

圣胡安 - GAC 关于 PSWG 的讨论会议

2018 年 3 月 13 日 (星期二) - 8:30 - 9:30 (大西洋标准时间)

ICANN61 | 波多黎各, 圣胡安

卡特兰·鲍尔·布尔斯特 (CATHRIN BAUER BULST): 好的。大家上午好。非常感谢各位在出席昨夜的绝妙晚宴后, 毅然放弃留下享受加勒比海岸阳光的绝佳机会, 来到这间大会议室出席会议。我们感谢大家对公共安全工作组所做的卓绝奉献, 本次会议是政府咨询委员会公共安全工作正式会议。我叫卡特兰·鲍尔·布尔斯特。目前是本工作组的 2 名联合主席之一, 这是另一位联合主席劳伦·卡宾 (Laureen Kapin)。在本次会议日程中, 我们共安排了 2 项主要议题。首先将讨论公共安全工作组的工作计划, 然后讨论 OCTO 工作和 DAAR 工具。稍后将从工作计划开始讨论, 但首先我想请公共安全工作组的各位同仁跟大家打个招呼。

未知身份的发言者:

大家好, 我叫劳伦·卡宾, 来自美国联邦贸易委员会, 主要负责消费者保护工作, 感谢各位出席我们的首次会议, 尽管本次会议自 8:30 开始启动, 但后面还会安排更多会议。本次会议结束后, 我们将会转换主题, 重点讨论系统和 GDPR。今天上午的会议出席人数众多, 但愿大家至少认为这是一次愉快的尝试, 趣味性十足。

---

伊朗嘉·卡函嘉玛 (IRANGA KAHANGAMA): 大家上午好。我叫伊朗嘉·卡函嘉玛, 来自美国联邦调查局。再次感谢邀请我出席会议。我主要负责与 DAAR 相关的 DND 滥用问题工作, 我们需要与一些 OCTO 工作人员共事。欢迎大家观看幻灯片, 思考我们可以提供的支持形式, 包括通过政策或其他建议辅助开展计划。这无疑有利于保障互联网社群的安全。期待通过工作计划与诸位进行交流。谢谢。

卡特兰·鲍尔·布尔斯特: 非常感谢。稍后将会启动相关工作。确实如此。劳伦提出了一项很好的建议, 请在座的公共安全工作组成员举一下手, 因为听众席中有很多人对我们的工作很感兴趣, 也可能希望透过今天的会议与我们当中的某位代表进行交流。请在座的公共安全工作组成员举一下手, 让大家看到你们坐在哪里。

劳伦·卡宾: 如果诸位存在疑问, 不仅可以向台上的各位代表提出, 我们有很多成员, 大家都乐意交流并解答问题。

卡特兰·鲍尔·布尔斯特: 众所周知, 经过星期日的会议, 我们即将在未来一段时间通过公共安全工作组工作计划。截至星期日, 我们的工作基本已经结束, 现在希望借此机会与大家重温一下工作现状, 看看是否需要先就此提出最终意见, 然后在会议结束时列入 GAC

---

公报。第一个讨论主题是滥用诉讼，伊朗嘉负责引领相关讨论，向我们进行全面介绍。

伊朗嘉·卡函嘉玛：

谢谢。正如我在前面所说，这是我们的主要工作计划之一，目标在于协助 ICANN 更有效地解决 DNS 滥用问题。很多公报将其列为重点解决问题。很多团队将它们列入大量报告，我们希望继续大力推进工作。我刚刚说过，稍后将会讨论域滥用活动报告项目，这是一项重大工作计划议程。然后，如果希望了解相关议题，我们还提供了 GDID 市场及标识符技术健康指数，这两项独立计划均与 ICANN 开放数据举措有关。ICANN 开放数据举措旨在提供更多的数据和数字辅助人们理解部分滥用，因为分别从宏观和微观角度提供某些健康指数，因而可以更有效地提供滥用报告。下面跳过几个议程项目，这些项目可以暂时搁置，集中精力制定原则。我们认为，通用基线理解机制应得到社群各方的一致接受。一旦获得集体通过，即可达成一致意见并投入实施。从网络的角度而言，还有一个社群尚未充分开发，那就是 SSAC。我们听说，他们推行了大量有趣的举措，我们打算与他们进行更正式的接洽。我记得，这场会议将于明天下午 3:15 召开，即 SSAC 开放会议。他们曾表示，任何人都可以出席会议，在座各位可能希望出席会议，了解他们开展的部分安全工作的进展情况。他们尤其关注注册服务及其背后的技术问题，显然还希望就部分 GDPR 事项进行讨论。所以，我想势必会有很多安全领域人士出席会议。为推进外展工作，我

