ICANN82 | GAC 与 SSAC 联合会议
2025 年 3 月 9 日（星期日） – 16:30 至 17:30（太平洋标准时间）

尼古拉斯 • 卡巴雷诺 (NICOLAS CABALLERO)	女士们、先生们，欢迎回来。我们马上就要开始了。请就坐。茱莉亚 (Julia)，请继续录制。
谷尔顿 • 泰普 (GULTEN TEPE)	大家好，欢迎参加当地时间 3 月 9 日（星期日）16:30 举行的 ICANN82 GAC 与 SSAC 的会议。请注意，本次会议正在录音，并受 ICANN 预期行为标准和 ICANN 社群反骚扰政策约束。 在本次会议中，如果要通过聊天窗口提交问题或评论，请注意形式要适当，我们会大声朗读您的问题或评论。请记得说出您的姓名，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。请清楚表达并保持合理语速，以便翻译人员能够准确地进行翻译工作。同时，请确保在发言时其他所有设备均保持静音。您可以在 Zoom 工具栏中访问此次会议的所有可用功能。接下来，我将请 GAC 主席尼古拉斯 • 卡巴雷诺发言。谢谢大家。交给你了，尼科 (Nico)。
尼古拉斯 • 卡巴雷诺	非常感谢谷尔顿。欢迎大家参加最后但也是最重要的一次会议，依我拙见，至少是与 SSAC 安全与稳定咨询委员会的一次最重要的会议。欢迎拉姆 (Ram)。欢迎你们的优秀团队。事实上，我们在谈论今天将要谈论的一些问题，以及昨天和前天讨论的问题。当我提到量子计算及其对域名系统 (DNS)、DNS 稳定

性和域名系统安全扩展 (DNSSEC) 实施等，以及一般的密码学，对称加密和非对称加密的潜在影响时，每个人都看着我，好像我疯了一样。但无论如何，我们将与这个专家团队深入讨论这个问题。正如我昨天提到的，我们将谈及量子计算及其对加密的影响。

然后，我们会讨论恶意域名注册的推断分析 (INFERMAL)。考虑到 60 名 GAC 新成员，我已经解释了 INFERMAL 的含义。但是我们将在讨论中详细解释。然后我们将讨论后续步骤。再次欢迎拉姆和你们出色的团队。交给你了。

拉姆 • 莫汉 (RAM MOHAN)

非常感谢，尼科。我谨代表 SSAC 对 GAC 的邀请表示诚挚的感谢。这是我们第三次和你一起开会。每一次，我们之间互动的内容都变得更加丰富，合作也更加深入。因此，我们非常珍惜这次机会，以加强我们在关键互联网安全和稳定问题上的合作对话。

对于那些刚接触 GAC 和 ICANN 社群的人，简单解释一下，SSAC 是 ICANN 的专家咨询机构。它致力于识别和分析针对互联网命名和寻址系统的潜在威胁。SSAC 由经验丰富的专业技术人员组成。我们向 ICANN 社群和董事会提供客观且基于证据的建议。

有些时候，我们不提供基于证据的建议。在这些情况下，我们会尽力指明这些是我们向社群和董事会提交的专家意见。我们关注的范围很广，从 DNS 漏洞和网络安全风险到新技术对互联网基础设施的影响，再到互联网监管的安全性、稳定性和弹

性。所以，我们跨越了整个架构。但从根本上说，我们的职责范围是关键基础设施领域。我们参与了这方面的工作。

现在，我们了解了 GAC 在代表政府对互联网监管发表观点方面发挥着重要作用。这种互动，尼科，这种互动确实让我们 SSAC 在技术和政策领域之间架起了桥梁，我们热切希望继续这一合作，确保我们的建议既中肯有力又符合公共利益。那么，这是我们正在开展的一项重点工作。我们渴望分享我们的见解，倾听你们的问题，一起为互联网的安全、稳定和弹性做出贡献。

这确实是我们工作的关键驱动力，也正因如此，我们非常重视与 GAC 互动。谢谢你提到这点。正如你已经提到的，我们确实有两个关键议题想和你们讨论。鲁斯 • 豪斯利 (Russ Housley) 就坐在我右边。鲁斯有着漫长而卓越的职业生涯。除此之外，他还花了相当多的时间研究量子计算及其对加密的影响。所以，我们想让鲁斯来分享他对这个议题的想法。我们的意图并不是让你们听讲座。我们的目的是真正分享我们的想法，然后真正邀请大家加入我们，来和我们聊天。

我们尽可能不让我们的演示过于专业，即使下面的材料非常专业。这就是我们的目标。那么，如果我们改成纯极客语言，就会大声说，嘿，那是什么意思？我们很高兴看到这样的转换。那么，就交给你了，鲁斯。

鲁斯 • 豪斯利　谢谢拉姆！我把导语放在了幻灯片上。还没有人知道答案。量子计算已经出现了一段时间。美国国家标准与技术研究院举办了一场大赛。由此得出的解决方案称为 ML-DSA。这是基于格的

