马拉喀什 – 基于 HTTPS 的 DNS (DoH) 和基于 TLS 的 DNS (DoT) 的政策方面及相关问题
2019 年 6 月 25 日（星期二）- 15:15 - 16:45（欧洲西部时间）
ICANN65 | 摩洛哥，马拉喀什

亚历贾德拉 • 雷诺索 (ALEJANDRA REYNOSO)：大家下午好。大家可以先就座吗？我们马上开始。非常感谢！

请问演示文稿已经准备就绪了吗？谢谢！在演示文稿准备就绪之前，我想先谢谢各位的参与。我们即将讨论关于基于 HTTPS 的 DNS 和基于 TLS 的 DNS 的高关注度主题。首先，我将向大家介绍会议目标，以及我们所有的专家组成员。

此次会议包括关于这个主题的技术概述，然后是提问和解答环节。在此之后，我们将介绍潜在的部署问题，紧接着，再次进入提问和解答环节，最后，我们将针对部署考虑事项进行专家组讨论，我们期待你们所有人都能参与到这个高关注度主题的讨论中来。为此，我们准备了流动麦克风。如果你们有问题，请让他们知道你们坐在哪里，你们会看到他们有一个编号。这些编号有 4、6、3，我猜 5 在后面那里。我看不到，但应该就在那里。是的，就在那里。

好的，如果你们有问题，可以举手，越高越好，这样他们就可以找到你并将麦克风交给你。如果现在演示文稿已经准备就绪，那就太棒了。

我先自我介绍一下。我叫亚历贾德拉 • 雷诺索，来自 .GT ccTLD。我是 ccNSO 的副主席。跟我坐在一起的是丹尼 • 麦克

费尔森 (Danny McPherson)。丹尼是威瑞信公司 (Verisign) 的执行副总裁兼首席安全官，同时也是 SSAC 的成员。

另外还有彼得 • 科赫 (Peter Koch)。彼得目前在德国域名注册管理机构 (DENIC) 担任政策顾问，该机构是 DE 的 ccTLD 经理人。我们还有巴里 • 雷巴 (Barry Leiba)。巴里 • 雷巴是 Futurewei 技术公司 (Futurewei Technologies) 的高级标准经理。自 20 世纪 80 年代初以来，巴里便一直致力于电子邮件和相关技术领域，目前专注于物联网、移动平台上的消息传递和协作、互联网应用程序的安全与隐私，以及互联网标准的制定和部署。巴里也是 SSAC 的成员。

我们还可以在那里看到艾莉莎 • 摩尔 (Alyssa Moore)。抱歉，我不是在指别人。艾莉莎是加拿大互联网注册管理局 (CIRA) 的高级政策和宣传顾问，该机构是 CA 的 ccTLD 经理人。

巴里和艾莉莎将担任提问和解答环节的主持人，专家组的其他成员还有帝姆 • 阿普里尔 (Tim April)，他是阿卡迈技术公司 (Akamai Technologies) 的首席安全架构师，专注于 DNS 网络安全和事件响应领域。帝姆也是 SSAC 的成员。

请向后切换几张幻灯片。我们专家组成员还有维托里奥 • 贝尔托拉 (Vittorio Bertola)。维托里奥 • 贝尔托拉是 PowerDNS 母公司 Open-Xchange 公司的政策和创新主管，在过去一年中，他参加了多次会议，并在会上讨论了加密 DNS 的政策影响。

最后，还有米凯莱 • 内伦 (Michele Neylon)。米凯莱是 ICANN 认证注册服务机构 Blacknight Solutions 的创始人兼首席执行官。米凯莱也是 GNSO 理事会的成员。

请向后切换几张幻灯片。我认为我们和往常一样，遇到了技术问题，但这个问题并不难解决。我不知道我们是否可以开始技术概述部分，也不知道其他幻灯片是否已准备就绪。为了节省时间，我们可以开始了吗？

我们将再等一分钟，看看幻灯片能不能显示出来。如果不能，那我们就不等了，但我们现在还是先等几秒钟。与此同时，大家还可以从会议日程安排网站中下载幻灯片来跟踪对话。我认为我们需要开始了。有请丹尼发言，如果你不介意没有幻灯片的话。

丹尼 • 麦克费尔森： 当然不介意。我将在没有幻灯片的情况下为大家进行介绍，可能对很多人来说，即便是有幻灯片，这也是一个非常难以理解的主题，所以这将会很有趣。

我叫丹尼 • 麦克费尔森，是 SSAC 的成员，在这里，我将展示 SSAC 幻灯片。所以，即便出错，那也是 SSAC 出错，不是我。我们将会使用这个幻灯片。

不管怎样，我们今天将讨论一个主题，我将介绍技术方面的内容，之后，彼得和专家组将讨论它的一些潜在影响。但这个一

般性主题最近引起了人们的广泛关注，它就是我们所谓的 DOH 和 DOT，也就是基于 HTTPS 的 DNS 和基于 TLS 的 DNS。

简而言之，这些技术旨在为 DNS 事务提供机密性。传统 DNS 并没有任何内置的机密性概念。实际上，它也没有任何内置的完整性概念，尽管 DNSSEC 可以为 DNS 提供完整性保护，但仍会让 DNS 暴露在一些事件之中，诸如监测、窃听以及可能出于一系列原因操纵对各种客户端的响应。它可以用于家长控制内容访问、国家审查或阻止访问恶意网站，以便保护用户。

总之，我们想要实现这种解决方案的动机有很多，当你们切换到第 6 张幻灯片时，你们就会看到其中的一些原因。因此，这里的关键在于传统 DNS 以及拥有机密性的 [概念]，而且在我们所处的地缘政治形式以及事件的各种经济后果中，提供 DNS 事务的机密性将会有众多好处，而且也会有一些衍生物。

所以，我们将讨论部署模型，但不一定会过多地讨论这些模型。如果你们在跟着听的话，就会发现第 6 张幻灯片中基本上涵盖了我刚才讲的内容。

因此，如果没有 DNS 事务的机密性，那么你们将面临信息泄露或者泄露攻击，这样其他人就可以查看你们的信息，对你们进行监控，或者了解你们在互联网上的动向并挖掘相关信息。

所以，DOH 和 DOT 的概念都是为进行的活动提供在线加密，这样的话，即便存在路径上的攻击者或观察者，他们也不会看

到这些信息。从非常浅显的层面来说，这就是 DOH 和 DOT 所涉及到的内容。

第 7 张幻灯片主要提供了传统 DNS 的概述，在这张幻灯片中，当你们考虑 DNS 时，可以设想你们有一个设备，在该设备上，你们将拥有一个应用程序，该应用程序想要解析 DNS 中的信息，然后它就会询问设备上的本地进程，举例来说，网络浏览器可能会询问你们的 iPhone 操作系统或者笔记本电脑，它会说：“嘿，我应该怎样转到 www.example.com？”

然后设备中会有一个 DNS 解析器，它将会与本地网络上的内容或者 ISP 网络上的外部内容进行通信。我们可以切换到后面两张幻灯片来看看相关图片，也就是传统 DNS 的示意图，如果你们愿意的话，可以查看幻灯片 8。

这就是我刚刚所说的内容。应用程序最终想要为用户或者设备上的进程解析某些信息，而传统上，该应用程序会与本地操作系统进行通信，再次说明，该应用程序可以是 iPhone 上的一个应用程序，也可以是笔记本电脑上的网络浏览器。

应用程序或网络浏览器将询问本地操作系统该目标名称在互联网上的位置，之后设备将会退出，而且它将与被称为本地转发器的某个程序进行通信，或者可能与递归解析器进行通信。

传统上，这些递归解析器位于 ISP 网络或网络接入服务提供商提供的本地网络中，但越来越常见的情况是，它们可能位于云基础设施中，例如 OpenDNS 或者 Google 的递归域名服务器，

这些基础设施可能会在互联网中，在云基础设施中的某个地方提供解析器。所以这是一个不断变化的架构 [参数]。在发生传统解析的网络中，它可能不是本地的。

递归域名服务器将访问权威基础设施，这可能是根基础设施、顶级域 (TLD) 基础设施或者权威基础设施，然后递归域名服务器将解析名称，紧接着将该信息传递回应用程序或者存根解析器，后者会将信息传递给应用程序，然后应用程序将能够连接到互联网上的所需目标。

正如大家从这幅图中看到的那样，如今所有的这些事务都没有机密性的概念，因此，如果在图中标有绿色箭头的任何地方都有一个路径观察者，那么他们将可能看到用户在试图解析的内容，这些内容可能是商业竞争信息，可能是与安全相关的信息，可能是敏感内容，也可能是任何的一系列广泛的事件。所以 DOH 和 DOT 所涉及到的是一些保护这些信息的方法。我们来看下一张幻灯片。

这两个解决方案中的其中一个被称为 DOT。DOT 是基于 TLS 的 DNS。TLS 就是我们所说的安全传输层协议，有趣的是，在互联网上最安全的事务中，如果你们看到了传统的挂锁或者你们访问金融网站或包含敏感信息的其他网站，TLS 可能是支持在网络和传输层提供加密的协议，它提供信息的加密或机密性，这样路径上的攻击者就无法操纵或观察这些信息。

