ASPJ AIR & SPACE POWER JOURNAL

中文（简体）

空天力量杂志

2013 年春季刊 — 第 7 卷第 1 期

本期主题：Cyber——网空

- 进取图强开拓网空使命，革故鼎新塑造空军未来
  David S. Fadok 空军中将；Richard A. Raines 博士
- 关于网空战争的法律与伦理交会的一些思考
  Charles J. Dunlap, Jr. 空军退役少将
- 对网空战争概念再思考
  Sean C. Butler 空军少校
- 震网——掀起网空战争军事革命
  Paulo Shakarian 陆军少校
- F-35——和时间赛跑
  John A. Tirpak，美国空军协会《空军杂志》执行编辑

AIM HIGH...FLY-FIGHT-WIN —— 志向高远…飞行—战斗—必胜

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。

2013 年春季刊 第 7 卷第 1 期

本期导读

Cyber——网空 2

将帅视角

进取图强开拓网空使命，革故鼎新塑造空军未来 4
David S. Fadok 空军中将；Richard A. Raines 博士

作战研究

论网空建设初级阶段 8
Robert M. Lee 空军中尉

对网空战争概念再思考 20
Sean C. Butler 空军少校

来自网空用于网空：明确网空情监侦作战的概念 28
Matthew M. Hurley 空军上校

以史为鉴

震网——掀起网空战争军事革命 41
Paulo Shakarian 陆军少校

军事变革

关于网空战争的法律与伦理交会的一些思考 50
Charles J. Dunlap, Jr. 空军退役少将

网空冲突中的软性竞争 62
Panayotis A. Yannakogeorgos 博士

军事技术

F-35——和时间赛跑 72
John A. Tirpak，美国空军协会《空军杂志 》执行编辑

争鸣建言

空军后备役单兵动员增补现役计划：目前的组织结构是否可行? 77
Robin G. Sneed 空军后备役上校；Robert A. Kilmer 陆军退役中校/博士

广域研究

载人航天国际五种合作模式与中国的战略选择 90
蒋翊民博士候选人；余万里博士/副教授（中国）

Cyberspace——网空

美军早将网络空间（网空）作为一个新兴作战领域来思考和开发，将之同陆、海、空、天四大传统作战空间并列，积极发展夺取制网权的能力。但美军对网空的认识经历许多曲折，在与电磁空间纠缠多年之后，才逐渐与后者剥离。例如，美国国防部 2006 年《国家网空军事战略》中将网空定义为“一个使用电子和电磁频谱、通过网络化的系统和相关实体基础设施存储、修改和交换数据与信息的领域。”2008 年参联会主席备忘录对此定义加以修正，始把电磁频谱分离出去，而后在联合作战准则文件 JP1-02《国防部军语词典》中进一步加以明确。至 2010 年组建由美国战略司令部统辖的二级网空司令部时，属下诸军种部队多由网络战、信息战及作战通信人员组成，显见对网空作战的界定已经比较明确。其他国家军队对网空的理解参差不齐，各取所需，但美军的认识过程堪为借鉴。

天空、太空、网空，从物空飞入虚空，从具象飞入虚象，美国空军翅不停振，一气呵成。美国空军大学校长著**“进取图强开拓网空使命，革故鼎新塑造空军未来”**一文，指出对于空中力量向网空发展而言，当前时代宛如两次世界大战之间的时期，时势造英雄，网空领袖人才呼之欲出。昔日陆军航空兵战术学校培养出大批精英，引领航空兵驰骋天空；这所学校的后身，即现在的空军大学，正积极建设成“网空航空兵战术学校”，引领空军在网空中也构建出“明显的非对称优势”，与美军在陆海空天的优势相辅相成。

把目前的网空开发比照当时的天空开发，正相适宜。空中力量发轫之初，涌现出包括杜黑（意大利）、特伦查德（英国）和米切尔（美国）等一大批重要军事理论家和领袖，共同为空中力量的发展指明了方向。而今网空作为一个与传统作战领域平起平坐的最新领域，若求巨大作为，必须得到正确引导，必须吸纳传统作战领域发展初期的经验教训。**“论网空建设初级阶段”**一文即为我们开启这样一个视角。

网络空间与电磁空间在认识上纠缠不清，或存在误区，或事出有因。比如过去常有“陆海空天电”的说法，近期有些文章继续将电磁脉冲炸弹、次声波武器、激光反卫星武器、动能拦截弹，高功率微波武器等硬杀伤武器都列为网空武器。本刊本期**“对网空战争概念再思考”**一文明确认为，电磁空间和网络空间不可混为一谈，基于电磁波的电子对抗武器及定向能武器与基于代码的病毒武器或逻辑炸弹有重大区别。因此必须开发独立的网空战争概念和网空作战准则。

Stuxnet 攻击成功，不仅震坏了浓缩铀离心机组，更震动了整个网空界，且震波深远，中国专家称此病毒为“震网”，颇为传神。这种病毒的攻击目的，既非瘫痪对方网络，亦非盗取对方信息，而是破坏工业设备，首开以软杀伤武器实现硬杀伤之先河。**“震网——掀起网空战争军事革命”**一文对这起网空战例——其技术、目标、目的、攻击行为，以及影响——进行了比较全面的分析。作者对这款病毒的影响预测，也印证了中国一位网络专家在最近《第四届香山论坛》上的警告：震网、以及火焰、Duqu 等病毒对国家安全的威胁，无论怎样估计都不过分。事实上，面对网空作战武器，所谓的战略纵深将失去意义。

军事强国在天空和太空大力开展情报 / 监视 / 侦察（情监侦或 ISR），有力支援现代化战争。现在网空被宣布为与陆海空天平起平坐的第五个作战领域，在此全新领域中开展情监侦也已是不争的事实。但如何界定“网空情监侦”，区分其与其他领域情监侦的不同，识别和应对相应挑战，**“来自网空用于网空：明确网空情监侦的概念”**一文就此发表看法。

隐然成形的网空作战和已经成熟的无人机遥控作战有诸多共同的特征，尤其是都是通过电脑屏幕远距离和匿踪执行攻击，参战人员如何合理约束战场行为？**“关于网空战争的法律与伦理交会的一些思考”**一文认为，网空战士接受包括武装冲突法在内的战争法律约束只是起码的底线约束，在更高层次上，必须自觉维护和接受伦理——军人荣誉感，军人责任感，军人道德感，军人价值观——的约束。

在 2012 年 12 月的国际电信联盟（ITU）迪拜大会上，美国连同大多数欧洲国家反对把因特网治理责任纳入 ITU，宣布不接受包含 ITU 监管和治理互联网措辞的任何协议。ITU 监管意味着国际共管，这与美国主张的“多相关方共管”模式有什么区别，两者冲突的原因为何？**“网空冲突中的软性竞争”**一文（成稿于此次大会之前）就各国为主导网空国际规则博弈提供一些理解线索。

美国空军汰选装备的努力沸沸扬扬已近二十年。F-22 可谓登峰造极，担当制空权 / 空中优势 / 对地攻击 / 电子作战等多重角色当仁不让，但造价和维护费用太沉。美盟各方翘首以待的下一代主战飞机 F-35 则姗姗来迟，与此同时，俄中研发五代机态势咄咄逼人。**“F-35——和时间赛跑”**一文介绍这款“空电一体”全向隐身全效能战机的一些重大优势，是以证明：F-35 虽然交付延迟（目前希望在 2017 年投入服役），但完全值得期待。

本刊 2012 春季刊曾围绕后备役问题发表数篇文章，本期再发一篇：**“空军后备役单兵动员增补现役计划：目前的组织结构是否可行？”**总体而言，此文述及一种称为“后备役单兵动员增补现役”的个别动员计划，将后备役队员单独派到部队，在定向岗位上每年锻炼 30 天，以便随召随用。但因这些编员身份独特，在管理上出现现役后备两不管（或者两都管）的现象，因此必须纠正。

中国载人航天事业发展迅猛，成果举世瞩目，但为多种因素制约而未能有效开展国际合作。**“载人航天国际五种合作模式与中国的战略选择”**一文回顾了自人类开启载人航天事业以来国际合作的重要案例，归纳总结出载人航天国际合作的五种模式，就中国将来开展载人航天国际合作提出建议。

应多位读者要求，从本期起，本刊在最后一页或封三刊登词汇表，所登词汇大多选自本期文章，或新近流行而未及被主流英汉军事词典收录，或虽被收录但词义有发展 / 缺失 / 偏差，或虽为熟词但久存争议 / 误解 / 欠译，或在特殊语境必须另行处理。一家之“译”，仅供参考。

《空天力量杂志》中文编辑姜国成

进取图强开拓网空使命，革故鼎新塑造空军未来

Driving towards Success in the Air Force Cyber Mission, Leveraging Our Heritage to Shape Our Future

大卫·S·费达克，美国空军中将 / 空军大学校长（Lt Gen David S. Fadok, President of Air University ）
理查德·A·雷因斯博士（Dr. Richard A. Raines）

仅在几十年前，我们对空中力量的概念不外乎是等级飞行员驾驶作战飞机格斗长空或轰炸目标；但今天，它的形象已远更丰富。比如，在以空军参谋长名义出版的《空军战斗英雄榜》(Portraits in Courage）最新一期中，获选的 18 名空军英雄中有 16 名不是飞行员，其中 15 人还只是士官。[1] 然而，他们都英勇战斗在前线投送空中力量：护送车队、清除爆炸物、警戒巡逻保护营地、担任阿富汗和伊拉克部队的教官、呼叫飞机实施精确打击，等等。从空军最新版总纲准则文件 AFDD 1《空军基本准则、组织与指挥》中，我们看到空军已经明确认识到空中力量的性质变化，将空中力量重新定义为“通过控制和运用天空、太空、网空来投送军事力量或影响从而达成战略、战役或战术目标的能力。”[2]

