ICANN68 | 虚拟政策论坛 — 全体会议：域名系统 (DNS) 和物联网：机遇、风险和挑战
2020 年 6 月 23 日，星期二 — 马来西亚时间 13:00 至 14:30

里亚 • 欧丹内斯
(RIA OTANES)： 大家好，欢迎参加有关 DNS 和物联网的全体会议：机遇、风险和挑战。我叫里亚 • 欧丹内斯，是本次会议的远程参与管理员。

请注意，本次会议正在录制中，并遵循 ICANN 的预期行为标准。在本次会议期间，只有在“问题与解答”窗格中以英语提交的问题或评论才允许被阅读。可以从“缩放”工具栏访问此功能。我将在会议主席或主持人设定的时间内阅读允许的问题和评论。如果您想口头提出问题或评论，请举手。当叫到您的名字时，您将获得取消麦克风静音的权限。请在此时取消麦克风静音并发言。为了方便记录，请说出您的姓名，如果您使用英语以外的其他语言，还要说明您要使用的语言。本次会议包括实时转录和口译。要查看实时转录，请单击“缩放”工具栏中的隐藏字幕按钮。

为帮助我们的口译人员，请以合理的语速清晰地发言。要收听口译，您需要下载口译应用程序。如需了解更多信息，请参见活动时间表中的会议详细信息，聊天中也提供了说明。

最后，我想提醒大家，如果您希望会议室中的每个人都可以阅读我们的聊天评论，请使用聊天窗格中的下拉菜单从“回复所有小组成员”切换为“回复小组成员和与会者”。

好了，现在由亚力杭德拉 • 雷诺索 (Alejandra Reynoso) 发言。亚历杭德拉，请继续。

亚力杭德拉 • 雷诺索： 非常感谢里亚。

大家好。我叫亚力杭德拉 • 雷诺索。我为危地马拉 ccTLD .grant Thornton 工作，很荣幸主持本次全体会议。

通过数百亿个被动和自主感知的作用于我们的物理环境的互联设备，物联网有望让我们的生活更轻松，社会更安全、更智能、更可持续。尽管这使 IoT 与传统的交互式互联网应用程序（如电子邮件和网络浏览）有很大的不同，但许多 IoT 设备将使用域名系统来找到所需的远程服务。

安全与稳定咨询委员会 (SSAC) 最近发布了文件 SAC105，这份报告讨论了 DNS 与 IoT 之间相互作用的机遇、风险和挑战。今天的全体会议将进一步充实这份文件旨在引发的对话，特别是使所有选区的社群成员能够与主题专家以及彼此之间讨论该主题。

本次全体会议是 ccNSO 在蒙特利尔会议上针对 SAC105 的会议的后续，该会议特别重点讨论了 ccTLD。

本次全体会议的目的是：更好地了解物联网与传统的交互式互联网应用程序有何不同，以及它如何使用 DNS；更好地了解 DNS 和 IoT 参与者如何在机遇、风险和挑战方面思考两个生态系统之间的相互作用；并进一步思考 ICANN 社群在此领域可能发挥的作用。

请播放下一张幻灯片。

这是今天的议程。首先，我们将对文件 SAC105 进行简要概述。然后，将有一个专家小组来分享他们对该主题的看法。之后将进行同行评审，评审人员将就专家的演讲提供反馈。最后是听众问答环节。

请播放下一张幻灯片。

我来简单介绍一下克里斯蒂安 • 黑塞尔曼 (Cristian Hesselman)，他将为我们进行 SAC105 的简要概述。

克里斯蒂安是 SIDN Labs 的董事，SIDN Labs 是 SIDN 的研究团队，而 SIDN 是荷兰 .NL 国家/地区代码顶级域的运营商。它的目标是通过基于经验测量的研究以及对新的互联网系统和工具进行原型设计和评估，来提高端到端互联网通信的运营安全性和弹性。

克里斯蒂安还是 SSAC 的成员，并且是撰写 SAC105 的 SSAC 工作组的领导，这份报告阐述了 DNS 和物联网、机遇、风险和挑战。

他还是荷兰特温特大学的兼职副教授，并担任 NLNetLabs 董事会主席。

克里斯蒂安，交给你了。

克里斯蒂安 • 黑塞尔曼： 好的。非常感谢，亚力杭德拉。

那么，今天我很荣幸向大家简要概述 SAC105，这是 SSAC 在 2019 年 6 月发布的报告。正如亚力杭德拉所总结的那样，该文件阐述了物联网 (IoT) 和 DNS 之间的相互作用，特别关注了引发和促进 ICANN 社群中的讨论。

这份报告也将在今年晚些时候以同行评审论文的形式发表在《IEEE Internet Computing》（IEEE 互联网计算杂志）上。

请播放下一张幻灯片。

物联网。我们在报告中使用的定义是 ISOC 在 2015 年提供的 IoT 定义 — 将网络连接和计算功能扩展到物体、设备、传感器和通常不被视为计算机的物品的应用。也就是将所有东西都连接到网络，即使是您之前从未想过能连接的东西。

大家知道，与传统交互式应用程序（例如电子邮件和网络浏览）的一些区别如下。因此，物联网不断地感知物理空间并与之交互。这是一个重要的区别。并且它还会解读从各种传感器接收到的信息，以实际作用于该空间。这通常是在用户没有意识的情况下发生的，因此请想一下嵌入墙壁或其他类型物体中的微型传感器，您会在不知道它存在的情况下与之交互。因此，这就是 ISOC 所说的被动交互，而不是互动式交互，例如与 Web 浏览器和电子邮件客户端进行的交互。因此，将会有大量的这些物联网设备。至少许多市场分析师的预测是这样。有人说这类设备数量为 200 到 300 亿，而且它们基本上是在我们日常生活的背景中运行的。因此，我们实际上看不到它们。我们与他们互动，但没有意识到它们的存在。

此外，区别还在于，IoT 设备通常远比我们所用的笔记本电脑和移动电话多样化。我们所说的是不同类型的操作系统。我们正在谈论不同的硬件体系结构，也在谈论不同类型的网络连接。因此，不仅仅是 Wi-Fi，还有 ZigBee，以及其他类型的无线网络。

好的。最后，物联网的不同之处在于，物联网设备的使用寿命更长，这可能是因为它们嵌入在物理结构中，并且还具有无人值守的运行特点。因此，没有网络管理员或真正看管这些设备的人员。它们只是在那里做它们的工作，并在您不知道的情况下连接到网络。

