ICANN76 | CF — ICANN 英才计划：ICANN OCTO 和 KINDNS 简介
2023 年 3 月 12 日星期日 — 坎昆时间 10:30 至 12:00

西兰努什 • 瓦尔达尼扬 (SIRANUSH VARDANYAN)：

大家好，欢迎参加 ICANN76 第二天的会议。希望你们都喜欢昨天的会议。我是西兰努什 • 瓦尔达尼扬，欢迎大家参加我们的技术团队和 IANA 团队的会议。他们会详细介绍所有这些缩写。

但在此之前，有一个简短的公告。我将担任本次会议的远程参与经理，本次会议将按照 ICANN 预期行为标准进行记录和管理。

这次会议期间，用聊天室中提供的正确格式在聊天室提交的问题和意见将会被大声读出来。如果想在本次会议期间发言，请在 Zoom 中举手。被叫到名字时，虚拟参会者将在 Zoom 中取消静音。现场参与者将使用物理麦克风。我们这里有两个移动麦克风。为便于其他参会者，请自报姓名，并以合理语速发言。

我们提供六种联合国语言的口译服务，我鼓励大家在就座前把耳机拿出来并使用口译服务。我们有一个很棒的口译团队。

我想介绍一下今天的主持人，首先是首席技术官约翰 • 克莱恩 (John Crain)，他和他的团队、戴维 (David) 和金 • 戴维斯 (Kim Davies) 将介绍和谈论 IANA。我们从约翰开始。约翰，交给你了。

约翰 • 克莱恩：

非常感谢。很高兴在这里见到大家。正如西兰努什所知，英才计划和新生代计划学员是我在 ICANN 最喜欢的小组，因为你们都是新面孔，有新鲜的想法等等。所以来到这里感觉很好。我是约翰 • 克雷恩。我是 ICANN 的高级副总裁兼首席技术官。我已经在 ICANN 工作

了几十年，甚至更长时间。已经有一段时间了。可以这么说，我是常客了。

我运营一个名为 IROS 的小组。你们在外面很少听说这个。这在很大程度上是我们内部的区别。我们是缩略词小组。我们喜欢缩略词。IROS 是标识符（关于域名、IP 地址、所有 [over] 标识符）研究、运营和安全。前面的“I”是重要的。我们都在关注标识符以及它们发生了什么。

你可以把它分成三种不同的模块。我们有一个名为 IANA（互联网号码分配机构）的小组，由我左边的这位先生金 • 戴维斯管理。我们有一个小组，专注于技术问题的参与，由一位先生管理，他是我的朋友，名叫阿迪尔 (Adiel)，但戴维就在我右边。进行大量的研究。我的两个经理负责这方面的工作。我看到其中一个人非常害羞，躲在社群中。嗨，莎曼内 (Samaneh)。你为什么不 … 如果你愿意，你甚至可以加入我们。我没有看到马特 (Matt)，但我知道 — 马特在那里。如果我们愿意，马特也可以来加入我们，或者他也可以害羞地呆在那里。由你决定。

现在这些就是我们所做的事情。我们围绕影响标识符的所有事物进行研究。IANA 链从运营角度管理其中的许多标识符。然后我们出去谈论那些事情。

我不想花时间向你们说教，所以我会给这些人一些时间来谈谈他们正在做的事情。我从可以说是 ICANN 所做的最重要的事情开始，因为你们在这里参加政策会议，但政策只有在你能够真正落实并实际管理这些标识符时才重要。交给金了，如果你愿意的话。能给我们介绍一些关于 IANA 角色的内容吗？

金 • 戴维斯： 我简单说几句，因为我实际上有一个演示文稿，我一会就会演示。IANA 的作用本质上是作为我们在互联网上使用的所有标识符的中央信息交换中心和记录存储库。我想这里的大多数人都知道域名。当我们谈论互联网标识符时，它们通常是最常想到的，但绝不是唯一的标识符。你们可能也很熟悉 IP 地址，但实际上有成千上万的标识符用于启用日常互联网通信，而你们可能不知道。为了让互联网发挥作用，需要有一些集中的地方，集中分配这些标识符，以便在世界范围内一致地完成。这实际上是 IANA 职能的核心所在。我们稍后会谈到这一点，但简而言之，这就是我们所做的。

约翰 • 克莱恩： 好的。“R”代表研究。莎曼内或马特，可以谈谈你们的团队所做的基础工作吗？

莎曼内 • 塔嘉利 (SAMANEH TAJALI)： 我是莎曼内 • 塔嘉利扎德胡 (Samaneh Tajalizadehkhoob)，我领导首席技术官 (CTO) 办公室内的安全、稳定与弹性 (SSR) 研究小组。我们的大多数主题与 DNS 安全间接或直接相关。可能是你们在 ICANN 会议上经常听到的一些主题，即 DNS 滥用以及 DNS 的安全性配置，所有影响名称的间接因素也会影响滥用 — 例如网络钓鱼、恶意软件、命令和控制、网络安全性、协议安全性等。

现在交给马特。

马特 • 拉森
(MATT LARSON)： 我是马特 • 拉森。我还运营一个研究团队。有时我们会做安全性工作，但不像莎曼内的团队那样始终专注于安全性工作。我们的工作有很多。我们处理一些大数据集。我们非常幸运能够访问 ICANN 管理的根服务器的流量。所以我们以此为基础进行研究。我们还仅根据 DNS 的内容进行研究。我们可以访问所有 gTLD 区域文件和一些 ccTLD 区域文件。这些也是要处理的非常丰富的数据集。我们在标准领域也很活跃，尤其是 IETF。因此，我们还将对协议进行澄清和增强，并制作与操作相关的文档。

约翰 • 克莱恩： 戴维，你可以谈谈合作工作吗？

戴维 • 胡博曼
(DAVID HUBERMAN)： 当然，嗨。大家早上好。我是戴维 • 胡博曼，在我们称为技术合作的部门工作。我们的员工基本上是来自世界各地的工程师，他们与技术和非技术社群合作，与 RIR 一起培养良好的 DNSSEC、安全路由以及 RPKI 角度方面的能力和技能。我们致力于就与 ICANN 相关的主题进行互动，尤其是与非技术社群的互动，以确保每个人都对支撑互联网基础设施的工程以及互联网的构建方式有良好、深刻的理解。我们与 ICANN 的许多朋友和同事密切合作，在政府和非技术社群内努力确保每个人都在谈论关于互联网工作方式的相同语言。

约翰 • 克莱恩： 概述得很好。

我请大家在一分钟内看看这些问题，因为你们对我们的了解已经足够多了，但在我开始之前，会议室的 IROS 员工能否站起来，让大家知道该去询问谁？

好的。我们有很多人在参加 ICANN 会议。员工比这多得多，但我们带了一个小团队来参加 ICANN 会议，这样我们就可以与社群互动并在这里开展工作。收到你们的意见很重要。

现在交回给我的同事，我们看看是否有任何问题。

西兰努什 • 瓦尔达尼扬： 谢谢约翰。这次会议是为英才计划和新生代计划学员专门计划的，所以我鼓励大家积极提问，因为这对你们所有人来说都是一次难得的机会。你们中的许多人都是著名的技术人员，但从技术角度了解 ICANN 的运作方式非常重要。所以，请务必不要害羞。正如我在第一场会议上所说的，从来没有愚蠢的问题。所以请尽管提出问题，我们甚至可以现在开始。任何你感兴趣的内容。我们有麦克风。请拿两个麦克风过来。我想我们确实有 [它们]。大家请举手。好的，麦克风来了。请给我们两秒钟。