数字签名算法。这个解决方案不太适合 DNSSEC。它太大了。它有非常大的公开密钥和非常大的签名值，所以如果你使用基于 UDP 的 DNS，它并不适合。就是这么简单。

那么，好消息是，我们还有一点时间。因为量子计算机最大的问题是我们所说的即刻收割，延迟解密攻击。因此，这里的问题是，如果你有一堆机密，攻击者会记录并保存这些机密，直到他们有了一台与密码学相关的量子计算机，然后他们可以用量子计算机攻击密钥管理，获得密钥，并解密这些机密。在 DNS 中，不存在机密，所以这不是问题。我们担心的是，我们要有一种数字签名方案，当未来需要应对量子计算机出现时，该签名可实现即时防伪造。

所以，我的第二张幻灯片讲的是我们可以做些什么来应用这些量子数字签名。这是正在进行的研究。互联网研究任务组中有一个小组正在研究后量子 DNSSEC。下周会有一次附属会议。Merkle 散列树似乎是答案的基础。它们是很多问题的答案，包括区块链和证书透明度以及一大堆其他技术。所以，它们在这里也充当基础也许并不奇怪。但是我在幻灯片中放了几个链接。

其中一个谈到如何应用基于有状态散列的签名，这些签名也很大，因此他们正在寻找其他技术。无论如何，下周 IETF 122 上将进行广泛讨论来进一步探索这些问题。但我不指望一年后就会有答案。但是我们还有时间。如果大家对此有疑问，我们是留到最后再提，还是想现在就提出来？好的，如果大家有问题，我很乐意回答。

尼古拉斯 • 卡巴雷诺 谢谢大家。非常感谢。现在是大家自由提问的时间。考虑到 GAC 全体成员，我想请你解释一下什么是数字签名，基础版本的数字签名是什么。

鲁斯 • 豪斯利 当然可以。数字签名是 DNSSEC 的基础。其思路是，在你获得查询响应时，数字签名会附加到响应中。它表示响应内容自最初发布以来未被更改过。因此，它提供了数据本身的完整性和身份验证。

尼古拉斯 • 卡巴雷诺 非常感谢。荷兰代表想要发言。

马尔科 • 霍格沃宁 (MARCO HOGEWONING) 谢谢主席先生。我是来自荷兰的马尔科。感谢你非常简短但深入的概述。我非常意见。还有很长的路要走。然而，我是政府代表。我知道较长的时间跨度往往比你想象的要短。在不涉及太多技术细节的情况下，你现在能给美国政府一些具体的建议吗？我们能做些什么来为不可避免的 DNSSEC 算法更改做准备呢？

鲁斯 • 豪斯利 对于 DNSSEC 可能为时过早。其他安全协议，我们有解决方案。我们也在其他 IETF 工作组中工作，比如 LAMPS，该工作组正在研究公钥基础设施 (PKI) 和 SMIME。我们有安全传输层协议 (TLS)。我们在这三个领域都有 IPSEC。抱歉，是安全 Shell。在

这四个领域，我们都有解决方案，其中的基础设施需要立即部署，以便我们根据需要随时使用。因为这需要几年时间。

如果回顾一下从 SHA-1 到 SHA-256 的过渡，我当时是 IETF 的安全总监，我当时认为五年时间足够了。结果花了两倍多的时间。所以，从基础设施开始，这样过渡才能进行，因为如果没有基础设施与之绑定，后续很多工作都无法进行。这就是我的建议。

尼古拉斯 • 卡巴雷诺　有请史蒂夫发言。

史蒂夫 • 克罗克 (STEVE CROCKER)　谢谢大家。鲁斯，跟进一下这个问题可能比较好，这对于一个政府来说很有意义，我们要做什么？你提到了之前从 SHA-1 到 SHA-256 的过渡。你能说一下在确定新算法后过渡是如何进行的吗？切换到这种新算法是否会与我们曾经经历过和将要经历的任何算法转变有质的不同，或者是否是我们已经有一些实践和经验的另一种算法转变？

鲁斯 • 豪斯利　谢谢史蒂夫。我们不确定答案是什么，但我们知道这次过渡更复杂，因为我们不仅仅是更改变速箱中的一个零件。我们要扔掉整个变速箱，装上一个新的。所以，我认为在这种情况下，你必须考虑，如果要考虑 PKI，那么你是在讨论从根本上改头换面。而不只是更改了其中一部分。我希望我的回答对大家有所帮助。没有？那很抱歉。

尼古拉斯 • 卡巴雷诺 感谢史蒂夫提出这个问题。谢谢鲁斯。还有其他问题和意见吗？鲁斯，我想提一个问题。假设某个政府很好地实现了 DNSSEC、MANRS 和 RPKI 等等。Blowfish 和 RSA 的任意组合，我不知道，DES 还是 SHA-256 或者任意组合，然后突然之间，量子计算有了突破。如果我错了，请纠正我，但是在那种情况下，政府，DNSSEC 基础设施将会自动过时。我理解的对吗？

鲁斯 • 豪斯利 对。然而，大家知道，还不清楚什么时候会发生。我们看到了很多关于量子位数和量子计算机规模不断增加的文献。但到目前为止，我们还没有找到与密码相关的东西。这类增加不是线性的。

