ZH

ICANN83 | 政策论坛 – GAC 安全与稳定会议
2025 年 6 月 11 日（星期三）– 欧洲中部夏令时间 09:00 至 10:15

丹尼尔 • 格鲁克 (DAN GLUCK)　欢迎大家参加于世界协调时 6 月 11 日星期三 7:00 举行的 ICANN83 GAC 安全与稳定会议。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。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。当被叫到时，将允许参会者在 Zoom 中取消静音。请先说出您的姓名以便于记录；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，并保持合理语速，以便翻译人员能够更准确地进行翻译工作。下面有请 GAC 副主席马尔科 • 霍格沃宁 (Marco Hogewoning) 发言。谢谢，交给你了。

马尔科 • 霍格沃宁　谢谢丹尼尔。大家上午好！本次会议由我来主持。我想我们尊敬的尼古拉斯主席正在后面的某个地方享用一杯香浓的咖啡。如大家所见，我们把本次会议分成了两部分。首先，SSAC 将向我们介绍他们即将开展的一些项目。然后，我邀请了 SDNLabs 的克里斯蒂安 • 海瑟曼 (Cristian Hesselman) 向我们进一步介绍

	量子技术如何与 DNSSEC 交互，作为我们在西雅图举行的 ICANN82 会议的后续行动。 在正式开始之前，我们先来快速介绍一下在座的各位。丹尼尔 (Dan) 已经介绍过我了。我是荷兰的 GAC 代表马尔科 • 霍格沃宁。马腾，要不你先开始？
马腾 • 阿尔森 (MAARTEN AERTSEN)	大家上午好。我是 SSAC 成员马腾 • 阿尔森。
沃伦 • 库马里 (WARREN KUMARI)	我是 SSAC 成员沃伦 • 库马里。
格雷格 • 亚伦 (GREG AARON)	我是 SSAC 成员格雷格 • 亚伦。
拉姆 • 莫汉 (RAM MOHAN)	我是拉姆 • 莫汉。我也来自 SSAC，目前担任 SSAC 主席。
克里斯蒂安 • 海瑟曼	我是克里斯蒂安 • 海瑟曼。我来自荷兰顶级域 .NL 的注册管理机构 SIDN。

马尔科 • 霍格沃宁 谢谢！事不宜迟，拉姆，我把发言权交给你了。下面进入第一个议题：域名注册。

拉姆 • 莫汉 谢谢马尔科。请切换到下一张幻灯片。我们想就域名注册数据访问与大家分享一些看法。请切换到下一张幻灯片。我们想确保与 GAC 分享的是我们的目标。我们希望确保关于 gTLD 注册数据访问的所有政策都是定义明确的、完善的，并且能够满足全球互联网社群在防范安全威胁方面的需求。这就是我们要解决的问题。

实现这一目标的方法是创建一个遵循结构化加急机制的访问系统，以便按优先顺序加快处理合法请求（特别是紧急请求）。对于响应时间方面的政策（即涉及“如何”、“什么”和“何时”的政策），这些政策都应明确定义并在社群内部获得广泛认可。我们还认为，ICANN 组织应继续分享关于域名注册数据请求的衡量标准。

我们认为访问注册数据非常重要。这是安全与稳定框架的基础组成部分。我们已经就此向 EPDP 提供了反馈意见，但我们想说的是，这并不是一个与隐私需求相冲突的领域。必须以适当的方式满足隐私需求，但安全和稳定显然是一个值得关注的问题。因此，我们希望确保社群在实施这些变更的过程中考虑到屏幕上列出的这些原则。这就是我们真正想说的。欢迎大家提问或发表意见。

马尔科 • 霍格沃宁 谢谢拉姆！当然，我认为 GAC 会赞同你关于注册数据访问的观点。还有什么问题吗？没有，时间还早。Zoom 中没有人请求发言。团队里也没有人请求发言。好吧，在会议快结束时，我们再回来讨论这个问题。下面转到下一个议题：开源软件。马腾要发言吗？

马腾 • 阿尔森 是的。我们正在研究一个大家可能有些熟悉的主题——自由开源软件。这种软件可以被自由使用、共享、修改甚至研究。我们正在专门研究这类软件在全球 DNS 中发挥的作用。我们认为，这种软件的依赖性很强，但此前并没有针对这类软件进行过广泛研究。

自由开源软件在开发和管理方面有其独特性。尽管世界各地的人们都在讨论基础设施、可靠性、软件等问题，但我们认为，让人们了解这类软件的作用和特性，以确保在政策讨论中能考虑到这些因素，这是件非常有价值的事情。这项工作有两个目标。一是让大家了解这种关键的依赖性。二是让大家了解这种软件的特性，并告知大家一些假设，这些假设对一般软件来说是合乎逻辑的，但对这种特殊类型的软件来说可能并不成立。这算是一个简短的预告性介绍。

请切换到下一张幻灯片。我们主要关注四个方面。我们开展了一项调查，旨在了解全球的状况。我们关注域名注册方面的情况。我们还关注 DNS 方面的情况；人们在 DNS 上发布和检索映射，从而了解全球状况。我们分析这类软件的特性（包括它的开发模式），这与实物或其他软件的惯常假设并不相同。我们

在自由开源软件领域内展开对比研究，验证这些通用特性是否适用于当前语境下重点关注的 DNS 流行软件。

第三部分旨在澄清我们在实践中看到的、那些不成立的假设，并指出存在误解的地方。最后，我们尝试列出在政策制定或监管中需要考虑的相关风险因素。这些风险既涉及这类软件的开发，也涉及运营。这些基本上就是我们涵盖的领域。

请切换到下一张幻灯片。在马斯喀特会议上，我们有望向大家介绍这方面的更多内容，因为我们计划在今天这次活动之后的几个月内发布这份报告。稍微透露一点，我们认为在 DNS 和域名注册中使用自由开源软件是一大优势，但需要考虑其中的风险。在这方面，我们可以就如何使用自由开源软件提供一些指导。以上就是今天的全部会议内容。我很乐意回答问题。

