NISTIR 8192

增强互联网的弹性和通信生态系统

NIST研讨会论文集

蒂姆·波尔克

该出版物可从以下网站免费获得：
https://doi.org/10.6028/NIST.IR.8192

National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 8192

增强互联网的弹性和通信生态系统

NIST研讨会论文集

蒂姆·波尔克
应用网络安全应用司
信息技术实验室

该出版物可从以下网站免费获得：
https://doi.org/10.6028/NIST.IR.8192

2017年9月

美国商务部
小威尔伯·罗斯·秘书

美国国家标准技术研究院
NIST代理主任兼标准和技术商务部副部长肯特·罗奇福德

美国国家标准技术研究院内部报告8192
33页（2017年9月）

该出版物可从以下网站免费获得：
https://doi.org/10.6028/NIST.IR.8192

关于这个主题的评论可能会在2018年2月5日之前提交给：

美国国家标准技术研究院
参加者：信息技术实验室应用网络安全司
100 Bureau Drive（Mail Stop 2000）盖瑟斯堡，马里兰州20899-2000
电子邮件：distributed.threats@nist.gov

有关更多详细信息，请参见本文档第5节。

所有评论都将根据信息自由法（FOIA）发布。

计算机系统技术报告

美国国家标准与技术研究院信息技术实验室（ITL）
技术（NIST）通过提供技术来促进美国经济和公共福利。
国家测量和标准基础设施的领导者。 ITL开发测试，测试
方法，参考数据，概念验证实施和技术分析来推进
开发和生产利用信息技术。 ITL的职责包括
制定管理，行政，技术和物理标准以及指南
联邦中与国家安全相关的信息以外的成本有效的安全和隐私
信息系统。

摘要

这些程序记录了2017年7月11日至12日“增强互联网和
“通信生态系统”研讨会由美国国家标准研究院和
技术。 13800号行政命令，“加强联邦网络和网络安全
关键基础设施”要求商业和国土安全部部长“联合
领导一个公开透明的过程，确定和促进适当的利益相关者采取的行动
改善互联网和通信生态系统的弹性，并鼓励
协作，以期大幅减少自动化和自动化造成的威胁
分布式攻击（例如僵尸网络）。”研讨会的目的是让利益相关者探索
一系列公开解决自动化，分布式威胁的解决方案
和透明的方式。研讨会吸引了来自不同利益相关方的150名参与者
社区，是根据查塔姆议院规则进行的。

关键词

僵尸网络；分布式威胁；分布式拒绝服务攻击（DDoS）；物联网；
弹性；信任的根源；安全更新

致谢

美国国家标准技术研究院（NIST）召开了此次研讨会，
150个行业参与者的出色贡献为我们带来了成功，
学术界，标准组织，非政府组织和政府机构。
我们特别感谢小组主席和小组成员的贡献；他们的想法
激烈的讨论对于接下来的分组会议的成功至关重要。

最后，如果没有我们的大力支持，这份研讨会报告是不可能的。
收到了NIST国家网络安全卓越中心（NCCoE）和MITER的好评
Corporation，NCCoE的运营商。 NCCoE是针对
加速集成网络安全工具和技术的广泛采用，并且
马里兰州和蒙哥马利县（医学博士）共同赞助
MITRE提供了主题专家，以吸引参与者和我们的贡献
研讨会结束后进行了详细分析，确定了关键关注领域和
关注。支持该过程的主题专家有：

- 布莱恩·安倍（
- 特雷·艾伦斯沃思（NCCoE）
- 布列塔尼·比昂多（Mitre）
- 大卫·丹达（Mitre）
- 卢拉·丹利（Mitre）
- Zachary Furness（NCCoE）
- 黛安·库拉（Mitre）
- 苏珊·普林斯（NCCoE）
- 朱莉·斯坦克（NCCoE）
- Caroline Tan（NCCoE）
- 亚伦·泰明（NCCoE）
- 特雷莎·托马斯（NCCoE）
- 玛丽·杨（NCCoE）

执行摘要

13800号行政命令，“加强联邦网络和关键网络安全
基础设施”于2017年5月11日发布。在第2（d）节中，行政命令要求
商务和国土安全部部长“共同领导一个开放透明
识别和促进适当的利益相关者采取行动，提高抵御能力的过程
互联网和通信生态系统，并鼓励实现以下目标的合作：
大大减少了自动化和分布式攻击（如僵尸网络）造成的威胁。”
行政命令指示各部门于2018年1月发布初步报告，并
在2018年5月11日之前向总统提交最终报告。[1]

这些程序记录了2017年7月11日至12日“增强互联网和
“通信生态系统”研讨会由美国国家标准研究院和
技术。讲习班是各方面同时开展的几个工作流程之一
部门的组成部分，以吸引利益相关者参与并确定适当的行动。的
讲习班吸引了来自不同利益相关者社区的150名参与者
根据查塔姆议院规则。

研讨会讨论中出现了六个总体主题：

1.问题的全球性：构成安全威胁的大多数设备
僵尸网络位于美国境外。与之协调的行动
将需要国际伙伴提高生态系统抵御气候变化的能力
这些威胁。
2.有效工具的可用性：实现以下目标所需的工具，流程和实践
大大增强生态系统的复原力
应用于特定市场领域，但利用不足。
3.在整个生命周期内保护产品的重要性：
部署时容易受到攻击，发现后缺乏修复漏洞的工具，
或在供应商支持终止后继续使用，组装僵尸网络并进行分布式
威胁实在太容易了。
4.教育和意识差距的影响：家庭和企业知识差距
客户，产品开发人员和基础设施运营商阻碍了部署
使生态系统更具弹性的工具，流程和实践。在
特别是客户友好型机制，可识别类似于以下内容的更安全的选择
需要能源之星计划或车辆碰撞等级来告知采购
决定。
5.市场激励与弹性目标之间的冲突：感知的市场激励确实
不符合“大幅减少由自动化和自动化造成的威胁的目标
分布式攻击。”市场激励措施激励产品开发商和供应商
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有效的安全保护
更新。

1行政命令全文可在以下网站获得：https://www.gpo.gov/fdsys/pkg/FR-2017-05-16/pdf/2017-10004.pdf.

6.需要采取协调一致的跨部门行动：没有一个利益攸关方共同体
有能力单独解决问题。来自各界的贡献将是
需要大幅提高生态系统对僵尸网络和网络的抵御能力
自动化的分布式威胁。

讲习班提供了重要的投入，并收到了响应
国家电信和信息管理局的评论请求和
国家安全电信咨询委员会的报告，将通知
编写报告草稿。对2018年1月报告的影响包括：

- 报告中建议的行动将涉及从中收集的每个总体主题
  讲习班的参与者。
- 报告将为每个利益相关者建议一项或多项建议的行动
  组（即基础设施提供商，产品开发人员，企业，家庭用户，
  学术界和政府）。
- 非政府利益相关者期望联邦政府以身作则，
  通过激励而非监管促进其他利益相关方的行动。
- 许多行动都依赖于分配给其他利益相关者的行动，因此
  报告中还需要确定协作机制。
- 建议可能包括立即采取行动以提高认识和
  部署当前可用技术，中期行动创造市场
  激励措施（尤其是确保整个产品生命周期的安全）并促进国际竞争
  协调与协作，以及开发新技术的长期行动。