---

们将努力通过更正式的方式与他们建立关系，以便制定更出众的反馈机制。以上概括介绍了我们要努力达成的目标。欢迎大家献计献策。显而易见，我们十分开放。互联网面临众多安全问题，DNS 的带宽有限，但我认为我们做得很棒，并且将在议题讨论结束时向大家通报进展情况。我认为在本次会议中，这项议程的重要性稍显逊色，因为 GDPR 议题占用了我们大量的精力，但仍会继续将此列为重点议程。谢谢。

卡特兰·鲍尔·布尔斯特：我想提醒在座各位 GAC 成员，你们也收到了这份工作计划副本，直接附加到议程简报当中，因为我们已在星期日向大家做过介绍，如果希望在闲暇时慢慢阅读，可以在简报中进行查看。

劳伦·卡宾：简单谈谈消费者保护，这项议题一直是竞争、消费者信任和消费者选择审核小组负责的工作之一。我一直领导子团队集中讨论保护问题，但从根本上而言，这项议程只是现有工作的延续，强烈呼吁出台在线用户保护政策。这也是这部分工作计划的首要目标，因而我们将广泛参与相关审核。我们广泛联络 ICANN 组织的各个团队，特别是合规与安全团队，同时还联络社群讨论相关议题，因为全体人员都热切盼望加强用户在线环境安全性，推动增进消费者信任，以便他们继续使用互联网。从这个角度出发建立了大量不同的利益相关方和工作阶段，包

---

括全新的后续流程审核 PDP，同时还协助实施隐私代理服务认知系统，而且从这一层面推进大量不同的工作阶段。

卡特兰·鲍尔·布尔斯特：好的。我想重点讨论下一页的 2 项议程：问责制和防止利用 DNS。关于问责制，我们仍在寻找涉及这项议程的议题。目前公共安全工作组正在讨论这项议题。公共安全议题涵盖大量工作阶段，它们与政策层面息息相关，旨在更有效地防范部分问题。这项工作指出可能希望代表用户为儿童营造安全空间，北京公报提供的保护需要接受有效性评估，可能在后续几轮详细工作中采用相关成果，而且这一工作阶段还会开展另外一些工作。在本次会议中，我不打算进行更详细地说明，请稍后与我本人或意大利 GAC 团队交流相关问题。我要讲的就是这些，有人要这就第一项战略目标发表意见吗？下面继续介绍第二项战略目标，主要集中探讨 RDS，其中一项主要议题是哪些用户有权访问 GDPR 注册数据。有请劳伦发言。

劳伦·卡宾：我打算暂时搁置这项议程，因为我们将会在茶歇之后深入讨论这项议题。大家只需要知道，这是 WHOIS 系统，涵盖我们工作阶段的所有优势和职责，事实上这也是我们最近研究的真正焦点。

---

卡特兰·鲍尔·布尔斯特：在它的推动下，我们将迎来新一代 RDS PDP。格雷格 (Greg)，你要对这个问题发表意见吗？不是。好的。我想是这样。

未知身份的发言者：继续讨论。

卡特兰·鲍尔·布尔斯特：继续讨论，好的。接下来，我们探讨一下注册数据准确性问题。众所周知，这项议题由来已久，目前正在实施注册数据条目的语法准确性检查。有一个问题尚有待社群加以解决：实际检查注册人身份。从公共安全角度而言，还存在大量提升空间，迫切需要提高 GDPR 注册数据的质量。我们发现，ccTLD 世界还出台了一些长远举措，如何经济可靠地落实这些举措？在我看来，我们将继续推进相关工作，确定如何拓展这些工作并在通用顶级域领域大力推广。

