ICANN72 | 虚拟年度大会 - 新生代计划学员讲演会
2021 年 10 月 25 日（星期一） – 10:30 - 12:00（太平洋夏令时）

黛博拉 • 艾斯卡勒拉 (DEBORAH ESCALERA)：大家好，欢迎来到 ICANN72 新生代计划学员讲演会。我是黛博拉 • 艾斯卡勒拉，负责管理 ICANN 新生代计划。我是本次会议的远程参会经理。

请注意，本次会议会被录音，并根据 ICANN 预期行为标准开展工作。在会议期间，只有在问答窗口内提交的问题或意见才会被大声朗读出来。我会在由会议主席或主持人规定的时间内大声朗读这些问题或意见。

本次会议的翻译服务将涵盖英语、法语和西班牙语。请点击“口译”图标，然后选择收听会议时使用的语言。

如果想要发言，请在 Zoom 会议室举手示意，当会议主持人叫到您的名字后，我们的技术支持人员将允许您启用麦克风发言。

在发言之前，请确保您已经从“口译”菜单中选择发言时要使用的语言。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。在发言时，请确保其他所有设备和通知提醒均保持静音。同时，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。

所有参会者都可以在聊天窗口中发表意见。要允许所有人查看您发表的意见，请使用聊天窗口中的下拉菜单，并选择“回复所有小组成员和参会者”。请注意，在 Zoom 网络研讨会中，只有小组成员之间可以进行私聊。由一位小组成员或标准参会者发送给另一位标

准参会者的聊天消息只有会议联合主持人、主持人和其他小组成员能看到。

在此，我要由衷欢迎各位参加本次会议，并感谢新生代计划参与者为准备讲演所付出的辛勤努力。我还要感谢我的两位导师，阿里斯 • 伊格纳西奥 (Aris Ignacio) 和德萨莱尼 • 耶瓦拉 (Dessalegn Yehuala)，感谢他们在过去的八周内孜孜不倦地为学员们提供辅导和指导，帮助他们为 ICANN72 做好准备。没有他们的付出，我自己一个人不可能走到今天。

此外，我要感谢我的同事西兰努什 • 瓦尔达尼扬 (Siranush Vardanyan)，他今天负责放映幻灯片。西兰努什，非常感谢你的帮助。本次会议只有 90 分钟，而一共有六个讲演，所以，我们马上开始吧。下面有请第一位讲演者，萨拉 • 阿尔萨曼 (Sarah Alsamman)。萨拉，请开始讲演，在你结束后，我们将提问。

萨拉 • 阿尔萨曼： 大家好。非常感谢黛博拉，感谢您邀请我做讲演。今天我想谈谈 DNS 和网络内容滥用问题，更具体地来说，应该是虚假信息问题。请切换到下一张幻灯片。

首先，简单介绍一下域名系统 (DNS)，DNS 是一个不可或缺的系统，互联网需要该系统才能连接用户和设备。然而，正如其他系统一样，它也容易被滥用。正如 ICANN 的政府咨询委员会 (GAC) 所言，若要使公众信任并依赖互联网开展通信和交易，DNS 基础设施管理当局必须采取措施，

保障此类公共资源安全可靠。因此，在本次演讲中，我想要呼吁利益相关方就这一重要的公共政策问题展开对话，并呼吁整个 ICANN 社群继续打击 DNS 滥用行为和与 DNS 相关的滥用行为。

要使 DNS 滥用问题得到妥善解决，注册服务机构和注册管理机构需要就如何定义 DNS 滥用达成共识。请切换到下一张幻灯片。根据互联网与管辖权政策网络组织制定的 DNS 滥用框架，目前已经确定了五大滥用形式，分别是恶意软件、僵尸网络、网络钓鱼、网址嫁接和垃圾邮件。

除此之外，还存在内容滥用的情况，但这不属于技术型的，因此需要进行单独区分。为了保护言论自由权，注册管理机构和注册服务机构通常不需要对网络内容滥用采取行动。然而，按照 GAC 框架，在某些特定情况下，应对网络内容滥用采取行动，这些情况包括发布儿童性虐待刊物、在线传播非法阿片类药物的信息、传播人口贩运信息以及发布煽动暴力行为的具体可信内容。请切换到下一张幻灯片。

在定义了 DNS 滥用中的内容滥用后，我想介绍一下在社交媒体上运行僵尸网络的问题。我相信，大家现在都能观察到，数据处理算法正日益成为可影响我们的认知，进而影响现实的强大工具。其中最常见的是被政客利用的僵尸程序，它们能够在我们每天使用的主要社交网络平台上操纵公众舆论。

僵尸网络引导公共问题构建的能力可以直接影响我们对社会和政治现实的认知，从而影响现实秩序。僵尸网络的这种能力最常应用于计算宣传，有研究表明，正如我将在下一张幻灯片中介绍的一项研

究，在危机期间或之后，很有可能会出现计算宣传，用于传播虚假或误导性信息，从而造成曲解和更大的危害。

危机时刻会让公众集体产生不确定性，因而导致社交媒体网络上的受众变得极易被影响和操纵。请切换到下一张幻灯片。

在曼彻斯特恐怖爆炸事件之后，《英国社会学期刊》针对 Twitter 和 Facebook 中的消息和言论做了一项研究。在一个案例中，一位女士通过其 Facebook 帐户发帖称她收留了 60 多名失踪儿童，并附上了她的电话号码，这篇帖子迅速在 Twitter 上传播开来。由于这篇帖子的传播范围很广，最终这位女士被《每日邮报》誉为“曼彻斯特天使”。

但问题是这件事情纯属捏造。这就是我们所说的“幽灵事件”。这位女士后来向警方解释说，她从未发帖，也没有公布她的电话号码，并声称她对这一事件感到非常震惊，因为她一晚上接到了无数电话。同一天晚上发生了 28 起类似的幽灵事件，加剧了此次恐怖爆炸事件之后的混乱。请切换到下一张幻灯片。

另一个事例是，同天晚上有一个 Facebook 帖子称在奥尔德姆医院有一名持枪者，而且医院的人都被困在里面。这个帖子是在爆炸发生后不久发布的，在 Facebook 截图流出后，至少有 368 个 Twitter 帐户分享了这个帖子。虽然医院否认了这一谣言，但是这一虚假信息仍在恐怖袭击后的关键恢复时段内继续传播。

由于这一特定的幽灵事件，一些紧急救援人员不得不根据这样的虚假线索去行动。这种情况可能会变得非常危险，原因是，当社交网络上的虚假信息可以扰乱紧急救援服务机构与公众之间的沟通时，社区安全会受到严重影响。请切换到下一张幻灯片。

所以，显而易见，网站内容滥用会对个人生命和社会安全造成威胁，因此应在今后探讨应对政策。为在今后确保互联网及其用户群体的安全，应采取行动，鼓励在新的或正在制定的《注册管理机构协议》条款中纳入积极主动的反滥用措施。谢谢！

