蒙特利尔 – GAC：DNS 滥用问题缓解
2019 年 11 月 5 日（星期二）- 10:30 - 12:00（美国东部夏令时间）
ICANN66 | 加拿大，蒙特利尔

玛娜尔 • 伊斯梅尔（MANAL ISMAIL，GAC 主席）：欢迎大家回来开会。请大家就座。现在开始举行 DNS 滥用问题缓解讨论，我们的进度略微落后于计划时间。请大家就座，我将不胜感激。我们有幸请到公共安全工作组成员出席本次会议，他们将负责主持本次 DNS 滥用问题缓解讨论。我应该将话筒交给谁呢？劳伦 (Laureen)，交给你吗？

劳伦 • 卡宾 (LAUREEN KAPIN)：实际上，主要由我的同事们负责演示，特别是美国联邦调查局的同事。另外，希望大家在发言之前先进行自我介绍，同时还要再发布一条特殊声明，我曾多次指出，有些同事刚刚开始接触这一领域而且新加入工作组，难以应对大量复杂问题。除非拥有术语表密码，否则首字母缩略词没有任何意义。我想特别感谢我的同事加布里埃 (Gabe)，他率先投入这项工作，而且在很短的时间内取得了令人赞叹不已的巨大贡献。我想向诸位重点强调这一点。

加布里埃 • 安德鲁斯 (GABRIEL ANDREWS)：下面开始介绍。我是加布里埃。刚刚说过，我在美国联邦调查局工作。专门负责办理网络犯罪案件，包括计算机入侵犯罪。这是我的工作职责，从左面开始，请各位同事依次自我介绍。

克里斯 • 刘易斯 • 埃文斯 (CHRIS LEWIS--EVANS)：谢谢，我是克里斯。来自英国国家打击犯罪局，同时负责处理国际打击犯罪机构下辖的国家网络犯罪部门的相关工作。

格雷格 • 穆尼耶 (GREGORY MOUNIER)：上午好，我是格雷格 • 穆尼耶，来自欧洲刑警组织和网络犯罪部门。

加布里埃 • 安德鲁斯：谢谢大家。下面开始开会。值得注意的是，整体网络犯罪和 DNS 滥用及二者之间的关联，哪怕不是最重要的问题，也是公共安全工作组关注的主要问题之一。这项威胁始终存在而且日益加剧，必须彻底予以解决。最近，WHOIS 基础设施做出调整，特别是 WHOIS 基础设施访问结构有所转变，大部分网络犯罪调查机构日常办公都要用到这款工具，因而局势更是雪上加霜。不只是像我一样的执法机构官员，还包括私营部门的同事们，以及丰富调查内容、改善调查结果和帮助我们完成调查

的网络安全从业人员和研究人员。因此，自 GDPR 实施以来，缺乏最新 WHOIS 工具对我们开展调查及顺利推行工作的能力产生了切实的影响。目前，公共访问模型的前景还不明朗。没有人知道这种局面究竟会发展到怎样的地步。与此同时，还出台了“合理访问要求”，但本身并不能发挥任何作用。在不求助任何特定机构的情况下，我们发现，哪怕是执法机构，在请求获取过去公开的 WHOIS 信息时，响应率同样不够理想。我不打算透露实际数字，但在某些情况下，响应率不足 50%，哪怕执法机构自行提出相关请求也不例外。加之没有明确的转售链，也不具备清晰的注册人信息，甚至不一定了解究竟应该最先求助哪个机构处理这些请求，因而情况势必更加糟糕。我的意思是，我们以调查机构的身份出席 ICANN 会议，全球大多数调查机构可能并不了解 ICANN，也可能不熟悉新的处理模式，还是按照老办法，只不过进入某个网页，输入关注的域名并获得回复。因此，我们面临严峻的挑战。

请切换到下一张幻灯片。

劳伦 • 卡宾： 我想打断一下，补充一点。除调查网络犯罪的执法机构以外，消费者保护和隐私机构也会参与隐私侵权调查。用户信息被盗，继而遭到滥用，隐私权遭到侵犯，这属于刑事事件，但也是隐私保护的核心。