伊朗嘉·卡函嘉玛：我认为这部分工作计划非常重要，因为大部分代表可能并未忘记，GDPR 呼吁提高数据准确性，而且还要在一定程度上掌握数据。在我看来，之所以一直未集中讨论相关问题，是因为目前还在竭力保留数据或维护访问权限，但也未触及第二个步骤，即确保数据的实际准确性。我想随着工作的进一步推进... 势必要发挥 RDS 审核小组的关键作用，GAC 提名美国国际刑事警察组织代表莉莉 (Lily) 和我本人参与相关工作。目前正在

---

开展相关审核，而且仍旧处于早期阶段。或许在下一届巴拿马城 ICANN 会议中，将会向大家汇报工作进展。这也算是出席下届会议的又一原因。

劳伦·卡宾：

这是我们的第 2 项战略目标。大家对此还有问题或意见吗？好的。下面继续讨论第 3 项战略目标，它也是一项基本议题。堪称主干战略目标。构建初步而又灵活的 PSWG 运营原则，切实重点开发组织框架和我们的程序。大家将会发现，首先需要制定工作计划。加强领导。正如星期日召开会议时指出的，希望获得深刻认识，以便人们能够集中探讨政策开发工作及利益相关方外展过程中涉及的大量重要主题。我们希望强化成员机制深化筹款募捐模式。我们曾与 GAC 领导开展过相关讨论，其中一个思路是鼓励 GAC 成员考虑提名机制，切实推动执法行动...每一个国家/地区均设立执法人员，拘捕到案人员对前线调查了如指掌，又该如何遏制犯罪行为。特别是，如果涉及 DNS，我们知道这些问题牵涉技术层面而且十分复杂，您所在的国家/地区势必聘请专家，您可以向他们咨询。我们建议大家正式提出咨询，深入接触此类群体，将他们提名为公共安全工作组顾问将会更好。将他们加入我们的电子邮件清单。如果刚好从事相关领域，还可以出席会议。这一点真的非常重要，我们可以借此机会要求每一位人员深入参与讨论这些至关重要的公共安全议题。我要强调的是，毫无疑问，我们同样身在咨询委员会，隶属于政府咨询委员会政府工作组，因而势必希望

确保与 GAC 和 GAC 领导团队进行一致沟通，相互配合工作，并在出现需要快速行动的热门议题时提出建议。我们对目前的工作了解深入，记得我们还曾要求大家审视复杂主题并进行快速审核，这并非理想场景，但遗憾的是，这就是我们目前面临的困境。我们要确保的是，可以尽量高效开展工作，为大家做出启发，使人们有机会审核 PSWG 开展的重要工作。如此一来，将可征询大家的意见并获得支持，共同确保产品反映 GAC 的共识态度，我们同样将此列入工作计划。从这个层面而言，我们会一直留心听取大家的意见，确定哪些方面成效显著，哪些方面还可以进一步改进。请大家畅所欲言。正如大家所见，我们从来都是踊跃发表意见，衷心希望在走廊及通过电话与大家交流。无论何时需要做出判断，都可以向我们反映。这是工作计划的第 3 项战略目标，欢迎大家据此提问或发表意见。有请詹森 (Jason) 发言。

加拿大代表：

我叫詹森，是公共安全工作组的加拿大成员。我发现，阿布扎比会议中存在这样一个事实：工作组的人员相对集中，不仅有很多北美代表，还有很多欧洲代表，我们希望加强成员多样化。如果发现适合从事公共安全工作组工作的候选人，请联系我们，我们可以提供参与方式。多样化程度越高，队伍越强大。或许我们需要广泛发布消息。事实上，我们当中的很多代表来自北欧或西欧，我们希望广泛了解世界各地的想法，而不仅仅是我们各自国家的意见。请与我们联系，