黛博拉 • 艾斯卡勒拉： 谢谢萨拉。非常棒的讲演。有要向萨拉提问的吗？我没看到有人举手。如果大家有疑问，也可以在会议结束时提问。下面，有请下一位讲演者，梅里 • 巴达萨扬 (Meri Baghdasaryan)。谢谢！

梅里 • 巴达萨扬： 谢谢黛博拉和西兰努什。各位上午、下午和晚上好。我是梅里 • 巴达萨扬，是刚从宾夕法尼亚大学法学院毕业的法学硕士。出于对 ICANN 隐私和政策制定工作的浓烈兴趣，我确定了今日讲演的主题，即隐私和代理服务认证。请切换到下一张幻灯片。

2013 年，ICANN 董事会批准了新的《注册服务机构认证协议》，即 RAA，这是一份用于管理 ICANN 与其认证的注册服务机构之间的关系的合同。正如我们所见，RAA 中的条款对注册人和域名系统中涉及的其他第三方有重大影响。

在 ICANN 与注册服务机构利益相关方团体于 2011 年 10 月启动 RAA 谈判时，ICANN 董事会还请求 GNSO 在谈判结束后提交一份问题报告，而且，为处理谈判中未解决的问题，GNSO 启动了政策制定流程。当时，与隐私和代理服务相关的问题被确定为未决问题之一。

2013 年的《注册服务机构认证协议》实际上包含一个临时规范，其中涵盖了注册服务机构在隐私和代理服务方面的义务。该临时规范

的截止日期已经延长了几次，当前的截止日期为2022年7月31日或ICANN实施新的认证计划之时，以先发生者为准。

在继续讲述后面的内容之前，我们需要了解什么是隐私和代理服务。隐私和代理服务是在上面提及的临时规范中定义的。隐私服务允许以注册人的姓名进行域名注册，但公开可用的注册数据目录服务中显示的所有其他联系信息实际上不是由隐私服务提供商提供，也不是由注册人提供。

在存在代理服务的情况下，该服务允许注册域名持有人许可实际使用域名的客户使用域名，并且注册数据目录中的联系信息由代理服务提供商提供。请切换到下一张幻灯片。

根据现行的临时规范，我们有一系列适用于隐私和代理服务的最低要求。四个主要的最低要求包括：披露主要服务条款、公布侵权/滥用问题联系人、公布业务联系人信息以及托管客户数据。正如我们所见，临时规范旨在管理非公开注册数据的处理。请切换到下一张幻灯片。

但是，我们为什么要讨论这个主题呢？这个主题为何如此重要？如果我们回到2011年，当时，ICANN董事会在请求GNSO提交问题报告时，就强调了有必要尽快解决隐私和代理服务问题，以便为注册人提供更有力的保护，并减少DNS滥用。

在这之后，隐私和代理服务问题实际上变得更加持久，甚至在疫情期间有所加剧。例如，在关于DNS滥用问题的ICANN68 GAC会议中，与会者指出，在疫情期间，用于进行诈骗的65%的域名都是通过隐私和代理服务隐藏的。此外，一些执业律师还发出警告，在GDPR生效后，世界知识产权组织(WIPO)收到的关于DNS滥用的UDRP投

诉数量大幅增加，其中大多数投诉涉及的问题都是隐私和代理服务提供商持续不遵守披露联系信息的规定。注册服务机构或其附属代理服务提供商要求知识产权持有人必须提起 UDRP 诉讼或获得法院传票，才能接收 DNS 滥用者的联系信息。

这显然引起了许多不必要的麻烦，比如需要更多的时间来完成简单的程序，以及花费更多的资源来获取联系信息以推进投诉程序。这也意味着，认证将有助于切实加强注册人保护，进而减少 DNS 滥用，并减少 UDRP 投诉数量。现在，让我们回顾 ICANN 董事会向 GNSO 提出的问题报告请求，并讨论在那之后发生了什么。请切换到下一张幻灯片。

这张幻灯片概要介绍了 GNSO 政策制定流程，也即 PDP。在董事会于 2013 年批准《注册服务机构认证协议》后，GNSO 于同年晚些时候启动了 PDP 并成立了一个工作组。

此 PDP 工作组提出的政策建议于 2016 年 1 月由 GNSO 理事会通过，随后于 2016 年 8 月由 ICANN 董事会通过。在这之后，董事会指示 ICANN 组织实施这些建议。请切换到下一张幻灯片。

正如我们在这张幻灯片中所看到的，新的认证计划实际上包含比我们之前讨论的临时规范更细致的要求。根据在幻灯片中看到的内容，新的认证计划显然旨在解决我们刚才讨论的与隐私和代理服务相关的问题。

例如，新的认证计划为服务提供商响应执法机构和知识产权持有人的请求提供了一个详细的框架，此外，它规范了服务提供商将来自第三方的通信转发给隐私和代理服务客户时所需遵循的要求，它甚至提供了一个强制性的服务提供商培训计划。

因此，正如我们所见，新的认证计划力图解决现行规范存在的问题，进而提供一个更加透明、更加合理的认证框架。请切换到下一张幻灯片。

正如我之前提到的，在 GNSO 理事会通过工作组提出的建议后，ICANN 董事会批准了这些建议，并将其发送给 ICANN 组织进行实施。按照预期，新的认证计划将取代《注册服务机构认证协议》中的临时规范。然而，由于 ICANN 当前正努力使现有的数据保护实践符合欧盟的《通用数据保护条例》，该计划的实施工作目前处于搁置状态。

如果大家还记得的话，2018 年 7 月，在 ICANN 董事会决定采纳 gTLD 注册数据临时规范后，GNSO 理事会发起并确立了快速政策制定流程 (EPDP)，这是 ICANN 历史上的第一个 EPDP。

随后，GNSO 理事会于 2019 年 3 月通过了一份报告，这是工作组关于 EPDP 第一阶段工作的第一份报告，该报告中共提出了 29 项建议，其中有 27 项建议后来得到了 ICANN 董事会的批准。然而，根据第一阶段工作报告中的建议 27，考虑到 ICANN 在增强 GDPR 合规性方面所开展的工作和取得的最新进展，显然有必要重新审视所有与非公开注册数据相关的实践。

正因为如此，新的认证计划目前仍处于搁置状态，等待社群反馈和审核意见，如果我们认真思考一下，便会发现 EPDP 和认证计划建议从本质上讲都是为了实现同一个目标，即确定一个合法机制以规范非公开注册数据的访问和处理。请切换到下一张幻灯片。在恢复认证计划的实施工作后，预计将就一些事项征询社群反馈意见。请切换到下一张幻灯片。

具体而言，将就以下事项征询社群反馈意见：隐私和代理服务认证政策，协议，认证项目和申请人指导手册，以及中止、取消认证和过渡程序。总而言之，隐私和代理服务认证是一个重要事项，且已通过 ICANN 政策制定流程加以处理并取得了一定进展。但是，作为 ICANN 为实现 GDPR 合规这一大目标而开展的多方面工作的一部分，认证计划的实施工作目前被搁置了，不过，这是有必要的，因为根据 EPDP 的建议，协调围绕实现 GDPR 合规这一大目标而开展的各个项目，让各方面的工作相辅相成至关重要。