在 DOT 模型中——让我们切换到下一张幻灯片，我将根据这张幻灯片来介绍这个模型。基本上，在 DOT 模型中，传统上发生的事情——再次说明一下，DOH 和 DOT 都可以部署，它们是两种不同的技术。在标准和运营社群中，这些技术仍在开发。但是基于 TLS 的 DNS 传统上被认为是一个本地系统，例如你们的 iPhone 或笔记本电脑，这些设备可能具有一个系统范围的设置，指示我将使用此解析器和基础设施来解析 DNS 中的信息，而且设备上的每个应用程序都可以使用该设置，并转到基础设施来执行解析。

所以，你们在这里看到的是，举例来说，网络浏览器可能会做传统上所做的相同事情。它将会询问本地存根解析器，它会说："嘿，我需要在互联网上访问 example.com。你可以解析这个域名吗？"

但是，存根解析器现在不是发送明文，而是在加密通道中以有效的方式将信息发送到云基础设施中的某个位置或 ISP 网络，以解析信息。这基本上就是你们在这里看到的红色箭头。

信息将会被加密，这样路径上的观察者或者攻击者就无法操纵信息，或者观察正在进行的活动。此外，在这里的权威基础设施中，对于 DOH 或 DOT 解决方案可能适用于根还是 TLD，也可能是二级域权威基础设施，我们今天并没有太多的考虑。不过，关于这方面的信息仍在不断充实中。

我们稍后会将这个解决方案与 DOH 进行对比，DOH 会将加密级别稍微提高一些。所以，让我们切换到下一张幻灯片，然后讨论一下 DOH。

我切换得太快了。很抱歉。DOH 基本上不使用 TLS 进行 DNS 传输，那么它实际上是怎么工作的呢，你们知道吗？我的设备上有很多网络应用程序，或者有很多网络流量，我还有在这个操作系统中或设备上围绕 HTTP 事务构建的大量软件，所以我实际上不会在基础设施中以本机方式使用 TLS，而是将在网络查询、HTTP 查询中对 DNS 响应进行编码，很有趣的是，接下来要将其放在 TLS 上，然后在网络中进行传输，TLS 是 HTTPS 的运行方式。

这为应用程序提供了许多挂钩，以便直接与解决方案基础设施进行交互并完全绕过本地存根解析器，或者使用在操作系统上运行的存根解析器。我们继续切换到下一张幻灯片，我将为大家进行介绍。

大体上来说，你们可以看到——再说一遍，它只是一个部署模型。它可能会有所不同。但可能发生的情况是，我的浏览器可能会在基础设施中使用一个采用 DOH 的递归域名服务器，而另一个应用程序可能会使用本地域名服务器，或者可能使用系统解析器。

现在，有趣的是，如果这个场景中出现了中断，而且不同的应用程序使用不同的 DNS，那么就会很难理解正在发生的情况。

另一件事情是，ISP 传统上可能使用 DNS 查询作为基础设施中的控制点，或者企业可能使用 DNS 查询作为控制点，他们可能不希望加密事务直接从应用程序跨越基础设施的某个外围或边界，因为他们可能会失去对安全性或家长控制或基础设施中的其他内容的监控。

因此，这里的关键是，不在 DOH 情况下使用存根解析器，对此，更传统的设想是，应用程序将直接查询互联网基础设施、解决方案基础设施以获取 DNS 响应并绕过操作系统和本地网络服务提供程序中的所有内容。这就是我们在这里说明的内容。

好，我们切换到下一张幻灯片。现在要指出的另一件有趣的事情是，如果从控制点、窃听或监控的角度来看待这个问题的话，你们就会发现 DOH 能够有效地将 DNS 解析流量与网络上的其他 HTTP 流量混合在一起。因此，它使得潜在的监控、窃听甚至是过滤变得更加困难，你们必须破解所有的 HTTP 流量，才能从控制点的角度对与 DOH 相关的 DNS 解析查询进行技术上的处理。

再次说明一下，DOT 是一个系统范围的设置，但你们也可能必须这样做，在这张幻灯片上，我认为我要指出的最后一件事情就是大家所看到的 DOH 和 DOT 模型，它们可能会混合在一起，这些箭头也可以翻转过来。这取决于应用程序想要启用哪种模型，系统管理员想要启用哪种模型等等。

像设备上的存根操作系统这样的系统实际上可能使用 DOH 而不是使用 DOT，这类系统也可能使用传统的 DNS。我认为这个问题仍在讨论之中。

我们今天并没有对权威基础设施进行太多的探讨，所以 [音频不清晰] net、gov、edu、jobs、其他 TLD，甚至可能是二级域名，另外还有一些其他诸如 QNAME 匿名化之类的技术可以提供一些隐私保护措施，尽管还有一些分支涉及各种不同的方面。

我认为我已经试着让大家跟上我的思路，就像米凯莱不断提醒我的那样，我可能说得有点快，但现在我会暂停一会儿，看看大家对此有没有什么问题，然后我们会进入到彼得的部署考虑事项部分。如果大家有问题，你们可以询问那些到目前为止我们所提及的专家组成员，你们也可以保留这些问题，先让彼得介绍 DOH 和 DOT 的一些其他影响，然后再提出你们的问题。

亚历贾德拉 • 雷诺索： 谢谢丹尼精彩的快速介绍。我们这里有一个问题。非常感谢！

奈杰尔 • 卡斯米尔 (NIGEL CASSIMIRE)：好的。下午好！我是奈杰尔 • 卡斯米尔，来自加勒比电信联盟。这对我来说是一个新主题，因此我一直在试着了解你们尝试使用这些技术解决的问题。你们是在尝试使 DNS 变得更安全吗？与 DNSSEC 相比，这种技术如何？

米凯莱 • 内伦： 好吧，现在大家都在争相发言。那么，我来说两句。DNSSEC 是在 ICANN 圈里经常被讨论的话题，就好像它是可以解决所有 DNS 问题的灵丹妙药一样。但其实不是。DNSSEC 是这样的一种方法：当你们访问银行网站时，无论你们访问哪个银行网站，都不会有人篡改你们的通信而在中间插入某些内容。

这种篡改通信的攻击就是你们所说的 DNS 投毒攻击，在过去某些网站一直存在这个问题。DNSSEC 解决的就是这个问题。至于 DOT 和 DOH，这两个解决方案一直都在试图提升隐私级别和安全级别，但两者都存在一些问题。在隐私方面，你们确实实现了这一点，然而我认为我们中的一些人可能会进一步讨论它对某些安全方面有何负面影响。但本质上，它所做的是转移这些 DNS 查询，即设备（也就是你们的笔记本电脑、手机、iPad 或其他设备）执行查找的方式，也就是将查询从传统的 DNS 转移到其他协议上。

那么 DOH 的情况又是怎样的呢？它被视为普通的网络请求。请注意，我不像丹尼那样对技术有着深刻的了解，所以对于我有说得不对的地方，他之后可能会进行纠正，但这是看待这个问题的一种简单方法。

亚历贾德拉 • 雷诺索： 谢谢，米凯莱。有位远程参会者想要发言。有请。

爱丽儿 • 梁 (ARIEL LIANG)：我们远程参会者有 2 个问题。第一个问题是穆罕默德 • 尤西夫 (Mohammed Yousif) 提出的。就解析查询的时间而论，基于 TLS 的 DNS 是否会导致性能下降？之后我们将朗读第二个问题。

米凯莱 • 内伦：这取决于存根解析器的实施方式。它可能会在初始连接设置时对解析器施加额外的惩罚或导致额外的往返，但如果您的存根解析器被配置为在一段时间内保持连接，那么其 [分摊] 成本可能与常规 DNS 大致相同。

爱丽儿 • 梁：下面我朗读一下远程参会者的第二个问题。这个问题是由来自贝宁的耶齐德 • 阿坎霍 (Yazid Akanho) 提出的。第 6 张幻灯片中提到，QNAME 最小化等技术也可以有效地保护用户隐私。那么所有的解析器如何实现这一点？

丹尼 • 麦克费尔森：我们不想过多地讨论 QNAME 最小化，这是一种非常轻量级的技术。传统上，DNS 是非常冗长的，如果我想在 DNS 中解析一些信息，我需要提供一个完全合格域名，例如 internalsecretserver.foo.verisign.com，我将向路径中的每个权威服务器发送完整的查询。然而事实是，根服务器只需要告诉我如何访问层次结构的下一级，也就是 .com。

当我向根服务器发送查询时，我不需要告诉服务器我需要查询的全部内容，我只需要询问如何访问 .com，然后 .com 将告诉我如何访问 verisign.com，之后 verisign.com 将告诉我如何访问 internalsecretserver。

所以，实际上你们不需要透露你们想要解析的完整域名，因此你们可以将名称最小化。这是一种保护隐私的域名解析功能，属于非常轻量级的技术，而且这种技术已经在大多数递归域名服务器实施中以不同的方式部署和实施，并且从隐私角度实现了某种可测量的攻击面最小化。

亚历贾德拉 • 雷诺索： 非常感谢！我会要求大家尽可能不要偏离主题。我知道在安全和互联网方面有很多相关的概念，但是现在，我们应该尽量将重点放在 DOT 和 DOH 上，以便专家组随后可以深入探讨。我将再请大家提两个问题。有请 4 号和 5 号麦克风的发言者依次发言，然后我们将请下一位演讲者发言。谢谢！

