免责声明:凡在本杂志发表的文章只代表作者观点，而非美国国防部、空军部、空军教育和训练司令部、空军大学或美国其他任何政府机构的官方立场。

树立太空依赖网空意识，做好网空作战准备

Preparing for the Cyber Battleground of the Future

克里斯·巴布科克，美国空军少尉（2nd Lt Chris Babcock, USAF）

对于美国空军的太空和网空战士而言，明天战争的胜负，很大程度上将取决于对网空依赖性概念的认识。笔者对这个概念所下的定义是：一种军事能力为了实现其军事行动效应而必须依赖其在网空领域某一部分所占优势的程度。[1] 我军对网空的依赖性在急剧增长，原因包括网空领域按几何级数快速发展和变化，民营市场力量强力推动，以及军方在海陆空诸领域对计算机技术实施战略性整合。[2]

在太空领域运用作战能力，若不依赖网空就无法开展，这一点非常不同于三个传统的作战领域。[3] 认识太空和网空之间的这种独特关系，对于兵员招募，战士的初始、中级和高级训练，以及在太空和网空职业领域的发展都有深远的意义。由当前的部队建设系统向认可太空与网空这种独特关系的新部队培养方向转变，还将产生更多益处，使广大作战部队成员都能明白这种关系的重要性，因为海陆空领域的战斗人员都越来越依赖网空和太空。本文探讨网空依赖性的含义，并提出六项建议，以期确保空军的太空和网空战士从招募到高级训练等各个阶段都能处于最佳战备状态，在其相互关联的各领域有卓越的表现。

太空行动高度依赖网空

> 太空和网空关系的独特性在于几乎所有的太空作战行动都依赖网空，而网空的某些关键功能也只有通过太空行动才能提供。
>
> — 联合出版物 3-12（R）《网空作战行动》，2013 年 2 月 5 日

目前美国武装部队执行的所有太空作战行动都依赖网空（图 1）。[4] 太空作战行动发生在实际的太空领域，不是在网空领域。但是，由于执行太空作战的战士通常不可能身处太空，因此必须完全依赖其对自己负责的那部分网空的控制，把操作指令传输给航天器，以执行太空作战行动。[5]

假设在某次太空军事行动中，有宇航员实际置身航天器舱内，对周围环境做出反应，以在太空实施作战效应，那末，该次太空作战行动就不是完全依赖网空优势。[6] 如果不是这种情况，太空战士则必须使用专门的计算机和计算机程序，通过计算机网络把信息传输给他们操纵的航天器并接收来自航天器的信息——而这些航天器本身也是复杂的信息系统。[7] 鉴于太空作战行动对网空的依赖，我们必须特别注意太空作战能力的网空防卫，这也预示了传统作战领域的未来状况。

