ICANN84 | 年度大会 – GAC 关于 DNS 滥用问题缓和的讨论
2025 年 10 月 28 日（星期二） – 13:15 - 14:30（爱尔兰标准时间）

茱莉亚 • 莎弗琳 (JULIA CHARVOLEN)：

欢迎参加于世界协调时 10 月 28 日（星期二）13:15 举行的“GAC 关于 DNS 滥用问题缓和的讨论”会议。请注意，本次会议正在进行录音录像，并根据《ICANN 预期行为标准》、《ICANN 社群参与者行为准则》和《ICANN 社群反骚扰政策》开展工作。

本次会议期间，只有在 Zoom 聊天窗口中以适当形式提交的问题或意见才会被大声朗读出来。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。如果各位想发言，请在 Zoom 会议室举手示意；如果您说的是英语以外的其他语言，为便于记录，请记得先说出您的名字和您将使用的语言。发言时请保持合理语速，以便翻译人员能够准确地进行翻译工作。

现在请 GAC 主席尼古拉斯 • 卡巴雷诺发言。谢谢，交给你了。

尼古拉斯 • 卡巴雷诺 (NICOLAS CABALLERO)：

非常感谢茱莉亚。欢迎大家回来开会。希望大家在都柏林这座美丽的城市度过了愉快的午餐时光。现在，我很荣幸地向诸位介绍我们的特邀发言人。他们是来自 DotAsia 的钟宏安 (Edmon Chung)。来自中华台北网络信息中心 (TWNIC) 的余若凡 (Jo-Fan Yu) 女士，希望我没念错你的姓氏。我还没看到麦克德莫特先生。不过我想他很快就会到。非常感谢各位。好了，人差不多到齐了。欢迎各位。不用着急，没关系的。“DNS 滥用问题缓和”是我们 GAC 非常重要的议题，介绍一下这个议题的 GAC 主

题负责人，他们是来自欧盟委员会的玛蒂娜 • 巴伯罗 (Martina Barbero)、来自美国的苏珊 • 查默斯 (Susan Chalmers) 和来自日本的宫本智则先生。再次感谢大家。现在，我把发言权交给宫本。他将为我们详细介绍这个议题的目标、这个议题与 GAC 年度计划的关系等内容。交给你了，宫本。

宫本智则 (TOMONORI MIYAMOTO)：

非常感谢主席先生。欢迎参加 GAC DNS 滥用问题缓和会议。我是来自日本的宫本智则。对，是这张幻灯片。

这是本次会议的议程安排。在进行简要介绍后，将由来自会议主办国的代表德克兰发言。他将向我们介绍爱尔兰在 DNS 滥用缓和方面所付出的努力。然后，我们将回顾 PDP 以及 DNS 滥用方面的最新动态；我们还将介绍在 ICANN 职权范围外，其他相关方为应对 DNS 滥用所开展的工作。接着，若凡和宏安将介绍由 TWNIC 和 DotAsia 主导可信通知者计划 (Trusted Notifier Program)。请切换到下一张幻灯片。

好的，谢谢你。现在由我简要介绍一下 DNS 滥用讨论的一些背景情况。大家都知道，应对 DNS 滥用问题对于 GAC 而言非常重要。据我猜测，参会的许多同事各自所在的国家和地区也都在为了应对这个问题而疲于奔命。此外，这对利益相关方来说也是一个大问题，正如大家在本次 ICANN 会议中看到听到的，多场会议都与 DNS 滥用有关。根据 ICANN 合同以及去年（也就是 2024 年）修订的《注册服务机构协议》(RA) 和《注册服务机构认证协议》(RAA)，通用顶级域 (gTLD) 的注册管理机构和注册服务机构必须对可操作的 DNS 滥用报告做出回应。

需要注意的是，ICANN 定义的 DNS 滥用的范围相当有限。具体而言，包括恶意软件、僵尸网络、网络钓鱼、网址嫁接以及作为传播机制的垃圾邮件。我知道，不同的国家或地区面临着不同的滥用问题，比如[系统]、加密货币诈骗，以及与执法部门合作方面的问题，等等。以日本为例，漫画盗版问题非常猖獗，相关盗版网站每月的访问量通常能达到数亿次。但这些问题都不在 ICANN 的政策范围内。

在这种情况下，正如我们本周早些时候讨论的年度计划中所提到的，GAC 采取了“双管齐下”的应对策略：首先，我们基于 ICANN 当前对 DNS 滥用的定义，持续推进政策工作。为此我们需要关注时间点和进度。我们希望在对新通用顶级域授权之前实施一项新政策。其次，我们将积极开展有关 DNS 滥用缓和的能力建设工作，包括分享最佳实践。这些措施或许有助于在各司法管辖区推进志愿计划，联合更广泛的社群采取各种必要的措施，应对各类 DNS 滥用问题。请切换到下一张幻灯片。

有些人可能还记得这张图表，它说明了相关社群的情况。其中绿色方块显示的是 ICANN 合同的范围，正如我所说，相当有限。范围的定义是[音频不清晰]，只规定了 ICANN 和签约方之间的关系。但这具有很强的合同约束力。因此我们的目标是及时实施有效的措施。换言之，是在对新通用顶级域授权之前。

当然，我们也需要考虑蓝色方框和红色方框中的措施，这涵盖了由注册管理机构、注册服务机构和 ccTLD 运营商组成的更广泛的社群，以及与更广泛合作伙伴的合作。请切换到下一张幻灯片。请切换到下一张幻灯片。非常感谢。

这是我们在推进目前的 PDP 讨论的过程中已经开展的工作。这在 ICANN 的职权范围内。为了实施政策[音频不清晰]，我们讨论了精准界定范围的 PDP。这张幻灯片上显示了一些关键要素。首先，在 2024 年 11 月 - 我想许多人应该记得，我们发布了非正式的报告 - 非正式的研究报告。报告指出了推动 DNS 滥用的一些因素，例如与批量注册有关的免费 API 就是推动滥用的一种因素。而对联系信息进行进一步验证则是有效抑制滥用的一种因素。

在今年 5 月，我们请 NetBeacon 发布了一份关于 DNS 滥用诉讼的 PDP 的白皮书。这张幻灯片显示了该白皮书所建议的五个要素。GAC 根据这些意见，讨论了我们关于启动精准界定范围的 DNS 滥用缓和 PDP 的建议。在上次的 ICANN 布拉格会议上，我们讨论了共识性其他意见、针对批量注册的优先措施以及相关域名检查，以鼓励推进这个流程。我们将稍后在本次会议上深入探讨这一点。请切换到下一张幻灯片。

