DNS操作的全球测量  
  
保罗皮尔斯本琼斯†弗兰克李Roya Ensafi†  
Nick Feamster†Nick Weaver‡Vern Paxson  
加州大学伯克利分校普林斯顿大学  
‡国际计算机科学研究所  
  
fpearce，frankli，verng@cs.berkeley.edu fbj6，rensafi，feamsterg@cs.princeton.edu nweaver@icsi.berkeley.edu  
  
  
摘要  
  
尽管互联网审查制度普遍存在，并且审查制度的实施方式和审查制度不断演变，但审查制度的方式仍然相对较少。了解互联网审查的范围，规模和演变需要定期执行全球测量。不幸的是，现有技术依赖于总体上要求用户直接参与收集这些测量的技术，这大大限制了他们的覆盖范围并且禁止定期收集数据。为了便于进行大规模测量，以弥补理解上的差距，我们开发了Iris，这是一种可扩展，准确且符合道德的方法，用于衡量DNS解析的全局操作。虹膜揭示了许多域名的广泛DNS操作;我们的研究结果都证实了以前工作的轶事或有限的结果，并揭示了DNS操作的新模式。  
  
1引言  
  
轶事和报告表明，互联网审查是普遍的，影响至少60个国家[29,39]。尽管其普遍性，但揭示互联网聚合的范围和演变的经验性互联网测量仍然相对较少。世界各地对互联网审查的更全面的了解，不仅要求跨越国家，而且还要在单一国家的区域内，从各种地理区域和互联网服务提供商处获得各种各样的测量结果。即使在国家内部，多样性也是重要的，因为政治动态可以在内部有所不同，并且因为不同的ISP可能以不同的方式实施过滤策

。  
  
不幸的是，大多数测量互联网审查制度的机制目前都依赖于运行测量软件的志愿者部署在自己的互联网连接设备上（例如笔记本电脑，手机，平板电脑）[43,49]。因为这些工具依赖于人们安装软件和执行测量，所以它们不太可能  
  
  
  
可以达到收集关于互联网审查持续和多样化测量所需的规模。对理解互联网审查范围和发展所必需的规模和频率进行测量，需要基本上不需要人为干预或参与的新技术。  
  
我们的目标是开发技术，可以对全球网间操纵进行广泛的纵向测量，而无需个别用户参与感兴趣的国家。组织可以在互联网协议栈的多个层次上实施审查制度;例如，他们可能会根据IP地址阻止流量，或者他们可能会根据关键字阻止各个Web请求。最近的工作已经开发出技术来持续测量交通运输[23,42]和HTTP [45]层面的广泛操纵，但是我们在理解全球信息控制方面存在重大差距，这些控制涉及互联网域名系统（DNS）。为实现这一目标，我们开发并部署了一种方法和系统，以检测，测量和描述全球各国DNS操作的操作。  
  
开发一种准确检测DNS操作的技术会带来重大挑战。尽管以前的工作研究了不一致的DNS或其他反常异常[32,34]，但这些方法主要集中在确定可能反映各种潜在原因（包括配置错误）的DNS响应。相反，我们的工作旨在开发用于准确识别DNS操作的方法，指示意图限制用户对内容的访问。为了实现高检测准确性，我们依靠一系列基于DNS域，分辨率和基础架构的基础属性的元数据。  
  
一套检测指标侧重于一致性 - 直观地说，当我们从不同的位置查询域时，DNS响应中包含的IP地址应该反映来自普通服务器（即相同的IP地址）或相同的自治系统。  
  
  
另一套检测指标则着重于独立可验证性，与独立信息（例如与该域对应的网站的TLS证书中的身份）进行比较。这些指标中的每一个自然都适用于例外情况：例如，使用内容分发网络（CDN）的来自不同位置的查询通常会接收不同的IP地址（有时甚至是不同的CDN）。但是，我们可以将违反所有指标作为DNS操作的强有力指标。  
  
 除了获得准确的结果之外，另一个重大的设计挑战涉及道德问题。与明确让志愿者参与测量的系统相比，通过在互联网上部署的开放式DNS解析器发送DNS查询的方法引发了可能牵连实际上不同意参与测量的第三方的问题。使用“开放式解析器”可能存在问题，因为其中大多数不是实际的解析器，而是家庭路由器和其他设备中的DNS转发器[46]。审查员可能会将这些资源的请求错误地视为单个公民尝试访问审查资源的要求。

对牵连公民个人风险的认识需要详细了解不同国家的审查员如何监控对审查材料的访问以及他们如何惩罚此类行为。这些政策和行为可能会非常复杂，随着时间，地区，涉及的个人以及审查内容的性质而有所不同;这些风险可能难以准确降低。为此，我们的设计需要采取措施，尽可能确保我们只查询托管在互联网基础设施中的开放DNS解析器（例如，互联网服务提供商或云托管提供商内部），试图消除任何使用解析器或转发器在个人用户的家庭网络中。这一步减少了我们可以使用的DNS解析器集，从我们的测试数千万到几千。然而，我们发现，由此产生的覆盖率仍然足以实现DNS操作的全球视图，并且 - 重要的是 - 比以前使用开放式DNS解析器的研究更安全。

我们的工作做出以下贡献。首先，我们设计，实施和部署Iris，这是一个可扩展的用于测量DNS操作的ethical系统。其次，我们开发分析度量标准，以消除恶意操纵域中DNS响应的自然变化。第三，我们进行全球测量研究，强调各个国家，解决方案和领域的DNS操作的异质性。我们发现，即使在一个国家内，各种DNS解析程序的操作也不尽相同

.2有关工作

国家特定的审查研究。近年来，许多研究人员已经调查了特定国家的审查制度的最新情况和最新情况。这些研究往往跨越很短的时间，并且反映了目标国家内的单一有利位置，例如通过租用虚拟专用服务器。例如，研究专门针对中国[55]，伊朗[7]，巴基斯坦[38]，叙利亚[12]和埃及[8]的审查制度。研究还探讨了各种审查方法的应用，例如注入虚假DNS答复[5,36]，阻止TCP / IP连接[54]和应用程序级别阻止[19,33,41]。一些研究表明，国家有时会在围绕政治事件的时代改变其阻断政策和方法。例如，自由之家报告了15起互联网关闭事件 - 政府仅在2016年就完全切断了对互联网的访问[29]。其中大部分显然是为了防止公民接触社会媒体散布不需要的信息。

其他研究表明，政府关注涵盖了各种各样的服务和主题，包括视频门户网站（例如youtube.com） [51]，博客（例如livejournal.com）[3]和新闻网站（例如bbc.com）[9]。审查人员还针对规避和匿名工具。最着名的是，中国的长城防火墙与Tor [24，53]进行了长达十年的猫捉老鼠游戏。虽然这些研究提供了重要的数据点，但每个数据点都反映了单个时间点的快照，因此无法捕捉审查实践中的持续趋势和变化。

全球审查测量工具。多次重新搜索努力开发了平台，通过从各种有利点进行实验来衡量审查制度。例如，CensMon [48]使用不同国家的PlanetLab节点，UBICA [1]通过在家庭网关设备和用户桌面上运行审查测量软件来增加有利位置。实际上，据我们所知，这些框架都没有被解雇和收集数据。 OpenNet Initiative [39]利用其公众形象在过去十年中每年在全球范围内招募志愿者，他们每年从家庭网络进行一次性测量。 OONI [49]和ICLab [30]是两个正在进行的数据收集项目，它们使用志愿者运行定制软件和定制嵌入式设备（如Raspberry Pis [26]），尽管每个框架都可以执行一系列测试，他们依靠在他们的互联网连接设备上运行测量软件的志愿者。这些人类的参与使得它更具挑战性 - 如果不是不可能的话 - 收集连续和多样化的测量.Pearce et al。最近开发了Augur，一种使用TCP / IP侧通道执行纵向全局测量的方法[42]。虽然Augur检查类似作为Iris的一组域和国家，它侧重于识别基于IP的中断而不是基于DNS的操作。