而是以跳跃和冲刺的方式出现。所以，当出现时，我们不一定会得到很多警告，基于此我回答了前面那个人的问题。但是 RPKI 和 DNSSEC 是独一无二的，因为他们只需要完整性。毫无疑问，要收割机密。因此，我们有更多的时间，因为现在没有记录，延迟收割，或即刻收割，延迟解密类型的问题。

尼古拉斯 • 卡巴雷诺 那么，我们应该可以接受 DNSSEC、RPKI 和 MANRS 的完美组合

鲁斯 • 豪斯利 对。我们只是在这些问题上有更多的时间，因为它们只处理公共数据并为其提供完整性。

尼古拉斯 • 卡巴雷诺 谢谢鲁斯。下面有请澳大利亚代表和荷兰代表。澳大利亚代表，请发言。

英格拉姆 • 尼布洛克 (INGRAM NIBLOCK) 大家好！我是澳大利亚代表英格拉姆 • 尼布洛克。我知道它们有不同的用途。但是我想知道，你是否能说明一下基于 HTTPS 的 DNS 和基于 TLS 的 DNS 所发挥的作用。很明显，一个是签名，一个是传输安全。但是，实现后量子加密、传输安全方面的新算法会更容易吗？这是否同样会带来我们目前从 DNSSEC 获得的任何优势，因为它也是在传输中加密？

鲁斯 • 豪斯利 是也不是。是的，它们会保护加密点和解密点之间的流量。将其应用于 DNS 时，这是一个逐跳系统。所以，将提供保护。正如我所说，正在通过 TLS 开展工作。我们还没有 PKI 来进行整合。顺便说一下，CA 浏览器论坛将在 IETF 东京会议后的一周讨论这个议题。我希望这个解释对你有所帮助。

尼古拉斯 • 卡巴雷诺 谢谢澳大利亚代表。谢谢你，鲁斯，考虑到 GAC 的新成员，解释一下，PKI 代表公钥基础设施，MANRS 代表路由安全相互协议规范。无论如何，我们可以提供链接和一切内容。接下来有请荷兰代表和那边的那位先生发言。对不起，我不知道你的名字，但荷兰代表请先讲。

马尔科 • 霍格沃宁 谢谢主席先生。我是马尔科，稍微跑题一下，也许连故意抬杠的人也试图避免出现过多的技术讨论。但是在上一张幻灯片中，你提到了 UDP 传输面临的挑战。我记得这不是我们在 DNS 行业中第一次遇到 UDP 作为传输协议的特殊限制。

我相信在当前与密钥长度相关的 DNSSEC 实施中，UDP 传输也发挥了重要作用。我想知道，根据澳大利亚同事刚才提出的问题，鉴于我们着眼于长远利益，是否可以考虑 UDP 之外的其他 DNS 传输方案？

鲁斯 • 豪斯利 已经了解并指定了其他传输方案，只是没有很好的部署。那么，在这一过渡过程中，也许会部署好。

马尔科 • 霍格沃宁 还是那个问题，我们是政府，我们如何提供帮助？

鲁斯 • 豪斯利 好的。

尼古拉斯 • 卡巴雷诺 鲁斯，关于这一点，你能举两三个例子吗？

鲁斯 • 豪斯利 两三个例子？

尼古拉斯 • 卡巴雷诺　　我的意思是替代 UDP。

鲁斯 • 豪斯利　　那么，基于 TCP 的 DNS，基于 QUIC 的 DNS，这些都是基于 TLS 的 DNS。这些例子中均没有单消息限制。

尼古拉斯 • 卡巴雷诺　　非常感谢。荷兰代表？请讲。

彼得 • 托玛森 (PETER THOMASSEN)　　大家好，我是彼得 • 托玛森。我也是 SSAC 的成员，我觉得有些已经说过的话也可以用不那么专业的方式重申一下。这就是我正在努力做的。那么，鲁斯早些时候说签名附在 DNS 响应中，证明 DNS 信息自发布以来没有被更改过。当然，如果每个人都可以附上签名，那就没什么用了。

因此，要附上签名，实际上需要控制一个私钥，并且需要它来计算签名。那么，来自量子计算机的威胁是以某种方式提取该密钥，即使你未被授权提取，然后你可以伪造那些签名。

现在，密码学的另一个应用是加密，就是保护机密数据，使其不可读，除非你有揭秘密钥。这也是密钥的一个应用。重要的是要认识到，量子计算威胁到这两种应用，既包括用密钥计算签名，也包括加密解密。但是这些是不同的使用案例，DNS 不涉及加密和解密。它涉及在你尝试连接到某处并进行 DNS 查询时，检查你获得的签名当前是否有效。

所以，如果你想用量子计算机来破解，必须在很短的时间内完成，几乎是实时进行，而如果你过去记录了来自 HTTPS 传输的加密信息，如果要解密，你可能需要花上五年的时间。那么，如果你的量子计算机有用但速度很慢，将威胁到你的加密数据，但那时它不会威胁到你的 DNSSEC 信息，因为如果伪造签名需要五年时间，到那时没人再对 DNS 响应感兴趣了，对吗？因为你的连接只需要几秒钟。

