ZH

ICANN81 | 年度大会 – GAC 与 SSAC 联合会议
2024 年 11 月 10 日（星期日） – 16:30 - 17:30（土耳其时间）

茱莉亚 • 莎弗琳 (JULIA CHARVOLEN)：欢迎参加 GAC 与 SSAC 的联合会议。我是来自 ICANN GAC 支持团队的茱莉亚 • 莎弗琳。请注意，本次会议会被录音录像，并根据 ICANN 预期行为标准和 ICANN 社群反骚扰政策开展工作。

在会议期间，在聊天窗口内提交的问题或评论会被大声朗读出来。本次会议的翻译服务包括所有 6 种联合国语言和葡萄牙语。如果您需要发言，请在 Zoom 平台中举手请求发言。请先说出您的姓名；如果您要用英语之外的其他语言发言，请同时说出您将使用的语言，并以合理的语速发言。下面我把麦克风交给奈杰尔 • 希克森。奈杰尔，有请。

奈杰尔 • 希克森 (NIGEL HICKSON)：大家下午好。大家今天已经听够了我的声音，是吧？所以，在这个会议上，我不会再多讲了。我保证明天我会保持安静。我先代表尼科 (Nico) 向大家表示歉意。他不得不去参加 ICANN 董事会的会议了。我却真的没什么事可做。大家可以看到，GAC 和 SSAC 的比例本就应该如此。不，这是 SSAC 的会议。

我们非常高兴有机会听取他们的简报。多年来，他们为 ICANN 的有效运转做了大量的工作。我相信你会发现他们所说的非常有趣。我会在以后处理这些问题和争论。而我现在要做的就是，把麦克风交给拉姆。

拉姆・莫汉 (RAM MOHAN)： 非常感谢。谢谢你邀请 SSAC 与 GAC 召开联合会议。很高兴和大家见面。我叫拉姆・莫汉。我是 SSAC 的主席。在我开始会议议程之前，先有请坐在这里的我的同事们花点时间做个自我介绍。他们都是 SSAC 的成员。大家将有机会在这里体会到知识、经验和专长的多样性。先从我的右侧开始。

罗德・拉斯穆森 (ROD RASMUSSEN)：罗德・拉斯穆森。

梅丽克・凯奥 (MERIKE KAEO)：梅丽克・凯奥。

格雷格・亚伦 (GREG AARON)：格雷格・亚伦。

罗伯特・盖尔拉 (ROBERT GUERRA)：罗伯特・盖尔拉。

沃伦・库马里 (WARREN KUMARI)：沃伦・库马里。

约翰・莱文 (JOHN LEVINE)：约翰・莱文。

史蒂夫・克罗克 (STEVE CROCKER)：史蒂夫・克罗克。

塔拉 • 瓦伦 (TARA WHALEN)： 塔拉 • 瓦伦，SSAC 副主席。

巴瑞 • 莱巴 (BARRY LEIBA)： 巴瑞 • 莱巴。沃伦还担任更好的角色。

苏珊 • 沃尔夫 (SUZANNE WOOLF)：苏珊 • 沃尔夫，他有时在 SSAC 担任太多角色了。

拉姆 • 莫汉： 谢谢苏珊。我看到后面还有几个成员。大家会看到他们在举手示意。他们也亲临会场，和我们一起参加这次会议。南金曼 (Najman)，感谢你亲临会场。加布 (Gabe)，你刚才没有举手。你应该举手的。好的。感谢大家的参与。考虑到不是你们所有人以前都见过我们，所以我们先花点时间介绍一下自己，我们是谁，做什么，然后再进入其余的主题。

看看 ICANN 自己的使命，这是相当清楚的。而 SSAC 则是根据 ICANN 的使命直接授权成立的。所以，我们是咨询委员会，就像你们是咨询委员会一样。在 ICANN 的结构中，我们并没有一种正式的权力。我们喜欢这种方式，因为我们的建议必须根据其自身的价值而生或死，而不是根据有无表决权，是吧？这就是我们。

我们是由世界各地的人们，至少是世界大部分地区的人所组成的。我们有着共同的目标，在衡量多样性的所有方面，我们都在增加成员的多样性。仅今年一年，我们就增加了 9 名新成员。在这九名新成员中，我们非常高兴地看到其中两名来自非洲和世界其他地区。不过，人们被选中加入 SSAC 的根本原因在于，他们带来了各自所

擅长领域的具体和深厚的专业知识。SSAC 中的大多数人都是技术专家。

他们拥有各种经验。有些人接触过互联网标识符系统的各个领域。我们主要是从这些人身上汲取灵感。大量的知识和专业技能都留在了 SSAC 内部。这是因为我们主要致力于为所服务的社群提供技术建议。因此，我们试图让一群掌握专业知识的技术人员加入进来。谢谢。