因此，有一段时间，物联网被认为是下一件大事。我认为，实际上这些东西自 1990 年代以来就一直在使用，之前被称为普适计算或类似的名称。因此，曾有不同的名称，但概念大致是相同的。但无论如何，现在我们正处于可以真正部署这类设备、传感器和致动器的阶段，因此，人们认为 — 人们坚信 IoT 将能促进更安全、更智能、更可持续的社会。例如，在智能交通系统领域，基于各种传感器、智能能源网格或智能家居和智能城市，在整个城市区域智能地安排交通路线。我认为后者是最有吸引力的示例，因为这是我们所有人都知道的，是如今我们家里都有的物品。

好的。因此，物联网带来很多希望，但有一个主要问题，那就是物联网安全性，我将在稍后讨论。

请播放下一张幻灯片。

谢谢。

因此，这是一个示例 — 是我们在 SSAC 中使用的思考物联网的模型。您在左侧看到的是物理空间的繁忙图片，我们来看看顶部。您在左上角看到的是家中的人，他们与我们所说的物联网部署进行交互。也就是您在屏幕中间看到的阴影区域。物联网部署由三部分组成。一是物联网设备。二是网络连接。三是后端服务，对不对？

这里有一个小手表和智能门锁的示例，当有人靠近门，人们靠近家里的门，并且也许还有某种智能门把手时，所有关于接近的信息都将通过人们佩戴的智能手表联合智能门把手的指纹识别进行收集，然后这些信息通过互联网发送到某个远程服务，并基于该服务做出决定，即是否打开门锁的决定。显然，这将由用户策略来驱动。

因此，您看到的是，在这个非常简单的示例中，信息由顶级设备，D1，例如这里的智能手表来感知。该信息通过互联网共享给服务，然后再次发送回门锁以对其进行锁定或解锁。

因此，您看到的是感知并作用于物理 — 感知并作用于用户的物理环境，并且透明地进行 — 用户没有意识到，对吗？

因此，例如，用户仅看到设备，他们看到了智能手表，也看到了智能门把手，但是看不到背后的整个机制。

DNS 就是机制中一个组成部分，因为我们从之前的研究中了解到，这些设备具有 — 它们与互联网上的服务交互以提供功能，对吗？因此，这与传统的网络浏览不同，在传统的网络浏览中，您与网络浏览器进行交互以从网络中获取某些信息或使用服务。在这个格局中，设备正在使用服务来执行其功能，对吗？

因此，例如，在这个具体示例中，服务可能正在分析来自用户的传感器信息，然后决定是否打开门锁。对吧？

因此，在这些交互中，DNS 扮演着重要角色，但是我在这里不讨论细节，因为在本演讲之后，艾略特 (Eliot) 将对此进行更多讨论。

好的。我认为这是目前最重要的一点，请播放下一张幻灯片。

好的。这份报告称为 DNS 和 IoT 机遇、风险和挑战。这三点各有一张幻灯片：一张是关于机遇，一张是关于风险，另一张是关于挑战。在 DNS 中，我们通常不会真正讨论机遇，因为 — 在 SSAC 中，我们最主要关注威胁和风险，但在这种情况下，我们认为有必要 — 这对于 DNS 而言是一个机遇，因为它是全球性的 — 大家知道，这

是一个全球性的信任基础架构，可以提高物联网的隐私性、安全性和透明度。因此，我们真的相信 DNS 可以在这里提供附加值。

我在这里列出了三点。如需更多详细信息，请参见 SAC105。第一点是，我们认为 DNS 可以减少用户被分析的风险，这是因为我们刚才谈到的那些设备与 DNS 交互。因此，DNS 查询，如果物联网设备的路径与其使用的远程服务之间有观察者，则它可以根据 DNS 交互来查看房屋中的人，例如他们所使用的设备类型，甚至他们是否是用设备，因为这会促使与 DNS 的更多交互。

另一种可能性是，如果您通过查看域名知道正在使用的 IoT 设备，您甚至可以 — 作为攻击者，甚至可以尝试提出 — 尝试找出正在生成这些查询的物联网设备，对吧？有更多的研究表明，许多物联网设备使用他们查询的一小部分域名，以便找到我们在上一张幻灯片中谈到的远程服务。有时，这些 DNS 查询或它们使用的域名也会揭露有关生成它们的设备类型的信息，对吧？这就是关于减少用户分析风险的背后想法。您可以通过对这些物联网设备生成的 DNS 请求进行明显加密来实现这一点。例如，您可以通过备受争议的 DoH 和/或 DoT 来实现这一点。

我们预见的另一个机遇是减轻将物联网设备重定向到另一个远程服务的风险。例如，在互联网上，我们已经看到了一个称为路由劫持的概念。它们导致流量被发送到恶意网络。这可能会对物联网产生严重影响，因为物联网设备将不再连接至它们本应连接的服务，而是可能会连接至恶意服务。而且存在这样的风险：人们正在与远程服务分享其私人数据，或者这意味着远程服务甚至可以作用于他们的物理环境，对吗？因此，这是一个风险。

我们认为 DNS 可以在这方面发挥作用，因为显然我们拥有 DNS — DNSSEC，对吧？因此，它可以验证来自 DNS 的消息的完整性。举例来说，如果发生路由劫持，DNSSEC 客户端将能够检测到该问题，因为它们可以 — 它们能发现这一问题，因为 DNSSEC 消息上的签名未通过验证。

我们看到的另一个机遇是 — 这是注册服务机构提供多因素身份验证的机会。多因素身份验证简称 MFA。

例如，他们可以通过使用多种因素（甚至是指纹识别或类似技术）来加大对物联网设备所用域名的保护。对吧？我们看到的这两个机遇可以降低通过恶意服务重定向物联网设备的风险。

最后，我们还看到了一个机遇，可以提供有关物联网设备使用的服务和解析器的更多见解。大多数时候，人们与物联网设备进行交互，但他们实际上并不知道他们与互联网上的哪些服务共享了什么类型的信息。例如，通过让用户设备生成的 DNS 查询对最终用户可见，这将有助于他们对这些交互有更多了解，对吗？

在前面的示例中，您将看到 — 例如，您将能看到手表与互联网上的远程服务共享信息。对吧？

请播放下一张幻灯片。

这是不利的一面，即风险。所以也许我应该只谈论 — 我尽量说的简短一点。我们看到的最大风险是物联网会导致对 DNS 的大规模 DDOS 攻击，对吗？我们之前遇到过这种情况，当然，臭名昭著的例子是 2016 年在 DNS 运营商 Dyn 上发生的 DDOS 攻击。但我们也看到了其他物联网僵尸网络在互联网上发展，并且它们的规模可以快

速增长。它们还可能开始使用开放式解析器，这会将 DDOS 流量反射到目标位置，甚至为这些人创造更大的流入流量。

另一个风险是我们所说的 DNS 不友好编程，它以一种不成熟的方式使用 DNS，例如，几年前，一个 iPhone 应用程序生成随机 DNS 查询，导致解析器的缓存失效，因为它们无法缓存任何内容，并且耗尽了镜像功能。