所以，底线是，就像政府现在可以做的那样，我认为荷兰代表提出的关于 DNSSEC 的问题，大家不要惊慌。这目前是一个需要研究的问题。如果你感兴趣的话，最好跟进一下。但更紧迫的问题当然是保护已存储或传输中的机密数据，此类数据也有同样的密钥提取问题，但这更为紧迫，而且已经取得了比 DNSSEC 领域更多的进展。对，这是我要总结的内容。

尼古拉斯 • 卡巴雷诺　非常感谢。

鲁斯 • 豪斯利　感谢你主持下周的会议。

拉姆 • 莫汉　谢谢尼科。尼科，我想向你和 GAC 提一点，那就是如果这一领域有某种现成的密码手册或入门手册会有所帮助，请写信给我们，我们可以为你提供一些材料，在你们与政府合作时，这些材料可能会对你们的成员有用。因为我认为，理解量子和

DNSSEC 的缺点与量子和共享机密的缺点之间的不同，并向你们政府中的其他人传达此类内容，将十分有用。

尼古拉斯 • 卡巴雷诺 感谢你的介绍。拉姆，谢谢你，鲁斯。我不确定，我并不完全认同你提到的五年时间框架。我忘了他的名字。彼得，但感谢你的解释。我真的认为在不久的将来我们可能会大吃一惊，但希望不会。但无论如何，在请杰夫发言之前，会场或线上还有其他问题吗？我没看到有人举手。非常感谢鲁斯。让我们继续。现在，有请杰夫发言，交给你了。

杰夫 • 贝瑟 (JEFF BEDSER) 谢谢尼科。我是来自 SSAC 的杰夫 • 贝瑟。提出这个问题是为了讨论 INFERMAL 研究。请切换到下一张幻灯片。谢谢大家。INFERMAL 研究是由 ICANN 首席技术官办公室 (OCTO) 的研究人员完成的。针对用于在线危害和滥用（主要是网络钓鱼）的域名，他们的学术研究人员会真正去调查恶意注册。

首先要提醒的是，我在第二段用粗体表示了，这不是一份提供解决方案的报告，这份报告旨在回答社群长期以来提出的问题，即关于网络犯罪分子出于这些滥用目从何处获取域名，某些因素的影响。报告中强调了截至去年 11 月报告发布时的经济激励、主动验证和一些在缓和域名滥用方面的严格限制。

因此，向那些没有读过报告的人解释一下一些关键的结论，经济激励是注册费降低，费用每减少一美元，恶意域名就增加 49%，免费服务，如网络托管，滥用率将提高 88%。域名注册

折扣与恶意注册的大幅增加有关。至于主动措施，对购买域名的人员施加严格限制可以减少 63% 的滥用。

API 访问，即一次进行大量域名批量收购的能力，可能导致注册的恶意域名数量上升 401%，当然，验证的做法，主动验证注册人信息（如电子邮件和电话号码验证）可显著减少恶意注册。请切换到下一张幻灯片。

被动措施，缓和时间，缓和时间对减少域名滥用的影响微乎其微。即使是短暂的正常运行时间也能让攻击者获得有价值的凭证和经济收益。此外，注册服务机构和 TLD 偏好，集中式滥用，恶意注册的分布并不均衡，往往集中在某些注册服务机构和 TLD 中，而且注册服务机构的做法，如提供低价和免费服务，更有可能吸引恶意注册。

这是经过验证的信息，反滥用社群很早就了解到这些信息。简单地说，问题在于它会引发经济方面的问题。买家都寻求最便宜的价格。买家都想找到可以批量购买的地方。我认为，目前世界上大多数国家或地区，都有较大的实体批量销售各类产品和商品，并以最低价格出售。虽然这是对数据的合理解读，但并不一定意味着解决了问题，因为如果你提高了价格下限，仍然有一个最低价格。除非你针对全球所有不同的经济体和不同的货币进行定价，否则无法消除这个问题。

此外，网络犯罪损失，我看到网络犯罪损失从每年 1 万亿美元增长到了每年 10 万亿美元。我知道这两个数字之间差了一个零，但我甚至连一万亿美元都无法想象。1 万亿美元和 10 万亿美元之间的差额，就损失而言，是一个非常庞大的数字。大多数研究表明，在全球范围内，每起网络钓鱼案件的每位受害者

的平均损失为 136 美元。但是，在美国，这一数字猛增，每起网络钓鱼案件的平均损失为 3,500 美元。

我看到了这类数字的不同表现形式，我相信大多数参与反滥用工作的人都知道，这些数字会因不同的研究而异。但事实是，如果每笔损失至少为 136 美元，那么你对一个域名收取多少费用，才能让购买域名用于在网络犯罪中获取暴利时，在经济上根本得不偿失？那么，这是值得考虑的问题，因为我们正在研究制定什么政策，做出什么改变，来缓和或减少利用恶意注册进行网络犯罪、伤害他人和窃取他人钱财的问题。

