
理事会特别报告2018年11月83日

# 零僵尸网络

## *建立全球努力*

## *清理互联网*

Jason Healey 和 Robert K. Knake

COUNCIL on FOREIGN RELATIONS

*理事会特别报告2018年11月*
*83日*

# 零僵尸网络

## *建立全球努力清理互联网*

Jason Healey 和 Robert K. Knake

对外关系委员会（CFR）是一个独立的，无党派的会员组织，智囊团和出版商，致力于为其成员，政府官员，企业高管，记者，教育和学生，公民和宗教领袖以及其他感兴趣的人士提供资源公民，以帮助他们更好地了解世界以及美国和其他国家面临的外交政策选择。 CFR成立于1921年，通过维持多元化的成员身份来开展使命，并设有旨在促进下一代外交政策领导人的兴趣和发展专门知识的特别计划；在纽约，华盛顿特区和其他城市的总部举行会议，高级政府官员，国会议员，全球领导人和著名思想家与安理会成员一起讨论和辩论重大国际问题；支持促进独立研究的研究计划，使CFR学者能够撰写文章，报告和书籍，并举办圆桌会议，分析外交政策问题并提出具体政策建议；出版《外交事务　　》，这是国际事务和美国外交政策的杰出期刊；赞助独立工作组，就最重要的外交政策主题撰写报告，并提供调查结果和政策建议；并在其网站CFR.org上提供有关世界大事件和美国外交政策的最新信息和分析。

**外交关系委员会在政策问题上不担任机构立场，与美国政府也不隶属。所有出版物和网站上表达的观点均由作者独自承担。**

理事会特别报告（CSRs）是简明扼要的政策摘要，旨在快速应对发展中的危机或帮助公众理解当前的政策困境。企业社会责任由个别作者（可能是CFR研究员或来自机构外部的知名专家）与咨询委员会协商编写，自成立至出版，时间为六十天。该委员会是一个共鸣委员会，负责对报告草案进行反馈。通常会举行两次会议，一次是在草拟草案之前，一次是在草稿进行审查时；但是，与工作队成员不同，咨询委员会成员无需在报告上签字或背书。一旦发布，企业社会责任将发布在CFR.org上。

有关CFR或本《特殊报告》的更多信息，请致信纽约东68街58号，外交关系委员会，纽约州10065，或致电212.434.9888联络通讯办公室。访问我们的网站CFR.org。



在美利坚合众国印刷。



要提交理事会特别报告的信函以在我们的网站CFR.org上发布，您可以发送电子邮件至。此外，也可以通过以下地址将信函邮寄给我们：外交部理事会东68街58号，纽约，纽约10065。信件应包括作者的姓名，邮政地址和白天电话号码。来信的长度和清晰度可以编辑，也可以在线发布。请不要发送附件。所有信件均归外交关系委员会所有，不予退还。我们感到遗憾的是，由于通信数量众多，我们无法回复每封信。publications@cfr.org.

该报告打印在由BM TRADA北美公司认证的打印机通过FSC®产销监管链认证的纸上。

# 目录

# 前言

网络空间越来越类似于旧的美国狂野西部，没有真正的治安官，而僵尸网络就像是持枪取缔的不法分子。僵尸网络或受恶意软件感染的计算机组（作为一个网络进行控制）可导致互联网的大部分网络犯罪。通过这样做，允许控制网络的人员出于恶意目的利用超级计算级电源。僵尸网络用于传播垃圾邮件，发送网络钓鱼电子邮件，猜测密码，破坏加密和发起分布式拒绝服务攻击。尽管为消除僵尸网络进行了高调的努力，但僵尸网络的数量仍在继续增加。

正如杰森·希利和罗伯特·纳克在这份新的《理事会特别报告》中指出的那样，僵尸网络是一个需要管理的问题这一传统观念的目标太低。僵尸网络可能会造成严重伤害，使外国政府窒息在国外的言论自由，并使它们能够关闭国家的本地网络甚至全球互联网。此外，随着互联网连接设备数量的激增，僵尸网络所造成的经济危害可能会随着时间推移而显着增加。因此，决策者应增强野心，摆脱僵尸网络世界。虽然僵尸网络为零可能是不可能的，但作者得出的结论是，制定这样一个雄心勃勃的目标对于集中政策至关重要。

作者提出了几种创新的政策规定。他们建议政策制定者应努力建立一项原则，即各国应对境内僵尸网络对他人的伤害负责。互联网服务提供商应相互负责应对离开网络的不良流量。应引入奖励措施，使互联网连接设备制造商采取措施保护设备安全。互联网生态系统的组成部分是

应对僵尸网络所使用的网络施加压力，要求警察自我监控，并防止其服务用于犯罪目的。最后，如果这些措施未能遏制僵尸网络的增长，可能需要国际社会采取措施拆除僵尸网络。僵尸网络的流行及其造成的问题进一步证明，二十一世纪的许多挑战不能在边界内遏制或在国家一级解决。相反，为了最大限度地减少僵尸网络的危害能力，各国应采用主权义务的概念，即主权国家相对于其他国家不仅拥有权利，而且还具有义务。各国政府不仅有义务避免从事被禁止的活动，而且有尽力阻止其他各方在其领土上开展这些活动。如果各国承担这种责任，世界将更接近实现零僵尸网络的目标，这对于任何议程良好的实体都是有利的。

Richard N. Haass
*总裁*

对外关系委员会（Council on Foreign Relations）
2018年11月

# *致谢*

我们要感谢我们的咨询委员会分享他们数十年的经验。虽然我们负责本报告的内容和建议，但许多想法和消息来源首先由咨询委员会成员提出。 Spamhaus提供了宝贵的僵尸网络访问权限，东北大学的贾斯汀·汉纳（Justin Haner）做到了这一点。我们还要感谢Matt Carothers和Gabriel Ramsey的深刻见解和经验。