不论如何，认证计划比现行的规范更为细致，这一点毋庸置疑。不过，隐私和代理服务存在的深层问题似乎并没有消失，而且，正如我之前提到的那样，这些问题在疫情期间甚至有所加剧。因此，考虑到新的认证计划的重要性，我希望能够尽快实施该计划，以解决这些深层问题。非常感谢，我很期待可以在 ICANN72 会议期间加深对这个主题和其他主题的了解。谢谢！

黛博拉 • 艾斯卡勒拉： 谢谢梅里。似乎有人在聊天窗口中提出了一个问题。问题是，“在当前所讨论的主题背景下，你能稍微解释一下数据托管吗？”

梅里 • 巴达萨扬： 可以。数据托管实际上是一个比较大的话题，解释起来需要比较长的时间，但是为了不占用太多讨论时间，我长话短说。简单来说，数据托管是关于隐私和代理服务提供商将如何处理来自执法部门或知识产权持有人的请求，以及他们如何保存和处理隐私和代理服务所持有的数据。这只是一个简短的回答，如果可以的话，我可以在聊天窗口中键入比较完整的说明。

黛博拉 • 艾斯卡勒拉： 当然可以。非常感谢。大家还有其他问题吗？好的，请大家关注聊天窗口。非常感谢。非常棒的讲演。下面，有请下一位讲演者，赛 • 常德拉瑟卡兰 (Sai Chandrasekaran)。赛，请开始你的讲演。

赛 • 常德拉瑟卡兰： 谢谢黛博拉和西兰努什。我是赛 • 常德拉瑟卡兰，今天我的讲演主题是我个人在研究中最感兴趣的一个主题，即内容审核。

具体而言，我今天将探讨内容审核带来的挑战、内容审核带来的隐私风险，以及如何解决如此复杂的问题。请切换到下一张幻灯片。

我先快速做一下自我介绍。我是印第安纳大学网络安全专业的研究生，在过去几个月内，我一直在开展与互联网治理相关的一些课题的研究工作，包括内容审核课题。所以，我很高兴可以在这个论坛上分享我在这个主题上的一些想法。请切换到下一张幻灯片。

对于大多数关注过新闻或接触过社交媒体的人来说，各位肯定遇到过围绕内容审核展开的热议。各位可能看到政府部门试图遏制虚假信息，尤其是在疫情期间，也可能看到社交媒体公司试图遏制滥用威胁，法律研究人员试图提出一些判例法来解决内容审核问题，还有隐私和人权倡导组织针对内容审核对言论自由和隐私构成的威胁提出深切担忧。请切换到下一张幻灯片。

我按照时间线对与内容审核相关的事件进行了简单地归纳。为了节省时间，我不会逐一讲述每个事件，而是只会讲述其中的几个事件，以说明为何这个主题如此重要，以及为何这个问题会如此复杂。

例如，在 2021 年，就在几个月前，美国公共卫生部部长公开呼吁遏制健康虚假信息，他表示，虚假信息对公共健康构成了严重威胁，

限制虚假信息传播实际上属于社会道德责任。事实上，[音频不清晰] 敦促社交媒体公司 [音频不清晰] 监测并阻止虚假信息的传播。

关于这个问题，我们需要知道的一点是，内容审核不只是美国特有的问题，而是一个全球问题。最近，印度通过了一系列数字媒体法规，要求社交媒体内容提供商对内容进行审核，并进行 [音频不清晰] 追踪。这遭到了 WhatsApp 公司的强烈抵制，该公司针对这一新法规提起了法律申诉。

此外，就在几周前，Facebook 的一名前雇员出席参议院听证会，指证 Facebook 采取的内容优化措施及其对社会的影响。请切换到下一张幻灯片。

如果各位去问安全和隐私领域的从业人员，他们会告诉你了解和解决此问题的最好办法是进行风险评估。因此，我根据著名隐私法学者丹尼尔 • 索洛夫 (Daniel Solove) 提出的标准隐私分类，进行了关于内容审核的隐私风险评估。

例如，假设我们正在通过某种端到端加密消息服务，如 WhatsApp 或 Apple Messages，共享信息或交换消息。在这种情况下，作为用户，我们会抱有基本的期望，希望我们所交换的消息的隐私性和保密性有所保障。

但是，假设我是一个服务提供商，我使用一种算法来检测这些消息是否有害，在这种情况下，[音频不清晰] 将这些信息暴露给一个工具，也就是说，我在某种程度上侵犯了用户的隐私权，违背了保密性要求。

我们需要知道的是，在历史的发展过程中，每当有新功能被开发出来，我们不应该只是考虑如何使用这项功能，还应该考虑这项功能会如何遭到滥用。例如，我们可以想一想扫描技术，尤其是加密系统中的扫描技术，它们可能会被政府机构和恶意威胁行为主体用来进行监控和窃听，这会对社会的言论自由产生巨大的影响，并产生严重的寒蝉效应。

另外，我还想说明一点，那就是信息泄露有时候可能是完全不同的情况，不能一概而论。例如，假设我是一个用户，我的私密信息，比如我的性取向和药物使用情况，遭到了泄露。在这种情况下，我无法采取任何措施来保护自己免受因信息泄露而造成的严重情绪困扰和精神影响。

相比之下，假设是财务信息遭到了泄露，那情况就完全不同了。在这种情况下，你实际上可以冻结信用卡，以防止产生任何不良影响。但是，如果是健康信息遭到了泄露，你根本无法采取 [音频不清晰] 措施。请切换到下一张幻灯片。

在上一张幻灯片中，我谈到了内容审核可能导致隐私威胁。但是，对于内容审核，另一方面也存在一些合理的相反观点。例如，有人可能会说内容审核可以帮助阻止暴力行为，甚至最终避免死亡，这对缅甸发生的暴乱事件而言尤其如此。

因此，我坚信我们可以采取一种可保护隐私的方法来进行内容审核，而这种方法基于三个重要支柱。其中一个重要支柱是技术，在技术方面，需要技术组织与教育机构之间开展合作，找出可以检测任何错误信息或虚假信息，并同时确保用户隐私和信息保密性的安全加密技术。

例如，我们可以使用一种安全的多方加密技术来扫描图像，并将图像与涵盖所有滥用行为的图像存储库进行比较。如果信息不匹配，则无需将图像报告给服务提供商。

另一个重要支柱是流程，也就是我所说的信息监察人模型。我希望用户可以负责任地向服务提供商披露他们获得的任何类型的虚假信息，以便能够建立一种信任模型，并主动打击虚假信息。

最后一个重要支柱是原则，这是希望各利益相关方之间可以建立信任。让我们来看一个例子。如果我是一个积极进行内容审核的服务提供商，我认为需要确保我所用的算法在一定程度上是透明的，以确保可以在内容审核过程中赢得所有利益相关方的信任。请切换到下一张幻灯片。

这是最后一张幻灯片，我认为内容审核问题与气候变化问题非常相似。不止一个国家/地区想要解决这个问题，几乎所有国家/地区都想要解决这个问题。但是，各个国家/地区会通过不同的方法来解决这个问题。而且大多数时候，这个问题在各个国家/地区并不是同时发生的。