接下来是会议的第二个议程，由会议主办国代表发言。我们有请来自爱尔兰 .ie ccTLD 运营商的德克兰 • 麦克德莫特先生。他将向我们分享 .ie 在应对非法滥用和技术性滥用方面的经验。感谢你，德克兰。交给你了。

德克兰 • 麦克德莫特 (DECLAN MCDERMOTT)：

谢谢大家！大家好。我叫德克兰。我是 .ie ccTLD 运营商的政策和监管事务经理。我具有政策领域的背景，而并非技术人员。因此我的发言不涉及技术方面的问题。如果各位有关于如何缓和滥用行为的技术问题，我想我不是合适的解答者。不过话说

回来，如果大家真有什么问题，可以在会后找我。即使我无法回答，我也会努力寻找答案。请切换到下一张幻灯片。

.ie 注册管理机构自 2000 年起就负责管理和运营爱尔兰的 .ie 域名。几个月前，我们刚刚庆祝了组织成立 25 周年的纪念日。我想向大家重点强调的一点是：.ie 域名的滥用案件数量非常少，滥用率也极低。数据库中总共只有大约 30 万项域名注册。大多数域名注册人都是自然人。我向我在 NetBeacon 的朋友索取了 .ie 滥用案件数量的简要快照数据。他们提供了最新的完整月的数据，也就是八月份，他们在这个月检测到了一起网络钓鱼案件。

可以看出，无论是滥用率还是滥用次数都非常低。此外，为了更全面地说明情况，我们还参考了 DNS 研究联盟的数据，他们的数据也表明，我们的滥用率约为 0.05%，在过去 365 天内，检测到的滥用案件只有约 100 起。所以我的主要结论是，与其他注册管理机构相比，我们的规模相对较小。我们的滥用率也相对非常低，据我所知，这种情况在 ccTLD 中相当普遍。请切换到下一张幻灯片。

.ie 还有一项独特的需求，我们称之为“与爱尔兰连接”。.ie 域名自创建以来，就旨在供个人或组织连接到爱尔兰的互联网。这主要可归为四类用户。其一，是居住或定居在爱尔兰的个人；其二，是居住在国外的爱尔兰公民；其三，是位于爱尔兰的组织，例如，具有爱尔兰 CRO 编号的组织；其四，是位于爱尔兰境外但可以证明向爱尔兰提供或销售商品和服务的组织。我们的“与爱尔兰连接”需求通常涵盖这四类个人和组织。但根据我的理解，这在某种程度上也不算是独特的需求。我想其

他注册管理机构应该没有类似“与爱尔兰连接”这样的需求。请切换到下一张幻灯片。

谈到滥用问题，我想说的是，.ie 在讨论这个问题时，视角要比 ICANN 对 DNS 滥用的传统定义更广泛一些。在内部，我们将 DNS 滥用分为三个类别。其一，是技术性滥用，包括恶意软件、网络钓鱼、僵尸网络。这比较接近于大多数人所说的 DNS 滥用。其二是内容滥用。这是指内容方面的非法行为，比如欺诈，或者像儿童性虐待材料 (CSAM) 这种令人发指的情况。其三是注册滥用，包括恶意注册等行为。

我想表达的一个主要观点是，定义固然很重要。但在我个人看来，更重要的是，我们应当具备各种不同的措施，能够对不同的情况做出恰当而且适度的响应。举例来说，注册管理机构不宜自行判定某项行为是否构成犯罪、是否违法或是否属于恶意。但如果法官、监管机构或裁决者确定某项行为违法或存在恶意，那么我们就应当采取相应的措施，对此做出必要但适度的响应。请切换到下一张幻灯片。

因此，我非常赞同 ATOM 这个缩写，也就是“采取适当的技术和组织措施”。这张幻灯片非常概括性地介绍了我们 .ie 可采取的各种措施，但并非详尽的清单。再次强调，我坚信，为了应对滥用，既需要组织层面的措施，也需要技术层面的措施。不存在能解决所有问题的灵丹妙药。没有任何单一管控措施能防范所有滥用风险。我们通常将域名暂停或是政府层面的法律法规等措施称之为严厉的手段，就像铁锤一样重重砸下。在需要的时候，它们非常必要。在需要的时候，它们非常有用。但如

果我要做一个鸟屋，却只用锤子这一种工具，那做出的鸟屋肯定十分粗糙。

由此可见，要形成全面的应对之策，就必须具备各种不同的工具和措施的组合。你们中的有些人可能来自网络安全领域或具备网络安全背景，因此对预防性管控、纠正性管控和检测性管控这类概念应该不会陌生。不过，我更喜欢源于公共健康领域的另一种框架。请切换到下一张幻灯片。

在公共健康领域，我们常听到“预防”或“缓解”，指的是通过适当干预，避免群体、生态系统或人类的健康受到不利影响。从根本上来说，预防的核心意义在于：采取必要且适度的干预措施，避免不良后果的发生。这也划分成不同的层次。需要说明的是，尽管这套理论源自公共健康领域，但我发现它已被应用于多个不同的政策领域。

比如预防无家可归问题、环境评估等。而且，在我思考各类措施以及缓和性管控手段时，也倾向于采用这一框架。接下来我们具体谈一下这些不同的层级：首先是一级预防。也就是在问题发展为风险之前，将其消灭于萌芽状态。举例来说，要想避免 60 岁时突发心脏病，就要在 30 岁时坚持运动。要想防止未来发生数据泄露，目前就要在默认配置和设计中融入数据保护机制。

在组织层面，一级预防本质上就是制定并实施完善的政策和治理实践。在政府层面，需要审视当前的立法与监管环境是否有助于实现目标。比方说，如果你的目标是提高网络安全水平，那么现行法律法规是否存在迫使注册服务机构等组织采取不安

全或低安全行动的情况？

如果目标是加强数据保护，那么现行监管措施或政策是否存在迫使组织采取不利于个人数据保护的行动的情况？

因此，归根结底，一级预防的核心在于更广泛更全面地审视监管环境，判断其是否真正有助于推进目标的实现、所采用的工具是否恰当，而非仅仅停留到“应当立法”这样简单思路的层面。