**测量DNS操作**。 DNS协议缺乏身份验证和完整性检查，使其成为攻击的主要目标。 Jones等人提出了检测未经授权的DNS根服务器的技术，尽管在实践中发现这种操作很少[32]。江等人。发现DNS缓存的最新策略中存在一个漏洞，即使从区域文件中删除，恶意域也可以保留在缓存中[31]。有几个项目利用有限数量的有利位置探索了DNS操作。韦弗等人。为了广告的目的，针对DNS重定向的前处理DNS操作[52]。作者还观察到DNS解析器将终端主机重定向到恶意软件下载页面的事件。有许多国家特定的研究显示了不同国家如何使用各种DNS操作技术来检测互联网审查。例如，在伊朗，政府期望互联网服务提供商配置其DNS解析器，将有争议的域名重定向到审查页面[7]。在巴基斯坦，ISP返回NXDOMAIN响应[38]。在中国，远程防火墙注入伪造的DNS数据包，其IP地址看似任意[5]。然而，这些研究都利用了一小部分或地理位置有限的有利位置，并在短时间内使用了开放式解析器。许多研究通过探测IPv4地址空间来查找开放的解析器，从而大规模地进行了DNS操作。 2008年，Dagon等人。通过使用200,000个开放式解析器运行测量发现腐败的DNS解析器[18];他们不会分析潜在审查的结果。 2012年匿名作者[4]进行的一次类似扫描显示，中国DNS审查制度影响非中国系统。Kuhrer等人在2015年开展了后续工作。解决了一个更大的范围：数百万个数百万的开放式解析器查找了155个域名[34]。该研究检查了广泛的潜在篡改结果，除审查外，还包括恶意软件，网络钓鱼，域名停放，广告注入，俘虏门户，搜索重定向和电子邮件传递。他们通过比较来自开放式重新求解器的DNS响应和查询控制解析器收集的地面实况分辨率来检测DNS调解。然后，他们使用一些启发式筛选阶段来识别合法的未经处理的答案，例如，如果其返回的IP地址与地面实际IP地址相同，则将不同的响应视为合法imate。我们尝试使用他们的方法专门为检测审查而进行全球测量。然而，审查检测并不是他们工作的重点，本文没有明确描述检测过程的细节。特别是，除了检查HTTP页面“被......排序” “措辞，该文件没有提供决定过程来确定给定的操纵操纵的实例是否反映了审查制度或其他一些现象。此外，他们的测量充分利用了开放式解决方案，这对最终用户可能因试图访问被禁内容而被错误地提出了道德担忧。相比之下，我们构建了一个明确的，可重复的方法，以道德负责的方式在全球范围内测量基于DNS的操作。2016年，Scott等人推出了Satellite [47]，该系统利用开放式解析器通过采集的分辨率识别CDN部署和网络干扰。给定一个双向图连接查询的域与从开放式解析器收集的IP地址答案，Satellite识别强连接的组件，这些组件表示由相同服务器托管的域。卫星将CDNs与网络干扰区分开来，将其作为具有高度相似域的组件（另外，其他启发式有助于改进此分类）.3方法在本节中，我们描述了Iris，一个可扩展的轻量级系统来检测DNS操作。我们首先研究问题空间，确定各种度量构件的能力和局限性，并说明我们对威胁模型的假设。我们阐述了我们选择（1）要测量哪些域名的过程，以及（2）考虑伦理和可伸缩性问题的有利位置来衡量它们的过程。然后，根据一组测量点和DNS域名，我们描述了我们如何表征测量结果，并根据一致性或独立性使用它们得出关于DNS操作是否正在发生的结论我们接受的回应的可验证性。接下来，我们根据现有的道德规范和准则考虑我们的技术方法，并解释各种设计决定如何帮助我们遵守尽可能地与这些原则相关联。最后，我们讨论Iris的隐含和技术局限性。3.1概述我们的目标是确定DNS操作，我们将其定义为DNS响应的实例，这两种操作都有（1）有贡献（例如，IP地址，自治系统，web内容）与一个明确的控制集不一致;和（2）返回与独立信息源（例如，TL​​S证书）相比证明不正确的信息。方法。检测DNS操作概念很简单：在高层次上，这个想法需要通过地理上分散的DNS重新求解器来执行DNS查询，并分析响应的活动，以表明DNS域的响应可能被调节。然而，尽管其显而易见的简单性，实现一个可伸缩地收集DNS数据并对其进行分析以进行处理的系统会带来道德和技术挑战。道德挑战涉及选择不涉及无辜公民的DNS解析器，以及确保虹膜不会给DNS解析基础设施带来不适当的负担; x3.2解释了我们用于推理设计选择的道德准则。 x3.3描述了Iris如何选择一套“安全”的开放式DNS重新求解器;技术挑战的核心是开发用于检测操纵的合理方法，我们在x3.4和x3.5中描述了这些方法。识别要查询的DNS名称。 Iris查询由Citizen Lab [14]编制的敏感URL列表。我们将此列表称为Citizen Lab Block List（CLBL）。这份网址列表由世界各地专家根据已知的审查报告编制，按类别划分。我们将URL提取到域名，并将此列表用作我们数据集的基础。然后，我们通过添加从Alexa Top 10,000 [2]中随机选择的其他域名来补充此列表。这些额外的域名有助于解决CLBL中的地理或内容偏见，同时不会显着增加查询的总数。假设和重点。首先，Iris旨在确定互联网服务提供商和国家的广泛操作。我们无法识别针对特定个人或使用高价值资源（例如有效但被盗的证书）的人群或人群或操纵活动的操纵。其次，我们专注于不依赖隐身的操纵手法;我们假设对手将使用DNS重新求解器来操纵对DNS查询的响应。我们假设攻击者不会返回不正确的IP地址，而是在相同的IP前缀中作为正确答案[5,7,38]。最后，在将DNS调解归因于某个特定的国家或属地时，我们依靠Cen-sys提供的国家信息[21]，并辅以MaxMind的[37]数据集，将解析器映射到特定国家（或从属terri- tory）.3.2伦理虹膜的设计融合了许多重新审视伦理的考虑。我们主要的道德问题是与Iris进行的度量相关的风险，因为通过我们不拥有的解析器发布可能被删除或操纵的DNS域名的DNS查询可能会牵涉其他无辜用户。第二个问题是，我们生成的DNS查询是否为我们不拥有的域的权威DNS名称服务器引入了过度的查询负载。考虑到这些顾虑，我们考虑用虹膜进行测量的道德标准，使用贝尔蒙特报告[10]和门洛报告[20]的道德准则来构思我们的讨论。一个重要的道德原则是尊重个人;从本质上讲，这个原则指出，实验应该尊重人类作为自主决策者的权利。有时候这个原则被误解为所有实验的知情同意要求。然而，在许多情况下，知情同意既不实际也不必要;因此，Salganik [44]将这个原则描述为“对大多数事物的某种同意”。就Iris而言，获得所有开放的DNS解析器运营商的同意是不切实际的。取代试图获得知情同意的做法，我们转而谈到善意原则，这对衡量与实验相关的风险进行实验的益处。请注意，善意的目的不是消除风险，而仅仅是尽可能减少风险。 Iris的设计在很大程度上依赖于这一原则：具体来说，我们注意到通过数千万重新解决方案发布DNS查询的好处具有快速递减的回报，并且仅使用我们可以确定的开放式解析器不太可能与个人用户在不显着降低实验效益的情况下降低任何个体的风险。我们注意到，我们在这方面对伦理的考虑与通过开放式DNS解析器inf发出查询的先前工作有很大差异但没有考虑道德问题。正义原则指出，实验的受益者应该是具有该实验风险的相同人群。在这方面，我们认为我们使用Iris收集的各种衡量标准的受益者范围广泛：规避工具的设计者，以及正在改进通信工具的决策者，重新搜索者和积极分子，为受压迫政权的公民提供互联网和连接都需要更好的关于互联网审查范围和范围的数据。简而言之，即使在一个开放的DNS解析器所在国的某个实体可能因为我们所进行的测量而承担一定风险的情况下，我们也设想这些相同的实体最终可能从研究，决策中受益，并且工具的发展促进了Iris的发展。最后一条准则涉及对法律和公共利益的尊重，它基本上将利益原则扩展到所有相关利益相关者，而不仅仅是实验参与者。这个原则对推理我们的DNS查询通过增加各DNS域名服务器上的DNS查询负载所创建的外部性很有用。为了遵守这一原则，我们对每个DNS域的DNS查询进行评级限制，以确保这些域的所有者不会因为我们发布的查询而面临巨额开支。