ICANN71 | 虚拟政策论坛 — 全体会议：理解信誉拦截列表
欧洲中部夏令时间 (CEST) 2021 年 6 月 17 日星期四 — 10:30 至 12:00

布伦达 • 布鲁尔
(BRENDA BREWER)： 本次会议现在开始。请开始录音。

[正在录制]

布伦达 • 布鲁尔： 大家好。欢迎参加 ICANN71 全体会议，理解信誉拦截列表。

我是布伦达 • 布鲁尔，是本次会议的远程参会经理。请注意，本次会议将录音，并将遵循 ICANN 预期行为标准。

在本次会议期间，只有在问答框内提交的问题或评论才会被读出。我将在本次会议主席或主持人指定的时间里读出这些问题或评论。本次会议的口译包括英语、中文、法语、俄语、西班牙语和阿拉伯语。在 Zoom 中单击口译图标，然后选择您将在此本次会议中收听的语言。如果您需要发言，请在 Zoom 会议室中举手。在会议主持人呼叫您的名字后，我们的技术支持团队将允许您取消麦克风静音。

发言之前，请从口译菜单中选择要使用的语言。请说出您的姓名以便记录，如果您使用的不是英语，也请指明您将使用的语言。

发言时，请将所有其他设备和通知静音。请以合理的语速清晰地发言，以便翻译员翻译。

本次会议的所有参与者都可以在聊天窗口中发表评论。请使用聊天窗口中的下拉菜单，然后选择回复所有小组成员和与会者。这将使每个人都能看到您的评论。请注意，在 Zoom 网络研讨会形式下，只有小组成员之间才能进行私聊。小组成员或标准与会者向其他标准与会者发送的任何信息，也会被会议的主持人、共同主持人和其他小组成员看到。

要查看实时文字记录，请点击 Zoom 工具栏上的隐藏式字幕按钮。现在，有请 LG 弗斯伯格 (LG Forsberg) 发言。谢谢！

LG 弗斯伯格： 谢谢，布伦达。我是 LG 弗斯伯格，是本次 ICANN71 全体会议的主持人，本次会议主题是：理解信誉拦截列表。

有些人可能还不认识我，我在瑞典域名行业工作多年，在注册服务机构方面担任过技术产品经理和注册服务机构联络人，在注册管理机构方面也有各种技术和渠道方面的经验。

我目前是 iQ 公司的首席技术官，这是一家为域名行业提供服务的商业机构，提供 iQ Abuse Manager 和域名分析等产品和服务。

在将下一个信誉拦截列表整合到 Abuse Manager 之前，我还为各个注册管理机构和注册服务机构提供技术和政策方面的咨询。

最后，但同样重要的是，我是北欧域名日的创始人和策划人，这是一个一年一度的斯堪的纳维亚域名行业会议。我非常期待能再次进行面对面的会议。

在今天的会议上，我们将与听众进行互动。我们准备了三个投票问题，供大家在讨论过程中回答。现在将向大家介绍其中的两个。而最后一个将在今天议程的最后阶段向大家展示。

请展示一下投票问题。

布伦达 • 布鲁尔： 谢谢！在你的屏幕上应该能看到第一个投票问题。您是否熟悉以下类型的安全威胁？请勾选所有适用的选项。

这些选项包括垃圾邮件、网络钓鱼、恶意软件、网址嫁接、僵尸网络或其他。再问一遍，您是否熟悉以下类型的安全威胁？

请勾选所有适用的选项。垃圾邮件、网络钓鱼、恶意软件、网址嫁接、僵尸网络或其他。我们将在大约五秒钟后结束投票。

谢谢！

我们现在可以结束投票了。

请展示第 2 个投票问题。

第 2 个投票问题：您管理的域名是否曾经遇到过这些安全威胁？您可以回答是、否、我不知道，或者我不管理域名。对不起，有四个选项。请选择一个。再问一遍，您管理的域名是否曾经遇到过这些安全威胁？是、否、我不知道，或者我不管理域名。

再给大家五秒钟时间。

非常感谢。

我们可以结束投票了。

LG，我把时间交回给你

LG 弗斯伯格： 谢谢，布伦达。

在我们继续讨论小组部分之前，我将继续分享该主题的一些简要介绍。今天，我们有多个团体在收听，他们以不同的方式与信誉拦截列表产生关联。这些团体，我想说的是 ICANN，他们使用信誉拦截列表在域名滥用活动报告 (DAAR) 内提供统计数据，他们还要求新通用顶级域 (NgTLD) 至少要监测他们的（听不清）。

我们有注册管理机构和注册服务机构这些形式的合同方，他们可能使用一个或多个信誉拦截列表来监控他们的顶级域，或者对于注册服务机构而言，监控他们的已注册的域名列表。

我们可能有像托管公司这样的服务提供商，他们可能使用信誉拦截列表来确保他们的客户电子邮件不会有垃圾邮件，或确保他们托管的网站不会因网络钓鱼或恶意软件等不良行为而被举报。

最后，我们有终端用户。在本次讨论中，终端用户被定义为域名和/或网站的注册人或运营商。我想，这是今天在座的一个不想与信誉拦截列表有关联的群体。

话虽如此，但我想说的是，信誉拦截列表对不同的人有不同的含义，这取决于你在这些群体中的身份。对于 ICANN 来说，如

果是注册管理机构或注册服务机构，它很可能是你使用的一个工具或与你合作的一个伙伴；而对于终端用户来说这可能意味着灾难，如果你的电子邮件被发送到垃圾文件夹的黑洞中，或者你在 Chrome 浏览器中看到谷歌的红色死亡屏幕而不是你的网站。

另外，正如此主题可能已经告诉你的那样，虽然信誉拦截列表难免涉及到对 DNS 滥用的讨论，但我们今天在这里不是为了对 DNS 滥用的定义进行 90 分钟的讨论。相反，我们在这里是为了进一步了解信誉拦截列表是如何起作用的，以及我们、受众、签约方、服务提供商和终端用户能够对它做些什么。

我们今天会听到很多关于信誉拦截列表的内容，但在讨论之前做一个简化的回顾并没有什么坏处。

信誉拦截列表是一个指示或报告的集合，以某种方式来帮助避免滥用行为。它的名字中的“信誉”部分往往意味着，在确定一个域名是否应该被列入时存在一些灰色地带。这往往不是简单的是或不是。

这方面的一个例子是 Spamhaus 实施的信誉打分模式：每个域名从零分开始，做好事减分，做坏事加分。

一旦积累了足够的分数，例如 5 分或 10 分，该域名就会被列入拦截列表。

而名字中的“拦截”一词是向那些首先在电子邮件服务器和防火墙中部署列表以抵御垃圾邮件或不必要流量的供应商致敬。列表起到阻挡之用，

以便减轻滥用的情况。当然，

减轻滥用可能不是唯一的使用案例，有时甚至还不是主要使用案例。

一些信誉拦截列表会提供关于如何发现某种不良资源的完整信息，而其他一些列表只是给予提示，告诉你某个特定的域名上发生了不好的事情。

大多信誉列表似乎都有一个共同点，那就是不太容易理解它们的内容、方式，以及它们的数据有什么帮助，特别是如果你是一个事先没有与这些类型的资源有任何联系的终端用户。

但是，为了弄清信誉拦截列表是如何收集数据、对内容进行分类并真正了解这台不时地生成一个新列表的“机器”是如何运作的，我们今天在这里聚集了一些来自信誉拦截列表的代表。