---

我们可以帮助您参与相关工作，或者帮助您所在警察部队的人员参与工作安全工作。谢谢。

卡特兰·鲍尔·布尔斯特：非常感谢詹森提出这项重要意见。我是卡特兰。我想就加强多样化问题补充几点。这样可以更全面地反映全体 GAC 成员的意见，对于我们推进工作至关重要，进而以工作组的身分帮助大家开展工作。如果可以在工作组中广泛反映 GAC 的不同立场，将可以更有效地促进工作。需要指出的是，在这些会议中，很多公司尚未完成。我们每月召集全体工作组成员召开电话会议。领导和成员则每周召开一次电话会议，无论身在何处，都可以参加会议。通常采用 Adobe 会议室。如果要提名纳亚 (Naya) 专家，他恐怕无法出席会议，这一点很关键。如果可以偶尔抽出时间召开面对面会议，但大部分工作仍在会后通过远程参与形式开展，势必会更加顺畅。因此，我想提醒在座各位，如果因人员安排问题担心无法参与公共安全工作组工作，那么这其实并不妨碍大家参与相关事务。我要讲的就是这些。关于第 3 项战略目标，还有没有其他意见？或者，有没有人对此特别关注，希望立即加入讨论？

[笑声]

只是玩笑话。如果没有其他意见，我们将继续讨论第 4 项战略目标，关于面向社群其他部分及本环境的外部利益相关方实施外展的工作。这项工作卓有成效，旨在评估我们推行工作计划

的效果。关键的一点在于，确保设定适当的优先级。毫无疑问，为实现这一目标，我们不仅要与在座一些人员进行交流，同时还要广泛联络未出席会议的众多群体，从会议政策层面判定他们面临的影响，包括如何实施当前政策为自身服务、可以在哪些方面做出改进，甚至指出希望公共安全工作组通知 GAC 或提供专家意见的重大问题。另外，我们还通过其他政府机构提升公共安全工作组的知名度，确保推进横向协调，使各个国家/地区充分意识到公共安全工作组的职责，当然并不仅限于维护治安。从官方层面而言，公共安全工作组负责解决大量公共安全问题，必须在工作中予以充分反映。同样，我们还会继续努力降低参与门槛。同时设法提供更有效的信息。我的意思是，或许大家对此已经了如指掌，在我向某些代表说明 ICANN 工作使命时，人们要么很快催眠，要么匆匆找借口离开。

[笑声]

鉴于此，真的很难征询适当的意见，因为当人们再返回时，很可能直接询问会议决议了。希望探究我们据此开展的具体工作。实际上，我们刚刚开始讨论，工作仍在进行当中，还需要一段时间才能完成。出于很多原因，可能很难使人们充分掌握会议进展及其重要原因，更无从使他们意识到为什么对于他们也很重要，以及他们可以做出哪些贡献。我们一直在设法从根本上降低这些门槛。依托新闻通讯。简要概括会议内容，使日常接触不到互联网治理问题的人们轻松掌握我们的工作动态。特别是在休会期间据此召开会议时，我们还会征集到一些非常

有效的意见，因为很多机构通常并不会参与这项工作，但却会提出大量很有建设性的问题，包括为什么要开展某些特定工作、如何开展工作、哪些人员会提出有效意见，以及如何更有效地推进外展工作，以便切实实施这些想法和意见。大家可能会发现，还有很多志愿者席位，请踊跃报名参与我们的工作。我感觉有点像募捐现场。

[笑声]

那么…

劳伦·卡宾：

接下来，由伊朗嘉对本次会议的外展工作进行介绍。

伊朗嘉·卡函嘉玛：

谢谢。或许应该简要说明一点：我们希望尝试开始与 SSAC 进行对话。SSAC 曾指出，他们正在开展一些有趣的工作。在外展过程中，我们一直与注册管理机构和注册服务机构探讨一些 RDS 问题，尽量征询他们对于整体事态的反馈意见。这一直是我们的外展工作的 2 个主要方向。显而易见，我们将立刻与 OCTO 进行交流。我们将本着开诚布公的态度讨论 DAAR。我认为，其中有很多创造性意见。无论任何人，只要有其他创造性提议，我们都希望深入了解。