已故空军上将亨利·阿诺德谆谆告诫我们说：“我们必须立足明天来思考。”[3] 在明天的空中力量中，将有一大部分发生在新兴的网空作战领域。计算机和通信技术的飞速发展，以及“ 数字领域”与物理操作的紧密耦合，都使网空对军事的成功日益重要。网空带来的挑战反映出它具备全球性、超越政治主权、以及以光速运作等特殊性质。无论我们怎么想像，美国在陆、海、空、天四个领域享有的明显非对称优势，在网空中尚未建立起来。

我们在因特网中通过电子邮件、社交网站和其它电子通信方式即时分享信息。虽然这种能力大幅度减少了制定决策所需的时间，但也增加了我们对通信系统的依赖。信息在网空中高速传播，网空攻击——全然有别于传统的动能打击——也能在瞬息间发起、中断和彻底改变通信状态，并且毫无预兆。因此，我们空军必须时刻准备应战，由此生成挑战。

“靠一台笔记本电脑闯荡网络世界”早不是传奇，它说明只需极低成本就能进入网空斗智斗勇。其结果，当前和未来的网空对手将始终灵敏精干，层出不穷翻新手段。我们竭尽所能快速并准确地制定出网空运作指导方针和政策，但是对手们同样精明，不断变换手法，利用网空开展攻击，甚至经常利用我们法律体系的约束来置我方于被动。网络环境的变化如此迅速，有人甚至认为，一项政策等到获准实施时，就已经大体过时。况且，我们在制定网空作战准则和战术方面，的确无法跟上变幻无穷的网空作战威胁的步伐，这是真实的危险。

多年来，网络间谍和攻击活动在全球范围内此起彼伏。活动者不只是来自某些主权国家，也来自工商业界、犯罪团伙、激进团体和恐怖组织。显然，各种团体的动机不同，但大多数情况下，网络间谍与攻击受金钱和知识产权利益的驱动。我们空军关心的是如何保护我们的关键资产和知识产权，以及根

据《美国法典》及各卷法律授权经由网络手段对攻击者施以必要的惩罚。为此，我们必须培养思想领袖、建设网络队伍、发展运行概念、以及在网络冲突和 / 或网络战中战胜敌人的技术能力。

延续至今的辩论主要围绕网空战争由什么构成以及网空战是否已经开打。本文不拟讨论这些问题，而是着眼于建议空军和空军大学应该如何引领并支持我们国家的网络安全需要。如此，本文着重探讨历史上类似的经验教训、我们目前的状况和需要达到的状态，以及我们建设网空能力的规划。

一脉传承，发扬陆军航空兵战术学校精神

在一战和二战之间的年月里，空军大学的前身，即陆军航空兵战术学校涌现出一批伟大的思想家。这些精英中的精英为我们界定、制定和展现了控制和利用天空这个新领域的最佳途径。空军的这批思想先驱运用他们的集体才智驱动了建设空中力量所需的技术发展。把教室小课堂学到的知识运用到天空大课堂，航空兵战术学校提供了发展空中力量早期概念的学习环境和验证及改进这些概念与技术的实验场地。学员和教员教学相长，在近 20 年中开创和分享各种思想和概念。他们通过传播空中力量的思想，对我们如何在二战中开展空中作战产生了巨大影响。

从这些伟大的思想家中，缪尔·费尔柴德（Muir Fairchild）上将成为空军大学第一任司令官。在这所大学于 1946 年开办之初，将军决定继续沿用航空兵战术学校的校训：革故鼎新、进取图强。从最初的航空兵战术学校开始，我空军就坚持创新，不断提升我们在天空领域的运行效能，引领空中力量概念与能力的发展。空军的成功，在很大程度上靠的是航空精英们奉献才智，发挥想象，不懈地解决各种问题。

应对今日网络挑战，建设明日新型空军

自航空兵战术学校为空中力量的发展奠定基础以来，世界发生了许多变化。当今环境呈现为全球一体，信息瞬息可得，冲突眨眼间就可能发生，且预兆不显。在电子网络构成的网空领域中，冲突可以来去无踪，对手难寻。如上所言，网空领域允许玩家以低成本进入游戏，其中不乏高学历高智商的技术高手。鉴于网空事件的快速性，如何保护和控制信息以确保我们使命的成功至关重要。对手极力从我们的网空资产捕获信息，并袭击我们的关键资源，对这些敌对行动，我们必须快速制定对抗措施，同时发展和壮大我们的网空打击行动能力。

空军和国防部必须具有领导能力和人才团队，他们必须了解网空，领会敌人在网空中发动攻击的可能性和手段，知道我们应如何运用网空为国家政治领导人提供行动选项。我们必须为我们的作战将士们提出、发展、检验和部署这些选项。我们的教育、训练、研究、测试、评估和发展等各种环节都必须以实现使命为目标，不受领域限制。

当前，空军为网空必须考虑两项任务：一是如何建立和维持一支能应对明日挑战的人才队伍，二是如何发展能对抗及挫败高超敌人各种企图的作战概念和能力。第一项任务将困难重重，主要是因为国防预算不断缩减，并且大量资源必须分配给空军的各种核心使命。

网空领域将不断出现突发情况，新兴威胁将快速涌现，局面将越来越复杂，这一切

对空军的网空作战构成严峻挑战。要构建卓越网空，首先需要具备卓越的网空教育和研究能力。以光速行动的网空，要求我们迅速并有效地发展和运用作战概念和技术能力，帮助减少对网络操作员 / 战士的需求。概念和能力必须保障指挥官的使命需要，确保极高度可靠及有效作战。

面向未来，建设网空航空兵战术学校

最近多次有人谈到，就网空而言，我们又一次处于两次世界大战之间的时期。若果真如此，也许我们应该考虑建设一所“网空”航空兵战术学校，把来自政府（空军大学校内外）和企业界各重要部门的具有批判思维的战略思想家汇集起来，共同为网空这个最新领域开发新概念。网空航空兵战术学校的成功，取决于：

- 能紧密联合及依托教育、科技以及作战界的人才与资源；
- 能接纳上述各界具有学术、研发及经验的卓越创新人才并密切互动；
- 能提供一个鼓励创造、革新和交流的平台，从而能不仅培育出新观念，而且能迅速研发和测试样机并实战部署；
- 能把技术革新和发展与战术和作战准则的发展牢固结合起来；
- 能把最先进的教育和验证式学习相结合（即把网络新概念付诸“飞行”）；
- 能把网络发展与总体使命保障需要密切整合，为决策者提供高效的非动能打击行动选择。

因为我们现在生活和行动在一个分散式环境中，所以不应该把这样的网空航空兵战术学校完全局限在一个单一组织结构中。我们有许多能够而且必须利用的娴熟网空运作的机构。在国家层面上，中央情报局、国防部、能源部、国土安全部和联邦调查局等，都拥有自主的网空运作和发展能力，各自肩负着既有不同也有重叠的网空使命。在国防部内，美国网空司令部、国家安全局和各军种都有网空行动机构，按照法典中第 10、18、32 和 50 卷所授权限开展行动。国防部各军种军官学院可提供网空基础教育；同时，空军理工学院和海军研究生学院等可提供继续教育、高级和研究生层次的网空教育。空军和海军分别通过空军教育和训练司令部及网络部队拥有强大的网空作战训练能力。陆军和海军陆战队可利用空军和海军现有的教育和训练能力，同时也通过它们自己的网空司令部来发展针对具体任务的能力。此外，每个军种的实验室都拥有研究与发展能力。工业和学术界也都在开发人才与网空技术资本方面发挥关键作用。

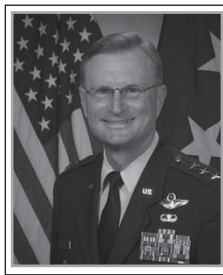
空军大学正在推进网空航空兵战术学校概念，以创造一个能更好分享信息和发展观念的环境。空军大学通过巩固现有伙伴关系和发展新伙伴关系，积极与第 24 空军的作战伙伴以及空军研究实验室的研发伙伴密切合作，确保对网空活动的投资取得最高回报。我们空军大学的所有资源都支持网空航空兵战术学校的建设，位于空军理工学院内的网空研究中心被命名为“空军卓越网空技术中心”，奉命协调网空航空兵战术学校的建设。这项任务是对空军部长 2008 年指派给网空研究中心的“连接各点”的任务的补充，确保网空教育、研究和发展任务都得到落实。

结语

空军正处在一个动态发展和变化的时期。在网空和经由网空的行动将要求新的战术、战技和战规，以及新的领导思维方式来对抗敌人。我们必须迅速培养和保持新一代的网空领导人和战士，培养他们在复杂信息时代和网空领域的作战能力。空军大学积极迎接这一挑战，为未来的网空领导人和战士开发并提供他们投身国家使命和打赢战争所需的知识和经验。遵循阿诺德将军的告诫，我们将继续立足明天来思考，在最新的网空领域革故鼎新、进取图强。♣

注释:

1. Department of the Air Force, Portraits in Courage: Airmen in the Fight [空军战斗英雄榜], vol. 6 (Washington, DC: Department of the Air Force, 2011), http://www.af.mil/shared/media/document/AFD-110921-035.pdf.
2. Air Force Doctrine Document 1, Air Force Basic Doctrine, Organization, and Command [空军作战准则 AFDD 1：基本准则、组织和指挥], 14 October 2011, 11, http://www.e-publishing.af.mil/shared/media/epubs/afdd1.pdf.
3. H. H. Arnold, Global Mission [全球使命], (New York: Harper, 1949), 615.



