ICANN76 | CF – GAC 讨论：DNS 滥用
2023 年 3 月 14 日（星期二）- 10:30 - 12:00（坎昆时间）

茱莉亚 • 莎弗琳 (JULIA CHARVOLEN)：大家好，欢迎参加 3 月 14 日（星期二）当地时间 10:30 举行的 ICANN76 GAC 关于 DNS 滥用的讨论会议。请注意，本次会议正在录音录像，并受 ICANN 预期行为标准约束。

在本次会议期间，使用正确格式在聊天中提交的问题或评论均会被大声读出来。如果您想要发言，请通过 Zoom 平台中举手请求发言。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，以便翻译人员能够更准确地进行翻译工作。在发言时，请确保您的其他所有设备保持静音。在本次会议中，您可以使用 Zoom 工具栏中提供的所有功能。

我就说这么多，下面请 GAC 主席发言。玛娜尔 • 伊斯梅尔 (Manal Ismail)，有请。

玛娜尔 • 伊斯梅尔： 非常感谢茱莉亚。各位上午、下午和晚上好。欢迎回来。这是 GAC 关于缓解 DNS 滥用问题的讨论会议，本次讨论计划持续一小时。在这次会议期间，我们将召集 GAC 成员继续审议 ICANN 组织和 ICANN 社群为防范和缓解 DNS 滥用问题而实施的计划，

我们还将听取相关工作进展情况的简要汇报，并继续讨论 GAC 与更广泛的 ICANN 社群可能做出的合作努力，以支持增强的合同条款和可能的政策制定流程，从而更好地缓解 DNS 滥用问题。

言归正传，请允许我把麦克风交给主题负责人。我们的主题负责人有美国联邦调查局加布里埃尔 • 安德鲁斯 (Gabriel Andrews)、美国联邦贸易委员会兼 GAC PSWG 联合主席劳伦 • 卡宾 (Laureen Kapin)，以及英国国家犯罪调查局兼 GAC PSWG 联合主席克里斯 • 刘易斯 • 埃文斯 (Chris Lewis-Evans)。有请克里斯。

克里斯 • 刘易斯 • 埃文斯： 非常感谢玛娜尔。各位上午、下午和晚上好。请切换到下一张幻灯片。我们将会举行关于 DNS 滥用的会议，今天还有一位 GAC 外部的演讲人。我看到互联网与管辖权政策网络负责人就在角落坐着，你可以在 GAC 的支持人员的帮助下整理一些幻灯片。

在此之前，我会先做一个简短的介绍，让大家知晓解决 DNS 滥用问题如此重要的原因。然后，我们将介绍网络犯罪统计数据及其与滥用 DNS 的关系。在此之后，我们将介绍社群内部正在开展的其他活动。然后进行总结，考量一下公报建议或者对我们来说重要的事情。请切换到下一张幻灯片。谢谢。

我其实觉得我都不需要这张幻灯片。关于 DNS 滥用问题，我们已经讨论过很多次。在这届会议期间，已经有一些会议就这个主题进行了讨论，并取得了良好成果。我要再次公开感谢星期六举行的能力建设工作坊会议。在那场会议上，大家就 DNS 滥用问题进行了良好的交流，大家可以回顾一下。

在这里，我们提供了一些链接，大家可以通过链接访问相应内容。与往常一样，大家可以在 GAC 网站上搜索 DNS 滥用，它会显示公报中的一些内容，我们的支持人员，贝内德塔 (Benedetta) 和其他支持人员一直在更新这些内容。他们在提供资源方面做得很不错，我们可以在网站上进行搜索。我们标记了很多内容。

这也是 PSWG 工作中极为重要的部分。也在我们的工作计划中，我们已经批准并认可了这次会议，这次会议大有裨益，可以让我们支持执法机构和公共安全官员来保护公众安全，而这也确实是他们针对 DNS 滥用问题所做的工作。

正如我所说的，社群内部正在开展很多工作，这些工作对于社群内部的其他利益相关方来说非常重要。当然，还有很多讨论正在进行，例如董事会磋商和通信。企业社群也发布了很多 DNS 滥用问题为何对他们如此重要的相关信息。还有一些审核小组，例如 CCT 审核小组、RDS-WHOIS2、SSR2 等，GNSO 围绕涉及 DNS 滥用问题的后续流程 PDP。

另一个点就是签约方所做的工作，我稍后会介绍这一点。签约方致信给董事会开启合同谈判，以帮助解决 DNS 滥用问题。这是一个良好开端。这表明，社群中的每个人都想要采取一些行动来解决这个问题，而且这个问题对大家来说也确实很重要，当然，这也是我们考量这个问题如此长时间的原因。

接下来，我想问下支持人员，我是不是要结束，以便下一位——

劳伦 • 卡宾： 不是。

克里斯 • 刘易斯 • 埃文斯： 不是。好的。也许可以给加布提个醒。

劳伦 • 卡宾： 这里就可以看出我们懂得灵活变通，可以适应当前环境，并进行相应调整。

克里斯 • 刘易斯 • 埃文斯： 好的。就想给你提个醒，加布。你是下一位发言者。接下来，我们将继续介绍网络犯罪趋势。我们可以切换两张幻灯片吗，这部分内容好像不在我的资料夹中？谢谢。加布，交给你了。谢谢。

加布里埃尔 • 安德鲁斯： 谢谢。嗨。我叫加布里埃尔，今天以公共安全工作组成员的身份发言。我们希望可以在会议期间做的事情就是，未来，我们可以每年举行一次讨论会议，我的这种想法可能有些乐观。我们提出这个建议的原因是，就像试图了解互联网犯罪的范围和规模一样，在了解 DNS 滥用为的范围和规模时，必须要承认的一点是，我们对这个事物的了解并不全面，这一点很重要。我们确实提出了很多不同观点。

就像这张图片中的盲人一样，大家可能在能力建设工作坊会议上见过，我在那场会议上也用过这张照片——我们有很多人都在尽最大努力观察他们面前的东西，谈论他们领会到的知识。我们希望通过合作，我们将能够全面地了解实际情况。

我在这里了解到，为了提供有关 DNS 滥用的数据、衡量标准、测量结果、观察结果，社群已经开展了大量工作，这些工作完成得很出色。我想说一下去年秋天开始的 DNS 滥用协会 Compass 报告。这份报告与 ICANN 的 OCTO 以及他们的域名滥用活动报告报告一样。

我也只是在两天前与高管人员约翰 • 克莱恩 (John Crain) 的谈话中得知有这个报告，他提到，除了我们期盼的注册服务机构级别的滥用报告，还希望能够将预测分析和机器学习的技术纳入到报告中。我非常高兴能够看到这类工作的成果。

但是，要补充这些社群驱动的工作，对于发送给我们的受害者报告，我们希望提供只有执法机构能够提供，并且只来自公共安全角度的一些观点。

需要澄清的是，我们并不是说所有互联网犯罪都是 DNS 滥用。相反，我们的理解是，在审议工作中，你们可能会认为需要将我们所收到的受害者伤害的范围和程度考虑在内，而如果我们将这份报告转换为这些伤害以何种方式并在何处与 DNS 滥用有关，那么这份报告将会更有帮助。我就说到这里，我认为克里斯可以介绍第一部分内容。

克里斯 • 刘易斯 • 埃文斯： 好的。在切换到下一张幻灯片之前，简单说一下。非常抱歉。可以退回到上一张幻灯片吗？谢谢。在上次 PSWG 会议中，我们呼吁所有成员向我们提供一些关于网络犯罪的统计数据，以及这些数据与滥用 DNS 的关系。

目前，我们只收到了美国和英国提供的数据。所以，如果你们正在与自己国家的执法机构或消费者保护机构接触，请随时向他们转达一下我们的诉求。我们真的很想知道其他国家所了解到的网络犯罪情况，并希望能够对这些统计数据进行更全面的审核。我们希望每年开展一次这样的工作，让大家对全局情况有一个了解。

接下来是英国方提供的幻灯片，在英国，我们设立了一个名为“防止诈骗行动处”单独报告机构，他们不只会报告欺诈行为。还会报告一些网络犯罪行为。但他们最开始是这样命名的，后面才加上网络犯罪报告这个职权范围。