好的，请讲。在这儿。你能来拿麦克风吗？然后从这里开始。

尼古拉斯 (Nicolas)，我们等会让你发言，好的。谢谢。

哈里什 • 乔德里 (HARISH CHOWDHARY)： 大家好。我是 ICANN 英才计划的学员哈里什 • 乔德里。我是印度国家法医科学大学的一名研究学者，我的研究是围绕 DNS 安全性进行的。我的问题是，对于研究团队，我可以如何做出贡献？因为我专门从事 .in ccTLD 安全性和相关测量方面的工作。那么我怎样才能为

工作做出贡献呢？我如何从团队中学习新技术，以便对这两者都有帮助？谢谢。

约翰 • 克莱恩： 莎曼内，你想回答这个问题吗？

莎曼内 • 塔嘉利： 好的。谢谢约翰。感谢你的提问。很高兴和大家一起在会议室。事实上，我知道一个事实 … 我不知道你们是否知道 ICANN 的 DAAR 项目，该项目已经存在四年了。它的全称是域名滥用活动报告工具。.in 是该项目的一部分。我们已经与 .in 进行了某种合作。如果您能提供便利，如果我们能一起合作，如果您能提供有用的数据或谈论它，我想听听您的意见，您研究什么类型的安全性主题。如果您需要，指出正确的方向。但我们围绕 TLD 安全性做了很多工作，所以应该有一些领域我们可以指导您，或是对您有某种帮助。

约翰 • 克莱恩： 好的。如果可以的话，我们还发布了很多文档，我们称之为 OCTO 系列。如果你们认为其中某个很有趣，并且你们认为它很好，或者认为它很糟糕 — 希望永远不会那样 — 请写信给我们。请发表意见。请抽出时间去与莎曼内或这里的任何团队成员交谈。我们一直在寻找可以合作的人，看看我们是否在做正确的研究，或者是否有办法改进我们的研究。

西兰努什 • 瓦尔达尼扬： 谢谢。尼古拉斯，请讲。你是下一个。

尼古拉斯 • 费玛莱利 (NICOLAS FIUMARELLI)： 大家好，我来自 ICANN 的 OCTO 团队。路由安全不是 ICANN 使命或目标的一部分，但您最近提到了 RPKI 及其对路由安全的重要性。那么，您如何才能明确路由安全与 ICANN 的工作的契合点呢？

此外，如果路由安全确实是 ICANN 研究的一部分，我很好奇大公司和流行应用程序的基础设施的弹性。例如，几年前，Meta（前身为 Facebook）发生了一起涉及 DNS 和 BCP 故障的事件。像 Meta 这样的公司如何处理路由安全以及他们采取哪些措施来确保基础架构具有弹性，您能发表一些见解吗？感谢您抽出时间发表见解。

约翰 • 克莱恩： 好的，这涉及很多问题。我来尝试回答一些问题，从第一个简单的开始，即路由是否在 ICANN 的职权范围内？ICANN 与 DNS 无关。ICANN 是关于标识符的。如果您认为路由对 IP 地址来说就像解析对 DNS 来说一样，那么显然我们对此很感兴趣。

现在，当我们处理有关 DNS 的事务时，我们的合作伙伴 — 因为 ICANN 是社群的一部分 — 往往是注册管理机构、注册服务机构和解决方案提供商。在 IP 地址领域，我们在这些讨论和研究中的合作伙伴往往是 RIR（地区互联网注册管理机构），有时是 ISP 等。

这是与 DNS 不同的领域，但我们不只是做 DNS 方面的工作。

现在交给戴维谈谈其中的一些内容。

戴维 • 胡博曼： 大家好。这是一个很好的问题，我们有时也会在内部讨论这个问题，因为我们永远不想超越我们的职权范围。但事实是，RPKI 和这个更大的路由安全理念，当互联网服务提供商和互联网路由的所有

参与者传递流量并传递关于他们是谁的公告时 —“嘿，这是我的网络；这些是我的服务。如果你想到达那里，请通过这些路由公告来找我。”— 三四十年来，这一直非常不安全。

现在我们正在保护它们。我们将它们保护在一个基础设施的后面，该基础设施有望预防你们有时会读到的许多事故和许多滥用行为。当然，作为一个行业，我们不希望你读到这方面的内容，因为我们不希望它发生，因为我们希望底层网络基础设施能够正常工作，这样当你获得建议时，你可以去你想要的任何网站，它可以正常工作，你不必考虑它。因此，我们拥有建立在其之上的这一层安全性，我们需要确保它做得好并且做得对。

与此同时，我们还必须认识到，整个名称和号码基础设施，当然在我们的职权范围内，都在这个安全基础设施的后面，在这个安全层的后面。如果它做得不好，我们就无法访问名称服务器和解析器，如果我们无法访问我们查看的各种组件，那就是一个问题，对吧？所以我们非常重视它。

你刚才专门询问了 Meta。你问，在 2021 年 10 月，Facebook 为何几乎一整天都完全不可用。原因是 DNS。这是互联网世界中的一个迷因，如果什么发生故障，那是 DNS 的错，因为显然，这通常是 DNS 的错。

在这里，Meta 有一个非常有趣的配置，他们对建筑物的物理访问，比如进入数据中心、进入 Facebook 办公室 … 他们使用胸牌，就像其他公司一样，对吧？但是整个系统都绑定到 DNS 系统。为了验证你的身份，它使用 DNS 来查找该信息所在的存储库，对吧？但里面出现了故障。内部发生了故障，连带着造成 DNS 不仅对世界而且对 Meta 内部的所有系统都不可用。这意味着，当你戴着胸牌进入一扇

门时，为了进行身份验证，它需要 DNS 来找到你。但它无法访问 DNS。这是一种非常有创意的突破方式。

我认为它不仅教会了 Meta，也教会了每个人真正思考，当你构建基础设施时，无论是企业 IT，还是许多人赖以访问或获取内容的巨大 WAN，你真的要考虑路由、授权、身份验证和 DNS 之间的相互作用。并且不要意外造成故障，这些故障会连带发生，让你成为一个无人能逃脱的孤岛。

这是非常有趣的事件，我认为每个人都从中学到了很多东西。

约翰 • 克莱恩： 如果大家环顾会议室，可能会在这里找到来自 Meta 的人。这是他们的网络和他们的问题，所以也许可以去听取他们的意见。

西兰努什 • 瓦尔达尼扬： 谢谢。为便于口译，请以合理的语速发言。

我们有一个来自 ICANN76 新生代计划学员的珊妮尔 • 麦克弗森 (Shanelle McPherson) 的远程问题。我们得在最后一分钟停下来，她的问题来自约翰 • 克莱恩的团队。“DNSSEC 部署情况如何，国家/地区 ISP 如何参与实施？”

约翰 • 克莱恩： 好的，首先，珊妮尔，听说你不能来，我很遗憾。希望我们将来能在某个地方见面。希望你继续申请参加 ICANN 会议，我们下次会面。

我首先请金谈谈这是如何整合到根中的，然后请戴维谈谈我们围绕 DNSSEC 合作所做的工作。金，你可以谈谈根吗？

金 • 戴维斯： 谢谢，约翰。我们尚未讨论的 IANA 职能之一是管理 DNS 根区。DNS 根区可以说是 DNS 中最关键的部分。访问 DNS 的计算机会首先在这里寻找他们正在寻找的地址。它包含有关存在哪些顶级域以及负责这些顶级域的服务器在互联网上的位置的权威记录。

我们管理 DNS 根区的部分职责包括管理保护 DNSSEC 根区的加密密钥。这是我们运营中特别涉及的部分。事实上，我们有很多资源专门用于 IANA 中的一项职能。原因很简单。DNSSEC 的工作原理实际上是拥有一个中央密钥，每个人都依赖该密钥来启动 DNS 查找流程。关键是以一种非常安全的方式保存密钥，并且以社群认可的可信赖方式保存，不会引入任何未经授权访问该密钥的风险。

