总统的
国家安全电信咨询委员会

NSTAC就互联网和通信弹性向总统报告

目录

执行摘要

僵尸网络助长的自动化和分布式攻击威胁着互联网生态系统和国家关键基础设施的安全性和弹性。在过去几年中，通过僵尸网络发起的分布式拒绝服务（DDoS）攻击的规模和规模急剧增长。这种事态发展加剧了人们对此类攻击可能淹没美国（美国）关键基础设施的担忧。令问题更加复杂的是，物联网设备的日益混合为恶意行为者提供了一个成熟的环境，使恶意行为者可以使用受损的物联网设备发起全球自动化攻击。这种情况威胁到互联网生态系统的安全。

2017年5月，总统执行办公室（EOP）要求总统国家安全电信咨询委员会（NSTAC）研究私营部门和政府如何提高互联网和通信生态系统的弹性。EOP为支持第13800号行政命令，加强联邦网络和关键基础设施的网络安全，特别要求NS TAC确定鼓励合作减少自动化和分布式攻击（僵尸网络）威胁的方法。这份NSTAC致互联网和通信弹性主席的报告（以下简称"报告"）介绍了NSTAC的工作及其建议。[1]

了解到的关键经验

需要更大的紧迫感。威胁只会随着IoT设备数量和类型的增长以及此类设备变得更加自治，强大和无处不在而增加。在可能的情况下，应并行（而不是顺序）进行研究，测试和实施可能的解决方案。必须努力克服威胁。

公私伙伴关系是关键。金融系统分析和弹性中心等公私合作伙伴关系，以及联邦调查局，微软和互联网服务提供商的努力表明，犯罪僵尸网络以及命令和控制结构可以被有效破坏。公共部门和私营部门之间的协作对于缓解僵尸网络至关重要。

解决方案取决于互联网生态系统的每个部分。分布式攻击是一项复杂的挑战。互联网生态系统中没有任何一个部门可以单独解决这个问题。

解决方案取决于网络和互联网基础设施层的标准和创新。尽管存在各种标准和最佳实践，但采用这些实践缺乏全球一致性。标准在确保互联网生态系统中至关重要在基础设施层需要新兴解决方案。此外，在设备上游开发标准，例如在芯片组一级，可能会有价值。

1新闻秘书白宫办公室。13800号行政命令，加强联邦网络和关键基础设施的网络安全。2017年5月16日。https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure.

教育和意识落后。国家需要一个知情的数字公民。个人和企业必须了解他们的决策如何影响网络，系统和彼此。

不清楚的国际规范使挑战复杂化。大多数威胁来自海外，因此国际调查和起诉至关重要。需要在技术标准，设备安全性，归属，流量和共享规范与防御方面进行全球合作。

需要一种新的信任模型。传输控制协议/互联网协议，边界网关协议，域名系统和互联网背后的许多其他协议在设计时并未将安全作为首要考虑因素。随着网络变得更加开放和互联，这种信任模型将不再是互联网安全的唯一基础。定义如何在互联网中建立更大的信任度，将是下文所述网络安全Moonshot计划的重点。[2]

关键建议

私营部门必须采取行动。应对自动化和分布式攻击，需要在整个互联网生态系统中保持警惕，包括网络服务提供商或ISP，设备制造商，软件开发商，云，应用程序和托管提供商以及其他实体，所有这些都构成互联网基础设施。NSTAC建议采取以下短期行动：

- **加速采用安全准则。通信部门应与国土安全部（通信部门特定机构）和美国国家电信**和信息管理局（NTIA）合作，确定通信网络的相关通用安全措施，以防止僵尸网络和分布式拒绝服务攻击。国内和全球标准机构（如最佳通用实践（BCP）38），确定采用的障碍和/或促进采用的激励措施。网络可能不限于大型互联网服务提供商（ISP），因为运行企业可公开寻址网络的任何实体（包括企业业务）都应部署多种实践。

- **制定物联网设备安全准则。**美国商务部（DOC）应通过NTIA和美国国家标准技术研究院（NIST）合作，促进与设备相关风险一致的建议常识安全实践基准的发展。DOC还应审查自愿设备认证和独立测试的作用和可行性，以确保设备安全。

- **继续围绕基于基础设施的解决方案进行创新。**政府和行业不能仅依靠一致采用标准来保护物联网。互联网服务提供商，无线服务提供商，路由器制造商，安全解决方案提供商等正在开发服务，以管理物联网安全。这些解决方案可以在家庭内部（例如，以太网，Wi-Fi）网络的不同层使用，包括：长期的

2通信安全可靠性和互操作性理事会第五次会议：第10工作组，降低传统风险（2017年）（降低传统风险报告），https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf.

演进或第五代无线网络基础设施；多协议标签交换网络核心；以及在应用程序层或云中。这些能力正在兴起，私营部门应继续投资这些技术。美国政府应通过将其纳入联邦采购要求并提高对其在物联网安全应用程序的认识，帮助推动这些功能。[3]

- **促进企业安全控制，提高IoT设备安全性。**NIST应该在NIST网络安全框架的基础上开发用例，使企业将物联网纳入风险管理。许多物联网设备将在消费者和企业网络中实现双重目的。企业和政府可以在采购安排中推广设备的IoT安全标准。

- **促进软件保障。**软件行业应与国土安全部（DHS）合作，推广通用的软件保证实践。意识到最佳实践，可以使买方了解供应商如何整合安全措施，并帮助他们做出更好的采购决策。

政府必须采取行动。政府应在三个基本领域应对僵尸网络日益增长的威胁。NSTAC建议政府（1）采取更多行动支持执法；（2）促进采用安全标准和最佳实践；（3）制定有效的国际网络安全战略。

- **执法**

  - **支持公私合作和删除。**包括司法部（DOJ）在内的政府应加大拆除工作，成功减轻僵尸网络的影响。美国政府应增加激励措施，尤其是在司法部内部，以优先防范网络犯罪和破坏僵尸网络。僵尸网络对国家安全的影响为预防和起诉辩护。司法部可能需要更多资源来加大力度，这也取决于与私营部门和潜在国际伙伴的合作。

- **促进采用安全标准和最佳实践**

  - **使用激励措施促进灵活的标准并消除采用障碍。**NTIA，NIST和其他机构应召集利益相关方，促进跨部门协调，以制定通用标准并在政府和关键基础设施中推广一致做法。政府应找出差距和激励措施，激励行业采用标准和惯例。一些行业如果滞后，可能需要更多激励措施，特别是在缓解现有设备风险方面。小型企业可能也缺乏与大型实体相同的资源和网络专业知识。最后，保险市场可能会推动

3思科提供了一个示例性框架，用于在以下网络的每个网络层进行物联网安全保护：https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html

承销商对公司的安全风险管理实践的成熟度进行调查，并向到期规模较大的公司提供较低的保费，从而改善财务状况。

- **寻求统一联邦，州和国际各级的安全要求。**网络安全标准，实践和法规通常采用的是零散的，有些无效的方法。在国内，一些州制定针对特定州的安全要求。在国际上，欧盟，日本，中国和其他几个国家正在研究开发物联网设备认证和测试计划。美国政府必须在国家和地区之间倡导一致的可互操作IoT安全标准，以鼓励采用统一方法。

- **增强政府网络安全。**美国政府应树立榜样，提高联邦网络的安全性。信息技术现代化是改善联邦网络安全的关键组成部分。政府应继续努力，使联邦信息技术现代化，推动私营部门采用新技术和安全解决方案。

- **国际网络安全**

  - **制定全面的美国标准参与策略。**传统上，美国依靠与私营企业的合作来加强政府在国际标准论坛上的努力。但是，近年来，外国实体在制定国际标准方面迅速增长。美国政府应与私营部门合作，确保在影响技术标准发展的关键论坛中派代表参加，未来可能会导致国家安全问题。

  - **制定有效的国际网络安全战略，重点提高攻击者的成本。**政府应优先考虑利用传统外交工具和支持全球执法的综合国际网络安全战略，以提高网络攻击者的成本。许多分布式拒绝服务攻击是国际性的，政府必须实施全球战略来应对威胁。网络攻击的持久性意味着即使拥有最佳实践的实体也可以被利用。国家必须提高攻击者的成本，同时采用标准，做法和新的创新技术解决方案，使攻击更加困难。

- **国家需要网络安全月球。**NSTAC未来的工作应分两个阶段分析启动网络安全Moonshot的概念。第一阶段将审查其他成功的Moonshot模型，包括网络安全领域以外的模型，以确定可应用于网络安全挑战的一致原则。首先，应包括研究至少具有以下特征的模型：

  - 国家行动呼吁；
  - 关注最终目标，在特定日期之前设定特定目标或最终状态；和
  - 政府主导的多利益相关方流程。

在研究的第二阶段，NSTAC将寻求澄清与确定的Moonshot原则（行动呼吁，最终目标重点和多方利益相关者流程）相关的关键网络安全考虑因素，并利用网络安全专家定义最终目标和依据-元素，并扩展了NSTAC在编写本报告时审查的内容。[4]

4一个例子是由史蒂夫·沃拉赫（Steve Wallach）提供的关于统一内存引用模型的简介。美光科技公司向NSTAC ICR小组委员会简介。 2017年9月7日。

1.0 引言

人们越来越担心恶意行为者使用僵尸网络促进大规模分布式拒绝服务（DDoS）攻击，这种攻击可能会破坏美国关键基础设施。攻击者利用域名系统（DNS），网络时间协议（NTP），简单服务发现协议，字符发生器协议（CharGen）和其他协议等互联网基本漏洞，大幅增加攻击规模和规模。此外，尽管僵尸网络并不是新鲜事物，但物联网设备将连接越来越多的人员，设备和网络，因此风险加剧。2016年的Mirai僵尸网络攻击是第一个产生重大影响的基于IoT的僵尸网络，但预计此类攻击还会增加。这些因素导致分布式拒绝服务攻击规模和规模迅速增加。例如，据一位消息人士称，到2012年中期，攻击规模约为100吉比特/秒，此后规模开始急剧增长。同一消息来源估计，2016年的峰值攻击规模约为800 Gbps，过去四年增长了八倍。本报告提供建议，减少僵尸网络和分布式拒绝服务攻击对国家关键基础设施的潜在影响。[5][6][7]

1.1 作用域和计费

2017年5月，总统执行办公室（EOP）要求总统国家安全电信咨询委员会（NSTAC）研究私营部门和政府如何合作提高互联网和通信生态系统的弹性。EOP为支持第13800号行政命令，加强联邦网络和关键基础设施的网络安全，责成NSTAC确定鼓励合作减少自动化和分布式攻击（僵尸网络）威胁的方法。此外，EOP要求NSTA C考虑采用何种参与规则才能开展合作努力，保护国家的网络安全态势。 2017年6月，NSTAC成立了互联网和通信弹性（ICR）委员会，以应对EOP的要求。 EOP表示，NSTAC的调查结果将为商务部和国土安全部于2018年1月发布的初步报告提供依据。[8][9]

分布式拒绝服务和僵尸网络攻击日益受到关注。 NSTAC在2014年观察到：“ [到2020年，将有数百亿台设备投入使用。现在是时候去影响那些设备的设计方式和协议控制使用范围了；部署新策略后

5 Arbor Networks全球基础设施安全报告，第十二卷，请访问：https://www.arbornetworks.com/insight-into-the-global-threat-landscape

6参见《计算机周刊》，“全球黑客僵尸网络超过600万被劫持设备”，2017年9月27日http://www.computerweekly.com/news/450427023/Global-hacker-botnet-tops-6-million-hijacked-devices

7 Arbor Networks全球基础设施安全报告第十二卷，请访问：https://www.arbornetworks.com/insight-into-the-global-threat-landscape

8新闻秘书白宫办公室。 13800号行政命令，加强联邦网络和关键基础设施的网络安全。 2017年5月11日。https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure.

9 ICR小组委员会的报告将于2017年10月提交。国土安全部和商务部将在2018年1月之前发布初步报告，在2018年5月之前发布最终报告。

只会影响边缘的变化。" NSTAC的目标是帮助政府深化政府和私人合作。[10]

这份NSTAC致互联网和通信弹性主席的报告（以下简称"报告"）介绍了NSTAC的工作及其建议。它为EOP提供了可行的路线图，以应对僵尸网络以及我们的互联网基础设施，在线服务和最终用户的其他分布式和自动化攻击带来的威胁。本报告研究了威胁和解决方案，包括短期补救措施和长期互联网架构开发。该报告的组织结构如下：

- 第1节介绍了范围界定和目标。
- 第2节介绍了全球互联网生态系统以及分布式攻击如何威胁日益紧密联系的世界的安全。
- 第3节确定了生态系统各部分中的挑战和缓解措施：网络，消费者/边缘/设备，企业和软件/应用程序/操作系统（OS）。
- 第4节提供短期和长期建议，以及后续的Moonshot研究，以更全面地整体应对网络安全挑战，包括自动化和分布式攻击。
- **第5节确定了政府使用其可用的独特工具并与私营部门合作的机会。**

1.2 方法

NSTAC使用了几种收集信息的方法，包括主题专家的简介，政策审查以及审查网络安全威胁报告，文章和最佳实践，以应对这些威胁。 NSTAC除其他事项外：

- 收到了来自行业，学术界和公共部门专家的二十二次简报，如附录A所示；
- 审查了私人和联邦政府的网络安全政策，法规，报告和最佳实践，例如美国国家标准技术研究院（NIST）的网络安全框架；
- 审查了当前行业网络安全最佳实践和研究；和

10总统国家安全电信咨询委员会（NSTAC）。 NSTAC就物联网向总统报告。2014年11月19日。附录E，C-5。 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.

- NIST和国家电信与信息管理局（ＮＴＩＡ）审查了有关网络安全的研究和评论。

NSTAC审查了生态系统安全方面的弱点，并确定了领域，以改善网络，设备和用户级别的安全。在本报告中，NSTAC建议采取步骤建立更安全的互联网生态系统，重点关注政府和行业合作伙伴应对恶意活动。

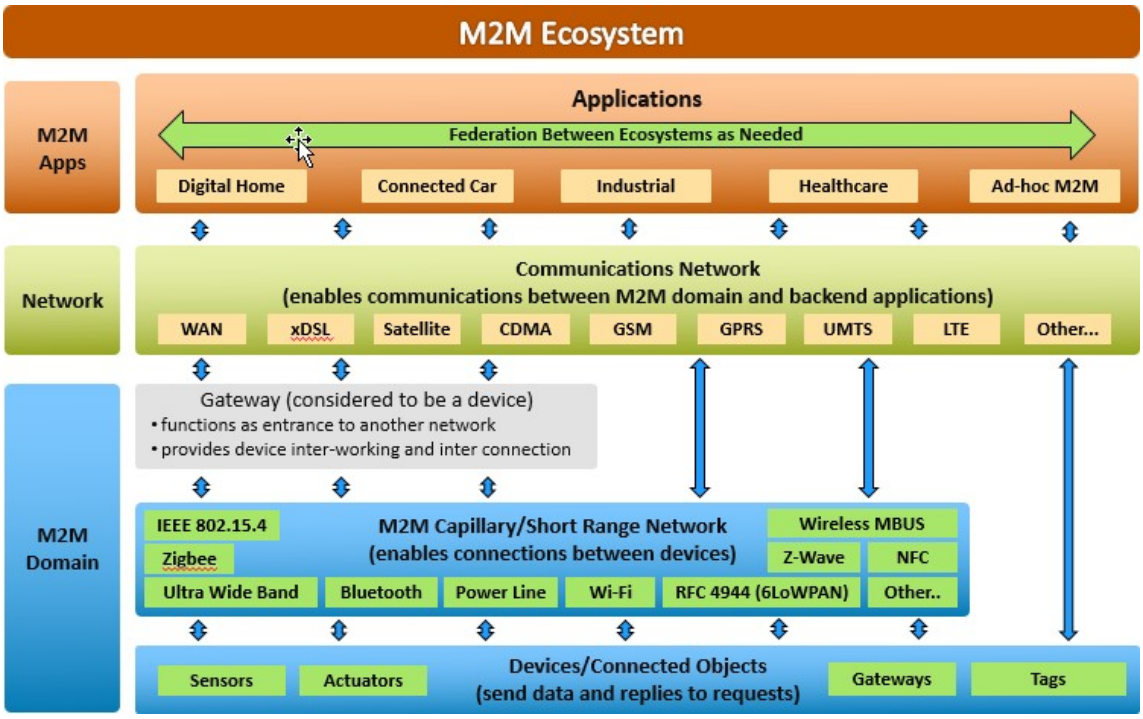
2.0 生态系统的全球性质促进了分布式攻击

互联网生态系统多样且分散，每个部分都在安全中发挥作用。通过将汽车和恒温器等日常物品连接到互联网，支持工业控制系统和监控关键基础设施的设备激增，生态系统将继续增长。控制被感染设备的恶意行为者会带来多种风险。首先，该设备可以用于另一台设备的拒绝服务攻击。其次，可以使用设备上的机器人软件窃取设备信息或跟踪设备。例如，国会议员车内导航软件上的机器人软件可以跟踪车辆的运动。第三，设备上的机器人软件可以用于在设备本身上生成拒绝服务（DoS）事件。第四，机器人可能操纵数据或导致不正确的设备行为，从而危及用户安全或破坏影响数据消费者结果的设备数据。随着物联网设备激增并服务于日益敏感的功能（如自动驾驶和工业控制），失去能力的物联网设备可能会对现实世界造成重大和危险的影响。

2.1 全球互联网和通信生态系统多种多样且不断发展

最终用户，互联网服务提供商（ISP），网络运营商，制造商和软件开发商组成了全球互联网生态系统。各国政府和国际体系也发挥着作用。下一页中的图1说明了支持组成生态系统的机器对机器（M2M）物联网的层。

图1. M2M生态系统



资料来源：AT&T在NSTAC上向总统提交的关于物联网的报告。 2014年11月19日。

尽管一些竞争激烈的互联网服务提供商（ISP）在缓解僵尸网络攻击方面处于最佳地位，但物联网由设备，传输网络，应用程序以及部署它们的公司和用户组成。每个环节都面临威胁，需要关注。

图2.威胁态势

资料来源：布莱恩·雷克斯罗德。 AT&T。 向NSTAC ICR小组委员会简介。 2017年7月20日。

专家预计，随着公司提供综合解决方案，向托管物联网服务过渡。随着物联网设备激增，僵尸网络规模不断扩大。[11]

11凯文·沃尔什。帕洛阿尔托网络公司向NSTAC ICR小组委员会做简报。 2017年7月18日。

2.2 僵尸网络和自动分布式攻击在演变

僵尸网络最初是为积极使用而设计的，后来被重新用于敌对行动。僵尸机器人是指安装在系统上的程序，能够使系统自动（或半自动）执行一项或一组任务，通常在远程管理员（又名僵尸机器人管理员或僵尸机器人牧者）的命令和控制下。
”这些程序可以运行供应商未提供或所有者未授权的代码。大多数机器人均可以支持垃圾邮件，网络钓鱼，点击欺诈和分布式拒绝服务等恶意活动。[12]

僵尸网络是“感染了僵尸恶意软件的互联网连接的最终用户计算设备的网络，由第三方出于恶意目的进行远程控制。”当命令计算机，IoT和其他支持互联网协议（IP）的设备网络运行未经授权的代码支持恶意活动（如垃圾邮件，网络钓鱼，点击欺诈和分布式拒绝服务）时，就会发生僵尸网络攻击。图3描述了僵尸网络攻击的发生方式。[13]

图3.僵尸网络攻击如何发生

资料来源：迈克菲，https://www.mcafee.com/us/resources/misc/infographic-threats-report-mar-2017.pdf

僵尸机器人通常通过受感染的网站或网络钓鱼电子邮件中嵌入的恶意网站的链接传递。用户可能会基于欺骗性电子邮件，网络指令或通过浏览器/操作系统漏洞无意中安装机器人。最终用户无需采取任何措施也可以部署僵尸机器人。例如，在Mirai僵尸网络中，没有任何用户感染了几台设备

12联邦通信委员会（FCC）。 CSRIC。第三部分，美国互联网服务提供商反机器人行为守则（ABC）。 2012年3月。https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-ReportFinal.pdf.