该机构的前 4 大收集统计数据并没有跟踪 DNS 滥用问题。他们收集了骇客袭击、社交媒体和电子邮件。病毒和恶意软件在某种程度上

来说属于恶意软件类别，但是病毒也含在内，所以这类统计数据并不符合我们所理解的 DNS 滥用。然后是骇客袭击，无论是个人攻击还是敲诈勒索，这往往是更侧重于勒索软件的资料信息。正如大家在这张幻灯片中看到的那样，这个统计数据从 2014 年开始，此类犯罪报告的总体呈上升趋势。请切换到下一张幻灯片。

他们还在做的一项工作就是，向企业和慈善机构进行调查，了解他们是如何受到影响的，他们面临何种攻击及其应对方法。进行这项分析的目的是，了解有多少组织发现了其系统中存在漏洞或遭受到了攻击。这些数据相对平稳，在企业方面，可能略有下降趋势。有趣的是，在慈善机构方面，这个数据有上升趋势。

出现这种情况的一些原因是，在 GDPR 生效之前，慈善机构可能没有建立自己的网络并进行分析。而一旦开始查找某件事情，往往就很容易找到它。关于出现这种增长的一些原因，究竟是因为慈善机构开始寻找这些攻击并真正发现了它们，还是因为这这种有针对性的攻击本身就在增加，我们很难下定论。或者说，很难判断。但这里显露了一些趋势。请切换到下一张幻灯片。

很明显，这张幻灯片中显示的是，那些遭受安全漏洞攻击的企业被问及，他们如何识别漏洞，以及初始攻击途径是怎么样的。多年以来，在 80% 的情况下，这个问题的答案都是网络钓鱼。网络钓鱼肯定属于 DNS 滥用领域。所以大家可以看到，从我在第一张幻灯片中展示的所有其他犯罪中，大约有 80% 与网络钓鱼有关，或者说最初的攻击途径是网络钓鱼。通过减少网络钓鱼，我们可以对日常处理的其他犯罪所造成的危害产生真正的影响。

第二个攻击途径的读音读起来与网络钓鱼有点相似。但这更侧重于相似的域、欺骗性电子邮件以及其他方面。这仅占其余部分的一部分。显然，其中的一些攻击也可能有一些重叠。下一张幻灯片。

我们向慈善机构提出的相同的问题，答案也非常相似。同样也是 80% 的攻击途径为网络钓鱼。所以，这项非常有力的分析表明，如果我们可以帮助减少 DNS 滥用问题并帮助解决网络钓鱼，这将会对减少这些企业和慈善机构所遭受犯罪的数量产生极为正面的影响。下一张幻灯片。

在英国，我们推出了一项名为“可疑电子邮件报告服务 (SERS)”的服务。不只是 ICANN 喜欢使用首字母缩略词，我们也喜欢。这项服务于 2020 年启动，借助这项服务，个人或企业可以向政府报告可疑电子邮件。这里提供了一些详细信息。他们接受电子邮件转发，也会发送短消息，因为这是网络钓鱼报告的另一个主要信息来源。在 2022 年期间，通过这项服务，我们收到了 640 万起举报。这个数量是非常庞大的。英国境内的很多受害者报告了这些可疑电子邮件。

就像我刚才所说，这项服务是在 2020 年推出，很显然，这在当时是作为对疫情期间发生的一些活动的回应。但自从这项服务推出以来，凭借该服务，我们已经收到了 1580 万起举报。这是一个上升趋势，但目前还没有足够的数据来表明这一点。所以，毫无疑问，在未来的几年里，我可能会将这类数据整合到一个美观的图表中。

这种攻击也会涉及到政府，从报告中可以看出，很明显，这些攻击者正在试图伪装成政府实体。在这些网络钓鱼攻击中，他们代表着我们的医疗服务、TV 许可、税务和海关还有 gov.uk。gov.uk 是一个网站，我们会在上面发布所有的公共信息，无论是应对 2019 冠状病毒病 (COVID-19) 的方法，还是差旅建议。所有的内容都会在上面公

布。还有一个是英国司机及车辆执照局。肯定会有很多针对政府部门的攻击，而这项服务可以帮助消除其中一些攻击。下一张幻灯片。

我刚才介绍了对企业的影响。现在来介绍对个人和互联网用户的影响，个人和互联网用户肯定也会受影响，同样，他们也会向我们举报一些犯罪行为。我们对一些受害者进行了电话调查，了解这些攻击对他们财务造成的影响。

大家可以在这里看到具体数据。这是一个令人震惊的图表。非常抱歉。这可能不是最新的图表。但是，大家可以看到，有很多人损失的金额位于 20 到 250 英磅之间。仔细想想，这笔钱的数目也不大。但是今年，我们有 640 万人报案。假设每个人损失了 20 英磅，就是 20 乘以 640 万，那么这笔钱的数目相当大了，对不法分子来说，这就是收益颇丰的一天或者一年了。

如果大家仔细研究这些数据，就会发现损失金额非常庞大。我的说法可能有点绝对。但是，特别是在目前，随着我们国家/地区的居民都面临生活成本危机，损失这笔钱对这些人来说影响确实会很大。下一张幻灯片。

我们介绍了很多网络犯罪所造成的金钱损失。它对人们造成的影响不只是金钱方面，特别是对这里的个体来说。对企业来说，数据丢失的影响非常大。但在个人层面，丢失数据也会有一些影响，也确实会让人心烦意乱。

我会简单讲解一个案例。我们通过电子警察系统收到了一些信息，曾有一名 17 岁少年向我们报案，他声称一名黑客要求他提供更多密码，并访问了他的一些社交媒体帐户。

接到报案之后，我们进行了一些调查。我们确定了嫌疑人，发现他们有黑客入侵许多个人社交媒体账户的劣迹。所以我们申请了搜查令去他家里搜查，找到了一些他用来犯罪的手机。这些手机上存有大量网络钓鱼的证据。请切换到下一张幻灯片。

这是其中一段通信示例。大家可以在这里看到，这个不法分子表示自己找到了某个人的一些信息，然后说“我在一个网站上找到了你的一些照片。你可能想要采取一些措施。”这个受害者回复，“什么链接？”然后，不法分子就会向受害者发送一个链接，让他们访问。

在查看手机时，我们发现了数百条发给年轻女孩的信息，它们的攻击手段通常是试图访问这些女孩的帐户。所以，大家可以看到，一个域名或者一个人就可以造成数百名受害者。这不是一个类似的事情，一个域，一个受害者。而可能是一个域就可以导致产生数百名受害者。这种影响范围完全取决于攻击的类型以及这种攻击发生作用的方式。当然，我们也调查了那个网站，以了解这个人是如何利用网站来敲诈他人的。请切换到下一张幻灯片。

这张幻灯片将会多次出现，我先说声抱歉，幻灯片上的字体有点小，但这是有原因的。屏幕右上方是一个托管在互联网上的网络钓鱼服务，通过这项服务，注册的用户将能够购买网络钓鱼页面，并且能在互联网上使用这个网页。你可以点击其中一个，例如，Netflix、Facebook、Snapchat 或者任何网站。你甚至可以选择你想要使用的语言。字体很小，这里显示了英语、西班牙语、法语和俄罗斯语，这些语言应该都包含在内。你可以选择想要显示的语言。然后支付该服务的相关费用。

左下角显示的是一个 Snapchat 示例。这个服务会创建一个恶意域，然后您可以将它附加到您的邮件中。那将会为你收集一些详细信息。底部的图片是他们创建的仪表板示例，然后你们便可以前往仪表板并查看所有收集的凭据。

显然，在不法分子收集这些凭据后，他们就会开始敲诈。不管照片是存储在私人设备上，是不是存储在 Google Drive 上，也不管有没有在社交媒体上分享，不法分子都会截取这些照片的快照。所以这会对人们造成很大影响。

在注册服务机构的支持下，我们关闭了这个网站。谢谢你们的努力。涉案人员将于下个月出庭，但鉴于该人员对大量受害者造成的伤害，该人员目前正在羁押候审。在这方面来说，解决滥用问题确实很重要。

