ICANN71 | 虚拟政策论坛 — 新生代计划演讲日 1
中欧夏季时间 2021 年 6 月 14 日星期一 — 14:30 至 16:00

黛博拉 • 艾斯卡勒拉
(DEBORAH ESCALERA)： 好的，感谢大家今天的参与。大家上午好，下午好，晚上好。大家好，欢迎参加 ICANN 71 演讲会。我叫黛博拉 • 艾斯卡勒拉，在公共责任支持部工作，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，本次会议正在录制中，请大家遵循 ICANN 预期行为标准。会议期间，只有在问答窗格中提交的问题或意见才会被大声读出来。我会在本次会议的主席或主持人指定的时间大声读出这些问题和意见。

本次会议提供多种语言的翻译。点击 Zoom 中的同声传译图标，并选择你要在本次会议中聆听的语言。

如果想发言，请在 Zoom 会议室里举手，待会议主持人叫到名字后，我们的技术支持团队将允许你取消静音。在发言之前，请确保从同声传译菜单中选择你要讲的语言。为了方便记录，请说出你的姓名，如果你使用英语以外的其他语言，还要说明你要使用的语言。

发言时，请确保将所有其他设备和通知静音。同时，请大家发言时口齿清晰并保持正常语速，以便口译人员能准确翻译。所有参加本次会议的与会者都可以在聊天窗口中留言。请使用聊天窗口中的下拉菜单，选择“回复所有讨论组成员和与会者”。这样所有人都能看到你输入的内容了。

请注意，在 Zoom 网络研讨会形式下，私聊只能在讨论组成员之间进行。专家组成员或标准与会者向其他标准与会者发送的任何消息都会被会议主持人、联合主持人和其他专家组成员看到。

好的，下面我要特别感谢我的导师们，它们帮助我指导学生，帮助他们在 ICANN 71 前的几周做准备。他们做得非常出色。切丽 • 斯塔布斯 (Cherie Stubbs)、阿里斯 • 伊纳希欧 (Aris Ignacio) 和德萨莱尼 • 耶华拉 (Dessalegn Yehuala)。非常感谢。他们给了我莫大的帮助，帮助学员们为 ICANN 71 做准备，是非常了不起的导师，引导学员通过整个流程，让他们为今天做好准备。

我们的第一位演讲者是达尼尔 • 格鲁贝夫 (Daniil Golubev)，希望他在会议室里并准备好了。我的同事费尔南达 (Fernanda) 今天将帮助我播放幻灯片。非常感谢费尔南达今天的协助。达尼尔，你在会议室吗？

达尼尔 • 格鲁贝夫： 是的，我在。我已经准备好演讲了。大家下午好。

黛博拉 • 艾斯卡勒拉： 好的。我要提醒所有演讲者讲慢一点，语速适中，因为我们的口译员需要翻译你们说的每一句话。我也要提醒你们，如果要切换幻灯片，只需要对费尔南达说“请放下一张”。非常感谢。达尼尔，你可以开始了。

达尼尔 • 格鲁贝夫： 好的。亲爱的各位同事，大家下午好。我想谈一个非常具体的问题，关于俄罗斯数字技术协会的互联网监管职位，以及俄罗斯互联网自由的总体情况。当然，这是一个相当具体的问题，但是这个问题可以从俄罗斯推及其他国家。请放下一张。

在俄罗斯，有多个旨在发展互联网产业的协会，称为互联网协会。它们存在的[听不清]和[听不清]的性质各不相同。本次演讲选择协会的主要标准是那些将自身定位为独立于国家的协会。但是，在我解释这些协会的工作和运行时，可能看起来并非完全正确，在本次演讲中，我会试着定义各协会在互联网监管方面通过不同渠道所表达的立场。

在本次演讲中，我考虑的协会和机构如下：互联网版权保护协会、媒体和通信联盟、地区互联网技术公共中心、俄罗斯电子通信协会以及互联网发展研究所。当然，在俄罗斯还有多种多样的协会，但是我选择的是在俄罗斯互联网部门规模最大和最重要的协会。请放下一张。

我想给你们介绍一下俄罗斯互联网自由方面的背景情况。俄罗斯当局试图尽可能地控制俄罗斯互联网部门，有一些关于互联网如何与俄罗斯政府相关联以及当地[如何]监管互联网的案例。

俄罗斯有一个名为 Roskomnadzor 的行政机构，负责审查俄罗斯的互联网部门，并且根据俄罗斯当局的授意，封锁许多被认为违反俄罗斯法律的网站。由于这个行政机构，许多信息在俄罗斯遭到了封锁。

同样，俄罗斯公民如果在互联网上发表对当局的攻击性言论，也会受到惩罚。在俄罗斯，最近举行了一些抗议示威活动，期间人们发现移动网络经常关闭，这与政府[脱不了]干系。

有人试图使俄罗斯的互联网与世界其他地方的互联网隔绝开来，即所谓的主权互联网，或者我们在俄罗斯称之为 RUnet。从事 IT 行业的国际公司有义务在俄罗斯境内存储他们关于俄罗斯用户的数据，这样俄罗斯当局就可以访问俄罗斯用户的数据。请放下一张。

好的，所以我想谈的第一个协会是互联网版权保护协会，在俄语中，它简称为 AZAPI。这是一个非营利性的伙伴关系组织，旨在打击在互联网上非法投放书籍和音频产品的行为。所以它主要与版权问题有关。AZAPI 参与讨论与保护俄罗斯互联网部门版权有关的法律草案，其客户包括努力捍卫其版权的俄罗斯主要图书出版商。遗憾的是，这个协会并没有提供非常令人满意的手段来满足这一需求。请放下一张。

AZAPI 是如何与俄罗斯政府互动的？2015 年，AZAPI 向莫斯科市法院提出上诉，要求封锁洪流跟踪器 RuTracker，该跟踪器恰好存储了 AZAPI 客户的版权客体。而且它并不满足于此，还要求封锁整个网站，整个洪流跟踪器，不幸的是，这对互联网的状况非常不利。

2016 年，AZAPI 已向莫斯科市法院提出上诉，要求责成 Yandex 搜索引擎 — 这是俄罗斯仅次于谷歌的第二大搜索引擎 — 从搜索中删除与 RuTracker 有关的书籍链接，这些链接位于 RuTracker 的搜索结果中。