此速率限制是必要的，因为一些DNS服务提供商基于峰值或接近峰值的查询速率收费.3.3开放式DNS解析器为了获得广泛的测量有利点，我们使用部署在世界各地的开放式DNS解析器;这样的解析器将解析任何客户端的查询。使用开放式DNS解析器进行测量是一个道德上复杂的问题。以前的工作已经确定了世界各地数以万计的这些解决方案[34]。考虑到它们的普遍性和全球多样性，开放式解析器是一个令人信服的资源，为研究人员提供了可观的数量和覆盖范围。不幸的是，开放式解析器不仅对互联网而且对个人用户构成威胁。开放式解析器可能是配置错误的结果，而且经常在最终用户设备上，例如家庭路由器[34]。使用这些设备进行测量可能会产生货币成本，并且如果测量涉及敏感内容或主机，可能会使所有者受到伤害。此外，开放式解析器也是各种在线攻击的常用工具，例如分布式拒绝服务（DDoS）放大攻击[35]。尽管有必要减少开放解析器的普及及其潜在影响[40]，但它们仍然普遍存在。由于这些以及我们在x3.2中讨论的伦理考虑，我们限制了一组开放的解析器，使用几千个解析器，我们可以确定地确定它们是互联网基础设施的一部分（例如，属于互联网服务提供商，在线云托管提供商），而不是归因于任何单独的个人。图1说明了Iris发现安全开放DNS解析程序的过程。我们现在更详细地解释这个过程。从概念上讲，这个过程包括两个步骤：（1）扫描Internet的开放DNS解析器;或者（2）修剪我们确定的开放式DNS解析器列表，以将解析器限制为一个我们可以合理地归因于Internet基础架构的集合。通过使用我们无法控制的DNS解析器，我们无法区分全国范围内的或州审查和本地化操作（例如，俘虏，恶意软件[34]）。因此，图1：Iris的DNS解析器识别和选择管道概述。 Iris首先对整个IPv4地址空间进行全局扫描，然后对所有开放式解析器进行反向DNS PTR查找，最后过滤解析器以仅包含DNS基础架构。我们必须在ISP或国家级别上汇总和分析结果。步骤1 ：扫描Internet的IPv4空间以获取开放式DNS解析程序。扫描IPv4地址空间为我们提供了所有开放式解析器的全局视角。为此，我们开发了ZMap [22]网络扫描器的扩展，以启用Internet上的DNS解析1。该模块使用递归DNS A记录查询查询所有IPv4地址的端口53。我们使用我们控制这些查询的目的注册的域名来确保已知的正确答案。我们从具有PTR记录的IP地址进行测量和扫描，将PTR记录标识为“研究扫描仪”。这些IP地址还提供了识别我们学术机构的网页，并提供了选择退出扫描的功能。从这些扫描中，我们选择所有返回此查询的正确答案的IP地址，并将它们分类为开放式解析器。在x4.1中，我们探讨了我们用于研究的开放DNS解析器的数量。步骤2：识别基础架构DNS解析器。给定Internet上所有打开的DNS解析器的列表，我们修剪此列表以仅包含可解析l的DNS解析器可能归因于互联网基础设施。为此，我们的目标是确定开放的DNS解析器，这些解析器可以作为给定DNS域的权威域名服务器。 Iris对所有打开的解析器执行反向DNS PTR查找，并仅保留具有以子域ns [0-9] +或名称服务器[0-9] \*开头的有效PTR记录的解析器。这个过滤步骤减少了可用的开放式解析器的数量 - 从数百万到数千 - 甚至剩下的一组开放式DNS解析器提供了广泛的国家和网络级覆盖（在x4.1中进一步表征）。使用PTR记录来识别基础设施可以拥有1我们的扩展已被接受进入开源项目，并且我们的扫描结果可作为Censys [21]系统的一部分。假阴性和假阳性。并不是所有的基础架构解析器都会有一个有效的PTR记录，也不是所有的权威名称服务器。这些虚假负面限制了我们测量的范围和规模，但对降低风险是必要的。同样，如果用户在他们的家庭IP上操作他们自己的权威域名服务器，或者如果PTR记录与我们的命名标准相匹配但是不具有权威性，我们的方法会将IP识别为基础设施（误报）。3.4执行测量提供要查询的DNS域名以及我们可以从中发布查询的全局开放式DNS解析程序集，我们需要一种机制，将这些域的查询发布到我们掌握的解析程序集。图2显示了测量过程的概述。在高层次上，Iris使用开放式DNS解析器提供的全局有利位置解析每个DNS域，使用来自外部数据集的信息以及额外的主动探测注释响应IP地址，并使用一致性和独立可验证性度量标准识别被操纵的反应。本节的其余部分详细描述了这个度量过程，而x3.5描述了我们如何使用这些度量结果来最终识别操作。步骤1：执行全局DNS查询。 Iris将输入合适的开放式DNS解析器列表，以及组合的CLBL和Alexa域名作为输入。除了我们对测试感兴趣的DNS域名之外，我们还包括3个受我们控制的DNS域名，以帮助我们在识别操作时计算我们的一致性指标。在成千上万的解析器中查询数以万计的域名需要开发一个新的DNS查询工具，因为现有的DNS测量工具不支持这种规模。我们在Go [27]中实现了这个工具。该工具将输入一组域和解析器作为输入，并协调每个解析器中每个do-main的随机查询。该工具支持多种查询类型，其中多个查询类型可以在每次运行中指定，包括A，AAAA，MX和ANY。对于每个（域，重新求解器）对，该工具都会创建一个递归DNS请求并将其发送给解析器。递归查询请求解析器解析域并返回最终答案，记录所有响应，包括超时。该工具遵循一组响应将每个域解析为IP地址。例如，如果解析器返回CNAME，则该工具会向解析器查询该CNAME的解析。为确保解析器不会过载，该工具包括可配置的速率限制。对于我们的实验，我们将解析器的查询限制在每秒5秒的上限。在实践中，由于到达解析器的网络延迟以及解析器执行草皮响应所花费的时间，此速率往往会低得多。为了处理经常不稳定或超时的特定解析器，该工具提供了一个可配置的失败阈值，如果太多查询失败，该工具会暂停特定解析器的一组测量。为确保我们查询的域不会过载，工具会随机化订单并且限制并行查询的解析器的数量，以便在最坏的情况下，没有领域每秒经历超过1次查询，期望。步骤2：使用辅助信息注释DNS响应。我们的分析最终依赖于对我们收到的DNS响应的一致性和独立可验证性进行特征化。要启用此分类，我们首先必须收集有关每个DNS响应中返回的IP地址的更多详细信息。 Iris使用有关每个IP地址的地理位置，自治系统（AS），端口80 HTTP响应和端口443 HTTPS X.509证书的附加信息来注释在DNS响应集中返回的每个IP地址。我们依靠Censys [21]数据集来获取这个辅助信息; Censys每天提供这些信息的快照。该数据集不包含每个IP地址;例如，数据集不包含没有开放端口的IP地址，或者攻击者可能会返回返回错误页面的IP地址或者否则无响应。在这些情况下，我们使用AS和来自Maxmind服务的地理位置信息注释我们数据集中的所有IP地址[37]。附加的PTR和TLS扫描。对于每个IP广告，我们执行DNS PTR查找以协助我们后续的一致性表征（我们在x3.5中详细介绍的一个流程）。注释练习中的另一个复杂因素是实际上单个IP地址可能通过HTTP或HTTPS（即虚拟主机）托管多个网站。因此，当Censys跨整个IPv4地址空间通过端口443（HTTPS）检索证书时，Censys检索到的证书可能与服务器响应通过TLS的服务器名称指示（SNI）扩展查询返回的证书不同。这种差异可能导致Iris将虚拟主机误称为DNS不一致。为了减轻这种影响，对于每个产生的IP地址，我们使用SNI形成额外的活动HTTPS连接，指定最初查询的名称。我们使用这些信息来注释所有响应，我们将其用于答案分类（在x5.1中进一步检查）.3.5识别DNS操作为了确定是否操纵DNS响应，Iris依赖于两种度量类型：一致性度量标准图2：DNS概述分辨率，注释，过滤和分类。 Iris输入一组域和DNS解析器，并输出指示被操纵的DNS响应和独立可验证性度量的结果。我们说如果满足任何一致性或独立的可验证度量标准，则反馈是正确的;否则，我们将反应分类为操纵。在本节中，我们概述了每类指标以及我们为分类答案而开发的具体特征。