当然，我们已经尝试联系每一个能够找到的受害者，并告知他们的数据已经受到保护，我们已经删除了这些数据，同时建议他们更新他们的密码和其他一切应用的密码。了解这种攻击对他们的影响非常重要。我们已经收到了太多类似“哦，谢谢你这么做。我不知道如何处理这种情况。”这样的回复。关键问题是，我们会如何处理这个问题，并消除它所造成的伤害。

我们来看下一张幻灯片。我想下面的时间要交给加布了。

劳伦 • 卡宾： 我想知道我们的同事贝特朗 (BERTRAND) 的演示文稿准备得怎么样了。准备好了吗？你是想现在发言，还是倾向于……你怎么看呢？

克里斯 • 刘易斯 • 埃文斯： 我想接下来应该邀请加布发言，因为他介绍的内容与我的内容衔接更顺畅。那么我们就先说到这里。非常抱歉。我还有一张幻灯片。这张幻灯片是对企业数据和个人数据的汇总。最近的报告是 2020 年到 2021 年的。在英国，他们收到了 87.5 万起欺诈和网络犯罪举报。非常抱歉。我们应该将这两者结合起来。在那份报告中，报告了价值 23.5 亿美元的损失。

80% 的欺诈也是通过网络实现的，这包括来自网络钓鱼电子邮件或其他网络方式。这种损失在很大程度上要归因于某种形式的网络活动。正如之前所说，网络钓鱼电子邮件可能占其中的 80%，这是犯罪分子用来发起网络攻击的工具一个主要途径。这绝对是我的最后一张幻灯片，下面有请加布发言。

加布里埃尔 • 安德鲁斯： 请切换到下一张幻灯片。谢谢。从美国的角度来看。就像克里斯所说，我们真心希望在座的其他人员能够鼓励你们所在国家的执法机构从全球各地分享自己的看法。

上周，美国联邦调查局刚刚发布了 2022 日历年的互联网犯罪报告，这是一个热点新闻。这也是我认为每年就 DNS 滥用进行讨论是件好事的原因所在，因为我们希望能在新信息出现的时候，就将其与大家分享。

这些是我们互联网犯罪投诉中心收到的所有受害者投诉的汇总数据。这是一个集中的门户，我们通过这个门户接收和汇总所有这些数据。然后再反过来，根据这些数据发布报告。但要注意的是，这并不能完全反映现存的所有互联网犯罪。这只是向我们报告一些情况。下一张幻灯片。

在过去的五年里，IC3——这是互联网犯罪投诉中心的简称——平均每年收到大约 65 万起投诉。平均每天有超过 2000 起投诉，这是一个合理的数字。但这个数字依旧严重低估了真实的犯罪数量。大家知道，我们不可能总是会收到所有投诉。

有一点值得关注，当你们去看实际投诉的数量时——这些是联系我们的人——在过去 3 年这个数字相对稳定，这个很有意思。但是它所对应的损失金额却在稳步增加。关于出现这种情况的原因，我希望未来可以给大家一个合理解释。我们现在并没有一个非常合理的解释，但这绝对是一件值得注意的事情。这表明，即使投诉的相对数量保持稳定，但它所导致的金钱损失仍在增加。请切换到下一张幻灯片。

正如克里斯在他的犯罪类别及其汇总方式中提到的那样，我们也没有将 DNS 滥用作为一个类别进行跟踪。但是在 IC3 报告中，我们将 DNS 滥用作为一个类别进行跟踪。我在底部特意指出了网络钓鱼。在查看向我们报告的 5 大类网络犯罪时，我们发现网络钓鱼是第一大类。

更重要的是，这张幻灯片表明在过去五年里，大家可以看到，出于这样或那样的原因，从五年前到今天，网络钓鱼的数量已经激增，至少从我们收到的投诉来看是这样。下一张幻灯片。

这里显示了所有犯罪类别，而不仅仅是前五种犯罪类别，其中还显示了网络钓鱼与它们之间的关系。就像克里斯刚才提到的那样，这里需要强调的是，尽管我们将网络钓鱼作为一个单独的类别进行跟踪，但它通常是不法分子用来危害受害者的最初途径，他们会通过这个途径实施一些其他类别的犯罪。

举个例子，你们可能会问“勒索软件 DNS 是滥用吗？”不，不是的。勒索软件是指不法分子在计算机上获取你的数据，他们对数据进行加密，除非向他们支付赎金，否则他们不会让你找回这些数据。但如果你们问“勒索软件是通过网络钓鱼传播的吗？”，答案是肯定的。

我的姊妹机构 CISA 上周刚刚发布了一份报告，内容涉及一种新的勒索软件变体，称为 Royal 勒索软件。在这份报告中，他们估计 67% 的 Royal 勒索软件感染来自网络钓鱼。同样，我们正在对最初类别进行跟踪，但它已经对下游产生了影响。

我只是想强调一点，当我们的朋友、合作者和 ICANN 社群中的同事在注册服务机构或注册管理机构级别采取一些负责任的反滥用行动来处理在网络钓鱼中使用的恶意注册域名时，他们不仅是在帮助解决最常报道的互联网犯罪类型，还是在帮助解决由此产生的所有其他类别的犯罪。请切换到下一张幻灯片。

除了分享这些来自年度报告的统计数据，在本次会议之前，我也向我的同事问过，“嘿，有什么新的热点新闻吗？有没有什么新的、即将到来并且引领潮流的攻击方式？最近几个月有什么值得注意的攻击？”他们给我的反馈就是所谓的“恶意广告”。为了方便翻译人员理解，我说明一下，这个词是恶意软件和广告的结合。从去年 12 月份开始，一直到今年前几个月，恶意广告攻击受到了很多关注。

就像网络钓鱼一样，这里的不法分子获得了一个出于滥用目的而注册的相似域名。有时，他们会得到一个看起来像软件包的域名，或者类似一些其他可信任的品牌，或者一些服务的域名。但是他们没有在电子邮件中使用这些域名，而是到搜索引擎提供商那里购买广告栏位。

在这个案例中，大家可以看到，这个案例来自 Abuse.CH。我从他们的 Twitter 中找到的案例。在这个案例中，不法分子假装拥有一个与合法的 Thunderbird 邮件客户端相关联的网站。这款软件备受很多人的青睐。但是很明显，不法分子并不是出于好意分享这款软件。

如果你前往他们的广告网站，就会在计算机上看到这款软件和一个恶意软件——在这个例子中，这个恶意软件是 IcedID。这是一个银行特洛伊木马。如果这个恶意软件安装到你们的计算机上，它会最终在你登录银行时捕获、窃取那些登录凭证，然后尝试清空帐户。

这个新攻击趋势值得关注，因为它仍然依赖于那些恶意注册的域名。它本质上是网络钓鱼吗？可能不是，因为这里没有电子邮件链接。但殊途同归，最后结果还是一样的。我向大家介绍这个新攻击趋势，原因有三：第一，因为这是新攻击趋势；第二，因为它与 DNS 有直接联系；第三，也是我个人认为重要的一点，就是在应对真实世界的各种情况时，我们必须保持敏捷和灵活，并愿意将这些新攻击趋势融入到我们的解决方案中。

但像以前一样，负责任的注册服务机构会对恶意注册的域名采取行动，同时它们也在努力解决这个问题，这一点很好。请切换到下一张幻灯片。这是我的最后一张幻灯片。

我只想在这里再强调一下。在英语中，我们可能会说“徒劳无功”。但是，在 ICANN 的所有社群成员中，网络钓鱼被普遍认为是 DNS 滥用。我刚刚从最近的报告中了解到，这也是目前报道最多的网络犯罪类型。网络钓鱼还会促成许多其他犯罪。

针对恶意注册的域名的迅速采取行动，而且我们可以通过政策提供一些激励措施，这一点很重要。它会影响我们所看到的内容。这就是我总结的一些关键要点，感谢大家的关注。

贝特朗现在已经在我这边了，他已经准备好发言了，下面请他发言。

玛娜尔 • 伊斯梅尔： 好的，有请贝特朗发言。请讲。非常感谢互联网与管辖权机构始终与 GAC 保持联系，让我们了解你们在 DNS 滥用方面所做的工作，当然，GAC 对这个主题也非常感兴趣。谢谢。