弗雷德 • 贝克 (FRED BAKER)：对于 TLS 和使用 DNSSEC 运行之间的差异，你们所做出的回复让我有点惊讶，因为这两者所保护的是不同的内容。DNSSEC 保障内容（即实际资源记录）的安全，而 TLS 则保障通道的安全。

你们可以将其比作管道和水。我们可以想象一下，我有一个镀金属的精美管道，它现在绝对是世界上最棒的管道，在它的上游，有一个充满毒液的湖泊。当这个镀金属的精美管道输送湖泊中的水时，它实际上仍是在输送毒液。

所以保障内容的安全才可以摆脱毒液问题。现在，我就不做不利于 TLS 的陈述了。拥有一个好的通道也是一件好事。但是，在确保域名实际载有你们想要得到的东西方面，DNSSEC 就变得非常重要。

丹尼 • 麦克费尔森： 我想回答一下这个问题。我认为这个观点不错，弗雷德。我认为，即便在生态系统中完全部署了 DOH 或 DOT，你们也仍会希望 DNSSEC 和 QNAME 匿名化能够提供更多的保护。它们解决的是不同的问题，这个观点不错。

亚历贾德拉 • 雷诺索： 谢谢！5 号麦克风的发言者要发言吗？

吉姆 • 彭德格斯特 (JIM PRENDERGAST)：是的。大家好。不可否认，我并不是 IETF 成员。我知道在座的很多人都是。丹尼，当你列举这些技术的优势时，你也谈到了一些可能会受到损害的事情。如果发生了一些意想不到的后果，这些技术将如何被批准作为标准呢？

未知身份的发言者（男）：[你应该问 IETF。]

未知身份的发言者（男）：这个问题问得很好，吉姆。

丹尼 • 麦克费尔森： 好。很抱歉。我认为这些技术已经存在，而且生态系统也会配合找出正确的部署模型。我认为生态系统中的任何人，从浏览器供应商到操作系统供应商，再到递归域名服务器运营商或权威基础设施运营商，都不希望有任何事情受到损害。

有趣的是，这确实会造成一些部署上的挑战，如果你是一个 ISP 且无法看到用户的网络浏览器 DNS 流量，而这个用户正在其他地方使用云服务来解析 DNS，然后该用户致电给你，让你解决他所遇到的 DNS 问题，在这种情况下，你可能无法解决他的问题。或者，如果你使用 DNS 实施家长控制，那么也可能无法解决这个问题。

因此，我认为生态系统必须适应这一点，这就是为什么我会认为对于 DOH 和 DOT 来说，真正重要的是要认识到部署模型将会有所不同并且将适应新的情况，因为我认为市场和动态决定了什么是最优的，什么是有效的，以及什么是不起作用的。

亚历贾德拉 • 雷诺索： 好的。非常感谢！总之，接下来将由彼得为我们介绍有关 DOH 和 DOT 的潜在部署问题。

彼得 • 科赫： 好的。谢谢亚历贾德拉。我叫彼得 • 科赫。正如先前所介绍的那样，我在 DENIC 担任高级政策顾问，而且我是该工作组中的 ccNSO 任命共谋者之一。

所以我受邀来向大家介绍潜在的部署问题。吉姆，非正式的副标题实际上是：协议是无辜的，这是常有的事。这大概可以解决一些问题。

第一部分可能带点技术性内容，我们有两个标准，这两者差不多都是解决相同的问题——噢，是的，我们需要，抱歉——

亚历贾德拉 • 雷诺索： [音频不清晰] 幻灯片，请切换一下。非常感谢！

彼得 • 科赫： 对，就是这个。好的，我将从这里开始为大家进行介绍。我们有两个标准，它们以略微不同的技术方式来解决相同的问题，即 DNS 往返流量的机密性问题。

大家只需要记住，为什么会这样，几年前有一个名叫斯诺登 (Snowden) 的人，他所发现或者至少分享的是，DNS 流量可以

作为情报的来源，可以用于识别个人，也可以用于识别人们从事的活动，例如访问网站。

但是，我们不能只关注 DNS 所用于的网站方面，还要关注其他各种服务。所以，这就是其中一个激励因素，IETF——我并不是在代表这个任务组发言，但他们已经发布了有关这方面的文件——宣称遍布各处的监控是一种威胁，这种威胁可以通过使用一些协议来缓解，而这些尝试实际上是使用普遍加密来响应普遍监控，以此方法来解决这个问题。

这关乎于动态加密 DNS 流量。另外，还有其他一些涉及技术端的方面，我们稍后会做介绍，但我只想补充一点，不仅仅是国家机构会这样做，系统中的其他人员也可能有兴趣研究 DNS 往返流量，因为尽管 DNS 信息大多是公开的，但事实是，有人在特定时间点询问的特定域名可能不是公开的，但它确实是有价值的信息。

也就是说，我们有两个相互竞争的标准，这很容易描述。这只是描述了一个部分（解析器）如何与另一个部分（在本例中，这就是所谓的 DOH 解析器）进行通信。它看起来像是一个外部的网络服务器，但它传递的是 DNS 响应，而不是传递网站。

到目前为止还没有解决的问题是，在这种情况下，用户或网络浏览器该如何获取信息，应该向谁询问？通常而言，这是操作系统在我们拥有此信息的情况下传递的信息，对于你们所使用的大多数笔记本电脑和智能手机，情况都是如此。这里将会有

一项操作，域名解析被深埋在操作系统中，而且对于你们手持或放在桌面上的整个设备而言，域名解析通常都是一致的。

这些事情可能会发生改变。IETF 或开发人员仍在研究自动配置，如何找到这个 DOH 解析器，以及一些正在进行的计划，以便为用户提供更多的选择，使他们能够手动配置 DNS 服务，但这些工作仍在进行中。

这里已经有一个网络浏览器，一家供应商为其网络浏览器启用了 DOH，即基于 HTTPS 的 DNS，它处理 DNS 域名解析的方式与网络浏览器类似，该浏览器包含一个硬编码 URL——这是一个标识符，而且网络浏览器将处理在访问网页时你希望从网页浏览器中获取的信息，并为 DOH 硬编码该信息。因此，该供应商的所有网络浏览器在该时间点都将使用特定的 DOH 解析器。再说一遍，这里不会只有一个实例，可能还会有其他更多实例。

而且，它将覆盖操作系统提供的信息。所以，应用程序现在将选择使用与操作系统其余部分不同的 DNS 解析路径。采用这种做法可能会面临一些挑战，正如幻灯片中所展示的，它可能会干扰一些网络管理者的安全策略，在这些策略中，人们通过拦截 DNS 流量来减少对某些信息（主要是网站或钓鱼网站等）的访问，然后正如有些人所指出的那样，这些安全策略将不再起作用。请切换到下一张幻灯片。

当然，还有一个有趣的问题，为什么有两个标准？我努力不深入到技术细节，但是 DOT（基于 TLS 的 DNS，TLS 是安全传输层协议）更像是工程方面的东西，也就是我们可以将网络看成是一层一层的，但 DOT 至少也存在一个问题，那就是如果需要获得特定的信息，那么就必须在防火墙上打一个洞，才能得到这些信息，而现在每个人都可以让任何人访问任意一个网络服务器。

DOH 流量看起来有些像是访问一个网站，并且不能与之分离，后面的幻灯片中将会介绍这一点。实际上是在这张幻灯片。很抱歉。

如果不同时阻止对重要网络服务器的访问，那么任何人都将无法阻止对基于 DOH 的域名解析服务的访问。可以说，这就是它背后的诀窍。

目前研究工作仍在开展中，以便将这种功能添加到基于 TLS 的 DNS，也就是 DOT 方法中。当然，在技术方面，也会涉及到一些高深细节，但它们并不是今天讨论主题的一部分。

所以，网络管理员可能无法再阻止域名解析，因为与此同时，他们可能会由此阻止对网站或流行搜索引擎的访问。这可能会——也许会，也许不会——干扰某些司法管辖区的一些监管要求，在这些司法管辖区中，ISP 根据相关指示阻止某些域名的解析。当我读到这些内容时，我并不是说这些阻止机制非常有效，但它们可能是监管要求。正如我所说的，它也并不是完美

无瑕的，你们可以通过配置自己的解析器，使用 VPN 或者在自己的系统上运行自己的解析器来轻松规避这些阻止机制。

在网络流量中 [伪装] DNS 查询可以帮助用户绕过基于 DNS 的过滤，你们也可以将其称为审查，即第三方向用户强加过滤，它也可以阻止恶意软件，这通常是用户订阅或据称为了用户的利益而制定的服务。请切换到下一张幻灯片。

所以，这是从一个较大范围来说的，因为协议是 [无辜的]，但常有奇怪的事情发生。基于 HTTPS 的 DNS 并未规定特定的部署模型。任何企业都可以运行 DOH 解析器，并将其网络浏览器指向该解析器，然后像以前一样运行。但是，在目前的讨论中，我们可以看到一个倾向于集中和整合的特定发展模式，比如网络浏览器供应商与 DNS 域名解析服务提供商合作——我将会在下一个列表项中再次提到这一内容——然后将其所有的网络浏览器用户、网络用户指向特定提供商的解析服务，这种模式可以为提供商提供更多的洞见信息，也可以为用户提供一点稳定性，但同时也促进了集中化。

