ZH

ICANN84 | 年度大会 – GAC 与 SSAC 联合会议
2025 年 10 月 28 日（星期二） – 15:00 - 16:00（爱尔兰标准时间）

谷尔顿 • 泰普 (GULTEN TEPE)：

欢迎参加于世界协调时 3 月 28 日星期二 15:00 举行的政府咨询委员会 (GAC) 与安全与稳定咨询委员会 (SSAC) 联合会议。

请注意，本次会议正在进行录音录像，并受 ICANN 预期行为标准、ICANN 社群参与者行为准则和 ICANN 社群反骚扰政策约束。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 会议室中举手请求发言。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 主席尼科 • 卡巴雷诺发言。谢谢大家。

尼古拉斯 • 卡巴雷诺 (NICOLAS CABALLERO)：

非常感谢谷尔顿。欢迎大家回来开会。我真心希望你们享用了很棒的爱尔兰咖啡。我很荣幸向大家介绍我的好朋友和他的团队——来自 SSAC 的拉姆 • 莫汉 (Ram Mohan)。我们还有苏珊 (Suzanne)、马腾 (Maarten) 和塔拉 (Tara)。欢迎你们。我们将进行一场非常有趣的——至少在我看来是如此——分为四个部分的会议。

第一部分，也是最重要的——同样是我的看法——自由与开放源码软件 (FOSS) 在 DNS 行业的重要性。我想补充说，在其他任何领域也是如此，但那是另一个需要讨论的话题。字符串冲突和相似性对安全和稳定的影响.这一点在目前看来是不可避免的。最后是 SSAC 与 GAC 之间合作的可能性。然后我将开放问答环节。

再次欢迎各位。现在有请我的好朋友拉姆 • 莫汉发言。接下来就交给你了。

拉姆 • 莫汉 (RAM MOHAN)： 尼科，谢谢你。很高兴能回到这里，在都柏林与你相聚，也很高兴在 GAC 与各位重聚。我们深感荣幸，你在连续多次会议中一直邀请我们，并在你非常繁忙的日程中为我们分配时间。我们不仅珍视与你们共处的这段时间，而且我们为此做了相当充分的准备，因为我们希望确保我们提供的信息、我们之间的沟通和互动，不仅层次得当，而且是可操作的，有你们可以采纳并带回去的实质内容。这就是我们工作的基础。

事不宜迟，我想做的是将我们第一部分的重点放在自由与开放源码软件在 DNS 行业的重要性上。为了介绍这个主题并与大家分享细节，请允许我将麦克风交给我的同事马腾 • 阿尔森，他是这个主题工作组的联合主席之一。马腾。

马腾 • 阿尔森 (MAARTEN AERTSEN)： 谢谢拉姆。谢谢尼科。今天我将和大家谈谈软件。SSAC 通常撰写的是技术性较强的文件。这份文件并非如此，而且 ICANN 社

群本身也不是其主要受众。这份文件是为世界各地的政策制定者和监管机构撰写的。所以我认为我来对地方了。如果你们不是直接负责这方面，我相信你们一定有处理网络安全事务的可爱同事们。

我们来谈谈软件。如果要用一句话概括我们的报告，那就是：我们发现 DNS 构建在自由与开放源码软件之上。这不是倡导。这不是我们在说自由与开放源码软件更好。这是关于 DNS 实际构建方式的事实陈述。请切换到下一张幻灯片。

FOSS 代表自由与开放源码软件。“自由”(Free) 指的是言论自由的“自由”，而不是演讲后免费喝健力士啤酒的“免费”。FOSS 由四项自由定义。使用——可以为任何目的使用该软件。研究——可以研究软件的工作原理，包括其源代码。分享——分享和重新分发软件的副本。最后，修改——可以更改软件以适应您的需求，并发布改进成果。

这些作为软件许可证一部分的自由，创造了一个与专有模式完全不同的生态系统，不仅针对软件开发，也针对分发和维护。尽管自由与开放源码软件之间存在理念上的差异，但本报告使用 FOSS 来涵盖这两个概念，其核心就是这四项自由。请切换到下一张幻灯片。

FOSS 模式具有与专有软件不同的风险特征。由于大多数自由与开放源码软件由志愿者维护，动机起着很大的作用。所以，如果人们作为志愿者从事软件开发，他们也可能会精疲力竭。这会导致项目被废弃。

FOSS 的另一个风险是没有担保，默认情况下没有保证的支持。因此，运营商需要承担责任，在内部保留开发专业知识，行使这些自由并在软件损坏时进行修复，或者可以购买支持合同。

在并非志愿者而是专业组织负责开放源码软件的情况下，存在搭便车的问题，因为软件是免费提供的。因此，可能会出现资金与使用完全脱节的情况，维护者可能属于一个支付维护者薪酬的小型倡议或组织。这些组织很容易因新的监管负担而遭受资金冲击，例如，在现有的资助模式受到威胁时。