我们也有一群来自先前提出的各方代表加入，谈论他们在信誉拦截列表方面的经验。

在此，我想有请我们今天的第一位参与者，让他介绍自己和他工作的公司。

有请来自 Spamhaus 的卡雷尔 • 比特 (Carel Bitter) 先生。

卡雷尔 • 比特： 大家好。我叫卡雷尔 • 比特。我在 Spamhaus 工作，主要参与我们在域名信誉方面的工作。我们有多个数据集，但今天我们将专注于我们所提供的域名部分。

我在域名声誉方面工作已经超过十年了。我以前参加过很多 ICANN 的会议。

因此，我很高兴能帮助大家并回答大家可能提出的任何问题。

LG 弗斯伯格： 非常感谢，卡雷尔！

有请来自 abuse.ch 的罗曼 • 休斯 (Roman Huessy) 先生做自我介绍。

罗曼 • 休斯： 我叫罗曼 • 休斯，是 abuse.ch 的创始人。abuse.ch 是一个非营利性项目，在伯尔尼应用科学大学 (Bern University of Applied Sciences) 运行，其目标是收集有关僵尸网络等的信息，并免费为大家发布他们的相应信息。

LG 弗斯伯格： 非常感谢，罗曼。

我们今天的最后一位参与者是来自 WMC Global 的本 • 库恩 (Ben Coon) 先生。

请进行自我介绍。

本 • 库恩： 谢谢！本 • 库恩，来自 WMC Global。我们主要运行一个网络钓鱼平台。我们为短信供应商和防火墙提供网络钓鱼 URL 拦截列表，服务对象还包括受到多诱饵凭证网络钓鱼攻击的用户。

非常乐意回答任何问题。谢谢！

LG 弗斯伯格： 谢谢你，本。

为了继续我们各方的讨论，我想首先介绍来自 ICANN 的莎曼内 • 塔嘉利扎德胡 (Samaneh Tajalizadehkhoob)。请进行自我介绍。如果你有任何想讨论的主要论点，也请现在提出。

莎曼内 • 塔嘉利扎德胡： 大家好，我是莎曼内 • 塔嘉利扎德胡。我在 ICANN 的首席技术官办公室工作，负责安全、稳定与弹性小组。我也是域名滥用活动报告 (DAAR) 项目的负责人，先前在学术界工作过，拥有信誉数据源方面的经验。

今天我会侧重谈一谈，作为一个 ICANN 组织，我们如何看待和使用这些数据源，以及在哪些项目中使用。

谢谢！

LG 弗斯伯格： 谢谢，莎曼内。

然后我想介绍来自 Verisign 的马特 • 托马斯 (Matt Thomas) 先生。请进行自我介绍，并说明你的任何主要观点。

马特 • 托马斯： 谢谢！我是马特 • 托马斯。我在 Verisign 的网络安全战略和研究部门工作，是一名资深工程师。

我也是 ICANN 安全与稳定咨询委员会 (SSAC) 的成员，目前还担任信息传递、恶意软件和移动反滥用工作组 (M3AAWG) 的董

事会副主席。我很期待今天有关信誉拦截列表各种使用案例的小组讨论。

谢谢！

LG 弗斯伯格： 谢谢，马特。

在注册服务机构方面，我们今天请到了来自 Tucows 的雷格 • 利维 (Reg Levy)。请进行自我介绍，并提出你的任何主要观点。

雷格 • 利维： 大家好，我是雷格 • 利维，是 Tucows 的合规部门负责人。我也是注册服务机构利益相关方团体 DNS 滥用小组的成员。我是 DNS 滥用小组的联合主席。

早上好。显然，我还在整理思绪中。

非常期待这次讨论。

LG 弗斯伯格： 谢谢，雷格。

最后但并非最不重要的是，我们有来一般会员社群的乔安娜 • 库勒萨 (Joanna Kulesza)。请进行自我介绍，并说明你的任何主要观点。

乔安娜 • 库勒萨： 谢谢 LG！谢谢您的介绍。感谢您邀请我，给我机会代表终端用户发言。

我是一般会员咨询委员会的联合主席。我专注于能力建设，并且我认为这次讨论、这次小组讨论和信誉拦截列表与能力建设有关联。

作为一个主要观点，我想声明一下，从投票本身和一般会员社群的参与来看，终端用户对信誉拦截列表不感兴趣这种说法是不正确的。正好相反。在我们的小组讨论中我会尽力说明这一点。

很高兴来到这里。谢谢您的介绍。

LG 弗斯伯格： 谢谢，乔安娜。

现在我们将从会议的介绍部分进入第一个访谈部分。在这个部分我们与信誉拦截列表小组交谈，尝试进一步了解他们的做事方式。

我想在这一部分的开头问一下卡雷尔，你自己是如何定义“信誉拦截列表”的？

卡雷尔 • 比特： 问得好。让我们从拦截部分开始。

我认为在许多情况下，它不仅仅是起到拦截作用。如果你从整个注册管理机构/注册服务机构的角度来看，即注册管理机构/注册服务机构通过查看数据来发现有问题的域名或客户，那么他们本身并没有真正参与任何拦截。这更像是一个补救型的使用案例。

因此，就我个人而言，我通常会谈论我们的数据集，而不是我们的信誉拦截列表，特别是在这样的背景下。所以我认为这是一个非常重要的事情，在任何时候开始处理任何数据集时，你都需要考虑到这一点。它的作用是什么？你在用它做什么？你是否按预期使用它？你是否按照它的设计使用方式来使用它？

如果不是，我的意思是，你应该……我不是说你不能把本来用于做某一件事的东西用于做另一件事。但你需要意识到，你的使用案例可能在某个部分有点不同。

你之前提到我们的系统是如何工作的，我们实际上是给域名打分。域名的分数越高，我们就越能确认有坏事发生。因此，这允许我们对不同的评分等级采取不同的行动。

所以我认为，你真的需要了解你正在处理的数据。如果你不了解，那么你需要联系创造数据的人，并告诉他们，我不理解这

一部分，或者我想用它来做这件事可以吗？在电子邮件背景下，你可能想阻止某些东西，但在 DNS 级别背景下你可能不会。一个很好的例子是缩短器。电子邮件中的缩短器是一个非常著名的问题电子邮件标志。合法的电子邮件通常不包括缩短器。