在过去的 30 多年中，DNS 域名解析历来都是高度分散的。也就是说，它可以在 ISP 中，甚至在你们的笔记本电脑上，或者是 30 年前的大型主机，或者其他设备上进行。然而，DNS 域名解析作为一种服务，已经随着时间的推移而发生了演变，这就是所谓的四元组，比如 1.1.1.1、8.8.8.8。你们可能已经在某些国家和地区的防火墙中看到过这些元组，在这些国家和地区，

当人们遇到 DNS 阻止问题时，他们会通过向其中一个域名解析服务提供商求助来规避这个问题。其他人在每个位置都会使用相同的数字。这可能只是出于好奇，或者因为使用方便。

但是，除了根据应用程序（而不是系统、企业甚至 ISP，其中 ISP 向其用户提供解析选择）选择解析路径之外，这些方面肯定会导致逐渐增大的解析器的集中度提高。随着数量的增加，我的意思是，解析器背后的使用人数在不断的增长，很显然，这意味着，特定解析器运营商的权重——这也可能意味着政策权重——有望提升，并变得越来越重要。请切换到下一张幻灯片。

好的。正如我们所说的，DOH 和 DOT 均在 [网上] 提供了隐私保护，而且我们已经谈论了原因。然而，解析器——ISP 的解析器，或者这些大型解析服务提供的解析器——确实会在不同级别的细节上看到用户的请求。

出于某种原因，有时会有特定的信息添加到查询中，这样用户便可以获得量身定制的响应，因为在最后一个列表项中——我将在这里简单转发一下——某些技术方案取决于这样一个事实，即并不是每个人在提出相同的查询时都会获得相同的响应，所谓的内容分发网络通常使用 DNS 将用户引导到最近的分发系统，以降低延迟并为用户提供更快的响应。

因此，隐私问题不仅可以通过在网上进行加密来解决，还可以通过使用 DNS 解析器策略来解决，比如，解析运营商告知你

们或者承诺要对查询数据所发生的事情负责等。你们可能已经绕过了 ISP 或者国家机构的保护策略，因为他们对你们的数据感兴趣，但如果之后有解析器运营商介入，这种规避方法可能不会有太大帮助。请切换到下一张幻灯片。

这种方法便不能奏效。因此，对于 DOH 解析器的策略问题，我们要公开讨论的有趣的事情是，应该如何进行选择？我们在之前的幻灯片中已经介绍过，对于这些解析器，其技术手段是什么；作为用户，我该如何决定使用哪个解析器；如果我已经决定使用其中一个，那么我该如何将其配置到我的应用程序、系统或其他设备中；以及这些 DOH 解析器运营商如何对他们的承诺和行为负责。因为他们可能需要根据任何实体的要求披露信息，在大多数情况下这种实体可能是执法机构。

对于由谁来决定接受哪些策略，这是另一个讨论话题，有一个供应商曾表示，“我们知道社群中有人担心我们合作的供应商只有一个。我们很乐意与其他供应商合作，但我们希望他们能够遵守某些解析器策略，这意味着，他们只能根据规定对用户数据执行和不执行某些操作。”请切换到下一张幻灯片。

所以从更大范围来说，当然这是因为其中一个问题是，为什么我们要在 ICANN 背景下讨论这个主题？现在，假设有一个合作的 DOH 解析服务提供商群体。这个群体的规模很小，并且不像早期那样分散。接下来，我们进一步假设存在某个应用程序，

它是一种主要在互联网络上使用的服务，就像大家通常都使用的服务那样。

有时候还会有人对附加的域名解析路径感兴趣。IETF 和 ICANN 也曾对 .onion TLD 进行过讨论，它不是真正的 TLD，但现在已经保留。不过，它是以某种方式适合命名空间的内容所需的不同解析路径。

实际上，当我们拥有这群合作解析服务提供商（他们背后有很多人提供支持）时，他们真的能够决定是否开放命名空间的新部分吗？这看起来会是什么样子，而且当权力转移时——人们只需要用脚或网络浏览器进行投票，对于 ICANN 在 DNS 根区方面的职责，它意味着什么？请切换到下一张幻灯片，应该就是这些内容了。

好的，那么现在进行总结。可能只是初步结论。我们已经了解到，DOH 和 DOT 的一些部署可能会影响到解析服务中的传统控制点。ISP、企业可以拦截 DNS 查询并发送不同的响应。其目的是为了投放广告，以及消除恶意软件和僵尸网络。

对于 DOH 和 DOT 的标准化，应用程序中的解析器以及如何选择解析器，这些问题仍在讨论中。目前还没有最终的结论。对于注册管理机构和注册服务机构运营商来说，目前的影响似乎不大。然而，也可能有人前往注册服务机构或者注册管理机构，并问道：“我是这些解决方案提供商之一。你们为何不给我一

份 DNS 数据的副本？我很乐意更快地为你们的用户提供这些数据。”

当然，现在谈论对用户的影响还为时过早。就像我们所听到的，这与 DNSSEC 以及诸如 QNAME 最小化之类的其他隐私机制完全无关。但人们对这些机制的需求并没有改变。应该就是这些。请切换到下一张幻灯片。好的。

亚历贾德拉 • 雷诺索： 非常感谢彼得。

彼得 • 科赫： 谢谢！

亚历贾德拉 • 雷诺索： 大家还有其他问题吗？我们还可以再提几个问题。大家可以提出 5 个问题。

沃伦 • 库马里 (WARREN KUMARI)：大家好。我叫沃伦 • 库马里，在 Google 公司工作。我不是 Chrome 团队的成员，但我将传达他们的一些想法。彼得，在你的介绍中，你提供了一种浏览器的部署模型。这不是唯一的部署模型。Chrome 团队目前正在计划通过两种方式向用户提供 DOH 服务。

如果用户的系统解析器已经支持 DOH 服务，那么 Chrome 将进行简单升级以使用该服务。如果你已经在使用 ISP 的解析器，而且事实证明它们支持 DOH 服务，那么将会通过这些解析器使用 DOH。

如果用户需要，他们也可以选择不同的解析器。这与目前的情况非常相似。如果用户对其 ISP 的解析器不满意，他们可以选择不同的解析器。

不管是哪种情况，Chrome 都不会在用户没有选择加入的情况下更改用户选择的内容。而且，我们也不会要求用户真的选择像 Google Public DNS 这样的域名解析服务。

所有这一切都意味着人们针对诸如恶意软件等内容采取的现有保护措施，如果他们使用企业级 DNS，那么所有这些都将继续以相同的方式工作。

所以，我认为值得注意的是，部署解析器的方式很重要，而不是传输本身。我不知道你们对此有何想法？

彼得 • 科赫： 很好。谢谢沃伦。我在幻灯片上故意没有列举名称，希望我没有提到任何名称。感谢你们在那种特殊情况下所做的事情。是的，这是对部署模型方案的一个有价值的补充。我们并没有力求做到详尽无遗，而且我认为幻灯片上已经提及，我们已经讨论了多个模型，而你所展示的模型显然是其中的一个。

另一方面，我希望专家组稍后不要抢先讨论，也许我们可以把重点先放在提问方面，我的这种做法可能会让人有些费解。

亚历贾德拉 • 雷诺索： 谢谢彼得。首先请远程参会者提出他们的一个问题，然后我们还可以提出 4 个问题，在那之后，我们将结束此环节的发言。

爱丽儿 • 梁： 这是由迪尔克 • 尤姆佩茨 (Dirk Jumpertz) 提出的一个问题。DOH 已经被滥用为一种攻击手段，也就是通过使用精心设计的 [TXT] 记录在网页中插入恶意内容来进行攻击。你们知道这件事吗？要阻止这种攻击非常困难，因为它使用可信的通道并与 DNS 结合来攻击 [THHP]。

这难道不是让 DOH 变成了一种威胁而非一种福音吗？

彼得 • 科赫： 这个信息很有趣，迪尔克。就我个人而言，我并不知道这件事。也许专家组的其他成员知道。我想将这个问题放在专家组会议上讨论，也许我们可以先记住这个问题。

亚历贾德拉 • 雷诺索： 当然要记住。3 号麦克风那边有人发言吗？

埃杜尔多 • 迪亚兹 (EDUARDO DIAZ)：我有一个问题。一个潜在的用户问题是，如果我下载了一个应用程序，而这个应用程序通过 [加载它] 在我不知情的情况下使用其自身的解析器，这样在我不知道后台发生了什么事情的情况下，它很容易地就影响了用户。谢谢！

彼得 • 科赫：是的。谢谢你的发言。没有提及的一个方面是，在理论上——大家知道，理论可以立即变成实践——不同的应用程序可以提供不同的结果，因此域名系统看起来与网络浏览器不同，比如说电子邮件应用程序或者 VOIP 电话，因为根据你选择的解析路径，一些域名可能被阻止，另一些域名可能会通过，你甚至可能会被发送到这里的 A 点和其他位置的 B 点。这确实是一种用户体验。但这正是最终用户实际预期的开始。谢谢！

亚历贾德拉 • 雷诺索：谢谢！4 号麦克风。

[雷米 • 恩韦克 (REMMY NWEKE)]：谢谢！我叫 [雷米 • 恩韦克]。我来自尼日利亚，代表非商业用户选区 (NCUC)。我关注的是幻灯片上所提到的一点，也就是现在谈论 DOH 和 DOT 对用户的影响还为时过早，但是我们至少可以尝试研究潜在的影响，以及可能对用户造成的负面影响。