网空的物理网络层包括太空战士用于指挥卫星的信息系统、把这些信息系统连接至

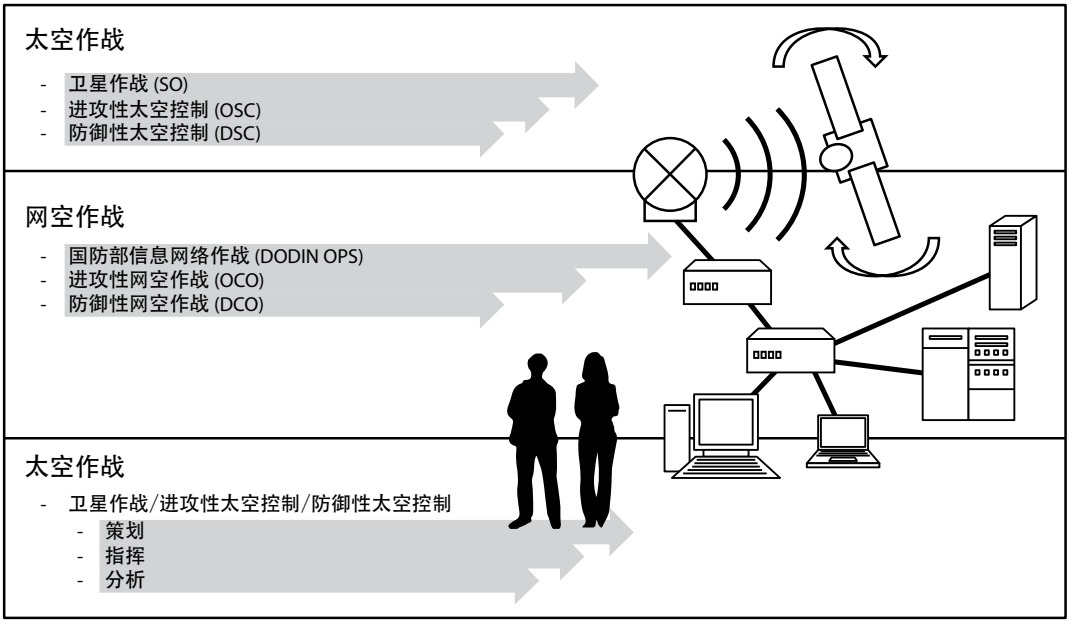

图 1：太空和网空作战行动。由于太空战士无法身置太空，太空作战行动在网空领域内外发生。

地面设备的电路，以及地面设备本身。网空的逻辑网络层嵌入于物理网络的各个部分。网空的人员层是指依赖物理网络层和逻辑网络层执行太空作战行动的太空战士（图 2）。

网空领域按几何级数快速发展和变化

> 如果你认为你在网空很安全，当你第二天醒来时，也许一切已面目全非。
>
> ——空军太空司令部司令约翰·海滕将军（Gen John E. Hyten）

英特尔集团共同创始人戈登·摩尔先生（Gordon Moore）曾在 1965 年指出，计算机电路的能力按几何级数的速度与时俱增。自那时以来，众所周知，计算机技术的创新以史无前例的速度涌现。[8] 一波创新带动另一波创新，信息技术一变再变，对网空战士带来独特的挑战，网空挑战与之前的四个作战领域大不相同。[9]

第一个挑战是，在多个技术创新领域，民营企业现已开始高速超越国防工业。[10] 出现这种情况的主要原因是，国防部大型技术计划的采购和配置管理流程像糖浆一样黏滞不动，而硅谷的创业公司却动作敏捷，办事利索。[11]

第二个严峻挑战是，网空的非对称性使得攻击方能够比防卫方更快和更容易地利用其中的快速变化而抢占上风。[12] 在基本层面，网空防卫方试图确保软件和硬件能够正常工作，而网空攻击方则试图破坏软件或硬件以造成危害效应。[13] 在这种对抗中，侵略方几乎总是占上风。此外，网空按几何级数的速度变化，使得体制教育下的知识和个人技能快速过时，过时之快，远超过传统作战领域的情形。这种情况给网空战士的训练和教育带来令人深思的挑战。

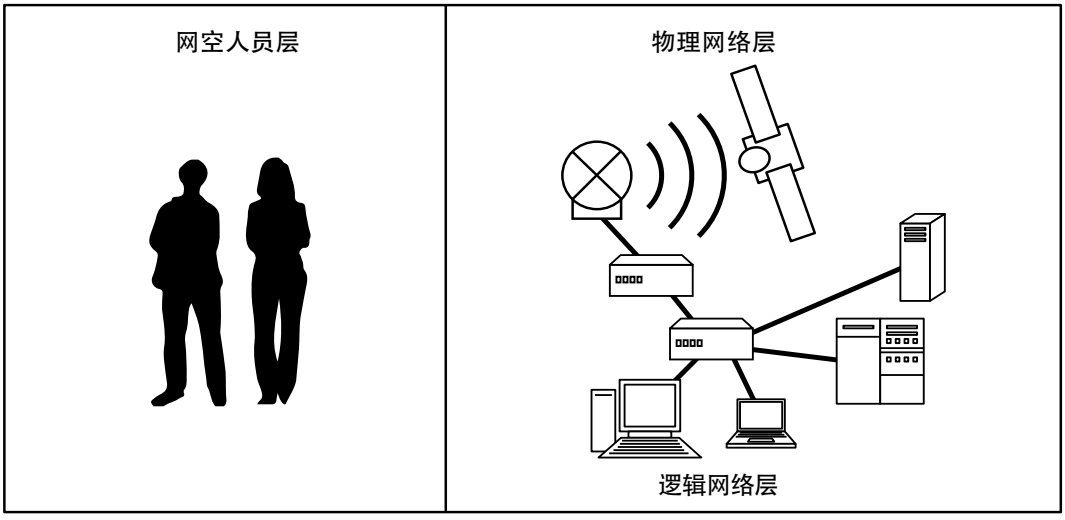

图 2：太空作战行动中的网空层次

尽管存在这些困难，美国空军还能很好地掌控目前的网空战场。但是，它必须充分考虑网空依赖性的特征，以及该依赖性对于不断扩展的未来网空战场的影响。

网空依赖性源自我们自身

> F-35 闪电 II 型是有史以来最复杂的武器系统之一，这种外形流畅的隐形喷气式战斗机是多年精心研发的成果，经常被称为飞行计算机，因为它有 800 多万条代码。
>
> ——克里斯琴·达文波特（Christian Davenport），《华盛顿邮报》

尽管太空领域是第一个完全依赖网空的领域，但是它不是唯一的。在天空领域，遥驾飞机就是很好的例子，它是一个完全依赖网空的武器系统。[14] 甚至最新的有人驾驶战斗机 F-35 也被称为飞行的计算机。此外，陆军正在研发个人无人机、穿戴式智能承重骨架和计算机操控的步枪；国防部先进研究项目局正在研发机器骡；而海军则在研发自主化无人器，包括无人潜艇和无人飞机。[15]

