ICANN84 | 年度大会 – GAC 与 ccNSO 联合会议
2025 年 10 月 29 日（星期三） – 10:30 - 12:00（爱尔兰标准时间）

尼古拉斯 • 卡巴雷诺 (NICOLAS CABALLERO)	欢迎各位。请就坐。我们马上就要开始了。我正想说这个。请讲，谷尔顿。谢谢，尼科。
谷尔顿 • 泰普 (GULTEN TEPE)	欢迎参加于世界协调时 10 月 29 日星期三 10:30 举行的政府咨询委员会 (GAC) 与国家和地区名称支持组织 (ccNSO) 联合会议。请注意，本次会议正在进行录音录像，并根据 ICANN 预期行为标准、ICANN 社群参与者行为准则和 ICANN 社群反骚扰政策开展工作。本次会议期间，如果在聊天窗口中以正确格式提交问题或评论，我们会大声朗读您的问题或评论。本次会议的翻译服务包括全部 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。请先说出您的姓名以便于记录；如果您使用的是英语以外的其他语言，还要说出您将使用的语言。发言时请保持合理语速，以便翻译人员能够准确地进行翻译工作。下面请 GAC 主席尼古拉斯 • 卡巴雷诺发言。感谢。
尼古拉斯 • 卡巴雷诺	非常感谢谷尔顿。欢迎各位。我很荣幸向大家介绍来自 ccNSO 的同事们，ccNSO 主席雅丽杭德拉，就在我旁边，在我右边，抱歉，就在我的右手边。我们今天将进行一场非常有趣而且——我认为——互动性很强的会议，大致类似于我们在西雅图采

用的方式，是在西雅图吧？我们希望大家积极参与、提问和互动。

没有错误的问题，只是提醒一下。我们将设置不同的“站点”，可以这么说。在我们介绍背景情况以及我们的同事、来自 FBI 的加布里埃尔 • 安德鲁斯 (Gabe Andrews) 就加密货币投资诈骗示例进行演讲之前，先有请雅丽杭德拉发言，请她就今天会议的流程细节做一些说明。欢迎各位。雅丽杭德拉，请发言。

雅丽杭德拉 • 雷诺索 (ALEJANDRA REYNOSO)：谢谢尼科。很高兴再次加入 GAC 并与大家一起尝试这些不同的方式。我们相信这非常有成效。在详细介绍互动环节之前，我认为最好先听听加布里埃尔的介绍。等他结束后，我将非常乐意向大家介绍下一部分的内容。谢谢您邀请我们。

尼古拉斯 • 卡巴雷诺：非常感谢雅丽杭德拉。那么，现在有请来自 FBI 的加布 • 安德鲁斯 (Gabe Andrews) 发言。加布，请发言。请讲。

加布里埃尔 • 安德鲁斯 (GABRIEL ANDREWS)：谢谢尼科。谢谢雅丽杭德拉。让我们开始。请切换到下一张幻灯片。我今天要向大家介绍的是过去几年向 FBI 报告的最主要的互联网犯罪类别。我们称之为加密货币投资诈骗。在媒体上，它也被称为“杀猪盘”。如果你听过那个术语，其实它们

指的是同一回事。我们讨论这个问题是希望它能为我们正在进行的 DNS 滥用对话提供信息。

这类犯罪是在新冠疫情期间诞生的。它是疫情期间给我们带来糟糕影响的一件事情。当时的情况是，东南亚的有组织犯罪集团在当地经营赌场酒店。新冠疫情爆发后，这些酒店无法盈利。因此，他们探索了其他赚钱的手段。

其中一种方法是引诱移民工人来为他们工作。这些工人到来后被扣押，变成强迫奴工，被迫向西方人实施欺诈计划。结果证明，这种方法非常有效，而奴工成分之所以非常重要，原因我稍后会讲到。

那么，我们快速浏览一下去年新闻中出现的一些头条。今年五月，联合国发布了一份报告，强调需要认识这一持续进行的骗局，呼吁全世界采取应对行动。过去七天，我们看到缅甸军队袭击了其中一个强迫劳工营地。下一张幻灯片。