其次是二级预防，更靠近问题本身。它旨在阻止即将发生或处于早期阶段的威胁。在健康领域，它应对的是疾病的早期阶段。当疾病已出现，症状已被检测出来时，通过及时发现问题并快速响应，防止病情进一步恶化。而在其他场景中，比如某个网站遭到入侵并被用于网络钓鱼攻击，是否有相应的系统能够检测到这一情况？是否有相应的流程来应对此类事件？如果遭遇 DDoS 攻击，是否部署了“任播”(Anycast) 之类的管控手段，以阻止迫在眉睫的攻击？

然后是三级预防，针对的是已经发生的情况。例如医院正在遭受勒索软件攻击。相关法律程序已启动。损害已然形成。那么现在要做的就是减损。在这个例子中，要做的就是采取管控措施，纠正目前的情况，或阻止进一步损害的发生。在域名场景中，如果认为有必要而且适度，极端情况下会采取域名关闭或暂停等措施。

最后一个是四级预防，我发现即使是在公共健康领域，这一点也往往被忽视。四级预防的目的是预防不当干预。如果说二级

预防旨在预防“假阴性”；那么四级预防就是预防“假阳性”。这包括以下情形：无需干预时却进行干预；干预方式不适合实际情况；干预措施侵犯基本权利；或是干预根本未触及主要问题。这就需要实施防范机制。例如政策审查、异议申诉机制、监管影响评估等。请切换到下一张幻灯片。

就 .ie 而言，我们强调实施分层次的预防措施。我们不仅有更广泛的政策和实践，还落实了更为具体的技术措施。但我想强调的核心要点是：尽管每项措施功能各异，但它们最终都服务于一个共同的目标：确保 .ie 域名的安全性与可信度。请切换到下一张幻灯片。

接下来我简要介绍一下我们实施的一项协议，这个例子反映了我们与监管机构、政府部门及同行同事之间保持着良好的协作关系。我们所建立的监管机构协议正是这种良好关系的体现。该协议的运作方式如下：如果某监管机构或执法部门发现了一个问题，报告称有人自称建筑师但实际上并不是，而这一行为违反了相关法律。建筑师行业的监管机构会指出，这个名叫 Art Vandelay 的人实际上并非建筑师，因此必须对此采取行动。

我们将启动一项名为“尽职调查审核”的流程，具体包括审核相关请求；明确对方的具体诉求是什么；确认对方是否提供了法律依据；确定对方是否提供了足够信息，以使我们能判定他们的诉求是否必要而且适度；确定他们是否提供了法律规定的必要信息。如果确定这是适度合理的请求，我们通常会通知注册服务机构和注册人。

如果是非紧急情况，我们会给予注册人一定天数来解决问题。同时向他们提供监管机构的联系方式，以便有问题时可与监管机构沟通。因为归根结底，我们不希望自己扮演“法官”的角色：“嗯，这是有害内容，必须删除。”我们更希望扮演“沟通桥梁”的角色：当监管机构发现问题时，我们帮助他们与存在问题的相关注册人联系，并给予注册人整改的机会。

在规定的期限结束后，如果监管机构反馈说仍未得到满意的回复，那么我们会视具体情况采取纠正措施，极端情况下甚至会暂停相关域名。但我想说的是，在几乎所有案例中，注册人通常都会说“哦，我并不知情”，随后迅速完成整改，问题也随之解决。

我想特别说明一点，当发生严重、紧急或极端事态的情况时...我们已明确告知监管机构及执法部门，他们也知道这一点...如果他们需要立即停止某个域名，必须直接联系网络托管提供商。因为我们虽然可以暂停域名，但相关违法内容并未从互联网上删除，如果有人知道 IP 地址，就仍可以访问这些有害内容。所以监管机构和执法部门必须知道，如果他们想要彻底移除互联网上的某些内容，就必须与网络托管提供商合作。

但是，在极为罕见的情况下，据我所知从未发生过，如果他们无法通过上述方式紧急删除某些内容，他们可以联系我们，协商域名层面的处置方案，我们至少可以通过增加访问难度来控制风险。值得庆幸的是，据我所知，截至目前这种情况从未发生过。请切换到下一张幻灯片。

最后，我还想和大家分享一个我个人非常欣赏的来自公共健康领域的框架 - 当我们评估各类可能的工具或干预措施时，这个框架非常有帮助。嗯，非常有用。它来自公共健康领域，叫做“干预阶梯”。从本质上而言，它会梳理政府或组织可采取的各种不同的干预方式，并按“侵入性”程度进行排序。其核心理念是：干预方式的侵入性越强，就越需要充分的正当理由。必须符合“适度”原则。

所以这个阶梯的最底层是“什么也不做”。在爱尔兰，几乎所有的监管影响评估都会将“什么也不做”作为默认选项，要采取的任何其他措施都必须与之进行对比。这意味着政府需要承担举证责任，说明为何必须采取相关措施。往上一层的干预措施是“提供信息”。也就是向公众传递相关信息，例如如何防范 DNS 滥用，如何保护自己免受网络钓鱼攻击。再往上是“提供选择支持”。

比如作为注册管理机构，我们提供注册管理机构锁定或 DNSSEC 等选择，但不会强制人们做出具体选择。接下来是“调整默认选项”，也就是把自己的首选选项定为默认选项。比如，默认情况下，我们不会公开注册人的 WHOIS 个人信息，除非出于某种原因他们明确表示“是的，我希望你这样做”。他们必须明确表示同意这样做。再往上的一层比较接近于行为经济学中的“助推理论”。

这包括激励措施，例如政府希望组织保持比较高的网络安全水平。那么可通过资金支持鼓励组织这样做。与之相反的就是督促手段，比方说，为了提高网络安全水平，对于没有通过 ISO

等机构认证的组织，政府会加大审核力度。接下来是“限制选择”。比方说你可以选择 A、B 或 C，但只能选择其一。

对于欧盟的注册管理机构，必须从 NIS2 核实注册人的信息。具体措施由各成员国自行决定。阶梯的顶层是“完全取消选择”。比方说，如果发现儿童性虐待资料 (CSAM)，必须立即报告，没有选择空间。如果法院下达命令，说你必须对某个域名采取措施，那么你必须照办，没有商量余地。

例如在爱尔兰，法官可以发出“访问阻止令”。我记不住法令的完整内容，但基本精神是，当发生性命攸关的状况时，如果不会过多侵犯互联网用户的基本权利，而且法官认定这是必要和适度的措施，就可以下达这项命令。我记得这项命令的有效期最长只有 28 天。到期后必须重新申请才能延长。