**Jason Healey and Robert K. Knake**

# 引言

僵尸网络是互联网的祸根。犯罪分子利用这些感染了恶意软件的计算机来传播垃圾邮件，发送网络钓鱼电子邮件，猜测密码，模拟用户和破坏加密。但是，它们最有害的用途是进行分布式拒绝服务（DDoS）攻击。分布式拒绝服务攻击利用构成僵尸网络的单个计算机的力量向目标发送互联网流量，从而阻止合法流量。僵尸网络可能占全部互联网流量的30%，其中大部分来自分布式拒绝服务攻击。[1]大多数分布式拒绝服务攻击本质上都是犯罪，通常由公司用来摧毁竞争对手的网站或服务器；但是，中国，俄罗斯和伊朗都出于地缘政治目的利用僵尸网络。中国对《纽约时报》，《法轮功》和美国的中国基督教教堂进行了分布式拒绝服务攻击。在爱沙尼亚在塔林拆除纪念俄罗斯士兵的雕像后，俄罗斯在2007年通过代理对爱沙尼亚进行了分布式拒绝服务攻击。2008年，俄罗斯与针对格鲁吉亚的军事行动一起，对俄罗斯进行了分布式拒绝服务攻击。为回应据称美国对其核计划采取的行动，2011年至2013年，伊朗对美国金融业进行了一系列持续，大规模攻击。据报道，这些攻击使一些银行每月花费超过2000万美元来维持网站对客户的访问。

传统观点认为，僵尸网络及其造成的问题需要“管理”——僵尸网络及其造成的危害（尽管是问题）只是开放式全球互联网的一部分。因此，减少僵尸网络感染的干预措施最终将损害互联网的活力，损害创新并扼杀自由。这种观点是错误的，原因有三点。

首先，它认真考虑外国政府通过扼杀美国的言论自由直接攻击受保护的自由所造成的社会伤害。应当高度关注美国政府乎无能为力阻止他们采取任何行动。当科技记者布莱恩·克雷布斯（Brian Krebs）的网站遭到分布式拒绝服务攻击下线时，克雷布斯只有在Google通过Project Shield计划接管并吸收了该攻击后，才能恢复在线。2依靠一家具有盈利动机的私营公司保护美国乃至全球的言论自由，引起关注。

其次，有积极性的民族国家行为者可以轻松利用数百万个系统关闭国家/地区的内部网络或定位核心互联网基础设施，并在全球范围内关闭互联网。对于外国政府而言，当然在某些情况下，他们可能会认为此类行为对其有利。

最后，虽然经济危害在今天可以控制，但明天可能不会。如今，网络犯罪每年可能会给全球经济造成6,000亿美元的损失，其中大部分损失与僵尸网络有关，而且这种损失只会持续增长。3物联网正在推动互联网数量的大规模增长连接的设备。这些设备通常在构建时就没有考虑到安全性，安装后很少更新，导致已知漏洞可以被攻击者利用，但不太可能打补丁。因此，作为僵尸网络的一部分，它们更容易受到接管，而且感染和发现和修复的可能性也较小。2016年，Mirai僵尸网络使域名服务提供商Dyn及其许多客户（包括Airbnb，亚马逊，GitHub，HBO，Netflix，PayPal和Twitter）脱机。犯罪分子仅用自己控制的机器人的一小部分进行攻击。

利用一小部分易受攻击的物联网设备，恶意行为者就可以使用可能破坏核心功能的流量泛洪互联网。随着剩余的30亿尚未上网的人们上网，这些用户的IoT设备的感染率可能会很高。如今，大约有160亿台设备连接到互联网，并且在未来五年内，这一数量以及易受攻击和感染设备的数量预计将翻一番。即使这些设备中只有一小部分感染了僵尸网络，恶意行为者也将拥有巨大的破坏潜力。因此，有必要实现零僵尸网络这一宏伟目标。

为实现这一目标，信息安全专家首先需要更好地衡量僵尸网络当前活动并为减少设置增量目标。然后，联合国和国际机构

努力建立原则，各国应对僵尸网络在其内部对他人造成的伤害负责。当政府无法或不愿意承担责任时，其他国家有理由采取行动跨入或移出网络领域，阻止跨境影响。同样，在互联网服务提供商（ISP）级别，好的在线空间管理员需要让其他ISP对离开网络的不良流量负责。需要激励容易成为僵尸网络一部分的设备制造商保护其设备安全，而这些设备的经销商应利用自身的杠杆作用追究责任。僵尸网络使用的托管提供商，域名注册服务商和互联网生态系统的其他组件应承受压力，必须自我监管，防止其服务用于犯罪目的。最后，如果这些措施不能抑制僵尸网络的增长，则有必要进行国际努力来拆除僵尸网络。

# 零的力量

零是一个强有力的概念，通常用作激发政策行动的工具。将不良目标设置为零的目标表示任何事件都是不可接受的。随着进展的进展，发生的事件成为例外，触发有力的响应来理解问题所在并防止重复相同的模式。

在航空业，直到2018年4月西南航空1380号班机乘客最近死亡，在过去九年内，没有一家美国注册商业航空公司的乘客因坠机或事故丧生。彻底审查发动机安全性和确认发动机安全性的协议。对于飞行公众，监管机构，航空公司股东和运营人来说，零是唯一可接受的安全事件数。

决策者在交通事故和公共卫生政策等领域也采用类似的方法。洛杉矶，纽约，华盛顿特区和其他三十个城市的市长正在推行所谓的交通零伤亡和零伤亡计划。这项工作是基于二十年前在瑞典开始的一项计划。在公共卫生领域，多项疫苗接种旨在实现全球零感染。天花疫苗接种工作于1978年成功实现零新感染的目标。与小儿麻痹症作斗争的努力，到2017年全球仅新感染22例。

当然，完全消除僵尸网络可能是不可能的目标。同样，世界不太可能达到零核武器（2009年，巴拉克·奥巴马总统推行全球零核运动的目标），就像瑞典，纽约市和华盛顿特区的可能性不大一样。导致交通事故死亡人数为零（零愿景的目标）。但是有时候集中政策需要一个极端的目标。数据显示，感染率极低（不到0.1%

在当今的美国）仍然可以允许组装强大的僵尸网络。因此，需要将感染率控制在远低于该数字的水平，以有效地达到零。

# *测量电流状态*
# *僵尸网络感染*

僵尸网络感染在全球范围内差异很大，在不发达国家，感染率极低，在发展中国家，感染率高，而在发达国家，感染率低且正在改善。在发达国家，一些国家已采取积极措施将僵尸网络感染率几乎降至零。值得注意的是，芬兰与互联网服务提供商建立了积极主动的伙伴关系，通知感染系统的所有者，并在必要时进行隔离。芬兰一直是发达国家感染率最低的国家之一。其他国家努力成效不佳。日本于2008年创建了网络清洁中心，以降低感染率，但就大多数指标而言，僵尸网络仍然存在重大问题。德国为减少家庭僵尸网络感染做出了多年努力，但其效果远不及芬兰。在没有协调一致的国家方法或法律要求的情况下，美国与拥有此类方法或要求的许多其他国家相比处于有利地位。追踪僵尸网络活动的国际组织Spamhaus提供的数据使美国在僵尸网络感染最严重的国家/地区中排名第14位（见表1）。

