致总统的报告

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

传输者
商务部长
国土安全部长

2018年5月22日

目录

执行摘要

本报告是对2017年5月11日行政命令“加强联邦网络和关键基础设施的网络安全”的回应。该命令要求“抵御僵尸网络和其他自动化，分布式威胁，”指示商务部长和国土安全部部长“领导一个公开透明的过程，识别和促进适当的利益相关者采取行动”，目标是“大幅减少自动化和分布式攻击（如僵尸网络）造成的威胁”。

美国商务部和国土安全部通过三种方法共同开展这项工作：主办两次讲习班，发表两份评论请求，并通过总统国家安全电信咨询委员会发起调查，旨在收集广泛的投入来自专家和利益相关者，包括私营企业，学术界和民间社会。这些活动都为制定本报告中建议的机构促进了信息收集过程。

这些部门与国防，司法和州部，联邦调查局，特定部门机构，联邦通信委员会和联邦贸易委员会以及其他有关机构进行了协商。

这些部确定，为减少自动化，分布式攻击的威胁而开展的机遇与挑战可以概括为六个主要主题。

1. **自动化的分布式攻击是一个全球性问题。近期值得注意的僵尸网络中，大多数受到攻击的设备都位于美国以外的地理位置。为增强互联网和通信生态系统抵御这些威胁的能力，这些威胁很多来自美国以外，我们必须继续与国际伙伴密切合作。**
2. **存在有效的工具，但并未广泛使用。虽然仍有改进的余地，但可以广泛获得为显着增强互联网和通信生态系统的弹性所需的工具，流程和实践，并且通常在选定的市场领域中应用。但是，由于多种原因，它们并不是许多其他部门产品开发和部署的通用实践的一部分，包括（但不限于）缺乏意识，避免成本，技术专长不足和缺乏市场激励措施。**
3. **产品应在生命周期的所有阶段得到保护。设备在部署时容易受到攻击，缺乏发现后修补漏洞的工具，或者在供应商支持终止后仍处于服务状态，因此组装自动化，分布式威胁非常容易。**
4. **需要意识和教育。家庭用户和一些企业客户通常不知道其设备在僵尸网络攻击中可能扮演的角色，可能无法完全了解可用技术控制的优缺点。产品开发人员，制造商和基础设施运营商通常缺乏部署工具，流程和实践所需的知识和技能，这些工具，流程和实践会使生态系统更具弹性。**
5. **应更有效地调整市场激励措施。目前，市场激励措施似乎与“大幅度减少自动化和分布式攻击所造成的威胁”的目标相吻合。产品开发人员，制造商和供应商都希望最大限度地降低成本和上市时间，而不是内置安全保护或提供高效的安全更新。开发产品时，必须重新调整市场激励措施，促进安全性和便利性之间的更好平衡。**

6. **自动化分布式攻击是整个生态系统的挑战。没有任何一个利益相关者社区可以孤立地解决问题。**

这些部门确定了五个互补和相互支持的目标，一旦实现，将大大减少自动化分布式攻击的威胁并提高生态系统的弹性和冗余性。针对主要利益相关者的建议措施清单可强化每个目标。目标是：

- 目标1：确定通往适应性，可持续发展和安全技术市场的明确途径。
- 目标2：促进基础设施创新，以动态适应不断发展的威胁。
- 目标3：促进网络边缘的创新，预防，检测和缓解自动化的分布式攻击。
- 目标4：促进和支持国内及全球安全，基础设施和运营技术社区之间的联盟。
- 目标5：提高整个生态系统的认识和教育。

建议的操作和选项包括应继续或扩展的正在进行的活动，以及新的举措。没有一项单一的投资或活动能够缓解所有威胁，但有组织的讨论和利益相关方反馈将使我们能够根据这些活动的预期投资回报率和可衡量地影响生态系统复原力的能力，进一步评估和确定优先次序。
本报告要求状态更新，评估利益相关方在应对自动化分布式威胁方面的进展水平。

这项工作不会随着本报告的发布而结束。有很多工作要做。但是，由于相关利益相关者社区的资源紧张等因素，我们预计并非所有行动都会同时发生。此外，一些行动已经在进行中，而其他行动则取决于外部因素。我们提出了一个模型来支持协调和协作以实施第三部分中所述的行动，尤其侧重于联邦要求。虽然与联邦政府直接相关的一些行动显然适合政府领导，但这种模式为利益相关者推进政府开展行动提供了一种途径，这些行动最好通过私营部门领导来实现。

I. 背景资料

2017年5月11日，总统发布第13800号行政命令，“加强联邦网络和关键基础设施的网络安全”，呼吁“抵御僵尸网络和其他自动化，分布式威胁。”总统指示商务部长和国土安全部部长“领导一个公开透明的过程，识别和促进适当的利益相关者采取行动”，目标是“大幅减少自动化和分布式攻击（如僵尸网络）造成的威胁”。[1]

自互联网问世以来，此类攻击一直是人们关注的焦点，并且在2000年代初就开始经常出现。自动化和分布式攻击所构成的威胁已经超越了任何一家公司或部门。这些威胁可用于各种恶意活动，包括使网络资源不堪重负的分布式拒绝服务（DDoS）攻击，发送大量垃圾邮件，散布键盘记录程序和其他恶意软件；由僵尸网络分发的勒索软件攻击，劫持系统和数据作为人质；以及通过社交媒体操纵和恐吓社区的计算宣传运动。传统的分布式拒绝服务缓解技术（如网络提供商过度吸收僵尸网络影响的能力建设）旨在防范预期规模的僵尸网络。借助利用数量众多的“物联网”设备的新型僵尸网络，分布式拒绝服务攻击的规模已增长到每秒超过1 TB，远远超过了预期的规模和容量过剩。因此，从这些类型的攻击恢复时间可能太慢，尤其是在涉及关键任务服务时。此外，这些缓解技术并非旨在补救由僵尸网络推动的其他类别的恶意活动，如勒索软件或计算宣传。[2] [3] [4] [5]

随着新场景的出现，迫切需要跨不同利益相关方的协调与协作。过去，联邦政府一直与利益相关方合作，应对新威胁的出现。此前的工作包括工业僵尸网络小组，该组织提出了“为减少僵尸网络在网络空间中的影响而做出的自愿努力的原则”（2012年）；在2012年分布式拒绝服务攻击银行后，金融服务行业信息共享和协调[6]

---

[1] 执行订单号13800，美联储82。注册22,391（2017年5月11日），网址：https://www.federalregister.gov/d/2017-10004.

[2] 美国诉莫里斯案，928 F.2d 504（2d Cir。1991）。

[3] 参见，例如，斯图尔特·斯坦尼福德，维尔恩·帕克森和尼古拉斯·韦弗，《如何在业余时间拥有零互联网》，第十一届USENIX安全研讨会论文集，加利福尼亚州旧金山，2002年8月5日至9日，网址：https：// /www.usenix.org/legacy/event/sec02/full_papers/staniford/staniford.pdf.

[4] 计算宣传是„社交媒体平台，自治代理和负责操纵舆论的大数据的集合。„ Samuel C. Woolley和Philip N. Howard，《政治传播，计算性宣传和自主代理人简介》，第10届国际通讯期刊4882，4886（2016），网址：http://ijoc.org/index.php/ijoc/article/viewFile/6298/1809.

[5] 物联网设备的示例包括（但不限于）连接的灯泡，门锁，停车收费表，个人健康监控器，工业自动化和传感器以及汽车。

[6] 工业僵尸网络小组，、为减少僵尸网络在网络空间中的影响而做出的自愿努力的原则„，https：//archive.is/20131015084520/（最新访问2018年4月4日）。www.industrybotnetgroup.org/principles/

2013年；通信安全，可靠性和互操作性理事会（CSRIC）反机器人行为守则（2013年），以及互联网服务提供商（ISP）网络保护实践（2010年）和基于服务器的分布式拒绝服务攻击补救（2014年）的报告；司法部及其许多合作伙伴在应对和"沉陷"支持这些威胁的基础设施方面正在进行积极而持续的工作。尽管这些举措取得了一些进展，但影响是渐进的，仍然存在重大挑战。通过积极应对这些挑战，本届政府和主要利益相关者都有机会增强未来互联网和通信生态系统的弹性。[7] [8] [9] [10] [11] [12]

例如，2016年秋天从Mirai僵尸网络发起的分布式拒绝服务攻击达到持续不断的流量水平，淹没了许多常见的分布式拒绝服务缓解工具和服务，甚至破坏了域名系统（DNS）服务，这是一个常用组件在许多分布式拒绝服务缓解策略中。这种攻击还突显了消费者级IoT设备不安全感和威胁不断增长。作为一种新技术，IoT设备通常在没有重要安全特性和实践的情况下构建和部署。原始Mirai变体相对简单，利用弱设备密码，随后出现了更复杂的僵尸网络。例如，收割者僵尸网络使用已知的代码漏洞利用一长串设备，而迄今为止最大的分布式拒绝服务攻击之一是利用相对不为人所知的新发现漏洞。[13] [14] [15]

---

[7] 评估美国金融部门的安全：调查恐怖主义融资工作队之前的听证会，众议院金融服务委员会，第114聪。40-59（2015年）（金融服务信息共享和分析中心（FS-ISAC）幕僚长约翰·卡尔森声明），网址：https：//www.gpo.gov/fdsys/pkg/CHRG-114hhrg96997/pdf/CHRG-114hhrg96997.pdf.

[8] CSRIC是联邦通信委员会的咨询委员会，其任务是向委员会提出建议，促进美国通信系统的安全性，可靠性和弹性。有关更多信息，包括过去的安全工作，请参阅CSRIC（最新访问，2018年4月4日）。https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0

[9] 通信安全，可靠性和互操作性理事会第三工作组，关于互联网服务提供商的美国反机器人行为守则（ABC）的最终报告，（2013年3月），见：https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%202013.pdf.

[10] 通信安全，可靠性和互操作性理事会第8工作组，互联网服务提供商（ISP）网络保护实践最终报告（2010年12月），网址：http://transition.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf.

[11] 通信安全，可靠性和互操作性理事会第四工作组，基于服务器的分布式拒绝服务攻击补救的最终报告（2014年9月），网址：https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG5_Remediation_of_Server-Based_DDoS_Attacks_Report_Final_(pdf)_V11.pdf.

[12] 参见，例如美国司法部，国际网络运营中拆除的雪崩网络（2016年12月5日），https://www.justice.gov/opa/pr/avalanche-network-dismantled-international-cyber-operation.

[13] 美国计算机应急准备小组，警报（TA16-288A）：Mirai和其他僵尸网络构成的分布式拒绝服务威胁加剧（最新修订，2017年10月17日）。https://www.us-cert.gov/ncas/alerts/TA16-288A

[14] 国家安全电信咨询委员会，NSTAC提交给总统的互联网报告，2014年11月19日，请访问：https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf.

[15] Brian Krebs，是害怕收割者，还是疯狂收割者？克雷布斯安全（2017年10月27日，下午4:39），https：//krebsonsecurity.com/2017/10/fear-the-reaper-or-reaper-madness/。

MemCacheD软件。这些示例清楚地表明了如此规模和规模的僵尸网络所带来的风险，以及预期的创新以及未来攻击规模和复杂性的增加。[16]

方法

商务部和国土安全部通过三种途径共同努力，从私营企业，学术界和民间社会等专家和利益相关者那里收集广泛的投入。这些部门与国防，司法和州部，联邦调查局，各部门机构，联邦通信委员会和联邦贸易委员会以及其他有关机构进行了协商。

2017年6月，商务部国家电信和信息管理局（NTIA）就“促进利益相关者采取行动抵御僵尸网络和其他自动化威胁”发表评论请求（RFC）。僵尸网络和其他分布式自动化攻击。” NTIA共收到47条评论，受访者从大型贸易协会（代表数千家公司）到个人技术专家不等。评论者还代表了不同的行业和领域，包括来自美国和非美国组织的互联网服务提供商，安全公司，基础设施提供商，软件制造商，民间社会和学术界。[17]

2017年7月，美国商务部国家标准技术研究院（NIST）主办了“增强互联网和通信生态系统的弹性”研讨会。该研讨会鼓励利益相关者探索开放和透明方式解决自动化分布式威胁的最新解决方案。 。它吸引了来自不同利益相关者社区的150名参与者，确定了所有利益相关者应对这些威胁的广泛协调行动。[18]

根据13800号行政命令，于2018年1月发布了报告草案，随后召开了第二次RFC和研讨会，利益相关方讨论了实质性公共意见和下一步措施。这些活动促进了机构在本最终报告中制定建议的信息收集流程。评论和研讨会讨论还将为发布本报告后将采取的许多行动提供信息。

国土安全部（DHS）参与这项工作的重点是总统的国家安全电信咨询委员会（NSTAC）互联网和通信弹性小组委员会，该委员会最终确定并批准了NSTAC报告。

---

16 Lili Hay Newman，GitHub，有线网络生存了有史以来最大的分布式拒绝服务攻击（2018年3月1日，上午11:01），https://www.wired.com/story/github-ddos-memcached/.

17其他信息，包括公众意见，请参见美国国家电信和信息管理局，《促进利益相关者对僵尸网络和其他自动威胁采取行动的意见征询》（2017年6月8日），https://www.ntia.doc.gov/federal-register-notice/2017/rfc-promoting-stakeholder-action-against-botnets-and-other-automated-threats.

18美国国家标准技术研究院，增强互联网和通信生态系统的弹性（最新更新，2017年7月10日）。有关会议摘要，请参见Tim Polk，“增强互联网和通信生态系统的弹性：NIST研讨会论文集，（2017年9月），NIST机构/内部报告第8192号，见https://www.nist.gov/news-events/events/2017/07/enhancing-resilience-internet-and-communications-ecosystem http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8192.pdf.