本节的其余部分定义了这些指标; x5.1探讨了它们各自的功效。3.5.1一致性即使从各种全球有利位置访问，对域的访问也应具有某种形式的一致性。这种一致性可能采用网络属性，基础设施属性甚至内容的形式。我们利用这些属性，无论是控制数据还是整个数据集本身，都可以对DNS响应进行分类。一致性基线：控制域和重新求解器。我们对一致性概念的核心是拥有一套我们控制的地理上多样化的解析器，可能（可能）不会被操纵。这些控制为我们提供了一系列高可信度的正确答案，我们可以使用这些答案来确定一系列IP广告服饰属性的一致性。地理多样性有助于确保特定区域的部署不会导致误报。例如，我们数据集中的多个域使用不同的内容分发网络（CDN）承载北美以外的基础设施。作为我们测量的一部分，我们插入我们控制的域名，并带有已知的正确答案。我们使用这些域来确保重新求解器可靠地返回非敏感内容的非操作结果（例如，不是强制门户）。对于每个域名，我们通过跨每个度量的并集创建一组一致性度量我们所有的控制解析器。例如，如果控制A返回答案192.168.0.10和192.168.0.11，而控制B返回192.168.0.12，我们创建一组一致的IP集（192.168.0.10,192.168.0.11,192.168.0.12）。如果对于每个度量，答案都是控件的非空子集，那么我们说答案是“正确的”（即不是操纵性的）。返回到我们的IP示例，如果全局解析器返回答案（192.168.0.10,192.168.0.12），则将其标识为正确。当请求返回多个记录时，我们检查所有记录，并且如果任何响应通过了适当的测试，则认为回复良好。此外，与我们在不同地理位置的多个国家/地区进行的实验同时收集的未操作被动DNS [6]数据可能会增强（或替换）我们的一致性指标。不幸的是，我们并不知道这样的数据集可以公开获得.IP地址。最简单的一致性指标是DNS响应包含的IP地址或IP地址。自治系统/组织。对于地理上分布的站点和服务（例如托管在CDN上的站点和服务），作为正常操作的一部分，单个域名可能会返回不同的IP地址。为了试图解决这些差异，我们还检查域的不同IP地址是否映射到我们通过控制解析器发出域名查询时看到的相同AS。由于单个AS可能有多个AS号（ASN），因此我们将两个具有相同ASN或AS组织名称的IP地址视为来自同一AS。尽管即使个别IP地址不同，许多响应也会显示AS一致性，即使其查询未被操纵的域也有时会返回不一致的AS级和组织信息。这种不一致性在larg中尤其常见e服务提供商的基础设施跨越多个区域和连续性，并且通常是收购的结果。为了解决这些不一致问题，我们需要在协议堆栈的更高层（特别是HTTP和HTTPS）中使用附加的一致性度量标准，如next.HTTP内容所述。如果IP地址在端口80上运行Web服务器，我们会包含作为附加一致性指标返回的内容的散列。这些内容哈希来自端口80的IP地址Censys爬网。此指标可有效识别动态内容有限的网站。正如x5.1中所讨论的那样，该指标在识别具有动态内容但共享基础设施的网站时也很有用。例如，由于这些哈希基于HTTP GET使用IP地址作为头中的主机提取，因此可以获取唯一的指纹并分类CDN故障或默认主机页。在另一个例子中，Google的大部分网络托管基础架构都会将字节相同的重定向页面返回给http://www.google.com/用于没有有效Google主机标头的HTTP GET。这些相同的页面允许我们将Google分辨率标识为正确，即使对于作为Point-of-Presence.HTTPS证书的IP地址也是如此。如果连接时显示的HTTPS证书的哈希匹配通过我们的控件返回的IP的哈希，我们会将响应标记为正确。请注意，这不是一个独立的可验证度量标准，因为证书可能或不可信，甚至可能对于CDN的域.PTRs不正确。根据我们的控制数据，我们根据PTR，AS和证书信息对特定CDN上托管的区域进行分类。如果该响应的PTR记录指向相同CDN，我们认为非控制响应是一致的。3.5.2独立可验证性除了一致性度量标准外，我们还定义了一组度量标准，我们可以使用外部数据源独立验证这些度量标准作为HTTPS证书基础设施。我们在下面描述这些方法.HTTPS证书。如果IP地址在没有SNI的情况下查询时为正确的域名提供有效的，浏览器信任的证书，我们认为DNS响应是正确的，与控件无关。我们进一步扩展这一指标以允许常见的配置错误，例如在请求example.comHTMLPS证书和SNI时返回\* .example.com的证书。我们添加了一个附加指标，用于检查从我们的后续启用了SNI的扫描返回的证书是否为正确的IP地址返回了有效的，浏览器信任的证书。3.6限制为了便于全球范围内的测量，我们的方法存在局限性，范围和限制我们的结果。本地化操作。由于Iris完全依赖于我们无法控制的开放式基础设施解决方案，在解决方案较少的地区，我们无法区分解析器运营商与ISP或全国范围内操作之间的本地化操作。分析不正确的结果，关注ISP或国家/地区的一致性，或检查网页内容，可能有助于识别本地化操作。域名偏差。从我们的基础设施解析器组中，我们测量CLBL的操作和Alexa顶级站点的子集。尽管CLBL是一项基于社区的努力，旨在全球范围内识别敏感内容，但其本质并不完整。缺少网址和网域，敏感内容可能会比列表更新更快。同样，该清单可能会根据项目的语言以及对其的贡献而表现出地理偏见。这种偏见可能会影响虹膜可以检测到的操作的相对数量和范围。尽管我们专注于ISP或国家级别的操纵，但一个活跃的对手仍然可以试图逃避我们的测量。上游解析器可以使用EDNS客户端子网[16]来仅处理某些目标IP范围的结果，或者ISP解析器可以选择仅处理他们自己的客户。执行注入的国家级防火墙可以识别我们的扫描IP地址，并且不会注入结果或完全阻止我们的通信。攻击者也可能利用我们的一致性指标并在与目标相同的AS内注入不正确的IP地址。地理位置错误。我们依靠Censys [21]和Max-mind [37]进行地理位置和基础设施解析人员的AS标记，以执行国家或ISP级聚合。不正确的标签会将全国范围内的操作标识为不完整（假阴性），或在不存在的国家/地区确定操作（误报）.4数据集在本节中，我们将收集的数据和我们如何处理以获得使用的结果在我们的分析中.4.1开放式解析器选择我们最初通过互联网范围内的ZMap扫描，在2017年1月使用我们对ZMap的DNS扩展名，确定了大量开放DNS解析器。总共有420万开放式解析器响应，并且答案正确到我们的扫描查询。这个数字不包括r解析器总数中位数/数据集解析器国家/地区所有可用4,197,543 232 659.5Ethically可用6,564 157 6.0实验组6,020 151 6.0表1 ：DNS解析器数据集。我们确定所有功能正常的开放式解析器都在IPv4地址空间中。实验集由通过超出我们基本扫描范围的附加功能测试的解析器组成。请注意，国家数量包括依赖地区。解散者数据集AF AS EU NA NA OC SA全部可用55 49 52 41 21 14Ethically可用29 42 42 25 8 11实验组26 41 41 24 8 11表2：国家（及其附属地区）由大陆持有可用的解析器。 AF =非洲，AS =亚洲，EU =欧洲，NA =北美，OC = Oceana /澳大利亚，SA =南美。我们可以在不同国家调查DNS调解的程度取决于地理分布选定的DNS解析器。通过使用Censys [21]和MaxMind [37]对这组初始解析器进行地理定位，我们发现这些解算器在232个国家和依赖地区2中重新组合，每个国家中位数为659个解算器。由于我们在x3.2中概述的道德考虑因素，我们将这组解决方案限制在157个国家的6,564个基础设施解决方案，同样每个国家的中位数为6个解决方案。最后，我们移除不稳定的或其他异常的重新求解器; x4.3更详细地描述了这个过程。这种过滤将151个国家的可用解析器集合减少到6,020个，每个解析器的中位数为6。表1总结了由此产生的解决方案人口;表2显示了各大洲的分布情况。