ZH

ICANN83 | 社群论坛 – GAC 关于缓和 DNS 滥用问题的讨论
2025 年 6 月 10 日（星期二） – 09:00 至 10:15（中欧夏令时间）

茱莉亚 • 莎弗琳 (JULIA CHARVOLEN)	大家好，欢迎参加于世界协调时 6 月 10 日星期二 7:00 举行的 ICANN83 GAC 关于缓和 DNS 滥用问题的讨论会议。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，并以合理的语速发言，以便准确翻译。下面有请 GAC 主席尼科 • 卡瓦耶罗发言。谢谢，交给你了。
尼科 • 卡瓦耶罗 (NICO CABALLERO)	谢谢茱莉亚。欢迎大家，欢迎各位主题负责人和演讲嘉宾：来自捷克共和国计算机安全事件响应团队 (CSIRT) 的马丁 • 昆肯、来自 Interisle 咨询集团的卡伦 • 露丝和格雷格 • 亚伦、来自 NetBeacon Institute 的格雷姆 • 本顿和苏珊 • 查默斯，当然，大家已经认识苏珊了，她是美国代表和公共安全工作组 (PSWG) 主

题负责人；还要欢迎欧盟委员会的亚诺什 • 蒂莱恩约斯科和来自日本的宫本友纪先生。

欢迎各位。我们将就缓解 DNS 滥用问题进行非常有趣的讨论，然后我们将进入问答环节，我希望是有趣而且大家积极参与的环节。话不多说，有请宫本友纪发言。现在请发言。请讲。

宫本友纪 (TOMONORI MIYAMOTO)

谢谢主席。大家早上好，在线参加会议的同事们下午好，晚上好。我是来自日本的宫本友纪，期待今天的讨论取得丰硕成果。以下是本次会议的议程安排。在我进行简短的介绍之后，我们将介绍 DNS 滥用情况和缓解措施的最新进展，主要侧重于网络钓鱼——来自主办国捷克的网络信息中心 (NIC) 代表将介绍网络钓鱼活动以及应对措施。

第二部分，我们将讨论后续步骤的政策制定流程 (PDP)。为了节省时间，我们会将讨论范围缩小至明年新通用顶级域 (gTLD) 的 PDP。请切换到下一张幻灯片。下面是 DNS 滥用讨论的一些背景情况。ICANN 合同——《注册管理机构协议》(RA) 和《注册服务机构认证协议》(RAA) 要求 gTLD 注册管理机构和注册服务机构在收到可采取行动的 DNS 滥用报告时采取缓解措施。

对滥用的理解和背景有多种多样，可能包括网络钓鱼、诈骗、版权侵犯，比如在我国日本，盗版漫画就是一个很严重的问题。但是，ICANN 合同中对 DNS 滥用的定义是有限的，即恶意软件、僵尸网络、网络钓鱼、网址嫁接和垃圾邮件。2024 年对

该合同的修订是缓解 DNS 滥用的第一步，我们将考虑采取进一步措施来应对 DNS 滥用挑战。

请切换到下一张幻灯片。感谢。有些人可能会熟悉这张图表，它介绍这一滥用问题的生态系统或者说现状。ICANN 或 ICANN 合同的限制范围是左侧的绿色方块，相当有限。为了有效地处理这个问题，我们需要考虑建立蓝色方块中的那些关系，如注册服务机构和分销商之间签订合同。

我们还可以在红色方块中的扩展社群之间寻求合作，如可信通知者项目。今天，我们将主要关注绿色方框中明年新通用顶级域下一轮可能出现的 PDP，但依然应该在整体合同框架下考虑。请切换到下一张幻灯片。在上一次西雅图 ICANN 会议上，我们审查了 DNA 服务缓解的情况和证据，包括恶意域名注册的推断分析 (INFERMAL) 报告。

上周，我们召开了 ICANN83 前的 GAC 网络研讨会，NetBeacon Institute 提出了关于 PDP 想法，签约方也分享了他们的观点并给出回应。此外，通用名称支持组织 (GNSO) DNA 滥用问题小组已于今年四月开始工作，也在该网络研讨会上并介绍了他们的时间安排和目标。与该 DNA 滥用小组的合作应是我们进一步发展方向。

在今天的讨论中，我们将讨论政策的制定。请切换到下一张幻灯片。这是简介部分的最后一张幻灯片。虽然不是百分之百准确，但我将有关 DNS 滥用的一些主题和讨论进行了可视化整理。可以看到右侧的双向箭头，在滥用报告和缓解期间采取的措施是反应性措施或滥用处理方式。正如我所说，这是 ICANN

合同中规定的义务，除了 ICANN 合规团队的出色监控工作外，我们还可以考虑报告透明度。

我们可以考虑采取缩短反应时间的措施，如实施可信通知者项目。除这些措施外，我们还可以采取主动措施，包括报告前的主动监测，以及左侧的圆圈或点表示的注册时的一些附加规则。

根据 INFERMAL 报告的结果，可以考虑限制批量 API 注册或用户信息验证的时间。请切换到下一张幻灯片。我们来看下一张幻灯片。首先，我们有请来自主办国捷克 NIC 的马丁发言。马丁，交给你了。

马丁 • 昆肯 (MARTIN KUNC) 感谢。我将分享我们在捷克选区的网络钓鱼案例。请切换到下一张幻灯片。简单介绍一下我们的项目，或许各位有所耳闻。其中最重要的项目，我认为可能是“路由侦测鸟”(Routing Demon Bird) 和注册表追踪项目。此外，各位可能也了解我们开展的高级 DNS 测量系统 ADAM、NodeDNS 服务器以及 TURRIS 路由器项目。

请切换到下一张幻灯片。我们是谁？CZ.NIC 是一家 .cz 域名管理机构，同时还运营着国家 CSIRT 或者说 CSIRT.cz，而我是其中的一名安全分析师。请切换到下一张幻灯片。故事要从 2022 年 6 月说起，当时我们看到了一个钓鱼网站，看似平平无奇，但出现在.cz 域名上就很不寻常。我们一直努力守护自己的域名，恰逢当时捷克推出了“住房补贴”政策。

这项政府补贴旨在帮助困境中的公民获得额外生活补助。请切换到下一张幻灯片。现在介绍下主要角色：劳动和社会事务部。虽然它的“戏份”不多，但各位需要认识它的标志。

请切换到下一张幻灯片。捷克有 BankID。我想这在其他国家并不常见，但在捷克共和国，各家银行联合推出了一种叫做 BankID 的东西，方便大家使用与银行相同的凭证访问政府网站。这样一来，坏人出现，公民就成了受害者。