我们看到，SpaceX 在上周切断了向其中一些缅甸诈骗营地提供的星链服务。同样在上周，我们美国国内司法部仅从其中一个犯罪诈骗团伙就没收了超过 150 亿美元的比特币，它就是“太子集团”。

我需要指出，这是 FBI——不仅是 FBI——是美国有史以来进行的最大规模的没收行动，最大规模的扣押行动。让我们继续，请切换到下一张幻灯片。

那么，它的运作方式是，在骗局开始时进行网络钓鱼，但不是通过电子邮件进行的，而是通常会通过手机上的某个短信应

用、或通过社交媒体、有时通过交友网站，让你看到诈骗信息。

你会收到来自某个人的意外信息，引诱你开始对话。他们常常会假装自己对建立友谊、恋爱关系或商业投资等感兴趣，但起步很慢。这一点非常重要，因为奴工成分使得钓鱼者能够真正花时间建立融洽关系并培养信任。

继续下一张幻灯片。这样，等到他们真正将对话转向投资某个新的、令人兴奋的加密货币机会的可能性时，已经是经过漫长的建立融洽关系阶段之后了。这使得它与我们过去看到的传统网络钓鱼非常不同，传统钓鱼可能只是一封精心设计的电子邮件。

这种则是一个非常缓慢的网络钓鱼过程，是在几天或几周内建立起来的，这之所以可以实现，仅仅是因为这些人本身被扣押，被迫成为奴工，对犯罪分子来说，劳动力本身只是一项微不足道的开支。

让我们继续，请切换到下一张幻灯片。这里的域名成分，因为我肯定你们在想，如果不是电子邮件，那么实际涉及的域名成分是什么？当鱼钩最终设下，坏人会说，对了，我刚刚在我的投资上获得了丰厚的回报，具体是这样..... 我很乐意与你分享这个机会，等等。

他们会通过那些聊天信息提供一个指向他们的加密货币交易所的链接。这通常是一个冒充其他合法的交易所的同音字域名。犯罪分子在注册这些域名时，会批量注册。说起批量注册或通

过 API 访问进行批量域名注册，这就是犯罪分子使用批量域名注册的方式之一。

他们会一次注册数百或数千个冒充这些加密货币交易所的域名。请切换到下一张幻灯片。当他们设置基础设施时——我道歉，这张幻灯片的字体非常小。我是从关于这个主题的另一份演示文稿或新闻稿中拿来的。

我来解释一下会发生什么：在左边那些粉色、紫色和黄色的矩形里，他们从一堆可以轮换使用的相似域名开始。每个域名使用时间不超过三个月。

如果其中一个被查封，他们会迅速转移到下一个，因为他们有非常多的域名可供选择。但是，通过使用一种称为 CNAME 转发或者说更改这些域名中规范名称设置的技术，他们会设置该域名路由到下一个域名，然后再到下一个域名，最后到达末端的加密货币网站。

这是一种技巧，可以使相似域名的名称保留在浏览器中，但在最终解析之前要经过多个基础设施跳转。我不期望每个人都熟悉 CNAME 设置，但对于听众中可能熟悉它的人，尤其是那些运营国家和地区顶级域 (ccTLD) 的人，我希望大家知道这种策略。

这样一来，如果你们遇到它，就能够辨认出来。在调查人员调查过程中，我们发现由于使用了这种策略，我们更难以探索他们的基础设施。他们这样做有两个原因：让调查人员更难调查；他们自己能够非常快速地轮换那些批量注册的域名，同时在后面保持数量少得多的受保护的基础设施域名。

为了给今天接下来的讨论铺垫，我想提出这个骗局让大家熟悉，同时也想问问从事于 ccNSO 的伙伴和同事们，他们是否在自己的领域看到这种情况。我知道在 gTLD 空间，.com、.top、.info、.net 被使用过，但我不敢说我们有完全把握，