这是 SSAC 的领导团队。在我的左边，在大家的右边，你会看到被选中的成员和被选入领导团队的成员。这些也是政策支持人员。我想花点时间谈谈这个。与 ICANN 的许多其他部门不同，在 ICANN 的其他部门中，支持人员最终扮演的是支持角色，而在 SSAC 内部，你可以看看这里列出的人员，例如史蒂夫 • 盛 (Steve Sheng)，他们都是各自领域杰出的专家。

他们最终参与进来，为我们的讨论做出贡献，而不仅仅是做一名抄写员。当我们就感兴趣的各种主题开展工作时，他们通常会提供非常有用的指导和有用的建议。观察这个领导团队的技能，你会发现这是一系列技能的集结。再看看整个 SSAC，种类则更加繁多。

我们中的一些人来自学术界。一些人来自公民社会，具有商业背景、政府背景、执法背景。人们一般是通过开放申请流程最终进入 SSAC。他们先递交申请。SSAC 内部有一个成员委员会，成员委员会对申请进行分类，然后进行面试。一旦面试结束，他们就会推荐人加入 SSAC。

SSAC 随即开始对这些人发表意见。当我们完成所有这些程序后，我们会向董事会提供一份推荐成员名单。每个 SSAC 成员都是由 ICANN 董事会任命的。我接下来将邀请塔拉来谈谈这个话题，因为这是我们工作的核心。

塔拉 • 瓦伦 (TARA WHALEN)： 谢谢拉姆！对于那些不了解 SSAC 的人，我们制作了大量的技术材料，几年来我们一直在这样做。主题可能会有所变化。它们涉及有关互联网标识符的安全性和稳定性的一系列主题。但有些主题会一遍又一遍地出现，几乎是我们永恒的话题。因此，我们正在寻找关注这些主题的方法，并使这些材料随时可供社群使用。

随着这些反复出现的重要主题的发展，大家可以在我们这里找到问题的答案。在我们概述的这些主题中，其中之一就是 DNS 滥用。当然，DNS 是一个重要的系统，这也使其成为大量网络滥用的滋生之地。对于想要制造巨大伤害的人来说，这是一个有用的工具。因此，如果有人在进行网络钓鱼攻击，有人在分发恶意软件，那么我们就要看看 DNS 是如何参与进来的，以及我们可以做些什么来缓和这一局面。所以，在这一领域，我们经常会发布建议，并与委员会合作，试图减轻伤害。

许多期待进入下一轮工作的人可能会想到的第二个领域是新 gTLD。每次要将新的域名添加到系统中时，都会涉及安全性和稳定性问题。例如，人们可能一直在关注域名冲突分析项目，想要了解当有一个扩展时会发生什么。我们不希望在字符串上出现混乱。所以，很多工作都是为了预测这些问题。这是一个非常及时的问题，人们要求我们就这一主题提出建议。

此外还有 DNSSEC。这是 DNS 领域的核心安全技术之一。我们和其他人一起，已经在这个领域工作了一段时间，目的是提供建议，推广这项技术，努力确保它不断推广和实施。我们认识到这项技术很复杂，人们经常需要一些帮助才能试图让它按照预期的方式工作。因此，我们希望确保人们能提出好的建议。例如，提升自动化水平，更便于人们采用这种安全功能，并使其随时可用。

除此之外，还有替代域名空间的问题。最近几年，随着区块链频上热搜，人们可能已经发现了这一问题。这个问题肯定不会凭空消失。但是还有许多其他命名系统与 DNS 中提供的不一样。人们正在为加密货币做一些事情，并允许你购买不同种类的域名，这当然会产生一些问题，那么它是如何与 DNS 交互或集成的呢？我们将如何预测这些系统共存产生的各种问题？我们会继续关注这个方面，因为这是一个不断发展的领域。

最后，在座的许多人可能会想到的一个话题就是互联网治理问题，尤其是围绕安全性和稳定性的问题，这是我们小组的工作重点，因为互联网中的许多问题都同时涉及技术和政策领域，且在这两方面错综复杂。如果你要在这个领域做出决策，在制定政策时，从技术人员那里得到明确而有用的指导会大有帮助。

我们希望我们能够从技术角度提供这些信息。但同时我们也注意到，如果我们能够从那些需要建议来引导正确工作方向的人那里获得意见，我们的工作就会日臻完善，就可以确保我们有的放矢地回答问题，确保我们以适当的细节、有效的沟通传递相关信息。

因此，当我们在提出一些建议时，我们非常希望能够与人们互动，或者与之交谈，邀请专家与他们磋商，从而在政策领域为受众发挥

作用，这在很大程度上是一种合作，使我们能够提出对受众有帮助的正确建议。

现在，我们有几个工作小组正在开展一些工作。顺便说一下，我们的工作可能会跨越多个领域。目前正在实施的两个计划涉及 DNS 基础设施中的免费开源软件。有些人可能知道 DNS 基础设施中推出了许多组件，例如，解析器中的组件，这其中的许多组件都是开源计划的一部分。所涉及的这些群体或大或小，资金数额不同，可能有不同种类的债务、合同协议以及与不同方的关系。这是运行 DNS 的关键基础设施部分。