请切换到下一张幻灯片。这种网络钓鱼很常见。人们收到短信，声称：这里有一些钱，只需点击这个看起来像政府网站的地址，你就会变得很有钱……不对，是你会得到很多钱。请切换到下一张幻灯片。这种渗透式的短信有许多。

请切换到下一张幻灯片。这张的内容，我知道很难理解具体的文字，主要是说：你只要点击这里，登录，你就能得到钱。请切换到下一张幻灯片。当你点击链接后，就会进入一个钓鱼网站，会要求你使用银行 ID 登录。我们有其他的 ID，可以使用其他类型的身份验证，但犯罪分子专门索要 BankID，因为他们有明确的方法可以滥用它。

有意思的是，这个操作只在所谓的工作日营业时段才能进行。捷克共和国就发生过一个涉及捷克邮政的案例，谎称他们弄丢了你的包裹之类的东西，并且要求你只能在营业时段访问网站。如果你了解捷克邮政的话，会知道他们有个网站不是 24/7 全天候运行，这种通知似乎很合理。但在刚刚那个案例中，这反而成了破绽。骗子之所以需要限制时间，是因为不法分子需

要实时盗用你的登录凭证，并且他们也能同时拦截你第二重验证因子发来的确认信息。

请切换到下一张幻灯片。这是一个网站的示例。当然，除了 URL 之外，看起来几乎差不多。请切换到下一张幻灯片。这是另一个。在这里选择银行，然而并不可以选择任何银行，他们会特别要求选择一些当时可用的银行。如果你能看到，在顶部 URL 栏，有一个数字，用户每点击一次这个数字都会增加。因此，我们可以估算出他们诈骗活动的成功率。

请切换到下一张幻灯片。这也是一个示例。请切换到下一张幻灯片。那么到了 2022 年，他们最初每月仅注册 11 个域名——这个数量在当时虽然异常，足够攻击者实施诈骗，但尚在可控范围。而到 2023 年 2 月，单月注册量猛增至 72 个，这给我们带来了巨大压力。所以我们做足准备，全力封堵。下一张。我们知道对手在不断改进，我们也希望自己提升应对能力。因此，我们从主动搜索开始，努力改进流程、学习并记录，不放过每一个小细节。

请切换到下一张幻灯片。关于主动搜索的方式，我们通过区域进行搜索，可以看到注册的域名。起初我们尝试了与网站相似的字符，但很可能因为他们在改变，有了新点子、新域名，所以这个方法并不那么有用。因此，我们最终选择了上周注册的域名，以此作为信息来源。请切换到下一张幻灯片。

我们据此建立了未来的网络钓鱼域名列表，并进行定期扫描，时间间隔大约是五分钟。每五分钟，我们都会对列表进行测试，没有遭遇过阻拦，IP 地址也从未被封锁——显然对方对我

们的扫描行为毫不在意。一旦发现钓鱼网站上线运行，我们的手机便会立即收到通知。即使是在非工作时间，我们也会非常迅速地采取行动，以最快的速度关停。

这项工作是与彼得 (Peter) 协作完成的，在此必须向他致谢。我们逐渐大幅缩短了关停响应时间。这一点至关重要，稍后各位在图表中将会看到具体数据。请切换到下一张幻灯片。我们记录了发现的问题，发现攻击模式很清晰：网站通常在域名注册数天后上线。因为他们需要先完成域名注册、配置 DNS 记录，并获取证书。

一切准备就绪后，他们会在该网站启用目录索引功能，并上传压缩包文件。在这一阶段，我们曾多次成功下载网站压缩包进行分析。这些样本时而相同，时而因攻击手法升级而有所差异。随后他们会解压文件，网站便正式上线。请切换到下一张幻灯片。

顺带一提，证书透明化至关重要。它不仅让我们发现了一个无需密码的管理面板子域名——通过该面板可查看所有信息，攻击者同样能看到所有已创建的会话。而且该机制目前帮助我们发现了非 .cz 后缀的域名，这类域名我们原先无法提前预知。请切换到下一张幻灯片。最终，我们将此视为一场胜利：在二月份疯狂注册 72 个域名后，三月份骤降，仅注册了 28 个域名。

此后，我们再也没有见过这样规模的攻击活动。当然，个别尝试依然存在：有人使用其他顶级域名或注册个别域名，但均未达到之前的规模。请切换到下一张幻灯片。这张图表理解起来可能稍显困难，但我会尽力解释。图中绿色部分代表未成功解

析的查询请求。通常这类数据会用红色表示，但这里我们用绿色，因为拦截这些钓鱼域名的访问正是我们乐见的成果。

黑色部分则代表已解析的请求。需要强调的是，这并非实际用户数量，因为我们无法得知单个解析器背后的用户规模，但至少提供了估算依据，让我们能评估自身防御成效及对抗进展。请切换到下一张幻灯片。与此前相比，这张图的数据显著优化。如各位所见，绿色柱状图在此占据绝对优势，我们视之为阶段性胜利，表明防御策略得当且成效持续提升。

请切换到下一张幻灯片。幕后机制方面：我们的规则体系包含第 17 条，授权我们对危害网络安全的可疑域名执行区外隔离。此时域名将被标记为区外状态，该状态可维持一个月，为我们留足时间通知域名持有者申诉澄清——这才是合规流程。

简言之，如果我们操作有误，此机制可以提供补救路径并推动流程优化。同时，我们会公开所有被拦截的域名。请切换到下一张幻灯片。我要说的就是这些。希望大家喜欢这部分内容，欢迎提问。

宫本友纪　谢谢你，马丁，谢谢你分享捷克的经验。现在进入问答环节。大家有什么问题吗？有请加布里埃尔。请讲。

加布里埃尔 • 安德鲁斯 (GABRIEL ANDREWS)　我是加布里埃尔 • 安德鲁斯。非常感谢你的介绍。我对这部分内容非常感兴趣，实际上，当你讲到你们识别出有可疑域名被注册时，我印象很深刻。不过我想你说的是，当时你们还没看

到钓鱼网站实际搭建起来，但你们已经开始监控这些域名，并设置了规则进行检查和警告。

如果我没理解错的话，你们非常主动。但我有些好奇，你们当时是否觉得需要等待，因为需要收集一定量的证据才能采取行动？不知你能否就这一点稍微详细说说？

马丁 • 昆肯　确实如此。当时我们确实在等待证据。这样万一我们封锁了域名，也会有凭据支撑，避免误伤某些正在进行的正当研究项目之类的，那就不好了。所以这种情况下，我们确实想再等等。而且我们的流程也是这么设定的：即使我们立案并记录了证据，在正式封锁的那一刻，该网站也必须仍然处于在线状态。