贝特朗 • 德拉查贝尔(BERTRAND DE LA CHAPELLE)：非常感谢玛娜尔。很高兴再次回到 GAC，多年前我曾作为法国代表参与过 GAC 的诸多事务，其中包括担任 GAC 副主席。我看到了当年的一些熟悉面孔。很高兴有机会参加这次会议。

我是互联网与管辖权政策网络的执行董事，这是我 10 年前与他人共同创立的一个组织。我很高兴来到这里，参与这场在 ICANN 社群内部活跃了几年的辩论，并向大家介绍为了帮助推动辩论以及寻求解决方案，我们已经开展的一些工作。

互联网和管辖权政策网络是……顺便说一下，阿吉斯 • 弗朗西斯(Ajith Francis) 就在后面，他是这个项目的主管。这是一个多利益相关方倡议，旨在将各国政府、公司、技术运营商、学术界、公民社会和国际组织聚集在一起，共同应对互联网领域的管辖权挑战。

具体来说，请切换到下一张幻灯片，我们有三个项目，关于前两个项目，我在这里不多做介绍。但是关于域名和司法管辖权标签下面的一个项目，专门讨论了何时才是在 DNS 层面采取行动解决滥用问题的最恰当时机？我们组建了一个联络小组，5 年多来，该小组已经与来自不同社群的 40 名成员进行了合作。

我很想告诉大家，玛娜尔非常友善，而且在场的其他成员，包括苏珊 (Susan) 在内，都非常积极地参与到这项工作中。我特别感谢她，尽管她的工作负担很重，但她还是抽出时间参加这项工作。因为这项工作很重要。

大体上来说，请切换到下一张幻灯片，我们在这里讨论的一个重要内容是，我们如何打击网络中存在的滥用行为？这些滥用行为变化多样。摆在我们面前的演示文稿就很好的说明了，人类的聪明才智绝对是无限的。我们可以想尽一切办法滥用所有可以滥用的事物。我们都了解这一点。

在大多数情况下，最主要的挑战就是跨境问题，这是第二点。最有趣的是在 GAC 中讨论这个问题，因为你们是政府代表。我也是政府代表。关于难以解决网络中滥用行为问题的原因，我们心知肚明，这是因为各国政府之间并没有一种合作工具来推动采取跨境行动。我们拥有一个基于主权分离的国际架构，而各个国家要依据这个架构开展合作是极为困难的。

我们的计划之一就是解决跨境获取电子证据的问题。这是一个非常棘手的问题，需要数年时间才能在各个国家之间建立正当程序以使用电子证据进行调查。所以，我们所面临的问题，除了网络的全球性以及不法分子可以跨境随意实施犯罪之外，我们还必须解决工具效率低下以及无法在这里促进各国政府开展合作的问题。

下一点是，为了解决这些问题，我们需要更全面地了解互联网自身的运营方式。当我们讨论 DNS 系统时，在你与同事讨论这个架构的运作方式时，在你们熟悉的圈子里，还会有很多人对 DNS 系统运营方式并不了解。如果你们想要了解如何联系注册人，了解 WHOIS 的

运作方式，以及寻找注册服务机构等等。这并不是一件容易做到的事情。

下一点更为重要，也就是我之前提到的，我们缺乏工具，但也存在一个能力问题。大体上来说，DNS 运营商只是提供域名。基本上说，他们没有任何能力来检查某个域名是不是用于网络钓鱼，某个软件是不是恶意软件，所以他们只能依赖通知程序。当我们谈论内容相关的滥用时，情况甚至会更糟糕，我稍后会向大家介绍。如何评估拼凑而成的司法管辖区中内容的合法性？

我还提到了资源，这是因为调查任何一个案例，或者成千上万的案例，需要花费很长时间。这是一个进展相对缓慢且利润较小的行业。

最后一点是，这是大家共同面临的一个问题。这对政府来说是个问题，因为你们有理由担心滥用问题得不到解决。这对企业来说也是一个问题，因为他们也是受害者，或者说他们有责任解决这些问题。对用户来说，这也是个问题。

接下来，我们需要——请切换到下一张幻灯片——了解一些基本信息。大家可能都很熟悉这种运营方式，但我还是想要分享一些，我经常与我们社群之外的人员分享这个信息，因为他们不一定确切地知道系统的运营方式。我们来看看注册人、注册服务机构、注册管理机构和用户之间的关系；从一端到另一端的查询；以及在让所知的互联网按照我们希望的方式运营的过程中，不同参与者所扮演的角色。

这是一个架构，我不想进行过多赘述。我要介绍的是，关于域名，DNS 运营商只能采取 4 种操作。

第一个操作是——请切换到下一张幻灯片——可以锁定域。一般来说，你不能更改注册人提供的信息。不能转移、删除、修改域名。并且你们不能更改已提及的服务器或 IP 地址。重要的是，这个操作不会影响大家访问内容。特别是，你可以锁定域名。这对之后的调查有好处。但是它并不会改变与运营相关的内容。

第二个操作就是，你们可以持有域名。在这一方面，你们可以持有域名，从公共 TLD 区文件中移除域名，但该域名无法解析。你们也不能更改有关服务器的信息。但是在这里，这个系统仍然可以运行。如果使用这个 IP 地址，则仍然可以访问该域名。

第三个操作就是重定向。当你们想要开展调查的时候，这经常被用来沉没特定域名。这个操作基本上是编辑区文件，以重定向到另一个服务器来观察行为，识别受害者，等等。

第四个操作是转移，当你将一个域名转移给另一个注册服务机构时，当在一个特定的注册服务机构以错误的方式进行注册时，这种情况就会发生。但不管出于何种原因，作为最后手段，人们都有兴趣将它转移到另一个注册服务机构，这也是本尼迪克特 • 阿迪斯 (Benedict Addis) 在非常积极参与的一项工作。

下一张幻灯片很重要，这里涉及到 4 个行动措施。你们也可以删除，但我不会对它进行过多赘述，因为出于各种原因，我们不建议这样做。关键的问题是，仅使用这 4 个操作在 DNS 层面上采取行动来解决滥用问题，是正确的方法吗？

在某些情况下，答案是肯定的，而在其他情况下，答案则是否定的。这并不是完美的解决方案。它也不是社群外部的一些人员所认为的那种大型控制面板。在那种控制面板中，如果你们遇到了域名问题

或者与域名相关的问题，只用按下开关，问题就可以解决。但情况并非如此，在某些情况下，采取这些行动是可以解决问题的。

主要有以下几个问题：首先，这涉及到一种工具，它不仅要处理访问域名站点的服务，还要处理许多辅助服务。例如电子邮件、文件传输和其他服务。所以这是一个非常直接的工具。

第二件事是 DNS 滥用具有全球性影响。世界各地都存在这个问题。你们没有办法采取一些措施。你们也不会对暂停的域名进行地理封锁。这里很有趣的一点是，因为你们将它看作是一项功能或者一个错误。作为一个错误，它具有全局影响，所以它不是某个具体层面的问题。但是联系到我之前所说的，也就是我们缺乏用于开展国际合作的工具。在某些情况下，拥有一些具备全球影响力的东西对于我们来说是有益的。

接下来的一点，就像我刚才所说，你们仍然可以通过 IP 地址访问大多数的服务。下一点是，在你们所处的环境中，DNS 运营商是更大的生态系统的一部分。我们需要考虑整个架构，包括托管提供商、ISP 和其他也可以采取行动的参与者。在正确的级别上采取行动是很重要的。

下一点是，目前，在与 ICANN 签订的注册服务机构认证协议和注册管理机构协议中，并没有规定要确定滥用行为以及进行调查的义务，但也有一些有限数量条款规定了阐明真正需要和必要内容的义务。

由此便导致了我们长期目睹的这种情况，即 ICANN 内部多年来一直在进行旷日持久的辩论，尤其是围绕“DNS 滥用”这个词及其含义的定义的讨论。大家在这个方面的立场极为不同。几年来，我们举行了无数场讨论会议。不同选区之间针对“DNS 滥用”定义的具体

内容的相互批判。甚至是不同选区内部就应采取或不应采取的行动量问题也产生一些紧张关系。

这并不是说他们是不良行为者。我们也知道存在一些不良行为者。当然，我们也有一些相对来说更有责任心的成员。但很明显，我们没办法就这个问题达成共识。其结果就是，我们只有深深的挫败感。