但是，在 DNS 层面上阻止缩短器对你的终端用户来说可能有点苛刻。所以有很多事情要考虑。

LG 弗斯伯格： 非常感谢，卡雷尔！

我想跟进两个专门针对 Spamhaus 的后续问题。它们是：有哪些典型的证据会使 Spamhaus 考虑将一个域名列入信誉拦截列表？这些证据是否会以任何方式与你们的数据集采用者分享？

卡雷尔 • 比特： 就我们自己而言，分享证据比较困难，因为我们得到的数据均来自互联网服务供应商和其他网络，我们与他们签订有分享数据协议，因此有时我们无法将这些数据继续分享出去。如果人们有疑问，我们始终愿意接受提问。

就我们合作的注册管理机构/注册服务机构使用案例而言，他们有一个支持渠道供人们使用。人们可以提问说，嘿，我们看到这个被列到列表上了，但我们并不知道为什么会这样。这也

许是一个误报？是否有其他事情发生？我们会进行调查，我们可能有一些东西可以分享。但并不是默认共享。例如，如果你得到一份列表，上面有 100 个不良域名，但这个列表并不提供 100 个垃圾邮件样本，或者 100 个恶意软件的二进制文件。基本上我们会根据个案来确定我们可以分享什么以及不能分享什么。

LG 弗斯伯格： 非常感谢，卡雷尔！

罗曼，在这个问题上你觉得 abuse.ch 有什么不同之处？

罗曼 • 休斯： 抱歉，你能重复一下最初的问题吗？我刚才在回答问答框内的问题。

LG 弗斯伯格： 抱歉，没问题！有哪些典型的滥用证据会使 abuse.ch 考虑将一个域名列入到你的数据集中？

罗曼 • 休斯： 问得好。谢谢！

典型的证据类型包括在被破坏的网站上提供的恶意软件，或已被威胁行为者注册的域名。

这意味着，系统实际上会检查每次提交的文件是否含有恶意的有效载荷。如果有的话，这些证据会被公布到项目网站上，每个人都可以使用。然后会向相应的托管公司发送滥用报告。

因此，在提供证据方面该项目是相当透明的，因为每一个证据都会在网站上公开，每个人都可以查看为什么某些域名会被列入。

LG 弗斯伯格： 非常感谢，罗曼。

为了更好地理解数据集，你能否描述一下，一份通用报告的生命周期，即在你的使用案例中是恶意软件，从首次提交给你直到它消失的生命周期？

罗曼 • 休斯： 没问题。说到这一点，恶意软件，不像钓鱼网站或垃圾邮件网站，它或多或少容易一点，因为我可以从远程主机获得某种响应。这意味着我可以很轻松地以自动的方式检查某个网站是否仍在提供恶意内容。这种检查是自动进行的。一旦这些恶意内容消失，该网站或域名就会被自动标记为离线。这实际上意味着该域名或 URL 自动从我提供的拦截列表中消失。

这种方式的好处是，URL 只在它真正有威胁时才会被列出。系统将每小时对它检查几次，通常是每 10 分钟检查一次，以确定它是否仍在产生威胁。

因此，一旦终端用户修复了威胁，该域名或 URL 通常会在一小时内自动从拦截列表中消失。

另一方面，它实际上意味着，如果问题没有得到真正的解决，例如，恶意内容刚刚被删除但根本原因没有得到解决，即威胁行为者再次上传恶意内容，则系统会自动检查恶意内容是否再次存在。如果再次存在，则该域名或 URL 将自动再次被列出。

LG 弗斯伯格： 非常感谢，罗曼。

本，你认为卡雷尔和罗曼在这里描述的情况与你们 WMC Global 在网络钓鱼报告、其生命周期和网络钓鱼证据方面的情况有很大不同吗？

本 • 库恩： 我想说的是，在 WMC Global，我们遵循的模式大体上与罗曼所谈到的模式相同。

在网站被列入拦截列表之前，我们会核实其恶意信息情况。当我们提供拦截列表给，比如说，短信供应商，来阻止网络钓鱼时，他们通常只使用过去 24 小时的列表，因为网络钓鱼网站会下线。如果一个网络钓鱼网站重新出现，我们会将它重新列出。我们有自动检查功能，可以测试该网络钓鱼网站的生命周期有多长。

我们的拦截列表与其他一些拦截列表的另外一个不同点是，我们不列出域名，而是列出完整的 URL。这样你可以准确地看到恶意内容的位置。然后，同样地，一旦这些恶意内容下线，它将被除名，除非它随后再次上线。

LG 弗斯伯格： 谢谢你，本。

我们回到卡雷尔身上。你之前提到，信誉拦截列表的用户需要了解拦截列表的用途。

你认为对于 Spamhaus 而言，它的主要使用案例是什么？以及它服务的主要用户有哪些？你认为主要用户在过去十年里发生了变化吗？

卡雷尔 • 比特： 显然，由于我们的公司名称中有“spam”（垃圾邮件）一词，所以我们的数据主要来自电子邮件。

数据集有点复杂。我们公开发布的数据集，即域名拦截清单，是我们对目前哪些域名有不良声誉的看法。它主要用于电子邮件，但其中也包含恶意软件域名。其中还有僵尸网络元控制。那里面还有钓鱼网站，所有我们认为它包含一大堆不良域名。在这种情况下，通过 DNS 返回代码来区分它们。因此，我们可以筛选出其中一部分，比如只筛选出网络钓鱼或恶意软件。

但我们做的是提供数据。我们几乎无法控制人们如何使用它。我们发布的公开免费版本采用一种主要用于电子邮件服务器内的格式。所以它是一个 DNS 拦截列表。你进行 DNS 查询，然后你得到一个答案，然后你用这个答案在你的本地政策范围内做一些事情。

有一些版本适用于特定的威胁和使用案例。因此，有不同的子集可用，例如，在 DNS 解析器层面使用。有一些版本可供注册管理机构和注册服务机构用来做调查和纠正。

那么主要的使用案例是什么呢？我想，主要的使用案例是人们希望根据域名做出信誉决定。

我认为它不只适用于电子邮件。这在过去可能是，但现在肯定不是。

大多数域名，就像罗曼会告诉你，用于恶意软件和僵尸网络的域名，你永远不会在电子邮件中碰到。你可以在你的所有电子邮件中检查这些域名，但你不会看到它们。它们被用在不同的层面上，而被感染的计算机会联系到某个域名，以联系其手动控制中心，下载更多的恶意软件。

因此，不是在你的电子邮件服务器里检查这些域名，而是在 DNS 解析器或 IDS 或任何类似的地方。

因此，使用案例实际上取决于你试图解决的问题类型。

正如本所说，例如对于短信检查，我们看到在短信或缩短器中使用的许多域名是通过某些域名重定向的，你不会在电子邮件中看到它们。

所以，我认为它比电子邮件要广泛得多。如果你有一个涉及域名的安全问题，则有一些数据集，比如我们提供的那些，比如罗曼提供的那些，比如本提供的那些，可以帮助解决你的安全问题或应对和了解正在发生的问题。