请播放下一张幻灯片。

那么，我们已经看到了 — 我们讨论了在 SSAC 制定的物联网模型。我们讨论了机遇，也讨论了风险。那么，下一个问题是：我们应该如何应对这些挑战并解决风险？

我们在这里写下了 DNS 和 IoT 行业面临的一些挑战。这实际上略微超出了 SSAC 的范围，因为我们认为物联网社群也在这里发挥着作用。

第一点是为这些物联网设备开发一个安全库，提供我们刚才在机遇幻灯片中谈到的功能。例如 DNSSEC 验证和 DoH/DoT 支持，以及使 DNS 查询以具有吸引力和直观的方式对最终用户可见的功能。

然后，我们认为存在培训方面的挑战。对物联网专家进行培训，使其了解 DNS 的含义、其安全功能是什么，以及使用它们需要采取什么措施，反过来，还要让 DNS 专家从根本上了解物联网的工作原理以及物联网将会改变域名的使用方式，也许这需要物联网的不同类型的功能 — 对于域名注册和安全性。

最后几点可能更具挑战性，难度更大。因此，第一点是与一组 DNS 运营商合作，以共享我们所说的 DDOS 指纹。这些就是 DNS 运营商发生的 DDOS 攻击的总结。然后，他们将相互共享该信息，以做好更好的准备。

这些 DNS 运营商甚至可能尝试共享 DNS 缓解能力。例如，擦洗设施。而且我们预见到，网络边缘的系统可防止边缘受到 DDOS 攻击和入侵。设备入侵。

最后，畅想一下，我们认为，拥有一个能够衡量物联网的演变并了解其发展以及对 DNS 的使用情况的系统将是非常不错的。

这些就是我的幻灯片，亚力杭德拉。

亚力杭德拉 • 雷诺索： 克里斯蒂安，非常感谢。

现在有请我们的专家小组，他们将按以下顺序分享他们对此事的看法。首先是艾略特，然后是利兹 (Lise)，之后是克里斯蒂安 (Cristian)。

首先我要介绍一下艾略特 • 李尔 (Eliot Lear) 和利兹 • 富尔 (Lise Fuhr)。艾略特 • 李尔是 Cisco Systems 物联网安全领域的首席工程师，重点关注设备和网络之间的通信方式。艾略特是互联网社群的资深人士，自 1998 年以来一直参与 IETF 社群，撰写了大量 RFC，并在互联网架构委员会任职，并且是 IANA 过渡期间 IETF 参与 ICANN 重组工作的领导者之一。他还曾在国际电信联盟 (ITU) 担任领导职务。艾略特居住在瑞士。

利兹 • 富尔自 2016 年 1 月起担任欧洲电信网络运营商协会 (ETNO) 的总干事。在 ETNO，她是协会的主要外部代表，领导并监督所有活动。

她作为协会的代表，还是欧洲网络安全组织的董事会和行政委员会成员。利兹还被再次任命为互联网协会公共利益注册管理机构董事会成员，任期自 2019 年 5 月开始，为期三年。

利兹在电信行业拥有 20 多年的经验。她的职业生涯始于丹麦科学、技术和创新部，在该部门撰写并实施了针对电信市场的法规。之后，她在电信、运营商和电信网络行业工作，领导多个团队处理互连设备、移动设备，抱歉，移动服务和行业合作过程中的问题。

艾略特，交给你了。

艾略特 • 李尔： 非常感谢，亚力杭德拉。

请放下一张幻灯片。

我想给大家讲一个有关烤箱的故事。这是一个烤箱。它已启用互联网。它支持物联网。我表妹购买并安装了一个这样的烤箱，一段时间后，它在早上 5:30 给她发消息，告诉她烤箱需要清洗。现在，我个人认为这是一种拒绝服务。但这就是它的设计工作方式。

我表妹不知道的是，为了使一切能正常工作，这台设备里有很多组件。这台烤箱不仅具有加热元件和恒温器、适当的绝缘以及烤箱具有的所有其他功能，而且还有收发器、CPU、一些存储器以及一些软开关和显示器。

这是一种威胁。也就是说，任何具有这些组件的东西都可能会受到攻击。那么，攻击者会做什么？好吧，如果成功了，攻击者可能会烧掉我的鸭子，或者在最坏的情况下，攻击者可能会发起协同攻击，在某个不方便的时间打开所有烤箱。假设某个地区因为天气炎热和空调运行而电力不足。所有烤箱同时打开会造成低电压。

此外，烤箱中的许多软件堆栈还被其他设备使用，例如空调、炉灶、收音机、门铃。因此，可能会同时启用大量设备，产生巨大的功率需求。因此，需要对该烤箱进行一些保护。

请播放下一张幻灯片。

请播放下一张幻灯片。

为了使烤箱正常工作 — 它不只是直接给我发消息。这是一张互联网图片，这是 KC 和她的团队在一段时间前制作的互联网的图片。

请播放下一张幻灯片。

实际上，要做到这一点，烤箱需要与云中的设备进行通信。就像门铃一样。这是一种常见的使用模式。

请往后退一页。谢谢。

实际上是云设备与她的 iPhone 通信。这是一种常见的模式。

为了使这些设备与云进行通信，它们需要使用域名系统。它们有一个基于云的端点。就像 cloud.example.com。它们就是这样通信的。

现在，为了让它们在互联网上的所有上游进行通信，必须通过最近的路由器来路由信息。

对于烤箱和门铃，我们正在谈论 WiFi。但还有很多其他方法可以做到这一点。但是，确实有很多是通过家庭，通过家庭路由器进行通信的。

请播放下一张幻灯片。

那么这是什么原理呢？例如，您会收到一个有关烤箱的查询 — 请放下一张幻灯片 — 查询“ovencloud.example.com”，返回了一个 IP 地址。IP 地址是来自特定地址的。现在，请回想一下克里斯蒂安所说的。这些设备大约有 200 亿个。互联网上有大量设备，但烤箱只需要与它的云端点进行对话，也许是几个端点，也许是家里的某些设备，但它不需要与所有设备进行对话。

如果 — 家用路由器可以提供控制点，并且该控制点限制了烤箱的威胁面。那么，这意味着即使烤箱中存在错误或漏洞，该控制点也可以防止它遭受大规模攻击。这是否意味着烤箱制造商在发现漏洞时不需要提供软件更新？显然不是。尽管有一些网络保护措施，威胁面仍然存在，但网络有助于减少威胁。

请播放下一张幻灯片。

这就是进入设备的通信，即已被 DNS 解析的云端点。为了使控制点发挥作用，它需要从烤箱接收查询和响应。因此，这意味着如果 DNS 查询被加密并且控制点不知道这一点，它将无法提供保护，也无法减少威胁面。

