议是董事会和 TEG 的联合会议，但是如果你们有问题，可以随时到 ICANN 来提问，因为它是开放的。有问题吗？

丹尼尔 • 达戴勒
(DANIEL DARDAILLER)： 丹尼尔 • 达戴勒，来自 W3C。你提到了 HTTPS 上的 DNS，这让我想起了史蒂夫 • 克罗克 (Steve Crocker) 早前在担任董事期间提出的一个意见，那就是实际上在更新客户端上无数的 DNS 软件时会有一个问题，出于各种各样的原因，HTTP 上的 DNS 有一个特性就是，当它集成到网页之后会自动更新；无论何时只要你重新加载网页，都会获得一个新代码来处理 DNS 事务。所以这个问题有没有人在研究，开放 HTTP 端口通过防火墙还有一个特性就是 Web 代码容易更新。

蒂姆 • 维森斯基： 我知道他们在研究这个问题；针对大多数 HTTP 上的 DNS，我们能不能研究出一个协议。我想我们要着手去做；至于我们要走向何方，这是一个问题。关键在于，他们不是想要超前，面面俱到，而是要拿出这个协议，解决这个问题。所以它相当于一个标准，定义它，公布它，让人们开始使用它。之后我想你们就会看到在应用端开始出现像这样的事物。

阿迪尔 • 阿科普罗根： 非常感谢，最后我想说一点。你把它和 IPv6 的缓慢吸收做了比较，事实上市场允许人们去获得 IPv4，但问题可能是，因为这涉及到隐私和人们对互联网的使用，以及对他们的部分隐私的保护，也许那可以是一个不同于 IPv6 的驱动因素，更多地是在基础架构层面。

琼尼 • 索尼能
(JONNE SOININEN)：

我是琼尼 • 索尼能，ITF 的 ICANN 董事会联络人。这些年我一直对 IPv6 空间有所关注。你说的没错，这里有一些可能的驱动因素是 IPv6 所不具备的。它没有隐私 — 好吧，你可以说它对隐私有一定支持，比 IPv4 做得更好，但它仍然不是杀手锏，仍然不是针对它的杀手应用。

从这个意义上说它有更多可能性，但是我可以看到它们都有同样的内在问题，就是不同软件的长尾效应，不同竞争者的长尾效应，所以需要有某种对策，我称之为行业或市场协调。在笔记本电脑或手机、主机端以及解析器端有不同的供应商，往上到根服务器也是一样，这种情况下必须进行协调才能确保它真正落实。

但是，在 IPv6 中，我要纠正一下，我认为实际上它的吸收情况一直很好，只是非常非常地不均衡。在有的地方，可能状况极佳。而在另一些地方可能完全没有。这就使得对整个空间进行协调或某种调整的原因更加清晰，它在一定程度上使得进展越发困难，实际上驱动着最终用户服务的提供者，IPv6 是最小公分母。我不知道 — 在这里你可以比在 IPv4 中更多地并行使用传统地址和新地址，所以它不一定有 V6 所具有的所有问题。

阿迪尔 • 阿科普罗根： 好的。非常感谢，这是一个需要关注的方面。下面我们进入议程上的第二个话题 — DNS 捕获和分析。这个报告将分为两部分。第一部分由莫里西奥 (Mauricio) 带来，他将给我们稍微谈谈 DNS Stats；这是一个由 ICANN 使用并维护的工具。第一部分将由迈特 • 拉森带来，他也将谈到在 ICANN 组织和工程团队中进行的一些实际衡量和分析工作。

莫里西奥 • 维尔加拉 (MAURICIO VERGARA)： 非常感谢，我是莫里西奥 • 维尔加拉。我在 ICANN DNS 工程团队工作，负责 ICANN 管理根服务器上的所有运营，以及 ICANN 域名组合。我将给大家介绍一点历史，回顾一下过去 4、5 年我们做了哪些工作，以及是什么促使我们创建了这个一整套的名叫 DNS Stats 的软件。

你们很多人可能都知道，在 DNS 领域有大量运营商目前在使用一个名叫 DSC 的软件，这个软件用于呈现在 DNS 上所反映出的他们服务器上的流量。目前，在我们使用 DSC 时，我们注意到在信息的呈现方式上存在一些问题，所以我们决定要创建一种新的方式来呈现这一信息。在 Sinodun 的帮助下，我们创建了一个名叫“刺猬”(hedgehog) 的工具。和 DSC 不同，它已经使用了一个后端数据库，并且在处理一些问题，比如当你拥有 100 多台服务器时会发生什么，要描绘它是有点难度的。

目前我们的一个主要担忧就是，我们不想使用一种没有其他人使用的服务，所以我们决定继续保持开源路由，让其他人也都可以使用它。

眼下这个软件仍在使用，并且运行到了 2.4 版本。你们可以在 stats.dns.icann.org 网站上实时查看 DNS 工程部目前正在提供的所有服务。在这里你们可以看到，这是一个小的截屏，显示了 Hedgehog 演示工具现在正在做些什么。它看起来可能就像在任意一天到达 ICANN 所管理的根服务器的流量，按五个不同的地区划分。我们使用它很正常，我们观察到的流量看起来就像心电图。

在我们使用它时注意到的第二个问题就是，我们需要改变我们收集 DNS 服务器内部文件的方式。正因如此，在服务器本身之上创建了这个第二部分，也就是要创建一个收集器来取代目前正在使用的所有 DSC 收集器。起初，我们注意到 DSC 收集器不具备一些我们认为有用的信息，像是 TCP 重置，或者 ICMP 消息。

据我所知 DSC 的维护者目前正在研究实现这些功能，但是在 4、5 年前，当我们决定采用的时候，对我们而言它还是一项需求。因此，我们注意到它们需要有一种新的格式来捕获我们在那个服务器上所拥有的全部信息。

