总统的
国家安全电信咨询委员会

NSTAC就网络安全Moonshot向总统报告

十一月14，2018

目录

“到2028年，确保互联网安全可靠，确保政府正常运行，并为美国人民提供关键服务。”

美国正处于一个拐点，同时面临日益恶化的网络安全威胁环境，以及对公共安全，经济繁荣和整体生活方式至关重要的互联网技术的依赖性日益增强。现在，我们的国家安全与网络安全紧密相关。因此，国家必须在过去的努力和当前的战略基础上抓住机遇，从战略上从被动的，渐进的，渐进的网络安全态势转向主动采取的方法，大胆地确保全体美国人的数字信任，安全和弹性。要实现这一大胆的成果，需要长期的强有力的国家领导，政治意愿和持续的整个国家投资。
美国政府可以立即采取行动，为国家长期共享网络安全愿景奠定基础，同时产生近期利益，确保持续的技术全球领导地位。

领导力必须以雄心勃勃的雄心勃勃的战略意图宣言开头，因为美国历史上在面对生存挑战时只做过几次。总统国家安全电信咨询委员会（NSTAC）认为，网络安全是21世纪最大的挑战之一，而美国作为国家战略迫切需要持久解决。为了传达这一点，
行政管理最高层必须发出清晰的志向和鼓舞人心的愿景，作为推动国家活动的力量。它必须宣布一项国家战略意图：到2028年确保互联网安全，保障政府的运转和向美国人民提供的关键服务。这种追求将确保社会对数字基础设施的信任，增强经济活力，并巩固美国创新领导地位。

> “我相信我们拥有必要的所有资源和人才。但事实上，我们从未制定过此类领导所需的国家决策或封送国家资源。我们从未在紧急时间表上确定长期目标。或管理我们的资源和时间，以确保其实现。”
>
> -肯尼迪总统在1961年5月25日举行的国会联席会议上的讲话

NSTAC采用了“网络安全Moonshot”（以“国家航空航天”命名）来描述这种方法
政府（NASA）阿波罗计划在约翰·肯尼迪总统于1961年5月在国会联席会议上致辞后，将一名男子送上月球。最初的面向月亮的集体国家行动旨在实现一个雄心勃勃的目标，将人类放到月球上，并在该十年末安全返回地球。重要的是，肯尼迪总统显然
明确说明了这一最终目标，但并未说明实现该成果所需的许多个人创新和行动。

然而，肯尼迪总统的月球愿景与预期的网络安全月球愿景的特征之间存在许多差异。原则上，网络安全“月球计划”的成功标准将不太精确和可衡量，因为其成就将是社会变革，而不是单一的视觉胜利。 NSTAC承认这些类比限制，但坚信Moonshot代表了

功能强大且高度适用的模型，用于网络安全所需的国家优先级，集体行动和加速创新。

为了实现其目标，网络安全Moonshot计划必须寻求对几个复杂问题的解答。首先，“安全”在现代数字社会中意味着什么？
哪些“关键服务”对于国家安全和公共安全最重要，必须在全国范围内优先考虑实现可衡量的安全互联网？在全国范围内开始与这些复杂问题公开竞争，与更具包容性的利益相关者社区竞争，对于实现这个更大胆和可持续的未来至关重要。在某些情况下，NSTAC试图在本报告中回答此类问题。在其他情况下，这些答案应从本报告建议发布的长期国家网络安全“月球计划”中得到证实。

当然，仅提供理想的目标声明还不够。网络安全Moonshot计划必须深深植根于清晰的战略框架和共同原则，这些原则应超越个人策略并强调真正的代际变革。它必须具有一种治理结构，使政府，私营企业，学术界和民间社会等各利益相关方团体能够将其集体精力和活动集中于网络安全“ Moonshot倡议”的已定义的更高阶国家目标。

在整个报告中，NSTAC尽力回答几个基本问题，包括什么是网络安全“月球计划”，为什么必要，以及国家如何有效实施该计划。第1.0节“简介”和第2.0节“网络安全为何需要登月”？重点关注为何需要网络安全Moonshot计划，为何当前网络安全逐步改进的轨迹不足以及为何这一挑战值得一代人定义。

网络安全“ Moonshot倡议”行动计划第3.0节提供了战略建议和可采取的行动，美国政府可以领导这一倡议，并利用其独特的权威机构战略性地支持，组织，指导，提供资源并赋权与其相关的整个国家活动目标。第3.0节定义了网络安全“ Moonshot倡议”剧本的开始要素，概述了与该倡议的实际组织和运营相关的建议。其中包括与治理，目标，里程碑，资金以及称为战略支柱的组织框架相关的关键因素。本报告中包含的关键建议摘要包括：

关键建议：网络安全Moonshot计划治理（第3.1-3.3节）

- 总统或副总统应提出并在战略上倡导网络安全“月球计划”，以明确表示，以持久方式应对网络安全挑战是国家未来的战略当务之急。这项声明应在具有历史意义的论坛上发表，例如，国情咨文或在国会联席会议上的特别讲话，以强调这一优先级。

- 网络安全Moonshot计划必须采用一种整体方法，包括跨越政府，企业和学术界的多层治理模型，使其内部能力和活动保持一致，以实现安全的互联网。这种模型可以包括促进合作，资源的联合体式业务结构。

并在适当的情况下奖励分享，并且对承诺最有效实现目标的竞争市场动态无害。还应该有正式的机制与政府和学术伙伴合作实现共同目标。

- 在美国政府内部，由政府领导的网络安全Moonshot委员会应领导和管理这项举措。理事会应负责并有权：提高国家知名度，倡导持续供资，制定国家级战略，制定政策和流程，赋权和激励非政府利益相关方，在明确的网络安全Moonshot计划扶持领域推动加速创新。理事会的任务授权应完全针对实现长期成果，与现有的政府网络安全领导职位（通常自然而然地满足短期和主题要求）不同，但应与之互补。

- 总统或副总统应由理事会正式主持，理事会由有关部门和机构的内阁级官员组成。网络安全Moonshot理事会应建立正式机制，让委任的非政府实体直接为网络安全Moonshot倡议战略和政策制定流程做出贡献。总统任命的执行董事应在运营上运行该计划，并负责对所有国家网络安全“ Moonshot倡议”活动和提升活动（对于实现安全的互联网环境具有最大战略影响）的可见性。

- 在经过一段时间的内部和外部协商之后，网络安全月亮射击理事会应公开阐明一项战略框架，以提供有助于组织网络安全月亮射击倡议的分布式，整个国家活动的共同结构。作为一个建议的起点，NSTAC提出了六个战略支柱，认识到在未来十年内实现更持久安全的互联网将需要采取综合，多学科的方法。

关键建议：网络安全Moonshot倡议战略支柱（第3.4节）

在未来十年内，朝着更加持久安全的互联网取得有意义的进步，并不是变革性解决方案的结果。网络安全挑战的复杂性将需要战略关注和跨技术，人员，流程和政策问题的加速创新，以战略为代表
支柱。有意义的进步将需要激励现有和已知解决方案，并追求实现新的转型解决方案。

NSTAC建议六个战略支柱来指导这一全国性的分布式活动：
（1）技术；（2）人类行为；（3）教育；（4）生态系统；（5）隐私；
（6）政策。这些支柱不应视为独立的工作流程。应将它们视为总体网络安全“月球计划”中至关重要的相互依存元素，包括与活动相辅相成的活动，对互联网安全的预期成果起到补充作用。

1. 技术领域

巨大的技术进步继续拓宽数字环境，并创造恶意行为者积极寻求利用的新的网络安全风险。但是，如果战略地利用这些相同且迅速崛起的技术，则可以启用更自动化和有效的防御安全功能。其中许多基础技术基础已经存在或正在开发中，但需要协调一致的国家研究和产品开发策略，才能应对国家网络安全挑战。技术战略支柱内的关键预期成果包括：

- 识别，确定优先级并投资被视为对互联网环境整体安全至关重要的战略技术，以加快其可用性。根据NSTAC的调查结果，认为关键技术领域包括：
    - 增强型智能，可帮助人类而非取代人类，提供自动化的威胁防护，可领先于攻击者。
    - 量子通信和抗量子密码技术，可以保护当前用于网络安全防御的加密方法；
    - 行为生物识别技术，提供身份评分，减少对传统密码的依赖，并减少经常泄露的个人身份验证身份；和
    - 5G通信和其他下一代网络从一开始就设计和架构，具有增强的安全性，连接性和可用性。
- 实施国家战略计划来加速这些关键技术领域的增长，包括在适当的情况下通过有针对性的网络安全大挑战，以超过竞争性国际努力。
- 制定了政策框架，精简了监管障碍，以激励和奖励私营部门在网络安全Moonshot计划基础技术上的投资和创新。

2. 人类行为

单靠技术无法解决国家的核心网络安全挑战。这些挑战将需要一个更广泛的，由多学科专家组成的创新社区，这些社区要激发自己的专业知识致力于网络安全的转型目标。公民和公司还必须了解其防范成功网络攻击的责任，并通过信息和工具赋权，以激励他们默认做出正确的安全决策。这样的工具就是有效的行为改变运动，如“熊上的烟火”和旨在增加社会压力，抵御危险的，破坏性的行为的反醉酒驾驶举措。

3. 教育背景

网络安全Moonshot计划必须解决关键战略研究学科（包括先前确定的关键技术）的专业知识和资金严重短缺的问题。该计划必须推广高度分散，指数可扩展的教育工具，并扩大指导和学徒制在关键领域的作用。战略网络安全教育计划还必须考虑增强智能等新兴技术将如何改变传统网络安全对劳动力的需求。

4. 生态系统的作用和责任

没有任何一个政府实体，公司或行业组织能够单独设计，概念化，构建或运行确保安全互联网环境的基础。努力必须是采取协调一致方法的结果，利益相关者对其各自的作用和责任有共同的了解，并采取措施促进生态系统互补能力的整合。互联网由数十亿设备，软件程序，服务和用户组成。要在为政府和关键服务提供基本安全的互联网环境的同时，保持互联网接入的普遍性，需要有意识地，协调一致地开展工作，与各种信任级别的各类参与者合作。

5. 私隐权

隐私是一项必不可少的核心原则，必须贯穿网络安全Moonshot的方方面面
倡议的发展，对于赢得美国人民的信任至关重要。美国公民必须能够信任提供关键服务的信息系统，并切实确定网络安全Moonshot计划不会创造隐私
漏洞，但可以增强隐私保证，并确保其个人数据和交易受到保护并受其控制。

6. 政策

政府必须仔细评估和实施相关政策，赋权和激励负责网络安全Moonshot计划的关键利益相关方，促进创新和实施。必须创建，改革或终止政策，以促进创建基本安全的互联网环境。例如，要确保安全的互联网环境，需要具有可信身份和经过完全身份验证的交互，将需要增强安全性，归属和责任感的策略基础设施。对于全球网络空间行为规范，与立法者，国家和国际社会以及私人合作伙伴密切协调，对于取得成功也至关重要。

关键建议：网络安全“月球计划”—严峻挑战（第3.5节）

NSTAC认为，当提出像网络安全Moonshot计划这样长期而复杂的建议时，至关重要的是，要确定离散的特定短期重点领域，作为代表整个网络安全Moonshot愿景更广泛原则的模型。完善的“大挑战”社区代表的原则-大胆思考，基于结果的激励，开放式创新，解决方案

众包—
非常适合这种模式。网络安全社区必须更坚定地接受这种“大挑战”方法。美国政府可以通过发起一系列网络安全大挑战来引领这种转变，这些挑战将为实现安全保障的互联网环境带来更直接，更迅速的突破。

- 作为整体网络安全“月球计划”的催化剂，网络安全“月球委员会”应通过开展为期六个月的协作程序，在全国范围内正式召集利益相关方，领导识别和发起一个或多个“大挑战”。这些重大挑战应围绕先前系统性顽固和市场失灵阻碍进度的关键技术开发领域开展。美国政府可以利用各种工具来激励和加速整个六大战略支柱下这些以大挑战为导向的活动的全国性融合。

- 在评估潜在的大挑战候选人时，政府应权衡以下几个方面的考虑因素和关键问题：（1）在以往的市场驱动力不足的情况下，政府在催化与大挑战相关的活动中是否发挥明确的作用；
  （2）大挑战是否需要开展超出政府权力和/或力量范围之外的活动，并会从更广泛的合作中受益；
  （3）社会，尤其是非网络安全专家，是否能够广泛理解大挑战的战略价值和重要性；（4）大挑战是否可以衡量和实现？
  （5）实现“大挑战”的目标是否会产生高度可扩展的结果；
  （6）大挑战的范围是否足够广泛，足以涵盖多个战略支柱的活动？

政府在历史上有独特的机会。数十个本意良好但相互干扰的活动使互联网对依赖互联网的关键服务的安全性逐渐下降。
NSTAC认为，作为一项国家级战略要务，我们必须大胆宣扬，我们的十年目标是确保美国人和政府与关键服务互动的互联网安全。
NSTAC对这一目标的重要性有清晰的见解，因此，这项建议充分把握了成功的紧迫性和先前，有善意的努力不足的关键问题。

历史为民族克服看似不可能的挑战提供了真正的先例。在这些历史事件中，领导人在没有明确了解最终手段的情况下宣布了战略意图。在像过去这样的历史性例子中，美国政府领导层曾使用一个明确的目标，有形的第一步，采用了整个国家的方法指导工作并激发成功。
21世纪也存在着类似的紧迫机遇。作为一个国家，我们未来的繁荣与成功从根本上取决于我们在网络安全方面的成功，还需要做出令人鼓舞的类似于Moonshot的努力来解决这一问题。

1.0引言

互联网及其带来的持续数字时代已成为不可估量的经济和社会利益之源。使用开放互联网的能力和使用互联网连接技术的自由已仅成为一项核心和基本权利。美国必须通过确保在国际上以身作则，确保美国人能够安全使用这些技术，这是国家战略需要，必须维护这种自由。

也许比21世纪任何经济和国家安全挑战都多，网络安全需要更全面的责任感和集体行动意识。

在目前的轨道上，美国在实现这一国内和国际必要任务方面面临明确的风险。网络安全威胁变得越来越频繁，更加复杂，以及更具破坏性的概念，逐渐削弱社会对数字基础设施的信任。随着技术的不断进步和日常生活的各个方面越来越紧密地联系在一起，可能性和失败成本急剧上升。世界各地的技术专家和网络安全专家都知道这一趋势，但许多政府领导人，企业高管或公众仍未广泛理解这一趋势。也许比21世纪任何经济和国家安全挑战都多，网络安全需要更全面的责任感和集体行动意识。在我们这个高度互联的时代，意味着风险由我承担，因为对最薄弱链接的攻击现在可能对更广泛的数字环境造成影响。[1]

网络安全的复杂性为技术，人员和流程问题带来了众多挑战。这种复杂性导致了将挑战划分为单独的，更容易理解的组件的趋势。持久解决方案的识别进一步复杂化，因为整个网络生态系统高度分散了网络安全功能，权限和职责。没有人可以单方面应对挑战。通常，网络安全攻击的主要成本并没有由最初的受害者承担，导致负面的外部性和动机错位，以改善网络安全风险行为。这些特征常常导致我们以过于分散，被动或增量的方式概念化解决方案。因此，应对分散的网络安全挑战的代价是主动预防网络攻击并从整体上降低系统的网络安全风险。

现在，网络安全威胁的规模，严重性和复杂性对国家的未来构成生存风险-要求探索一种根本性的新方法，为可持久防御和安全的互联网确定更勇敢的解决方案。总统国家安全电信咨询委员会（NSTAC）认识到，有许多已知的最佳实践和政策，如果能更明智地遵循，将会大幅度提高互联网的安全性。但是，本报告专注于寻求更多的变革性工作，从根本上改变互联网安全默认级别。这项追求将是一代代定义的挑战，就像之前的太空竞赛一样，可以为未来几十年美国在全球技术领域继续保持领先地位提供启发和基础。虽然美国尚未经历过类似人造卫星的镀锌活动

[1] Kirstjen M. Nielsen，“秘书Kirstjen M. Nielsen在RSA会议上的讲话”（讲话，加利福尼亚州旧金山，2018年4月17日）演讲，https://www.dhs.gov/news/2018/04/17/secretary-kirstjen-m-nie lsen-remarks-rsa-conference.