很有可能他们也在使用 ccTLD 空间。现在有多个不同的团伙在从事这类骗局，不同团伙可能使用不同的基础设施。因此，我希望为对话提出的问题之一是，你们是否看到涉及此类行为的滥用报告，这些报告可能涉及加密货币网站的批量注册，或者可能涉及你们能够观察到的 CNAME 转发？

进而，为了我们将在 gTLD 领域与 ICANN 进行的关于潜在政策制定的讨论，当我们考虑围绕或许我们称之为“关联域名检查”的政策时——即当你收到关于一个域名的滥用报告时，将要求查看同时注册的其他域名，看看它们是否也参与了该骗局。或者如果我们针对通过批量注册的访问控制（例如通过启用它们的 API）制定单独的政策，我们想知道 ccNSO 是否有可以为我们探索此类政策提供参考的经验。

那么，在做了相关铺垫之后，我想我快到八分钟的计时了。感谢大家的关注。我认为目前针对这个骗局正在形成真正大规模的全球响应。我非常高兴你们能参与对话并共同解决它。感谢。

尼古拉斯 • 卡巴雷诺　非常感谢加布。非常有趣。那么现在，好了，问题来了。这对 ccTLD 运营商来说尤其重要： 你们是否收到了关于这方面的滥

用报告？这是一方面。另一方面，你们是否在寻找批量注册以及 CNAME 转发？然后还有一些更多的问题。但在我们深入探讨之前，请允许我请雅丽杭德拉发言，她将在本次与 ccNSO 会议剩余的 75 分钟时间里，向我们详细介绍我们将如何运营以及一些细微差别。交给你了，雅丽杭德拉。

雅丽杭德拉 • 雷诺索 谢谢你，尼科，也谢谢你，加布里埃尔，所做的介绍。我知道时间有限。我们之后会处理你们的问题并给予反馈。在接下来的活动中，我们将像之前一样，进行一次更具互动性、真真实实的需要大家起身参与的活动，与 GAC 和 ccNSO 的人员讨论关于 DNS 滥用的几个主题，以理解不同的主题，例如在第 1 站，我们有人工智能在滥用检测和防范中的应用。

在第 2 站，我们有批量域名注册带来的挑战，这与我们刚刚听到的内容非常契合。在第 3 站，有调查域名组合中的滥用行为。第 4 站，针对诈骗和欺诈防范的国家框架。第 5 站，可信通知者安排。

所以，活动将这样进行：根据大家上次的反馈，大家希望我们进行更多轮次。但进行更多轮次意味着每轮的时间更少。所以，这次我们将进行三轮。在每一轮中，你可以选择你想前往哪一站。时间一到，可以换到任何想去的站点。是的，我们有五站。

你们将有三次机会参与互动。但最后，我们也会有每站的总结汇报，这样你就不会因为没去过某个站点而错过信息。

就是这样。一共有这些站。我们留着这些信息，大家可以走动起来了。我们如何控制时间？巴特 (Bart)？哦，我们会在这里展示一个计时器？好。就是这样，尼科，我们开始吧？

尼古拉斯 • 卡巴雷诺 非常感谢，雅丽杭德拉。在我们继续并开始各站和各轮活动之前，我只想回到加布提出的观点和问题。我想听听现场或线上与会者的一些反馈。

为了处理加布提出的问题，请允许我在我们真正开始各轮、各站和这场重头戏“DNS 冠军赛”之前，留出三到五分钟来处理此事。请大家畅所欲言。有任何反馈吗，特别是来自 ccTLD 运营商关于 CNAME 转发主题的？再次说明，我们并不期望房间里的每个人都是 DNS 跳转或 CNAME 转发这类事情的专家。雅丽杭德拉？好的，请讲。

雅丽杭德拉 • 雷诺索 为了开始这个讨论，我想先回答特别向 ccNSO 提出的问题，即我们是否会考虑为此制定一项政策。我只想重申，ccNSO 在可以制定政策的领域权限非常有限。这些政策旨在指导互联网号码分配机构 (IANA) 如何管理 ccTLD。例如，ccTLD 的撤销、转让以及 IANA 中的所有那些操作。