2019 年，AZAPI 向莫斯科市法院提出上诉，对 Archive.org 资源提起一系列诉讼，该资源在缓存中存储了作家迪米崔 • 高佛斯基 (Dmitry

Glukhovsky) 和达里亚 • 顿佐娃 (Daria Dontsova) 的有声读物的数字副本，他们也是 AZAPI 的客户。

2020 年，AZAPI 又呼吁欧盟委员会追究谷歌的责任，因为它拒绝从 Google Play 删除允许“大规模侵犯版权”的电子书的应用程序。这些网站是 Ok.ru、Mail.ru、Telegram、YouTube 和 WattPad。请放下一张。

下一个协会是媒体和通信联盟，在俄语中简称为 MKS。它是由媒体和电信行业的最大参与者在 2014 年成立的。这是一个由俄罗斯媒体公司和电信运营商组成的非营利性伙伴关系组织，是电信和媒体市场公司之间的中介。请放下一张。

媒体和通信联盟在不同年份向俄罗斯政府提出了几项法律草案，主要是在帕维尔 • 斯捷潘诺夫 (Pavel Stepanov) 的管理下，他在 2016 至 2018 年担任 MKS 的主席。MKS 提出了诸如[听不清]法外封杀盗版网站的镜像、封杀 UDP 协议级别的洪流、限制 VPN 服务的运行、监管 Messenger 应用程序以及监管在线电影院的运营。请放下一张。

另一个协会是地区互联网技术公共中心，在俄语中简称为 ROCIT。它成立于 1996 年。ROCIT 董事会的成员包括政府机构和商业公司的代表。它的资金来自于俄罗斯总统资助基金 (Russian Presidential Grants Fund)。所以它是由政府间接资助的，尽管它是一个非政府协会。它的目标是创造一个友好的互联网环境，普及互联网技术。它的定位是作为用户、企业和国家之间互动的平台，以及解决与 IT 行业有关的问题。请放下一张。

ROCIT 与俄罗斯当局对抗议活动的反应有关。2021 年，俄罗斯发生了大规模的反政府抗议活动，受到了政府在现实和数字方面的严厉

镇压。而 ROCIT 的回应，根据该组织的说法，社交网络的内容传播助长了像这样的极端主义行动。

“ROCIT 专家注意到互联网上针对公共安全的内容材料急剧增加。”在这一讯息中，他们批评了一些内容，而那些内容只不过是告知人们抗议活动的相关情况。并且他们还称有关抗议行动的材料是极端主义，甚至是恐怖主义。

ROCIT 呼吁社交网络停止传播此类与抗议活动有关的内容。ROCIT 的立场与政府的立场不谋而合。请放下一张。

另一个协会是俄罗斯电子通信协会，俄语中简称为 RAEC。它成立于 2006 年。它被列入电子媒体领域的国家支持接收者名单，所以它也是由政府资助的。RAEC 的主要参与者包括 Mail.ru 集团、卡巴斯基实验室、VKontakte、Rostelecom 等俄罗斯最大的 IT 公司。

此外也有一些国有公司，如“今日俄罗斯”新闻社和塔斯社。这是一个由俄罗斯电子通信市场代表组成的非营利性协会，其目的是整合行业领导者的意见，并与政府机构互动。请放下一张。

关于 RAEC 在互联网监管上的立场可以通过 Runet 奖来表达。这是一个由 RAEC 组织的奖项，旨在表彰俄罗斯互联网产业部门的成就。自 2011 年以来，Runet 奖充满了与俄罗斯互联网部门监管有关的提名，如安全 Runet、没有极端主义的互联网、社会重要项目，特别是儿童保护、增强 Runet 的数字免疫力。

在大多数情况下，在这些类别中，只有那些旨在审查俄罗斯互联网部门的国有公司才能成为获奖者。在与互联网信息内容有关的类别中，大都会优先考虑国家资源。请放下一张。

我想谈的最后一个协会是互联网发展研究所，俄语中简称为 IRI。它是在总统府的支持下于 2015 年成立的。不过，它的目标仍然是作为一个非政府的协会。它是一个自治的非营利性组织，其主要活动是在互联网上制作具有社会意义的内容，并就特定行业的法律草案开展研究。它是数字产业成员和政府机构之间的中介，并宣布举办以社会广告和爱国主义内容为主题的视频制作比赛。基本上，它就像俄罗斯互联网部门的一个关于社会主题的互联网内容市场。请放下一张。

IRI 在不同年份是如何参与数字产业监管的？它提出了一个在笔记本电脑和智能手机上预装的俄罗斯软件清单。它提出了一个电竞选修课程。它建议制定一个关于社会广告的备忘录。它建议为年轻一代创造一个安全的数字环境。它建议创建数字技术的教育项目。它还建议对俄罗斯的匿名者进行监管，也包括 VPN。请放下一张。

这些协会是如何联系起来的？对于这些协会来说，没有一个合作机构来研究互联网治理问题。但是，各协会的成员是彼此交叉的。基本上，MKS 的成员也是 ROCIT 成员，而俄罗斯政府是所列各协会的成员，或以某种身份对各个协会施加影响。

这与 ICANN 有什么关系？ROCIT 和 IRI 是俄罗斯顶级域名协调中心的创始人之一，该中心负责维护俄罗斯顶级域（如 .ru 和 .rf）的功能。因此，基本上，通过这些非政府协会，即使它与政府有关，政府也可以影响顶级域的政策和每个协会的工作。请放下一张。

总结一下，首先，许多互联网协会，尽管它们注册为非盈利和非政府性质，但它们与俄罗斯的国家机构有联系，从国家预算中获得资

金，并根据国家命令开展工作，政府的代表也在协会中，政府影响着这些协会的意见表达。

协会所表达的意见反应是由大多数成员达成的，其中包括俄罗斯当局。在大多数情况下，他们是积极的，他们支持对互联网的监管。在极少数情况下，他们对某些问题进行适度批评。

第三，协会本身也从法规中受益，因为它们致力于执行国家命令，以实施已通过的法律。他们在讨论或引入法律草案时为自身利益进行游说，并试图通过将某些方面集中在一个协会并削弱竞争对手来垄断某些商业领域。

最后，我想说的是，俄罗斯政府正试图尽可能多地控制互联网，而协会是政府、俄罗斯当局达到目标的途径之一，即使这些协会都不是政府性质，至少书面上来说是这样，但它们还是受到政府一定程度的影响。谢谢大家。