网络安全方面，国家必须表现出果断和远见，在此类灾难性的，强迫行动事件发生之前采取大胆而积极的措施。

2.0为什么网络安全需要单月付款？

NSTAC的第一阶段研究有意侧重于网络安全以外的领域，在这些领域中，国家（有时在世界范围内）组织了旨在实现高度雄心勃勃的成果的活动。在回顾这些历史性的"类似月球射击"的努力时，出现了一个共识：月球射击在历史上有不同的时间和地点。他们需要政治，社会，技术和其他力量的独特融合，创造成功所需的有利环境。最终，这些力量汇聚在一起，围绕两大原则达成社会共识：（1）挑战意义重大，失败是不可接受的结果；（2）缺乏根本的新方法，认为失败是当前轨迹的必然趋势。这些原则直接和完全适用于当前和未来的网络安全环境。[2]

但是，仍然需要开展大量工作，以增进各国对网络安全挑战的性质和严重性的共识。首先，要明确回答"为什么？"问题，以证明国家为应对这一特别复杂的挑战取得真正，持久进展所需的重大国家投资，优先事项调整甚至个人牺牲。本报告的基本目标之一是帮助推动重新定义和提升网络安全的国家行动计划，将之视为近乎单一的国家安全和经济挑战。

作为一个国家，美国从根本上未能以激励和确保这种水平的集体行动的方式阐明网络安全挑战。由于网络安全的复杂性，国家常常将挑战的全部范围划分开来，并以技术术语为特征。这种方法通常将关键利益相关者排除在讨论范围之外，使他们不知情，并认为自己没有责任或能力帮助应对挑战。美国政府必须从更广泛的角度应对网络安全挑战，明确政策，教育和人类行为因素与技术创新对长期解决方案同等重要，必须聘请更多专家。

网络安全作为一项全国性挑战，对于"为什么现在呢？"这个问题也有一个明确而令人信服的答案。美国人以技术方便为代价，接受了会破坏个人信息的数据泄露。但是，他们不太可能容忍未来对其生活造成直接和物理影响的网络攻击。在数字环境中，信息越来越仅以比特和字节的形式存在，在狭窄的界线之间建立起了一个相互信任的数字基础，一个平稳运行的数字社会与由信任破裂导致的社会混乱崩溃。

按照目前的轨迹，在未来十年内，美国极有可能遭受比迄今为止更严重的人为破坏性网络攻击。预防这种情况需要采取积极，战略和系统的防御方法，

[2] Lisa Goldman和Kate Purmal，"如何发起成功的Moonshot"（向NSTAC网络安全Moonshot小组委员会简介，弗吉尼亚州阿灵顿，2018年2月20日）。

激发美国人民的集体行动。这种方法必须首先在美国政府，企业和学术界最高层级的支持下，由国家领导人发表声明，将网络安全挑战视为不再是可以接受的风险，而是对美国人民基本生活方式的生存威胁。。

国家领导人必须以抱负和乐观的态度阐明这一"为什么和为什么现在"。尽管对无所作为的负面后果直言不讳，但国家领导层也应支持针对根本安全的互联网采取有针对性的，加速的，全民行动的积极和连锁反应。这些积极和连锁反应可能类似于全国围绕空间方案动员的结果。在最初的月光下，美国政府，私营企业和学术系统在研究与开发（R&D）上进行了巨额投资，导致了医学，材料科学和全球定位系统技术的重大工程突破和意外创新，奠定了美国的基石。在随后的数十年里，技术领域一直居全球领先地位。

美国拥有网络安全中的许多技术基础，因此，开展这项追求不仅仅是一项学术活动。在量子计算，人工智能（AI）和机器学习，云计算和5G通信等领域，近期和近期的技术突破（在NSTAC给新兴技术战略愿景的报告中更深入探讨）创造了潜力。更加简化和自动化的网络安全防御，将更多的杠杆作用和总体力量平衡转移给网络安全防御者。[3]

政府和行业必须考虑这些技术问题以及相互依存的政策，流程和行为问题，以便可以有效地评估，优化和激励针对那些能够最大程度地发挥杠杆作用并最终为恶意网络行为者带来优势的创新行动。首先以注重结果，有抱负和鼓舞人心的战略意图陈述开始。

3.0网络安全月球倡议行动计划

在解决网络安全问题上，美国树立了渐进主义之路。构想从根本上崭新的发展轨迹，很难将其概念化，但是，国家必须从围绕网络安全的不可持续且代价高昂的思维模式转变。这就要求最高层级的国家领导层调动资源和精力，大胆追求。为取得成功，该计划必须真正成为"整个国家"，由具有超凡魅力的领导层，全面的里程碑驱动的执行计划以及由政府，行业和学术界专家组成的参与联盟推动。

本部分网络安全Moonshot计划行动计划，详细介绍与网络安全Moonshot计划的实际执行和运营相关的战略建议。它详细说明了美国政府可以采取的可操作步骤
通过其独特的权威和能力从战略上倡导，组织，

[3] NSTAC。NSTAC就新兴技术战略愿景向总裁提交报告。（华盛顿特区：NSTAC，2017年7月14日）2017 NSTAC出版物，https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Emerging%20Technologies%20Strategic%20Vision.pdf

指导，资源化和授权与定义的目标保持一致的整个国家活动。这里的总体信息很简单：尽管可能很难想象，也无法预测未来十年实现基本“安全的”互联网环境所需的所有长期行动，但本届政府可以通过采取具体行动来展现领导才能短期行动可立即产生收益，为长期，大胆的网络安全愿景奠定基础。

由于NSTAC是根据章程向总统提供建议的，因此本报告中所载建议的其余部分旨在针对美国政府为推动该倡议所采取的具体行动。
NSTAC认识并庆祝互联网的全球互连性质。与志趣相投的伙伴关系保持密切合作至关重要。但是，鉴于NSTAC章程的范围，我们的建议重点是美国政府可以采取的行动，成为志同道合的国家的榜样。但是，这些建议不应解释为美国政府应单方面采取的行动，而应由NSTAC建议美国政府采取行动，为更广泛的生态系统赋权。通常，这需要在政策和倡议制定过程中与非政府利益相关者进行直接直接磋商。因此，本节中的许多建议直接参考了美国政府行使其召集和动员能力领导这一协作进程。

网络安全Moonshot倡议
建议的操作：时间轴

- 在发布时宣布网络安全Moonshot计划/发布抱负声明（第3.1节）
- 启动时建立网络安全Moonshot委员会（第3.2.1节）
- 建立理事会的非政府部门（第3.2.2节）。发射+ 60天
- 定义网络安全战略框架和国家研发优先级（第3.4节）启动+ 120天
- 启动多利益相关方流程定义重大挑战（第3.5节）启动+180天
- 发起首个网络安全大挑战（第3.5节），发起+1年

3.1 传达理想目标

关键建议：总统或副总统应提出并在战略上倡导网络安全“月球计划”，以明确表示，持久应对国家的网络安全挑战是一项特殊的战略任务。这项宣布应在具有历史意义的论坛上进行，例如国际电联国情咨文或向国会特别联名致辞，以强调这一国家优先事项。

在回顾包括肯尼迪总统的原始“月球运动”演讲在内的大规模举措的历史信息时，NSTAC确定了总统或副总统级网络安全宣言必须牢记的几个共同特征。主要特征包括：

- **明确而引人注目的目标：声明以目标为基础的简洁目标明确表达了将复杂性降低到可以在整个社会广泛理解的目标。**

- **理想的口气：声明以促进国家目标的乐观态度界定了挑战及其预期解决方案，而不是"诉诸恐惧"或不作为的消极后果。**

- **压缩时间表：声明明确规定了时间表，强调了解决问题的紧迫性。**

- **大胆且非强制性的方法：该声明在本质上是故意大胆的，对其可实现性表示怀疑和富有成效的对话。**[4]

关键建议：考虑到这些特征，国家计算机科学与技术委员会（NSTAC）建议总统或副总统发表抱负目标的声明："到2028年确保互联网安全保障政府的运作和向美国人民提供的关键服务。"

NSTAC认为这一理想声明是有效的，因为它的意图被认为是具体的，但解释灵活。之所以专门选择"安全"一词，是因为社会安全概念被确定为更普遍理解，直觉和可识别的，尤其是与网络安全通常相关的模棱两可的技术术语相比时。
"安全"也被认为具有指导意义，因为随着社会越来越多地拥抱互联汽车和依赖互联网的关键基础设施系统，网络安全威胁现已超越数字领域，对公共安全构成真正的物理威胁。

"安全"一词也被确定为具有生产性歧义，对促进更强有力的全国对话至关重要。例如，实现"安全"互联网；对于长期的研发投资，国家需要优先考虑哪些核心技术？美国需要如何改革教育体系，培养全面的网络安全专家，并激励公民更好的网络安全实践？信息技术供应链政策需要如何适应才能从根本上确保安全？

对于这些困难的问题，NSTAC并不能完全解决，其中很多是风险管理的折衷，并不是二元的。NSTAC希望通过其调查结果，促进更广泛的全国对话，包括这些复杂的，有时是艰难的对话，因为这是为国家的未来必须克服的挑战。第3.4节"定义战略框架和支柱"进一步深入探讨这些类型的问题。

也许是第一个信息的传递者和个人在哪里传递的信息，甚至比抱负声明更为关键。这个人必须是坚强的

[4] 丽莎·高曼（Lisa Goldman）和凯特·普马尔（Kate Purmal），《月球效应：颠覆传统业务》（加利福尼亚州圣卡洛斯，Wynnefield Business Press，2016年）。

具有超凡魅力的领导者，受多方利益相关者认同，具有更广泛的国家利益。个人必须明确表达愿景，强调对网络安全Moonshot计划进行长期持续性和持续投资的承诺-行政过渡和政治党派不可渗透。这将需要一段时间内从未见过的行政和立法部门之间和跨部门的抱负和共同努力。

NSTAC的评估是，只有总统或副总统的重视程度才能像战时一样紧急产生适当的全国动员来应对这一挑战。当总统或副总统首次提出该倡议时，应与内阁有关官员，国会领导，首席执行官和学术领袖密切协调，以体现真正和象征性的努力，并跨越社会各领域，超越自我。传统网络安全社区。交付地点和论坛也必须是历史地位较高的国家之一；美国国会大厦国情咨文演讲或国会特别联席会议都是恰当的代表性例子，可以传达这一国家倡议的战略和历史重要性。

3.2 建立面向全国的治理方法

然而，仅仅提供理想的目标声明还不够。该声明必须深深植根于明确的战略框架和共同原则。必须有清晰的治理结构作为后盾，使政府，私营企业，学术界和民间社会的利益相关者团体能够为网络安全Moonshot计划已定义的更高阶国家目标贡献和集中集体力量和活动。

在由总统或副总统正式向公众介绍该计划之前，白宫应领导内部流程，为网络安全Moonshot倡议建立治理结构。从广义上讲，NSTAC将治理定义为"网络安全Moonshot计划"组织参与者，授权决策机构，确定目标并实施问责措施以确保进展的方式。对适当的治理和组织模型进行有力而全面的评估，将为分布式国家网络安全Moonshot计划的长期可行性和有效性奠定基础。

关键发现：只有通过共同努力，充分利用整个政府的独特权限和能力，以及整个行业和学术界的协调努力，网络安全"Moonshot倡议"才能取得成功。

网络安全是一项固有的分布式挑战，具有在更广泛的公共，私人和学术生态系统中共享的独特权限，角色和责任。所有这些功能都必须在集体安全模型中有效利用，才能实现有意义的进步。网络安全Moonshot计划的实施和成功取决于高度分散的利益相关者群体系统，这些群体必须有效地赋权，分配资源和动员起来。

NSTAC根据多次简报的调查结果整理了下图，从概念上可视化了对分布式角色，职责，

战略远景可以帮助（而非限制或窒息）针对性创新到定义的领域，从根本上实现更安全的互联网服务。从概念上讲，这包括美国政府最高层上下定义战略意图的自上而下的压力，以及积极定义创新重点和领先进展的私营部门和学术界的运作引擎所施加的向上压力。