2017年11月16日，互联网和通信抵御能力领域总裁，最终用户设备和物联网）。 NSTAC通过研究得出结论，僵尸网络助长的自动化和分布式攻击威胁到互联网和通信生态系统的安全和弹性，进而威胁国家的关键基础设施。此外，NSTAC判定，受到攻击的IoT设备将越来越多地被恶意行为者用来发起全球自动化攻击。[19]

主要主题

六大主题总结了我们在努力大幅降低自动化分布式攻击威胁方面面临的机遇和挑战。

1. 自动化的分布式攻击是一个全球性问题。近期值得注意的僵尸网络中，大多数受到攻击的设备都位于美国以外的地理位置。为增强互联网和通信生态系统抵御这些威胁的能力，这些威胁很多来自美国以外，我们必须继续与国际伙伴密切合作。
2. 存在有效的工具，但并未广泛使用。虽然仍有改进的余地，但可以广泛获得为显着增强互联网和通信生态系统的弹性所需的工具，流程和实践，并且通常在选定的市场领域中应用。但是，由于多种原因，它们并不是许多其他部门产品开发和部署的通用实践的一部分，包括（但不限于）缺乏意识，避免成本，技术专长不足和缺乏市场激励措施。
3. 产品应在生命周期的所有阶段得到保护。设备在部署时容易受到攻击，缺乏发现后修补漏洞的工具，或者在供应商支持终止后仍处于服务状态，因此组装自动化，分布式威胁非常容易。
4. 需要意识和教育。家庭用户和一些企业客户通常不知道其设备在僵尸网络攻击中可能扮演的角色，可能无法完全了解可用技术控制的优缺点。产品开发人员，制造商和基础设施运营商通常缺乏部署工具，流程和实践所需的知识和技能，这些工具，流程和实践会使生态系统更具弹性。类似于能源之星计划或国家公路交通安全管理局（NHTSA）5-星级安全评级等计划的客户友好机制可以识别更安全的选择，以提高消费者的意识并为购买决策提供依据。[20] [21]
5. 应更有效地调整市场激励措施。目前，市场激励措施似乎与“大幅度减少自动化和分布式攻击所造成的威胁”的目标相吻合。产品开发人员，制造商和供应商都希望将成本和上市时间降至最低，而不是构建安全保护或提供高效安全保护

[19] 国家安全电信咨询委员会，NSTAC致总统关于互联网和通信弹性的报告（2017年11月16日），网址：https：//www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20ICR%20FINAL%20%2810-12-17%29%20%281%29-%20508%20Compliance_0.pdf。

[20] 能源之星，关于能源之星，（最新访问2018年4月4日）。 [21] 国家公路交通安全管理局，搜索NHTSA的5星级安全评级，（最新访问时间：2018年4月4日）。 https://www.energystar.gov/about https://www.safercar.gov/Vehicle-Shoppers

更新。开发产品时，必须重新调整市场激励措施，促进安全性和便利性之间的更好平衡。

6. **自动化分布式攻击是整个生态系统的挑战。没有任何一个利益相关者社区可以孤立地解决问题。**

关于威胁的注意事项

本文不对民族国家，网络犯罪分子和其他威胁行为者进行区分。虽然最初很难确定某些攻击的类型，但生态系统仍必须整合在一起以缓解攻击。这一开放透明的流程重点关注的领域将吸引整个互联网和通信生态系统的利益相关方在安全改进以及攻击之前，期间和之后的合作方面进行广泛了解，了解特定威胁行为者的身份可能最初是未知。国家情报局局长办公室发布的《2018年美国情报社区全球威胁评估》提供了网络威胁前景的见解。[22]虽然超出本报告的范围，但区分民族国家，网络国家和犯罪和其他威胁行为者，以确定如何最好地应用各种针对特定威胁的美国政府机构。一些讲习班参加者还认识到在应对特定类别的威胁行为者方面的局限性。未来应将注意力放在这些问题上，酌情让更广泛的生态系统利益相关者参与。

II. 生态系统的现状和未来愿景

本节描述了互联网和全球通信生态系统技术和政策领域的现状，并展望了美好的未来。生态系统的技术领域包括：

- 将其他技术领域连接到单个系统的基础设施；
- ***企业网络，包括使用专用IP地址空间或替代协议，具有区域互联网注册（RIR）分配的互联网协议（IP）第4版（IPv4）和IPv6互联网地址的本地连接设备以及本地连接的子局域网（LAN）（例如低功耗蓝牙）；***[23]
- ***边缘设备，如个人计算机，移动设备，边缘服务器和物联网以及其他连接的设备；和***
- ***家用和小型企业网络，由使用私有IP地址空间的设备组成，可通过网络地址转换（NAT）从外部寻址。***

策略域与技术域交织在一起，包括：

- **公私伙伴关系，包括信息共享安排；**

[22]见美国情报共同体全球威胁评估国家情报总监丹尼尔·考茨（Daniel R. Coats），参议院情报委员会精选报告（2018年2月13日），见：https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

[23]„区域互联网注册管理机构（RIRs）是非营利性公司，在定义区域内管理和注册互联网协议（IP）地址空间和自治系统（AS）编号。„美国互联网号码注册管理机构，区域互联网注册管理机构（最新访问，2018年4月4日）。https://www.arin.net/knowledge/rirs.html

- 自愿证明或认证过程，供应商和客户选择共享安全目标和期望；
- 在多利益相关方论坛中制定的标准和准则；
- 制定市场激励措施的采购政策，特别是在联邦政府内部；
- 联邦和/或州一级的监管和立法措施；和
- 基于共同目标和最佳实践的国际参与。

增强抵御自动化分布式攻击的弹性，需要跨国家，部门和技术层在技术，策略和其他解决方案组合上进行协作。有效的策略将为使用标准和准则提供清晰的期望，随着安全风险的发展，这些准则和准则将保持灵活和适应性。没有单一的解决方案或框架能够解决所有风险，但跨领域更好的协作将提高生态系统成员缓解僵尸网络威胁的能力。

技术领域

基础设施：现状

面对自动分布式攻击，数字生态系统下的当前基础设施已展现出显着的弹性，但攻击规模和范围的不断扩大似乎正在测试这种弹性的极限。在2016年Mirai僵尸网络攻击临时中断互联网基础设施提供商的服务，中断北美和欧洲许多主要在线服务和网站之后，产生了这两种观点。但是，中断只是暂时的，关键参与者迅速做出了反应。这种回应强调了基础设施的相互依存性，以及个人和组织快速学习和适应的能力。

在本报告中，“基础设施”包括支持连接，互操作性和稳定性的技术和组织，超越了物理线路，无线发射器和接收器以及卫星链路，包括硬件，软件，工具，标准和实践。生态系统取决于（例如，路由器，交换机，互联网服务提供商，域名系统（DNS）提供商，内容交付网络，托管和云服务提供商）。由于现代基础设施的复杂性，关键工具和参与者遍布整个生态系统，因此没有单一的工具可以保护基础设施。传统上，随着新威胁的出现，基础设施参与者的特定子集会协同工作，以了解风险和缓解风险的途径。[24]

一种这样的工具就是对流量进出网络进行过滤（称为入口和出口过滤技术）。 IP欺骗是分布式拒绝服务攻击中常用的一种技术，攻击者制造源IP地址，防止受害者按流量来源过滤不良流量。网络提供商可以通过将传入流量限制为实际上来自其既定网络的传入流量，过滤声称自其预期网络空间之外的流量，从而限制欺骗。[25]

---

[24] 虽然总统政策指令（PPD）21将通信和信息技术行业的系统和资产视为关键基础设施，但本文档使用„互联网基础设施„一词进一步涵盖了互联网生态系统所依赖的组织和实践。

[25] 国土安全部正在开发和支持开源软件工具，以评估和报告源地址验证（SAV）最佳反欺骗实践的部署。有关更多信息，请参见Spoofer应用互联网数据分析中心，https://www.caida.org/projects/spoofer/.

工作组（IETF）和其他以基础设施为中心的组织。可以通过出口过滤进行补充，在出口过滤中，组织或网络运营商在网络边缘部署过滤器，以防止似乎不是源自网络内部的流量退出进入全球互联网。[26]

大型国内运营商至少在部分网络中实施入口过滤标准。但是，这些标准在全球范围内或较小的国内基础设施提供商中并未得到普遍支持。许多技术和业务专家都反对在国际骨干网级别更高一级在互联网上应用入口过滤的提议，因为这样更有可能阻止合法流量。出口过滤被提倡作为企业的通用安全措施，但对于中小企业来说，这种情况仍然不常见。尽管尚未实现，但网络入口/出口过滤（如果实施）可以有效缓解利用IP源地址欺骗的分布式拒绝服务攻击。[27] [28]

基础设施提供商和其他公司提供商业反分布式拒绝服务，可以在限制针对特定目标的攻击影响方面发挥关键作用。但是，由于将这些服务集成到企业网络的其他组件中的成本和复杂性，并非所有企业客户都购买完整的反分布式拒绝服务服务。同时，攻击者会迅速学会利用现有服务中的漏洞。当遇到依赖于庞大流量的攻击时，场外分布式拒绝服务缓解解决方案要么提供更多的网络容量，要么使用网络自身的形状限制到达目标的流量。其他攻击目标是网络服务器或应用程序本身。企业内部设备和工具可以检测并过滤目标网络上的此类攻击。

当前的最佳实践包括采用混合方法，该方法同时使用本地过滤和分布式拒绝服务防御工具，以增加内部部署容量。但是，实施最佳实践的成本可能很高，难以管理，并且需要熟练的员工。这些最佳实践通常也是围绕过去的危机而建立的，例如，很难在遭受攻击之前争辩大量的过剩容量。主动检测漏洞和攻击趋势的威胁检测程序可以补充这些工作，帮助受害者组织根据需要做出响应。内容交付网络（CDN）是另一种可以利用大型专用私有基础设施保护客户的工具。当出现不同的攻击或对手选择新的目标时，组织通常会投资于特定于威胁的防御。

及时响应需要准备和知识。鉴于现代互联网需要大量的安全控制措施，因此，并非所有小型基础设施提供商或关键企业的员工都意识到过滤和其他工具的好处。许多基础设施提供商会提供有关折衷和持续攻击的警告，但如果企业忽略这些警告，则基础设施提供商不太可能会努力跟进其他警告。受害者经常挣扎

[26]见例如P. Ferguson和D. Senie，网络入口过滤：击败利用IP源地址欺骗的拒绝服务攻击，（2000年5月），互联网工程任务组－网络工作组，见（“BCP 38”）；以及F. Baker和P. Savola，《多宿主网络的入口过滤》（2004年3月），互联网工程任务组网络工作组，网址：（“BCP 84”）。https://tools.ietf.org/html/bcp38 https://tools.ietf.org/html/bcp84

[27]出于合理原因，数据包可能会在不同实例上通过不同的路径及时在互联网端点之间路由。

[28]参见，例如克里斯·布伦顿（Chris Brenton），SANS研究所的出口过滤常见问题解答（最新修订，2006年4月19日）。https://www.sans.org/reading-room/whitepapers/firewalls/egress-filtering-faq-1059

当遇到第一次大规模攻击而没有制定响应计划时，因为他们依靠被攻击网络来理解并联系服务提供商寻求帮助。

基础设施未来愿景

各种类型的基础设施提供商必须对共享防御方法的好处有广泛的了解，社区应共同努力，推动采用最佳实践。这项工作包括在与客户网络（包括多租户基础设施，如云提供商）的接口处普遍采用过滤。理想情况下，基础设施提供商应了解当前的攻击级别，维持足够的容量，以吸收实际预期的恶意流量，并将这些功能传达给客户。无论客户选择哪种服务水平，用于分布式拒绝服务缓解的基础设施提供商服务都应与客户现有的网络解决方案集成。

随着新产品和工具的问世，整个生态系统中的参与者都应了解其行为如何帮助（或阻碍）其效力。日益智能的网络可以自动划分不同类型的流量，以隔离或缓解作为攻击源和目标的应用程序或设备。企业使用适当的工具来应对应用程序级攻击的能力日益增强，这些工具的供应商应与客户及相关应用程序供应商合作，使安全决策更轻松，更高效。

越来越多地实施多种现有技术将有助于减轻这些攻击。一些现有基础设施建立在较旧的协议上，例如IPv4网络和传统路由协议。广泛采用当前标准和最佳实践将带来安全优势。例如，IPv6网络可以更好地实现跨网络设备特定识别，以检测设备级异常行为。中小型组织应采用行业最佳实践，随着新基础设施标准和实践的需要和验证，提供者应有效地采用它们。[29]

作为基础设施的核心，关键参与者已经共享了有关威胁不断演变的性质的信息。尽管许多组织聘用的专家会与全球各地的同行进行协调，但未来，信息共享必须通过新的自动化工具和实践扩展到包括规模较小，资金缺乏或利基市场的参与者。奖励措施可以促进投资，用于更好，更有效地检测恶意流量，以及做出更多避免携带恶意流量的公共承诺。这些承诺将建立在社区现有关系的基础上，帮助建立更稳定的全球网络。

企业网络：当前状态

支持企业的网络（如大中型企业，政府机构和学术机构）是互联网和通信生态系统中的另一个关键技术领域。这些网络通常很复杂，具有企业拥有的和运营的边界网关协议（BGP）路由器，域名解析器以及依赖于本地和基于云的服务混合的应用程序。边缘设备通常包括功能强大的服务器，个人计算设备，移动电话以及企业托管和非托管物联网设备。企业网络上的设备可以静态或静态混合使用

[29] 当前的IPv4解决方法网络地址转换（NAT）确实具有防火墙优势，尤其是在家庭网络级。但是，应该指出的是，一旦实施了IPv6，攻击者就可以识别目标设备的特定地址，而这些地址以前很难在NAT之后识别。专家们还对某些IPv6实施的安全性表示了担忧。

从一个或多个公共IP地址范围动态分配的地址（例如，从RIR获取的地址）以及从本地管理的私有IP地址范围分配的地址。企业网络连接到互联网的大量存在，意味着它们不仅是潜在的受害者，而且还是风险来源。

许多著名的分布式拒绝服务攻击（2012年和2013年针对美国银行的攻击）都针对与大型企业相关的面向客户的服务。2016年Mirai攻击正好使一些企业在面对漏洞时表现出了弹性，2012- 2013年的袭击事件刺激金融部门及其合作伙伴发现弱点并展示增强抵御能力的途径。[30]
这些攻击具有破坏性，但该行业通过加大对技术和资源的投资，以及社区（包括其网络服务提供商和技术合作伙伴）与政府之间的积极协作，减轻了攻击的影响。随着攻击继续，各组织分享了经验教训，金融服务信息共享和分析中心（ISAC）和金融服务圆桌会议等机构促进了与主要互联网服务提供商的信息共享和协调。攻击规模极大地鼓舞了高层管理人员的领导层，与政府专家建立了更持久的关系，并承诺投资工具和服务。

与企业网络相关的资源也是执行自动化分布式威胁的重要因素。企业级设备（从IoT设备到数据中心服务器）可能受到威胁，并被整合到僵尸网络中。管理不善的企业资源（如开放域名解析器）通常被用来放大攻击。对于某些企业而言，如何在其全球网络上对所有系统和设备进行修补和更新可能是一个挑战。由企业运营的不执行入口和出口过滤的路由器促进了以地址欺骗为特征的攻击，僵尸网络参与者可以隐藏其真实位置。就云提供商而言，企业资源已被租用（通常使用被盗的信用卡），以快速组建重要的僵尸网络。在许多国家/地区，盗版软件的广泛使用使传统系统所面临的问题更加复杂，因为盗版软件通常不打补丁，因此容易受到已知漏洞的利用。
大量使用盗版软件的企业很难保护，这为恶意行为者提供了可轻松组装为分布式威胁的系统资源库。

遭受到分布式拒绝服务攻击的企业，或者来自受到此类攻击广泛影响的部门，通常会将潜在攻击纳入其风险模型，并采用基础设施提供商提供的分布式拒绝服务缓解措施和企业管理的内部缓解措施。了解风险并实施这些机制的企业例外。许多高风险企业并未意识到分布式拒绝服务攻击对其运营的潜在影响。此类企业可能无法完全了解其保护网络以及响应攻击并从攻击中恢复的能力。例如，他们可能不了解与基础设施提供商的合同的局限性，或无法缓解分布式拒绝服务攻击的产品和服务的可用性。他们也可能不完全了解从这种攻击中恢复的成本。

在没有持续攻击的情况下，企业传统上会将重点放在可用性，功能和成本上。因此，企业很可能会依赖不再能够充分安全保护的旧设备，或者部署从未设计为安全的物联网和其他设备。哪里

[30]见戴维•高德曼（David Goldman），美国有线电视新闻网（CNN）（美国东部时间2012年9月28日，美国东部时间上午9:27），
http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/index.html.