这些研发努力肯定会提升作战能力，但同时也将提高网空依赖性，并为此付出代价。这些代价可能体现为这些技术所支持的作战任务将面临更大的风险，或者是新的依赖性系统需要有精密的网空安全保护和积极防卫。[16] 在各种情况下，网空依赖性带来的内在风险都会很大。在民间，黑客已经能够控制车辆（最值得注意的是，能够完全遥控最新型号的吉普车）、智能枪和业余无人机，他们甚至已经渗入商业飞机的内部网络。[17] 对于未来的网战部队而言，战区武器系统的安全和防卫——从地面、空中到太空——都必须是首要任务之一（图 3）。

网空战士将面临的一个特别棘手的挑战是，必须在武器系统的实时运行网络上执行网空作战行动。但是，他们必须而且能够克服这个挑战。[18] 如果放弃安全保护和防卫，则将面对更大的风险，因此更不可取。在网空，未及时补救的薄弱点存在时间越长，它被敌

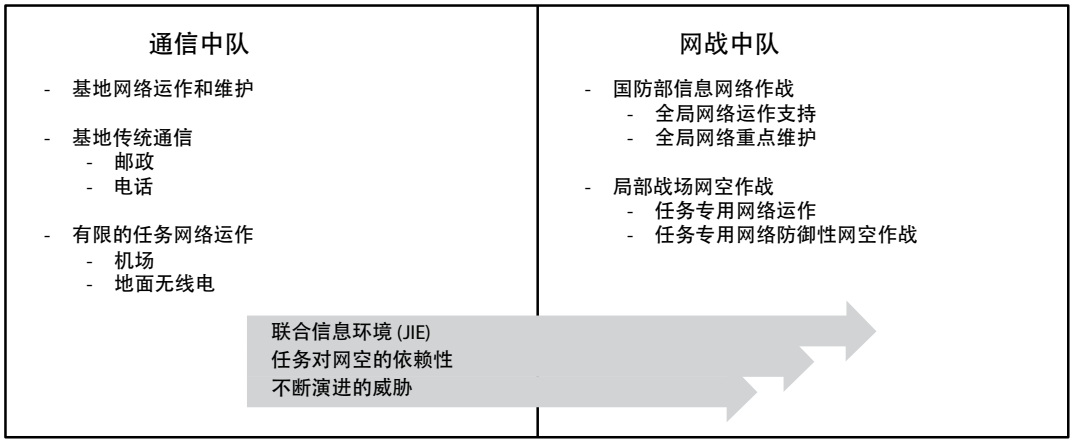

图 3：从通信到网空（部分根据戴维・卡纳迪中校 [Lt Col David Canady] 的战况简报，主题：Cyber Squadron of the Future [未来的网空作战部队], Headquarters US Air Force / A6CF, May 2014, http://www.safcioa6.af.mil/shared/media/document/AFD-140512-040.pdf.）

方乘虚而入加以利用的可能性就越大。根据某些资料，从发现漏洞到乘虚而入进行攻击，黑客只需要大约一个星期的时间就可以完成。[19]

国防部并未因为担忧网空安全问题而停止采购越来越依赖网空的武器系统。在民间，普通消费者似乎也没有因为担忧网空安全问题而不再购买相关消费品。

网空依赖性因市场驱动而加强

> 这些特征和条件导致网空内出现自相矛盾：一方面，美国的繁荣和安全因我们使用网空而显著提升，另一方面，这些事态发展却又导致我们有了更多的薄弱点，并且更紧密地依赖网空，美国全国如此，具体到我们的联合作战界尤其如此。
>
> ——联合出版物 3-12 (R)《网空作战行动》，2013 年 2 月 5 日

民间的市场力量正在把许多类别的消费产品快速推向“物联网”。据估计，到 2020 年，世界上将有 500 亿至 1000 亿台装置通过网络相互联结，形成物联网。[20]

从冰箱到咖啡壶和恒温器，各种各样的自动联入互联网的网感联装置越来越多地涌入商业市场。[21] 可以说，在最近的将来，市场上的大多数装置都将具备因特网感联功能，从而使得像国防部这样小心谨慎的消费者很难找到不受计算机操控的替代装置。[22] 于是军方将面临两难抉择：是接受风险，还是接受与这些新一代联网冰箱和咖啡壶相关的网空安全及防卫代价。

如果我们相信，今后将有更高比例的装置、基础设施和系统具有计算机联网能力，它们将是军事单位的一个永久组成部分（例如监控与数据采集 [SCADA] 装置）或者将会经常进入军事单位（例如智能手表和自驾汽车），那末，这些装置将在实际上成为网空作战空间的一部分。未来的网战部队应该承担保护和防卫这些装置的责任。随着组织和结构变更（例如转换到联合信息环境）所提供的效率提升，以及新的技术（例如软件定义

的联网能力)，我们可以腾出很多必要的资源，使得未来的网战部队能够保护和防卫扩展的网空领域；但是，我们还需要做出其他投资和改革，以支持这些新的要求。[23]