---

卡特兰·鲍尔·布尔斯特：谢谢。为了更有效地了解我们所属的社群机构，我想提醒大家，今天晚上将与注册服务机构举办社交活动。我记得是 6:30 在露台上开始。所以，请出席我们的活动。如果还想加强了解社群的其他机构的话。我认为，这项总结很棒，我想稍微暂停一下，看看大家对于第 4 项战略目标还有没有其他创意看法。如果没有，工作计划审核将到此结束。如果对工作计划有任何其他意见、问题、建议或调整想法，希望大家与我们联系，或在今天之前向我们发出电子邮件，否则我们将默认本项议题到此结束，并拟定 GAC 公报语言以通过这项工作计划。好的。大家都没有意见了吗？这意味着，我们可以继续讨论会议的下一项议题：通过 OCTO 和 DAAR 开展对话。好极了，我看到戴维 (David) 来了。戴维，感谢你抽出时间出席本次会议，我知道你感冒十分严重。

戴维·康纳德 (DAVID CONRAD)：各位早上好！抱歉，声音有些嘶哑，可能偶尔还会咳嗽，但我需要代表约翰 (John) 出席会议，他昨夜在晚宴上玩得实在太尽兴了。

[笑声]

这不能责怪晚宴，谢谢。让我们来看下一张幻灯片。我敢肯定，在座大部分代表对 DAAR 的内容有所了解。我想向不太了解 DAAR 的代表说明一下，DAAR 是我们在 iThreat 网络社群的帮助下开发的一款报告系统，旨在从 GAC 在北京公报中确定

的滥用中找出自身感兴趣的部分进行跟踪。而 ICANN 却未关注取模问题，也未关注垃圾邮件问题。DAAR 与我们提供的其他很多报告工有着怎样的不同？从根本上而言，收集的数据量有所不同。基本上会汇总大量建议。实际上，我们会在收集数据时做出规划，以便开展历史研究。重点关注滥用多样性，以便生成透明而又可复制的信息，简化通信过程，促进 ICANN 社群内部的政策制定流程。请切换到下一张幻灯片。我已经据此进行过说明。一个问题在于，我们授予了相当一部分数据供 DAAR 使用，但这些数据的可用性不确定。请切换到下一张幻灯片。DAAR 的作用有哪些？显而易见，它的主要目标是报告顶级域或注册服务机构层面的威胁活动。我们可以用它来研究安全威胁或域名注册活动历史。它可以帮助运营商、注册管理机构、注册服务机构及后端运营商了解或考虑如何通过反滥用系统管理声誉。也包括使用声誉名单及相关数据。这样，我们将可以研究恶意注册行为，从而为安全和运营安全社群提供帮助。我们使用顶级域分区，收集各类相关数据执行通用顶级域注册分析。主要使用集中区域数据服务，还会在可行的情况下进行区域传输。DAAR 将仅使用出现在区域中的名称。我们不会提前深入查询注册管理机构或注册服务机构数据库，而是直接将名称保存到区域中，目前共有约 1240 个通用顶级域，生成了约 1.95 亿个域。很多 ccTLD 一直与我们接洽，希望参加 DAAR，我们将竭力将它们纳入 DAAR 系统。DAAR 同样使用 WHOIS。它只占互联网很小的一部分。主要问题在于注册服务机构，甚至会造成相当大的麻烦。由于 DAAR 希望开发

任何用户均可复制的系统，我们将避免使用 ICANN 内部提供的任何信息，仅限在 ICANN 内部使用这些信息。我们将实际利用通过这样或那样的方式面向公众发布的信息。因此，我们将竭力通过现有的 WHOIS 服务器从数百万域中提取信息，因为在座很多代表想必明白，流量限制可能颇具挑战。请切换到下一张幻灯片了解威胁数据集，我们使用了大量威胁数据集。我们会尝试对数据执行独特的 FI 处理，避免出现太多误报。我们使用多个域或 URL 滥用数据集生成与互联网和垃圾邮件的网络钓鱼基数关联的每日域计数。我们计算照片 ASL 和累计滥用域，创建直方图和使用周期天数。DAAR 侧重反映 ICANN 外部人员和 ICANN 社群对域名生态系统的看法。请切换到下一张幻灯片。请切换到下一张幻灯片。我们不会在 OCTO 或 ICANN 中自行编写组织名单。这不是我们的工作范围。究竟是否可以妥善实现，我还有所疑惑。我们将合成或汇总通过外部各方获取的数据，各当事方之所以生成这些名单是为了切实阻止威胁。DAAR 收集报告给相关行业的滥用数据，因而无需在此重新生成数据。人们普遍存在一个担忧，害怕生成的新数据可能不够准确，我们曾在多种场合反复重申，这就是互联网服务提供商和邮件运营商日常运营所使用的工具。我们并没有做出任何新的尝试。请切换到下一张幻灯片。将某个表示阻止名单纳入 DAAR 系统的标准。必须提供威胁分类，匹配我们研究的这一系列威胁，运营安全社群必须信赖 RBL 的流程准确性和清晰性。它们必须在学术文献中标识积极表示，RBL 必须得到运营安全社群的广泛采用和接受。通常表现为将大量建议纳