请播放下一张幻灯片。当然，门铃和许多其他消费类设备也会出现这种情况。

在工业界，情况略有不同。今天我重点介绍消费类设备的情况。我们看到各种不同设备使用各种不同云端点。

请播放下一张幻灯片。

那么，这一切意味着什么呢？这意味着我们需要 — 可以加密。加密 DNS 查询是有充分理由的，克里斯蒂安提到了很多。但是，如果控制点 — 如果您打算用来减少威胁面的网络路由器本身无法访问该查询，或者它没有以某种方式经过查看查询和响应通信的授权，那么该路由器将无法提供必要的保护。因此，DNS 和启用这种保护的路由器之间存在联结。IETF 已将这项工作标准化，作为一种提供保护的手段。

因此，我们并不是说不要加密。恰恰相反。我们说的是要加密。但在进行加密时，要确保是对经过授权可提供某些（听不清）的组件进行加密。

这是我的最后一张幻灯片。

亚力杭德拉？

亚力杭德拉 • 雷诺索： 谢谢你，艾略特。

现在有请利兹。

利兹 • 富尔： 谢谢。大家好。我想提出另一种观点，因为我来自电信行业，也就是互联网服务提供商 (ISP)。

请播放下一张幻灯片。

因此，我的演讲将围绕为何说 5G 和物联网是个有趣的话题。我想谈谈 5G 带来的新机遇，但我也想阐述人们围绕 5G 和 DNS 提出的一些担忧，并谈谈 5G 和物联网以及 DNS 对世界带来的改变。

请播放下一张幻灯片。

如果我们要谈论物联网，为什么说这相对于 5G 是个有趣的话题呢？这是因为我们作为电信公司，实际上认为 5G 是固定网络和移动网络的混合，而不仅仅是新的 4G 技术。这是一种更加融合的技术。因此，我们认为这实际上将促进物联网的发展，也是物联网发展的一个重要组成部分。

因此，您在这里看到的数字只是移动物联网的数字，甚至可能是一个很小的数字。2018 年，我们看到有 1.4 亿个移动连接 — 物联网连接，我们预计到 2026 年将达到近 7.4 亿。

5G 中有趣的新事物是什么？是窄带物联网吗？当然，未来还会有一些机器 — 一些 MTC 增强功能 — 这将在 4G 技术的基础之上得到发展。

因此，当我们展望 5G 时，它将是建立在 2G、3G 和 4G 基础之上的许多服务，而 4G 现在已经支持物联网。但新的物联网将在更大程度上基于 IP 基础架构，也在更大程度上基于 DNS 基础架构。

因此，目前我们所看到的并不是我们所说的物联网，它也基于 IP，但更大程度上基于其他服务。我们希望能够开辟 5G 物联网的新用途。而且我们认为这将是更好、更安全的使用方式。

我们看看这张幻灯片上的内容，物联网和 5G 物联网并不是在真空中发展的。它实际上建立在更广泛的服务组合之上。DNS 和 IP 通常将在这里成为联合者。

请播放下一张幻灯片。

而且，如果我们看一下 5G 移动和 DNS 的传承关系，那么 5G 从一开始就不会是独立的 5G。目前，我们看到的是，有许多基于 4G 基础架构的 5G 网络。因此，我们看到的是配备 5G 设备的 4G，但它并不是发展成熟的 5G 网络。

在这些移动核心系统中，DNS 和域名的使用并不普遍，但我们确实使用了大量的 DNS，但到目前为止，这是有限的。

当然，我们确实看到了依赖 DNS 进行路由的例外情况，其中 VoLTE 就是一种情况。但我们在移动系统中使用域名是为了什么呢？我们看到域间名称目前受到限制，它们是从旧 ID 衍生而来的，并且移动互联网访问是非特定的。这是对移动而言。

因此，在 DNS 方面，从 4G 到 5G 的使用没有什么新的方面，我们在 5G 中的使用方式与在 4G 中相同。请放下一张幻灯片。

那么，为什么说 5G 有趣，为什么它比 4G 有趣呢？我之前说过，这是因为这是一个更加融合的网络。它是一个虚拟化网络，将使用更多软件，对硬件的依赖程度低于 4G。它将是一个更加灵活的网络。正如我们所说，它将使用 IP native 协议。尽管由于 IPv6 地址太长，实际管理和运营 IPv6 地址是很棘手的，但由于 IPv6 的结构，我们仍然看到 DNS 在这方面被大量使用。

我们还看到，我们的域间将是 IP native，并且我们将以管理网络的方式逐渐将 IP 转换为域名。

在欧洲，我们仍然主要基于线路交换进行互联，但我们认为，借助 5G，我们将拥有更多的 IP 互连。这就是 5G 网络运营方式演变的方式。

请播放下一张幻灯片。

因此，如果我们要看看域名的使用将如何实现，从本质上讲，它对用户是透明的，这意味着对于用户而言，我们使用 DNS 的方式是不可见的。因此，我们与网络交互主要是出于技术目的，并且网络将嵌入设备中，因此其使用不应与域名绑定。因此，名称并不是其中非常重要的部分，但 DNS 技术当然是。

同样，在物联网上，如何实施是真正的关键，因为我们的实施方式实际上定义了其设置。因此，尽管我们发现 5G 并非 — 我们不认为 5G 将成为新的二级注册的重要来源，但我们实际上认为这将由更多的子域来定义。因此，我们预期不会出现域名的使用激增，因为它被定义为更多地使用子域。这其中的许多内容实际上并非在互联网上解析，而是将被解析为域间或域内名称。

请播放下一张幻灯片。

那么为什么我们认为 5G 对物联网、互联网以及 DNS 有利呢？首先，我们认为，正如我所说，在核心网络级别，我们将拥有更多的软件，这将使窄带中的机器类型通信更灵活、更轻松。通过 5G，我们能够以更简单的方式定义网络。在安全性方面，网络切片对我们而言至关重要。网络切片将是网络的一部分，我们可以在其中为这

种特定使用类型定义切片。例如，作为巨大物联网的自动驾驶汽车将需要非常低的延迟频带。因此，为自动驾驶汽车提供一种服务非常重要。

此外，我们认为 AI 的使用实际上将开放我们的网络标准，既可以促使它们变得更好，也让我们能发现网络是否存在任何威胁或问题。我们认为 AI 将极大地提高我们的工作效率，并以更好的方式发现问题。

回到挑战问题，请翻到下一张幻灯片。

如果我们看看所面临的挑战以及如何缓解这些挑战，会发现网络切片非常有用。有人担心这会造成互联网碎片化。我们认为这根本不是问题。我们认为，这就像 VPN 一样，而且 — 它是面向最终用户的更具针对性的服务，不会造成互联网碎片化。