打赢明天的战争

鉴于整个军方快速向着更加依赖网空的方向发展，空军太空司令部应该审视和考虑下列关于网空和太空部队建设系统的建议，不可掉以轻心。[24]

利用大数据进行决策

空军太空司令部应该制定三套标准测验，并且在部队建设流程中实施这些测验，用于评估空军的太空和网空战士。第一套测验应该着眼于检验网空技能熟练程度和资质，主要测定新兵或受训学员理解网空概念和掌握网空技能的潜力，无论被测验者是否接受过正式的网空训练。[25] 第二套和第三套测验专注知识检查——其中一套是关于网空作战适用知识的测验，另一套是关于太空作战适用知识的测验。起初，也许不可能确定究竟要达到什么程度才算熟练，这不要紧，不应该导致司令部放弃这些测验。把这三套测验的分数汇总时，必须与各个被测验者关联，并且与其他衡量数据综合考虑，以确定测验分数与个人的专业能力是否优秀、中等或不合格有何相关性。数据汇编和分析流程应该不断地充实对这些测验的周期性评判，借以确保测验能正确地评估个人能力和知识。

与测验分数关联的数据点分为三大类：教育、训练、经验。通过综合考虑熟练程度和知识测验分数以及来自这三大类的数据点，空军太空司令部将能够确切把握和安排教育、训练和经验的轻重缓急，据此做出部队建设决策。通过在关键时刻重复测验空军战士，太空司令部将能够了解特定的训练活动或教育课程对于测验分数有何影响。[26]

提供针对特定任务的网空训练

空军太空司令部即将建立一个最佳框架，用于网空作战行动初始、中级和高级训练系统。目前的中级训练注重特定任务的针对性，有别于一般中级训练和在职训练，是朝着正确的方向迈出了一大步。[27] 随着网空依赖性越来越强，我们将需要提供更多的特定任务针对性训练课程，例如监控与数据采集和物联网防御作战行动，也需要有更多的针对空军各种地面、太空和空中任务系统的中级网空防卫训练。

对于应征入伍的空军士兵而言，1B 初始训练课程应该分为一门 3D 和 1B 综合初始训练课程，以及若干中级训练课程，后者针对 1B 和 3D 空军士兵将遇到的特定任务要求。通信职业领域作战化不应该剔除 3D 职业领域，因为该领域在网空战场的安全和防卫方面起着重要作用，并且将继续如此。划分 3D 和 1B 职业领域训练要求的工作应该遵循美国国家标准与技术研究院国家网空安全教育框架计划的准则。[28] 入伍的 3D 和 1B 空军士兵在接受共同的基础训练之后，其各自的训练课程很快岔开，但是这两个职业领域的空军士兵必须有一套共同的核心“网空作战”基本要则。[29]

向依赖网空的战士提供专门训练

空军中许多官兵，虽不属网空部队，但是其所执行的使命和任务具有高度网空依赖性，例如太空作战人员和遥驾飞机驾驶员，应该给他们提供学习机会，让他们参加适合其任务的中级和高级网空作战训练。训练计划在录取非网空编制官兵时，应将其网空技

能熟练程度和知识测验分数作为考虑依据之一。

正如让武器军官了解各类武器系统是有益的做法；同样地，让执行网空依赖性任务的军官了解网空作战也是有益的做法。[30] 我们应该建立一个在许多方面类似美国空军武器学校提供的训练计划（只是规模小些），从战略上看，完成此训练的毕业生在各自的网空依赖性职业领域内可发挥重要作用。[31]

扩展与业界伙伴的合作机会

空军太空司令部应该与负责采办的空军助理部长办公室和空军理工学院携手合作，建立一个特别管道，让太空和网空职业领域的空军官兵能够进入业界合作教育（EWI）计划学习。如果无法实现这样的安排，空军太空司令部应该考虑建立一个类似的课程计划，其重点是把业界的先进创新和专门技能推介给军方，同时继续扩展与业界合作伙伴的联系。

业界合作教育计划的毕业生不仅能够帮助军方弥补自身落后于民营企业的技术和技能缺口，而且能够在太空和网空领域发展的关键时刻帮助军方和民营企业加强合作和联系。[32] 太空司令部应该注重让空军官兵融入拥有先进太空和网空技术的公司，并且扩展与业界的联系，不仅继续与传统的具有机密资格的国防承包商合作，还要扩大这个范围。

尽管一般空军士兵不可能都进入业界合作教育计划，但是参加业界合作教育计划学习的军官可以培养和发展太空及网空领域所要求的独特技能，借鉴领导和管理方式，吸收创新思想，而参加合适课程学习的空军士兵则可提升其任务和职业领域需要的特定编程或其他技能。