如果域名从每年 2 美元涨到 10 美元，价格更改会让犯罪分子牟取数十万美元利益的动机有所动摇吗？我提出了这样的问题。再说说验证过程，正如我指出的，这项研究是在 11 月发布的，基于当时的数据。AI 问题，人工智能问题，继续以明显超过量子的速度加速发展。

但是现在能够创建数字化方式生成的身份，你可以用某人的真实姓名，比如对一个 AI 算法说，我需要一个来自这个特定国家的这个特定地区的驾照，格式精准，但是我需要一个真实的人名，这个人要在这个年龄层并且照片要像我本人，或者把我的照片放在上面，目的是以数字方式生成一个身份，然后在注册域名的过程中使用，这确实产生了极大的影响，如果他们能够检查每个注册人的 ID，就可以解决这个问题。

当真人拿着错误的照片或相似的照片冒充时，真中辨伪的能力需要达到一定的水平，你将需要使用 AI 来应对这个问题，因为人类无法以必要的速度做到这一点。那么，除了人工验证流

程，还有什么更好的流程可有助于防止域名遭到欺诈性注册呢？

还有从授权到缓和的检测率问题。这是一个有效的度量吗？我在这里建议的是，所做的大多数研究使用的 DNS 滥用量数字都来自公开来源。不要误解我的意思，这个数量很大，令人震惊。但我认为，DNS 滥用和网络钓鱼的最大问题是，它依赖于实体来查看，成为它的受害者，或试图摧毁它们，并报告。

那么，我们现在正在看的大多数是关于这个议题的报告，我们正在查看所报告的危害。在座的有多少人在手机或电子邮件中收到过网络钓鱼或垃圾邮件，你看了一下，说，这次没上当，然后删除了？如果这个房间里的任何人都没有这样做，并总是报告此类邮件，我给大家点赞。但我不想进行举手表决。这些危害中有很大一部分未被报告。如果没有报告，行业便看不到这类危害，无法进行缓和。

因此，改变注册方法是一个潜在的解决方案或可遵循的途径，但也是更有效检测的机会，这样可以快速缓和这些问题，一个域名出现六七秒钟，就会被捕获并扼杀，而不是出现两天，有人报告，再需要两天来验证，然后关闭。在这四天的时间里有出现多少受害者，而如果我们能更有效地检测，更快地扼杀，又会怎么样？老实说，度量的另一个要点是，这非常难以度量，我不是不管了，我们早就应该进行度量了，但每个域的受害者数量十分庞大，一个做得很好的网络钓鱼，一秒钟内就可能有 100 个受害者。

因此，不一定是进行网络钓鱼的域名数量，上当的受害者数量便能真实地度量问题的规模，因为我们已经知道这个数量，即

使我们讨论的是冰山一角，这些是有关网络钓鱼的公开来源，告诉我们有数百万个域名正在被使用，我们完全承认还有很多没有报告出的域名，我们没有看到，但我们也没有看到有多少受害者真正受到影响，以及这对地球公民的经济影响有多大。

所以，我提出这些内容供进一步讨论，因为 INFERMAL 报告为我们提供了一个很好的验证，是的，我们一直知道低价推动了这种类型的业务，我们知道对注册人的验证和核实极不严谨推动了这种流量。回声加强了效果。但是现在，我们如何采取下一步行动呢？我们如何应对，如何做到更好呢？我们可以做些什么来更好地度量影响，同时看看如何更好地检测，以便更有效地阻止这个问题？

因为我敢说，即使我们开始收取每个域名每年 1000 美元的费用，真正的结果是因为成本而剥夺了地球上大多数人注册域名的能力，但对于网络犯罪分子来说没有任何改变，为了弥补受害人数上的损失，他们会在每个域名上至少赚取 20,000 美元，所以他们不会介意成本的增加。这会略微削减他们的利润，所以我们必须找到其他解决方案。谢谢大家。

尼古拉斯 • 卡巴雷诺　谢谢杰夫。我们能不能，好吧，是的，这正是我的观点。请切换到下一张幻灯片，对。400% 的增长，我很想现在就进行讨论，还有 API 的事宜，就是应用程序编程接口，你在这方面有什么看法？这真的存在问题吗，不法分子可以访问 API，通过使用人工智能或其他方式，他们能够造成更大的损害并增加网络钓鱼活动？是这样吗？

杰夫 • 贝瑟

尼科，批量注册是大量获取域名进行滥用的一种不良手段，对此我毫不怀疑。然而，400%，401% 的指标，不好意思，一个为僵尸网络或恶意软件宣传注册 DGA 或域名生成算法域名的不法分子可能一次会注册 10,000 个域名，这并不会让 API 出问题，因为基于 API 的百分比可能是所有使用 API 的用户中的一个。另一方面，如果你愿意的话，应该加暂停，一旦有人注册了 50 个域名，就暂停一下，看看这些域是否被注册，有没有被用于一些不好的事情，并且可以使用大量基础设施信息来查看它们是否被设置为按预期方式使用。