归根结底，所有这些框架设计都旨在确保侵入性最强的“完全取消选择”措施仅适用于最极端的情况。因为即便这些工具或工具的组合有用，但如果不适度地使用，反而可能产生负面效果。请切换到下一张幻灯片。

最后我总结一下自己的发言：要有效缓和 DNS 滥用，单单依靠某种工具是远远不够的。必须结合使用适当的技术和组织措施。干预必须适度。所有干预措施必须是必要而适度的。以 .ie 为例，我们发现监管机构、注册服务机构以及注册管理机构之间开展富有成效的合作，对于应对这些状况非常有帮助。最后强调一点，必须防止过头和不适度的干预。谢谢大家。

宫本智则： 非常感谢你，德克兰，你的发言非常精彩。出于时间关系，大家可以提一到两个问题，有人要提问吗？好吧，我没看到有人举手，那么...等等，我看到孟加拉国代表举手了，请讲。

沙姆斯佐哈 (SHAMSUZZOHA) 博士： 谢谢。我是来自孟加拉国的沙姆斯佐哈。非常非常感谢你的精彩发言[音频不清晰]。看到爱尔兰的 ccTLD 运营开展得如此富有建设性，令人感到非常振奋。我有两个小问题。第一个是关于监管机构协议。听你刚才所说，这个协议基本上是被动响应。也就是等待监管机构提出相关诉求才采取行动。但在主动采取措施以缓和滥用行为方面，比如在注册环节，是否规定了应当审核哪些流程和文件以提前防控风险？此外，对于监管机构主动介入与否，是否存在相关规定？这是我的第一个问题。

第二个问题，为检查干预体系的“适度性”，你们采取哪些措施来判断干预行为是否适度？.ie 注册管理机构是否实施了定期的审核机制？是否存在法定的审核体系？还是说，仅依靠基于诚信的流程或自发的流程？谢谢。

德克兰 • 麦克德莫特： 谢谢。我先回答第二个问题。我们拥有多种不同的政策审核机制。我们设立了一个外部多利益相关方咨询委员会，成员来自各个注册服务机构。爱尔兰政府在该委员会拥有一个常设席位，此外爱尔兰互联网社群中的众多当地组织也积极参与其中。我们通过这个机制审核政策变更，任何重大的政策变更最

终都必须经过政策咨询委员会的审议。他们的作用是确保政策变更不会对任何主体造成不利影响，并且符合 .ie 的价值观。

此外，对于重大政策变更，我们还可以选择启动公共协商流程，过去我们在进行重大政策修改时就曾采取过这种方式。对于你的第一个问题，我认为最终得取决于具体的背景。对于我们 .ie 而言，我们是一家规模较小的注册管理机构。实施主动的内容监管既没有多大的意义，也可能超出我国法律允许的范畴。

归根结底，是否主动介入，要取决于注册管理机构所处的监管环境，找到风险敞口的平衡点。因为从统计数据来看，.ie 实际发生的滥用情况非常少，当然，风险敞口也很低。

宫本智则： 非常感谢你的问题。接下来进入会议的第二个议程，PDP 方面的最新动态[音频不清晰]。交给你了，玛蒂娜。

非常感谢，宫本。我将尽可能快速地介绍这个非常重要的议题，因为我们已经落后于原定的时间安排。请切换到下一张幻灯片。

非常感谢。宫本刚才提到了在布拉格会议上，GAC 发出了一份沟通文件，建议董事会敦促 GNSO 启动精准界定范围的政策制定流程 (PDP) 的准备工作。之后，在九月份，发布了有关 DNS 滥用政策制定流程的初步问题报告。在随后的公共评议环节

中，GAC 提交了回复，我将简要介绍 GAC 在回复中重点强调的几点。

对于尚未阅读该问题报告的同事，需要了解以下内容：报告建议将不受限制的 API、关联域名检查和域名生成算法（也就是 DGA）这三个缺陷作为 DNS 滥用缓和工作的优先议题。报告认为，前两个议题，也就是不受限制的 API 和关联域名检查，适合通过政策工作加以解决，而域名生成算法则未必需要通过政策工作进行处理。

GAC 在回复中表示...请切换到下一张幻灯片...我们可以看到，GAC 支持将不受限制的 API 和关联域名检查这两个议题纳入政策工作的范畴。当然，GAC 始终秉持务实态度，我们会优先选择能最有效、最快速产生成果的方法。此外，GAC 也着重指出，问题报告中还包含其他许多需要解决的缺陷。因为尽管即将启动两项 PDP，有望使 DNS 滥用缓和工作取得重大进展，但遗憾的是，DNS 滥用是一个覆盖范围极广、牵涉方面极多的议题，仅靠这两项 PDP 不足以彻底消除 DNS 滥用问题。

因此，问题报告中指出的其他缺陷也必须得到解决；GAC 特别强调，解决其中某些缺陷尤为关键，具体事项已在 GAC 的回复中列出。我们还强调，GAC 希望参与到 PDP 中，为此，我们需要获得有关工作方法的更多信息。此外，我们提议在现有参与者基础上增设备选参与者，因为 GAC 曾在其他 PDP 流程中这样做过，而且效果不错。我们来看下一张幻灯片。

昨天，GNSO 牵头召开了一场关于潜在 PDP 的社群会议。我想简要介绍一下会上讨论的一些要点。关于 PDP 的结构，参会者

似乎倾向于分设两个 PDP 而非合并为一个，但昨天的讨论并未具体涉及章程和运作机制的细节。部分社群代表还建议重新考虑将域名生成算法作为非 PDP 议题进行处理的决定。有些社群代表希望针对该议题也启动一项 PDP。

针对当前重点关注的两个特定议题，也就是不受限制的 API 和关联域名，会议围绕与不受限制的 API 有关的问题定义展开了一些讨论。在 GAC 以往的意见中以及通常情况下，我们更多地会讲“批量注册”而非“API”；今天晚些时候我们将与安全与稳定咨询委员会 (SSAC) 开会，他们认为，API 只是实现域名批量注册的方式之一。如果我们仅针对 API 问题制定政策，可能无法解决我们期望消除的根本问题。

至于关联域名议题，解决起来相对比较容易，但关键在于把握平衡：既要明确根据哪些特征（如注册人身份、支付方式）执行哪些检查，以确保流程透明；又要允许注册服务机构采取灵活的方法，避免向滥用者泄露规避检测的关键信息。这一点非常重要。我们来看下一张幻灯片。