最后一行说的是，如果你提出的问题本身就是错误的，那么就不太可能会获得正确的答案，这就需要我们重构问题。我们可以重新整理下问题，请切换到下一张幻灯片，真正的问题是：何时适合在 DNS 级别采取行动来解决网络中滥用行为问题？我认为大家已经对这种表述达成一致意见，而且这种表述也将各种不同元素考虑在内。

下一张幻灯片是，在这种重新整理工作中，我们已经与先前提到的联络小组合作了很长时间，并缩小了对 DNS 滥用的理解范围，我们曾一度将其称为技术滥用。但是，在一些参与者的帮助下，我们缩小了 DNS 滥用概念的范围，现在为以下 5 种类别：恶意软件传播、僵尸网络、网络钓鱼、网址嫁接和垃圾邮件，在某种程度上，它被用作上述问题的交付机制。

大家可以找到有关这 5 个类别的更多详细信息，这些内容首先在 I&JPN 于 2019 年 4 月编制的运营方法中提及。在此之后，DNS 滥用的这些定义被纳入到社群中一些参与者于 2019 年 12 月编制的滥用应对框架中，紧接着，2021 年的 SSAC 报告 115 纳入了 DNS 滥用的这一定义。

这可能不是完美的定义，但这是区分这两者的一个非常重要的元素，我们可以称之为 DNS 滥用，每个参与者都知道有理由接受调查，并且在运营商的职权范围内，我将在稍后处理与内容相关的滥用。

在这种情况下，我们于 2021 年制作了一个工具包，我不会展开所有细节，但我鼓励大家在线查看，以帮助 DNS 运营商、通知者、立法者或执法机构了解不同的参数，并为会议和合作提供指导元素。

下一张幻灯片提到了一个重要元素，即在处理任何类型的滥用时，都有围绕四个元素的工作流程。第一个元素基本上是识别滥用本身。可以来自通知者或由运营商自己。二是对这种滥用的评估。这真的证明了 DNS 级别的行为是正当的吗？

第三个元素是，在我提到的四个元素中，应该采取什么行动？第四个元素我们还没有讨论过，但它是整体情况的一部分，也就是当已经做出决定，但出于某种原因必须改变时，有哪些求助途径。可能会发生错误。

我就不过多讲述了，对于每一个阶段，我们已经产生了一定数量的结果，比如更清楚地定义滥用的类型。提及一些元素，关于通知者在尽职调查方面应采取哪些行动来记录这些元素。仅发出通知而没有任何可持续的证据是不够的。通知注册人的条件是什么，尤其是当网站受到威胁时？

关于评估，有一个关键问题，即采取行动的门限和标准是什么？什么时候需要达到门限？以及行动的选择。正如我提到的，有不同类型的行动。有一份文件准确地解释了我之前给你们看的那些图。最后，关于求助，还有求助渠道和透明度元素的问题。

这是一个过程。与试图补救滥用行为的调查相关的所有工作都要经历涉及不同参与者之间合作的不同阶段。请转到下一张幻灯片。在这种情况下，联络小组编制了一系列文件，我希望这些文件对整个社群有用，但对一般性辩论也有用。

第一个问题是通知应当包含哪些内容？支持证据的通知有哪些组成部分？第二个问题是有哪些类型的通知者？例如，作为儿童性虐待图像或商业商标侵权的通知者是一样的吗？

接下来的问题我之前说过，通知者应该进行什么样的尽职调查，才能确保验证的负担不完全由运营商承担？在可信通知者之间可以做怎样的安排？可信通知者的安排是怎样的？

我想在这里澄清一下。没有人可以自己说，“我是可信通知者。”充其量你可以说，“我在这个特定领域拥有专业知识，这使我成为一个专业的通知者。”可信通知者关系是一种双方认可的关系。你可以是一个运营商的可信通知者，但不能成为其他运营商的可信通知者。这是一个重要区别，我们需要在通知者的概念上做更多的工作。

有一份专门的文件正在解决僵尸网络的问题。我就不详细介绍了。但是有一个非常重要的问题，称为算法生成域。在执法机构、ICANN 和 DNS 运营商之间围绕算法生成域找到更好的合作是一个非常重要的元素。我认为这份文件有助于将讨论向前推进一点。

最后，关于网络钓鱼和恶意软件，我们与联络小组合作，就注册管理机构和注册服务机构在不同阶段的角色分配制定了清晰的图形化工作流程。有哪些信息渠道等？

我非常高兴在这里提到这一点，因为格雷姆 • 邦顿 (GRAEME BUNTON) 就坐在角落里，你们中的有些人已经见过他了。它促成了两项重大举措，我非常高兴这些举措建立在 I&JPN 中开展的工作的基础上，在 PIR 的帮助下成立了 DNS 滥用协会，并在此背景下推出了我们在联络小组中讨论过的内容，这是一个报告滥用的界面，现在名为 NetBeacon。

CleanDNS 已经……杰夫 • 百瑟 (Jeff Bedser) 已经帮助实现了这一点。PIR 的布莱恩 • 辛博里克 (Brian Cimbolic) 就坐在他旁边。布莱恩实际上是我们在 I&J 的联络小组的协调员。对我来说，这项工作取得的成果是惊人的，因为它是五年工作的结果，导致了一个非常具体的元素，一个可操作的元素，而不仅仅是讨论或论文。真的是可操作的元素。向那些正在向前传递火炬的人们致敬。

这一点很重要，因为除此之外，这也引发了本届 ICANN76 会议期间关于改进认证协议的讨论。

我现在结束这一部分内容，之后我将做一个简短讨论。是关于 DNS 滥用，被理解为我们刚才在谈论的五个元素。请切换到下一张幻灯片。总的来说，我认为负责任的参与者之间有一个共识，即以这种方式理解的 DNS 滥用确实是在有确凿证据的情况下在 DNS 层面采取行动的正当行为，除非该网站已被破坏或存在其他情况。但总的来说，我们看到了朝着可实施合作的积极方向发展。

我要讲的最后一部分是与内容相关的滥用问题，目前正在确定，这一问题要复杂得多，因为在这里，图像有点像镜像。一般来说，由于许多原因，DNS 级别不是解决与内容相关的滥用问题的正确位置，包括它不够精细的事实。很难有针对某个地区或另一个地区的非法行为量身定制的内容。

评估是否存在滥用的能力大不相同。这是一个运营商不知道的技术问题。一般来说，它不是一个有效的工具，因为在大多数情况下内容仍然可用。

但是，仍有一定数量的情况非常特殊，足以证明在遇到这些情况时需要在 DNS 级别采取行动。在我们在柏林组织的全球会议之前，我

们在 2019 年制定的运营方法中，有四个非常初步的要素，可以考虑猜测或评估何时适合在 DNS 层面对内容相关的滥用采取行动。

这是全球一致认为有问题的内容是非法的吗？在这里，你可以完全区分两种情况，一种是以某种方式处于一个极端的 CSAM 中，另一种是世界各地立法极其不同的情况。关于什么是违法的，什么不是违法的，存在很大差异。专用于侵权内容的网站比例。注册人或网站运营商的意图或恶意。此外，其他级别是否已经用尽了网站运营商、注册人或托管服务提供商。

我不会在这个问题上纠缠不休，但真正区分这两类事情是很重要的。两者都很重要，但不应该以完全相同的方式处理。最大的挑战之一是我们没有空间来讨论第二个问题。ICANN 是以我们之前描述的方式讨论 DNS 滥用问题的合适场所。但是很明显，根据授权 - 社群完全同意这一点 - 它不是讨论与内容相关滥用的地方。一直以来都有关于“ICANN 不是内容警察”等的博文。而且完全可以理解。

问题是，除此之外没有什么地方可以讨论。这就是为什么在 2022 年 5 月，相当一部分参与 I&J 联络小组的人要求我们基本上成为讨论网站内容滥用的地方，以探索这些特殊情况，找到门限、标准和机制。

这就是我们今年着手开始的工作。这是初步的工作。刚刚开始。但我认为，对于 GAC 社群来说，重要的是要了解全局，并理解 ICANN 确实是在我们共同努力解决 DNS 滥用问题的基础上向前发展的。它并不完美，但是还得执行，还得加强。但它确实在这方面在向前迈进，变得更清晰、具有更好的机制和更好的合作。