黛博拉 • 艾斯卡勒拉： 太棒了。谢谢达尼尔。大家有问题要问达尼尔吗？你们可以举手或者在聊天室里提问。

达尼尔 • 格鲁贝夫： 帕布罗 (Pablo) 提了一个问题。

黛博拉 • 艾斯卡勒拉： 好的，帕布罗，请打开你的声音并提问。

帕布罗 • 博迪亚克 (PABLO BURDIAK)： 好的。大家好。首先，非常感谢达尼尔带来如此精彩且信息丰富的演讲。我对这个话题非常感兴趣，因为我也在某种程度上研究俄罗斯的案例，我想知道你能不能再提供一些细节，说明有没有一些与政府没有直接联系或与政府有间接联系的互联网协会，即独立互联网协会。

达尼尔 • 格鲁贝夫： 谢谢你的好问题，帕布罗。遗憾的是，由于时间限制，我只能介绍 10 分钟。的确，有些协会是完全独立的，但它们在大多数情况下不允许合法注册，因为为了完全注册，你需要遵守俄罗斯法律和立法。你需要找到一些折中方案，而在大多数情况下，这是不可行的。

有一个名为 Roskomsvoboda 的协会。它致力于互联网上的自由，在某些方面它是 ICANN 在俄罗斯的一个授权分支机构。它为互联网的自由而努力，并试图争取到尽可能大的俄罗斯互联网自由。然而，遗憾的是，在大多数情况下，他们不允许在官方层面运作。

黛博拉 • 艾斯卡勒拉： 好的。谢谢。还有一个问题来自里卡多 • 南尼 (Riccardo Nanni)。里卡多。

里卡多 • 南尼： 谢谢，也谢谢达尼尔非常有趣和清晰的介绍，因为有时当我们听到关于 Runet 的信息时，它往往是一个口号，很难衡量它的实际含义。

因此，最近有一些关于俄罗斯建立某种俄罗斯 DNS 的可能性的讨论。这只是一个一般性讨论，还是有一些更具体的事情可能会发生？你对此有什么看法吗？谢谢。

达尼尔 • 格鲁贝夫： 谢谢你的问题，里卡多。是的，有人试图建立一个所谓的主权互联网 Runet 和俄罗斯 DNS。我想，从 2010 年开始就有这方面的讨论，或者类似的讨论。俄罗斯政府和为政府工作的 IT 专家试图建立起所谓的俄罗斯独立互联网地位。

然而，他们的资格还不够。2017 年，俄罗斯试图封锁 Telegram。但并未凑效。Telegram 仍然在俄罗斯运营。今年，他们试图封锁 Twitter。这也没有成功，而现在有关于封锁 YouTube 的讨论也是相当...我认为这是不可能的，因为为政府工作的 IT 专家根本不合格。

的确，存在一些使其更加主权化的讨论，但我认为在俄罗斯目前的互联网传播状态下，不大可能产生类似于中国的情况。在俄罗斯的互联网部门全球社区过于一体化，因此我认为这在很大程度上是不可能的。

黛博拉 • 艾斯卡勒拉： 非常感谢你的精彩演讲，达尼尔。好的，我们将继续有请下一位演讲者，维罗妮卡 • 斯罗敏思卡 (Weronika Slominska)。

维罗妮卡 • 斯罗敏思卡： 大家好。

黛博拉 • 艾斯卡勒拉： 提醒一下，你将有 10 分钟的时间，如果超过了，我肯定会给你一个警告。另外，请说得清楚一点、慢一点。谢谢。

维罗妮卡 • 斯罗敏思卡： 好的。谢谢。大家好。感谢达尼尔非常有趣的演讲。我是维罗妮卡，主修国际公共管理，今天我想谈谈网络安全和该领域政策制定者的相关挑战，以及提高对该问题认识的必要性。请放下一张。

谢谢。在全球各地，讨论网络安全话题的范围和频率在不断增加。新型网络威胁层出不穷，网络攻击可以对所有的人和组织产生非常严重的后果，这意味着这个问题确实需要采用自上而下的方法来处理。

网络安全是一个高度多面向的问题，它需要处理技术方面的人员和处理治理的人员合作，这就是我今天要探讨的角度。

在物联网的世界里，越来越多的物体具有互联网连接和通信的 IP 地址，这意味着社会更加依赖网络空间。然而，尽管管理网络空间是如此的关键，政府似乎并没有做足够的工作来确保其安全，网络安全并没有真正得到应有的重视。请放下一张。

这是因为网络安全领域的政策制定正面临着许多悖论，首先是政府希望确保网络安全，但另一方面，他们出于监控目的又想要公民的数据。因此，一方面，政府希望公民保护自己，但另一方面，他们并不希望公民真正使用加密和其他网络安全措施，因为这些措施也可以被犯罪分子和恐怖分子利用。

另一个悖论是，网络安全是一个真正的全球现象，它不能在国家边界内处理，它需要跨国合作。但一些政府甚至彼此不信任，他们不愿意合作。他们甚至可能互相入侵。所以这就使情况变得复杂。

另一个非常重要的悖论是，政府在网络安全方面的支出没有固定的适当数额，因为支出太少不能确保足够的保护，但支出太多可能会发出一个信息，即一些非常令人担忧、非常错误的事情正在发生，它可能会造成恐惧。因此，确保平衡非常重要。请放下一张。

所以已经确定了四个主要原因，解释为什么网络安全领域的政策制定如此具有挑战性，首先是有限的可见性。由于网络安全漏洞的影响在物理意义上往往是不可见的，而且这个话题不容易向公众解释，公众并没有真正感受到这个问题的影响。所以很难制定政策，在不可见的事物上组织新的东西。

第二个问题是网络安全的社会技术复杂性，因为虽然 IT 基础设施和政策在确保网络安全方面至关重要，但人在其中发挥主要作用，他们负责维护系统和执行政策，然而很多人和组织缺乏意识，或者他们甚至没有资源来采取行动。

第三个问题是网络安全的争议性。攻击者大多是匿名的，所以不清楚谁是真正的敌人。而第四个挑战是模糊的影响。因此，很难提前判断网络安全风险，更难衡量新的网络安全政策的影响，这使得招募投资变得困难。请放下一张。

正如我们所看到的，在网络安全方面有很多模糊不清的地方，缺乏认识，这导致了政策制定者面临的种种挑战。那么可以做些什么来解决它们？请放下一张。

研究人员提出了一个信息框架的概念，即以简单和令人信服的方式来沟通一个复杂的问题。由于政策制定者和专家经常被批评不能传达他们的信息来向公众解释，而且网络安全是一个非常复杂的现象，影响时间很长，很难解释，所以必须将其简化为一个简单的信息，抓住本质，向人们展示网络安全的重要性。请放下一张。