图1：针对确定的网络安全“ Moonshot倡议”目标的全国性关注的概念模型。

3.2.1 整个政府

关键建议：在美国政府内部，白宫应建立一个网络安全月亮计划委员会（“理事会”），以战略方式领导和监督该倡议。理事会将负责并有权：确立战略意图，提高国家知名度，倡导持续供资，合作制定国家一级战略，召集利益攸关方，并制定政策和程序，赋予非政府实体权力和激励，推动加速发展定义网络安全Moonshot支持领域的创新。

理事会应由总统或副总统正式主持，由有关部门和机构的内阁级官员组成。应在现有的部门和机构内设立新的办公室，负责执行理事会的机构间政策指令。必须包括部门在报告建议中确定的具有指定责任和权力的高层实体，负责领导私营部门和网络安全Moonshot计划的学术活动。基于已证明的领导关键基础设施社区合作的能力和国会权力，NSTAC建议授权国土安全部（DHS）负责此类利益相关方参与。

此外，理事会应建立正式机制，任命非政府实体直接在理事会的官方机构内部为倡议的战略和政策制定流程做出贡献。理事会应有一个官方的非政府组织，由私营部门和学术界的关键实体的代表组成。总统应确定管理非政府实体参与的结构和权限，以及这些代表在安理会总体决策中的权限级别。但是，非洲国家科学和技术咨询委员会坚信，安理会领导结构内非政府参与者的职责和权限必须超过传统上由政府咨询机构非政府参与者承担的职责。

说明模型：政府间国家航天局

2017年6月，特朗普总统签署了第13803号行政命令，恢复了国家空间理事会的地位，将国家空间理事会重新确立为美国政府主导的多方利益相关方论坛，协调国家空间政策的制定和实施。国家航天理事会（NASA）建议网络安全Moonshot理事会应体现网络组织提供的有用治理模型，其中包括许多组织属性，包括：

由副总统主持，内阁一级代表组成理事会。

非政府组织通过国家航天理事会用户咨询小组正式参与决策过程，由私营企业和学术界的高级专家组成。

负责执行国家空间理事会政策的相应部门/机构级别办公室（包括国防部，商务部和NASA）

具有有效制定和发布行政部门政策的能力，这些政策旨在降低障碍并赋予更广泛的国家航天工业生态系统权力。国家太空理事会在成立的第一年发布了三项国家太空政策指令。

由总统任命的执行董事应在运营上运行该计划，并负责并有权保持其对所有国家“网络安全Moonshot计划”活动的可见性。执行主任应负责：

- 传达倡议的长期战略目标，将工作分解为核心要素，与利益相关者沟通，各组成部分如何适应总体倡议，并指导其实施；
- 认识并协调每个利益相关者团体可以为总体目标交付的价值，以及各团体如何创造协同效应进一步优化价值；和
- 识别利益相关者并就如何激励利益相关者采取行动支持共享的网络安全Moonshot倡议目标提供建议。

- 提升旨在为安全互联网环境的结果提供最大战略杠杆作用的活动；

3.2.2 全行业和学术界

私营部门和学术界在更广泛的网络安全“ Moonshot倡议”中的领导作用不仅限于正式任命为官方理事会成员的人。
构造。政府实体不能单独发起，管理或维持网络安全“月球计划”。该计划的结构必须反映互联网的高度分布式性质，并积极促使具有网络安全角色，职责和权限互补的不同利益相关者团体对理事会的热情承诺和持续参与。

为此，网络安全“ Moonshot计划”的治理必须认识到，这个国家的创新重心已经从以美国政府资助的主导转变为由私人资助的研发。在最初的月光下，肯尼迪总统提出了作为一项国家使命的愿望，呼吁自由与暴政之间的斗争，并在此期间确保了私营承包商和公司的显着参与。网络安全Moonshot计划必须在很大程度上更加依赖各种私营部门和学术利益相关者团体。

关键建议：网络安全“月球计划”必须采用一种整体方法，包括将政府，企业和学术界联系起来的合作治理模型，以协调其固有能力和活动，实现安全的互联网目标。其中应包括一种联盟形式的业务结构，促进合作，共享资源和奖励，并与政府和学术界的合作伙伴密切合作以实现共同目标。

网络安全Moonshot计划的领导者必将出现在许多分布式论坛中。如果在总统或副总统级别上有效发挥作用，理想状态将是无数个独立的非营利性财团，教育协会以及为实现既定倡议目标而开展的其他共同努力的自愿开展。如果与网络安全Moonshot计划的战略目标保持一致，美国政府通过网络安全Moonshot委员会的职责是激励，宣传甚至选择资助这些独立实体的成就。

许多历史例子说明了这种模型。例如，在1990年代后期，美国政府通过白宫，美国国立卫生研究院和国会提供了大量资金，并从战略上倡导了人类基因组计划的大部分内容。然而，该项目的最终成就是由Celera公司等实体与国际人类基因组测序联盟（International Human Genome Sequencing
Consortium）组成的全球20余所大学和研究机构在很大程度上独立活动的产物。[5]

在1980年代和1990年代，发起了一系列多方利益相关者努力，捍卫美国技术优势，抵御外国公司大量补贴的外国公司。

---

5 “人类基因组计划完成：常见问题”，国家人类基因组研究所，2010年10月30日，https://www.genome.gov/11006943/.

政府。结果就是创建了商业联盟，如半导体制造技术联盟（SEMATECH）和微电子与计算机技术公司（MCC）。这些财团是由国会特许成立的私有非营利性公司，旨在帮助国家在特定研究和商业开发领域中发展。最终，超过100家公司共同解决了当今的大规模技术问题，实现了微芯片和互联网基础设施等领域的关键突破。[6]

说明性模型：整个行业/学术界 微电子与计算机技术公司 面对因日本政府提供的政府援助水平增加而失去美国技术优势的原因，微电子和计算机技术公司（MCC）成立于1982年。由里根政府赞助，由美国情报共同体前成员制定，由在最近的政府领导者大会上，MCC邀请了主要的计算机和半导体制造商，精英技术学校代表以及相关团体来促进技术增长。 根据1984年的《国家合作研究法》，MCC对于开发AI技术，逆向工程策略和创建基本的互联网搜索功能至关重要。它是最早注册“ .com”电子邮件地址的公司之一。 “我的客户中心”由不同的组织组成，共享稀缺的研究人员和投资资金，就共同的目标进行协作，并制定解决方案，造福整个国家。

*来源：微电子与计算机技术公司[7]

3.3 其他关键的网络安全Moonshot举措注意事项

发起正式的网络安全“ Moonshot计划”需要做出与治理，政策，预算和许多其他因素相关的复杂决策，才能使这项工作具有包容性，持久性和可操作性。本节重点概述一些初步考虑因素，以及为执行董事在网络安全Moonshot计划启动之前必须做出的关键组织决策提供依据的具体建议。

3.3.1 预算注意事项

历史提供了无数委员会和咨询委员会为总统提供资源分配建议但不控制任何预算资源的例子。在这种情况下，至关重要的是，执行总监必须在预算规划和执行中发挥正式作用，以支持网络安全Moonshot计划的流程和建议，包括与非政府实体有关的活动。总统和执行董事必须阐明联邦预算资源需求，使资源与网络安全Moonshot计划的具体目标相匹配，并确保结果证明投资合理。美国政府在网络安全方面的资金和投资水平应超过当前水平几个数量级，并且在该倡议的十年内必须保持在战时水平。

[6] Robert Hof，“ Sematech的经验教训”，《麻省理工学院技术评论》，2011年7月25日，https://www.technologyreview.com/s/424786/lessons-from-sematech/.

[7] David V. Gibson和Everett M. Rogers，《研究与试验合作》（波士顿：哈佛商学院出版社，1994年），引言，第15页。

关键建议：网络安全Moonshot计划执行主任应在预算计划，制定和执行中发挥稳固的作用。总统应考虑任命执行主任为管理和预算办公室主任共同制定政府年度预算提案。总统还应考虑要求执行主任证明年度预算完全支持网络安全Moonshot倡议的目标。最后，执行主任必须与拨款委员会以及相关的美国参议院和众议院授权委员会保持定期直接联系。

3.3.2 衡量成功，定义进度里程碑和建立动力

主要发现：网络安全Moonshot计划的总体成功取决于理事会明确阐明战略最终目标，确定重大进展里程碑以及制定衡量指标以证明成功的能力。政府如何表达和衡量网络安全"月球计划"的成功与其最终影响以及美国人如何记住和感受该计划至关重要。

就像原始的太空月球一样，政府必须确定公众容易掌握的具体里程碑，即使底层细节非常复杂。肯尼迪总统在1961年5月发表的公开讲话中隐含地提出了一个稳健可见的前进道路：亚轨道飞行，水星计划的多轨道飞行，双子座计划期间的工程对接演习和车外活动，三人阿波罗研制太空舱，更长的载人轨道飞行，无人登月飞行，最后是1969年7月登月。

在这些重要的，公开广播的事件中，工程师取得了一系列稳定的发展成就：更大的助推器，更大的动力，新燃料的开发，更高
可靠性，以及更好的营养和废物消除系统。同样，交流网络安全" Moonshot计划"的进展对于保持公众对努力的关注，并断断续续（即使不是连续的）提醒其国家重要性至关重要。

总体目标的难度和复杂性以及采取行动的力度和步伐，要求政府观察，衡量并在一定程度上强制网络安全Moonshot计划的进展和完成。理事网络安全Moonshot委员会应与确定的利益相关方协调，负责制定网络安全Moonshot计划的里程碑和指标。有几种理论上的指标可以说明网络安全"月球计划"如何衡量十年目标中次级目标的实现，包括：

- 在国家情报局全球威胁评估总监办公室，网络安全不再是首要威胁。
- 运营商反复，可衡量地展示关键规模的网络基础设施，无论规模大小，均能在网络攻击期间保持服务连续性；

- 劳工部或行业协会对网络劳动力空缺和赤字的衡量指标有所下降；
- 改善公众对互联网基础设施和互联网连接技术的感知安全和信任的民意测验；
- 向州和联邦监管机构，包括证券交易委员会报告的重大网络安全事件数量显着减少；和
- 缩短了报告此类数据所需的关键基础设施提供商纠正已知漏洞的时间（“修补时间”）。

3.4 定义战略框架和支柱

关键建议：在经过一段时间的内部和外部磋商之后，网络安全月刊理事会应首先公开阐明一项战略框架，以提供共同的结构，以帮助组织网络安全月刊倡议组织的分布式整个国家活动，这是其第一步行动。作为推荐的起点，

NSTAC提出了六个战略支柱：技术，人类行为，教育，生态系统，隐私和政策；认识到要在未来十年内实现更持久安全的互联网，就需要采取综合，多学科的方法。

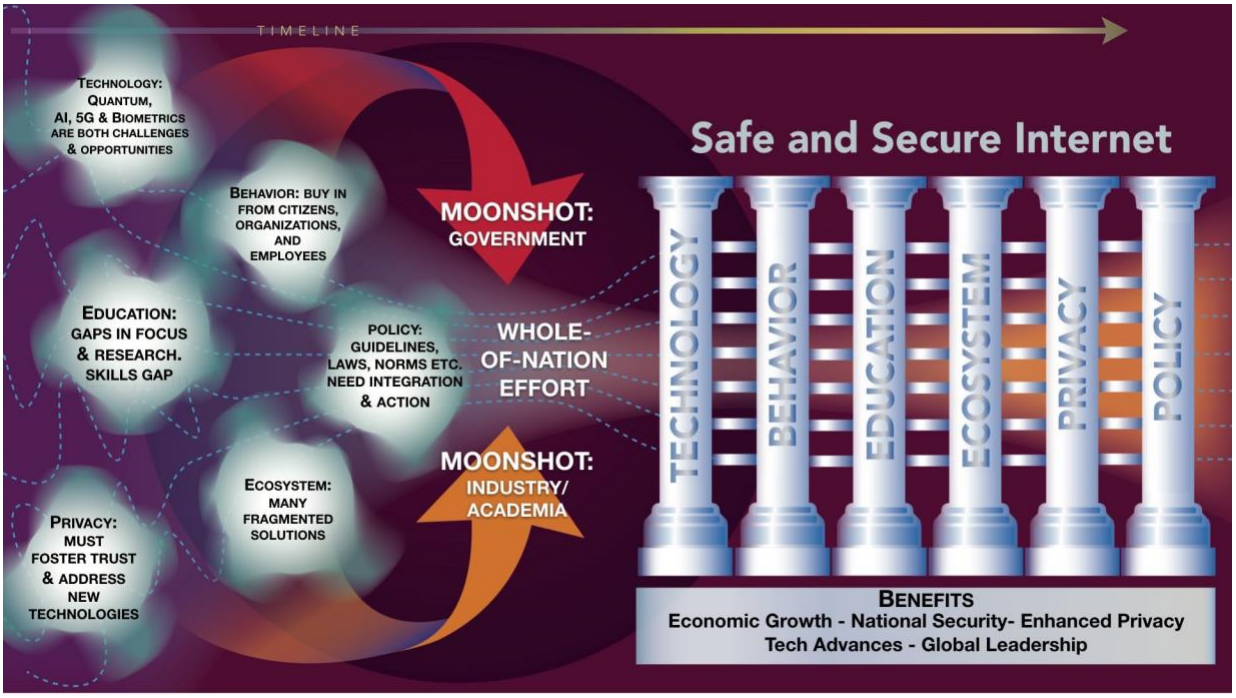

图2：NSTAC关于网络安全“ Moonshot倡议”的战略支柱的建议。该倡议是针对广泛但相互依赖的各类活动而提议的组织架构。

NSTAC使用“战略支柱”结构来描述广泛的活动类别，必须组织整个国际，跨学科的行动，追求实现从根本上安全的互联网环境，确保数字连接的政府和关键机构的信任和弹性服务相对于现状在根本上更高的水平上。应将战略支柱解释为加强和相互依存，而不是单独，独立的工作流程。确实，一些战略支柱（如政策支柱）主要专注于直接实现其他支柱目标。这些相互依赖的，使能的关系在“相互依赖”部分中进行了探讨。