入商业安全活动和产品，再由网络运营商用来自保护用户和设备，电子邮件提供商将为它们提供保护或使用它们提供保护，从而防止垃圾邮件及其他攻击。请切换到下一张幻灯片。我们普遍应用 RBL。RBL 不仅可以阻止自发商业电子邮件，还可以在 Google Chrome 等浏览器中使用，进而利用 APWG 名单。在云和内容服务系统中使用...使用 SERBL 和 Amazon 作为 Web... 我不记得 WAF 代表什么，进而使用 RBL 阻止容量耗尽攻击滥用，使用 Google Safe 阻止恶意 URL 及消息欺诈。在 DNS 中，人们通过所谓的资源政策区域使用 RBL。资源政策区域采用视觉技术开发，如今在多种解析服务中广泛应用。垃圾邮件及其他威胁究竟如何使用 RPZ 格式提供这些 RBL，这与解析服务的使用方法息息相关，这样将可避免我们陷入危险境地，确保使用以实验为基础的数据。事实上，此类技术广泛应用于生产服务及商业产品。请切换到下一张幻灯片。另外，我们还一直呼吁学术界审核这些 RPL，确保遵循最佳实践并通过研究人员可以信赖的方式使用。我们整理了一份名单，其中涵盖大量关于在 DAAR 中引用 RBL 的学术报告。请切换到下一张幻灯片。目前使用的 RBL 集包括：仅 SERBL 域名单、SPAM house 域阻止名单、反网络钓鱼工作邮件列表。恶意软件巡逻是指大家看到的这份综合列表，包括 PhishTank Ransomware Tracker 和 THEODO Tracker。在后面几张幻灯片中，DAAR 并未识别所有滥用。任何一款声誉提供程序都不可能识别所有滥用。每一种提供程序对互联网滥用都有自己的理解，不同的 RBL 关注的焦点也各不相同。因此，出于这样一个原因，我们对这些 RBL



进行了合并，试图更全面地了解互联网。请切换到下一张幻灯片。我们经常听到有人询问：为什么在垃圾邮件域中进行报告？在海得拉巴公告中，GAC 表达了对垃圾邮件相关信息的关注。从我们的角度而言，大部分垃圾邮件通过非法或欺骗方式发送，通常是僵尸网络。鉴于不再通过电子邮件与内容特别关联，出现了垃圾链接，还有垃圾推文。Facebook 及其他一些消息系统中也存在垃圾邮件。实际上，大部分其他安全威胁主要通过垃圾邮件传播。GAC 在北京会议公报中曾指出相关问题。您可以将垃圾邮件视作云服务，以及为客户提供域名注册服务的雪崩僵尸网络，以便切实简化垃圾邮件传播。在 DAAR 中，我们使用垃圾邮件正文中发现的域名。用户需要单击域名，才能触发恶意软件下载或类似威胁。最重要的是，垃圾邮件域表示会广泛或综合影响安全管理员或电子邮件管理员应用筛选。人们通常会发现，系统管理员首先关注垃圾邮件，因为这是域受损的一个有效标志。请切换到下一张幻灯片。下一张幻灯片。目前，DAAR 系统仍在创建之中。内部使用已有一段时间了。我们并未对外发布 DAAR 生成的报告；相反，我们希望保证一切妥当后再予以推出。因此，我们组织外部第三方独立审核 DAAR 用来收集数据的方法。这些审核就像昨日刚刚完成一样。过几天还会进行第二次审核。我们会直接将这些报告传输至社群，如果提供的报告暗示任何变化，我们势必会做出相关调整。我们的目标在于提取这些审核结果，将它们发送给 SSAC，要求 SSAC 就 DAAR 使用特定方法应该执行的操作发表意见，但现阶段，大家会发现内部报告和图形还仅限内部使