我们认为，有必要让人们明白哪里存在依赖关系，这样人们就可以知道这些开源软件在哪里，你在什么地方依赖它们，并且还可以就人们对这些软件的一些假设提出质疑，明白他们能做什么和不能做什么，以及对这些软件的可靠性和优势有什么想法。

现在，会场里至少有一位主席。马丁 (Martin) 不在这里。目前有一位主席在场。只是想请您核实一下我说的是否正确 - 主席给了我一个大拇指，说明我正确地总结了工作小组。这项工作才刚刚开始。因此，如果你对开源软件感兴趣，我们希望你们中的一些人能够一探究竟。我们正在研究的另一个方面是 DNS 拦截和过滤。在线拦截内容的机制之一，就是使用 DNS 作为管理最终用户和资源之间内容拦截的方法之一。

这作为一项技术，已经存在一段时间了，SSAC 也关注到了这一点，但我们上一次发布建议大约是在十年前。自从我们上一次编写这方面的文章以来，技术领域早已发生变化，监管领域也发生了变化。所以，我们认为是时候重新审视这些内容了。

例如，在技术方面，许多 DNS 查询现在是在传输过程中运行的，这使它变得不那么明显。人们不能像以前那样看待查询了。因此，这可能改变了人们在弄清楚如何拦截内容时的反应和获得的信息。

在这个领域，我们肯定会一直与政策领域的人进行沟通交流。我们很荣幸在最近与 ICANN 的政策人员进行了讨论，知道了在他们了解政策领域时，他们从所关注的方面听到了什么。我们非常感谢能获得这种类型的反馈意见，这样我们就能把控文档的编写方向，从而再次解决那些最紧迫的问题。所以，我们再次重申，我们很喜欢这种协作过程。

这就是相关主题的简要概述。我们确实还会更深入的展开，其他人将接替我在下一张幻灯片中详加介绍。

拉姆 • 莫汉： 在看下一张幻灯片之前，奈杰尔，我想知道我们是否需要花点时间问一下大家有没有任何问题或意见。

奈杰尔 • 希克森： 对，谢谢拉姆。我正打算这么做，因为我们已经有了相当多的信息。非常有趣的是，话题比较稳定，因为它们都非常相关。在深入研究人工智能和区块链问题之前，大家有什么问题或观察结果吗？如果有，请大声说出来。丹尼尔 (Daniel)？哦，我们的朋友。有请欧盟代表发言。

杰玛 • 卡罗里洛 (GEMMA CAROLILLO)：谢谢奈杰尔。我是杰玛 • 卡罗里洛，来自欧盟委员会。简单评论一下。首先，很高兴看到你所说的大部分内容都是我们所关心的。也许我们应该更频繁地交流，比现在还要频繁。其次，我要简单提一个问题，因为我知道关于开源安全的工作刚刚开始或者说最近才开始，这是一个我们非常感兴趣的话题，我们是否可以精准定位，是否有时间重新建立联系，获得关于这项工作的更多信息。谢谢。

巴瑞 • 莱巴： 好的，下面由我来回答。我是巴瑞 • 莱巴。我是工作小组的联合主席，该工作小组将编写这份文档。随着工作的进展，我们很乐意定期向大家展示相关情况。我们希望这个特别的工作小组能迅速开展工作，在接下来的两次 ICANN 会议中，我们应该能完成这项工作。所以，也许接下来在西雅图会议上，我们可以告诉大家我们的最新进展。

杰玛 • 卡罗里洛： 那太好了，谢谢。

拉姆 • 莫汉： 在巴瑞刚才所说的基础上，我想补充一点，根据主席的决定，工作小组也有机会邀请专家或掌握信息的人提供相关简报，介绍工作小组正在做的工作。所以，巴瑞，也许在闭会期间也有机会这样做。

奈杰尔 • 希克森： 还有人要发言吗？好的，下个环节还有机会再提问。拉姆，请继续。

拉姆 • 莫汉： 非常感谢。现在让我们切换到下一张幻灯片。杰夫 贝瑟 (Jeff Bedser) 原本计划到场发言，但不幸的是，他感觉不太好。所以由我来介绍这个部分。我们认为，听听我们自己的成员对人工智能和 DNS 滥用的一些看法可能会对大家有所帮助。SSAC 作为一个委员会，尚未委托某个工作小组去研究这个主题，也没有在 SSAC 内部达成一致意见。

在接下来的几张幻灯片中，大家将会看到我们自己的一些成员提供的专业知识。所以说，这并不代表 SSAC 的意见，而体现的是我们在 SSAC 的一些成员的技术知识和专长。这就像一个早期的集合一样，有机器学习，然后还有人工智能。机器学习是一个子集。在这个子集中，算法从数据中学习，以做出预测或决策。而人工智能则包含更广泛的技术，使机器能够模仿人类智能。所以说，机器学习是人工智能领域的一个关键方法。