我们这样做的方式是确保该密钥安全。这是我们职责的一部分。我们将其保存在几个高度安全的设施中。每三个月，我们就会去访问该密钥，以便通过我们称之为密钥仪式的非常公开的活动来使用它。我们带着社群。我们进行直播。这是一个非常公开的活动。但我们采取了一种方式，让安全专家可以监控和观察我们正在做的事情，并且可以从中得出结论，“是的，ICANN 遵循了一套很好的程序，这样做不会导致以未经授权方式使用密钥的风险。”每个人都满意地离开了。

正如我所说，这是我们运营流程的关键部分。我可以用一个小时的时间来描述它们是如何工作的。这是一个很有趣的话题。但这确实是 IANA 以及 ICANN 对 DNSSEC 安全的最基本职责之一。

但我注意到问题是关于 DNSSEC 背景下的 ISP。现在我要把麦克风递给戴维，让他谈谈这个问题。

戴维 • 胡博曼： 好的。在金的团队出色地确保 DNSSEC 在根区启动并运行之后，我们必须使用它。那么，我们如何使用它呢？那么，我们进入下一个级别，即顶级域：.com、.org、.museum。或者，在这里，我想重点介绍国家/地区代码。我们在墨西哥：.mx。因此，如果我们想在墨西哥为 .mx TLD 下的任何域设置 DNSSEC，我们会去注册管理机构 — .mx 的注册管理运行机构。注册管理运行机构签署他们自己的区域，并为其下的每个域提供 DNSSEC 签名和验证。

我看着观众席的时候，看到了我的同事尼古拉斯 • 安东尼艾罗 (Nicolas Antoniello)。尼古拉斯，他在南美洲的乌拉圭…尼古拉斯所做的是，他将到不同的 ISP 和不同的国家和地区顶级域注册管理运行机构那里去，他将与他们合作设置 DNSSEC 签名，向他们传授关于它如何运作的一切必要知识，重要的是，需要哪些工具来维护它。他可以与 ISP 合作，确保他们在解析器上进行验证，即当域经过 DNSSEC 签名后，他们可以验证他们的签名并传递它们。

因此，ICANN 在根级别工作，以确保所有内容都经过签名，并确保所有内容都可以使用密钥进行验证。然后，ICANN 还与 ISP 和注册管理运行机构合作，以确保他们拥有在下一级别提供 DNSSEC 所需的所有知识、所有工具和所有支持。

西兰努什 • 瓦尔达尼扬： 谢谢。

瑟隆吉 (Setondji)，你已经举手了。

谢谢贝蒂 (Betty) 帮我。

然后，奥利弗 (Oliver)，后面轮到你和菲鲁兹 (Firuz)。

瑟隆吉 • 洪赞吉 (SETONDJI HOUNZANDJI)： 我想用法语发言，谢谢。谢谢。我叫瑟隆吉。我是一名系统管理员，负责管理 Linux 服务器。我来自贝宁，但我住在法国。

我的问题关于 ccTLD。我对与 DNS 相关的一切都非常感兴趣，并且致力于研究如何保护 DNS 服务器。所以我的问题与 ccTLD 有关，因为大家知道，在许多国家/地区，ccTLD 和注册管理机构是由政府决定选择的。我们注意到，ccTLD 通常配置不当、管理不善。我的问题是研究是否有可能让 ICANN 审计所有 ccTLD，发布关于需要采取什么措施的规则。大家知道，目前很多 ccTLD 都没有实施 DNSSEC。那么 ICANN 做什么？

我希望 ICANN 能够采取强制措施。例如，你们可以对某些 ccTLD 进行审计，然后告诉他们，“你们没有及时更新，我们无法继续与你们开展业务。我们将派一名审计员。我们将强制实施某些措施，让你们可以更新。”因为，如果欧洲和美国的 ccTLD 受到保护，但非洲的却没有，那将成为一个问题。我们说，ICNN 是同一个世界，同一个互联网，所以同一个世界不应该有许多种互联网。

这就是我的问题。谢谢。

约翰 • 克莱恩： 好的，我把这个问题分成两部分。一是关于 ccTLD 环境状态及其技术状态的一些声明。你对此发表了一些有趣的意见，但我想私下讨论这个问题，因为我很想看看你有什么数据，因为作为研究人员和

科学家，我们对数据非常感兴趣。你发表了很多关于基础设施质量的声明，如果你有支持数据，我们很乐意看看。如果没有，我们想讨论一下什么是可见的，什么是不可见的。其中之一是你说很多 ccTLD 都没有签名。我认为这只是一个评判，因为有很多签名。所以我们可以进行数据讨论。

另一个其实不是技术问题，而是关于如何管理 ccTLD 的政策问题。现在，ccTLD 没有由 ICANN 或在 ICANN 内部制定政策，但 ccTLD 是国家/地区代码，它们有不同的机制。因此，ICANN 没有任何机制可以介入并强制执行该领域的特定政策。不存在这个机制。我们所做的是，我们与 ccTLD 进行了很多合作 — 我的意思是很多。戴维可以谈谈我们在 ccTLD 方面所做的工作量。

因此，像 ICANN 这样的论坛正是你可以来讨论这类问题和政策问题的地方。ccNSO 是许多 ccTLD 聚在一起处理所有这些类型问题的地方。他们在大多数甚至所有 ICANN 会议上都设置了技术日，他们会在会议上讨论这些问题。

因此，ccTLD 之间以及与 ICANN 之间有很多协作，尤其是我的一些员工在改进方面进行了很多协作，但我认为如果要让我们审计，我们需要该政策流程的所有权。该政策流程不在 ICANN 内部。

所以，不，在可预见的未来，不会出现 ICANN 可以走进 ccTLD 注册管理机构并进行审计的情况。根据政策制定的方式，有人可能会争辩说不应该这样，因为这不在我们的职权范围内。这不是我们的职责。

金，不知道你是否有什么要补充，或者 …

金 • 戴维斯： 好的。我认为这是一个很好的总结。我认为值得再次强调（因为在座的许多人可能不熟悉）通用 TLD (gTLD) 与国家和地区代码顶级域之间的区别。对于通用顶级域，像这样的 ICANN 会议上发生的大部分政策制定都是围绕设置运行 gTLD 所需的规则和要求以及它们运行的参数。ICANN 工作的一个重要部分是，一旦这些规则由社群决定，就实施这些规则，然后监督对这些规则的遵守情况。ICANN 有一个合同合规部门。gTLD 的每个运营商都需要满足特定要求才能继续成功运营。如果他们在很长一段时间内没有达到该标准，则可以使用补救措施。

你似乎正在寻求某种类似的安排，可能是针对 ccTLD，但对于 ccTLD，这是一种非常不同的关系。回到 DNS 的最初，回到 1980 年代，当时做出了一个决定 — 这个决定一直保留到现在 — ccTLD 确实归属于他们各自的国家/地区。ICANN 的职责相对有限：在该国家/地区寻找一个受托人，为该国家/地区的公共利益运营 ccTLD。这个概念是，在该国家/地区内将建立所有相关的监督机制，以确保该运营商保持责任感并采取必要的措施。显然，这是一个复杂的世界，任何许多不同的国家/地区都有许多不同的机制。有些比其他的更好。这很清楚。

我认为 ICANN 可以通过我们的技术合作活动和类似活动，积极促进能力建设的最佳实践，帮助告知 ccTLD 管理人员他们的义务是什么以及如何履行这些义务。它是 ccTLD 的一个强大的基本组成部分，它们在国家/地区运营，运营商没有完全控制权，但主要负责当地的运营方式。这意味着我们在 ccTLD 方面的使命和授权相对有限。谢谢。