是的，一次 10,000 个域名，我认为简单的答案是，不可能，但 API 本身应该没有问题。问题在于对 API 的无限制访问。

尼古拉斯 • 卡巴雷诺

谢谢杰夫。那么，现在我来回答 GAC 成员在现场或线上提出的意见或问题。大家可以畅所欲言，会场中没人举手。对不起，有两个人举手。有请印度代表和澳大利亚代表依次发言。首先有请印度代表。谢谢大家。

苏希尔 • 帕尔 (SUSHIL PAL)

谢谢杰夫。我认为很明显，问题在于验证，对不对？我认为，如果我们有注册服务机构的认证证书，DNS 滥用的可能性或影响就会下降，对吗？使用 DGS 算法也是这样，问题并不在于 AI。这是因为，大家知道，这些未经验证的凭证可以通过批量 API 进行共享，对吗？

不知何故，我想也许，虽然问题非常清楚，但我们仍在与 GNSO 权衡如何定义数据的准确性，数据的范围是什么，因为如果我

们不冻结 WHOIS 数据准确性的范围，我想大家永远不会想到去验证，对吗？所以，我认为，GAC 或 SSAC 成员能不能也督促 GNSO 加快这些事情的进展？我的意思是，因为，大家知道，我们都在讨论，我们都知道问题所在，但我们没有任何实质的进展，来遏制这一点。

杰夫 • 贝瑟

我在演讲中有一件事没有说，我可能应该说得清楚一些，就是我们的对手，那些将域名用于此目的的人，领先我们 10 步，领先我们 100 步。最近的一个趋势是，拥有合法凭证的合法人员将创建一个帐户，并在几个月内慢慢建立一个域名组合，然后他们将该域名组合和凭证一起出售给犯罪分子，犯罪分子将这些域名用于某种目的。

虽然更有效的凭证确认或验证肯定有所帮助，但我的观点是，严重依赖这种解决方案是有问题的。真正令人担忧的另一个问题是，这是一次公开会议，我保证我们的对手也会看到这段录像，他们会说，我们知道了什么？我们已经知道他们的策略是什么，他们在做什么，所以他们可以决定下一步要怎么行动。

那么，你的问题是将域名交给合适的小组，接下来呢？我相信这可以追溯到之前提出的观点，也就是说，我认为可以追溯到之前的观点，在之前的幻灯片中，即需要更有效的检测。更有效的检测将会加速缓和过程，这才是真正需要关注的地方，因为我们无法消除人们行窃的经济动机。在人类历史上，人们一直试图消除犯罪的经济诱因，但至今还没有真正成功。

犯罪总是存在的，但是如果我们基本上能找到一种方法让你在成为受害者之前阻止犯罪，或者至少在犯罪动机消失时将危害降至最低，因为有更加有利可图的犯罪。我也不知道这是不是一个好的观点，我是说，让他们进行一些其他类型的犯罪，但重点是，当然，如果能更有效地检测和缓和，将真正有助于这些问题。

苏希尔 • 帕尔

我的意思是，并不是说更有效的检测一定能怎么样，我认为这是最终目标，我所说的验证，并不是说这是全部，但这是第一步，对吗？只是，尽管我们还没有行动，我的意思是，我们一直在谈论，但我们没有采取有效的措施，甚至到目前为止验证流程也没有任何进展，特别是在 gTLD 中，对吗？我们运营的 ccTLD 没有任何问题。

我想我可以分享一下我自己国家的经验，大家知道，我们已经实施了双因子验证流程，滥用者的人数已经显著下降。我希望同样的事情可以重复发生。对注册服务机构来说，这点成本并不算多，但因为这些网络攻击，我们正在付出巨大成本，没有人意识到这一点，因为这些攻击并不指向我们。但这确实会伤害我们的公民，我的意思是，我们所代表的人，但重要的是我们要认识到这是第一步。让我们迈出第一步，不要低估检测和获取监控能力的重要性。

尼古拉斯 • 卡巴雷诺

非常感谢。印度代表，接下来是澳大利亚代表、欧盟委员会代表、英国代表和荷兰代表。澳大利亚代表，请讲。

英格拉姆 • 尼布洛克

大家好，我是澳大利亚代表英格拉姆 • 尼布洛克。我只是想知道 INFERMAL 研究的后续步骤是什么。这份报告中有一个明显的限制，即这不是犯罪分子所做的。这只是他们在看的一个注册服务机构的特征。但我想知道，是否有可能与注册服务机构一起验证假设，因为他们的阻止列表上有他们用于研究的特定域名，比如大批量获得一些可用数据，比如基于注册服务机构可能拥有的数据，在那些特定情况下实施滥用的人实际上使用了什么。是的，我只是想知道实际研究的后续步骤。

杰夫 • 贝瑟

好的，我不得不让你去首席技术官办公室问这些问题，因为我知道报告的作者，以及他们的后续行动。充其量，我只能给你一些道听途说的消息。这可能并非合适的答案。所以，好的。

尼古拉斯 • 卡巴雷诺

谢谢澳大利亚代表。请欧盟委员会代表发言。

杰玛 • 卡罗里洛 (GEMMA CAROLILLO)