现在，DNS 滥用实际上可能是人工智能的一个很好的应用。这可能正是那些不惜以身试法或已经以身试法的人想要使用和利用的东西。因为人工智能，尤其是生成式人工智能，有很好的方法来创造新的文本、图像、视频和其他人工制品。比如，几乎能以假乱真的银行或者电商网站徽标。再加上生成式人工智能和机器学习的功能，以及机器学习中的模式识别，人工智能系统能够创建电子邮件、短信和其他提示，看起来几乎像是由人写的或者由人创建的。你做得越真实，锁定的目标就越有可能成为它的受害者。

同样，凭借生成式人工智能及其自身的能力，在过去，当你收到一封网络钓鱼邮件时，你几乎可以凭借一些缺陷、一些制作不正确的东西、语法错误、拼写错误、大写错误等来做出判断。而现在，不

仅所有这些在基础语言中做得很好，而且它还可以自动翻译成一大堆其他语言。这意味着问题的规模和范围在急剧扩大。

看看 DNS 滥用，到目前为止，大规模打击 DNS 滥用已使用模式识别、模式匹配作为主要机制。举例来说，你可以查看域名背后的信息，或者正在发生的特定级别欺诈背后的信息。NS 记录、主机名、与之相关联的 IP 地址、向谁注册了名称或资源以及注册管理机构和注册服务机构。你可以找到模式或者分析内容。可以查看 HTML 文件，可以查看模板，它们被重用，或者查看文件散列值，因为在过去，这都是人类完成的，具有可访问和可重复的模式。

而有了生成式人工智能，每个特定的域名或 URL 可以完全随机化。每一次发生网络钓鱼 - 四个小时内产生 100,000 次网络钓鱼，通常都会将名称添加到区域文件中。在过去，您可能会将一封网络钓鱼邮件发送给 100,000 个目标。而现在，你可以单独发送 100,000 条消息，每一条看起来都很真实，似乎是来自某一个人，由某一个人写的。这是引诱目标上钩的非常有效的方法。

对于滥用而言，人工智能还有其他哪些用途？我们看到人工智能最近也被用于假扮他人，创造和使用假身份、假账户、假评论。通过与注册域名和托管账户相结合，它也被用于制作非自愿的亲密图像，以及儿童性虐待资料 (CSAM)。还可以直接用于伪造，捏造数据、文件和图片。在某些司法管辖区，可以创建这些身份证明文件或其他文件。例如，你所在国家规定，必须提供身份才能注册域名。

而现在，不必大费周折即可生成身份。目前已创建的安全方法之一可以很快被绕过。你还会注意到，也许你已经注意到了，伴随所有这些内容的图像是由人工智能生成的，它们与内容链接在一起。你

会发现，有些图像看起来很真实，有些虽然不真实，但也比以前好多了。两年前或六个月前的同一套提示则可能会产生看起来不像是平面设计师生成的图像。

阅读这张幻灯片上的所有内容有点困难，但这是一份研究报告中的一些数据，它说明了使用生成式人工智能的滥用策略的运用频率。正如大家所看到的，最常见的是模仿，这也用于扩展和放大现有攻击和伪造等。我在上一张幻灯片中已经讲过了，但这张幻灯片会带大家一直看到最后。它目前正在被广泛使用。

正如这次演讲的前一位演讲者所说，生成式人工智能似乎正在生成越来越难以分辨的图像。随着我们深入探究这个幻灯片集 - 我们原本并没有尝试这样做，这就是它所做的。也许那里存在某种信号。尽管这种能力不一定会导致更复杂的攻击，但我们确实认为生成式人工智能有潜力扩大攻击的规模和范围。我们在这里说，网络罪犯将逐步整合这些技术。错了。我们应该说，他们已经整合了人工智能技术，并且已经在计划中使用了人工智能系统。这就是我们在广阔世界中所目睹的。 但这并不全是坏消息。除了图像，你还会看到现在形成的面部。这是我们要求它做的，同样，我们告诉引擎，用目前为止所看到的一切生成这个，这就是你所得到的。

因此，尽管人工智能机器学习可以用来扩大这些攻击的规模和增加频率，但人工智能实际上也可以非常有效地检测钓鱼电子邮件。事实是，人工智能生成的钓鱼邮件，至少以其当前的体现，在其当前的世代中，它们不同于人类生成的常规电子邮件。它们也不同于手动生成的网络钓鱼诈骗电子邮件。如果你将机器学习和自然语言处理结合起来，这就有助于生成式人工智能工具理解、处理，然后制

造出读起来像人类编写的真实文本。知道了这个技术的存在，你就可以部署人工智能去抓捕人工智能。这才是它真正的发展方向。

对于攻击媒介和策略使用人工智能来达到滥用的目的，即使不是所有人，很多人应该已经对此很熟悉了。政治上的虚假消息，轻而易举即可生成。你不再需要人类做那么多了。当然，以利润为导向的滥用和犯罪企业的规模化迅速发展，也随之而来。归根结底，网络犯罪与网络犯罪最终为犯罪者创造的金钱直接相关。人们在必要时会改变策略来确保利润。