LG 弗斯伯格： 非常感谢，卡雷尔！

我现在有一个问题，要问我们这三个信誉拦截列表提供者。你们三个人都谈了一些关于你们如何接收和收集报告或指示的问题。我们可以从中看出，我们谈论的主要是报告或爬行于互联网之类或检查你们可以访问的电子邮件的机器检测。

那么在你们的公司里，对于“信誉拦截列表”，你们是否有一种人工调查的形式？让我们从本开始。

本 • 库恩： 是的。我们使用一大批威胁猎手，他们会仔细检查或抽查我们所发现的很多凭证式网络钓鱼。我们也会查看任何得分不够高而未被列入我们信誉拦截列表的域名。

我们遇到的任何类型的误报也会被发回给团队。该团队将进行调查，并手动将它添加到列表或从列表中删除。

我想说，我们还是有相当多的人为干预。

LG 弗斯伯格： 谢谢你，本。

罗曼。

罗曼 • 休斯： 是的。我想特别提一下 URLhaus，这是一个由社群主导的跟踪恶意软件网站的项目。这意味着我提供的数据集只是整个数据集的一部分。其他部分是由社群提供。

当我们谈到社群时，有两种类型的报告者很重要。一类是陌生人报告者。这些是我不知道也不信任的用户。每当他们向项目报告某个域名时，都会有人手动进行审核。

另一方面，我们有可信的报告者。可信的报告者意味着，如果他们向项目报告了一个网站，该网站就会自动被列出。但是，

系统仍会检查该网站是否提供任何恶意内容。但是 URL 将直接进入数据库。

但是，如果你现在将其用于拦截列表的方法中，而这只是数据集的一个使用案例，网站将 — 或域名将仅在实际提供恶意内容时被列在拦截列表中。

因此对于你的问题，简而言之，它是人工审核 URL 或域名和机器审核 URL 的结合。

LG 弗斯伯格： 非常感谢，罗曼。

卡雷尔？

卡雷尔 • 比特： 好的。在我们这里，它也是一个自动化和人工调查的结合体。如果你想给地球上存在的每个域名分配一个信誉，那么你必须用到自动化。我们有太多的域名，而且每天都会有很多新的域名，因此无法由人工来查看所有域名和进行所有调查。

因此，它有一部分是自动进行的，但肯定也有人工进行的部分。我们的调查员会查看那些可疑的域名，调查那些得分足够接近但没有被列入列表中的域名，或那些本应得分更高但实际并没有的域名。因此，它始终是人类和机器智能的结合体。

LG 弗斯伯格： 非常感谢，罗曼。

这部分会议的时间已经不多了。我们有一个比较受关注的问题接下来要问小组。你们认为一个报告或指示有多大的可能性是误报？误报最常见的原因是什么？让我们从本开始。

本 • 库恩： 我想说，在我们看到的拦截列表上报告的数据中，总会有一些误报。尽可能地减少这些误报是我们的一个目标。

我想说的是，我看到的误报的主要原因是人们对什么是恶意的和什么不是恶意的缺乏了解，或者人们会在看到一些他们不喜欢的内容时会将它报告为恶意，尽管它实际上不是。

LG 弗斯伯格： 谢谢你，本。

罗曼。

罗曼 • 休斯： 是的，当然会有误报。一直都会有。而且每个人都可以通过网络用户界面进行报告。

如果一个可信的报告者开始提供已知为恶意软件的数据 — 例如网络钓鱼或垃圾邮件网站或其他东西 — 他将被直接拦截并从项目除名。

因此，在我看来，数据流是不错的。但正如我所说，误报是可能发生的。

LG 弗斯伯格： 最后是罗曼。不，最后是卡雷尔。抱歉。

卡雷尔 • 比特： 是的，误报总是会发生。正如本所说，我们的工作是确保误报数量尽可能低。

至于人们报告的内容，大家知道，许多年前当电子邮件供应商开始在他们的白电子邮件界面上提供“这是垃圾邮件”按钮时，人们报告的最多的实际上不是垃圾邮件或和恶意邮件，而是他们不喜欢的邮件，比如他们不想支付的发票或工作申请的拒绝信。因此，在这种情况下，大多数系统的工作方式是，如果有足够多的人，如果有一定的数量的人进行了报告，有迹象表明某个 IP 或域名或发件人或信标选择器或其他方面有信誉不良的问题，那么自动化就会启动。不过总会出现这种情况，即用户报告的内容，就像本所说的，他们只是不喜欢，那么它可能不是垃圾邮件、可能不是恶意内容，也可能不是网络钓鱼。但对很多人来说，“删除”按钮和“这是垃圾邮件”按钮并无很大的区别。

所以，是的，这始终是一个问题。你想一想，这是很明显的。我想这对罗曼和本来说也是一样的，我们数据集会有误报。你可能有一个星期没有任何误报，然后下一个星期可能会有三五

个误报。事实是误报总是会发生。重要的是你如何处理它，迅速找出这些误报，确保妥善处理它们。
但是作为数据的提供者和创造者，确保数据尽可能完好符合我们自身的利益。如果我们的数据不好，人们就会停止使用它，那么到那时，我们的数据还有什么意义？

对于数据的创造者来说，我认为，罗曼可能会认同这一点，数据变得越强大，会有越多的人开始使用它。如果一个域名被用于像僵尸网络命令与控制类型的情况，这个域名越快被删除，或越多的人拦截它，互联网就越安全。

如果我们...或者罗曼对它进行了报告，而人们表示这些报告不好，那么这就与我们的使命相反。

我们想要的是我们提供的数据能被尽可能广泛地使用，我们希望人们尽可能地接受报告，这样互联网最终会成为一个更安全的地方。因为，我认为对我们三个人来说，对本和罗曼来说，这就是我们所做工作的动力。我们一直在尝试为网络、注册管理机构、注册服务机构以及终端用户解决安全问题。归根结底，这一切都是为了保护终端用户。使用数据的人越多，终端用户就越能得到保护。如果数据不好，人们就不会使用它。

所以，我的意思是，这是一个非常重要的事情，我们一直想做。

我们有很多的方法来变得更加积极主动，你可以说，如果我这样做，我会阻止更多 — 我将阻止更多坏事发生。但在很多情况下，总是在某个地方有某个人在做与坏人几乎一模一样的事情，或者有同样的那种奇怪的 URL，或者有同样的那种奇怪的主机名。就像我看到这个主机名；它一定不是好东西。是的，100 个中有 99 个可能是不好的，但最后一个其实是好的。

因此，这始终是一种平衡行为，你只需要确保尽量做好，并有一个良好的程序来处理任何出现的问题。

但是，就像我在一个问答里的回答，在我们这里，任何人都可以删除一个域名。你不需要填写冗长的表格，也不需要通过电话或其他方式与我们联系。这是一个互联网上的自我服务，就像罗曼说的按钮。