我希望你们澄清的另外一件事情是，对于 DOT 或 DOH 的这些负面影响，我们可以采取哪些防范措施，还有就是用户的责任是什么，对于用户有何成本影响，而不是现在的技术方面。谢谢！

彼得 • 科赫： 好吧。我认为这是一种建议，而不是一个直接的问题，它可以作为讨论的素材。在进入专家组讨论之前，我们还有两张幻灯片。我看大家没有其他问题了。

亚历贾德拉 • 雷诺索： 没有问题了，现在我们将开始专家组讨论。请切换到后面几张幻灯片。非常感谢！现在，专家组成员将回答你们面前的这些问题。我将阅读所有这些问题。

你们预见部署 DOH 和/或 DOT 会对你们的运营产生何种影响？

是否存在属于 ICANN 使命范围内的 DOH/DOT 问题？

你们认为应该如何在网络浏览器等应用程序中实施 DOH？

你们对 DOH 和/或 DOT 有什么顾虑？

我们将从帝姆开始。

帝姆 • 阿普里尔： 回答所有这些问题需要花费很长时间，但我脑海中印象最深的问题是，从安全背景出发，我对 DOH 和 DOT 有什么顾虑，这个问题主要是针对最终用户，还有一个问题就是他们对命名空间的看法可能会有何变化。

基本上来说，如果从浏览器或应用程序到解析器的第一英里使用的是 DOH 或 DOT，你就可以获得通道的隐私保护，但你不能保证从解析器到权威服务器的连接都有某种形式的保护。

你可能担心会通过通信通道泄露数据，这种情况可能发生在解析器之外，在一些情况下，也可能是由最终用户造成的。

另外还会有调试问题，这取决于实施情况，特别是在 DOH 中，如果应用程序在你不知情的情况下使用 DOH 解析器，你可能会认为一些解析问题是由 ISP 的解析器造成的，并且会致电 ISP 以寻求帮助，这些 ISP 可能也不知道发生了什么事情，然后这个问题将变成了一个长期的调试问题，除非最终用户具备丰富的技术知识或者知道要找什么，否则对他们来说，这将是一个晦涩难懂的问题。

我将请其他成员继续回答其他问题。

亚历贾德拉 • 雷诺索： 好的。维托里奥要发言吗？如果可能的话。

维托里奥 • 贝尔托拉： 我有几点要说。从第一个问题开始，作为其中一些最大的 ISP 的软件供应商和 DNS 服务提供商，不可否认的是，在实施新协议以及使其在现实世界、在 [每秒服务数百万个 DNS 查询的平台] 中发挥作用方面，我们确实具有一定的影响力，但这不是真正的问题。

作为软件公司和开源公司，我们更关注互联网的开放性问题，以及它可能对 DNS 解析服务市场和一般服务产生的影响。

所以我认为真正的问题不在于加密，也不在于通过加密的连接进行传输，对于保护隐私来说，这些都是有益的措施。对于 DNS，新增了一些举措，将其从网络服务（由操作系统作为网络服务的一部分提供的服务，比如 TCP IP 堆栈）更改为应用程序服务（由每个应用程序直接管理的服务）。

这将会导致很多问题。其中一部分问题与潜在的混淆有关，正如我们所说，不同的应用程序以不同的方式运行。但最令人关注的是应用市场，特别是我们在使用网络浏览器时，网络浏览器是迄今为止使用最广泛的应用程序，它比网络市场更加集中。

目前，如果你想汇总全球 95% 的 DNS 查询，则必须将前 1000 个 DNS 解析器组合在一起。在网络浏览器中，这基本上只针对公司而言。顺便说一下，所有这些解析器都在同一国家和地区的同一司法管辖区内。

因此，就潜在的策略影响而言，特别是在管辖权、主权和所有这些问题方面，情况发生了很大的变化，因为我们都知道这对

于政府的影响，我认为有几个选区也受到了影响。一个是 ISP，但我认为在这个背景下，也许更值得提及的是对政府和最终用户的影响。

对政府来说，其所受影响和问题实际上是失去了对 DNS 解析的控制，尤其是对于决定使用这些 DNS 解析来提供其他服务（例如家长控制），或者对他们的公民实施任何形式的内容控制和过滤的国家和地区而言。

最终会发生的事情是，网络浏览器可以开始使用这些全球平台，届时所有的控制权都将消失，并且会转移到其他不受国家管辖的地方。所以，这就是为什么至少英国政府一直在关注这个问题的原因，我希望未来会有更多的政府关注这个问题。

对于用户而言，这是一个潜在的选择问题，因为应用程序可能会开始决定只向他们认定的一方发送 DNS 查询，甚至限制选择，并指出“我们现在 [音频不清晰] 是决定谁可以运行解析器的人，这是我们在全球范围内认可的 10 个解析器列表，以及我们不允许使用的其他解析器列表”。

然后，他们将成为维护者，并决定 DNS 解析的策略。所以最后，这取决于策略，我想说的最后一条信息是，这实际上取决于部署模型，但是要就部署模型达成一致意见，还需要一些共享策略，无论是采用自下而上还是其他方式。对于应用程序，人们不只是要去做他们想做的事情，还要对将要发生的事情有一个共同的认知。

亚历贾德拉 • 雷诺索： 谢谢维托里奥。米凯莱要发言吗？

米凯莱 • 内伦： 谢谢！我认为我们在这里看到的问题并不简单。这些是大家都关注的问题，也是难以回答的问题。我认为有些东西是理论和学术上的，而目前，它还处于非常早期的阶段。直到最近，DOH 和 DOT 都还只是假说。现在，它们正在变成现实。

那么这种现实是什么呢？它将如何对我们产生影响？再来说说第二个问题。如果你们最终处于公共标识符不再公开的情况中，那么 ICANN 使命可能会在某些方面受到影响。现在，你们最终会遇到这样一种情况：较少数量的 DNS 解析器运营商正在决定 DNS 中信息、人们可以访问的信息以及他们可以获取的信息。所以，我认为这存在一些潜在的影响。

我自己的公司是一个托管提供商、注册服务机构，我们也运营 ISP 服务。人们可能不了解什么是域名。他们不了解域名和浏览器之间的区别，不了解搜索引擎和浏览器地址栏之间的区别。

所以，当有人说，“噢，用户可以选择更改他们使用的服务”，如果你是在对一群骨灰级技术狂说这样的话，那么这可能是真的。在座有多少人是在运行自己的域名服务器？好的。我环视了一下会议室里的同事，我知道举手的这些同事都是骨灰级技术狂。

你们中有多少人运行自己的邮件服务器？顺便说一下，举手的大部分都是同一群人。现在，请诚实地回答，你们是典型的互联网用户吗？好的。

事实就是这样。我想说，这里的选择并不完全是真的。最后，从政策和技术方面来看，它在某些方面打开了潘多拉的盒子。但我们为什么会面临现在这种状况？如果你们回顾丹尼的演示文稿，看看有关不同技术的比较，你们可能会问，为什么会发生这种情况？这种情况是从何处发生的？

事实是，在我们现在生活的世界中，隐私和安全是人们关心的问题。如果你们没有关注隐私和安全问题，那么在过去几年中，你们在关注什么呢？DNS 在许多方面都过于公开。它存在很多有趣的问题。

现在，我们有一个可以解决这些问题的潜在方法，这个方法可能会引起一系列新的问题，当然，这会让我们中的一些人将余生都奉献在解决这些问题上面。

从运营的角度来看，我不确定我到底要如何向一些客户解释某些功能不起作用的原因，因为在他们致电求助时，情况就已经变得很糟糕了，客户会告诉你们，他们在使用 Outlook 时遇到了问题，而实际上他们当时并没有使用 Outlook，他们这样说是因为，他们认为 Outlook 是唯一的电子邮件客户端，或者说 Firefox 是唯一的浏览器。

所以我认为，我们必须要解决一些有趣的运营问题，如果你们关注将在未来几个月发生的事情的话，因为它会在一小部分浏览器和潜在的其他应用程序中发生，那么你们将会发现这些安全问题，你们将——而人们已经在寻找新的有趣方法来利用这项新技术。他们使用 DNS 中的 TXT 记录来传播恶意软件。几周前，我观看了关于这个问题的演讲，我当时想，“哇，这实在是太可怕了，我怎么没想到呢？”抱歉，开个玩笑。

但我认为这是我们必须密切关注的事情。我个人对交出控制权、决定权的想法存有很多顾虑。从我们自己的办公网络来看，我们是否能够保护我们自己的员工免受恶意软件和其他各种类型的攻击？我们是否有技术来实现这一点？

我觉得答案是否定的。但从根本上说，这是一件坏事吗？我认为不是，但相关技术必须不断发展才行。

亚历贾德拉 • 雷诺索： 非常感谢米凯莱。现在，我们还是继续请专家组成员回答我们的问题。先请 6 号麦克风那边的发言者发言，然后是 5 号麦克风。好的，有请 6 号麦克风的发言者。

米尔顿 • 穆勒 (MILTON MUELLER)：大家好。“整合和集中”一词出现在许多关于 DOH 的讨论中。据我了解，确实不是在 DOT 讨论中。但对于从事经