NSTAC建议在现有的开放互联网上追求一个安全的互联网环境，以确保以更抗拒，更灵活的方式与关键服务进行安全交互。实现这一目标的关键特征包括：

- 归因于端点和行动；
- 恶意行为将产生后果；
- 身份将超越密码和个人识别信息；
- 隐私和信任将得到加强和执行；和
- 自愿加入流程，实现全方位收益。

NSTAC认为，在挑战变得更加困难和复杂之前，这项工作需要在整个国家范围内完成，到2028年。

这是最佳时机，让该国更有效地利用新兴技术能力实现基本安全的互联网环境-伴随着第五代（5G）通信技术的不断发展，将大大提高连接性并实现
防御性基础设施，为实现更自动化的网络威胁预防而在人工智能和增强智能方面取得的突破，可以提供全新身份识别方式的行为生物识别技术，以及可以抵御未来更深层攻击的量子加密新功能。尽管所有这些进步（包括美国和我们的对手）即将到来，但没有一个国家框架指导他们的研究，开发和部署朝着共同利益发展，但我们冒失去这一世代相遇的机会的风险。

需要明确的是，NSTAC并未倡导互联网平衡，建立完全独立的互联网基础设施，也未规定任何特定类型的技术架构。
NSTAC提倡为关键服务建立一个基本安全的互联网，其特点是利用重大技术进步，对促进安全选择，网络安全政策和教育改革的用户行为采取更加紧密一致的激励措施和后果，对生态系统有更清晰的了解在此基本安全环境中为特定关键服务构建和运营的角色和职责。确定的其他所需要素包括：

- 抵御攻击的能力；
- 保证服务的可用性；
- 对于特定的关键服务功能，用户应完全归因于操作；
- 恶意行为的后果；
- 确保保护私人信息；

- 消费者和企业对系统的信心；
- 生命线服务的主要交付渠道；和
- 所有需要它的人都可以访问。

在本报告全文中提到“关键”和“生命线”服务时，NSTAC使用的定义是根据美国政府完善的政策制定的。通过涵盖当前政府和前三个政府的一系列政策，美国政府已结成网络安全风险管理战略，优先考虑保护互联网关键基础设施。为响应第13636号行政命令，“改善关键基础设施网络安全”，国土安全部和相关行业机构每年确定并维护“第9节”实体的列表，这些实体被定义为“网络安全事件可能合理导致灾难性区域性或重大事故的关键基础设施”。国家对公共健康或安全，经济安全或国家安全的影响。”在2018年9月发布的《国家网络安全战略》中，美国政府进一步定义了七个优先领域来确定关键职能并集中开展风险降低活动：国家安全，能源与电力，银行和金融，健康与安全，通信，信息技术和运输。但是，NSTAC的生命线服务概念并不是单纯地定义[8]
行业特定的基础。
NSTAC完全支持新兴的关键基础设施风险管理优先级划分工作，包括国土安全部国家风险管理中心倡导的工作，这些工作旨在确定和确定对安全保障互联网至关重要的跨部门功能的保护。

可达性框架

NSTAC在网络安全Moonshot倡议的10年时间表内，根据对倡议的评估可能性，对倡议进行广泛考虑和分类，从而发现价值。本报告将一些举措分类为例。这些类别基于直接的专家简介和研究，具有主观性，仅用作一般指导。这样的框架对于网络安全Moonshot委员会评估提议的举措很有用。这些类别包括：

A：预计将根据目前的轨迹得到解决，包括技术创新和发展的预测速度。
B：预计将通过增加投资，在国家一级重点关注和在关键技术发展方面的合作以及其他五个战略支柱的创新应用来解决。
C：如果没有针对性的大挑战，使用各种激励工具来显着加速整个国家的创新，那么就无法解决。
D：未知的合理方法（注：NSTAC不包括任何“ D”倡议，因此本报告中提出的建议可在网络安全Moonshot的10年时间表内实现）。

[8] 执行订购。 No.13800，82 FR 22391（2017年5月11日），https://www.dhs.gov/sites/default/files/publications/EO-13800-Section- 9-Report-Summary-20180508-508.pdf.

3.4.1 技术支柱

战略支柱目标：从战略上利用新兴技术的发展，为普通公民提供安全的互联网环境；商业；以及联邦，州和地方政府实体，以进行关键服务交易而不必担心妥协。

简介和背景

为了国家安全，公共安全和经济繁荣，美国越来越依赖互联网和数字连接技术。网络安全Moonshot倡议致力于识别，区分优先级，协调和加速技术开发，从而创造更加可信的互联网环境，并能够满足现代超连接网络的安全，保障和隐私需求。关键基础设施环境。

身份范式转变

对于在线身份，我们需要超越身份，密码和个人身份信息（所有这些都可能受到破坏），向身份用户提供更安全的方法。
NSTAC建议利用行为生物识别技术的增强，增强智能和5G通信推出时可用的新传感器数据，在需要身份凭证时提供实时身份评分（从1％到99％）。这种方法为无摩擦交易提供了透明性，基于许多数据点，大大降低了在线身份风险。

这些技术的代表性示例包括增强智能，量子通信和量子抗密码技术，生物识别，5G通信和身份验证技术。这些技术将为实现更安全，更安全的互联网提供技术基础。
NSTAC知道，对手也正在为自己的目标追求同样的技术。因此，网络安全Moonshot计划必须包括这些新技术的强大防御实施，包括 防止基于硬件的增强智能训练数据中毒 生态系统供应链中引入的安全漏洞，以及能够解密现有数据的量子通用计算机。

NSTAC的历史：与新兴技术相关的先前和未来研究

2017年NSTAC致总统互联网及通信弹性报告攻击。该报告还强化了NSTAC提交给总统的新兴技术战略远景报告（2017年）的发现和建议，并得出结论认为，新兴技术领域，包括人工智能，云计算，量子计算，生物识别和认证方面的重大进步提供了必要的基础。实现网络安全的巨大转变。
NSTAC目前正在制定一份报告，探讨如何提高抵御能力和促进信息通信技术生态系统的创新，该报告将研究对美国国家安全和应急准备至关重要的技术能力，以及政府如何管理短期风险，支持创新，并增强NS / EP关键功能的供应商多样性。 NSTAC计划在2019年春季完成这份报告。

在本报告中，NSTAC的作用不是规定与技术相关的特定技术
计划，作为实现网络安全Moonshot计划预期成果的唯一解决方案。确定优先重点最高的领域（为关键服务实现安全的网络安全环境提供最大战略杠杆作用的领域）必须从更加分散的过程中诞生。但是，存在广泛的技术类别，这些技术对于将来实现安全网络安全环境至关重要。以下仅是说明性示例。随着网络安全"月球计划"的启动，美国政府领导层可以使用各种政策杠杆激励私营部门和学术界并赋予权力，以加速研究和开发这些关键的，范式转换技术：

- **5G通信和下一代网络：提供设计提高安全性，互连性，隐私和可用性的5G通信网络（无线和有线）。这将提供更具弹性的基础设施，为物联网（IoT），工业控制系统，移动，医疗保健等扩展安全连接，并显着提高带宽和近实时延迟。**[9]

- **人工智能：确保开发机器学习和人工智能以壮大（而不是替代）人类，同时最大程度地降低人工智能系统数据中毒等风险。允许以机器速度对网络威胁进行近乎自主的响应，以实现自我修复计算环境，识别缺陷，防止这些缺陷的利用并减轻故障的影响。**

- **身份行为生物识别技术：行为生物识别技术与人工智能功能相结合，可以减少对容易遭到破坏的个人身份识别的依赖，允许创建身份评分，使密码过时，并提高识别用户的透明度和信心。***10*

- **量子通信和抗量子密码技术：利用量子技术提供可信赖的加密和通信平台，可抵抗量子通用（QGP）计算机，防篡改并适用于所有服务。这需要能够解密现有敏感数据的QGP计算机问世之前就已经存在。**

- **通用弹性：通过自动化和简化面向威胁防御的网络安全工具和功能的使用模型，确保关键服务所需功能的访问和可用性。***11*

- **微细分：在分布式网络中实施加密保证的微细分可以减少攻击面，限制横向侦察并显着降低恶意软件的影响，从而帮助支持运营弹性和零信任方法。**

---

9 威廉·奥恩（William O'Hern），"AT&T NSTAC Moonshot简报"（向NSTAC网络安全Moonshot小组委员会简介，弗吉尼亚州阿灵顿，2018年9月18日）。

10 John M. Poindexter，"互联网问责制"（向NSTAC网络安全Moonshot小组委员会简介，弗吉尼亚州阿灵顿，2018年3月22日）。

11 塞缪尔·维斯纳（Samuel Visner），"网络安全Moonshots"，（向NSTAC网络安全Moonshot小组委员会简报，弗吉尼亚州阿灵顿，2018年3月29日）。

预期成果

尽管NSTAC并未寻求规定特定的技术解决方案，但确实将所需的最终状态定义为对创新者的组织挑战，他们将利用先前概述的技术。国家必须开发更大的信任模型，以支持更强大的身份验证和其他安全机制，并确保及时响应新的安全和隐私挑战。预期成果包括：

- 增强对关键基础设施所有者和运营商的信任和信心；
- 确保关键基础设施系统的弹性；[12]
- 通过数据控制确保用户隐私，通过透明化增强信任，同时确认共享信息所有权和衍生信息的复杂性；
- 确保用户可以依靠设备和基础设施正常运行；和
- 确保合理保护信息和设备免受不断发展的威胁。

为了充分利用潜在的技术进步提供基本的安全保障，需要更具体的要求。这些要求包括：

- 促进基于行为生物识别的身份评分（类别B）；
- 开发基于人工智能的网络和计算防御（B类）；
- 为物联网数据管理提供5G（C类）；
- 鼓励增强抗量子加密和密钥管理的研究和开发，以适应量子计算的发展（C类）；
- 促进以公民为中心的安全在线运营，如投票和归档税，以及其他关键基础设施功能（C类）；
- 使能够在机密，完整性和弹性下在两个实体之间进行交易的能力（类别B）；
- 管理连接到互联网的物理和虚拟设备的关系（类别B）；
- 具备防御，抵御攻击，成功运行以及自动删除恶意代码的能力（B类）；和
- 预防，识别，跟踪和补救关键基础设施各个方面的数据损坏和危害（类别C）。

[12] 同上。

列间依赖

本节包括对影响技术的其他战略支柱的成果，计划和活动的引用，包括在适当支持下可以加快技术发展速度的领域。例如：

- 如果更容易获得教育，并将战略重点放在关键计算机科学领域，则可以加快关键支持技术的进步；
- 对政府行政，立法和司法部门进行技术教育可以帮助确保政府提供正确的政策框架，促进迅速发展，并确保美国在必要的技术进步中发挥领导作用；
- 确保政策框架并简化监管障碍，以激励和奖励支持网络安全Moonshot计划的私营部门对技术的投资和创新；
- 建立一个框架，激励生态系统中的利益相关者共同努力实现技术目标；和
- 开发默认情况下从最终用户那里提取安全复杂性的技术，使人类能够更安全地采取行动。

3.4.2 人类行为支柱

战略支柱目标：实现和维持安全可靠的互联网将需要对网络安全生态系统的所有组件（包括用户，提供商和员工）进行重大的行为更改。各方将需要了解其特定角色和成功的关系，以及网络安全与国家安全之间的紧密联系。要实现这一目标，需要采取以下几种行动：

- 通过激发和扩展对网络安全的兴趣，激发美国固有的创新社区，这是从利基技术专家到主流的社会敬佩的追求；
- 通过各种工具加强切实选择安全和身份验证的选择，而不是最便宜的选择，切实鼓励互联网用户做出更安全的决策；[13]
- 通过向公民提供清晰，引人注目的，最低限度的技术信息，向公民证明良好的网络安全实践是国家安全的一部分；和
- 确保无论技术水平如何，广泛的美国公众都可以使用足够的安全工具，选项和技术。

[13] 纽约网络工作队，建立可防御的网络空间（纽约：哥伦比亚大学国际公共事务学院，2017年9月28日），https://sipa.columbia.edu/sites/default/files/3668_SIPA%20Defensible%20Cyberspace-WEB.PDF.

简介和背景

以往的国家网络安全措施未能取得广泛成功，部分原因是缺乏综合的人类行为成分。这些早期工作虽然为国家带来了巨大收益，但又过于孤立或孤立无援，无法提供网络安全挑战所需的整体方法。

与最初的"登月计划"类似，"公民集体"必须被视为网络安全"登月计划"的关键利益相关方。公众通常不会受到国家面临的严重网络安全威胁的影响，也不认为问题是影响国家福祉的问题，更不会影响国家安全。利用"公民集体"的能量和重点不仅面临和解决技术挑战，而且要应对政治环境，这对于网络安全Moonshot计划的成功至关重要。[14][15]

此外，这项举措就像最初的月球计划一样，可以推动其他领域的创新，并为关键服务留出持久的遗产，而不仅仅是一个可信赖的，有弹性的环境。互联网的稳定性，安全性是其他关键生命线行业（如医疗保健，电力和运输）创新的关键推动力。实践证明，要摆脱当今当今互联网所面临的挑战，我们不可能出路-
核心网络安全挑战没有技术银弹。此外，做出艰难抉择导致更简单，更安全的环境没有有意义的进步。公民，技术开发人员和运营商，政府官员和互联网用户的行为全面改变显然令人沮丧地难以捉摸。

预期成果

与人类行为支柱相关的整个国家活动应着重于以下理想成果：

- **激发美国公众的想象力和活力：提供关键服务的安全技术基础将需要传统上专注于这些挑战的不仅仅是技术提供商，网络运营商和安全专业人员。要实现这一宏伟的目标，就需要对环境运行方式，用户互动方式，在线身份观念以及每个人的角色进行根本性改变。只有我们拥有一支敬业，知情和参与的平民，这些变革才能成功。**

- **激励创新社区：必须承认创新是美国人生活的关键文化组成部分。高级研究的总资金仍在占国内生产总值的百分比下降，这使得**

---

14 迈克尔·丹尼尔（Michael Daniel），《网络月球的必要政策基础》，（向NSTAC网络安全月球小组委员会简介，弗吉尼亚州阿灵顿，2018年3月27日）。

15 Dov S. Zakheim，"组建政府应对网络挑战"（向NSTAC网络安全Moonshot小组委员会简介，弗吉尼亚州阿灵顿，2018年9月27日）。

研究美元的应用更为关键。在传统上，大学是创新社区的重要参与者，因此在这方面大学可以提供更多服务。建立和培育一个致力于共同研究目标的社区，已在物理和材料领域取得了重大成果；该模型需要在网络安全领域进行调整和加速。*16*

- **将更安全的决策作为默认选择：所有用户，包括员工，学生，消费者和公民，必须自觉将网络安全视为对社会福祉至关重要，并了解其在通过增强网络安全实践帮助美国方面的作用。同时，必须尽可能透明地选择安全选项，以免增加重大负担或不需要高级技术知识或复杂程度，因此最终用户可以做出正确的安全决策。例如，研究表明，当安全功能默认情况下处于打开状态且无需用户操作时，就会发生一些对安全性影响最大的更改。*1718***

- **激励措施会加强对安全和认证要求的适当选择，而不仅仅是最便宜的选择：美国政府通过国土安全部，商务部和特定部门机构，长期鼓励并提供建议和自愿性准则，以鼓励取得安全成果。成功的网络安全“ Moonshot计划”的必要要素将包括对激励行动的私人行为者进行定向影响。政府可以通过财务激励措施激励行为，例如以结果为导向的采购指南，进行重大挑战或举办有奖竞赛。同时，具有广泛组织影响力的公共关系运动可以帮助消费者做出正确的安全决策。最后，政府可以通过建立公共与政府间互联网交互的安全要求来促进安全。*19***

为了将参与转化为行动，必须为用户提供直接且低开销的方法，以提高安全性。这些机制必须为广泛的美国公众所熟知。利用机器学习，自治和计算领域的创新技术，可以建立并加强关键交易安全路径的选择，并管理5G有助于解决的超连接问题
建立。，*2021*

16 杰弗里·梅维斯（Jeffrey Mervis），“数据检查：美国政府在基础研究资助中的份额下降到50％以下。”《科学》杂志，2017年3月9日，http://www.sciencemag.org/news/2017/03/data-check-us-government-share-basic-research-funding-falls- below-50.