加布里埃 • 安德鲁斯： 很有道理。谢谢大家。请切换到下一张幻灯片。这里列出了 CCT 审核之前得出的一些建议，稍后将引用具体说明，但在此之前，我们必须从社群的角度对 DNS 滥用问题进行定义。我们发现，过去我们曾对这个问题进行了仔细定义。根据讨论结果，我们在 2013 年 GAC 北京会议建议中做出了相关定义，其中安全威胁是指租借、网络钓鱼、恶意软件和僵尸网络，我们发现现阶段仍面临非常严重的危害。虽然人们正常努力探索完美的 DNS 滥用定义，只不过完美也会成为优秀的敌人。人们面临持续伤害。现阶段滥用 DNS 基础设施的网络钓鱼攻击造成的全球损失高达数十亿美元，我想这一点恐怕没有人会做出反驳。今年 9 月，我们刚刚报告过一次网络钓鱼行动，迄今为止全球损失已高达 260 亿美元。这次行动波及多达 177 个国家，还未衡量对国家维基百科的影响，蔓延至多达 195 个市区...堪称全球性灾难。

劳伦 • 卡宾： 加布里埃，什么是商业电子邮件欺诈？

加布里埃 • 安德鲁斯： 通过电子邮件进行欺诈。一般而言欺骗人们发送电汇。我想大家都已经看到了。如果您所在的组织未了解过相关信息，或许只是因为您不知道所在组织受到影响，但并不妨碍恶意用户发送电子邮件，冒充首席执行官、首席财务官及具有付款权限的

人员。欺骗他人实施行为。电汇付款 50,000 美元、20,000 美元乃至百万美元。有时，恶意用户会使用专门注册的域冒充受害者的域，通过欺诈性电子邮件导致数十美元的损失，甚至还会造成数十亿美元的巨额损失。还有其他意见吗？好的，请切换到下一张幻灯片。您愿意介绍一下 CCT 吗？

劳伦 • 卡宾： 当然。这个问题属于工作范畴，我们可以就定义进行辩论，另外还要指出的是，ICANN 合同中已经做出了大量定义，这里列出了现有的一些要求，已纳入北京会议公报等文件的 GAC 建议部分。与此同时，消费者信任和消费者选择审核也指出了一些现有定义，现已纳入社群出台的共识性政策。特别是，我要说明的是，我加入了 CCT 消费者选择审核小组，或许这对我长久以来开展的工作具有一定的促进作用。尽管如此，这份报告完成了大量出色的工作，哪怕只是阅读 DNS 滥用问题部分，也会发现有很多详细引证指向 ICANN 发布的现有定义。其中包括 DNS 滥用和 DNS 安全滥用定义。另外，还提供了其他一些权威来源，例如去年 4 月发布的互联网与管辖权政策网络规定。

同时，还探讨了相关定义，这也是我要强调的内容。其中很多定义来自一些极为常见的核心元素。如果使用恶意软件、网络钓鱼、僵尸网络和垃圾邮件，某些类型的滥用将一直存在，包括商业电子邮件诈骗和网络钓鱼攻击，主要取决于 DNS 系统。比方说，一旦您点击链接，将锁定信息，继而破坏系统。

加布里埃 • 安德鲁斯： 请切换到下一张幻灯片。我们意识到，注册管理机构与注册服务机构处理滥用投诉的能力存在一定程度的差异。在注册管理机构级别，可能采取的应对措施包括删除域、暂停域及锁定域，避免做出任何进一步的更改，进而杜绝转移域。注册服务机构级别的预防措施更为广泛，包括识别注册人身份。我想我们在现实世界中已经见过一些示例，在 .DK 文件中，大家可以验证注册人的身份。犯罪大幅减少，滥用同样大大减少。瞧，恶意用户不喜欢曝光，不愿意公开真实身份。这具有一定的直观意义，但可以客观地看待这个问题。具体而言，在一些真实旧案例中，用户可以进行验证，我们发现结果朝预期方向发展。犯罪逐步减少。同时还发现，犯罪分子需要一些工具或者对域名注册进行调整，而像你我这样的普通注册人则可能不需要这样做。

例如，犯罪分子在注册域名时会模仿想要攻击的受害者。我们可以称之为同形异义词或相似域。我想不到太多的合法理由证明善意用户希望使用此类同形异义词或相似域。此外，犯罪分子可能希望利用域名，他们可以通过工具创建很多很多不同的域名。僵尸网络使用工具，恶意用户使用工具控制其创建的大量僵尸网络。同样，我也想不到此类做法的合法目的。我发现，当今世界确实有些 SOP 注册服务机构允许在实际注册页面上为潜在注册人提供这款工具。我想请其他同事指教，或许有某种合法理由，只是我还没有想到。此外还有批量注册。注册随机域，每次注册的域哪怕没有达到数千个，也有数百个之多。