13同上。

互动。可以泄露设备管理或供应商安装后门的默认密码，允许未经授权访问和控制设备。僵尸机器人也通过网络钓鱼，垃圾邮件和其他安全威胁进行分发。僵尸网络活动的一个关键方面是攻击的持久性，即试图利用任何可用的弱点获得访问权限。僵尸机器人可以在机器上更新安全补丁和防病毒软件，以确保稳定运行并排斥其他机器人。人们在讨论僵尸网络时，常常会想到分布式拒绝服务攻击。但是，僵尸网络可以促进数据窃取，非法内容分发，处理窃取，电子邮件垃圾邮件，点击欺诈和其他攻击。[1415]

随着物联网的发展，僵尸网络攻击的规模和复杂度不断提高。一些僵尸网络使用人工智能（AI），量子密码学或神经形态计算技术制造出能够适应互联网速度的更智能病毒。报告的最大攻击为800 Gbps，大约三分之一的攻击峰值超过100 Gbps。在2012-13年金融机构遭受分布式拒绝服务攻击后，互联网服务提供商（ISP）大大增强了分布式拒绝服务保护，但拒绝服务攻击规模有所增加，攻击者改变了策略。例如，攻击者针对具有最大域名系统记录的域名以放大攻击的有效性。[161718]
此外，随着设备变得更加自主，并包括复杂的人工智能，通过物联网对网络违法行为的影响将带来新的严重风险，必须在短期内预计和计划。

缓解可以增强预防。网络攻击将会发生。根据美国国土安全部科学技术局的数据，70%的黑客利用丢失，被盗或虚弱的凭证，60%的恶意软件利用特权提升或被盗的凭证。专家们并没有阻止僵尸网络攻击，而是建立了更具弹性的网络并减轻攻击影响。减轻攻击的最佳实践集中于用户和企业对网络卫生和漏洞管理的教育。这包括强身份验证，关闭不需要的功能和更新服务。其他缓解工具包括网络和数据分析，反向代理，应用程序和网络防火墙以及负载平衡器，以及重新配置/保护互联网路由器。如果辅以数据中心/边缘服务，大规模分布式拒绝服务攻击缓解效果最佳。数据分析，信号，系统措施，异常检测，数据感测和触发器都有助于缓解僵尸网络攻击。审查联合特征和依存关系以识别相似行为并将其分配给参与者，这一点很重要。[192021]

14 Kim Zetter。"骇客词汇：什么是拒绝服务和分布式拒绝服务攻击？"有线。2016年1月6日。https://www.wired.com/2016/01/hacker-lexicon-what-are-dos-and-ddos-attacks/.

15 NTIA。通信部门协调理事会。行业技术白皮书。2017年7月17日。https://www.ntia.doc.gov/files/ntia/publications/cscc_industrywhitepaper_cover_letter.pdf.

16安东尼·斯克里菲尼亚诺。Dun&Bradstreet，Inc.向NSTAC ICR小组委员会简介。2017年8月15日。

17 Arrabelle Hallawell。Arbor Networks，Inc.向NSTAC ICR小组委员会简介。2017年8月3日。

18比尔·奥赫恩。AT&T，Inc.向NSTAC ICR小组委员会做简报。2017年7月20日。

19安东尼·斯克里菲尼亚诺。Dun&Bradstreet，Inc.向NSTAC ICR小组委员会简介。2017年8月15日。

20安·考克斯。国土安全部。向NSTAC ICR小组委员会简介。2017年8月1日。

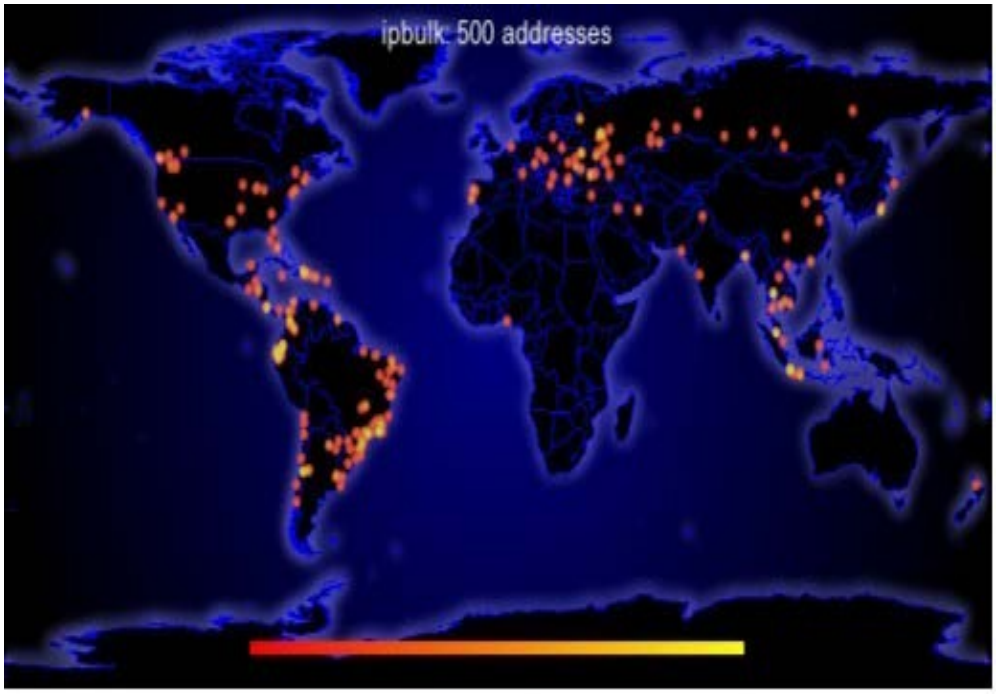
21安东尼·斯克里菲尼亚诺。Dun&Bradstreet，Inc.向NSTAC ICR小组委员会简介。2017年8月15日。

2.3 僵尸网络和自动分布式攻击全球通用，响应复杂

受感染的设备，目标，不良行为和受害者遍布全球。不良行为者包括民族国家，有组织犯罪集团，黑客主义者和个人。法治影响不大，违法者掩盖其足迹的能力会使归属复杂化。恶意行为者通常是出于经济利益或造成服务中断的能力所驱动。目标存在于医疗保健行业，学术界和公共部门。美国的受害者更有可能支付赎金。[22][23]

僵尸网络超过80%的流量来自海外，大多数流量看起来都是合法的。中国的僵尸网络数量最多，接近140万。印度以不到一百万美元排名第二，俄罗斯以不到六十万排名第三。在2017年第一季度，中国和韩国"继续在攻击国中名列前茅……大部分攻击（50.8%）起源于中国，其次是韩国（10.8%）"，美国占7.2%。"攻击中使用的大多数开放式域名解析器都在美国以外。[24][25][26]

图4.域名解析器的位置



资料来源：比尔·奥赫恩。 AT&T。向NSTAC互联网和通信弹性（ICR）小组委员会简介。 2017年7月20日

22同上。

23 Raj Samani。英国迈克菲。向NSTAC ICR小组委员会简介。 2017年8月15日。

24 Spamhaus项目。世界上最糟糕的僵尸网络国家。 2017年8月18日。https://www.spamhaus.org/statistics/botnet-cc/.

25封装。全球分布式拒绝服务威胁格局。 2017。https://www.incapsula.com/ddos-report/ddos-report-q1-2017.html.

26比尔·奥赫恩。 AT&T，Inc.向NSTAC ICR小组委员会做简报。 2017年7月20日。

2016年10月，Mirai僵尸网络针对域名系统提供商Dyn发起了分布式拒绝服务。这次攻击破坏了一些全球最大的网站。Mirai利用许多物联网设备的弱安全性，不断扫描可通过互联网访问的，仅受出厂默认设置保护且包含硬编码用户名和密码的物联网设备。Mirai用恶意软件感染设备，迫使设备向中央控制服务器报告，将其转变为可用于分布式拒绝服务攻击的机器人。相对较少的制造商及其下游供应商以开发脆弱的物联网设备而闻名。[27]

行业内部和执法部门合作关闭僵尸网络主机，但跨政治边界开展协作时面临挑战。美国政府拥有权威和工具，可能允许政府对僵尸网络采取平权行动（包括攻击性和防御性），但使用此类工具会引发政策问题。关于"主动防御"和进攻性网络运营，存在复杂的问题，包括应进行哪些操作，如何提高效果的可预测性（作为限制的关键原因之一是缺乏可预测性/影响的精确性）以及谁应该参与其中。这些问题需要美国政府，外国合作伙伴和行业共同讨论和制定计划。"主动防御"是指不同背景下的不同事物，需要进一步讨论。

3.0 生态系统的每一部分都必须寻址安全

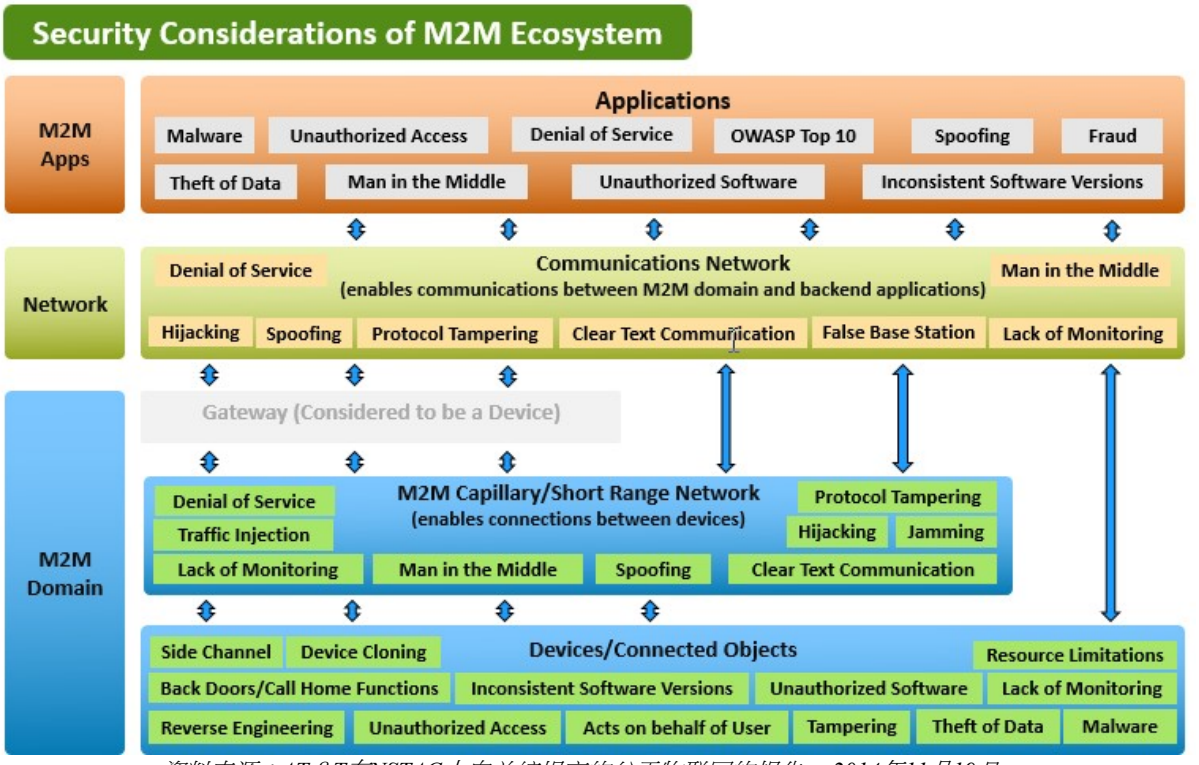
就本报告而言，NSTAC将生态系统划分为以下几层：

- 网络（3.1）
- 消费者/边缘设备（3.2）
- 企业（3.3）
- 应用程序/软件/操作系统（3.4）
- 政府（3.5）
- 国际（3.6）

网络安全要求在生态系统的每个部分都采取积极行动。

27赛门铁克。Mirai：您需要了解的近期僵尸网络分布式拒绝服务攻击背后的僵尸网络。2016年10月27日。https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-

图5. M2M生态系统的安全考虑



资料来源：AT&T在NSTAC上向总统提交的关于物联网的报告。 2014年11月19日。

<u>与生态系统每一层相关的核心发现</u>

几个步骤可以帮助保护互联网生态系统免受分布式和自动攻击。不同的行为者必须（单独或集体）做出贡献以创造更好的安全性。本报告重点关注关键角色及其在加强互联网安全中的作用。

网络层。网络服务提供商已采用各种通用实践来缓解分布式攻击。这些实践包括网络服务提供商的分布式拒绝服务通用实践；互联网服务提供商的反僵尸网络行为守则（ABC），互联网工程技术论坛（IETF）BCP和联邦通信委员会（FCC）通信安全，可靠性和互操作性委员会（CSRIC）方法。通讯部门在FCC的CSRIC上针对许多问题制定了实践，包括分布式拒绝服务最佳实践，僵尸网络缓解和实施NIST改善关键基础设施网络安全框架。许多提供商已经实施了这些做法，但是，其他国内外的ISP以及运营网络的ISP[28]

28 CSRIC及其前身组织网络可靠性和互操作性委员会（NRIC）首次讨论了2002-2004年NRIC VI中的网络安全最佳实践。见https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-4.

还必须采用这些功能以减少分布式攻击的影响。
CSRIC报告中的建议包括：阻止发往和来自某些互联网端口的流量；增强网络智能和流量流量可见性；在发生大规模攻击时传输中的跨ISP流量过滤；以及将机器学习应用于检测网络流量。僵尸网络。[29][30]

网络服务提供商还可以帮助保护连接到其网络的IoT设备；例如无线运营商可以与生态系统中的各种其他参与者合作，提供服务，帮助管理与长期演进或第五代（5G）网络连接的IoT设备安全。例如，AT&T，IBM，诺基亚，帕洛阿尔托网络，赛门铁克和Trustonic最近组建了物联网网络安全联盟，旨在推动成员公司之间的协作，开发出解决物联网网络安全挑战的多层解决方案。网络提供商当前正在网络层开发能力，利用大数据分析和机器学习来检测和缓解基于物联网的攻击，并且可能会继续引入新功能和服务，帮助更好地管理物联网设备。

设备/边缘层。随着设备武器化及其在分布式拒绝服务攻击中的潜在使用仍然是一个主要问题，设备安全必须提高。在开展许多私人活动的同时，政府应召集利益相关方，推动采用标准和最佳实践。私营部门应领导标准的制定，政府可以召集专家演示如何通过用例应用此类标准。随着最佳实践的出现，生态系统可能会考虑采用自愿性，行业驱动的设备认证，其中还包括制造商对产品生命周期的支持。
NSTAC以前建议"应考虑建立一个承销商实验室来认证特定证券政策。"
NSTAC支持这样的结论：基于国际标准的某种形式的行业驱动的IoT设备认证会有所帮助。[31]

在一定程度上，这种努力已经在进行。
UL正在制定设备认证计划，网络安全独立测试实验室（CITL）等其他组织也在测试设备。消费者报告已开始与包括CITL在内的实体合作，考虑设备审核的安全性，这可能会提高消费者的意识。此外，政府已启动流程，例如NTIA在IoT设备升级性方面的工作以及NIST的网络物理系统的工作。政府和行业可以通过要求设备满足专有设置中的部署标准来推动采用。一个框架[32]

29虽然针对互联网服务提供商（ISP）广泛讨论了BCP 38/84等通用实践，但任何运营自己的IP地址空间的人（包括企业业务和提供某些网络功能的其他实体）都必须部署反欺骗技术。

30参见NCTA –互联网与电视协会通信部门协调委员会Matt Mattey,

关于僵尸网络和自动威胁的行业技术白皮书。

31 NSTAC。 NSTAC就物联网向总统报告。2014年11月9日。附录E，C-5。https://www.dhs.gov/sites/default/files/publications/2012-05-15-NSTAC-Cloud-Computing.pdf, 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.

32网络独立测试实验室（CITL）。http://cyber-itl.org/.