如果我们看看域名和避免冲突，我们使用的是公共域，我们认为这不是问题。如果存在用于内部路由的任何域，则它将是一个公共域，并且在这方面不会产生任何冲突。

在 DNSSEC 这个重要方面，这将是一个机遇。这不是标准 — 这目前不是 5G 的强制性标准。我们还没有看到将 DNSSEC 作为 5G 网络标准的需要，但未来将使用它。

然后，在 5G 网络中，对于拒绝服务以及 DDOS 攻击和僵尸网络，我们当然可以处理这些问题。但是有加密趋势。而且，如果您要监视这些攻击，我们需要能够看到流量。

因此，在拒绝服务方面，如果我们要积极参与这项防御工作，那么我们就需要能够看到流量。

请播放下一张幻灯片。

那么，我们该何去何从？关于 5G 的标准化，还有许多悬而未决的问题。我们只是在建立 5G 网络。而且，我之前说过，到目前为止，我们还没有看到很多独立的 5G 网络。因此，我们目前正在构建的是具有 5G 组件的 4G。

基础架构很昂贵。因此，正如我所看到的，5G 并不是发展成熟的独立设备。5G 并非指日可待，因为（听不清）这些网络的商业案例非常昂贵。

最后一件事是，我们实实在在地看到了 COVID 危机，这对我们所有人来说都是可怕的危机，但我们看到，全世界都非常关注数字化需求。我们看到了对安全性的关注加大。

因此，从这个角度来看，我们看到人们越来越意识到基础架构很重要、安全性很重要，并且我们看到网络的使用得到了增强。因此，我们认为未来的出行将减少。我们今天在这里。这是一个很好的例子，我们都没有外出参加 ICANN 会议，而是远程参加。

关于物联网，我们也认为，当然，这场危机也会促使建立更多的远程监控和更多的物联网。

这就是我的发言。谢谢。

亚力杭德拉 • 雷诺索： 非常感谢利兹。

现在有请克里斯蒂安。

克里斯蒂安 • 黑塞尔曼： 好的。谢谢亚力杭德拉。

我要换个角色。我之前 — 我之前代表 SSAC。现在，我要代表 .NL — 请翻到下一张幻灯片。

.NL 是荷兰的注册管理机构。我们是欧洲的一个小国。不过，我们可以起步了，因为上周我们达到了 600 万个域名的界线。这真的很棒，值得在线庆祝。

但是，我们要做的重要事情之一就是 — 我们的重要任务之一就是我们旨在提高互联网的安全性和弹性，正如大家在幻灯片中看到的那样。这就是为什么几年前我们决定开始致力于物联网的原因，以解决我之前在讨论演示文稿的“机遇、风险和挑战”部分时谈到的一些挑战。

下一张幻灯片讲述了我们开始这样做的原因。其实就是是 2016 年发生的 Dyn 攻击，DNS 运营商受到了发送大量流量的僵尸网络的攻击。僵尸网络是成千上万受感染的物联网设备，并且它同时向其特定目标发送大量流量。结果，它导致 Twitter、Spotify 等流行服务中断。

因此，当我们看到这种情况时，我们认为，我们是 DNS 运营商。对于荷兰以及整个互联网来说，我们都是至关重要的基础架构，因此我们希望对此有所作为。也就是在那时，我们开始开发 SPIN 原型。SPIN 是家庭网络安全性和隐私性的首字母缩写。

该系统的目的主要是进行监视 — 因此，您可以将设备放置在家庭网络中，或者像艾略特所说的那样，通过附加的安全功能来增强家庭网关。然后，此功能将监视您的本地网络是否存在任何 DDOS 流

量，例如，查看是否有迹象表明您家中的某个物联网设备已被僵尸网络感染，比如将加入其中一种大型 DDOS 攻击。

然后，我们将尝试使该设备与互联网暂时断开连接，以防止互联网基础架构受到这些 DDOS 攻击。可以说它就像是反向防火墙。

这是我们在 SIDN 开发的一些示例。该系统目前处于原型阶段，尽管去年我们对该软件进行了投资，以使其达到生产水平，因为我们想要的是帮助 ISP 以及帮助消费类设备制造商也能在其设备上使用这些类型的功能。但是事实证明，这比我们想象的要困难得多，因为它是一个与我们习惯的 DNS 生态系统不同的生态系统。

而且，可以说，这是一个不同的业务生态系统。因此，例如 ISP，至少对于与我们沟通过的 ISP，他们正在努力确定应该在多大程度上帮助其客户解决未经认证的物联网设备的安全性问题。他们有点不太乐意，因为这类附加服务会给他们的支持造成负担，例如，会带来额外成本。这就是使这类系统难以部署的因素之一。

另一个因素是设备制造商，他们基本上 — 如果其客户（也就是 ISP）要求，他们基本上会添加这些功能。因此，其中也存在鸡与蛋的问题。

但是，我们确实知道这是一个重要的问题，因为如果您 — 至少在欧洲，如果您看看荷兰国家电信监管局，他们有一个关于物联网安全性的特定计划。在欧洲，人们也正在尝试一些举措 — 欧洲内部不同的电信监管机构都在尝试扩展无线电设备指令，这是我们针对任何无线电传输设备的法规，通过基本物联网安全要求来扩展这些规范。可以这么说，这表明从公众的角度来看，这是一个重要的问

题。但是，在行业中，尤其是在 ISP 世界中，会有更多的吸引力。可以说，世界的连接无处不在。

请播放下一张幻灯片。

您刚刚看到的软件是开源的。您没有看到软件。您看到了图片。如果需要的话，URL 在下面。

我们开发的具有相同原型的另一个示例是提高物联网透明度。您可能还记得，我之前曾说过，DNS 有机会以直观、易于使用的方式为用户可视化 DNS 查询。我们开发了一个原型来说明这一点。这就是您在此屏幕上看到的内容。

总体上，灰色圆圈是网络中的设备。我认为最上面的是一部手机，因为它连接了很多设备。

而蓝色和绿色形状基本上是这些设备连接到的远程服务。这是一个屏幕截图。

实际的应用程序是非常动态的。您会看到 — 实际上，您会看到与远程服务的交互会弹出。因此，这是基于对 DNS 查询的分析。

我还要补充一点，SPIN 是一种可保护隐私的解决方案，因为它将所有测量和分析保留在家庭网络中。因此，它不会与云服务或类似的东西共享这些信息。

好的。这些就是我们正在尝试用来解决 SSAC 报告中提到的挑战的系统的两个示例。

然后，我还有一个示例，在下一张幻灯片中。

最后一个示例其实是关于几年前的 ISOC，即所谓的协作安全性。多个组织在共同努力保护互联网，这对于互联网至关重要，因为互联网是一项重要的协作。因此，如果要保护它，就需要协作。