关于与内容相关的滥用，虽然这不属于 ICANN 的范围，但我们作为 I&JPN 将继续围绕下一张幻灯片中的以下元素开展这项活动。第一，触发与内容相关的滥用的 DNS 层，要么是因为有绝对的理由直接进

入该层，要么是因为在用尽堆栈中的其他级别后，这是最后的手段。以及你如何联系网站运营商、注册人和托管服务提供商的问题？首先要讨论的是升级路径是什么。

第二个元素是如何制定门限标准。举个例子，你可以说，“整个网站应该专用于侵权内容或活动。”或者你可以说，“除此之外，网站上没有其他合法的内容。”或者你可以说，“网站运营商的意图是做 x、y 和 z。”配方很重要，我们正在推动这些讨论。

最后，可达性的概念很有趣。当我们说有升级路径时，你如何发送通知，以及如何联系注册人、网站运营商或托管服务提供商？这是我们将要深入探讨的问题，因为对于托管服务提供商来说，还没有明确的 WHOIS 对等系统。弄清一个特定的网站实际上托管在哪里比仅仅找到谁是注册服务机构要复杂一点。

最后，我提到了可信通知者协议的概念。这是非常重要的一点，因为特别是对于与内容相关的滥用甚至比网络钓鱼更严重，但是对于与内容相关的滥用，如果没有三类行为者之间的合作，就没有解决方案，这三类行为者是执法机构、必须提高其能力和可信度的各种通知者，以及现有协议中的 DNS 运营商。

对于那些还记得 NTIA 和 ICANN 在过去制定《义务确认书》的人来说，我相信有一个框架概念，那就是相互义务确认。我们需要建立机制，将具有正当程序能力和程序的通知者、促进合作的执法机构以及运营商聚集在一起，以便在适当的时候在 DNS 级别采取行动。

我想强调的是，我们在这里讨论的不是处理大平台的监管问题。这个平台不是 Facebook，不是这个世界的 Twitter。你不会要求删除 Facebook.com，因为那里的一个次级小组中有一些内容。但是，当有人在一个域名后面建立了一个怀有恶意的网站时，找到这些人并

基本上停止这种打地鼠式的练习，即在这里停止，然后在那里停止，并努力抓住真正做这种事情的人，这是需要的重要合作。

所以我的观点是这是一项共同责任。这需要不同行为者之间进行合作。互联网和司法协会的座右铭是“支持多利益相关方合作”。我们这样做是为了促成一定数量的协议。我们很高兴这促进了 ICANN 环境的进步。这是我们解决这些问题的唯一途径。

在幻灯片中，你有一系列……不，之前应该有一张幻灯片。但消失不见了。我重新整理一下。这里有一张幻灯片，上面有我展示的所有文件的链接。在最后一张幻灯片上，这是我的联系方式和阿吉斯 • 弗朗西斯的联系方式，如果你想在会后和我们讨论这个问题，请联系我们。非常感谢给我这个演讲的机会。

玛娜尔 • 伊斯梅尔： 非常感谢贝特朗为我们做了一次非常全面、结构合理且内容丰富的演讲。在请我们的 GAC 主题负责人发言之前，我想感谢 Zoom 会议室中伊朗代表非常耐心地举手。你想先讲吗？好的。卡沃斯，请等一下。先请克里斯发言，然后再请你发言。非常抱歉。

克里斯 • 刘易斯 • 埃文斯： 谢谢玛娜尔。实际上我想提一下建议。我们收到了很多意见和建议，很多人都在讨论。如果大家对最近几次演讲有任何想法或问题，现在欢迎大家提出来。然后，我们将讨论 ICANN 社群内正在进行的活动，以及坎昆会议公报语言的考虑因素。这也是一个问题。但是就在我们已经做的最后两个演示中，也许现在讨论一些问题和想法比较好。谢谢。

玛娜尔 • 伊斯梅尔： 非常感谢，克里斯。卡沃斯，对于本次会议的第一部分，无论是对主题负责人，还是对贝特朗，你有什么要说的吗？请发言。

卡沃斯 • 阿斯特 (KAVOUSS ARASTEH)：非常感谢玛娜尔。让我向主席台上的各位表示衷心的感谢。在我看来，这是我们关于 DNS 滥用的最有趣的讨论之一。虽然我不想在不同的部分之间做比较，但最后一部分，在我看来非常有趣。

正如我昨天提到的，我们有一些问题。我们已经解决了这些问题。我的建议是，首先，尊敬的主席和 GAC 未来的主席尼科尔 (Nicol)，我们需要在下一次会议的 GAC 议程中投入更多时间来讨论这个问题。从表面上看，我们不可能得出结果，不能像今天这样深入探讨问题的核心，以了解实际情况。有许多问题 [要讨论]。我不知道。我们现在没有时间解释。我有一些建议。我不知道你们要向我提出什么建议。但有一条前进的道路。

但我想我只想谈其中一点。主席台右手边的一位尊敬的朋友提到了国际政府间合作。这个问题已经讨论了很多年。这不是 ICANN 的问题，因为 ICANN 不是国际政府间组织，GAC 也不是国际政府间组织。GAC 是政府咨询委员会。政府是国际政府间的。他们在别处，但不在这里。

抱歉。我对 [每个人] 都很坦诚。很多时候，我们想解决这个问题，即国际政府间合作。一些政府对此表示反对，称网络犯罪是一个国家问题，不应该在国际处理。他们说，如果 [签订] 条约，任何国际政府间合作都是有益的。不可能就此达成条约。

因此，让我们深入了解情况，而不是在本次会议上，因为本次会议即将结束。尊敬的 GAC 主席，如果可能的话，我们将进一步讨论这

个问题，看看我们能做些什么。提出了许多好的观点。到目前为止，主要是提出问题。但是仍然没有提出解决方案。这很重要。我要说的是，解决问题有时不太容易，但提出问题很容易。提出解决方案建议就更难了。解决方案在哪里？

我们必须采取最务实的方法，而不是通过立法来看看我们能做些什么。根据我们能做的工作的优先程度，对工作进行分类。目前，国际政府间合作问题不是那么容易解决的。但是还有许多其他问题要解决。

我们收到了来自英国代表和美国代表的报告。我们可以问一下所有 GAC 成员："你们有过同样的经历吗？报告的内容是什么？你们遇到……？"我遇到过，但从未报告过。我个人多次通过我的电子邮件……我昨天告诉说，[另一个人] 说 [他们有一辆外交车] 以 10% 的价格。我没有打开那封电子邮件，因为我儿子很聪明。告诉我，"爸爸，不要打开这些东西。不要打开。如果你收到一封电子邮件，你不知道发件人，不要打开它。我可能做得不好，没有 [音频不清晰]。但不要打开它，因为如果打开，你可能会马上……"

还有其他方法。一些电子邮件提供商，他们有双重安全措施，如果你的密码等被除了你的桌面或设备之外的其他人拿走，没有人能使用它，因为他们要求使用第二种安全措施。所以我们必须给人们提供一些好的建议，作为初步的预防措施。那些至少能减少这些问题的措施什么？这是我们需要讨论的问题。

我还有很多其他问题要讨论，但是没有时间。所以很抱歉，如果我 [音频不清晰]，但这就是我要讲的全部内容。谢谢。

玛娜尔 • 伊斯梅尔： 非常感谢伊朗代表。克里斯，如果可以的话，我们还有另外两位同事请求发言，也许你可以稍微回应一下。我们只剩下 20 分钟时间了，先请刚果民主共和国代表发言，然后请美国代表发言。请讲。请刚果民主共和国代表发言。

布莱斯 • 阿兹特米娜 • 基金吉 (BLAISE AZITEMINA FUNDJI)：非常感谢。感谢所有发言者。有点像卡沃斯，我真的很想提一下这个演讲有多重要。从政府的角度来看，对于大多数政府，尤其是非洲政府来说，我认为我们政府希望在 GAC 中有一名代表，主要是为了解决这种滥用问题。

显然，我的问题或意见当然主要是，这里的标题或主题是滥用。但我真的想问一下，政府是否可以采取任何行动来防止这个问题。当然，我们谈论的是缓解，是治愈。但是你知道，在法语中，我们说，“预防总比管理好。”有没有像 ICANN 建议的那样，有一些行动？