所以，我们并不制定政策来告诉 ccTLD 如何开展工作。不过，我们确实有一个 DNS 滥用常设委员会，它在安排本次与大家进行的会议中发挥了巨大作用。通过这个常设委员会，我们正在收集最佳实践的资料库，与全世界分享每个 ccTLD 是如何处理

这个问题的。我相信我们即将进行的这项活动可能会进一步扩展这个讨论，因为我没有看到很多人举手。感谢。

尼古拉斯 • 卡巴雷诺　非常感谢你的反馈，雅丽杭德拉。那么，再给我一分钟来处理第二个问题，关于 ccNSO 运营商可能拥有或可能没有的、可能为此类政策提供信息的经验。会场上没有人请求发言。线上也没有人请求发言。好的。交还给你了。让我们再次感谢加布，如果你还在线的话。非常感谢。这非常重要，并且肯定与所有 GAC 代表相关。非常感谢你的介绍。雅丽杭德拉，交还给你。

雅丽杭德拉 • 雷诺索　谢谢。我们了解到这些问题，并会将反馈带给加布里埃尔。谢谢你。那么，现在请大家起身，走去自己偏好的站点。我会把计时器放在这里。第一轮，我们有 18 分钟。现在开始计时

大家好，时间到。请结束你们的谈话并更换站点。谢谢。我们将在一分钟后开始计时。

快速提醒，我们将开始第二轮。所以请更换你的站点，移动到下一站。可以重新启动计时器吗？谢谢。

大家好！这是两分钟提醒。两分钟。

好了，时间到。请结束讨论并更换站点进行第三轮。我们将在一分钟后开始计时。谢谢。

好的，希望大家已经走到第三个目的地。现在开始计时。谢谢。

这是两分钟提醒。两分钟。

时间到。谢谢大家。请返回你们的座位。主持人及速记员，请留在你们的站点，以便我们准备好进行总结。其他各位，感谢参与，请回到你们的座位，我们要开始总结这次活动。

好的，还有十秒钟返回座位，然后我们就可以开始总结。

我想我们准备好了。我们将使用流动麦克风，逐个站点进行总结。可以从第 1 站开始吗，关于人工智能在滥用检测和防范中的应用。有请尼科。

尼古拉斯 • 卡巴雷诺 非常感谢。我们第 1 站关于人工智能和机器学习的使用，首先，我们与来自 .nl 的克里斯蒂安 (Christian) 一起解释，我们进行了一场精彩的三轮小型会议，讨论了 AI 和 ML，我们解释了什么是 AI，什么是 ML，什么是深度学习，什么是生成式 AI，还有 ChatGPT 等等的区别，以及算法实际上如何用于检测 DNS 威胁和所有这类事情，还有 DNS 流量以及许多其他实际上不一定与 LLM 或生成式 AI 相关的内容及其区别等等。

以及在这种情况下，荷兰团队正在实施的用于打击 DNS 滥用的措施，提出了许多好的问题，聪明的问题，不仅关于技术本身，还有关于实施、内部机制，以及整个系统在内部层面实际如何运作，幕后发生了什么，可以这么说。

非常有趣。我非常喜欢，我希望参与者们也喜欢。那么，再次非常感谢克里斯和那边的 .nl 团队。这就是我从第 1 站带来的简短的迷你报告。交还给你了。

雅丽杭德拉 • 雷诺索 非常感谢，尼科。接下来转到第 2 站，关于批量域名注册的挑战，有请彼得 • 科奇和玛蒂娜 • 巴贝罗。

彼得 • 科奇 (PETER KOCH) 是的，谢谢。我们讨论了批量注册，别担心，我们并没有得出批量注册的定义是什么，但我们花了一些时间讨论了为什么它是一个挑战但又不那么重要。