马尔科 • 霍格沃宁　这确实是一个简明扼要的预告性介绍。关于这项工作，大家有什么问题要问马腾吗？我来看看有没有人举手。我看到印度代表又举手了。

萨吉德 (SAJID)　谢谢主席先生。我是印度代表萨吉德。我实际上想向拉姆 • 莫汉先生提问。因为时间不够，刚才错过了向你提问的机会。我们有一个共同的目标，即应在 24 小时内提供注册数据。但现在已经过去 24 个多月了，我们仍在努力让 ICANN 就时间表达成一致——更别提 24 小时了。我的意思是，不要去管什么时间表。到目前为止，我们还没有任何时间表。

尽管 GAC 和 SSAC 都多次强调了紧迫性，但由于时间太长，我认为现在已经进入了双轨制：一边是认证轨道，另一边是政策轨道。拉姆，作为 SSAC 的主席，或许还是 GAC 副主席，你认为 SSAC 和 GAC 发表一份联合声明，是否能有效地促使 ICANN 董事会尽快就时间表做出决定？

拉姆 • 莫汉 谢谢你的发言。我们赞同，对于紧急请求，处理流程应非常明确。我相信，目前已经在与必须实施这些变更的各方进行讨论。我还不能代表整个 SSAC 表态，我需要与成员们商议。但我们一直非常明确地表示，如果某事被界定为紧急情况，就应该将它当作紧急情况处理，而且应对措施应该非常迅速。这不该是一个耗时很长的事情。如果与 GAC 共同采取行动有助于推动此事，我们对此持开放态度，以此彰显此事的重要性。我们认为这是一个重要的问题 部分原因在于，我们必须明确“紧急”即是真正紧急，“紧急”就意味着不能按常规流程处理。

马尔科 • 霍格沃宁 谢谢拉姆，我完全赞同。众所周知，GAC 至少在最近的五份公报中都提到了紧急请求，我记得还包括一些建议。我们很积极，或者说我们的一些同事很积极地加入了研究这个问题的小组。在我看来，这项工作正在取得进展。我同意你的看法，对于紧急请求来说，其进展速度可能并未达到所需的紧迫程度。我很乐意与拉姆保持一致。我们要记住这一点，并考虑一下是否认为联合行动有助于推动进展。我很乐意接受这个观点，我

们稍后再讨论这个问题。大家还有其他问题吗？我看到有人在示意我。抱歉，有请拉塞尔发言。

拉塞尔 • 沃鲁巴 (RUSSEL WORUBA)

谢谢主席先生，也谢谢我们尊敬的 SSAC 同事们。你们的工作非常出色。我是 SSAC 的忠实粉丝，感谢你们在这方面所做的工作。我有一些感想。我认为，欠服务地区的许多国家在 ccTLD 层面运行 DNS 时严重依赖开源软件，主要是 BIND。当然，随着形势变化，我们非常期待这项研究的结果。你们能否提供一些目前的基本情况（尤其是各地区的情况），以便我们更好地了解情况？谢谢。

马腾 • 阿尔森

谢谢你提出这个问题。我先稍微透露一点。在现状调查中，我们试图获取关于“谁在使用什么”的硬性数据。目前的草案（尚未定稿）指出，全球 DNS 在开源软件上运行。并非只有你们是这样，我们也有统计数据证明这一点。例如，在 ccTLD 领域，排名前 25 的运营商中有 20 家使用开源软件。如果把 gTLD 领域也加进来，则 10 家中有 9 家在使用开源软件。如果看一下根服务器系统，12 个系统中有 9 个专门使用 FOSS。

我认为这份报告的价值之一，就是向更广泛的受众揭示——也许一些从事技术工作的人已经知道——这类软件无处不在。我们希望能揭示这些信息，因为我们发现在一些地区，软件受到监管，而 FOSS 却是事后才考虑的选择。由于自由开源软件在开

发模式、资金来源以及用户群体方面的特性是如此不同，现行策略可能难以奏效。是的。

马尔科 • 霍格沃宁　谢谢。我听说德国代表也在等待发言。下面有请鲁迪发言。

鲁迪 • 诺德 (RUDY NOLDE)　谢谢。我是德国代表鲁迪 • 诺德。我原本想问你们对政策制定者有什么建议。我看过最后一张幻灯片后，已经知道你们将为政策制定者提供相关指导，你刚才已稍微透露了一点。我有些心急，你能否大致透露一下，给我们提供的这些指导或建议会朝哪些方向展开？

马尔科 • 霍格沃宁　好的，我不想占用同事的时间，我就长话短说。我们目前的思路是揭示一些常见的误解。举例来说，一个很自然的误解是，你可能把合同关系当作政策机制。比方说，我们负责监管本地区的关键基础设施运营商，然后他们会对其供应商进行监管，这些供应商又会对自己的供应商进行监管，以此类推。

这种做法可能适用于实物材料，有时也适用于软件。由于软件基本上是从互联网上下载的，这种做法就行不通了，因为这种情况下不存在合同链。所以，认为这种机制会有效的想法是一种误解，在实践中它并不奏效，因为有大量软件是由专门的团体开发和维护的，但其使用范围远远超出了支持合同或此类机制所能覆盖的范围。

在建议方面，我们可能会就特定领域提出一些想法，比如如何在这方面与开发者打交道，或者如何思考。但是，如果你对运营商施加的要求限制了其选择一流软件（很有可能就是自由开源软件）的能力，你可能无法实现自己希望达到的政策目标。这就是我们要探讨的方向，不过拿到现在讨论就有点不合时宜了。我们需要先发布这份报告，之后我很乐意回来和大家探讨这个问题。

马尔科 • 霍格沃宁　报告公布后，我们很乐意邀请你回来，继续与大家探讨这个问题。我想没人要发言了。时间有限，我建议我们进入最后一个 SSAC 议题——这也是我个人非常感兴趣的一个议题——即“DNS 拦截再探讨”。格雷格要发言吗？

格雷格 • 亚伦　好。谢谢。这份报告是 SSAC 约在 12 年前撰写的两份报告的更新版。DNS 拦截并非新鲜事物，但我们认为现在是更新这份报告的时候了，因为世界各地出现了许多实施 DNS 拦截的新案例，我们也观察到了这些行动所带来的后果。在此期间，还开发了一些新技术，对 DNS 拦截以及人们获取互联网资源的方式产生了影响。这个小组由大约 20 名 SSAC 成员组成。沃伦和我共同担任该小组的联席主席。