这些做法将同国防部长阿什顿·卡特提出的、在国防部范围内增加创新活动和加强军方与业界联系的行动计划相一致。[33] 除了与负责采办的空军助理部长办公室和空军理工学院就业界合作教育计划进行协调之外，空军太空司令部还应该寻求与国防部设在硅谷的新机构即国防创新试验部建立直接联系。[34] 由于国防创新试验部的主要工作是在网空作战领域发展和加强与业界的联系，太空司令部通过与该部协作，可在网战部队建设方面获益匪浅。[35]

鼓励新形式的教育和训练

民间市场设有各种基于互联网的微学位课程、纳米学位课程和其他形式的短期专题训练课程，极大地增加了空军官兵可以利用的、成本效益高的教育和训练机会。[36] 微学位课程和其他新形式的网上课程所需的时间比副学士课程短，但比传统的训练课程长，此类新形式课程在最近几年大量涌现。空军太空司令部应该积极接纳和探索这个趋势，视其为训练和教育太空及网空战士的一个途径。与 Udacity、Coursera、edX 等网上教学公司或其他大型公开在线课程提供商建立伙伴合作关系，可以带来很多机会，让空军官兵能够获得适合空军太空司令部需要的专题教育和训练，而学员面临的入学费用及时间负担却要少得多。[37]

传统型教育仍可发挥非常重要的作用，但是太空司令部应该采取积极措施，调研这些教育技术正在如何改变民营教育市场。[38] 微学位课程可以向空军官兵提供更敏捷、更具有专题针对性和能够更好地对实际需求做出反应的教育形式，使空军官兵能随时跟上信息技术领域的快速发展步伐。除了符合个人需求的教育和训练之外，太空司令部与大

型公开在线课程公司的伙伴合作关系也可为空军太空和网空全体部队官兵提供成本效益较为理想的训练方式。[39]

加大对网空训练单位的投资

在所有的作战领域中，按几何级数快速变化的网空领域使得“讲授网空课程”经常成为颇具挑战性的任务。相对而言，飞行员接受的空中作战训练或太空战士接受的太空作战训练，年复一年，没有多大变化，但是网空领域的训练教材也许不出几个月就会过时。[40]

不仅网空战士的技能和知识更新远比其他领域更快，为网空训练和教育编写的教材同样很快就会过时。[41] 对于每一门网空课程，也许指派一名教员已经不够，空军太空司令部应该考虑再配备一名教员，其职责包括根据网空领域的状况变化快速修订课程教材以及根据对学生反馈和学业表现的分析及时调整教材。

授课的教员负责讲课、评分和管理，编写教材的教员则负责确保课堂教学符合预定进度和教材内容切题。编写教材的教员应该尽可能融入作战单位和 / 或民营业界合作伙伴企业，在那里短期蹲点，借以获得最新的知识和技能。[42] 网空教程像一个具有已知薄弱点的信息系统一样，不能一成不变，否则要出问题；必须把这些教程视为持续不断在演变的系统。对于每一个授课教员群体，应该有一个人数相等或更多的教材编写教员群体，责成他们持续不断地修订教程。

结语

在所有的作战领域中，网空是变化最急速的。这些变化推动空军的任务和武器系统向更紧密依赖网空和太空的方向发展。空军太空司令部需要理解、预测和在全军实施更高程度的网空依赖性，从而培养空军太空和网空战士做好与时俱进的战备，确保在未来的网空战场致胜。

空军太空司令部应该考虑采取本文的几项建议，包括利用大数据做决策，继续发展针对特定任务的网空训练，向依赖网空的战士提供网空训练，加强与业界伙伴合作，鼓励新形式的教育和训练，以及加大对日益壮大的网空训练单位的投资。这些投入或大或小，但一旦空军太空司令部突然置身于未来的网空战场时，它们都会产生可观的回报。我们可以想象，在不远的将来，我们的空军将成为一支完全依赖太空和网空的部队；我们还可以预见，这支空军的网空防卫能力远远超过其对太空和网空的依赖所引发的新威胁。克服网空依赖性挑战，让我们从现在开始。★

注释:

1. 可以用网空依赖程度来描述任何军事能力、技术或战略。网空领域主宰优势类似于制空权，本文作者给其定义是：对网空某一部分或某一区段保持一定程度的优势，使敌网空部队在那里无法进行有效干扰。
2. 市场力量将驱动军方占有和防卫更大的作战空间，而美军自身也会以更有成效的方式有目的地扩展网空作战空间。
3. Joint Publication (JP) 3-12 (R), Cyberspace Operations [网空作战行动], 5 February 2013, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf. 联合出版物 JP 3-12 称其为太空与网空的“[独特] 关系”。本文作者则称其为“领域的网空依赖性”，因为太空领域的所有作战行动目前都依赖网空优势。
4. 同上；以及 JP 3-14, Space Operations [太空作战行动], 29 May 2013, http://www.dtic.mil/doctrine/new_pubs/jp3_14.pdf.