17 纽约网络工作队，建立可防御的网络空间，https://sipa.columbia.edu/sites/default/files/3668_SIPA%20Defensible%20Cyberspace-WEB.PDF.

18 Randy Sabett，“基于激励的政策在整个国家网络安全战略中的作用”（向NSTAC网络安全Moonshot小组委员会简介，弗吉尼亚州阿灵顿，2018年9月26日）。

19 保罗·阿方索（Paul Afonso），“与网络安全Moonshot计划相关的公用事业监管与州级机构的协调”（向NSTAC网络安全Moonshot小组委员会简介，弗吉尼亚州阿灵顿，2018年9月26日）。

20 布鲁斯·麦康奈尔（Bruce McConnell），“确保[全球]互联网安全”。。。到2028年。”（向NSTAC网络安全Moonshot小组委员会简介，弗吉尼亚州阿灵顿，2018年8月22日）。

21 O’Hern，“ AT＆T NSTAC Moonshot简报”。

列间依赖

美国人的机智和创造力将是网络安全Moonshot计划成功的关键因素。这种独创性和人类意志的建立，维持和运用是通过关注，行动和资源来衡量的，并将受到其他战略支柱的重大影响。例如，教育改革，隐私权保护，技术的演进和采用，以及通过激励行为推动互联网安全指数级提升的政策，都需要在战略支柱上进行协调和共同开发。

3.4.3 教育支柱

战略支柱目标：国家必须显着提高网络安全Moonshot倡议战略重点领域的网络安全人才的可用性，质量和多样性，同时教育所有公民共同创造安全的网络环境。这包括对风险的基本理解和积极安全地履行职责的积极动机。

简介和背景

安全环境使能技术的开发和实施将带动对合格从业人员开发和运营其基础网络安全基础设施的更大需求。为满足这一需求，需要增加K-12科学，技术，工程和数学（STEM）计划的广度和深度，为网络安全Moonshot计划的战略重点领域提供支持。国家必须制定协调一致的国家战略，以迅速增加熟练的网络研究人员和专业人员的数量。这些网络安全专业人员必须有能力促进对发展和维持安全互联网环境至关重要的变革性技术突破。必须及时完成这些突破，以支持开发，部署和部署。
培育最佳实践，特别是在量子计算，人工智能和5G等关键领域。

必须采取新的激励措施来增强正常的市场供求机制，以保持STEM毕业生在学术界以及政府国家安全和基础设施领域的作用。这些激励措施可以帮助吸引和挽留可能会进入私营部门的政府网络安全人员。这将需要政府，非营利组织和私营企业之间额外的资金投入和创新合作，以制定新的网络安全教育计划。[2223]

所有年龄段的人都必须进行强大的STEM教育，这也是网络安全教育和员工队伍发展计划的基础要素。必须利用基于云的创新技术来提高STEM教育的速度和质量。例如，人工智能，大数据和增强现实技术有可能帮助解决K-12和高等教育中的障碍。这样的程序可以利用游戏化，媒体和分布式平台进行学习。努力

---

22 理查德·海曼（Richard Heimann），“学科现状：人工智能”（向NSTAC网络安全Moonshot小组委员会简介，弗吉尼亚州阿灵顿，2018年9月6日）。

23 Maughan，“向NSTAC网络安全Moonshot小组委员会简介。”

还必须留住美国高校中最优秀，最聪明的毕业生，其中许多是非美国居民，留在美国并加入美国劳动力大军。此外，生态系统成员应考虑采用轮换或交换制度，在这种制度下，政府雇员是自愿分配给主要商业提供者的，反之亦然。尽管一些网络安全教育和劳动力发展计划正在进行中，但美国面临着严重且有据可查的劳动力短缺。研究报告有所不同，但表明到2021年，美国将至少有350,000个空缺网络安全职位，以及多达350万个与网络安全相关的职位在网络安全平均工资是全国平均收入的三倍的环境下，这种巨大的赤字仍然持续存在，私营行业的薪酬大大超过政府补偿。*242526272829*

最后，在基本安全的网络安全环境中运行可能会带来一定程度的个人不便：对普通用户而言是一种范式转变。最终用户通常是系统中最薄弱的安全链接，无论是出于恶意意图，缺乏培训还是疏忽大意。必须与政府，学术界和私营部门合作，帮助教育这种文化转型。*3031*

预期成果

整个国家与教育支柱有关的活动应集中在以下理想成果上：

- 全国范围内对教育当务之急的关注可以分为两大类：（1）网络安全相关科学和技术专业职业；（2）针对总体用户而言，安全可靠的网络安全基础设施；
- 为研究和开发网络安全计划提供更多资金，包括纯技术研究和应用研究，以配合技术支柱中确定的有利领域的近期发展；
- 建立基于财团的教育结构，在政府，企业和学术界之间轮流任职和相互授粉；*32*
- 奖学金，助学金和助学金的大幅增加，使STEM教育更加便捷；实习，学徒制和研究生安置，以帮助填补关键劳动力

24 扎克海姆“组织政府应对网络挑战。”

25 “遇见千禧一代”，2017年，网络安全与教育中心，https：//iamcybersafe.org/research_millennials/。

26战略与国际研究中心，弥补技能短缺，（华盛顿特区，迈克菲，2016年），https://www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf.

27 同上。

28 道格拉斯·莫恩（Douglas Maughan），“向NSTAC网络安全Moonshot小组委员会简介”，向NSTAC网络安全Moonshot小组委员会简介，弗吉尼亚州阿灵顿，2018年8月28日。

29 肯尼斯·科宾（Kenneth Corbin），“高需求，高薪和高选择性网络安全专家”，2013年8月8日，首席信息官，https://www.cio.com/article/2383451/careers-staffing/cybersecurity-pros-in-high-demand--highly-paid-and-highly- selective.html.

30 Robert Hinden和Russell Housley，“对在互联网上部署安全性的挑战”（向NSTAC网络安全Moonshot小组委员会简介，弗吉尼亚州阿灵顿，2018年9月25日）。

31 Sabett，“基于激励的政策在整个国家网络安全战略中的作用。”32同上。

需求；早期和持续的指导，特别是对于STEM中传统上代表性不足的人群；

- 不断发展的STEM教育课程，旨在通过高中（包括通过网络安全高级安置课程）在幼儿教育中引入计算机科学主题，因此，网络安全被视为一条明确定义且在社会上令人钦佩的职业道路；

- 到2028年，每位K-12学生都应具备网络卫生最佳实践的基本知识，并且应了解美国国家标准技术研究院（NIST）概述的计算机系统基础知识；和

- 通过有针对性的签证配额和经济奖励措施留在公民身份中的公民机会美国劳动力从美国教育系统输送外国出生的网络安全人才。

列间依赖

教育成果与其他战略支柱有着显着的相互依存关系。代表性的例子包括：

- **人类行为：为达到关键的教育成果，需要采用"胡萝卜"和"坚持"式激励措施，包括开展公众意识运动，以（1）推动学生进入网络安全"Moonshot"倡议的相关学科领域；（2）显着改善普通民众的网络安全行为。**[33]

- **生态系统：将需要培训越来越多的公共和私营部门网络安全专业人员，以建设和运营基本安全的互联网环境的基础设施。**

- **隐私：向美国人介绍数据隐私的作用，维护数据隐私所需的相关责任以及国家政策对其行为的影响，这是一项至关重要的教育成果。**

3.4.4 生态系统支柱

战略支柱目标：到2028年，美国需要一个由自愿性利益相关者组成的一体化生态系统，共同为关键和生命线服务设计，开发和运营安全环境。这样的生态系统并不是一个单一的实体，甚至连联邦政府也无法简单地授权。取而代之的是，它需要一组具有商业和国家安全激励措施的代表组织，对所有信任级别的各方开放，并采用全国家方法运作，在整个过程中采用"市场安全"措施。"首先进入市场"的心态。

[33] Craig Fields，"国家网络计划"。（向NSTAC网络安全Moonshot小组委员会简报，弗吉尼亚州阿灵顿，2018年8月21日）。

简介和背景

如今，技术公司在很大程度上提供了商业上可获得的竞争产品和服务，这些产品和服务通常被信任，具有弹性，可访问且有望不断发展。单独而言，这些实体几乎不会产生任何变化，但作为一个凝聚生态系统的一部分，集体可以提供所需的更高度集成的安全解决方案。这个网络安全生态系统包括政府（联邦，州和地方），学术界和私营部门，具有竞争和合作的内在倾向。[34]

生态系统的参与者包括提供或使用关键服务基础设施的所有人。除了研究人员，制造商，运营商和用户外，还包括制造商和运营商的供应链。生态系统包括私营部门实体，各级政府，公民，标准组织，外国实体，非营利组织，开源社区等的参与者。生态系统的物理和逻辑组件包括设备，组件，网络，服务和应用技术，这些功能共同创建互联网，关键基础设施系统和政府服务。

在网络安全Moonshot计划的背景下，政府服务和关键基础设施需要更高的身份验证，完整性，安全性，隐私，可访问性，弹性和归属保证。虽然网络安全"月球计划"要求政府拥有最终战略领导权，但私营部门将使技术商业化并设想，构建和启用可确保持续安全互联网环境的功能。虽然网络安全Moonshot计划是一项基于美国的计划，但美国政府应继续与"五眼"盟友和其他志趣相投的国家密切协调。

当今的生态系统提供的产品和服务带来了极大的便利，资源利用率提高以及无数其他好处。在这些解决方案中，不断扩大的传统安装基础具有不同级别的安全性，弹性和耐用性。美国ICT产品市场一直在努力平衡成本，可用性和客户可见功能与（通常）无形安全性和弹性能力之间的平衡。试图提供高于平均水平的安全性的公司会被那些首先将产品推向市场或以比现有产品更低的成本提供等效功能的公司所取代。

广泛采用的商业现货解决方案可提供规模经济效应，使构建更安全的定制解决方案的尝试不可行。充其量地说，拥有强大品牌的公司会尝试通过分配用于风险管理，安全性，弹性或事件响应的资源来降低风险。需要广泛部署以提高安全性但与本地化价值本质上不相关的标准或技术通常使用不足。[35]

在所有领域，NSTAC简报员预计，新技术将发生空前的变革性应用。预计解决方案将不断集成，互连和融合。

---

34 同上。

35 Hinden和Housely，"对在互联网上部署安全性的挑战。"

复杂。简报者列举的一些例子包括交通基础设施的5G应用以及向电网添加分布式能源。量子计算对传统加密协议的威胁增加；以及人工智能的双重性质，可以用作预防性安全工具或网络武器。[36][37]

预期成果

最终，政府需要与生态系统中的所有参与者互动，在2028年之前优先降低网络安全风险，并为关键服务实现安全的环境。美国政府需要实现三个基本的理想成果，以增强整个国家的活动能力与生态系统支柱有关：

- 领导和组织跨部门的生态系统，基于重要的风险缓解，标准，防御技术，共享的基础设施和服务，团结志愿利益相关者实现安全环境所需的共同目标。一个公益组织，紧随SEMATECH和MCC自1980年代以来的成功脚步（在行业和学术界第3.2.2节中有更深入的探讨），对于此类自愿性联合体结构而言，是一个有用的模型。

- 在10年内参与设计和执行阶段之间的过渡，以实现安全可靠的环境，致力于跨政府和关键服务。应在政府服务，关键基础设施和其他自愿参与的部门中确定安全有保障的环境基础设施所需的安全性，弹性和可访问性的核心要素。实施障碍（无论是财务，技术，监管还是透明度）必须通过美国政府领导层共同解决。[38]

- 将以安全可靠的方式提供政府和关键服务所需的所有要素提供给其他应用程序和业务解决方案。内容包括基础弹性基础设施，共享服务，使用生物识别技术的用户身份验证，可以替代传统密码的可信身份提供商，强大的设备和服务身份，归因，制造商事件响应和补丁，网络安全最佳实践，远程恢复机制，软件保证，网络响应组织和当局调查和补救非法活动。

列间依赖

根据定义，生态系统支柱将包括跨所有其他支柱的相互依存的活动，因为它代表了网络安全Moonshot计划的收集，汇总，集成和执行。每个支柱对于成功完成项目至关重要的基本方法不可夸张。

---

36 Terry Halvorsen，“5G网络技术和能力”，（向NSTAC网络安全Moonshot小组委员会简介，弗吉尼亚州阿灵顿，2018年9月5日）。

37 阿方索（Afonso），“与网络安全Moonshot计划相关的公用事业监管与国家级机构的协调”。

38 詹妮弗·古斯蒂卡（Jennifer Gustetic），“设计和实施重大挑战：借鉴美国宇航局的经验”（简报）NSTAC网络安全Moonshot小组委员会，弗吉尼亚州阿灵顿，2018年8月23日）。