于是我们就开始开发一种新的格式，称为压缩 DNS，或者简称为 C-DNS。这是一个高效的文件格式，帮助我们传输并且看到

DNS 流量上有些什么。在这个格式上所有特定代理都以草案的形式向 ITF 提交了意见，这份草案得到了非常积极的反馈，目前已经发展到了第 06 版本。我们希望在不久的将来把它推进到后续的阶段。

这个工具也是开源工具，并且是在 Mozilla 公共许可证这个开源许可证之下。DNS Stats Compactor 基本上是由两个程序组成，一个叫 Key Compactor，和目前在一些联网应用程序上使用的 tcpdump 非常相似。这个压缩工具的主要功能就是读取来自一个或多个接口的流量，或者甚至是另一个更大的文件，另一个创建的 TCP 文件，并生成我们一直以来开发的 C-DNS 格式。

所有没有包含到 C-DNS 格式中的信息，我们仍然可以以 PCAP 的形式存储，以便未来可以进行分析。另一方面这个压缩工具还有一个名叫 Inspector 的工具，可以用来反其道而行之，不是从 PCAP 到 C-DNS，而是我们可以在 C-DNS 上重建生成的流量，然后生成一个 PCAP 文件，这种语言就是如今大多数研究或分析人员正在做的。

在过去的几周，这个压缩工具出了一个新版本，添加了伪匿名化和 Inspector 的输出。这有助于我们为所有在 DNS 运营的电子邮件清单上讨论的、即将到来的变化以及一些关于数据匿名化的 RSAC 做好准备。我们在努力推动这个 CDS 的新版本，使它得到更广泛的部署以及其他研究工具的采用。提醒一下，压

缩 DNS 目前使用常规 PCAP 文件的大约 30%，当你把它重新传输到研究工具侧时从带宽方面来说可能会非常非常有利。

未来这个演示工具有望会推出新版本，也就是第 3 版，代码名称将是 Wombat，并且我们将用一个 ClickHouse 和 ZooKeeper 群集取代 PostgreSQL 作为后端。我们不会像从前那样绘制特定图表，而会开始使用 Grafana 来绘制数据，而且你们还将能够创建自己的图表，或者甚至可以按请求导出 PCAP 文件。

在演示工具方面，目前一切都在开发当中。稍后我会给你们展示它的一个截屏。而在压缩工具方面，我们在努力获取更详细的捕获数据，以便能够帮助所有研究工具进行更好的时间分析。我们已经在和 DNS 组织的人对话，以便可以开始经常性地开展这项工作，使 C-DNS 格式成为使用的唯一格式。如果他们需要的话，他们可以创建新的后端工具来直接从 C-DNS 操作，或者可以把它转换为 PCAP 文件，并且使用到目前为止所使用的工具。

此外，正如我以前告诉你们的，我们和多个团体合作开发了匿名化计划，并且已在大约一周前发布，因此我们很高兴看到它将在不久的将来开始工作。

最后，我想向你们介绍新的演示工具未来看起来是什么样子以及我们想要如何朝着这一方向发展。这是我们现在正在使用的其中一个内部测试部署。我们使用这个新格式的其中一个主要原因就是，它能够传播大量信息而尽可能不丢失信息。我们已

经用它来制定所有 OCTO 研究工具的框架，这样它们就可以进行分析，比如 KSK 轮转以及诸如此类的事情。

所以我们邀请大家开始使用这些工具，如果你们有任何问题，我很乐意现在或者在本周内做出解答。

阿迪尔 • 阿科普罗根： 谢谢莫里西奥，但是接下来我们先请迈特发言，之后再回答问题。迈特？

迈特 • 拉森： 谢谢。杰伊提出了“DNS 捕获和分析”这个主题，所以这是有关这个主题的另一个演示。它很简短，我只想高度概括一下首席技术官办公室研究团队在这方面所做的工作。

我们能够访问几种不同类型的 DNS 相关数据。目前我们有来自根服务器 B、D、F 和 L 的流量。B、D 和 F 是以 PCAT 格式，尽管我们在 2018 年已经逐步淘汰了对这个数据的访问，并且将专门关注根数据，这个数据就像莫里西奥说的是 CDS 格式。

实际上多亏了团队中的罗伊 • 亚伦兹 (Roy Aarons)，我们才能够非常聪明地把根服务器数据后处理为一个纯文本格式。而且如果你们想要放弃部分细节，你们可以最终得到一个文件或一个充满文件的目录，里面有查询当中的部分参数的名称，还有

文件本身当中的其他参数。你们可以使用自己熟悉并喜爱的 UNIX 文本处理工具，比如 GREP、SED、AWK 和 Friends 来方便快捷地进行大量分析。所以，SQL 是为失败者准备的。

rzkeychange 插件我提到过，如果你们在这里听了我做的有关 KSK 轮转的演示就知道，那是一个针对 DNS CAP 的插件，目前能够让我们获取来自 12 个根服务器的统计数据。这些是高层次的统计数据，统计已处理的数据包和查询数目，以及 RFC8145 信任锚报告。我们还有一个解析器测试实验室，它和 DNS 捕获的关系就在于，它让我们在一个受控的环境下捕获 DNS 流量。我们已经使用它来研究根 KSK 轮转的不同方面，比如看看解析器在 DNSSEC 和根密钥方面的行为如何，我们可以捕获这一流量。下一项和 DNS 捕获数据不直接相关，但是我们确实有根和 TLD 的历史区域文件，它们唾手可得，到处都是。

这里是一个非常简短的、高度概括的 DNS 数据使用项目的列表；罗伊进行了一个公司/家庭/邮件分析，并且将统计数据和几年前的跨通道 (inter-aisle) 报告做了比较。如果你们在这里也就是波多黎各待了一段时间，不管多长，可能就不可避免地听过我介绍 KSK 轮转，以及 RFC8145 数据在其中扮演的角色。