5. JP 3-12 (R), Cyberspace Operations [网空作战行动], 把网空定义为“许多不同而且经常重叠的网络，以及这些网络上的节点（带有互联网协议 [IP] 地址或其他相似标识符的任何装置或逻辑位置），还有支持它们的系统数据（例如路由表）”(I-2)。

6. 同上。

7. 同上。就太空作战行动而言，网空的物理网络层包括：太空战士用以执行指挥与控制操作以及接收和分析远程数据的信息系统；把这些信息系统连接至地面设备的电路；地面设备本身，这些设备准备和传送数据给航天器；以及航天器本身。网空的逻辑网络层内嵌在物理网络的各个部分。当太空战士变更物理网络层任何部分的配置或向其传送指令、加密或解密传输内容，或者执行数据融合和分析的时候，他们就是在网空的逻辑网络层内进行操作。在某种程度上，这些动作可以被视为网空作战行动。网空的人员层是指依赖物理网络层和逻辑网络层执行太空作战行动的太空战士。网空人员层还包括可能通过其网空作战行动而扰乱太空作战行动的潜在敌方人员。

8. Damon Poeter,“How Moore's Law Changed History (and Your Smartphone)”[摩尔定律如何改变了历史（以及您的智能手机）], PC, 19 April 2015, http://www.pcmag.com/article2/0,2817,2482133,00.asp.

9. JP 3-12 (R), Cyberspace Operations [网空作战行动]; 另参看 Mark Pomerleau,“Army Cyber Chief Outlines Key Challenges, Goals”[陆军网空首长概述关键的挑战和目标], Defense Systems, 18 March 2015, http://defensesystems.com/Articles/2015/03/18/Army-cyber-Cardon-outlines-challenges-goals.aspx.

10. Max Boot,“The Paradox of Military Technology”[军事技术悖论], New Atlantis, no. 14 (Fall 2006): 13-32.

11. Jose Pagliery,“Love, Not War: Pentagon Courts Silicon Valley”[出于爱而非战争：五角大楼向硅谷示爱], CNN, 23 April 2015, http://money.cnn.com/2015/04/23/technology/security/military-silicon-valley/.

12. Lt Col Gregory Conti and Col John“Buck”Surdu,“Army, Navy, Air Force, and Cyber—Is It Time for a Cyberwarfare Branch of Military?”[陆军、海军、空军，还有网空 — 是否到了应该建立网空作战军种的时候 ?], IAnewsletter 12, no. 1 (Spring 2009): 14-18; 另参看 Andrew Phillips,“The Asymmetric Nature of Cyber Warfare”[网空战的不对称性质], US Naval Institute, 14 October 2012, http://news.usni.org/2012/10/14/asymmetric-nature-cyber-warfare.

13. 同注 3，“网空作战行动”。

14. Katia Moskvitch,“Are Drones the Next Target for Hackers?”[无人机是黑客攻击的下一个目标吗 ?], BBC, 6 February 2014, http://www.bbc.com/future/story/20140206-can-drones-be-hacked; 另参看 Aliya Sternstein,“How to Hack a Military Drone”[如何对军用无人机进行黑客攻击], DefenseOne, 29 April 2015, http://www.defenseone.com/technology/2015/04/how-hack-military-drone/111391/.

15. Christian Davenport,“Meet the Most Fascinating Part of the F-35: The $400,000 Helmet”[F-35 飞机上最令人惊叹不已的部分：价值 400,000 美元的头盔], Washington Post, 1 April 2015, https://www.washingtonpost.com/news/checkpoint/wp/2015/04/01/meet-the-most-fascinating-part-of-the-f-35-the-400000-helmet/; 另参看“Insects Inspire Military Mini Drones”[昆虫启示了军用微型无人机的研发], Fox News, 18 September 2014, http://www.foxnews.com/tech/2014/09/18/insects-inspire-military-mini-drones/; 另参看 Joyce P. Brayboy,“Army Researcher's Interest in Robots Leads to Innovative Device”[陆军研究人员对机器人的兴趣导致创新装置问世], US Army, 2 July 2015, http://www.army.mil/article/151527; 另参看 Terri Moon Cronk,“Robot to Serve as Future Military's 'Pack Mule'”[机器人在未来充当军方的“驮载骡”], US Department of Defense, 19 December 2012, http://archive.defense.gov/news/newsarticle.aspx?ID=118838; 另参看 Brendan McGarry,“U.S. Military Begins Testing ‘Smart' Rifles”[美国军方开始测试“智能”步枪], DefenseTech, 15 January 2014, http://defensetech.org/2014/01/15/u-s-military-begins-testing-smart-rifles/; 另参看 Kris Osborn,“Navy to Deploy First Underwater Drones from Submarines”[海军将从潜艇部署第一批无人潜水器], Military.com, 13 April 2015, http://www.military.com/daily-news/2015/04/13/navy-to-deploy-first-underwater-drones-from-submarines.html.