安全更新已发布，企业可能需要非常繁琐的流程来评估补丁或计划维护之间的长时间间隔，从而扩大漏洞窗口。[31]

尽管企业通常拥有专业的信息技术（IT）运营人员，但通常缺乏特定于网络安全的专业知识。通常，组织决策者缺乏类似的意识，而决策者又负责组织内部IT运营的资源配置或监督IT运营，因此，挑战通常会加剧。 IT运营团队通常不知道开放解析器和其他攻击放大来源的风险，也不知道入口和出口过滤的重要性。例如，当互联网服务提供商向客户报告潜在的威胁时，互联网服务提供商通常会发现企业无法识别或定位受感染的设备，即使企业能够识别和定位设备，也可能没有工具或专业知识可以恢复到正常状态。安全状态。在遭受攻击时，企业可能很难与服务提供商进行协作。如果无法实施基本备份程序，企业将更有可能面临挑战，难以从僵尸网络分发勒索软件进行恢复。

企业可以通过融合现有技术和新兴技术，运营和采购政策以及对信息技术人员和决策者的意识和教育，为更灵活的生态系统做出贡献。

企业网络未来愿景

朝着这一愿景迈进的基础步骤是增加企业对NIST网络安全框架（CSF）中包含的原则的应用。大多数必要的行动可以归因于框架的五个并发和连续功能：[32]

- **识别。企业查找遗留设备和其他无法保护的设备。企业将这些高风险设备从服务中删除，并用本质上安全或可以保护的设备替换。**
- **保护。系统架构为所有剩余的高风险设备提供了额外的保护层（例如，对传统设备的访问将受到网络架构的限制）。企业部署或采购内部和外部本地分布式拒绝服务缓解服务。企业的网络架构可限制设备遭受恶意行为者攻击，并限制设备遭受的破坏**
  受感染的设备。实施入口和出口过滤以防止网络地址欺骗，并重新配置攻击放大器（例如，开放式解析器）。高效的更新过程将网络上所有设备的漏洞窗口最小化。多租户基础设施还强制执行入口和出口过滤，以减少基于云的僵尸网络的影响。
- **检测。基于ISP的检测服务与企业运营的网络及服务监控相结合，可实时检测出站恶意流量，入站攻击并识别受感染的设备。**
- **回应。当企业或企业检测到受损设备（例如，更换，缓解或修补参与僵尸网络的设备）时，企业拥有相关政策和程序。**

---

31 见Dan Goodin，未能修补导致大规模Equifax违规的两个月大漏洞，Ars Technica（2017年9月13日），另见联邦贸易委员会，移动安全更新：了解问题（2018年2月），https：//issues/mobile_security_updates_understanding_the_issues_publication_final.pdf。https://arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-failure-to-patch-two-month-old-bug/. www.ftc.gov/system/files/documents/reports/mobile-security-updates-understanding-

32 美国国家标准技术研究院，网络安全框架，（最新访问2018年4月4日）。https://www.nist.gov/cybersecurity-framework

ISP。当在本地检测到攻击时，企业还具有适当的流程联系其ISP或其他反分布式拒绝服务服务提供商。关键运营资源继续在有限的资源下运作。

- **恢复。企业有能力重组受感染的系统（例如，从备份中恢复），而不是提交勒索软件付款以恢复运营。**

上面强调的技术和运营政策只有在适当组合采购政策，意识和教育举措的支持下才是现实的。企业员工和管理人员必须意识到分布式威胁对企业资源造成的安全风险，以及保护，响应和恢复选项。 IT员工必须具备实施缓解和预防所选选项的技能。组织采购政策必须确保安全生命周期问题在采购决策中占主导地位，以防止将不安全的产品添加到系统或保持与系统的连接。这些变化必须在全球企业中发生，而不仅仅是在国内企业中发生，才能对生态系统产生重大影响。

边缘设备：当前状态

设备是生态系统的一个多元化且不断发展的技术领域。互联网同时支持多用户计算系统，个人计算和移动设备，运营技术（例如，工业或制造环境中的监控和数据采集[SCADA]系统），以及整个生态系统中的IoT设备。通常，边缘设备在分布式威胁方面扮演两个截然相反的角色：恶意行为者危害边缘设备以创建分布式威胁，边缘设备也可能成为威胁的目标（例如，僵尸网络发布的勒索软件攻击）。安全不良的端点既可能成为攻击的来源，也可能成为攻击的受害者。[33]

恶意行为者被驱使以尽可能便宜和高效的方式构建僵尸网络。多年来，目标不断演变，从商用机器到安全性较差的家用设备，再到托管提供商和云服务提供商运行的易受攻击的系统，最近又演变为物联网设备。目标定位的这些变化反映了该技术领域在创建更具弹性的生态系统方面所带来的希望和挑战。个人计算机和移动设备比过去几年更加安全。同时，互联设备达到了复杂和高度的水平，可通过自动代码轻松定位，而这些设备却缺乏现代安全工具的优势。

边缘设备可能会因多种原因容易受到攻击：

- 通常，设备设计时并未考虑安全性。开发人员要么不了解好的安全设计规范，要么假定设备将无法访问（例如，在无法通过互联网访问的本地网络上），要么希望避免采用会增加成本，延长产品上市时间或制造设备的安全解决方案。消费者更难以使用。最终的设计选择（例如，硬编码管理密码）会创建本质上不安全的设备。在其他情况下，可以使用适当的安全控制措施，但可用性和用户界面会导致安全性降低。

33 Gartner，Gartner说，2017年将使用84亿个互联..物联网,,，比2016年增长31%（2017年2月7日），网址：
https://www.gartner.com/newsroom/id/3598917.

- 常见的软件开发技术乐观地认为，每2000行代码（或以许多其他指标衡量）会出现漏洞。其中许多漏洞会产生可利用的安全漏洞，如缓冲区溢出。[34][35]
- 如果在部署产品后发现错误，则可能很难或不可能打补丁。这些漏洞通常比利用起来容易纠正。
- 带有不适当的默认配置设置（例如，硬编码密码）的系统在操作中更容易受到攻击。
- 系统也可能容易受到攻击，因为无法获得支持。对于旧设备，通常会出现这种情况。
- 部署设备的规模和多样性使其难以修复，并为恶意活动提供了额外的攻击面。

许多主要软件开发人员都牢记这些教训，并建立了可以显着减少边缘设备漏洞的最新最佳实践。例如，微软软件开发生命周期（SDLC）确保从一开始就考虑安全性。
安全软件开发工具（如输入模糊测试或静态分析）减少了软件漏洞的数量。安全更新服务可以在发现漏洞后纠正漏洞。系统出厂时采用的是更安全的配置，因此无需更改默认设置。因此，现代服务器，台式机，笔记本电脑和智能手机提供的妥协机会大大减少。[36] [37] [38]
这也转化为云环境，更安全的边缘设备已成为现实。硬件信任基础证明了系统未被篡改，是现代系统中出现的另一项创新。

不幸的是，物联网设备通常非常缺乏以安全性为中心的功能。这些系统现在为恶意行为者提供了最诱人的目标，并且在生态系统中的设备越来越多。事实上，2016年11月《爱立信移动报告》预测，2018年物联网设备将超过手机成为最大的联网设备类别。[39]

---

[34] 参见 Coverity Scan：2014 年开源报告，Synopsys，第 4 页，（2015），http://go.coverity.com/rs/157-LQW-289/images/2014-Coverity-Scan-Report.pdf.

[35] 参见，例如，史蒂夫·麦康奈尔（Steve McConnell），《代码完成：软件构建实用手册》，第 521、652 页，（微软出版社，2004 年第 2 版），国际标准书号：0735619670。

[36] “模糊测试（fuzzing）是一种质量保证技术，用于发现软件，操作系统或网络中的编码错误和安全漏洞。它包括向测试对象输入大量随机数据（称为模糊），以使其崩溃。” TechTarget – SearchSecurity.com，模糊测试（模糊测试）的定义，（最新更新于 2010 年 3 月）。https://searchsecurity.techtarget.com/definition/fuzz-testing

[37] “静态分析，也称为静态代码分析，是一种计算机程序调试方法，通过检查代码而不执行程序来完成。” TechTarget – SearchWinDevelopment.com，静态分析（静态代码分析）的定义，https://searchwindevelopment.techtarget.com/definition/static-analysis（最新更新于 2006 年 11 月）。

[38] 一个行业财团的代码卓越软件保障论坛（SAFECode）发布了一份报告，以总结这些教训，并为 SDLC 模型提供进一步指导。Mark Belk 等人，“安全软件开发的基本实践：当今使用的最有效安全开发实践指南”，SAFECode，（第二版）（2011 年 2 月 8 日），https://www.safecode.org/wp-content/uploads/2014/09/SAFECode_Dev_Practices0211.pdf.

[39] 爱立信，《爱立信移动性报告：网络社会的脉搏》（2016 年 11 月），https://www.ericsson.com/assets/local/mobility-report/documents/2016/ericsson-mobility-report-november-2016.pdf.

此外，生态系统的这一领域并不仅仅由现代设备组成。今天，有许多传统服务器，台式机，笔记本电脑和移动电话在使用，并且在可预见的将来也会如此。传统设备不再由制造商提供支持，因此漏洞很容易解决。更糟糕的是，这些设备或其易受攻击的代码组件的攻击工具仍然广泛可用。[40]

最后，互联网上大量个人计算系统运行盗版软件。一个行业协会2015年的统计数据从美国的17％到中国的70％，印度尼西亚的84％不等。制造商通常仅将安全补丁分发限制在运行合法购买的软件的系统上，因此无法防止这些系统受到已知漏洞的影响。虽然不能合理地期望供应商为无牌软件提供支持，但这些不受保护的系统为恶意行为者提供了另一类简单的目标，并强调了这一挑战的国际性。[41]

不安全的设备通常不是底层技术限制的结果。虽然不完美，但如果正确应用，则目前的最佳做法相当有效，可以确保设备在交付时具有合理的安全性，并提供在设备整个生命周期内维持该安全级别的工具。采纳了这些做法的商业部门，例如操作系统开发人员，在安全性和弹性上已取得了显着改善。不幸的是，这些安全做法的执行不一致。许多产品附带已知错误，不包括更新机制，和/或不遵循最新最佳实践来进行管理访问。[42]

可以通过提高认识和教育来应对其中一些挑战。一些产品开发人员不了解如何利用当前可用的工具进行安全的产品开发。运营技术产品开发人员了解其产品线（例如冰箱），但可能不了解其产品网络连接的基本安全要求。企业客户在做出采购决定时，无需考虑整个生命周期成本以及网络不安全的外部性。最终用户可能缺乏了解某些产品功能如何保护其免受安全风险或设备如何对生态系统造成负面影响的工具。

市场激励措施似乎加剧了这一问题。产品开发人员将上市时间和创新功能置于安全和弹性之上。安全功能不容易理解或传达给消费者，这使得很难产生需求。

---

40 例如，微软在2014年4月停止了对十二岁Windows XP的支持。两年后，所有台式机中仍有7.4％至10.9％仍在运行XP，被称为„攻击网络罪犯的鸭子"。 John Zorabedian，„数百万人仍在运行Windows XP"，裸安全（2016年4月11日），https：//nakedsecurity.sophos.com/2016/04/11/millions-of-people-are-still-running- Windows XP /。

41 请参见BSA。软件联盟，"通过许可证合规抓住机遇：BSA全球软件调查"（2016年5月），
http://www.bsa.org/~/media/Files/StudiesDownload/BSA_GSS_US.pdf.

42 参见Steven D.Vaughan-Nichols，《2014年安全性：漏洞在于应用程序，而非操作系统》，ZDNet（2014年2月28日，格林尼治标准时间19：46），
http://www.zdnet.com/article/security-2014-the-holes-are-in-the-apps-not-the-operating-systems/.

边缘设备未来愿景

如果我们要构建更具弹性的互联网和通信生态系统，边缘设备技术领域的广泛进步既有可能，也至关重要。为实现有效，这些进步必须是全球性的，因为大多数互联网设备位于美国境外。这种全球行动将要求全球公认的安全标准和实践必须强大，广泛理解和普遍应用。这些标准应灵活，适当的时机，开放，自愿和行业驱动。

设备必须能够在整个部署生命周期中抵御攻击，无论是在装运时，使用期间还是直至使用寿命结束。为此，安全必须成为主要设计要求。供应商不得运送具有已知严重安全漏洞的设备，不得包含安全更新机制，并且必须遵循最佳最佳实践（例如，没有硬编码密码，禁用对操作而言并非关键的软件功能）以进行系统配置和管理。
供应商应向客户披露支持的最短期限，设备制造商应在承诺的期限内维护安全更新服务。[43]

如今，硬件信任基础和受信任的执行技术已经成为许多现成计算平台的组成部分。未来的产品将需要利用这些技术在初次部署以及整个使用期间展示真实性和完整性。现代开发技术依赖于开源和商业组件的组合。为了满足未来的安全需求，此类组件必须在整个供应链中可追溯，并提供更大的保证。

要取得这样的进步，就需要在产品开发人员的意识和教育方面迈出重要的一步。所有产品开发人员必须具备应用可用工具进行安全产品开发所需的知识和技能。这些供应商使用的工具套件和组件必须反映安全问题，才能实现规模扩张并与不断变化的开发人员并驾齐驱，推动标准化技术的合作伙伴和财团必须授权开发人员制定和传达安全决策。同时，运营技术产品开发人员必须在其特定于产品的知识和技能中添加基本安全要求。同时，客户必须具备足够的知识和信息，可以选择在其环境中安全设计的产品，并且必须意识到所有设备（包括旧设备）带来的风险。

最后，市场激励措施需要与这些安全改进相结合，以便奖励与上市时间和创新功能同等优先考虑安全和弹性的产品开发人员。客户可获得的有关产品安全性和弹性的明确信号将有助于改善这些激励措施。但是，由于规模经济，更好安全的价值主张可能始于企业环境。一旦给定产品类别的安全态势普遍接受，几乎没有制造商可能会忽略它。

[43] 例如，参见《NTIA 物联网多利益相关方流程》，安全升级和修补，沟通升级能力和提高透明度，工作组，沟通 IoT 设备安全更新能力，提高消费者透明度，（2017 年 7 月 14 日），https://www.ntia.doc.gov/files/ntia/publications/draft_communicating_iot_security_update_capability_-_jul_14_2017_-_ntia_multistakeholder_process.pdf （帮助制造商与消费者共享有关安全更新的详细信息，并为消费者提供了解所需内容的工具）。

家用和小型企业网络：现状

家庭和小型企业网络正变得越来越复杂。传统计算设备与云和其他服务提供商进行交互，以支持不断增长的一系列业务和个人应用程序。 IoT设备已经在消费者家庭中大量扩散，从照明，车库开门器和恒温器等家庭自动化设备，到连接的家用电器以及个人健康和健身监视器，一应俱全。在小型企业中也是如此，企业家和管理者可能会寻求利用现成的技术，但缺乏管理员或协调一致的IT战略或政策。根据所有估计，预计已连接的消费类设备数量将会增长。

不幸的是，这一增长领域也是严重缺乏安全性的领域。绝大多数家庭和小型企业用户并未意识到网络安全风险，许多人在将设备连接到网络时未采取最基本的安全措施。如果设备是由他人代为设置和配置的，或者设备使用的不是消费者自己的网络（例如，小区网络），则可能会在没有客户输入或知识的情况下做出与安全相关的决策。同时，对于小型企业而言，威胁信息共享面临挑战，而小型企业通常缺乏大型组织接收和处理威胁信息的资源。

就像上面详述的领域一样，为减轻网络安全风险，通常存在许多工具，但期望普通民众能够驾驭复杂的安全环境是不现实的。小型企业和消费者可能成为分布式拒绝服务攻击的受害者（通常以勒索赎金停止攻击），以及为僵尸网络使用的设备不知情的主机。家庭网络产品的设计通常不会允许家庭用户轻松划分网络或配置安全策略。许多家庭用户依靠传统设备或非许可系统。此外，当家庭用户的设备成为僵尸网络的一部分时，网络提供商通常很难确定哪个设备正在传输数据，因为NAT功能允许家庭用户在一个家庭后面的多个设备之间共享一个IPv4地址。路由器，隐藏被利用的设备。[44]

在家庭和小型企业市场，大多数家庭设备不受管理，因此，如果没有自动更新功能，则不太可能手动更新。消费类设备通常随附包含已知漏洞或硬编码管理密码的过时软件。典型的用户可能无法确定设备软件是否已更新，或者甚至具有软件更新机制，而许多消费类设备则无法。典型的用户甚至可能不知道这方面的重要性，并且可能无法访问有关给定设备上软件的实质性信息。

即使家庭或小型企业网络的架构合理且具有强大的安全控制措施，某些受支持的设备也可能是移动设备，在典型的一天中可能会连接到多个网络。这些网络可能没有得到很好的管理，而且设备在外部网络上使用期间可能会受到威胁。这些设备会带来额外的网络安全风险，允许在引入恶意代码的同时规避本地控制。

通常，家庭和小型企业用户无法轻松访问选择安全产品所需的信息，而且通常没有管理产品的工具。虽然

[44]我们还注意到，NAT技术通过限制对特定端点的入站流量访问，提供了一些安全优势。这可以阻止（但不能完全消除）自动扫描和感染工具带来的威胁。

企业网关更可能提供集成安全产品，家庭用户不太可能访问相同级别的服务，而对于那些网关用户，许多人并不知道安全产品或实施这些服务的原因。根本的安全步骤（例如，从默认密码更改设备密码或启用安全加密）通常超出了消费者的意识或能力。在某些情况下，对此类要求的实施不力可能会挫败用户实施这些基本做法的努力。