欢迎就此主题做出更多公共贡献，并可以提交给
distributed.threats@nist.gov. 2017年10月15日之前提交的文稿将被考虑
包含在初步报告中，并将于或之前与社区共享
2018年1月5日。

公众意见征询和对初步报告的意见将持续到2月
2018年5月5日。意见征询期结束后，将于2月在
讨论计划中的评论解决方案。根据举行的公众评论和讨论
在第二次讲习班上，各部将完成报告并提交给主席
在2018年5月11日或之前。

目录

附录清单

图形列表

1.引言

13800号行政命令，“加强联邦网络和关键网络安全
基础设施”于2017年5月11日发布。在第2（d）节中，行政命令要求
商务和国土安全部部长“共同领导一个开放透明
识别和促进适当的利益相关者采取行动，提高抵御能力的过程
互联网和通信生态系统，并鼓励实现以下目标的合作：
大大减少了自动化和分布式攻击（如僵尸网络）造成的威胁。”
行政命令指示各部门在2018年1月发布公开初步报告，并h a
在2018年5月11日之前向总统提交最终报告。[2]

这些程序描述了2017年7月11日至12日“增强互联网和
“通信生态系统”研讨会由美国国家标准研究院和
技术（NIST）是此过程的第一步。讲习班是在
查塔姆之家规则。鼓励与会者分享意见和信息
在研讨会上进行了介绍，但被要求避免识别发言人或发言人
隶属关系。为遵守规则，本报告不关联在内部解决方案中提出的问题
与组织或行业部门举办的研讨会。

研讨会补充了各个组成部分同时开展的几个工作流程
部门的利益相关者参与并确定适当的行动，包括请求
国家电信和信息管理局公布的票据m
（NTIA）和国土安全部（S）负责国家安全和[3] DH
电信咨询理事会（NSTAC）。[4]

会议论文集由五个主要部分组成：本引言；简要叙述
组织研讨会和制定会议记录的过程；一个讲习班
摘要强调研讨会的共同主题；预期的影响
从讲习班参加者获得的关于报告公开草案的信息，
商务部和国土安全部将于2018年1月发布;以及继续参与的机会
这个话题。

2行政命令全文可在以下网站获得：https://www.gpo.gov/fdsys/pkg/FR-2017-05-16/pdf/2017-10004.pdf.

3国家电信和信息管理局（NTIA）发布了“
促进利益相关者对僵尸网络和其他自动威胁采取行动”，6月8日。其他信息，包括
NTIA收到的公众意见可在以下网站获得：https://www.ntia.doc.gov/federal-register-notice/2017/rfc-promoting-stakeholder-action-against-botnets-and-other-automated-threats.

4有关NSTAC的更多信息，请参阅https://www.dhs.gov/national-security-telecommunications-advisory-committee.

2.讲习班的计划，执行和分析

车间规划

发出E.O. 13800，与此同时，NIST
开始与NTIA和DHS的合作伙伴一起筹划公共研讨会，
促使利益相关者参与报告制定的第一步。讲习班是
旨在使利益相关者公开透明地探索一系列当前和
新兴解决方案可增强互联网和通信生态系统的弹性（
生态系统）以应对自动化，分布式威胁。研讨会于2017年6月6日宣布
仅有五个星期的交付时间，以确保可以在一月份反映出捐款
公共草案。尽管有很多时间，但研讨会很快就完成了150人的充分注册
代表不同利益相关者社区的参与者。车间规划团队
特别感谢我们的小组成员，发言人和
提前期短和航空旅行意外中断，促进者参与。[5]

研讨会概况

议程安排为一系列主持小组讨论和分组讨论，探讨
五个关键利益相关者社区的潜在贡献：通信基础设施
提供者；产品开发人员；客户；研究人员；和政府。除了提供
主题专门知识，小组旨在激发分组讨论
会话。分组讨论协调人被引导指导讨论，确定广泛的
特定利益相关者社区（如基础设施提供商，产品）的一系列选择
开发人员或网络所有者）以增强生态系统抵御自动化的弹性
分布式威胁。要求协调人推迟讨论其他特定方案
社区参加适当的会议，但讨论重点在于
鼓励不同利益相关者社区采取可能的行动。主持人是
指示分组讨论参与者不必就特定问题达成共识
选项，或为这些选项建立顺序或优先级。

诉讼分析与准备

NIST的国家网络安全卓越中心（NCCoE）提供了网络安全主题
问题专家（SMEs）担任分组讨论的抄写员并进行了初步
对收集到的投入进行技术分析。大约有787项贡献被归类为
十大类别；313个贡献也被归类为五种之一
正交次要类别。

[5秒]ee https://www.washingtonpost.com/news/dr-gridlock/wp/2017/07/10/hazmat-incident-at-air-traffic-control-center-delays-flights-around-the-washington-region/?utm_term=.d009260f400e.

主要类别为：

- 意识
- 业务挑战
- 产品开发和生命周期
- 生态系统的复杂性
- 消费者角色
- 治理
- 信息共享，协作和隐私
- 数据
- 指标
- 基础和新兴技术

抄写员根据分组讨论分组讨论会提出的讨论主题。
类别和汇总百分比。 787项贡献的分配
如下图1所示。将近一半的捐款被视为业务
挑战或治理问题。

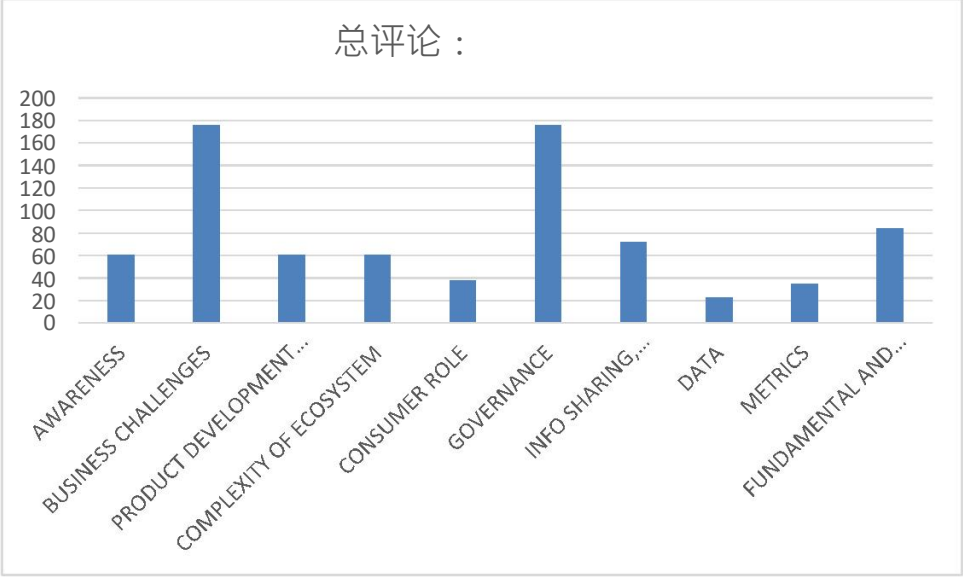

图1.抄写员表征的贡献分布

次要类别为：

- 对手
- 沟通
- 网络安全
- 经验教训和最佳实践
- 标准

抄写员根据分组讨论分组讨论会提出的讨论主题。
次要类别，汇总百分比。 313的分布
贡献见图2。超过一半的评论分配给未成年人
类别被视为网络安全问题，包括经验教训，沟通和
标准得到其余评论的大部分。