加布里埃尔 • 安德鲁斯　坦白说，我觉得这种程度的主动监控——甚至可以说闻所未闻。这种做法实在令人印象深刻，也非常有意思。据我所知，过去我在网络安全领域报告那些预计将被用于非法用途、但尚无确凿证据的域名时，就遇到过挑战——如何找到这个平衡点始终是个难题。

而你们能主动制定规则进行自我监控，在可疑域名完成注册或刚投入钓鱼使用的瞬间就采取行动，这真是太棒了！或许这正是值得我们借鉴的经验。谢谢。感谢。

马丁 • 昆肯 谢谢你的肯定。需要补充的是，这次是针对单一钓鱼活动的打击。正因如此，我们才能锁定关键环节，从而提前预判哪些域名将成为钓鱼网站。如果遇到新型钓鱼手法，我们目前还没有追踪线索的能力。感谢。

宫本友纪 有请阿什温。

阿什温 • 萨松科 • 萨斯特罗布罗托 (ASHWIN SASONGKO SASTROSUBROTO) 好的，谢谢。我是来自印度尼西亚的阿什温。感谢两位的发言。我想问的是，第一，在网站中启用域名系统安全扩展 (DNSSEC)（安全 DNS）以及获得 ISO/IEC 27001 认证，实际效果如何？

这些措施是否能有效遏制 DNS 滥用，还是作用有限？第二，请问来自 SEC .cz 的发言人，你们通常展示很多网络钓鱼等案例，这些网站通常使用捷克的国家顶级域名 .cz，还是更常用通用顶级域名，如 .com 之类？感谢。

马丁 • 昆肯 我可能没完全理解第一个问题，稍后请再重复一遍。不过关于第二个问题，这是专门针对 .cz 域名的，所以追踪起来相对容易。当然，我们也遇到过使用其他域名的案例，但规模相对较小。

阿什温 • 萨松科 • 萨斯特罗布罗托

第一个问题是，在 ICANN 网站，我们被敦促启用 DNSSEC。那么激活 DNSSEC 协议对于缓解 DNS 滥用究竟有多大效果？另外，印度尼西亚和许多国家一样，是国际标准化组织 (ISO) 和国际电工委员会 (IEC) 的成员。我们共同制定了 ISO/IEC 27001 标准——信息安全管理体系。我想了解你们的实践经验。这项 27001 认证在对抗 DNS 滥用方面实际效果如何？感谢。

马丁 • 昆肯

好的，对于 DNSSEC，它对防范网络钓鱼没有任何帮助。我认为它在这方面行不通。关于 ISO 标准，我得说我不是回答这个问题的人，因为这不属于我的工作重点。很抱歉。

宫本友纪

下一位是阿德伦克。抱歉我的发音不标准，请发言。

阿德伦克 • 阿德尼伊 (ADERONKE ADENIYI)

大家好。谢谢马丁。我要向马丁提问。正如前一位发言人所言，你的演讲非常精彩，对我而言也极具新意。我是来自尼日利亚的阿德伦克。我的问题是关于 BankID。

在尝试缓解 DNS 滥用时，你们是否考虑过与银行监管机构合作？因为在尼日利亚，我们有一个类似的系统叫做银行验证码，它是所有银行通用的数字服务平台基础。因此我想了解：你们是否曾与金融服务监管机构或 BankID 的颁发机构进行过协作？感谢。

马丁・昆肯 是的，从我们的角度来看，我们并未能成功与他们建立联系。但幸运的是，他们主动采取了行动，开始向用户通报这些钓鱼攻击企图，并通过银行官方应用推送通知。因此我认为，他们已经在尽力而为了。

宫本友纪 好的，谢谢大家。现在我们进入下一部分。有请来自 Interisle 的卡伦和格雷格介绍网络钓鱼的范围和分布。接下来的时间交给你了。

卡伦・露丝 (KAREN ROSE) 谢谢，大家好，早上好。我是卡伦・露丝，这位是格雷格・亚伦，我们来自 Interisle 咨询集团。格雷格和我二人在域名领域均有 25 年的工作经验，非常荣幸能与各位交流。过去五年间，Interisle 持续研究网络犯罪中各类互联网资源滥用问题。

本次会议特别要求我们聚焦与网络钓鱼相关的 DNS 滥用行为。更广泛的资源滥用分析，请查阅我们已发布的报告。鉴于时间有限，我们直接进入主题。请切换到下一张幻灯片。核心结论是网络钓鱼与 DNS 滥用正以惊人速度增长，这令人忧心。仅过去 12 个月内，全球就发现了超过 200 万次钓鱼攻击及 150 万个独立钓鱼域名。过去五年间，该数据的季度平均增幅高达 425%；

而这还远未反映全貌——大量攻击根本未被上报；其中 77% 的钓鱼域名是专门为实施网络攻击而注册的。网络钓鱼给社会造成巨额损失：每分钟产生的直接经济损失超过 18,000 美元。实

际影响同样被严重低估——尤其在全球范围内，大部分损失未被上报。由此可见，当前 DNS 反滥用措施整体收效甚微。

如果各位注意到图表中段出现的低谷，那是由于一家名为 Freenom 的域名注册公司被关停，该公司曾是钓鱼犯罪的重要温床。Freenum 的倒闭虽短暂遏制了犯罪势头，但如数据所示，钓鱼活动迅速反弹并再创新高。请切换到下一张幻灯片。网络钓鱼者在注册域名时，主要利用两点：价格低廉和注册便捷。

网络钓鱼者的理想价格区间是域名定价在 2 美元左右或更低。这个价位在新通用顶级域名中非常普遍，而钓鱼者正以不成比例的高比率利用这类域名。请看上方图表：新 gTLD 的市场总份额仅占 11%，由那块小的黄红色楔形区块表示。然而再看下方图表：过去一年中，新 gTLD 却占所有钓鱼域名的 51% 以上。

尽管如此，.com 和 .net 域名对网络钓鱼者依然颇具吸引力，占所有钓鱼域名的 32%。网络钓鱼者能低价获取 .com 和 .net 域名的一种途径，是利用某些注册服务机构提供的免费促销活动或主机捆绑套餐。网络钓鱼者还瞄准那些注册门槛低、数据审核少的顶级域名和注册服务机构，利用其简易的注册流程。关于批量注册的问题，我的同事格雷格稍后会详细说明。

网络钓鱼者还有其偏爱的供应商——那些既提供“低价”又非常“便捷”的注册服务机构和顶级域名。被滥用最严重的公司几乎每年都位列前五或前十名。今天时间有限，无法逐一分析这些排名，但大家可以在我们近期的报告中查阅详细信息。