我们还讨论了自动化注册，并且我们区分了注册服务机构和注册管理机构之间的沟通与为其他人提供的自动化注册支持，而且发现后者可能在哪些方面值得关注。我把麦克风交给玛蒂娜，让她介绍更多讨论结果的细节。谢谢。

玛蒂娜 • 巴贝罗 (MARTINA BARBERO) 非常感谢。这也是一次非常有趣的讨论，有很多好的问题，但简而言之，我们讨论的是如何应对与批量注册相关的问题，我们讨论了识别与理解批量注册意图的能力之间的对立关系，因为一些批量注册的用例是合法的，比如品牌注册多个域名。

那么设置哪种摩擦、如何在不阻碍合法用例的情况下处理识别问题？在这方面，当我们谈到识别时，提到了识别组织和识别个人之间的区别，这需要不同的实践和方法。

我们还提到了 ccTLD 空间的许多不同实践，一些注册管理机构确实在授权后查看可疑行为并识别这些行为，并在其链接至批量注册时尝试处理，而其他一些注册管理机构则在授权本身之前就处理这类可疑行为。

总的来说，我们谈到了认识到网络钓鱼活动在极短时间内可能造成的损害的重要性，正如我们早些时候从同事加布那里听到的那样。因此，应对恶意行为的反应速度和所需时间必须迅速，这当然是一个限制因素，在我们讨论补救措施时需要加以考虑。遗憾的是，我们刚刚并没有想出很多绝妙的主意来解决这个问题，但我希望这已经有所帮助了。

雅丽杭德拉 • 雷诺索 非常感谢。接下来转到第 3 站，在这张桌子这里，有克里斯托 • 彼得森和苏珊 • 查默斯负责“调查域名组合中的滥用行为”。

苏珊 • 查默斯 (SUSAN CHALMERS) 非常感谢。我是来自美国的苏珊 • 查默斯，来自美国国家电信和信息管理局 (NTIA)，它是 .US 国家顶级域的政策主管机构。这位是克里斯托 • 彼得森，她来自负责管理 .US ccTLD 的注册管理机构服务。我只分享几个要点，然后交给克里斯托。总的来说，我们这一站探讨的是在政策制定、即将到来的关联域名检查政策制定流程中会审核的内容，这指的是当收到滥用报告时的情况。

美国顶级域 (TLD) 注册管理机构实际上是 .US 区域中注册人信息的权威来源，所以这是相当独特的。另外，我应该指出，美国 TLD 有一项政策，禁止使用隐私和代理服务。因此，数据库中所有的注册人数据都是真实的注册人数据，这使我们处于一个独特的位置，能够根据收到的信息来缓解滥用行为。克里斯托，接下来可以交给你吗？

克里斯托 • 彼得森 (CRYSTAL PETERSON)

当然。谢谢你，苏珊。在我们三轮会议期间的讨论中，我们回顾了我们作为一个注册管理机构如何检测关联域名和域名组合，我知道这也回到了加布在我们会议开始时提出的其中一个问题，就是他关于加密货币政策的问题。

正如苏珊提到的，.US 在其禁止隐私代理的政策以及我们还有 whois 准确度验证这方面是独特的，我们正从注册管理机构的角度考虑，如何通过注册人联系人数据来识别关联域名，以支持社群的滥用缓解工作。

所以，我们的会议很有成效，我们回顾了如何定义关联域名，以及在缓解方面所关注的内容，并且在这方面收获了一些很好的问题。

雅丽杭德拉 • 雷诺索

非常感谢。转到第 4 站，关于诈骗和欺诈防范的国家框架，有请布鲁斯 • 托金 (Bruce Tonkin) 和伊恩 • 谢尔登。

伊恩 • 谢尔登 (IAN SHELDON)

谢谢。我在这里。第 4 站，我们进行了一场关于国家反诈骗框架的精彩讨论。布鲁斯 (Bruce) 向我们介绍了在国家层面应对诈骗所需的几个不同步骤，需要治理、预防、检测、干扰、响应以及将信息反馈回相关方。