所以这些风险是真实存在的，并且是 FOSS 模式固有的。不考虑这些权衡的监管可能会使这些风险恶化，而不是改善。请切换到下一张幻灯片。

当然也有优势。这里我们特别关注 DNS，与上一张幻灯片我们泛泛讨论 FOSS 不同，特别关注 DNS，我们看到它有强大的透明度和协作安全优势。学术界和运营商社群保持着一种强大而活跃的文化，公开审查自由与开放源码 DNS 软件，并且他们已经这样做了数十年。大家可以找到上世纪 90 年代研究软件缺陷或改进方法的论文。这些缺陷会被公开讨论和修复。

我们为此项研究调查的运营商——我们邀请了超过 100 家运营商参与——他们赞赏开放供应链带来的诊断、验证和修补漏洞的能力。因为他们不依赖供应商的速度，而是可以积极主动地处理。

特别是在 DNS 领域，许多流行的 DNS 项目并非由志愿者维护，而是由长期存在且稳定的组织维护。这些组织维护软件实施已超过 20 年。这种长期维护造就了值得运营商信赖的优秀记录。

FOSS 在 DNS 领域的另一个优势是通过多样性实现运营弹性。多种 FOSS 实施允许运营商运行不同的软件，减少单点故障，并且降低了组织运行自身基础设施的门槛，防止发生集中风险，或者像最近的热门话题——对外国实体的依赖。我们看下一张幻灯片。

我们来谈谈安全性。SSAC 注重安全，理解具体是什么决定了安全性非常重要。源代码是开放还是封闭的无法决定安全性；开发人员是受薪还是志愿者无法决定安全性；来自商业公司还是非营利组织无法决定安全性。

那么，对安全性起决定作用的是严格的代码审查和全面的测试、得到充分实践的漏洞处理流程，以及有持续资源支持的主动长期维护。

引用报告中的话：任何软件项目的安全性取决于其开发和维护流程的质量，而不是其源代码的可见性。

我们经常听到一个问题：FOSS 比专有软件更安全还是更不安全？答案是：都不是。安全性取决于开发过程的质量，而不是许可证模式。

政策制定面临的挑战在于，FOSS 具有不同的风险特征。不能从专有软件领域复制粘贴法规，并期望它们在有 FOSS 存在的领域中发挥作用。

我在开头提出了一些强烈的论断。让我们看一些数据。请切换到下一张幻灯片。从根服务器系统层面开始，我们调查了 12 家根服务器运营商，并试图识别我们使用的软件。我们看到自由与开放源码软件占主导地位。12 家根服务器运营商中至少有 9 家完全使用自由与开放源代码。即使是使用专有软件执行此角色的运营商，也常常同时运行 FOSS 以实现多样性和冗余。这里的关键要点是，这不是一个小百分比。在根服务器系统中，FOSS 占绝大多数。请切换到下一张幻灯片。

我们还调查了顶级域运营商。这些实体提供权威 DNS 服务。关键发现是，如果观察服务于最大数量顶级域 (TLD) 的运营商，10 家中有 9 家在其 DNS 基础设施中使用 FOSS。

对于在座的各位来说，在国家和地区顶级域 (ccTLD) 领域的情况可能更具相关性。如果只看国家和地区域名，我们发现 25 家运营商中有 20 家使用 FOSS。总的来说，这些 ccTLD 运营商使用 FOSS 服务于 234 个不同的 ccTLD，而这仅仅是在我们调查的数据层面。所以实际上这个数字更大。

这些都不是小型或实验性的 TLD。这些是负责数百万个域名的主要服务提供商。举几个例子，英国的 Nominet 在运行 FOSS，中国互联网络信息中心 (CNNIC) 使用 FOSS。请切换到下一张幻灯片。

让我们看看注册管理机构系统，看看存储 TLD 内域名的数据库。我们看到两种模式。第一种是完全的 FOSS 系统。确实存在这种，虽然不是主流，但存在即表明它是可行的，这很重要。

最流行的模式是注册管理机构系统是专有的。但即使在这里，我们也发现这些专有系统并非从头构建。相反，它们是基于自由与开放源码软件构建的专有集成。在我们调查的十个主要平台中，都包含了 FOSS 组件。因此，即使顶层的业务逻辑是专有的，其基础也是 FOSS。请切换到下一张幻灯片。

解析器生态系统是最难测量的，但此次我们再次发现了自由与开放源码软件的实质性使用和存在。全球 80% 的用户使用本地解析器，而且 FOSS 占主导地位。即使查看众多的商业解决方案，在大多数情况下，如果你去了解他们销售的产品，会发现也是 FOSS。公共解析器也是如此，其中许多是 FOSS。