同样，我努力为此类批量注册寻求合法目的。如果注册服务机构能够使用现有的一些工具查找过去的滥用行为，切实利用这些数据作为持续注册预测指标，那么势必可以采取措施阻止滥用。我们在 ID 实施过程中发现了这一点，在此过程中，机构可以使用过去的滥用指标识别注册时发生的滥用行为。尝试标记供人类审核，我们受到一些示例的启发，因为我们将它们视为难得的经验教训，共同致力实现缓解社群滥用的共同目标。此外，我还要指出最后一点，犯罪分子对价格极为敏感，特别是在注册方面，每次注册的域哪怕没有达到数千个，也有数百个之多，如果注册服务机构提供几乎免费的域，势必会吸引大批犯罪分子。或许社群不应该鼓励此类行为。

我记得现阶段出台了一些合作方法，必定可以有效应对上述这些类型的滥用行为。如果没有记错的话，目前有些激励机制促使犯罪分子向注册服务机构付费批量注册域名，如何从社群层面出台反激励机制？可不可以出台政策，采取主动反滥用措施？我认为值得合作探索。我会尽我所能。

格雷格 • 穆尼耶 (GREG MOUNIER)：谢谢，加布里埃。在我看来，这些幻灯片对 GAC 成员带来了一项启示：请记住，注册管理机构和注册服务机构可以采取大量具体措施，增加恶意用户实施犯罪的难度。因此，只需加大犯罪分子出于恶意目的注册域的难度，这一点显而易见。不一定要设定高昂的价格。确实存在这样的方法。某些 ccTLD

已经开始采取此类措施，而且还可能出台一些具体措施，但就我个人而言，我们更倾向于采取合作方法，因为这是一种基于共识的政策制定环境，我们深刻意识到注册管理机构和注册服务机构都在积极开展业务，务必确保公共安全利益与商业利益保持一致，我们希望这一空间演变成为蓬勃发展的商业环境。所以，ID 建议出台经济激励机制，要求注册管理机构对注册服务机构的安全行为予以奖励，这个主意不错。很多娱乐行业注册管理机构都在采取这种做法，我们应该推广此类举措，就像可信机构发布计划一样。我想现已达成这样一项共识：不同参与者之间相互信任，一些参与者拥有特定的专业知识，注册服务机构可以根据这些专业知识安全采取措施，无需开展复杂的法律讨论，以上是我要就这个问题发表的全部看法。

加布里埃 • 安德鲁斯： 说得好，格雷格。好吧。请切换到下一张幻灯片。您愿意再次介绍一下 CCT 吗？

劳伦 • 卡宾： 当然。这是面向信息商业世界发出的行动号召。ICANN 可以采取哪些行动？接着，还会讨论 GAC 可以采取哪些行动？但我们认为最重要的一点在于，实施竞争、消费者信任和消费者选择审核小组建议。实际上，这家机构负责严格审查第一轮呈指数级增长的通用顶级域 (gTLD) 系统，确定哪些方面运作良好，

哪些方面运作失败，而且团队中设有注册管理机构代表。注册服务机构与各利益相关方团体相互合作达成了 30 多项共识性建议，我记得是 35 项建议 -- 遗憾的是，大部分建议未能得到董事会的采纳。大多数建议被搁置。ICANN 可以开展一项工作，那就是采纳这些针对 DNS 滥用问题提出的特定建议，这实际上是 ICANN 董事会的职责。其中一些建议十分具体，势必可以更有效地解决此类问题。一是，支持刚刚就奖励机制开展的讨论。出台奖励机制，针对良好行为予以奖励。确保在合同中切实标识有效条款，坚决打击特定注册服务机构和注册管理机构面临的系统性滥用问题，我们将其简称为“三次出局规则”。如果参与者持续从事不良行为且拒不遵守合同条款，应采取有效应对措施。绝不能任由他们一再重复不良行为。

另外，还应确立一些具体的滥用阈值，支持 ICANN 合规组织自动开展调查。

如果事态发展到一定的严重程度，则需要实施细致审查和调查。最后，我们还提出了一项十分具体的建议：发出一个简单的倡议，务必确保收集域名负责人信息。这并不是呼吁披露，也不是在探讨隐私，更不是要求披露应当予以保护的信息。只不过在讨论一项技术性问题，这是横亘于注册服务机构和注册人之间的问题。如果有人既是域名所有者又是所有权链中的另一实体，也就是分销商，那么提供给执法机构和公众的官方记录中可能并不会注明此类信息。所以这项建议指出，我们发现收集的信息存在缺陷，只是简单询问您是否有一群人出售域名，确