3.4.5 隐私支柱

战略支柱目标：隐私是传递为国家提供关键服务所需信任的关键组成部分。到2028年，美国公民必须能够信任提供关键服务的信息系统，并切实确定网络安全Moonshot Initiative活动不会造成隐私漏洞，反而会增强隐私保证，并确保个人数据和交易的安全，保护和控制。隐私是一项基本原则，与安全和保障目标交织在一起，必须渗透到网络安全Moonshot计划的所有方面。[39]

简介和背景

在安全有保证的互联网环境中，隐私权应是一项权利，与第四修正案的权利相呼应，即美国人将"确保其人员，房屋，纸张和财物安全，防止不合理的搜索和扣押。"艾伦·威斯汀（Alan Westin）的开创性定义"隐私是个人，团体或机构断言自己确定何时，如何以及在何种程度上向他人传达信息的主张"，这是另一个基础。网络安全Moonshot计划的设计和指令必须体现隐私原则，并扩展到安全环境中的所有互动。隐私支柱的基本要素是个人，团体和机构确定如何以及何时传递个人信息。最后，由于物联网和物联网技术的增长，安全互联网环境的架构必须考虑个人数据的大量暴露。5G实施驱动传感器连接。*404142*

数字世界的隐私动摇了部分原因是信息不断受到损害，以及基于信息的商业惯例的泛滥，在某些情况下还没有适当的安全惯例。几乎每个美国人都受到数据泄露的不利影响，这会严重影响其个人隐私。在我们目前不变的情况下，随着连接设备和数据交换数量的增加，未来隐私泄露的可能性和影响呈指数增长。面对这些挑战，网络安全Moonshot计划必须建立信任，透明和隐私级别，以确保在安全互联网环境中最佳采用。

对于隐私，重要的是要了解匿名和归属之间的相互作用。所有用户，无论他们在网络活动中的归属或匿名级别如何，都对隐私具有有效的期望，并对数据的使用方式有所选择。虽然匿名保护隐私，但这并不意味着每笔互联网通信（包括对关键基础设施的访问）都应该匿名。实际上，这种匿名往往导致对有害活动缺乏威慑力。同时，必须保护匿名，特别是在恐惧或无法行使基本，基本人权的地区。在当前的在线环境中，几乎没有恐惧进行恶意活动的后果。安全环境必须解决这一现实，并努力确保特定关键服务的归因是绝对的，因此对个人造成的后果不仅可能而且很可能。

[39] Poindexter，"互联网问责制"。

[40] 威斯汀，艾伦，《隐私与自由》，纽约：IG出版社，1967年。

[41] "书评：隐私与自由"，2004年11月24日，Privacilla.org，http://www.privacilla.org/fundamentals/privacyandfreedom.html.

[42] O'Hern，" AT&T NSTAC Moonshot简报"。

预期成果

隐私支柱倡导解决方案，帮助解决许多基本隐私领域的挑战。必须解决的特定领域包括：归因和责任，透明度，身份，加密，传感器数据和增强智能。成功将透明地展示，并将基于客观和主观结果，例如：

- 安全互联网环境中的所有交易均应以积极的身份和完整的归属全权负责；[43]
- 整个网络安全Moonshot计划整合了强大的隐私治理，包括领先的隐私权倡导组织以及政府和行业利益相关者的投入和监督。
- 公众普遍认为，关键服务交易是安全，可靠和可信赖的。

必须能够在安全环境中实施归因和责任制，而如今这几乎是不可能的。在安全环境之外，归因和责任制缺乏是道德上的当务之急（例如，支持言论自由而不惧怕报应）；但是，在同样的环境下，越来越多的活动和行为成为对我们社会的威胁。风险和报酬的不对称有利于恶意用户。

为确保隐私，身份管理，加密，传感器数据使用和增强智能部署必须发生变化。例如，身份必须是上下文相关的，并根据特定的已知需要提取必要的属性，以肯定实体的身份；加密协议必须具有量子抗性；必须采取保护措施，防止侵犯人工智能使用的隐私；IoT设备和传感器的数据必须得到管理和保护。建立和供应身份分数，而不是密码，源自实时传感器和生物特征识别数据将贬低个人可识别信息的价值，同时增加安全环境内的隐私并扩展到在线使用的其他方面。

列间依赖

虽然隐私取决于其他五个支柱的成功互动，但三个支柱具有特别强的相互依赖性：对人类行为的深刻理解对于成功实施隐私保护至关重要，必须制定支持和激励隐私创新的政策制定，尤其是技术，尤其是技术。随着5G的出现和针对网络安全应用程序的AI成熟。

[43] Poindexter，“互联网问责制”。

3.4.6 政策支柱

战略支柱目标：国家必须在政策（包括法律，法规，规范，规则和标准）上进行有针对性的重大更改，以实现其他战略支柱的重大进步。这些变化可以由激励措施，国家和国际准则制定，新出现的威胁以及新技术驱动，所有这些共同目标都是促进更加持久安全的互联网。政策将需要识别，奖励和奖励积极行为的行为者，并对消极行为实施责任追究，归因和后果。必须做出必要的政策调整，以确保网络安全Moonshot计划取得成功，并意识到挑战的国际规模。 *44*

简介和背景

时至今日，国家正努力跟上日益复杂的网络威胁，这些威胁从根本上威胁着美国的生活方式。国家在维护和尊重社会开放和所有人自由方面的坚定决心为罪犯和对手创造了机会，通过网络攻击剥削和伤害我们。类似于为阻止针对软目标的恐怖主义所面临的执法挑战，互联网政策使关键系统很容易盗窃私人和敏感数据，并可能造成破坏或破坏。网络安全政策可能需要做出调整，以应对数字化世界所面临的当前和未来挑战，这可能不仅仅是国家历史上的任何变革。

案例研究：政策与汽车安全

在这项工作中，应考虑过去使用广泛的政策改革来激发变革的经验教训。在1960年代后期，政府与汽车工业合作应对挑战，为道路上越来越多的人员和车辆创造更安全的条件。政府于1968年制定了严格的安全法规，从强制性膝部安全带开始。1989年，强制要求简单驾驶员安全气囊，但如今，市场需要多个前，侧面和后方安全气囊系统，以增加乘客在事故中幸存的可能性。政府还通过道路设计法规，交通控制和强制性限速措施以及针对驾驶员的严格指导原则（如针对车辆类别的牌照）以及违反交通法规的严重后果解决了这一问题。如今，工业界正在引入自动制动等新技术，以进一步降低发生事故的可能性。所有这些改变都是为了为日益依赖汽车的社会带来更大的收益。尽管交通事故，伤害和死亡人数仍然过高，但如今驾驶员使用的车辆和基础设施比20年前安全得多。

预期成果

如果不进行政策改革，政府，企业界和学术界都无法从整体上解决网络安全挑战。从为所有人提供更安全的汽车出行的多学科方法中可以了解到，要在促进对企业，消费者和政府安全的网络安全环境之间找到适当的平衡，同时又不扼杀创新和竞争，这将需要各种政策工具的精细应用。

44 Visner，“网络安全Moonshots”。

国内和国际政策，包括法律，标准和各种机构的指导，包括国会，政府标准，行业和技术标准，以及国际互联网标准，可以包括以下内容：

- 定义和投资必要的基础设施，以从根本上更安全的方式设计和运营互联网；
- 定义网络安全生态系统利益相关者的责任和权力，以激励与其具体角色相符的主动和自愿行动；
  责任；[45]
- 界定安全环境内网络安全规范的边界，并促进公众和私人对其决定在国家安全中的作用的了解；
- 为利益相关者定义决策路径（包括鼓励市场驱动力或开发新的非技术资源），以鼓励采取积极激励措施，并避免因违反在安全环境内开展活动而制定的行为规范所造成的后果。例如，为网络安全产品和服务定义类似"保险业者实验室"的认证；
- 制定政策，鼓励通过使用高可用性和冗余技术以及服务提供商问责制交付承诺的服务，定义关键基础设施的弹性；和
- 定义行业，政府和学术界之间网络安全研究与创新合作伙伴关系的奖励，使网络安全技术开发朝着网络安全Moonshot计划定义的要求发展，并在未来的员工队伍中提高美国网络技术和网络专业人员的数量和质量。

列间依赖

政策是美国政府确保网络安全Moonshot计划成功实施的主要手段。为此，政策支柱支持技术支柱，特别是因为定义了解决安全问题的技术路线图；行为，其中
政策将推动并在某些情况下规范用户的活动；隐私：随着新法律法规的出台，确保公众有权决定使用其个人信息；和教育，政府为增加网络专业人员而做出的努力影响了K-12教育政策。这些支柱有助于确定倡议的总体治理方向，以创建可信任，有弹性且可访问的安全环境。为了支持总体网络安全"月球计划"，应进行以下政策改革：

- 基于积极奖励措施和避免消极后果；

[45] 例如，企业用户和关键基础设施提供商均应期望实施公认的网络安全框架，如NIST或SANS研究所，可通过现有部门责任通道实施。

- 从其他网络安全“Moonshot倡议”战略支柱的初期和整个阶段开始考虑，而不是在事后考虑或结果考虑；和

- 公平公正地维护美国共同利益，并成为世界榜样，并在可能的情况下促进积极的国际成果和互联网自由。

3.5 网络安全Moonshot计划的挑战

关键建议：在定义了网络安全Moonshot计划的战略框架和相关的国家网络安全研发优先级之后，网络安全Moonshot理事会及相关部门级实体应领导一个国家多利益相关方流程，定义，识别和发起一个或多个网络安全大挑战。网络安全Moonshot委员会也可以在提高知名度和激励符合其目标的分布式行动。

在整个研究过程中，专家们反复强调指出，必须确定一两个特定的初始领域，加快整个国家的发展重点，可以在三到五年的时间范围内取得明显的进展。这些专家强调了这种方法对于立即取得更大突破，帮助建立势头以及为整个网络安全Moonshot计划的长期（10年）愿景建立基础模型的重要性。

NSTAC采用了公认的“大挑战”模型来描述针对特定目标人群的这种方法。简报提供了关于“大挑战”的各种定义，包括：

- 大胆但可实现的科学，技术和创新目标，需要跨技术和非技术学科开展大量活动；

- “北极星”，是政府，企业，大学，非营利组织与国家精英科学家，工程师和公民之间具有高影响力，跨学科合作的平台；

- 组织利用一种独特的技能和能力解决问题的机制，其规模超过其自行解决的规模；和

- 解决本世纪许多最棘手的问题的方法，特别是抓住社会想象力的问题，从而获得政治支持。

NSTAC聆听了在政府，私营企业和非营利组织内部开展“大挑战”倡议的直接经验的专家。这些活动涉及多个学科，在航天，生物医学和公共卫生等领域最为普遍。我们的研究还发现，整个联邦政府都建立了重要的大型挑战社区，并通过总务管理署管理的Innovation.gov和Challenge.gov等资源集中提供了与学科无关的最佳实践最佳实践资源。纪律还没有[46][47]

46 “挑战的挑战”，2018年，Challenge.gov，https://challenge.gov/list.

47 “更好的政府工具包为通过创新建立更好的政府提供了资源，”2018年，Innovation.gov，https://innovation.gov/toolkit/.

建立了同样强大的开放创新文化，以大挑战社区为代表。 NSTAC认为这必须改变。

为此，NSTAC建议网络安全Moonshot委员会牵头确定和发起一个或多个目标网络安全大挑战。为确定合适的大挑战候选人，理事会和相关部门实体应运行六个月的协作流程，让全国私营部门和学术利益相关方正式参与。至关重要的是，这一过程应包括没有专业协会或网络安全专业知识的公民，为对话注入新思路。

3.5.1 鉴定和评价标准

“重大挑战”称号适用于特定重点发展领域，而整个国家的进展轨迹不足，将受益于有针对性的国家关注和战略重点。第3.4节“定义战略框架和支柱”的开头）。在此多利益相关方流程中评估潜在的大挑战候选人时，理事会应提出并衡量几个评估标准和关键问题，包括：

- **明确的政府角色：政府在促进与倡议相一致的全国性活动中是否发挥明确的作用？在先前市场驱动力不足的情况下，政府的战略关注，减少障碍，资源配置或要求可以激励采取行动吗？**

- **合作带来的好处：倡议是否需要开展超出政府机构权限或优势范围之外的活动？这项计划会受益于更广泛，更广泛地利用各种伙伴关系和合作来源的努力吗？**

- **社交共鸣：能否以一种在整个社会，特别是对于非网络安全专家而言在全国范围内具有根本重要性和战略意义的广泛理解来阐明这项倡议？**

- **可衡量和可实现：在整个网络安全Moonshot计划的十年内，是否有可实现的明显里程碑和目标？**

- **高度可扩展：实现该计划的目标是否会产生能够在网络安全防御环境中轻松甚至自动利用的成果？**

- **多维：倡议是否具有广泛的范围，足够全面地涵盖多个战略支柱活动？**

尽管六个月多利益相关方流程提供了多种投入，但仔细考虑这些标准和其他标准，应最终确定一个基于结果的声明，并开展与实现所有六个战略支柱的成果相一致的活动。

大挑战举措的说明性示例：网络安全人工智能

- 白宫宣布在五年内实现网络人工智能技术“圣杯”的奖项
- 面向人群的竞赛，用于自动化威胁防护算法开发
- 开展政策创新/传播运动，使“网络人工智能”与“自动驾驶人工智能”享誉全球
- 教育联盟模型，将学术界和私营企业联系起来，激发，增长和保留用于网络安全应用程序的人工智能专业知识

3.5.2 美国政府在通过网络安全挑战激励行动中的作用

识别阶段完成后，美国政府可以在整个生命周期内提高和维持网络安全大挑战的知名度。代表性的例子包括总统或副总统级别宣布大挑战赛，或高调庆祝大挑战相关重大突破。美国政府还可以通过使用各种工具激励和加速与完成大挑战相匹配的国际活动，不断提高和维持人们的兴趣。其中包括以“ moonshot”方法原理为基础，主要奖励示范和成果实现的工具。