我们在报告中做了一个关于 Cloudflare 的小型案例研究，他们有一个围绕着 FOSS 专有核心。至少四家最大的超大规模提供商在其 DNS 解决方案中使用 FOSS。其他公司在专有解析器中使用 FOSS 库作为组件。请切换到下一张幻灯片。

引用报告中的话：在 DNS 基础设施最关键的不分，使用 FOSS 是常态，使用专有软件是例外。这不是夸张。这不是倡导。这只是我们从所做研究中得出的严谨发现。互联网核心命名系统主要基于协作开发、自由分发的软件运行。请切换到下一张幻灯片。

传统的供应链监管方法要求安全标准，可能通过将其强加于关键基础设施的运营商来实现。如果让他们对故障负责，他们会转而求助于自己的供应商，通过合同设定这些要求；并通过采购和市场准入来执行规则。

为什么这种方法对 FOSS 行不通？FOSS 通常以零成本提供下载。可能不存在传统意义上的供应商关系。没有运营商与供应商的合同，甚至没有可以监管的供应商，只有一个志愿者。

因此，将合规负担加在运营商身上以影响其供应链，可能会导致他们破坏维护这些特定软件的小型组织的稳定。或者，如果将其强加于志愿者，他们可能会失去兴趣，这会导致项目因法律风险而被废弃、转向使用专有许可证、甚至规避某些司法管辖区。结果是，每个人都依赖的软件变得可用性降低，安全性下降。请切换到下一张幻灯片。

我们收录了一些案例研究，因为像美国、英国和欧盟这样的主要司法管辖区一直在制定考虑到 FOSS 的政策。我不会详细讨论这些，除非大家有兴趣，但这是可以做到的。请切换到下一张幻灯片。

这些是我们提出的五项可操作指南。SSAC 对你们是否监管持中立态度。我们也没有立场发表意见。但是，如果考虑到所在司法管辖区的法规，请承认 FOSS 的关键作用，需要认识到全球基础设施依赖于它，并且这是一种需要维护的优势。

咨询开源社区。让维护者、基金会和运营商参与政策制定过程，避免意外后果。

利用我们收集的目前的案例，并从新兴模式中学习。

激励可持续性。例如，鼓励对自由与开放源码软件做出贡献，将其视为对公共基础设施的投资。

并且集体应对整个软件领域——不仅仅是 FOSS——确实存在的系统性风险。资助生态系统范围的解决方案，共享依赖条件，而不是将负担压在个别维护者身上。

我想以上就是我们本次的演示。我很期待大家的问题。

马尔科 • 霍格沃宁 (MARCO HOGEWONING)： 谢谢马滕，感谢你清晰简洁的介绍。当然，正如我之前转达拉姆的信息一样，我建议大家点击链接阅读实际报告。

时间安排上，我们还有时间回答几个问题。目前队列中的第一个问题实际上来自于坐在我旁边的人。

尼古拉斯 • 卡巴雷诺： 不，不，是来自于欧盟委员会。

马尔科 • 霍格沃宁： 好的，我们先请欧盟委员会代表发言。谢谢。

杰玛 • 卡罗里洛 (GEMMA CAROLILLO)： 非常感谢主席和副主席，但如果您希望 [音频不清晰 00:19:36] 先发言，我很乐意稍后发言。我是来自欧盟委员会的杰玛 • 卡罗里洛。我想，你通过四个案例研究中的三个所解决的对象也包括我们。

这对我们来说是一个非常重要的主题，我想强调，作为监管机构，我们也从这个过程中学到了如何将开源的各种特性融入数

字监管。可以说，这是一个痛苦但非常有用的过程，我认为我们都在从中学习，并且正在取得良好成果。

我的问题关于供应链安全性，因为这仍然是一个问题。即使我们想试图绕开它，它仍然是个问题。你对像软件物料清单这样的举措有何看法，以及它如何能从根本上帮助解决供应链安全问题。谢谢。

马腾 • 阿尔森： 谢谢杰玛。你问 SSAC 对软件物料清单有什么看法。很遗憾，我要代表 SSAC 表示，我们尚未研究这一具体措施。我愿意给出我的个人意见，所以先提前声明。

是的，安全性在软件领域是一个问题——无论是专有软件还是自由与开放源码软件。我认为软件物料清单能够提供帮助购买软件，组织购买软件，主要是内部使用 FOSS 的专有软件。因为这种情况下会出现：某个组件存在漏洞，对所有人来说都可能受到影响，甚至是市场上所有产品。如果供应商甚至购买者不知道内部有什么，那么如何开始修复问题呢？从这个意义上说，这是一个有趣的工具。不过现在还只是刚刚开始。