16. 对网空安全最常见的理解是，严格遵守制度规定，例如按规定管理薄弱环节和实施保护措施。这与主动防卫不一样，主动防卫是指预期会发生网空事件或与敌交战，因而在之前、之中或之后主动实施相应的防卫措施或行动。

17. “The Pentagon Got Hacked While You Were at Def Con”[当您正在参加国防会议时五角大楼遭到黑客攻击], Wired, 9 August 2015, http://www.wired.com/2015/08/security-news-week-pentagon-got-hacked-def-con/; 另参看 Andy Greenberg,“Hackers Remotely Kill a Jeep on the Highway—with Me in It”[黑客远程攻击导致一辆吉普车在高速公路上熄火 — 而我当时正在车内], Wired, 21 July 2015, http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/; 另参看 Kim Zetter,“Is It Possible for Passengers to Hack Commercial Aircraft?”[客机上乘客有可能对民航机进行黑客攻击吗 ?], Wired, 26 May 2015, http://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft/; 另参看 Hallie Golden,“Security Experts Point to OPM's Biggest Cybersecurity Failure”[安全专家指出联邦人事管理局最大的网空安全漏洞], NextGov, 21 July 2015, http://www.nextgov.com/cybersecurity/2015/07/security-experts-point-opms-biggest-cybersecurity-

failure/118274/. 这些例子中的安全隐患都是安全专家发现的，而不是专业的“军事化”黑客。如果有一个组织良好、技术先进和锲而不舍的威胁集团动用其资源攻击类似的目标，其后果可能会严重得多。

18. JP 3-12 (R), Cyberspace Operations [网空作战行动]. 历来，网空领域需防卫的作战空间大部分是支持主要任务的通信基础设施。网空依赖性增强之后的一个影响是，需防卫的作战空间将扩大到包括任务系统本身。由此产生的挑战是，在直观层面，出于防卫目的而在任务或武器系统上操作时，己方行动对任务的扰乱可能大于防卫通信基础设施时造成的扰乱。

19. Recorded Future Special Intelligence Desk,“Week to Weak: The Weaponization of Cyber Vulnerabilities”[一周内即可乘虚而入：利用网空薄弱点实施攻击], Ref ID: 2014-02 (Somerville, MA: Recorded Future, 4 December 2014), http://go.recordedfuture.com/week-to-weak-report. 2014 年底发布的“一周内即可乘虚而入”报告展现了网空薄弱点被快速利用和公开暴露的情况。据 Recorded Future 公司的分析揭示，一个网空薄弱点平均在 7.5 天之内就会被人利用。作为参考资料，该报告引用了美国国家标准与技术研究院（NIST）发布的数据，即 2014 年大约有 7,000 个新揭示的网空薄弱点。这说明薄弱点管理等网空安全措施必须以令人难以置信的速度加以实施，才能将风险控制在适宜的水平。

20. “Standards Are Making the Internet of Things Come Alive”[标准给予物联网生命], IEEE Standards Association, 8 April 2013, http://standardsinsight.com/ieee_company_detail/standards_iot; 另参看 Dr. W. Charlton Adams Jr.,“The Internet of Things and the Connected Person”[物联网和联网者], Wired, December 2014, http://www.wired.com/insights/2014/12/iot-connected-person/.

21. Klint Finley,“Hacked Fridges Aren't the Internet of Things' Biggest Worry”[遭受黑客侵入的冰箱不是物联网最需要担心的事情], Wired, 12 March 2015, http://www.wired.com/2015/03/hacked-fridges-arent-internet-things-biggest-worry/; 另参看 Bill Wasik,“In the Programmable World, All Our Objects Will Act as One”[在可编程世界中，我们的所有物件都将会连接成一个整体], Wired, 14 May 2013, http://www.wired.com/2013/05/internet-of-things-2/; 另参看 Dan Saffer,“The Wonderful Possibilities of Connecting Your Fridge to the Internet”[把冰箱联入互联网的奇妙可能性], Wired, 29 October 2014, http://www.wired.com/2014/10/is-your-refrigerator-running/.

22. 如果消费大众没有因为隐私和安全疑虑而有所顾忌，他们会喜欢购买自驾汽车和联网冰箱等智能装置，从而让这些产品的供应商享有竞争优势。倘若如此，与这些“首创”公司竞争的厂商也许会寻求采用相同的技术或研发他们自己的技术，并且可能将技术商品化，把不采用这些技术的替代产品逐出市场。

23. Cade Metz,“Mavericks Invent Future Internet Where Cisco Is Meaningless”[不按常理出牌者发明了未来的互联网，思科公司将变得无足轻重], Wired, 16 April 2012, http://www.wired.com/2012/04/nicira/; 另参看 Klint Finley,“GE's New Cloud Must Be the Most Tempting Hacker Bait Ever”[通用电气公司新的云技术必定是对黑客最有诱惑力的诱饵], Wired, 5 August 15, http://www.wired.com/2015/08/ges-new-cloud-may-tempting-hacker-bait-ever/.