需要明确的是，NSTAC并没有建议美国政府单方面领导开发和发布这些网络安全大挑战并开展所有相关活动。许多非政府实体，例如XPrize和盖茨基金会，在成功实施大挑战和相关奖项竞赛以实现雄心勃勃，注重成果的目标方面拥有丰富的经验。但美国政府可以在激发兴趣，应对挑战，创造潜在民主化和未来商业机会的途径方面发挥关键作用。通过将鼓舞人心且富有影响力的愿景与低成本增材制造，云应用和人工智能等有机新兴技术结合起来，这些网络安全大挑战可以自然地由服务于自身优先事项的公司，学术和非营利资源支持。

Category	Types
1. Pay-for-Performance	A. **Incentive Prizes**: Results-based market incentives that are designed to overcome market failures and catalyze innovation. Unlike "recognition" prizes that honor past achievements, "inducement" or "incentive" prizes encourage participants in the competition to achieve a particular goal.
	B. **Pay-for-Success Bonds**: Also known as a social impact bonds. The financing organization and the Federal, state, or local government enter into a contract that specifies the population to be served, the outcomes to be achieved, the measurement methodology to be used, and the schedule of payments to be made. The financing organization works with philanthropic and other investors to invest in innovative, data-driven service providers that can achieve results.
	C. Mi**lestone-Based Payments**: Terms in a contract in which the payment for each performance milestone established in the statement of work is not made until the prior milestone is proven to have been achieved. Risk is placed on the performer or vendor, unlike other contracts in which payment is either guaranteed with limited protections for quality of performance or in which payments are designed to support in advance the performer's effort to complete the next milestone.
	D. **Challenge Based Acquisitions**: A Federal Acquisition Regulation (FAR)-based acquisition approach that uses challenges to communicate the needed capability, encourage innovation in a minimally prescriptive environment, assess candidate offerings, and, ultimately, purchase the proven solution(s).
2. Purchase Commitments	A. **Advance Market Commitments (AMCs)**: Binding commitments to purchase, or to subsidize purchase, of a certain volume of a product at a fixed prize, if the product meets pre-defined performance characteristics
	B. **Non-Binding Purchase Commitments**: Non-binding commitments to purchase products can provide market pull, if there is both a clearly defined performance specification and a strong expression of interest from potential buyers.
	C. **Buyer's Consortia**: Cooperative agreements between purchasers of products that leverage the combined buying power of those purchasers to drive down the price of products
3. Accelerated Review or Exclusive Access	A. **Priority Review Vouchers**: An accelerated regulatory review offered to products that meet certain performance or cost criteria
	B. **Exclusive Access**: Unique or accelerated access to training, partnership, or procurement opportunities
	C. **Pilot and Third-Party Evaluation Opportunities**: Dedicated opportunities to deploy a pilot implementation a solution/intervention, potentially with resources for third-party evaluation 8

图3：美国政府提供了广泛的"拉机制"，这些工具可以激励与定义好的"大挑战"相一致的以结果为中心的行动。[48]

4.0结论

NSTAC的这份报告介绍了建立全国网络安全" Moonshot倡议"的案例，其基本目标是到2028年确保互联网安全。这一案例是在面对重大国家挑战的基础上实现集体成就的强大历史先例。风险。

这份报告为互联网未来的发展提供了一种抵抗力和弹性，重视个人隐私和问责制，可用和可访问，并充分利用新兴技术能力的路径。这条道路将要求教育和政策发生重大变化，建立美国人可以应对的重大挑战，针对安全行为和恶意行为后果采取更加紧密一致的激励措施，并对互联网的全球互联性质进行基本了解。该报告提出了一条榜样，美国可以以身作则，引领世界，在维护互联网的信任和安全以及我们的数字方式时，应作为指导和警告。依靠生命，失败不是一种选择。

[48] Jennifer Gustetic，"设计和实施重大挑战：借鉴美国宇航局的经验"（向NSTAC网络安全Moonshot小组委员会简介，弗吉尼亚州阿灵顿，2018年8月23日）。

附录A：小组委员会研究方法

总统国家安全通信咨询委员会（NSTAC）网络安全Moonshot小组委员会由来自信息技术，电信和网络安全生态系统的20多个政府，学术界和私营企业实体的代表组成。小组委员会除由NSTAC成员公司派代表参加外，还任命了学术界成员，以确保该小组代表网络安全Moonshot计划倡导的整个国家/地区方法的重要观点。
NSTAC使用多种方法收集信息，包括主题专家的简介，审查大量网络安全报告和文章以及进行策略审查。具体来说，NSTAC：

- 从行业，学术界和公共部门的专家那里收到27份官方简报（附录E），以及与外部专家的许多其他非官方访谈；和

- 对私营部门和联邦政府网络安全政策，法规，报告和最佳实践文件进行了审查。

> “每当遇到无法解决的问题时，我都会把问题放大。我永远无法尝试通过缩小尺寸来解决它，但如果将其放大到足够大，我就可以开始看到解决方案的轮廓。”
>
> -德怀特·艾森豪威尔总统

在2018年2月开始的研究期内，网络安全Moonshot小组委员会举行了约50次会议。在研究的第一阶段，小组委员会有意侧重于接收在网络安全领域以外的类似于“ moonshot”的工作中具有直接经验或专业知识的专家的通报。这种方法的目的是最好地识别领域不可知论 过去如何有效利用整个国家资源实现宏伟成果的实践模型和方法。
NSTAC认为，这对于解放思想超出正常范围至关重要，我们认为，正常范围通常限制我们围绕网络安全开展的全国对话。代表性的例子包括人类基因组计划的情况介绍，高级研究计划局网络的创建 /互联网，美国国际开发署全球公共卫生大挑战以及阿波罗计划。

在研究的第二阶段，小组委员会听取了领先的网络安全专家的意见，开始确定共同的组织原则和预期成果，以实现从根本上安全的网络安全环境。代表性的例子包括专家介绍关键技术，教育，研究与开发，重大挑战和创新政策，以及为网络安全Moonshot倡议结构提供信息的治理模型。

小组委员会成员

Unisys Corporation和小组委员会联席主席Peter Altabef先生Palo Alto Networks和小组委员会联席主席Mark McLaughlin先生

帕洛阿尔托网络和网络安全Moonshot工作组共同领导Sean Morgan先生
Unisys公司和网络安全Moonshot工作组联合领导Thomas Patterson先生

名称	公司
Mr. Mark Bentley	Unisys Corp.
Mr. Christopher Boyer Ms. Cherilyn Caddy	AT&T, Inc.
Mr. John Campbell	National Security Agency
Mr. James Carnes	Iridium Communications, Inc.
Ms. Terri Claffey	Ciena Corp.
Mr. Mark Cohn	Neustar, Inc.
Ms. Kathryn Condello Ms. Amanda Craig-Deckard	Unisys Corp.
Mr. Michael Daly	CenturyLink, Inc. Microsoft Corp.
Mr. Darrell Durst	Raytheon Co.
Mr. Victor Einfeldt	Lockheed Martin Corp.
Mr. Patrick Flynn	Iridium Communications, Inc.
Dr. Boaz Gelbord	McAfee, Inc.
Mr. William Gravell	Dun & Bradstreet, Inc.
Ms. Katherine Gronberg Mr. Dean Hullings	Diogenes Group, LLC
Mr. Rodney Joffe	ForeScout Technologies, Inc.
Ms. Ilana Johnson	ForeScout Technologies, Inc.
Mr. Kent Landfield	Neustar, Inc.
Mr. Gregory Lebovitz Mr. William Ryan	Neustar, Inc.
	McAfee, Inc.
	Equinix, Inc.
	Department of Homeland Security

Mr. Jerry Scarborough	雷神公司Raytheon Co.
Mr. John Scimone	Dell, Inc.
Mr. Robert Spiger	Microsoft Corp.
Ms. Roberta Stempfley	Software Engineering Institute
Mr. Kent Varney	Lockheed Martin Corp.
Mr. Milan Vlajnic	Communication Technologies, Inc.
Dr. Prescott Winter	Oracle Corp.

小组委员会管理

Ms. Helen Jackson	President's National Security Telecommunications Advisory Committee (NSTAC) Designated Federal Official (DFO)
Ms. Sandra Benevides	Alternate NSTAC DFO
Ms. DeShelle Cleghorn	Alternate NSTAC DFO
Ms. Kayla Lord	Department of Homeland Security NSTAC Support
Ms. Stephanie Curry	Booz Allen Hamilton, Inc.
Ms. Laura Karnas	Booz Allen Hamilton, Inc.
Mr. Barry Skidmore	Total Systems Technologies Corp.

AI	Artificial Intelligence
DHS	Department of Homeland Security
DOJ	Department of Justice
DSB	Defense Science Board
FDA	Food and Drug Administration
GPS	Global Positioning System
ICT	Information and Communication Technology
IoT	Internet of Things
MCC	Microelectronics and Computer Technology Corporation
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NS/EP	National Security/Emergency Preparedness
NSTAC	National Security Telecommunications Advisory Committee
NTIA	National Telecommunications and Information Administration
QGP	Quantum General Purpose
R&D	Research and Development
SEMATECH	Semiconductor Manufacturing Technology Consortium
STEM	Science, Technology, Engineering, and Math

5G –
未来的第五代移动网络，国际电信联盟（ITU）的规范尚未完全定义。预计将支持每秒1 0 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）

增材制造–
定义为连接材料以三维（3D）模型数据制造对象的过程，通常是逐层的，与减法制造方法（如机械加工）相反。（增材制造测试工件，Shawn Moylan，John Slotwinski，April Cooke，Kevin Jurrens和M.Alkan Donmez，美国国家标准技术研究院，第119卷（2014））http://dx.doi.org/10.6028/jres.119.017

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）

增强智能–
人工智能的另一种概念化，专注于人工智能的辅助作用，强调其旨在增强人类智能而不是替代人类智能这一事实。（whatis.techtarget.com/definition/augmented-intelligence）

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）

行为生物识别–
学习或获得的行为特征，例如动态签名验证和击键动态。
（NIST生物识别标准计划和资源中心）

生物识别–
使用可测量的生物特征（如指纹识别，语音识别以及视网膜和虹膜扫描）进行身份验证。（牛顿电信词典）

云计算–
一种模型，用于启用按需网络访问共享池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），可以以最少的管理工作量快速配置和发布或服务提供商互动。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任何其他方面造成破坏性影响

这些问题的结合。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，美国法典第42卷519c（e）]（CNSSI 4009，改编）

网络攻击–
针对企业使用网络空间的网络空间攻击，目的是破坏，禁用，破坏或恶意控制计算环境/基础设施；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**）

工业控制系统–
一种用于控制工业过程（如制造，产品处理，生产和分配）的信息系统。工业控制系统包括用于控制地理位置分散资产的监督控制和数据采集系统，以及使用可编程逻辑控制器控制本地过程的分布式控制系统和小型控制系统。（**NIST SP 800-53A，修订版4**）

信息技术–
用于在组织内部以及与客户和供应商联系的系统中提供和支持信息系统（计算机和手动）的设备，过程，程序和系统。（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）

机器学习–
一种人工智能，其中计算机使用大量数据来学习如何执行任务，而不是通过编程来执行任务。（牛津学习词典）

重大网络安全事件–
实际或潜在对公司的信息系统或数据造成不利影响的事件，合理地预期会影响（公司）证券的价值或影响投资者的决策。（**SEC 33-10459**）。

材料科学–
对建筑或制造材料（如陶瓷，金属，聚合物和复合材料）的特性和应用的科学研究。（梅里亚姆-韦伯斯特字典）

国家安全/应急准备（**NS / EP**）通信–
电信服务，用于保持准备状态或响应和管理任何事件或危机（本地，国家或国际），造成或可能造成人员伤害或伤害人口，财产损失或财产损失，退化或威胁到美国的**NS / EP**态势（《联邦法规法典》第二章第**47**章第**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**通信还包括那些系统

和各级政府和私营部门的能力，这些是确保国家安全并有效管理事件和紧急情况所必需的。（NS /
EP通讯执行委员会，根据行政命令（EO）13618，国家安全和应急准备通讯功能分配[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– NIST IR 7298 –修订版2）

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）

量子通信–
与量子信息处理和量子隐形传态紧密相关的应用量子物理学领域。它最有趣的应用是通过量子密码保护信息通道免遭窃听。
（www.picoquant.com/applications/category/quantum-optics/quantum-communication）

量子计算–
一种发展中的计算技术，利用原子的特性通过量子物理学创建完全不同类型的计算机体系结构。量子计算依赖于原子的基本特征，如自旋的方向（从左到右，从右到左）创建状态，如传统的“ 1”或“ 0”计算机使用电能的变化（正负极性）。（牛顿电信词典）

防量子密码学—
防量子密码是一套部署的公钥加密算法，可被功能完备的量子计算机破解（NSTAC提交给新兴技术总裁战略愿景的报告，2017年）

软件保障–
信心十足的程度，即软件无漏洞，不是故意设计在软件中，还是在软件生命周期中的任何时间无意间插入，并且可以按预期的方式运行。（NIST SP 800-163）

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E：书目

阿方索，保罗。
“与网络安全Moonshot计划相关的公用事业监管与州一级机构的协调。”向总统国家安全通信咨询委员会（NSTAC）网络安全Moonshot小组委员会简介，弗吉尼亚州阿灵顿，2018年9月13日。

“阿波罗计划（1963-1972）。”
2013年9月16日。美国国家航空航天局（NASA）。https://nssdc.gsfc.nasa.gov/planetary/lunar/apollo.html.

鲍德·加文。“科学家们告诉参议院，'暗网'和量子通信可以增强网格网络安全。”实用潜水。
2017年10月27日。
https://www.utilitydive.com/news/darknet-and-quantum-communications-could-enhance- 。grid-cybersecurity-scie/508357/

鲍威尔·卢霍。“网络安全，人工智能和机器学习：机遇与挑战。”
2018年9月18日向弗吉尼亚州阿灵顿市国家安全咨询委员会网络安全Moonshot小组委员会简介。

“更好的政府工具包提供了通过创新建立更好的政府的资源。”
2018.Innovation.gov。https://innovation.gov/toolkit/.

“书评：隐私和自由。”
2004年11月24日。Privacilla.org。http://www.privacilla.org/fundamentals/privacyandfreedom.html.

布拉加，马修。“将来，我们将把软件错误搜索留给机器。”主板。
2016年6月16日。https://motherboard.vice.com/en_us/article/mg73a8/cyber-grand-challenge.