我非常感谢你关于集体学习的评论，尽管我此刻是以个人身份发言。我发现观察欧盟的政策制定流程非常是有趣的，我很高兴我们有一个可以纳入本报告的案例研究。

马尔科 • 霍格沃宁： 谢谢欧盟委员会代表提出这个问题。谢谢马腾。我的队列中接下来是孟加拉国代表，然后是我旁边的主席先生。之后我将停

止接收问题，鉴于时间关系，我们将继续议程。那么，孟加拉国代表，请发言。

沙姆斯佐哈 (SHAMSUZZOHA) 博士：

谢谢。我是来自孟加拉国的沙姆斯佐哈。我认为这是一个非常好、很全面的陈述。尤其对于我，作为孟加拉国代表并负责与不同机构合作制定孟加拉国安全标准的人而言。他们产生了一些非常 [音频不清晰 00:22:49]。

我个人特别感兴趣两个方面。一是我们也在与孟加拉国 [音频不清晰 00:22:57] 合作制定他们的安全标准和他们的 [音频不清晰 00:23:01]。这也包括在特定 [音频不清晰 00:23:06] 中发布软件。

除此之外，我们还负责与国家关键基础设施部门合作与协调，特别是为他们制定 [CM] 和 SWOT 类型的安全运营解决方案。

所以我们内部确实存在争论，当我们试图 [音频不清晰 00:23:24]，甚至在政府采购系统中推广自由与开放源码软件时。但我们遇到的一个论点是关于 [音频不清晰 00:23:38] 内部固有能力的，特别是对于 [音频不清晰 00:23:40]，以及快速和 [音频不清晰 00:23:47] 需求的问题。

如果 [音频不清晰 00:23:52] 内部没有固有能力，尤其是在处理国家关键基础设施时，会存在很大风险。这在某种程度上也涉及运营成本。

所以这可能是一个问题，或者想听听你对此的见解，尤其是关于我们处理敏感的关键基础设施。谢谢。

马腾 • 阿尔森： 谢谢。从这个意义上说，我认为专有软件和 FOSS 之间的差异比人们想象的要小。因为如果你运营关键基础设施，运营商则有责任确保一切顺利运行。如果你选择 FOSS，而且大多数人都这么做，那么你需要在组织内部有专业知识，这是有成本的。你需要专家。或者，你需要从别处找专家，在许多情况下，如果查看最流行的软件，这些组织是通过支持合同获得资金的。

现在，如果情况不同，只有专有软件，那么你需要支付许可费用，这样大概也能获得支持。所以从这个意义上说，我认为与我们陈述中列出的所有优势（例如没有供应商锁定等）所带来的差异相比，实际差异并没有那么大。

但是，是的，关键基础设施的特殊性在于它有这些正常运行时间要求，并且需要专业知识来实现。每个运营商可根据其政府所给予的决策灵活度来做出选择。

马尔科 • 霍格沃宁： 谢谢两位。我们将结束这部分讨论，并请尼科发言，他是一位非常坚定的 FOSS 支持者。

尼古拉斯 • 卡巴雷诺： 谢谢。我也会言简意赅。谢谢马滕带来如此精彩的陈述。能否非常简要地评论一下开放源代码如何为政府，特别是发展中国家政府，避免锁定情况，不仅是在成本方面，而且实际上在..... 这样说吧，在内部安全成本方面。

马腾 • 阿尔森： 供应商锁定是指决定投资某个特定产品，然后由于投资太大或转换成本太高而无法迁移的情况。

FOSS 在供应商锁定情况下的优势，包括在网络安全方面，是实际上不需要与最初的维护者保持联系。有时也有其他组织能够支持这种部署，包括打补丁。

当然，需要始终依赖于原始开发人员来开发补丁，但这并不像专有软件那样只有唯一一个实体可以合作。所以我认为，也许预算较小的国家或地区会将其视为一种创新推动力，尝试在当地建立专业知识，而不是向国外其他实体付费。但我想，这是他们可以做出的选择。

我想这就是我对供应商锁定的看法，而且这也是我的个人观点，因为我们在报告中涉及这一点的内容不多。

马尔科 • 霍格沃宁： 谢谢尼科的问题和马滕的精彩回答。考虑到时间，我认为我们可以继续进行下一个主题，同样邀请 SSAC 做一些能力建设方面的分享。回顾一下，我知道在座有许多新的或较新的 GAC 成员，这对他们来说可能是一个相对较新的主题。但这个主题很重要，而且在我们开始下一轮次申请时，它变得愈发重要。所以我想既然苏珊在场，我想我可以请你就这个主题发言。谢谢。

苏珊 • 沃尔夫 (SUZANNE WOOLF)：

好的，谢谢您，马尔科。也谢谢你，马滕。一如既往地出色。你们树立了一个难以企及的标准。是的，正如马尔科所说，我来讲讲域名冲突分析项目 (NCAP) 域名冲突问题，因为我曾是域名冲突分析项目的联合主席，该项目最初由 SSAC 提出，之后的实施由一个社群范围的讨论组执行。