你们或许也听到了阿兰 • 杜朗德 (Alain Durand) 和克里斯蒂安 • 胡伊特马 (Christian Huitema) 介绍 ITHI 也就是标识符技术

健康指标项目，以及他们正在开发的衡量标准，其中有一些标准是基于 DNS 流量。还有他们实际上正在使用一个 DNS CAP 插件来进行某些衡量。过去，大概是一年前，我们和 APNIC 联合进行了一个解析器行为研究，将我们看到的根服务器数据和他们基于谷歌的广告衡量数据进行了合并。我们拥有 WHOIS 跟踪的 DNS 部署统计数据、运营参数的不同使用数据，然后就像我刚才说的，我们也在我们的测试实验室环境中研究了验证解析器的行为。我就介绍到这里，我只想简单概括一下我们在做什么。

阿迪尔 • 阿科普罗根： 太棒了！谢谢迈特，也再次谢谢莫里西奥。对于今天在使用的 DNS 衡量统计工具，大家有什么问题吗？真的没有问题了？哦，这里有一个。

马丁 • 萨顿 (MARTIN SUTTON)： 我们知道有很多人也想知道我们如何更好地保障互联网安全，使它变得更加可靠，他们能不能找到某种途径来获得这些统计数据？首席技术官办公室的人是否也是局外人？ICANN 能不能用它来改进数据？要怎么做？我知道这不是一个单纯的技术问题，但是我希望你来回答一下。

迈特 • 拉森： 抱歉，请再解释一下，我想我可能没有理解你的问题。

马丁 • 萨顿： 基本上，你们第一时间了解到许多变化，你们衡量这些变化，你们可以生成海量的数据，这些数据可以用于分析并从中发现漏洞和问题，对此你们还可以采取行动。所以我可以看到，有些局外人可能也对这些能够派上用场的数据感兴趣，还是说它仅供你们自己使用？

迈特 • 拉森： 哦，不是，它肯定不是仅供我们自己使用。虽然我承认在宣传和公布这些数据上我们可以做得更好，虽然在另一方面，有一些事情，就像我说的，你可能没能听到我对这个根 KSK 轮转数据的介绍。所以不是这样，我们的目的肯定是要将我们的研究结果提供给社群，尽一切可能带来帮助。

马丁 • 萨顿： 但是目前还没有这么做？

迈特 • 拉森： 我想这要具体来看 — 在有些信息上是这样，毕竟我们还有一些尚未公布的、正在进行的工作。但是我们当然也公布了一些信息，而且就像我说的，我们对 RFC 8145 数据做了大量研究。关于这个数据，我在这里已经详细介绍过。

莫里西奥 • 维尔加拉： 我想澄清一个问题，我们说的是原始数据还是已经完成的研究和分析成果？

马丁 • 萨顿： 我的深层意图是，我想要了解我们在这里所生成的数据的价值。而且我说了，我不擅长技术，但是我可以看到，我们有海量的数据，如果这些数据能够得到最充分利用那就太好了。

沃伦 • 库马里 (WARREN KUMARI)： 沃伦 • 库马里，谷歌。没错，迈特小组公布的 RFC8145 数据确实非常有用；有很多人都参考了这些数据，它们在其他地方其实是找不到的。所以我想，这个数据尤其揭示了很多人们意料之外的事情，并且为许多其他决策提供了非常宝贵的意见。我专指这个数据而非其他数据，因为对其他数据我没有那么了解。

阿迪尔 • 阿科普罗根： 好的，让我们继续进入下一个报告，杰伊。

杰伊 • 戴利： 谢谢。我是杰伊 • 戴利，我要谈的是域名分类。这几乎不涉及技术，让你们高兴一下。

那么简单介绍一下分类。首先是标准的行业分类，这里有几个类别，大部分都是经国际协调的，比如欧洲的《欧盟经济活动统计分类》(NACE) 或者国际性的《国际标准产业分类》(ISIC)，但美国标准落后了一代，而且和它们截然不同。

然后你们可以按网站内容对域名进行分类，我说明一下，它有两种方法。一种是人工，人们访问一个网站并对它进行分类。一个受过训练的人，甚至是一个只有几天经验的牧师，一天都可以分类 500 到 1000 个域名。另一种方法是机器学习。在这里你们有一个网络爬虫来从网站捕捉信息，并使用一个训练有素的神经网络来对它进行分类。其输出是基于网站的对域名的单一主要行业分类。有时人们也会有多个次级分类，特别是如果你使用一个神经网络，它会给你一些可能性的意见。

我所说的“分类”是指从 ISIC 提取的分类。ISIC A 级是农、林、渔业，在 01 之下你们可以看到是作物和牲畜养殖、狩猎和相关服务活动。我打赌以前在 ICANN 没有人说过这些。接下来，进一步划分是非多年生作物的种植，再细分下来是谷类（水稻除外）、豆类和油籽类作物的种植。所以这就是行业分类的方式，有一定的深度在里面。

现在，对你们的域名进行分类的好处就是，第一，国家统计机构会使用分类来确定国内各个产业的规模，他们想要衡量特定类别下公司和组织的数量、从业者数量以及营业额，或者全行业的总营业额。

所以，现在你可以开始确定某个国家内域名行业的经济价值。你可以按公司和营业额来看市场渗透率，以及域名所服务行业的价值。之后，在注册服务机构级别也有好处，你可以帮助注册服务机构了解它们是不是专注于特定行业中的特定垂直细分领域，由此注册服务机构可以确定销售和广告投入的方向。

所以，分类是过去几年才出现的新兴事物，最多三年前，现在被一些更先进的公司和注册管理机构采用。

我所知道的就有三个世界领导者，可能还有更多。.nz 正结合人工和机器学习方式，设法对它们注册下的每个域名进行分类。CENTR 拥有一个由欧盟最大注册管理机构和注册服务机构组成的工作组，创建了一个新的具体域名分类标准，这是一项意义重大的工作。另外还有一家经常来参加 ICANN 会议的商业服务公司 Dataprovider，对域名和许多其他数据点进行分类。