大卫·S·费达克，美国空军中将（Lt Gen David S. Fadok, USAF），美国空军军官学院毕业，牛津大学文科硕士，空军大学空天高级研究学院军事艺术科学硕士，现任阿拉巴马州马克斯韦尔空军基地的空军大学校长暨司令官。该校提供全方位、多层次的教育、科研和外联，涵盖专业军事教育、专业继续教育及学位授予教育等。将军领导下的空军大学是美国空军的学术与领导培育中心，每年有超过 50,000 名住读和 120,000 名非住读军官生以及士官生与文职生毕业。此外，他还负责军官训练学院和后备役军官训练团的军官授衔。此前他担任李梅准则研究与教育中心司令官暨空军大学副校长。费达克将军以罗兹奖学金学者身份完成研究生学业，于 1985 年获授飞行员证章。他是拥有超过 4,000 小时经验的指挥飞行员，担任过中队、大队和联队层级指挥官。他在“正义事业”、“沙漠盾牌”、“沙漠风暴”和“南方守望”等行动中担任过各种作战与作战支援飞行任务。将军是空军中队指挥官学院和空军指挥参谋学院的优秀毕业生，以及国防研究员，并于 1988 年获得空军部长领导奖。

理查德·A·雷因斯博士（Dr. Richard A. Raines），佛罗里达州立大学电气工程理学士，空军理工学院理科硕士，弗吉尼亚理工学院博士，现任空军网空研究中心主任、国防部军力转型计划主持人，及俄亥俄州赖特 - 帕特森空军基地的空军理工学院电气工程教授。他担任多个美国政府机构及联邦网空安全工作组的技术顾问。雷因斯博士就通信及网空安全问题撰写过 150 余篇技术和战略性文章。他于 2007 年因对信息作战的贡献而被纳入国际电子与信息战协会（Old Crows）名人堂，2008 年获授空军科技工程教育年度奖。雷因斯博士是电气电子工程师学会资深会员。

论网空建设初级阶段

The Interim Years of Cyberspace

罗伯特·M·李，美国空军中尉（First Lieutenant Robert M. Lee, USAF）

率先倡导新事物殊为不易，其把握之难，其推行之险、其成败之不测，无更甚者。

——马基雅维利

网空发展的现阶段，类似于第一次世界大战和第二次世界大战之间的过渡时期。当时，空中力量作为一种重大和强大的军事工具已然崛起，但同时受到挑战。把目前的网空比照当时的天空，正相适宜。惟空中力量发轫之初，涌现出包括意大利空军元帅杜黑、英国皇家空军元帅特伦查德和美国空军准将米切尔等重要军事理论家和领袖，共同为空中力量的发展指明了方向。而今网空作为一个与传统作战领域平起平坐的最新领域,若求巨大作为,必须得到正确引导。

本文分为两个主要部分。第一部分论述空中力量的初级发展时期，由此总结出一些重要的经验教训，作为网空发展之鉴。在此基础上展开第二部分的论述，提出指引网空领域发展的三点建议，其一是为作战指挥官提供实用的网空行动情报；第二是军民结合保卫国家；第三是培养网空文化，加强网空教育，形成网空发展的长远战略。通过了解过去，借鉴经验教训，规划未来方向，我们方能确保真正的网空优势。

空中力量建设的初级阶段

在第一次世界大战前，飞机的使用极为有限，很多人没有意识到飞机的潜在军事用途。例如，威廉姆·H·皮克林（William H. Pickering）在 1908 年出版的《航空学》一书中说："还有一种谬论认为，飞行器能够用于战争，往敌人头上投炸弹。"时隔仅六年，在

1914 年 8 月 14 日,一架法国"瓦赞"(Voisin)飞机载弹轰炸了德国梅斯 - 弗拉斯卡蒂的齐柏林飞艇库。[1] 空战能用于作战的观念迅速受到重视。几年之后，战略轰炸机横空出世，实施空袭,其中包括德国对英格兰的多轮"哥达空袭"(Gotha Raids)。[2] 其实，在战争中使用飞行器和气球的概念古已有之，早在第三世纪的中国，军师诸葛亮曾使用孔明灯向部队传递军事信号，吓跑敌人。[3] 但是，直到航空技术出现重大进步并通过第一次世界大战展示其强大力量，天空作为一个领域的军事重要性才凸显出来，其应用才得到加速。

空中力量在第一次世界大战中的成功运用，包括弗兰克·小卢克中尉击毁 14 只重兵护卫的德军热气球，[4] 启发了很多军事领导人，他们清醒认识到，飞机可对传统的陆

战和海战领域发挥支援作用。当时，辩论已经不是围绕是否应该运用空中力量，而是如何发展空中力量，以及由哪个军种统领。在一战和二战的间隔期间，航空部队的主要使命是提供对敌防御能力。[5] 防御固然是首要任务，但一些空中防御能力也具备进攻潜力。由于陆军航空兵能填补海军传统上发挥的作用，空中力量的灵活性在陆军和海军中引起激烈的争论。

1921 年，威廉姆·“比利”·米切尔将军进行了一次试验，即驾驶 MB-2 轰炸机从弗吉尼亚州兰利机场起飞炸沉海军的军舰。这次试验大获成功，轰炸机炸沉了用于试验的三艘海军军舰，包括一艘从德国人那里缴获的“东弗里斯兰”号现代战舰。[6] 米切尔将军的试验表明，飞机能单独行动攻击离岸的目标。试验也显示，如果陆军继续加强其航空兵能力，海军可能会丧失其提供海岸防御的主要责任。

1925 年，海军公布了一项发展计划，将其岸基飞机的数量从 334 架增加到 583 架，[7] 动机之一是抵消米切尔将军炸毁“东弗里斯兰”号的试验的影响。陆军航空兵司令梅森·帕特里克少将认为，海军此举是要接管整个海岸防御任务。[8] 陆军和海军之间的争执继续升级，两个军种的领导人都担心，如果达不成解决方案，国会可能会成立一支独立的空军。[9] 尽管战争部进行干预，国会也设法满足陆军和海军的要求，争斗仍然不停。[10] 在两个军种的分歧中，米切尔将军强烈倡导组建独立空军。他呼吁公众发声，借助舆论敦促国会采取行动。[11] 米切尔将军被送上军事法庭后，于 1926 年从陆军航空兵辞职，并继续为组建独立空军而公开活动。[12]

1934 年，亨利·“哈普”·阿诺德将军受命同 10 架“马丁”B-10 轰炸机一道，从俄亥俄州代顿市飞到阿拉斯加。在返回俄亥俄途中，他故意偏离航线，没有穿越加拿大上空，而是绕行大洋上空。此举显示出轰炸机的海岸航程范围，但他的做法激怒了陆军参谋长道格拉斯·麦克阿瑟将军。[13] 很显然，国会议员和战争部开始意识到，可能需要一个单独的军种。米切尔将军和其他空中力量的倡导者继续为组建独立军种活动。[14] 阿诺德将军和米切尔将军等关键人物的不懈努力，最终推动空军成为独立军种。虽然我们现在不需要为网空领域组建单独军种，但是，网空力量的真实潜能，一如在天空领域早期的空中力量一样，尚未释放出来。了解了这一点，就能从空中力量早期发展中汲取关键的经验和教训，应用于网空领域的建设。

从空中力量发展中汲取经验

第一条经验：以统一军事领导的方式维护一个战争领域的做法更为可取。当初在全面释放空中力量潜能的努力中，所面对的问题之一就是陆军和海军为了控制天空领域的早期军种竞争，竞争的结果是创建了空军。空军整合各方努力，以国家行动方式更有效地领导航空技术和战略的发展；若空军能更早些组建，或许成就更大。相较而言，网空力量发展的环境较好，这个领域并不侵蚀陆军、空军或海军的传统角色。网空行动既可从网空独立进行，也可与诸军种及诸传统领域形成合力。这种诸军种联合方式有益于整个网空领域，同时应鼓励各军种之间的竞争，每个军种都应发挥重要作用。

第二条经验：空中力量能超出其本身的摧毁能力，做出有影响力的政治宣示。早期的飞行员豪气干云，认为以空军之力就能打

赢战争，却意识不到肆意实施空中摧毁的后果，也不知道限制冲突的重要性。[15] 在越战期间，约翰逊总统和国防部长麦克纳马拉每周会面，商讨轰炸的目标。亲自选定目标的真正用意，是要控制空袭所造成的政治影响，这曾被视为政治上的微观管理。[16] 空袭生发出新的、常常令人恐惧的威力，不仅是对北越人的强烈宣示，而且是对密切关注事态的其他国家的警示。网空力量也具备做出有影响力宣示的能力，因此不可随意使用。网络攻击能摧毁飞机，瘫痪舰船，暴跌股市，对政治格局产生巨大影响。这种攻击不仅威力巨大，而且不受地域限制。最具威力的网空能力,应始终在国家层面的监督下加以运用。

第三条经验：空中力量以其技术先进特性，能模糊战争界限。杜黑相信，飞机航程之大将足以使平民同作战人员一样成为未来战争的目标；他推论，空中力量既不承认传统战场的限制，就能不受制约地使用。战场若无边界，平民便无安全之地。[17] 同理，网空力量能在全球范围内迅速并明确地锁定目标网络和信息系统,因此模糊了战场的界限。正因为网空力量具有这种特性连同其摧毁性的力量，人们才对网空能力心存恐惧。公众一旦感到随时都可能受到网络攻击的影响，其之恐慌，可能不亚于恐怖袭击造成的心理冲击。这种感受对公众舆论和政治的影响，以及其对网空能力发展方向的指导性影响，绝不可低估。一个国家使用网空力量时，首先必须审慎评估本国公民的安全感，确定网空力量的部署和运用可能对民众的安全感产生什么影响。

第四条经验：战争的性质不随技术发展而改变。技术将消除战争之恶性的观点，在整个战争史中一直影响着军事家。[18] 杜黑认为，空中力量的固有攻击性质，其实将限制战争的流血，他的这种论断后来被斯坦利·鲍德温爵士的名言“轰炸机总是所向披靡”[19] 进一步强化。杜黑相信，轰炸城市和攻击平民造成的伤亡，比地面敌对部队交战的伤亡以及由此引起的战争伤亡要小。[20] 杜黑的观点是：战略轰炸将摧毁平民的士气，迫使民众要求他们的领导人早日结束战争。这种观点被证明是错的。实际上，空中轰炸常常激发民众同仇敌忾认准敌人，强化抵抗的决心和士气。[21] 而现在网空领域所面对的问题是，攻击来源可能无从判断，不知道敌人是谁。这种状态对民众会产生什么影响难以估量，有可能造成民众心理崩溃，类似杜黑当初对空中力量的预言。但是，不管未知网络攻击者造成什么影响，杜黑对技术能结束流血的论断依然是错误的。因此应继续研发用于网空和传统作战领域的先进技术，然而战争的性质永远不会变。在部署和运用网络能力的同时，应认识到适度使用网络能力能限制流血，而滥用则会放纵流血。战争是丑恶的，这是永远的真理。[22]