卡尔弗特（Calvert），肯尼斯（Kenneth）和詹安丹丹尼（Gianchandani），欧文（Erwin）。“NSF / CISE：概述和'Moonshots'。”向NSTAC网络安全Moonshot小组委员会简介，弗吉尼亚州阿灵顿，2018年3月15日。

战略和国际研究中心。破解技能短缺。
（华盛顿特区：由McAfee赞助，2016年）。https://www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf.

塞尔夫·文顿。“物联网的未来。”
2018年4月5日向弗吉尼亚州阿灵顿市的NSTAC网络安全Moonshot小组委员会简介。

“挑战的挑战。” 2018.Challenge.gov。https://challenge.gov/list.

传播部门协调理事会。行业技术白皮书。
华盛顿特区：NTIA，2017年7月17日。https://www.ntia.doc.gov/files/ntia/publications/cscc_industrywhitepaper_cover_letter.pdf.

通信安全，可靠性和互操作性委员会。2A工作组：网络安全最佳实践最终报告。华盛顿特区：联邦通信

委员会，2011年3月。https://transition.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf

肯尼斯·科宾。“高需求，高薪和高选择性网络安全专家。”
2013年8月8日。首席信息官。https://www.cio.com/article/2383451/careers-staffing/cybersecurity-pros-in-high-demand--highly-paid-and-highly-selective.html.

“关键基础设施领域。”
2018年8月22日。国土安全部（DHS）。https://www.dhs.gov/critical-infrastructure-sectors.

丹尼尔，迈克尔。“网络登月计划的必要政策基础。”
2018年3月27日向弗吉尼亚州阿灵顿市的NSTAC网络安全Moonshot小组委员会简介。

Diamandis，彼得。“量子计算即将带来大规模破坏。”
2016年10月10日。SingularityHub。https://singularityhub.com/2016/10/10/massive-disruption-quantum-computing/.

国土安全部。关键基础设施合作咨询委员会章程。华盛顿特区：国土安全部，2016年11月30日。https://www.dhs.gov/sites/default/files/publications/cipac-charter-11-30-16-508.pdf

“ DHS网络安全计划。”2013年2月6日。美国计算机应急准备小组。https://www.us-cert.gov/security-publications/dhs-cyber-security-initiatives。

司法部。“司法部主持网络安全行业圆桌会议。”
*2018年9月28日。*https://www.justice.gov/opa/pr/justice-department-hosts-cybersecurity-industry-roundtable.

美国司法部。“总检察长宣布发布网络数字任务组报告。”
*2018年7月19日。*https://www.justice.gov/opa/pr/attorney-general-sessions-announces-publication-cyber-digital-task-force-report.

国防科学委员会（DSB）。网络作为战略能力，执行摘要。
华盛顿特区：国防研究与工程部副部长办公室（USD-R&E），2018年6月。
https://www.acq.osd.mil/dsb/reports/2010s/DSB_CSC_Report_ExecSumm_Final_Web.pdf.

DSB。网络威慑。华盛顿特区：美元汇率，2017年2月。https://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf.

DSB。网络供应链执行摘要。华盛顿特区：美元汇率，2017年4月。https://www.acq.osd.mil/dsb/reports/2010s/1028953.pdf

经济学家。“ Equifax遭受的大数据突破具有惊人的暗示。”
*2017年9月16日。*https://www.economist.com/finance-and-economics/2017/09/16/the-big-data-breach-suffered-by-equifax-has-alarming-implications.

“在网络空间中启用分布式安全。”
DHS，2016年10月4日。https://www.dhs.gov/enabling-distributed-security-cyberspace.

弗格森（David Ferguson）和洛林（Lorin）Kavanaugh-Ulku。
“美国国际开发署发展大挑战。”
2018年3月1日向弗吉尼亚州阿灵顿市的NSTAC网络安全Moonshot小组委员会简介。

菲尔德，克雷格。“国家网络计划。”
2018年8月21日向弗吉尼亚州阿灵顿市的NSTAC网络安全Moonshot小组委员会简介。

食品和药物管理局（FDA）。医疗设备网络安全的市场后管理：工业和食品药品监督管理局工作人员指南。华盛顿特区：FDA，2016年12月28日。https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

弗朗廷，迈克尔。“微电子与计算机技术公司。”德克萨斯州
*历史协会。2010年6月15日。*https://tshaonline.org/handbook/online/articles/dnm01.

加拉格尔，帕特里克。“与关键网络安全技术开发相关的教育和研究计划。”
2018年9月11日向弗吉尼亚州阿灵顿市的NSTAC网络安全Moonshot小组委员会简介。

Gibson，David V.和Everett M.
Rogers。研发合作。波士顿：哈佛商学院出版社，1994年。

“全球信息安全劳动力研究。”
2017年。网络安全和教育中心。https://iamcybersafe.org/GISWS.

高盛，丽莎和普马尔，凯特。
“如何发起成功的月球射击，”向NSTAC网络安全月球射击小组委员会简介，弗吉尼亚州阿灵顿，2018年2月20日。

高盛，丽莎和凯特·普马尔（Kate Purmal）。
Moonshot效应：中断日常业务。加利福尼亚州圣卡洛斯：温尼菲尔德商业出版社，2017年。

邓肯Greatwood。“使关键基础设施轻松遵守网络安全法规。”CPO杂志。
2018年10月3日。https://www.cpomagazine.com/2018/10/03/making-compliance-with-cybersecurity-regulations-easy-for-critical-infrastructure/.

格林堡，安德鲁。“NOTPETYA的不朽故事，历史上最具破坏性的网络攻击。”有线。
2018年8月22日https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world

珍妮佛·古斯塔蒂克。“设计和实施重大挑战：借鉴美国宇航局的经验。”

Gustetic，Jennifer等。“美国宇航局小行星挑战：战略，结果和经验教训”。太空政策（2018）。 10.1016 / j.spacepol.2018.02.003。

特里·霍尔沃森。“ 5G网络技术和功能。”
2018年9月5日向弗吉尼亚州阿灵顿市的NSTAC网络安全Moonshot小组委员会简介。

特里·霍尔沃森。“传入：我们现在必须预测5G后果。”信号。
2018年3月1日。https://www.afcea.org/content/incoming-we-must-anticipate-5g-consequences-now.

霍金斯，德里克。“网络安全202：国会准备让国土安全部牵头联邦网络安全。”华盛顿邮报。
2018年9月25日。
https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/09/25/the-cybersecurity-202-congress-poised-to-allow-dhs-to-take-the-lead-on-federal-cybersecurity/5ba915ba1b326b7c8a8d162c/?utm_term=.706f4fe7dca5.
。
海曼·理查德。“学科状态：人工智能。”
2018年9月6日向弗吉尼亚州阿灵顿市的NSTAC网络安全Moonshot小组委员会简介。

Hinden，Robert和Russell Housley。“在互联网上部署安全性的挑战。”
2018年9月25日向弗吉尼亚州阿灵顿市的NSTAC网络安全Moonshot小组委员会简介。

霍夫，罗伯特。“来自Sematech的经验教训。”麻省理工学院技术评论。
2011年7月25日。https://www.technologyreview.com/s/424786/lessons-from-sematech/.

“人类基因组计划完成：常见问题解答。” 2010年10月30日。
国家人类基因组研究所。https://www.genome.gov/11006943/.

艾萨克森·沃尔特。
“建设下一个互联网：为在线通信建立安全和经过验证的身份识别系统的Moonshot”，向NSTAC网络安全Moonshot小组委员会简介，弗吉尼亚州阿灵顿，2018年3月6日。

卡利尔，托马斯。“从白宫和私营部门Moonshots中学到的经验教训。”
2018年2月27日向弗吉尼亚州阿灵顿市的NSTAC网络安全Moonshot小组委员会简介。

刘易斯，詹姆斯。“网络安全Moonshot问题。”
2018年8月30日向弗吉尼亚州阿灵顿市的NSTAC网络安全Moonshot小组委员会简介。

马可夫，约翰。“杀死计算机进行保存。”纽约时报。 2012年10月29日。https://nyti.ms/S91QbY.

道格拉斯·莫恩。“与关键网络安全技术开发相关的加速努力。”
2018年8月28日向弗吉尼亚州阿灵顿市的NSTAC网络安全Moonshot小组委员会简介。

麦康奈尔，布鲁斯。“确保[全球]互联网安全。 。 。到2028年。” 2018年8月22日向弗吉尼亚州阿灵顿市的NSTAC网络安全Moonshot小组委员会简介。

Mervis，Jeffrey。
“数据检查：美国政府在基础研究经费中的份额下降到50%以下。”科学。
2017年3月9日。http://www.sciencemag.org/news/2017/03/data-check-us-government-share-basic-research-funding-falls-below-50.

美国国家航空航天局。美国宇航局概况：阿波罗的好处：技术上的巨大飞跃。德克萨斯州休斯顿：美国宇航局。
2004年7月。https://www.nasa.gov/sites/default/files/80660main_ApolloFS.pdf.

“国家应急通信计划目标。”国土安全部，2018年5月17日。https://www.dhs.gov/national-emergency-communications-plan-necp-goals.

NSTAC。 NSTAC就新兴技术战略愿景向总裁提交报告。
华盛顿特区：NSTAC，2017年7月14日。https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Emerging%20Technologies%20Strategic%20Vision.pdf.

NSTAC。
NSTAC致信息和通信技术动议主席报告。华盛顿特区：NSTAC，2014年11月19日。
https://www.dhs.gov/sites/default/files/publications/NSTAC%20-%20Information%20and%20Communications%20Technology%20Mobilization%20Report%2011-19-2014.pdf。

NSTAC。 NSTAC就互联网和通信弹性向总统报告。
华盛顿特区：NSTAC，2017年11月16日。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%20compliant_0.pdf.

NSTAC。
NSTAC就物联网向总统报告。华盛顿特区：NSTAC，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.

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，华盛顿特区：NTIA，2017年7月。https://www.ntia.doc.gov/files/ntia/publications/iotsecuritystandardscatalog.pdf.

NTIA。促进物联网发展。华盛顿特区：NTIA，2017年1月。https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf.

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

纽约网络任务组。建立可防御的网络空间。纽约：哥伦比亚大学国际与公共事务学院，2017年9月28日。

https://sipa.columbia.edu/sites/default/files/3668_SIPA%20Defensible%20Cyberspace-WEB.PDF.

Nielsen，KirstjenM。“ Kirstjen M. Nielsen秘书在RSA会议上的讲话。”讲话，2018年4月17日，加利福尼亚州旧金山。演讲。https://www.dhs.gov/news/2018/04/17/secretary-kirstjen-m-nielsen-remarks-rsa-conference.

奥赫恩，威廉。“向NSTAC网络安全Moonshot小组委员会5G网络和标准简介。”向NSTAC网络安全Moonshot小组委员会简介。弗吉尼亚州阿灵顿，2018年9月18日。

管理和预算局（OMB）。关于使用挑战和奖项促进开放政府的指南。2010年3月。https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2010/m10-11.pdf.

彭斯，迈克尔。彭斯副总统在国土安全部网络安全峰会上的讲话。2018年7月31日。https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-dhs-cybersecurity-summit/.

佩里罗，杰里。向NSTAC网络安全Moonshot小组委员会简报“洲际交易所/纽约证券交易所”。弗吉尼亚州阿灵顿，2018年9月27日。

Poindexter，JohnM。“互联网问责制”。向NSTAC网络安全Moonshot小组委员会简介。弗吉尼亚州阿灵顿，2018年3月22日。

罗森布拉姆，托德。“网络安全：国家权力的整体方法。”密码简介。2017年1月11日。https://www.thecipherbrief.com/column_article/cybersecurity-a-whole-of-national-power-approach.

Rung，Anne E.和Tony Scott。“数据采集创新实验室和数字数据采集创新实验室试点。”备忘录由Anne E. Rung和Tony Scott致首席采购官，高级采购执行官和首席信息官。2016年3月9日。https://www.dhs.gov/sites/default/files/publications/March%202016%20Memo.pdf.

肯尼思·鲁特科夫斯基。“主持会议。”2018年4月10日向弗吉尼亚州阿灵顿市的NSTAC网络安全Moonshot小组委员会简介。

萨贝特，兰迪。“基于激励的政策在整个国家网络安全战略中的作用。”2018年9月26日向弗吉尼亚州阿灵顿市的NSTAC网络安全Moonshot小组委员会简介。

“ SANS信息安全培训。”2018年。SANS研究所。https://www.sans.org/.

塞弗斯，乔治。“ AFCEA：需要采用全国网络安全方法。”信号。https://www.afcea.org/content/afcea-whole-nation-cybersecurity-approach-needed.

瑟布，贾里德。
“国防网络小组说，外国网络武器“远远超过”美国防御关键基础设施的能力。”联邦新闻网。 2017年3月17日。https://federalnewsnetwork.com/dod-reporters-notebook-jared-serbu/2017/03/foreign-cyber-weapons-far-exceed-u-s-ability-defend-critical-infrastructure-defense-panel-says/.

火花。“我们的政府如何适应不断变化的网络安全和信息技术基础设施需求。”
*2017年7月。*https://www.icf.com/blog/cybersecurity/how-government-can-adapt-to-evolving-cybersecurity-needs.

“利益相关方参与和网络基础设施弹性。”国土安全部（DHS），2018年8月22日。
https://www.dhs.gov/stakeholder-engagement-and-cyber-infrastructure-resilience.

斯图德曼，威廉。“与NSTAC网络安全Moonshot小组委员会的对话。”
2018年3月22日向弗吉尼亚州阿灵顿市的NSTAC网络安全Moonshot小组委员会简介。

美国选举援助委员会（EAC）。起点：美国选举系统为关键基础设施。马里兰州银泉市：EAC
https://www.eac.gov/assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf.

维斯纳，塞缪尔。“网络安全Moonshots。”
2018年3月29日向弗吉尼亚州阿灵顿市的NSTAC网络安全Moonshot小组委员会简介。

Waldrop，M。Mitchell。“大转变。”
2017年3月8日向弗吉尼亚州阿灵顿市NSTAC网络安全Moonshot小组委员会简介。

威斯汀，艾伦。隐私和自由。纽约：IG出版社，1967年。

扎克海姆，DovS。“组建政府应对网络挑战。”
2018年9月27日向弗吉尼亚州阿灵顿市的NSTAC网络安全Moonshot小组委员会简介。