下面我会分别介绍它们的一些数据。.nz 在其注册管理机构中拥有 700,000 个域名，他们有一个庞大的群集系统名叫 Hadoop。在这个系统中，他们自定义分布式网络爬虫，让它出去获取页面，涵盖所有 700,000 个域名。他们请来了一组学生对 100,000 多个域名进行分类，之后又使用经测试的多个机器学习模型对剩下的进行分类。

他们所获得的准确度因 ANZSIC 代码而异。因为可适合各个代码的域名数量不等，所以可能没有足够的数据来正确界定

它。.nz 正推出一个商业产品，其中会将分类和流量衡量数据相结合。这样注册人就可以将他们的流量与同行业中的其他网站进行比较，从中了解与同行业的其他注册人相比，他们在比方说市场营销或网站改进上的投资是否带来了相对的流量增加，这一点其他人是没办法告诉你的。

接下来是 CENTR。这里在前排坐着的有安德里亚斯 (Andreas)，他是其中的一位成员，这是脑力劳动的产物。他们有一个注册管理机构/注册服务机构数据组，里面汇集了欧洲最大的 ccTLD 和注册服务机构，他们正雄心勃勃地研究制定一些框架、分类和工具。其目的是帮助整个行业更好地了解域名市场，它得到了 CENTR 的支持。

其中最重要的输出之一就是域名行业分类法。这是一个对行业和子行业的分类，匹配欧洲的 NACE 代码。现在，他们之所以要重做这项工作是因为出现了许多新的业务类型，特别是在互联网上，例如各种各样的拍卖网站，在标准行业代码中未必正确纳入了它们。而且他们有一个专门的网站，同样可以对相对市场渗透率进行国内和跨国的比较，这一点对 CENTR 成员非常有用。

最后一个要介绍的是 Dataprovider。现在 Dataprovider 是一家商业服务公司，他们进行大规模的全球数据调用。他们试图获取每个网站的 30-50 个页面，比大多数方法要深得多，并收集

150 个数据属性。其中包括行业分类，并且还会建立一个信任分数。

他们也试图了解语言，所以你们是用另一组标识符来了解国家，比如 ccTLD 或者语言等等。有趣之处就在于，他们对网站国家的识别是以内容为基础，这是一种完全不同的形式，而且比通过 WHOIS 来识别更加准确，因为 WHOIS 包含的基于注册人的数据很容易发生变化。

你们可以看到，他们的客户类型既有行业内的也有行业外的。到目前为止的公司用例包括：了解特定类型的公司，了解一个网站的数字足迹，还有各式各样的市场情报。

我要讲的就是这些。有问题吗？

阿迪尔 • 阿科普罗根： 杰伊，非常感谢。大家对杰伊有问题吗？

丹尼尔 • 达戴勒： 丹尼尔 • 达戴勒，W3C。关于存在的类别，已经有适用的标准。我想知道的就是，它是不是更加精细，比如精细到可以区分 ICANN、IETF 和 W3C，而不是都归入到技术组织这一个类别，你懂我的意思吗？比如，技术社群业务类型的定性分级。

杰伊 • 戴利： 就我们行业而言，没有，我们不需要这样的精度。在更成熟的行业中，达到了这么深的精度。但是有一个问题就是，要做到完全充分的分类是非常困难的。而且有的时候人们会退一步，只分类到比如第 2 或第 3 级，而不用到第 4级。不过，有部分这种类型的子分类，像第四级分类，已经纳入到这些标准下一版本的制定工作当中，所以日后我们可以获得更高的精度。

阿迪尔 • 阿科普罗根： 还有其他问题吗？没有了。好的，那么我们讨论“其他事务”。针对其他事项我们收到了一些请求，目前有三个。一个来自卡韦赫，要求讨论 BTC 公开会议和 TEG 的关联；一个是来自拉姆的反馈问题；我也为本次会议增加了一个未来的话题。在电子邮件清单上有一些关于 5G 讨论，我们也要看看怎么样制定讨论框架。那么我们从卡韦赫开始，请你为我们介绍。

卡韦赫 • 兰杰巴尔： 首先我要提供一点背景信息。TEG 好像非常不正式，经过了一段时间之后我们基本上发展为每年召开两次会议，通常是在政策会议上，也就是在年中举行的那场会议。ICANN 会议，没有 TEG 会议，它是第一次会议，最后一次是年度大会。下一次 TEG 会议已经确定将在巴塞罗那举行。

此外在阿布扎比，董事会成立了一个新委员会，称为董事会技术委员会 (BTC)。董事会技术委员会有三个独立的职责，如果你们看了章程就知道，概括来说，一是调查[听不清]和 ICANN 中的内部 IT 实践，也就是 IT 项目，这基本上属于受托职责。第二部分是调查技术请求或者与选区的技术互动。我想大都是与 RSSAC 和 SSAC 的互动，但是如果董事会和其他选区之间展开了其他技术讨论，BTC 将会成为引导这些讨论的渠道。

最后是与首席技术官办公室合作，展望未来或 DNS 领域中的相关发展和研究，这实际上和 TECH 的工作非常接近。在成立 BTC 时，我们也试着尽可能保持它的开放性。我提到的第一项，受托部分，因为它大致上是 ICANN 项目和 IT 相关事务的报告，有时是与组织有关的安全问题。目前，我们决定保持封闭可能更容易一些，但是我们每次都会评估会议，只要有可能就会开放。