确保处理任何可能发生的误报的过程对任何误报受害者来说都尽可能顺畅，这显然对我们有利。

LG 弗斯伯格： 非常感谢，罗曼。让我打断你一下。

我们正处于观众提问环节，在我们进入下一个环节之前，我想再提一个问题。

我想问一下罗曼，“信誉拦截列表”或威胁情报资料 — 让我们称之为原始数据，它们的提供者之间是否会相互合作？举例来说，abuse.ch 是否会向 Spamhaus 提供你可能拥有的关于误报或重要通知的数据？

罗曼 • 休斯： 是的，这个问题之前就在问答框里提出过，我认为这是一个非常重要的问题。

因此，当然也有与信誉拦截列表提供者共享当前威胁信息的流程。其中一些流程是双边的。例如，Spamhaus、Safe Browsing 或其他信誉拦截列表提供者都设有该流程。但就 abuse.ch 而言，数据集是对每个人公开的。每个人都可以使用它。例如，有很大一部分商业威胁情报供应商也在使用这些信息，并利用这些信息做他们想做的事情。

当然，由于不需要注册，我这边有一个问题是，我不知道谁在使用我的这些数据集，因为它是公开的。

另一方面，关于交换误报信息的问题，我认为这是一个重要的话题。据我所知，目前还没有建立报告误报的机制。

我的处理方法是，当某些域名被标记为误报时，它会被从数据集中删除。我想其他信誉拦截列表提供者或威胁情报供应商也会注意到并删除该条目。但当然，我在这方面没有任何影响

力。我认为这是一个需要讨论的话题。我们需要建立一个交流平台，可以在上面发布有关误报的信息以便与其他供应商分享。

LG 弗斯伯格： 非常感谢，罗曼。

我们现在到了本次会议的 ICANN 演示时间。有请莎曼内发言。

莎曼内 • 塔嘉利扎德胡： 大家好，我是莎曼内 • 塔嘉利扎德胡。我今天代表 ICANN 的首席技术官办公室谈一谈信誉拦截列表和我们对它的看法。

谢谢！请翻到下一页。

到目前为止，我们进行了非常好的讨论。我认为一些观点已经在演讲中被小组成员和所回答的问题所涵盖。如果有重复的地方，请原谅。

我想从基础概念开始，即什么是信誉拦截列表。它们可以是 IP 拦截列表或基于域名的拦截列表。它们通常代表的是被认为恶意、不值得信任或仅仅是信誉不佳的实体。我列举了一些行业或研究或学术界存在的使用案例。人们将它用于构建 DNS 防火墙，以防止恶意流量。它还用于过滤不必要的流量，这些流量通常是垃圾邮件和钓鱼邮件。它被内容分发网络 (CDN) 用于

防止向客户分发恶意内容，也被用作事件响应或执法的一部分，用于识别参与攻击的恶意基础设施。

它们有不同的分享机制。今天我们有一些例子，其中一些是开源例子，另外也有一些商用例子，它们可以通过费率限制、基于许可的方式提供，或按使用量付费的方式提供，并且通常由专门从事威胁情报的营利性公司维护。

一些开源的例子主要是由学术界使用，也有用于其他领域的。其中包括 Spamhaus、abuse.ch、Phish Tank，我所熟悉的那个，以及其他几个例子。

它们也可以是针对特定威胁的例子。因此某些列表仅专注于某些威胁。例如，由罗曼维护的 abuse.ch 有不同的数据源，这些数据源要么专注于僵尸网络，要么专注于恶意软件、勒索软件等等，我想那个现在已经停止了，或者专注于更通用的领域。它们包含各种威胁，其中一个例子是 SURBL。

请翻到下一页。

我们已经在小组中广泛地谈论了这个问题。标题幻灯片说的是列表的特点和缺点。我想把重点放在这两个方面，因为某些东西对于一个研究者来说可能是一个特点，但对于另一个研究者来说可能是一个缺点。

因此，从我们的角度来看，使用信誉拦截列表的要点是了解你想做什么，这一点很重要。实际上，更重要的是要了解信誉拦截列表背后的方法，它代表了什么，以及你如何能够最好地利用它来实现你的目标。

有一些特点是，一些列表可能过度专业化，因为它们面向特定的目的。任何想使用它们的人都必须了解这一目的，并看看它是否符合自己的目的。

我是作为一个研究人员从一般意义上提出这些观点。通常情况下，由于物理限制，它们的覆盖范围和优势有限。数据源供应商一般位于某些地理区域，因此他们在某些地理位置上的代表性可能较低。

我在这方面已有七、八年的工作经验，因此我知道，随着时间的推移，大多数的列表在覆盖面方面已经得到了改善，但仍然有一点很重要，那就是在对列表进行任何形式的分析时，要记住这点。

另外一点是，研究拦截列表的质量和不同的可靠性衡量标准的想法并不新鲜。自 2009 年、2010 年以来，它就已经被研究过了。因此，在本次演讲中，我列出了一些已经完成的关于列表的学术和行业研究，但如果你需要的话，可以联系我了解更多。

信誉拦截列表的另一个问题或特点是，关于内部方法的文件通常很有限。通过与列表提供者的交谈，我了解到的一个原因是，记录整个流程并不简单，因为有些过程可能是临时性的，也可能是非常详细或反应性的。因此，信誉拦截列表提供者很难为特定数据源维护一个实时、全面的文档。

由于我们有如此多的信誉拦截列表提供者，因此在拦截列表的数据收集、管理、维护和标记上，我们预计会有各种不同的方法。这导致对报告的覆盖面、可靠性、有效性和速度产生不同影响。

重要的是，这并不一定是一件坏事。这实际上可能是一件好事。只要用户理解多样性并正确处理它，那么多样性可以为我们带来更多信息。

请翻到下一页。

这一点我已经说过了。那么为什么要了解这些缺点，也就是特点呢？首先，对于每一个用户来说，无论是网络运营商、研究人员还是安全公司，重要的一点是他们要通过这些资源了解列表之间的区别、缺点以及注意事项，并通过了解它们来设计出更有效的防御和管理方法，同时在做研究或报告结果时牢记这些特点。

我自己在 ICANN 社群经常碰到的一个很好的例子是，我们经常说，这份研究显示网络钓鱼活动的趋势正在上升。但 B 做的另一个研究表明趋势在下降，为什么两者会相反？

这正是我想说的，也是我这套幻灯片的主要观点，即根据所使用的数据集、所考虑的时间范围、获得数据集所使用标签流程等等，某个趋势是可以不同的。

因此，在任何数据源中都没有绝对的趋势，至少从我的经验来看，没人可以报告说这是绝对趋势。趋势总是局部，它总是从数据源的角度出发。正如罗曼、卡雷尔和本已经多次报告的那样，我们对信誉拦截列表的看法是，它总是局部的，而且始终取决于方法。