因此，我希望可以采取一种多利益相关方方法来积极解决内容审核问题。按照这种方法，个人用户需要借助教育者和教育机构提供的知识和工具，负责任地向服务提供商披露任何类型的虚假信息。与此同时，科技平台需要识别虚假信息，尽早发现虚假信息超级传播者和惯犯，并同时保护隐私。

在这一过程中，一个非常关键的利益相关方是全球政府部门，它们需要召集各种类型的私营非营利组织，一同寻求共识或通约，从而找到适当的法律和监管措施以解决内容审核问题。我的讲演到此结

束，谢谢聆听。如果大家有任何问题，欢迎提问，我很高兴能解答大家的疑问。

黛博拉 • 艾斯卡勒拉： 谢谢赛。大家有问题要问赛吗？好的，口译员在刚刚翻译时遇到了一些困难，但是我想提醒大家，这个会议会被录音，大约在一周内，大家就可以访问会议录音。如果有人想要访问会议录音，请等待一些时间。

好的，伊诺奇 (Enoch)，你是想要提问吗？有请。

伊诺奇 • 尼克邦 • 杜特 (ENOCH NIKINGBOUNG DUUT)： 是的。非常感谢。关于内容审核，我有一个简单的问题。内容审核问题涉及两个方面。一方面，我们不想妨碍言论自由。另一方面，我们也想阻止不适当的内容出现在可公开访问的地方。

因此，我在想是否存在一个折衷的解决方案，既可以降低允许人们随时随地发表言论所带来的风险，又可以不妨碍人们的言论自由？例如，如果大家想一想传统媒体，会发现存在相应的监管机构。但是，对于社交媒体，我们是否可以设立独立的监管机构来帮助解决这个问题呢？非常感谢。

赛 • 常德拉瑟卡兰： 谢谢伊诺奇提出的问题。不幸的是，我们目前还没有找到既可以解决虚假信息问题，又可以保护言论自由的现成解决方案。如果各位最近有关注新闻的话，肯定听说过 Apple 客户端扫描事件。Apple 希

望在用户端执行客户端扫描，以检测与儿童性虐待相关的各类图像和内容，但是，这遭到了隐私倡导者和安全专家的抨击。

由此可见，目前并没有现成的解决方案，但是正如我在讲演中提出的建议，我们可以使用安全的多方加密技术，这种技术会将这些图像与滥用图像存储库进行比较，只有当信息匹配时，才会向服务提供商报告，否则，不会将信息传输给服务提供商。希望以上说明能够解答你的疑问。

伊诺奇 • 尼克邦 • 杜特： 谢谢！不知道你是否可以将刚才的回答放到聊天窗口中，以便进一步 [音频不清晰]。谢谢！

赛 • 常德拉瑟卡兰： 当然可以。谢谢！

黛博拉 • 艾斯卡勒拉： 好的。谢谢伊诺奇的提问。还有其他人要提问吗？好的，下面有请下一位讲演者卡迪 • 翰墨 (Kady Hammer)。卡迪，请开始你的讲演。

卡迪 • 翰墨： 大家好。我是卡迪 • 翰墨，是华盛顿特区美利坚大学的一名法律系学生。我今天将谈论一个非常具有千禧一代特色的术语，即把关，这指的是为网关协议把关，或者称为网关协议（特别是边界网关协议）的安全机制。请切换到下一张幻灯片。

首先，我想要简要概述一下发展历程，并讲一讲我为何要讨论边界网关协议。声明一点，我不是技术专家，我是学法律的。所以，我花了相当多的时间来理解互联网基础设施的工作原理。但是，我相信大家都很清楚，互联网最初是为了促进交流而诞生的。在我们开发互联网基础设施时，安全并不是首要或主要的考量因素。但是，在当今世界，安全问题越来越令人担忧，尤其是考虑到网络威胁和网络不法分子日益猖獗。

1989 年，边界网关协议作为众多协议之一被开发出来。为了方便，后面我将采用边界网关协议的简称形式，即 BGP。BGP 依赖于彼此之间不断共享关于可用数据链路、可用 IP 地址的信息的各个网络，这也正是互联网能够持续发展成为现如今庞大的全球网络的原因所在。

需要注意的一点是，BGP 不要求对与之交互的 IP 地址或自治系统进行身份验证。相反，BGP 在所谓的信任框架下运行，大家可能知道这是一种诚信制度，在这个制度下，各个网络相信彼此是良好行为者。

总的来说，BGP 的运行原理很简单，它为满足路由协议需求提供了一个解决方案，并且提供了一个足够完备的结构，因而一直沿用到今天。请切换到下一张幻灯片。

这张幻灯片中提供了一个图表和一个路由协议列表。正如我之前提到的，BGP 是众多路由协议中的一个协议。路由协议的主要目的是在其他网络系统、设备之间路由互联网流量。但是，需要注意的一点是，路由协议不能确保信息传递的安全性。所以，这又回到了之前提到的信任框架或诚信制度。

正如各位所见，路由协议类型的列表很长。我不会将这些路由协议一一念出来，大家看一下即可。幻灯片右侧的图表大致展示了 BGP 或另一种路由协议 EGP 的工作原理。大家可以看到各网络之间是如何相互交流的，以及网络是如何与自主系统交流的，这只是一个概要图，大家如果感兴趣的话，可以看看，我将稍后进行进一步说明。请切换到下一张幻灯片。

下面我将更深入地讲解一下边界网关协议的细节，BGP 是一种路径向量路由协议，在互联网上的自治系统之间运行。BGP 路由器不会跟踪整个互联网拓扑图，而是会依赖邻居路由器或系统的信息，然后选择最短路径的路由以将其包含到路由表中。在这之后，每个路由器都会向正在寻找最短路径路由的其他邻居宣告该路由。如果政策允许，它们便会交换该信息。

这里需要考虑的一个问题是，当谈论 BGP 用于通信的自治系统或网络时，大家可能会听到它们被统称为自治系统，这意味着一个单一的系统。但是，自治系统有时包含一个完整的组织，其中包括多个路由器或设备。所以，这个术语更多用于表示更加宽泛和抽象的含义。

互联网自治系统编号由互联网服务提供商分配，以便像我们这样的最终用户可以通过互联网进行连接，自治系统编号有时也由注册管理机构分配。

BGP 最后会帮助路由器选择一条最优路径，即获取所需信息的最短路径。由此可见，BGP 协议之所以如此重要，是因为跟踪整个互联网系统本身就是一项伟绩，而且 BGP 依靠邻近网络来交换信息，从而可以更快地让用户访问所需信息或网站。

这里需要特别注意的是，由于 BGP 的工作方式，所有系统可能同时成为攻击目标。恶意行为者可以攻击包括组织、公司等在内的整个自治系统，而不是攻击单一设备。请看下一张幻灯片。

今天，我要谈论的最重要的事情是，协议中出现的安全问题，感谢布莱恩 (Brian) 在聊天窗口中提供的解释说明，不过，我特指的是 BGP 中出现的安全问题。我要谈论的安全问题不是 BGP 特有的，它们也确实存在于其他路由协议中。