非常感谢，尼科。我是来自欧盟委员会的杰玛 • 卡罗里洛。我的同事玛蒂娜 • 巴贝罗 (Martina Barbero) 是 DNS 滥用这一议题的负责人，已经在聊天中提到了这一点。那么，我们将在 DNS 滥用会议上进行报告演示，OCTO 也将参与其中，因此我们可能会向他们提出一些问题。我有两个问题。

还有一个更普遍的问题是，由于这份 INFERMAL 报告得到了很多回应，我们听到了你们对某些方面的一些评论，你们是否有一些针对报告的评论，这样我们就可以查看这些评论，并具体了

解报告中的滥用情况或某些观点，因为这也将有助于我们阅读文件。第二，我明白，API 本身当然不是问题，但问题在于技术方面。那么，既然批量注册似乎存在问题，我们的结论是应该对 API 的使用加以限制，但是我们有没有可能采用批量注册的做法呢？谢谢大家。

杰夫 • 贝瑟

那么，对第一部分的回答是，没有，这些谈话要点和评论并非来自 SSAC 协商一致的文件，虽然我们基本上可以把它作为指引，看看我们是否能够就一份我们可以在 INFERMAL 上阅读的文件声明以及后续步骤达成一致，这显然是值得跟进的。抱歉，第二个问题我已经想不起来了。

那么，就我个人而言，我认为我可以预见公司建立新品牌或新公司标识的机会，他们可能需要在许多 TLD 中注册相同的标识，届时可能会有 2,000 个注册，这些工具将成为一个有效的目的。但我很难看出比这更高的批量注册数量的合理性。但可能有一些我不知道的业务案例。但是我认为，比如说，在印度的那位先生来看，打个比方，拿到驾驶摩托车的执照需要遵循一定的规则。

拿到驾驶汽车的执照也要遵循一定的规则，驾驶半卡车也有不同的规则。根据驾驶车辆的技术不佳所造成人员伤害的程度，你需要拿到不同的执照。如果人们需要驾驶这种车辆，那么我会将大量使用的 API 视为一种更像半卡车或火车司机的工具，在你可以访问它之前，你实际上必须通过更严格的验证，来确

认你是谁以及你的业务目的是什么。那么这就不是工具的问题，而是许可谁使用这种工具的问题。

尼古拉斯 • 卡巴雷诺　非常感谢。下面请英国代表发言。

奈杰尔 • 希克森 (NIGEL HICKSON)　好的，我是奈杰尔 • 希克森，来自英国。将这份重要的报告放在适当的背景下看是非常有趣的，感谢 SSAC 对此的关注。我们一直知道你们会关注。我知道这可能还为时过早，但鉴于你们不时提到的那些建议的重要性，我只是想知道，你们是否会就此继续讨论，形成某种建议或什么的。谢谢大家。

拉姆 • 莫汉　非常感谢，奈杰尔。我们还没有到那一步，还无法决定我们是否应该就此提出建议。我们也请 OCTO 向 SSAC 介绍过这个议题。但是我们没有基于这个议题看看还能做些什么？一部分原因是，这里需要进行的一些工作可能更多地属于 ICANN 政策制定部分，而不是 ICANN 的技术咨询部分。

这份 INFERMAL 报告提供了相当多的技术建议。但这些只是我的想法，但我们还没有在 SSAC 内部进行过具体的讨论。但是谢谢你的建议，我们将在 SSAC 的下一次谈话中提出来，看看成员们的反应如何。

尼古拉斯 • 卡巴雷诺　谢谢你。下面有请荷兰代表。谢谢你。

马尔科 • 霍格沃宁 荷兰代表再次发言。我是马尔科。拉姆，你说得很有道理。我确实认为，就缓和而言，这在很大程度上是一个政策问题。然而，我也听到杰夫谈到改进检测和改进 API。那么，我想知道，在政策讨论之外，是否可以讨论一下改进检测或 API 行为方面的技术标准，从而解决部分问题？是否可以讨论一下技术解决方案？

拉姆 • 莫汉 谢谢。我来简单地说几句，杰夫，也许你也可以补充一下。我不知道是否一定有技术上的解决方案，但我认为可以进行培训。当你遭遇网络钓鱼并上当后，你知道该怎么做吗？你不仅知道如何去检测，还知道如何报告？

因为此时的问题之一肯定是在我们的社群内部，如果没有报告，那么你没有收集到足够的数据来表示报告了 1,000 个案件，另外 1,000 个案件，其中的 10% 没有以某种方式得到回应，接下来我们看看这 10% 或者不管百分之多少，我们看看谁是幕后黑手，看看他们采用的模式是什么，从而试图了解我们生态系统内部的一些行为和特征。

因此，一个可行的做法是真正组建一场有效的培训活动，介绍如何报告滥用问题，报告网络钓鱼，报告这些问题。完成这项工作后，我们就去跟踪接下来会发生什么。然后，我们可以获得数据，这些数据可以给出关键问题的答案，即问题可能在哪里，或者可能是谁导致了问题。