济分析的人来说，这些词语都有非常具体的含义。整合和集中是贬义的，因为它们可能会给予供应商垄断权和定价权。

我的理解是，人们现在使用的大多数 DNS 服务是不集中的，是分散的，他们根本没有为此付费，是吗？那么你们是担心这种集中会导致某种形式的 DNS 服务垄断定价，还是其他问题？你们能否更准确地说明这个问题具体是什么，以及互联网服务的整体市场将受到何种影响？

亚历贾德拉 • 雷诺索： 大家还有其他问题吗？

维托里奥 • 贝尔托拉： 我认为这不是一个定价问题，因为你们现在从 ISP 获得的 DNS，实际上是你们购买的互联网访问服务的一部分。这个问题更偏向于是集中信息和控制权的问题。

例如，这是一个协议，通过 [音频不清晰] 提升隐私保护，然而如果世界上 60% 的人使用相同的解析器，没错，这个解析器将会获取到世界上 60% 的浏览器的信息，这可能最终会对隐私带来巨大损害。

亚历贾德拉 • 雷诺索： 米凯莱要发言吗？

米凯莱 • 内伦： 谢谢！米尔顿，我认为，正如维托里奥所说，这个问题与定价无关，而更多地与互联网运作有关，因为它是分散的。这是一个包含多个网络的网络。每个 ISP 都可以设置自己的解析器，在每个网络中，我们都可以拥有自己的解析器。如果你们将其进行集中，那么就会失去稳定性和弹性。这种弹性有可能会消失。

此外，还有一个问题，即 DNS 流量中存在大量数据，不仅仅包含应该存在的数据，还包含不应该存在的数据。所以，人们试图访问的数据实际上可能并不存在。我们可能需要花费很多资金才能解决这个问题。

亚历贾德拉 • 雷诺索： 非常感谢！现在请 5 号麦克风的发言者发言。

未知身份的发言者（男）： 这里有一个困惑需要澄清，在浏览器级别谈论 DNS 时，也就是用户级别，这种情况下由谁来应用策略呢？我们如何从策略层面进行说明？这就是我的问题。我就说这些。

帝姆 • 阿普里尔： 我认为你是在问，谁可以授权或定义在浏览器中实施的策略。这就是你要问的问题吧？这完全取决于浏览器制造商及其任何用户，这些用户将为这些制造商提供有关他们实际选择实施内

容的反馈。目前没有任何政策机制来强制他们做任何事情。这是他们的软件，他们基本上可以做他们想做的任何事情。

亚历贾德拉 • 雷诺索： 谢谢！3 号麦克风。

埃杜尔多 • 迪亚兹： 非常感谢！如果我有一家拥有大型解析器的大型公司，那么我是否可以开始销售或提供顶级域而不需要前往 ICANN？然后，如果其他解析器没有找到这些顶级域的根，那么它们就可以联系我们，对吧？能这样做吗？这种情况可能发生吗？

帝姆 • 阿普里尔： 在技术上是可行的。关于这一点，目前还没有相关的禁令。

丹尼 • 麦克费尔森： 我认为 DOH 或 DOT 根本不会改变这一点。

帝姆 • 阿普里尔： 这与确定 .onion 的方式非常相似。

亚历贾德拉 • 雷诺索： 谢谢！4 号麦克风。

弗雷德 • 贝克： 我所关注的问题是互联网路由。对于我将要谈论的案例，你们可能非常熟悉。它是一个国家实体，但我会尽量避免提及它的名称。

这个问题通常也是一个企业问题。一些公司将强制实施信息安全模型，他们会通过以某种方式拒绝访问特定名称集来做到这一点。

现在，我所提及的那个实体中的工作人员决定开始使用 Google 解析器，而这被规避了，这个特性被相关公司规避了，该公司会劫持通往 Google 解析器的路由。

在安全解决方案变成劫持路由的时候，作为关注互联网路由的人员，我对此表示很担心。我很想知道你们对此的看法。

亚历贾德拉 • 雷诺索： 丹尼想要发言吗？

丹尼 • 麦克费尔森： 我只想说，是的，路由系统是一个信任网络，它的工作方式就是所谓的“传闻路由”，你们可以选择相信他人告诉你的信息并将其进行传播，也可以选择不相信，而且现在还没有主要的权威技术。我们现在已经有一些技术，诸如 RPKI 和所有运营任何关键基础设施服务的人员都应该使用的技术，还有可以更好地保障路由系统安全的一些其他技术。但我同意，并且也认

为基础路由系统可能是当今互联网上最大的安全问题之一，当然，在我们提升其安全性之前，每一项服务都会受其限制。

帝姆 • 阿普里尔： 还有一个例子——这也是一个很好的机会来说明，人们应该考虑使用 DNSSEC 和 [DANE] 来为他们正在使用的任何解析器进行 [音频不清晰]，以便在设备或解析器或者任何部分实际提出请求时，尝试联系服务器，它可以通过 DNS 验证其证书，并且使用 DNSSEC 来验证这实际上就是要与之通信的服务器，如果你位于可以访问 [证书存储区] 信任的密钥的区域，那么你不能仅仅依靠通过信任链检查 X.509 证书，因为此时你不能真正地信任它。

亚历贾德拉 • 雷诺索： 非常感谢！6 号麦克风。

马克 • 思凡卡瑞克 (MARK SVANCAREK)：在大家所提出的问题中，关注度最高的是 DNS 提供商的集中问题。为什么这里没有提出与这些协议相对立的问题呢？如果默认情况下，最流行的浏览器——这是我的理解，默认情况下——将转到 8.8.8.8，那么不管这些新协议如何，您都已经拥有了巨大的集中度。为什么这不是我们最关心的问题？这只是简单地加速了该趋势。

所以我认为，除了这些协议问题之外，这也是我们要在这里提出的问题之一。谢谢！

帝姆 • 阿普里尔： 我将抢先沃伦一步提出我的看法。沃伦曾说过，Chrome 在默认情况下不会选择 8.8.8.8。这只是一些可以选择的东西。还有其他浏览器——

马克 • 思凡卡瑞克： [沃伦说它只是针对 DOH 而言。][音频不清晰]

亚历贾德拉 • 雷诺索： 请使用麦克风。

帝姆 • 阿普里尔： 沃伦可以对我进行纠正，如果——

马克 • 思凡卡瑞克： 抱歉，我曲解了沃伦的意思。

帝姆 • 阿普里尔： 如果我说得不对，沃伦可以对我进行纠正，但我认为 Chrome 计划实施这一方案的方式是，默认情况下，如果你们已经配置了解析器，而且你们的系统解析器接受 DOH，那么 Chrome 将使用 DOH 作为解析包。如果不是这样，它将返回到系统解析

器，然后用户可以选择将 DOH 用于支持它的任意解析器。因此，你们可以选择 8.8.8.8。它可能是你们可在下拉菜单中选择的一个预配置选项，但默认情况下，它不会在 Chrome 中打开。

维托里奥 • 贝尔托拉： 我想补充一些更为一般性的内容，你说得很对——当用户前往地址栏并输入其中一个服务器的地址（例如 8.8.8.8），而不是他们从网络中获取的默认地址时，我们一直在讨论的有关安全性、隐私、主权方面的许多问题 [音频不清晰] 已经存在。

重点是这实际上是默认的，这使得浏览器可以更容易地将用户从本地解析器切换到最大的解析器，而且我也认为任何类型的集中都已经成为令人关注的问题。我很高兴 Google 说他们现在并没有采用这种部署模型，当然，对于 5 年、10 年后会发生什么事情，我们也就不得而知了。

亚历贾德拉 • 雷诺索： 非常感谢！5 号麦克风。

罗伯托 • 加埃塔诺 (ROBERTO GAETANO)：非常感谢！我曾亲眼见证了网络软件是一系列专有解决方案的时代，这些解决方案一直在解决不同领域的各种不同问题。之后，我们缔造了一个 7 层的架构，其中包括传输层、物理层等等，总共有 7 层。

其结果是我们可以拥有开放软件，并且能够为每一层提供彼此相互竞争的解决方案。现在，有了 DOH 和 DOT 这种方法，我们难道不是又回到了专有解决方案，限制拥有竞争解决方案，又回到了 [60 年代] 被不恰当地称为——特别是对于作为意大利人的我来说——意大利面条式的代码时代。谢谢！

丹尼 • 麦克费尔森： 我认为这个观点不错。我认为这仍然是在使用 TCP IP 堆栈和分层模型，它只是在进行顶级域名解析，而不是在本地系统中使用存根解析器。

当然，如果你看到本地系统上的解析路径扩散，或者它们完全绕过这一点，那么这将对用户、网络运营商和基础设施产生影响，届时可能会有不同的相关方从中受益，也可能有不同的相关方会在某些方面蒙受损失。

所以一方面，我可以理解你的观点。另一方面，我认为它并没有背道而驰，我只是认为，如果你们拥有最终用户应用程序并且能够直接连接到你们想要的域名解析基础设施，那么你们就可以看到该事务的两面，而且它可能会影响网络运营商，正如沃伦和 Google 员工所指出的那样，他们可以升级其解析器以支持这些新功能，而且有时候，用户受到该域名解析基础设施和服务提供商的限制可能比他们实际意识到的要多，这可能是个问题。