其中一个主要问题是人为错误。我们可以看看 Facebook 宕机事故，虽然这个事故并不完全属于 BGP 问题，但从这个事故可以看出，人为错误可能会造成意外的错误配置，导致整个组织或自治互联网系统关闭或从互联网上消失，从而造成严重破坏。

不过，我想谈论的主要问题其实是恶意干扰。所有路由协议都可能成为攻击目标，无论是在 IP 欺骗、会话劫持、拒绝服务攻击，还是许多其他形式的攻击中，恶意行为者基本上都可以将虚假信息引入到 BGP 表中。

这方面的一个例子是，由于 BGP 依赖于相邻网络，您的相邻网络可能是恶意行为者，它会在您的请求中引入虚假信息，从而将您路由到恶意网站或其他地方。

但是，正如我之前提到的，由于 BGP 路由器之间相互信任，BGP 中不存在真正的身份验证机制。因此，目前根本无法验证对方是谁，或者其他网络系统传递的信息是什么，也就是说，无法确定信息是否经过验证，是否可信，是否值得信赖。另一个问题是加密认证不是强制性的，这是我将在下一张幻灯片中讨论的问题。

为了便于大家更好地理解这个问题，我想讲一个案例，这个案例将说明 BGP 劫持是什么样的，以及它是如何在 Amazon 域名系统中发生的。2018 年，恶意行为者发起 BGP 攻击（一种“中间人”攻击），利用位于芝加哥 IBX 数据中心的一台服务器，将流量重新路由到 Amazon Route 53 服务，从而能够在全球范围内拦截流量。

具体来说，这些恶意行为者以 MyEtherWallet.com 为攻击目标，试图将这个以太坊区块链平台的客户流量重定向到虚假页面或空壳页面，以窃取所有客户信息。

为了做到这一点，恶意行为者将互联网流量重定向到在俄罗斯托管的一台服务器，该服务器通过使用伪造证书伪装成 MyEtherWallet 网页，从而窃取客户的加密硬币。这里需要注意的一点是，这一攻击需要访问互联网服务提供商的 BGP 路由器，并且需要大量的计算资源，这是因为恶意行为者要重新路由 MyEtherWallet 网页的所有流量，因此必须得处理进入他们服务器的大量互联网流量。

由此可见，这一攻击凸显了 BGP 和 DNS 中存在的安全问题，更广泛地讲，此攻击可以反映出不同路由协议中存在的安全问题。这是迄今为止同时利用 BGP 和 DNS 漏洞发起的规模最大的攻击，关于 DNS 漏洞，其他新生代计划学员在讲演中已经有所介绍了。幻灯片底部的信息图大致展示了这次攻击是如何发生的。请切换到下一张幻灯片。

面对 BGP 中存在的安全问题，要如何做好把关呢。总的来说，在思考如何使路由协议更安全，特别是如何使 BGP 协议更安全时，我们需要考虑采取一些措施。

首先，我们需要可实施 IPsec（即 IP 安全）的路由器软件，这可以通过公钥基础设施或数字签名来实现。

其次，我们需要确定地区注册管理机构在明确认证机构职责方面所发挥的作用，即明确由谁负责认证地址前缀和自治系统号，包括其分配情况和位置。

为此，需要进行的一项重大投资是升级硬件基础设施，其中包括互联网服务提供商 (ISP) 向订阅用户提供的路由器，以确定互联网服务提供商在认证和处理这些信息方面所起到的作用。升级物理硬件显然是一项巨大投资。

然后，我们需要从更高的战略层面认真思考今后如何改进 BGP，特别重要的一点是，我们今后在做出改进时要时刻牢记安全性，而且要从被动走向主动。最后，我们还需要确定评估标准，也即如何判定任何网络、路由器、个人或实体是否可被视为安全可信或经过验证的信息源，换言之，我们需要确定将使用什么标准来允许或禁止网络在互联网生态系统中进行交互和运行。

基于上述考量，我在幻灯片中列出了三个解决方案，这三个方案并不是新方案，而是之前就已经提出的。其中有方案实际上可以追溯到 BGP 于 80 年代和 90 年代初创建之时。由此可见，其实我们有可用于保护 BGP 安全的现有解决方案。

第一个方案是采用安全边界网关协议，该协议提供了三种特定的安全机制。第一种安全机制是公钥基础设施，用于验证一个或一组 IP 地址的所有权。

第二种安全机制是“可传递”路径属性，用于携带可认证路由器信息的数字签名。如此一来，随着信息传输，信息中会出现某种安全标志。第三种安全机制是我之前提到的 IPsec，IPsec 一般可用于在通过 BGP 交换任何信息之前提供数据以对信息进行认证。

第二个解决方案是 BGP 起源安全机制，称为 Secure Origin BGP。这实际上与第一个解决方案中的第三种安全机制有关。也就是说，在交换信息之前，每个实体都必须对其他实体进行认证或接受其他实体的认证，以确保凭据经过验证。而且每个授权证书都必须经过验证。这里涉及到之前谈到的注册管理机构和互联网服务提供商起到的作用。授权证书中包含的信息还必须与托管这些证书的数据库相关联。因此，需要考虑注册管理机构或互联网服务提供商在维护这样的数据库中发挥的作用。此外，还必须考虑数据库的安全性。

第三个解决方案称为 BGP 可扩展传输，在这个方案中，会使用一种专有的传输协议取代 TCP，TCP 是另外一种路由协议。这个解决方案可能不是最可行的，因为它需要进行私有化，但是它将使用一种称之为泛洪的技术，这种技术将通过仅向其邻居发送连接消息来传输数据，而不是连接到网络上的所有网络或所有路由器。请切换到下一张幻灯片。

实现安全的边界网关协议显然存在挑战，这也是为什么提议的现有解决方案到目前仍未通过，也正因如此，我们现在还在讨论这个问题。其中最大的一个挑战在于现有的这些解决方案涉及到基础设施、人力、协调和责任分配，需要高昂的成本投入。而基础设施、人力、协调和责任分配正是前两个解决方案的主要考量因素。

对于最后一个解决方案，正如我之前提到的，它涉及到整个协议的改变，因此需要开展大量工作，而且它还涉及到私有化，也就是涉及到费用和访问权限问题，因为在私有化后，最终的权限或控制机制完全掌握在所有者手中，正因为如此，这个解决方案需要得到广泛支持才有可能施行。

另外一个最大的挑战在于，在危机爆发之前，我们似乎满足于现状，缺乏做出改变的紧迫感。正如我前面提到的，对于安全问题，大多数利益相关方，甚至包括我自己，都倾向于采取被动响应方法，即在发生事故后再采取急救措施，而不是采取主动防御。

当然，考虑到互联网的寿命和互联网存在的时间，化被动为主动确实比较困难。另外，还有一个问题是，考虑到已发生的此类攻击的规模都比较小，我们因此并没有太重视这个问题。我在前面提到 MyEtherWallet 攻击是此类攻击中已知的最大规模的攻击，虽然它只针对一家公司。但是，如果 BGP 成为恶意行为者的新目标，大家可以想象此类攻击的规模会有多大，以及它们可能造成的破坏有多严重。请切换到下一张幻灯片。