为了提高人们对网络安全的认识，研究人员提出了一个网络安全信息框架的策略，包括六个步骤或规则，首先是不要加剧网络安全，不要夸大风险，把它放在一个真正现实的角度，因为夸大只会使问题变得更糟。

第二条规则是要明确谁是坏人，我们到底在和谁斗争，谁可能是敌人，我们可以预期谁会带来威胁。

第三条规则是把英雄放在聚光灯下，例如，展示那些在国内保护网络安全的人，他们有什么能力、获得的成就等。

第四条规则是展示网络安全对社会的重要性，所以要把改善网络安全的需求与经济增长或国家繁荣联系起来。

第五条规则是将网络安全与人们的日常生活联系起来，以证明网络安全如何影响人们的日常生活，在哪些方面有影响。

第六条规则，也是最后一条，是将与网络安全相互关联的其他两个问题联系起来，比如说政治。

下一张幻灯片，谢谢大家。我的演讲到此为止。谢谢。

黛博拉 • 艾斯卡勒拉： 谢谢，维罗妮卡。讲得非常好。大家有什么问题要问维罗妮卡吗？聊天室里有没有问题，或者有没有人要举手？好的，非常感谢。如果你们后续有任何问题要问，可以发电子邮件给我们或者直接发给她。我们可以提供她的电子邮箱，或者你们可以给我们发送电子邮件，地址是 engagement@icann.org。

好的，那么下一个是阿特龙诺斯 • 穆鲁格塔 (Atronos Mulugeta)，他今天没法来做演讲，但他提交了一个视频演示。我以前没有这样做过，这是新的方式，接下来我会共享屏幕，看看行不行，希望一切顺利。你们能看到吗？

阿特龙诺斯 • 穆鲁格塔： 大家好。我是阿特龙诺斯[听不清]。我想说，如果你有任何问题、任何建议或评论，请使用我的电子邮箱与我联系[听不清]电子邮箱，所以如果你对本次演讲有任何问题，非常欢迎你提出来。

当谈到一个[听不清]话题，我们如何用人工智能帮助 ICANN？[听不清]把它说得更具体一些，也就是对域名系统安全应用人工智能。所以[后来我试着去看]这个域名系统是什么时候发明的。它是在 1980 年发明的，没有任何保护措施来确保数据或[听不清]。

所以，在那个时候，互联网并不像今天这样广泛，也不像今天这样大，所以他们并不关心安全问题，或者说他们并不太关心保护问题，也就是说他们在没有保护的情况下制造了它。但是现在，随着互联网变得越来越宽，越来越大，[听不清]而且，这使得攻击者可以将用户从预定的目的地转移到攻击者选择的目的地。

因此，当互联网工程任务组第一次关注这个问题时，他们试图提供一个解决方案，于是发明了 DNSSEC，也就是域名系统安全扩展，通过使用基于公共密钥的数字签名来加强域名系统中的数据原始身份验证和数据完整性。

我来谈谈[听不清]数据原始身份验证、数据完整性，我说的数据原始身份验证，意思是 — 我说域名系统一开始不提供数据原始身份验证，意思是域名系统不提供数据相关[听不清]的保证。而我们说它一开始不[听不清]数据完整性，意思是如果域名系统响应中的数据被修改或更改，它不提供[听不清]。所以一开始，我们可以看到，这个域名系统并不是那么安全。但是在实施 DNSSEC 之后，这个域名系统扩展提供了数据原始身份验证[听不清]数据完整性的保证，所以它变得更加安全。

但是，当我们看到这个域名系统扩展的运作方式时会发现，它不是自动的。它应该由运营商和域名系统所有者启用。这意味着每个域名所有者都必须知道这个域名系统扩展，以使互联网更加安全。

域名所有者多种多样，例如有商人，[听不清]用例子来解释[听不清]拥有域名的网站，一个他用来销售产品的商业网站。那么这个人，正如我所说的，是一个商人，所以他没有那么多技术方面的知识，这意味着他不能为安全目的启用 DNSSEC [听不清]。也就是说黑客可以使用与[他创建的]相同的页面，[抢走他的]客户。

所以我的想法是，为了保护这些人，我们为什么不把这个系统做成自动的？我认为我们应该应用人工智能，使这个系统自动化。

当谈到这一部分时，我认为有一些人是在技术[部分]之外的，所以当你试图解释什么是人工智能和什么是机器学习时，人工智能就像

计算机科学的一个广阔分支，它涉及到建立机器或系统，这些机器或系统可以执行需要人类思维能力或人类推理能力的任务。

从这个[听不清]，我想介绍一个具体的部分来应用到这个领域，所以我选择机器学习人工智能。所以当你看到机器学习是做什么的，它是如何工作的，这个机器学习，人工智能的这个部分是通过训练机器[来执行这个机器学习的具体部分]，也就是监督学习。监督学习是机器学习的一部分，它被用来标记数据或定义数据，用定义的数据来训练一台机器。

我知道这是一个最技术性的话题，也是一个非常复杂的话题，但请允许我试着稍微提几句，我们如何应用这个机器学习或人工智能？我认为我们可以训练一台机器来[感知]新域名系统的注册，然后自动[启用] DNSSEC 来提高域名系统的安全性。

所以我的想法是制造一台机器，当一个新的域名系统被注册时，它可以感知并自动启用 DNSSEC，而不需要由域名所有者和运营商来启用。我认为这将提高互联网的安全性。

所以我的研究是 — 我没有得到结论，但我仍然在努力，所以我的研究是我们是否可以通过利用这种机器学习，来自动启用它。所以[我想]看看其他人在这个领域，在互联网安全领域正在做什么，以使互联网变得更安全。不同的专家正在研究如何应用机器学习来检测[听不清]。

我知道这有点复杂，这是一个技术性较强的[听不清]算法，就像其中一个算法[听不清]，它用于注册和分类[听不清]，他们也在使用 — 额外的信息，他们也在使用 Python 作为编码基础。

我知道我们不能在这个[限定的]时间内涵盖这个庞大的主题，但这是我今天要说的全部内容。如果你有任何问题，正如我在开始时提到的，非常欢迎你通过我的电子邮箱联系我。非常感谢你的[听不清]，还有，我有一个特别的[听不清]，所以我正在准备我的演讲。感谢大家，祝大家有愉快的一天。