所以，即使部署人工智能来捕捉这类问题，演变进化现象也仍在发生。人工智能本身的发展非常迅速。但总的来说，我们的观点是，这实际上是随着科技的发展而存在的相同威胁态势的延续。有些行动者决定使用技术，利用技术以某种方式获利，以某种方式赢得优势。实际上，我们的工作是确保我们与正在发生的事情保持同步，然后部署可以减轻乃至抵抗这些类型威胁的措施。

我刚刚谈到了人工智能和 DNS。我不打算在区块链和 DNS 上花太多时间。我们已经在 ICANN 内部的其他论坛上讨论过这个问题了。我们发布了一份报告 - SSAC123。今年 9 月，我们还在华盛顿特区举办的 2024 年 SSAC 研讨会期间主持了一场小组专题讨论会。那也是公开的。会议内容已经记录下来。已公开提供。这个小组涵盖了当今区块链领域的专家，还包括了 ICANN 首席技术官办公室 (Office of the Chief Technology Officer, OCTO) 的人员。

SSAC 和 ICANN 的 OCTO 之间正在进行大量合作，旨在确保我们在研究领域保持一致。我们并没有协调我们所做工作的确切产出，但我们努力确保我们的工作没有重复。

请切换到下一张幻灯片。至少从我的角度来看，这是最重要的幻灯片，也是 GAC 对大家的最大要求。随着时间推移，我们发现决策者尤其需要能力建设。他们希望了解重要的关键话题，希望那些真正知道他们在说什么并且能够以易于理解的方式谈论这些话题的人能给出意见，他们不希望只是滔滔不绝地说出一堆专业术语。我们有能力这样做，也有机会这样做。

我们还提供报告。我们创建报告。但这些报告往往长达几十页。我们目前正在将这些内容提炼成 500 到 1000 字的摘要，只有一两页，将内容汇总在一起。但真正有帮助的是，作为政策制定者，希望大家能告诉我们，对你们来说哪些才是最重要的主题，因为我们已经写了 126 篇论文，我们认为单纯编写这些内容的摘要没什么效率。请告诉我们哪些对于你们有价值，我们非常乐意与大家一起为各位及其他受众提供简报。

最后，我们真心希望与你们和你们的政府合作。大家可能正在召开关于安全性、稳定性和弹性议题的重要会议。毫无疑问，你们参加一些这样的会议，其他同事或其他决策者也会参加，他们虽然对实际情况了解不多，但仍可以就这个特定领域应该做些什么提出建议。然后，你可能会发现，政策解决方案和实际技术可行性并不匹配。我们认为，在你帮助制定政策时，该政策最好基于确凿的事实，即在你和你的政府帮助制定这些政策时有助于你了解情况的实际数据。

我们真心希望与各位一起打开这个渠道，提供我们所拥有的宽广而深厚的技术专业知识，而不仅仅是提供文档。现在我要把麦克风再交给奈杰尔。

奈杰尔 • 希克森： 非常感谢你的详细解释。就你最后说到的观点，我认为很明显，作为政策制定者，我们非常感激技术社群和其他 ICANN 部门给我们提出的建议。我清楚地记得几年前，当我们从新 gTLD 轮次和 SSAC 报告的其他问题角度讨论 DNS 滥用时，我不记得具体的编号，但我记得曾详细阅读过，您提出的关于 DNS 滥用的建议对我们在会议中提出的其他建议有一定的影响。

所以，我确实认为我们有很大的合作空间。我还可以思考一下人们对区块链和 DNS 滥用的极大兴趣，并就此开展工作。毫无疑问，我们将会在适当的时候再次讨论这个话题。非常感谢大家就这些问题找到我们。我现在将听取大家的提问和意见。有请荷兰的朋友。

艾丽莎 • 希维尔 (ALISA HEAVER)：谢谢。感谢你对 SSAC 所有工作的介绍。这应该是我所了解的，但我实际上并不确定 GAC 是否有联络人与 SSAC 联系，或者相反。如果没有，我想这已经很有帮助了。

拉姆 • 莫汉： 谢谢。我认为我们没有这样的正式角色。如果你愿意担任这样的角色，我们当然很欢迎。我们在 SSAC 内部做的一件事就是，任何人，即使是联络人，即将加入的联络人，最终都要经过同样的审查程序，这样他们才能成为正式成员并参与进来。你们具备丰富的专业知识。这会对我们的工作有所帮助。坐在大家面前的加布 就是 SSAC 的成员。在某些情况下，他发挥了非正式的信息传递作用，但肯定不是以正式的方式。

奈杰尔 • 希克森： 非常感谢你提出这个中肯的问题。答案应该是我们目前还没有。但我们肯定应该关注这一点，因为它确实让我觉得它很重要。我的意思是，这是一个非常透明的咨询委员会，论文广为人知。但即便如此，对你们正在做的工作有一些深入的了解可能也是恰当的。我戴不戴眼镜都没用。还有其他人吗？是你吗？伊恩？是的，有请。就在你前面。但首先是伊恩。