第二部分，我们讨论的计划是也把它的第二部分开放，基本上也就是与选区的技术互动，大部分信息已经开放了。我们也希望开放审议。

第三部分，展望 DNS 的未来和研究，基本上就是不断演变的技术，这部分从一开始就一直是开放的，每一次会议都是公开的，总共只有三场会议。当我们提出议程时，那是在阿布扎比之前的一场会议，我们只做了一次试运行，我们召开了一次会议，是在洛杉矶工作坊期间在洛杉矶召开的一场会议。

在提出议程的时候，我们实际上发现在我们收到的议程项目和 TEG 讨论的内容之间有很多重叠。所以我们的想法，或者如果我没弄错的话，在本周早些时候提交的对周六的 PTC 公开会议的建议是，可以合并这两场会议并延长一点时间，但我们只能将 PTC 会议的公开部分和 TEG 会议合并。所以基本上，我们将召开一次更大规模的会议，参会者为董事会技术委员会成员，加上 ICANN 中对技术问题感兴趣的任何其他团体。

这只是 PTC 的一个建议，召开这个会议获得了支持。如果真的这么做的话，那么我们就需要研究会议的机制，比如如何收集议程项目以及安排其余的事项。但是首先，大家是否同意，有没有人反对我们探讨这么做的可能性，怎么样组织它？之后我们需要研究如何推进的相关程序。请问大家有没有异议或意见？

发言人（姓名不详）： 没有异议，我认为这是一个不错的主意。我认为董事会可以先确定他们的预期，他们希望演示的技术性有多强，以及他们想要从中获得什么。之后社群就可以在此层面上反馈相应的意见。

卡韦赫 • 兰杰巴尔： 我知道了，谢谢你。对此还有其他意见吗？好的，阿迪尔，请讲。

阿迪尔 • 阿科普罗根： 我也想补充一点，我们讨论了如果真的这么做，那么公开部分可以移到会议周举行，这样人人都可以参加。

卡韦赫 • 兰杰巴尔： 哦，当然。我想会这么做，因为阿迪尔说得对；通常我们会在会议召开之前的工作坊部分召开 BTC 会议，或者在实际 ICANN 会议之前，我们肯定会把它推移到会议周期间，比如，在这些大型会议期间召开。所以，我们将会那样做。好的，既然没人有异议的话，接下来我要 —

阿迪尔 • 阿科普罗根： 这里有一个问题。

发言人（姓名不详）： 我有一个小问题。你说 BTC 在每次 ICANN 面对面会议上碰头，但是 TEG 不是，TEG 只有一场会议。所以无论如何，你们会和我们召开一次会议，也就是说，如果我们共享议程，这个新的小组就有更多行动事项，同时我们还会取消掉一次会议。

卡韦赫 • 兰杰巴尔： 不是，基本上，我应该再解释一下。正如我所提到的，BTC 有三个主要目的，我们计划基本上在年内的首场 ICANN 会议期间讨论所有这三个部分，最后一个部分是和 TEG 一起的。第

二场会议我们将只讨论前两个，目前已经关闭了。我们有意要开放它们。一旦实现开放，我们就将讨论它，以及如何让他们参与进来。而 TEG 会议，也就是年内的最后一场会议，我们将再次讨论这三个部分，最后一个部分将和 TEG 一起讨论。所以我不认为这会引起任何问题。

所以，在此基础上，我将会和首席技术官办公室合作，并与 TEG 沟通，我们将接收电子邮件，我们将设法在这里提出一个流程，从务实的角度来说我会设法在 BTC 内进行。我们将分发一个关于如何推进的提案，基本上是关于程序、如何收集议程等等所有这些事项。我们还将设法在 TEG 内达成基本共识。如果大家都同意，那么我们就将开始这么操作，在巴塞罗那会议之前我们有足够的时间。谢谢大家。

阿迪尔 • 阿科普罗根： 谢谢卡韦赫。其他事务的第二项，拉姆，有请。

拉姆 • 莫罕： 谢谢，我是拉姆 • 莫罕。趁着董事会成员都出席了本次会议，我想花一点时间现场邀请董事会成员提供对这类会议价值所在的反馈，他们希望 TEG 增加什么、改进什么，做出什么改变。

我想它不仅仅是一个提供反馈的机会，也是在这里互动交流的机会，我们有时间，所以这是我想要建议的。包括没有坐到桌

前的董事会成员在内，如果你们不介意的话，我现在就想开始轮流来问你们。首先从贝基开始，你有什么反馈意见？

贝基 • 伯尔 (BECKY BURR)： 我没有。我一直在认真听。但有点尴尬的是，我得承认这里有很多关于隐私的内容，有关 DNS 隐私标准的重要讨论有点超出了我的理解范围。我对它感兴趣，我不惧怕技术，但我不是工程师，所以这是我的一个观察。我希望对它有更多了解。

拉姆 • 莫罕： 我看到有两个人要发表意见，一个在那里，还有一个在这里。

蒂姆 • 维森斯基： 蒂姆 • 维森斯基。作为新人，我其实是第一次参加 TEG 会议，并承担这个任务。我对数据的呈现方式、话题和内容的介绍都十分谨慎。所以我尽量避免讲得太深，但是我也意识到，因为是技术受众，所以有时我会偏向技术方面。我很乐意坐下来和你交流 — 没能充分了解与会人员也是我的失误，所以这也是一次学习经验。谢谢。

沃伦 • 库马里： 沃伦 • 库马里，谷歌。大约 4 到 5 场 TEG 会议之前，我可以回头查找一下实际链接，我想我对 DNS 隐私做了一个更通俗易

懂的入门介绍。我相信它们都有记录，所以我可以看看能不能为她找到这个材料和更通俗易懂的介绍。

拉姆 • 莫罕： 谢谢，还有其他意见吗，贝基？

贝基 • 伯尔： 没有了。我认为这些会议非常有趣，我能学到一些东西。我并不是建议你们把它简化，因为我有印象它的目的实际上是技术性的，但我每次总能收获一些有价值的东西。