黛博拉 • 艾斯卡勒拉： 好的。我想这对口译员来说有点困难，所以这部分内容不会出现在会议记录中。我想我漏掉了要问维罗妮卡的问题。那么，有没有人有问题要问维罗妮卡？可以举手吗？有吗？好的，如果没有其他问题，我就继续。

我们的下一位演讲者是维罗妮卡 • 皮科罗 (Veronica Piccolo)。维罗妮卡，你在线上吗？

维罗妮卡 • 皮科罗： 是的，我在这里。

黛博拉 • 艾斯卡勒拉： 好的维罗妮卡。你也有 10 分钟时间，请说慢一点、清楚一点。欢迎维罗妮卡。谢谢。

维罗妮卡 • 皮科罗： 谢谢。欢迎大家。我要和大家谈谈意大利两家法院在 2019 年和 2020 年就知识产权保护问题作出的一个判例，特别是关于这些裁决如何妨碍互联网的完整性和所谓互联网式联网的关键属性。请放下一张。

这是议程。我将给你们介绍一点背景，谈谈互联网式联网，然后解释什么是动态禁令，以及对互联网的关键属性、对互联网式联网的影响，然后我将做出行动呼吁。请放下一张。

介绍一点背景。2019 年，一家意大利媒体公司对 Cloudflare 寻求禁令救济。Cloudflare 是一家提供内容分发网络服务、DDoS 缓解、互联网安全和分布式域名服务器服务的供应商。

这家意大利公司声称，Cloudflare 的客户非法复制了它的许多电视节目，并要求 Cloudflare 删除或禁止访问这些网站。

在这种情况下，意大利的法规强制规定，只有在国家法院或行政机关要求时，互联网中介服务提供商才必须终止或阻止侵权行为。

2020 年，我们收到了国家足球联盟和意大利天空电视台就非法直播足球比赛发出的类似投诉。在这种情况下，救济是很难的，因为 Cloudflare 被命令禁用其对一些客户的内容分发网络服务。请放下一张。

那么，什么是互联网式联网？互联网式联网是由国际互联网协会开展的一个项目，该项目指出，互联网的成功不仅归功于技术本身，还归功于其运作和发展的方式。

不妨这样想，我们可以通过互联网进行许多活动。我们可以学习，可以联系，可以分享，可以借助互联网组织起来。我们这样做是因为互联网是这样发展的，我们需要认识到，到现在为止，究竟是什么让互联网对每个人都有用。由此，国际互联网协会得出了五个关键属性，它们更像是道德原则而不是技术属性。请放下一张。

好的，第一个属性是可访问性。换句话说，无论你来自哪个国家，无论你在哪里，总是能连接到全球网络。你所需要的是一个设备和一个接入点，然后你就在互联网上。你可以与世界上的每个人联系或合作。

第二个属性是开放性和互用性。我们必须把互联网看成是一个乐高房屋。我们可以在底层结构上有一个积木，而且我们知道这个积木将永远适合，可以在任何地方和任何时候进行无约束创新。

第三个属性是去中心化。我们知道互联网是一个由网络组成的网络。每个独立的网络都选择与其他网络连接，每个人都属于同一个网络并从中受益。

第四个属性是公用全球标识符。换句话说，有一种公共语言来理解 IP 地址和数据包从 A 点传递到 B 点的方式。

第五项属性不需要介绍，因为它是网络中立性。请放下一张。

因此，在我的国家，有一种打击网络盗版的趋势性做法，即要求法院不仅关闭目前活跃的盗版网站，而且还要关闭未来可能拥有相同二级域的网站。我们称之为别名。

换句话说，无论哪个顶级域跟在该二级域的后面，无论是现有的还是将要激活的，都将被关闭。它的诡异之处还在于，动态禁令是可以自行执行的。当侵权内容被镜像到具有相同二级域名的其他网站时，知识产权所有者将不需要任何进一步的法院命令。他会直接去找互联网中介服务，要求他们关闭。

而动态禁令影响的是尚未存在的侵权行为，可能是展示合法内容的网站。最重要的是，如果基础设施运营商不遵守命令，可以认定为需要对损害负责。请放下一张。

在本案中，法院命令 Cloudflare 有针对性地禁用其内容分发网络服务，由此针对特定的 IP 地址或域名。

所以，我剖析这个话题的方法是，探索五个关键属性中，哪些属性受到这个判例法的影响。我也研究了属性二和属性三，但我知道这个案例肯定会影响到属性五，也就是网络中立性，因为不能认定基础设施运营商需要对其客户在互联网上发送的内容负责，也不应该要求他们控制数据和进行定向内容分发。

这一点在考虑到上周发生在 Fastly 内容分发网络服务提供商身上的事情时最为真实。许多网站中断了一个小时。请放下一张。

好了，我的行动呼吁。这是一个值得在各个层面讨论的问题，在 ICANN 政策论坛上，在 ICANN 社群内，在 IGF 上，无论哪个社群或利益相关方受到这种裁决或这种判例法的影响，都可以加入讨论。这在我的国家是很普遍的，但我知道其他司法管辖区也一直试图从这个判例法中得到启发。

因此，我要做的是开始观察是否有一些相关的问题已经在 GNSO 内部讨论过，特别是在互联网服务提供商选区和知识产权选区讨论过，以了解他们正在做什么、他们怎么想、他们是否对此有所了解。如果没有的话，就请参加本次会议的来自这些利益相关方团体的任何代表注意这个问题。

我想我的时间到了，所以交回给黛博拉。谢谢大家耐心的聆听。

黛博拉 • 艾斯卡勒拉： 谢谢，维罗妮卡。很不错的演讲。大家有问题要问维罗妮卡吗？我没看到有人举手或在聊天室提问。做得好，维罗妮卡。好的，这次我要确保没有漏掉问题。好的。太棒了。很好。我们将有请下一位演讲者西范 • 沙尔玛 (Shivam Sharma)。你好西范，欢迎你。好的，你有 10 分钟的时间，提醒一下，请说慢一点、清楚一点。谢谢。

西范 • 沙尔玛： 基本上，我将探讨 IoMT 设备的网络安全问题。请放下一张。什么是 IoMT？IoMT 表示医疗物联网。它是物联网即 IoT 技术的一个子集。它是医疗设备的集合，包括传感器、医疗[听不清]应用程序，它们连接到互联网，并将患者数据发送到云端，可由保健医生或医生远程访问，由此可以减少[听不清]的机会。请放下一张。