令人担忧的是，消费者不会为安全性更高的设备支付更高的费用。现实情况是，消费者的体验通常不会受到设备妥协的直接影响；实际上，消费者可能永远不会知道设备是僵尸网络的一部分。从消费者的角度来看，网络摄像头仍在流媒体播放，或者冰箱仍在变冷。因此，要让所有者负责在僵尸网络中使用其设备的挑战。由于缺乏明确的感染后果，在激励消费者采取措施提高安全性（例如，更新可更新设备）方面面临挑战。[45]

家庭和小型企业网络的未来愿景

期望家庭用户和小型企业所有者成为安全专家是不现实的。但是，行业利益相关者和其他利益相关者可以采取一些措施来改善这种状况。除了改变消费者行为的意识和教育工作外，另一种方法是设计设备时要牢记用户的行为。理想情况下，面向消费者的设备设计应内置安全功能。消费产品应设计得尽可能安全，应包括安全的自动更新机制，对产品的管理几乎没有要求。

理想情况下，消费者可以访问实施当前最佳安全实践的商业产品，并能够轻松识别这些产品。小型企业所有者同样可以将购买的商品映射到其独特的安全考虑和义务。他们将意识到与不安全的IoT设备相关的各种风险，并将选择更安全的设备。
非营利组织和商业实体已开始评估产品的隐私和数据安全；诸如此类的努力将提高知名度，并且随着知名度的提高，设备制造商对安全开发的兴趣也应提高。随着时间的流逝，制造商和集成商采用安全的开发生命周期应该变得越来越便宜。[46]

虽然家庭用户可能不会因为担心设备可能会在僵尸网络中使用而特别受激励，但对于隐私，数据或服务访问权限可能受到损害的担忧，他们可能会感到更加受迫。许多连接的设备使用云服务进行管理和信息存储，这对安全性和隐私具有额外的影响。幸运的是，为提高隐私或数据安全并确保不中断访问服务，将采取许多相同的步骤，也将减少设备成为僵尸网络一部分的机会。

运用适当的激励措施，市场力量可以在提高设备安全性方面发挥关键作用。为使消费者广泛采用更安全的设备，安全设备的成本不能超过

45 Bruce Schneier，物联网安全经济学，Schneier谈安全（2016年10月10日，上午10:26）（最新更新于2016年10月17日）。
https://www.schneier.com/blog/archives/2016/10/security_econom_1.html
46消费者报告，“开始评估产品的消费者报告，隐私和数据安全服务”（2017年3月6日），网址：
https://www.consumerreports.org/privacy/consumer-reports-to-begin-evaluating-products-services-for-privacy-and-data-security/.

不安全的设备。消费产品和服务应设计有内置的基本隐私和安全保护措施。针对特定家庭和小型企业需求的易于理解并提供可行建议的购买指南，可以产生必要的市场信号，奖励开发商和卖方进行投资在安全方面。

智能路由器和防火墙应广泛用于缓解攻击和检测设备受到威胁的时间。随着越来越多的家庭用户IoT设备过渡到可公开寻址的IPv6地址，互联网服务提供商会发现，更容易识别传输恶意流量的终端设备。家庭用户网络实施虚拟网络分段。根据设备的预期用途限制设备的功能（例如，将连接的烤面包机在网络上的活动限制为仅执行敬酒任务所需的那些活动）会大大限制僵尸网络捕获家用设备的能力。全球范围内传统产品和盗版软件在家庭使用的减少也将大大限制僵尸网络攻击者的机会。

家庭用户应该能够识别网络上增加网络安全风险的设备。正在进行研究和开发，以帮助注重安全的消费者更好地管理其网络。 2017年，联邦贸易委员会（FTC）的物联网家庭检查员挑战赛向一项基于移动应用程序的工具提案提供了最高奖项，该工具可帮助用户在家中管理物联网设备。该应用程序将使用过期软件和其他常见漏洞标记设备，并提供有关如何更新每台设备软件和修复其他漏洞的说明。[47]

即使设备能够更好地满足消费者的预期技能水平，也需要提高消费者教育的效率。同时，新的员工队伍有机会满足消费者和小型企业的网络需求。经过适当的培训，这种角色可能成为一种新职业，比电气工程师更像是电工，而不是电气工程师。网络和设备行业还可以通过标准化和协调，简化支持流程，降低支持成本。

治理，政策与协调

由于全球互联网上的自动化，分布式攻击是一个生态系统范围的问题，因此，需要跨部门的政策和治理解决方案进行协调。没有任何一个参与者或部门可以单枪匹马应对这些风险，也没有任何一个实体可以断言这些风险都是别人的问题。例如，尽管许多解决方案都涉及与ISP的主动协调，但将责任完全放到网络层将不明智地使所有流量依赖于此连接层来确定什么样的“良好”流量，迫使ISP来从根本上决定哪些是允许的。在互联网上。此外，这种ISP决策总是会阻塞实际上是“良好”的流量，而会丢失应被阻塞的流量。加密流量会加剧该问题。

考虑到风险的网络性质，必须充分协调才能充分理解问题并确定解决方案的路径。尽管信息技术和通信行业积极开展工作来理解安全风险，但一些行业发现共享信息和在自身行业以外进行协调具有挑战性。一些实体在国内或区域一级进行协调，但在全球范围内需要更多地共享有关威胁，解决方案及其采用和效力的信息。在

[47] 联邦贸易委员会，“物联网家庭检查员挑战赛”，（最后访问日期：2018年4月4日）。https://www.ftc.gov/iot-home-inspector-challenge

在许多情况下，角色和职责不明确会阻碍集体行动，导致安全失败。

一些政府依赖过于具体的法规，这些法规很快就会过时，阻碍创新并限制动态行业的消费者福利。遵从要求或强制执行特定法规可能会解决一些风险，但可能带来更大的负担，同时仍然使更广泛的生态系统不安全，或发出信号表明遵守法规已足够，而不是最低要求。边缘设备，运营技术和基础设施的州或地方法规，使监管形势更加复杂。针对特定国家或地区的解决方案可能使生态系统的全球性面临风险，在这种生态系统中，位和产品都相对轻松地流动，并使本地创新者处于不利地位。

网络技术的跨域性质进一步加剧了这个问题。消费者技术，组织所依赖的企业级工具和设备以及生命所依赖的安全关键技术之间的界线已经模糊。可以在整个生态系统中使用相同的硬件和软件。视频游戏网络和公司的公司网络均可使用关键基础设施服务。

在执法领域，关闭僵尸网络的行业合作正在改善，但并不普遍。近期僵尸网络成功删除，包括与Kelihos，Gameover Zeus和Coreflood等行业广泛合作。执法部门和私营部门之间的积极合作，通过扣押关键指挥和控制资产，实现了破坏。在美国，2016年对联邦刑事诉讼程序规则41（b）（6）进行了修订，以应对调查僵尸网络活动的独特挑战，澄清指出，法院可能会发出授权书，要求在识别出的计算机所在的位置搜索多台计算机在多个司法区。此外，联邦执法部门获得民事禁令的能力（在过去的僵尸网络入侵中不可或缺）仅限于包括窃听或某些类型欺诈的案件。以安全可靠的方式关闭僵尸网络是一项耗费大量人力且漫长的过程。此外，执法部门在识别和起诉应对僵尸网络负责的恶意行为者（尤其是在美国境外活动的恶意行为者）方面面临挑战。

治理，政策和协调未来愿景

将来，无论是最终消费者还是大型企业，购买者都应该能够更好地了解连接设备的风险和安全属性。需要采用物联网和计算设备的方法，这些方法不仅有助于提高消费者的意识，而且可以推动市场，增加设备制造商对更好的网络安全实践的普遍采用和使用。也就是说，安全风险快速发展；今天被认为是安全的东西，明天可能就不安全了，从现在开始的十年后，也不太可能得到保证。市场透明度解决方案可以使买家做出正确的决定，但也必须根据产品生命周期的时间范围和规模来构建。依靠传统上反映静态风险的方法（例如采购需求或保险）的机构，将进行调整以反映网络安全风险的不断演变的性质。改进系统软件和硬件组件的透明度将有所帮助，同时有适当的奖励措施，以了解给定背景和整个生态系统的相关风险。

基础设施运营商将更好地共享和分析数据，以增强对整个生态系统声誉的认识，并评估网络合作伙伴以不断发展，高效，分散的方式应对风险的能力。信息共享机制应以现有机制为基础

多方利益相关者机制和社区，创造新的机会在本地和全球参与。

随着分布式威胁的发展，可能需要新的标准，指南和度量标准来回答以下新出现的问题：第三方如何以足够敏捷的方式评估产品对消费者的利益，以跟上快速发展的安全实践？哪些指标和网络管理实践可见性可以为我们提供有关基础设施投资的信息？更加形式化但适应性强的安全期望将使我们能够在安全实践中引入一些责任制。自愿框架等机制既可以帮助制定激励措施，促进更安全的设计，也可以为未能考虑安全性和对安全设备进行投资建立责任。任何问责机制都应奖励做出基于风险的明智决策的人员，同时承认不存在完善的安全措施。

为应对各种威胁，国内外所有利益相关方都必须更充分地应对自动化的分布式攻击。从根本上讲，这涉及减少可访问互联网的不安全设备的数量，将僵尸网络保持在可管理的规模；开发机制，向当事方（或当事方）共享有关被感染系统的信息以及网络堆栈上下的新兴攻击趋势），以最佳方式应对威胁。

由于技术部署真正是跨国的，而且信息跨国际边界流动，因此，如果没有国际合作就无法实现。在国际领域，美国政府大力倡导行业主导的方法和自愿，基于共识的标准。正如NSTAC报告所述，解决方案在网络和互联网基础设施层依赖标准和创新。尽管存在各种相关标准，框架和最佳实践，但全球范围内并未充分利用它们。

各国政府可以通过支持开放，自愿，行业驱动的标准等步骤，建设性地影响更安全产品的开发，通过制定自己的技术和设备采购决策，为更安全产品创造市场激励。
还可以通过在反滥用和全球网络基础设施社区之间，以及在传统上不专注于IT的行业（例如，公用事业或医疗设备）的网络安全和运营技术要素之间增加多方利益相关者的参与，促进安全。例如，与僵尸网络管理者用于命令和控制的互联网资源相关的运营和多方利益相关者参与对于网络管理和僵尸网络检测威胁信令至关重要。美国应加强在这一领域的国际参与，特别是与已经在这一问题上积极开展行动的国家。

此外，行业和执法部门应努力寻找方法，更频繁，更早地发现和阻止威胁活动，并管理发生的事件。新的工具和程序可能会改善国际执法机构之间的信息共享。执法部门和行业组织应更有效地就成功破坏恶意网络并起诉恶意网络所需要的内容进行沟通，同时牢记隐私问题。美国和国际上的数据保护政策均不得干扰现有工具，例如广泛使用的域名所有权数据WHOIS数据库。

法律环境

一些利益相关者强调了将不确定性和法律风险降至最低的重要性，以鼓励私营部门与执法机构合作，更多信息共享，漏洞披露以及采取有效对策的能力。许多人还强调，需要协调跨部门的法律方法，以避免可能阻碍物联网市场的法律拼凑而成。

改善公共与私人关系的努力已经在进行。国土安全部国家网络安全和通信集成中心（NCCIC）是一个中央场所，由参与网络安全的各种私营部门和政府合作伙伴协调工作，包括信息共享，协作和技术援助。一些不确定性和法律风险。例如，2015年《网络安全信息共享法案》（CISA）向共享网络威胁指标的私人实体授予责任保护和其他法律保护，例如反托拉斯保护，披露法律和某些法规用途的例外以及特权豁免保护。 CISA将NCCIC指定为与联邦政府共享网络威胁指标和防御措施的中央枢纽。这些NCCIC网络安全功能和CISA法律保护适用于IoT网络安全的方式与它们更广泛地应用于网络安全。此外，CISA并不排除私人实体在刑事调查的正常过程中与执法部门强力共享情报；实际上，CISA允许与执法机构或任何其他联邦实体共享网络威胁指标和防御措施，此外，在某些情况下与执法机构共享此类信息时，其责任保护也适用。[48] [49] [50] [51]

许多利益相关者还强调了市场激励措施对物联网设备安全的重要性。一些人谈到共同的最佳实践和标准所指导的责任制度是否可以改善物联网设备安全责任制。虽然本报告并未对与IoT设备安全相关的责任进行全面分析，但我们预计，随着连接设备（可能影响物理世界的设备）的使用增长以及对危害，隐私问题的疑问，这一问题将继续引起人们的关注。，消费者保护，因果链，风险管理以及可能的州和法院诉讼应运而生。责任与新兴的物联网市场一样，法律是一个复杂的法律领域，必须小心避免静态和无效的合规要求，尤其是在动态网络安全形势下。必须进行投资，通过创新做法应对风险，并与利益相关方进行跨行业协调。如果法律不确定性普遍存在，直接解决这一问题的压力将越来越大。

一些利益相关者指出，如果未就供应商可以采取哪些措施限制暴露程度做出明确指导，则任何新的法律或法规制度可能会对IT行业产生意想不到的负面影响。但是，拥护者们提倡不要一揽子责任保护，而不能从改善的安全流程中获得明显的社会收益。一些利益相关者，包括民间社会组织，呼吁进一步明确各司法管辖区的现行法律在这一领域的适用情况，这些法律如何或应该影响供应和分销链上的不同利益相关者，以及如何妥善解决危害。随着这一领域的不断发展，至关重要的是，联邦政府必须更好地理解责任与市场激励措施之间的相互作用，以及任何拟议的变更如何改变这一动态。必须谨慎确保我们的责任法使消费者受益，在适当的时候保护利益相关者，并避免在当今的数字环境中冷却创新。随着公私部门在这一领域的合作不断发展，联邦政府应当继续监测在当今环境下针对信息共享负有责任的保护是否足以有效应对持续存在的新威胁。

III. 目标和行动

这些目标和行动旨在提出一系列相互支持的行动，如果得以实施，将大大提高生态系统的复原力。建议采取的措施包括应继续或扩大的正在进行的活动，以及新的举措。没有一项单一的投资或活动能够消除所有威胁，但有组织的讨论和利益相关者反馈将使我们能够根据这些活动的预期投资回报率和可衡量地影响生态系统弹性的能力，进一步评估和确定优先次序。我们期待整个生态系统中的利益相关方与政府合作实施拟议的活动，实现支持和领导的机会，并消除实施障碍。

目标1：确定通往适应性，可持续发展和安全技术市场的明确途径。

为增强互联网和通信生态系统的弹性，至关重要的是，我们的技术市场必须支持和奖励创新安全技术和流程的不断发展，采用和演变。当市场激励措施鼓励制造商以安全创新为功能和性能的平衡补充时，就会增加工具和流程的采用，从而生产更安全的产品。随着这些安全功能的日益普及，需求的增长将推动进一步的研究。随着此类工具的不断完善，制造商，集成商和系统所有者/系统运营商采用安全开发生命周期的组件变得更加便宜，鼓励更多制造商根据安全功能的质量来区分产品，从而促进更大的竞争。本节确定了关键利益相关者可以采取的建立适应性，可持续性和安全技术市场的措施。

行动1.1：使用自愿性行业驱动国际标准，建立由行业主导的包容性流程，建立国际适用的IoT能力基线，支持家庭和工业应用生命周期安全。

---

48 见6 U.S.C. §148。

49 同上第148（c）节。

50 参见《2016年联合拨款法》，N部门– 2015年《网络安全法案》（法律公告第114-113号，第129条，第2242条）（编纂于美国法典第6卷第§§1501-1510号法律）。

51 CISA为根据法规与联邦实体共享的网络威胁指标和防御措施提供了一系列法律保护。例如，它提供了反托拉斯责任的保护（《美国法典》第6卷第1503（e）节）；联邦和州披露法律（《美国法典》第6篇第1504（d）（3）和1503（d）（4）（B）节）；放弃特权（6 U.S.C.第1504（d）（1）条）；以及联邦和州法规使用（《美国法典》第6篇第1503（d）（4）（C）和1504（d）（5）（D）节）。如果通过联邦政府由国土安全部运营的能力和流程与NCCIC共享网络威胁指标和防御措施，则此类共享还将获得额外的责任保护。 U.S.C. 6第1504（c）（1）（B）条。在有限的情况下，还可以与其他联邦实体共享这些额外的责任保护。参见美国法典6第1504（c）（1）（B）（i）和（ii）条。