西兰努什 • 瓦尔达尼扬： 谢谢。

有一些 [破坏] 吗？

好的。我们从这里再接受一个问题，然后再接受一个远程问题，然后我们让金做演讲。我们将继续 [糖果消消看]。

奥利弗 • 里斯特斯基 (OLIVER RISTESKI)： 你好，我叫奥利弗。我来自马其顿。我在内政部工作。我也是安全研究中心的一员。我的问题是关于最近我们在公立学校、机场、商场和交通中心收到带有假炸弹的电子邮件。我们部门花费了大量的资源。这种犯罪的追踪率很低。而且侦破/侦查这种犯罪的效率太低了。此外，这个问题在所有 [听不清] 巴尔干地区都很常见。有没有可能对这些问题进行研究？

约翰 • 克莱恩： 你似乎主要是在谈论网络钓鱼攻击等，以及恶意软件和类似的问题，这些都是令人厌恶的，是我们互联网上日常生活的一部分。是的，当涉及到域名系统时，我们可以围绕它进行研究。

莎曼内，你可以谈谈我们正在进行的一些研究吗？

莎曼内 • 塔嘉利： 谢谢你的问题，奥利弗，谢谢约翰。正如约翰所说，这是大多数互联网用户日常遇到的典型问题。目前我们 SSR 小组正在做这方面的研究。它将很快发布：确定方法或更有效的方法将网络钓鱼电子邮件分类为不同类别的垃圾邮件、恶意软件等。因此请继续查看我们的 OCTO 文档或出版物。我们计划发布我们的方法。首先要通过学

术出版物，但是一旦经过同行评审，就会发布这些方法。也许这些方法对在其他领域、提供商、运营商等中实施很有用。

约翰 • 克莱恩： 你还可以考虑其他事情。现在，如果你拥有国家计算机紧急事件响应小组 (CERT)，请确保他们是 FIRST 的成员，FIRST 是全球 CERT 机构。ICANN 本身实际上是 FIRST 的成员，FIRST 是紧急响应者的论坛。因此，请参与该社群。确保你的事件响应者在事件响应社群中，因为这不是任何人独有的问题。

你可以长期做的另一件事是投资于你的大学，培养人才，让整个国家理解所有这些问题，无论是研究还是事件响应，甚至只是良好的网络技能等，就像在技术网络中一样。这是你可以做的另一件事。

如果你真的主要对互联网使用方式的公共安全方面感兴趣，并且想知道如何影响或参与该领域的政策，我们有一个政府咨询委员会。这是 ICANN 流程中非常重要的一部分。在其中，他们实际上有一个名为公共安全工作组的工作组。因此，如果你的政府正在参与 GAC，并且他们对该领域特别感兴趣，那么他们可以关注并参与公共安全工作组。

现在，在 ICANN，我们专注于与标识符系统相关的技术滥用或安全威胁。并非你在互联网上看到的所有威胁 — 事实上，你在互联网上看到的许多威胁 — 都与你所做的工作无关。但这个特定主题始终是 ICANN 的热门话题。而目前，社群内部正在发生各种各样的事情。围绕成为注册管理机构和注册服务机构的意义以及需要如何应对 DNS 滥用展开了合同谈判。当前的合同规定必须接收报告并进行调查。这些不是合同中的确切内容，但我不是律师。但我们的合同措辞中缺少的一件事是这些人必须减轻滥用行为。我们在签约方机构

（注册服务机构和注册管理机构）的委托下开展工作。他们来找我们说，“我们想将此添加到我们的合同中，因此我们有合同义务减轻滥用行为。”目前正在进行讨论。

我们进行了大量培训。莎曼内和我们的团队在该领域进行了大量研究并发表了很多文章。这是我们非常感兴趣的事情。

如果有执法部门愿意与我们讨论教育和外展问题，我们很乐意与他们沟通。我们的员工会花很多时间与世界各地的执法部门沟通。我们的主要职责是向他们解释生态系统是如何运作的，有时还会在他们和生态系统中的其他人之间进行介绍、建立信任，如果你愿意的话，因为这对我们为每个人开展工作的能力至关重要。

所以来和我们谈谈吧，我们可以进行一对一的讨论，讨论我们如何帮助你的部门和政府更多地参与进来。

西兰努什 • 瓦尔达尼扬： 谢谢。

我可以请技术团队打开 IANA 演讲稿吗？

同时，我将提出远程参与者的问题。ICANN76 新生代计划学员罗慕洛 • 查金 (Romulo Chacin) 想知道不同的安全威胁缓解项目和计划如何在它们之间相互作用 — 我猜是它们之间如何相互作用。

约翰 • 克莱恩： 我们还有多久？我的意思是，如果你看看 ICANN 的核心职权范围，如果你看看我们的章程，如果你看看 ICANN 的宗旨，它非常清楚地表明我们必须关注互联网标识符系统的安全性、稳定性和弹性。那

不是人们的网站等，而是 … 你好。你好，邻居们。我在听 … 嗯，我在听声音。

所以在某些方面，它是我们所做的一切的核心。一切都与安全性相互作用。每次在 ICANN 作为员工以及作为社群成员的大部分时间，当我们审视某件事时，我们总是会牢记这一点。这对安全性有何影响？这对稳定性有何影响？一切都相互作用。

现在，在我们小组内 — 我向你介绍了 IROS 的一群人 — IANA 正在出色地完成其工作，他们一直这样做，因为他们很棒，这对系统的安全性和系统的稳定性至关重要。我们必须对标识符进行妥善的注册。然后我们进行研究、进行外展和教育。这就是我们所做的。但正如金所说，我们也遵守我们的合同。我们进行合同谈判。我们支持所有这些政策讨论。一切都会影响标识符系统的安全性和稳定性，因为归根结底，这就是我们的工作。这就是我们所做的。

西兰努什 • 瓦尔达尼扬： 谢谢。

金，请介绍一下 IANA 的工作。

金 • 戴维斯： 当然可以。这似乎是一个很好的机会，在我们进行讨论时，可以快速浏览一下 IANA 的职能是什么。大家在 ICANN 会议期间可能会听到很多这样的话。假如你知道“IANA”一词的含义，那么这个词就随处可见。这只是为了相对简要地概述 IANA 职能的组成。希望这也能有所启发。我们将在之后继续提问。如果出现任何希望我们详细说明的内容，请告诉我们。

我们已经谈了一点：IANA，互联网号码分配机构。尽管名称如此，但我们所做的不仅仅是号码方面的工作。我们也做名称方面的工作。我们做协议参数方面的工作。我们做各种不同标识符方面的工作。

从本质上讲，它是互联网上最古老的机构之一。回到互联网的最初几年，当它是一个研究项目时，当第一批节点在 1960 年代末和 1970 年代初连接时，有人需要记录哪些计算机连接到谁。这个角色最初是由一个名叫乔 • 波斯特尔 (Jon Postel) 的人扮演的。他就是视频中温特 • 瑟夫 (Vint Cerf) 右边的那个人。乔 • 波斯特尔从一开始就是 IANA 的个人化身。

后来，IANA 得名并成为 1980 年代被广泛使用的名称。IANA 得到了成长，不再是只有一个人。它成为了一个团队。

但归根结底，这就是它当时的最初目的，也仍然是它现在的目的：标识符的用途是什么，这些标识符的用途的权威记录在哪里？

因此，在 1990 年代，人们认识到 IANA 的具体职能和根区的管理确实需要一些更正式的结构，而不仅仅是一个学术人员（乔 • 波斯特尔在大学工作），这超出了他个人和他的团队的能力。整个 90 年代都在努力使这一点正式化，以认识到互联网的商业化、互联网的发展以及对 IANA 职能的日益增长的需求。