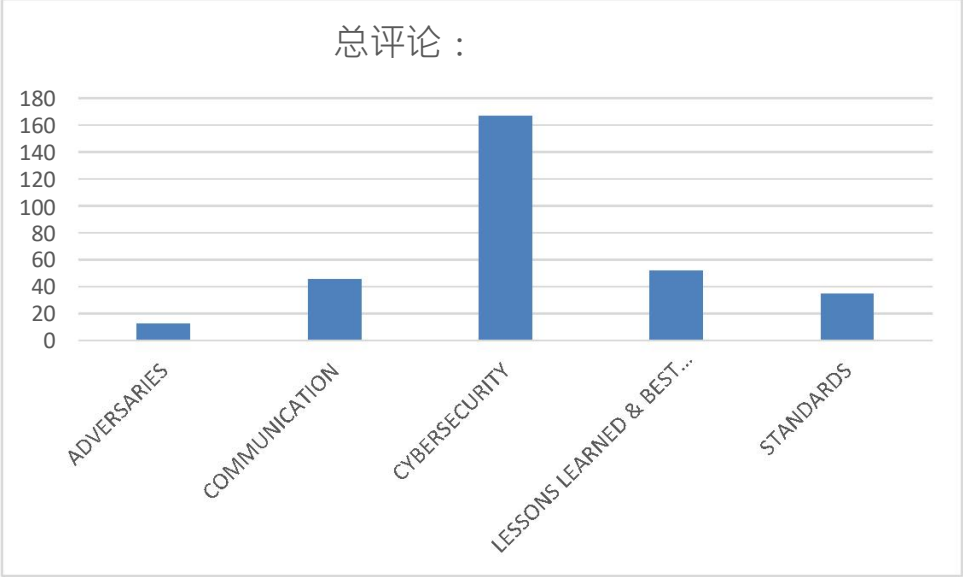

图2.按次要领域划分的文稿特征

NIST主题专家根据NCCoE提供的原始注释进行本程序
抄写员，抄写员准备的重点摘要项目符号列表以及NCCoE提供的分析，如下
以及NIST中小企业自己的个人笔记。

3.研讨会总结

本节总结了演讲者和研讨会参与者在会议期间提出的问题。
研讨会的课程，分为两个小节。

- 第一小节介绍了讨论中出现的六个总体主题。
  这些主题适用于多个行业，由不同的参与者提出
  多次。虽然尚无共识，也不应假定达成共识，但很少
  反对这些概念。

- 第二小节按行业分类（即针对利益相关方社区）
  问题和观察。在某些情况下，这代表了更详细的视图
  总体主题，但在另一些概念中，该概念仅是该领域独有的。的
  研讨会小组组织针对具体行业的观察。

虽然讲习班的范围涵盖了所有类型的自动化分布式威胁，但应
指出对话通常集中在物联网上。显然，Mirai
僵尸网络对于许多参与者而言是“首要考虑因素”，为以下主题的讨论提供了共享上下文
确保产品生命周期，培训和意识以及许多其他主题。物联网环境
仅在问题或意见针对的摘要中重申
物联网（与说明框架相反）。

如前所述，讲习班是根据《查塔姆议院规则》举行的，主持人
旨在集中精力采取行动，而不是达成共识或
获得客观的支持措施。本摘要使用了“多个参与者”一词。
“许多参与者”和“许多参与者”表示我们对
在正常基线以上增加支持或兴趣水平。

总体主题

在整个研讨会讨论中遇到了六个总体主题：[6]

1.问题的全球性质；
2.有效工具的可用性；
3.在整个生命周期中保护产品的重要性；
4.教育和认识差距的影响；
5.市场激励与复原力目标之间的冲突；和
6.需要采取协调一致的跨部门行动。

讲习班与会者反复指出，僵尸网络和分布式威胁是一个全球性问题。
尽管有例外，但构成僵尸网络的大多数被感染设备都是
地理位置位于美国境外。增强设备安全性的措施
在美国销售，或可抵御来自国内电信威胁的产品

6请注意，研讨会参与者不同意这些意见或确定优先重点。因此，六个主题的顺序为
不重要。

流量，只能解决部分问题。与国际伙伴的协调行动
将需要提高生态系统抵御这些威胁的能力。虽然分辨率
将需要采取全球方针，广泛达成共识，美国可以并且
应当以身作则并促进
适当的行为规范。

也有广泛的共识，即可以采取立即行动。引用
一位发言人说："我们不是从一张白纸开始。"通过套用一套完善的工具，
已知有效的工具，流程和实践，我们可以显着增强抵御能力
生态系统。这些工具已在个人计算领域证明了其价值。
但是，这些技术和流程未包含在产品的通用实践中
开发和部署在许多其他领域。一套或几套最低标准或
需要建立（尽管可能不是正式的）需求，以确保最佳实践
适用于所有行业。

使用这些工具，流程和实践应对整个产品/网络生命周期是
另一个总体主题。从一开始就构建安全的重要性
而不是将其附加到以后，是一种广泛认同的信念。运送的产品太多
已知漏洞；这些产品可能会在以下时间内被检测，攻击和破坏
分钟的部署。需要安全更新机制来解决漏洞
在正常产品生命周期内发现。明确有效的流程来解决末尾问题
还需要解决生活问题，因为无法解决过时产品中的漏洞，请确保
在渗透企业或建立企业时，对手有一个可靠的起点
僵尸网络。

与会者指出了系统的教育和意识问题。近6%的
研讨会分组会议上的建议/意见集中于
教育和认识。许多与会者列举了交通安全，安全带使用和
碰撞测试评级作为教育和知名度成功案例，带来了更好的结果。
其他人则把同一个行业作为一个警示故事，交货时间长，但不普及
接受安全带和其他技术改进。能源之星也是主题
重复讨论，为消费者提供简单指标。一个独立的测试机构
经常引用证明与安全相关的功能并提供更易访问的评分方案
作为向消费者识别具有强大安全功能的产品的重要一步。

知情人士认为，市场激励措施与我们的安全和弹性目标不符
许多研讨会的参与者。产品开发人员和供应商将成本和上市时间降至最低，
而不是构建安全性或提供有效的安全更新。许多讨论集中在
有关创建市场激励措施的技术，如独立产品认证，但有些
认为最终需要更积极的政府干预（例如，监管）
克服市场失灵。但是，与会代表指出，监管合规也可以达到ip
与我们的安全和弹性目标不符。[7]

7例如，一些与会者列举了卫生保健部门历史上不愿修补医疗设备以避免
由食品和药物管理局重新认证。请注意，目前的FDA指南解决了这个问题，
在某些情况下无需重新认证即可打补丁。请参阅"医疗网络安全的上市后管理