拉姆 • 莫罕： 谢谢，马修。

马修 • 希尔斯 (MATTHEW SHEARS)： 这是我第一次参加 TEG 会议，非常感谢你们做的这些演示。贝基说的基本上就是我要说的，但我只想补充一点。我认为对我而言缺少一个对意义的解释，也就是它们对 ICANN 的运营有何影响。虽然也许并没有具体的关联，但是有没有办法为我们这些来到这里的听众提炼一下，把这些信息整合起来，那样会非常有帮助，谢谢。

拉姆 • 莫罕： 谢林，你是要回应吗？如果不是的话，稍后会轮到你。我会问到每一个人。但是现在有没有 TEG 成员要回应马修的意见，他要求解释意义，不要仅仅谈论技术，还要稍微谈谈它的意义。杰伊？

杰伊 • 戴利： 对，我想我们从来都没有一套演讲者指引来确定他们要达到的目的。

拉姆 • 莫罕： 好的，看来这是一件有用的事情，值得去做。琼尼？

琼尼 • 索尼能： 好的，作为回应，我认为首先杰伊是对的，我们实际上从来没有想过这方面，从来没有想过应该对“我们要做什么”给出一些指引，而且我认为这是一个很好的起点。但是我们也许应该更进一步，从中提供一些切实的指引，那就是“实际上我们期望从中获得什么”。

拉姆 • 莫罕： 谢谢琼尼。下面转到另一边，也就是你这里，谢林，你有什么反馈意见？

谢林 • 查拉比： 我对这些会议充满期待，因为我总是能学到一些新东西。但有一些形式上的东西我不敢苟同。请看这里，演示长达 60 分钟，对话却只有 15 分钟，对我来说少得可怜，因为既然我们在这里面对面，就应该开展对话。演示可以通过电子邮件发送，所以你们可以看幻灯片，对吧？

关于 DNS 隐私，演示 20 分钟，对话只有 5 分钟，这个时间对于任何对话来说都远远不够。DNS 捕获，演示 20 分钟，对话只有 5 分钟。还有域名也一样。所以基本上都是演示、演示、演示，非常少的互动、互动、互动。如果可以的话我希望反过来，这就是我的建议。

拉姆 • 莫罕： 谢谢。卡韦赫？你是要回应谢林的请求吗？

卡韦赫 • 兰杰巴尔： 对，我基本上同意所有意见。我认为这些意见非常中肯。我的建议是，作为 BCT 主席由我来做这个工作，我会从董事会角度制定一个提案并发送给 TEG，看看大家有没有异议或者建议，然后…

拉姆 • 莫罕： 谢谢，卡韦赫。有没有 TEG 成员要回应谢林的意见？蒂姆？

蒂姆 • 维森斯基： 我同意谢林的观点。我喜欢互动。在我介绍我的本职工作的时候，在材料的中间有很多重复。所以我也喜欢互动，完全同意你的意见。

拉姆 • 莫罕： 谢谢蒂姆。帕特里克？

帕特里克 • 弗斯特朗姆 • 莫罕 (PATRICK FALTSRAM MOHAN)： 非常感谢，我是来自 SSAC 的帕特里克 • 弗斯特朗姆。我认为谢林的提议真的非常好。应该是 5 分钟的演示，20 分钟的对话，我们应该把它反过来。其次，我也支持卡韦赫的建议，现在，考虑到结构，我认为整个 TLD 一类的事务应该由董事会技术委员会和技术联络组来推动。我们剩下的人应该把他们用作资源，可以在这个对话中提供帮助，谢谢。

拉姆 • 莫罕： 谢谢，沃伦？

沃伦 • 库马里： 沃伦。我想这是个好主意，但是我也应该提一下，在之前的 TEG 会议中，我们也会做多个演示，而且之后完全没有对话。我猜不是因为时间原因，而是因为临近会议结束时每个人都很累，和/或也许这些演示组织得不是很好。

所以未来我们会做一个十分钟的演示，之后可以把更多工作放在确保这些演示真正引起了董事会的兴趣，并且提供了有用的信息上，而不是让我们站在一个小小的临时表演台上演讲。

拉姆 • 莫罕： 谢谢沃伦。

谢林 • 查拉比： 快速回应一下，我认为演示应该 — 这是一个建议，对吧？我认为演示的形式应该是抛出一个问题，然后邀请大家来讨论，这是我的建议。

拉姆 • 莫罕： 谢谢，谢林。乔治？

乔治 • 萨多夫斯基 (GEORGE SADOWSKY)： 谢谢。对我来说这是一次充电。我认为它非常重要，但也让我学会谦卑，让我清楚地明白“不知为不知”。从这个意义上说，它非常有价值。因为在我们讨论诸如此类的问题时，我们没有获得这种专业知识的价值。至少我有时就会掉入这个陷阱，自以为理解这个问题。所以我有我的解决方案，并且这是对的解决方案。深入理解这个小组所讨论的各种各样的事情让

我更加清楚自己可以贡献什么、哪些具体问题是我解决不了的。

拉姆 • 莫罕： 谢谢乔治。有 TEG 成员要回应乔治的意见吗？好的，那么请你，马丁？

马丁 • 萨顿： 好的，谢谢。我参加过其中一些会议，必须要说，每次都能有所收获。我 100% 赞同已经提出的建议。对我来说，如果今后能解释它们的目的所在会很有帮助。我们为什么要谈论它，它说的是董事会和技术，而不是 BTC 和技术，对吧？

所以，如果你们可以考虑它对我们的战略意义是什么，我们为什么应该了解，那会促使我更好地聆听。我认为提供一点技术信息是好事，稍微深入一点也可以满足我，仅仅在董事会我是得不到这些信息的。

但是事实上，另外一个要素是，它意味着什么、组织能做什么、我们怎么样做出改变？最好是有一个问题、请求或者行动建议可以拿出来讨论。最后也是最重要的一点，我认为演示可以超过三分钟，但还是要预留至少一半的时间来进行对话。如果不这么做的话，那就让我们早点去喝东西好了。