*表1.感染最多的国家*

| Rank (most to least infected) | Country | Average number of bots |
|---|---|---|
| 1 | China | 1,976,804 |
| 2 | India | 1,689,265 |
| 3 | Brazil | 606,216 |
| 4 | Iran | 566,353 |
| 5 | Vietnam | 560,720 |
| 6 | Russia | 506,982 |
| 7 | Thailand | 419,979 |
| 8 | Turkey | 412,390 |
| 9 | Mexico | 360,876 |
| 10 | Indonesia | 317,988 |
| 11 | Pakistan | 201,315 |
| 12 | Philippines | 166,177 |
| 13 | Venezuela | 156,718 |
| 14 | United States | 154,719 |
| 15 | Egypt | 148,298 |
| 16 | Algeria | 145,273 |
| 17 | Japan | 142,461 |
| 18 | Italy | 115,546 |
| 19 | Argentina | 113,470 |
| 20 | Malaysia | 101,093 |

*资料来源：Spamhaus，2018年。*

但是，按人均计算，美国网络是世界上最干净的网络之一。在经济合作与发展组织（OECD）国家中，美国网络清洁度排名第八（见表2），这可能是由于盗版或不受支持的软件比率较低以及反病毒软件的普及。德国名列第十二，日本名列第十六。4

但是，鉴于过去和僵尸网络可能造成的危害，鉴于互联网上系统的数量不断增长，即使感染率远低于百分之一的十分之一，也太高了。尽管美国的感染率处于世界最低水平，但在2017年每个季度，美国还是分布式拒绝服务攻击的前五个来源国之一（见表3）。5因此，管理僵尸网络问题需要推动绝对感染数达到或接近零。

*表2. 十个经合组织国家僵尸网络感染率排名*

| Rank (least to most infected) | Country | % of IP addresses infected |
|---|---|---|
| 1 | Denmark | 0.0258% |
| 1 | Finland | 0.0258% |
| 2 | Switzerland | 0.0353% |
| 3 | Netherlands | 0.0549% |
| 4 | France | 0.0574% |
| 5 | United Kingdom | 0.0583% |
| 6 | Canada | 0.0608% |
| 7 | Belgium | 0.0627% |
| 8 | United States | 0.0629% |
| 9 | Estonia | 0.0816% |
| 10 | New Zealand | 0.0830% |
| 11 | Sweden | 0.0835% |
| 12 | Germany | 0.1039% |
| 13 | Austria | 0.1079% |
| 14 | Korea | 0.1123% |
| 15 | Iceland | 0.1171% |
| 16 | Japan | 0.1204% |
| 17 | Luxembourg | 0.1430% |
| 18 | Slovakia | 0.1447% |
| 19 | Czech Republic | 0.1509% |

*资料来源：Spamhaus，2018年。*

*表3.分布式拒绝服务攻击的前五个视频源国家，2017年*

| Q4 2017 | | Q3 2017 | | Q2 2017 | | Q1 2017 | |
|---|---|---|---|---|---|---|---|
| Country | Percentage Source IPs | Country | Percentage Source IPs | Country | Percentage Source IPs | Country | Percentage Source IPs |
| Germany | 30% 128,350 | Germany | 22% 58,746 | Egypt | 32% 44,198 | United States | 44% 594,986 |
| China | 28% 118,716 | United States | 14% 38,628 | United States | 8% 11,113 | United Kingdom | 13% 177,579 |
| United States | 8% 36,441 | India | 7% 19,722 | Turkey | 5% 7,049 | Germany | 7% 87,780 |
| Ecuador | 3% 14,685 | China | 6% 15,323 | China | 4% 5,711 | Canada | 5% 60,581 |
| Austria | 3% 13,503 | Mexico | 5% 13,501 | India | 4% 5,224 | Brazil | 3% 43,863 |

*来源：McKeay，“互联网状况/安全性：2017年第四季度报告”。*

# 为什么僵尸网络坚持存在

尽管针对僵尸网络采取了高调的措施，但僵尸网络和受感染系统的数量仍在继续增长。过去的工作分散在一起，分别集中于向感染系统所有者的ISP通知，或者协调执法行动，逮捕所谓的僵尸机器人，破坏他们用来控制僵尸网络的基础设施。

联邦通信委员会（FCC）与通信安全，可靠性和互操作性委员会（CSRIC）下的主要互联网服务提供商合作，于2012年制定了《反机器人行为守则》。6该守则是一项自愿活动，旨在向僵尸网络用户提供教育，检测僵尸网络活动，通知客户可疑感染，并提供有关如何纠正僵尸网络感染的信息。虽然许多互联网服务提供商采用了行为守则中倡导的做法，但其有效性尚不清楚。

2013年4月，FBI宣布了Clean Slate行动，其既定目标是减少或消除威胁美国经济安全和公民隐私的僵尸网络。7尽管FBI在关闭系统方面取得了一系列成功在某些僵尸网络中关闭这些措施并没有导致僵尸网络数量，受感染设备数量或僵尸网络造成的危害明显减少。

为了从多个媒介解决问题，有必要采用除执法，ISP通知和隔离之外的更全面方法。消除僵尸网络的挑战来自三类：现有技术和新技术；运营，组织和流程问题；以及政策和经济学。

易于欺骗。领导分布式拒绝服务攻击的犯罪分子会利用每一个机会掩盖其踪迹，并使响应者难以识别攻击源。由于分布式拒绝服务攻击无需双向通信，而只需向受害者泛洪流量，因此，僵尸网络管理员通常会对其恶意软件进行编程，使其“欺骗”或伪造数据包的互联网协议（IP）地址，即使其看上去由于数据来自不同的地址，因此很难确定攻击源。美国的欺骗性IP块数量最多，但在样本数据中仅占其所有IP地址的4.8％。在许多发展中国家，100％的IP块都是可欺骗的。8在1990年代后期，互联网安全社区成员开发了解决此问题的协议，称为最佳通用实践38。该协议呼吁ISP实施“出口过滤，”中，任何声称来自未分配IP地址的数据包将被阻止。

防弹托管。防弹托管服务提供商是指托管合法托管公司不会遵守的犯罪活动的提供商。改进的滥用行为报告系统不会改变防弹托管提供商的运营方式。他们通常位于执法不力，腐败水平高或与西方关系不良的国家/地区。这些提供商通常以低成本提供服务，但声称没有足够的资源来监管用户的内容或对每次滥用举报做出回应。因为它们几乎总是托管一些由低价服务吸引的合法业务，所以完全关闭或停止所有来自它们的流量不是适当的应对措施。