通过公私合作开发的设备部署应建议风险管理流程，并根据功能和上下文确认需求有所不同。政府应以NIST成功的"改善关键基础设施网络安全框架"为模型。不断推出新服务以帮助管理和保护IoT设备。互联网服务提供商，无线服务提供商，路由器制造商，安全解决方案提供商等正在开发服务，以管理物联网设备安全。如前所述，无线运营商还与各种实体合作，将解决方案推向市场，帮助管理物联网安全。
McAfee和Symantec等反病毒和安全公司也提供安全家庭服务。思科正在IETF推广标准，例如制造商使用说明（MUD）标准，允许设备在家庭中进行自我识别，并使路由器和网络能够针对设备应用安全策略。这些仍然是新兴功能，可以作为设备安全标准的补充。[3] [3] [34]

企业。企业必须在购置，使用和寿命终止期间规划和管理连接的设备。这些组织拥有许多用户，这些用户可能会遭受简单的攻击，但也可以从安全教育中受益匪浅。企业还应该采用最佳实践，确保网络，数据（例如防止勒索软件的备份），云服务产品和域名系统的冗余和弹性。企业通过采用和要求供应商的安全措施，在管理环境中发挥关键作用，这种方法可以推动整个互联网生态系统更好的IoT安全标准。

应用程序/软件/操作系统（请参阅第3.4节）。生态系统要求更多地使用安全软件开发和管理实践。正如NIST解释的那样，"在成熟度不同的层次上，有很多方法可以减少软件漏洞的数量。"但是，安全软件开发和管理实践的使用并不平衡，特别是在资源较少，专业知识较少的小型或非传统技术供应商中。行业和政府必须推广最佳实践，在初创企业中为开发人员提供支持，并强调软件工程师和安全专家之间的有效沟通。[35]

3.1 网络

结果

网络在防御僵尸网络和分布式拒绝服务攻击中扮演着不可或缺的角色。网络提供商会采取各种措施，但可以做更多工作来应对僵尸网络和分布式拒绝服务攻击。
一项重大挑战是鼓励采用现有的最佳实践。
NSTAC确定了行业采用的以下技术和面临的挑战，并提出了解决这些问题的建议。

33国家标准技术研究所。改善关键基础设施网络安全的框架。2014年2月12日。https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

34例如，请参阅迈克菲的安全家用平台https://securehomeplatform.mcafee.com

35 NIST ITL出版物。2017年1月。http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=922589.

当前活动

网络运营商每天使用不断发展的工具和大量资源为客户和其他终端用户提供安全连接，从而缓解数以千计的威胁，僵尸网络和分布式拒绝服务攻击。例如，提供商实施反欺骗，阻止攻击媒介以及检测和缓解针对或影响网络服务的攻击的标准。服务提供商可以帮助识别源IP地址，过滤/阻止与黑名单签名匹配的电子邮件，以及过滤/阻止发往网络钓鱼站点的流量。互联网服务提供商（ISP）采用的一些网络安全技术包括：

- **最佳通用实践（BCP）38。主要运营商至少在其部分网络中实施了**BCP38。 BCP38是一种IETF惯例，其目的是防止IP地址欺骗，并防止最终用户使用欺骗源地址发起流量。实施BCP38可以增加僵尸网络流量被阻止（因为其源于伪造源地址）的可追溯性，或者可追溯，因此一旦被发现，运营商就可以应对安全隐患。大多数大型IS P都集成了BCP38，越来越多的小型ISP也开始采用BCP38。
- **端口阻止/过滤/速率限制。**许多运营商实施端口阻塞，过滤和速率限制。这些技术广泛用于企业和政府客户的托管安全服务。 服务提供商还会在其骨干网上阻塞已知会造成安全风险的某些端口。虽然如今已经进行了一些端口阻止，但与公用互联网相比，阻止或缓慢部署企业网络流量的风险计算方法有所不同。互联网服务提供商（**ISPs**）担心与互联网范围封锁相关的误报，而且更为激进的封锁或过滤模型可能无法扩展。 **NSTAC**认识到，也许有机会加强这些努力，但需要与政府建立伙伴关系，制定政策框架，支持**ISP**采取更积极的行动来阻止和过滤内容。考虑到可能存在误报和不确定的监管环境，互联网服务提供商对于这些问题一定要保持保守，尤其是考虑到**FCC**的网络中立性法规。此外，许多指挥和控制站点利用合法的通信手段，可能会造成附带损害。互联网服务提供商（**ISP**）已经阻止了广泛用于安全事件的端口。例如，**AT&T**试图通过阻止某些传输恶意或破坏性流量的端口（如端口**25**、**135**、**139**、**445**和**1900**）来隔离威胁，并将对网络的危害降至最低。其他提供商则采取类似步骤。对于某些名义使用或使用受限或通常消耗少量带宽的协议（例如**CharGen**或**NTP**），提供商还可以对流量限制速率，这可以正常使用此类协议，但有助于减轻其在分布式拒绝服务攻击中的使用。任何超出上述示例（显然已被网络攻击利用）扩展这些活动的措施，都需要与政府合作，确保建立支持这些活动的政策框架。[36]

36参见AT&T。网络实践。；2017年4月24日。 Xfinity。https://www.att.com/gen/public-affairs?pid=20879

*Comcast阻止端口列表。 2017。*https://www.xfinity.com/support/internet/list-of-blocked-ports/.

*CenturyLink*http://www.centurylink.com/aboutus/legal/internet-service-disclosure/full-version.html

- **NIST网络安全框架。**工业界鼓励使用NIST改善关键基础设施网络安全的框架，并在NIST确定的每个核心职能领域实施该框架：

  - *识别：*识别关键资产，信息共享。

  - *检测：*数据包采样，签名分析，启发式/行为分析。

  - *保护：*访问控制列表，警务，黑/漏孔，分布式拒绝服务"清理器"，边界网关协议（BGP）流规格，内容交付网络，任播，最终用户反病毒软件，客户托管安全服务。

  - *响应和恢复：*减少攻击流量，与上游供应商合作过滤并通知客户。ISP阻止正在进行攻击的端口（例如，端口445）。

- **互联网服务提供商的基础知识。**业界鼓励采用CSRICIII，工作组7制定的《美国互联网服务提供商反机器人行为守则》。ABC是一套自愿实践，"通过自愿参与，解决了住宅宽带网络中的僵尸网络和僵尸网络威胁。"它强调了十项关键原则：自愿参与；技术中立；接近中立；尊重隐私；遵守法律；分担责任；可持续性；信息共享；有效性；并与消费者进行有效沟通。要遵守ABC，需要对最终用户进行培训，僵尸网络检测，最终用户可能的僵尸网络感染通知，僵尸网络补救和ISP合作。实施的潜在障碍包括：技术限制（当前解决方案可能不足以消除僵尸网络威胁和/或带来意想不到的后果）；消费者和市场壁垒（客户可能认为解决方案无效或不受欢迎，如消费者成本增加）；运营壁垒（影响组织的主要任务和资源）；财务障碍（难以量化与具体建议相关的成本/收益）；以及法律，法规或政策壁垒（阻碍协作和信息共享的法律或政策）。

- **流量管理。**互联网服务提供商和网络运营商在流量管理功能上投入了大量资金。一些示例包括端口阻止，机器学习和帮助检测机器人的人工智能，目的地黑洞过滤和恶意IP地址沉陷。

- **消费者通知。**互联网服务提供商（ISP）投入大量时间和资源来实施消费者感染通知，这是ABC原则的关键组成部分。根据自愿，机密地向消息传递，恶意软件和移动反滥用工作组（M3AAWG）提供的汇总数据，2012年报告的ISP通知被僵尸感染客户的比例介于98.41%至99.13%之间，被僵尸感染客户的比例介于94%至99.82%之间消费者教育在2013年成为客户。但是，如下所述，消费者教育的应用受到限制，并且这些努力对减少恶意软件和僵尸网络扩散的影响尚不确定。

- **行业协作。该行业致力于协作和共享最佳实践。**例如，由索协作解决方案

例如分布式拒绝服务开放威胁信令。参与者进行协作以识别对其服务器的攻击，并在针对其他网络的攻击发生之前共享信息以制定威胁响应。分布式拒绝服务缓解平台之间遥测的实时交换有助于分布式拒绝服务缓解和网络到网络状态更新。 FCC CSRIC V信息共享工作组最近的报告详细概述了通信行业内的信息共享。其他工作正在进行中，包括在大型运营商之间进行试点，以在主要对等点大规模分布式拒绝服务攻击期间合作并中断流量。

- **信息共享。** FCC CSRIC V工作组5最新报告概述了该行业从事信息共享。行业与可信赖的同行和商业伙伴共享信息；合同政府机构；执法；行业同行，作为行业政策和计划流程的一部分；以及D HS国家协调中心和国家网络安全与通信集成中（NCCIC）等政府机构。国土安全部还与国务院合作管理国际观察和警告网络，在国际上共享信息。[37][38]

- **软件定义的网络/网络切片/虚拟化。** 5G等架构发展，向全IP网络的过渡以及软件定义网络（SDN）和虚拟化技术的出现将促进安全性。SDN是一种新兴的架构，将网络控制和转发功能分离，使网络控制可以直接编程。该架构结合开放的，易于编程的接口，可以更轻松地混合和匹配来自不同供应商的解决方案并开发新功能。尽管任何新方法都有可能遭到破坏，但SDN可以帮助运营商应对网络威胁，这是基于运营商对网络的集中查看。网络切片将允许5G网络运营商按服务提供网络。借助网络切片，可以将单个物理层划分为多个虚拟网络，使运营商可以为不同的客户支持不同的服务。服务包括过滤，路由，协议限制和速率限制。运营商可以自定义网络切片的安全性以动态响应。网络虚拟化包括内置安全性，如隔离和多租户，分段，分发防火墙以及服务插入和链接。[39]

- **托管安全服务/消费者安全。**许多ISP向企业客户消费者提供托管安全服务（如分布式拒绝服务防御服务），帮助他们管理安全风险。在消费者方面，互联网服务提供商（ ISP）提供有关潜在感染的通知，与住宅宽带服务一起提供的免费反病毒服务，帮助补救的技术支持等功能。在企业一级，互联网服务提供商（ISP）为私有和公共部门提供安全，网络监控和管理服务。

37 FCC CSRIC V，第5工作组最终报告，信息共享，2017年3月15日。https://www.fcc.gov/files/csric5-wg5-finalreport031517pdf.

38同上，第6页。

39比尔·奥赫恩。 AT&T，Inc.向NSTAC ICR小组委员会做简报。 2017年7月20日。

挑战

这些现有解决方案面临若干挑战：

- **网络管理法律框架。**许多用于公共互联网或消费者空间的技术都涉及解决方案，如阻止，黑洞或沉没IP地址，阻止恶意流量利用端口，通知终端用户潜在感染，以及部署IP地址反欺骗常见做法（如BCP 38） /84。这些方法面临的挑战是可能出现误报和意外后果。要有效补救这些问题，互联网服务提供商（ISP）必须采取更积极的措施监控和检查流量，这引起了政策关注。例如，虽然FCC先前的网络中立性规则中存在安全例外，但人们普遍认为，互联网服务提供商不会干扰流量，会增加与某些活动相关的风险。

- **加密。随着更多流量的加密，**互联网服务提供商（ISP）失去了知名度。如今，大多数互联网流量都是经过加密的。对于僵尸网络运营商而言，加密僵尸网络流量非常简单。一位专家预测，到2016年底，超过三分之二的互联网流量将被加密。虽然ISP可能对网络流数据（如源和目的地IP地址）有所了解，但ISP不太可能具有广泛的有效负载可见性，而主动阻止可能需要这些负载。[40]

- **互联网协议版本6（IPv6）。**运行支持IPv6的网络的运营商需要安全性，检测和监控工具。由于IPv6引入的独特安全挑战，生态系统必须使对IPv6的安全支持成熟，改进资产发现和检测工具以识别恶意IPv6设备，并确保网络监控同时支持IP版本4和IPv6网络资产。

- **可扩展性。**关于解决方案是否能够大规模使用仍存在疑问。在企业中，互联网服务提供商（ISP）监控与其企业客户对应的IP地址范围，识别，检测和阻止网络攻击。目前尚不清楚，随着大型网络在一天之内承载大量流量，整体互联网的更精细解决方案是否会扩展。[41]

- **小型/中型航空母舰。**大型组织和小型组织及其实施BCP38或其他安全措施的能力必须区分开。小公司可能需要通用服务资金才能有效保护安全。出售低利润互联网服务且缺乏用于安全投资的收入模型的公司面临重大挑战。NSTAC建议，政府应重新考虑部署激励措施的问题，特别是对于中小型运营商而言，即使是边际投资也可能需要此类实体的激励措施。

- **消费者通知。** ISP都有通知程序，但这些程序的整体效果尚不清楚。即使消费者许多收到通知

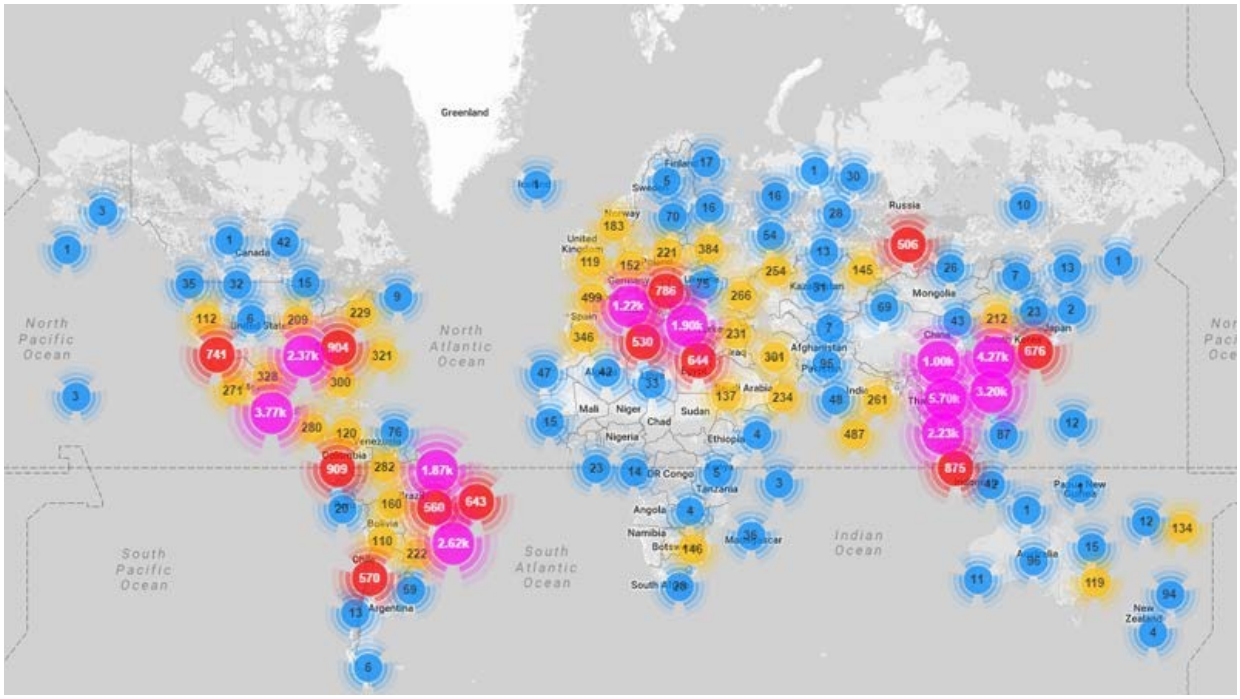
40 Sandvine。全球互联网现象：加密互联网流量。2016。https://www.sandvine.com/resources/global-internet-phenomena/spotlight/internet-traffic-encryption.html.

41比尔·奥赫恩。 AT&T，Inc.向NSTAC ICR小组委员会做简报。2017年7月20日。例如，每天有超过168 PB的数据流经AT&T网络。

安全问题，许多人缺乏清洁系统的技能。再感染率也很高，因为消费者通常会首先重复破坏设备的行为。

- **国际。**僵尸网络对美国的攻击很大程度上来自海外。例如，下图显示了日Mirai僵尸网络攻击的流量来源，主要来自美国境外。 2016年8月17

图6. Mirai僵尸网络攻击的流量来源2016年8月17日



资料来源：布莱恩·雷克斯罗德。 AT&T。向NSTAC ICR小组委员会简介。 2017年7月20日。

其他问题

NSTAC解决了其他与ISP安全相关的问题，包括域名系统安全扩展（DNSSEC）和安全域间路由的部署。DNSSEC可能不是一个可行的解决方案，因为它最初很有用，但随着网络的发展，DNSS EC不能得到最佳实施，从而降低了有效性。互联网服务提供商（ISP）会遇到放大攻击，并注意到一些安全框架依赖关键基础设施和验证。网络准入控制和访问保护有助于在访问网络之前强制进行验证。主要问题是信任和声誉，因为网络上的每个数据包都带有一定程度的风险。NSTAC还审查了信令系统7（SS7）问题。尽管SS7获得了相当大的关注，但SS7本身并不是问题。相反，互连和不当访问是问题所在。（参见CSRIC V，WG10（2017年3月）和2017年5月3日关于SS7 / 2FA的报告）。工业界继续与参与犯罪行为的流氓运营商作战，[42]

42特拉维斯·罗素。甲骨文。向NSTAC ICR小组委员会简介。 2017年8月11日。

向不良行为者出售网络标识符和身份验证。工业界正在努力加强互连（或漫游）合作伙伴的审查，并改善网络卫生状况。

另一个问题是保护BGP路由。这包括对实体在互联网上发布虚假路由的担忧，这些虚假路由可用于路由流量，使实体能够监控流量或进行监控。迄今为止，该问题的解决方案一直集中在资源公钥基础设施（RPKI）的开发上，这将使ISP和其他实体能够验证路由。NIST国家网络安全卓越中心（NCCoE）最近启动了安全域间路由路由试验，以探索围绕RPKI开发的若干问题，许多ISP正在参与其中。

网络服务提供商的建议

- **共享可操作的威胁信息。ISP协作应包括网络内共享检测，通知和计划或利用的缓解方法。**
- **增加流量分析。许多ISP会执行分析，但应将其合并到更强大的托管安全服务中，以帮助企业管理潜在的分布式拒绝服务攻击。**
- **适应并应用机器学习进行异常检测。**
- **确保网络运营商可以过滤恶意流量。**
- **鼓励开发使分布式拒绝服务流量缓解尽可能靠近源的实践，以避免其传输网络。**
- **扩大 ISP之外的B C P38/84的使用，使企业包括在内。**
- **在适当的情况下，继续实施端口阻止，速率限制和过滤。**
- **继续参与业界为 B G P安全性所做的 努力。提高**

3.2 消费者/边缘/设备

结果

网络边缘的弱点，连接网络的设备以及购买和使用设备的用户的安全隐患。
NSTAC在研究中同时考虑了消费者和边缘设备。

消费者起着至关重要的作用。人为错误可能会破坏行业对技术和软件解决方案的投资。许多攻击仍然有效地部署网络钓鱼等低技术手段，不良行为者利用不良的网络卫生状况发起僵尸网络攻击。
70%的黑客利用丢失，被盗或虚弱的凭证；所有恶意软件中有60%使用特权升级或

凭证被盗。 FCC CSRIC建议强调了对最终用户进行保护措施教育的重要性，例如强密码，防病毒软件，防火墙和接受更新。政府拥有足够的资源来教育消费者，但是，消息可能会因提示页面的数量过多，联邦调查局（FBI）咨询和其他现有通信而丢失。[43][44]

用户在做出购买决定时可能会忽略安全性，可能无法正确安装或配置设备。最终用户不得更改密码或使用可用的安全工具，并且可以忽略可用的更新。此外，更换用户时，用户不得擦除设备中的个人数据或设置。用户可能没有足够的信息，但也可能会忽略可用信息。皮尤研究中心的一项调查发现，其中28% 美国智能手机用户无法使用简单的四位数个人识别码或其他安全功能来保护对其设备的访问。尽管大多数智能手机用户报告更新了设备应用程序或操作系统，但大约40%的用户表示将更新推迟到方便为止。研究发现，有14%的智能手机用户从未更新过智能手机操作系统，有10%从未更新过应用程序。不良的卫生状况并非商业用户独有，政府用户还必须改善网络卫生状况。代理商可能受到资源限制，政府需要考虑其未来安全需求的成本。 EO 13800适当地强调了对机构负责人的问责制和责任。[45][46][47][48]

设备至关重要。许多设备开发时都缺乏安全功能，因为一些供应商对安全问题没有给予足够的重视。Mirai僵尸网络攻击利用密码和凭据薄弱的超过一百万个摄像头。设备可能具有不可更改的默认密码，这使得它们很容易被利用，或者可能无法支持更新，这使得在出现安全漏洞时更难进行补丁管理。联邦贸易委员会（FTC）指出，设备安全性会有所不同，但在合理特征方面已经出现了一些共识。预期为280亿[49][50]

43安·考克斯。国土安全部。向NSTAC ICR小组委员会简介。 2017年8月2日。

44 FCC。 CSRIC II，第2A工作组：最终报告。网络安全最佳实践。于2011年3月91日。https://transition.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf.