那么，什么是 DNS 拦截呢？当你在电脑前想要访问某个网站时，你需要输入网址（域名），然后你的查询会被转到 DNS 解析器。我们称之为“递归解析器”。它通常由 ISP 运行。然后，递归解析器负责查找你目的地的 IP 地址，将你的域名转化

为 IP 地址，最终 DNS 系统会确定目的地，让你能够与你想要访问的网站进行通信。

通常，这个过程几乎是瞬间完成的。你就能到达你想去的地方。然而，递归解析器可以拦截域名。这意味着解析器会告诉你一个与预期不同的结果。基本上，可通过两种方式实现这一点：第一种方式：递归解析器可能告诉你，你想要访问的域名不存在，而实际上它存在。例如，你想访问维基百科，但没有得到答案，你无法连接到维基百科。第二种方式：你不是被带到想要访问的网站，而是被重定向到另一个目的地。所以，一种说法是，递归解析器给了你一个意料之外的答案，有些人甚至会说是它在欺骗你。它没有给你 DNS 中实际存在的答案。

因此，DNS 拦截是一种技术，也是一种工具。与任何工具或技术一样，它可用于各种目的：既能被娴熟运用，也可能操作笨拙——就像一把锤子。你可以用锤子盖房子。这很棒。但你也可能用锤子砸别人的头，这就不是好事或好的用法了。它的设计目的基本上是阻止人们获取内容或使用某项服务。这不仅影响网站访问，也影响任何使用 DNS 的行为。因此，它还会影响电子邮件、网络管理以及其他所有依赖 DNS 的功能。

请切换到下一张幻灯片。DNS 解析器就是甘道夫 (Gandalf)——在 SSAC，我们总喜欢搞点流行文化梗。请切换到下一张幻灯片。DNS 拦截会被用于许多不同的目的。因此，动机很重要。它的用途之一就是提供安全保障。解析器可能不会把人们带到——哦，太戏剧化了。电力被切断了。可以设置 DNS 解析器，

使其不会将人们带到含有恶意软件、网络钓鱼攻击或类似内容的网站。此时，DNS 拦截被设置成一种有益的服务。

我们在座的每个人都可能以某种方式受到 DNS 拦截的保护。例如，几乎所有的网页浏览器都有一个这样的系统：当你访问已知的网络钓鱼网站时，它会弹出一个警告页面，不允许你访问这个网站，直到你决定真的要访问这个网站为止。DNS 拦截在许多系统中普遍存在，几乎无处不在，其设计初衷通常是帮助和保护人们。这通常是在本地层面完成的。因此，你可以在公司选择一家提供商来帮助你确保网络安全。

有些人使用 DNS 拦截进行内容控制。例如，你当地的公共图书馆可能不允许读者访问社群认为不应该从图书馆访问的某些类型的网站。例如，赌博或色情网站，因为图书馆里有儿童。某些公司在内部使用 DNS 拦截，因为他们不希望员工在工作时间内使用公司网络进行某些活动，如访问社交媒体或赌博网站。这也是一种本地设置，由公司决定其工作场所要采取的政策。

最有争议的是利用 DNS 拦截来阻止人们访问内容，尤其是在国家层面进行拦截的情况。换句话说，阻止整个国家的公民访问特定位置或查看特定内容。这就是我们为什么希望向政策制定者、GAC 成员等展示这些信息的原因之一，因为这些决定会影响很多人。

有时候是因为法律有规定，所以才需要进行拦截。例如，某些国家不允许公民访问已知分发儿童性虐待图片的网站。这样做是为了保护儿童和公民。各国都拥有这些域名的列表，并将它们分发给自己的 ISP。最具争议的是，在某些地方，DNS 拦截被

用来阻止访问表达政治观点的内容。此时，DNS 拦截就是用于审查目的。

请切换到下一张幻灯片。我们要区分 DNS 拦截与域名暂停。它们有相同的目的，即阻止某些内容。但 DNS 拦截并不会从互联网上删除内容。如果某些人被拦截了，其他人仍然可以访问这些内容。域名暂停则是通过撤销域名使其失效，从而阻止访问内容。如今，每天都有数千个域名因安全和滥用问题（如网络钓鱼网站）而被暂停。

有时候，网站也会因法院命令而被关闭，这样它们就对所有人停止服务了。例如，在这幅图上，执法部门会根据法院命令关闭网站，以防止犯罪活动。他们可能会完全关闭网站，也可能会重定向并接管网站，将其放在新的域名服务器上。这是两个不同的概念，但它们通常用于类似的目的，即阻止访问。

请切换到下一张幻灯片。这是这份报告中的一个说明。在这份报告中，SSAC 讨论了用于 DNS 拦截的各种技术以及部分动机。当然，人们可能会对具体情况有不同看法。在一个国家非法的东西在另一个国家可能并不违法。人们可能对法院决定阻止某件事情的利弊持不同意见。我们不会对任何具体案例做出评判。请切换到下一张幻灯片。

沃伦 • 库马里　　谢谢。正如格雷格所说，DNS 拦截是一种工具。与任何工具一样，它也有自己的优点和缺点。了解这个工具的工作原理也很

重要，这样你才能更好地了解如何使用它，而不会在使用过程中意外伤到自己。

DNS 拦截的工作原理是：在递归解析器上设置列表，规定哪些域名应该被解析，哪些不应该被解析。这带来的一个影响是，它只适用于实际使用这个递归解析器的用户。这意味着，如果用户决定使用其他递归解析器，他们将能够绕过或规避拦截。

在下图中，用户将自己的查询发送到其 ISP 提供的某个标准解析器。如果用户要查询的域名没有问题，就可以正常解析该域名。但如果该域名在 DNS 拦截列表上，就会发生其他情况。要么你会收到该域名不存在的响应，要么递归解析器可能会尝试将你重定向到其他地方。但如果用户的查询没有发往负责执行拦截的递归解析器，而是发往了其他解析器，并且那里没有执行拦截，用户就能够正常访问互联网。

请切换到下一张幻灯片。那么，用户如何才能使用不同的解析器呢？目前存在大量的公共解析器，而且很多用户都在使用公共解析器，这是一种显而易见的方法。杰夫 • 休斯顿 (Geoff Huston) 的 APNIC 研究显示，目前约有 21% 的用户在使用全球知名的公共解析器。例如，谷歌的公共 DNS、Cloudflare 运营的开放式公共解析器，Quad9 也有类似的解析器，这些解析器还有政府提供的版本。这方面一个众所周知的例子就是 DNS4EU，这是一项由政府赞助的公共解析器服务。因此，即使是技术不太精通的用户，也能轻松更新他们的递归解析器设置，选择指向其中一个替代 DNS 服务器。