伊恩 • 谢尔登 (IAN SHELDON)： 抱歉，奈杰尔，网上正在排队。我只是想引起你的注意。我还是排在最前面。

奈杰尔 • 希克森： 那你就先发言吧。

伊恩 • 谢尔登： 谢谢拉姆。我是伊恩 • 谢尔登，来自 GAC 澳大利亚。谢谢你提供的帮助。我了解了大家丰富而深厚的专业知识。你应该知道，GAC 成员通常拥有相当广泛的职责。我们负责 ICANN 内部和外部的很多事情。因此，我很想听听你对于提供专业知识和支持的想法。职权范围有多广？我们谈论的仅仅是 DNS 问题，还是能够利用本论坛之外的一些专业知识？

拉姆 • 莫汉： 谢谢伊恩。这个问题很好。就 SSAC 本身而言，我们将保持在我们的职权范围和我们所拥有的范围内。但你可以与我们的成员接触。

如果这些成员愿意在 ICANN 领域之外的主题上帮助你们，你们两个都有更多的权利。

奈杰尔 • 希克森： 谢谢伊恩。我想先有请美国代表发言。然后我再去看一下排队列表。

伦纳德 • 豪斯 (LEONARD HAUSE)：我是来自美国国务院的伦纳德 • 豪斯。当生成式人工智能与 DNS 滥用相结合时，他们是否通过注册流程或在流程中的某个地方制定出任何最佳实践，他们由此可以更深入地挖掘，找到相关根源，无论是某种图灵测试还是类似的东西，如果你愿意的话，都可以在生成式人工智能变得松散之前完成并锁定它。这是就报告中关于该领域是否存在最佳实践提出的一个问题。谢谢。谢谢你在这方面的出色工作。

拉姆 • 莫汉： 谢谢。我不知道该如何回答。但我可以问问 SSAC 内部研究这个主题的专家，然后再回来告诉你。ICANN 内部至少应该考虑的一点是，如果生成式人工智能的情况属实，你可以在几个小时内将一个域名添加到解析中，这样就可以发出数量庞大的辱骂性消息。在 ICANN 内部有什么办法可以快速缓解这种情况吗？如果在几个小时内发生滥用，是否有可能在检测到它的几分钟内减轻其影响？我认为这是我们应当解决的问题。

奈杰尔 • 希克森： 非常感谢。谢谢你的回答。现在网上有两三个人。首先有请来自欧盟委员会的杰玛。

杰玛 • 卡罗里洛： 非常感谢奈杰尔。你询问了一些令人感兴趣的话题，我想在 GAC 讨论 DNS 滥用时，我们已经讨论了预测工具的使用。欧盟在这方面有一些经验。如果在采取缓和措施之前，我们已经掌握相关材料，或者可以利用预测工具的潜力进一步防止 DNS 滥用，那就太好了。然后，我只想澄清一点。如果我理解正确的话，通过使用人工智能和生成式人工智能，我们并没有真正扩大威胁态势。我想说的是，攻击数量可能十分庞大，但它们并没有变得更加复杂。我们没有受到更多的威胁，至少目前没有报道过。

拉姆 • 莫汉： 谢谢。对于第二个问题，是的，确实如此。我们认为威胁态势并没有扩大，但是数量、频率和规模显著扩大了。关于第一个问题，这里有来自 SSAC 的成员愿意对我们的同事作出回应吗？

加布里埃尔 • 安德鲁斯 (GABRIEL ANDREWS)：我可以从执法角度简要回答一下。我们看到的是非常相似的威胁团伙、相同的犯罪集团，他们手动操作，或者采用人工智能工具来提升效率，就像好人一样。所以，我们观察到的并不是什么特别新鲜的事物。这是同样的老把戏，只是使用新的工具来完成罢了，这实际上是我们现在可透过目前的可见性获得的一般信息。

拉姆 • 莫汉： 谢谢加布里埃尔。我认为你应该重申一下第一个问题，这样其他成员就能够注意到，然后或许能做出回应。

杰玛 • 卡罗里洛： 这真是太好了。非常感谢。我会尽可能清晰地表达出来。你刚才询问了 SSAC 的潜在工作主题以及可能对 GAC 有用的简报。在 GAC 中，当讨论 DNS 滥用时，我们有时会提到在进入缓和阶段之前，存在一些预测工具可防止 DNS 滥用。因此，我想知道你手头是否有相关材料，或者在这一领域是否可开展进一步的工作。谢谢。

拉姆 • 莫汉： 谢谢。有人想谈谈对此的看法吗？有请本尼迪克特和史蒂夫先后发言。

本尼迪克特 • 阿迪斯 (BENEDICT ADDIS)：大家好。我是本尼迪克特 • 阿迪斯。我没能登上主席台。有一些 DNS 滥用是很容易预测的。特别是僵尸网络和恶意软件使用高度可预测的算法来生成未来数周、数月和数年的域名。现在，这些域名已经不存在了。它们被称为 DGA 域。我们可以非常准确地预测它们。但我要提醒大家，对于任何声称使用魔法人工智能以更普遍的方式预测糟糕情况的工具，我都会非常小心。所以说，有些领域很适合预测。但这并不广泛。