ICANN 的创建是为了成为 IANA 的大本营。这是它最初的职权范围。事实上，在 ICANN 有名字之前，它被称为新 IANA。ICANN 至今仍然是为了这个根本目的而存在。除 IANA 之外，ICANN 还有其他标识符职责，但 IANA 仍然是 ICANN 使命的核心。

现在的 IANA 是 ICANN 的一个部门，它负责维护互联网唯一标识符的注册管理机构（我在这里所说的“注册管理机构”是一般意义上的注册管理机构，不是域名注册管理机构，而是官方记录中的注册管理机构）。这些注册管理机构中的每一个都有不同的政策，因此我们团队的部分工作是根据标识符的类型和所涉及的情况应用这些政策。因此，当你听到“IANA”时，它指的是分配职能，即由 ICANN 内的 IANA 部门运营的官方记录保管职能。

那么，为什么需要 IANA 之类的机构来担任互联网的官方记录管理员呢？互联网不是不受任何集中控制的吗？计算机使用技术协议相互交流，这些技术协议必须相同，这样计算机才能相互理解。虽然内容是通过这些协议传输的，但这些核心协议是 TCP/IP 之类的东西，例如。

它们需要在每台设备上以相同的方式工作，网络才能运行，所以我们在 IANA 中所做的很多工作并不是你看到的协议，比如域名，而是在你的计算机和网络设备的较低层级运作的东西，以确保不同互联网设备之间的传输有效、准确，发送的文件附件在另一端以正确的格式接收，并且当你连接到服务时，你不会接到语音电话而没有连接到网站。诸如此类的东西。所以所有这些标识符都有一个特定的目的来帮助这种交流。它主要由软件供应商使用。软件供应商使用这些 IANA 分配来确保他们的软件能供互联网上的其他人使用。

所以目前这些职能由 IANA 团队执行。有多个不同的合同。老实说，合同相当复杂混乱，但尽管如此，现在有很多合同管理着 IANA 职能的执行方式。

本周你们可能知道或听到的另一个术语是 PTI。PTI 是 ICANN 的一个附属机构。可以把它想象成 ICANN 的一个子公司，它实际上执行

IANA 的职能。对于大多数意图和目的，PTI 不是一个重要的区别。2016 年 ICANN 多利益相关方移交时实施的一项保障措施是将 IANA 职能置于与 ICANN 不同但由 ICANN 控制的组织中，即 PTI。所以你们会听到 PTI。我的建议是：不要太担心 PTI 这个词。只需要知道，它是运行 IANA 职能的实体的正式法定名称。

日常运营？我们的运作方式与任何其他 ICANN 部门一样。我们大约有 16 个人，这就是我们的基本业务。这就是我们的工作。

那么更详细一点的 IANA 职能是什么？通常，我们将它们分为三个部分：协议参数、号码资源和域名。这种区分有点武断。这些部分之间有一些重叠。但对于有关 IANA 职能的高层讨论，将其分为这三个领域会很有效。

我要关注的第一个是协议参数，因为它们实际上是我们所做工作的最基本方面。协议参数。有数千种不同类型的协议参数。协议参数的分配即使不超过一百万，也有数十万。它们有很多。有很多。其中 99% 你们都没有听说过。其中 98% 我甚至都没听说过。有很多。其中很多用于非常特定的应用程序。除非你正在创建软件来做一件非常具体的事情，否则你可能永远不需要使用这些注册管理机构之一。但是对于在一个非常特定的行业中工作并围绕这些唯一标识符集之一部署软件的 5 名、10 名或 50 名员工来说，IANA 所做的工作是无价的。如果你想了解完整列表，可以在 IANA.org/protocols 找到一个索引，但那里有很多。

对于协议参数，IANA 发挥直接的作用，实施者通常是软件供应商和协议开发人员，他们直接来到 IANA，与我们的团队交谈，并直接从我们那里获得他们需要的分配。这是与域名和号码资源的主要区别，我稍后会讲到，因为一般来说，人们不会来 IANA 获取域名。人

们来 IANA 不是为了获得号码资源。相反，他们有分层分配系统，其中有中间人。不同的人有不同的职责。IANA 只是在分配故事中扮演一个小角色。部分原因是申请号码资源和域名的政策多了很多。

那么这些协议参数注册管理机构从何而来呢？其中绝大多数是在 IETF（互联网工程任务组）中制定的。这是互联网的主要标准化机构。是大多数互联网标准化发生的地方 — 不是全部，而是大部分。当人们在 IETF 中制定互联网标准时，其中的一个组成部分是制定 IANA 注册管理机构以符合这些互联网标准。

你们可能听说过 RFC。这是一个文档系列，其中发布了互联网标准。许多 RFC 创建、引用或修改 IANA 注册管理机构。它们包括有关 IANA 需要做什么以及需要执行的政策的说明。

稍微谈谈号码资源，对于那些不熟悉的人来说，号码资源通常指的是三个关键部分：第 4 版互联网协议地址、第 6 版互联网协议地址和 AS 编号。对于那些不熟悉 IP 地址的人，有这两种版本：v4 和 v6。但这些是分配给互联网上每台设备的唯一号码。你的笔记本电脑有一个。你的手机有一个。你家里的智能设备有一个。你的电视可能有一个。世界上越来越多的不同物品都拥有它们，它是用于从一个设备传输到另一个设备的唯一标识符。从本质上讲，通过互联网进行传输时，称为数据包的每个传输都需要有一个“发件人”地址和一个“收件人”地址。“发件人”和“收件人”是 IP 地址。

因为几乎有数十亿个这样的地址，你需要某种方法将它们聚合成一个大集合，以便于处理，这样网络工程师就不必单独输入每个 IP 地址。他们为此使用的方式是使用自治系统编号，也就是 AS 编号。我喜欢考虑 AS 编号的方式是它们有点像互联网的邮政编码。网络提供商将大量 IP 地址组合在一个编号下 — 一个 AS 编号 — 然后，当他们

谈论通过互联网向何处传输流量时，他们使用 AS 编号来代替，大大减轻了任务的复杂性。

我刚刚谈的是这些是什么。我想指出第 4 版 IP 地址 — 我们都用完了。几年前，我们提供了最后一个可用的 IPv4 地址。将它们分配到网络的地区互联网注册管理机构也大多不在了。所以 IPv4 的供应量很少，因此你们会听到有很多过渡至 IPv6 的倡议，它具有更大的互联网增长能力。

我刚才提到了地区互联网注册管理机构。对于那些不熟悉这个概念的人，我之前提到过，人们不会直接来 IANA 获取 IP 地址。作为最终用户，你的网络提供商会自动为您分配一个 IP 地址。他们使用一种协议，DHCP — IANA 在幕后处理的另一种协议。DHCP 会为每台设备分别分配一个 IP 地址。每个网络提供商，无论是你的 ISP 还是酒店会议网络，都有一组 IP 地址，供其设施内或网络上的人员共享。

他们从哪里得到积木？好，他们去地区互联网注册管理机构。有五个地区互联网注册管理机构。LACNIC 是墨西哥的地区互联网注册管理机构。对于其中的每一个，他们的基本业务就是将这些 AS 编号和 IP 地址分配给他们所在地区的网络运营商。而 RIR 从 IANA 获得分配。

最后，域名。我们在域名方面的作用是什么？我先跳过这个。那么，在 DNS 层次结构方面，域名空间中最关键的部分是根区。这是我们在 IANA 中所做工作的重要组成部分。大家可以在此图中的根下方看到顶级域。他们在此之前分配标签，二级域等等。