物联网的增长。物联网技术使僵尸网络问题的管理更加困难。设备数量庞大，这意味着即使感染率较低，恶意行为者也可以访问令人难以置信的大量受感染设备。此外，这些设备的“一劳永逸”性质意味着拥有者不太可能安装软件更新或以其他方式保护其设备。预测物联网设备增长的大部分原因是因为它们价格便宜，导致不良的开发实践，从而降低了设备的安全性。此外，所有互联网应用程序中有60％包含具有已知软件漏洞的开源组件9。

*加密货币的出现。犯罪分子从运营僵尸网络和分布式拒绝服务勒索方案中获得的价值大部分来自比特币和以太坊等加密货币。犯罪分子将发起分布式拒绝服务攻击，然后要求以加密货币支付阻止此类攻击-通常远低于分布式拒绝服务缓解公司收取的费用。加密货币允许罪犯要求在金融系统中很难追踪的赎金支付-无序发行100美元面额无标记公文包的日子已经一去不复返了。尽管所有比特币交易均公开记录在相关的区块链中，但根据设计 ，与这些交易相关的个人未知。将非犯罪加密货币交易与犯罪交易结合在一起的"翻转"服务的开发，使执法部门很难将系统中剩余的脆弱点作为目标，例如当犯罪分子试图将虚拟货币转换为法定货币时。较新的货币如monero，zcash和dash似乎专门用于刑事交易。10*

*操作，组织和过程问题*

*僵尸网络删除的复杂性。执法机构，互联网服务提供商（ISP），软件公司，安全公司和学术界协调对僵尸网络进行删除，可以大幅减少全球受感染机器的数量和相关疾病。然而，事实证明，随着时间的推移保持持续不断的努力是困难的。僵尸网络下架绝非全职工作。在十年期间，发生了23次部分或全部僵尸网络删除（见表4）。恶意攻击活动一触即发：在2012年，僵尸网络进行了四次恶意攻击，2013年发生三起，2014年，2015年发生三起，2016年发生一起，2017年发生两次。11从多个角度攻击僵尸网络：使用法院命令在全球范围内夺取服务器和网络域名，执法部门逮捕僵尸网络背后犯罪组织的已知和可访问成员，互联网服务提供商（ISP）漏洞通信，软件供应商发布补丁，并且在执法下如果是授权机构，技术专家会尝试一次接管或删除潜在的恶意软件。*

这些工作的领导层是分散的。没有单个组织负责协调下架活动。仅微软一家公司就追求了十几个。网络安全公司，包括CrowdStrike，FireEye，Lastline，赛门铁克和趋势科技，也领导了其他工作。联邦调查局，美国司法部和秘密服务局也进行了协调。正式和非正式第三方

*表4.过去十年的主要僵尸网络数量*

| Date | Botnet |
|---|---|
| November 2008 | McColo |
| November 2009 | Mega D |
| December 2009 | Mariposa |
| February 2010 | Waledac |
| September 2010 | Pushdo |
| November 2010 | DNSCHanger |
| March 2011 | Rustock |
| April 2011 | Coreflood |
| November 2011 | Rove Digital |
| March 2012 | Zeus Botnet |
| July 2012 | Grum |
| September 2012 | Nitol |
| December 2012 | Butterfly Bot |
| February 2013 | Bamital |
| June 2013 | Citadel |
| December 2013 | Sirefef/ZeroAccess |
| June 2014 | Gameover Zeus |
| February 2015 | Ramnit |
| April 2015 | Simda |
| December 2015 | Dorkbot |
| December 2016 | Avalanche |
| April 2017 | Kelihos Botnet |
| December 2017 | Gamarue/Andromeda |

*资料来源：作者的研究。*

包括欧洲刑警组织欧洲网络犯罪中心，互联网系统财团，恶意软件反滥用工作组，马里波萨工作组，国家网络法证学培训联盟和Spamhaus在内的多个组织已经协调下台。这些工作只吸收了有限的技术人才，并使组织做出了贡献。简而言之，删除僵尸网络并不是每天的工作。

*滥用行为报告流程中断。分布式拒绝服务攻击，其他恶意活动和易受攻击的系统的报告流程已损坏。托管服务提供商和互联网服务提供商通常会忽略滥用报告或仅缓慢解决这些报告。有效地举报滥用行为通常依赖于全球公司非正式的，但并不总是有效的个人网络。一名Mirai受害者的努力很好地说明了这一问题：随着针对Minecraft服务器的分布式拒绝服务缓解提供商ProxyPipe的攻击持续进行，该公司副总裁罗伯特·科埃略（Robert Coelho）无法保持其客户端服务器的访问权限。他诉诸于向托管服务提供商和ISP提出滥用投诉，这些攻击支持僵尸机器人指挥和控制攻击服务器的命令和控制服务器。*

*Coelho得出的结论是，控制服务器耗尽了乌克兰一个臭名昭著的防弹托管提供商。该提供商BlazingFast没有回应Coelho的滥用行为举报，也没有回应BlazingFast的分布式拒绝服务缓解服务Voxility。然后，Coelho与四个上游互联网服务提供商（ISP）联系，后者没有提供帮助 ，而第五个互联网服务提供商-芬兰TeliaSonera响应了他的请求并关闭了控制服务器网络连接。*

*"Telia采取的措施将僵尸网络发起的攻击规模降低到80Gbps，"ProxyPipe可以管理这一级别的流量。12*

然而，更快，自动化的滥用行为报告系统可能会产生自己的问题。即使对于那些打算成为网络空间好管家的公司，这种系统也可能相当于在线"交换"，滥用系统被滥用来关闭合法活动。13一些公司在受信任的各方之间开发了经过验证的网络自动执行此过程。没有响应的主机提供商和互联网服务提供商（ISP）几乎不会受到影响。缺乏任何第三方资源，恶意活动的受害者可以自己与通常无动于衷和敌对的公司合作。

*国际合作机制差。在互联网生态系统中，国家计算机应急响应小组（CERTs）的作用定义不清：只有一些能够向外国政府和外国公司提供援助。在国家电信运营商和法律都支持通知和隔离的国家/地区，国家CERTs发挥着重要作用。在美国，计算机应急准备小组在进行分布式拒绝服务攻击时只能提供有限的协助。*