请切换到下一张幻灯片。如果你在过去几年看过任何流媒体服务，肯定会看到过各种 VPN 服务的大量广告。常见的如 NordVPN 和 Surfshark，但这类服务数量庞大。它们为用户带来了一些好处。它们增强了用户隐私，提供了更高的匿名性，并且它们的广告也相当明确地指出，这些服务旨在绕过地域限制。

例如，如果你在旅行，并希望观看本国的流媒体服务，或访问本国可用的内容，你只需启动 VPN，互联网便会认为你身处那个国家。另一个典型用途是：如果你在一个国家，但想观看该国不可用的内容，你可以启动 VPN，选择你想出现在的国家的端点，互联网便会认为你身处那个国家。

这意味着，你正在使用一组不同的递归解析器，并且在互联网看来，你并不在你实际所在的国家。如果某一组递归解析器实施了拦截措施，你只需开启 VPN 就可以轻松绕过这些解析器。请切换到下一张幻灯片。下面的时间交给你了。

马腾 • 阿尔森

请切换到下一张幻灯片。这个过程会出现什么问题呢？过度拦截是指拦截范围过广。例如，你可以拦截三级域名，这比拦截二级域名或在 TLD 层面拦截更精确。如果拦截范围过广，可能会切断对多个目的地或多个网站的访问，这会给那些访问本身并无问题的网站访客带来不便。

这通常发生在你拦截了错误的地方时。顺便说一句，报告中有很多关于这些情况的案例，如果你想深入了解细节，我们建议你看一下这些案例研究。举一个过度拦截的例子：意大利有一

个系统，它会向 ISP 分发一些需要拦截的域名列表。有一次，他们不小心列出了一个用于基础设施的域名，从而造成了过度拦截，例如，这导致意大利用户短时间内无法访问 Google Docs，直到有人意识到这个错误。这个错误给人们带来了不便，阻止他们访问各种完全没有问题的内容。这是一种附带损害。如果操作不当，就会影响到你本不想影响的人。

请切换到下一张幻灯片。正如沃伦所说，人们可以绕过拦截。因此，每当发生拦截时，你可能应假定有些用户会设法绕过它，特别是当他们有强烈动机这样做的时候。他们可以使用 VPN。他们可以使用替代解析器。事实上，还有其他技术可以帮助人们保持内容可用或允许用户访问内容。因此，DNS 拦截的有效性往往是一个程度问题。有人以为，拦截某个域名并向我们国家的 ISP 下达命令，问题就能解决。这确实能解决一部分用户的问题，但很可能无法解决所有用户的问题。请切换到下一张幻灯片。

沃伦 • 库马里

当拦截某个域名时，递归解析器可能会做出两种常见回应。一种是直接回复该域名不存在。另一种是递归解析器将用户重定向到其他地方（这种回应越来越受青睐）。这种类型的拦截似乎正在增多。我们认为这相当危险。

原因在于：如果用户试图访问某个网站（例如 foo.bar.com），但却被重定向到其他地方，他们的网络浏览器会弹出一条警告，说该用户试图访问 foo.bar.com，但该用户正在连接的网络服务器并不是 foo.bar.com。用户会被训练成习惯性地直接点击

这些警告消息，而这会带来严重的安全隐患。主要问题是他们学会了直接忽略这些警告弹窗。虽然这次发生在访问某个被 DNS 拦截的网站时，但下一次，就很可能是发生在访问他们的网上银行或类似的重要网站时。所以，德鲁克曼 (Druckmann) 提出的一个观点就是：如果你打算执行 DNS 拦截，请不要进行重定向。

这就引出了下一部分内容，即建议部分。还是由我来介绍这部分内容。正如我们多次强调的那样，DNS 拦截是一种工具，就像任何工具一样，尤其是功能强大的工具，它们可以用来做好事，但如果你不完全了解它的具体工作原理，并且没有阅读警告说明，你最终可能会严重伤害到自己。因此，如果你要实施或强制实施 DNS 拦截，请确保你真正了解其工作原理，同时也了解其附带损害和副作用。

马腾 • 阿尔森

请切换到下一张幻灯片。因此，SSAC 提出的第二条建议是，如果有人打算强制实施某种拦截（可能在公司内部、在单个 ISP 层面或在国家层面），你应该遵守以下指南。其中一些指南主要基于医疗领域的“不造成伤害”原则。

首先，你应该了解 DNS 拦截能否实现你的目标。可能有其他替代方法来解决你的问题。又比如，如果你要实施拦截，可能会有一些用户会绕过拦截。这对你有帮助吗？还是说这还不够？其次，你应该制定明确的政策，规定你要拦截什么以及如何实施拦截。你应该有明确定义的程序来审查拦截列表上的内容，并将风险降到最低。例如，你应该了解如何纠正错误。我们不

会推荐具体的政策和程序，因为它们应因你的目标和任务而异，但这却是一项重要原则。

第三，在实施过程中要尽量减少过度拦截或可能影响用户的附带损害——即你负有管理责任的人群。比如，你公司里的员工。最后，你不应影响你管理责任范围之外的人群。以欧洲为例，这里有许多国家。欧洲的某些 ISP 同时为多个国家的客户提供服务。如果你在 A 国，而 ISP 同时为 A 国和 B 国的用户提供服务，那么当 ISP 收到 A 国的拦截令时，会发生什么情况？

因为 A 国是该公司所在的司法管辖区。

ISP 如何做到在拦截的同时不影响 B 国（司法管辖赛区之外）的用户？我们必须意识到，虽然地图上的国界线清晰可见，但互联网的边界并不与之完全重合。因此，核心原则是：谨慎避免对无权干预的对象造成影响。请切换到下一张幻灯片。

沃伦 • 库马里

我会讲得非常快，因为我们没时间了。最后一条建议是针对解析器运营商的。SSAC 建议他们使用这份新的 RFC 来注释错误消息（包括拦截）并说明出错原因。我们继续。实际上，我觉得我们也没时间提问了。