我将非常简单地说一下，如果这些 PDP 按照现在的情况推进下去，目前处于细化章程阶段，那么 GAC 最有可能基于既往成功经验参与进来。哦，抱歉，看来我得放慢语速了。我本想加快进度以弥补超时情况，但看来不能讲得太快以至于影响理解。在以往的政策制定流程中，有一个行之有效的做法，那就是组建小型团队。大家知道，在政策制定流程中，GAC 通常会派出 1 到 2 名代表；如果章程能按 GAC 的要求进行修改，还可能增设

备选代表，但并非所有 GAC 成员都参与。我们清楚，DNS 滥用对于在座的许多人而言是一个极为重要的议题。

因此，要确保每个有兴趣参与的人都能参与并提出自己的意见，一种可行的方法就是组建小型团队，也可以称之为小组，为 PDP 的工作做好准备，让感兴趣的人可以坐下来就 PDP 与 GAC 代表进行交流。这种模式在注册数据相关的 PDP 中效果显著，我们认为，对于即将启动的这些 PDP，这也是一种可行的方法。请切换到下一张幻灯片。

这是我的最后一张幻灯片，希望我们就此展开一些讨论。我们为大家准备了三个问题。第一个问题：根据今天我们在这场 GAC 会议中的讨论，以及昨天与社群进行的讨论，关于即将启动的 PDP，包括 PDP 的结果和/或议题，是否需要向 GNSO 或更广泛社群重点说明进一步的信息？此外，如果大家有兴趣参与 PDP 相关工作或加入小型团队，也请告知我们 - 了解哪些人有意愿参与这项工作，对我们而言非常重要。

第二个问题，除了 PDP 之外，还需要针对 DNS 滥用开展哪些额外的工作？我们已整理出仍需解决的潜在议题的清单，除了 GAC 公众意见中已提及的内容外，各位是否还有其他需要向社群传达的建议？如果有，现在就是提出来的时候。

最后一个问题是更广泛的开放问题：基于那份初步问题报告，如果大家认为在 DNS 滥用方面还有其他需要讨论的事项，欢迎在此刻提出，任何希望在后续讨论中体现的议题，都可以提出来。尼科，交还给你。

尼古拉斯 • 卡巴雷诺： 再次感谢欧盟委员会代表玛蒂娜做了如此详尽细致的发言。谢谢你。我们非常期待尊敬的 GAC 同事就这三个问题，当然还可以就其他事项，发表看法和意见。有请德国代表发言。

鲁迪 • 诺德 (RUDY NOLDE)： 谢谢。我是德国代表鲁迪 • 诺德。首先，我要感谢各位主题负责人精彩的发言，也感谢各位几个月乃至几年来的全情投入。我们德国代表团认为，DNS 滥用无疑是 ICANN 中的头等大事，我们非常乐意以任何身份参与 GAC 所需的工作，包括在小组中做出贡献，而且我们会在最需要的地方灵活地发挥作用。

关于第二个问题，也就是其他方面的政策缺陷，我认为这更具有普遍性，我希望即将启动的 PDP 能成为未来工作的成功范本。这样我们就能够精准界定议题范围，迅速采取行动。因此，我也希望 GNSO 内部也能达成共识：在攻克这两个议题后，会有更多议题提上处理日程。我们不会采取“等上两年观望一下”的态度，而是会继续成功解决其他议题。

这就是我的两点看法。非常感谢。

尼古拉斯 • 卡巴雷诺： 非常感谢你的建议，德国代表。顺便说一句，我是不是可以认为德国主动请缨解决这个问题的 1A 部分？开个玩笑。谢谢。谢谢德国代表。下面有请印度代表发言，之后是美国代表。印度代表，请发言。

桑托什 • 索廷格尔 (SANTHOSH THOTTINGAL)：

谢谢主席先生。我是桑托什。是的，我们非常有兴趣参与 PDP 工作，我们支持启动精准界定范围的 PDP，主要是解决两个高优先级问题，也就是初步问题报告中指出的不受限制的批量 API 访问和缺少针对关联域名的检查。

基本上可以说，这两个问题是通过大规模自动化注册导致系统性滥用的直接诱因。因此，我们认同 ICANN83 届会议达成的共识性建议，也就是对上述问题采取有针对性的 PDP。谢谢。

尼古拉斯 • 卡巴雷诺：

谢谢。谢谢印度代表。你的意见很好。下面请美国代表发言。

苏珊 • 查默斯：

抱歉。我很乐意补充几点。关于第二个问题，我想起今天早些时候我们与一般会员咨询委员会 (ALAC) 就透明度与报告机制进行的讨论，我们指出，目前合同中并未对签约方的报告要求作出规定。例如，我们要求注册服务机构保留收到的滥用报告记录，但对于保留的滥用报告数量以及应对方式，目前还没有任何公开报告方面的要求。

我提出这一点，是因为在跨社群讨论期间...顺便说一句，这场讨论非常精彩...有人对拟议中关联域名检测 PDP 的合规性提出问题：如何有效地实现合规性。在我看来，如果建立透明度报告机制，将有助于实现合规性，这虽然是技术性干预措施，但无论如何对合规工作具有积极意义。我们已在 GAC 提交的意见中表明，希望从讨论一开始就能参与其中。谢谢。芬恩，交给你了。

尼古拉斯 • 卡巴雷诺： 非常感谢美国代表。下面有请丹麦代表。

芬恩 • 彼得森 (FINN PETERSEN)： 非常感谢。我叫芬恩 • 彼得森，来自丹麦。非常感谢各位的精彩发言。关于第一个问题，这在[音频不清晰]中也提到过，采用“API”的说法可能把范围界定得太小了点，我们过去使用“批量注册”的说法，至少在 GAC 是这样。尽管这是个精准界定范围的 PDP，但也要尝试调查除 IP 外的其他方法。这些方法或许也能纳入这个精准界定范围的 PDP 中，这样我们就不会去解决错误的问题，从而能够更有效地实现成果。

关于另一个问题，也就是域名注册或关联域名问题，我当然理解，如果事先披露要进行的检查，让被检查方可以做好准备，那么实际开展检查工作时就会面临困难。但反过来讲，如果没有明确的检查指南，那么问题来了，合规团队该如何判断相关方是否切实履行了该 PDP 的要求？因此，我认为还有一个问题值得探讨：我们如何才能做到一方面不向不良行为者透露关键信息，另一方面又能为 ICANN 合规团队提供必要工具，使他们在未来能够有效监督该 PDP 的实施情况。