从这个角度来看，我认为这个观点很不错。

彼得 • 科赫： 罗伯托，你和前一位发言者都没有提到这是一种孤岛构建方式，当然，从更大的范围来说，这是一种倒退。但这种趋势与这些协议的标准化没有直接关系。就像我所说的，这些协议可能是非常无辜的。但这是一种普遍趋势。

大多数人的智能手机上都安装了很多应用程序，而且关于它对于标准化以及中央基础设施的使用意味着什么，我们也进行了长期的讨论，当我使用只用于通话的应用程序时，除了 HTTP 级别以外，我的 [音频不清晰] 标准是什么，所有的事情都已经在那里完成，那么我自己还可以做些什么？

这是更大趋势的一部分。这并不是唯一的，当然，这也是另一种趋势，它与 ICANN 处理的基础设施有关，这也是向大家介绍这一问题的主要原因之一。

亚历贾德拉 • 雷诺索： 谢谢！3 号麦克风。

约尔格 • 施魏格 (JÖRG SCHWEIGER)：我认为得出的结论是，DOH 的好坏取决于部署模型，但我想知道这是否属实。如果只有用户可以做出选择的话，那么使用 DOH 将是有益的。但需要考虑到，用户下载应用程序后，解析路径将被深埋在应用程序中。

所以当前并没有提供选择，而且如果该应用商店属于主要参与者，那么当然也不会提供选择。因此，它的好坏真的是关乎于部署模型吗？

维托里奥 • 贝尔托拉： 这也是 IETF 的一个热议主题，当然，针对这在多大程度上属于协议问题，以及这在多大程度上属于人们使用方式的问题，我们也进行了一些讨论。

无论如何，我认为最重要的事情是，我们要了解，是否可以并且如何让所有利益相关方参与到有关适当部署模型的讨论中来。因为最后，如果应用程序需要让用户做出选择，甚至使用用户在设备、操作系统中配置的默认设置，而且如果他们按照规则这样做，那么至少大多数问题都会开始消失。

但问题是，我们如何才能开展这样的讨论？因为这里很少有来自浏览器制造商的人，可能所在公司相同，但他们并不参与浏览器制造工作。那么我们如何让这些人参与政策讨论呢？

亚历贾德拉 • 雷诺索： 谢谢！远程参会者有两个问题，请讲。

爱丽儿 • 梁： 第一个远程问题是由克里斯托弗 • 威尔金森 (Christopher Wilkinson) 提出来的。20 年来，集中度一直是一个全球性问题。比如根服务器、域名服务器、[ISP]、DNS 等等。

为什么我们现在要朝着相反的方向发展？这些 [导致不安全] 的解析器将位于何处？

维托里奥 • 贝尔托拉： 我想指出的一点是，解析器平台可能是分散式的，你可以在每个国家和地区都拥有一台服务器。但如果公司仍位于某一特定司法管辖区内的特定营业地点，那么他们将始终受制于此。因此，我认同克里斯托弗所提出的问题。

丹尼 • 麦克费尔森： 我只想补充一点，无论是从地理位置还是从解决方案的角度来看，根服务器系统以及一些注册管理机构可能是当今世界上分布最广泛的解决方案和互联网服务系统。所以，我认为如果——[完成了] 过去我们称之为超级巨星的工作，其中 20 个左右的互联网实体占所有互联网流量和目标的 80% 左右，如果这些实体是正在运营这一业务的实体，而且 ISP 和其他人员没有选择保护解析数据的机密性，那么这些实体将会看到更多的流量，当然，这肯定会导致管辖权和其他问题。但我认为，随着时间的推移，自然经济学和资本主义将有助于解决和梳理这个问题。这是我们正在讨论的一项新兴技术。所以我认为完善这项技术还需要很长时间。

亚历贾德拉 • 雷诺索： 谢谢！第二个问题？

爱丽儿 • 梁： 第二个问题是由迈克 • 巴格利 (Mike Bagley) 提出来的。难道 DOH 不是在允许更好地绕过基于 DNS 的安全系统并阻止广告拦截软件吗？这不是在增加安全风险吗？

米凯莱 • 内伦： 简单来说，是的。

丹尼 • 麦克费尔森： 我想对此补充一下。我已经在幻灯片中提到了这一点，我的意思是，如果你们的 DNS 解析发生在相同协议中并且到达相同的目的地，而且它位于发生网络流量的应用程序层，那么任何想以某种方式操纵它的人都必须做更多的工作来对其进行梳理，并找到想要操纵的内容。

坦率地说，这是其中的一个问题，也就是现在仍有一些人操纵 DNS 响应，如果你们是浏览器供应商或者系统内或应用程序运营商，并且可以阻止人们操纵响应，那么你们就可以在某种程度上影响事物的经济性。

在这一方面，也会有赢家和输家，所以我认为安全系统必须加强，你们可能会在企业中大规模地阻止这些协议，这可能是许多企业将要做的事情，或者你们也可能想要代理这些协议。在

非常受控的环境中，你们可能不会让这些内容在顶部以本机方式解析，特别是从主权的角度来看，这可能会给生态系统带来一些问题。

亚历贾德拉 • 雷诺索： 4 号麦克风。

卡沃斯 • 阿斯特 (KAVOUSS ARASTEH)：非常感谢！我只想发表一些看法，而不是提出问题。米凯莱，非常感谢你。你曾问过，我们中有多少人了解什么是 DNS 以及它的工作方式。我无法回答这个问题，因为我们没有任何统计数据，所以我无法代表任何人发言。这是你的陈述。

接着你又问，我们是否关心安全问题？答案是肯定的。

我们是否关心隐私问题？答案也是肯定的。

我们是否关心 [音频不清晰] 技术问题？答案还是肯定的。

但对于我们中的一些人来说——并不是很多人，这些都是新问题。我们必须消化这些内容。我们必须了解这方面的内容。在回答任何这些问题之前，我们需要了解它的工作方式，以及它是对安全和隐私问题的回答还是响应。这是一些动态的问题或主题，我们必须时刻关注这些问题，而且我们很难回答其中的任何一个问题，即便是与 ICANN 使命直接相关的第二个问题。

也许我们还有更多的问题要补充，也许 [只有] 那一个问题。不管怎样，我们需要一些时间。非常感谢！

米凯莱 • 内伦： 谢谢卡沃斯。这一次，我们实际上达成了一致意见。这种情况并不多见。我认为这样的技术是非常新的，而且我们中的一些人已经提到它是新兴的技术。

我们中的很多人一直在努力做的事情是，试图鼓励生态系统各个部分的人员开始提出这些问题，提出一些简单的问题、比较复杂的问题以及仅仅在某种理论层面上确实难以解决的问题，然后尝试与实际已经部署这些技术的公司进行交流。

他们会说，“哦，很好，很棒！我们所做的事情是为了实现更大的利益。”但除非你们真的细致入微地进行观察，否则你们不会知道它是否会永远这样。一些最初纯洁无瑕的事情可能会变成另一番模样。或许，它也可能一直保持纯洁无瑕。

所以，我认为这就是我们需要研究的事情，另外我们还要与在座的一些人（也许还有会议室以外的一些人）进行交流，然后开始继续进行这样的对话，因为这是 IETF 和一些科技圈之前已经讨论过的主题，也许是在 3 年或者 4 年前？也许是更长的时间。这种对话是以一个简单的问题开始的，“我们如何使 DNS 更加私密？”接着，这个问题不断发展变化。但在座的很多人并不在 IETF 空间，也就是骨灰级技术狂空间中，并没有

真正研究这项技术，现在这项技术已经变成了现实，所以我认为现在是我们开始进行这种对话的时候了。

亚历贾德拉 • 雷诺索： 非常感谢！5 号麦克风。

安迪 • 贝茨 (ANDY BATES)： 大家好。谢谢！我叫安迪 • 贝茨，来自全球网络联盟。我们是 9.9.9.9 的联合创始人之一，我发现这是围绕整合展开的一场令人耳目一新的辩论。我想，我们向专家组提出的问题是，我们不希望用户只停留在普通的 DNS，因此无论你们使用任何四元组还是任何解决方案，我认为关键是真正保护用户免受网络犯罪的侵害。

所以我认为这个问题是，你们想要整合还是抵御网络犯罪？没有其他真正的选择了。我很欢迎你们提出意见。

维托里奥 • 贝尔托拉： 我认为，对路径加密是我们应该做的一件积极的事情。我们向运营商 [音频不清晰] 提出的建议是部署 DOH。同时，如果你们在解决了一些隐私和安全方面的问题之后，又制造了其他更大的隐私和安全问题，那么你们还没有真正取得进展。

因此我认为，解决这个问题的积极方法是要对正在发生的事情有一个共同的理解，并就其实施方式制定一项通用的政策，这样你们就可以最大限度地发挥积极作用，并解决消极因素。

亚历贾德拉 • 雷诺索： 非常感谢！3 号麦克风？

沃尔夫冈 • 科纳沃茨特 (WOLFGANG KLEINWAECHTER)： 非常感谢！这里是 GAC 会议室，你们在一张幻灯片中提到，这将对国家监管框架产生一些影响。你们是否了解政府在这里的职责，或者你们是否已经从执法机构那里获得了一些意见？

米凯莱 • 内伦： 沃尔夫冈，我们不负责这件事。我们只是一群因为各种各样的原因而被要求讨论这个主题的人，但如果你们想要提出这个问题，请不要问我们，我认为这可能是最好的说法。