马尔科 • 霍格沃宁

好的，虽然时间紧迫，但非常感谢。这份报告内容非常详尽。作为目标受众之一，我对此深表赞赏。它引发了许多值得思考的问题。尽管时间有限，但我想还可以再接受一个简短提问。

我看到巴布亚新几内亚代表已在聊天区留言。拉塞尔，你是否要提问？

拉塞尔 • 沃鲁巴

谢谢马尔科。我国此前受邀参与了关于“保护性 DNS”的试验。我想确认这是否就是本次讨论所指的保护性 DNS？

马腾 • 阿尔森

是的，保护性 DNS 可通过 DNS 拦截来实现。例如，我们提到的公共解析器就是提供保护性 DNS 的。例如，它们会拦截网络钓鱼和恶意软件以保护用户。这确实是可用于保护用户的技术之一。需要补充说明的是，本报告已被用于为日本当前正在讨论的一些政策决策提供参考，该国正考虑对特定类型的内容实施境内拦截。

沃伦 • 库马里

补充一个非常简短的更新。Cloudflare 是提供公共解析器的机构之一。他们至少提供三种不同地址：第一种是标准的 1.1.1.1，它根本不做任何拦截。第二种是 1.1.1.2，它拦截恶意软件。第三种是 1.1.1.3，这是一种保护性更强的 DNS，它拦截恶意软件和成人内容。

我个人认为，如果要向一大批用户提供保护性 DNS 服务，用户应该能够选择他们想要的防护级别。如果你是家长，你可能想要拦截成人内容。你可能会选择提供这种功能的保护性 DNS 服务。但如果你是成年人，你可能希望能看到这些内容。因此，我认为这是一个选择加入与选择退出的问题。这又回到了我们

之前说过的一点，即存在不同类型的拦截以及不同的受影响人群。如果是你自己选择这样做，或者说你主动选择接受这种保护，这很可能比由他人强加给你的保护更站得住脚。

马尔科 • 霍格沃宁 很好。谢谢沃伦。还有三个人在等待发言。我就此关闭队列。请大家长话短说。如果每个问答都只用一分钟时间，时间上就能回到正轨。首先有请刚果民主共和国代表布莱斯发言。

布莱斯 • 阿兹特米娜 • 基金吉 (BLAISE AZITEMINA FUNDJI) 好的，非常感谢。我是刚果民主共和国代表布莱斯 • 阿兹特米娜。我对 VPN 有个担忧。虽然我非常感谢 VPN 工具所能提供的安保与安全，但同时，从公共政策的角度来看，我对“位置伪装”(de-location) 感到担忧。主要是在所谓的发展中国家，人们使用 VPN 并非真正出于安全与安全考虑，而主要是为了隐藏到另一个地址（通常是另一个国家），只是为了显示我在另一个国家。而这有时对一些国家来说构成安全或公共政策的违规。

我们看到一些流媒体平台已经找到某种解决方案。当你通过 VPN 或代理连接时，它肯定会告知“你没有资格或你没有访问权限”。那么，如何在安全、安保与地理位置准确性之间取得平衡呢？谢谢。

马腾 • 阿尔森 我认为 SSAC 并未考虑所有影响。事实上，VPN 的使用范围很广，就像很多工具一样，它们的用途也有好有坏。犯罪分子利用 VPN 隐藏自己的行踪。VPN 利用了互联网的工作方式，因此

它们会长期存在。有些公司会维护已知 VPN IP 的列表。例如，他们会利用这个列表对来自这些地址的流量进行风险评级。因此，可以使用一些工具来检测和分析 VPN 流量。

沃伦 • 库马里

对此再补充一点。VPN 的设计初衷是使其看起来像普通的互联网流量。因此，一些地方（无论是在公司内部还是在国家层面）都曾试图禁止使用 VPN。最终的结果似乎是，他们能够拦截大型 VPN 服务，但用户希望能够访问他们想访问的内容。因此，用户会改为使用知名度较低、追踪较少的 VPN，而这最终可能给他们带来更大的风险。我认为，当你试图阻止某项能让用户访问他们想要内容的技术时，应始终考虑其带来的负面后果。他们会找到办法达到目的，而且可能采取风险更高的方式。

马尔科 • 霍格沃宁

谢谢沃伦。我先来回答前两个问题，然后你可以简要回应一下。第一个举手的是印度代表。我们要做简要介绍吗？

苏希尔 • 帕尔 (SUSHIL PAL)

谢谢。我是印度代表苏希尔。你认为政府支持的 DNS（如欧盟 DNS）与其他公共 DNS 相比有什么显著优势吗？第二个问题是，我认为 VPN 有其存在的必要性。当然，前提是它们是已知的 VPN。安全机构是否正在研究用于监控未知 VPN 的方法？

马尔科 • 霍格沃宁	阿什文要发言吗？好的。
马腾 • 阿尔森	关于“欧盟 DNS”，我能告诉你的就是他们在网站上介绍的内容。他们表示，他们是为了维护主权而建立这个 DNS。欧洲提供“欧盟 DNS”是为了将流量留在欧洲内部，而不是将流量发送到大型商用公共解析器。请自行理解其说法。安全机构是否会想方设法地监控未知 VPN？我并不确定。
苏希尔 • 帕尔	这是否是安全机构担心的问题？
马尔科 • 霍格沃宁	最后有请印度尼西亚代表发言。
阿什温 • 萨松科 • 萨斯特罗布罗托 (ASHWIN SASONGKO SASTROSUBROTO)	好的，谢谢。我只想听听你对拦截的看法，因为你提到了拦截的负面影响。如果采用的方法是“不允许所有 DNS 进入我们的网络空间，而是只允许我们想要的 DNS 进入”，那会怎样？例如 .go.id，好吧，大家都可以访问这个域名。这个是 .com 域名。我会发现，这个是允许的，这个也是允许的，其他的都是不允许的。与其说是拦截，不如说我们实际上是拦截一切，只允许我们批准的 DNS。谢谢。