拉姆 • 莫罕： 谢谢马丁。萨拉和杰伊？

萨拉 • 多伊奇
(SARAH DEUTSCH)： 作为新人，我建议编制演示材料时假设董事会的所有人都一无所知，因为至少有的人是这样。我们知道技术，但是只有在用平实的语言解释给我们听的情况下才能理解。所以，请把内容保持在基础层面。此外我们不仅要了解影响，可能还要进一步说明，比如你们熬夜是为了什么、这些话题最令人担忧的是什么，这样我们就知道应该关心哪些方面。

拉姆 • 莫罕： 谢谢萨拉。杰伊？还有 TEG 的其他成员想要回应吗？杰伊，请讲。

杰伊 • 戴利： 另外，我认为演示材料可以在最后加一项行动或者风险之类的内容。我认为大的技术环境、在我们行业中发生的其他事情也很重要。这就是为什么我要在这里带来网站分类的介绍，你们不需要对它做什么，但是如果你们很多人知道在发生什么的话，那么我会非常惊讶。而且它是我们行业中正在发展的一个很大的领域，未来我们将会解释它的影响。

另外，在这些影响当中还有一些事情需要我们大家了解。你们是一个以行动为导向的董事会，这一点很好，但是我认为并不是我们的每一次演示都一定要得到回应。

拉姆 • 莫罕： 谢谢，蒂姆？

蒂姆 • 维森斯基： 我认为萨拉的建议 — 我认为所有董事会成员都提出了一些很棒的意见。我想如果下次我还有机会来为大家做演示的话，我可以做得更好，这就是我要说的。所以谢谢。

拉姆 • 莫罕： 谢谢蒂姆。露丝薇斯？

露丝薇斯 • 范德朗 (LOUSEWIES VAN DER LAAN)： 谢谢。我想实际上大部分问题都已经提出来了。我还在考虑的一点是，我想要知道技术团体内部的观点集中程度。我只参加过一场 ITF 会议，根据我的经验，你们会把五位工程师请到一间会议室里，他们会带来二十种不同的观点，这样我就可以放心 ITF 不会一边倒。

所以在这里我想知道，在座各位的观点是不是相当协调，我们有没有多元化的观点或者对技术情形有没有进行竞争分析，或者你们大家是不是都达成了一致意见，或者你们是不是都太过优秀，每个人都协同合作。因此我想要了解的就是，意见的构成有没有全面反映出全球的技术知识。

拉姆 • 莫罕： 我可以肯定，在这个问题上我们的观点是多元的。沃伦，还有谁？

沃伦 • 库马里： 我想对于我们讨论的这些具体问题，基本上每个人谈的具体事项都不一样，而且，我们基本上是站在一个足够高的高度上去谈，或者说还不够深入细致，所以我们的意见都非常融洽。话虽如此，我还是认为如果可以带来不同的观点会很有用。

而且，基本上我们在这里探讨的事情没有太大争议性，通常一说出来每个人都认同，然后才会拿到这里来介绍。不过如果能来一场“铁笼赛”会更好玩一些。

拉姆 • 莫罕： 关于这个话题，TEG 的其他成员要发言吗？哦，蒂姆？

蒂姆 • 维森斯基： 没错，我是尽量从运营的角度来说明要部署大规模基础架构，特别是隐私部分。但是从 ITF 的角度，我也指出了 HTTPS 上的 DNS 可能会是更大赢家，但它也不尽如人意，因为我认为其他办法在技术上更胜一筹。但是经过研究后我说“从长期来看，它实际上可能会最终胜出。”基本上我设法平衡二者，而且，我确实是从运营的角度来考虑如何部署这个服务器的，对吧？

谁会关心，我们为什么要关心，诸如此类的事情。从企业界来看，我们和在座的很多人都不一样，对吧？我们运行着庞大的基础架构，但我们本质上是一家销售公司，对吧？人们是这样想我们的。我们在雷达下飞行，我们构建了非常庞大的基础架构，解决这些非常复杂的问题。安全事务对我们来说非常重大，所以我们十分重视它。我其实在尽量平衡所有这些事情，但是对其中的一些问题解释得不够深。不过的确，我也非常喜欢那样的观点。

拉姆 • 莫罕： 谢谢，琼尼？

琼尼 • 索尼能： 对于从 ITF 挑选出来站到这里的代表，我想要说一点，之所以会选择他们就是因为他们可以平衡各种观点。我想，比如蒂姆就是这么做的，虽然这不是“铁笼战”，但是就像你说的，你尽量说明它们是对同一个问题的不同解决方案，其中有的解决方案看起来比其他解决方案具有更大的可能性。所以来到这里的人也是能够以一种非常平衡的方式表述这些观点的人。

拉姆 • 莫罕： 谢谢。琼尼，你是要补充反馈吗？

琼尼 • 索尼能： 是的。首先，这里的演示一直都有很高的质量，也非常精彩，这一点毋庸置疑。有一点显而易见，作为董事会，我们可能没有花足够的精力来给出一些切实的指引，说明我们想要看到什么。这一点我认为是本次讨论取得的一个积极成果，但是我认为它实际上不是给演讲人的反馈，他们的演示都非常精彩。

这是给董事会的反馈，实际上我们可以给出合理的预期。而且就像杰伊说的，我们从来没有制订过一个样式表或指引，来说明做到何种程度方为正确。显然我认为这是董事会可以采取行动的一个方面，他们可以回来更加主动地征求这些意见，并问问自己我们希望达到何种程度。