当然，维托里奥接下来会纠正我的说法，这是他在这个专家组的职责。彼得也会纠正我的说法。

彼得 • 科赫： 这是我第一次做纠正，米凯莱。这是一个非常好的问题。我认为整个有关阻止问题的辩论涉及到几个方面，有一些政府信赖

DNS 阻止，而且 DNS 将阻止某些内容的专门用户访问这些内容。

我们知道这些方法很容易被规避。但是，在另一方面，使用域名解析来防止意外访问内容或其他任何内容，抵御恶意软件、网络钓鱼等等，或者 [音频不清晰] 连接僵尸网络命令与控制系统，这可能有效，但目前并没有说明解析服务提供商——他们中的一些人，现在已经提供了一些特定的服务，比如在 DNS 保护方面，我不确定它是否有商标，但它应该是 DNS 防火墙等诸如此类的保护。它们是开放的。你们实际上可以采用这些防护措施。

回到米尔顿的问题上面，是的，其中一些提供商收取费用，另一些是针对数据收费，这是一个不同的主题。他们中的一些人会向你们收取费用，然后才会提供解析服务，而该服务实际上是提供已知的恶意软件和网络钓鱼网站的黑名单。至少对于我们正在谈论的一些提供商来说，他们并没有理由不部署它。因此，从这个意义上讲，并非所有的内容都与监管有关，而且关于它可以被轻易规避这一点，我们应该习以为常。这里可能会碰到一些困难并涉及到一些细节。

如果你们信赖 DNS 阻止，那么你们可能也会信赖使用基于 HTTPS 的 DNS 进行的 DNS 阻止。

维托里奥 • 贝尔托拉： 我只想补充一点。就我个人而言，我并不是特别喜欢 DNS 阻止，但我认为真正重要的是，关于是否阻止内容的决定是由每个国家和地区及其互联网社群以民主方式做出的，还是由互联网公司和浏览器制造商共同做出的。我认为，从这个意义上看，这确实是一个权威问题。这就是让我感到恼火的地方，因为一些 DOH 支持者接受采访时说，“我们要把世界从审查制度中拯救出来，任何形式的内容控制都是审查制度，即使在民主国家和地区也是如此。”

作为一名欧洲公民，这真的让我很恼火。就其他政府而言——我只知道英国政府，但如果有其他政府来处理这个问题，我们将非常欢迎。

亚历贾德拉 • 雷诺索： 非常感谢！现在请 4 号麦克风的发言者发言，在远程参会者发言之后，我们将关闭发言队列。

塞巴斯蒂安 • 巴肖莱 (SÉBASTIEN BACHOLLET)：谢谢！我将用法语发言，因为我们有口译工具，而且会议室里还有合格的口译人员。我是一名个人最终用户，也是 ALAC 的成员，我想问一些问题。但对于这些问题，我已经有答案了。

我还有两个问题：在所有这些情况中，最终用户的选择是什么？难道我们不存在一种风险，会发现自己处于几年前使用

MSN、CompuServe 等软件时所处的境地吗？现在这将是其他软件。但有人会为我们选择发生解析的位置。

第二个问题与 ICANN 有关。在域名服务器、根服务器以及将来管理所有这些内容的方式上面，可能会产生什么后果？我们能否想象到未来将不再需要 ICANN 存在时的情况？因为这些解析器、服务器可能会决定在文件中添加新扩展名、新名称或者删除这些名称？也就是屏蔽一些内容或添加一些内容。在我看来，这些问题很重要。

我同意你之前所提出的观点。重要的是我们要继续解决这些问题。遗憾的是，在我们能够与所有利益相关方讨论这些议题之前，这些标准化工作就已经完成了。非常感谢！

米凯莱 • 内伦： 塞巴斯蒂安，谢谢你的问题。对于你的第一个问题，我认为我们在会议早些时候的问答环节中已经进行了讨论。是的，确实有可能最终由几个供应商来选择所发生的事情。正如我前面提到的，确实会有与阻止相反的情况，在这种情况下，有可能会添加一些内容。这是一种风险。

但是协议和标准是由 IETF 和其他标准机构内的人员制定的。他们当时已经进行了讨论。你可以关注这些讨论。这些讨论是公开的。

当然，要加入讨论，还存在一个技术壁垒。这并不是面向所有人的。有一些标准会影响我们的日常生活，我们中的很多人都不知道他们在谈论些什么，因为这不是我们的专业领域。

而现在，大家已经了解这些事情，并且可以开展这些讨论。所以关于为何现在开展这些讨论是行之有效的，我认为这就是原因所在。我不知道其他人是否还有要补充的内容？帝姆，你要发言吗？

帝姆 • 阿普里尔： 我只想补充一点，DOH 和 DOT 技术本身并不是造成这种情况的罪魁祸首。这取决于真正影响这些决策的实施，而这些决策可能是在 DOH 或 DOT 没有被作为 IETF 拟定标准的情况下做出的。它可以由浏览器供应商直接实施。

它现在之所以成为了一个热点问题，是因为它们是拟定的标准，而且当前还有很多关于在 DNS 请求的第一英里增强或添加这种隐私机制的讨论。

我敢肯定，即便有人在这种部署中设置了路障，IETF 中的一些聪明人士也能继续在这些路障周围寻找其他方法。

亚历贾德拉 • 雷诺索： 很抱歉打断你，但我认为我们需要先让远程参会者提出最后一个问题，因为我们已经超时。抱歉打断了你的发言。大家也可以在会后继续讨论。有请远程参会者发言。

爱丽儿 • 梁： 这实际上是由保罗 • 霍夫曼 (Paul Hoffman) 提出的一个意见。DOT 和 DOH 是新的协议，但是 20 多年来，应用程序和操作系统已经能够完成与它们相同的工作。

维托里奥 • 贝尔托拉： 他是 DOH 标准的创建者之一。这个观点很不错。

亚历贾德拉 • 雷诺索： 好的，非常感谢你的意见。现在 [我先总结一下]，然后我们将结束这个高关注度主题会议，我想请你们每个人快速思考一下，大家应该从这次对话中获得什么信息。你们现在可以开始了。谢谢！

帝姆 • 阿普里尔： 我先从简单的开始。就像我刚才所说的，DOH 和 DOT 是 IETF 中的两个拟定标准，它们没有向域名系统添加之前无法通过使用非标准方法来实现的任何技术能力。

至少在我看来，最令人担忧的是，我们在这里所开展的很多对话很大程度上取决于 [音频不清晰] 应用程序，或解析器和权威服务器中这些协议的政策和实施细则，因为我们正在推进这些措施。

维托里奥 • 贝尔托拉： 我的意思是要去继续了解相关知识，特别是如果这是你们第一次参与此类讨论的话。当然，会有很多人乐于向你们提供帮助，而且很多资料已经在网上公布了。你们可以联系相关员工。但是还请大家考虑一下，利益相关方与社群其他成员进行交流，以及在 IETF 或者一些尚未确定但可能涉及更多技术性和政策性问题的政策场所参与讨论的 [频率]。

彼得 • 科赫： 是的，我想说的是，IETF 制定的标准可能对我们所看到的发展有所帮助，但它们不是根本原因，因此我们应该关注根本原因，也应该深入到更大的层面，即这对 ICANN 和 ICANN 环境以及命名空间治理的未来意味着什么？

丹尼 • 麦克费尔森： 很好。从运营的角度来说，我认为这可能会涉及到一些开销，但是从隐私和安全角度来看也会有一些好处，而且了解部署这些技术的位置和方式将能够实现这些好处。

作为 SSAC 的成员，我认为 SSAC 才刚刚开始考虑这个问题，当然我们也非常欢迎大家提供反馈意见。我们还在消化这些内容，而且这是一个不断变化的目标。这些拟定标准都处于 IETF 的标准轨道上。它们还不是完全的标准，但肯定处于标准轨道上，而且 [我认为] 让大家了解这对 ICANN 以及政策人员，尤其是参与 ICANN 的人员的影响，就是希望 SSAC 的建议将有助于提出

或提供更多的见解，以供这些人员在 ICANN 开展工作时进行考量。谢谢！

米凯莱 • 内伦： 亚历贾德拉，你做了件非常危险的事情。你将最后的总结发言权交给了我。

亚历贾德拉 • 雷诺索： 请讲。

米凯莱 • 内伦： 谢谢！在座各位以及其他远程参会者都提出了一些非常有趣的问题和意见。就我个人而言，我在参与这次会议之前就对这些技术有一些了解，而在听取大家向我们提出的一些问题以及一些意见的同时，我个人对这些技术的想法也在不断发生改变。对我来说，这意味着在实际开展对话方面，我们可能正朝着正确的方向前进。

我想告诉你们的是，如果你们现在看一下屏幕上的幻灯片，就能了解在即将举行的 IETF 会议上，你们可以从哪些环节获取更多信息。在 dnsprivacy.org 网站上，我认为有很多关于基础技术的信息。另外还有很多不同公司发布的博文，我想，还有其他一些团体，比如 CENTR 最近也发表了一篇文章。所以请大家花点时间，多阅读有关这些技术的内容，然后提出一些问题。

亚历贾德拉 • 雷诺索： 非常感谢！本次会议到此结束。让我们向专家组成员致以热烈的掌声。

[听力文稿结束]