我们还使用4个不同地理位置的解决方案进行受控实验; 2台谷歌公共DNS服务器[28]，一台在亚马逊AWS上托管的Ger-man开放式解析器，以及我们在加利福尼亚大学伯克利分校管理的重新求解器.4.2域选择我们调查了对已知被截取的两个域的DNS操作和流行网站的域名。我们从公民实验室阻止列表（CLBL）[14]开始，由1376个敏感域组成。我们通过从Alexa Top 10,000中随机选择的1,000个域名以及我们人类的3个控制域来增加此列表，这两个域是由ISO 3166-1 alpha-2代码（Maxmind的国家地理位置的粒度）定义的.Response Total Number NumberDatasets响应Resolvers域所有响应14,539,198 6,564 2,330过滤后13,594,683 6,020 2,303表3：过滤前后的DNS响应数据集问题解析器，域和失败的查询。不应该被操纵的数据。由于两个域集之间的重叠，我们的组合数据集包含2,330个域。我们排除了通过我们的数据收集过程确定的27个有问题的域名，导致我们的最终人口为2,303个域名.4.3响应过滤我们为2,330个预过滤域发布了1450万DNS A记录查询，涉及6,564个基础架构和控制在2017年1月的2天期间开放解决方案。我们观察到需要进一步过滤的各种错误行为。排除这些退化情况后，我们的数据集收集量减少到2,303个域和6,020个解析器，共计1,350万个响应，如表3所示。本节的其余部分详细介绍了这个过滤过程。我们发现在我们的实验中，有341名解决方案人员停止了对我们的查询的回应。尽管以前在我们的全网扫描期间正确回答，但额外的202解析器错误地解决了我们的控制域名。这种行为的常见原因是速率限制，因为我们的互联网范围内的扫描仅查询解析器一次，而我们的实验需要重复查询。我们发现了另一个有问题的解析器，由于积极的速率限制，查询失败率高于70％。我们从我们的数据集中消除了这些解析器及其关联的查询响应，将有效响应的数量减少了510K。域名。我们的控制DNS解析器无法解析15个域名。我们排除了这些数据集及其相关的90K查询响应。我们重新移动了另外12个域名及其相应的72​​K查询响应，因为他们的DNS解析失败了自动配对的完整性检查;各个国家/地区的解析器为这些域中的每个域提供了相同的错误DNS解析，并且每个域返回的IP地址是唯一的（即，不是块页面或过滤设备）。我们并没有期望审查员展示这种行为。一个单一的审查员不可能跨越多个国家或地理区域进行操作，而诸如在各个国家之间使用单一IP地址的块页面等操作也应该分布在多个域中。这些域不支持HTTPS，并在地理位置上显示出来cific部署。随着控制解析器的地理多样性的增加或这些站点的HTTPS部署，我们的一致性或可验证性度量将考虑这些域。查询。我们过滤了另一个返回失败错误代码的256K查询;所有错误中有93.7％是超时和服务器故障。超时表示解析器在15秒内未响应我们的查询的连接。服务器故障指示解析器何时不能在其预先配置的时间分配内重复解析域（在BIND中默认为10秒）。表4提供了错误响应的详细分类。失败类型计数响应百分比超时140,551 0.97％服务器失败107,826 0.74％拒绝接受7,823 0.05％连接错误3,686 0.03％截断3,451 0.02％NXDOMAIN 1,713 0.01％表4：265,050 DNS响应重新导致了一个不成功的错误代码。返回一个NXDOMAIN响应代码[38]，它告诉客户端一个域不存在，是一种明显的潜在DNS检查机制。不幸的是，一些CDN在正常的操作中返回这个错误，大概是由于速率限制或客户机配置设置。我们发现在汤加和巴基斯坦国家发生的最流行的NX行为;两国都展示了多种内容类型的审查制度，包括成人和LGBT。先前的研究已经观察到巴基斯坦NXDOMAIN阻塞[38]。这些实例仅占整个NX-DOMAIN响应的一小部分。鉴于NXDOMAIN的许多非审查反应以及它们用于审查的相对频繁次数，我们将这些从我们的分析中排除。另外72K的答复有一个SUCCESS响应代码，但在响应中没有包含IP地址。这种失败模式经常与CNAME响应一致，无法进一步解决。我们排除了这些查询。表5提供了NXDOMAIN响应的地理分类。删除有问题的解析器，域和失败的查询后，数据集包含13,594,683个DNS响应。通过应用我们的一致性和独立可验证性度量标准，我们确定了41,778条被操纵的答案（0.31％），分布在58个国家（和附属地区）和1,408个域名。国家％NXDOMAIN汤加2.93％巴基斯坦0.37％波斯尼亚/黑塞哥维那0.12％Isle男性0.04％佛得角0.04％表5：NXDOMAIN回答的查询百分比中排名前五位的国家/地区。 7000相同CDN相同证书w / SNI正确证书相同HTTP Page 6000正确证书带有SNI相同IP地址解析器相同证书相同AS 5000 4000数量3000 2000 1000 0 0.0 0.2 0.4 0.6 0.8 1.0响应比例按特征修正图3：每个正确性度量将反应分类为正确的能力。表格按从左到右的顺序排列（从上到下，从左到右）.5结果我们现在评估我们的DNS操作指标的有效性，并探讨在互联网审查环境中操纵的DNS响应。评估操作指标为了评估一致性和独立可验证性指标的有效性，我们量化了每个指标识别未操作反应的能力（以排除进一步调查）。图3显示了每个指标的功效。水平轴代表来自特定解析器的响应的分段，其被特定的度量分类为正确的。垂直轴表示分解器的数量，表现出正确响应的相同分量（同样在给定度量下）。例如，在“相同CDN”度量标准下，近6,000名解析者大约有8％的答案被确定为正确答案。窄带表示许多重新求解器在该度量下展示类似的正确响应分数（即，它更稳定）。直方图的中心质量越接近1.0，其相应度量的效果越好，因为使用该度量将响应的大部分分类为正确（即，不是操纵）.1.00 0.98解析器0.94 0.96比例0.92 0.90 0.88 0.86 0.00 0.05 0.10 0.15 0.20 0.25 0.30 0.35被操纵的响应比例图4：每个解析器操纵的响应比例。对于89％的解算器，我们没有观察到操纵。国家（#Res。）中值平均值最大值最小值伊朗（122） 6.02％5.99％22.41％0.00％CHina（62）5.22％4.59％8.40％0.00％印度尼西亚（80）0.63％2.81％9.95％0.00％希腊（26）0.28％0.40％0.83％0.00％蒙古（6）0.17％0.18％0.36％0.00％伊拉克7）0.09％1.67％5.79％0.00％百慕大（2）0.04％0.04％0.09％0.00％哈萨克斯坦（14）0.04％0.30％3.90％0.00％白俄罗斯（18）0.04％0.07％0.30％0.00％ 10个国家按每个解析器的操纵响应的中位数百分比。我们还为每个国家的解析器提供平均值，最大值和最小值。每个国家的解析器数量与国家名称一起列出.AS一致性度量（“相同AS”）是最有效的：它将90％的DNS响应分类为一致。同样，在我们的控制解析器和我们的实验解析器的响应之间标识匹配的IP地址，在大多数解析器中，大约80％的响应都是正确的。 “相同的HTTP页面”也相对有效，因为同一站点的许多地理分布式部署（例如存在点）具有相同的内容或基础结构错误特征（请参见x3.5.1）。此图还说明了SNI的重要性，将正确和有效的HTTPS证书的有效性从38％提高到了55％。相同的HTTPS证书（“相同证书”）度量标准比简单地使用正确证书（“正确证书”）更有效，因为许多站点错误地部署了HTTPS。5.2操纵DNS响应我们检测到将近42,000个受操纵的DNS响应;我们现在调查这些响应在解析器，域和国家的分布。通过解析器处理响应。图4显示了返回至少一定操纵响应分数的结果的累计分数：88％的解算器没有表现出操纵;对于96％的解决方案，我们对少于5％的响应观察操纵。 CDF中的模式突出显示了解决方案子群体之间的差异，经过进一步调查，我们发现了不同国家间不同的操作实践。