45肯尼斯·奥尔姆斯特德和亚伦·史密斯。 “美国人与网络安全。”皮尤研究中心报告。 19岁。 2017年1月26日。http://assets.pewresearch.org/wpcontent/uploads/sites/14/2017/01/26102016/Americans-and-Cyber-Security-final.pdf.

46同上。在20。

47同上。

48新闻秘书白宫办公室。 13800号行政命令，加强联邦网络和关键基础设施的网络安全。 2017年5月16日。https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure.

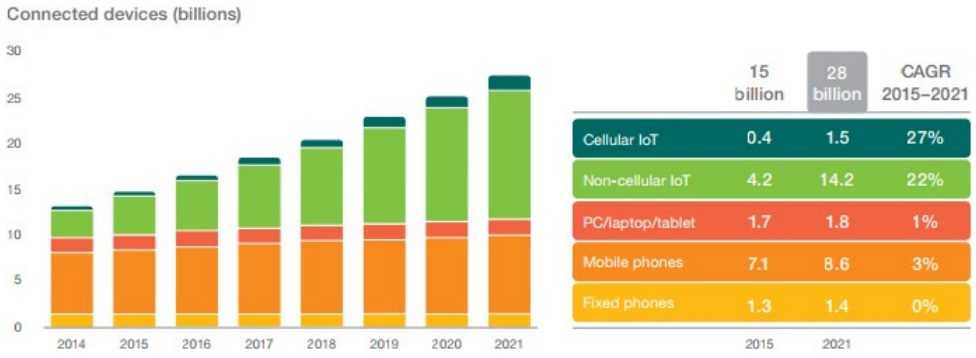
49洛伦佐·弗朗西斯·比奇埃拉伊，如何劫持150万台联网摄像机，打造前所未有的僵尸网络。 2016年9月29日。https://motherboard.vice.com/en_us/article/8q8dab/15-million-connected-cameras-ddos-botnet-brian-krebs.

50托马斯·帕尔。 FTC。从安全开始，并坚持不懈。 2017年7月28日。 （“在数据安全方面，合理的选择取决于业务规模和性质以及处理的数据类型。”）；互联网https://www.ftc.gov/news-events/blogs/business-blog/2017/07/start-security-stick-it

物联网世界中的隐私和安全。 FTC。 n.130。 2015年1月。 （“可能还有其他适当措施，因为https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

到2021年，全球互联网连接量将达到73%，移动，网络或个人无法为所有这些设备提供安全保护。[51]

图7.联网设备的增长



资料来源：《爱立信交通报告》（2016年6月）[52]

物联网设备的武器化提出了重大挑战。僵尸网络破坏了安全性差且始终开启的设备，可能会造成灾难性后果。物联网提供商及其最终用户有时对脆弱设备可能造成的伤害不感冒，可能没有动力来确保设备运行所需的安全投入。

物联网应支持更新以及身份验证和验证系统。新型恶意协议可以击败过时的安全模型，因此需要升级较旧的安全性。网络服务提供商可能能够帮助管理网络中的非安全设备，但存在复杂因素。例如，全球约有70%的互联网流量经过加密，并且这一数字预计还会增长。更复杂的是，许多消费类设备无法公开寻址，无法在不受ISP管理的家用路由器和网络地址转换系统后面运行。用户通常有多个路由器。一些公司，包括互联网服务提供商和安全解决方案提供商，正在试验安全管理服务，但市场潜力尚不确定。[53][54]

安全性不仅限于设备层。我们不能完全依靠将安全内置到设备中来解决安全问题。例如，网络提供商可以对穿越其网络的流量进行分析，并应用机器学习来帮助识别和缓解威胁。

公司应实施的方法各不相同，具体取决于未授权访问设备带来的风险以及所收集信息的敏感性。"）

51爱立信移动报告。论网络社会的脉搏。2016年6月。思科。思科视觉网络指数：预测和方法论，2016-2021年。白皮书。2017年6月7日。https://www.ericsson.com/res/docs/2016/ericsson-mobility-report-2016.pdf; https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html.

52爱立信移动报告。论网络社会的脉搏。2016年6月。https://www.ericsson.com/res/docs/2016/ericsson-mobility-report-2016.pdf.

53 Raj Samani。英国迈克菲。向NSTAC ICR小组委员会简介。2017年8月15日。

54参见桑德维恩。全球互联网现象：加密互联网流量。2016。https://www.sandvine.com/resources/global-internet-phenomena/spotlight/internet-traffic-encryption.html.

一些物联网设备。还有一些提议，如IETF引入的思科MUD标准。 MUD允许设备自我识别，并由路由器和其他网络设备使用速率限制和白名单管理安全性， 将其放置到不同的服务类别中。此外，McAfee等公司也开始提供家用设备安全管理服务。这些努力尚处于起步阶段，但可以随着市场发展提高安全性。

供应链也很重要。运营商正在改善防御，但不能独自做到。芯片制造商和平台供应商必须加大力度，生态系统必须促进对家庭网络的新兴"螺栓式"安全升级。行业和政府必须专注于安全营销，承认共同责任并鼓励团队合作。

NSTAC承认，对于政府在物联网安全中的作用，存在不同的看法。但是，很明显，必须重点缓解这些漏洞。

当前活动

正在开发大量创新解决终端用户和设备层。芯片制造商和平台供应商正在为复杂的I oT设备构建更高的安全性。正如消费者技术协会（CTA）解释的那样：[55]

- **英特尔安全计算合作研究所开发了TrustLite安全框架，以增强小型IoT设备的安全性。**[56]
- Altera现场可编程门阵列或片上系统使用硬件 A E S安全的远程软加密加速和件升级。
- ADI公司的物联网产品使用加密硬件加速，安全启动和在线存储器读取保护。
- 苹果，高通，三星电子 A R M S的T rustZ on e芯片。等使用
- IBM，微软，英特尔，恩智浦，松下和三星的物联网平台为实施者提供了内置的安全或安全指导。

消费者网络监控设备（NMD）和智能路由器正变得越来越普遍。消费者NMD包含的规范包括虚拟专用网络（VPN）模式，拒绝服务攻击防护，未授权访问阻止以及病毒和恶意软件扫描。智能路由器现在具有类似的功能。业界正在设计能够为消费者的家庭网络提供"螺栓式"安全升级的硬件。

工业为客户提供了多种工具来保护设备。其中包括向消费者提供防病毒工具，帮助检测病毒和清理机器；来自一个威胁分析

55 Mike Bergman。消费者技术协会。向NSTAC ICR小组委员会简介。 2017年8月3日。

56 Koeberl，帕特里克等。 " TrustLite：微型嵌入式设备的安全架构。"http://www.icri-sc.org/fileadmin/user_upload/Group_TRUST/PubsPDF/trustlite.pdf

网络角度；通知最终用户并提供自我修复工具和有偿护理选项；并为订阅客户提供分布式拒绝服务缓解服务。

有一些自愿性指南和最佳实践可以缓解设备漏洞并提高消费者意识，行业也在这些努力的基础上发展。

- 例如，GroupeSpécial移动协会（GSMA）已制定了开发安全IoT产品和服务的指南，包括面向IoT终端设备制造商的指南。[57]

- CTA正在开发稳健的最佳实践，以增强室内连接设备的安全性。[58]

工业界正在与政府合作，在最终用户阶段为物联网安全提供资源。例如，行业成员正在与NTIA进行多方利益相关者协作，开发用于物联网升级的通用词典。在此过程中，工作组已从30多个美国和国际组织中确定了有关该主题的指南，确保空中更新的功能以及向消费者传达IoT升级性的指南。[59]

对消费者/边缘/设备的建议

- **建立和推广共识设备安全准则。应使用基本的网络卫生习惯强化设备，包括接收升级**和补丁程序的能力。政府为提高网络安全卫生状况做出了几项努力，但还需要更多努力。政府和行业应确定是否需要制定最低安全标准。设备制造商，尤其是物联网设备开发套件制造商，需要确保其中包括好的工具，并使用安全的默认配置，自动修补和从恶意软件感染中恢复的功能。[6061]

- **促进家庭管理服务。**政府应支持行业对家庭管理服务的投资，以监督家庭中联网设备的运行。此功能可以在路由器中提供，也可以在家庭内部作为独立设备提供。

- **促进消费者意识/教育。**行业应继续教育用户，包括完成更新的重要性。政府应扩大和

57请参阅《GSMA IoT安全指南》。https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/.

58消费者技术协会。项目概述：为家庭消费者保护互联设备。

CTA-CEB33。2017年7月7日。https://standards.cta.tech/apps/group_public/project/details.php?project_id=429.

59参见NTIA。现有物联网安全标准目录（草案版本0.01），有关物联网安全升级和修补的NTIA多利益相关方流程，现有标准，工具和举措工作组。

2017年7月。https://www.ntia.doc.gov/files/ntia/publications/iotsecuritystandardscatalog.pdf.

60阿拉贝拉·哈拉韦尔。Arbor Networks，Inc.向NSTAC ICR小组委员会简介。2017年8月3日。

61参见NIST草案。特别出版物800-193。平台固件弹性指南。2017年5月。https://csrc.nist.gov/csrc/media/publications/sp/800-193/draft/documents/sp800-193-draft.pdf

协调其消息传递。现有一些广告系列，例如STOP.THINK.CONNECT，可用于此目的。

- **支持增强的信息共享。**政府应鼓励设备制造商之间共享信息，包括安全港和责任保护。

3.3 企业

结果

企业用户和系统起着至关重要的作用。企业-僵尸网络以两种方式对企业（包括拥有成千上万个设备的公司，依赖于连接性的政府机构，部署工业传感器并携带自己的设备（BYOD）的小型企业）造成影响。首先，企业是僵尸网络攻击的目标。其次，企业集中存在大量物联网设备，如果易受攻击，可以将其用作全球僵尸网络的一部分。多年来，对手一直使用启用僵尸网络的分布式拒绝服务攻击破坏企业运营。由于民族国家针对美国基础设施，黑客主义者试图发表声明，犯罪分子分心于更阴险的攻击或其他企图破坏竞争的企业，企业可能成为分布式拒绝服务攻击的目标。随着企业的信息技术，物理基础设施和业务连续性越来越依赖基于IP的设备，企业变得更容易长期或永久禁用其运营；有人称之为"服务破坏"。即使企业本身并不是僵尸网络的目标，但脆弱的设备仍可以充当网关渗透网络，窃取高价值数据，甚至从内部破坏IT和运营基础设施。由于几乎每个企业网络上连接设备的激增，企业自己的物联网设备可用于对企业自身发起拒绝服务攻击。

设备数量庞大，组织更难以跟踪设备，增加了被盗风险，并使设备容易受到攻击。各种规模的企业必须管理其网络（包括VPN）上的更多交互点，以促进异地访问。连接数量的增加使企业面临更多威胁，包括安全性可能不高的设备发出的威胁。供应，监控，更新和寿命终止管理的需求可能比现有公司的IT部门可以应对的挑战更大。
僵尸网络对企业的威胁不仅仅是对设备的攻击。一项重大挑战是防止遭受企业用于开展业务的共享资源的攻击。当企业服务跨越其内部IT网络，云产品和共享资源时，必须防止针对其中一项服务的业务影响事件发生。例如，许多企业的互联网服务在2016年10月Mirai攻击Dyn的活动中断时，其互联网服务中断。

企业在缓解僵尸网络威胁方面可以发挥重要作用。内部网络中的企业物联网部署应通过应用与已识别风险相称的适当安全技术，更易于管理。为降低企业风险，必须在IoT价值链中始终交付这些安全功能，以实现企业必需的可视性和自动化，以防止网络威胁针对连接的元素，并保护网络和控制器环境免受设备发起的攻击。

这些功能必须本地集成，并在各个功能之间实现高度自动化，以快速识别高级攻击并确保可以在所有环境中近实时实施预防性安全控制。在物联网部署的背景下，在整个企业物联网价值链中防范网络威胁至少需要：（1）端点安全；
（2）局域网的安全性；（3）相关服务提供商网络内部的安全性；
（4）云环境和物联网主机控制器的安全性。

例如，海军陆战队采用积极的企业管理方法。海军陆战队会跟踪尝试连接到网络的每台设备，并确保在连接之前对设备进行充分修补并遵守安全协议。海军陆战队对个人设备保持严格的政策。在允许BYOD的情况下，将设备放置在虚拟容器中以保护设备和政府网络上的数据。海军陆战队还确保用户具有执行职责，使用两要素认证以及审核用户每次文件创建，修改和删除的最低特权。[62]
尽管这种方法比大多数企业更具攻击性，但它可以显示一些步骤，可以作为保护企业免受僵尸网络和其他威胁攻击的一部分。[63]

NSTAC的发现之一是，IoT设备具有广泛的特性和功能。在企业环境中，一些具有先进处理能力的高价值物联网资产（如汽车）可能会承受一定程度的网络安全风险，使部署专用端点安全解决方案可行。但是，许多其他企业物联网设备缺乏单独的计算能力，而是依靠控制器主机的命令和控制功能实施安全实施。此外，很大一部分企业物联网平台和控制器依赖于内部数据中心，公共云或服务提供商内部环境中托管的云连接。所有这些平台和控制器（无论位于何处）的一致性，高度集成的安全性对于防止损害和执行未经授权的命令和控制活动（对于大批企业物联网设备进行自动化和分布式攻击）至关重要。

SDN和网络功能虚拟化（NFV）等有望帮助企业的有前途的创新以及其他方法将优化系统的架构和组织方式，并允许采取创造性的安全措施。
SDN将为企业安全提供多项优势：

- 集中控制：提供改进的安全优势；
- 管理：通过全面的网络可见性改善安全管理；
- 应用程序：SDN 应用程序提供本机安全控制功 能；
- 数据收集：本地收集和分析可增强响应能力；和

62雷·莱特尔。美国海军陆战队向NSTAC ICR小组委员会简介。2017年8月29日。

63同上。

- 效率：SDN支持更直接的重新路由和基础设施更改（动态实施）。[64]

NFV也很有希望。欧洲电信标准协会解释说，5G NFV将支持网络切片，即在同一网络上创建多个逻辑网络实例（即片），可利用该逻辑实例以自动化，灵活的方式部署和管理网络片。云原生设计原则通过基础设施上更细粒度的复用最大程度地提高了企业资源的有效利用。[65]
端到端服务管理（即为不同的客户提供不同的服务）允许客户选择最能满足其需求的基本网络服务组件。具有高度分布式系统的边缘计算允许网络功能在最接近最终用户设备的服务器上运行，即在网络架构的"边缘"上运行。预计无线接入网络的云化将为运营商提供前所未有的灵活性，敏捷性，资源/服务管理和编排能力。多站点/域服务，包括不同管理域中基础设施即服务，NFV即服务和网络服务组合的支持，对于向5G过渡至关重要。NFV许可证管理，将底层许可证管理机制标准化，可以避免增加许可证的复杂性。这些创新可提升企业安全性中的安全性，可靠性和可扩展性。

企业应为应对这些风险制定一些明确的目标，包括：

减轻传统僵尸网络攻击企业网络的风险。企业必须探索所有可用方法，以减轻针对其网络的传统僵尸网络攻击的风险。其中包括与互联网服务提供商合作，在拒绝服务攻击之前实施网络级防御，例如端口阻止，流量路由，反欺骗和其他归因方法。许多企业希望网络提供商将控制或功能作为托管安全服务的一部分提供，可以限制设备与授权控制器外部域的任何通信，并启用高级安全解决方案，如由大量动态威胁情报支持的基于应用程序的防火墙。