请切换到下一张幻灯片。网络钓鱼者通常按特定模式批量注册域名，且这些模式往往非常明显且易于识别。今天我带来了真实网络攻击案例供各位参考。左侧展示的是常见手法之一：算法生成的域名——通常围绕特定主题进行变体组合，甚至使用完全随机的字符串。

右侧则是模仿知名品牌的域名，目的在于欺骗不知情的消费者。网络钓鱼者还倾向于重复使用相同的注册信息，甚至直接填写明显伪造的虚假资料。然而，我们可以部署自动化工具来筛查此类恶意注册模式。目前已有部分国家和地区顶级域 (ccTLD) 部署了专门的 DNS 筛查系统，同时也有商用工具（如地址验证系统）可供使用。请切换到下一张幻灯片。

格雷格・亚伦 (GREG AARON) 我们每年都会研究这些域名的注册方式。当网络钓鱼者和其他犯罪分子注册域名时，通常不会一次只注册一两个，而是批量注册一整套域名。正如卡伦所说，他们通常遵循某种模式，因此这些注册行为往往非常显眼。只要你观察在特定注册服务机构那里连续注册的域名组，就能发现这些迹象。

至少有 37% 的钓鱼域名是以批量形式注册的。而我们的统计方法实际上低估了这一比例。我们发现哪些域名被用于钓鱼攻击，并确认它们相互关联。但在这些批量注册组中，还存在其他我们尚未发现和捕获的域名，因为有时收集数据非常困难。某些批量注册的规模极其庞大。去年我们就发现了一个案例，单名犯罪者就使用了超过 17,000 个域名。

关键在于，如今的网络钓鱼者行动极其迅速。钓鱼网站一旦上线，受害行为主要集中在前 8 小时内发生。因此，网络钓鱼者预见到自己会被发现，他们的域名可能会在某个时刻被暂停。但他们早已准备好备用的域名。我们观察到被滥用的域名越来越多，自动化批量注册正是原因之一。

他们准备好快速消耗大量域名以维持攻击活动。只要有利可图且网站能维持一小段时间，他们就会持续作案。网络钓鱼如此泛滥，恰恰证明这个方法是有效的。因此，我们必须思考：为何这种现象持续发生？为何形成了这种源源不断的域名消耗循环？请切换到下一张幻灯片。

卡伦 • 露丝

因此，DNS 滥用的根源在于一系列选择。这包括 ICANN 在塑造市场运作方式的政策和商业标准上所做的选择，以及企业在经营过程中所做的选择。我们常听到一种论调：竞争是好事，那么增加更多竞争必然更好，对吧？但从经济学角度看，事实并非总是如此。

如果没有合理的规则，过度竞争会带来负面影响。DNS 滥用及其助长的网络犯罪，如同行业的污染源。它是一种经济负外部性，会将成本强加给消费者和社会。如今，DNS 市场竞争相当激烈。现在有超过 2,000 家注册服务机构、数百个开放的通用顶级域名。域名几乎相当于大宗商品，基本可以互换，且行业几乎能以零边际成本生产。

因此，在缺乏有效反滥用政策的情况下，犯罪分子如今正极其轻易地利用这些市场动态和选择。我们认为，现在真正需要的

是合理主动的措施，才可以在域名滥用发生之前就加以遏制，而不仅仅是在损害已经造成之后才做出补救（尽管更高效的补救措施永远是有用的）。

现在采取行动并实施相关政策至关重要。因为随着新 gTLD 下一轮次项目的开展，一批新 gTLD 将进入市场，这将进一步压低域名价格，并加剧市场竞争压力。如果无所作为，图表上的曲线将持续向右上方攀升。请切换到下一张幻灯片。

格雷格 • 亚伦

我们观察到的一个趋势，尤其在欧洲，是注册管理运行机构正在采取新举措。例如，部分机构不再要求所有注册人预先提供身份证明，而是采用风险分级管控。我们看到多家注册管理运行机构表示，批量注册本身就是高风险行为。

当出现注册人身份不明却大批量注册域名的情况时，他们可能会要求其进行身份核验，并在确认身份可信度之前，暂停这些域名的解析功能。这正是目前部分欧洲顶级域名实施的风险管控模式。ICANN 现行的核验要求门槛极低。

事实上，ICANN 近期一项合规审查发现，20% 被抽查的注册服务机构甚至没有执行当前最基本的数据验证步骤。我们认为这正是一个机遇——通过推行风险分级核验与预防机制，增加犯罪分子的作案难度。

请切换到下一张幻灯片。我们计划实施的措施包括强化身份核验要求以及整治批量注册问题。而且这两件事可以同时进行。另一个值得关注的现状是 ICANN 合同规定，注册管理运行机构

必须与所有 ICANN 认证注册服务机构开展合作。这种规定的背后是有原因的：它旨在防止企业相互排挤，确保公平竞争的市场环境。

然而问题在于，注册管理机构仍被迫与大量引入违规业务的注册服务机构合作。我们建议对这种情况进行研究，因为它常使注册管理机构陷入被动局面，劣质注册人的涌入还会损害其声誉。这方面或许存在改进空间。

当然，注册管理机构和注册服务机构并非束手无策。部分机构正试点新系统，尝试在域名遭到滥用之前就进行筛查，相关解决方案也于本周开始讨论。因此，我们想告诉大家的是，现在已有技术工具与解决方案，还有配套政策，局面有望改善。请切换到下一张幻灯片。

卡伦 • 露丝

今年第三季度，我们将发布一些新的数据报告，敬请期待。关于我们的报告，我们不仅会分析域名数据，更涵盖托管滥用、子域名滥用等维度。部分研究还涉及网络钓鱼、垃圾邮件及恶意软件。我们邀请大家访问我们的网站查阅报告详情。

我们的数据来源、研究方法及补充数据集均公布在“网络犯罪信息中心”(Cybercrime Information Center) 网站上——这是 Interisle 旗下的项目平台。该平台提供海量数据及详尽排名，欢迎访问。我们还会在 Substack 上每周更新分析博文。大家可以前往网站查看，期待与各位通过电子邮件交流。非常感谢。

宫本友纪 谢谢卡伦和格雷格的介绍。由于时间关系，让我们进入下一部分内容。如果有任何问题，请稍后提问。接下来交给亚诺什。请讲。

亚诺什 • 蒂莱恩约斯科 (JANOS DRIENYOVSZKI) 谢谢宫本。下面我们讨论关于政策制定和可能的小型政策制定流程的后续步骤，以解决已经讨论过的问题。下面请来自 NetBeacon 的格雷姆发言。