此外，62％的域由至少一个解析器操纵，预计在我们选定的域中有一半以上是CLBL上的敏感站点。我们将在本节后面更详细地探讨这些变化。按国家/地区管理的响应。以前的研究表明，一些国家部署了全国范围的DNS审查技术[5];因此，我们预计在同一个国家会看到多个解决方案团队，每个团队都操纵一组类似的领域。表6列出了每个解析器在每个国家的解析器中汇总的操纵响应的百分比。伊朗的解析者表现出最高的操纵程度，每个伊朗解决者的操纵反应中位数为6.02％;中国的中位数值为5.22％。这些排名取决于我们域名列表中的域名，并且可能仅仅反映CLBL包含更多在这些国家被审查的域名。表6中显示的前10位国家都至少有一个解析程序不会操纵任何域; IP地址地理位置不准确可能部分解释这一令人惊讶的发现。例如，香港未经审查的解决方案可能被错误地标为中文。另外，对于那些不直接实施技术操纵机制而是依赖个别互联网服务提供商这样做的国家来说，一个国家内的互联网服务提供商的实际操作表现可能会有所不同。解析器操作员在国家解决方案操作员的局部操作也可能影响这些结果。 x5.3进一步调查了这些因素。图5显示了各国数据集中的反应表示。例如，最左边的一对竖条表明，尽管我们数据集中所有答案的少于5％来自伊朗解决方案，但我们收到的答案占数据集中操纵答复的近40％。同样，中国的解决方案在数据中表示1％的答复，但贡献了15％的操纵响应。相比之下，我们的DNS响应中有30％来自美国的解析器，但仅占被审查响应的5％。表7显示了最高操纵国家的细分0.5 0.4操纵响应所有响应按类型分类，0.3响应0.2比例。 0.1 0.0中国土耳其俄罗斯国家法国阿根廷新西兰其他印度尼西亚全部伊朗联合罗马尼亚新图5：各国数据集中所有反应的比例（蓝色）以及相应国家数据集中所有操纵反应的比例（红色）。通过出现在操纵答案中的IP地址进行响应。在伊朗境内的大部分回复中都出现了前两个特殊用途（即私人）IP地址。第三种最常见的响应是OpenDNS（一种DNS过滤和安全产品ct [13]）阻止页面显示成人内容。第四种最常见的反应是一个IP地址，它承载了一个已知在土耳其DNS操作中使用的HTTP错误页面[11]。私有和专用IPv4地址在受管理的DNS响应中。在大约42,000次调整的DNS响应中，17,806对应于RFC 6890定义的专用IPv4地址[17];剩余的23,972条回复与公共IP地址空间中的地址相对应。表8显示了各国回复私人IP地址的情况，根据DNS操作的相对数量排名前十位的国家与该国的结果总数进行比较。例如，我们观察到来自土耳其的操作响应比伊拉克更多，但是Iris在土耳其使用了更多开放的DNS解析器，因此观察到的频率需要正常化。在这里，我们注意到，操纵DNS的国家倾向于返回操作响应中的专用IP地址（如伊朗，伊拉克和科威特的情况），或者只返回公共IP地址（中国）。图6显示观察我们数据集中操纵响应的公共IP地址。最常返回的公共IP地址是OpenDNS阻止页面，占所有包含公有IP地址的操纵响应的近15％。前10个公共IP地址占近60％的答复。在以前的中国DNS审查研究中观察到许多IP答案[5,25]。这些地址答案结果名称类别10.10.34.36 12,144 140私人10.10.34.34 4,566 776私人146.112.61.106 3,495 801 OpenDNS成人195.175.254.2 3,137 129 HTTP错误页面93.46.8.89 1,571 88中国\* 118.97.116.27 1,212 155安全/过滤243.185.187.39 1,167 88中国\* 127.0.0.1 876 267私人95.53.248.254 566 566解析器自己的IP95.53.248.254 565 565解析器自己的IP8.7.198.45 411 75中国\* 202.169.44.80 379 113安全/过滤212。 47.252.200 371 371解析器自己的IP212.47.254.200 370 370解析器自己的IP213.177.28.90 352 22赌博Blockpg208.91.112.55 349 320 Blockpg180.131.146.7 312 145安全/过滤203.98.7.65 303 78中国\* 202.182 .48.245 302 100成人Blockpg93.158.134.250 258 86安全/过滤表7：针对公共非分解IP地址手动分类的最常见的按体积操纵的响应。 “中国\*”类别是Farnan等人先前观察到的IP地址。在2016年[25]。看似任意;他们没有托管服务，甚至没有一个基本的网页。中国最频繁的10个回答中，约有75％是中国人的回应。剩下的25％分布在近乎1,000个看似随意的非中国IP地址的长尾上。5.3国家内部的操纵图7显示了一个国家内部的解析器部分对每个域的DNS操纵，对于10个国家最正常的操纵量。每个点代表一个域;垂直轴表示该国的解算器的一小部分来操纵它。阴影显示该部分分布点的密度。情节揭示了一些有趣的现象。伊朗大约80％的解算器操纵了一组域，而另一组域的解算器则少于10％。第二组域由较小的解析器操纵，也返回非公有IP地址。这些影响与DNS操作基础架构所使用的以前所指出的黑幕一致[7];这一现象值得进一步调查。同样，中国的一套领域经历了大约80％的解体人员的操纵，另一套体验只有一半的时间经历了操纵。相比之下，希腊和科威特的操纵在解析者之间更为一致。国家（＃Res。）％Incor。 ％Pub。伊朗（122）6.02％0.01％中国（62）4.52％99.46％印度尼西亚（80）2.74％95.08％伊拉克（7）1.68％1.49％新西兰（16）1.59％100.00％土耳其（192）0.84％99.81％罗马尼亚（45）0.77％100.00％科威特（10）0.61％0.00％希腊（26）0.41％100.00％塞浦路斯（5）0.40％100.00％表8：按国家操纵的反应中的公共IP地址百分比。各国按操作的总体频率排序。 1.0答案0.8 0.6的比例0.4 0.2 0.01 10 100 1000唯一的答案，按流行率排序（日志缩放）图6：操纵，但我们的数据集中的公有IP地址。水平轴按最常见的IP排序。域名前25位域名其他域名的反应名称0.8 100 0.6被操纵的域名密度0.4 10 0.2比例0.0 1印度尼西亚伊拉克西兰土耳其罗马尼亚科威特希腊塞浦路斯伊朗中国新图7：一个国家内部解体者对每个域进行操纵的比例。 1.0名域名0.8域名0.6比例0.2 0.4 0.00 5 10 15 20国家数量图8：国家（或属地）数量每个区域都有观察到的操纵响应，按操控流行程度排序。一个国家的异质性可能表明一个情景，其中不同的ISP使用不同的区块列表实施过滤;它也可能表明一个国家内地理区域的变化。一个国家内某一组别的解决者之间的调整率变化的事实可能表明概率操纵或操纵反应的注入（[5]之前已有记载的现象）。还有其他更为良性的解释，例如企业防火墙（美国常见）或解析器运营商的低级操作。针对一个国家内进行操纵的解析器的百分比，例如中国没有域名正在经历操纵超过约85％的解析者认为IP地理位置错误是常见的.5.4通用操作域通常在各国操纵域。许多领域都经历了一系列国家的操纵。图8显示了至少有一个解析器处理每个域的国家（或属地）数量的CDF。 30％的域名只在一个国家被操纵，而70％的域名在5个或更少的国家被操纵。在超过19个国家/地区没有任何域名被操纵。表9列出了在许多国家（或属地）经历操纵的域名。最受操纵的两个域名都是赌博网站，每个网站都经历了19个不同国家的审查制度。色情网站的DNS解决方案同样受到操纵，占了未来3个最常受到影响的域名。