确保设备在购买时和产品生命周期内均具有内置安全保护。企业可以采取几个步骤来确保连接的设备在网络上安全运行。这些步骤包括购买时考虑设备安全；向潜在的供应商询问有关供应商如何保护设备的各种问题，包括如何对设备进行身份验证以及如何修补或更新设备；并可能由独立组织对设备进行测试。许多企业拥有强大的购买力，可以在设备开发生命周期的设计和生产阶段提高整体安全性。

部署后，企业必须理解并采用所有可用方法，防止设备被征召（或用于攻击自己的网络）。在保护设备网络安全时，企业最重要的考虑因素包括：检测（

64比尔·奥赫恩。 AT&T，Inc.向NSTAC ICR小组委员会做简报。 2017年7月20日。

65 ETSI NFV行业专业小组。网络运营商关于5G NFV优先级的观点。 2017年2月21日。 https://portal.etsi.org/NFV/NFV_White_Paper_5G.pdf

实时检测所有连接设备），分段（从网络其他部分分段或"隔离"端点）能力和自动化（选定解决方案以自动化方式运行的能力），对于实现规模规模至关重要随着连接设备数量呈指数增长，提供了多种选择，包括允许企业对设备进行可靠身份验证的工具；支持设备行为分析的工具（检测可能表明危害的异常设备行为的能力）；以及以及扫描技术，使企业能够更积极地寻找漏洞和恶意软件，从而不干扰设备运行。企业应适应新兴的方法和工具，帮助他们保护网络设备安全，包括安全信息和事件管理以及允许实时分析和共享上下文信息的编排平台信息。

对企业的建议

激励和启用企业安全非常困难，部分原因是企业环境和需求的多样性。
NSTAC已确定应采取的几个步骤：

- **将上述针对消费类设备的适用建议视为改善企业环境（尤其是自带设备）安全状况的工具。**

- **提高对最佳实践的认识。国土安全部和其他机构应与以行业组织为代表的行业垂直合作（对于被视为"关键基础设施"的企业，则应通过行业协调理事会），以确保了解最佳实践，以减轻僵尸网络攻击的影响并确保连接设备的安全。在可能的情况下，国土安全部和行业应提供针对特定行业的实践指南。此外，国土安全部应以NCCoE正在开展的工作为基础。**

- **考虑鼓励采用标准的激励措施。联邦机构和国会应考虑利用联邦资金鼓励在联邦资助项目以及实施项目的企业中采纳本报告的建议。这些激励措施仅适用于对联邦政府指导或监督的设备（如医疗设备）的固定保护要求尚未到位的情况。**

- **部署托管安全服务。各种规模和类型的企业应考虑部署托管安全服务。每个组织都需要评估其安全状况，并仔细考虑是否部署某种托管安全方法。此外，监控功能应针对所有类型的连接设备。僵尸网络推动攻击时，分布式拒绝服务防护等服务非常有用，因为越来越多的公司要求对安全性负责。**

- **解决企业安全问题。企业应该利用网络隔离，微分段和过滤技术来保护和限制对互联网的访问。其他有助于企业安全的选项包括：**

    - *领域意识：企业应该跟踪和阻止来自威胁主机域的流量。企业还应该采取措施保护自己的域名。攻击者*

通常会针对具有最大域名系统（DNS）条目的域名，以放大攻击效果。

- *在适当的地方部署补偿控件。并非每个组织都能部署规定的协议。正如N IST解释的那样，在工业环境中，“[工业控制系统或ICS]可能无法支持安全控制或控制增强，或者组织认为不建议通过ICS实施这些措施。在这种情况下，组织可以提供理由，说明补偿控制如何为ICS提供同等的安全功能或保护级别，以及为什么不能采用相关的基准安全控制。”此类控件的示例包括网络感知的实时检测，身份验证和授权，漏洞管理，行为分析，分段和缓解。补偿控制不能解决全球僵尸网络问题，但是保护企业的重要一步。*[6667]

- *利用云。成熟的云服务提供商已经增强了安全状况，可以为企业提供重要的安全优势。企业（无论是私人企业还是政府企业）都应探索云提供商及其提供的安全性。*

- *使用动态配置。这是网络虚拟化和分段的重要组成部分，使公司能够加快并更好地控制设备和用户在系统中的授权使用方式。动态供应自动执行IT流程并执行安全要求，并能够对安全问题做出更快的响应。*

- *冗余。所有企业都应考虑域名系统和所有关键业务互联网服务的冗余。*

- **考虑一下保险市场。保险市场可能会推动保险业改善，因为承保人会就公司安全风险管理实践的成熟度向公司进行调查，并向成熟度较高的公司提供较低的保费。**

3.4 应用程序/软件/操作系统

结果

应用程序和操作系统中的软件在成功解决僵尸网络中扮演着至关重要的角色，随着软件集成到更多系统和设备中，僵尸网络正日益加剧。
此外，随着软件激增，许多非传统技术公司已成为提供商。虽然安全软件有了重大改进和共享

66 NIST ITL公告。定制工业控制系统的安全控制。2015年11月。http://csrc.nist.gov/publications/nistbul/itlbul2015_11.pdf. 67华莱士·桑。前景色。向NSTAC ICR小组委员会简介。2017年8月22日。

开发和管理流程，非传统软件提供商，初创企业及其他人员可能不知道或没有资源来实施这些流程。此外，在物联网环境下，软件漏洞风险可能会增加；联网汽车可能会坠毁，而智能烤面包机可能会引起火灾。[68]

僵尸网络挑战与应用程序/软件/操作系统的相关性

应用程序，软件和操作系统至关重要，因为它们对于端点安全以及由端点利用的服务或资源的安全至关重要。多个开发人员提供嵌入设备，应用程序和服务中的软件；这种多样性是创新不可或缺的，但也带来了安全挑战。利益相关者在软件开发和软件管理中处于不同的成熟水平。尽管软件开发从一开始就是限制软件漏洞数量和严重性的关键，但管理对于确保能够解决发现的漏洞至关重要。

如果没有任何漏洞，开发软件是不切实际或不可能的。虽然对小型，高度关键生命系统的正式验证方法正在取得进展，但大规模使用此类方法或复杂的网络物理系统仍然是中长期挑战。相反，实施安全软件开发和管理最佳实践，指南和工具可以提高基准安全性。[69]

但是，尽管有供应商实践，指南和工具，但供应商和客户的认知度和实施水平仍然相差甚远。首先，并非所有软件都由大型供应商开发或管理，安全开发实践不一定能在小型开发环境中轻松或一致地应用。其次，开源代码不断增长。它通常由志愿者维护，他们可能没有安全开发的要求或流程，清晰的责任制或对安全问题做出响应的资金。第三，用户可能会中断实施，许多企业难以在消费者和企业环境中对产品，服务或设备实施安全补丁或缓解措施。

解决威胁的努力正在进行中

15年前，软件供应商开始致力于提高代码安全性（即软件开发）。这一实践领域通常称为软件保证，鼓励开发人员构建更安全的软件并满足安全合规性要求。许多大型供应商已经开发了用于代码开发，实施和优化的程序，培训和工具。例如，使用安全开发生命周期（SDL）可确保在设计，开发和部署软件时，应牢记整个生命周期的安全性。厂商通过非营利组织（如软件保障论坛）进行合作[70]

68查理·米切尔。内部网络安全。黑帽创始人将软件责任视为主要的网络安全政策挑战。 2017年7月26日。https://insidecybersecurity.com/daily-news/black-hat-founder-sees-software-liability-major-cybersecurity-policy-challenge.

69凯文·哈特奈特。有线。计算机科学家研究完美的，防黑客攻击的代码。 2016年9月23日。https://www.wired.com/2016/09/computer-scientists-close-perfect-hack-proof-code/.

70微软。什么是安全开发生命周期？https://www.microsoft.com/en-us/sdl/default.aspx.

代码卓越奖（SAFECode）颁布软件保证实践。供应商为开发国际标准化组织（ISO）/国际电工委员会（IEC）27034做出了贡献，这是一种基于过程的国际标准，用于指定，设计/选择和实施信息安全控制。[71]

软件供应商一直在通过开发，实施和促进协调的漏洞披露（CVD）策略，流程和程序来改善软件管理。漏洞披露和处理涉及与第三方发现者进行沟通；验证和分类漏洞；开发缓解漏洞的更新（例如"补丁"）；并对运行中的系统应用更新或缓解措施。与改善代码保证的工具一样，技术提供商也在漏洞披露和处理的最佳实践方面进行了投资。有两个ISO标准，ISO / IEC 29147和ISO / IEC 30111，描述了从第三方发现者接收漏洞信息，与发现者就报告的问题进行交流以及调查，分类和解决漏洞的流程。

一些技术提供商已投资促进心血管疾病，美国政府也加大了在这一领域的投入。许多软件供应商参与了NTIA的漏洞披露和处理多方利益相关者流程，以增加对现有最佳实践的采用，提高对涉及多方的复杂披露挑战的响应，并帮助安全关键行业更好地理解如何采用CVD。在NTIA的努力基础上，美国食品药品监督管理局发布了鼓励医疗器械制造商采用化学气相沉积方法的指南，参考了ISO / IEC 29147和ISO / IEC30111。美国国家公路运输安全管理局发布了鼓励汽车制造商制定方法和政策的指南用于接收来自安全研究人员的漏洞报告。此外，国防部和总务管理局还创建了化学气相沉积程序和/或漏洞赏金计划，从而与研究人员进行协调。最近，司法部发布了一个框架，协助组织制定自愿协调的网络漏洞披露计划。[72][73][74][75][76]国会也在考虑这个问题。尽管并不适合每个组织，但CVD可以帮助解决软件管理难题。

71安全代码。https://safecode.org/about-safecode/.

72我是骑兵。DOT政府协调披露时间表。https://www.iamthecavalry.org/wp-content/uploads/2016/12/IATC_Gov-Coordinated-Disclosure-Timeline_v1.0.jpg.

73 NTIA。多利益相关方流程：网络安全漏洞。2016。https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities.

74卫生与公共服务部。"医疗设备网络安全的上市后管理-工业和食品药品监督管理局工作人员指南。"2016年12月28日。https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

75国家公路交通安全管理局（NHTSA）。"现代车辆网络安全最佳实践。"2016年10月。https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf.

76国防部。"国防部宣布了数字漏洞披露政策，并宣布"陆军开战"。新闻稿。GSA。2016年11月21日。漏洞披露政策。https://www.defense.gov/News/News-Releases/News-Release-View/Article/1009956/dod-announces-digital-vulnerability-disclosure-policy-and-hack-the-army-kick-off/;https://hackerone.com/deptofdefense; https://18f.gsa.gov/vulnerability-disclosure-policy/.

对软件开发人员的建议

改善软件保证，管理和响应举报或其他方式发现的漏洞的努力明显改善了网络安全，但同时制定激励措施和不利措施的组合可能会有所帮助。为此，NSTAC建议考虑以下因素：首先，针对软件保证和漏洞管理的政策（无论采用何种实施机制）必须利用国际标准，包括IEC / ISO 27034，ISO / IEC 29147和ISO / IEC30111。它们必须专注于开发和修复流程软件（而不是漏洞的存在）（即，如何构建软件来减少漏洞数量以及如何修补或缓解漏洞）。其次，政府和企业都没有有效利用市场力量来驱动更安全的软件的开发，因为目前尚不清楚标准的市场力量应达到什么水平。NSTAC建议美国政府提高对软件保障和技术购买对运营风险的作用的认识。政府还应强调现有最佳实践和标准，使信息和通信技术（ICT）买家与供应商就技术产品和服务开发以及安全管理惯例进行对话。

NSTAC特别建议以下内容：

- **政府和教育机构应努力将安全性纳入课程。“科学，技术，工程和数学”倡议的计算机科学**
- **软件开发社区应提供有关DevSecO ps流程的指南。**
- **业界应考虑合理和审慎的协调一致的漏洞披露计划。如果组织无法内部管理，则可以包括组织管理的CVD程序或外包程序。**
- **工业界应为开发人员提供安全编码工具。改进代码开发工具，增强可追溯性和安全性。**
- **共享解决漏洞的最佳实践。**
  NTIA已审查了此问题，行业可以支持源自多利益相关方流程的建议以及其他指南。[77][78]

77 NTIA。多利益相关方流程：网络安全漏洞。2016。https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities.

78司法部。“在线系统漏洞披露程序框架。”2017年7月。https://www.justice.gov/criminal-ccips/page/file/983996/download.

- **对于那些公开解决漏洞的政府，政府应考虑采取责任保护措施。国家如何应对这些挑战可能需要转变范式。**

- **政府和行业应在促进软件保证的活动中开展合作-验证软件以限制安全漏洞。这可能需要推广最佳实践或指南，为软件开发人员树立榜样。**

- **仔细考虑如何保护开源开发。工业界通过核心基础设施倡议为全球信息基础设施的关键要素提供资金的集体努力将有助于解决某些问题，但是，NSTAC认为需要做出更多努力。**

- **政府和行业应提高技术用户对及时修补重要性的理解。可以通过将这些组件合并到现有安全意识计划中来完成。**

3.5 政府

结果

政府在互联网和通信弹性方面发挥着关键作用。它是连接设备的购买者和管理者；是制定政策的监管者或召集人；它拥有主权来起诉罪犯，捍卫国家并与其他国家进行谈判。每个角色都是不同的，面临不同的挑战，提供不同的机会。

作为管理者和采购者，政府与其他企业用户一样面临着许多相同的僵尸网络挑战。政府内部已连接设备的用户数量众多，使得设备管理困难。政府还有责任保护敏感的政府信息和公民数据，使政府成为高价值目标。此外，美国政府实体管理多个易受攻击的IP块。它在监管和采购政策环境中面临进一步挑战，这限制了灵活性，必须提前做出采购决定，并受到监督和外部约束。[79]

政府拥有独特的机会来增强安全性。作为管理人员，政府可以采取措施改善移动使用管理惯例-
利用任何数量的现有设备管理服务，增强对采用基本网络卫生惯例重要性的认识。作为技术采购商，政府可以要求使用更安全的设备。政府标准通常会导致私营部门采用这些标准，避免发展不同且可能相互竞争的做法。参议员马克·沃纳参议员提出了一项法案，即《
2017年物联网（IoT）网络安全改进法案》，该法案提议通过制定最低限度要求的IoT设备提高IoT安全

79安·考克斯。国土安全部。向NSTAC ICR小组委员会简介。 2017年8月1日。

由联邦政府采购。但是，如果未认真采取措施，则诸如《物联网网络安全法》之类的立法可能会产生意想不到的后果。目前的草案一旦颁布，可能会因繁重的认证要求而使政府承包商承担责任，鼓励"黑客"政府设备，并限制承包商适当管理漏洞披露的能力。可以通过灵活的，以市场为导向的解决方案来最好地确保网络安全，这些解决方案体现了私营部门的领导力和创新能力，是通过行业和政府之间合作开发的。[8081]

作为监管者或召集人，政府可以制定政策和标准，同时促进创新。在美国，网络政策强调政府是召集人。政府应继续将利益相关者聚集在一起，与来自不同行业，跨通信和ICT生态系统的利益相关者共同制定最佳实践。政府必须弥合复杂和不复杂行业之间的知识鸿沟。在国际上，政府可以促进大规模合作，鼓励其他国家共享信息并采用适当的最佳实践来减轻僵尸网络。这些努力可以显着减少此类攻击的次数和规模，因为许多攻击是从海外发起的。

政府在确保网络安全和攻击缓解研究资金中发挥着重要作用，其收益不可低估。除了直接支出外，政府还应继续寻找机会与公众互动，增强安全。今年，FTC举办了一场大奖赛，旨在创建解决方案，"防止在家中使用IoT设备的软件出现安全漏洞。"获胜者（来自新罕布什尔州的软件开发人员）开发了一款移动应用程序，可以帮助用户确定设备是否过时或网络不安全。[8283]

政府在公共安全方面也发挥着独特作用，应与NIST等机构合作，提高公共安全系统的安全性。
FTC对制造商采用的安全措施严重不足采取的强制措施使业界意识到需要实施基本安全保护，并向消费者如实地表示其设备的安全性。[84]

作为主权国家，政府具有保护公民，执行法律和保护国家免受僵尸网络等外部威胁的独特权力和职责。通过这些权力，

80马克·华纳。"参议员提出两党立法，以改善"物联网"设备的网络安全。"新闻稿。2017年8月1日。https://www.warner.senate.gov/public/index.cfm/pressreleases?ID=06A5E941-FBC3-4A63-B9B4-523E18DADB36.

81 Mike Bergman。消费者技术协会。向NSTAC ICR小组委员会简介。2017年8月3日。

82 FTC。物联网家庭检查员挑战赛。2017。https://www.ftc.gov/iot-home-inspector-challenge.

83 FTC。"FTC宣布其物联网家用设备安全竞赛冠军。"新闻稿。2017年7月26日。https://www.ftc.gov/news-events/press-releases/2017/07/ftc-announces-winner-its-internet-things-home-device-security.

84 FTC。"FTC批准了针对TRENDnet的最终订单结算费用。Inc."新闻稿。2014年2月7日。https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc; https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put.

政府可以阻止或阻止某些恶意活动。有效的工具包括域名注册阻止，IP阻止，刑事调查和僵尸网络删除。

私人和公共部门之间的执法合作非常有效，美国应该寻找机会扩大这些努力。执法部门，计算机应急响应小组等通常依靠私营部门从电信提供商，反病毒供应商和金融部门获取威胁情报和数据。情报对于识别具有动机，意图和支持进行网络攻击的个人至关重要，这些伙伴关系可帮助全球政府和互联网服务提供商识别和补救威胁。
NSTAC建议政府加强与私营部门的合作，特别是在调查方面。这种公私合作伙伴关系在英国蓬勃发展，美国安全公司和其他组织愿意与政府合作，支持悬而未决的调查和未来的调查。[85]

司法部在与联邦调查局，其他执法机构和私人实体的协调下，成功实现了僵尸网络删除。首次成功拆除是在2011年4月，当时政府停止了"
Coreflood"攻击，影响了超过37.8万台设备。自那时以来，还取得了其他胜利，包括最近在外国政府的合作下，两个在线黑市AlphaBay和Hansa倒闭。[8687]

僵尸网络主要删除案例[88]

- 2011年：域名系统更改[89]
- 2011年：Coreflood（378,000台）
- 2013年：Citadel（200万台）
- 2014年：GameOver Zeus（50万至100万台）
- 2016年：Avalance（500,000台）
- 2017：Kelihos /W aldec（100,000台）

通过减少限制行业参与的监管壁垒，政府甚至可以更有效地应对最复杂的僵尸网络攻击。

政府可以消除限制行业参与的障碍，从而增强僵尸网络的攻击力。僵尸网络下架需要时间，金钱和资源，而且很少有公司有动机采取必要的法律行动来进行僵尸网络下架。对于行业而言，僵尸网络的删除通常包括承担基础设施控制权，重定向[90]

85拉吉·萨马尼（Raj Samani）。英国迈克菲。向NSTAC ICR小组委员会简介。2017年8月15日。

86美国司法部。"司法部采取行动禁用国际僵尸网络。"2011年4月13日。https://www.justice.gov/opa/pr/department-justice-takes-action-disable-international-botnet.