*识别受感染系统所有者的难度。当网络防御者能够将受感染或易受攻击的系统追溯到*

通常，它们只能到达提供服务的ISP。在美国，不允许互联网服务提供商根据《电子通信隐私法》（ECPA）中的法定语言与第三方共享有关客户的信息。除非发出法律传票，否则该禁令将扩展到政府机构。在国际上，本地法律也阻碍了系统所有者的身份识别，如欧盟的《全球数据保护条例》（GDPR）。现在开始生效的GDPR将IP地址视为受保护的个人数据。因此，通知系统所有者和鼓励补救措施的工作需要依靠ISP（除非系统位于具有自己地址空间的大公司的网络上）。由于成本和隐私问题，许多互联网服务提供商不愿主动通知客户感染情况。

*政策和经济问题*

*有利于攻击者的经济刺激措施。据网络安全专家吉姆·刘易斯（Jim Lewis）说，“每天仅花费60美元的僵尸网络可能对受害组织造成高达72万美元的损失，控制僵尸网络的黑客在向他人租借服务时享有超过70％的利润率。14应该识别和实施干预措施，这些干预措施会增加实施这些攻击的成本并降低利润。*

*分布式拒绝服务缓解的不正当奖励措施。提供分布式拒绝服务缓解服务的公司不想看到攻击停止，而是希望以可管理的水平继续进行。正如ProxyPipe副总裁Coelho在与Mirai背后的僵尸机器人进行文本交换时说的那样：“我们只是想使攻击规模进一步缩小”，但他并不是说他希望停止攻击。15*
分布式拒绝服务缓解是一项正在增长的业务。像Akamai和Cloudflare这样的公司提供的固定费率服务就像保险单一样，可以适当调整激励措施，因此缓解服务提供商对清理生态系统有兴趣。从分布式拒绝服务受害者到僵尸网络源的反馈循环最终可能会将僵尸网络数量降至零，但仍在进行中。

*僵尸网络的间接成本。僵尸网络通常不会对其感染的系统造成损害，而会对第三方造成损害。僵尸网络对计算资源的使用和*

大多数受感染系统的所有者和运营商似乎并不十分关注带宽。一些人不用担心自己的个人信息被盗，几乎不会注意到在为他人挖掘加密货币时计算机的性能下降。一些公司对盗窃知识产权视而不见。然而，尽管僵尸网络管理员从受感染的系统中提取任何价值，但维护僵尸网络的真正价值却在于利用它来针对第三方。

*隐私问题以及缺乏针对互联网服务提供商行动的经济诱因。过去，网络中立一直助长了互联网服务提供商的不干预行为，互联网服务提供商坚持认为，作为公共运营商，他们有义务传递流量，除非对自己的系统造成直接伤害，而不是对其他互联网服务提供商或更下游的终端用户造成直接伤害。随着FCC终止网络中立性规则，互联网服务提供商（ISP）担心通过阻止僵尸网络活动违反网络中立性问题也得到了解决。此外，2015年《网络安全法》对ECPA的更改使互联网服务提供商可以广泛地免除阻止恶意流量的责任。更广泛的问题仍然是，许多互联网服务提供商并不认为将僵尸网络作为其业务模型的一部分。为客户过滤分布式拒绝服务流量或为受害者提供更多带宽是一项好业务。至少在美国市场，互联网服务提供商不太可能接受阻止其客户访问互联网的措施。AT&T和CenturyLink正在测试一种更有前途的方法，该方法不是试图清除感染，而是破坏其对网络的命令和控制，使僵尸机器人无法指导僵尸机器人的活动，使僵尸病毒威胁呈惰性。*

# *推荐建议*

在第13800号行政命令中，美国总统唐纳德·J·特朗普指示商务部和国土安全部与私营部门合作，确定“大幅度降低自动和分布式攻击（如僵尸网络）造成的威胁”的方法。 ”随后的报告《增强互联网和通信生态系统抵御僵尸网络和其他自动化分布式威胁的抵御能力》于2018年5月发布，是定义问题的宝贵资源，其许多建议可为以下内容提供建议.16数十个与减少僵尸网络威胁息息相关的组织表示，这项努力缺少的一项明确而可衡量的目标。建立全球零僵尸网络目标是解决这一问题的第一步。

从那里开始，应寻求国家承诺在国家网络内实现零僵尸网络。临时目标和衡量实现这些目标进度的系统至关重要。此类目标可以主要在国家范围内解决。应根据国家/地区内已连接设备的数量在特定时间范围内设定目标。发达国家应该有更严格的要求和更快的时限，对发展中国家的初始要求也要少一些。

*制定全球目标和衡量措施*

为实现零僵尸网络，有必要设定临时目标并衡量针对这些目标的进度。僵尸网络的目标应得到政治领导人，民间社会和全球公司高管的同意。制定这些目标并获得主要合作伙伴的同意是创建运动的最重要的第一步。

这些目标应首先达成一项协议，目标是主要互联网服务提供商实现零僵尸网络，就像美国和中国国家主席在领奖台上握手一样简单。然后，更大的社区可以制定更具体的指标，规范和实施。所涉人员可以看到实现这些里程碑的成功和失败，进行正确的路线调整，并从成功的国家和公司那里汲取教训。难以达成共识并衡量成功的标准。 Spamhaus和其他组织多年来一直在按国家跟踪僵尸网络和感染率。17同样，“网络绿色倡议”一直在科学跟踪僵尸网络。18这些团体可以衡量向零僵尸网络迈进的过程。

*建立由僵尸网络造成的危害的国家责任原则*

随着二十一世纪恐怖主义，核扩散和污染等挑战成为国家安全挑战，国家主权的观念也发生了变化。如今，主权不是对国家公民的绝对主权，而是对其他国家的主权义务。19僵尸网络对个人，公司和国家造成损害，但前提是这种损害是跨界的从本质上讲，这是否会成为一项国际政策关注点，造成损害的国家对其他国家负有主权责任解决这一问题。20通过这种推理，只要损害造成伤害，各国就可以选择允许高比率僵尸网络感染它们造成的范围仅限于自己的领土。但是，它们应由国际系统负责

如果其他国家不积极，合作地做出反应，可能会对其他国家造成任何伤害。

*鼓励国际合作与行动*

各国应采取诱使措施，减少国家网络中僵尸网络的流行。将国家置于不同的责任范围内可能会有用。首先是积极使用僵尸网络胁迫其他国家的国家：国际机构应专门针对这些国家。接下来将是那些隐藏着僵尸网络运营背后的犯罪企业的州。根本无法监管其境内发生的事情的国家将处于最底层。