那么，我们在 IANA 中的主要职责是管理 DNS 根区 — 这是顶级域的权威记录 — 然后是所有与之相关的技术信息和管理信息，比如谁是联络点？运行该 TLD 的实际公司是什么？诸如此类的东西。所以我

们是这些事实的官方记录员。我们收到这些运营商的请求，要求对其 TLD 进行更新和管理更改。我们对某些类型的请求进行尽职调查。然后，一旦 IANA 认为对 DNS 根的任何变更都是合适的，我们就会发送这些变更，以在 DNS 根服务器中实施。

之前在回答问题时，我已经提到了这一点，所以我会讲快一些，但我们确实管理这个密钥签名密钥，这个中央密钥也保护 DNS。我们通过密钥签名仪式来做到这一点。我们以非常公开的方式这样做的原因是为了促进信任。我们可以在私下里做所有关于 DNSSEC 和确保互联网安全的工作，然后说，“嘿，我们是 ICANN。相信我们”，但更好的方法是让你们所有人都参与到这个过程中，让社群能够访问，保持可见。我们相信这能更好地促进信任，因为每个人都可以亲眼看见。他们可以审视他们所做的事情，来自世界各地的安全专家可以审视我们所做的事情，共同审视并说：“是的，它正在以安全可靠的方式进行。我们可以相信这个系统是有效的。”

我们还在域名中履行一些其他职能。我们运营顶级域之一 .int。这仅适用于国际政府间条约组织。它不适用于一般注册。我们还运营 .arpa。我将 .arpa 总结为技术管道。这是一个你可能永远不会直接看到的域，但它对某些互联网运营很重要。我们还运营一个标签生成规则集的存储库。这是运营国际化域名的注册管理机构共享并遵守最佳实践的地方。

这就是 IANA 运营范围的总结。显然，这是一个非常简要的描述。但我最后想提一下安全性。实际上，你们知道吗？我要跳过那张幻灯片。IANA 的其他一些方面。

我认为我们所做的一切都基于公正和中立。我们在这里是为了执行所制定的政策。我们可以以中立的方式提供建议。这就是我们本周

在这里参与的工作的一部分。我们非常注重绩效。有很多 SLA 规范我们的工作。我们一直在衡量我们所做的工作。我们不断报告我们所做的工作。所以这是关键。我们希望不断改进，这是我们工作的另一部分：持续改进。其中一部分是进行外部第三方审计，并且通常对社群负责。你们可以在 ICANN 空间了解 IANA 的许多监督委员会。

总而言之，IANA 负责维护唯一号码分配系统的注册管理机构。他们在那里是为了保持互联网的互用性。大多数 IANA 注册管理机构都非常简单。人们直接来到 IANA。你们可能从未听说过它们。它们非常简单，但也有一些复杂的、知名度高的。我们谈到了根区。我们谈到了保护根区的密钥。对于那些，IANA 是这些命名系统的全球根源。

这就是对 IANA 的简要介绍。谢谢。

西兰努什 • 瓦尔达尼扬： 谢谢金。谢谢你为我们提供了这么多信息。提醒一下我们的参与者，此 PowerPoint 演示文稿已上传到 ICANN76 网站上本次会议的详细信息下。如果你们想下载并使用它，请随意。

我们现在可以再回答几个问题。我们为此安排了 30 分钟。所以请不要害羞。

菲鲁兹，是的，我知道轮到你了。请讲，菲鲁兹。我看到戴维？好的。但我们会开始 …

菲鲁兹 • 阿齐莫夫 (FIRUZ AZIMOV)： 大家好。我叫菲鲁兹。我是 ICANN 英才计划的学员。我在等，我已经有两个问题了。我的第一个问题是关于 … 正如我们之前提到的 Meta 的问题，我记得 Meta 也有关于那个 Meta 子网的问题，是由另一个 ISP 公告的。这通常会发生。在我们国家，我们遇到了这个问题：我们分配给 DNS 的子网是由另一个 ISP 公告的。我们不仅失去了这个子网的互联网，也失去了我们所有用户的互联网。我的问题是，[听不清] 解决方案是否可以防止此类问题。并且互联网上的每个边界路由器都必须在路由表中安装 [路由] 之前启用 RPKI 检查。正如你提到的，我们如何才能在较低层（例如第 3 层）中防止它并保持稳定性？

约翰 • 克莱恩： 好的，这也是关于我们如何保护路由的讨论。你所指的通常被称为边界网关协议 (BGP) 劫持。

我交给戴维来谈谈这个问题。

戴维 • 胡博曼： 所以 RPKI 在某种程度上帮助解决了这个问题。有趣的是，你刚才描述的问题每天都在互联网上发生，有时一天发生多次。我们在国际互联网协会的朋友实际上建立了一个观察站来观察这些事件，他们每年测量 500-1,000 个这样的事件。这些自 1990 年代以来一直在进行。这不是什么新鲜事。其中一些是恶意的。其中一些是针对那些出于某种原因想要制造恶作剧的人。很多都是偶然的，因为多年来，构建互联网的工程师实际上是将配置手动输入路由器。我们是人，我们会打错字。我们会犯错误。如果你在路由器中犯了错误，

那将是非常糟糕的。RPKI 旨在帮助解决大部分问题，尤其是第二种情况，尤其是人为错误配置。RPKI 有很大帮助。

我喜欢 RPKI 的原因是，它不要求每个使用 BGP 的路由器都验证公告。事实证明，它实际上只需要世界上最大的传输网络就可以这样做，因为当我们共享路由信息时，从你的部门、从你的 ISP，到坎昆的 ICANN 会议网络，再到加利福尼亚的 Facebook，再到委内瑞拉或其他地方，所有这些数据包通常都会经过一个相当少的 — 大约 800 个 — 为这些数据包提供传输的大型互联网提供商。事实证明，如果只有这 800 家左右的提供商验证和签署路由，任何无效的东西都会被丢弃，流量也不会到达不应该到达的地方。

过去几年 RPKI 和安全路由的成功案例之一是被世界上 800 家左右最大的 ISP 100% 采纳用于验证数据包，这意味着，如果你运营一个网络或如果你监管一系列的网络，至关重要的是，这些网络为他们的路由前缀发布证书、ROA（路由起源授权），以确保所有人都能对其进行验证。

为了充分保护通道、完全保护通信，我们不仅需要 RPKI。我们还需要验证路径。一个数据包，当它离开您的设备并到达目的地然后返回时，会经过一系列中间网络，我们需要确保路径始终得到验证，以便 — 我们称之为中间人攻击 — 当我们不授权他们这样做时，没有人能拿走那个数据包并开始处理它。

工程社群 IETF 有一些解决方案。我们将继续开发和研究更好的解决方案，让每个人都能实施。这将是我们在路由安全领域安全之旅的下一阶段。

西兰努什 • 瓦尔达尼扬： 谢谢。

大卫，如果我们可以 … 然后是尼古拉斯。我知道你有一个关于 IANA 的问题。

大卫 • 蒙德拉贡： 大家好。我是来自 NIC 哥斯达黎加的丹尼尔 (Daniel)，高级网络工程师。NIC 哥斯达黎加负责哥斯达黎加的 TLD 域。我有两个问题。第一个问题是，ICANN 或 IANA 是否正在努力推行政策或技术，以使用 DNS 或 TLS 而不是 基于 TLS 的 DNS (DNS-over-TLS)？因为对于大多数网络工程师来说，这可能是个问题。

第二个问题是，从政治路由和安全角度来看，IANA 和 ICANN 对这个问题有何看法？

约翰 • 克莱恩： 第一个问题很简单。答案是否定的，因为它不在我们的职权范围内。我们研究这些东西。我们测量它们。我们对它们很感兴趣。在其他领域有很多围绕该影响的讨论。如果你正在做研究，正在查看 DNS 数据包，并且你想要进入数据包，显然你不能在 [DAAR] 和类似的东西之下这样做。你们可以进行争论。那样好吗？那样不好吗？我不知道答案，所以我只是从个人角度发言，因为在这类技术中，安全和隐私之间总是存在紧张关系。