87美国司法部。"关机，最大的在线"暗市场" AlphaBay。"
2017年7月20日。https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down.

88伦纳德·贝利。美国司法部。向NSTAC ICR小组委员会简介。2017年8月10日。

89http://www.dcwg.org/dns-changer/

90同上。

通信和减轻危害。此类活动通常需要最终用户授权或手令，临时限制令或民事禁令。当恶意攻击源于ISP自身网络之外时，这是具有挑战性的。因此，政府和行业支持将最有能力领导僵尸网络删除活动。[91]

另一个可能阻碍缩编的问题是对检察官的成功评估。在实体世界犯罪活动的背景下，政府的目标和激励机制反映出对识别和起诉被告的重视。对于虚拟世界而言，此类传统目标和激励机制可能尚未完全优化，这使网络罪犯拥有更大的匿名性，因此大大挫败了识别和起诉其为被告的努力。但是，在虚拟世界中，检察官还有其他方法可以破坏和阻止犯罪活动，包括启用恶意软件的僵尸网络攻击。在继续寻找和起诉仍然至关重要的刑事被告的同时，也可能会鼓励检察官更广泛地侧重于预防犯罪和国家安全。
检察官可以帮助防止僵尸网络扩散和负面影响。即使没有潜在被告人，他们也可以破坏和拆除僵尸网络操作。

破坏和拆除僵尸网络可能会产生重大的积极影响。例如，为切断被感染的计算机和Citadel基础设施之间的关系而建立的公私合营努力停止了90%的僵尸网络活动。Citadel是有记载的最大僵尸网络之一。同样，政府对Coreflood的收购也利用恶意软件吸取了毫无戒心的用户的个人和财务信息，允许受害者从其计算机上删除恶意软件，防止进一步的隐私损失和用户财务安全损失。在9天之内，被感染计算机发送到服务器的信标数量大幅减少。[92][93]

但是，许多僵尸网络并未受到政府的干扰，或者干扰延迟，因为根据其激励机制，许多检察官最专注于识别和起诉刑事被告。根据现行指南，仅当联邦检察官认为某人的行为构成联邦犯罪，并且可以接受的证据足以获得和维持定罪时，才可提起诉讼。这种以起诉为重点的做法限制了政府对僵尸网络的破坏和拆除，因为在很大程度上，即使在犯罪活动持续进行的情况下，也没有一个容易确定的起诉人。[94]

在其他情况下，政府有效地加大了对预防的关注；司法部有效地将更多的资源和精力用于反恐领域的预防。从这些成功经验中吸取的教训可能适用，因为政府正在考虑如何以不完全依赖于网络犯罪的方式发展网络犯罪相关的激励结构

91见《计算机欺诈和滥用法》（CFAA）（《美国法典》第18卷第1030节）；窃听法（美国法典第18卷第2511条）；笔登记/诱捕和追踪法规（《美国法典》第18卷第3121节及以下）。

92 Zach Lerner，微软僵尸网络猎人：公私合作伙伴关系在缓解僵尸网络中的作用，28 HARV。 J.L.＆TECH。 237，247（2014）。

93政府支持临时禁令的补充备忘录，第10页。 4，图1在美国

v.John Doe，No.3：11-cv-561（VLB）（D.Conn。提起2011年4月11日）。

94美国检察官办公室（USAO）的年度预算和绩效指标与定罪数量直接相关。

起诉和定罪，而是鼓励在破坏和拆除僵尸网络之间进行跨联邦机构和私营部门的协调。例如，联邦调查局虽然担负着调查网络犯罪的重要职能，但其行动权力并非没有限制。联邦调查局必须合作，协调并寻求联邦检察官批准使用某些调查工具，除非有可能被定罪，限制政府预防网络犯罪和防范国家安全风险的能力，否则通常会予以拒绝。重新调整资源和激励结构的重点，还可以使政府更定期有效地利用私营部门并与私营部门合作预防网络犯罪，更好地保护僵尸网络受害者并增加罪犯使用僵尸网络的成本。增加刑事诉讼费用具有积极的连锁反应；减少有能力参与网络犯罪的罪犯数量，还可以减少生态系统中的"噪音"，使公共和私营部门实体都能更有效地识别更隐蔽的高级持续威胁。

NSTAC建议采取以下行动来加强拆除行动：

- **司法部的政策应更支持政府干预。司法部可能需要更多资源来加大力度，这也取决于与私营部门和潜在国际伙伴的合作。**

- **僵尸网络对国家安全的影响证明，司法部将重点放在预防和破坏僵尸网络攻击上，而不是提出起诉。**

- **联邦一级的网络犯罪预算应反映预防的重要性，不应与起诉和定罪挂钩。**[95]

政府还必须确保现行法律不限制行业信息共享或适当的"主动防御"活动。诸如《计算机欺诈和滥用法》，《窃听法》以及《笔记录/捕获和追踪法》等法规可能无意阻止互联网服务提供商采取某些"主动防御措施"，如实施入口/出口过滤（BCP 38和84），阻止报告由于法律责任方面的考虑，导致流量过大，并抵制了攻击提供商网络的系统。针对错误的法律保护有限，而且公司可能会因错误而受到批评。政府应寻找方法将责任风险限制在真诚采用主动防御措施的供应商中。[96]
2015年《网络安全信息共享法案》（CISA）授权出于网络安全目的监控信息系统信息，并为此类活动和其他防御措施提供责任保护。
CISA等法规允许行业保护其网络并支持政府拆除行动。如果期望私营部门提供更多保护，则应考虑采取其他保护措施。改善网络安全将需要行业与政府之间互惠互利的伙伴关系。[97]

95理查德·博斯科维奇。微软。向NSTAC ICR小组委员会简介。 2017年8月16日。

96《计算机欺诈和滥用法案》（CFAA）（《美国法典》第18卷第1030节）；窃听法（美国法典第18卷第2511条）；笔登记/诱捕和追踪法规（《美国法典》第18卷第3121节及以下）；伦纳德·贝利。美国司法部。向NSTAC ICR小组委员会简介。 2017年8月10日。

97 2015年《网络安全信息共享法》，发布。 L. No. 114-113，129 Stat。 2242（2015）。

推荐建议

正如总统在第13800号总统令中所反映的那样，正在努力加强对机构的问责制。政府必须以这些为榜样，在这些努力的基础上继续前进。此外，政府必须积极利用其执法工具，消除私人诉讼的障碍。[98]

- **通过合理利用采购能力树立榜样。政府应投资于提高联邦网络的安全性。当前的工作，如扎根于NIST的最佳实践，例如为民用机构推出连续诊断和缓解，以及为国防部遵照连接，允许机构检测，清点和补救所有物联网和运营技术设备，以及联邦网络上基于Windows的端点。在这一领域的领导地位可以为私营企业树立榜样。**
- **采用《联邦信息安全管理法》和《信息技术管理》的N IST标准和指南。NIST与私营部门合作，正在不断改善网络安全最佳实践。这包括努力改善框架，升级密码功能（尤其是量子抗密码技术）以及探索人工智能和物联网安全功能。NIST还致力于改善互联网体系结构，包括域和BGP安全性。政府应率先实施这些标准。**

- **增加执法部门僵尸网络清除率。政府应利用最近在僵尸网络删除方面取得的成功来证明预防的有效性。除其他事项外，政府应考虑：**

  - 确保激励机制反映预防的重要性，而不是与起诉和定罪有显着联系；
  - 简化僵尸网络删除活动的执法流程，包括使用权威的量刑指南；
  - **支持公私合作下架；和**
  - 允许分析师在更长时间内专注于一个目标，从而实现其网络智能收集方法的现代化，从而成为一名专家，更有能力对抗特定攻击。在考虑加强僵尸网络攻击的方法时，政府必须透明行动。

- **避免重复。政府应巩固和协调为更有效地增强国家网络安全所做的努力。例如，DHS和FCC等多家机构为提高供应链安全性进行了多次重叠的努力。物联网安全方面也有重叠的工作，包括DHS，NIST和NTIA，以及监督各个物联网垂直领域的多个机构（如车辆，智慧城市等）。这些重要问题将从协调方法中受益。**

98新闻秘书白宫办公室。 13800号行政命令，加强联邦网络和关键基础设施的网络安全。2017年5月16日。https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure.

- 保持召集和促进作用。政府拥有召集行业的独特能力，可以将现有框架应用于物联网等新领域，并为不断发展的技术制定最佳实践。应鼓励多方利益相关方流程，例如NIST和NTIA中的流程，并推广其实践建议。尽管政府不应该发布命令，但可以通过鼓励措施鼓励实体采用这些标准。同时，政府需要审查这些流程中产生的标准，以识别和填补可能影响物联网的所有空白。

- 加强对采用防御措施的互联网服务提供商的保护。现有法规经常不鼓励业界采用主动防御措施。因此，政府应寻找方法限制对试图保护其系统免受僵尸网络攻击的提供商的法律责任。

- 资助网络安全和标准制定研究。研发资金势在必行。政府应在财政上支持这些工作，包括研究基线路径测量，路由器级拓扑，设施级拓扑，性能和安全卫生最佳实践。随着威胁的发展和加密效率的降低，必须研究新技术，尤其是量子技术。

- 推广自愿共识标准和准则。公私伙伴关系和自愿准则比任务授权更为有效，而在这种不断发展的环境中，这已很快过时。任何法规都应侧重于缓解风险和限制责任，这些责任可能来自行业共享信息和采用防御措施的努力。[99]

3.6 国际

结果

在没有特别关注国际行为者的情况下，对分布式攻击的讨论是不完整的，国际行为者是以上每个生态系统层的一部分。国际影响者和挑战包括：

- 国际技术公司。设备制造商和服务提供商遍布全球，在全球范围内销售产品。其中包括各种设备制造商（如智能手机，家电，汽车，工业传感器和医疗设备），以及全球互联网和移动服务提供商（移动虚拟网络运营商，网络所有者，ISP，专用网络运营商，批发商和代理商））。

- 全球供应链。物联网设备和全球通信网络的软件，芯片组和其他组件来自世界各地。

99拉杰·萨马尼（Raj Samani）。英国迈克菲。向NSTAC ICR小组委员会简介。2017年8月15日。

- **互联网管理实体。从域名到流量路由，各种实体参与全球互联网基础设施的核心管理和功能。互联网名称与数字地址分配机构（Internet Corporation for Assigned Names and Numbers）及其他众多机构参与治理问题以及日常活动。**

- **个别政府和地区性障碍。每个政府与美国拥有相同的权益和角色：用户/购买者，监管机构和主权国家。不同的国家对技术法规和政策采用不同的方法。各地区也开展了合作，欧洲和亚洲国家就包括物联网在内的技术和互联网政策共同开展工作。国家和区域努力融入全球系统和机构。**

- **全球标准机构和行业合作社。数十个标准机构（包括电气电子工程师学会，电信行业解决方案联盟和ISO）共同制定国际技术标准和协议。他们的工作依赖于共识来促进通信网络真正的创新，包括互操作性。他们依靠国际社会的专门知识和参与。行业小组也一起工作；例如，GSMA，电信行业协会等。一些区域性组织，如美国互联网号码注册管理机构，对于更广泛的全球通信网络至关重要。**

僵尸网络是全球性威胁。僵尸网络超过80%的流量来自海外。应对僵尸网络挑战需要国际合作以制定标准，所有国家/地区都必须努力保护其网络和设备的安全。[100]

英国政府的努力就是一个例子

各国采取不同的方法，但最有希望的努力包括私营部门与政府之间建立真正的伙伴关系，而不必担心承担责任或受到指责。例如，英国正在进行的前瞻性工作，包括提高公众意识运动，内部政府实践和私营-公共伙伴关系，已经建立了更安全的网络。[101]

- **公众意识运动。英国政府发起了各种公众意识运动，旨在向公众宣传更安全的做法。它与大型设备制造商合作推出两因素身份验证帐户，从而减轻了与密码被盗有关的安全隐患。政府还使用其网站提醒用户升级软件。例如，使用过时软件提交纳税申报表的税收申报人会被警告更新其软件，如果在下一个申报期之前未更新，则无法申报。政府开始与学术界合作，将有关网络安全和卫生的数据和统计数据转换为信息和图形**

100 Mike Bergman。消费者技术协会。向NSTAC ICR小组委员会简介。 2017年8月3日（指出，Mirai / Dyn攻击的攻击地点中约有89%位于国外）。

101伊恩·利维（Ian Levy）。英国国家网络安全中心。向NSTAC ICR小组委员会简介。 2017年8月9日。

公众可以理解。这些重要步骤将帮助公众理解网络安全的重要性，并采取适当行动改变其行为。

- **政府内部实践。英国保护在线足迹。它还添加了基于域的消息身份验证，报告以及对美国每个政府域的遵从性，以防止电子邮件欺骗。为减少恶意软件攻击，政府会对使用gov.uk名称的任何站点进行自动扫描。政府还通过积极追踪和删除spoofing.gov.uk网站，保护gov.uk品牌。政府也正在采取步骤，更好地管理企业。它收集有关哪些机构落后于最新数据的数据，并利用这些数据迫使系统集成商改善或冒险政府发布该信息供公众消费。政府还试图不购买不安全或未经验证的软件。**

- **私人-**
  公共伙伴关系。英国政府与私营部门之间的合作伙伴关系有助于防止攻击并提高网络安全性。例如，政府要求主机删除或修复有害流量，导致网络钓鱼，网络注入和政府品牌网络钓鱼的可用性急剧下降。根据英国政府通信总部（GCHQ）提供的信息，政府成功清除了153个网络钓鱼工具套件凭据商店，2570笔预付费欺诈攻击和23,000个邮件中继。为了保护网络，政府建立了公共部门规模的递归域名系统，包括过滤服务。它免费向ISP提供此服务。据GCHQ称，截至2017年7月，该服务已阻止23,046个唯一托管恶意内容的域。利用政府网络钓鱼和恶意软件缓解服务，成功清除了79,567起攻击。政府还采用"名与耻"策略鼓励银行和互联网服务提供商等行业将安全流程纳入防御之中。

其他国际伙伴关系

在欧洲，"不再勒索"项目是欧洲网络犯罪中心，荷兰警察和包括亚马逊网络服务在内的商业公司的合作。创建该计划的目的是作为单个加密密钥存储库，目的是提高全球安全性。社区会向受害者告知他们感染了什么勒索软件，并共计删除了Shade，Chimera和WildFire等各种恶意软件。该计划还为勒索软件受害者提供了50种公开可用的加密工具。"无更多赎金"等努力是国际社会与僵尸网络作斗争所采取的重要步骤。[102]

政府建议

- **美国政府应制定能够减慢僵尸网络扩散的国际规范。英国表明，政府可以在建模安全模型以及与私营部门合作建立私有和公共网络方面发挥重要作用**

  –更安全。其他政府可以从这个例子中学到东西。但是，政府

102 Raj Samani。英国迈克菲。向NSTAC ICR小组委员会简介。 2017年8月15日。

不能独自行动。美国政府应与私营部门合作，在国际标准机构内部合作，制定以最佳实践为指导的标准，指导政府和服务提供商。标准的广泛采用将提供重要的防御措施。

- **美国政府应推动建立国际设备安全框架。开发安全设备需要国际合作。这包括识别一个或多个机构，这些机构可能是开发用于共享设备安全功能和行为指纹和/或补丁和可升级性要求的信息的框架或平台的负责人。这些标准可以帮助制造商开发更安全的设备，并帮助企业和消费者更好地管理其设备。**

- **发展对民族国家攻击的国际威慑力量。民族国家现在发起大量僵尸网络攻击。遏制这种行为将要求国际机构和个别国家对此类行动采取强硬立场。这些措施将消除此类攻击的重要来源，更重要的是，开始增加攻击者的成本。**

4.0网络安全月球

本报告的前一部分（第3.0节）重点关注与现有已知最佳实践和技术相关的短期建议，如果更广泛地实施，则可能对减少自动化和分布式网络攻击的威胁立即产生切实影响。NSTAC
ICR小组委员会的调查结果加强了NSTAC在NSTAC提交给新兴技术战略愿景总裁报告中的先前建议，即国家当前的网络安全挑战主要不受技术环境限制，但受人为控制因素（如各种法律，行为，迄今为止，教育和教育挑战限制了广泛接受的网络安全最佳实践的部署。[103]

虽然全面执行第3.0节中的建议将对国家的网络安全产生切实影响，但这些集体建议最终仍代表增量解决方案，不足以解决国家更基本，更持久的网络安全挑战。此外，NSTAC得出结论，当前和新兴技术格局（包括机器学习，云计算和量子计算方面的重大进步）为实现网络安全领域的巨大变革提供了必要的基础。
NSTAC认为，努力主要缺少全国一致的努力和战略指导。因此，NSTAC重申其建议，即建立国家网络安全“ Moonshot”，这是NSTAC提交给新兴技术战略愿景主席的报告。

103 NSTAC。
NSTAC致新兴技术战略愿景总裁报告，https://www.dhs.gov/sites/default/files/publications/Draft%20NSTAC%20Report%20to%20the%20President%20on%20Emerging%20Technologies%20%287-10-17%29%20v3%20%281%29-%20508.pdf

在白宫的支持下，NSTAC承诺发起网络安全“ Moonshot”概念，就政府如何最有效地协调国家努力提供私营行业建议。根据NSTAC和E OP的共识，这项研究将有时间反映网络安全挑战的短期紧迫性，同时确保针对如此规模倡议的彻底性和严格性。在进行这项研究时，NSTAC提出了一项初步的两阶段行动方案。