第五条经验：空中力量运用各种方式获得制空权。米切尔将军并不认为轰炸机是最完美的空中力量形式，他认为空军需要各种类型的飞机，包括执行攻击和侦察使命的飞机。[23] 米切尔的空中力量概念，更类似目前网空力量和各种网络资产的不同特性。网空能力能向国防、情报搜集、以及攻击行动提供支援。我们因为拥有各种类型的飞机，才有可能发展出持续情监侦空中平台和空中进攻能力，才能有效保持制空权和对其他作战领域提供支援。[24] 增加各种类型的网空能力，也将直接加强已经建立的情监侦和攻击作战能力，同时保障其他新作战行动的实施。

向指挥官提供网空行动情报

为网空发展指示方向的第一个建议是，运用网空能向指挥官提供更多实用的行动情报。网空力量能为战役策划提供关键的优势。为了向指挥官提供更及时的选择，以情报为基础的网空作战应从作战环境准备阶段就开始启动和参与。这个阶段包括破坏敌人网络并为发生冲突时使用网空武器做好准备。在准备网空进攻作战态势的同时，可以利用从被攻破的敌方系统中获取的信息，为作战环境联合情报准备提供帮助。[25] 指挥官了解这些信息后，就能对战场形成更好的态势感知。

指挥官使用战役策划来“协同力量”，并制定实施指导方针。[26] 而战役策划中的两个主要阶段，应急规划和危机行动规划，都受益于网空力量提供的及时信息和攻击选择，包括了解敌人能力和战略。如果应急规划阶段做出的假设和规划能更准确匹配危机行动规划阶段，那么整个联合作战规划程序就能加快。[27] 这个程序的目标选择和决策速度快，指挥官就能先机制敌，锁准目标，或更快作好反击准备。从作战环境准备阶段获取的信息，还有助于挫败敌人可能采取的欺骗战术。

敌军由于能获取军事作战准则，有可能避开我方原本有效的行动方案，避我实而就我虚。我方结合运用网空能力和情监侦能力，就能及时察觉敌人的欺诈图谋。多重的情监侦平台，包括有人驾驶飞机，遥驾飞机，卫星和人员搜集的情报，共同构成战场情报准备。[28] 网空系统和情监侦系统分别都能严重阻碍敌人藏匿军队、敏感信息、作战计划和重心的企图。而若将两者结合起来，即经由图像情报、信号情报、人工情报和计算机网络作战将二者融合，就能为指挥官提供前所未有的高透明战场态势感知。这种态势感知也能使网空作战成为可能，可指示武器系统平台降低、中断和摧毁敌人的通信、控制和有形资产。网空系统和情监侦系统向指挥官提供的态势感知，能帮助指挥官制定全面和切实可行的意图陈述，如联合作战规划程序模型中所述。指挥官的意图陈述做得好，其作战规划指南就越精确，就有助于选择更好的行动方案。[29]

鉴于敌人非常依赖网空进行通信联络，我方搜集和利用敌人网空信息的能力也越来越大。但是很多指挥官不能充分利用这些能力，不能从获得的情报中受益。在整个军事作战中存在着大量选择，审时度势做好选择，就能降低克劳塞维茨所称的“战争迷雾”的战争不确定性。[30] 若能善加分享网空作战的成果，还可增加其他领域作战的成功机会，从而在整体上降低作战的人力和财务成本。

当然，网空能力并非未受重视，美国网空司令部的成立，表明网空的建设在朝着正确的方向发展。[31] 然而，我们过去和现在都需加强努力，通过网络作战向指挥官提供行动情报和能力。布雷特·T·威廉姆斯少将(Brett T. Williams) 在其“网空作战 10 点建议”中阐述了他对网空发展方向的论点。威廉姆斯少将指出，联合部队司令官和作战司令部应被赋予网空能力和网空作战指挥控制权。如果不能看到对作战使命成功起关键作用的网空部队的作用，指挥官就处在劣势。威廉姆斯少将建议，组建类似战区特种作战司令部的战区网空作战司令部，在作战司令部的控制下，向战区作战司令官提供网空能力。[32] 通过建立类似战区网空作战司令部的方法，指挥官将得到更多行动情报，然后可提出与其使命相关的网空能力需求。具备网空态势感知，准确提出网空能力需求，是运用网空力量的关键之一。

自从威廉姆斯少将发表其论述以来，在作战司令部如何有效地利用网空力量方面，已经引起关注。2011 年夏，美国网空司令部司令基斯·亚历山大上将讨论了通过部署远征网空分队来支援伊拉克和阿富汗作战已取得的进展。他接着表示，在支持作战指挥官开展作战规划方面也取得了进展，使他们更方便地随时提出网空作战支援需求。[33]

自不必说，就如何向指挥官提供更多网空情报和能力而言，网空建设还有很多工作要做。在为指挥官配备了更直接获取网空情报的方式之后，有些网空行动情报仍然无法实用，原因是情报的保密级别森严。为了保护网络能力，不暴露某些详情和技术固然很重要,以免给敌人造成反制或防卫之机。但是，目前对从网空获取的情报所设保密级别过高。很多指挥官根本就不知道他们可看到的全部信息，更谈不上请求获得这些能力。我们不能只为指挥官配备提出网空能力请求的程序，更必须尽最大努力降低网空情报和信息的保密等级，前提是只要不削弱我方网空作战能力。这不仅将支援指挥官，还有益于战术层级的领导人，从而他们可向上提出合理要求，以提升对日常作战的支援。此外，一些网空情报和信息解密后，能让在执法部门行动的政府机构和文职领导人更多地分享。更重要的是，通过分享能够帮助网络防御的行动情报，文职领导人将指导如何更好地保护有关行业，如关键的基础设施。这种信息的分享，对加强国家整体安全有直接相关。

网空武器和国内战线

对网空建设和初级阶段发展的第二个建议是，加强军民合作，共同保卫我们的国家。最近的网络事件表明，网空武器的多样化和专业水平，能攻破精心打造的防御。把军队和民间专业人士的经验和知识结合起来，能更好地防御这些高科技威胁。在网空目前所知的各种高科技威胁中，最典型的例子当数 Stuxnet（震网）蠕虫病毒。

Stuxnet 病毒出现于 2010 年，随即恶名远扬，成为迄今被发现的最具威胁的恶性软件之一。这种病毒软件能够自我复制，在信息系统之间蔓延。它利用微软系统中四个前所未有的未修补“零日漏洞”，同时使用一个根工具包（即一套保持持续进入的代码）、两个指挥和控制伺服器，以及合法化的数字签名来实施攻击。[34] 这个网络武器分为两个部分：武器系统和有效载荷。包括上述特性的武器系统部分令人印象深刻，而有效载荷部分的先进设计更令人叫绝。

Stuxnet 病毒专门用来攻击监控与数据采集系统和工业控制系统，更确切地说，这个网空武器的有效载荷部分专门锁定伊朗纳坦兹核设施离心机的可编程控制器，使离心机不断加速和减速到精确预设速度，降低其效能，并造成最大程度的物理损坏。[35] 虽然这种病毒的全部后果尚不得而知，通过卫星成像看到，纳坦兹核设施的 1000 多台离心机被毁。[36] 这份病毒能取得如此战绩，幕后必有一批世界顶级编程高手和工业控制系统 / 可编程控制器工程师，同时，他们对神秘的纳坦兹核设施布局的了解，甚至超过在该设施工作的大部分工程师。[37]

Stuxnet 病毒被广泛视为是由至少一个国家行为体制造和使用的网空武器，由此引发有关将网空变成又一个作战领域的热烈辩论和大量学术论文。俄罗斯驻北约大使甚至说，如果该病毒对离心机的破坏不只是降低其性能，而是释放其中的铀气体，那就可能制造“一

个新的切尔诺贝利”事故。[38] 虽然此前网空中也曾发生过网络作战，但媒体对 Stuxnet 的威力的描述，使有关网空战争的讨论吸引了大量公众关注。Stuxnet 对网空的影响，就像第一次世界大战初期轰炸对空中力量产生的影响一样，导致讨论公开化，并毫无疑问地促使很多公司和国家行为体加大对网空能力的研究。在某种意义上，这次事件以及过去若干年来的网空作战实例，包括 2007 年爱沙尼亚政府和金融行业遭受的网络攻击，[39] 和 2008 年与俄罗斯入侵格鲁吉亚在时间上巧合的网络攻击，[40] 代表了网空发展过渡时期的开始。

虽然 Stuxnet 病毒能感染并传播到数千台电脑，但迄今为止唯一得知的目标是伊朗纳坦兹的离心机。这次事件并没有严重影响美国的系统，或达到网络攻击程度而将国家推向战争。但是，国防部长帕内塔称：“下一个珍珠港事件很可能发生在网空。”[41] 亚历山大将军对此表示认同，他说，美国关键基础设施的某些部分目前还没准备好经受网络攻击，这令他尤其担忧，[42] 保卫这些财产免遭网络攻击无疑是重大任务。此外，Stuxnet 事件显示了网空能力的能量，且至少已被一个国家行为体使用。

不过，Stuxnet 病毒事件并未就此结束。2011 年 10 月 14 日发现了一种称为“Duqu”的软件病毒，并很快被认定同 Stuxnet 病毒有关。Duqu 与 Stuxnet 的区别在于，前者是一种有针对性的远程访问控制木马（RAT），它窃取信息，而不是损坏离心机。[43] RAT 感染了为数不少的网站，包括大学，制造商和证书部门，其攻击方式能被用来制造另外一种 Stuxnet 式的网空武器。[44] 虽然在类型和目标上不同，Duqu 使用大部分源于 Stuxnet 的相同原始码，这两种病毒被认为是由相同代码团队使用一个名为“Tilded”的常见编码平台制造的。[45]