所以我认为我们对 DoH 没有特别官方的立场。我们对此做了一些研究。

马特一直很安静，我想看看他是否还醒着，是否想谈谈这个问题。

马特 • 拉森： 我在。我醒着。是的，我们对基于 HTTP 的 DNS 和基于 TLS 的 DNS 做了一些研究。事实上，研究团队的保罗 • 霍夫曼 (Paul Hoffman) 从标准的角度为这些工作做出了贡献。我们实际上帮助制定了这些标准。

鉴于人们对隐私的总体兴趣不断增加，我认为我们不可避免地会看到这些协议被越来越多地部署。

然而，与此同时，它们的计算密集度和网络密集度更高，因为普通 DNS 只是一个用于查询的数据包和一个用于回复的数据包。也许这发生在 TCP 连接上，在这种情况下，会交换一些数据包来建立和断开该连接。

但是一旦你开始讨论向其添加加密，你就是在讨论与更多数据包的日益复杂的交互。回应大量 DNS 查询的提供商，如 TLD 运营商和根服务器运营商，对于这对他们的基础设施意味着什么感到有些紧张。如果突然之间，出现的每个查询都不仅仅是 UDP 上的一个数据包，而是需要建立连接并进行加密验证，那么这会更加密集。因此，大规模运行关键基础设施的人对此有顾虑和疑问。

但我认为，作为一个行业和一个社会，这就是我们要去的地方。我认为我们不可避免地会看到这些协议的部署增加。

西兰努什 • 瓦尔达尼扬： 谢谢。

丹尼尔，抱歉。我刚才叫你大卫。

尼古拉斯？我们再回答尼古拉斯的一个问题，然后戴维将为我们所有人介绍 DNS 和域名安全的知识共享和实例规范 (KINDNS) 项目。谢谢。

尼古拉斯 • 费玛莱利： 谢谢。我认为上周我实际上参与了最后一次 KSK 轮转。这是一个与此相关的问题，但也与 [听不清] DNSSEC 相关。IETF 是否正在努力将后量子密码学纳入 DNSSEC 协议，尤其是在根区管理方面？鉴于 IETF 已经努力将后量子算法纳入其他协议，PTI 团队预计在 DNSSEC 中实施这些新算法会遇到哪些挑战，你们打算如何应对这些挑战以确保 DNS 系统的安全性和稳定性？谢谢。

金 • 戴维斯： 谢谢你的问题。截至目前，我们还没有积极关注任何后量子密码学计划，但我们正在做一些准备工作来改变根区的密码算法。目前我们使用 RSA-SHA256。我们实际上从未更改过该算法。目前尚不清楚更改算法是困难还是容易。实际上，我们在过去几周内组建了一个社群设计团队。他们将在两周后在横滨开会详细讨论这个问题。该设计团队的真正目的是研究如何更改根区中的算法，无论是后量子密码学还是其他东西，例如椭圆曲线密码算法，这将产生更小的数据包大小 [和] 其他有益成果。

我们正处于那个阶段。我认为现在开始考虑后量子密码学还为时过早。我们已经开始大致关注这个问题了。

但就该领域正在进行的活动而言，我要交给马特来谈谈研究活动，因为从我的运营角度来看，我认为后量子密码学目前更像是一项研究活动。

马特 • 拉森： 谢谢金。谢谢你的问题。我现在有机会参考一下约翰几年前提到的 OCTO 文档系列。我们实际上已经写了关于这一点的文件。我不在 Zoom 会议室，所以我无法粘贴链接，但它叫做 OCTO-031：量子计算和 DNS。这正是关于这个话题的。由于后量子加密受到越来越多的关注，OCTO 委托一位非常有名的密码学研究者对后量子进行研究并撰写了一篇相关论文。它的可读性很好，但它是一篇内容丰富的论文。所以我们做了一个更通用的版本，那就是 OCTO-031。其中给出了我们对行业状况的看法以及我们必须为后量子密码学担心的事情。我认为答案是：我们距离需要担心后量子算法还有很长很长的路要走，因为即使是可以对我们今天用于公钥加密的算法构成威胁的量子计算机，我们也还有很长很长的路要走。

我认为这是一个例子，说明这个行业有很多炒作，人们也在谈论它。只要看看行业刊物，你的感觉就是，“哦，我的天哪！这迫在眉睫，世界正在崩溃，我们都需要做好准备！”这并不意味着我们不必做好准备，但我们有数年甚至数十年的时间。这就是我们的立场：现在研究它还为时过早。我们有大量时间，因为我们距离拥有可能对当今密码学构成威胁的量子计算机还很遥远。

西兰努什 • 瓦尔达尼扬： 谢谢马特。链接已发布在 Zoom 空间的聊天室中。请大家打开它，并阅读文档中的详细信息。

同时，我想请戴维谈谈 KINDNS 项目。

戴维 • 胡博曼： 谢谢，西兰努什。我想在今天剩下的几分钟内转换话题，我想告诉大家我们在 ICANN 正在做的一些工作，关于尝试帮助改善互联网技术状况的工作。

我昨晚出去吃饭了。我和一个朋友去了一家餐厅，我度过了非常愉快的时光。在为我们提供晚餐时，服务员做了一件我认为对于服务员是噩梦的事情。他在给我续杯时把我的酒倒在我身上，把我身上淋湿了。发生这种情况时，我认为我们作为人类可能有两三种不同的反应方式。我们可以很生气，说：“什么？！你在干什么？！”然后大吵大闹，这对每个人来说都很难堪和尴尬。我们可以坐在那里不作任何反应。或者我们可以采取更好的方法，那就是我们可以大笑，我们可以微笑，我们可以说：“没关系。你只是犯了一个错误。别担心，我的朋友。”我们可以把糟糕的情况变成好事。

是的，所以我们昨晚就这么做了，服务员很好，我们都笑了，我们是朋友，没什么大不了的。没关系。那么我为什么要谈论这个呢？因为我们可以在 DNS 中做同样的事情。我们可以友善，我们可以通过采取某些行动，一些小的行动，对彼此友善，让每个人的生活更美好。

ICANN 创建了一个名为 KINDNS 的项目。它在一个网站上，KINDNS.org。该举措适用于所有 DNS 运营商，无论规模大小，无论你是 Google 还是 Facebook，也无论你是马其顿的全新小型 ISP … 无论你是谁，作为 DNS 运营商，你都可以采取一些措施变得更友善。如果每个人都更加友善，DNS 本身就可以拥有一个加强的改善的技术姿态。

在这个项目中，你被归类为一种运营商类型。你运行一个小型的私有递归解析器。你运行一个权威服务器来响应 DNS 名称和问题。或

者，也许你是一个公共解析器，你希望世界上的每个人都能够使用。通过 KINDNS 项目，你可以作为运营商进行自我评估，看看你的表现如何，根据社群（ICANN 和 DNS 技术社群）约定的一组规范进行判断，这些规范是一组基本标准，每个人都应该遵守，如果每个人都遵守，DNS 就能更好地运作。它会更安全，更稳定。因此，你可以针对这组规范进行测试，看看你的表现如何，得到一个私人结果，看看你处于什么位置，并且，在存在差距之处，你有机会填补这些差距。

这是一项仿照国际互联网协会的朋友在路由安全方面所做的工作。他们称之为具有良好的礼仪。我们称之为友善。通过这些类型的举措，整个社群可以努力为每个人创造更好的生活，并且只需采取一些非常小的措施，通常不需要花钱，也不会花费很多时间。它只是帮助你了解你的网络所处的位置，并做出微小的改变，以改进该网络并改进 DNS 基础设施，以便每个人都能受益。