沃伦 • 库马里

我真的不确定这样做是否可行。互联网上有数百万个网站，因此建立一个允许查看的网站列表是非常困难的。不过，即使你能做到这一点，如今在技术上也不可能完全拦截所有的 DNS 访问。现在有许多新技术，如基于 TLS 的 DNS、基于 HTTPS 的 DNS、基于 QUIC 的 DNS，在使用这些技术的情况下，查询实际上根本不会被识别为 DNS 查询。它看起来就像其他互联网流量一样。因此，你唯一能做的就是拦截你国内的所有互联网访问，将整个国家与互联网断开连接，并禁止 Starlink 和其他卫星提供商。只要你还连接到互联网，就总会有一些 DNS 流量能够出去，人们也就能够访问内容。

马腾 • 阿尔森

沃伦提到的那些技术基本上是加密相关技术，旨在保护发出查询的最终用户的身份。这些技术都是为了在互联网上提供更强的隐私保护。谢谢。

马尔科 • 霍格沃宁

抱歉打扰一下，这是一个非常有趣的议题，已经引起了热烈的讨论，我认为它值得后续跟进。同时，我们身后是完整报告的二维码。请大家务必阅读这份报告。它已经发布一段时间了。在此，我要感谢拉姆、格雷格、沃伦和马腾。请随意留下来。话不多说，我想把话题转到我所说的后续议题上，即我们在西雅图会议期间关于量子计算及其部分风险的讨论的后续内容。我想请来自 SIDNLabs 的克里斯蒂安 • 海瑟曼向我们介绍这如何影响 DNSSEC，特别是我们作为政府代表可以做些什么来帮助缓解其中一些问题。有请克里斯蒂安发言。

拉姆 • 莫汉 马尔科，在此之前，我想代表 SSAC 向 GAC 表示感谢。我们非常珍视我们持续的互动与合作，并期待未来有更多这样的交流。谢谢。

马尔科 • 霍格沃宁 谢谢。抱歉，有请拉姆发言。然后才是克里斯蒂安发言。

克里斯蒂安 • 海瑟曼 谢谢马尔科。好。正如马尔科所说，本次演讲是关于量子计算机和 DNSSEC，以及这些未来机器可能带来的影响。在演讲的最后，我从政府角度向 GAC 提出了一些行动建议。幻灯片不见了。不管怎样，我还是继续讲吧。你们刚才看到的图片是我从德国莱布尼茨计算中心获得的，他们正在那里研究这些量子计算机。但这些量子计算机仍处于实验阶段，我不会说是科幻小说。我们这里讨论的是长期研究。好了，幻灯片恢复了。好的，谢谢大家。

请切换到下一张幻灯片。好的。你对量子计算机的期望是什么？我要补充一点，我并不是量子计算机方面的专家。我是分布式系统方面的专家。量子计算机或量子计算机方面的专业知识主要属于物理学家的范畴，而我并不是物理学家。这就是我在文献中读到的内容。人们对量子计算机的期待是它能带来新的应用，比如新的药物研发方法、改进的机器学习技术或革命性材料的开发。

但正如格雷格已经提到的，技术可以有不同的使用方式。这就是格雷格谈到的“锤子”，你可以用它做好事，但它也存在某

些风险。量子计算机的缺点在于，它们可能会破解我们当前使用的加密算法。其中可能包括 DNSSEC 使用的算法，这些算法正被用于验证 DNS 消息的真实性和完整性。

幻灯片又没了。你们希望我继续讲，还是等幻灯片恢复？好了。幻灯片恢复了。好了。DNSSEC 使用量子计算机的风险在于，它们有可能破解 DNSSEC 用来验证 DNS 响应真实性和完整性的加密算法。潜在的风险是，攻击者可以使用被破解的密钥重新签署 DNS 消息，并伪装成合法来源发送虚假消息。其后果包括：人们最终访问错误的网站，或者软件组件会连接到错误的网站。

我要补充的是，这里假设的是我们已经生活在后量子时代。所以，不是现在，而是未来。这不是“现在存储，稍后解密”类型的攻击，而是一种几乎可以实时解密或破坏 DNSSEC 密钥的攻击。但专家认为，这还需要 10 到 15 年才会发生。你们可能会问，为什么我们现在就要研究这个课题？

请切换到下一张幻灯片。这是因为在 DNSSEC 中添加新的加密算法或更换加密算法需要很长时间。这张图来自一篇论文，它展示了 DNSSEC 中一种加密算法的发展过程。从 IETF 的初稿，到右侧达到实质性的部署水平。如各位所见，这大约需要 10 年时间。我认为这是基础设施更新的典型特征。引入新的 DNSSEC 算法也是如此。因此，如果量子计算机将在 10 到 15 年后成为现实，我们最好从现在就开始思考 DNS 领域该如何应对。

好了。请切换到下一张幻灯片。除了时间因素外，DNSSEC 目前已有相当规模的部署。在左侧，你可以看到哪些国家已用

DNSSEC 签署其 ccTLD。绿色的国家（图例中绿蓝相间）是那些实际已投入运营的国家。这大约占全球的 48%。如大家所见，右侧显示的是验证情况。这张地图看起来更偏红色和琥珀色。这是因为这些签名的验证采用率较低。因此，这方面仍有待改进。但如大家所见，目前 DNSSEC 的部署规模相当可观。结合量子计算机来看这一点就尤为重要，特别是在假设验证率和签署率（左侧）在未来都会增加的情况下。

请切换到下一张幻灯片。如果你想保护 DNS 免受量子计算机的威胁，我们确定了三种策略来实现这一点。它们分别是替换、重新设计和弃用。“替换”是指用新的后量子安全算法替换 DNS 中现有的加密算法。“重新设计”是指彻底重新设计 DNSSEC 系统，这是表格中的第二个选项。“弃用”是指完全放弃使用 DNSSEC。

这三种方法各有优劣。例如，“替换”策略相对容易实施。它是标准化的，但存在操作风险。稍后我还会介绍这个策略。“重新设计”实际上是对 DNSSEC 的一种推倒重来的方法，此方法会使用诸如 Merkle 树之类的新技术。它会降低操作风险，但需要全面改造整个 DNSSEC 系统和协议。因此，这将需要很长时间。

“弃用”听起来很容易，但也会产生影响。如果你弃用 DNSSEC，就会将 DNS 暴露在 DNSSEC 试图防范的各种攻击之下。你还可能影响那些依赖 DNSSEC 的协议。在 SIDN 的工作中，我们选择了第一个选项，即“替换”。因此，第一行显示为绿色。