我其实已经在前面讲到了这张幻灯片中列出的每个要点，但是，我想着重强调一点，BGP 安全是一个不容忽视的重大问题，我们可以考虑采用现有的模型，思考如何获得各利益相关方的支持，从而彻底改变保护 BGP 安全的方法。如果大家想一想从 HTTP 转变为 HTTPS 的历程，我们完全可以采用类似的方法来解决 BGP 问题。请切换到下一张幻灯片。

这就是我要讲的所有内容。非常感谢各位抽出时间听我的讲演。

黛博拉 • 艾斯卡勒拉： 讲演很精彩，也很有趣。非常棒。在讲演过程中，大家在聊天窗口中也开展了如火如荼的讨论。这显然是一个很不错的主题，引起了很多人的兴趣。大家有什么问题要问卡迪吗？卡迪，讲演非常棒，内容的组织结构也很合理。

好的，如果没有其他问题的话，我们将请下一位讲演者，斯科特 • 金 (Scott Kim)，开始讲演。请记住，大家仍然可以在会议结束后提问。斯科特，轮到你了。谢谢。

斯科特 • 金: 谢谢。大家好。我是斯科特 • 金，目前是一名研究生，也是信息安全领域的从业者。我的工作主要是收集信息、分析信息，并将信息传播给相应的相关方。今天，我讲演的主题是如何使用 ICANN 查询工具来查找失陷指标。请切换到下一张幻灯片。

具体而言，我将先概要介绍 APT41 威胁组织，然后介绍一些用例，最后提出建议。

APT41 对于社会大众来说比较陌生，但是对于信息安全领域的从业者而言却是如雷贯耳。APT41 组织成员具有不同的名称，包括 Blackfly、Earth Baku、Wicked Panda。简单来说，APT41 是由中国政府资助的高级持续性威胁组织，于 2012 年开始开展与间谍活动相关的恶意软件活动。APT41 组织经常被认为是服务于中国共产党在“十三五”规划中的“中国制造 2025”计划中提出的目标。据我们所知，APT41 组织近期的攻击目标主要为视频游戏公司、电信行业组织和学术机构。9 月份，美国司法部起诉了多名与 APT41 入侵和行动有关的个人。请切换到下一张幻灯片。

最近，BlackBerry 威胁研究和情报团队发现了由 APT41 组织开展的恶意软件活动，在这个活动中，APT41 使用自定义的配置文件来隐藏其网络流量。此外，APT41 还使用了不同的恶意软件，如 PlugX、Cobalt Strike、[音频不清晰]、ShadowPad。BlackBerry 威胁研究和情报团队通过将此攻击活动与另外两家安全企业（Positive Technologies 和 [音频不清晰]）记录的两个攻击活动进行比较，发现了重叠的失陷指标，并由此揭露了 APT41 的基础设施。正如大家所见，APT41 团伙在攻击时会试图伪装成合法的 Microsoft 域名，例如，前三个以及后三个、五个或六个域名都是伪装的 Microsoft 域名。请切换到下一张幻灯片。

ICANN 注册数据查询工具使您能够查询域名和互联网号码资源的当前注册数据。为了进行查询，用户需要访问 WHOIS.icann.org，然后输入任意域名。作为示例，我特地选择了 isbigfish.xyz，这是我在输入这个域名后收到的信息。

通过在各种开源智能库中搜索域名和 IP，可揭示一些关联关系，而这些关联关系值得进一步研究。我之前提到的 isbigfish.xyz 域名属于 107.182.24.93 IP 地址，它出现在 Positive Technologies 公司发布的恶意软件活动博文中。因此，Blackberry 研究人员能够通过使用这些开放资源，找出 APT41 威胁组织用于访问不同基础设施和网络的一些 IP 地址和域，由此找出关联关系。

正如证书日期所显示的那样，这些域名只持续了大约一年时间，从安全领域从业者的角度来看，这是一个危险信号，因为通常情况下，威胁行为者会利用这些伪造域名或停放域名进行一些恶意活动。由此可见，我们可以从不同的资源获取大量信息。请切换到下一张幻灯片。

总而言之，Blackberry 通过关联由不同从业者和安全企业公开发布的的不同博文，成功找到了 APT41 威胁组织使用的一些 IP 地址和域。为此，我们由衷鼓励信息公开和共享，以便可以获得有关威胁或威胁行为者的更为全面的信息。通过共同努力，我们也可以揭露目前正在进行的一些犯罪活动。如果大家有任何问题，欢迎向我提问。谢谢。

黛博拉 • 艾斯卡勒拉： 谢谢斯科特。大家有什么问题吗？好的，谢谢！斯科特，非常棒的讲演，谢谢。下面有请最后一位讲演者，詹姆士 • 派克 (James Paek)。詹姆士，有请。谢谢。

詹姆士 • 派克： 非常感谢黛博拉。我是詹姆士 • 派克，我讲演的主题是如何对抗数字威权主义。请切换到下一张幻灯片。

很多人会问，什么是数字威权主义？根据已提供的定义，数字威权主义一般是指具有独裁倾向的领导人利用互联网和相关数字技术来降低公众对公共机构的信任，增强社会和政治控制，并削弱公民自由。因此，数字威权主义包含任何可能侵犯隐私或侵犯公众自由的行为，以及社会生活中存在的各种隐性独裁行为，即因为没有意识到存在控制而认为理所当然的独裁行为。

我认为，这些行为在很大程度上与数字威权主义的成因有关。数字威权主义的成因与独裁政府的成因一样，包括：政治、社会、经济的不稳定；公众对公共机构的信任的减弱；独裁者合法性的增强；对公众舆论的控制和操纵。这些成因背后的共同之处在于恐惧。毫

无疑问，面对充满不确定性的社会，我们对不可预测的未来充满了迷茫和恐惧。疫情和目前正在发生的所有其他事情也导致恐惧和信任缺失日益严重。

当然，也导致了不满。我们享有的权利有很多，但是我们并不知道这些权利从何而来。但是，在民族主义和民粹主义盛行，且很多政治实体都开始产生影响的情况下，为什么数字威权主义还会在各个国家/地区成为常态？请切换到下一张幻灯片。

我们现在可以看到数字威权主义呈现增长态势。以中国为例，在中国，数字威权主义最近可谓是大行其道，例如，中国城市的每个角落现在都增加了监控摄像头。在中国，你到的每一个地方和每一个街道角落都有监控摄像头。在中国，你显然可以看到每一个区域都安装了大量闭路电视监控系统，这些系统可能会对你能想到的每一种行为进行审查，无论是攻击性驾驶行为、不当的社交行为，还是任何其他可能会被视为违反规则的行为。这些都是我们在中国普遍看到的真实情况。此外，我们还看到，中国政府开始对香港公民施加管控。在 2019 年，从香港修改引渡条例以符合中国国家安全法规，我们便可以看到中国政府的管控行为。我不想对这件事展开详细讨论，但是，我想指出一点，中国最近的管控革命可以追溯到 20 世纪 50 年代的文化大革命时期或冷战时期。我们最近开始在中国看到很多这样的管控现象。那这种情况会发生在其他国家/地区吗？当然会。我们只是不知道具体会发生什么而已，但是有一件事情是可以肯定的，那就是，我们会看到社会信用体系的盛行。