保所有权链中的每一方均可识别并收集相关信息。这样，一旦发生不良事件，执法机构明确知道向哪一方进行讯问。以上是专门针对处理 DNS 滥用问题而提出的消费者信任具体建议，暂时遭到搁置。顺便说一句，这项分销商信息建议在技术层面得到董事会的采纳，但还面临一个小问题，因为现阶段允许随意收集这些信息。也就是说，目前允许收集此类信息。CCT 审核小组建议强制收集信息。尽管董事会明确表示接受这些地区，但仍有地区尚未达成共识。建议强制采取这项措施。目前是选择性采取措施。这是需要做出调整的一个方面。

加布里埃 • 安德鲁斯： 谢谢，劳伦。稍后，我将会重新做出说明。身为执法调查机构，我们发现托管基础设施面临类似的问题。用户运行服务器，租用服务器空间，我们遇到了大量困难。在某些情况下，托管公司的分销商本身拥有分销商客户，分销商本身也是客户的分销商，我曾去过一个房间，机器旁边是 20 英尺高的服务器机架，但却不知该去哪里查找现有数据的实际所有者，因为可能存在 2 层、3 层乃至 10 层分销商。在域名空间，我们绝不允许出现此类情况。我的意思是，我们深知这种局面的恶劣影响。

克里斯 • 刘易斯 • 埃文斯：请切换到下一张幻灯片。谢谢。接下来，GAC 该怎么做呢？我们介绍了 ccTV -- CCT 审核建议，我认为将此纳入 GAC 建议并具体实施是一个重大的进步。众所周知，我们之前也提出过 GAC 建议，务必确保这些建议得到有效实施，密切关注相关工作非常重要。我们与注册管理机构团体进行了良好的交流，同时像我们这样国家/地区都有自己的 ccTLD，其中一些 ccTLD 在跟踪 DNS 滥用问题方面形成了一些卓有成效的最佳实践。如果能够识别并推广这些最佳实践，以及面向社群分享一些成功经验，势必可以提高 ccTLD 和 gTLD 解决 DNS 滥用问题的基准。

在这种情况下，接下来需要与各利益相关方建立合作。身为 PSWG，我们一直努力从社群中脱颖而出。我们已与很多利益相关方召开过卓有成效的会议，人们衷心希望遏制由来已久的不良行为及 DNS 滥用问题。畅享清洁的系统环境。这是一种正确做法，我们希望面向更多的用户敞开大门，但还有一些注册管理机构和注册服务机构未能出席会议，我们必须郑重宣布现已妥善确立政策与合同，哪怕这些机构未出席会议，也要遵循最佳实践和运营原则。但最重要的是，PSWG 成员数量有限。无法吸纳每一个国家/地区的 GAC 代表，只能依靠诸位向所在机构传达违规行为及违规报告方法，甚至向 PSWG 反馈问题，如果诸位在报告违规行为时遇到困难，我们非常乐意帮助大家了解报告过程。我认为，我们的工作范围十分宽泛。请切换到下一张幻灯片。在我看来，我们应集中研究一些更具体的领域，

所以列出了 3 项议题。这样略微清晰一些，我想确定究竟需要针对未来建议进行审议，还是针对这项建议进行审议。

澄清 DNS 滥用问题包含哪几个部分。众所周知，我们将利用这一整周时间召开进一步会议，讨论什么是 DNS 滥用，以及它会对每个人造成怎样的影响。在 2013 年 GAC 公报中，我们对此有了良好的基本了解，实际上是为了确保大家愿意接受基准。下面继续澄清。再来看看最佳实践。我们提到过多次。无论加布里埃还是劳伦，在发表意见时都曾提到最佳实践。实际上是指获取最佳实践。确保每一个人在解决 DNS 滥用问题方面达到一致的水准。同时，我记得我们还多次提到了 CCT 审核，实际上，落实这些建议对于启动 DNS 滥用问题解决流程至关重要。

加布里埃 • 安德鲁斯： 这是最后一张幻灯片吗？还有哪些后续工作？请切换到下一张。是，我想轮到您了，劳伦。谢谢大家。

劳伦 • 卡宾： 我在。在此提醒各位，这些建议属于 FYI 类别。如果列入问题提交 ICANN 董事会，势必可以使这项主题得到妥善解决，之所以强调这一点，是因为确实对此存有疑问。实际上，这些问题基于 ICANN 在战略规划中提出的行动事项战略目标。这份 ICANN 战略规划将 DNS 滥用列为工作重点。我的意思是，我们

向董事会提出了一些非常具体的问题，主要询问他们如何实现这一目标。我们将此列入董事会讨论议程。大家将会发现，目标在于采取协调性方法，有效识别和缓解 DNS 安全威胁并遏制 DNS 滥用问题，同时提高社区透明度，ICANN 希望维护其不偏不倚、可靠和据实报道 DNS 帮助信息的名誉。