请翻到下一页。

在接下来的几张幻灯片中，我将介绍我们在 ICANN 内的一些使用案例。即我们是如何使用信誉拦截列表的。

DAAR，即域名滥用活动报告，是使用信誉拦截列表的主要项目之一，你们大多数人可能都熟悉。

在这里我就不详述 DAAR 的具体工作内容了。总的来说，系统从注册管理机构域文件中获取域名，然后从预选的一组包含网

络钓鱼、恶意软件、僵尸网络命令和控制以及垃圾邮件的数据源中获取域名。然后，它将来自域文件的域名与它们的信誉拦截列表重叠起来，并进行处理、计算和创建指标，包括每日和每月衡量标准，以用于不同的分析。你可能在 ICANN 的月度报告 — DAAR 月度报告中熟悉这些分析。DAAR 报告在 ICANN 网站上公开。这些报告显示了 DNS 安全威胁在每个时间点集中的趋势，以及这种集中是如何随时间变化的。

我们要记住的是，系统已经做了大量的预处理和清理工作，统一了它所采用的信誉拦截列表数据源，并提供了所有边角案例等。详细信息列在项目的方法文件中。
请翻到下一页。

布伦达 • 布鲁尔： 抱歉。在你继续之前，能否放慢你的语速以便口译员进行翻译？谢谢！

莎曼内 • 塔嘉利扎德胡： 没问题。

我们还做过一个项目。作为安全、稳定与弹性 (SSR) 研究小组，我们还为 ICANN 合规支持做了一个项目，其中我们为注册服务机构创建了一个快照衡量标准。到目前为止这是一次性项目，我们做了一个与 DAAR 类似的事情，但只针对注册服务机构。它将重点关注特定时期的网络钓鱼和恶意软件，所以只有特定的数量。

我们还为注册服务机构计算了衡量标准，其中显示在一个点上和随着时间推移的威胁集中情况。

对于这个特定的项目，我们还进行了批量注册数据访问(BRDA)，因为我们目前只能将其用于合规目的。

请翻到下一页。

目前在首席技术官办公室 (OCTO) 内部正在进行的其他研究项目中，我们使用信誉拦截列表来开发预测模型，以便预测某个域何时会变成恶意域名，也用于提取模式来描述恶意域名的特征。

我们还计划采用一种类似于 COMAR 研究中所使用的方法（该研究已在之前的 ICANN 会议技术日上演示过），以便使用信誉拦截列表作为其中一个输入来区分恶意注册的域名和受影响的域名。

请翻到下一页。

目前我们 — 或对于我在前面的幻灯片中列出的大多数项目，我们评估了 — 或对选择的信誉列表做了评估，并在将其纳入我们的研究工作之前对数据源进行一段时间的监测。

我们所使用的基本上是已发布的学术界和行业内最有声望的列表。根据已发布的列表来确定信誉，因为它可能是主观的。我们选择了那些具有更好的数据净化、记录删除流程并在覆盖范围方面对我们现有的标准有所补充的列表。

好的。

请翻到下一页。

然而，我们正计划转而采用更有力的评估标准。这是一项持续的工作。

而且，我想再次强调，信誉拦截列表评估的工作并不新鲜，我们已经做了。我们所做的只是为了使其更加完整，并使其与今天的数据源更相关。
我们正在努力开发我们称之为纯度的衡量标准，也就是列表的误报/漏报率。提示一下，这些不是直观的衡量标准，鉴于拥有真实数据，也就是这组数据中的人工标注的数据并不直观；实际上这是任何从事信誉拦截列表工作的研究人员面对的首要问题。

我们正在研究估计列表的覆盖范围、响应性或响应时间、准确性、数据源的详细程度、它们随着时间的推移而表现出的稳定

性，以及活力程度，当它们出现在一个数据源中时，有多少列出的域名是确定的和活跃的。

这些衡量标准目前还有没有固定下来。我们正在努力工作，看看我们是否能取得可靠的结果。在我们进行研究项目时，它们可能会随着时间的推移而改变，也可能保持不变。但我们会随时向你们通报这项工作的情况。至于现在，它只是正在进行中的工作。

请翻到下一页。

以下是我在演讲中使用的参考资料。我的演讲就到此结束。

我想说的最后一点是，因为作为ICANN 首席技术官办公室，我们正在做几个使用信誉拦截列表的试错项目，特别是针对注册管理机构和注册服务机构，目标是在安全威胁方面提供更多信息。

我们先前在社群中谈到制定某些衡量标准并不直观，我们不想公布不可靠的内容，其中的一些原因正是我们今天讨论的问题。

例如，我们之前谈到了响应时间，即运营商对某些安全滥用问题作出响应的时间。如果我把它与小组讨论中进行的讨论联系

起来，同时也与这个演讲中关于每个列表背后的方法差异联系起来，那么大家可以很快意识到，如果我们采用几个列表，并试图为某个运营商创建一个代表响应时间的衡量标准，那么我们是在混合不同的方法。而这个衡量标准本身对于每个运营商而言并不可靠。它还取决于信誉拦截列表提供者的方法。

这些是我们在项目中遇到的困难示例，我们正在努力解决它们。但是在社群讨论中把它提出来讨论个好事，是个好机会。感谢大家。如果大家有任何问题，我很乐意回答。不知道我们还有没有时间。

LG 弗斯伯格： 这里是主持 LG 弗斯伯格发言。由于时间有限，我们现在进入本次会议的下一环节。

下一个环节是总结性讨论，我想把话筒递给小组成员中的签约方机构，即雷格和马特。

我想问问你们俩，你们现在是否使用信誉拦截列表，如果是，如何使用？让我们从雷格开始。

雷格 • 利维： 谢谢，LG。

目前，Tucows 没有为他们的数据使用任何零售的拦截列表。然而，我们确实定期收到多个有名的拦截列表公司的报告。

不过大多数报告往往不包括完整的 URL，所以我们很难针对各个案例来减轻影响，因为我们无法准确区分问题是什么，即它是一个受影响的域名还是一个恶意的注册人？

在某些情况下，我们可以区分。我们可以提取这个域名，将它放到我们的系统中检查，然后确定它也参与了欺诈性信用卡购买。在这些案例中，往往在我们收到报告之前，该域名就已经下线了。但我们仍然得到了报告。

所以目前而言，我们没有。我们目前正在研究一些可用的选项。我们看重的包括从拦截列表中删除的速度。因此，对我来说，仅仅报告某个域名是恶意的还不够，它还能让我这样说，好的，非常感谢你的报告，我们已经处理了，然后让他们把它从列表中删除。

LG 弗斯伯格： 谢谢，雷格。

马特？

马特 • 托马斯： 在。我只想对一些小组成员已经提出的信誉拦截列表的实用性补充几点。更多是围绕卡雷尔开始提出的其他小组成员也提到的背景概念。

我认为理解信誉拦截列表的应用背景是非常重要的。首先，如果在适当的背景下使用，它们是非常有效的工具。我认为这在很大程度上要回到对这些信誉拦截列表的设计初心的理解上。它们是经过设计，用于保护终端用户和网络及环境的工具。