我们所参与的示例之一就是您在此处看到的内容。它称为 DDOS 信息交换机构。其目的 — 目前是一个集中式系统，使人们可以共享他们在其系统上处理的 DDOS 攻击的摘要。因此，他们获得入站流量。他们会生成一个指纹，并与该组中的其他运营商共享该指纹，以便其他运营商知道发生了这种攻击，这样他们就可以准备基础架构，以防成为下一个攻击目标。

因此，这实际上是关于主动预防。对于受害者，为时已晚。这仍然是反应性的。对于该组中的其他运营商，这是主动的，因为他们掌握了有关其他服务提供商可能遭遇的 DDOS 攻击的更多信息。

因此，这实际上是一个信息层，可以附加在现有 DDOS 缓解基础架构之上，而不是替代它。这是一个附加系统 — 在顶部添加的分布式系统。

我们目前正在荷兰进行相关试验。有一个密码，我忘记说了，它叫做 nomoreddos.org。去看看吧。那里有一个博客提供了更多信息。

我们目前正在探索 — 我们目前正在荷兰进行一项试点，该试点本身就是一个名为 CONCORDIA 的大型欧洲项目的一部分，总体上是关于网络安全。但是，该项目的四分之一实际上与这些 DDOS 信息交换机构有关。

我们认为 — 我们目前以全国性的方式组建了 DDOS 信息交换机构。因此，这意味着成员是来自荷兰的组织，例如政府、ISP、互联网交换、注册管理机构以及许多其他组织。例如银行。

也可以用其他方式进行组织。您还可以想象一个用于 DNS 行业的 DDOS 信息交换机构，例如，注册管理机构层级的 DNS 运营商，也许是注册服务机构层级的运营商将协作共享有关 DDOS 攻击的信息。

这些就是我想从 .NL 角度给出的三个示例，我们希望它们有助于解决这些问题 — 有助于解决风险并抓住我们在 SSAC 报告中谈到的机遇。

谢谢。

亚力杭德拉 • 雷诺索： 克里斯蒂安，非常感谢。

请播放下一张幻灯片。

现在是同行评审时间。我来介绍一下我们的评审员。首先是菲利普 • 富卡尔 (Philippe Fouquart)。他是互联网服务提供商和连接提供商选区 (ISPCP) 的代表。菲利普是 Orange Labs Networks 的命名、编号和地址领域的高级专家。自 2001 年以来，他一直负责 Orange Labs 的 NN&A 活动，以设计 Orange 的网络体系结构，并在此领域中向全球范围内的业务部门提供技术支持。

拉菲克 • 丹马克 (Rafik Dammak) 是一名计算机工程师，在东京大学攻读应用计算机科学硕士学位后在日本工作和生活。自 2007 年以

来，他一直参与公民社会和互联网治理问题，以演讲者或研讨会组织者的身份参加了多个互联网治理论坛以及其他与互联网相关的会议。

他的主要工作领域是 ICANN 决策流程，曾在非商业用户选区 (NCUC) 和非商业利益相关方团体 (NCSG) 中担任过不同职务，并致力于在 MENA 地区提高对互联网治理问题的认识。

金伯利 • 克拉菲 (Kimberly KC Klaffy) 是加州大学圣地亚哥分校的应用互联网数据分析中心主任。2017 年，她获得了 Jonathan B. Postel 服务奖，并于 2019 年入选互联网名人堂。她还是加州大学圣地亚哥分校计算机科学与工程系的兼职教授。她的研究兴趣涵盖互联网拓扑、路由、安全性、经济学、未来的互联网体系结构和策略。自 2003 年以来，她一直在 ICANN 的 SSAC 任职，并拥有加州大学圣地亚哥分校计算机科学专业的博士学位。

各位同行评审员，请发言。

我们可以从菲利普开始。

菲利普 • 富卡尔： 谢谢亚力杭德拉。能听到吗？

亚力杭德拉 • 雷诺索： 可以，非常清楚。

菲利普 • 富卡尔： 谢谢，也感谢我们所有的小组成员。我想讲一些我的收获和意见。艾略特介绍了一些用例，其中物联网本质上是为框架服务的设备，而不是设备对设备。我了解到有人认为，让本地网络属于物联网的网关不完全忽视传出和传入的 DNS 请求，原因是可以使用入口筛选来减少许多安全威胁。

利兹，您对 5G 移动网络中的两个维度之间进行了区分，一个维度是移动互联网上的物联网，以及运营商提供的物联网应用程序和服务。您说 5G 和切片对一个互联网、一个 DNS 不构成威胁（听不清）。在某些架构中，DNS 架构已在移动网络中使用，并且这些架构与我们所知的互联网上的 DNS 不同。所以其中并没有什么新鲜事物。

最后，克里斯蒂安讨论了通过 SIDN 的 SPIN 进行 IoT DNS 网关概念试验，以监控传出的 DNS 流量；特别是为了对抗 DNS 拒绝服务攻击。

这些就是我从他们的演讲中取得的收获。

我想对挑战提出意见或问题。物联网是一个复杂的参与者生态系统，这些参与者可能不参与该组织或不负责定义标准，例如，始终有一个非常普遍的问题，即您通常如何促进或执行项目目标的良好实践，尤其是 DNS。以及您如何与该社群的参与者联系。

因此，也许对我们的小组成员来说，或者是值得深思的，我希望了解更多有关如何 — 您在生态系统中的地位的信息，无论您是运营商、注册管理机构还是供应商。我们如何联系您，或者您可以联系设备制造商社群以推广这些良好实践。

谢谢。交回给您，亚力杭德拉。

亚力杭德拉 • 雷诺索： 谢谢菲利普。

关于您的问题，我想我们的专家会进一步考虑，我们也许可以先让其他评审者发言，最后再回来讨论您的问题，这样会比较好一些。

现在请拉菲克发言。

拉菲克 • 丹马克： 好的。谢谢亚力杭德拉，感谢小组成员的演讲。

我也想讲一些我的收获，并想了解一下范围问题。

因此，我认为一个重要问题是，这似乎超出了 ICANN 和 SSAC 的职权范围，但是由于 DNS 在这方面的技术或生态系统可以为物联网提供什么，这对我们来说是一个有趣的话题，但也许我能注意到的是我们谈到了不同的参与者，物联网参与者、生态系统和不同的参与者，也许他们 — 他们在改善安全性方面需要做些什么，我不清楚用户可能扮演什么角色。也许不是那么简单，但我们对用户的期望是什么？作为这些不同技术的消费者，我们需要他们具有什么样的意识？有时候，甚至他们也受到这些技术的影响，我的意思是，当我们谈论物联网和所有这些他们不是直接消费者的智能家居设备时。

我认为克里斯蒂安谈到了我们需要提供使用方面的帮助，用我的话来说，就是明智地使用 DNS 和最佳实践。我想根据 ICANN 自身的经验进行思考，例如当我们引入新 gTLD 和 IDN 时，我们具有关于普遍适用性的经验，这对于学习者（语音）— 而言是否有用或合适？或