正如马尔科所说，在座各位中没有多少人资历深到记得它，但这并不是一个新问题。我们最早是在上一轮新通用顶级域中遇到了域名冲突的挑战。但我们不得不重新审视它，因为就我们必须适应的网络生态系统中的技术和期望而言，许多事情已经发生了变化。请切换到下一张幻灯片。回退一张。

那么，什么是域名冲突？其实非常难以定义，除非它确实是那种一看到就能认出来的事情。一种理解方式是，把域名想象成房屋地址。如果两栋房子共享同一个地址，就很难知道哪一栋应该收到邮件或包裹。如果邮件被投递到错误的地址，也会存在安全问题。单是想想隐私影响就知道了。

在 DNS 中，当某个域既用于全球 DNS 域名空间，即我们通常所说的公共互联网，又用于不同的域名空间，例如由你的 VPN 提供商运营的私有网络，其中不同的域名是有效的，这没问题，但同一个域名代表不同地址时，就会发生域名冲突，导致寻找时造成误解。这会很快变得混乱。请切换到下一张幻灯片。

接下来的几张幻灯片会过得比较快，不会介绍过多细节，我尝试概括总结一下。但幻灯片将会提供给大家，并且我们很乐意讨论技术细节。

什么不是域名冲突？如果你仔细阅读过《申请人指导手册》或任何围绕新 gTLD 完成的工作，会很熟悉其中一些术语。例如，域名冲突不同于字符串相似性或混淆相似度字符串。

域名冲突是一个技术问题，会导致安全性和稳定性问题，它源于将一个私有网络中已在使用的 TLD 授予了公共授权。例如，私有网络中的 .corp，如果它与公共互联网中的某个名称相同，并且含义不同，那就会引起麻烦。风险在于，对私有域名的查询将泄漏到公共 DNS 中，这也会引起技术冲突和安全故障。

字符串相似性也是新 gTLD 项目以及《申请人指导手册》等面临的挑战，但它更多基于用户感知。它是一个用户问题，由在人类看来外观或发音相似的不同的公共 TLD 引起，导致混淆性问题。例如，一个域名中带有小写“L”，另一个域名中有大写“I”，我们可能会混淆，就会面临网络钓鱼、欺诈、用户信任丧失以及给用户带来影响等风险。

需要注意的是，有很多方式会导致冲突问题。重点是，当计算机面对模棱两可的问题时，可能造成混乱又危险的结果。下一张幻灯片。谢谢。

概括起来说，撇开技术细节不谈，理解域名冲突对于互联网安全很重要，并且属于 ICANN 对 DNS 根服务器安全性与稳定性的职责范围。当企业使用了可能泄漏到全球互联网的内部 TLD 域名时，存在意外后果的风险。

引入更多新 gTLD 增加了这些挑战的可能性，因为可能有更多域名已在私有环境中使用，但同时也在被授权引入公共互联网域名空间。

此外，由于技术和网络基础设施逐渐发展，特别是自从我们上次实施新 gTLD 项目以来，测量域名冲突变得困难。例如，DNS 中实施的隐私增强措施，就使得准确测量网络活动变得更为困难。而这本身也正是隐私增强措施的目的之一。此外，各种替代域名系统的出现使得 DNS 的格局更加复杂，总体上也让相关测量工作挑战倍增。下一张幻灯片。

我说这个问题由来已久并非开玩笑。再翻一张。下一张。好了。谢谢。

2012 年，新 gTLD 轮次加速了根区的增长，引发了关于添加可能已在有限环境中（而非公共根区中）使用的新字符串时会发生什么情况的问题。

2013 年，SSAC 着手研究该主题并发布了一份咨询意见，强调域名冲突可能导致重大的安全性和稳定性问题。

检测到的最重要的字符串冲突，再次提醒，你们中有些人可能听说过，是 .home、.corp 和 .mail，它们在许多私有环境中被使用，存在大量数据，并且在尝试将它们授权引入全球根区、公共域名系统时，存在许多需要识别的风险。

2017 年，ICANN 董事会要求 SSAC 进行全面研究，以使所有未来的 gTLD 授权能够以安全、稳定和可预测的方式进行。

NCAP 项目，我想是有两个独立的项目，就是源于董事会的这项任务和一些后续问题。

在最后阶段，NCAP 第 2 项研究于 2024 年初发布，因为我们希望确保能够汇总的研究结果以及我们的建议能够为下一轮新 gTLD 提供信息。

我们第一次组建一个来自整个社群而不仅仅是 SSAC 成员的团队，我认为效果非常好。但我们确实承接了先前的工作和一些近期的研究，并在此基础上进行了拓展。下一张。

NCAP 项目的主要任务是分析与发现和缓解域名冲突相关的现状，并就更新即将到来的新 gTLD 轮次中域名冲突的处理方式提出建议。呈现方式是一个新的风险评估框架，它不仅用于发现域名冲突，还用于评估可能造成多大程度和何种类型的损害，以及可能采取何种缓解或预防措施。