随着时间的推移，传统计算设备的安全标准，基准和最佳实践也在不断发展，增加了使用这些设备组装僵尸网络的成本。快速增长的不安全物联网设备部署带来了有害的副作用，无法实现经济高效地开发超大型分布式僵尸网络。例如，Mirai僵尸网络由于采用硬编码的管理密码而入侵了成千上万的设备。最近，收割者僵尸网络针对著名的软件漏洞，使设备受到攻击。虽然存在缓解措施，但许多受影响的设备无法修补。由于无法更改密码和修补漏洞，因此这些设备在整个生命周期中仍将保持脆弱状态。如果将传统计算设备的当前最佳最佳安全实践（如安全默认配置和有效的软件更新机制）应用于物联网设备，则可以在未来的物联网系统中缓解这些漏洞。

过去僵尸网络的影响已被互联网服务提供商等基础设施提供商采取的行动（主要是停止和阻止行动以及吸收过多流量）减轻了，但过去的缓解措施本质上是被动的，物联网设备和系统呈指数级增长，表明回报递减。这些传统的缓解策略。生态系统必须变得更具抵御分布式威胁的能力，首先应采取积极主动的针对性措施，在整个生命周期中减少互联网连接设备的已知漏洞。

为加速开发和部署物联网设备和系统，需要基于绩效的安全性能基线，该基线确定了代表一系列特定威胁环境生命周期安全最佳实践的自愿标准，规范和安全机制套件。例如，家庭环境的基准可能包括安全更新机制，例如自动应用安全补丁和默认安全配置，以最大限度地减少用户操作。一个行业的安全基线可能会假设一个敬业的，知识渊博的安全人员使用诸如集中管理的更新之类的流程。这些基线必须具有足够的灵活性，以适用于IoT设备既是产品又是服务的地方（即云服务是产品运营不可或缺的部分）以及在IoT设备系统之间分布安全功能的地方。[52]

在制定这些基准时，我们必须在基准需求的投资与不使用基准的成本（即，潜在受到伤害的成本，产品生产商的成本以及其他利益相关方的成本）之间取得平衡。能力基准必须务实，以确保制造商能够以具有成本效益的方式满足要求，同时为客户和生态系统带来明显的收益。为达到这种平衡，应在行业领导者与目标客户（例如，代表工业部门的财团或代表家庭用户的消费者权益保护组织和民间社会团体）的协作下制定这些基准，并酌情由政府积极参与。基准线的协同开发为制造商提供了交货周期和对客户期望的早期洞察，并增加了及时提供合格产品的可能性。客户参与基准开发可能还会向市场发出信号，表明买家更喜欢在目标环境中安全设计的物联网设备，还可以调整下文所述的教育活动。随着基线中指定的功能成为事实上的标准，这将支持更安全设备的可持续市场。

[52]基于绩效的标准描述了必须实现的目标，而不是如何实现，减少或消除了对创新的负面影响。

为确保失去的创新机会成本不会超过基准价值，识别少量灵活安全功能的IoT安全基准应在设计和实施方面施加最低限度的约束（如果有）。也就是说，基于结果的方法而非规定方法）将有助于管理与相应评估计划相关的成本。作为限制功能集的附加好处，通用开发平台将这些功能集合并到IoT组件中，简化一致性产品的开发，也变得更加实用。[53]

未来基准的基础

最近发布了一些规范，至少为将来的IoT安全能力基准奠定了坚实的基础。这些工作从高级规范到极为详细的文档，并针对一系列应用环境。自2017年6月以来，针对消费者级设备的高级别规范的显着示例包括在线信任联盟的IoT安全框架，[54]数字标准（由包括消费者报告，数字权利排行和网络独立测试的联盟开发）[55]）和设计安全：英国数字，文化，媒体和体育部提高消费者物联网的网络安全[56]。详细基准规范的一个例子是关键信息基础设施背景下的IoT基线安全建议，[57]由欧盟网络和信息安全局于2017年11月发布，确定了适用于IoT的83种技术措施和良好安全做法安全。另一个例子是“生命关键嵌入式系统的安全原则”，由国防工业基础和信息技术部门成员组成的跨部门工作组制定。[58]

行动1.2联邦政府应酌情利用行业开发的能力基准，为美国政府环境中的IoT设备建立能力基准，以满足联邦安全要求，促进采用行业主导的基准并加速国际标准化。

行动1.1专注于针对不同威胁环境下的物联网设备，以行业为主导，开发能力基准。这种方法带来了多种挑战，从开发多个竞争档案到缺乏关键环境的任何基线。此外，在行业主导的工作集中在国内的情况下，获得国际认可可能会面临挑战。联邦政府可以在存在多个基准的情况下加速融合，启动新的工作

[53]例如，基线可能会指定对无人值守补丁管理的要求，而未指定拉模型或推模型，是否应加密补丁，或应用于补丁的完整性保护的确切类型。 [54]参见物联网在线信任联盟（最新访问，2018年4月4日）。https://otalliance.org/initiatives/internet-things

[55]数字标准，The Standard（最新访问，2018年4月4日）。 [56]数字，文化，媒体与体育部，“设计安全：提高消费物联网的网络安全”，（2018年3月7日），网址：
https://www.thedigitalstandard.org/the-standard
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf.

[57]欧洲联盟网络和信息安全局，“关键信息基础设施背景下的物联网基线安全建议”（2017年11月20日），网址：
https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot.

[58]美国国土安全部，《生命关键嵌入式系统安全原则》（最新发布于2017年1月12日）。
https://www.dhs.gov/publication/security-tenets-lces

通过制定不存在基准的讨论草案，并通过建立联邦物联网基准鼓励国际标准化。

通过与行业，公民社会和国际合作伙伴协作，建立联邦物联网安全能力基线，联邦政府可以证明特定能力的实用性和有效性，促进市场激励，并为实践评估计划奠定基础（见行动5.1）。和5.2）。这种方法还可以确保联邦政府的基准线能够反映最新技术水平，并随着行业和市场的发展而演进。美国国家标准技术研究院（NIST）负责制定信息安全标准和指南，包括对联邦系统的最低要求。 NIST应确定联邦环境中IoT设备和系统的安全要求。如果存在行业主导的共识基准，NIST应评估其对联邦安全要求的适用性，并在适当的情况下通过引用制定联邦标准。这些联邦能力基准将类似于（并跟踪）行动1.1中制定的行业主导基准。如果没有合适的基准，美国国家标准技术研究院（NIST）应寻求行业合作伙伴制定切实可行的基准，并为以后的行业主导工作进行讨论草案。

在证明了这些基准的有效性之后，美国政府和行业也应与行业主导的自愿性国际标准和规范的开发商共同参与，建立全球相关的标准。随着这些标准和规范的出现，应酌情创建，更新或替换联邦基准。

必须仔细选择这些基准的标准化场地。应在私营部门机构中制定安全基准以及任何支持标准和规格，所有相关利益攸关方均可参加，并应以透明的方式制定，采用平衡的基于共识的程序，并采用基于结果的-而不是基于需求的方法。这种基于性能的标准最适合解决物联网等迅速发展的技术空间带来的挑战。这些过程并不排除政府参与，但可以确保政府，行业，公民社会和用户利益得到充分体现，并确保最终解决方案反映该技术领域的最新水平。
这些流程的灵活性还使标准可以随着技术，威胁和解决方案的发展而更新。企业使用自己开发的标准与各国政府对这些工具开发的大力支持紧密结合，有助于大规模采用这些标准。

必须认识到，鉴于技术空间的广度，没有单一的标准或规范开发组织可以开发所有解决方案。世界各国政府需要支持具有专业知识和经验的标准与规范机构之间的合作与协调，并按照上述原则开发产品，以确保提供健壮，及时且适用的解决方案。在美国，NIST应继续领导和协调联邦机构在相关标准活动中的参与，包括与私营部门的参与，探索支持国际标准的联邦政府战略，以应对僵尸网络和其他自动化，分布式威胁。

美国政府和私营部门的互补行动可能会大大增强这些联邦物联网能力基准的影响。联邦政府可以通过要求基线中的功能来使用采购规则和采购准则来放大市场信号（请参阅

行动2.3），并在适当的情况下偏爱也符合给定私营部门标签计划的产品（见行动5.1和5.2）。

行动1.3大幅降低现成商业软件中安全漏洞发生率的软件开发工具和流程必须在行业内更广泛地采用。联邦政府应与业界合作，鼓励进一步改进和应用这些做法，并提高市场采用率和问责制。

常见的软件开发技术导致软件每2,000行代码中至少有一个错误，而现代系统则包含数千万行代码。这意味着系统中有成千上万的错误，其中许多会创建安全漏洞。安全更新机制（在操作1.1中被视为重要的基线功能）使供应商能够在相对短暂的漏洞周期后纠正这些错误。但是，完全避免此类漏洞在降低安全风险方面会产生更大的影响。虽然有可能开发出错误数量很少的代码，而执行任务的重要性必须大大降低生产率，但挑战是开发出机制，在不过度降低生产率的情况下产生更好的代码。[59]

机构间工作队（记录在NIST机构间/内部报告[NISTIR] 8151中）确定了多种开发漏洞少的软件的方法，并实施了三种基本策略：[60]

- 尽早停止漏洞，包括改进的用于指定和构建软件的方法；
- 查找漏洞，包括更好的测试技术和更有效地使用多种测试方法；和
- 通过构建更具弹性的体系结构来减少漏洞的影响，使漏洞无法得到有效利用。

支持这些方法的工具现已上市，并已被一些前瞻性公司采用。软件开发人员应立即开始过渡到这些工具，首先专注于风险最高的产品。国土安全部和联邦贸易委员会也为小型软件开发人员提供资源。[61] [62] [63]

---

[59] 参见覆盖率扫描，上文注34，第4页。

[60] Paul E. Black，Lee Badger，Barbara Guttman和Elizabeth Fong，戏剧性减少软件漏洞：向白宫科学技术政策办公室报告（2016年11月），NIST内部/机构报告8151号，见 http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8151.pdf.

[61] 例如，SANS研究所，CWE / SANS排名前25位的最危险软件错误（最新更新，2011年6月27日）。https://www.sans.org/top25-software-errors/

[62] 例如，软件保障市场（SWAMP）旨在通过减少部署在软件中的弱点数量，更轻松地持续测试这些应用程序的质量和安全性，并为软件保障领域带来变革性的变革。有关更多信息，请参见软件保障市场（最近访问于2018年4月4日）。https://continuousassurance.org/

[63] DHS支持SWAMP的开发，SWAMP同时提供基于云和开源软件保障工具。有关更多信息，请参见软件保障市场，关于沼泽，（上次访问2018年4月4日）；联邦贸易委员会，“谨慎连接：物联网中的安全保护”（2015年1月），https://continuousassurance.org/about-us/

NSTAC在报告中还建议，联邦政府应通过提高投资回报率或为落后行业或行业集团创造市场激励措施，支持行业采用这些工具。联邦政府应通过赞助或开展有针对性的研究（见行动1.4），赞助安全工具链（软件开发的多工具流程）竞赛，证明其有效性和生产力，促进安全编码实践工具的进一步开发。联邦政府还应与行业和公民社会合作制定战略，使其更容易，更便宜地采用这些方法（包括以下详细讨论的教育和培训），同时牢记小企业的需求，并与各种企业开展合作。利益相关者，使第三方可以观察和验证这一过程。

例如，现代产品使用许多软件组件，库和模块，其中一些可能已过时或脆弱，并且在快速开发周期中并非总是被制造商密切跟踪。尽管围绕软件组件透明的概念并不是新鲜事物，但尚未实现广泛的支持和采用。 NTIA应与不同的利益相关方合作，研究必要的战略和政策，以建立一个更高的软件组件透明度市场，包括确定和探索可能阻碍该领域进展的市场和其他障碍。
知道产品中已经集成了什么软件，是保持软件更新并在威胁发生时减轻威胁的基本步骤。

行动1.4：工业界应加快发展和部署创新技术，预防和缓解分布式威胁。因此，在相关情况下，政府应优先考虑运用研究与开发资金和技术过渡工作来支持分布式拒绝服务防御和缓解技术的发展，以及防止僵尸网络创建的基础技术。民间社会应酌情加大这些努力。

基于物联网的僵尸网络提供的分布式拒绝服务容量的快速增长削弱了当前分布式拒绝服务缓解技术的有效性。迫切需要进行技术研究和开发，以提供更接近源头的缓解措施，或利用新数据分析，机器学习或人工智能（AI）领先于恶意行为者。将需要创新来解决僵尸网络支持的其他恶意活动，如勒索软件和计算宣传。为应对这些以及未来的攻击，将需要基础技术来防止，检测和从僵尸网络和僵尸网络融合中恢复。

为了增强生态系统的弹性，必须通过积极部署来利用研发成功。创新的设备技术（例如，硬件信任根或增强的设备身份验证机制）可在整个产品生命周期中显着增强安全性。网络工具的发展，如IETF中目前正在制定的制造商使用说明（MUD）标准，可以通过管理安全通信和进行精细的网络管理来增强网络的弹性。[64]

https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf.

64参见E. Lear，R。Droms和D. Romascanu，制造商使用说明规范（草案），互联网工程任务组_网络工作组，https：//datatracker.ietf.org/doc/draft-ietf-opsawg-mud /（最新更新于2018年4月19日）。

更便宜，更容易。加速采用此类创新技术将提高生态系统的弹性，但众所周知，商业化和采用有前途的研究结果来创造可行的产品或可销售的服务仍面临挑战。民间社会和非营利组织也可以扩大新平台或解决方案，如互联网协会和全球网络联盟为促进路由安全而各自采取的行动，以及美国公民自由联盟针对隐私和技术所采取的行动。[6566] [67]

作为网络安全基础研究的重要资金来源，联邦政府应通过有针对性的资助和协作技术过渡活动来支持这项行动。部门和机构还赞助应用研究，以支持任务需求和各种技术转型活动。机构应优先考虑开发和部署可增强生态系统弹性的创新，并通过网络和信息技术研发协调这些投资（（NITRD）计划。与使用任何缓解技术一样，应采取措施确保这些创新技术不会使消费者承受不必要的隐私风险。可以通过NISTIR 8062中描述的隐私风险评估工具或通过隐私影响评估来完成。[68] [69] [70] [71]

行动1.5：政府，行业和公民社会应合作确保在整个数字生态系统中广泛采用与物联网相关的现有最佳实践，框架和指南，以及确保透明度的程序。必须以开放和包容的方式应对物联网领域的新兴风险。

先前的几次努力已经产生了与僵尸网络和更好的IoT安全相关的指南和最佳实践，但僵尸网络仍然是一个问题。例如，NTIA的IoT安全升级和修补多方利益相关方流程中的利益相关方制定了一套文档，为IoT消费者市场的供需双方提供解决方案，但利益相关方还强调了在整个IoT社区推广这些想法方面的共同作用。仅发布文件还不够。我们必须努力确保文件在整个生态系统中得到广泛采用。 IoT社区必须协同合作，确定并采用现有的最佳实践，框架和指南[72]

---

[65]参见互联网协会，MANRS：相互同意的路由安全规范，（最新访问，2018年4月4日）。
https://www.internetsociety.org/issues/manrs/

[66]参见全球网络联盟，Quad9：安全，隐私和性能的四个简单步骤，（最新访问日期：2018年4月4日）。
https://www.globalcyberalliance.org/initiatives/quad9.html

[67]见美国公民自由联盟，隐私与技术（最新访问，2018年4月4日）。https://www.aclu.org/issues/privacy-technology

[68]国土安全部的分布式拒绝服务防御项目就是此类研究的一个例子。参见美国国土安全部，分布式拒绝服务防御，（最新访问2018年4月4日）。另请参阅国家科学基金会，安全可靠网络空间（SaTC），（最新访问，2018年4月4日）。https://www.dhs.gov/science-and-technology/csd-ddosdhttps://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504709