Tilded 平台与“乐高拼装玩具”（Lego set）类似，能将不同编码模块组合起来，创造出完全不同的恶意软件。[46] 这种以平台为基础的方式，能让设计团队开发出一种网空武器，然后迅速适改装和使用不同模块和有效负载，便可针对完全不同的目标实施攻击，产生不同的结果。此外，从该平台开发的恶意软件能用不同的隐形措施来更新，包括改变加密算法来隐藏其编码。2012 年 2 月被发现的一种 Duqu 病毒更新版就是一例。[47]

基于平台的武器方式，是空中战争多年来发展的方向。国防部早已放弃研制单一功能飞机的做法，而是采购诸如 F-16、F-22 和 MQ-1 等多功能平台，在同一平台上配置不同的有效载荷，以执行不同类型的任务。这种基于平台的方式，现在显然流行于网空领域，对国家安全各个方面构成一系列的风险。同一个网空武器平台，可能造成大学和制造商信息遭窃，由此制造出多种网空武器，然后攻击飞机、指挥控制系统中至为关键的因特网节点、防空系统和重大基础设施。

空军前参谋长施瓦茨将军说，空军正在推动研制“打败飞机的网络方法”，而其它消息来源表明，这种技术已可获得。[48] 赫伯特•卡莱尔中将（Herbert Carlisle）称：“俄罗斯和中国已设计出特定的电子战平台，来针对我们高价值资产。电子攻击能成为渗透系统植入病毒的方法 .”[49] 随着基于传统平台的武器系统越来越多样化，并使用先进雷达系统等更多的能力，它们就更容易遭受网络攻击。我方的这些薄弱环节使敌人更加看重网空武器平台。薄弱环节的存在，加上 Tilded 平台展示的能力，表明未来基于平台的网空武器

系统完全有可能攻击我们的多个国防和民间部门。没有军民联合,就无法对付这种武器。

正是在网空建设发展的当前初级阶段，我们的政府必须鼓励军方同民间关键基础设施等部门的领导人合作，确保国家安全。关键基础设施的操作人员，工程师和研发人员确切知道哪些系统必须严加保护。假如有了切实可行的网空情报，并解密到适当层次，民间部门领导人就能就如何保卫他们运行多年的系统提出更好的建议。

甚至与网络无关的工业控制系统及监视控制和数据获取系统事件也可产生重大影响，有能力影响大范围民众。2009 年 8 月 17 日，高 245 米的俄罗斯最高舒申斯克大坝，经历了与网络攻击无关的事件，震惊了西伯利亚中南部。大坝的水压突然猛增，致使 940 吨重的涡轮机被撕裂，原因来自 500 英里以外一个发电厂火灾。这次事故导致 75 人死亡，重建费用 13 亿美元。[50] 这次事件与网络攻击无关，舒申斯克大坝也不是哪个国家行为体攻击的对象，但是这次事件表明，这种事件能够经由蓄意锁定的网络攻击而激发。如果类似的事件是起源于高度针对性的攻击，有可能造成更深远的影响，公民死亡人数和财政成本会增加。

纳坦兹核浓缩设施和舒申斯克大坝只是使用工业控制系统和监视控制和数据获取系统的两个例子。这些系统影响日常生活的方方面面，包括股市、石油工业、电网、饮水过滤、互联网和卫星通信网络等各种人类服务行业。因此，工业控制系统和监视控制和数据获取系统是一些国家行为体运用网空武器实施打击的首当其冲的可行目标，因此对这些系统必须采取适当保护措施。在网空进化的过程中，保护这些系统非常重要，而我们只有依靠军民联合才能提供有效的保护。

赢得下一代

取得网空优势的第三个建议是，接纳网络文化的发展，重点教育和培养下一代网空操作人员。要想在网空立于不败之地，远期战略必须是培养下一代，包括我们国家的年轻人。我们严重缺乏熟练的网络安全专业人才，调查取证和编程等领域都人手不足；许多岗位，如联邦调查局网络部门的岗位，因为人才短缺而无法填满。[51] 国防部在这方面也处境艰难，担心着对下一代人才的培养。国家安全局研发主任迈克尔·韦特海默博士（Dr. Michael Wertheimer）向美国参议院武装部队小组委员会汇报时说，其主管的机构很难招聘并留住电脑科学方面的专业人才。他接着说，国家安全局信息技术雇员中有 77% 在退休前就辞职。[52] 政府薪酬难与私营行业竞争固然是需要解决的问题，但我们在思考长期战略时必须从天空领域的发展汲取经验。

在空中力量发展的早期，人们对飞机和飞行员充满兴奋和崇拜。早期的飞行员艺高胆大，在前所未知的领域创造纪录，留下无数珍贵记忆。1909 年 8 月 22 日在法国举行的兰斯航空比赛，是世界第一个重大的航空展，堪称后世全球各地航空展的楷模。[53] 在航空展和空中比赛中，这些早期的飞行员令观众为之倾倒，由此不仅激励了未来的飞行员，也让公众了解了空中力量的能力。[54] 在一战和二战的间隔期间，航空展空中比赛吸引了更多的关注，例如，1929 年的美国国家航空展就吸引了 50 多万观众。[55]

1920 年代是飞行技术发展的黄金时代，一切充满神秘。飞行员竞相飞得更高、更快、

更远。在 1919 年和 1921 年间，陆军飞行员三次打破世界飞行高度的记录。[56] 网络操作员不需要像早期飞行员那样，不顾危险追求速度和特技的刺激，但网空自有其神奇，也能博得公众的敬慕，从而激励下一代投身网空事业。

黑客事件和网络安全研讨会都能展示网络安全技术的进步、薄弱性和最新发展动态。研讨会还促进来自不同背景但都对网空发展感兴趣的与会者互相切磋交往。可惜的是，这些聚会不像早期航空展那样便宜和吸引公众。一些著名的会议，如国际黑客大会（DEF CON），仅需 150 元就能参加，[57] 另一些会议的费用则需数千美元，若选择接受培训的话，费用更贵。[58] 虽然这些网空发展相关会议的价格根据与会对象和运营成本制定，即使代价不菲也自有其道理，但毕竟难以吸引主流公众参加，因此需要检讨。

其它一些精心组织的研讨会和提供的网空相关教育，也有益于网空领域的发展。国防部网空犯罪中心（DC3）主办每年一度的网空取证挑战赛和会议，这对了解同行交流、网空技术发展、报名参加培训课程来说，是个极好的机会。网空取证挑战赛免费参加，但用意好并有益的会议需要 500 美元报名费。[59] 政府和国防部必须加大步伐，多承办类似航空展的低成本会议，通过这些集会展示网空的能力和神奇魅力。

参谋长联席会议前副主席海军陆战队退役上将詹姆斯·卡特赖特指出，应该公开讨论和训练一些网空攻击能力，是以加强我们的网空威慑。[60] 网空研讨会应成为国防部展示美国网空能力的理想场所，将吸引观众，鼓励下一代投身这个事业，同时威慑挑战美国的敌人。此外，网空操作人员可以提供低费或免费的有关网络安全和黑客攻击的基本原理课程，营造有趣和互动教育环境，引发下一代对他们将继承的领域产生兴趣。

让年轻人受教育并对网空感兴趣非常重要。国防部正在采取正确步骤，教育和训练年轻一代领导人，鼓励军官和士官报名参加网空教育。密西西比州基斯勒空军基地的空军网空训练技术学院就是一个典型例子。该学院于 2010 年 6 月 21 日成立，向网空军官提供为期六个月的培训课程，结业者获网空飞行章。[61] 未能结业者要么被纳入新的空军专业代码重新受训，或从空军退役。

网空训练技术学院以强大师资提供高质量教学。教官主要来自拥有网空作战实际知识和经验的空军士官和军官，他们积极引导和训练下一代网空军官，并通过参与教学来实践施瓦茨将军的观点：成功的军事生涯应包括担任一轮教官经历。[62] 这些军官走上讲台，不仅有机会提高自己的专业水平和学术追求，也训练那些未来将成为中队年轻领导人的学员，同他们建立师生之谊。教官和学员之间的这种关系，将有助于网空文化的整体建设。

在空中力量的早期文化中，有着放任学员蔑视上级和非飞行员教官的倾向，学员这样做是为着在战友中建立威信。陆军航空兵成员有时会故意生事来引发上级训诫，以此提升自己在小圈子中的威望，他们喜欢离经叛道，并乐此不疲，由此建立背景不同的圈子和有关飞行的文化。[63] 军队网空专业人员无需如此鲁莽作为或挑战上级。目前军队的环境有利于网空领域的发展，如前所述，我们没有必要像当年陆军航空兵时代鼓吹组建空中力量一样组建独立的网空部队。但是，军队的网空文化可以鼓励离经叛道的观点和

想法，因为这个领域相对较新，许多潜在能力仍被误解和仍未开发。

网络文化雏形已成，我们应张臂接纳而非回避。通过大力加强教育和在军队中鼓励竞争担任前程光明的教官工作，网空文化自能发展。网空战士中的精英应当竞争教官岗位，对教官应增加前程发展机会作为回报。循此方式，网空教育可以不断更新，网空战士也有参与教育的动力，由此推动发展出一种强大而独特的网空文化，吸引并留住人才投身网空建设事业。

结语

网空领域在其结构上独一无二，将在历史上作为一种战争领域留下自己的位置。但是，传统作战领域，尤其是天空领域，与网空有许多相似之处，有许多经验教训可供借鉴,有助于领导人引领网空建设的发展方向。通过理解这些经验教训，通过鼓励军民之间公开交流对网空领域的发展的看法，应能着力于正确的发展重点。这些重点包括运用网空能力提供行动情报，加强军民专业合作共同建设国防，以及培育网空文化和培养下一代。