另一个主题是任何特定部门都无法影响生态系统的弹性。
孤立地。基础设施提供商可以提高抗分布式拒绝服务机制的效率，但
始终可以通过大量设备来克服它们。设备制造商可以改进
产品的质量，但我们没有构建完美产品所需的技术
产品，因此某些设备始终容易受到攻击。同样，企业所有者
可以增加其在安全方面的投资，但其中一些系统容易受到攻击，并且
攻击者可以利用整个互联网对企业发起攻击。研究人员可以
开发更好的技术，但只有供应商将这些技术包括在内，安全改进才能实现
产品中的技术，客户购买这些产品并适当部署。
将需要来自各部门的捐款，以大大提高灾后恢复能力。
针对僵尸网络和自动化分布式威胁的生态系统。

行业特定摘要

本节从每个角度回顾研讨会的问题和意见。
利益相关者社区反过来。在某些情况下，这代表了更详细或细微的变化
总体主题，但在另一些概念中，该概念只是该领域独有的。

基础设施

基础设施提供商部门是第一个研讨会小组的主题，其次是
分组讨论会话。小组讨论的重点是基础设施的现状，趋势和现状
和有希望的方法来缓解分布式分布式拒绝服务等自动化分布式威胁，
特别关注僵尸网络和物联网。

几位与会者指出，互联网基础设施如今的弹性更强，而且
几乎每天都能抵御以前无法想象的分布式拒绝服务攻击。这个
展示了当前工具的有效性以及分布式拒绝服务军备竞赛的本质
保护。

与会者明确确定了多种分布式拒绝服务保护工具和技术。这些是
下面列出了优缺点。 （演示文稿的顺序没有
意义。）

- 入口/出口过滤：许多参与者提到了互联网工程任务
  部队（IETF）最佳实践（BCP）38，“网络入口过滤”，以及BCP 84，
  “多归属网络的入口过滤。”从历史上看，分布式拒绝服务攻击一直依靠
  网络地址欺骗，其中受感染的系统断言源地址esses
  来隐藏攻击者资源的位置，在本地网络上不存在。[8]
  在企业边界进行过滤并丢弃明显非法的流量，这是
  可能会限制这些攻击的有效性和范围。

设备”，
https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

8最近的一些分布式拒绝服务攻击（例如Mirai）断言合法源地址。

BCP 38和BCP 84分别于2000年和2004年发布，但采用和发布
部署缓慢且不平衡。虽然目前的支持水平在
在研讨会上，普遍支持流量过滤
用于边缘网络。简短讨论了过滤器内部的局限性
互联网骨干网，不对称路由（两个端点之间的流量
沿每个方向遵循不同的路径）使合法流量的区分变得复杂
从欺骗的网络地址。

- 场外分布式拒绝服务保护服务：互联网服务提供商提供场外分布式拒绝服务保护
  为客户提供的服务，在将流量传递到网站之前重新路由和过滤流量
  客户网络。分布式拒绝服务保护服务需要额外配置
  吸收和处理资源的资源（根据专用系统和额外带宽）
  预计会有更多流量。事实证明，这些服务在许多情况下都是有效的，但
  服务提供商不断被迫增加额外资源的水平，因为
  僵尸网络越来越大，攻击的总带宽也越来越大。

  这些服务的有效性在一定程度上受到客户认知度的限制。分布式拒绝服务
  保护服务需要配置大量额外资源（
  专用系统和额外带宽），因此基本网络中不包含这些功能
  服务产品。客户可能不知道分布式拒绝服务攻击带来的风险
  直到成为受害者为止，或者这些服务甚至可用。即使在
  企业了解并渴望购买反分布式拒绝服务，架构
  可能需要进行更改以优化达到的安全级别。

  （注意：客户与服务提供商之间的通信代表了另一种
  挑战非本地分布式拒绝服务保护服务的有效性。查看实时
  信号，如下）。

- 本地分布式拒绝服务保护：针对企业企业量身定制的分布式拒绝服务攻击
  关键资源，如关键应用程序或公司防火墙，本地保护
  机制可能更有效。这些"本地"服务现在可以作为
  传统服务提供商（场外）分布式拒绝服务保护服务的补充
  由ISP提供。如上所述，客户对风险和可用技术的意识是
  通过这些技术增强复原力的先决条件。

- 实时信令：如上所述，与分布式拒绝服务保护服务和
  设备在攻击期间可能会出现问题。几位与会者强调了互联网
  工程任务组的分布式拒绝服务开放威胁信令（DOTS）工作组为
  在不久的将来有望成为解决方案的来源。 DOTS目前正在开发一套
  分布式拒绝服务相关遥测和威胁处理实时信令标准
  通过可能被攻击流量阻塞的链接发出请求。

与会者还强调了基于基础设施的方法面临的一些具体挑战
增强生态系统的弹性。

- 全球协调：威胁也是互联网的全球基础设施。
  基于基础设施的方法要求密切合作与协调。参加者

表示，国内同行之间的合作已相当稳健，但
国际交流与合作不平衡。有努力
建立规范和规范做法，但这些努力滞后了问题。

与会代表指出，近五十家公司已同意共同商定的规范
路由安全（MANRS），并且可以将此协议视为
针对僵尸网络的努力。其他人指出了《美国互联网反机器人行为守则》
联邦通信开发的服务提供商（ISP的ABC）
Commissio的通信安全，可靠性和互操作性委员会n
（以下简称“ CSRIC”）。[9]

- 复杂性：基础设施问题日益复杂。
  互联网–不仅是物联网的到来，而且还扩展了多租户基础设施。
  尚未广泛应用到PC和服务器的标准和实践
  统一应用于物联网领域，带来不幸的后果，较小的互联网服务提供商
  没有能力实施与大型ISP相同的标准和实践。
  即使企业了解并渴望购买抗分布式拒绝服务，
  可能需要进行体系结构更改，以优化实现的安全级别。

- 指标：缺乏用于表征攻击并记录其严重性的可用指标。
  一位与会者指出，联邦调查局已经制定了75
  属性框架描述分布式攻击，但需要完成描述
  花费了这么长时间，攻击往往结束了。可用和广泛认可的指标是
  需要促进协调与合作。

- 相互依存：与会人员注意到与其他部门的一系列依存关系。较差
  边缘设备（尤其是物联网设备）的安全属性使其变得极为重要
  基础设施很难抵御这些攻击。

- 教育和意识：迫切需要客户的教育和意识；什么时候
  互联网服务提供商（ISP）联系企业以提醒他们出现问题，企业通常设备不足
  理解问题或履行职责。他们通常认为
  互联网服务提供商“将处理”，无论“可能”如何。

- 对业务人员的教育和认识也被认为是有问题的。在
  特别是，一些人认为，BCP 38过滤在国外互联网服务提供商中的部署较弱，规模较小
  家用ISP和企业维护的BGP路由器在很大程度上是技能差距的结果
  这些组织内部。

产品制造商

第二个小组讨论会探讨了当前的努力和未来的机会

9美国通信安全可靠性和互操作性理事会（CSRIC）第三版，
互联网服务提供商（ISPs），第7工作组最终报告（2012年3月），
http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-Report.pdf

网络组件和设备制造商（包括物联网解决方案提供商）来解决
近期僵尸网络的根本原因（不受限制的网络访问，硬编码密码和越野车
软件）。讨论包括为企业和家庭开发的产品。

产品开发问题有两个大致特征。最
普遍表征表明产品中的漏洞数量必须为
显着降低了攻击能力，使其更难以大规模入侵设备并发起大规模攻击。
另一方面，产品将永远不会完美，因此一些参与者认为我们应该
专注于限制受到损坏设备损害的技术。两者
表征并没有冲突，而且大多数人似乎都认为应该采用两种方法。