我们必须指出，由于各种原因，评估变得更加困难。我们之前表明过这一点。事实证明，过去我们能够获取大量关于用户查询记录的数据，但如今这些数据已变得难以获取，因为 DNS 为保护用户隐私所采取的措施已远胜以往。这种情况对互联网和用户来说固然是好事，但对于试图全面理解网络动态的我们而言，却未必有利。

因此，我们在这个过程中遇到了一些非常值得探究的挑战，但能够利用可掌握的数据开展工作，并且能够实现所确立的目标。

目标 1：确保能够评估域名冲突。我们有一个逐级提升审查细节水平的框架，具体取决于特定域名冲突集可能存在的风险。

目标2：为ICANN确立一套评估流程，评估针对已识别的域名冲突的缓解与补救方案。我们发现，与以往相比更为显著的是，所有这些案例彼此之间至少都会存在一定差异。请切换到下一张幻灯片。

不会有测验，但这是报告中关于 NCAP 第 2 项研究所提出框架的图示，该框架考虑了域名冲突的风险以及发现和缓解这些冲突所面临的不断演变的挑战。

其中一个关键特点是，我们有一个技术审查团队来监督整个过程，并对特定案例可能附带的风险做出合格的判断。我们能够假定，在许多情况下，不一定存在持续的风险。

缓解或预防是可能的，但由于没有两个案例完全相同，我们假定需要相当程度的判断才能确保域名冲突风险得到恰当处理。因此，该框架有一部分依赖于自动化手段，有一部分将提交给专家小组——这与 ICANN 在处理其他复杂问题时的做法非常相似，即情况复杂且需要借助判断来推进流程。下一张。

因此，NCAP 第 2 项研究为社群推出的冲突风险评估框架的益处在于其主动的风险管理，能够识别域名冲突风险，并允许在造成损害之前制定和审查缓解策略。

该框架，我们非常努力地使其保持一致性和有效性。部分分析采用集中化方法，确保对所有新 gTLD 申请进行彻底的风险评估和缓解，再次强调，因为ICANN负责根区。

该框架是数据驱动的，能够为安全扩展互联网域名空间做出明智决策。

我们还能够解决围绕该工作领域的大量隐私担忧。因为虽然评估域名冲突存在固有风险，但我们最终强调的一点是，未能准确评估域名冲突、导致错误数据传输至错误的人或正确数据传输至错误的人，这本身就是一个隐私风险。我们认为，未能准确评估域名冲突的隐私风险大于与评估相关的风险。

再次强调，每个案例都不同，但能够对采取行动与不采取行动的风险进行比较分析，这为我们分析这些案例提供了一个额外的工具。因此我们得出结论：早期风险检测与知情缓解对于 DNS 的安全性与稳定性至关重要。

以上就是概括性要点。如果有时间，我很乐意回答问题。

马尔科 • 霍格沃宁： 谢谢苏珊。非常感谢。我也将永远引以为戒，不再混淆域名冲突和字符串相似性。我不会再犯这个错误了。同时，非常高兴看到 SSAC 多年来为这个主题带来的机构性 [音频不清晰 00:41:25]。我看到尼科举手了。我们还有时间提一两个问题。目前排队名单上没有人，所以尼科，请讲。

尼古拉斯 • 卡巴雷诺： 我有个简短评论。如果可以的话请翻回第 23 页的幻灯片。好的，就是这里。我们看到这里有四个步骤，我的问题关于时间。平均需要多长时间？是几天、几周还是几个月？我只是想将其与之前的 32 个步骤进行比较。你还记得昨天 GNSO 的演讲

吧，关于效率、速度等很多方面的讨论。那么平均来说，这个过程需要多久？

苏珊 • 沃尔夫： 这实际上是我们深入讨论过的一个问题，但未能就是否该提出具体建议达成最终共识。因为正如你所说，既有要求尽可能快速推进的压力，但我们也不希望遗漏重要风险。所以我们当时的考虑是以周为单位，而不是数月或数年——但这件事实际上必须留给工作人员和社群来做最终决定。

马尔科 • 霍格沃宁： 谢谢。我们还有时间再回答一个问题，但现场似乎没有人提问。那么，苏珊，感谢你详尽的阐述。如你所说，幻灯片会上传到网上。

苏珊 • 沃尔夫： 好的。

马尔科 • 霍格沃宁： 现在我们可以继续下一个主题了。这个主题实际上是由 DNS 滥用主题的负责人提出的，他们想知道既然现在问题文件已经发布，拉姆，你和你的 SSAC 同事们能否就该文件分享任何技术建议或看法。