指挥官们必须知道能从网空操作员获得哪些网空作战支援来直接支持其作战使命。有关网空情报和网空能力的信息需要适当降低保密等级，使战术、战役和战略层次的领导人都能充分受益。解密的信息还需与文职部门分享，以提高民间的网空意识，建立有意义的国防战略。这将推动民政部门领导主动保护本部门网络安全，而非一味依赖国防部和国土安全部，从而有效加强国家安全。另外，应通过研讨会和学习活动等公开场合展现我们的网络能力和网络情报，这将不仅强化我们对敌人的网空威慑，而且能激励下一代投身网空建设。保护网空领域，发展制网权能力,长期战略必须着眼于培养下一代。

正如亚历山大将军所言：“我们要让那些企图从网空攻击我们的人知道，他们不可能轻易得手并将为此付出沉重代价，藉此迫使他们改变行为模式。相关的技术已经准备就绪。”[64] 就绪的不仅是技术,网空界各相关方，包括国防部、文职部门和我们的下一代，也都在为未来的挑战做好准备。网空力量是一个强大的政治和军事工具，其之建设必须善加引领，以发挥其应有的历史作用。网空发展正处于初级建设阶段，各级领导人当须努力，为下一个时代的成功打下基础。♣

注释:

1. Alan Axelrod, Little-known Wars of Great and Lasting Impact: The Turning Points in Our History We Should Know More About [鲜为人知但影响深远的战争：应引起更多注意的历史转折点], (Beverly, MA: Fair Winds Press, 2009), 222.
2. D. Stevenson, With Our Backs to the Wall: Victory and Defeat in 1918 [背水一战：1918 年的胜利与失败], (London: Penguin, 2012), 186.
3. Andreas Wittmer and Thomas Bieger, Aviation Systems Management of the Integrated Aviation Value Chain [整合航空价值链的航空系统管理], (Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg, 2011), 7.
4. The Official Web Site of the U.S. Air Force, "2nd Lt. Frank Luke Jr" [法兰克・小卢克少尉生平], 2 November 2010, http://www.af.mil/news/story.asp?storyID=123006460.

5. Lt Col Dr. James P. Tate (ret.), The Army and its Air Corps: Army Policy Toward Aviation, 1919-1941 [陆军及其航空兵：陆军 1919-1941 年的航空政策], (Maxwell Air Force Base, AL: Air University Press, 1998), 33.

6. Capt B. Chance Saltzman and Thomas R. Searle, Introduction to the United States Air Force [美国空军简史], (Maxwell AFB, AL: Airpower Research Institute, College of Aerospace Doctrine, Research and Education and Air University Press, 2001), 6.

7. 见注释 7，第 62 页。

8. Pamela Feltus,“Mason Patrick and the Creation of the U.S. Air Corps”[梅森・帕特里克和美国航空兵的创建], U.S. Centennial of Flight Commission, http://www.centennialofflight.gov/essay/Air_Power/Patrick/AP15.htm.

9. 见注释 7，第 67 页。

10. 见注释 7，第 68 页。

11. 见注释 7，第 109 页。

12. National Museum of the U.S. Air Force,“Brig. Gen. William 'Billy' Mitchell”[比利・米切尔准将生平], 11 February 2010, http://www.nationalmuseum.af.mil/factsheets/factsheet.asp?id=739.

13. 见注释 6，第 12 页。

14. 见注释 6，第 12 页。

15. Col David A. Moore, The Art of Aerial Warfare [空战艺术], (Maxwell Air Force Base, AL: Air University Press, 2005), 17.

16. 同上，第 19 页。

17. Giulio Douhet, The Command of the Air [制空权], (Washington, D.C.: Office of Air Force History, 1983), 9.

18. 见注释 15，第 68 页。

19. Sir Stanley Baldsin,“A Fear for the Future”[对未来的恐惧], a speech to the British Parliament on 9 November 2011.

20. 见注释 17，第 22-23 页。

21. 见注释 15，第 33 页。

22. John Stuart Mill, "The Contest in America," [在美国的较量], Dissertations and Discussions 1 (1868): 26.

23. David R. Mets, The Air Campaign John Warden and the Classical Airpower Theorists [空中战役：约翰・沃登和空中力量理论家前辈], (Maxwell Air Force Base, AL: Air University Press, 1999), 39.

24. Benjamin S. Lambeth, "Airpower, Spacepower, and Cyberpower", In Toward a theory of Spacepower: Selected Essays [《太空力量研究论文集》中“天空力量、太空力量和网空力量”文], edited by Charles D. Lutes, Peter L. Hays, Vincent A. Manzo, Lisa M. Yambrick, and M. Elaine Bunn (Washington, DC: National Defense University Press, 2011).

25. Joint Publication 5-0, Doctrine for Joint Operations [联合作战准则 JP 5-0：联合作战准则], 11 August, 2011.

26. U.S. Army War College, Campaign Planning Primer [战役策划入门], Department of Military Strategy, Planning, and Operations, AY 08.

27. Joint Publication 5-0, Doctrine for Joint Operations [联合作战准则 JP 5-0：联合作战准则], 11 August, 2011.

28. Maj Eric D. Trias and Capt Bryan M. Bell, "Cyber This Cyber That, So What?" [这也网空那也网空，究竟是什么 ?], Air and Space Power Journal (Spring 2010): 90-100.

29. Joint Publication 5-0, Doctrine for Joint Operations [联合作战准则 JP 5-0：联合作战准则], 11 August, 2011.

30. Carl von Clausewitz, Michael Howard, and Peter Paret, On War [战争论], (Princeton, NJ: Princeton University Press, 1976), 101.

31. U.S. Department of Defense, "News Release: Cyber Command Achieves Full Operational Capability" [网空司令部实现全面作战能力], News Release, 3 November 2010, http://www.defense.gov/releases/release.aspx?releaseid=14030.

32. Maj Gen Brett T. Williams, "Ten Propositions Regarding Cyberspace Operations" [关于网空作战的 10 点建议], Joint Force Quarterly, no. 61 (2nd Quarter 2011): 10-17.

33. Gen Keith B. Alexander, “Building a New Command in Cyberspace”[建立一个新网空司令部], Strategic Studies Quarterly 5, no. 2 (Spring 2011): 3-12.

34. Nicolas Falliere, Liam O Murchu, and Eric Chien, W.32 Stuxnet Dossier [W.32 Stuxnet 病毒档案], Symantec White Paper (Symantec: Security Response, February 2011), 1-2, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

35. Ralph Langner, “Stuxnet: A Deep Dive”[Stuxnet 病毒：深入观察], 18 Jan 2012 video, http://www.digitalbond.com/2012/01/31/langners-stuxnet-deep-dive-s4-video/.

36. Yaakov Katz, "Stuxnet May Have Destroyed 1,000 Centrifuges at Natanz" [Stuxnet 病毒可能摧毁了纳坦兹的 1000 台离心机], The Jerusalem Post, 24 December 2010, http://www.jpost.com/Defense/Article.aspx?id=200843.

37. 见注释 35。

38. Ellen Messmer, "Stuxnet Could Have Caused 'New Chernobyl,' Russian Ambassador Says" [俄国大使称 Stuxnet 病毒可以引发“新的切尔诺贝利事故”], Network World, 27 January 2011, http://www.networkworld.com/news/2011/012711-stuxnet-chernobyl.html.

39. Biony Kampmark, “Cyber Warfare Between Estonia and Russia”[爱沙尼亚和俄罗斯之间的网空战争], Contemporary Review (Autumn, 2003): 288-293.

40. John Markoff, "Before the Gunfire, Cyberattacks" [硝烟未起网战先行], The New York Times, 12 August 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1.

41. Jason Ryan, “CIA Director Leon Panetta Warns of Possible Cyber-Pearl Harbor”[中情局长帕内塔警告可能发生网络珍珠港事件], ABC News, 11 February 2011, http://abcnews.go.com/News/cia-director-leon-panetta-warns-cyber-pearl-harbor/story?id=12888905#.T5M2ABHoK5I.

42. Charlie Rose, "Charlie Rose Talks to General Keith Alexander" [查理·罗斯采访基斯·亚历山大上将], Businessweek, 21 July 2011, http://www.businessweek.com/magazine/charlie-rose-talks-to-general-keith-alexander-07212011.html.

43. Boldizsar Bencsath, Gabor Pek, Levente Buttyan, and Mark Felegyhazi, Duqu: A Stuxnet-like Malware Found in the Wild [类 Stuxnet 病毒 Duqu 横空出世], Laboratory of Cryptography and System Security Technical Report (Budapest University of Technology and Economics: Department of Telecommunications, October 2011), 6-7.

44. Symantec, “W32.Duqu: The Precursor to the Next Stuxnet”[Duqu W32：下一个 Stuxnet 病毒先兆], Symantec Security Response, 24 October 2011, http://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet.

45. Kaspersky Lab, “Duqu and Stuxnet Not the Only Malicious Created by the Responsible Team”[某组织制造的恶意病毒不止是 Duqu 和 Stuxnet], Virus News, 29 December 2011, http://www.kaspersky.com/about/news/virus/2011/Kaspersky_Lab_Experts_Duqu_and_Stuxnet_Not_the_Only_Malicious_Programs_Created_by_the_Responsible_Team.

46. Rob Waugh, "Lethal Stuxnet Cyber Weapon is 'Just one of Five' Engineered in Same Lab" [致命 Stuxnet 网空武器仅是同一实验室设计的“五种病毒之一”], Daily Mail, 29 December 2011, http://www.dailymail.co.uk/sciencetech/article-2079725/Lethal-Stuxnet-cyber-weapon-just-engineered-lab.html.

47. Greg Masters, "Duqu Variant Uncovered" [发现 Duqu 病毒变异版], SC Magazine, 23 March 2012, http://www.scmagazine.com/duqu-variant-uncovered/article/233385/.

48. TSgt Richard A Williams Jr., "CSAF Stresses Importance of Ready Future Force" [空军参谋长强调未来部队做好备战的重要性], Official Site of the U.S. Air Force, 24 February 2012, http://www.af.mil/news/story.asp?id=123291264.