者也可以通过某种方式来帮助传播或更多地使用有关 DNS 和物联网背景的更好的用法或最佳实践。

因此，我想知道克里斯蒂安是否可以根据他自己的经验以及他在 .NL 的工作经验，在此基础上继续发掘，看看是否有共同的领域，以及我们可以从该经验中学到什么。

我再说一点。很高兴听到关于 5G 及其在物联网环境中作用的更多信息。也许我们要了解如何在该领域使用 DNS。但希望利兹能够进一步阐述我们需要了解的有关 5G 的任何政策领域。

就说到这吧。这是我的看法。

谢谢。

亚力杭德拉 • 雷诺索： 谢谢，拉菲克。我之前说过，我们先让所有评审者发言，然后再回答问题。

有请 KC。

KC • 克拉菲： 大家好。是的，这些演讲很棒。真的很感谢他们所做的工作，并且我对 SIDN 正在进行 SPIN 工作特别感兴趣。

我想知道人们对于政府对此类活动支持的了解程度。我知道在美国，NIST 已在这一领域研究了多年，我认为他们希望帮助行业克服其中的一些问题。我所看到的是，物联网运动正在或将要迫使人们克服互联网体系结构中嵌入的许多基本安全性挑战，也许我们还没

有遇到过失败的情况。而且，我们已经花费了大量时间和精力开发 DNSSEC 和 BGPSEC 之类的技术，其中标准组织尝试构建一种协议增强功能，以解决特定的安全性问题，但他们需要全球部署，而遗憾的是，全球部署尚未真正进行。

人们已经尝试了替代方法来提出操作实践，例如在 BGP 空间中，MANRS 代表“关于安全性的相互保证规范”。实际上，这是 ISP 世界中的一种行为准则，如果您执行这些特定的准则，则将减少我们无法克服的内置的路由安全漏洞的攻击面。这是技术手段。

我想知道小组成员是否可以谈谈他们认为在物联网领域中有价值的东西，因为在物联网领域中，甚至没有办法像我们在路由和命名协议时一样尝试创建技术覆盖，因为有许多不同的物联网协议无法互操作。因此，我希望了解大家在这方面的看法。

我的内容讲完了。辛苦了，伙计们。

我将聊天框内提供 NIST 工作的一些 URL。

亚力杭德拉 • 雷诺索： 非常感谢 KC。

那么，专家们，谁想先开始？

艾略特 • 李尔： 我是艾略特。

亚力杭德拉 • 雷诺索： 请讲。

艾略特 • 李尔： 首先，所有评审者都讲的很好，感谢你们 — 以及在聊天室进行的精彩对话。这真的是一场非常吸引人的讨论。

KC 说的一点也没错，因为 NIST 花费了大量时间和精力来应对物联网安全性挑战，而且这些挑战多种多样。例如，NIST TR8228 讨论了管理物联网、网络安全实践和风险的注意事项。还有一份建议草案 SP1800-15，着眼于管理物联网中的拒绝服务攻击，重点阐述了制造商使用说明。

我再讲一点，那就是物联网不是 — 是一个非常模糊的概念。它涉及不同的垂直面。我们一直重点关注消费者，但是还有行业，有智慧城市，有医疗保健。我们要认识到，许多垂直面已经受到严格监管。

举例来说，FDA 监管所有的治疗性医疗设备，无论是否有互联网连接，它们都受到监管，并且他们对于设备的安全性会发表大量意见。其他关键基础架构也将如此。物联网触动了核工业。当然，这是受到严格监管的。

问题是，在许多其他领域，我们看到物联网的新用途可能受到更可靠的监管，对此需要什么样的法规或最佳实践。甚至消费者也有受监管的空间，但更有可能受到监管。

谢谢。

亚力杭德拉 • 雷诺索： 谢谢你，艾略特。

利兹 • 富尔： 如果可以的话，我想接着讲。

亚力杭德拉 • 雷诺索： 请讲，利兹。

利兹 • 富尔： 对于菲利普的发言，如何最好地解决不同参与者的问题，我认为 SSAC 的合作或报告是一个很好的例子，展示了我们作为电信公司如何利用这些信息回馈客户、企业对企业、政府和其他机构，并讨论最佳做法以及如何最好地确保安全性。因此，我认为在 ICANN 和 SSAC 之间进行的对话，在欧洲，我们拥有 ENIS（语音）和 ETSI。我认为这很重要。需要进行这样的跨界。作为 ETNO，我们实际上是在跨界并利用它。

对于拉菲克的发言，如果 DNS 和 5G 领域中有任何政策，那么欧洲目前有许多有关 5G 和安全性的政策。我们有一项新的安全法案，该法案也与 5G 有关，而不是特定于 DNS 的，但我认为 5G 发展的越多，实际上它也将更多地关注 DNS 和 IoT 如何被纳入安全性领域。

我们拥有所谓的 5G 安全工具箱，该工具箱主要是关于设备，但我认为这是一项重要的法规，实际上还将关注 DNS 领域。

对于 KC 的发言，在无法克服安全性问题上，这是事实。这是个不断发展的领域，由于技术发展的速度非常快，因此我们一直在处理安全性问题。

在欧洲，我们有 ANISA，这是委员会方面的安全机构。他们实际上已经建立了一个利益相关方安全小组，所有利益相关方都将讨论与安全有关的标准化。而且我绝对确定，关于物联网和 DNS 的领域也将成为此讨论的一部分。谢谢。

亚力杭德拉 • 雷诺索： 谢谢你，利兹。我建议我们 — 请讲。

克里斯蒂安 • 黑塞尔曼： 我想回应拉菲克关于用户角色的发言。

亚力杭德拉 • 雷诺索： 请讲，克里斯蒂安。

克里斯蒂安 • 黑塞尔曼： 我们尚未研究这一点。

我认为用户显然是等式的重要组成部分，因为这就是我们所做的一切的目的。我认为我们需要以某种方式授权用户在有意识地与物联网设备交互时更好地了解物联网中发生的情况，例如，可以将他们当前正在与互联网上的远程服务共享的一些个人信息可视化或展示出来。如果可能的话，这实际上可能引发对安全解决方案的讨论或客户需求，而 DNS 可能在其中发挥作用。

另外，我认为，从公民的角度来看，而且我也是最终用户，我认为，政府和其他政策机构也需要在其中发挥作用。我已经看到这种情况正在发生。例如在荷兰，荷兰电信监管机构在该领域非常活

跃。例如，美国的 NIST，我们也看到了与此相关的活动 — 关于我之前谈到的欧洲无线电设备指令。因此，我认为最终会出台政策，在该政策中，政府机构和 ICANN 等政策机构可能会为物联网设备上所需的最低网络安全级别制定标准。