关于使系统难以妥协的问题，许多与会者强调说，
是产品生命周期的问题。他们认为，至关重要的是管理以下漏洞：
设备，从最初的产品发货，使用到报废。许多技术可以
降低产品漏洞的讨论：

- 为减少初始部署产品中的漏洞，与会人员建议
  越来越多地应用一些辅助工具和最佳实践。对于
  例如，按设计开发流程进行安全保护很可能导致违约
  设置通常是安全的，避免使用硬编码的管理密码和
  其他常见陷阱。安全敏感的软件开发工具链可以消除
  常见的编码错误，例如大多数缓冲区溢出。

- 即使使用按设计安全方法开发且注重安全
  工具链，很可能会检测到软件漏洞，持续几个月或
  首次部署产品后数年。针对这些漏洞的恶意软件通常为
  检测后数天或数周可广泛获得。管理这些漏洞
  产品，许多参与者断言，安全更新（最好是自动更新）
  绝对必要。此外，他们断言制造商应承诺
  在部署后的最短时间内修补安全漏洞。

- 信任根是一项互补技术，被众多参与者引用。
  通过提供一组基本且高度信任的功能，我们可以增强对以下方面的保证：
  软件和固件不变或仅通过安全更新进行了更改
  机制。可信平台模块（TPM）是一个广泛可用的示例，但
  对于廉价设备而言可能成本太高。新的努力，如可信计算
  组（TCG）设备身份合成引擎（DICE）可能会扩展
  结合了这些技术的产品，为设备标识和
  验证是否已安装软件更新。设备需要由
  制造商，因此有一种方法可以知道设备类型和配置，
  软件和补丁程序仅用于设备。 NIST SP 800-193出版物草案
  2017年5月30日开始描述保护，检测和恢复的信任根
  可以作为远程恢复设备的构建块应用于物联网领域。人
  不太可能单独管理IoT设备，因此需要自动恢复。

- 生命周期终止问题和未许可软件：与会人员还强调了
  制造商不支持的设备相关的漏洞。在

在这种情况下，更新不再发布（或也许从未发布），因此
漏洞会无限期存在。这与未经许可的软件具有相似之处，其中
安全更新通常不可用。

与会人员称赞微软为缓解Windows XP更新Windows XP的决定。
WannaCry漏洞利用，尽管在三年前就终止了支持，但他认为这是一个
特殊情况。与会者考虑了过去的报废一般解决方案建议
问题，例如将不受支持的产品的软件发布到开源
社区，不切实际。

与会者指出，以上技术众所周知且众所周知。他们是
广泛应用于某些行业（如操作系统），但几乎从未应用于其他行业（如
物联网）。建议了一些障碍和根本原因，包括：

- 消费者教育和意识：产品制造商受销售激励，
  消费者没有优先考虑安全优先级所需的观点或能力
  确定具有更高保证的产品。消费者可能并非出于自然动机
  选择此类产品，因为受到危害的产品通常会继续发挥作用
  它们在参与分布式攻击时的既定功能。消费者教育应
  专注于潜在的安全隐患和性能影响，而非僵尸网络
  预防–用户可能并不在乎保姆对大型银行的攻击，但他们会在意
  关于陌生人侵犯家人隐私的信息。

  一旦获得激励，消费者仍将需要帮助来选择可能会
  在整个部署生命周期中具有较少的漏洞。没有令人满意的机制
  向消费者传达有关产品安全的信息的方法已经存在。
  能源之星，能源效率和国家公路交通安全
  政府（NHTSA）对车辆安全的五星级安全评级被评为
  重要而成功的例子。

- 产品开发人员的教育和意识：介于 和传统之间
  产品线模糊，向产品开发人员宣传安全性已迫在眉睫
  需要。家用电器设计师了解如何确保食品安全
  温度，干净的织物或吐司面包。随着这些产品成为
  生态系统，我们要求这些设计人员纳入新的安全要求，
  对他们来说是陌生的。特别是，行业需要认识到安全更新
  机制是“一切”的要求。

- 与市场激励措施不一致：许多产品开发人员担心投资
  安全性将使其产品更昂贵，并延迟创新产品的推出
  建立市场份额的新功能。较大的供应商发展更强劲
  流程，但初创公司和小型公司通常依赖不太成熟的流程。

- 责任不明确：还讨论了责任 谁
  应该对产品的安全负责？业主？供应商？对于家庭用户
  小型企业，要让他们承担家庭硬盘录像机或
  便利店中的安全摄像头已经遭到破坏，并添加到了僵尸网络中。对于

工业用户，也许可以有更高的期望，但随着物联网设备的增长
那里也可能有限制。在这两种环境中，诸如
制造商的使用说明（MUD，请参阅下面的虚拟网络分段）
可能有助于以扩展方式将部分责任转移给制造商。

第二种观点是，产品永远不会是完美的，而激励措施就不会完美。
专注于安全性。这强化了以下观点：安全更新是基础安全
要求，但我们还需要找到方法来限制受损设备造成的损失。
提出了一些前进方向，包括：

- 虚拟网络分段：从历史上看，互联系统享有盛誉t-co
  网络和传输层完全连接。人类用户的需求是[10]
  不可预测，因此严重限制流量将难以管理。安全性
  完全连接的含义非常重要：互联网上的任何设备都可以用来
  在任何其他设备上发起攻击；一旦受到威胁，设备就会启动
  企业内部横向移动和其他互联网攻击的防护垫-
  连接的设备。随着物联网（IoT）通信的出现
  许多设备的需求变得更加可预测，充分安全性对安全的影响
  连接不可接受。例如，物联网恒温器可能需要进行通信
  与制造商的网站进行更新，但可能不需要通信
  与证券交易所。

  IETF目前正在开发的MUD标准提供了一条潜在途径
  向前。当设备加入网络时，它们会通过动态请求IP地址。
  主机配置协议（DHCP）。使用MUD时，设备还会指示
  安全地从以下位置获取设备通信要求的描述：
  制造商。网络设备供应商利用MUD文件和现有文件
  能够对每个设备实施数据包过滤的功能。如果受到威胁，攻击者
  无法使用IoT恒温器横向移动咖啡壶或攻击机器人
  股票交易所。

- 威胁信令提供了一种替代方法来限制网络访问。第三
  第三方服务识别对主机构成相对威胁的主机系统或域
  生态系统（或某些行业）。该信息传递给订阅
  企业网络，建立适当的路由过滤器并可能丢弃
  有害流量。虽然MUD专为支持定义明确的设备而量身定制
  通信需求，威胁信号增强个人安全
  具有用户驱动（和不可预测）通信需求的计算设备。

客户：企业，家庭用户和政府

第三小组讨论会探讨了客户（尤其是企业客户）如何实现
两者都可以保护自己免受分布式攻击（包括分布式拒绝服务），

10稍后，网络管理员可以通过跨企业应用的防火墙规则限制访问，但存在
企业内部通常没有限制。

应用程序和欺诈行为，并避免成为问题的一部分。要求参与者突出显示
当前最佳实践和新兴技术的能力和局限性，并考虑
跨部门合作的潜力。

许多参与者将客户分为三大类：家庭用户；企业；和
政府。在一些讨论中，企业在规模上进一步区分-或大或小
与中小型企业（SMBs）或初创企业与成熟公司的竞争。
参与者对不同类别的客户有不同的期望
意识，最佳实践，技术适用性和协作。