用。应该发布这些报告，现阶段的目标在于开始面向社群发布这些内容，以便开展与 DNS 滥用政策有关的讨论，为巴拿马城会议做好准备。在这张幻灯片中，大家可以看到，随着时间的推移，各通用顶级域至少报告一个滥用域，不同颜色表示不同时段报告的滥用的变化趋势。显而易见，迄今为止垃圾邮件仍在报告中遥遥领先，但不乏网络钓鱼、恶意软件和僵尸网络的身影。在 DAAR 系统或 OCTO 中，我们一直提取 DAAR 生成的数据并执行这些气泡图。如果有动画，大家将会发现威胁随时间不断增减的动态画面。事实上，如果是董事会成员，其实还会显示一些有趣的 LAVA 指示灯。这是为了展示网络钓鱼域滥用。通常，一些较大的域往往为相对狭窄的区域服务。请切换到下一张幻灯片。大家想必已经开始发现一些不诚信的提供商。数据将超出正规统计范畴，未来我们计划公布提供商名称，使人们对滥用程度较高的注册管理机构和注册服务机构有所了解。显然，垃圾邮件变得越来越有趣，不同时段对比查看尤其明显。这些起泡升起又落下。左右滑动，这种显示模式极为有趣，提供了一些有趣的信息，综合反映所谓的滥用阻止场景，人们可以在这里查看多家及一家注册管理机构的变化趋势。请切换到下一张幻灯片。这张幻灯片展示了旧通用顶级域和新通用顶级域中的解析域百分比。大家可以看到，旧通用顶级域仍然显示数字序列，而新通用顶级域则显示垃圾邮件、滥用及注册数总计。请切换到下一张幻灯片。域滥用比例。DAAR 中列出了域滥用比例。同样，随着新通用顶级域的减少，旧通用顶级域有所增加。关键在于，DAAR 为热衷滥用的

用户提供了海量数据，只需坐在这里就能全面掌握动态。我的团队可以本着娱乐的态度进行最有效地了解。大家一定不希望这些人深夜流落街头！请切换到下一张幻灯片。滥用的核心焦点是什么？这些统计信息表明，大部分滥用由相对少量的域造成。这曾一度被人们引为笑谈。DAAR 为我们提供了具体数据，切实展示相关状况。切换到上一张幻灯片。项目状态。请切换到下一张幻灯片。正如我刚刚所说，我们的工作重点是求稳，而不是一味追求速度。我们提到过，即将发布审核报告，启动收集系统 RBL，保证相对一致的使用，进而确保及时灵活更新。第二版正在开发当中。我们希望自动完成大量报告流程，以便尽量减少人工作业，确保及时交付成果。期待实现精细归因，未来还将推行另外一些措施。请切换到下一张幻灯片。就是这样。关于 DAAR，我们发现有一个问题十分棘手：在收集注册服务机构信息时，函数仅限于用户身份和流量限制，现在我们不太确定会不会对注册服务机构相关数据丧失足够的信息，以致无法满怀信心地在第一版中发布。但愿未来版本不需要确切考虑如何有效收集注册服务机构数据。我就讲到这里，下面再次有请法比恩 (Fabien) 发言。如果有任何问题，我很乐意尽量解答。

卡特兰·鲍尔·布尔斯特：谢谢戴维所做的精彩演示，我要说明的是，ICANN 十分愿意参与此项工作。我认为，政策制定工作至关重要，因为这样可以精确剖析值得关注的政策制定细节问题，以及可能需要对哪些

---

程序环节做出调整或改进，从而应对愈演愈烈的系统和滥用问题。我认为，掌握需要落实的工作很有趣。想想看，在部署这项举措之前，是否需要实际发布滥用信息，包括特定域、注册管理机构、注册服务机构及其他机构？