定义过程：Moonshot模型的核心原理

NSTAC研究的第一阶段将回顾成功模型，无论行业或主题如何，该模型通常反映Moonshot努力的核心原则。NSTAC的工作将远远超出网络安全领域，以识别从先前成功的国家动员工作中吸取的教训。研究的第一阶段将重点回答以下基本问题：在成功的Moonshot模型中定义一致的核心原理是什么？

作为一个起点，国家科咨机构将重点确定以下列原则为特征的其他举措。这些拟议要素仅是指导初始研究范围的指导原则，并不被认为是全面的。截至撰写本文时，NSTAC得出的结论是，要想获得Moonshot资格，必须至少具有以下要素：

- **国家行动纲领：**最高层政府必须公开认为重大国家后果问题，并宣布解决方案为国家战略重点。
- **聚焦于最终目标：**政府必须强调针对宏伟最终目标的战略愿景，有明确的基于时间的截止日期，而无需规定实现最终目标所需的增量步骤。
- **多方利益相关者流程：**政府必须利用其独特的召集机构并建立适当的协作机制以正式利用多方利益相关者社区（至少包括私营企业和学术界），以执行既定的战略最终目标，促进国家努力。

明确定义网络安全月球

NSTAC研究的第二阶段将专注于将从这些国家Moonshot努力中汲取的与领域无关的课程应用于网络安全领域。第二阶段将就与已确定的Moonshot原则（行动呼吁，最终目标重点和多方利益相关者流程）以及尚待确定的其他原则相关的关键网络安全考虑因素，进一步澄清和建议。因此，在研究的第二阶段，NSTAC将听取各种网络安全专家和其他人士的意见，以适当定义既定的最终目标和最终目标的子要素。此阶段将寻求回答以下问题：什么是适用于网络安全领域的适当范围的登月射击？

5.0政府必须与行业合作

政府必须带头应对对互联数字未来的网络安全威胁。威胁来自民族国家，有组织犯罪，黑客主义者，恐怖分子等。私营部门不能独自做到这一点。联邦政府必须通过促进跨经济部门和政治边界的合作，在国内外领导。
NSTAC建议政府应对物联网安全必须开展的以下活动。

保护和扩大公私合作伙伴关系，这一直是联邦网络政策的基础。数十年来，行业一直与DHS在NCCIC和美国计算机应急准备小组等领域合作。工业界还在CSRIC，技术咨询理事会以及其他机构（包括NIST和NTIA）中与政府合作。

工业界已与政府合作保护关键基础设施。为响应要求识别和保护关键基础设施的第13636号行政命令，八名金融部门首席执行官启动了旨在增强核心金融服务网络安全的工作，该系统被称为金融系统分析和弹性中心（FSARC）。
FSARC与政府合作，协调针对主要对手的运动，开发和分享最佳实践和经验教训，为支持联邦执法的刑事案件做出贡献，并利用美国政府的访问权限和信息来确定犯罪活动在哪里或与之结盟由外国情报人员使用。私营部门帮助塑造了这一格局，并一直在实施NIST的网络安全框架，而且各个部门都在将其映射到其独特需求。例如，CSRIC IV于2015年3月发布的最终文件《网络安全风险管理和最佳实践》为帮助通信提供商使用和采用NIST网络安全框架提供了指导。此类举措对于在预算有限的情况下运营的小型医疗服务提供商特别有用。[104][105]

这种伙伴关系依靠信任，必须不受监管和执行威胁。

考虑培养有关漏洞的信息共享的创新方法，包括责任保护和安全港。如果运营商和制造商要讨论产品和服务漏洞，则必须认识到这样做所带来的风险，并保护此类活动。漏洞披露程序很有趣，但可能缺少工作的关键组件。国土安全部在2016年指出，除其他事项外，应召集一组合作伙伴审议赔偿责任。美国商会法律改革研究所和其他机构一直在研究这些问题，例如，在《未来侵权法》中，商会指出："
[联网产品制造商面临的重大责任风险源于[106]

104斯科特·德帕斯夸莱。金融服务分析和响应中心。向NSTAC ICR小组委员会简介。

2017年8月10日

105 FCC，CSRIC IV，第4工作组：最终报告，网络安全风险管理和最佳实践工作组。

2015年3月.https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

106参见DHS。"确保物联网（IoT）安全的战略原则。"版本1.0。

2016年11月15日。https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_pdf.

网络攻击或窃取私人信息。"联邦政府必须考虑民事诉讼风险和我们的诉讼司法系统如何阻碍有益活动。[107]

确定并解决限制私营部门防御措施的法律限制。分布式拒绝服务和其他缓解措施可能会使公司承受联邦法律的风险。如果归因错误，也会对第三方造成意外后果。政府必须确定主动防御的目标和私营部门的作用。此外，政府必须考虑CISA的保护和权限是否足够。保护共享网络威胁指标和防御措施可能还不够。适当地保护互联网服务提供商（ISP）和其他提供商的责任，对于进一步制定防御措施和信息共享至关重要。责任保护立法语言必须与生态系统成员的任何扩展角色同步更新。[108]

调整应对网络威胁时美国情报部门的运作方式。国家基础设施咨询委员会（NIAC）最近评估了英国和以色列的情报收集方法。NIAC建议："高效有效协调由中央机构负责，可以为国家协调网络优先级，调整行业和政府资源，为网络防御提供国家领导。"报告进一步讨论了英国在创建英国国家网络安全中心和以色列国家网络局方面的努力。NSTAC建议美国政府评估这些模型，并确定英国和以色列正在开发的任何概念是否有助于组织美国政府的网络安全工作。NSTAC还建议美国考虑改变其网络情报收集方法，允许分析师在更长的时间内仅专注于一个目标，从而成为专家，并且更有可能对抗目标的特定攻击。[109][110]
改善与私营部门的信息共享。政府有权获取情报信息；但是，在分类级别共享信息的过程可能很麻烦。NSTAC建议总统指示联邦政府对现有信息计划进行审查，以确定它们是否达到目标，并建议新方法（甚至在试验基础上），以实现更好的信息共享。政府还应该承认，并非所有信息接收者都具有相同的能力。应该有一系列与各方能力相称的信息共享模型。消除联邦，州和地方各级的监管悬而未决。私营部门担心监管义务，技术任务和报告制度将

107美国商会法律改革研究所。"未来侵权行为-解决新兴技术的责任和监管问题。"2017年3月。http://www.instituteforlegalreform.com/uploads/sites/1/Torts of the Future Addressing the Liability and Regulatory Implications of Emerging Technologies April 2017.pdf?pagename=uploads/sites/1/Torts of the Future Addressing the Liability and Regulat.yy

108 2015年《网络和信息共享法》第104（c）节，第6条。1504。

109 NIAC。"保护网络资产-应对关键基础设施的紧急网络威胁。"2017年8月。https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17-508.pdf.

110 NIAC致总统的报告"安全网络资产"，19日（2017年8月），可从以下网站获取：https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17-508.pdf

占用宝贵的资源并鼓励遵循合规思维模式，优先考虑"检查框"思维模式，而不是敏捷和积极的创新。在网络安全领域，威胁，漏洞和响应的移动速度是任何监管机构的指数级速度。如果政府想要真正的合作伙伴，则必须明确，在监管和惩罚性执法方面，合作和尽最大努力不会使私营部门反弹。联邦政府应劝阻州政府开展活动，无论是在技术授权，在线隐私负担还是其他措施方面，都可能使产品和服务开发复杂化并阻碍其发展。

政府可能会认识到，无论是在技术授权，在线隐私负担还是其他措施方面，都存在着国家活动，而且将继续存在，其中一些努力可能会使产品和服务开发分散和复杂化。考虑到这一现实，NSTAC建议联邦政府鼓励各州首先为州自己的行政组织和系统采用并实施一致的网络安全最佳做法和建议，然后再为州居民和企业生态系统推广。应鼓励各国与主要利益攸关方一起参加国家级场所，采取一致的网络安全方法。其中应包括全国州长协会，全国州首席信息官协会；全国州议会会议，国土安全部州，地方，部落和领土政府协调委员会。

积极代表国外的美国政策和经济利益。全球信息和通信技术部门需要美国政府领导国外。地区和国家正在以不同方式应对安全和技术。美国大力倡导开放市场，技术中立和透明的标准程序符合国家安全和经济利益。如果美国不领导，其他国家的法律标准和规定性法规可能会设定国际基准，并减慢美国公司的国际增长。

促进网络安全劳动力发展。许多报告建议政府解决网络劳动力不足的问题，这些缺陷可能削弱我们应对不断扩大的威胁的能力。例如，NIAC报告（建议采用公私专家交流计划），CSRIC最终报告，网络安全劳动力发展最佳实践建议，DHS的各种努力，包括建立国家网络安全职业和研究倡议，国家网络安全劳动力框架，网络安全劳动力开发工具包，[111][112][113][114][115]

111 NIAC。"保护网络资产-应对关键基础设施的紧急网络威胁。"建议2017年8月4日。https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17- 508.pdf.

112 CSRIC。第7工作组最终报告。"网络安全劳动力发展最佳实践建议。" 2017年3月。https://www.fcc.gov/files/csric5-wg7-finalreport031517pdf.

113 NICCS，https://niccs.us-cert.gov/.

114 NICCS。NICE网络安全劳动力框架，https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework.

115 NICCS。"网络安全劳动力开发工具包—如何构建强大的网络安全劳动力。" 2017年3月。https://niccs.us-cert.gov/sites/default/files/documents/pdf/cybersecurity_workforce_development_toolkit.pdf?trackDocs=cybersecurity_workforce_development_toolkit.pdf.

以及《改善卫生保健行业网络安全的报告》（2016年6月）。此外，网络安全人员可能需要理解编码和外语，因为大多数僵尸网络均使用英语以外的其他语言进行编码。有很多工作要做，但已经达成共识，这是政府关注的关键领域。[116]

注意使用采购系统解决物联网网络安全问题。政府应考虑如何确保其产品和服务得到适当保护。但是，政府应避免过分关注设备或依靠单方面授权来实现这种增强的安全性。NSTAC建议政府探索可以由私营部门专家提供的托管服务。这将使政府能够利用私营部门的专业知识和规模（互联网服务提供商（ISP），云提供商，向第三方提供服务的其他提供商），而不使用更基本的设备安全要求。

开发智囊团，探索月球机会。政府应该重复寻找新方法，而不是重复先前尝试的尝试，例如扩展新的IP协议。NSTAC建议政府探索建立协作和创新的合作伙伴关系，并与NIST的国家网络安全卓越中心相似的智囊团，与私营部门，学术界和其他机构合作，寻找技术问题的解决方案。可以考虑的另一种方法是类似于以网络为中心的国防高级研究计划局，该机构得益于特别的法定招聘机构和替代合同工具，使该机构抓住机会推进任务。

6.0结论

僵尸网络及其带来的攻击预计只会增长。缓解这一复杂问题将需要整个互联网生态系统采取多种措施。尽管本报告为设备制造商，网络服务提供商，软件开发商，企业和政府提供建议，但并非唯一参与缓解威胁的实体。网络安全是共同的责任，取决于生态系统的各个部分。NSTAC还预计，随着时间的推移，解决方案的范围也会不断变化。因此，NSTAC预计本报告或任何后续程序不会是静态的。应对这一挑战需要私营部门与政府之间不断的合作与承诺。最后，许多建议是迭代的，不会从根本上改变问题的根本性质。因此，NSTAC建议对NSTAC进行进一步的研究，调查旨在针对底层互联网基础设施的网络安全Moonsh ot的可能性，并提出长期改进建议。

116卫生保健行业网络安全工作队（HCIC工作队）。"关于改善医疗保健行业网络安全的报告。"建议6.4。2017年6月。https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.

附录A：会员

小组委员会成员

Sonus Networks Inc.的Raymond Dolan先生和小组委员会联席主席
AT&T Inc.的John Donovan先生和小组委员会联席主席
AT&T Inc.Chris Boyer先生和ICR工作组联席主席
Kevin Rile先生Sonus Networks Inc.兼ICR工作组联席主席

AT&T, Inc.	Mr. Jonathan Gannon Mr. Bill O'Hern
Avaya, Inc.	Mr. Vico Loquerico
CenturyLink, Inc.	Ms. Kathryn Condello Mr. Paul Diamond Mr. John Schiel Mr. Donald Smith
Communication Technologies, Inc.	Mr. Milan Vlajnic
Department of Homeland Security	Mr. Gregory Shannon
Diogenes Group, LLC	Mr. William Gravell
Dun & Bradstreet Corporation	Mr. Gregory Mortensen Mr. Jon Rose
Equinix, Inc.	Ms. Cindy Liu
ForeScout Technologies, Inc.	Mr. Tamer Baker Ms. Katherine Gronberg
Lockheed Martin Corporation	Mr. Darrell Durst
Microsoft Corporation	Mr. Richard Boscovich Ms. Amanda Craig Deckard
McAfee, LLC	Mr. Patrick Flynn Mr. Kent Landfield
National Security Agency	Ms. Cheri Caddy
National Telecommunications and Information Administration	

	Ms. Evelyn Remaley
National Institute of Standards and Technology	Mr. Tim Polk
NCTA – The Internet & Television Association	Mr. Matt Tooley
Neustar, Inc.	Ms. Terri Claffey
Oracle Corporation	Dr. Prescott Winter
Palo Alto Networks, Inc.	Mr. Sean Morgan
Raytheon Company	Mr. Michael Daly
Unisys Corporation	Mr. Mark Cohn Mr. Tom Patterson
USTelecomm	Mr. Robert Mayer
Verizon Communications, Inc.	Mr. Kevin Kirsche Mr. Timothy Vogel

简报–主题专家

Arbor Networks, Inc.	Ms. Arrabelle Hallawell
AT&T, Inc.	Mr. Brian Rexroad Mr. Bill O'Hern
CA Technologies, Inc.	Mr. Jaime Brown
Center for Democracy and Technology	Ms. Michelle Richardson
Consumer Technology Association	Mr. Mike Bergman
Cyber Threat Alliance	Mr. Michael Daniel
Department of Defense	Mr. Mitchell Komaroff
Department of Homeland Security	Dr. Ann Cox
Department of Justice	Mr. Leonard Bailey
Dun & Bradstreet Corporation	Dr. Anthony Scriffignano
Embassy of Japan	Mr. Daisuke Hayashi

Federal Bureau of Investigation	Mr. Tom Grasso
ForeScout Technologies, Inc.	Mr. Wallace Sann
Financial Services Analysis & Response Center	Mr. Scott DePasquale
Financial Systematic Analysis & Resilience Center	Mr. Bill Nelsen
Japanese Ministry of Internal Affairs & Communication	Mr. Atsushi Goto Mr. Yasu Taniwaki
Japanese National Center of Industry Readiness and Strategy for Cybersecurity	Ms. Kasumi Sugomoto
Intelligence Advanced Research Project Agency	Mr. Kerry Long
McAfee United Kingdom	Mr. Raj Samani
Micron Technology, Inc.	Mr. Steve Wallach
Microsoft	Mr. Richard Boscovich Mr. Rob Spiger
NCTA – The Internet & Television Association	Mr. Matt Tooley
National Security Agency	Ms. Cheri Caddy
National Institute of Standards and Technology	Mr. Andrew Regenscheid Dr. Charles Romine
Neustar, Inc.	Mr. Barrett Lyon
Oracle	Mr. Travis Russell
Palo Alto Networks, Inc.	Mr. Kevin Walsh
Raytheon Company	Mr. J.F. Mergen
sn3rd LLC	Mr. Sean Turner
Unisys Corporation	Mr. Brent Houlahan Mr. Jack Koons
United Kingdom Nation Cyber Security Centre	Dr. Ian Levy
US Marine Corps	Dr. Ray Letteer

USTelecom	Mr. Robert Mayer
Venable LLP	Mr. Ari Schwartz
VeriSign, Inc.	Mr. Danny McPherson Dr. Eric Osterweil

小组委员会管理

NSTAC Designated Federal Officer	Ms. Helen Jackson
Alternate NSTAC DFO	Ms. Sandy Benevides Ms. DeShelle Cleghorn
Booz Allen Hamilton, Inc.	Ms. Ursula Arno Mr. William Hyde
Total Systems Technology Corporation	Mr. Robert Carter

5G	Fifth Generation
ABC	Anti-Botnet Code of Conduct
AI	Artificial Intelligence
BCP	Best Common Practices
BGP	Border Gateway Protocol
BYOD	Bring Your Own Device
CharGen	Character Generator Protocol
CISA	Cybersecurity Information Sharing Act
CITL	Cybersecurity Independent Testing Laboratory
CNSSI	Committee on National Security Systems Instruction
CSRIC	Communications Security, Reliability and Interoperability Council
CTA	Consumer Technology Association
CVD	Coordinated Vulnerability Disclosure
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DOC	Department of Commerce
DoD	Department of Defense
DOJ	Department of Justice
DoS	Denial of Service
EO	Executive Order
EOP	Executive Office of the President
ETSV	Emerging Technology Strategic Vision
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FSARC	Financial Systemic Analysis and Resilience Center
FTC	Federal Trade Commission
Gbps	Gigabits Per Second
GCHQ	Government Communications Headquarters
GSMA	Groupe Spécial Mobile Association
ICR	Internet and Communications Resilience
ICS	Industrial Control System
ICT	Information and Communications Technologies
IEC	International Electrotechnical Commission
IETF	Internet Engineering Technical Forum
IoT	Internet of Things
IP	Internet Protocol
IPv6	Internet Protocol Version 6
ISO	International Organization for Standardization
ISP	Internet Service Providers
IT	Information Technology
M2M	Machine to Machine
M3AAWG	Messaging, Malware, and Mobile Anti-Abuse Working Group

MUD	Manufacturer Usage Description
NCCIC	National Cybersecurity and Communications Integration Center
NCCoE	National Institute of Standards and Technology National Cybersecurity Center of Excellence
NFV	Network Functions Virtualization
NIAC	National Infrastructure Advisory Council
NIST	National Institute of Standards and Technology
NISTIR	NIST Glossary of Information Security Terms
NMD	Network Monitor Devices
NS/EP	National Security/Emergency Preparedness
NSTAC	National Security Telecommunications Advisory Committee
NTIA	National Telecommunications and Information Administration
NTP	Network Time Protocol
OS	Operating System
RPKI	Resource Public Key Infrastructure
SAFECode	Software Assurance Forum for Excellence in Code
SDL	Security Development Lifecycle
SDN	Software Defined Network
SS7	Signaling System 7
U.K.	United Kingdom
UL	Underwriters Lab
U.S.	United States
VPN	Virtual Private Network