拉姆 • 莫汉： 史蒂夫？

史蒂夫 • 克罗克 (STEVE CROCKER)：谢谢。为了运行预测流程，您必须能够快速、灵活地访问注册数据和注册本身。我想说，我们正处于一个严重泡沫化的时期，非常强调隐私，这是为了防止各种形式的骚扰、垃圾邮件等等。但与此同时，这使得出于合法目的访问数据变得很困难，介于困难和不可能之间，特别是出于某些目的，如进行预测分析和跨域关联。

因此，有一些棘手的难题需要解决，即如何提供对信息的访问，以便您可以做好必要的预测分析，同时还能保护隐私。这两个方面是相互影响的。

奈杰尔 • 希克森： 非常感谢。谢谢你提出的问题，这引发了一些非常不错的回答。我想接下来是我们来自印度的朋友桑托什。

圣 • 桑托什 (T. SANTOSH)： 谢谢奈杰尔。感谢拉姆 • 莫罕关于人工智能和 DNS 滥用的详细介绍。我们先从基础的方面说起。现在，人工智能可以帮助提高 WHOIS 的准确性吗？因为这是恶意行为者所涉及的基本问题，WHOIS 中大多数信息都是不准确的。我们能不能有一个系统，让人工智能工具可以分辨出这不是准确的 WHOIS，所以这个域名不能被授权？谢谢。

拉姆 • 莫汉： 谢谢。对于这个问题，你当然可以将人工智能或其他机器学习算法应用于数据库，并将它们与真实地址和人等进行比较，并得出某种程度的结论。但正如史蒂夫所说，这些数据现在大多模糊不清或不

可用。所以，即使今天存在这种技术并且可以使用，为那些工具提供信息的数据集也是无法获得的。

巴瑞 • 莱巴： 拉姆，我快速补充一点。不仅检查所需的数据不可用，训练引擎所需的数据也不可用。这是一个双重问题。

格雷格 • 亚伦： 我换一种方式来说。如果 WHOIS 中没有域名的联系数据，我们中的大多数人都无法获得这些数据，例如，安全公司、执法部门。但是，存在一些确实掌握数据的相关方，即注册服务机构和注册管理运行机构。现在，注册管理运行机构和注册服务机构使用各种方法进行准确性检查。比如，在荷兰，使用域名后缀 .nl。现在我们基本上有了注册服务机构，尤其是能够检查准确性和潜在网络犯罪的各方。

他们有 WHOIS 数据，也有购买数据，如用于注册域名的金融工具、源 IP 地址等等。因此，人们有潜力使用人工智能，它现在掌握在这些相关方的手中。

奈杰尔 • 希克森： 非常感谢。我们在聊天中还有两三个其他问题，我将继续讨论这些问题。我们还有七分钟时间，实际上是六分钟，因为我们还需要总结。我不是很清楚具体的顺序，但是马尔科，你为什么不进来呢？

马尔科 • 霍格沃宁 (MARCO HOGEWONING)：我会快速而简短地回应一下我的同事，非常感谢 SSAC 出席会议，也感谢你们向我们伸出援助之手。你问了一个简单但又很棘手的问题，我们认为什么是重要的？一切。这就好比挑选自己最喜欢的孩子一样，这真是一个很难回答的问题。我很欣赏 SSAC 的工作，尤其是帮助我们理解新兴技术对 DNS 系统和整个互联网稳定性的影响。但是，关于优先事项，退一步讲，一方面，我想知道 SSAC 是否也从这个意义上看待我们的一些全球对话和一些全球进程，例如，最近发表的《全球数字契约》。

至于你认为在哪些方面可以做一些重要工作来帮助我们所有人，同样，你是否认为 SSAC 有机会为这些正在进行的全球对话做出贡献，例如，WSIS 审核或几项 WSIS 行动方针也提到了系统的安全性和稳定性。谢谢。

拉姆 • 莫汉：非常感谢。互联网治理及其安全性、稳定性和弹性是我们持续关注的五个领域之一。我们肯定想参与其中。我们没有建立某种结构，通过这种结构，最终向这些领域派遣一名联络人或某个人。但我们现在有成员在关注这一点，他们在日常工作中直接参与其中。这为我们的工作带来了很多启示。事实上，这促使我们成立了开源工作小组，我们的一名成员意识到政府层面也对此有所关注。所以说，这可能是有用的。

巴瑞 • 莱巴：我来回答这个问题。基本上，SSAC 通过三种方式来决定要处理的工作。一是有一名或多名 SSAC 成员对此感兴趣并提出了建议。二是董事会要求我们查看某些方面。三是社群要求我们查看某些方面。