[69]网络和信息技术研究与开发计划（最新访问，2018年4月4日）。https://www.nitrd.gov/

70 Sean Brooks’ Michael Garcia’ Naomi Lefkovitz’ Suzanne Lightman和Ellen Nadeau’《联邦系统隐私工程和风险管理简介》（2017年1月），NIST Interagency /内部报告第8062号，网址：https：// nvlpubs。 .nist.gov / nistpubs / ir / 2017 / NIST.IR.8062.pdf。

[71]有关一种类型的隐私影响评估的更多信息，请参阅美国国土安全部隐私影响评估指南（最新发布于2018年4月13日）。
https://www.dhs.gov/publication/privacy-impact-assessment-guidance

[72] NTIA物联网安全升级和修补多方利益相关方流程（最新更新，2017年11月7日）。 https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security

与物联网相关。 IoT社区还应努力提高对这些最佳实践，框架和指南的认识。 NSTAC报告也注意到了这一需求，并建议行业应与国土安全部和商务部合作，加快采用安全准则。

联邦政府应通过与社区互动，确定为什么先前的建议未得到广泛实施或不成功，支持成功采用最佳实践的适当途径，并专注于实用，可靠的工具和杠杆，支持最佳实践的广泛采用。例如，当前的开发实践强调开源和商业软件的重用，这些软件可能已经过时或容易受到攻击，但是（不安全性）这些属性在开发人员和客户中均难以理解。 NTIA关于软件组件透明性的多方利益相关者流程（请参阅操作1.3）可以探索如何提高产品未附带已知漏洞的保证。

一个需要利益相关者共同参与的特别令人烦恼的问题是遗留和孤立代码或“死软件”问题。 NTIA修补多方利益相关者流程中的利益相关者确定了沟通提供安全更新期限的重要性，但并未就不再提供安全更新时会发生的情况提供明确指南。如果使用脆弱的代码，这个问题将会加剧。甚至一位安全专家甚至倡导将废弃软件开源。但是，访问代码只是一个障碍。更新仍必须编写和测试。如果将证书或MUD文件签名（请参阅操作1.4）绑定到域，破产供应商将面临进一步的挑战。解决核心支持不足的软件的外部性的一种模式来自核心基础设施计划，但系统应对全球分布的未维护系统的前景将需要广泛的利益相关方的投入。[73] [74][75]

透明且可验证的软件资产管理（SAM）实践可以帮助企业识别由于不再可用更新或许可证已过期而无法打补丁的软件。一旦确定，企业可以通过更换产品或重新架构网络来管理风险来解决这些漏洞。企业和政府利益相关者应采用基于国际采购和资产管理标准的SAM做法，以及缓解通过这些做法确定的风险的程序。

如行动5.3、5.4和5.5所述，为提高认识并对产品开发人员和制造商进行教育而进行的补充努力可能会大大增强这些最佳实践，框架和指南的影响。

---

73 FTC关于移动安全更新的报告建议公司考虑在安全支持期结束之前披露最低支持期和通知。联邦贸易委员会，移动安全更新：了解问题，（2018年2月），https：//security-updates-understanding-issues/mobile_security_updates_understanding_the_issues_publication_final.pdf。

74 Dan Geer，《2014年美国黑帽大会主题演讲：网络安全作为现实政治》（2014年8月6日），可从（名义交付草案）获得。视频可在以下网址获得：https：//www.ftc.gov/system/files/documents/reports/mobile-http://geer.tinho.net/geer.blackhat.6viii14.txt www.blackhat.com/us-14/video/cybersecurity-as-realpolitik.html.

75 核心基础设施倡议，（最新访问，2018年4月4日）。https://www.coreinfrastructure.org/

目标2：促进基础设施创新，以动态适应不断发展的威胁。

为建立更具复原力的互联网和通信生态系统，应对和预期到不断演变的威胁，应在生态系统的所有领域中持续实施和升级阻止，防止和/或缓解僵尸网络和分布式威胁的标准和实践。本节确定了利益相关者可用来支持有效和动态基础设施开发的行动。

行动2.1互联网服务提供商及其对等伙伴应扩大现有信息共享范围，以在国内和全球范围内更及时，有效地共享可采取行动的威胁信息。[76]

建立僵尸网络后，僵尸网络将被重新出售或租赁给多个客户，并重定向到新目标。这意味着随着时间的推移，许多互联网服务提供商及其对等伙伴将遭受类似的攻击。当ISP首次面临特定威胁时，必须分析异常行为并开发缓解方法。僵尸网络通常分布在许多ISP上，只要有足够的知识，僵尸网络就可以为缓解活动做出贡献。共享有效抵御特定威胁的网络管理技术和防御策略，是大型网络提供商提高共享信息的先发性价值的另一种方式。

当前，互联网服务提供商及其对等伙伴之间的信息共享安排在其范围内非常有效。通过共享有关已知，持续和新出现威胁的信息，互联网服务提供商可以更有效地做出响应。但是，当前的信息共享安排通常由人际关系驱动，并不全面，尤其是在处理更细微差别或敏感威胁时。不断变化的网络格局以及不断变化的网络参与者范围，规模，重点和多样性，也会影响共享关系的有效性。互联网服务提供商（ISP）及其对等伙伴之间的合作应该正式化，包括网络内检测，通知和计划或利用的缓解方法的共享。如果出于商业考虑而阻碍共享，互联网服务提供商应寻求方法解决对等和传输协议中的共享安排和响应协调。

工业界应领导努力，扩大互联网服务提供商及其对等伙伴之间信息共享的范围和效用，并消除在操作共享信息方面的差距。尤其是，行业应与民间社会和政府合作，改善对可操作信息的协调响应，并领导信息共享协议的开发，完善和标准化，以提高速度并允许自动响应。应特别注意小型互联网服务提供商的参与和包容性以及促进其参与的协议开发。

虽然行业起主导作用，但联邦政府可以通过与网络运营商团体（NOGs）结成伙伴关系，通过通信信息共享和分析中心（ISAC）（即国家通信协调中心）在国内促进此项活动。在国际上，通过继续参与事件响应和安全团队论坛（FIRST），并扩大与国际同行（如日本ISAC电信公司）的信息共享协议。政府可以在这些讨论中发挥重要作用，召集

[76]包括运营自己的BGP路由器和域名服务器的企业。

必要时召开多方利益相关方会议，提供全球视野，并确保所有利益相关方公平参与。国家计算机安全事件响应小组（CSIRT）也可以直接进行协调，并可以促进本地资源管理者和基础设施参与者的响应。

行动2.2利益相关者和主题专家应与美国国家标准与技术研究院（NIST）协商，领导制定企业分布式拒绝服务预防和缓解CSF概况。

希望减轻将来的分布式拒绝服务攻击影响并减少内部资源被并入僵尸网络攻击其他企业的可能性的分布式拒绝服务感知企业希望发现尚无全面指南。大型企业被迫投入大量人力物力来确定和采购或部署适当的机制。小型企业通常缺乏专业知识，或者无力转移这些资源来制定反分布式拒绝服务策略。全面的解决方案非常复杂，通常需要结合本地管理和外部商业服务，因此与供应商沟通需求至关重要。

NIST开发了改善关键基础设施网络安全的框架版本1.0（CSF），由私营部门投入，2018年4月发布的1.1版本也是如此。CSF提供了一种灵活的方法来管理包含行业标准的网络安全风险和最佳实践，具有足够的通用性，可以在包括物联网在内的各种环境中广泛应用，并且已被业界广泛接受。框架概要可以补充CSF，将框架组件应用于特定情况。尤其是，行业部门可以使用配置文件记录最佳实践，以防御特定威胁。 CSF旨在随着网络安全环境的变化而发展。

希望增强自身网络抵御分布式拒绝服务攻击的弹性并抵御僵尸网络整合其资源的企业，将可以从用于企业分布式拒绝服务预防和缓解的CSF配置文件中受益。业界领导的工作应与NIST，学术界和其他主题专家协商，为企业分布式拒绝服务防御制定CSF配置文件，重点关注组织网络安全所需的状态以缓解分布式拒绝服务攻击。CSF配置文件将提供指导企业，并为与产品供应商，ISP和其他基础设施提供商进行分布式拒绝服务保护机制的讨论建立通用语言。通过将当前状态与期望的目标状态进行比较，概况可以帮助企业识别改善分布式拒绝服务威胁缓解的机会，并帮助确定网络安全优先级。概要可能包括多个级别，以支持具有不同弹性要求的行业。[77] [78]

CSF配置文件的范围至少应包括内部和外部本地分布式拒绝服务缓解机制，路由安全功能（例如，最佳现行实践[BCP] 38/84入口过滤），以及关闭反射向量的指南。为实现最广泛的应用，配置文件的覆盖范围应涵盖可能运营其分布式拒绝服务缓解策略关键组件的大型企业和通常完全依赖服务提供商的小型企业。

[77]《CSF概况》是遵循已建立的CSF模型的针对特定威胁的指南和最佳实践的汇编。

[78]网络安全政策与法律联盟（网络安全联盟）已经发起了有希望的工作，目前处于草案形式。参见网络安全联盟，使用NIST框架进行分布式拒绝服务攻击的威胁概况，（2017年7月28日）。 https://www.cybersecuritycoalition.org/threat-profile-ddos-nist-framework

政府利益相关者应参与开发，确保概况广泛适用，足以用作联邦分布式拒绝服务预防和缓解的CSF概况。为创造市场激励措施，应按照行动2.3的规定，在整个联邦政府范围内积极采用这项行动，通过直接应用配置文件或使用现有的《联邦信息安全现代化法案》程序采用相应的控制措施。

行动2.3联邦政府应以身作则，展示技术实用性，为早期采用者创造市场激励。

在发布设备物联网安全基线（行动1.1）后，联邦政府应制定采购指南，为早期采用者提供市场激励。许多物联网产品供应商已经制定了提高产品安全性的计划，但观察人士表示，市场激励措施在很大程度上取决于成本和上市时间。如果没有证据表明客户会承担开发更安全产品的额外成本，则行业可能会竞相追逐最低利润。尽管联邦采购不再主导市场，但其购买力和影响力仍然很强，美国政府可以作为榜样。通过基于物联网设备安全基准制定联邦采购行动指南，美国政府可以为早期采用者建立市场激励机制。管理和预算办公室，总务管理局（GSA）和国防部可以通过对GSA时间表和联邦采购法规进行政策和修改来满足这些采购要求。[79]

在发布适当的《CSF概况》（行动2.2）后，联邦政府应对所有联邦网络实施基本的分布式拒绝服务防护和缓解措施，以增强生态系统的弹性并证明该概况的实用性和有效性。过去，黑客利用开放解析器和其他机构资源，利用联邦网络进行分布式拒绝服务攻击，放大攻击。联邦政府应以身作则，确保联邦资源不会吸引参与者，并确保联邦网络做好必要的检测，缓解和响应的准备。主管部门应在所有概要完成并发布后的固定时间内，强制所有政府机构实施《联邦CSF分布式拒绝服务预防和缓解CSF概要》。

联邦政府应评估和实施有效方法，鼓励使用软件开发工具和流程，大幅降低所有联邦软件采购中的安全漏洞发生率，例如通过证明或认证要求。为了建立市场上的激励机制，促进安全软件开发，联邦政府应建立有利于或要求使用此类流程开发的现货供应软件的采购法规（如果有）。联邦政府还应确保政府资助的软件开发项目使用最佳可用工具来深入了解这些法规的影响。

[79]由美国国土安全部（DHS）领导的信息技术协调委员会IoT安全工作组正在为采购官员草拟指南，询问客户，其IT和安全团队以及供应商，以确保采购的连接设备适合该机构的风险管理态势。。本指南将补充但不等同于针对安全基线构建的合规性指南。

行动2.4：工业界，政府和公民社会应与所有利益相关方合作，继续加强和标准化信息共享协议。

为应对自动化的分布式威胁，利益相关者必须以近实时方式共享强大的信息。 NSTAC报告指出，作为一个重要经验教训，公共部门和私营部门之间的合作对于缓解僵尸网络至关重要。当前使用的信息共享协议由联邦政府开创，来自广泛的利益相关者的积极投入，但可能无法满足所有利益相关者的需求。

例如，小型企业的代表性不足；它们不会促进或受益于大多数最新的信息共享安排。为了满足通常缺乏强有力的内部网络安全团队的小型企业的需求，协议可能需要启用自动化措施。例如，互联网服务提供商通常可以识别与被感染设备相关联的客户网络，但缺乏识别特定设备的可见性。如果小型企业与其互联网服务提供商（ISP）联系，则可能无法识别这些设备。信息共享协议允许互联网服务提供商与支持小型企业的路由器共享检测到的受感染设备信息，可以自动识别网络设备并对其提供更强大的客户控制。客户也可能选择与互联网服务提供商共享缓解措施的结果，类似于与供应商共享软件故障信息。

为了满足高度灵活的基础设施的协调和协作需求，这些信息共享协议必须涵盖范围广泛，可供广泛的企业访问，并且必须足够精确以允许自动化处理和响应。为确保实现这些目标，工业界应与联邦政府和其他利益相关方共同努力，增强信息共享协议，以满足利益相关方的需求，并建立促进全球协调的国际标准。

行动2.5联邦政府应与美国和全球基础设施提供商合作，在整个生态系统中扩展最佳网络流量管理实践。

虽然不能指望网络提供商充当流量警察并识别所有不良数据包，但常见的工具和实践都可以帮助过滤某些类型的不良流量。许多市场参与者使用非正式信誉信号或更正式的对等和传输协议来解决流量管理。由国内外专家组成的广泛联盟（行业，学术界，公民社会和政府）应研究自治系统，互联网对等网络和传输协议在多大程度上可以改善流量管理问责制（例如，适用于反欺骗和过滤。学术界和工程界应该研究如何结合和实施开发中的新工具和实践。工业界，学术界，公民社会和联邦政府应基于这些发现，在整个生态系统中扩展建设性政策和最佳实践，同时牢记小型企业的需求。应审查现有工具和框架，例如《美国互联网服务提供商反机器人行为守则》和自愿性相互同意的路由安全规范（MANRS），并在多方利益相关方流程中探索新解决方案，其中应包括以下内容的不同代表：映射到当今生态系统环境的网络参与者。

目标3：促进网络边缘的创新，预防，检测和缓解自动化的分布式攻击。

为了建立弹性的互联网和通信生态系统，应通过增强检测和缓解家庭或企业网络以及这些网络连接到互联网的被感染设备的能力，补充旨在防范攻击的基础设施服务。从本地知识中获取更多背景信息可以改善检测，并且可以简单地对异常行为异常的特定设备或服务进行分段或防火墙处理。本节确定涉众可以采取的措施，管理在自动化分布式攻击中使用的被感染设备的影响。

行动3.1：网络行业应扩大当前产品开发和标准化工作，以在家庭和企业环境中进行有效和安全的流量管理。

网络行业正在寻求各种专有和基于标准的机制，以更好地管理企业网络内的流量。这些机制旨在防止与可疑系统进行通信，或者限制与主机进行正确操作所需的通信。
这些系统可以利用人工智能或机器学习，外部商业服务提供的威胁检测和缓解方法，或特定于设备的信息。工业界应加大力度，加快为家庭和企业环境交付高效，经济高效的网络安全。

本地网络集线器和网关扫描器充当流量管理器，识别和阻止恶意流量访问IoT设备，并限制本地网络中设备发出的有害流量。云提供商还正在开发可能与这些以网关为中心的解决方案分层的解决方案，潜在地在网络堆栈中提供多种制衡措施，从而更好地保护IoT生态系统。随着这些安全创新的不断涌现，政府和利益相关方应携手合作，提高消费者，中小企业和国际合作伙伴对安全解决方案的认识。如果采用或提升存在特定障碍，则应召集政府和利益相关方，找出障碍，促进新兴标准的部署，并研究更广泛产品空间的实用防火墙政策。[80]

行动3.2：家庭IT和物联网产品应易于理解，使用安全性应易于理解。

家用IT和物联网产品应减少或消除安全和私下使用它们所需的知识。企业网络受益于负责维护网络和系统安全的专业人员的关注。此类人员通常意识到并足够熟练地将这些设备配置为安全基准。大多数IT和IoT设备的管理界面都是为具有这种背景和技能水平的人员设计的。