丹麦方面也很乐意作为关联成员的身份 - 无论你们怎么称呼 - 为这项工作做出贡献。谢谢。

尼古拉斯 • 卡巴雷诺： 非常感谢。你的意见很好，丹麦代表。我想这是关于 1A 部分的。对吗，芬恩？非常感谢你。大家仍可以畅所欲言。接下来请欧盟委员会代表发言。

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。首先我想指出，我们在过去几年中已经取得了显著的进展。关于 DNS 滥用问题，我们不能仅仅是开展讨论，而是要携起手来，因为光靠 GAC 自己无法解决这个问题。但作为一个社群，我们已经取得了长足进步，为此我颇感欣慰。

关于第二个问题...因为恐怕我们绕不开第一个问题...欧盟委员会代表已经是主题的负责人之一，我想呼应美国代表苏珊的意见，芬恩也提到了这一点。这并非因为我们有多高明，而是因为早在合同修订阶段，GAC 就已提出透明度问题。我们当时就认为，透明度是一个至关重要的议题，本应在合同修订时就得到解决。我们已将透明度问题视为要优先处理的剩余政策缺陷，并在问题报告中列出。

问题报告中还强调了另外两个要素：一是使用主动预防措施，尼科，报告中提到使用检测算法，想必你听到后会感到很高兴。我们已建议将这个问题作为另一个工作阶段加以推进。二是问题报告中指出，有必要解决注册数据的准确性问题，尤其是验证方面的问题。好消息是，如果我对 GNSO 准确性小组主席的表述理解无误的话，该小组计划将此项工作移交给负责 DNS 滥用的 GNSO 小组，如此一来，围绕这个重要议题的相关活动也将开始。谢谢。

尼古拉斯 • 卡巴雷诺：

非常谢谢欧盟委员会代表的发言。确实，我很高兴听到报告中提到了这个问题，提到了算法，但我也心存担忧，因为请记住，不法分子也知道这些工具。我并不想讨论 ChatGPT、生成

式 AI 或大语言模型 (LLM)。我要讨论的是使用随机森林、聚类分析等技术的精密算法。我们前几天讨论过这个话题。我不打算详述细节，但你是对的。

大家仍可以畅所欲言。出于时间关系，在讨论其他事项之前，我们还可以提一个问题。好的，我看到现场和线上都没人举手。接下来将由苏珊介绍可信通知者计划问题，之后会有个问答环节。苏珊，交给你了。

苏珊 • 查默斯： 谢谢主席先生。接下来我们将稍微转换议题方向。正如我的同事宫本之前提到的，GAC 有关 DNS 滥用问题的战略目标分为两大类。第一类，我们一直在推动 ICANN 内部有关 DNS 滥用的政策工作，目前在这方面，我们鼓励相关 PDP 取得进展。第二类则是能力建设相关工作。

主题联合负责人已着手开展相关工作，还将持续推进，为 GAC 代表提供相关资源，以全面培养在 DNS 滥用问题方面的能力。大家可以看一下报告的第 4.7 节，其中提到的一个想法就是提供有关可信通知者计划的信息。我们来看下一张幻灯片。

这张幻灯片的内容大家可能并不陌生。大家可以看到，可信通知者计划可用于处理 ICANN 合同职权范围之外的 DNS 滥用活动。今天，我们非常荣幸地邀请到了来自 DotAsia 和 TWNIC 的代表，他们远道而来，为我们介绍可信通知者计划。好了，我把发言权交给他们。有请。

钟宏安： 非常感谢苏珊。我是钟宏安。我和若凡商量好了，我先发言，然后由她做介绍。非常感谢邀请我们参加此次会议。这个议题我一直在密切关注。我将简要回顾一下这个问题的历史背景，我认为这部分内容非常重要。

请切换到下一张幻灯片。这张幻灯片的内容可以说是我对这个问题的个人解读，也是对宫本和苏珊所介绍的幻灯片内容的延伸。可以看到，有些 DNS 滥用活动超出了 ICANN 的职权范围。认识到这一点非常重要，因为滥用行为可能在网络的各个环节中发生。正因如此，如果仅将注意力集中在 ICANN 的职权范围内，很可能无法取得令人满意的结果。

请切换到下一张幻灯片。这张幻灯片呈现了另一个视角，我想这和德克兰此前就更广泛的滥用视角所进行的讨论相呼应。大家可以看到，DotAsia 和我们都认为：这个较大的范围是网络滥用，而 DNS 滥用只在其中占一小部分。而真正适合由顶级域注册管理机构处理的，其实只占更小的一部分。这其中有一部分在 ICANN 的职权范围内，另一部分则在 ICANN 的职权范围外，包括儿童性虐待资料 (CSAM) 和其他问题。对于超出 ICANN 职权范围的部分，同样值得关注，而且解决这类问题不一定非要通过 ICANN 的 PDP。

请切换到下一张幻灯片，这是个很好的例子，介绍了我们与 DotKids 的合作。这个计划在上一轮申请期之前启动，当时我们就非常清楚，针对 DotSex 的政策，很可能与应对 DotKids 域名滥用的政策有所不同。这就引出一个重要问题...抱歉，请允许我回过头讲一下。注册管理机构可以将 ICANN 职权范围作为处

理滥用行为的基准线，但不应止步于此。在某些情况下我们必须超越基准线，DotKids 就是个很好的例子。

今天我还想重点强调一点，两年前我们启动 DotKids 时，过去 15 年所建立的 DNS 滥用处理平台与技术确实为我们提供了极大帮助 - 正是依靠这些基础，我们才能进一步采取行动，应对更多滥用行为，甚至建立了监视列表，这一点我稍后还会提到。请切换到下一张幻灯片。

正如我所说，我们在这方面的工作始于 2011 年。大家可能有所不知，当时我们举办了一场有关 DNS 滥用的论坛，那或许是 DotAsia 参与发起的首批相关论坛之一。过去 15 年间，我们在这一领域取得了长足进步。

在最后一张幻灯片中，我将讨论可信通知者。正如我之前提到的，目前我们正致力于超越合同要求采取行动，而我们的切入点是“注册管理机构间协作”模式。因此，我们的可信通知者 - 至少是已正式确定的通知者 - 主要是其他 ccTLD 注册管理机构；未来我们可能还会接纳更多 gTLD 注册管理机构加入。但我想先说明一下，为什么 ccTLD 在其中扮演着至关重要的角色。