这就是 KINDNS。因此，如果你们有空的话，不妨看看 KINDNS.org 网站。其中以简洁明了的语言介绍了我们认为每个人都应该遵守的一些社群接受的规范。

这就是我想与你们分享的全部内容。谢谢。

西兰努什 • 瓦尔达尼扬： 谢谢戴维。

来自 ISOC 苏丹的穆罕默德 • 努尔 • 阿卜杜勒 • 哈菲兹 • 法德尔 (Mohamed Elnour Abdelhafez Fadul) 提出了一个远程问题。“路径验证对全球路由表安全非常重要。引入了 BGPsec 扩展来解决这个问题，但由于 BGPsec 消耗的大量资源，它在可部署性方面面临困

难。需要研究以优化扩展并使其可部署。ICANN 在这件事中的角色是什么？”

约翰 • 克莱恩： 我们可以在这里扮演两个角色。一个当然是合作，另一个当然是参与研究。

现在交给戴维。你想回答这个问题吗？

戴维 • 胡博曼： 这个问题问得非常好。谢谢。正如我之前所说，通往安全路由基础设施的两条路径是 RPKI 和路径验证。问题非常正确地指出，我们已经有了解决方案。IETF 已经开发了一个名为 BGPsec 的解决方案 — 大概是 BGP 安全，对吧？但正如我们的朋友指出的那样，部署 BGPsec 目前不太现实，因为路由器的计算开销如此之大 … 我们不会破坏互联网。不，我们会做一些更糟糕的事情。我们会让它变慢。

因此，对于 ICANN，我们参与研究和参与其他解决方案，在某种程度上是马特的团队将做的事情，以及 ICANN 的其他团队在参与协议标准制定流程方面所做的事情 — 我在这里指的是 IETF。当解决方案问世时，我们当然可以衡量这些解决方案的影响。我们可以通过科学方式正式衡量它。我们可以通过我们与社群成员的对话和互动来凭经验衡量它。我们也可以成为讨论的推动者，尤其是在 ICANN 社群中更关注名称和数字，以了解影响、了解驱动因素、了解其中一些技术如何改善（或不改善）实地情况的动机。

约翰 • 克莱恩： 好的，谢谢你，戴维。

我想知道，会议室里有多少人实际上曾经参加过互联网工程任务组？

哦，很好。有几个人。如果你是技术专家并且对协议感兴趣，那是个不错的去处。如果你不是极客，在那里会很困惑。但对于我们当中的极客来说，IETF 是非常好的地方。

重要的是要记住 — 你听到这个消息会感到震惊 — ICANN 不运营互联网。ICANN 不开发互联网。我们不制定所有协议。这是一种伙伴关系。实际上是工程师和使用互联网的人组成的社群。所以很高兴在 IETF 和其他论坛中看到大家，而不仅仅是在这里。

我认为会议到这里应该结束了。大家还有其他问题吗？

西兰努什 • 瓦尔达尼扬： 我们可以再回答最后一个问题。

好的，请讲。阿菲法 (Afifa)，我看到你举手了。

好的。阿菲法，请讲。

阿菲法 • 阿巴斯 (AFIFA ABBAS)： 大家好。我是阿菲法。我是英才计划导师。两年来，我一直在指导我的学员。学员经常问我的一个问题是，在 ICANN 中，就网络安全新人而言，他们是否可以参与其中，他们可以在哪里自豪地说他们属于 ICANN 中这个特定的网络安全领域。作为一名导师，我很难回答这个问题，因为 … 你们可以介绍一下哪些平台可以让他们参与吗？因为，作为一名导师，我可以说有一大群人对网络安全非常感

兴趣。正如你所说，ICANN 英才计划就是要吸纳新人。我们不想失去他们，我也确信 ICANN 也不希望失去他们。那么我们如何利用他们在网络安全方面的才能呢？谢谢。

约翰 • 克莱恩： 好的，谢谢阿菲法。你好。看到回归的学员总是令人欣慰，尤其是当他们成为导师时。棒极了。这是一个有趣的问题，因为 ICANN 不是网络安全论坛，对吧？这不是我们所做的。但我们确实有一个安全轨道，在 ICANN 议程中，该轨道中的事情 [听不清]。

如果你现在正在寻求有关在 ICANN 内部更多地参与网络安全问题的建议，我们有一个名为 SSAC（安全与稳定咨询委员会）的委员会。你可以申请成为该委员会的成员。他们正在寻找经验丰富的安全专业人员。因此，如果你作为学员、经验丰富的安全专家来参加 — 因为你知道，我们确实有一些人作为学员在该行业工作了一段时间 — 那里就是你们要关注的地方。

我们有技术日。ccNSO 举办了一系列技术日活动，其中有很多安全方面的讨论。

当然，你可以随时来找我们，我们可以帮助你找到其他领域和可以沟通的人。

ICANN 的很多重要事情不仅仅是政策讨论中发生的事情。请记住，ICANN 是一个政策讨论论坛。这是关于标识符的策略，不仅是安全性方面的，当然也不仅仅是网络安全性方面的。但你在这里做的重要事情是在走廊和活动中与人们互动。

因此，如果你看到想要见的人 — 我不知道 — 你所在领域的人，无论是网络安全还是其他领域 — 请随时与你的导师沟通或来找 ICANN

员工，或坦率地在社群中说：“嘿，我对 X 话题真的很感兴趣，而且我发现这个人似乎非常精通这个话题。能给我介绍一下吗？”我们都会这样做。我们作为一个社群自下而上地共同努力。为此，我们实际上必须形成社群。

这是我能给你的最好的建议。有一个安全轨道，请看看那个。看看 ccTLD，技术日。与 SSAC 的人员沟通。与 RSSAC 的人员沟通。也就是根服务器系统咨询委员会。如果你是 ccTLD — 这里有人来自 ccTLD 吗？我知道有几个。请举手。

你做安全方面的工作吗？

你在 ccTLD 安全列表中吗？

如果你在 ccNSO，他们也有安全方面的工作。

所以没有一个直接的答案，这就是为什么你很难告诉他们。[将我们] 介绍给其他人。我们将与你进行一对一的讨论，看看我们是否能找出真正适合你的东西。问题是，你使用了“网络安全”这个词，它对不同的人有很多不同的含义。但我们很乐意为你提供帮助。

我认为莎曼内也想说点什么。请讲。

莎曼内 • 塔嘉利： 我想补充一下约翰已经说过的一点，这是一个有趣的问题，因为我们有时会讨论这个问题，但不是以系统方式进行讨论。我们过去也有实习生，还有 … 我们会开展项目 — 或大或小的项目。我们没有在内部讨论过这个问题，但我们是 … 无论如何，作为研究团队，我们确实有项目，我们确实希望我们团队内外的人提出想法或进行操

作。因此，如果你的学员对研究和开展项目感兴趣，请随时介绍他们联系我们，我们可以进行讨论，看看我们如何继续进行。

西兰努什 • 瓦尔达尼扬： 非常感谢。

说到这里，我要感谢我们所有的主持人 — 马特、莎曼内、戴维、约翰和金，感谢你们抽出时间。我知道你们的日程安排很忙，但感谢你们抽出时间来与我们、英才计划学员和新生代计划学员交流。他们热切地希望了解更多信息。

这里的人，我们的参与者，你们现在认识这些面孔了。如果在走廊看到他们，并且想问任何问题，请随时联系他们并提出你的问题。

在结束本次会议时，我想说：善待彼此。非常感谢。本次会议到此结束。现在可以停止录音了。非常感谢。

[会议记录结束]