因此，在这种使用案例下，它们有某些用于这个目的的属性。在信誉拦截列表中纳入内容方面，它们可以更自由一点。但在删除一些条目方面它们可以更保守一点。

因此，作为一个安全从业人员，从企业安全的角度或使用案例来看，这是一个很好的属性，对吧？在这种情况下，你不太关心误报，你更关心的是保护这些终端用户。

但是，当你开始在其他背景下使用信誉拦截列表时，了解这些信誉拦截列表的属性，以及这些属性将如何影响你在不同的测量、工具或研究中使用这些信誉拦截列表的方式是很重要的。了解这些信誉拦截列表如何构建、如何维护、如何运作、如何审核的细微差别，将最终影响你以任何其他系统方式使用该信誉拦截列表的能力。

因此我认为很重要的一点是，我们要了解这些列表的使用方式，并相应地应用它们。

谢谢！

LG 弗斯伯格： 谢谢！

雷格 • 利维： 我想简单强调一下，在了解信誉拦截列表是如何构建的过程中，透明度对那些使用其数据的人是非常有帮助的。

LG 弗斯伯格： 谢谢，雷格。

雷格和马特，你们是否觉得，签约方、注册机构、注册商可以做更多事情，在信誉拦截列表的帮助下，如果他们以某种方式为你提供数据或更新？

马特 • 托马斯： 我是马特 • 托马斯。

这是个非常有趣的问题，LG。我认为在这个问题上，让我印象深刻的是“更多”这个词。这到底是什么意思？你如何来衡量“更多”？

在域名滥用的背景下，“更多”是否意味着有更多的域名被取缔？还是说我们在取缔支持 DNS 滥用类型的底层基础设施工具方面更加有效？

所以我认为，我们应该退一步，因为在这个生态系统中不仅仅只包含信誉拦截列表和签约方。我们需要更广泛的社群关注

DNS 滥用。社群包含许多不同的实体，需要一起协作，以使其更容易实现，对吧？

我们需要让托管提供商、CDN、邮件提供商、执法部门参与进来。通过整个社群一起工作，我们可以更有效地打击滥用问题。

我相信，信誉拦截列表提供者可以给你很多这类例子：他们收集了数据，确定了钓鱼域名，该域名被纳入信誉拦截列表，该域名被关闭，两个小时或一天后域名滥用又出现在几个新的域名上。那么，实际上滥用补救措施是否做得更有效？还是说它只是造成了域名的扩散，将那个域名滥用推到了别的地方？实际的滥用行为本身是否被阻止了呢？

因此，根本的问题是，我们需要对支持这些滥用的基础设施和系统性的东西采取行动。

另一个很好的例子可能是 DGA 和僵尸网络。例如 Conficker，是吧？它已经持续了十年了，还在继续。另一个例子 Avalanche。我们仍然需要努力打击这些类型的 DNS 滥用，因为根本问题是，主机没有打上补丁，相关系统没有得到修复，这是问题的真正核心所在。

因此，LG，我认为你的问题的后半部分，即从签约方的角度来看，可以用信誉拦截列表在哪些方面可以做得更多一点，是有机会的。我认为信誉拦截列表实际上在生态系统中定位非常好。基于他们独特的观察空间，他们可以获得遥测数据，有助于了解取缔这些系统性地支持域名滥用的相关平台的效果如何。

因此，我希望我们能够与 ICANN 社群一起努力，向这个方向推动。谢谢！

LG 弗斯伯格： 谢谢，马特。

雷格，你有什么补充吗？

雷格 • 利维： 是的。我同意马特对在这种情况下什么是“更多”的论述。

我们持续与各种拦截列表提供者合作，以确定我们能否使用他们的服务，因为我们这边有误报补救措施以及删除后的补救措施。因为如先前的一些讨论所提到，会有一些误报。我们必须了解，为了找出所有恶意域名所有者，我们能够接受在什么程度上惩罚无辜的域名所有者。对我来说，这两点都很重要。

LG 弗斯伯格： 谢谢，雷格。

现在我将请我们的一般会员代表乔安娜发言。我想向你提个问题：你觉得信誉拦截列表提供者可以通过什么方式来进一步帮助被列入信誉拦截列表，或在信誉拦截列表方面有问题的终端用户？

乔安娜 • 库勒萨： 谢谢 LG！我知道时间有限，但请允许我简要地回顾一下我们到目前为止所进行的这场热烈的讨论。

我是乔安娜 • 库勒萨。

实际上，这是一般会员社群试图回答的核心问题。信誉拦截列表如何直接影响最终用户？如果他们的域名被不小心误报为有害域名，他们可以向哪里求助？因此，对我们来说，这是一个将本届会议的信息传达给更广泛的社群的问题，也代表了终端用户的问题和制定信誉拦截列表的标准。

我们希望有机会参与在签约方机构和政府咨询委员会 (GAC) 进行的讨论，正如我在聊天窗口中说的那样。
在通常情况下，终端用户会求助于他们当地的服务提供商或执法部门来保护他们的域、域名、商标、资源和他们提供的服务。但这些方法有可能无效，因为如果一个终端用户沿着信誉拦截列表线索来找，他们最终会找到这个特定的小组。

所以对我们来说，这个问题有两个方面。一方面，我们希望能够为终端用户提供一个具体的答复，告诉他们如何能将一个因错误的原因而被列入列表的网站除名，因为这个网站确实没有进行任何恶意活动。

因此，对我们来说，讨论自动和手动黑名单，既是在终端用户中建立能力的一个要素，也是在确保黑名单的标准能够反映他们的需求和期望。目前看来，正如彼得 (Peter) 在问答框中指出的那样，信誉拦截列表的治理和问责是一个比较大同时又被忽视的问题。

在今天的讨论中我们可以看到，我们考虑了各种标准。信誉拦截列表提供者之间进行过一些对话；但是对我们来说，为了能够了解这整个系统是如何运作的，我们希望有一些共同的标准或像本次会议这样的机会来更好地了解系统如何运作，并能够为其发展作出贡献。

因此，用于将某些网站列入黑名单的标准需要在 ICANN 社群内进行讨论，需要听取一般会员的意见。

我们已经听说了垃圾邮件的情况。一般会员社群组织了网络研讨会、会议以及内部政策讨论来确定 DNS 滥用的类别，以尝试定义它们。事实证明，垃圾邮件是较有争议的一种，在一些司法管辖区是合法的，在另一些司法管辖区则是非法的。

因此，对我们来说，看待信誉拦截列表的一个基本要素是设定这些标准的依据。我们希望有机会参与这些讨论以及周一关于监管进展的全体会议，这可能也会影响到注册管理机构和注册服务机构在不同管辖区的工作方式。
我就讲到这里。我知道我们的时间比较紧，LG，但我认为这是一个需要继续推进的讨论。