之所以选择与注册管理机构合作，主要是因为我们希望各方对域名暂停这一严厉措施保持相似的敏感度。因为注册管理机构有能力暂停域名，但这会产生较大的影响。我们希望不同的注册管理机构能够在这个问题上保持相似的敏感度，这样他们在发现问题后，就会将相关信息传递给我们，以便我们启动“快速暂停”措施。我们已经和 .TW 以及 .UK 和 Nominet 开展了两个试点项目，我们建立了可信的沟通渠道。

这其实非常简单。这是一个使用共享密钥的专用电子邮件渠道，这样我们就能确认发送信息的是可信来源。我们要求对方按照特定形式进行尽职调查，然后我们就能迅速采取行动。以上就是我们正在开展的工作，我们希望以此为基础，邀请更多的 ccTLD 加入我们的计划。我可以简单介绍一下进展。在过去几个月…嗯，在过去一年左右的时间里，我们一直在筹备此事。而在过去几个月，该计划开始投入实际运行，我们已经收到了一些通知。

其中一个原因是…想必大家可能也有所了解，我们发现在实际情况中，有时候网络钓鱼攻击是专门针对特定地区的。例如，如果网络钓鱼攻击专门针对台北，我们的某些监控系统就无法捕捉到攻击，但中华台北的同事可以发现这类攻击，并向我们发送通知，随后我们就能进行处理。这也是我们非常乐于和不同的 ccTLD 开展合作的原因之一：因为从全球范围来看，我们的监控手段和能力有限，可能会遗漏一些针对特定地理位置的网络钓鱼攻击或其他攻击。

借此机会，我想强调的是，我们也在探索其他方面的工作，同样是在 ICANN 的职权范围之外。我们从 ICANN 界定的 DNS 滥用入手，然后我们将重点工作放在扩大可信通知者网络方面，以涵盖其他类型的滥用行为。这也是我们邀请其他 ccTLD 与我们合作的原因。通过这些 ccTLD，或许还能与各国的搜索与响应团队建立合作关系。这样一来，我们就能通过 ccTLD，在注册管理机构层面保持对滥用问题的敏感度，同时努力解决 ICANN 职权范围之外的滥用问题。我的介绍就到这里。接下来我是把发言权直接交给若凡，还是苏珊你想要说几句…

苏珊 • 查默斯： 非常感谢宏安。抱歉，我想先稍作补充，请大家谅解。我本该在发言开始前就说明这一点：今天我们邀请到了一位运营通用顶级域 (gTLD) 的注册管理机构的代表；同时还有 TWNIC 的 CEO，该中心负责管理 ccTLD。所以我希望指出这一点。我认为这一点很重要。

若凡，在你开始做介绍之前，我只有一个问题，或许可以稍后作答。但我认为，解释一下是什么样的通知者才称得上可信，或许可以帮助我们理解。谢谢。

余若凡： 谢谢。我是余若凡。大家下午好。感谢你们的邀请。我非常荣幸能在这里做分享，尤其是从 ccTLD 的视角，谈谈我们对可信通知者框架的看法。请切换到下一张幻灯片。就是这一张。

我们为什么需要可信通知者框架？大家都知道，DNS 滥用...我的意思是，[音频不清晰]已经蔓延到全球范围。当然，另一方面，公众对于问责的要求也在不断增长。我认为目前传统的应对方法通常不够迅速，而且还面临司法管辖权方面的障碍。所以，这就是我们需要可信通知者框架的原因。

但我还想从 ccTLD 的角度提出一个重要观点，正如你们从这些数据中看到的那样，实际上，作为 ccTLD，我们经常会从政府机构那里收到有关非法网站的通知。这是我们 2025 年截至 9 月底的数据。从这些数据中可以看到，实际上只有不到 1% 的非法网站采用 .tw 域名。这意味着，超过 99% 的非法网站超出了我们的司法管辖权范围，我们无法对其采取行动。这就是为什么

从 ccTLD 的角度而言，我们认为这个框架非常重要。请切换到下一张幻灯片。

那么，究竟什么是可信通知者框架？我认为这是一个基于信任和预先商定的规则快速采取行动的框架。当然，其目标是更高效、更富有成效地处理滥用问题，尤其是严重的滥用案例。我们还认为，必须将信任、透明和正当程序作为这个框架的核心原则，这一点非常重要。目前，我们通过现行的可信通知者框架，和注册管理机构以及注册服务机构开展合作。

比如宏安所在的 DotAsia，还有 .uk、.kr，以及 gTLD 和一些注册服务机构。除了内容滥用问题，目前我们主要还关注 DNS 滥用问题，特别是网络钓鱼。我们使用 SOP 和协议与合作伙伴进行协商，将信任、透明和正当程序等原则纳入其中。这就是我们目前正在开展的工作。请切换到下一张幻灯片。

在这些幻灯片中大家可以看到，如果没有可信通知者，我们的工作流程是这样的：从政府机构、执法部门、网络安全社群以及我们自己和民众那里获取情报。然后我们进行调查并报告。然后注册管理机构和注册服务机构还要自己再进行一次调查。他们将根据自己的调查结果，采取某种措施，比如封禁或暂停域名。请切换到下一张幻灯片。

而有了可信通知者框架后，流程就简化了：我们完成调查并向注册管理机构或注册服务机构提交报告后，他们可以直接依据和我们预先商定的 SOP 和协议采取行动。无需投入精力进行重复调查。请切换到下一张幻灯片。

在我们看来，这个框架主要有三个优点：首先，当然是创建了一个框架，有助于加速获取威胁情报和处理滥用问题。其次，它减轻了注册管理机构和注册服务机构的调查负担。第三点，我们认为也非常重要，那就是我们可以更主动地采取行动，因为大家知道，网络钓鱼攻击可能只存在几天时间。所以，如果可以更快地采取行动，获得更可靠的威胁情报，我们就能够在事态升级之前采取行动。请切换到下一张幻灯片。

我还想分享一下 TWNIC 2025 年的数据概览。截至目前，也就是今年到现在，我们在 2025 年总共处理了 51 个域名。我们预计数量会更多，因为我们今年下半年才开始与合作伙伴进行合作。所以我们预计明年数量会更多。其中 78% 被确认为网络钓鱼，我们的合作伙伴采取了相应措施。

此外，目前响应时间总体上少于两天。通常是一到两天。但我们也认为可通过自动化来加快处理过程。还有一个好消息，到目前为止我们没有收到任何申诉。这或许说明我们的处理结果是比较可靠的。请切换到下一张幻灯片。请切换到下一张幻灯片。谢谢。