参与者确定了一些当前和新兴的最佳实践：

- 如前所述，许多参与者确定了所有网络设备的安全更新，
  包括适当的更新机制和供应商承诺提供
  补丁程序，这是当前最重要的最佳实践。“适当的”细节
  更新机制取决于目标客户。例如，参与者
  建议家庭用户仅在以下情况下受益于安全更新：
  自动无人值守。大型企业需要更高级别的控制
  通过集中管理工具。中小企业的需求和期望可能会有所不同
  取决于网络架构和专业知识。

- 实时信息共享被认为是政府的最佳实践
  和大型企业。在企业内部和整个企业之间共享信息
  生态系统，将使企业更好地保护资源。与会者观察到
  恶意行为者在这方面比我们做得更好。

  但是，信息必须以可操作的形式共享，而不是未经格式化
  文字。当前，有多种解决方案可用于一般网络安全
  信息共享。与会者尤其明确了结构化威胁
  信息表达（STIX™）和可信的指标自动交换
  信息（TAXII™）为当前最佳实践。分布式拒绝服务开放威胁信令
  IETF当前正在开发的（DOTS）标准将提供特定于分布式拒绝服务的方式
  解决方案。

- 限制流量的网络架构，以限制潜在的攻击手段和
  还讨论了可以从受感染系统发起的约束攻击。
  建立虚拟分段网络的新兴技术，如MUD
  协议（请参见上面的产品制造商）将向
  家庭和企业网络以可扩展的方式。对于旧设备，网络
  设备可以利用“威胁信号”（例如，信息共享来识别本地
  受感染的系统和可疑的外部系统或域）并限制流量
  适当地。

由于许多必要技术被广泛理解，因此进行了重要讨论。
致力于发现阻碍采用的潜在障碍。

- 人们广泛辩论了网络保险当前和潜在的影响。经验其他行业的研究表明，保险可以推动技术的采用。对于例如，鼓励为防抱死制动系统和安全气囊提供汽车保险折扣消费者优先考虑这些功能。建筑物保险往往需要烟检测器，并可能为洒水装置或其他有效措施提供折扣。但是，网络保险产品通常不一致，被认为只有很少量产品迄今为止对网络安全技术部署的影响。

- 一些参与者建议，需要更多的精算数据才能肯定影响市场。一旦获得数据以施加统一要求并提供折扣优惠，网络保险可能会对企业产生积极影响业主。

- 教育和意识是一个系统性问题，特别对于中小型企业和家庭用户而言。开平均而言，政府和大型企业应该有很高的意识对安全要求有较深的了解，以支持产品选择和实施最佳实践。另一方面，国家网络安全池专家不足以将这些期望强加给中小型企业，家庭用户不能有望成为网络安全专家。

  在淹没信息的同时，客户无法区分蛇油和有效技术。例如，一位参与者收到了32封有关产品的电子邮件声称在发动攻击的第二天防御WannaCry。很少客户将有能力评估其索赔，因此大多数客户不采取任何行动。

  为促进生产性采购和部署决策，客户需要可访问数据。与会者强调了产品认证的重要性。辩论了各种认证制度的影响。 NHTSA 5星级安全评级和美国能源部能源之星记分卡被列为包装认证示例数据以无障碍形式提供。与会者对正在进行的倡议充满希望保险商实验室和消费者报告，尽管这些努力的标准尚不清楚。 NCCoE的示范项目及其相关实践指南提供另一个有希望的选择。

- 与会者对严格自愿的可能性持多种看法领养。尽管所有与会者均表示倾向于自愿措施，但仍有担心采用缓慢会迫使政府介入，特别是在某些部门已经受到监管。在州一级制定法规的前景尤其明显与参与者有关。 50套略有不同的规定的可能性将会适得其反，使产品和服务的提供复杂化。但是，对政府实体本身增加了要求，经常建议以身作则，树立初步市场。

- 明确法规（如果已实施）对于避免突发事件至关重要后果。当被迫推断时，通常会想到监管障碍或阻止实施适当的安全机制。

- 与会者还对成本表示担忧。没有政府激励，成本增强网络安全性必须传递给消费者。在全球经济中环境，在国内实施要求可能会阻碍企业的竞争力国外业务。

总而言之，与会人员一致认为，家庭用户和家庭用户之前必须进行文化变革。美国企业对生态系统复原力的贡献最大。

研究与学术界

研讨会的第二天从"研究方向"面板开始，主题是当天晚些时候，这也是唯一的第2天分组讨论的一部分。这些目标讨论旨在确定和探索在提供网络弹性方面的差距领域，并强调解决这些差距的机会。

参与者确定了可能对研究产生积极影响的广泛研究方向。生态系统的复原力，包括：

- 指标和分类：自动化指标和分类方法分布式威胁可以提高缓解风险和法律资源的优先级执法行动。

- 僵尸网络分布式拒绝服务建模：针对僵尸网络和其他自动化威胁的鲁棒模型包括检测，传递数据和强制实施可以使更全面和协调的响应。

- 恶意行为者行为：分布式拒绝服务行为者行为的变化将对目前许多技术的功效。这些变化包括国家国有化黑手党和网络犯罪组织；从"被盗资源"到"犯罪"的转变基础设施"；以及从用户驱动流量向自动化系统/ IoT的转变。需要预测这些变化对当前的反分布式拒绝服务技术的影响。

- 社会技术问题：弹性就像网络安全的许多方面一样，具有社会影响力。尺寸，不能仅靠技术解决。与会者重点介绍研究方法必须考虑人，社会，组织，经济和技术因素，以及对部署和运营的影响弹性基础设施。人机界面（见下文）是一个特别的重点。还需要研究以了解如何设计更具弹性的组织面对网络攻击，更高效地进行事件或灾难恢复流程。

- 人机界面：鉴于我们的员工面临网络安全挑战，迫切需要改进人机界面。关系运营技术（如SCADA组件）及其运营商之间特别感兴趣。自动化可能会带来许多安全优势，但运营商在信任之前需要提高算法的透明度机器决策。

家庭用户提出了另一个机器接口挑战。根据用户行为进行设计，而不是假设不可能的改变，可以提高当前技术的效率。

- 机器学习人工智能（）：机器学习和人工智能技术可能为早期发现和适应压力（包括分布式）提供新途径威胁。有关机器决策，假设情景建模的其他研究，以及使用大数据（来自网络和系统传感器）建立正常基准可能为生态系统的复原力做出贡献。

- 归因：计算机安全事件的归因有问题，可以说是有争议的僵尸网络和分布式威胁的难度更大。识别恶意行为者和受到攻击的系统将为缓解攻击做出积极贡献，并且采取能够阻止后续行为者的执法行动。

- 功效证据：与计算机安全其他方面一样，工具和需要有效的技术来证明持续投资的合理性。

- 补救措施：检测到侵害后，用户通常会面临令人不快的选择：尝试清洁系统；或丢弃设备。经常清洁系统不可靠补救过程可能很复杂，并且持续存在高级威胁（APT）旨在在修复中生存。丢弃设备昂贵且昂贵在大多数情况下不切实际。简化修复工作，提高可靠性的研究用户可以在发现危害后澄清这些选择并提高弹性。