下面我将详细地介绍社会信用体系。首先，什么是社会信用体系？社会信用体系是一种根据公民的社会行为对公民进行评级的国家信用体系。正如我在前面提到的，在中国，当你出现侵略性驾驶行为

或任何其他可能被视为不守规则的不当社会行为时，不论是什么原因，你都会受到处罚，你的评级可能会降低，你可能会因此失去很多特权，比如无法出国，也可能会面临一些惩罚。

当然，这种情况以前也发生在韩国，例如，韩国国家情报局根据韩国名人发表的政治言论将其列入黑名单。此外，韩国政府在过去几年也开始进行心理战，并开始恐吓互联网用户。而且，在韩国，我们会看到政府对从事反政府活动的人的监视和审查大大增加，凡是涉嫌反对政府政策的人士都会被监视和审查。请切换到下一张幻灯片。

其他国家也是如此。我们现在也开始在俄罗斯、白俄罗斯和法国看到大量监视和审查。例如，白俄罗斯最近发生的亚历山大 • 卢卡申科 (Alexander Lukashenko) 总统选举操纵事件，和互联网关闭事件。在俄罗斯，我们也开始看到干涉本国选举和其他国家选举的行为。选举操纵在其他国家/地区也是不断上演，让公众对选举可信度，包括选举本身和投票系统的可信度，产生了巨大担忧。在选举操纵中，基本上可以通过宣传手段来影响很多公民的行为，由此达成目的。我们在法国也可以看到类似的情况，在法国，国家安全法赋予法国政府最高的监视权力，允许根据对执法部门的骚扰程度来监控任何公民，并起诉违反法律的公民。请切换到下一张幻灯片。

数字威权主义的呈现形式有多种，包括我之前提到的监视和审查，也包括选举操纵、警察暴行、虚假信息、错误信息以及审查制度。下一张幻灯片将继续列出数字威权主义的更多呈现形式。请切换到下一张幻灯片。

显而易见，数字威权主义还有很多呈现形式，包括面部识别、网络攻击和黑客攻击。其中还有很多呈现形式是我们根本没有想到的，包括间谍活动、假新闻以及深度伪造，深度伪造是指基于原始照片或视频本身进行操纵。深度伪造情况现在越来越普遍，导致许多公民和普通互联网用户无法识别照片或视频是真实的还是伪造的，这可能会对日常社会生活以及我们的认知产生很大影响。请切换到下一张幻灯片。

数字威权主义的崛起会带来哪些威胁？对于数字威权主义产生的常见危害，已经取得了广泛共识，具体而言，数字威权主义会动摇民主，包括制度，它还可能危害社会经济和政治以及文化，同时侵犯人权和公民自由。除此之外，还可能产生不常见的危害，即对妇女权利的影响，因为数字威权主义可能会导致性骚扰或其他人为伤害的增多。请切换到下一张幻灯片。

这张幻灯片中列出了数字威权主义可能产生的所有其他威胁。我之前提到，数字威权主义有很多的呈现形式，这里便列出了每种形式在不久的将来可能产生的意想不到的后果。请切换到下一张幻灯片。

这张幻灯片中提供了经济学人智库公布的“民主指数”的最新数据，正如大家所见，在全球疫情爆发的背景下，世界上许多国家/地区的政府都开始动用大量监视和审查工具，并用各种借口来合理化这些工具的使用，称使用这些工具是为了应对疫情，恢复正常生活，包括恢复民主机构和公共秩序，从而创造更美好的未来。

大家可以看到，根据民主指数，我所在的国家，美国，目前属于有缺陷的民主政体，而且离成为混合政体只有一步之遥。起初，根据民主指数得分，美国一直都属于完全民主政体，但不幸的是，由于

最近的事件，主要是选举操纵，我们的民主状况在逐渐恶化。不止美国，同样的事情也在世界其他国家/地区上演。许多国家/地区的民主状况都开始恶化，这种情况实在是令人担忧。如果我们不采取任何措施来对抗这种数字威权主义，任由政府采取全面干涉的行事方式，使用这些工具来干涉我们的日常生活，这可能会产生朝鲜或中国这样的极权主义，危害我们的社会。因此，无论如何，我们都必须要结束这种情况。请切换到下一张幻灯片。

那么，我们要如何对抗这种情况呢？其实方法有很多。其中最重要的是，我们需要在国内倡导和宣扬民主和人权，这是首要任务。

我希望美国能够以身作则。如果我们不处理美国国内的民主问题，那么就无法为世界其他国家/地区树立榜样，也就只能通过胁迫手段来迫使其他国家/地区遵循我们的制度，为此，美国必须要维护一切人权，确保每个人都享有自由的权利。

如果美国自身无法做到这一点，并且不愿意挑战这些 [音频不清晰] 问题，那么就没有理由让其他国家/地区效仿我们。这就好比是在外交活动中，如果你代表的是美国或其他国家/地区，则其他外交代表们会根据你的性格或为人处世对你进行评判，并由此确定是否要接纳你的观点并追随你的脚步。一个国家也是如此。因此，我们需要增强对包括政府在内的公共机构的信任。

为了做到这一点，我们必须要加强文明建设，增强政治信任和社会信任。为此，我们必须要缓解美国国内的种族矛盾，防止国家分裂。种族矛盾是我个人最厌恶的一件事情，我们必须得解决这个重大问题，以确保国家团结统一。我知道，这肯定很难做到，但是我们必须要加强文明建设，确保展现良好的社会品格和行为方式，包括加

强互联网自由、数字包容性和可访问性，以成为其他国家/地区的榜样。请切换到下一张幻灯片。

这张幻灯片中列出了美国要做的一系列事情。首先，要加强构建多边联盟，最近，美国和 [音频不清晰] 开展了四方安全对话，此外，美国还与其他四个国家建立了“五眼情报联盟”等等。我们未来可能会面临亚洲版北约，虽然目前不无法确定，但是这是一个趋势。

其次，要进行大量的政府投资。毋庸置疑，我们需要投资人力资本。据我所知，中国将增加人力资本投资，培养更多的网络安全专业人才，以确保人才供给持续增加。但是，在美国，我们正经历显著的网络安全人才短缺。如果我们这方面人才大量短缺，而且科学、技术、工程、数学等领域的人才也大量短缺，我们将可能远远落后，并且可能面临不良后果。此外，还要增加研发投资，如果不重视研发投资，我们也会远远落后于其他国家。重要的研发领域包括各种数字技术和加密强化技术。

然后，我们必须要加强工作场所的多样性和包容性。企业要发展壮大无疑需要招纳贤才，而人才和企业的蓬勃发展，才能确保国家能够应对一切危机，例如，当前的全球疫情。除此之外，我们还必须要做许多其他事情，以确保我们继续在技术上处于世界领先地位。请切换到下一张幻灯片。