拉姆 • 莫汉： 谢谢马尔科。在回答你的问题之前，我也想向 GAC 通报一下上一张幻灯片中提到的、与域名空间相关的一项我们刚刚启动的

工作。我们成立了一个名为“负责地融入 DNS 生态系统”(RIDE) 的工作组。我们关注的重点是，当其他域名空间中的标识符——具体来说是区块链域名空间中的标识符——希望与 DNS 系统中的标识符、域名及其他系统链接和交互时，会发生什么。我们已经在此方面展开了工作，并期望能就此提供一些评论和结论。

具体来说，我们关注并担忧域名生命周期、用户混淆、欺诈等问题，以及当其他域名空间中的系统使用与我们习惯的域名空间相似但不完全相同、却又以某种方式关联的术语、词语时，可能给 DNS 本身带来的安全和稳定风险。这项工作刚刚启动，我们会随时向各位通报进展。

马尔科，关于你的问题，请看下一张幻灯片。我们非常高兴看到已经开始有一份政策文件，或者至少已经开始了一些关于 DNS 滥用的工作，并且政策制定工作也已启动。请切换到下一张幻灯片。

过去，SSAC 的做法是在政策建议提出后提供评论和建议。我们正在与 GNSO 的同事们合作改变这一模式。我们受邀在那个 PDP 流程中派代表参与。

我们现在做的是，我们不参与关于应该采用单轨、双轨、三轨还是全部合并等类似问题的讨论。那些是政策制定者们需要贡献意见的地方。然而，我们打算介入并谈论与滥用相关的具体问题，我们的观察是什么，特别是因为我们花了大量时间关注滥用的演变及其发展趋势。

因此，我们非常专注于这方面。我们认为这是我们与 ICANN 董事会对话中的一个重要话题，例如关于 2026 年的优先事项。我们赞同 GNSO、签约方一直在讨论的一些事情，即 DNS 滥用必须在其优先事项列表中排名靠前。列表中的事项总会相互竞争，但如果我们不能正确处理，如果我们搞砸了，受影响的不仅仅是终端用户。还有我们所有人都奉为典范的这种自我监管的多利益相关方模型的声誉也会受损。我们必须做正确的事情，DNS 滥用必须成为一个重点。

所以我们深度参与其中，并打算比过去更多地参与设计阶段。

马尔科 • 霍格沃宁： 谢谢拉姆。听到这些真是太好了。既然是如此开放的讨论，我想知道是否有反对 DNS 滥用的同事想对此作出回应？或者还有其他问题要问 SSAC 吗？当然，也欢迎其他对这个主题有疑问的人提问。有请欧盟委员会代表亚诺什发言。

亚诺什 • 蒂莱恩约斯科 (JANOS DRIENYOVSZKI)： 再次感谢你今天到场并演讲。我们对 PDP 有点疑惑的是，抓住正确的范围很重要。我们将投入大量精力。我们想了解你对批量注册这一轨的看法，我们姑且这么称呼它，关于批量注册问题。因为当然，我们想要实现的是，在政策制定流程结束时，可以获得一些有影响力、并且真正针对我们想要的目标的东西。

所以我们提到了 API，但我们想知道这种方法是否能真正完全覆盖支持大量注册的大多数技术或措施。如果你能就这是否是一

个好方法，或者范围的界定是否应以确保最终具有某种面向未来的验证方式来处理，我将非常感激。这是我个人的兴趣点。我不知道还有什么其他技术可能实现这种大量注册。谢谢。

拉姆 • 莫汉： 谢谢。这个问题需要详细回答，因为存在合理进行批量注册的例子。比如一家公司想保护其新产品，于是跨多个域名注册了上百个。还有，他们是跨多个 TLD 注册，还是在一个 TLD 内注册？这里面有具体的情况。

我想指出，API 访问并非批量注册的唯一途径。我们已经看到很多案例，有不良意图的人使用非 API 模式进行注册，以此作为一种隐藏手段，因为他们知道 API 访问正在被监控。

话虽如此，我认为这是一个很好的调查方向。批量注册需要被定义。我们与社群中其他一些成员共同的一个担忧是，如果你设定一个阈值，如果你说低于某个你选定的数字的注册将不会受到同等程度的审核，那么我们可以预测这会被人钻空子。所以这方面还有一些工作要做。

我希望最终能制定一项政策，为我们想要阻止的行为类型提供一个广泛的框架，而不是针对实施这些行为的具体方法。我认为这是我们在政策制定流程中应该努力瞄准的区别。

马尔科 • 霍格沃宁： 谢谢拉姆。我看到排队列表差不多没有人了，那么现在是时候过渡到下一个主题。再次非常感谢你的意见。正如你所说，你将在开场提到的 PDP 中发挥作用，而且我们正在加强 GAC 和