在澳大利亚，我们设立了一个国家反诈骗中心来应对这一挑战，澳大利亚民众可以来这里报告遭遇的诈骗并找出如何为其面临的挑战获得补救。该中心与 .au ccTLD 运营商紧密合作，该运营商在收到诈骗警报时会采取许多相当及时的行动。

关于诈骗在多大程度上是网络安全问题，以及多大程度上是消费者保护问题，我们也进行了一些很好的讨论。在澳大利亚，我们的国家反诈骗中心隶属于我们的竞争与消费者委员会，因此它在很大程度上被视为一个消费者保护问题，而且我们的网络安全机构与政府的消费者保护部门之间有着良好的互动。

此外还讨论了一些我们为确保消费者受到保护而采取的措施，其中有很多围绕关联要求以及它在多大程度上真正有效减少了许多此类问题（但并未完全消除）的精彩讨论，因为存在大量围绕凭证被盗的行为，所以即使有那个关联要求，那些身份凭证也会被盗并在许多诈骗中被使用。

关于讨论，你还有什么想补充的吗，布鲁斯？我想我们这边就这些了。谢谢。

雅丽杭德拉 • 雷诺索

非常感谢，现在转到最后一个站点，第 5 站，关于可信通知者安排，有请杰克 • 文塞特和宫本智则 (Tomonori Miyamoto)。

杰克 • 文塞特 (JAKE VINCET) 谢谢。因为时间关系，我就长话短说了。我们讨论了我们在 .UK 实施的可信通知者安排及其不同层级，我们还花了很长时间讨论了实施可信通知者安排的一些风险和回报。

我认为一起参与讨论的小组明确的是：第一，可信通知者似乎并不那么流行和广泛；第二，可能在涉及外国司法管辖区时会遇到一些挑战，例如如何验证那些报告者的准确性，但总体而言，我们看到了 Nominet 和 .UK 所建立的这类安排的好处。你还想补充什么吗？我们的讨论就是这样。谢谢。

雅丽杭德拉 • 雷诺索 非常感谢大家。在我开始总结本次会议之际，请在 Mentimeter 加入我们并为本次会议评分。我们希望得到你们对这次会议的反馈。如果你觉得以上总结提供的信息不够，别担心。我们会将在所有这些站点讨论的内容的摘要发送回 GAC 进行分发，方便大家掌握并使用所有信息。我就说到这里，交给你了，尼科。

尼古拉斯 • 卡巴雷诺 非常感谢。谢谢雅丽杭德拉。感谢 ccNSO。这是一次非常精彩的会议，说实话，这是我最喜欢的会议之一，无意冒犯所有其他咨询委员会和选区。我真的认为我们也应该与其他选区举行更多这样的会议，可以说非常吸引人，非常有互动性。

所以，谢谢，再次非常感谢 ccNSO。请大家务必花——我不确定——两分钟或者 45 秒来完成 Mentimeter 的调查，因为这有助于我们决定，例如，分配给各轮讨论的时间是否足够，是太短

还是太长，应该是 18 分钟，还是 15 分钟，我们是否应该为总结分配更多时间等等，对吧？

非常感谢大家。本次会议到此结束。事实上，抱歉超时了四分钟。我再简要补充一下会务安排。接下来是午餐时间。有一个好消息，大家将有额外的 15 分钟时间，因为我们有一个 GAC 领导层会议，所以你们需要在 13:30 回到会场，而不是 13:15。

谷尔顿 • 泰普　　13:45，尼科。

尼古拉斯 • 卡巴雷诺　　抱歉，抱歉，更好了，这样更好了。13:45。有强烈的反对意见吗？有人反对吗？现在正是表达意见的时候。那么非常感谢诸位。本次会议到此结束。请各位在 13:45 回到这里。非常感谢，让我们为 ccNSO 的同事们热烈鼓掌。

雅丽杭德拉 • 雷诺索　　非常感谢。

[听写文稿结束]