这张幻灯片中列出了所使用的参考文献和引文。请切换到下一张幻灯片。我的讲演到此结束。感谢各位抽出时间聆听我的讲演。非常感谢。如果大家有任何问题，请尽情提问。

黛博拉 • 艾斯卡勒拉： 谢谢詹姆士。布莱恩在在聊天窗口中提出了一个问题。这个问题其实是针对所有讲演者提的，但是既然现在是你在做讲演，所以就有请你回答这个问题吧。问题是：你如何看待人们在 COVID-19 疫情期间在互联网上的言论自由？

詹姆士 • 派克： 感谢布莱恩提出这个问题。但是，我不确定这个问题具体问的是什么，不知道布莱恩可不可以进一步解释一下。

黛博拉 • 艾斯卡勒拉： 布莱恩，你可以解释一下吗？

詹姆士 • 派克： 我是应该等待布莱恩的回复，还是尝试按照自己的理解回答这个问题？

黛博拉 • 艾斯卡勒拉： 你可以先按照自己的理解回答布莱恩的问题。

詹姆士 • 派克： 在我看来，布莱恩提出的问题涉及到很多方面。关于人们在 COVID-19 疫情期间在互联网上的言论自由，正如我在今天的讲演中提到的，数字威权主义正在兴起。我介绍了很多案例，比如中国、俄罗斯、白俄罗斯，但是，不要误会，美国其实也存在这样的情况，美国也并没有在互联网上实现充分的自由，美国要改进的地方也还有很多。例如，从 2014 年的爱德华 • 斯诺登 (Edward Snowden) 事件中，可

以看到美国政府在发生“9 • 11”恐怖袭击事件后以保护国家安全为由秘密收集了大量的个人数据。

正如我之前提到的，我们现在已经可以开始看到试图控制社会生活的独裁行为大幅增加，互联网自由开始被削弱，各类监控与审查工具和技术被广泛应用。例如，最近，尼日利亚和一些其他非洲国家/地区关闭了互联网，至于具体有哪些非洲国家/地区受到影响，我并不是很清楚。但是，这无疑可以说明，政府不应该有能力控制互联网上的言论自由，如果任由目前的这种情况继续发展下去，那我们最终将遭受可怕的后果。如果政府开始通过算法来评判你的行为是否符合规矩，并根据你的行为来施加控制，那么这无疑是非常可怕的事情，政府根本无权对你进行窃听，并根据你的行为进行审查。你享有自由权利，包括言论自由和人身自由，这是你的基本权利，因此，你完全有权利也有能力确保政府不越界。政府根本不应该干涉你的个人日常生活。

正如我在前面提到的，我们不希望再看到过去出现的威权主义。但是，现在，威权主义在朝鲜和中国大行其道，难道我们还想在世界其他国家/地区看到这种情况吗？我绝对不想看到。这完全是对个人隐私权的侵犯，也是对言论自由权、公民自由权的践踏，因此，威权主义绝对是不可接受的。

不幸的是，很多国家/地区现在都开始展现出独裁倾向，这绝非是我们希望看到的，我们必须严肃对待此问题，坚决维护我们的言论自由和公民自由权，如果将这一切视为理所当然，任由这种情况继续发展下去，那么，世界终将落入独裁主义者之手。这绝非我们希望看到的未来。为此，我们必须要做出改进，我们需要增强教育，并增加公众对公共机构的信心。

我知道，现在不论是在美国，还是其他国家/地区，这一点都很难做到。但是，我们必须要能够积极倾听他人的意见，并尊重他人的行为。这就是我之前提到的要加强文明建设，以确保彼此之间能够互相尊重。文明建设不仅有助于解决数字威权主义问题，还有助于解决许多其他问题和冲突，文明建设旨在促进心理健康，确保人们保持开放宽容的心态，彼此尊重，求同存异。非常感谢。

黛博拉 • 艾斯卡勒拉： 好的。谢谢詹姆士。布赖恩在聊天窗口中对他前面提出的问题做出了解释。我们只剩下几分钟时间了，接下来我先将布赖恩的解释读一下，然后再请詹姆士快速回答布赖恩的问题。布赖恩写下的内容是：“你提到政府比以前更严格地控制人们的互联网言论自由。那么，你认为这是民主世界的一个良好发展趋势吗？”

詹姆士，你有两分钟时间来回答这个问题，谢谢。

詹姆士 • 派克： 正如我前面提到的，我们必须要投资人力资本。这意味着我们必须要加大在人身上的投资，以确保提高公民的技术素养。如果不这样做，我们将会面临很多意想不到的不良后果。此外，我们还必须促进民主发展，为此，我们必须确保先在国内促进民主，从而确保其他国家/地区跟随我们的脚步，促进它们国内的民主发展。

但是，我并不是鼓吹民主是世界上最好的制度。当然，我也不是说民主不好，我只是想要强调，我们现在需要增强民主。这肯定会增加公众对公共机构的信心，为此，我们必须要增强自信，并加强国内的文明建设，以确保人与人之间能够彼此尊重。

黛博拉 • 艾斯卡勒拉： 好的。谢谢。伊诺奇似乎提出了一个问题，但是留给这个问题的时间只剩一分钟了，我们的会议马上要结束了。伊诺奇，你的问题是什么？

伊诺奇 • 尼克邦 • 杜特： 非常感谢。我不是要提问，而是想对前面提出的问题做一下补充。我认为，我们有必要认识到一个事实，那就是一些政府确实利用了 COVID 疫情通过了一些法规，这些法规让政府能够访问或获取人们的数字通信内容，并以此为理由对发布特定内容的人采取迫害行动，这实际上是一种更高层次的内容审核。

由于在 COVID 疫情环境下，每个人都反对虚假信息，因此，一些相关法规并没有因引起强烈反对而成为新闻头条，但是，要注意的是，这些法规并不会在 COVID 疫情结束时就废除，所以我们可能会看到在疫情结束后，政府仍利用在 COVID 疫情期间通过的这些法规妨碍人们的言论自由。我认为这是一个非常重要的话题，值得我们更加深入地思考。非常感谢。

黛博拉 • 艾斯卡勒拉： 感谢伊诺奇提出的意见。好了，今天的会议到此结束。感谢各位出席本次会议，谢谢大家的支持。感谢西兰努什今天为我们放映幻灯片。也要感谢今天的各位讲演者，你们的讲演非常精彩，不仅主题选的好，而且陈述地也很好。最后，要感谢会议支持人员和口译员，没有你们的支持，本次会议不可能顺利开展。总之，非常感谢出席本次会议以及为本次会议提供支持的所有人员，很高兴能与大家共同完成本次会议。新生代计划学员们，请好好享受 ICANN 第 72 届会议吧。我们本周还有很多工作要做，我知道，首字母缩略词和其他

事情可能会让你们感到不知所措，但是不用着急，尽情享受吧。感谢大家的到来，本次会议到此结束。祝大家度过愉快的一天。

[听写文稿结束]