附录C：词汇

5G –未来的第五代移动网络，国际电信联盟的规范尚未完全定义。预计将支持每秒**10 GB**的数据速率或更高。预计到**2020**年左右才能实现商用**5G**。（牛顿电信词典）

人工智能–由机器或软件展现的智能。由艾伦·图灵（**Alan Turing**）推广使用的术语，在历史上描述的是一种可以通过图灵测试欺骗人们认为它是人类的机器。最近，该领域的科学家很大程度上放弃了这一目标，专注于机器智能的独特性，学习以智能，有用的方式使用机器智能。（牛顿电信词典）

认证–
用户，信息源或简单信息证明自己是自称身份的过程；确定试图访问网络和/或计算机系统的用户身份的过程。（牛顿电信词典）

僵尸网络–
互联网连接的计算机网络，已感染了恶意第三方的命令和控制软件，并且能够远程指示第三方执行有害操作，如通过互联网发起攻击。（牛顿电信词典）

云计算–
一种模型，用于使按需网络访问共享池中的可配置信息技术功能/资源（例如，网络，服务器，存储，应用程序和服务），可以通过最少的管理快速配置和发布努力或服务提供商交互。它允许用户从网络云访问基于技术的服务，而无需了解支持他们的技术基础设施，专业知识或对其进行控制。用户数据和基本安全服务都可以驻留在网络云中并在内部进行管理。（国家安全系统指令委员会（**CNSSI**）**4009**，改编）（**NSTAC**报告**2016**）

关键基础设施–
对美国至关重要的系统和资产，无论是物理还是虚拟的，如果丧失能力或被破坏，将对安全，国家经济安全，国家公共卫生或安全或以下各项的任何组合产生不利影响这些问题。关键基础设施可由公共和私营部门拥有和运营。
[2001年《关键基础设施保护法案》，**U.S.C**。**42**。 **5195c**（**e**）**]**（**CNSSI 4009**，改编）

网络攻击–
通过网络空间进行的攻击，针对企业使用网络空间破坏，禁用，破坏或恶意控制计算环境/基础设施的行为；或破坏数据完整性或窃取受控信息。（**CNSSI 4009**）

网络安全–保护或捍卫网络空间使用免受网络攻击的能力。（**CNSSI 4009**）

拒绝服务攻击–
阻止对资源的授权访问或时间紧迫操作的延迟。关键时间可能是毫秒，也可能是几小时，具体取决于提供的服务。（**CNSSI 4009**）

分布式拒绝服务攻击–
拒绝服务技术，使用大量主机进行攻击，阻止对资源的授权访问或延迟时间紧迫的操作。（**NIST**信息安全术语表–（**NISTIR**）**7298** –修订版**2**）

防火墙–
一种硬件或软件，或硬件和软件，可防止未经授权的人员访问计算机或计算机网络。（牛顿电信词典）

物联网–设备网络的总体互连集合。（牛顿电信词典）

互联网协议（**IP**）–传输控制协议/
IP协议家族的一部分，描述跟踪节点的互联网地址，路由传出消息和识别传入消息的软件。它还在网关中用于连接第**3**层及以上开放系统互连网络。（牛顿电信词典）

恶意软件–
为恶意目的而创建和分发的软件，例如以屏蔽其他破坏性功能的病毒，蠕虫或其他插件和扩展形式入侵计算机系统。（牛顿电信词典）

国家安全/应急准备（**NS / EP**）通信–
电信服务，用于保持就绪状态或响应和管理任何事故或危机（本地，国家或国际），造成或可能造成人身伤害或伤害，人口，财产损失或财产损失，或恶化或威胁美国的**NS / EP**态势（《联邦法规法典》第二章第**47**节第**201.2**（**g**）节）。 **NS / EP**通信主要包括由政策和计划支持的技术能力，使行政部门能够在任何时候，任何情况下进行通信，以执行其任务的基本职能并应对任何事件或危机（本地，国家或国际））， 包括与自己进行交流；立法和司法部门；州，地区，部落和地方政府；私营部门实体；以及公众，盟友和其他国家。 **NS / EP**通信还包括确保国家安全并有效管理事件和紧急情况所需的各级政府和私营部门系统和能力。 （**NS / EP**通信执行委员会的定义基于第**13618**号行政命令，国家安全和应急准备通信功能分配**[2012]**）

网络–
信息系统，由一组互连组件组成，可能包括路由器，集线器，电缆，电信控制器，密钥分配中心和技术控制设备。（**NIST**信息安全术语表（**NISTIR**）**7298** –修订版**2**）

网络虚拟化–
一种提高网络效率并降低成本的手段。它涉及在单个硬件上创建多个虚拟分区。减少了

所需的网络硬件数量，并允许从一个控制台管理多个功能。（牛顿电信词典）

协议–一组规则和格式（语义和语法），允许信息系统交换信息。
（**NIST**信息安全术语表– **NISTIR 7298** –修订版**2**）

软件定义网络–
虚拟专用网络。具体来说，它指的是**AT&T**的软件定义网络服务，于**1985**年为**AT&T**的最大客户推出，仅提供专用访问服务。（牛顿电信词典）

威胁–
可能通过信息系统未经授权访问，破坏，披露，修改信息和/或信息系统对代理机构运营（包括任务，职能，形象或声誉），代理资产或个人产生不利影响的任何情况或事件。拒绝服务。（**NIST SP 800-53**，**CNSSI 4009**，改编）

附录D：书目

AT&T。网络实践。 2017年4月24日。https://www.att.com/gen/public-affairs?pid=20879

乔木网络。全球基础设施安全报告，第十二卷，请访问：https://www.arbornetworks.com/insight-into-the-global-threat-landscape

贝纳，伦纳德。美国司法部。向NSTAC ICR小组委员会简介。

2017年8月10日。迈克·伯格曼。号召性文字。向NSTAC ICR小组委员会简介。

2017年8月3日。博斯科维奇，理查德。微软。向NSTAC ICR小组委员会简介。

2017年8月16日。克里斯·鲍耶。

M3AAWG公共政策联席主席（AT&T），新的M3AAWG僵尸网络指标报告*分享网络运营商的观点。* *2014年10月20日。*https://www.m3aawg.org/blog/new-m3aawg-bot-metrics-report-shares-network-operators%E2%80%99-perspective.

伯克，塞缪尔。 CNN。中国企业承认在网络攻击中的无意角色。2016年10月24日http://money.cnn.com/2016/10/23/technology/ddos-cyber-attack-chinese-firm/index.html

思科。思科视觉网络指数：预测和方法论，2016-2021年，白皮书。2017年6月7日。https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html

《计算机欺诈和滥用法案》（CFAA）（《美国法典》第18卷第1030节）；窃听法（美国法典第18卷第2511条）；笔登记/诱捕和追踪法规（《美国法典》第18卷第3121节及以下）；伦纳德·贝利。向NSTAC ICR小组委员会简介。 2017年8月10日。

计算机周刊，"全球黑客僵尸网络排名第六，被劫持设备数量达600万"，2017年9月27日http://www.computerweekly.com/news/450427023/Global-hacker-botnet-tops-6-million-hijacked-devices.

消费者技术协会，项目概述：为家庭消费者保护互联设备，CTA-CEB33，2017年7月7日。https://standards.cta.tech/apps/group_public/project/details.php?project_id=429

考克斯·安国土安全部。向NSTAC ICR小组委员会简介。

2017年8月1日。网络独立测试实验室（CITL）。 。http://cyber-itl.org/

国防部。“国防部宣布了数字漏洞披露政策，并宣布“陆军开战”。新闻稿。
2016年11月21日。https://www.defense.gov/News/News-Releases/News-Release-View/Article/1009956/dod-announces-digital-vulnerability-disclosure-policy-and-hack-the-army-kick-off/.

卫生与公共服务部。“医疗设备网络安全的上市后管理-
工业和食品药品监督管理局工作人员指南。”
2016年12月28日。https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

国土安全部（DHS）。“确保物联网（IoT）安全的战略原则。”版本1.0。
2016年11月15日。https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL pdf.

国土安全部。美国计算机应急准备小组。建立安全性。https://www.us-cert.gov/bsi.

司法部，在线系统漏洞披露程序框架，2017年7月。https://www.justice.gov/criminal-ccips/page/file/983996/download.

美国司法部。“关机，最大的在线“暗市场” AlphaBay。”
2017年7月20日。https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down.

美国司法部。“司法部采取行动禁用国际僵尸网络。”
2011年4月13日。https://www.justice.gov/opa/pr/department-justice-takes-action-disable-international-botnet.

ETSI NFV行业专业小组。网络运营商关于5G NFV优先级的观点。
2017年2月21日。https://portal.etsi.org/NFV/NFV_White_Paper_5G.pdf

爱立信移动报告。论网络社会的脉搏。
2016年6月https://www.ericsson.com/res/docs/2016/ericsson-mobility-report-2016.pdf

联邦通信委员会（FCC），通信安全可靠性和互操作性委员会（CSRIC）III，美国互联网服务提供商反机器人行为守则，2012年3月。https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-ReportFinal.pdf.

FCC，CSRIC II，2A工作组：最终报告，网络安全最佳实践。
2011年3月。https://transition.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf.

FCC，CSRIC
IV，第4工作组：最终报告，网络安全风险管理和最佳实践工作组。三月

2015。https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

FCC CSRIC
V，第5工作组最终报告，信息共享，2017年3月15日。https://www.fcc.gov/files/csric5-wg5-finalreport031517pdf.

FCC CSRIC。第7工作组最终报告，网络安全劳动力发展最佳实践建议。
2017年3月。https://www.fcc.gov/files/csric5-wg7-finalreport031517pdf.

FCC CSRIC
V，第10工作组，降低传统风险（2017年）（降低传统风险报告），https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf.

Fitzgerald，Brian和Chris Wysopal。 Veracode。向NSTAC ICR小组委员会简介。
2017年8月1日。

联邦贸易委员会（FTC）。“宣布其物联网家用设备安全竞赛冠军。”新闻稿。
2017年7月26日。https://www.ftc.gov/news-events/press-releases/2017/07/ftc-announces-winner-its-internet-things-home-device-security.

FTC。“FTC批准了针对TRENDnet的最终订单结算费用。 Inc.”新闻稿。；
2014年2月7日。https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inchttps://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put.

FTC。物联网：互联世界中的隐私与安全。 n.130。
2015年1月https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

FTC。物联网家庭检查员挑战赛。

2017。联邦贸易委员会。员工报告。物联网：互联世界中的隐私和安全，FTC。一月https://www.ftc.gov/iot-home-inspector-challenge.
2015。https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

洛伦佐（Franceschi-
Bicchierai），洛伦佐（Lorenzo），如何劫持150万台连接摄像头，打造前所未有的僵尸网络。 2016年9月29日https://motherboard.vice.com/en_us/article/8q8dab/15-million-connected-cameras-ddos-botnet-brian-krebs

乔治华盛顿大学网络与国土安全中心。进入灰色地带：私营部门和积极防御网络威胁。

GSMA。物联网安全准则。 2016年2月https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/

哈拉韦尔，阿拉贝尔。 Arbor Networks， Inc.向NSTAC ICR小组委员会简介。 2017年8月3日。

哈特奈特，凯文。有线。计算机科学家研究完美的，防黑客攻击的代码。 2016年9月23日。https://www.wired.com/2016/09/computer-scientists-close-perfect-hack-proof-code/.

卫生保健行业网络安全任务组。关于改善医疗保健行业网络安全的报告。 2017年6月。https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.

我是骑兵。 DOT政府协调披露时间表。https://www.iamthe cavalry.org/wp-content/uploads/2016/12/IATC_Gov-Coordinated-Disclosure-Timeline_v1.0.jpg.

封装。全球分布式拒绝服务威胁格局。 。https://www.incapsula.com/ddos-report/ddos-report-q1-2017.html

Koeberl， Patrick等。 " TrustLite：微型嵌入式设备的安全架构。"http://www.icri-sc.org/fileadmin/user_upload/Group_TRUST/PubsPDF/trustlite.pdf

勒纳·扎克，"微软，僵尸网络猎人：公私合作伙伴关系在缓解僵尸网络中的作用，" 28 HARV。 J.L.＆TECH。 237，247（2014）。

莱特尔， 雷。美国海军陆战队向NSTAC ICR小组委员会简介。

2017年8月30日。伊恩，利维。英国国家网络安全中心。向NSTAC ICR小组委员会简介。 2017年8月9日。

迈克菲。 Mirai IoT僵尸网络攻击：蜜罐插图。 2017年4月5日。https://www.youtube.com/watch?v=vnitAXYGmI0.

迈克菲。安全家庭平台服务。微软。什么是安全开发生命周期？https://securehomeplatform.mcafee.com/.https://www.microsoft.com/en-us/sdl/default.aspx。

米切尔， 查理。 "黑帽创始人将软件责任视为主要的网络安全政策挑战。"内部网络安全。 2017年7月26日。https://insidecybersecurity.com/daily-news/black-hat-founder-sees-software-liability-major-cybersecurity-policy-challenge.

国家公路交通安全管理局（NHTSA）。“现代车辆网络安全最佳实践。”
2016年10月。https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf.

NIAC。“保护网络资产-应对关键基础设施的紧急网络威胁。”
2017年8月。https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17-508.pdf.

网络功能虚拟化-5G NFV优先级白皮书。
2017年2月21日。https://portal.etsi.org/NFV/NFV_White_Paper_5G.pdf.

NICCS。 NICE网络安全劳动力框架。 。https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework

NICCS。“网络安全劳动力开发工具包—如何构建强大的网络安全劳动力。”
2017年3月。https://niccs.us-cert.gov/sites/default/files/documents/pdf/cybersecurity_workforce_development_toolkit.pdf?trackDocs=cybersecurity_workforce_development_toolkit.pdf
。

美国国家标准技术研究院（NIST）。改善关键基础设施网络安全的框架。
2014年2月12日。http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

NIST。特别出版物800-193。平台固件弹性指南。
2017年5月。https://csrc.nist.gov/csrc/media/publications/sp/800-193/draft/documents/sp800-193-draft.pdf

NIST信息技术实验室（ITL）公告。显着减少软件漏洞。
2017年1月。http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=922589.

NIST ITL公告。定制工业控制系统的安全控制。
2015年11月。http://csrc.nist.gov/publications/nistbul/itlbul2015_11.pdf.

国家电信和信息管理局（NTIA）。现有物联网安全标准目录（草案版本0.01），有关物联网安全升级和修补的NTIA多利益相关方流程，现有标准，工具和举措工作组。
2017年7月。https://www.ntia.doc.gov/files/ntia/publications/iotsecuritystandardscatalog.pdf.

NTIA。通信部门协调理事会。行业技术白皮书。
2017年7月17日。https://www.ntia.doc.gov/files/ntia/publications/cscc_industrywhitepaper_cover_letter.pdf.

NTIA。多利益相关方流程：网络安全漏洞。
2016年12月15日。https://www.ntia.doc.gov/other-publication/2016/multistakeholder-

NSTAC。 NSTAC就物联网向总统报告。
2014年11月19日。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.

奥赫恩，比尔。 AT&T，Inc.向NSTAC ICR小组委员会做简报。

2017年7月20日。奥尔姆斯特德，肯尼斯和亚伦·史密斯。

"美国人与网络安全。"皮尤研究中心
*报告。于2017年1月26日。*http://assets.pewresearch.org/wp-content/uploads/sites/14/2017/01/26102016/Americans-and-Cyber-Security-final.pdf.

Pahl，Thomas B. FTC。从安全开始，并坚持不懈。
2017年7月28日。https://www.ftc.gov/news-events/blogs/business-blog/2017/07/start-security-stick-it.

安全代码。https://safecode.org/about-safecode/.

萨玛尼，拉杰。英国迈克菲。向NSTAC ICR小组委员会简介。

2017年8月15日。前景色。向NSTAC ICR小组委员会简介。

2017年8月22日。Sandvine，全球互联网现象：加密互联网流量。 2016。
https://www.sandvine.com/resources/global-internet-phenomena/spotlight/internet-traffic-encryption.html。

施耐尔，布鲁斯。我们需要从物联网中拯救互联网。
2016年10月6日https://www.schneier.com/essays/archives/2016/10/we_need_to_save_the_.html

斯克里菲尼亚诺，安东尼。 Dun&Bradstreet，Inc.向NSTAC ICR小组委员会简介。
2017年8月15日。

Spamhaus项目。世界上最糟糕的僵尸网络国家。
2017年8月18日。https://www.spamhaus.org/statistics/botnet-cc/.

赛门铁克。 Mirai：您需要了解最近的大型分布式拒绝服务攻击背后的僵尸网络。
2016年10月27日。https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks.

Tooley，Matt。国家有线和电视协会（NCTA），通信部门协调理事会，有关僵尸网络和自动威胁的行业技术白皮书。

美国商会法律改革研究所。"未来侵权行为-解决新兴技术的责任和监管问题。"

沃拉奇，史蒂夫。美光科技公司向NSTAC ICR小组委员会简介。 2017年9月7日。

沃尔什，凯文。帕洛阿尔托网络公司向NSTAC ICR小组委员会做简报。
2017年7月18日。

华纳，马克。“参议员提出两党立法以改善物联网设备的网络安全。”新闻稿。
2017年8月1日。https://www.warner.senate.gov/public/index.cfm/pressreleases?ID=06A5E941-FBC3-4A63-B9B4-523E18DADB36.

白宫新闻秘书办公室。
13800号行政命令，加强联邦网络和关键基础设施的网络安全。
2017年5月11日。https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure.

Xfinity。 Comcast阻止端口列表。 。https://www.xfinity.com/support/internet/list-of-blocked-ports/

泽特，金。“骇客词汇：什么是拒绝服务和分布式拒绝服务攻击？”有线。
2016年1月16日。https://www.wired.com/2016/01/hacker-lexicon-what-are-dos-and-ddos-attacks/.