点对点文件共享排名域名分类＃Cn＃Res 1 \* pokerstars.com赌博19 2512 betway.com赌博19 2343 pornhub.com色情19 2224 youporn.com色情19 1925 xvideos.com色情19 1746 thepiratebay.org P2P共享18 2367 thepiratebay.se P2P共享18 2178 xhamster.com色情18 2009 \* partypoker.com赌博17 22610 beeg.com色情17 183 80 torproject.org Anon。 ＆cen。 12 159181 twitter.com推特9 160250 \* youtube.com Google 8 165495 \* citizenlab.org自由expr。 4 148606 www.google.com谷歌3 561086 google.com谷歌1 5表9：在大多数国家（或附属地区）操纵的域名，按照受操纵响应的国家数量排序。以\*开头的域以“www。”开头，网站通常也是针对性的，特别是Pi-rate Bay。 Tor项目[50] DNS域名是在12个国家操纵的匿名和审查工具中受到最广泛干涉的域名。 Cit-izen实验室[15]也经历了4个国家的操纵。我们注意到，www.google.com在google.com以外的国家受到影响，这并不令人惊讶，因为对google.com的所有HTTP和HTTPS查询都立即重定向到www.google.com;例如，中国操纵www.google.com查询，但对google.com的这些查询不以为然。这一结果强调了对包含完整域和子域的域数据集的需求，而不是简单的二级域。我们还注意到，诸如The Tor Project，Google和Twitter等通常测量的网站的操作经验显着减少国家比一些网站。这种差距意味着需要一个多样化的主要数据集。中国的DNS操作不仅针对成人内容，还包括主要的英语新闻网站，如nytimes.com，online.wsj.com和www.reuters。 COM。中国是唯一观察到操纵这些域名的DNS响应的国家;它也审查了中文维基百科的域名。通常被操纵的类别。表10显示了CLBL类别的操作流行率。如果该国内的任何解决方案人员操纵该类别的域名，我们会将该类别视为在该国家内操纵的类别。 Alexa Top 10K排行榜域名＃Cn中的域名。 ＃Resolv。 1 Alexa Top 10k 36 4422表达自由。 35 3843 P2P文件共享34 3944人权31 2885赌博29 3776色情29 3427酒精和毒品28 2748匿名。 ＆censor。 24 3039仇恨言论22 15810多媒体共享21 293 20谷歌16 23434脸谱10 17538推特9 160表10：根据国家（或属地）的数量排序的十大领域类别，操控性答案最多，这些领域没有出现在CLBL中，这突出了衡量来自领域专家的策划名单以及大众网站的广泛样本的重要性。尽管没有单个领域在超过19个国家经历过操纵，但有几个类别在30多个国家经历了操纵，表明虽然广泛的猫类似乎是通常的目标，但具体的区域可能因国家而异。为了研究如何操纵类别在不同国家有所不同，我们分析了每个国家的解决方案的比例删除特定类别。各国的顶级类别差异很大。表11显示了前10个国家使用规范化操纵数量最常操作的类别。伊朗操纵内容的最高类别“挑衅服装”不是其他十大国家中的任何一个类别。从Alexa中随机选择的do-mains的操作，但不在CLBL（“Alexa Top 10k”）中的流行在许多国家流行，这再次强化了对不同领域数据集的需求。匿名和审查工具广泛应用于中国85％的解析人员，但并未跨越前10名的其余部分。色情和赌博网站被操纵.6总结互联网审查是广泛的，动态的，并不断演变;理解审查制度的本质因此需要技术来进行连续的大规模测量。不幸的是，最先进的测量操纵技术（一种常用的离心技术）依赖于人类志愿者，限制了测量的规模和频率。这项工作介绍了一种用于测量国家/地区域类别％Resolv DNS操作的方法。 IR挑衅服装90.98％Alexa Top 10k 90.16％表达自由。 90.16％CN Alexa Top 10k 85.48％表达自由。 85.48％匿名。 ＆censor。 85.48％ID色情57.50％Alexa Top 10k 56.25％P2P文件共享52.50％IQ政治博客57.14％Alexa Top 10k 28.57％表达自由。 28.57％新西兰Alexa Top 10k 12.50％表达自由。 12.50％P2P文件共享12.50％TR Alexa Top 10k 18.23％expr的自由。 17.71％色情16.67％RO Alexa Top 10k 37.78％赌博37.78％表达自由。 2.22％KW Alexa Top 10k 10.00％expr。 10.00％P2P文件共享10.00％GR赌博50.00％Alexa Top 10k 46.15％CY Alexa Top 10k 40.00％赌博40.00％表11：每个国家/地区排名前三的域名类别实验操作细分。国家按照该国受操纵回应的相对数量进行排序。希腊（GR）和塞浦路斯（CY）都只是经历了2种类别的操纵反应。在全球范围内，通过利用互联网基础设施的一部分开放DNS重新解算器来实现。我们的主要贡献是:( 1）虹膜：用于测量DNS操作的可扩展的道德系统; （2）用于消除DNS反应（例如由于CDN引起的）自然变化中来自更加恶劣类型的操纵的分析技术; （3）一项大规模的测量研究，突出了各国，解决方案和领域中DNS操作的异构性。值得注意的是，我们发现即使在一个国家内，操作在各个DNS解析器之间也是异质的。 Iris支持定期连续测量，这将最终便于随着时间的推移跟踪DNS操作趋势;我们的下一步是实施这些测量以促进纵向分析。致谢作者感谢Manos Antonakakis，Randy Bush，Jed Crandall，Zakir Dumermeric和David Fifield的帮助和支持。这项工作得到国家科学基金会的部分支持CNS-1237265，CNS-1406041，CNS-1518878，CNS-1518918 CNS-1540066和CNS-1602399。参考文献[1] G。 Aceto，A. Botta，A. Pescape，`N. Feamster，M. F. Awan，T. Ahmad和S. Qaisar。利用UBICA监控互联网审查。在国际交通监测和分析（TMA）研讨会上，2015。[2] Alexa Top Sites。 http://www.alexa.com/ topsites。[3] C。安德森，P.冬天和Roya。在RIPE Atlas网络上进行全球网络干扰检测。 USENIX互联网自由和开放通信研讨会（FOCI），2014年。[4]匿名。 DNS注入对互联网审查的间接损害。 SIGCOMM计算机通信评论，42（3）：21-27，2012年6月。[5]匿名。全面了解防火墙的DNS检查。 2014年USENIX互联网自由和开放通信研讨会（FOCI）。[6] M。 Antonakakis，R. Perdisci，D. Dagon，W. Lee和N. Feamster。构建DNS的动态信誉系统。在USENIX安全研讨会上，2010。[7] S。雅利安，H.雅利安和J. A. Halderman。伊朗的互联网审查：第一眼看。 USENIX互联网自由和开放通信研讨会（FOCI），2013。[8] M。贝利和C.拉博维茨。互联网基础设施的审查和合作选择。技术报告CSE-TR-572-11，密歇根大学，美国密歇根州安阿伯市，2011年7月。[9] BBC。 BBC的网站正在全国范围内被封锁。 http://www.bbc.com/news/ world-asia-china-29628356，2014年10月。[10]贝尔蒙报告 - 保护人类研究的伦理原则和准则。 http://ohsr.od.nih.gov/ guidelines / belmont.html。[11] S。 Bortzmeyer做了大量。劫持通过土耳其路由.https：//ripe68.ripe.net/presentations/ 158-bortzmeyer-google-dns-turkey.pdf。