我们想问的是：如何实现这一目标？如何保证社群识别善意参与者？因为确实有很多善意参与者。善意参与者比恶意参与者多得多。与此同时，谁又是恶意参与者？如何传达相关信息？如何召集各利益相关方召开会议，讨论如何将这些保护措施纳入 ICANN 合同启动准则？我们将与董事会讨论这些问题。同时还会召开 DNS 滥用跨社群会议，加布里埃将代表我们出席此次会议。建议大家在星期三 10:30 出席会议。当天下午的社群会议结束后，我们将举行第二次讨论。即将开展的重点工作就是这些。我想这该是最后一张幻灯片了。好的。是的。

玛娜尔 • 伊斯梅尔（GAC 主席）：谢谢大家。非常感谢大家。这已非常详实。是的，DNS 滥用是经跨社群讨论一致认定为热点问题的主题之一，正如劳伦所说，还有一些 CCT 建议等待在这次跨社区讨论中进行研究。这些是社群讨论搁置的一些主题，希望明天开展讨论期间以某种方式发布或实施这些建议。我想提一个简单的问题：是否可以切换到介绍签约方的那一张幻灯片？当然，大家可以畅所欲

言，欢迎提问或评论。我将做一下总结。是否还有任何其他问题？首先请瑞士代表发言。请讲。

瑞士代表： [口译员讲话] 我是瑞士代表奥利维尔•吉拉德 (Olivier Girard)，我将用法语发言。感谢你们的精彩演讲。在我看来，我们提出了很多阻止攻击的举措。我想了解一下大家的观点，究竟可以采取哪些预防措施防范攻击，增加发动 DNS 滥用攻击的难度？但还有很多其他技术可供使用，以便阻止欺诈等其他各类滥用问题。ICANN 在促进实施这些开放性技术实践或规范方面发挥着怎样的作用？至少这样可以加大恶意行为者攻击 DNS 或从事 DNS 滥用活动的难度。大家对此有何看法？谢谢大家。

加布里埃 • 安德鲁斯： 这个问题非常有意思。谢谢您提出这个问题。希望我的同事们加入讨论，因为我猜想每个人都有自己的看法，但我要指出一点，我甚至不太确定技术手段是最有效的手段。有些浪费唇舌 -- 很抱歉，我的发言过于口语化 -- 最有效的措施是对注册人注册进行全面身份验证。我认为不属于技术手段。很多人可能对实施难度有不同看法。不过，我发现很多非常有趣的对话就解决这个问题提出了看法。我认为，我们应该继续开展相关对话。无论是否确立某种数字识别机制便于人们在某些情况下验证个人真实身份，总有一些国家能够采用现有的国民身份，并

非所有国家都有这种机会，然而一旦取消匿名机制，势必令不法分子无所遁形，恶意身份昭然若揭。他们不希望暴露自己的真实身份。若要处理此类问题，我想这是最有效的方法。除此以外，我还听说一些注册服务机构为实施开放性技术标准进行了艰苦卓绝的努力。我不想令本就为缩略词感到困惑不已的受众雪上加霜，但 D-Mark 这一类技术可以从根本上打击网络钓鱼及欺诈电子邮件。我不打算深入探讨这个问题，因为实际上在我看来，任何方法都不及验证注册人信息有效，我想请我的 --

格雷格 • 穆尼耶： [口译员讲话] 我相信，ICANN 内部设立了一些团体，比如 RSSAC，不仅可以发布有趣的研究报告，还能推广新型技术举措。我的意思是，除技术举措以外，还可以从域名注册角度采取一些基本步骤，防止恶意行为者以注册域名为掩护实施犯罪行为。增加恶意行为者注册域名的难度。目前已经有一些技术工具，但我们也可以使用其他工具，谢谢。

玛娜尔 • 伊斯梅尔（GAC 主席）：还有问题和意见吗？如果没有，在此我想就第 4 点提一个问题。可不可以详细说明一下究竟如何从 DNS 级别入手解决问题？我们只剩下 2 分钟时间 -- 不过正如劳伦所说，本周晚些时候还会再召开一场会议。经我们与董事会讨论决定，在跨

社群专家组会议结束后，刻意增加了一场会议。这样，我们将可以从 GAC 的角度阐述立场，我想将这个问题留到稍后解答。特别是，在座的一些董事会成员还要出席董事会 - GAC 互动小组会议。再次感谢各位进行的详细演示。我们将在利用本周时间继续讨论。谢谢大家。

[听写文稿结束]