谢谢！

LG 弗斯伯格： 谢谢，乔安娜。我想接下来向信誉拦截列表提供者问一个问题，这个问题与乔安娜的发言直接相关。

对于被列入信誉拦截列表的终端用户如何解决这个问题，你们有什么建议？卡雷尔。

卡雷尔 • 比特： 好的。我不知道别人怎么做。但我可以告诉你我们怎么做。我们有一个网站，你可以在上面查看你的域名是否被列入到我们的数据集中。如果被列入，那么在大多数情况下你可以直接申请删除，我们会直接处理，你的域名会在几分钟内从我们的数据集中删除。我们每时每刻都在建立数据集。

在某些情况下，因为我们收集到了某些指标，你需要创建一个服务单。我们有 24 小时的工作人员来处理服务单，并帮助你了解出现了什么问题，我们认为你需要做些什么来获得除名。

将会有人工审查列表，然后帮助你了解发生了什么，或者将该域名除名。

LG 弗斯伯格： 非常感谢，卡雷尔！本，这与你的情况是否有很大区别？

本 • 库恩： 有意思的问题。我们的情况是，我们的列表主要是在 24 小时内使用，因为钓鱼网站会下线。但我们做的事情大多与卡雷尔所说的一样，如果有人向我们报告有误报，或者如果有人向我们报告一些不正常的事情，我们会认真看一下，不仅是查看自动化中发生了什么情况以至于该域名会被列到列表中，而且查看该域名具体发生了什么情况。

当我们向注册服务机构或托管服务提供商提供报告时，他们会为我们提供反馈。我们会非常认真地对待这些反馈，并会直接进行调查，以确保我们列表上的域名真正存在网络钓鱼或恶意行为。如果没有此类行为，我们会立即删除它。就像卡雷尔说的，在几分钟内。

LG 弗斯伯格： 谢谢你，本。从今天的讨论中我们可以看出，没有一个通用的反馈路径来报告滥用迹象已解决或是误报。

罗曼，你是否希望建立一个标准化的方式来接收来自众多来源的此类信息？你会需要什么来促进你对它的信任？

罗曼 • 休斯： 这是一个很有意思的问题。当然，我没有一个直接的答案。但我认为在社群中建立信任是一个很好的方式。这是我们可以为之努力的事情。问题是，谁来负责这样的事情，是 ICANN 的责任，还是必须由行业来解决？

LG 弗斯伯格： 非常感谢，罗曼。

乔安娜，我想回到你这边问一个问题。这个问题并不直接针对信誉拦截列表。你认为需要哪些保护措施来确保，注册管理机构和注册服务机构在禁用有迹象参与 DNS 滥用的域名时，不会超出其授权范围？

乔安娜 • 库勒萨： 我支持马特的说法。我是乔安娜。这与透明度有关。标准越清晰，信誉拦截列表提供者对正在应用的标准的讨论越开放，普通的最终用户就越容易理解这个过程，并且他们的声音越容易被听到。

我相信一般会员可以在这方面帮助确定有哪些期望。响应可以是区域性的。我们在周一的会议上也讨论过这个问题。一般会员正在开展 DNS 滥用能力建设活动，该活动将按区域开始。因此，这些响应可能代表某个区域的终端用户。在不同的国家，不同的地区性一般会员组织 (RALO) 的期望可能不同。在周一的会议上，我们已经看到了它们在欧洲的样子。

我认为这将有利于多利益相关方模型的进一步发展。

因此，为了使我们能够更好地促进这一讨论，正如马特所强调的，关于这些程序的透明度、了解它们是如何工作的，并像 ICANN 社群所做的那样，真诚地采取行动，我认为这将有助于我们向前迈进，有效地推进信誉拦截列表。谢谢！

LG 弗斯伯格： 谢谢，乔安娜。

接下来我们有一个听众发来的问题。这是福尔克尔 • 格莱曼 (Volker Greimann) 发来的，他问道：为什么大部分“信誉拦截列表”在报告中没有提供任何证据？如果没有证据或具体的参考资料来对报告进行核实，就很难对它采取行动。

我将把这个问题转给卡雷尔。

卡雷尔 • 比特： 好的。让我们来谈谈这个问题的垃圾邮件方面。这是我比较熟悉的领域。

我们从大型互联网服务供应商那里获得垃圾邮件报告，他们与我们分享他们得到的垃圾邮件的某些特征，或者从我们自己的垃圾邮件陷阱或蜜罐获得这些报告。

垃圾邮件发送者非常善于将各种小的跟踪细节嵌入到 URL、域名、图像和整个电子邮件中。我们收到这些邮件的规模使我们基本上不可能确保从那里剥离所有这些细节，并确保我们提供的任何证据已清除任何识别我们蜜罐的内容。因此，在这一点上，我们要做这样一个决定：如果你分享时不能保护你的来源，那么你就不能分享。

就像我说的，在个别情况下，我们总是愿意给人们提供他们需要的证据，如果我们可以分享它。但从自动化的角度来看，这不太可行。

为了让大家有个概念，举个例子，我们运行的一组蜜罐每秒就会收到 2000 到 3000 封电子邮件。我们没有办法对所有这些进行筛选以确保所有的标识符都不在那里，确保我们提供的数据将是干净的，不会识别出来源。

因此，就像我说的，如果那些正在进行补救工作的人需要具体的证据，那么获取我们的数据以用于该目的的人将知道在哪里与我们联系，他们可以获得额外的详细信息，如果有的话。

LG 弗斯伯格： 非常感谢，卡雷尔！遗憾的是，我们的时间已经不多了，今天的会议将到此结束。

看看本次会议早些时候的投票问题的答案，我想说，我们的听众相当广泛。对于不同类型的滥用，有些人没有听说过，也有人听说过。对于滥用缓解，有些人没有经历过，也有些人经历过。

希望我们当中的一些人能从今天的讨论中学到不少东西，并能在他们的工作中继续推进这个特定的主题。

我想感谢所有小组成员的积极参与，感谢 ICANN 员工的宝贵支持，最后也感谢在这个繁忙的会议周中抽时间参与的听众。

了解信誉拦截列表、其功能、目的以及使用方式或与它们的提供者联系以纠正错误，是制定与它们合作的方式以及反对 DNS 滥用的一个非常重要的步骤。
在这方面我们还有很长的路要走，但我个人认为我们今天取得了一些进展。

再次感谢大家的参与。

布伦达 • 布鲁尔： 我们还有一个最后的投票问题。我们将马上开放这个投票问题。请稍等。

投票问题应该出现在大家的屏幕上了。你知道如何报告安全威胁或采取其他步骤来减少这些威胁吗？请回答是或否。

再说一次，问题已显示在大家的屏幕上了。你知道如何报告安全威胁或采取其他步骤来减少这些威胁吗？请回答是或否。

谢谢！现在我将结束投票并分享结果。
非常感谢大家的参与。本次会议到此结束。

谢谢大家。

布伦达 • 布鲁尔： 现在可以停止录音。

谢谢大家。

[会议记录结束]