很明显，我们不能什么都做。但是如果有一些社群成员进来说，这对我们真的很重要，你们能看一下吗？这是一种可能性。

奈杰尔 • 希克森： 谢谢。我们还有其他几个问题。有请美国代表欧文。

欧文 • 弗莱彻 (OWEN FLETCHER)：嗨，奈杰尔。王朗应该排在我前面。

奈杰尔 • 希克森： 哦，好的。很抱歉。对不起，王朗。我搞不清楚具体顺序了。先生，请发言。

王朗 (WANG LANG)： 谢谢奈杰尔。谢谢欧文。我想要感谢拉姆精彩的演示。你刚才提到了区块链和 DNS，但没有深入探讨。我们知道 ICANN 接受它作为认证注册服务机构是不可阻挡的。我的问题是，你对 Web3 DNS 的未来有什么看法？谢谢。

拉姆 • 莫汉： 谢谢。SSAC 还没有专门针对区块链的报告，但我们确实做了一份关于 DNS 和新技术发展的报告。总的来说，技术终将不断发展。我们应该拥抱这些新的域名空间，而不是说只保护自己的域名空间，对其他人的域名空间加以阻止。然而，重要的是，如果要将其他域名空间集成到 DNS 域名空间中，就必须以负责任的方式完成。这样做必须考虑到稳定性和安全性。所以，在较高层次上，这就是我们看

待它的方式。此外，还存在其他的人为因素和其他问题。如果我们只写一份关于区块链的报告，我相信会有其他问题被揭露出来。我们还没到那一步呢。

奈杰尔 • 希克森： 非常感谢拉姆。有请欧文发言。

欧文 • 弗莱彻： 谢谢奈杰尔。我是来自美国的欧文 • 弗莱彻。我认为这是一场精彩的会议，人工智能和 DNS 滥用是一个很好的例子，说明 SSAC 的技术专业知识可以真正让我们 GAC 受益，我们正在努力就 GAC 可能想要评论的各种问题基于证据和丰富信息摆明立场。

我认为开展更多这样的互动很不错，或许也包括 GAC 举办的能力建设会议。我在聊天中也看到了一条关于该影响的评论。拉姆，该演示描述了一些滥用类型，很显然，这些类型不是 ICANN 所描述或定义的 DNS 滥用，尽管如此，许多内容还是可能会被滥用 DNS 的人所利用。但就 ICANN 定义下的 DNS 滥用而言，您是否认为我可以从陈述中得出，不良域名的加速创建会导致报告的滥用案例不断增加？例如，当我们在未来几个月或几年中查看有关 DNS 滥用的统计数据和报告时，我们应该记住这一点吗？谢谢。

拉姆 • 莫汉： 我只说说个人的观点，因为 SSAC 对此没有立场。我个人认为这是合乎逻辑的后续步骤。当技术可以轻而易举地帮助实现复杂性和规模时，你就会有所期待了，因为这可以赚这么多的钱。杰夫 • 贝瑟

昨天曾说过，一条上好的“鱼”价值大约 2 万美元。所以，如果注册一个域名要花 200 美元、100 美元，甚至 1000 美元，那也不一定有足够的威慑力。如果看一下逻辑链，预期会看到更多的这类滥用事件和相关报告。这就是我个人的观点。还有其他人要发言吗？梅丽克？

梅丽克 • 凯奥： 从个人角度来看，我的意思是，我每天都在从事安全工作，所以我基本上不相信任何东西。但这对我来说真的很有趣。我不会过滤垃圾邮件，因为我想了解相关活动和正在发生的事情。真正有趣的是，这一定是人工智能造成的，但钓鱼电子邮件的类型正日渐变得极其可信。我还认为，他们实际上是在看你在 Facebook 或 LinkedIn 上发布的内容，实际上有可能针对特定的组织、特定的领导层，这样他们就有了更加可信的情报。这也是我们能够更快采取行动来检测和阻止的事情，这确实非常重要。

奈杰尔 • 希克森： 谢谢。非常感谢拉姆。恐怕我们就要到此为止了。我们已经没时间了，但此次交流确实很有成效。这表明大家对自己正在从事的这项不可思议的工作是多么感兴趣。看到主席台上这些专家也让人很开心。我一直都很自豪，能够与史蒂夫 • 克罗克博士坐在一起，这是一种激励，你们中的许多人不仅为 ICANN 的工作做出了贡献，还为技术社群解决了许多问题。

期待大家再次相聚。这不会是最后一次。感谢各位主动提出要跟进各种问题。好了，我想我们应该结束此次会议了。虽然我尊敬的同

事就在后面，但你能告诉我们上午的会议是什么时候吗？你能提醒一下我们吗？

茱莉亚 • 莎弗琳： 稍等一分钟。你知道吗？

发言人（姓名不详）： 是 1:15。在此之前还有欢迎仪式、乔伊纳 (Joiner) 政治论坛，但 GAC 将于当地时间 1:15 开始讨论 WHOIS 注册数据问题。

奈杰尔 • 希克森： 没时间了。

拉姆 • 莫汉： 奈杰尔，我代表 SSAC 非常感谢你邀请我们来到这里。希望这不是最后一次。我们期待大家能够加强互动。

[听写文稿结束]