[12] A。 Chaabane，T. Chen，M. Cunche，E. D. Cristo-faro，A. Friedman和M. A. Kaafar。策野外探索：分析叙利亚的互联网过滤。在ACM互联网测量会议（IMC），2014年。[13]思科OpenDNS。 https://www.opendns.com/。[14]公民实验室。阻止测试列表。 https：//开头github上。 com / citizenlab / test-lists。[15] Citizen Lab。 https://citizenlab.org。[16]℃。 Contavalli，W. van der Gaast，D.C.劳伦斯和W.库马里。 DNS查询中的客户端子网。 RFC 7871. [17] M。 Cotton，L. Vegoda，R. Bonica和B. Haber-man。专用IP地址注册管理机构。 RFC 6890。[18] D. Dagon，N. Provos，C. P. Lee和W. Lee。破坏的DNS解析路径：一个麻烦的决议权威的崛起。在网络和分布式系统安全研讨会（NDSS），2008。[19] J。 Dalek，B. Haselton，H. Noman，A. Senft，M. Crete-Nishihata，P. Gill和R. J. Deibert。一种识别和确认使用URL过滤产品进行审查的方法。在ACM互联网测量会议（IMC），2013年。[20] D. Dittrich和E. Kenneally。门洛报告：伦理原则指导信息和通讯技术研究。技术报告，美国国土安全部，2012年8月。[21] Z。 Durumeric，D. Adrian，A. Mirian，M. Bailey和J. A. Halderman。一个由全网扫描支持的搜索引擎。 ACM计算机和通信安全会议（CCS），2015。[22] Z。 Durumeric，E. Wustrow和J. A. Halderman。 ZMap：快速互联网扫描及其安全应用。在USENIX安全研讨会，2013。[23] R。 Ensafi，J. Knockel，G. Alexander和J. R. Cran-dall。通过TCP / IP侧通道检测互联网上的故意数据包丢失。在被动和主动测量会议（PAM），2014年。[24] R。 Ensafi，P. Winter，A. Mueen和J. R. Crandall。中国跨时空防火墙分析。 Privacy Enhancing Technologies Sym-posium（PETS），1（1），2015。[25] O。 Farnan，A. Darer和J. Wright。中毒 - 探索防火墙中毒的DNS响应。在ACM电子社会隐私讲座（WPES），2016年。[26] A。 Filasto`和J. Appelbaum。 OONI：开放的网络干扰观察。 USENIX 2012年互联网上自由和开放式通信（FOCI）工作间。[27] Go编程语言。 https：// golang.org/.[28]Google公共DNS。 https：//开头开发商。 google.com/speed/public-dns/.[29]F。屋。网络自由。 2016年[30] ICLab。 ICLab：审查测量平台。 https://iclab.org/.[31]J。 Jiang，J. Liang，K. Li，J. Li，H. Duan和J. Wu。 Ghost域名：撤销但仍可解析。在网络和分布式系统安全研讨会（NDSS），2012。[32] B。 Jones，N. Feamster，V. Paxson，N. Weaver和M. Allman。检测DNS根操纵。在被动和主动测量（PAM）中，2016年。[33] B。琼斯，T.-W. Lee，N. Feamster和P. Gill。检查屏蔽页的自动配对检测和指纹识别。在ACM互联网测量会议（IMC），2014年。[34] M。 Kuhrer，T.Hupperich，J.Bushart，C.Rossow和T.Holz。走向疯狂：开放DNS解析器的大规模分类。在ACM互联网测量会议（IMC），2015。[35] M。 Kuhrer，¨T. Hupperich，C. Rossow和T. Holz。从地狱出去？减少放大DDoS攻击的影响。在USENIX Security Sympo-sium，2014年。[36] G。 Lowe，P. Winters和M. L. Marcus。中国的DNS墙。技术报告，纽约大学，2007。[37] MaxMind。 https://www.maxmind.com/.[38]Z。彩蝶。巴基斯坦网络审查的解剖。 USENIX互联网自由和开放通信研讨会（FOCI），2013。[39] OpenNet Initiative。 https://opennet.net/.[40]打开解析器项目。 http：// openresolverproject.org/。[41] J。 C. Park和J. R. Crandall。一个全国范围的分布式入侵检测系统的实证研究：中国HTML反馈的骨干级过滤。在IEEE国际分布式计算系统会议（ICDCS），2010年。[42] P。 Pearce，R. Ensafi，F. Li，N. Feamster和V. Pax-son。 Augur：互联网广泛检测连接性干扰。在IEEE安全和隐私（S＆P）2017年研讨会上。[43] A。 Razaghpanah，A. Li，A. Filasto，R. R. Nithyanand，V. Ververis，W. Scott和P. Gill。探索纵向审查测量平台的设计空间。技术报告1606.01979，ArXiv CoRR，2016。[44] M。 Salganik。点点滴滴：2016年数字时代的社会研究。http：//www.bitbybitbook。 [45]萨姆伯内特和尼克费马斯特。 Encore：使用跨源请求进行Web审查的轻量级测量。在ACM SIGCOMM，2015。[46] K。 Schomp，T. Callahan，M. Rabinovich和M.Allman。测量客户端DNS基础结构。在ACM互联网测量会议（IMC），2013年。[47] W。 Scott，T. Anderson，T. Kohno和A. Krish-namurthy。卫星：CDN和网络干扰的联合分析。在USENIX年度技术会议（ATC），2016年。[48] A。 Sfakianakis，E. Athanasopoulos和S. Ioanni-dis。 CensMon：网络审查监视器。在USENIX互联网上免费和开放式通信研讨会（FOCI），2011年。[49] Tor项目。 OONI：打开网络干扰的观测台。HTTPS：//ooni.torproject。 org /。[50] Tor项目。HTTPS：//www.torproject。组织/。[51]-G。 Tuysuz和I.沃森。 土耳其封锁Twitter天气下的YouTube天数.http：//www.cnn.com/2014/03/27/world/europe/turkey-youtube-blocked/，2014年3月。[52] N。 韦弗，C.克雷比奇和V.帕克森。 重定向广告和利润的DNS。 USENIX互联网自由和开放通信研讨会（FOCI），2011年。[53] P。 冬季。 菲律宾阻止Tor？ Tor Trac门票，2012年6月。https：// bugs。torproject.org/6258.[54]P。 冬天和S. Lindskog。 中国防火墙如何阻止Tor。 在USENIX互联网自由和开放通信研讨会（FOCI）上，2012年。[55]十。 Xu，Z.M. Mao和J.A.Halderman。 中国的互联网审查：过滤发生在哪里？ 在被动和主动测量会议（PAM）中，2011。