当然，我们谈论的是涉及国家主权的网络安全问题。但是即使就主要对企业和主要对政府的建议而言，有哪些建议呢？我们如何防止这种情况发生？

我们看到了一些来自联邦调查局的介绍，大部分也是来自英国的经验。我知道有一些研究。有一些统计数据可能有助于理解为什么我们会有这种滥用问题。我们知道，对于最终用户来说，主要是网络钓鱼，是电子邮件，密码泄露。但是对于企业，主要是政府来说，除了坐等滥用得到缓解或治愈之外，有没有一些行动可以预防呢？谢谢。

玛娜尔 • 伊斯梅尔： 非常感谢刚果代表。下面依次请美国代表和法国代表简略发言。然后请克里斯发言。请美国代表发言。

苏珊 • 查尔莫斯 (SUSAN CHALMERS)：谢谢玛娜尔。实际上，我很高兴能够发言，这样我们同事的问题就能够得到回答。谢谢。

玛娜尔 • 伊斯梅尔： 非常感谢美国代表。下面请法国代表发言，然后请克里斯发言。这样可以吗，克里斯？有请法国代表发言。

乔纳斯 • 鲁尔 (JONAS ROULE)：首先，让我感谢所有小组成员的精彩演讲。我很荣幸代替我以前的同事来这里参加会议。我只是想参与一下，想对讨论的问题谈一下我的看法。我是新 GAC 成员，我觉得在开始工作之前，我应该对某些主题有更多的了解。

首先，作为新成员，我想探索一些辅助手段，看看我是否可以做一些工作来预防外部攻击。我感觉一些参与者提出的有利价格导致了 DNS 中的一些滥用现象。所以我想知道我们如何才能看到域名更新的频率。也许这可以帮助社群在这方面做一些工作。

我们知道哪些参与者的参与是不合法的。也许我们能发现他们使用的一些机制。但是我们观察到的一些困难需要用证据来证明。我认为这是我们需要的。感谢大家的关注。

玛娜尔 • 伊斯梅尔： 非常感谢法国代表。我看到卢旺达代表举手了。请简明扼要，因为我们的会议结束时间就要了。

文森特 • 穆斯米纳利 (VINCENT MUSEMINALI)：非常感谢。我想感谢各位演讲的同事，感谢介绍美国和英国关于网络犯罪的报告的小组成员。我想澄清一下关于 [音频不清晰] 加密货币的问题。大多数人现在都面临一些挑战，这些挑战是使用与加密货币 [相关的] 网络犯罪的相关域名。这些域名有时会被关闭，导致人们 [音频不清晰] 损失金钱和投资。他们 [现在] 必须跟进这项投资。我只想知道他们如何与 INTERPOL 合作。谢谢。

玛娜尔 • 伊斯梅尔： 非常感谢卢旺达代表。下面请克里斯发言。抱歉挤压了你的时间，但还是很高兴听到 GAC 同事发言。请讲。

克里斯 • 刘易斯 • 埃文斯： 谢谢玛娜尔。当然，非常感谢你们提供的意见和建议。我将试着快速总结一下我的一些意见。关于建议，我们刚才听刚果代表和法国代表说到，我们现在不打算在这里讨论。有很多建议。你可以做很多事情。也许这可以作为未来 ICANN 能力建设工作坊的讨论内容。因此，这可能是 GAC 需要考虑的一个问题，因为需要在一个稍微长一点的会议上进行讨论。所以，这可能是我们可以考虑的事情。

那么，围绕伊朗代表提出的观点，“我们能做什么？”我想贝特朗回答了几个问题。NetBeacon 当然是作为一种报告工具被提及的，是一种行动方式，也是对抗其中一些问题的一种方式。如果能转到这些幻灯片，就能很好地引出正在进行的活动。我们将介绍社群中一直在进行的支持缓解 DNS 滥用问题的一些行动。

关于加密货币，我认为这也有点符合贝特朗的观点。这可能来自网络钓鱼电子邮件，属于 DNS 滥用，也可能是与内容相关的问题，属于此类机制。

然后，去参加社群活动。还有不少正在进行的工作。注册管理机构正在努力自愿共享统计数据。从执法机构的角度来看，我们认为这非常重要。它让我们了解了整体情况。对于支持这项工作的注册管理机构也是如此。

再提下一个，那就是 acidtool.com。贝特朗说，没有工具来识别托管服务提供商和电子邮件提供商。事实上，注册服务机构创建了这个工具来帮助人们识别正确的切入点，从而采取有效行动。我们从 I&J 演示中了解到，采取有效的行动非常重要。无论是分销商、注册服务机构、注册管理机构，还是托管服务提供商，找到正确的切入点都非常重要。

在这里，我再次提到 NetBeacon，作为采取行动的一种方法。这非常符合 SSAC115 中的建议。SSAC 为我们做了关于这方面的很好的介绍，在 I&J 报告中也提到了这一点。这些都是有助于缓解目前正在进行的 [建议] 的活动。此外，DNS 滥用协会正在分享其收集的数据分析结果，并纳入到 DNS 滥用报告中。请转到下一张幻灯片。

对于口译人员来说，我可能说得太快了，所以我现在要道歉，说慢一点。DNS 滥用问题 GNSO 小组也非常活跃。我只想在这里指出，他们的发现反映了我们在海牙公报中的一些重要问题，即任何未来关于 DNS 滥用的 PDP 工作都应该有针对性，以产生一些及时和可行的结果。回应一下伊朗代表的观点，我们在社群中做的任何工作都需要有针对性，以使其能够发生并迅速发生。我知道有时事情发生得不够快会让人感到沮丧。请切换到下一张幻灯片。

在 ICANN 的职权范围内，他们有 OCTO 小组，有 DAAR 系统。我们在周六也听说了这一点，我相信是这样的，他们正在分析 1,145 个 gTLD 的数据，这让我们对有这么多 gTLDs 感到惊讶。我想还有 21 个 ccTLD。同样，这也是一个更好的概况介绍，可以更好地了解正在发生的事情，以便能够采取有效的行动。请转到下一张幻灯片。

这只是一个关于路径和联系人的提示。这是一个复杂的空间。这是一个 ICANN 图表，非常感谢。我根本画不出那样的图表。我们听说只有找到对的人，才能在适当的时间采取正确的行动。当然，在我看来，我们看到了我们能够做到这一点的地方，这也减少了伤害。所以，能够明白去哪里，快速去哪里真的很重要。所以像 NetBeacon、ACID Tool 这样的工具真的很有帮助。

这幅图实际上也比这个稍微复杂一些。在右边是注册人，然后是分销商。并不总是有分销商，有时不止一个分销商。理解这一点对找到正确的切入点非常重要。请转到下一张幻灯片。

仅在分销商方面进行说明，在 EPDP 的第 1 阶段工作中，建议注册服务机构应为与注册人有关系的分销商生成一个分销商数据元素。这在有多个分销商的地方很重要。因此，在目前的 WHOIS 回应中，有一个分销商字段，但不一定收集所有这些信息。正如我所说的，能够直接找到能够做出最有效回应的人对我们来说非常重要。这也反映在 CCT 审核中。请转到下一张幻灯片。

下面请劳伦发言。很抱歉我说得太快了，但如果可以的话，我想继续讨论我们的第二组问题。

玛娜尔 • 伊斯梅尔： 劳伦，已经有同事请求发言。先请这位同事发言好吗？好的。我看到英国代表举手了。尼戈尔，请讲。

尼戈尔 • 希克森 (NIGEL HICKSON)：非常感谢主席女士。我很乐意让劳伦先讲，我们也许可以晚一点再讲。劳伦，请发言。

劳伦 • 卡宾： 谢谢尼戈尔。我以公共安全工作组联合主席之一和这一非常重要议题的主题问题专家之一的身份发言。请转到下一张幻灯片。

我很高兴这次会议是互动式的，甚至在这之前的会议也是这样。但是已经有很多关于 GAC 想要什么的讨论、观点和信息……让我重新介绍一下。分享了很多信息和观点。现在我们可以讨论 GAC 希望在公报中强调什么，也就是潜在的问题。