考虑到这一框架，可以采用奖励措施帮助那些最底层的人群减少排放。羞辱，限制投资和制裁等处罚可能针对的是那些正在积极使用僵尸网络的国家，或者是隐瞒使用僵尸网络的国家。发达国家需要为发展中国家减少僵尸网络活动提供支持，包括帮助解决生态系统中长期存在的问题，例如盗版软件的普及。美国政府，志同道合的国家以及对减少僵尸网络活动感兴趣的公司应资助一个独立的第三方组织的年度报告，跟踪州一级在减少僵尸网络方面的成功经验。

一旦确立了国际义务，不采取应对行动便可以为各国采取有限的行动，以最窄的方式预防危害而又不造成更多危害提供合理的依据。例如，如果一个国家未能建立及时接收和处理虐待投诉并采取行动的机制，外国政府可以授权拆除指挥控制服务器。鉴于各国可能将其视为侵犯主权和敌对行动，无论受到多么有限，都应采取此类行动作为不得已的措施。

*为ISPS创建激励措施清理网络*

一些互联网服务提供商检测到客户何时感染了恶意软件，通过短信通知该人，然后将他们转移到“围墙花园”，在清理计算机之前，他们有时无法访问更广泛的互联网，有时需要互联网服务提供商的帮助。至关重要的是，不是被禁止上网的人，因为那样会限制言论自由，而是

对他人造成伤害的设备。然而，尽管这种做法已经实施了十多年，但仍不被接受为互联网服务提供商的常见责任。

尽管互联网服务提供商对在这一领域的监管保持警惕，但互联网服务提供商作为一个社区可以自我警惕。互联网服务提供商可以同意一个标准，例如，一个拥有一亿台设备或一个月PB流量的互联网服务提供商可以被感染一定比例的设备或排放。如果ISP的费用超过此上限，则必须支付费用或从更清洁的网络购买积分，直到能够将数字降低到阈值以下。

*制定标准以妥善保存设备*

正如总裁报告总结的那样，“基于性能的安全能力基准-确定代表特定威胁环境的生命周期安全最佳实践组合的一组自愿性标准，规范和安全机制，21这份报告没有做的是确定谁应该制定这些标准；然而，美国国家标准技术研究院（NIST）已经完成了制定此类标准的大部分前期工作，并且在与行业合作方面拥有出色的往绩。总裁或商务部长应指导NIST快速建立IoT设备安全标准。这些标准应包括以下内容。

- *在生产时消除已知漏洞。开源组件应为最新版本，设备制造商应扫描其编写的代码中的漏洞。*
- *遵循设备加固的最佳实践。该标准还应要求制造商采取措施，使对手更难以破坏设备。*
- *使设备可更新。新运营技术在环境中的持久性可能比办公技术更长，因此，物联网设备具有远程和自动更新功能以解决安全漏洞至关重要。此类更新默认情况下应为自动化，用户可以选择在部署前测试更新。*

- *维护软件组件的"物料清单"。随着在开源组件中发现漏洞，技术所有者应该知道软件是否已使用安全组件构建。*

- *为每台设备提供唯一的密码。整个IoT设备生产运行通常使用相同的默认密码。更改此程序将消除攻击者获得设备控制的最简单方法。22*

*利用市场压力激励设备制造商达到标准*

就像汽车如果过度污染也无法出售一样，转售商也应拒绝出售未经证实是安全的产品。消费者报告和其他组织正在开发电子设备的网络安全评级。23这项工作需要一段时间才能成熟，但这是减少不安全设备传播的正确机制。如果做得好，它可以以较低的成本更好地调整市场和激励措施，但效果很好。

除了透明度之外，零售商还应拒绝出售不符合NIST标准的产品。在许多问题上，沃尔玛和亚马逊已经是最强大的"监管者"：它们规定了容器的大小和允许的包装形状。要求物联网设备符合安全标准，比减少僵尸网络流行率的几乎任何其他行动都要重要。百思买（BestBuy）决定停止销售卡巴斯基实验室的防病毒软件美国政府声称，这与克里姆林宫间谍活动有关，是采取此类行动的先例。

对不安全设备执行类似操作可能会产生重大影响。银行通常是分布式拒绝服务攻击的受害者，应拒绝向不符合标准的公司贷款，向设备制造商和经销商施加压力。关键基础设施的监管机构应禁止不符合标准的设备。尽管在当前的政治环境下，不太可能授予新的监管权，但具有现有权限的监管者应制定此要求。

*召集启用僵尸网络活动*

运用零概念（例如，在交通事故或飞机失事中）的成功广告系列可以积极衡量进度并进行宣传

达到目标的成功与失败。这种透明性可以帮助对僵尸网络活动负责人施加压力。

当网络罪犯需要用于命令和控制分布式拒绝服务攻击的计算资源时，往往会转向领先的云计算服务。2017年，由Mirai发起的分布式拒绝服务攻击目标OVH托管了世界上僵尸网络命令和控制服务器数量最多；亚马逊托管第二大。24这些命令和控制服务器都是通过简单地购买公司的服务而创建的，通常使用在暗网上购买的信用卡号码被盗。总部位于美国的域名注册商NameCheap是僵尸网络运营商购买用于命令和控制的网址最流行的地方（僵尸网络需要联系网络域名才能接收指令）。2017年，域名便宜域名注册的僵尸网络注册数量为11,878，占此类注册总数的四分之一。

执法部门，股东和客户可能会向网络犯罪分子青睐的云计算和网络域名卖方施加压力，使僵尸网络的运营更加困难。快速识别和删除这种犯罪活动涉及的账户完全在这些公司的技术能力范围内，但是，在没有这样做压力的情况下，这并不符合其财务利益。美国及其盟国还应对活动发芽的国家施加压力，对它们开展活动的机器人和服务进行命名和羞辱，制裁和刑事起诉。

如果合法的服务提供者进行自我监管，从而迫使犯罪集团使用有意无视的供应商，就有可能孤立和惩罚这些集团。过去，互联网服务提供商阻止此类提供商访问互联网的大部分。但是，只有在这些群体从目前的高水平恶意活动中脱颖而出时，才能更广泛地采取这些行动。互联网服务提供商（ISP）已经在尝试机械方式丢弃不良流量。

*建立僵尸网络独立组织*

即使下撤带来了令人难以置信的结果，成功通常还是出色工作水平的结果。应对此进行更改，以便大规模实施删除，收益超过投入。正如一位编辑在TechTarget博客中解释的那样：“如果我们确定一个僵尸网络每天发送数百万条消息，则命令服务器在俄罗斯，部分基础设施在西班牙，而僵尸机器人