格雷姆 • 本顿 (GRAEME BUNTON) 感谢。大家上午好！我是格雷姆 • 本顿，是 NetBeacon Institute 的执行董事。NetBeacon Institute 隶属于公共利益注册管理机构 (PIR)。PIR 负责运营 .org 顶级域，旨在践行其非营利性公益使命。就在约两周前，我们发布了一份白皮书，提出了五项潜在的 PDP 构想，希望与社群分享。

由于时间有限，我不会深入探讨这些 PDP 构想的细节。稍后我会提供完整的、长达 22 页的白皮书链接，相信各位会去阅读。接下来我对其中的内容进行概括介绍。请切换到下一张幻灯片。简要说明一下我们开展这项工作的原因。NetBeacon Institute 的日常工作就是思考如何减少 DNS 滥用。同时，作为签约方的一员，我们拥有相对独特的视角。

我们的工作与 InterIsle 在许多方面颇为相似：我们运营着一个名为 NetBeacon Map 的项目，旨在测量和了解整个生态系统中的 DNS 滥用问题。我们还运营着一个名为 NetBeacon Reporter 的集中式滥用报告服务项目，用于分析数以万计的滥用域名。

基于这些数据与观察，我们希望……慢下来？好的，抱歉，我说得太快了。

我们在探索能否通过支持社群协商，提出一些我们认为能够及时实现、对缓解 DNS 滥用问题具有渐进式影响力的构想，并向社群具体展示何为“范围精准限定的 PDP”。请切换到下一张幻灯片。我不准备谈论过多的细节。简而言之，第一是关联域名检查，该措施将要求注册服务机构以滥用报告为线索展开行动。

注册服务机构在收到一份证据充分、可执行的恶意域名滥用报告时，就有义务核查是否存在与该域名关联的其他域名，并在发现滥用证据时采取行动。请切换到下一张幻灯片。API 访问限制；ICANN 的非正式报告——在此特别感谢 ICANN 首席技术官办公室 (OCTO) 团队——指出一个关键发现：开放无限制 API 的注册服务机构，

其域名滥用率高出 401%。那么我们能做些什么呢？如何在注册人访问此类支持大规模批量注册的工具前设置必要门槛？请切换到下一张幻灯片。子域名滥用联系人。这项提案探讨能否将注册服务机构层面的 DNS 滥用责任义务应用于向第三方提供子域的注册人。

请切换到下一张幻灯片。注册人救助机制。在注册管理机构和注册服务机构努力大规模打击 DNS 滥用的背景下，失误在所难免。我们需要确保那些因滥用缓解措施而遭受错误影响的注册人，需要有明确的纠错渠道。请切换到下一张幻灯片。僵尸网络与域名生成算法 (DGA) 协同打击。目前，要打击僵尸网络和

域名生成算法，执法机构通常需要逐一联络各家注册管理机构，效率低下。

因此，我们提议在 ICANN 内部设立一个集中协调职能，负责收集并分发相关信息，从而更高效地协同打击僵尸网络。请切换到下一张幻灯片。我可以就这五项潜在的 PDP 构想逐一详细介绍，大家如果想与我交流，欢迎稍后在会场外找我详谈。

但此刻，我想向在座各位强调几个关键要点：目前正是社群推进 PDP 良机，可以通过政策制定来缓解 DNS 滥用。我们必须承诺，确保流程范围精准限定、聚焦具体议题。没有人能得到自己想要的一切。进展需要专注力。及时取得进展更需要高度聚焦。这些议题本身极其复杂，一旦社群决定采纳相关构想，具体实施起来必将面临重重挑战。

虽然会对运营产生实际影响，会有实际问题需要解决，但我们能够取得一些进展。我们可以实现一些虽小却及时见效的渐进式成果，这总比毫无进展要好。我认为解决问题的规模与所需投入的精力密切相关。我们真正希望看到的是，整个社群能够循序渐进地采取行动，最终实现目标，从而及时改变 DNS 滥用的现状。

最后我想重点强调，基于之前 Interisle 关于发现的 DNS 滥用模式的观点，从宏观层面看，我们必须实现从处理单一滥用报告到规模化解决 DNS 滥用的转变。虽然去年实施的合同修订条款有效，数据也持续显示注册管理机构和注册服务机构关停了大量恶意域名，但目前义务仅存在于个体滥用报告层面。

因此，我们提出的前两项方案——关联域名检查与 API 访问限制——正是为了探索能否以合理且负责任的方式，将治理重心从单一报告转向规模化处置恶意攻击活动。即便具体方案尚不完美，但这个思路代表着社群未来应对 DNS 滥用的方向。从我们的视角看，发布白皮书的目标已达成。

当前社群讨论的方案都经过严谨论证，有望取得成功。即便最终方案另有选择，其框架设计也是正确合理的。这正是我们期待在社群中持续看到的良性互动。我们希望社群围绕类似构想开展讨论并最终落实。感谢今天给我发言的机会。非常感谢。

尼科 • 卡瓦耶罗

非常感谢格雷姆的发言。在交给宫本主持之前，我想恳请尊敬的 GAC 代表们关注采取迅速行动的必要性，因为不法分子此刻正密切关注着我们的动向。如果我们耗费五年制定 PDP，届时他们早已领先我们两三步了。依我看，我们必须快速采取行动。交给你了，宫本。

亚诺什 • 蒂莱恩约斯科

谢谢尼科。接下来我们将阐述 GAC 在限定范围内的 PDP 中应聚焦的方向。在开始演示前，请允许我简要梳理签约方机构在昨天会议上提出的四项方案——这对今天的讨论具有参考价值：

一，建立恶意注册域名可执行报告机制，通过该机制可同步关停同一注册账户下的其他恶意域名；二，修订合同条款，要求提供 API 或分销商计划的注册服务机构具备合同约束力，确保其分销商履行 DNS 滥用缓解义务；

三，构建运营框架，为所有 gTLD 注册管理运行机构提供经验证的僵尸网络域名清单；四，制定网络钓鱼攻击举报最佳实践指南，提升举报质量。关于 GAC 应重点关注的议题或者说需要后续讨论的构想，今天讨论已多次提及主动防御措施及批量注册管控问题。

我们正处于探索主动防御与被动响应措施的关键阶段。但正如尼科所说，如果我们的核心目标——尤其是在新一轮 gTLD 之前——是快速取得实质性成果，就必须对特定行动进行优先级排序。这与格雷姆提出的精准化 PDP 的想法相同。