请切换到下一张幻灯片。从现在开始，我将重点讨论这种特定的方法。我不会解释这张图，所以大家不用担心。你在这里可以看到的是解析器与权威域名服务器之间的交互，并展示了相关的 DNSSEC 消息。带有红色和黄色标记的消息是那些包含密钥材料的消息（即签名或公开密钥），而这些正是需要更新的部分。

请切换到下一张幻灯片。为了让大家对这些签名有个直观感受，这里有两个例子。顶部目前有两项，左侧是一个公开密钥。左侧灰色部分是用 DNSSEC 中当前使用的密钥签署的公开密钥。右侧灰色部分是由该密钥生成的签名。蓝色部分是由后量子算法创建的公开密钥和签名，这种算法足以抵御量子计算机的攻击。正如大家所见，后者长度明显更长。好了。这只是从技术角度让你有个大致印象或感受。

请切换到下一张幻灯片。目前正在开发各种量子安全算法，通常是在 NIST PQC 竞赛领域内。这就是美国国家标准与技术研究院。他们设立了一个竞赛，邀请密码学家提出能够抵御量子计算机的算法。我们一直在试验其中的一些算法。正如你在这张表中看到的，MAYO Falcon 和 SQSign 就是其中的例子。

这些名字有点奇怪，而且还有更多这样的算法。但我们的工作一直是试验这些算法，并验证签署区文件所需的时间。例如，用于验证 DNS 记录的 .nl 区。我们还研究了涉及的签名大小和密钥大小，因为在之前的幻灯片中，你们看到它们差异很大。从这张表中可以看出，这是一种权衡，如果你的签名大小较小，

你就会得到——如果你的密钥大小较小，那么签名速度可能会提高，反之亦然。

请切换到下一张幻灯片。我们继续。这是我们对 .nl 区运行的第一个实验。我们尝试用两种后量子加密算法来签署该区——或者说，我们不是尝试，而是实际使用了两种算法来签署该区。这两种算法分别是 Falcon 和 MAYO。你可以在图中右侧看到它们。具体细节我就不多说了，但你可以看到，使用这些 PQC 算法签署该区所需的时间大约是前者的两倍。一般情况下，签署 .nl 区约需要 10 分钟时间，而使用这些 PQC 算法则需要 20 分钟时间。这个时间还在可接受范围内。从运营角度来看，这些结果是可以接受的。

请切换到下一张幻灯片。这就是我们 SIDN 目前所处的情况。我们还确定了一些未来要研究的新工作项目，这些项目主要与这些签名和公开密钥的大小有关。我们也希望更详细地研究解析器的验证时间，例如，结合缓存的作用来进行研究。是的，我看到了。谢谢。

最后一张幻灯片是向 GAC 提出的一些行动建议。也许你们可以与美国政府机构 NIST 合作，探讨如何使他们正在开发的 PQC 算法与 DNS 的要求保持一致。我知道他们对这个特定的使用案例很感兴趣。另一项可能的行动是鼓励开发开源软件，将 PQC 算法集成到 DNS 基础设施中。因此，这或许可以通过 NLnet 或 Sovereign Tech Fund 等基金来实现。至少我知道这两个基金会愿意赞助此类工作。

或许还可以促进部署。例如，可以通过像 internet.nl 这样的网站来实现，你可以在该网站上检查域名属性或互联网连接属性。也有可能增加对域名 PQC 就绪状态的检查。最后，稍微扩展一下上一张幻灯片的内容：如果采用“替换”策略，我们还需要深入研究这些新的 PQC 算法对运营的影响，以及这对 DNS 及其运营商（例如根区运营商）意味着什么。

好了。请切换到下一张幻灯片。我们开发的软件，我们进行的实验，都是在试验床上进行的，而试验床是开源的。你可以从我们的网站上下载该软件。这是二维码。如果你还有其他疑问，请与我联系。这是最后一张幻灯片。

马尔科 • 霍格沃宁

谢谢克里斯蒂安。这么说，我们都可以下载一些量子软件或者量子安全软件来试试了？太好了。谢谢！我获得的关键信息是，我们确实在采取行动。从荷兰政府的角度来看，我们开始做的是资产管理，就像你刚才简要展示的那样。正如沃伦在演讲中提到的，DNS 无处不在。这意味着 DNSSEC 也无处不在。也就是说这种加密技术基本上存在于所有事物中。因此，我们内部已经在非常努力地尝试建立一个列表，列出这种加密技术具体用在哪些地方，以备我们需要替换。根据我的经验，这说起来容易做起来难。说到这里，我收到了两个提问。一个是现场的巴瑞提出的，另一个是线上的彼得提出的。先请巴瑞提问。

巴瑞 • 莱巴 (BARRY LEIBA) 谢谢。我是 SSAC 成员巴瑞 • 莱巴。我只想澄清一点，我发现每当我们讨论后量子密码学时，都需要强调这一点，因为存在一个普遍的误解，认为量子计算机会危及我们所有的加密技术。我想说明的是，克里斯蒂安提到的签名是一种特殊的加密方式，会受到量子计算机的威胁。我们用来加密互联网流量的普通加密技术并不会面临风险。具体受到威胁的是用于数字签名和密钥交换的那些加密类型。这就是为什么我们在讨论这个问题时总要强调这些方面。

克里斯蒂安 • 海瑟曼 是的。特别是，DNS 有特殊要求，例如所有内容都需要装入 UDP 数据包。而这些使用案例并没有被 NIST 的那些研究人员充分考虑进去。因此，可以联系他们，让他们将这个关键的使用案例纳入考虑范围，将会是一个值得探索的前进方向。

马尔科 • 霍格沃宁 谢谢。我想，彼得已经在线了。彼得 • 托玛森 (Peter Thomassen) 要发言吗？

彼得 • 托玛森 嗯，其实我就在现场。大家好。我是彼得 • 托玛森。我是一名 SSAC 成员。我想补充一个方面。DNSSEC 签名的相对比例实际上很低，例如在 .com 域名中大约只有 5%。但如果你看绝对数量，它仍然超过 1000 万个域名。因此，这是一个相当大的数字。当然，目前尚不清楚当 DNSSEC 必须过渡到后量子方法时，未来的签名方法会是什么。但显然，未来肯定会有某种形

式的过渡。而目前已有超过 1000 万个域名完成了签名，或者到需要过渡时这个数字可能更大，如果协调不好，完成这样的过渡将会很困难。因此，重要的是要通过自动化来支持这一过程。