所以，这是一些 IoMT 设备，像个人健康，像智能手表，像健康手环，以及一些临床级的可穿戴设备，如监测糖尿病或测量血压的设备。所以这是一些临床可穿戴设备。

下一个是数字药丸。这些药丸里含有传感器，可以进入患者的胃里[听不清]，并开始向体外发送数据。这些数据可以通过智能手机或手环等设备查看。通过这些设备，保健医生可以[听不清]更详细地了解身体内部究竟发生了什么。

下一个是自动轮椅。这是指一些自动控制的轮椅。下一个是远程医疗。远程医疗是看医生时不再需要身体互动。所以基本上，在这种情况下，它不需要医生亲自去看病人。为实现这一点，有一些不同的[网亭]或某种视频会议服务，医生可以通过这些服务看到病人的细节，并提供远程健康咨询。

接下来是移动视网膜相机。这是一些可以戴在眼睛里的隐形眼镜，将向智能手机或某种便携式设备提供所有数据。接下来我们有一些机器人手术器械。基本上，这些器械用于内窥镜检查和腹腔镜检查。提供者或医生拍摄身体内部影像，这样他们就可以通过这些摄像机获得更多身体部位影像。

接下来是便携式病理学。我们不必去实验室进行检测，而是可以在家里使用一些设备来收集病人的数据。比如我们要进行血液测试，就可以在家里取样，设备会收集所有的数据并上传到云端，医生可以从云端获取所有的数据。

接下来是一些[听不清]。请放下一张。

黛博拉 • 艾斯卡勒拉： 西范，抱歉打断你。你可以调整一下你的电脑或耳机的音量吗？我们收到很多反馈和静电。我不知道怎么回事。

西范 • 沙尔玛： 抱歉。我换一副耳机。

黛博拉 • 艾斯卡勒拉： 好的，谢谢。你在用耳机吗，西范？

西范 • 沙尔玛： 是的，我在用耳机。

黛博拉 • 艾斯卡勒拉： 好的，很好。谢谢。

西范 • 沙尔玛： 大家听得到我说话吗？

黛博拉 • 艾斯卡勒拉： 可以，请继续。谢谢。

西范 • 沙尔玛： 现在，这是 IoMT 架构，那么这些 IoMT 设备如何工作。基本上，它们是[听不清]患者体内的不同传感器，比如一些[生命体征]传感器，像血压或像上升的血糖，或是一些智能健康手环，它们通过传感器收集数据，然后将数据传输到一个设备，该设备进一步通过 Wi-Fi 或某种电信方法如 4G 或 5G 将数据转发到云端，医生可以从云端访问所有数据，并为患者提供远程健康咨询。请放下一张。

这里，我们来看 IoMT 设备的增长，根据 AllTheResearch 的一份报告，2018 年，IoMT 市场价值为 440 亿，在 2016 年至 2026 年期间，它正以 24.4% 的速度逐年增长。而在 2026 年，预计将达到约 [2540 亿美元]。

因此，在预测年内，智能可穿戴设备类别可能会在市场上占据主导地位。2018 年，全球 IoMT 市场由智能可穿戴设备主导，占到市场的 27% 左右。即时医疗套件的 CAGR 最大，在全球 IoMT 市场中占 30%，预计实时监测应用的 CAGR 为 [25%。]跟踪和警报应用将以 [21%] 的 CAGR 增长。所以基本上，CAGR 就是复合年增长率。请放下一张。

这些是 IoMT 设备的一些好处，比如可以减少医疗费用。假设一个病人患有某种普通疾病，或者不需要立即住院，那么医生可以通过互联网提供远程咨询。所有数据将发送到云端。从那里，医生将访问报告并提供远程健康咨询。由此，它将减少住院的机会，也将减少费用。

同样，它也将改善患者的体验，所以没有什么可...患者不必担心什么，他或她不是非得去看医生。其次是增强医药的可管理性和医疗依从性。它将提供适当的管理，智能设备将能够自动管理一切事物，并提供一个良好的体验。同时，这些设备减少了出错的几率，由于具有良好的准确性，因此这些设备将提供良好的结果。此外它还将对医疗部门的浪费提供更好的控制，因为很多东西正被白白浪费掉。因此，它也将有助于减少某种[听不清]，它将提供更高效的服务，由此将产生更好的医疗结果。请放下一张。

IoMT 的一些缺点是，随着互联网的发展，一些网络攻击正与日俱增，将出现一些安全漏洞或网络攻击的机会。所以它们会攻击和感染设备。

基本上，EMR 即电子医疗记录的管理充满挑战，因为如果我们要收集病人的数据，就不得不遵循某些合规标准，如 HIPAA、FHIR，而要符合所有标准，确实是一个相当耗时的过程。在欧洲，有一些条例，如 GDPR，所以我们必须确保自己遵循这些条例。此外还有一些医疗标准，如 FHIR 和 SMART。这些都需要更多的时间来实施。请放下一张。

与 IoMT 设备相关的一些风险，比如开发这些设备需要很长的开发周期，所以基本上，如果我们制造了一个设备，就必须确保通过一些补丁持续更新它，并进行一些使它更安全的更新。

这些设备以患者生命安全为主要目标，所以[不是]设备安全性，但如今，随着技术日新月异的发展，这些设备的安全性也会不断改善。还有一些设备，以 Fitbit 为例，它使用蓝牙技术进行通信，可能会被黑客劫持。因此，我们可以收集患者的所有数据，包括位置和所有健康细节，这可能会影响患者。

有些设备有一个硬编码的密码，这是另一个重大风险，如果黑客能够访问这些设备，就可以轻易地入侵这些设备，从而轻而易举地从设备上收集所有数据。

此外还有未加密的通信。由于通信是以未加密的形式进行，所以将有机会被第三方读取，如中间人攻击，它可以读取所有数据。

下一个是缺乏设备管理。基本上，为了管理这些设备，我们应该确保遵循所有要求，不断更新所有设备，并且员工经过适当培训，知道如果出现网络漏洞或某种网络攻击，该如何应对。请放下一张。