首先，这属于“如果值得说，就值得说很多次”的范畴，我们在注册管理机构、注册服务机构和 ICANN 之间正在进行的合同谈判。此外，该流程的整体目标是提高最低限额，从而改进针对 DNS 滥用采取行动的合同义务。所以是义务，而不是自愿的工作。这些义务的目的是反映一种覆盖所有人的义务。这将有望包括不良参与者，并给予 ICANN 比它已经处理有关 DNS 滥用情况更多的工具。

同样，这只是第一步，未来还会有更多的步骤。但对于 GAC 来说，这可能是一个重要的时机，可以承认并赞扬这项工作正在进行，并且是在签约方的倡议下进行的。这是一个积极的步骤，总是受到欢迎。

这是许多步骤中的第一步，因此可以预见未来的政策工作。我想回应一下伊朗同事的意见，即在这里确定优先事项和重点工作非常重要，因为这是处理事务的方式。我们可以将这两个指导原则应用于任何 PDP，这些 PDP 不一定以其快速和专注的行动而闻名，但在这种情况下，这些 PDP 可以而且应该如此。此外，签约方和 ICANN 之间可能有更多的谈判机会。

值得一提的是，签约方公布他们的工作成果后，将会有一个征询公众意见的机会，这是我们热切期待的。然后，GAC 将有机会决定希望广播哪种类型的意见和建议。请切换到下一张幻灯片。

分销商的这个问题也已确定。正如我们来自互联网和司法协会的同事贝特朗所指出的那样，与 DNS 滥用有关的原因是因为它太重要了。当你处理 DNS 滥用时，能够找到正确的实体是非常重要的。该主题一直是 GAC 以多种不同形式提出意见的主题，与 CCT 最终报告以及最近的第一阶段域名注册数据建议相关。请转到下一张幻灯片。

现在请我的 GAC 同事发言，请他们就 GAC 公报中可能包含的内容提出想法和意见。我还注意到，我知道因为时间紧迫，我们有公报起草会议。但这将是一个很好的机会来了解大家的想法。

玛娜尔 • 伊斯梅尔： 非常感谢你，劳伦。下面依次请英国代表、伊朗代表和欧盟委员会代表发言。我们有三分钟时间，所以我希望……请尽量简明扼要。请英国代表发言。

尼戈尔 • 希克森： 好的。非常感谢玛娜尔。非常感谢坐在前排桌子前为我们演讲的各位同事。正如其他 GAC 成员所指出的那样，这是一次非常有用的会议。请允许我简单说四点。

一是重申我们对即将进行的合同谈判的立场。我非常肯定。我认为昨天我们与注册服务机构和注册管理机构代表的会议非常成功。我们当然期待公共协商。完全无意干涉这些谈判。当然期待了解最新进展。正如各位代表昨天所说的那样，这是第一步。很可能会有其他针对 DNS 滥用的计划 - 迷你 PDP 或其他。

其次，就公报而言，我们无疑将讨论这些问题。我认为，我们应该在公报中非常明确地表示我们如何欢迎这些举措，但也应该逐项列出这些建议：GAC 关于 CCT 审核建议 17 的意见，以及我们讨论过应该标记的分销商方面的其他问题，以便整个社群了解在下一个 SubPro 流程之前需要采取的特定行动。我要说的就这些。非常感谢。

玛娜尔 • 伊斯梅尔： 非常感谢英国代表。下面请伊朗代表发言，在日本代表发言之后我就要关闭发言队列了。伊朗代表，请讲。

卡沃斯 • 阿斯特： 非常感谢玛娜尔。我和包括你在内的一些尊敬的同事讨论过，DNS 滥用问题是 ICANN 当前和近期以及长期的核心问题。这是很重要的问题。但是每个人，包括董事会、ICANN 组织、成员和每个人都在研究这个问题。在这方面没有必要有任何 GAC 建议。让大家喘口气，想一想，消化一下这个问题，不要要求大家做超出我们需求的工作。他们知道问题是什么。

另一方面，在对 GAC 重要的问题中，我们首先需要提到的是，认可 ICANN 董事会或 ICANN 与签约方、注册管理机构和注册服务机构之间正在进行的协商，这是一个很好的步骤。然后我们应该提到，我们需要在下一次 ICANN 会议上，即在华盛顿哥伦比亚特区召开的 ICANN77 会议上，收到一份关于正在进行的工作的进展情况报告。

我们预计最终报告将是 78、79 或 80，但也有足够的措施，以便建议政府或 GAC 人员如何应对，如何抵御，或如何应对这种情况，正如我的同事提到的，并看到克里斯、劳伦和加布里埃尔的报告中提到的许多其他内容，将对 GAC 重要的问题纳入报告中。

试着强调一下这个问题的重要性。努力把文字写得更清楚、更精确、更简洁，并试着 [标出要点] 并采取后续行动。但我建议，在现阶段，我们不要在 GAC 建议中包含任何关于 DNS 滥用的内容。谢谢。

玛娜尔 • 伊斯梅尔： 非常感谢伊朗代表。下面依次请欧盟委员会代表和日本代表发言。友情提示，请尽量简短。请欧盟委员会代表发言。杰玛，请讲。

杰玛 • 卡罗里洛 (GEMMA CAROLILLO)：非常感谢玛娜尔。我已经在聊天中推荐了这些演示，因此出于时间原因，我不再重复了。关于公报的要点和考虑，我简单说一下，正如劳伦友好地要求的，我们当然同意这是一项伟大的举动。关于谈判，我们在 GAC 内部已经呼吁了很长时间。所以这肯定是我们应该支持的工作。

就附加内容而言，我们可能希望在重要问题下添加 DNS 滥用部分。他们会接受，但当然是为了进一步讨论。首先，预防措施的重要性。我们有点担心，到目前为止我们所听到的，主要是关于反应性措施。

但是从我们的角度来看，防止 DNS 滥用是非常关键的。我以前也从一两个同事那里听说过。然后，可能探讨激励措施的问题，PSWG 等组织的同事在这项很好的建议中提出了这个问题。

最后但同样重要的是，结合尼戈尔关于下一轮次 gTLD 的发言，总体而言，我们希望确保不会忘记之前的工作，特别是与防止 DNS 滥用的合理措施有关的工作。但 GAC 在将公报 71、72、73 中的数据准确性、域名注册准确性和 DNS 滥用联系起来方面相当强大，我敢肯定还有更多。因此，这并不是要列出这些内容，而是要表明我们希望在注册数据准确性方面以及防止 DNS 滥用的重要性方面所做的工作不会丢失。非常感谢。

玛娜尔 • 伊斯梅尔： 非常感谢欧盟委员会代表。最后但同样重要的是，下面请日本代表发言。

西泻信步 (NOBU NISHIGATA)： 非常感谢玛娜尔和 PSWG 联合主席。大家晚上好。现在日本已经是晚上了。我从东京向各位问好，大家上午好，下午好。非常感谢组织了今天这次精彩的会议。

我想就劳伦关于公报审议的演讲谈一下看法。日本支持正在进行的合同谈判，对于到目前为止所取得的进展，我们非常欢迎。

但另一方面，日本希望在《注册服务机构认证协议》第 3.18.1 条中提出一个问题，关于注册服务机构报告非法活动需要采取的行动。日本政府 [已报告] 并意识到一些注册服务机构没有采取任何行动，甚至没有回应日本方面的非法活动报告。这就是为什么日本政府不断要求改进这份合同文本或条款的原因。

日本政府提供了一些证据。但尽管如此，还有一大堆其他类似的证据 - ICANN 的审计报告或最近来自 ICANN、GNSO 等机构的报告。我们的观点是，日本期待看到发布报告草案。当然，如果我们取得了一些进展，他们很乐意在闭会期间进行讨论。

最后，我要感谢上次会议为我们提供了关于合同谈判的最新情况。我们愿意继续讨论，也很高兴与大家进行讨论。非常感谢。

玛娜尔 • 伊斯梅尔： 非常感谢日本代表。非常感谢互联网和司法协会的贝特朗，以及 GAC 主题负责人加布里埃尔、克里斯和劳伦。谢谢大家。我们将在坎昆时间 15:00，世界协调时 20:00 再次在这里开会，召开与董事会的双边会议。请准时参会。谢谢。

[听写文稿结束]