那么，我们面临哪些挑战呢？因为各个注册管理机构和注册服务机构采用不同的标准，所以我们依赖于双边协议。这会在框架扩展方面造成问题。但我认为，如果我们下一步打算继续扩大可信通知者的合作关系，我们还可以开发并展示一种非监管模式，也许对于行业合作而言会是一种成功的模式。我们也希望与 ICANN 和 GAC 的 DNS 滥用缓和最佳实践保持一致。请切换到下一张幻灯片。

我们认为可信通知者框架是履行互联网社群共同责任的关键一步。所以我们也鼓励 GAC 的代表敦促你们的 ccTLD 考虑、了解并加入这个框架。如果你们有问题或感兴趣，欢迎和我们联系。谢谢。

苏珊 • 查默斯： 非常感谢若凡和宏安的精彩发言。现在我们看看 GAC 代表有没有问题。我看到 WIPO 代表举手了，请讲。

布莱恩 • 贝克汉姆 (Brian Beckham) 非常感谢苏珊。谢谢若凡。我是布莱恩 • 贝克汉姆，来自世界知识产权组织 (WIPO)。我对于你最后一张幻灯片上的第一点有个问题，是关于注册管理机构和注册服务机构可能采用不同的标准以及框架扩展。我想知道，如果考虑建立一个标准化的框架来解决这个问题是否有用，这样可信通知者或许能将他们在某一环境中经过审查的信息更广泛地用于整个生态系统。

余若凡： 是的。谢谢你提出这个非常好的问题。我也这么认为，如果我们有一个平台，特别是技术平台，用于进行这种协商或信息交流，那确实非常有帮助。但我觉得目前的困难首先在于，社群对这个问题的认知程度。据我们所知，尽管认知程度在不断提高，但仍处于相当低的水平。所以，社群如何制定有关情报共享与行动措施的标准，仍是需要解决的另一个问题。

尼古拉斯 • 卡巴雷诺： 非常感谢。宏安，想回答这个问题吗？好，请讲。

钟宏安： 是的。我是钟宏安，简单补充一下。简单来说，答案当然是肯定的。实际上，DotAsia 正在与 .tw 密切合作，规范所提供的证据材料的格式，以便我们能够加快任何形式的暂停措施。我们还与 CleanDNS 和 NetBeacon 等组织合作，尝试至少达成一种事实上的标准或行业标准，不一定是非常严格的标准。

尼古拉斯 • 卡巴雷诺： 非常感谢宏安。接下来请日本代表发言。

宫本智则： 非常感谢你的精彩发言。我想问的是，也许你们已经在最后一张幻灯片中介绍了：你们对我们有什么期望呢？我的意思是，我们、GAC 成员或者各个国家或地区的政府机构可以如何协助你们实施项目？谢谢。

钟宏安： 我是钟宏安。是的，我们鼓励你们的 ccTLD 加入进来。正如我刚才提到的，目前我们优先考虑注册管理机构，这是因为顶级域注册管理机构在处理域名暂停通知时，需要对措施的适度性保持高度敏感。所以，我希望 GAC 成员能鼓励你们的 ccTLD 加入我们的网络。

余若凡： 是的，我认为 ccTLD 确实能够起到非常重要的作用。所以，我认为，如果 GAC 代表能够帮助社群提高认知水平，并鼓励他们加入，我觉得会非常有帮助。谢谢。

尼古拉斯 • 卡巴雷诺： 非常感谢日本代表。在我把发言权交给美国代表讨论公报相关事宜之前，我们还有最后五分钟时间，大家还有其他意见或问题吗？有请哥伦比亚代表发言。

蒂亚戈 • 达尔-托易 (THIAGO DAL-TOE)： 非常感谢。非常感谢你的发言。我的问题正与此有关。基本上，在国家层面，我们不必设立自己的可信通知者计划，实际上我们可以加入其他现有的计划。如果是这样，我们该如何加入呢？加入的流程是怎样的？此类申请的接受流程又是怎样的？谢谢。

钟宏安： 我是钟宏安。目前，我们采用双边协议的方式，因为每个 ccTLD 可能都有略微不同的要求。哦，我忘了说一点，除了相互通知之外，我们还共享数据。我们基本上按季度分享。我们与 .tw 共享有关域名暂停的数据，也从对方获得此类数据。但有些安排可能不包括这部分内容。

所以目前，我们与其他 ccTLD 之间签订双边谅解备忘录 (MOU) 协议。至于是否需要系统等问题，正如我所说，我们的沟通渠

道非常简单，就是使用交换密钥的可信电子邮件。但在后台，我们有自己的系统。ccTLD 自己决定是否需要后端系统。

尼古拉斯 • 卡巴雷诺： 宏安，我想简单追问一下。你们是如何共享数据的？采用什么数据格式？是采用 CSV，也就是逗号分隔值格式？还是开放文档格式 (ODF)？是哪种...？

钟宏安： 是的，我们就采用 CSV 格式，用于说明被暂停的域名以及暂停原因的简单代码。

尼古拉斯 • 卡巴雷诺： 非常感谢。苏珊，下面请你发言。

苏珊 • 查默斯： 谢谢主席先生。只剩下几分钟了，我们可以进入最后一项议程了吗？GAC 成员可能已经看到，我们分发了一些关于公报相关事宜的文本，旨在鼓励大家为都柏林会议上关于 DNS 滥用问题的公报提供思路。目前，主题联合负责人没有什么建议。我们对布拉格会议上提出的建议以及自那以后社群在这方面所取得的进展感到非常满意。

所以，我们正在考虑以下重要事项，我就不一一念了，大家可以在屏幕上看到。如果有人想为重点议题部分补充建议，非常欢迎提出。我们目前正在撰写草案文本。请大家畅所欲言。

尼古拉斯 • 卡巴雷诺： 非常感谢美国代表。正如苏珊所说，现在仍可以发言。如果大家有任何想法，我们一如既往地欢迎所有好的建议。在会议结束之前，大家还有什么要补充的吗？线上和会议室中都没有人请求发言，这意味着我们基本上达成一致意见。

非常感谢。我们不需要延长时间。虽然我们还有两分钟，但不需要延长会议时间了。非常感谢大家。随后是茶歇时间。茶歇时间为 30 分钟。请务必在下午 03:00 准时回到会议室。非常感谢。

[听写文稿结束]