- 设计网络以增强弹性：网络设计会影响弹性并限制分布式拒绝服务机制的选项。研究网络设计以最大化需要弹性和保留选项。

- 关于网络弹性的最新研究大多集中在提高对网络弹性的可见性边缘网络，但可能存在利用新传感器并建立互联网的机会“更智能”的核心。为实现这些下一代架构，需要进行研究标识传感器的类型，放置位置以及应提供的信息与谁共享。

与会者还指出，以研究为重点的旨在增强抵御能力的努力有若干障碍网络网络，包括：

- 教育和意识：介绍物理，化学和其他科学领域一般而言，在美国的教育系统中，计算机科学比计算机科学要早得多，尤其是网络安全。延迟接触田野限制了兴趣，因为许多学生在上大学之前已经确定了一个研究领域。吸引更多的优秀和最聪明的人可能会对整体知识产权产生连锁反应。

- 缺乏货币资源：公共预算和研究预算都在缩减私营部门。国家科学基金会承销了领域的基础研究和应用研究，但可用资金总额不足资助所有有前途的研究工作。

政府与公共政策

第2天的第二个小组讨论了增强弹性的政府和公共政策选择
生态系统。作为研究的一部分，还讨论了该主题以及研究方向。
第2天分组讨论当天下午晚些时候。

与其他部门一样，与会人员指出，政府和政府部门正在开展许多活动。
公共政策已经在实施，以增强生态系统的弹性，其中包括：

- 执法行动：各级执法机构正在采取更多行动
  网络安全相关犯罪，包括涉及自动分布式威胁的犯罪。在
  与会者特别指出，联邦调查局已删除了
  近年来引人注目的僵尸网络数量。这些成功为
  未来的案例并创造威慑措施。

- 监管执行：监管机构正在制定和实施以下政策：
  传统意义上的网络安全。例如，食品和药品
  政府已建立了与基本设备脱钩的医疗设备指南
  现有产品认证制度和联邦贸易的安全更新
  欧盟委员会（FTC）已针对众多与隐私和安全相关的案件采取了行动。物联网
  设备已经采取了一些强制措施。

- 政策举措：物联网设备的隐私和数据安全问题一直是关注的焦点
  多个部门和机构的政策举措。 FTC的IoT研讨会系列
  专注于特定的物联网设备（如无人机，智能电视）和FTC公众
  竞赛“ IoT家庭检查专员挑战赛”是长期以来的两个突出例子
  活动列表。

- 教育和意识：联邦政府正在努力缩小教育差距
  在全国范围内，通过《国家网络安全教育倡议》，
  其中包括许多政府机构。监管机构是独立的
  开展补充教育活动，如发布指南和博客
  面向利益相关者的职位。

- 国际协调与合作：其他国家政府也在响应
  对生态系统的自动化分布式威胁，并且正在向传统威胁扩展
  合作伙伴和盟友协调和交换信息。

与其他部门一样，这些努力也是巨大的，但需要做出更多努力以缓解不断发展的趋势
威胁。参与者确定了几种不同的媒介来推动政府影响灾后恢复力。
网络，包括：

- 采购：尽管认识到联邦政府的购买力已不再
  与会者鼓励信息技术市场的主导力量
  政府与明确指定的技术配合使用钱包的权力
  要求，迈向关键目标并引领私营部门。例如，通过
  要求供应商支持自动化安全更新，政府可能会增加

联邦政府拥有和管理的生态系统组成部分的弹性；以及
扩大针对以安全为重点的私营部门实体的可用选项范围。

- 基础研究：参与者指出，联邦政府仍然是主要政府
大多数科学学科基础研究的资金来源。行业是
可以理解，重点放在后期研发上，因此联邦政府必须确保
资金既充足又有针对性。

- 国际合作与协调：如前所述，生态系统是全球性的，
要有效应对分布式威胁，需要以下各方的合作：
与非美国服务提供商，制造商和企业用户进行协调。在一些
在这种情况下，这些实体与民族国家紧密相连。联邦政府是
在促进和促进与此类合作和协调方面的独特定位
实体。

- 执法：执法部门拆除僵尸网络并缓解僵尸网络
威胁得到了参与者的广泛支持。谨慎支持审核和
修改了阻碍起诉的政策，并提出了警告
必须在执法关注与隐私和财产权之间取得平衡。

- 建立市场激励措施：几位与会者确定了文件草案
沟通IoT设备安全更新功能，提高透明性
消费者，是通过NTIA的多利益相关方流程在物联网上开发的
安全升级补丁程序，例如可能产生市场激励措施的示例y a
用于安全升级。[11]

- 监管和市场激励措施：与广泛竞争相比，参与者更喜欢市场激励措施
监管举措，但对过去的市场失灵表示一定程度的悲观情绪。
与会代表指出，当前受监管的新的以网络安全为中心的法规
如果仔细考虑，行业可能会适当，并产生积极影响。医疗
设备被强调为此类行业之一，FDA最近的声明
关于修补的说明被认为是周到且平衡的监管示例。
规章制度也可能通过澄清责任和问责制产生积极影响
在产品生命周期或事件响应流程的不同阶段。

    - 有人建议遵循国际劳工组织所采用的模型
    电信联盟–无线电部门（ITU-R），用于管理无线电频谱
    在国际上可能是确定如何开展合作的好方法
    国际网络空间。

11有关文件草案，请参阅
https://www.ntia.doc.gov/files/ntia/publications/draft_communicating_iot_security_update_capability_-_jul_14_2017_-_ntia_multistakeholder_process.pdf. 有关由NTIA领导的物联网工作的更多信息，请参阅
https://www.ntia.doc.gov/category/internet-things.

- 教育和意识：已经有很多防御性网络安全指南可用，未知或被忽略。也许应该更多地强调关于更普遍地实施基本保护的问题。
    - 如果我们要依靠消费者来处理网络安全，则需要比现在提供的更早，更轻松，提供更多的教育，帮助人们理解网络安全的模型。
- 简化补救措施：也许政府可以做更多工作来简化补救措施违反后。公民可以从违规中获得帮助吗？更容易通知个人和组织新帐户正在建立和使用中帐户无效。
- 建立指导：与会人员建议，总体而言，联邦政府，尤其是NIST，可以通过其他指导来支持行业自愿行动。许多参与者列举了NIST用于开发改善关键基础设施网络安全的框架（网络安全）框架），作为达成有用和可接受指导的共识模型。参与者明确建议扩展网络安全框架以解决ici物联网。[12]
- 以身作则：与会者指出，最近僵尸网络中使用的设备相对较少位于美国的，验证国内安全方法。这个成功的故事很大程度上是被忽略，无法复制。为美国境外人士提供激励措施安全措施，我们必须证明自己的成功，然后在国际上进行宣传，分享我们的解决方案。通过这一成功，我们作为一个社区可以说服权利人们采取行动并做出网络安全支出决策。
- 激励非市场行为：从互联网服务提供商的角度来看，存在相关成本某些任务会增加网络的弹性，但不能直接受益客户还是ISP。（隔离和通知客户被认为是例如。）政府可以通过提供资金来激励这些非市场行为或以其他方式允许企业收回成本。