拉姆 • 莫罕： 有人要回应吗？好的，让我 — 哦，谢林。

谢林 • 查拉比： 等一下，如果按顺序来的话，你走了一圈选了所有董事会成员来问他们的反馈意见，你不会漏掉你自己的，对吗？

拉姆 • 莫罕： 不会，我要先确保其他人都有机会提供意见。谢林？

谢林 • 查拉比： 我希望没有人把我的意见理解成暗示这些演示的质量不好，因为它们都非常好。我要反馈的是，我们也在和其他选区的联合会议上听到人们说这些面对面会议召开的次数不多，一年可能就两到三次。

所以让我们利用它们进行真正的对话而不是演示。所以我要反馈的只是说可能要改变一下这些会议的方向，那样将有助于我们进行更多对话，这才是我想要表达的意思。因此请不要误会，我不是批评这些演示，它们的质量都无可挑剔，谢谢。

拉姆 • 莫罕： 谢谢，艾芙丽？

艾芙丽 • 多利亚 (AVRI DORIA)： 我不知道要反馈什么。我想有的内容讲得太快了，我还想了解得更多；我想要看到一些工具，看到它们如何工作，以及在哪里使用。在分类方面我有点疑惑，我想要了解这个领域的发展。对我来说其实时间还不够，因为这确实是看待事物一种新颖的视角，所以这个内容我有点跟不上。

我本来想进一步了解为什么这个比那个更成功，因为你知道，我认为这个已经很好了。在某种程度上，我想，我确实希望进一步了解正在发挥作用的东西、正在使用的东西、它们的适用

性如何，尤其是像工具。这就像，好吧，我不了解所有这些工具，所以，了解它们的作用以及如何使用会很有趣。

拉姆 • 莫罕： 谢谢艾芙丽。卡韦赫？

卡韦赫 • 兰杰巴尔： 我很喜欢它。基本上，我在这里看到了很多大的机会，还有非常好的反馈。所以我认为基于我收到的讯息，的确，这个会议应该更多地用作对话的机会，所以我已经在尝试考虑一些可能的模型。当然，我们需要更多时间，也许可以缩短演示或取消演示，以便专注于董事会的战略要点。所以在提出议程请求时，我们应该强调它们，并且需要大量的时间反复讨论，这就是我所设想的。

拉姆 • 莫罕： 谢谢卡韦赫。利托？

拉斐尔 • 利托 • 伊瓦拉 (RAFAEL LITO IBARRA) 谢谢。我同意已经提出的大部分意见。我想强调几件事情。第一，在议程上，我认为它最好是在 TEG、OCTO 和 BTC 的共同努力下筹备。并且我也同意演示应该更短，技术更少一些，还

可以再介绍一下某些技术可能会在生态系统中造成的影响或后果，这样我们就会更重视眼前的技术。

最后，我还想纳入对我们已经看到的前几个主题的跟进。比方说，我们在前几次会议上看到过区块链，也许我们可以跟踪该技术的当前状态，还有本次会议的 DNS 隐私，等等。我们可以在下一次会议时跟进。

拉姆 • 莫罕： 谢谢利托。沃伦？

沃伦 • 库马里： 我想提醒大家的一件事是，TEG 和 TLG 的目的应该是作为给董事会答疑的技术资源。我的意思是，董事会成员具有广泛的背景和自己的专业知识，我们存在的合理性在于，如果董事会成员有一系列他们想要进一步了解的问题或事情，我们就是一个资源，你们可以向我们提问。

我认为这里的每个人都对他们关心的事物充满激情，所以他们会非常乐意说到你的耳朵起茧。因此如果有任何董事会成员想要更多地了解任何事情，请随时询问 TEG、TLG，不管是谁，我们很乐意谈。

拉姆 • 莫罕：

谢谢沃伦。我想沃伦，这也是我的意见或反馈。在 TEG 与董事会最后一次会面时，在会议结束后，我和一些 TEG 成员坐了下来，我说：“我们真的需要 — 这次会议的价值是什么？”因为有一些事情大家都会洗耳恭听，还有一些事情看起来只是某些人的热情或兴趣所在，而你只是过来介绍它，对吗？关于相关性的信息并不多。

但你已经听到其他人这么说。作为出席这些会议的董事会成员，我对什么会让我真正感兴趣有一些想法。什么会让我不仅仅是安排这个会议，而且还要亲自来这里参加，并且也希望其他董事会成员来参加。实际上我很希望把会议分成四个部分。一个是解释部分，你知道，就是选取一个话题并加以解释，让董事会成员对它有一些更深层次的理解。

我还想有一个“下一代”部分，也就是你们应该知道的即将到来的事情。这部分我并不期望深入探讨技术，而就是说明这是接下来会发生的事情，它即将来临，那样会很有趣。另外我想如果有一个现场展示部分也会非常有趣。上一次做现场展示时，我们观看了某些事情的发生，这非常非常吸引我们。虽然我们知道示范通常在现实中行不通，但即使是一个视频示范实际上也很有用，对吗？

它会使一切活起来，使它成为现实。而最后一部分，我认为可以谈谈我们，作为董事会，应该担心什么？我们应该考虑哪些即将来临的风险？而且，这不一定是还没有人想到的风险，所

以它的意图不是讽刺说，你怎么这么蠢，连这个都没想到？而是确实存在于这个领域；我们认为这些事情都是即将到来的风险。

所以以上这四件事情，我认为将会带来非常有价值的互动，谢谢。

阿迪尔 • 阿科普罗根： 非常感谢拉姆。时间刚刚好，现在刚好到了本次会议的预定时间。我认为反馈环节非常非常有用，对首席技术官办公室也是如此，因为这有助于与 BTC 就未来会议进行真正的合作。我要撤回我提出来的最后一个议项，也就是讨论下次会议，并简要谈谈电子邮件中讨论的 5G。但我们会在筹备下一次董事会和 TEG 会议时对它进行整理。感谢大家的贡献和宝贵意见，感谢所有的发言人。我想本次会议到这里就结束了，谢谢大家。

[会议记录结束]