49. Eloise Lee, "Electronic Warfare Weapons" [电子战武器], Business Insider, 15 March 2012, http://www.businessinsider.com/electronic-warfare-weapons-2012-3.

50. Thomas Rid and Peter McBurney, “Cyber-Weapons”[网空武器], The RUSI Journal 157, no.1 (February/March 2012), 6-13.

51. Kevin Coleman, "United States at Risk from Shortage of Trained Cybersecurity Professionals" [美国缺乏训练有素的网络安全专才而面临风险], Defense Systems, 22 June 2011, http://defensesystems.com/articles/2011/06/08/digital-conflict-cyber-worker-shortage.aspx.

52. Brian Donohue, "Experts Tell Senate: Government Networks Owned, Resistance Is Futile" [专家告知参议院：政府网络无法抵抗外来攻击], Threatpost, 21 March 2012, http://threatpost.com/en_us/blogs/experts-tell-senate-government-networks-owned-resistance-futile-032112.

53. David H. Onkst, "Explorers, Daredevils, and Record Setters: An Overview" [综述：艺高胆大惊险迭出], U.S. Centennial of Flight Commission, http://www.centennialofflight.gov/essay/Explorers_Record_Setters_and_Daredevils/EX_OV.htm.

54. David H. Onkst, "The First U.S. Airshows - the American Air Meets of 1910" [首次美国航空展—1910 年美国航空盛会], U.S. Centennial of Flight Commission, http://www.centennialofflight.gov/essay/Explorers_Record_Setters_and_Daredevils/Early_US_shows/EX4.htm.

55. David H. Onkst, "Air Shows - An International Phenomenon" [航空展成国际潮流], U.S. Centennial of Flight Commission, http://www.centennialofflight.gov/essay/Social/airshows/SH20.htm.

56. 见注释 5，第 27 页。

57. DEF CON, "Official DEF CON FAQ" [黑客大会常见问答], https://www.defcon.org/html/links/dc-faq/dc-faq.html.

58. Hacker Halted, "Registration" [注册], http://www.hackerhalted.com/2011/Registration.aspx.

59. DoD Cyber Crime Conference, "Registration" [注册], http://www.dodcybercrime.com/12CC/register.asp.

60. Andrea Shalal-Esa, "Ex-U.S. General Urges Frank Talk on Cyber Weapons" [美军退役上将敦促坦诚关注网空武器], Reuters, 6 November 2011, http://uk.reuters.com/article/2011/11/06/us-cyber-cartwright-idUKTRE7A514C20111106?mid=520.

61. Bruce Rolfsen, "3,000 Officers Switch to Cyberspace Specialty" [三千军官转入网空安全专业], Air Force Times, 17 May 2010, http://www.airforcetimes.com/news/2010/05/airforce_cyber_careers_051710/.

62. Gen Norton A. Schwartz, Chief of Staff, To all Airmen [致空军全体官兵], Memorandum, 8 March 2012.

63. 见注释 5，第 192 页。

64. 见注释 33。

罗伯特·M·李，美国空军中尉（First Lieutenant Robert M. Lee, USAF），美国空军军官学院及空军本科网空训练技术学院毕业，现驻德国，服务于美国空军情监侦局。李中尉在国际范围就控制系统网空安全、网空作战、高危网空威胁及未来民族国家的网空武器等课题发表著述并演讲。

对网空战争概念再思考

Refocusing Cyber Warfare Thought

肖恩·巴特勒，美国空军少校（Maj Sean C. Butler, USAF）

2007 年 9 月，来自美国空军各部的六十五名专家聚集空军军官学院，研讨如何建设网空训练和部队培养体系。[1] 此前在 2006 年 11 月，空军已经组建暂编网空司令部（属大司令部级别）。更在此之前，空军已将网空纳入其 2005 年的使命声明中。这些实质性的发展，是过去十多年网空力量倡导者努力的结果——网空最终被完全认可为一个作战领域。遗憾的是，这些认识和成就经历过一段弯路，弯路之始，就是本文开始提及的那次研讨会。[2]

研讨会组织者向与会者解说了国防部在 2006 年颁布的《国家网空军事战略》对网空所做的定义："一个使用电子和电磁频谱、通过网络化的系统和相关实体基础设施存储、更改和交换数据与信息的领域。"[3] 组织者进一步介绍了空军构建网空专业部队的大概思路，拟主要从两类人员中培养，一类是计算机网络操作人员，另一类是作战系统（电子作战 [EW]）军官，即从带有这两类专业后缀代码的人员中选拔。[4] 此言既出，立刻引发一些难以回答的问题和尴尬。空军为什么把这两个有巨大差别的专业纳入同一个培养渠道？雷达信号干扰是否与计算机网络黑客攻击同属一个类别的作战？我们是否因为机载激光使用电磁频谱而将它也归入网空战？身为空军各路专家的与会者就这些问题尖锐交锋，却未找到答案。

幸而，国防部和空军在经过大量曲折之后，终于解决或消除了网空中的这些基本概念错误。在上述为网空做出定义的《国家网空军事战略》颁布后不到两年，国防部在相关联合作战准则中对此定义做出更新，新的定义更准确更符合实际，虽然稍嫌具体化："信

息环境内的一个全球性领域，由相互依存的信息技术基础设施网所组成，包括互联网、电信网、计算机系统、嵌入式处理器和控制器。”[5] 此后不久，空军撤销暂编网空司令部，降格为一支编号空军部队，隶属于新成立的二级统辖网空司令部，空军也没有将作战系统军官全部整合到其网空专业部队之中。[6] 总体而言，空军在对网空的界定上放弃了对电磁频谱和物理特征的坚持。

早期网空力量倡导者呼吁将网空视为一个军事作战领域的努力在最近几年取得了成果。[7] 但是，网空概念和网空作战准则继续受到当初克服保守派阻挠的斗争过程的影响（虽然这种影响可能是无意为之的）。我们经常看到一些人和文章，在描述网空时把网空与陆地、海洋、天空和太空等四个传统领域随便地加以类比。现行的网空作战准则不仅强调网空的物理特征，还把其它作战领域的基本原则和教条照搬给网空，不假思索就确凿地假定这些领域的基本原则同样适用于网空这个新环境（后面再详细举例）。

网空无疑带有一些物理元素及其相关的作战意义，战争的许多基本原则也无疑适用于网空战争。但是，网空作战准则千方百计地想证明“网空和其它领域一样”而不是充分强调网空独有的特质,这样的方法有问题。军事研究者不应专注于网空的相对物质性的物理元素，而应强调其独有的逻辑或虚拟性质，并思考这种性质的意义。只有理解了网空的特质，才能从根本上理清思维，发展出此领域独有的理论与作战准则。

能否把网空视为物理领域

把网空描述为作战领域的早期努力倾向于将网空立足于物理世界并以此作为定义性特征。当时这样做情有可原，因为早期的努力企图将网空定位成与陆地、海洋、天空和太空并列的领域——所有领域都处于物理世界之中。这些倡导者们试图为之开辟出一片同样的物理环境，从而奠定网空与其它领域平起平坐的地位。

例如，由空军退役上校格雷戈里·赖特瑞（Gregory Rattray）编写的一部影响巨大的早期专著《网空中的战略战争》就告诫勿将网空视为完全虚像的环境：“网空……实际上是一个物理领域，是信息系统和网络创造出来的结果。”[8] 显然，网空有其物理表现，这就是需要电子装置来通信；赖特瑞也正确地提醒信息战士不要忽略与网空物理交互的重要性。但是，这种说法本身无法为那些力图将网空提升为名正言顺的作战领域的人们提供充分的说服力，毕竟，其他领域并不是依靠在其环境内运作的设备来定义的。于是，一些人便指定电磁频谱作为网空的物理表现。

美国国防大学的丹尼尔·库尔博士（Dr. Daniel Kuehl）是把网空紧密联系到电磁频谱的长期倡导者（他自 1997 年就开始鼓吹这种关系），并在国防部 2006 年对网空的定义中发挥了重要作用。[9] 他在许多文章和演说中继续宣扬这种以物理为中心的网空定义，其观点被广泛引用。空军网空特遣部队也许正是受这种影响，又急于建立网空的合法作战领域地位，便在 2006 年抛出“网空纲领”，声称“网空是一个作战领域，电磁频谱是其机动的空间。”[10]

把电磁频谱指定给网空自有许多诱人的理由。首先，这个频谱是物理世界中一种带弥漫特征的已有明确定义的现象，看起来完全有资格与其它物理领域平起平坐。大多数数字通信，从直觉来理解似乎属于网空（实

际上难说），这些通信以无线电波、微波或激光（无线方式或光纤方式）为载体传播，所有这些载体正好也属于电磁频谱。从这一点开始，把网空的定义延伸到包括雷达（某种意义上可视为一种信息系统），并进一步联系到电子对抗，似乎也顺理成章。于是，只要网空真能将这相对尊贵的、业经验证的、效果显著的电子战场据为己有，它便在那些传统作战人士的眼中突然获得了登堂入室的地位。在当时想把网空定位成一个新作战领域的急切背景下，人们可以理解为什么国防部最初接受了库尔博士对网空的物理定义。

但是，这种说法不久便遭遇麻烦。如果雷达属于网空，那么声纳为什么不能属于网空？毕竟广义而言，声纳在实质上也服务于相同的目的，只是几乎不利用电磁频谱。再看机载激光，似乎也难圆其说，虽然正出于相反的原因——它几乎完全依靠电磁频谱来产生效能；只是，任何网空定义中如果包括了激光武器，就变得过于宽泛而失去了实际意义。因为所有情监侦、战术传感器，甚至人类的肉眼，都要依赖电磁频谱。

虽然我们有理由根据网空对电子和电磁频谱的使用来界定网空的特征（怎样定义都可以），然而这样做，对作战理论造成一些实际的问题。例如，把电子频谱和网空关联，就会导致把电子战、甚至定向能作战，置入和计算机网络作战的同一个篮子里。其结果是，把数种高度专业而完全不同的技能聚集在同一种结构中管理，虽然它们在训练和作战准则上极少共同点。进一步，从理论和作战准则上来看，电子和电磁频谱对定义网空并无多大作用，把它们包含进来只会起到偏离作用，影响对网空特征的真正界定。