12将CSF扩展到物联网很可能需要制定物联网行业概况，就像CSRIC IV为通信部门。参见CSRIC IV，《网络安全风险管理和最佳实践》，最终报告，第4工作组（3月。2015），https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf。

4.结论与启示

13800号行政命令指示商务和国土安全部
向总统提交报告，“酌情确定和促进采取行动
利益相关者，以提高互联网和通信生态系统的弹性，并
鼓励协作，以期大幅减少自动化威胁
和分布式攻击（例如僵尸网络）。”

研讨会提供了重要的意见，以及NTIA征求意见稿和
NSTAC报告将为报告草案的制定提供信息。一月份的影响
报告包括：

- 报告中建议的行动将涉及从中收集的每个总体主题
  讲习班的参与者。

- 报告将为每个利益相关者建议一项或多项建议的行动
  组（即基础设施提供商，产品开发人员，企业，家庭用户，
  学术界和政府）。

- 非政府利益相关者期望联邦政府以身作则，
  通过激励而非监管促进其他利益相关方的行动。

- 许多行动都依赖于分配给其他利益相关者的行动，因此
  报告中还需要确定协作机制。

- 建议可能包括立即采取行动以提高认识和
  部署当前可用技术，中期行动创造市场
  激励措施（尤其是确保整个产品生命周期的安全）并促进国际竞争
  协调与协作，以及开发新技术的长期行动。

5.下一步合作的机会和机会

在发布本报告的同时，NTIA将发布声明摘要a
提交以回应2017年6月的征求意见稿。[13]
安全部门将根据向公众提供的反馈意见，开始编写报告
日期，包括收到的其他投入。同时，NSTAC将继续致力于
报告将于2017年10月31日发布。

欢迎就此主题做出更多公共贡献，并可以提交给
distributed.threats@nist.gov. 2017年10月15日之前提交的评论将被视为
包括在初步报告中，并将在或之前与社区共享
2018年1月5日。

公众意见征询和对初步报告的意见将持续到2月
2018年5月5日。意见征询期结束后，将于2月在
讨论计划中的评论解决方案。根据举行的公众评论和讨论
在讲习班上，各部门将完成报告，于或提交主席。
在2018年5月11日之前。

[13秒]ee https://www.ntia.doc.gov/federal-register-notice/2017/report-responses-ntia-s-request-comments-promoting-stakeholder-action

议程

以下页面介绍了研讨会之前发布的研讨会公共议程。

“日常”议程有两项更改：Arbor Networks的Carlos Morales参加了
代表阿拉贝拉·哈灵顿（Arabella Harrington）成立的首个小组（通信基础设施）；和克雷格
思科的Hyps代替Eric Wenger参加了第二个小组（产品）。

增强互联网和通信生态系统的弹性

NIST国家网络安全卓越中心，马里兰州罗克维尔

2017年7月11-12日

研讨会的目的：研讨会的目的是探索一系列当前和新兴的
解决方案，增强互联网抵御自动化分布式威胁的弹性，例如
僵尸网络。部署这些解决方案将取决于各方的能力和意愿。
采取行动。根据具体解决方案，基础设施提供商可能需要采取措施，
设备制造商，系统和网络所有者，研究社区，政府和/或
标准开发人员。 NIST通过探索广泛参与者的解决方案空间，
希望为各方寻找有希望的途径，以增强互联网的弹性。

讲习班输出：NIST将产生一份讲习班会议记录文件，总结会议情况
讨论，捕获发现并确定下一步机会。该讲习班的产出将
还可作为与第13800号行政命令相关的实施活动的投入
联邦网络和关键基础设施的网络安全。

议程

2017年7月11日星期二

7:30	**注册人签到**
8:30	**欢迎和研讨会概述**
8:45	**搭建舞台** *本次全体会议将总结问题空间（例如僵尸网络生态系统），确定* *利益相关者（标准/协议开发商，基础设施提供商，消费者，* *（制造商，监管机构）缓解僵尸网络，并回顾过去的方法和产出。* **阿里·施瓦兹（Ari Schwartz），维纳布尔**
9:30	**基础设施提供商的观点：现行和新兴标准，最佳实践，与技术（小组1）** *本次全体会议将探讨目前的努力和未来的机会，以增强* *基础设施（例如互联网）的弹性。该小组将讨论当前状态，* *趋势，以及减轻自动化分布式威胁的当前可行方法* *例如DDOS，尤其是僵尸网络和物联网。* **Russ Housley，警戒安全（主持人）** **理查德·巴恩斯（Richard Barnes），思科** **阿拉贝拉·哈拉韦尔，阿尔伯网络** **威瑞信丹尼·麦克弗森** **AT&T的Brian Rexroad**

10:15	**休息**
10:30	**会话1分组讨论（已分配）**
12:00	**午餐**
1:00	**产品开发（面板2）** *本次全体会议将探讨网络目前的努力和未来的机会* *组件和设备制造商（包括物联网解决方案提供商）解决根源* *近期僵尸网络的原因（不受限制的网络访问，硬编码密码和越野车* *软件）。会话范围包括企业和家庭使用。* **Yolonda Smith，Pwnie Express（主持人）** **Anura S. Fernando，保险商实验室** **赛门铁克杰夫·格林** **微软Rob Spiger** **思科Eric Wenger**
1:45	**第2部分分组讨论（已分配）**
3:00	**休息**
3:15	**客户观点：当前方法（小组3）** *本次全体会议将探讨互联网用户（尤其是企业用户）如何能够* *保护自己，避免成为问题的一部分。小组成员将以* *概述企业可能面临的分布式攻击挑战，包括* *分布式拒绝服务，网络应用程序和欺诈。讨论将突出功能和局限性* *最佳实践和新兴技术的研究，以及跨行业的潜力* *合作。* **波士顿咨询集团Nadya Bartol（主持人）** **史蒂夫·柯伦（Steve Curren），卫生与安全准备与响应助理部长办公室** **马特·埃格斯（Matt Eggers），美国商会** **国土安全部NCCIC的US-CERT副主任Bradley Nix** **斯宾塞·威尔科克斯，埃克塞隆**
4:00	**会议3分组讨论（已分配）**
5:00	**休会第1天**

2017年7月12日

7:30	**注册人签到**
8:30	**欢迎辞和开幕辞**
8:45	**研究方向** *该小组将确定和探索缓解僵尸网络方法的空白领域，以及强调解决这些差距的机会。* **Pat Muoio，网络技术咨询（主持人）** **大卫·达贡（David Tech）** **大学Keith Marzullo。的医学博士** **Phil Reitinger，全球网络联盟**
9:30	**政府角色** *本次全体会议将讨论各国政府目前的努力和未来机会增强基础设施的弹性，其中可能包括政策和法规方式，激励措施和市场激励因素，经济影响和国际注意事项。* **NEC Grace Koh（主持人）** **FTC安迪·阿里亚斯（Andi Arias）** **联邦调查局汤姆·格赫特** **约翰尼科尔森（John Nicholson），英国大使馆** **Malhah（Mikki）Smith，HHS / ONC**
10:15	**休息**
10:30	**研究与政府角色突破**
11:15	**休息**
11:30	**第一天分组讨论摘要**
12:00	**公开讨论**
12:30	**结束语和后续步骤（DOC / DHS）**
12:45	**休会**