在《西雅图公报》中，GAC 尤为重视 INFERMAL 报告中指出的域名批量注册主题，这是造成 DNS 滥用的高度相关的因素，建议进一步研究讨论。今天上午的数据已清晰表明：批量注册域名不仅更容易导致 DNS 滥用，其危害程度也远远大于单一恶意域名。

INFERMAL 研究进一步证实，严格的注册政策与主动验证机制能有效缓解 DNS 滥用。因此，在批量注册流程中增设管控环节势在必行。我们认为，可行的方案之一是要求签约方实施针对批量注册的主动防御措施。

这可以包括限制批量 API 注册，例如，通过将 API 访问权限限制在已知或经过审查的用户中来实现，审查依据可以是身份验证、注册人活动或声誉，正如格雷姆在发言中提出的那样。我们相信这个想法是短期内最有可能达成共识的方案之一。此外，还可以采取其他措施，例如对批量注册的域名收取更高费用、延迟注册或限制注册数量等。

这些主动措施将补充签约方机构提案中提出的应对措施或缓解措施，该提案旨在处理可采取应对行动的报告，以及 NetBeacon 提案，该提案建议检查关联域名并在确认恶意注册后采取适当行动。这样，我们就能在批量注册方面实现主动措施与应对措施的结合。

现在谈谈其他可能的主动措施和其他缓解措施。在《汉堡公报》中，GAC 重申了主动监控的重要性；在《西雅图公报》中，也提到了解决 DNS 滥用的主动实践，以及解决 DNS 滥用与域名注册数据工作之间的联系。GAC 还鼓励注册服务机构探索使用人工智能驱动的 DNS 滥用检测系统。

关于这方面，注册行为监测可能是另一个值得探索的领域。这意味着识别出恶意注册的特征指标，这些指标将触发签约方在注册时或注册后不久采取行动。这项措施符合 2022 年 10 月发布的 DNS 滥用小组向 GNSO 理事会提交的报告中的建议一。这意味着所有呈现一定恶意注册风险等级的注册都应进行身份验证。

此处，我们可以借鉴欧洲 ccTLD 领域的主动实践案例，他们采用了人工智能驱动的 DNS 滥用检测系统。另一项措施可以是在域名生命周期内进行定期验证，这意味着在域名续期或转让时进行检查。我就说这些，接下来有请苏珊发言。

苏珊 • 查默斯 (SUSAN CHALMERS)

感谢亚诺什。我来简要谈谈 GAC 主题联合负责人讨论过的第三个 PDP 想法，即报告义务。健全的政策需要基于证据来制定，GAC 在参与 DNS 滥用政策制定时也需要考虑相关的证据。

ICANN 提供了来自测量平台的信息，例如 ICANN 自身的平台“域名衡量”(Domain Metrica) 以及 NetBeacon Institute 提供的测量数据。

我们还可以参考来自 Interisle 等公司的网络犯罪研究报告（我们今天也听到了这种报告），以及在 ICANN82 西雅图会议期间被广泛讨论的 INFERMAL 报告，这些也都是相关证据。ICANN 合规部门每月都会发布关于 DNS 滥用的报告，这些都是能够支撑健全政策制定的有力证据。通过这些合规报告，我们也能很好地了解签约方是如何落实 2024 年 DNS 滥用相关义务的。

但我们掌握的情况并不全面。目前并没有要求签约方自行公开报告其在缓解 DNS 滥用方面的活动或其对修订条款的落实情况。因此，一个想法是，可以专注于要求签约方提交滥用数据统计报告。这只是在昨天和今天我们所听到的一系列想法基础上，补充的另一个建议。

请切换到下一张幻灯片。那么，这些是 ICANN 政策行动的后续步骤和途径。如果各位参加了我们在 ICANN83 会议前举办的网络研讨会，应该听到了 GNSO DNS 滥用小组的发言。该小组正在开展工作。他们的任务本质上是评估目前 DNS 滥用缓解工作的成效，并确定是否需要进一步的政策工作。调查结果草案和建议将于今年 9 月提交，最终报告将于 10 月提交。

目前我们了解到，这个时间表有可能缩短，但我今天当然不能代表 DNS 滥用小组发言。我只是希望 GAC 代表们了解，这项工作正在 GNSO 层面推进。我们今天将举行与董事会的会议，如果可以的话，请支持员工翻到我们向董事会提出的问题那一

页。我们将就此与董事会进行讨论。我认为，如果询问 ICANN 的任何一位成员、任何一位同事，大家十有八九会同意缩短 PDP 时间。有些 PDP 需要耗时数年。

我们向董事会提出的问题是——虽然这不特定于 DNS 滥用问题——我们如何能推动改革 PDP 流程，以便我们能更快地看到成果？不是十年，不是五年，也不是三年，而是 12 个月或更短时间？因此，我鼓励 GAC 代表们今天下午关注这个问题。谢谢大家。

如果可以的话，请翻回上一张。现在，许多 GAC 代表都了解应该如何参与并帮助推动 ICANN 的政策变革。对于新加入的代表，我想非常简要地概述一下这些途径。第一条途径是政策制定流程——这正是我们今天主要讨论的内容。ICANN 的多利益相关方政策制定流程需要 ICANN 社群各利益相关方的广泛参与，其中就包括 GAC 代表。

PDP 最终产生共识性政策。共识性政策将成为合同的一部分，因此对各方具有约束力。ICANN 政策变革的下一条途径是合同修订。政策可以通过修订 ICANN 与注册管理机构之间、以及 ICANN 与注册服务机构之间的合同来确立。然而，与多利益相关方政策制定流程不同的是，修订条款主要通过双方磋商达成。

因此，我们就有了一套具有里程碑意义的 2024 年 DNS 滥用修订条款得以实施。我记得这些条款是在去年 4 月 5 日生效的。这些条款为 ICANN 注册管理机构和注册服务机构确立了基础性义务，但它们主要是双边磋商的成果。虽然对拟议修订条款开展

过公共评议，但与 PDP 不同的是，非 ICANN 和非签约方的利益相关方并不直接参与公共评议程序。

对于 GAC 代表而言，当然，我们的主要工具是 GAC 建议，即我们能够形成共识性建议并向 ICANN 董事会提交。经过充分考量与协调的 GAC 建议，是 GAC 在推动 ICANN 政策变革方面最有力的工具。我就简短概述以上内容，特别是给新加入的 GAC 代表们介绍一下。请切换到下一张幻灯片。我想我们还剩下 15 分钟。好的，很好。我们希望节省出时间供 GAC 代表们进行讨论。