在你展示的地图上（这部分不必展开细讲），地图上有几个蓝色国家。这些蓝色国家的 ccTLD 支持自动完成这些变更。因此，需要考虑的一个问题是，你们的国家——也可以是任何人的国家——是否想要增加对这种自动过渡的支持。我想，SSAC 将很乐意就任何此类问题进行进一步的交流。如果你对此感兴趣，请联系我或任何其他 SSAC 成员。

克里斯蒂安 • 海瑟曼　　这一点说得非常好。谢谢。

马尔科 • 霍格沃宁　　谢谢。我们还剩一点时间。看看大家还有没有其他问题。尼古拉斯主席，请发言。

尼古拉斯 • 卡瓦耶罗 (NICOLAS CABALLERO)　　谢谢。非常感谢。也感谢拉姆和你的团队带来的精彩演示。很高兴你能来参加这次会议。我快速说两件事。第一件是，拉姆，克里斯蒂安，考虑到我尊敬的同事詹姆斯 • 加尔文 (Jim Galvin) 也在现场，我们能否为董事会安排一场关于 10 月阿曼马斯喀特会议的演示。可能需要准备一个基础版本，不过有三四位董事会成员具备很强的技术背景。这是一方面。

另一方面，同样要利用这个机会——此刻我正坐在我尊敬的巴西同事旁边——我们正在为拉丁美洲国家在圣保罗或巴西利亚组织一场区域能力建设会议（具体地点待定）。但在阿曼会议前后，你们能否在这方面为我们提供一些支持？我们基本上会讨论 DNSSEC 实施、密码学的简短回顾（对称与非对称）以及关于 RSA 算法的情况——如果我说错了请纠正——但大约两三周前似乎有消息说 RSA 被破解了（不确定是否属实）。我不知道这是否属实，但我听到一些传闻。

总之，这是一方面。另一方面，是开源软件对政府的诸多优势。作为深度使用者，我很难用简单的语言向没有技术背景的人解释 GPL-2、GPL-3 和一般许可证在技术和经济方面的优势，以及为什么它是一件好事。因此，有了你们的帮助和专业知识，我们可能会更成功一些。所以，就是这两件事：一方面是为董事会做演示，另一方面是帮助我们为南美国家组织一场区域能力建设会议（这次可能在圣保罗或巴西利亚举行）。

拉姆 • 莫汉　　尼古拉斯，谢谢你的发言。我们非常赞同这两个想法，也很乐意直接参与这两项工作。请随时联系我协调具体事宜。

克里斯蒂安 • 海瑟曼　　好的，我这边也一样。

尼古拉斯 • 卡瓦耶罗　　抱歉打断一下，你能说说 RSA 被破解的事吗？

沃伦 • 库马里

好的，我猜你说的是谷歌最近发表的一篇学术论文，其中指出破解 RSA 的门槛降低了。目前尚未发生实际破解事件。只是后量子密码学所需规模（更准确说是量子计算机的复杂度要求）受到了质疑。要构建一个可靠的系统，你实际上需要多少量子比特？

这篇论文的观点是，你并不需要我们最初想象的那么多，但我们还不确定未来多久才需要担心这个问题。如果你问一群不同的专家，你会得到非常不同的数字，但并不是说 RSA 已经被破解了。而是看起来在未来若干年内，它有可能被破解。但实际的估计值却大相径庭。我在找某个页面，他们基本上取了一大批量子科学家的估计值的平均值，那个数字一直在变。也有可能就是明天。也可能是 50 年后。也可能是 500 年后。实际上，这很难预测。可能更接近几年后，但这也是很难预测的。

这有点像核聚变。过去多年，人们总说“核聚变能源将在未来 20 年内实现”，但至今仍未实现。过，这绝对值得我们现在就做好准备，因为如果它真的发生，RSA 或其他加密算法被轻易破解，我们需要在它发生之前很久就开始为此做准备。

尼古拉斯 • 卡巴雷诺

未雨绸缪，对吧？

马尔科 • 霍格沃宁

好了。谢谢。还有两分钟就可以休息了。我看到澳大利亚代表举手了。我建议我们快速处理一下。英格拉姆要发言吗？

英格拉姆 • 尼布洛克 (INGRAM NIBLOCK)

大家好，我在这里。谢谢。我刚刚在思考前一张幻灯片上的表格，那上面列出了各种权衡因素，比如密钥大小、签名速度之类的参数。密钥大小我完全理解，因为 UDP 数据包大小有限制。但我想知道，签名时间变长会有什么实际影响？比如说，.nl 域名的签名时间从 2 分钟延长到 10 分钟（具体数值记不清了），这会导致出现问题吗？在 DNS 系统中这种操作频率会导致出现问题吗？

克里斯蒂安 • 海瑟曼

我们的区域内有 620 万个域名，其中约 60% 已经签名了，我们的发布窗口期约为 30 分钟。因此，我们需要每 30 分钟重新签署一次。如果签名耗时过长，我们可能会面临时间不足的问题。是的。这就是我们想知道的原因。

马腾 • 阿尔森

这也取决于部署模式。克里斯蒂安描述的是全区域定期签名的特定部署模式，但也存在增量签名甚至针对每个查询实时签名的部署模式。这个问题很难一概而论，但签名速度确实很重要。

彼得 • 托玛森

也许重点在于，签署时间越长，部署模式所需的其他改动就越多。

马尔科 • 霍格沃宁

谢谢。希望这可以解答你的问题。我们的时间差不多了。很高兴看到后续行动的第一批预约已经完成。如果你想了解更多信息，建议在茶歇时找我们的同事交流。我相信这里有不少来自 SIDN 的同事，当然 SSAC 的成员也几乎全员到场。再次感谢拉姆、沃伦、格雷格、马腾和克里斯蒂安提供的所有精彩内容，带我们踏上这段有时技术性很强的旅程，并努力帮助我们了解发生了什么。

在放大家去喝咖啡之前，半小时茶歇后，我们将回到 GAC 会议室参加 WHOIS 和数据准确性会议。所以，GAC 的同事们，期待稍后与你们再见。对其他参会者来说，希望本次会议信息量充足。感谢参与，请尽情享受茶歇时间吧！谢谢。

[听写文稿结束]