在北美，所有这些团体都必须有一种实时或真正快速合作的方式。因为当您关闭一个僵尸网络时，如果不同时删除整个结构，这些人很容易抓住控制权并将所有流量重定向到其他位置。”25

僵尸网络下架涉及高技能，费时的技术工作，而不是全职工作。但应该如此。一种可能的是建立网络事件协作组织（CICOs）。26这样一个小组可以专注于每种主要类型的事件，如反分布式拒绝服务或反恶意软件爆发。反向僵尸网络CICO将“在全球范围内由私营部门领导，成员包括在下台事件中起最大作用的全球组织，例如微软，FireEye和司法部。 ”该小组将与相关的CICO合作，应对恶意软件和分布式拒绝服务攻击，因为它们通常是相关的。这样的组织“不能简单地成为一个拥有额外管理费用的新组织。相反，CICO的目标应该是简化针对事件类型的当前响应流程；提供一把伞，使这种工作更轻松或规模更大。”27

一个相对较小的组织，在五年期间内每年资助1000万美元，可能每年能够进行多次合并。该组织还可以在全球范围内衡量僵尸网络，并为努力降低感染率的国家和公司提供技术援助。为此类组织提供资金可能是一个挑战，但考虑到分布式拒绝服务攻击所造成的成本，为降低威胁的组织提供支持符合金融部门，电信部门，云计算提供商和政府机构的利益。

这些群体从诞生之日起就应该是国际性的，而不是国家网络安全官僚机构的增长。国家CERT应该参与其中，但对于政府来说，直接跨境协调和协调所需的灵活性可能太难了。

# 结论

僵尸网络对互联网健康和依赖互联网的现代数字经济威胁仅在持续增长。在未来十年内，数十亿新设备将加入互联网，现在正是时候建立一个国际制度，努力使易受攻击的设备远离互联网，一旦受到感染就减轻设备攻击并做出响应受感染设备导致的问题。如果没有持续，有组织的斗争来应对这个问题，僵尸网络和控制它们的恶意行为者将利用互联网及其连接系统创造的价值不断增长。

零僵尸网络是一次有效的集会号召，旨在激发技术制造商，互联网服务提供商，消费者，网络安全公司，非营利组织和执法机构的不同联盟，这些组织必须将僵尸网络感染降低到不会构成威胁的水平互联网或互联网运营组织的持续运营。如果动机适当，这样的联盟可能会随着时间推移降低僵尸网络感染率，增加恶意行为者操作恶意行为的成本，并否认这样做的价值。

# 尾注


1. 马云（Joy Ma）和蒂姆·马修斯（Tim Matthews），“地下机器人经济：机器人如何影响全球经济”，Imperva Incapsula，2016年7月5日，http://incapsula.com/blog/how-bots-impact-global-economy.html。
2. Google，“ Project Shield”，访问日期：2018年5月21日，http://projectshield.withgoogle .com / public。
3. 詹姆斯·刘易斯（James Lewis），“网络犯罪的经济影响-不放慢脚步”，战略与国际研究中心和迈克菲，2018年2月，http://mcafee.com/enterprise/zh-CN/assets/reports/restricted/economic-impact-cybercrime.pdf。
4. Spamhaus提供的2018年表1和表2的数据；数据分析由东北大学贾斯汀·汉纳完成。
5. Martin McKeay编辑，“互联网/安全状态：2017年第四季度报告”，Akamai，http://akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2017-state-of-the-internet-security-report.pdf。
6. *最终报告：美国互联网服务提供商反机器人行为守则（ABCs），通信安全，可靠性和互操作性委员会（联邦通信委员会：华盛顿特区，2012年），*http://m3aawg.org/system/files/20120322-wg7-final-report-for-csric-iii_5.pdf。
7. *第113聪，攻下僵尸网络。（2014年）（联邦调查局网络部助理主任约瑟夫·德马雷斯特声明），*http://fbi.gov/news/testimony/taking-down-botnet
8. Spoofer，“去年数据的国家/地区统计数据”，应用互联网数据分析中心，最新修改，2018年6月8日，http://spoofer.caida.org/country_stats.php.
9. 《黑鸭软件》，“ 2017年开源安全和风险分析”，http：//blackducksoftware.com/sites/default/files/images/Downloads/Reports/USA/OSSRA17_Rpt_UL.pdf。

10. Kieran Corcoran，“法律执法对这三种加密货币存在巨大问题”，《商业内幕》，2018年2月27日，http://businessinsider.com /law-enforcement-problems-with-monero-zcash-dash-cryptocurrencies-2018-2.

11. 作者的研究。

12. 布莱恩·克雷布斯（Brian Krebs），《谁是未来派蠕虫作家安娜·森派》？（博客），2018年1月17日，http://krebsonsecurity.com/2017/01/who-is-anna-senpai-mirai-worm-author。

13. 城市词典，s.v。“ Swatting”，Droct，2014年8月27日，http://urbandictionary .com/define.php?term=Swatting.

14. 刘易斯，“网络犯罪的经济影响”。

15. 克雷布斯，《安娜·森派是谁》。

16. 美国商务部，美国国土安全部，“致总统关于增强互联网和通信生态系统抵御僵尸网络和其他自动化，分布式威胁的能力的报告”，2018年5月22日，http://commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report _-_ finalv2.pdf。

17. CB（综合阻止列表），“按国家分类的CBL细分，按计数最高”，Spamhaus，2018年4月24日访问，http://abuseat.org/public/country.html.

18. 赛博绿色研究院（网站），2018年5月21日访问，http://cybergreen.net.