家用和小型企业网络的所有者获得此类支持的可能性较小，网络和产品部署不安全不可避免。 IT和物联网行业不应期望消费者成为安全专家，而应优先考虑面向家庭和小型企业销售的设备的简单，直接的部署和配置过程。对于

[80]网关是位于网络子组件之间的网络体系结构组件。有关智能网关等的讨论，请参见上文第二节。

例如，如果安装过程不强制更新管理密码，这些产品将很容易成为并入僵尸网络的目标。对于预期的使用范围，默认配置应该是最安全的，并且基于云或基于应用程序的界面应直观并依赖于最佳的最新设计实践。安装安全补丁程序应该是自动的或易于管理（例如，无需下载到闪存驱动器）。

行动3.3企业应迁移到有助于检测，破坏和缓解自动化分布式威胁的网络架构。他们还应该考虑自己的网络如何使他人面临风险。

当前有多种有效的抗分布式拒绝服务产品和服务，而创新的新产品（如行动3.1中所述）也已出现。但是，大多数企业为简化和性能而非安全性而架构网络。企业可以结合使用《CSF分布式拒绝服务预防和缓解配置文件》，重新架构网络，隔离不安全的设备，管理通信流，并总体上增强生态系统区域的弹性。例如，依赖传统系统的企业应设计其网络，以使这些不安全的设备不会受到来自通用互联网的攻击。

企业网络带来的风险超过了被劫持的物联网设备的风险。一些基于网络的服务允许恶意行为者通过“反射器”或可以向欺骗目标发送大量流量的服务放大攻击。如果配置错误以允许从互联网上的任何地方查询，域名系统（DNS）服务器等漏洞服务将使攻击者向受害者发送大量流量。 2018年，迄今为止最大的分布式拒绝服务攻击之一是利用相对默默无闻的MemCacheD软件中的一个新发现漏洞，这些漏洞通常更具问题性，因为易受攻击的系统位于企业级机器和网络上，具有高可用性和高带宽。企业应遵循面向互联网工具的最佳实践，并确保它们是最新的。[81]

随着企业将更多的物联网设备集成到其网络环境中，并逐渐意识到面向外部应用程序的风险，这种向更好的网络实践演进的过程可能会有机地发生。但是，政府，行业和公民社会应通过合作伙伴关系活动和战略参与活动等合作，努力提高用户和企业对威胁和最佳安全实践的了解。随着此类知识的形式化，可以考虑将其包含在NIST网络安全框架的未来版本中。

行动3.4：联邦政府应调查更广泛的IPv6部署如何改变攻击和防御的经济状况。

2015年，北美耗尽了容易分发的未使用IPv4地址，但目前极少有消费者和小型企业利用IPv6地址空间和功能。政府和行业一直在计划和努力更广泛地采用IPv6，但也应考虑如何改变潜在的攻击空间和自动分布式攻击规模。

81 Lili Hay Newman，GitHub，有线网络生存了有史以来最大的分布式拒绝服务攻击（2018年3月1日，上午11:01），https://www.wired.com/story/github-ddos-memcached/.

通知消费者网络上的设备已链接到恶意活动是一个挑战，通常有大量设备连接到家庭或小型企业网络。启用了NAT的路由器可以阻止许多设备，就好像它们具有相同的IP地址一样。随着我们过渡到IPv6，当IPv6地址未经过NAT转换时，消费者ISP可能会更好地观察特定于设备的行为。反过来，这些信息可以映射到其他边缘解决方案。

在消费者和小型企业级实施支持NAT的路由器有时有时是易受攻击端点的关键保护。 NAT工具充当附带的防火墙，防止通过传播大量恶意软件并导致广泛感染的大规模扫描工具直接访问家庭设备。安全摄像头是Mirai僵尸网络的常见目标，因为它们通常不位于启用NAT的路由器后面。在当前架构中，基于IPv6的网络可能会允许每个设备寻址。从理论上讲，IPv6地址空间太大，无法使用现有工具扫描。

NTIA应与利益相关方合作，从行业和其他国家吸取经验教训，进一步研究障碍和方案，以调整激励措施，鼓励互联网服务提供商更快地完全过渡到IPv6。启用防御和缓解风险，需要在网络边缘进行进一步的创新。如果IPv6的使用变得更加广泛，那么早日了解这一点将提供更好的解决方案。

目标4：促进和支持国内及全球安全，基础设施和运营技术社区之间的联盟。

为增强互联网和通信基础设施的弹性，跨越地缘政治，公共-私营部门，工业部门和技术边界的协调行动必须变得更加容易实施。本节确定了增加关键利益相关者社区之间互动的关键措施。

行动4.1互联网服务提供商和大型企业应增加与政府机构的信息共享，并提供更多及时和可操作的信息，涉及自动化，分布式威胁。

虽然本报告中的许多措施将增加自动化分布式攻击的成本或降低有效性，但执法措施对僵尸网络社区具有独特的影响。通过关闭指挥和控制系统，执法部门可以快速“分解”分布式威胁。
对僵尸网络经济中主要参与者的起诉不仅减慢了当前参与者发展分布式威胁的速度，而且阻止了潜在的开发人员加入。

执法部门依靠大型和小型ISP，事件响应小组，网络安全和事件响应公司，反病毒供应商，商业实体和网络威胁情报公司，通过提供有关威胁和威胁的可行信息，支持正在进行的调查和其他应对自动威胁的措施。影响其网络和客户的趋势。通过提供更加及时和可操作的信息，互联网服务提供商和其他关键基础设施提供商可以促进，支持和加速执法行动，包括影响跨僵尸网络分布的僵尸网络。

地球仪。例如，利益相关者建议，将事件报告扩展为不成功攻击，可以提供预警，并支持执法部门的早期干预。此类数据还将帮助安全社区更好地了解风险状况。

执法部门可以主动识别哪些数据将帮助他们调查和起诉不良行为者，并与基础设施提供商合作，在保护互联网用户隐私的同时，更廉价，更轻松地与政府共享此信息。改善网络安全信息共享仍然是其中之一。预防和缓解当前和新兴网络犯罪问题的关键要素。为促进证明有效的信任和更广泛的关系，执法部门应继续与安全和网络社区进行外联努力，帮助他们确定和了解政府的合适合作伙伴。[82]

政府机构，包括执法部门，应继续改善共享的网络安全信息的及时性和相关性，以预防和减轻网络事件。执法部门将遭受入侵或分布式攻击的公司视为犯罪的受害者，并酌情调查此类举报的犯罪，避免在不必要的情况下不必要地发布有关事件的信息。此外，私营组织应通过信息共享和分析组织以及在适当的情况下与政府机构共享其行业内的网络安全信息，同时明确确定应与其他实体共享哪些信息，以防止进一步的伤害。

RIR和注册服务商可以通过维护准确的WHOIS数据库促进不良行为者的归因。此外，联邦政府应努力与欧洲同行合作，确保及时获取WHOIS信息，因为欧洲数据隐私保护得到实施，为国内和全球调查僵尸网络的关键工具保留了重要手段。各国政府可以与负责遵守数据隐私保护法规的私营部门实体以及参与僵尸网络调查工作的实体合作，以确保保护这两种资产（合规和僵尸网络调查）。

行动4.2联邦政府应通过双边和多边国际参与，促进国际采纳最佳做法和相关工具。

单靠家庭行动是无法实现生态系统复原力的显着提高。美国应利用联邦机构内部的专门知识，与双边，区域和国际网络安全方面的国际伙伴定期接触。对于与域名系统（DNS）相关的问题，NTIA应与联邦机构协调，并在多方利益相关者论坛中代表美国立场，例如互联网名称与数字地址分配机构（ICANN）和互联网治理论坛。

国际标准化可能特别有益。 IoT产品和服务的国际标准以及可能会破坏自动化分布式攻击的标准可能会扩大有助于生态系统弹性的产品市场。根据NSTAC报告的建议，参与标准制定的行业和联邦机构应

[82]见，例如，信息共享和分析组织（ISAO）标准组织，ISAO SP 4000：在网络安全信息共享v1.0中保护消费者隐私，（2017年7月26日），https：// 0 /。www.isao.org/products/isao-sp-4000-protecting-consumer-privacy-in-cybersecurity-information-sharing-v1-

协调制定战略，让相关的行业驱动国际标准机构参与进来，确保美国的代表性和领导地位，并通过这种参与倡导一套灵活且可互操作的IoT安全国际标准套件。

行动4.3相关行业的监管机构应与行业合作，确保非欺骗性营销并促进针对行业的安全考虑。

由于整个物联网领域的复杂性和多样性，很难设想一套一套千篇一律的规则，既可以确保安全，又可以保持变化速度和威胁环境的动态特性。但是，特定行业的监管机构可以与行业合作，确保所部署产品的安全性适合产品的使用，从而提高生态系统的弹性。例如，美国食品药品监督管理局已经建立了医疗设备指南，将基本安全更新与现有产品认证制度脱钩。这些指南对消费者和医疗制造商都有好处，因为他们所依赖的医疗设备可以更有效地抵御网络安全威胁，而制造商则可以明确认证要求。利益相关者强调，联邦政府可能会受益于跨部门物联网协调机制，以促进和分享此类创新实践和经验教训，避免监管冲突。[83]

谨慎的执法行动可以使市场上的消费者和诚实参与者受益。 FTC已针对众多与隐私和安全相关的案件采取了行动，其中IoT设备属于此类执法行动.FTC可以通过阻止和阻止欺骗性营销来增强消费者对IoT和信息技术供应商对安全声明的信心，并支持积极市场激励措施。 FTC还利用了《 FTC法案》第5节中的不公平权力，对包括物联网领域在内的不合理安全实践提出了质疑。此外，特定部门的机构（例如美国卫生与公共服务部）在相关行业中实施信息安全法规。这些政策可以促进更广泛的生态系统安全讨论，并从中受益。[84]

行动4.4社区应识别杠杆点并采取具体步骤破坏攻击者的工具和激励措施，包括积极共享和使用信誉数据。

许多威胁源于不对称现象，这种不对称现象通过在生态系统中分散的行为者之间分散利用，从而有利于攻击者。防御者可以使用数据和信息共享措施来跟踪攻击者工具，也可以使用伤害发生率识别工具和行为者。在某些情况下，相对较少的协调工作应该能够中断更广泛的攻击类别。第3.3节强调了组织识别放大分布式拒绝服务攻击的反射器的重要性。社区可以跟踪这些威胁的存在，以帮助锁定目标意识和减少威胁。这种共享有助于应对垃圾邮件等威胁，并且可以用于抵御其他攻击手段。

---

83 食品和药品管理局，医疗设备网络安全的上市后管理，（2016年12月28日），参见84。例如，参见联邦贸易委员会，TRENDnet，Inc.，FTC事务/文件号122 3090，（最新更新于2014年2月7日）。

https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.https://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter

“快速流量托管”是自动快速修改域名系统（DNS）中分配给主机的IP地址，隐藏支持恶意，非法或犯罪活动的网站的位置。 2008年安全与稳定咨询委员会（SSAC）的咨询意见考虑了某些注册服务机构和当今注册管理机构今天实施的措施：监控指示快速通量托管的域名系统（DNS）记录更改，限制域名系统（DNS）更改频率和值范围，以及监控注册帐户访问以防止自动化。委员会进一步考虑了注册服务商如何运用此类措施加快对非法网站和域名的暂停流程。这些措施在遏制僵尸网络活动的努力方面可能会产生重大差异，但尚未得到广泛实施。攻击者的新发展，包括“双通量网络”，需要在网络层面进一步创新和协作。包括联邦政府在内的广大社群应在相关的多利益相关方论坛（例如ICANN和RIR）中倡导更广泛地实施这些措施，或实现这一目标的替代机制。[85]

一些生态系统威胁是由特定的非法市场驱动的。活跃的出租分布式拒绝服务市场在游戏社区中蓬勃发展。游戏公司和支付处理方之间的合作可能会跟踪和惩罚使用这些服务的人，从而使市场枯竭。同样，更难通过数据验证来破坏被盗凭证市场。在网络上使用基本的反自动化工具可能会增加攻击者验证被盗凭证价值的成本，从而降低窃取和使用获利。更广泛地说，研究表明，针对上游合作伙伴并告知已暴露漏洞可以在推动补救中发挥关键作用。[86] [87]

政府投资可能是另一个杠杆。代理机构对HTTPS采用等安全问题的指标和透明度做出了响应。在一些指导和管理下，网络卫生声誉可以作为政府收购过程中的一个因素。英国政府已经开始尝试这种方法。[88] [89]

行动4.5：网络安全社区应继续与运营技术社区互动，以提高认识并加速网络安全技术的纳入。

将网络功能整合到运营技术（OT）中（例如，工业环境中的SCADA系统）带来了新的网络安全挑战，只有通过网络安全和OT社区共同的专业知识才能应对。对于网络安全主题专家来说，与OT实例相关的主要要求通常不适用，并且OT主题专家通常不熟悉基本的网络安全实践。

---

85 ICANN安全与稳定咨询委员会，SAC 025：SSAC关于快速流量托管和域名系统的咨询，（2008年3月），https：//www.icann.org/en/system/files/files/sac-025-en.pdf.

86见Timothy Peacock和Allan Friedman，“被盗支付卡市场的自动化与破坏”，（2014年），*可在*http://www.econinfosec.org/archive/weis2014/papers/PeacockFriedman-WEIS2014.pdf.

87参见，例如Orcun Cetin，CarlosGañán，MaciejKorczyński和Michel van Eeten，《再次发布通知：学习大规模漏洞扫描时代的通知》（2017年），见 http://weis2017.econinfosec.org/wp-content/uploads/sites/3/2017/05/WEIS_2017_paper_17.pdf.

88参见，例如，埃里克.米尔，《追踪美国政府转向HTTPS的进展》，美国一般服务管理局，第18层，（2017年1月4日），https：//18f.gsa.gov/2017/01/04/tracking-美国政府移动中的进展https /。

89见伊恩.利维（Ian Levy），《活跃的网络防御__一年后》，英国国家网络安全中心，（2018年2月5日），网址：https：//www.ncsc.gov.uk/information/active-cyber-defence-one-year.