谢谢。

亚力杭德拉 • 雷诺索： 非常感谢克里斯蒂安和所有人。

现在，我们将讨论“问答”部分中插入的问题。请注意使用“问答”窗格进行提问。聊天不会被读出来。

那么我们进入问答环节。里亚？

里亚 • 欧丹内斯： 你好，亚力杭德拉。安吉拉 • 玛尔塔朋 (Angie Matlapeng) 提出了一个问题：较小的物联网（例如与使用 DNSSEC 和加密来保护设备有关的可穿戴设备）可能存在解决存储问题的方法吗？

艾略特 • 李尔： 也许我可以讲几句。

亚力杭德拉 • 雷诺索： 请讲。

艾略特 • 李尔： 安吉拉，非常感谢您的提问。物联网在加密和存储使用方面存在几个挑战。首先，很明显，当您谈论消费类设备，尤其是其他小型设备时，存储非常宝贵。实际上，我与物联网开发人员就任何字节进行过辩论。

而且，如果您看看它们使用的堆栈，它们是专用的加密堆栈，OV SSL 是一个很好的示例，它们具有高度优化的加密堆栈。如果您看看开放 SSL 的大小，它的大小可能会超过一兆字节。而 OV SSL 的起始容量大约为 14 KB，您可以感受一下差异。

但是，对于物联网，还有另一种令人困扰的担忧，那就是这些设备，正如之前有人提到的那样 — 克里斯蒂安在其简介中曾提到，它们的使用寿命很长。

加密 — 加密世界经历了多年的变化。五年前、十年前我们认为可以接受的加密现在非常容易受到攻击。而且，如果您设想一下，将诸如井架和石油平台之类的设备放置在地面上达 40 年之久 — 不要想象。回想一下我们 40 年前的技术水平。现在，想想一下尝试更新设备以使用当前技术。已有 40 年历史的设备，想象一下更新有 40 年历史的设备。对于物联网而言，这是一个巨大的挑战。并没有简单的解决方案。

M.I.T. 的丹 • 吉尔 (Dan Gear) 曾发表过一篇精彩的文章，其中提到物联网设备实际上有一个自毁开关，可以使它们从网络中消失。显然，有时会发生这种情况，而有时则不可能。但这是值得深思的。这是一篇很棒的论文。谢谢。

亚力杭德拉 • 雷诺索： 非常感谢您，艾略特。我们还有一个问题。

里亚 • 欧丹内斯： 是的。下一个问题，来自阿努潘 • 阿格拉沃尔 (Anupam Agrawak)：您认为现有的标识符系统在物联网情况下是否能够满足隐私要求？

艾略特 • 李尔： 我认为您会看到很多人对此保持沉默，因为这是一个很难回答的问题。

克里斯蒂安，请讲。

克里斯蒂安 • 黑塞尔曼： 我们谈到了 — 实际上，我认为有两个部分。一是标识符系统，在这种情况下，我们正在谈论的是域名作为标识符。这可以加以保护以增强用户隐私。我们在早前的讨论就谈到了这一点。

但是，当然还有第二个维度，那就是您的设备与远程服务共享什么样的信息，对吗？因此，这可能与实际内容有关，但也可能与流量模式有关，因为已有研究显示，人们可以评估您家中将使用的设备类型。只需要通过查看流量模式，而不需要过多查看流量的内容。

因此，我认为如果要增强用户隐私，需要考虑各个方面。这与保护我们用于标识符系统（在本例中为 DNS）的消息有关。但这也与交换的实际流量有关，即您发送到远程服务或从远程服务接收以保护该信息的实际流量，无论是在加密方面，甚至在混淆方面，您都是在尝试隐藏与远程服务进行交互的设备类型。

我同意艾略特的观点，这是一个复杂的问题。

[笑声]

亚力杭德拉 • 雷诺索： 非常感谢艾略特和克里斯蒂安。艾略特，你要不要再补充一点什么？

艾略特 • 李尔： 我想回答尼戈尔的问题。他询问了对 I.P. 作为标准世界中物联网中 5G 的交付机制的挑战。

我认为 5G 面临一些挑战。原因之一是如何限制这些设备的威胁面？提供商如何 — 提供商限制威胁面的作用是什么？在基于云的世界中，网络控制点（本质上是一个数据包过滤器）与 DNS 之间如何进行交互？

我之前谈到的关于家中的问题也是 5G 社群必须解决的问题。我们已经开始进行这些讨论，但才刚刚开始。

亚力杭德拉 • 雷诺索： 非常感谢您，艾略特。

我们还有最后一个问题，因为我们时间不多了。

里亚，请讲。

里亚 • 欧丹内斯： 苏达 • 哈卓维奇 (Suada Hadzovic) 提了一个问题。如果我们有物联网云提供商，那么与 Mist、边缘、雾计算节点的关系如何？根据 NIST，雾计算节点是网关等物理组件。

艾略特 • 李尔： 好的。我想讲几句。

亚力杭德拉 • 雷诺索： 谢谢你，艾略特。

艾略特 • 李尔： 谢谢。我已经试过回答这个问题。物联网设备有不同的计算模型。

正如我在其中一个回答中所说的那样，如果可能的话，实际节点上的商品和服务成本 — 制造商会尽量将其保持在非常低的水平。

但是有时您想要 — 因此他们做的是将许多 Mule 功能转移到高度可扩展的云中。如果云 — 如果制造商或服务支持者需要更多，他们可以在扩展时添加更多。云对此非常有用。

云可能存在的局限是，当您需要本地功能时，可能存在延迟。这就是雾计算的概念。

我要说的是，这是一个需要更多探索的领域。在消费者空间中不会看到这种情况，但在工业空间中您会看到很多雾计算，那里有本地控制器，它们在本地处理和协调物联网设备之间的通信方面提供了额外的功能。

这在工业领域已经大量存在，但这也是一个成熟的探索领域。

亚力杭德拉 • 雷诺索： 非常感谢您，艾略特。

我想用几句话总结一下。对于我们而言，保持关于 DNS 与物联网的交互带来的机遇、风险和挑战的对话非常重要。

重要的是要意识到存在被动互动。这意味着用户不知道他们的设备正在发生什么。这是需要解决的问题。

隐私是一个问题，安全也是一个问题。这些方面存在一些挑战。ICANN 社群可以重点致力于深入了解这些风险和挑战，以及不同的社群组织和咨询委员会如何为促进物联网与 DNS 之间的更好的互动做出贡献。

我要感谢所有小组成员和评审员的打字和协作，以及所有支持本次全体会议的 ICANN 员工。大家辛苦了。

全体会议到此结束。非常感谢大家的出席。下次会议再见。

再见。

[会议记录结束]