戴维·康纳德：

我刚刚说过，在根据我们了解的数据发布名称之前，需要重点实施外部独立第三方审核，验证确认我们并未利用这些数据对您或者第三方做出任何无聊或愚蠢的行为，尽量降低人们收到误报的概率，将用于错误归类为 DNS 滥用源，试图为社群提供某种程度的自信，使他们认定我们提供的信息对您有利，完全可以提供一定的具体数据驱动信息促进制定政策。正如我刚刚所说，我们是完成这项工作的独立审查机构之一。第二版有望于几周后完成，一旦最终完成，我们将发布这些报告。至此，全面启动生成报告和发布报告的过程，使大家全面掌握统计数据，以及这些统计数据的影响因素。

卡特兰·鲍尔·布尔斯特：你刚刚提到了一个术语“流量限制”，我不太确定大家是否了解它的含义，希望可以简单解释一下。

戴维·康纳德：

当然可以。任何一类网络服务都可能受到 DAAR 或服务攻击。在攻击过程中，必然会在系统未做出反应前快速建立连接，因

而网络运营商和服务运营商通常会设置限制，主要通过减少可能发生的连接数来遏制滥用。在注册管理机构和注册服务机构中，事实上据我所知，所有注册管理机构和注册服务机构都设置了流量限制，尝试减少通过数据库获取联系信息的用户数，防止利用这些联系信息生成垃圾邮件及其他攻击向量。但是，这种做法有一个副作用：如果研究人员尝试收集信息，将域名与注册服务机构关联，则意味着必须取消相关流量限制。在某些情况下，这些流量限制相当极端，比方说，每小时只能提交 5 项查询或者类似限制。提供流量限制的原理完全合理，即确立谨慎的网络运营机制。如果可以通过某种方式将经过认证或认可的研究人员添加至白名单，避免他们受到流量限制的困扰，但现阶段我们仍在努力克服这一障碍。

卡特兰·鲍尔·布尔斯特：非常感谢，戴维。我是卡特兰。我想强调一下个人问责制问题。据我所知，人们对于特定注册服务机构始终有一项投诉：从外交角度而言，注册服务机构总是面临大量滥用，简直不成比例。我明白，这项投诉的一个方面在于，投诉根据 2017 年 1 月开始统计的一份 SADAG 报告做出。这份报告并非依靠最新数据做出，而这也是 DAAR 报告的价值所在，因为它不仅可以用于分析当前的滥用状况，还能够用于执行持续分析。它开发了特定的要素，实现某种程度的透明度，最终还有望为合规工作提供支持。我们十分感谢大家所付出的努力，我们将争分夺

---

秒地开展工作。在结束本次会议之前，有没有人要做最后的提问？

劳伦·卡宾： 我还有最后一个问题：我认为这款工具很棒，当然大家必然注意到 WHOIS 系统的潜在变化。我想知道情况究竟如何，还有您认为这可能会对 DAAR 举措造成怎样的影响。

戴维·康纳德： 幸运的是，DAAR 系统并未使用个人身份信息。ICANN 在处理相关信息时，仅在 DAAR 报告中利用至少与报告相关的信息，我们要生成的信息是与域名相关的注册服务机构信息。如果要深入剖析并尝试理解特定攻击向量或类似要素，其他各类信息也会有所帮助。但是，为了生成报告，其实只需要考量注册服务机构信息。理论上是这样的。至少，应该通过公共 WHOIS 提供相关信息，不需要限制访问，因为全体人员都清楚正在开展持续讨论，最终需要公开的信息仍未确定。

劳伦·卡宾： 以上就是...举措实施情况。这势必会为社群带来巨大的优势，我知道仍在开展大量工作，因此我们十分感激。这部分 PSWG 讨论即将结束，讨论成果将纳入工作计划，然后再由 ICANN 整合至特定举措。一旦发生 DNS 滥用，将可据此执行分析并向广大社群成员通报趋势，进而推动政策制定工作。本部分讨

---

论到此结束，下面继续讨论下一项议题。下一项议题是 WHOIS 和 GDPR。下面有请 GAC 领导。

[听力文稿结束]