这些是与这些设备相关的一些攻击。

黛博拉 • 艾斯卡勒拉： 西范，你已经超时了，所以请尽快结束。谢谢。

西范 • 沙尔玛： 好的。基本上，这些是攻击 — 我不打算解释，因为时间有限。这些攻击包括标签克隆、篡改和窃听，这些攻击可以影响 IoMT 设备。请放下一张。

如何提高这些设备的安全性？我们不应该使用[听不清]设备密码，而是必须将这些密码更新为一些强大的凭证。我们必须及时提供一些补丁，这样如果有任何安全漏洞，就将被及时修复。还要确保我们的网络更加安全，使它能够远离任何未经授权的网络访问。此外，我们的员工可能有机会将这些设备用于某种恶意目的，所以要确保我们根据要求列举白名单。所以，假设一名员工不使用设备，我们就要确保不允许他们访问这些设备，并确保这些设备受到[全天候]监控，这样如果任何恶意活动开始出现，就将被立即阻止。

接下来是缺乏遏制措施。[这不仅对击退攻击很重要。]我们必须确保能够在攻击发生之前处理它，因而必须确保我们的基础设施是安全的。请放下一张。

未来可能会出现挑战，它将改善医疗基础设施，所以未来几年会有更多的设备问世。以上就是全部内容。非常感谢大家花时间聆听我的演讲。如果你们有任何问题，请提出来。

黛博拉 • 艾斯卡勒拉： 谢谢西范。看起来里卡多举手了。里卡多，你有什么问题？

里卡多 • 南尼： 谢谢。谢谢西范，感谢你的精彩演讲。我不是物联网方面的专家，但我对它很好奇，据我所知物联网已经推动了很多非 IP 形式的连

接、互连和网络的发展。它是否也存在与物联网 IP 连接相同的那些安全问题，还是说它们有质的不同？谢谢。

西范 • 沙尔玛： 实际上，你可以在聊天框里发送你的问题吗？我想我的耳机坏了。

黛博拉 • 艾斯卡勒拉： 好的。谢谢。那么达尼尔，你可不可以也这样做？因为我们已经有点超时了，我们只剩下很少的时间，我想确保里卡多有机会介绍，并有时间提问。所以达尼尔，如果你能把你的问题也发在聊天框里，我会非常感激。

那么，我们的最后一位演讲者是里卡多 南尼。里卡多，下一个是你，请记住，你将有 10 分钟来演讲，然后我们将用最后的 5 分钟来提问。谢谢，里卡多。

里卡多 • 南尼： 谢谢，谢谢你邀请我。很抱歉，我没有真正的耳机，但我想通过耳机来减少任何类型的反馈噪音。我将从总体上谈一谈互联网碎片化，具体讲一个案例研究，再回到总体影响上。请放下一张。

好的，让我们从一些定义开始，什么是碎片化。[有些人开始]以许多不同的方式将它定义为：在不同的地方根据不同的规则提供不同的信息和服务。当然，这是一个非常广泛的定义，并将碎片化视为一个包罗万象的词语。例如，当我们在意大利和美国无法访问相同的 Netflix 内容时，我们会认为我们正面临互联网的碎片化吗？有监

管影响，有某种市场分割，但称其为互联网碎片化可能是一个充满了想象力的延伸。

因此，有些定义试图对碎片化进行分类，比如政府的、商业的和技术的。还有人试图把网络中立的概念纳入其中，并检查它是否与互联网碎片化有任何关系。接下来，我们对互联网碎片化下了最严格的定义，即基本标准、协议、不同 IP 的不兼容，不同的非兼容传输协议，而[听不清]会采取其他名称，其他标签。

因此，这些都是分类法，我们对碎片化有许多不同的定义。而我倾向于侧重技术性的定义，给所有其他现象另外的名称。请放下一张。

接下来说明我所认为的碎片化的含义，并说明为什么至少在技术层面上，我们可以对互联网保持整体统一持乐观态度。我想给大家展示一个案例研究，关于中国利益相关方和他们在 ICANN 的参与，说得更大一点是他们对唯一标识符治理的参与。

当然，在我们谈论碎片化的时候，我们倾向于谈论许多大国，而不仅仅是中国。也可以是俄罗斯 — 我们今天已经谈到了俄罗斯 — 但也有些人指责美国的一些项目易导致互联网碎片化。我只是拿中国举例，因为那是我研究的地理区域，也是我的强项。

观察中国的利益相关方，我们可以看到，在 ICANN 成立之初，中国似乎以非常对立的姿态对待 ICANN。当涉及到承认中国台湾的 GAC 成员地位，以何种形式采用何种名称时，中国政府便不再参与 ICANN 的活动。但是，私人组织或公共组织，甚至是国家资助的组织，仍然参与其中。

此后多年来，实际上，中国的利益相关方和中国政府一直在参与 ICANN 的活动，他们已然成为国际化域名的强大推动者，当然，在汉字域名空间中承载了很多利益，包括经济、政治以及文化利益。

起初，ICANN 和中国之间就谁应该在汉字域名方面拥有主导权发生了一些争执。人们甚至担心中国会建立一个独立的 DNS。但这种情况并没有发生，实际上，中国利益相关方充分参与了 ICANN，参与了 IDN 工作。

这时我们看到 ICANN 和中国之间有一个[听不清]。中国重新全面参与到政府咨询委员会中，并于 2013 年在北京主办了一次大型的 ICANN 会议。2014 年，当时的中国国家互联网信息办公室主任在 ICANN50 会议上认可了多利益相关方主义。请放下一张。

这当然对中国利益相关方在互联网碎片化和唯一标识符治理相关方面的立场产生了影响。例如，我们看到，在 IANA 管理权移交之后，中国 GAC 代表成为副主席，这标志着中国政府也有了更多的参与。同时，中国的利益相关方，甚至像华为这样的私人利益相关方，在与关键互联网资源和唯一标识符相关的其他领域，如 IETF，变得越来越有影响力。

然而，当华为、工业和信息化部以及其他中国参与者提出所谓的新 IP 提案时，在国际电信联盟 (ITU) 这个多边[场所]出现了新的地缘政治难题。

但是，尽管有各式各样的模糊性，我们看到中国的利益相关方已经越来越多地参与到 ICANN 中。通过下一张幻灯片，我将向大家展示其中的含义。请放下一张。

好了，我们现在的情况是，经过这么多年的对抗，中国的利益相关方，包括中国政府，开始更多地参与到 ICANN 中。他们使用和其他国家一样的 DNS 和协议。他们参与 ICANN。他们在 IETF 中很有影响力。跳过所有的方法论部分，我主要使用定性的方法，包括专家访谈，来收集这些数据。