24. 由于太空作战行动在很大程度上依赖网空优势，这些建议中有几个（但不是全部）是以网空为中心。

25. 网空技能熟练程度测验可以评估基于逻辑的问题解决能力和抽象思维，这两种技能都是在网空（和太空）成功而必须具备的。

26. 重要的是，在实施这些测验的头几年，不应该让它们影响受测官兵的职业发展方向。随着时间推移，当测验已逐步完善，并且能够从数据点梳理出结论时，它们会有助于做出决策。在测验尚处于调整的过程中急于得出结论和做出职业发展方向决定，将会扭曲测验结果，只能导致事先预定的结论，不能获得真正的深入了解。

27. Capt Kinder Blacke,“Intermediate Network Warfare Training Up and Running”[中级网络战训练正在顺利开展], Air Force Space Command, 3 March 2011, http://www.afspc.af.mil/news/story.asp?id=123245023; 另参看 SSgt Jarrod Chavana,“Airmen Train for 'New Wild, Wild West' in Cyber Domain”[空军战士接受网空领域“新的荒蛮西部”作战训练], Santa Maria Times, 10 October 2014, http://santamariatimes.com/news/local/military/airmen-train-for-new-wild-wild-west-in-cyber-domain/article_1633ec02-eb22-54e5-ad04-f4bea53b776c.html.

28. “National Cybersecurity Workforce Framework”[国家网空安全工作组框架], National Initiative for Cybersecurity Education, http://csrc.nist.gov/nice/framework/.

29. 除了熟悉美国国家标准与技术研究院（NIST）标准之外，接受初始和中级训练的空军士兵还应该熟悉联合部队采用的作战技能，例如计划、简报、执行、汇报（PBED）流程。

30. J. R. Wilson,“Interview: Col. Robert‘Shark' Garland, Commandant, USAF Weapons School”[采访美国空军武器学校司令官罗伯特・夏克・嘉兰德上校], Defense Media Network, 6 November 2011, http://www.defensemedianetwork.com/stories/interview-col-robert-%E2%80%9Cshark%E2%80%9D-garland-commandant-usaf-weapons-school/.

31. 该训练计划的学员录取和毕业后工作安排可以采用与美国空军武器学校训练程序类似的管理方式，不需要针对毕业学员的特定任务制定与传统型中级和高级网空课程截然不同的全套训练计划。

32. Jim Garamone,“Winnefeld: DoD Must Strengthen Public, Private Ties”[温尼菲尔德将军说：国防部必须加强政府机构与民营企业的联系], US Department of Defense, 14 May 2015, http://www.defense.gov/news/newsarticle.aspx?id=128810; 另参看 Kevin Gilmartin,“Education with Industry Program Offers Different Perspective”[业界合作教育计划提供不同的视角], Air Force Print News, 14 March 2008, http://www.hanscom.af.mil/news/story_print.asp?id=123090306.

33. Cheryl Pellerin,“Carter Seeks Tech-Sector Partnerships for Innovation”[国防部长卡特寻求与科技界合作创新], US Department of Defense, 23 April 2015, http://www.defense.gov/news/newsarticle.aspx?id=128655.

34. Mark Pomerleau,“Carter Details DoD's Innovation Plans”[卡特详述国防部的创新计划], Defense Systems, 6 May 2015, https://defensesystems.com/articles/2015/05/06/carter-dod-innovation-plans-congress.aspx; 另参看 Patrick Tucker,“Pentagon Sets Up a Silicon Valley Outpost”[五角大楼在硅谷设立新前哨机构], Defense One, 23 April 2015, http://www.defenseone.com/technology/2015/04/pentagon-sets-silicon-valley-outpost/110845/.

35. 同上 ,“Carter Details DoD's Innovation Plans”[卡特详述国防部的创新计划].

36. Stuart M. Butler,“How Google and Coursera May Upend the Traditional College Degree”[谷歌与 Coursera 可能会颠覆传统的大学学位课程], Brookings Institution, 23 February 2015, http://www.brookings.edu/blogs/techtank/posts/2015/02/23-mooc-google-coursera-butler/.

37. 同上。

38. 除了与这些公司建立伙伴合作关系之外，还可以考察其根本的技术和方法，揭示军方训练课程或许可采纳的高效诀窍。

39. Jeffrey R. Young,“Will MOOCs Change the Way Professors Handle the Classroom?”[大型公开在线课程将改变大学教授的课堂讲课方式吗 ?], Chronicle of Higher Education, 7 November 2013, http://chronicle.com/article/Will-MOOCs-Change-Campus/142869/.

40. 同注 12，“陆军、海军、空军，还有网空”，14-18 页。

41. 同注 12，“陆军、海军、空军，还有网空”，14-18 页。

42. 授课教员和教材编写教员应该按一定的方式定期轮换职责，以便随时了解最新知识发展。

克里斯·巴布科克，美国空军少尉（2nd Lt Chris Babcock, USAF），印地安纳大学理学士，现任空军网络作战安全中心第 50 太空通信中队卫星控制网络小队长兼副科长。他是网空作战官，专精网络防卫及情报融合。