按照惯例，主席在 ICANN83 会议前发出了议题征集通知。GAC DNS 滥用主题联合负责人议题在会前向 GAC 电子邮件清单提供了一些文本。在此，我只重点标出了我们提供的要点。关于重要问题，我们可以在会议期间，特别是本次会议上，讨论与 DNS 滥用相关的事项。

我们建议重点审视 DNS 滥用现状及缓解措施相关的 PDP 主题和后续步骤。我们还建议鼓励开展目标明确、范围精准的 PDP，以便在更快的时间内达成共识性成果。因此，我们希望 GAC 代表们注意，请将这些要点提供给你们的同事，并就此进行讨论。

尼科 • 卡瓦耶罗　非常感谢美国代表。如果可以的话，请翻回到第 12 张幻灯片，也就是最后一张。对，就是这张。不对…这张。那么，关于政策制定，在我请印度尼西亚代表发言之前（抱歉让您久等了）——哦，是阿什温之前举的手吗？是吗？你举手了。在请你发

言以及大家提问或发表意见之前，有一件非常重要的事情需要考虑，那就是 GAC 成员参与政策制定流程的事情。

我们希望确保各位感到自在，并有机会以有意义的方式参与。关键点在于……如果你没有机会畅所欲言，说出你想表达的意见，那么参与 PDP 流程的意义何在？只是举个例子——我并非说这种情况正在发生，只是假设——如果会议过程不够高效，你的想法无法传达，或者可能你在 PDP 中遇到了问题，而发言机会却给了别人。

我的想法，正如我一开始所说，就是要确保各位在参与这些 PDP 时感到自在。当然，我完全同意美国代表刚才提到的观点，即我们需要更短、更快、且高效得多的 PDP。从政府的角度来看，我们不能花费两年、三年、四年，甚至我认为不能超过一年，这没什么意义。我不需要解释政府的运作周期，

有些国家的总统任期是四年。通常，信息和通信技术 (ICT) 部长或外交部长的任期是两年、三年或一年。当然，这取决于不同国家的规定，但大家明白我的意思，对吧？那么，再次抱歉让你久等，印度尼西亚代表，请发言。

阿什温 • 萨松科 • 萨斯特罗布罗托

很抱歉。谢谢尼科。实际上，我的问题和我上次问捷克同事的问题相同，是关于 ISO/IEC 27001 标准的——它对于防止 DNS 滥用是否足够有效？或者你在这方面有什么经验？我提出这个问题的原因是：第一，DNS 滥用是印度尼西亚面临的一个巨大问题，如今已经非常严重了。

其次，印度尼西亚以及其它国家和地区当然也是 ISO/IEC 的成员。第三，ISO/IEC 设有第一联合技术委员会负责 ICT，其下的第 27 分技术委员会专门负责网络安全。因此，我的提议是：如果 27000 标准不足以应对 DNS 滥用问题，那么我们必须告诉 ISO/IEC 组织，我们将在明年 9 月召开大会，并询问：“你们为什么不审查 27000 标准呢？”

因为在该组织内也有所谓的“PDP DECO”政策制定流程。其中一项政策制定内容就是利用 27000 认证体系来保护我们的系统。那么，如果根据 ICANN 的工作经验，这套标准还不够，我们就应该告诉他们并推动审查，或者与他们进行讨论。甚至，尼科，你甚至可以直接给 IEC 发封信函。当然，这没有问题。感谢。

尼科 • 卡瓦耶罗 谢谢印度尼西亚代表。我清楚你的想法了。接下来有请印度代表发言。

苏希尔 • 帕尔 (SUSHIL PAL) 谢谢主席，也感谢各位小组成员，特别是 Interisle 和 NetBeacon 提供的这份内容翔实的报告。我们非常乐意接受并且全力支持这种时间更短、范围更精准的 PDP。不过，我仍然认为我们更多地是在关注表象而非根源。我们关注的是批量生成、成本低廉、访问便捷与恶意域名使用之间的关联性。但据我理解，这些仅仅是表象，而非根源所在。

我认为根源实际上在于 WHOIS 数据准确性以及身份识别。我想就此回应一下专家组成员，因为我只是从我们现实世界中做个类比。我认为我们生活在现实世界中，但我们都清楚地知道住在附近的邻居都是谁，对吧？我仍然认为，这些恶意域名的出现，仅仅是因为匿名的存在。

恶意域名注册人缺乏问责制，这实际上给了他们肆无忌惮地在任何时候逃脱的机会。我们能做的仅仅是关停那个域名，除此之外别无他法，对吗？因此，从这个类比来看，我不认为将成本从 2 美元提高到 10 美元或 20 美元就能真正减少恶意域名的数量，因为其收益巨大——正如我们所见，每分钟的收益就有大约 18,000 美元。

所以，在我们看来，有必要引入问责制，这不仅针对注册服务机构，也应针对注册人本人。虽然这会给注册服务机构和注册人双方都带来额外成本，但我认为我们应当寻求这样的解决方案。感谢。

尼科 • 卡瓦耶罗 谢谢印度代表。我们现在还有 7 分钟时间，而发言名单上还有一、二、三、四、五、六、七——七位发言人。因此，我恳请各位发言简洁扼要、直奔主题。苏珊，你还有什么要说的吗？没有？那么有请..... 很好。接下来有请欧盟委员会代表发言。请发言。

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。感谢组织本次信息丰富会议的 GAC 同事们，也感谢各位嘉宾发言人的分享。我想就公报审议事项及可能的后续行动路径所提出的问题进行回应。从我们的角度来看，看到当前这股势头确实令人欣喜。

在合同修订之后，社群的许多部分似乎都对推进 DNS 滥用缓解工作表现出兴趣，我们对此给予了非常积极的评价。我们看到了来自签约方机构的倡议，例如刚刚听到的 NetBeacon 的项目，以及 Interisle 的研究，非常好的发展势头。

因此，我认为我们必须把握住，并与其他社群成员协作。鉴于 GAC 的优先事项一直是在新轮次之前确认一些新措施，我们也应秉持务实态度，努力在既定时间框架内确定可实现的措施。这意味着需要确定优先事项，但并非忘记全局，而是着力于优先事项。

从这个角度看，我们认为重要的是考虑就目标明确、范围精准的 PDP 提出建议的可能性。但同时，我们也建议 GAC 在审议时，应明确这些优先主题。今天，我们听到了结合某些主动措施的可能性，例如监控注册数据的行为模式和批量注册。

我们看到提出了几项值得探讨的提案，此外，我们认为考虑透明度义务也很重要。这一点在早前关于 DNS 滥用合同修订的公开意见征询阶段，就是 GAC 立场的一部分了。感谢。