究其原因，是因为强大的全球公司，强大的全球参与者想要获取网络利益。分裂的标准将迫使华为等公司为不同的市场生产不同的设备，因为他们应该能够连接到不同的非互用标准，而对于一家全球性的公司来说，在全球范围内生产一种设备要轻松得多。这样更加有利可图。

因此，可能发生的情况是，像中国和俄罗斯这样的国家，可能倾向于在国内监管方面拥有更大的影响力，规范在互联网上可以做什么，公民可以在互联网上从事何种活动，由此施加他们的政治影响，同时不考虑标准，以允许国内公司蓬勃发展。这就是中国在参与 ICANN、IETF 以及关键的[互联网资源]和整个互联网治理方面所采取的步骤，可以这么说。请放下一张。

所以我们现在看到的是，技术上的互联网碎片化是弱者的武器，而强者则更愿意保留网络利益。也许他们希望能够控制流量，特别是当涉及到信息以及涉及到公民社会组织起来的时候。但当涉及到技术标准时，他们希望能够在世界各地生产相同的设备，并在世界各地销售，保留[听不清]网络利益。

这告诉了我们关于互联网碎片化的什么信息？它告诉我们，最强大的参与者正试图从保持互联网统一中获得利益，只有最弱的参与者可能才试图在技术层面上分割互联网。而这使得互联网，IP、

TCP/IP，互联网的技术核心，非常具有弹性。毕竟，中国有强大的审查制度，但是在技术层面，只需要一个 VPN 就可以搞定它。当然，在某些语境下，如果你属于某些群体，那么使用 VPN 在政治上可能非常危险，例如，如果你是维吾尔族人。但是在技术层面上，只需要一个 VPN 就可以了。

因此，对互联网而言，在某种程度上保持其技术核心的统一是个好消息。虽然在互联网的一些非常基本的方面仍然存在争论的情况，模糊的情况，地缘政治冲突的情况，甚至是在技术层面，但系统似乎显示出了一些弹性。请放下一张。

这是我的结论。感谢你们的关注我很乐意回答大家的问题。

黛博拉 • 艾斯卡勒拉： 好的。谢谢，里卡多。大家有问题要问里卡多吗？有人举手或要在聊天框里提问吗？达尼尔，请讲。

达尼尔 • 格鲁贝夫： 谢谢里卡多的精彩演讲。它很有见地，也非常连贯。我想问一下，你对未来的碎片化状态可能会做出什么样的预判？你认为互联网的统一会占上风吗？还是你预感没那么乐观，有一些部分将变得孤立和碎片化。谢谢。

里卡多 • 南尼： 谢谢你的问题。这实际上是一个非常相关的问题。我想说，会有某种形式的市场分割，比如说许多西方国家不希望中国参与者介入他们的国内基础设施，即使是与电话有关的基础设施，比如说 5G，反

之亦然。因此，可能存在一个市场分割的问题。但是，当涉及到标准时，我看到一个融合的趋势，比如，IP 和 DNS 的情况就是如此，5G 也是如此。

回到 3G 时代，还有许多不兼容的区域标准或国家标准。即使它们得到了国际电联的认可，当时也只是在地方层面上部署，与世界其他地方部署的同一代标准无法互用，但仍然得到了国际电联的认可。从这个意义上说，现在我们有了更强的融合。我们有三个 5G 标准，但它们是可互用的，至少国际电联在批准它们时是这么说的。

所以有标准的融合，因为正如我所说的，大公司更喜欢能够在全球范围内生产设备，而不是以某种方式拥有自己的标准，他们希望在全球技术的专利方面拥有重大[机会]，并希望能够在世界各地销售设备和网络，从全球[规模]经济中受益。

但与此同时，我们可以看到由政府主导的商业碎片化，我们可以看到加强监管的趋势。在俄罗斯和中国是这样，我们看到政府在审查制度、数据本地化法规方面的影响力越来越大，但在欧洲和美国也是如此，特朗普政府一直高度干预 — 例如，看看干净网络项目，还有欧盟。GDPR 是一部非常先进的数据保护法规，但它也有很强的治外法权效力。

现在，当然，对于我作为欧盟公民来说，这是非常理想的。我觉得受到 GDPR 的高度保护，所以我完全支持它，不会批评它。我想说的是，欧盟也试图在数字市场和数字技术的未来发展中占有一定的分量，这也包括未来的互联网标准，因为互联网标准将对诸如人工智能等技术的未来发展产生影响，反之亦然，人工智能也[深深扎根

于] 5G，5G 是人工智能的推动力量，反之亦然，人工智能又融入 5G 网络中。

因此，如果你对数据有强大的控制力，当涉及到任何形式的人工智能发展时，你就可以发挥强大的杠杆作用，因为数据是真正的原材料。

所以，长话短说，在法规层面，也可能在信息控制方面，国家干预将加强，至少我们在中国看到的情况是这样，据我所知，在俄罗斯也是如此，但我不是俄罗斯的专家。但是有标准的融合。希望这个回答能让你满意。有的观点说得很绕。

达尼尔 • 格鲁贝夫： 好的。非常感谢。

黛博拉 • 艾斯卡勒拉： 好的。非常好。正好到时间了。谢谢，里卡多。演讲很精彩。还有今天的每位演讲人，我们所有的新生代计划学员，你们出色地完成了工作，非常棒。我为你们所有人感到骄傲。你们做得很好。

我要感谢今天出席的所有人。感谢今天负责播放幻灯片的费尔南达 • 伊恩斯 (Fernanda Iunes)。感谢我们的翻译，当然还有我们神通广大的技术团队，他们在整个会议期间，在每一场会议上都支持了我们。请加入我们明天新生代计划学员演讲的第二部分，时间是世界协调时 (UTC) 8:30，中欧夏季时间 (CEST) 10:30。谢谢大家的参加。感谢你们的支持，也感谢你们参加今天新生代计划学员演讲的第一部分。干得漂亮，各位。非常棒。谢谢你们的到来。如果有问题，请发送到 —

切丽 • 斯塔布斯： 谢谢，黛博拉。

黛博拉 • 艾斯卡勒拉： 谢谢。Engagement@icann.org，如果你有任何其他问题和后续问题要问我们的演讲者的话。非常感谢大家今天的参与。

切丽 • 斯塔布斯： 大家再见。

[会议记录结束]