SSAC 之间的联系。这就引出了一个更开放的问题：我们在哪些地方看到合作的机会？GAC 和 SSAC 都将参与这个 PDP。这可能不是推进的唯一途径。

请切换到下一张幻灯片。印度代表，你还要就 DNS 滥用提问吗？还是关于这个具体问题？我看到你举手了。

印度代表： 关于 DNS 滥用，总的来说，我想也许我愿意听听拉姆在那方面的看法。关于将 [保持准确性] 的 15 天窗口期缩短，可能对 DNS 滥用产生什么潜在影响。我认为这是可以采取的最简单的步骤之一。它实际上可以在很大程度上减少和缓解 DNS 滥用。

也许在十年前，真实的验证或核实可能是个挑战，但现在这些事情都能做到。我们每天至少做三四次。你在酒店办理入住，要进行验证；去机场贵宾厅，也要进行验证核实。但我真的想知道，我们怎么能允许某人在甚至没有验证的情况下就拥有一个域名。请注意，甚至没有识别身份。这仅仅是个验证。

就此，我想听听你的想法，因为我真的觉得你理解为什么 [音频不清晰 00:53:03] [应该] 被给予的理由。

马尔科 • 霍格沃宁： 谢谢。我理解这是关于中间的两周，即用于验证的两周宽限期，对吗？拉姆，关于这个时间框架有什么看法吗？

拉姆 • 莫汉： 非常感谢。我们之前就紧急请求发表过意见，我想简而言之就是，如果称之为“紧急”，那的确有它真正的含义。我们认为，这需要非常快速的响应时间，而不应该……这相当于在现实生活中呼叫紧急服务。当你呼叫紧急服务时，你不会期望在 15 天内或两个工作日内才得到回应。所以我们的方法是，这很重要。

关于验证和核实的问题，从 SSAC 的角度，我不确定我们是否已经必然形成了一个共同的、代表整个 SSAC 的观点。但我们确实注意到，一些安全研究人员和执法部门人士表示，他们感到受阻，因为无法以容易获取的方式获得某些注册人信息。所以我们一直在鼓励发展分级访问系统，能够向对这些信息有合法利益的各方披露信息。

这大致是我们的立场。具体到紧急请求，我们认为，特别是当 GAC 和董事会在这方面合作时，你们应该真正牢记“紧急”在字典中的定义，而不仅仅将“商业合理”树立为基准。谢谢。

印度代表： 不，我的问题不是关于紧急请求。我的问题是关于通过缩短验证或核实与域名注册之间的 15 天窗口期来缓解 DNS 滥用的潜力。我认为这是我觉得在当今时代真的难以理解的事情。

拉姆 • 莫汉： 是的，谢谢你的说明。再说一次，我不知道我是否能代表整个 SSAC 发言。我认为这是一个需要认真审视的领域。我们应该关

注用户损害，并将其与现有的其他合同要求和政策制定流程进行权衡。但我们应该在这个领域将用户损害放在首位。

马尔科 • 霍格沃宁： 谢谢印度代表。谢谢，SSAC 的拉姆。还有其他迫切要问的问题吗？我们还剩两分钟。我也很乐意就此开始总结，然后让大家去喝咖啡。那么请允许我补充一下，正如这里写的“未来合作的可能性”。尼科？

尼古拉斯 • 卡巴雷诺： 谢谢荷兰代表。我还有最后一个问题，关于开源软件方面的合作。这部分会包含在合作方案中吗？我之所以这样问，是因为在上届挪威互联网治理论坛 (IGF) 期间，挪威政府一直在分享开源解决方案。目前已有超过 45 个国家和地区正从中受益。那么如果我们 GAC 的杰出同仁们有意了解如何开展此类合作，具体流程是什么？

拉姆 • 莫汉： 我建议他们与主席——也就是我——联系，或联系我们优秀的 SSAC 工作人员。我们将推动对话，共同探讨如何以最佳方式为大家提供内容及其他支持，并开展协同合作。我们对此领域深感兴趣。这是少数几份真正为各位量身打造的 SSAC 报告之一，请来与我们携手合作。我们希望能为各位实现这项工作的价值。如果真的前来合作，这将向我们证明开展此类工作确实是有益的努力。

马尔科 • 霍格沃宁： 谢谢。在此，我要衷心感谢拉姆、苏珊、马腾、塔拉再次参会。也呼应本页幻灯片的主题：期待未来的合作。那么最后，还有谁要发言吗？尼科，我想我们可以享用咖啡了。

尼古拉斯 • 卡巴雷诺： 没有了，只是有些会务通知。我们现在开始茶歇时间，尽情享受吧。我们的会议在 4:30 重新召开。感谢大家。本次会议到此结束。谢谢拉姆。

[听写文稿结束]