我认为，现在我们正处于这样一种模式，我们经常试图对此采用一种笼统的方法，比如我们制定一项适用于所有人的新政

策，或者我们以某种特殊方式描述某一群体的所有参与者，而这个群体中的参与者，有些可能工作出色，而其他人表现糟糕。

我认为，我们的重点应该放在那些没有达到标准的人身上。一旦我们有了这些数据，我们就可以说这是最佳实践，这是应该遵循的规范，对吗？我认为最佳实践可以在无需政策制定的情况下完成，因为你会说这样更安全，这样可以形成更加良好的生态系统。没什么要补充的。

尼古拉斯 • 卡巴雷诺　谢谢你。拉姆，下一个是多米尼加共和国代表。

安帕罗 • 阿兰戈 (AMPARO ARANGO)　这是一个重要的小组。我是多米尼加共和国代表。这非常偏技术性，但我认为这是当今我们各自国家或地区面临的核心问题。我希望在这里看到，作为像我们这样一个小国家的政府，也就是多米尼加共和国，最后，你确实提到了我们的诉求，我们作为一个政府必须做什么。

首先，我们需要了解我们国家的情况，我们自己的域名管理员和运营商的情况。我作为一名监管人员，监管着电信部门，运营商，我们所有的网络安全中心，我们的攻击响应中心，因为在过去的几年里，比如，两年前，哥斯达黎加刚刚经历了糟糕的情况，花费了他们数百万美元，最后甚至破坏了他们的卫生系统。

所以，这是从政府的角度来看，也许代表你，你没法说得那么清楚，但我认为我们需要策略。需要就如何在我们国家推广 DNSSEC 提出一些明确的方向。有多少人知道这件事，无论是我们的运营商，我们的安全中心，还是我们自己的注册管理机构。我不知道我们国家有没有。但是，如何攻克这个对我们来说至关重要的不安全因素，这个网络安全问题呢？我想听听你们的建议，但我认为必须是来自 SSAC 和 GAC 的建议，因为从长远来看，这必须转化为具体的工具，因为这与培训有关。

制定一个国家层面的战略，让我们所有的系统都在 DNSSEC 内得到监管，这样做成本很高。我不知道你能不能回答这个问题，但是这个问题真的很令人沮丧。我认为我们确实有工具可以至少缓和一下这些影响。谢谢你。

拉姆 • 莫汉

我们在 SSAC 面临的挑战之一是，我们能够提供大量的技术专业知识和技术信息。我们没有完全理解你的需求是什么，你需要那个层面的信息，对吗？所以，我认为我们需要合作，这样我们才能了解你希望我们提供什么样的信息。

我们已经开始着手的事情之一是，过去我们会开展工作，然后发布报告，非常技术性的报告，长度从 10 页到 40 页不等。而我们已经开始着手的事情之一是将这些报告提炼为 50 万字的汇总报告，提供了一种执行简报，介绍了我们在这些报告文章中试图表达的关键内容。但这仍然集中在我们的研究领域，我们认为的重要需求。

那么，我建议你具体和我们谈谈。我们很高兴直接与你合作。但总的来说，请 GAC 辅助我们的工作，澄清两件事。第一，对你有用的信息类型。第二，你需要哪个层面的信息，需要哪个层面的技术细节。因为我们默认是从非常深入的技术层面开始。这就是我们所擅长的。但如果你想让我们提升一个层面或几个层面，请告诉我们，我们可以帮助到你。

尼古拉斯 • 卡巴雷诺　非常感谢。安帕罗，这就是你提的全部内容吗？好的。下面我们需要做个总结。我们还剩一分钟。GAC 最后什么问题或意见吗？请日本代表发言。请讲。

发言人（姓名不详）　非常感谢你的精彩陈述。我想你已经强调了收集有关网络钓鱼和 DNS 滥用的数据的重要性。我认为有各种类型的 DNS 滥用，不仅是 ICANN 定义的那些，还有一些其他的滥用，如 CSAM，可能是侵犯版权，如在日本，盗版漫画是一个非常大的问题，也是一个非常大的经济增长点。我认为根本问题是相似的，我认为有必要收集各种滥用类型和滥用数据，也许可以与政府合作收集数据。你有何看法？

拉姆 • 莫汉　我认为这是一个重要的议题，我们已经准备好和你一起提供技术细节和技术建议，促进合作。但我认为，最终的解决方案可能是将政府部分、技术部分和政策部分结合起来，并在这个论坛内找到将它们融合在一起的方法。

尼古拉斯 • 卡巴雷诺

非常感谢拉姆。我们需要做个总结。感谢你的提问。和往常一样，拉姆，会议非常精彩。很高兴大家能来到这里。尽管对一些人来说，这些对话有点偏技术性，但我们已尽力传达信息。尽大家所能，一方面给我们一些好的建议，另一方面帮助我们打击不法分子。

再次感谢大家。非常感谢。谢谢鲁斯。谢谢你。你有一个出色的团队，拉姆，希望我们能够在布拉格再开一次会。非常感谢各位。向我们来自 SSAC 的朋友致以热烈的掌声。非常感谢你们。现在休会。明天上午 9 点会举行欢迎仪式和社群杰出奖颁奖典礼，到时见。非常感谢。晚安。

[听写文稿结束]