尼科 • 卡瓦耶罗 非常谢谢欧盟委员会代表的发言。我完全同意这一点。提醒一下，我们将举行六次公报起草会议，因此我们将有足够的时间来讨论。请加拿大、荷兰、瑞士和丹麦发言。有请，加拿大代表。

伊恩 • 谢尔登 (IAN SHELDON) 谢谢尼科。感谢所有的演讲嘉宾，这次会议真的非常、非常有趣。我的发言会很简短，因为 Zoom 会议室里有很多人在排队。再次感谢大家，特别是格雷姆，感谢你带来的 NetBeacon 报告。我非常认同你关于“不要因追求完美而阻碍进步”的观点，我们也看到了其中的发展。

我认为，考虑采用范围精准、目标明确的 PDP 来获得及时成果至关重要。因此，我敦促 GAC 成员们阅读 NetBeacon 报告。这份报告撰写得非常好，内容是关于政策讨论的，技术性并不强，并且包含了许多非常好的建议。再次表示万分感谢，我们当然期待未来在 GAC 内部就如何推进这些 PDP 进行探讨。谢谢。

尼科 • 卡瓦耶罗 谢谢加拿大代表。有请荷兰代表。

马尔科 • 霍格沃宁 (MARCO HOGEWONING) 感谢。我是荷兰代表马尔科。首先和其他发言人一样，感谢各位组织了这场内容翔实的会议。我认为，正如我的加拿大同事刚才所说，我们必须认识到“完美是够好的敌人”。

并且，正如欧盟同事所说，我认为现在是时候开始缩小选项范围了。我希望在接下来的时间里，提醒我们所有人，与 GNSO 和董事会一起，在下次会议召开前的这段时间内，切实就一两个主题达成共识，并推进相关工作。感谢。

尼科 • 卡瓦耶罗 谢谢荷兰代表。有请瑞士代表。

乔治 • 坎西奥 (JORGE CANCIO) 谢谢尼科。我是来自瑞士的乔治 • 坎西奥。是的，我也同意前面几位发言者的观点，我认为重要的是要看我们与 GNSO 和董事会讨论的内容，以及讨论的方向。但我确实认为这个目标明确、范围精准的 PDP 的想法很有潜力。另外，或许需要对苏珊乐观的评估做一点微小的修正。据我所知，还从未有过耗时少于一年的 PDP，不过如有错误，欢迎指正。感谢。

尼科 • 卡瓦耶罗 非常感谢，但愿我们能改变这种状况。谢谢瑞士代表。下面有请丹麦代表。

芬恩 • 彼得森 (FINN PETERSEN) 谢谢主席。我叫芬恩 • 彼得森，来自丹麦。感谢各位的发言，非常感谢。我们确实同意应推进范围精准的 PDP，并且我们希望能在下一轮次启动前看到它们。因此，这需要相当早地进行。我们尤其关注的是主动措施，我认为批量注册就是其中之一。

我们还希望看到对身份要求或联系数据等的核查比现在更加严格。这就是我们将关注的重点。当然，还有其他方面，例如透明度，但如果我们要确定优先事项并在下一轮次之前有所进展，那么在我们看来，重点应放在主动措施上。

而且，这仅仅是通往理想情况的又一步，或者说我不知道我们最终会走向何方。有一个问题想问 Interisle：关于批量注册，在你们的研究和考量中，是否定义了何为“批量”？界限应该设在哪里？是否应为连续五次注册？感谢。

格雷姆 • 本顿

非常快速地回应一下。我是 NetBeacon Institute 的格雷姆。关于批量注册问题，我认为，试图为单次可购买的域名数量设定一个具体上限，很快会遇到问题。恶意行为者会立即将注册量控制在限额以下并实现自动化操作。这种做法还会以意想不到的方式影响市场——例如在搜索结果中显示域名时，用户通常会一次添加一两个到购物车，而此类数量限制会影响搜索结果中可显示的域名数量。这样实际上是在干扰市场运作。

因此，我认为这种方法是存在风险的。在思考如何解决批量注册问题时，尤其是 INFERMAL 报告中提出的问题，我们考虑了两点。第一，由于正是 API 支持着大规模注册，我们需要限制 API 的访问权限，在工具访问环节设置障碍，而不是具体规定工具的使用方式，这将是更有效的解决途径

第二点是，围绕关联域名检查采取措施，检查关联域名可以破坏恶意活动。这是一个很好的应对手段。但如果注册服务机构有义务去检查客户账户中的所有域名，可能涉及 10、20、30 甚

至 100 个域名，这实际上相当于对注册服务机构征税，因为执行检查会耗费他们的成本。

这将激励注册服务机构更谨慎地选择允许谁进行大批量域名注册，因为他们现在有义务审查所有这些域名。我们希望——这也是我们将其写入报告的原因——这一措施将在行业内产生实质影响，它能鼓励并激励我们期望的正确行为，从而解决批量注册问题。感谢。

尼科 • 卡瓦耶罗　非常感谢。我们需要做个总结。考虑到如今的国际形势，我们能在这方面达成广泛共识，对所有人来说都是一件幸事。我要告诉大家，如今并不流行达成共识。我看到大家对这个公报审议问题的方法和重要问题下的三个主题达成了广泛共识，我不再全部读一遍了，也不提什么建议了。最后，苏珊，你是 PSWG 的主题负责人，在这方面你有什么要补充的吗？

苏珊 • 查默斯　好的，谢谢主席。我的发言会非常简短。从美国的角度来看，PDP 的时限必须大幅缩短，以便在 DNS 因新 gTLD 下一轮申请而扩展之前取得政策上的成果。最后，我要为更广泛的 ICANN 社群发言。我们已经听取了 NetBeacon 的建议，签约方机构也提出了建议。

商业利益相关方团体也有一些想法。一般会员咨询委员会 (ALAC) 对域名系统滥用问题有一些构想和政策优先事项。非商业利益相关方团体致力于提供建设性意见和政策建议，已针对

DNS 滥用政策提出了优先考虑事项。我们可以看到很好的发展趋势，我们正朝着一个共同的方向前进，ICANN 的多利益相关方社群应共同努力，针对 DNS 滥用问题取得成果。现在是 ICANN 取得政策成果的重要时刻。非常感谢。

尼科 • 卡瓦耶罗 非常感谢美国代表。我们的时间只够到此为止。最后几句话..... 很抱歉会议超时了，我们现在有 30 分钟的茶歇时间。之后，我们将分别与 GNSO 和 ALAC 举行会议，每场 45 分钟，随后是午餐时间。非常感谢各位。尽情享受茶歇时间吧。

[听写文稿结束]