联邦政府可以通过扩大目前的参与程度来促进这一过程，将网络安全和旧约社区团结在一起，共享知识和专业知识，提高认识并加速网络安全社区的技术采用。特定领域的机构与各自部门紧密合作，了解网络安全风险，将部门与联邦资源联系起来，促进弹性规划。工业控制系统网络紧急响应小组（ICS-CERT）致力于降低所有关键事件的风险，并与国际和私营部门计算机事件响应小组（CIRT）合作，共享与控制系统相关的安全事件和缓解措施。联邦政府网络安全社区目前正在与特定的OT社区开展针对设备的互动活动，主题涉及输液泵安全更新。 OT社区应参与本报告中引用的行业行动，推动针对其个人网络风险的针对特定行业的解决方案。infrastructure sectors

目标5：提高整个生态系统的认识和教育。

为增强互联网和通信生态系统抵御分布式威胁的能力，所有利益相关者必须理解并准备执行其角色和职责。本节确定针对分布式威胁的特定措施，这些措施将缩小当前技能和职责之间的差距。

这些拟议的行动并不能代替提高网络安全意识和教育的一般努力。利益相关方表示，这些广泛的网络安全意识和教育举措对于以可持续的方式提高生态系统的弹性至关重要。例如，在公众意见和会议及研讨会上的贡献中反复强调了在K-12流程早期开始网络安全教育的重要性。

由美国商务部NIST领导的国家网络安全教育倡议（NICE）是政府，学术界和私营部门之间的合作伙伴关系，专注于网络安全教育，培训和员工队伍发展。其使命是激发和促进强大的网络和网络安全教育，培训及劳动力发展生态系统，重点是网络安全工作者。计划范围包括K-12网络安全教育和大学学术课程，例如国家网络安全学术卓越中心，以及基于绩效的评估和培训计划的开发和管理。国土安全部补充了NICE的贡献，在通过STOP开展宣传活动中发挥了至关重要的作用。认为。CONNECT。程序。[90] [91] [92]

以下行动基于这些更一般的网络安全意识和教育努力，确定与缓解或预防分布式威胁特别相关的意识和教育机会。

[90] 美国国家标准技术研究院国家网络安全教育倡议（最近访问2018年4月4日）。 https://www.nist.gov/itl/applied-cybersecurity/nice

[91] 个国家安全局网络安全卓越学术研究中心（最新访问，2018年4月10日）。 [92] 停止。想想。 Connect。，（上次访问2018年4月4日）。 https://www.nsa.gov/resources/educators/centers-academic-excellence/ https://www.stopthinkconnect.org/

行动5.1私营部门应为家庭物联网设备建立和管理自愿信息工具，并由消费者信任和直观理解的可扩展且具成本效益的评估流程。

私营部门应与民间社会和政府专家协商，为物联网设备设计一种高效有效的评估和标签方法，以便注重安全的消费者可以做出明智的选择，并为设计安全产品开发创造市场激励措施。许多商用物联网产品在设计时并未考虑安全性。这些设备会对生态系统的所有成员造成系统性风险，并使消费者的隐私和安全面临风险。在理想情况下，消费者更喜欢能够保护自身安全和隐私的物联网产品，但注重安全性的消费者无法轻松确定哪些物联网产品旨在确保安全。没有这些信息，其选择标准将仅限于价格和功能集。

私营部门最适合创建和维护轻量级和敏捷机制，但通常可以从政府的召集力量中受益。联邦政府应在多利益相关方流程中召集行业，公民社会和政府利益相关方，探讨可行标签方法的要求。这项工作可以建立在NTIA IoT安全升级和修补多方利益相关方计划等计划最初成功的基础上，该文件详细列出了制造商应在购买前后与消费者进行沟通的关键要素。供应商断言是可行的，可以满足家庭消费者的需求。这种机制的可行性可能部分取决于现有禁止商业欺诈的禁令。例如，联邦贸易委员会可以通过采取措施防止欺诈性营销（例如虚假合规声明），并了解与长期保持静态的安全主张相比，不能提供类似的担保，从而保护评估机制的完整性。国土安全部还可以通过其现有的意识活动（如停止）来支持评估计划。认为。连接。 （请参阅操作5.3）。[93] [94]

虽然物联网安全和隐私并非完全相似，但NHTSA 5星级安全评级和能源之星计划等机制已成功提高了客户认知度，并创建了安全车辆和节能设备市场，支持了可行标签的假设这种方法将有助于减少自动化和分布式攻击。但是，大量不同的物联网设备以及许多此类设备的销售周期相对较短（与汽车和热水器相比）表明，将需要更轻巧，更灵活的机制。鉴于当今业务的全球性质，评估方案应尽可能以国际认可的标准为基础。此外，任何使用安全评估和标记方法的行为都需要反映安全断言（不能随时间推移保持不变）和安全断言（不能提供类似保证）之间的差异。国土安全部可以通过探索可能有效支持关键基础设施需求的认证制度的机会，来补充此类广泛适用的机制。

IoT设备及其可用性的主观评估也有作用。面向消费者的测试组织通常会在舒适性或可用性方面进行更主观的评估，从而补充基于特征的分析和维修历史。管理接口在安全性方面的可用性尤其重要

93 NTIA物联网安全升级和修补多方利益相关方流程（最新更新，2017年11月7日）。 94停止。想想。 Connect。，（上次访问2018年4月4日）。
https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security
https://www.stopthinkconnect.org/

困难的问题。面向消费者的测试组织可以通过对可用性进行周到的评估，帮助消费者确定适合其技能水平的产品。

行动5.2：私营部门应为工业物联网应用建立自愿性标签计划，并采用可扩展且具有成本效益的评估流程，为物联网关键基础设施应用提供充分保证。

在自动化，分布式攻击的背景下，物联网的关键基础设施和工业应用对国家的风险要大于家庭应用。这些设备还部署在非常不同的环境中，得到专业管理员的支持。行动5.1中设想的自愿性轻量级评估机制无法为这些客户提供足够水平的保证，并且可能需要其他功能。评估功能（如设备身份验证，硬件信任根或托管更新功能）需要与产品直接交互（如果不检查源代码）。

这种过程取得成功的例子在政府和私营部门都有。例如，超过20年的时间，NIST的密码模块验证计划利用独立测试实验室评估密码模块是否符合联邦信息处理标准（FIPS）140标准。在私营部门，安全和认证公司UL针对商业和消费市场提供各种认证和合规计划，2016年产品上出现超过200亿个UL商标。然而，零散或过于复杂的标签可能适得其反。美国联邦贸易委员会在标签方面拥有丰富的专业知识，支持清晰的披露，但警告称，“不良披露，包括过度广泛的披露，实际上可能会阻碍消费者做出明智选择的能力。”[95]

私营部门应建立有效但稳健的评估流程，以确保这些部门的物联网设备在适当的保证水平下具有增强的弹性。建立评估产品清单将使注重安全的企业做出明智的选择，并为稳健的安全开发生命周期流程创造市场激励措施。

行动5.3：政府应鼓励学术和培训部门将安全编码实践充分纳入计算机科学和相关程序。

如行动1.3所述，通过使用适当的安全开发工具（如模糊器，静态分析器和安全编程语言），可以在产品开发过程中避免或纠正许多常见的安全漏洞（例如，缓冲区溢出）。虽然学术机构，编码训练营和工作再培训计划正在创建更大的编码队伍，但其毕业生很少熟练掌握这些语言或善于使用这些开发工具。相反，学生会在不考虑安全性的软件开发工具和不将安全性放在优先位置的软件开发方法学上积累大量经验，在软件开发人员中树立了“断断续续”的思维方式。

希望改进编码实践的公司可能会因准备不足，有时甚至抵触的员工队伍而受阻。熟练的编码人员如果对学习新技术不感兴趣，可以轻松地换工作。

[95] 联邦贸易委员会，关于“交流IoT设备安全更新能力以提高消费者透明度的公共评论”，第6页，（2017年），网址：https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-comment-national-telecommunications-information-administration-communicating-iot-device-security/170619ntiaiotcomment.pdf.

做法，并且可能很难替换。通过讲授设计安全软件方法论，并鼓励在整个计算机科学和网络安全相关课程中使用安全意识软件开发工具链，我们可以为构建高质量软件和增强对以安全为重点的软件开发工具链的接受度的员工队伍做准备。 。

联邦政府可以通过与学术界和培训行业的现有关系促进这些变化。特别是，NICE应与学术界和私营部门合作，在研究过程的每一步中纳入设计安全原则和支持工具。 NICE网络安全劳动力框架（NICE框架）的"安全提供"类别包括安全软件和产品开发所需的知识，技能和能力。 NICE应该与教育和培训提供者合作，鼓励他们使用NICE框架作为开发课程内容的参考工具。再举一个例子，FTC每年举办一次PrivacyCon会议，为学者和安全研究人员提供有关隐私和安全工作的展示柜。[96]

行动5.4：学术界应与国家网络安全教育倡议合作，将网络安全确定为所有工程学科的基本要求。

随着信息技术被集成到全系列产品和服务中，新型产品将带来网络安全威胁。产品设计师通常不了解将IT集成到传统产品线时可能带来的风险。随着我们在各种环境（包括土壤，高速公路和建筑物）中嵌入传感器，对这些员工理解网络安全风险管理的需求正在日益增长。例如，自1949年以来，闭路电视（CCTV）相机开始在市场上销售，但直到最近才演变为互联网连接设备。 2016年，Mirai僵尸网络入侵了100,000多台CCTV摄像机，以支持分布式拒绝服务攻击。在其他情况下，用作婴儿监视器的连接互联网的摄像头会利用默认管理密码遭到黑客攻击，侵犯了车主的隐私。[97]

为确保产品设计人员意识到运营技术带来的风险，教学工程及相关学科的学术机构应将基本网络安全纳入必修课程。如上所述，NICE应与学术界和私营部门合作，将原理纳入工程和相关学科的学习过程中。

行动5.5联邦政府应开展公众意识运动，支持家庭物联网设备安全基准和品牌的认可和采用。

为达到影响，安全意识型消费者必须识别并偏爱家用物联网设备安全基线，增强安装设备的家庭网络的弹性，并为安全意识型供应商建立市场激励机制。联邦政府在利益相关者的支持下开展公众宣传运动的历史由来已久，涉及各种各样的话题：如何预防森林火灾，安全带的价值以及艾滋病毒检测的重要性。停止。想想。
连接。这是由国土安全部赞助的全国公众意识运动，旨在提高

[96]见联邦贸易委员会，PrivacyCon 2018，（最新访问日期：2018年4月4日）。https://www.ftc.gov/news-events/events-calendar/2018/02/privacycon-2018

[97]见达琳·暴风雨，黑客劫持无线Foscam婴儿监视器，保姆谈话和怪胎，计算机世界（2015年2月2日，太平洋时间下午12:09），https：// wireless-foscam-baby-monitor-talks-and-freaks -out-nanny.html。 www.computerworld.com/article/2878741/hacker-hijacks-

了解网络威胁并授权美国公众更安全，更安全地上网。联邦政府应考虑利用Stop。想想。连接。或发起补充性的公众意识运动，提醒家庭用户和小型组织家庭IoT设备基线的重要性，并教育他们如何识别更安全的产品。更一般而言，增强用户对网络安全风险的意识对于建立有弹性的生态系统至关重要，政府应加强与目标用户社区和民间社会的战略参与和召集能力，以提高安全采用率和认识，并欢迎希望发挥更大作用的任何非政府利益相关方参与角色。

* * *

利益相关方行动的初步后续步骤

上一节详细介绍了旨在实现五个目标的24项措施。这五个目标相互支持。必须实现所有五个目标，以可持续提高互联网和通信生态系统的弹性。许多动作在设计上也相互支持，即使在多个目标之间也是如此，因此，排除或省略某个动作可能会延迟实现多个目标。但是，由于相关利益相关方社区的资源紧张等因素，我们预计并非所有行动都会同时发生。此外，一些行动已经在进行中，而其他行动则取决于外部因素。联邦政府将不会领导实施针对行业的行动。但是，了解到在某些情况下私营部门可能需要一些时间，美国政府将立即开始协调以下概述的初始步骤。

制定优先路线图，采取协调行动，增强互联网和通信生态系统抵御分布式威胁的能力。

为确保利益相关者有足够的资源和有效地执行最重要的行动，利益相关者社区大力鼓励联邦政府明确划定行动重点，尤其是一些行动不直接涉及联邦政府，但支持或支持依靠联邦参与或领导才能采取的行动的支持。通过表明自己的优先事项，联邦政府可以增强利益相关者的信心，即投入资金用于由联邦领导的行业主导行动将产生富有成果的结果。[98]

除联邦依赖性外，一些行动还具有自然的时间顺序：例如，行动5.1和5.2中的评估计划取决于行动1.1中适当安全能力基线的建立。其他优先行动的时机已经成熟，因为筹备工作正在进行中，例如行动2.2中所述的CSF简介。最后，由于准备周期长，一些行动特别紧急（例如，行动1.3、5.3和5.4），或者事态发展正在缩小美国影响方向的窗口（行动1.2）。

商业和国土安全部应与行业，公民社会协调并与国际伙伴协商，负责制定初步路线图，并在批准本报告后120天内采取优先行动。该路线图应与

[98] 在利益相关方对2018年1月5日的请求征询意见稿以及2018年2月28日至3月1日的研讨会上均强调了这一要求。

在完成第13800号行政命令赋予的任务后，将确定行政管理重点。政府和私营部门将共同努力，确保在利益攸关方完成所确定的行动后，对路线图进行更新和维护。

联邦政府将以身作则。

利益相关者表示，联邦领导对其他利益相关者实施报告至关重要。利益相关者表示，联邦采用主要有益于生态系统和采购活动的“好邻居”做法，将为进一步开展活动减少自动化，分布式威胁奠定基础。尤其是，联邦机构实施出口过滤以防止网络地址欺骗，关闭用于放大流量的反射器并衡量机构合规性（以及可能有名无实的不良行为者）的措施，将表明联邦政府决心并鼓励其他各方采取有益行动。 NIST，OMB和DHS应探索确保联邦机构政策，标准，指南和监督正确反映这些最佳实践的步骤。

同样，强制实施比今天更安全或更灵活的产品和服务的联邦采购活动被视为建立市场激励措施的重要步骤。利益相关者建议立即关注行动1.1、1.2和2.3，以支持联邦采购指南。然后，这项设计工作可以评估现有的采购指南和标准，以及针对更新指南以反映安全要求的具体建议。

促进私营部门的领导，支持跨部门协调，跟踪路线图的执行情况。

许多路线图行动应由工业部门，学术界或民间社会领导。为这些活动确定或建立私营部门治理结构将是可持续性和国际认可工作产品（如技术规格或评估计划）的关键因素。如果现有机构已经采取相关行动或已经代表关键社区，则应鼓励它们牵头。采取行动可能需要超越当前结构的包容性，例如，增加民间社会或国际参与者或观点。

随着社区组成实施这些行动，在这些社区之间建立定期协调的场所将变得越来越重要。如果无法及时建立评估方案，则物联网安全基线的价值将受到限制。为了使对基础设施弹性的影响最大化，需要对投资进行协调和协调。在确定共同商定的一个或多个私营部门政党之前，联邦政府将提供协调和沟通机制以继续实施，并将召开有关政党的定期会议。

向总统提供365天的路线图实施状态报告。

为跟踪进展情况，美国商务部和国土安全部将为总统制定365天状态更新，该路线图首次发布后一年。此更新将审阅：
1）整个社区在反对路线图方面取得进展；2）这些路线图活动的影响；3）重新评估自动化分布式攻击的威胁，包括是否

威胁正在增加或减少，以及此类变化的任何已知原因；4）是否需要对路线图进行任何调整。

通过加强利益相关者和美国政府在国际政策和标准制定方面的参与，促进全球参与。

在商务和国土安全部执行的过程中，经常强调分布式威胁的全球性。利益相关者强调了国际标准，政策和最佳实践对促进国际参与和协作的重要性。通过继续倡导以行业为主导的方法，并积极参与基于共识的自愿国际标准的制定，联邦政府可以为满足所有利益相关者需求的务实有效的基于结果的标准做出贡献。联邦政府在领导建立广泛接受的政策和最佳实践所需的国际参与方面也处于独特地位，并将在这些方面加强与利益相关方的协调。

附录：首字母缩写词列表

AI	人工智能
BCP	当前最佳实践
BGP协议	边界网关协议
CCTV	闭路电视
CDN	内容交付网络
CIRT	计算机事件响应小组
CISA	2015年网络安全信息共享法
CSF	NIST网络安全框架
CSIRT	计算机安全事件响应小组
CSRIC	通信安全，可靠性和互操作性委员会
DDoS	分布式拒绝服务
DHS	国土安全部
DNS	域名系统
FIPS	联邦信息处理标准
FIRST	事故响应和安全团队论坛
FTC	联邦贸易委员会
GSA	总务管理局
HTTPS	超文本传输协议安全
ICANN	互联网名称与数字地址分配机构
ICS-CERT	工业控制系统网络应急响应小组
IETF	互联网工程任务组
IoT	物联网
IP	互联网协议
IPv4	互联网协议版本4
IPv6	互联网协议版本6
ISAC	信息共享和分析中心
ISP	互联网服务提供商
IT	信息技术
LAN	局域网
MANRS	相互同意的路由安全规范
MUD	制造商的用法说明
NAT	网络地址转换
NCC	国家通信协调中心
NCCIC	国家网络安全和通信集成中心

NHTSA	国家公路交通安全管理局
NICE	国家网络安全教育倡议
NIST	美国国家标准技术研究院
NISTIR	NIST机构间/内部报告
NITRD	网络和信息技术研发
NOG	网络运营商组
NSTAC	总统国家安全电信咨询委员会
NTIA	国家电信和信息管理局
OT	运营技术
PPD	总统政策指令
RFC	请求发表评论
RIR	区域互联网注册中心
SAM	软件资产管理
SCADA	监督控制和数据采集
SSAC	安全与稳定咨询委员会