19. 见理查德·哈斯（Richard Haass），《混乱的世界：美国外交政策与旧秩序的危机》（纽约：企鹅出版社，2017年）。

20. 杰森·希利和汉娜·皮茨指出，国家主权与国际义务之间的紧张关系已在国际环境法中得到解决，“通过对在一个州领土内造成对另一州或国家或地区造成伤害的某些行为明确规定有限的国家责任”其公民。” Jason Healey和Hannah Pitts，“将国际环境法律规范应用于网络治具”，*I / S：《信息社会法律与政策杂志》，第8期，2（2012）*。主权义务原则在环境法中以“特雷尔冶炼厂”（Trail Smelter）案为代表。在该案中，美国和加拿大之间涉及污染的跨境争端确立了一项原则，即各国有义务根据国际法防止对邻国造成伤害。见凯瑟琳·普鲁内拉，“国际环境法案例研究：线索冶炼厂仲裁，”*国际污染问题，2014年12月，*http://intlpollution.commons.gc.cuny.edu/国际环境法律案例研究熔炼厂仲裁。

21. 美国商务部，美国国土安全部，“致总统的报告”。

22. 这些建议借鉴了非营利组织I Am the Cavalry的工作，该组织致力于改善IoT设备的安全性。参见http://iamthecavalry.org；为更全面的讨论请参阅“增强互联网的弹性”：“行动1.1。使用行业主导的包容性流程，建立自愿性行业驱动国际标准，建立支持家用和工业应用生命周期安全的国际适用IoT功能基线。”

23. “《消费者报告发布数字标准，保护复杂市场中消费者的安全和隐私》，”新闻稿，消费者报告媒体室，2017年3月6日，http://consumerreports.org/media-room/press-releases/2017/03/consumer_reports_launches_digital_standard_to_safeguard_consumers_security_and_privacy_in_complex_marketplace.

24. Spamhaus Malware Labs，“2017年Spamhaus僵尸网络威胁报告”，Spamhaus，2018年1月1日，http://s pamhaus.org/news/article/772/spamhaus-botnet-threat-report-2017.

25. 凯思琳·理查兹（KathleenRichards），“僵尸网络下架：一种戏剧性的防御”，搜索安全（博客），Tech Target，2013年3月，https://searchsecurity.techtarget.com/feature/Botnet-takedowns-A-dramatic-defense.

26. Jason Healey，“网络协作创新：规模杠杆”，大西洋理事会，2018年5月，http://atlant iccouncil.org/images/publications/Innovation-Cyber-WEB.pdf

27. 同上。

# 关于作者

**杰森·希利（Jason Healey）**是哥伦比亚大学国际与公共事务学院的资深研究学者，专门研究网络冲突，竞争与合作。在此之前，他是大西洋理事会网络治具国际倡议的创始董事，至今仍是高级研究员。他曾在高盛（**Goldman Sachs**）工作，包括在香港的执行董事。在**2003**年至**2005**年担任白宫网络基础设施保护总监期间，他为乔治·**W**·布什总统提供咨询服务，并协调美国为保护美国网络空间和关键基础设施所做的努力。从**2001**年到**2003**年，他担任金融服务信息共享和分析中心副主席。 **Healey**的职业生涯始于美国空军，在五角大楼总部空军网络运营早期工作中获得两枚优异奖章，并担任联合特遣部队计算机网络防御联合创始人之一，这是世界上首次联合网络战单位。他曾在乔治敦大学担任网络政策讲师，并在约翰·霍普金斯大学高级国际关系学院担任网络国家安全研究讲师。

Healy是1986年至2012年的《激烈领域：网络冲突》的编辑，也是《网络安全策略指南》的合著者。他的文章和论文由包括阿斯彭策略集团，大西洋理事会和国家研究理事会在内的智囊团出版，以及布朗大学和乔治敦大学等学术期刊发表。他是国防科学委员会网络威慑工作组成员，也是网络冲突研究协会主席。 Healy拥有美国空军学院政治科学学士学位，约翰·霍普金斯大学人文科学学位以及詹姆斯·麦迪逊大学信息安全学位。

**Robert K. Knake**是对外关系委员会（CFR）网络政策高级研究员。他还是东北大学全球复原力研究所的高级研究科学家。 Knake于2011年至2015年期间担任国家安全委员会网络安全政策主任。在此期间，他负责制定网络安全总统政策，并建立和管理联邦网络事件响应和漏洞管理流程。在加入政府之前，纳克曾在CFR担任国际事务研究员。

Knake的出版物包括《网络战争：对国家安全的下一威胁和应对措施》和CFR委员会特别报告，《网络不安全时代的互联网治理》。他曾就网络安全信息共享和网络空间归属问题在国会作证，并就网络安全政策撰写并广泛演讲。 Knake拥有康涅狄格大学的历史和政府学士学位，以及哈佛肯尼迪学校的公共政策硕士学位。

# 咨询委员会
# 零僵尸网络

**David Altshuler**
*TechFoundation*

**Chris B. Baker**
*Dyn Inc.*

**Chris Boyer**
*AT&T*

**Fred H. Cate**
*Indiana University*

**Benjamin Dean**
*Iconoclast Tech LLC*

**Matthew Eggers**
*U.S. Chamber of Commerce*

**Kristen E. Eichensehr**
*University of California, Los Angeles School of Law*

**Ben Flatgard**
*JP Morgan Chase & Co.*

**Margie Gilbert**
*Team Cymru, Inc.*

**Ryan M. Gillis**
*Palo Alto Networks*

**Nathaniel J. Gleicher**
*Facebook*

**Brittan Heller**
*Anti-Defamation League*

**Cameron F. Kerry**
*Brookings Institution*

**Jongsun A. Kim**
*U.S. Senate Select Committee on Intelligence*

**Douglas J. Kramer**
*Cloudflare, Inc.*

**Michael Kuiken**
*Office of Senator Charles Schumer*

---

本报告反映了作者的判断和建议。它不一定代表咨询委员会成员的意见，决不可将其理解为对报告本身或与其所属组织的认可。

**David Altshuler**
*TechFoundation*

**Chris B. Baker**
*Dyn Inc.*

**Chris Boyer**
*AT&T*

**Fred H. Cate**
*Indiana University*

**Benjamin Dean**
*Iconoclast Tech LLC*

**Matthew Eggers**
*U.S. Chamber of Commerce*

**Kristen E. Eichensehr**
*University of California, Los Angeles School of Law*

**Ben Flatgard**
*JP Morgan Chase & Co.*

**Margie Gilbert**
*Team Cymru, Inc.*

**Ryan M. Gillis**
*Palo Alto Networks*

**Nathaniel J. Gleicher**
*Facebook*

**Brittan Heller**
*Anti-Defamation League*

**Cameron F. Kerry**
*Brookings Institution*

**Jongsun A. Kim**
*U.S. Senate Select Committee on Intelligence*

**Douglas J. Kramer**
*Cloudflare, Inc.*

**Michael Kuiken**
*Office of Senator Charles Schumer*

*Cover photo: Empty cabinets in the data center of T-Systems, the largest German information technology company, on July 1, 2014, in Biere, Germany.*
(Thomas Trutschel/Photothek via Getty Images)

Council on Foreign Relations
*www.cfr.org*

58 East 68th Street
New York, NY 10065
tel 212.434.9400

1777 F Street, NW
Washington, DC 20006
tel 202.509.8400