以对电子和电磁频谱的使用来为网空划界，直觉上虽容易接受，其实只是对这个领域的肤浅描述。如果网空主要是利用量子效应来处理、储存和交换信息，那么从作战行动角度来看，它们还有什么不同？事实上，网空技术为产生效能所使用的物理机制不能作为这个领域的定义特征——正如我们不可用坦克和大炮来作为陆地这个作战领域的定义特征一样。[11]

而今网空已经在军方考虑中占有一席之地，可是那种把网空比作其他领域的牵强类比难以消失，继续在网空理论和作战准则的发展中发挥影响。如上所述，国防部和空军已经纠正了从物理角度定义网空的做法，这从军方推行的新定义、新组织和新程序可以看出。我们已经不再把电磁频谱视为网空的一部分，我们已经把网空视为以计算机网络为中心并立足此基础开展网空专业训练和部队培养。[12] 空军新建的网空作战专业主要包含有通信技术背景的人员。[13] 网空作战准则和思维也开始沿正确的路线发展。

遗憾的是，描述网空的旧观点旧模式继续保持着对传统军事人士的吸引力，对他们产生着惯性的影响。最近发表的一些著述，表面上是想构建网空特有的理论，实质是在继续引述甚至强调网空的物理特征，虽然超越技术和战术层面之后这些物理特征便失去了意义。兹举 2009 年一篇讨论中国网空威胁的论文为例，此文向国防部在 2008 年更新的网空定义发难，呼吁回归到原先以物理因素界定领域的模式，认为“网空不仅包含实际的军事和民用电子设备，还容纳信息……传播的电磁频谱。”[14] 这位作者进一步强调：“严格独立的［计算机网络战］、电子战和太空行动［其实］都被容纳在这个包罗万象的、形虚像而实‘具象’的网空领域之中，与陆地、

海洋及天空领域并无不同。”[15] 再举《联合部队季刊》2011 年某文为例，此文明确称“网空（就是电磁频谱）。”[16] 即使在空军作战准则 AFDD 3-12《网空作战》（2010 版）中，也不经意地流露出过分强调电磁频谱的余痕，只因遵循国防部规定的定义，而未将两者等同。[17]

不适当地强调网空的物理面向，可能产生误导或人为地圈定这个领域，从而模糊对这个领域的观察，阻碍各种更有益的真知灼见。国防大学副教授塞缪尔·莱尔斯博士（Samuel Liles）认为：“片面强调网空的一个面向（电磁频谱）会对决策层造成一个战略上和概念上的盲点，还可能把对风险的思考固定在信息传发设备的威胁和薄弱环节方面。”[18] 就是说，继续宣扬物理网空思维模式只能强化这些错误的观点在学术界甚至作战界继续流行。网空无疑有其物理的元素，但是这些元素作用和影响相对清晰，显然归入现有的物理攻击、电子战，以及其他熟知的范畴。但是网空与其他作战领域有许多根本性的区别，由于这些区别，一些现成的军事原则可能无法适用。

因此我们需要理清网空战的真正有意义的、独有的特征，以帮助理论专家调整思路，更有效地推进研究，使网空战与现成的作战理论和准则充分区分开来。进一步，他们便能够就这个相对新奇及陌生的作战领域澄清原则性疑问，为战略决策人和指挥官提供正确信息，帮助他们做出更知情的决策，更好地开展网空行动。

网空的独有特征

网空的一个定义性特征，是能使用自动化系统迅速处理、储存和交换大量信息——但这些物理方法只是表象。事实上，将网空与其他领域真正区别开来的，不是这些物理设备，而是网空的代码逻辑性质或者说虚拟性质。这种特征产生许多重大的明显或非明显的意义。

网空的一个最常提及的显著属性，是在其内行动的速度。[19] 网空作战“（几乎）快如光速”我们已耳熟能详。在大多数情况下，物理距离对网空而言几乎没有意义——惟其逻辑拓扑结构举足轻重。策划和准备网络攻击可能需要数周时间，需要研究各种情报和攻击目标，但一旦实施攻击，或许几秒钟之内就能完成。这意味着，我们在许多情况下可能根本没有时间对正在实施的攻击做出反应。经常，防卫方能做的，就是提前阻止最危险的攻击通道，开展监测，并在攻击发生之后迅速缓解和修补。攻防双方实时性迎头对抗的情况极少可能发生。

由此引起另一个有趣的看法，这就是和其他领域相比，网络战进攻部队和防卫部队高度不对称。[20] 防卫方的组成主要包括监管各种网络的系统管理员、迅速执行取证分析和系统修补的响应小组、入侵监视分析员，等等，可能还包括那些能快速编写补丁程序的编程工程师、能提供过滤新恶意软件的私营杀毒软件公司等。[21] 高度专业化的进攻部队，则运用各种不同的工具对网络实施攻击，经常有能力在发动攻击的同时逃避监视。这两支对立的网空部队在网空中作战，却不像其他“动能打击”领域那样互相照面；即使双方露踪显形，也无物理意义上的杀身之险，这一事实，使削弱对方网络作战能力的努力更加艰巨。[22]

美国兰德智囊集团研究专家马丁·利比奇（Martin Libicki）在其专著《网空威慑和

网空战争》中，详细解说了解除敌人网空作战能力的难度甚至不可能性："是的，黑客所需，惟一台随意取用的计算机和一个网络连接；对敌国的网络攻击能力，我们即使用武力打击也不敢保证能够将之摧毁。"[23] 一个国家的最难以替代的网空作战能力资产，就是那些高智商黑客群体及其大量的战绩积累，国家会尽力保护这些人不受人身和网络攻击，除非被战争结局已定的现实逼迫得没有选择余地。再者，国家网空部队用于网空攻击的计算机虽然通常不昂贵，但经过特别固化，既不影响功能却比一般的计算机或服务器更高效，很难被受攻击的对方判定和摧毁；事实上，想从网空确定攻击源本身就十分困难，遑论打击。对一个国家实施物理打击和淹没式攻击固然在理论上可能将一个国家从互联网隔离从而阻绝其网空部队的攻击通道（如果他们没有暗中转移到盟国或未知第三国的话），但这种做法是双刃剑，因为攻击方也将无从进入敌人的网络。

所有这些意味着，空军作战准则 AFDD 3-12 中那句缺少解说的"进攻性制网权作战"术语可能毫无意义，或者至少与其所模仿的天空领域的术语"进攻性制空权作战"大相径庭。[24]"进攻性制空权作战"的定义相当宽泛(甚至可被理解为在一定程度上包括网空)，但我们通常认为其含义就是通过动用自身的空中力量来削弱对方的空中进攻能力。[25] 但如上所述，在网空中，我们仅仅通过运用进攻性网空能力（甚至动用动能打击能力）很难指望有效削弱敌人的进攻性网空作战能力。这不是说我们的进攻性网空作战能力没有用处，而只是想表明对抗的双方部队不容易大幅度削弱对方，至少难以直接打击对方，或难以像"进攻性制空权作战"那样瘫痪对方。

一个国家，不仅其网空进攻部队总体上可以免受打击，其网空防卫部队也可在网空战争的逆境中很快成长壮大。具体而言，网络一旦遭受攻击，便暴露出漏洞，其防卫者就能实施网络修补或以其它方式堵住这个攻击通道，使对方原来使用的攻击工具无法长期续用。如利比奇所言："攻击方若想连续打击对方的类似目标将越来越困难，因为对方能够从每一次被攻击中恢复并加以巩固。"[26] 这样，"网空武器"高度易耗易报废，而其研发却相对耗时和耗钱，从而导致攻击潜能在交战期间渐渐消减。[27]

与此同时，作战指挥官并不需要通过削弱某部分来"集中兵力"去实施其它作战任务。在网空领域，进攻部队可能与防卫部队技能不同且互相分离，我们不需要考虑如何调度其它作战能力来"翼侧掩护"，或者为了保证关键交通线和后方的安全而有意转移对方的一部分火力。这些因素结合起来告诉我们，在网空战争中可能不存在所谓的消耗战略，至少不存在传统意义上的消耗对方有生力量的说法。

如果网空部队不能在本领域中有效实施打击军事力量使命，那么空军就必须改变实现网空作战目标的方式，必须有别于空中作战。空军作战准则 AFDD 3-01《制空权作战》指出："取得空中优势通常是联合部队的首要目标，尤其是当敌人有能力从空中威胁友军部队或者阻止联合部队司令官开展有效作战时。"[28] 空军中有人简单地把这段论述中的"空中"换成"网空"，表明这些人如何轻易做出类比并从中得出结论，以为网空部队的首要任务就是夺取"网空优势"。所谓网空优势在某些情况下也许成立，但在更多情况下也许只不过是说我们的进攻和防卫能力应该胜过

敌人，亦即，稍作深究，便知只是一句空话而已。

我们确保“网空优势”，不是靠对敌人实施网空攻击行动来削弱对方能力而保护自身能力，更多的，是我们必须部署一支相对于敌人而言更能干的、训练有素的、资源充分的队伍。如此说来，这样的网空优势不仅仅是一种希望通过作战达成的目标，而是从双方敌对的一开始就基本确定的态势，是在敌对行为发生之前的和平时期就通过战略规划和准备获得的结果。我们即使在网空中和一支劣势部队交战，也不是凭借优势战术来征服对方、消耗对方，或者转变战局（理由如上所述）。因此，“网空优势”作为一个作战准则术语，其实没有什么实用意义，因为这不是我们战役设计中所想达成的目的，它只是一个表示在战争中司令官难以施加影响的双方部队相对质量的浅近解说符。如果敌人从网空占据明显更大的军事上风（亦即取得“网空优势”），那么我方司令官唯一能做的，或许就是在一定程度上将网空“撤出作战”，亦即要么把自己的部队从互联网隔离，要么通过物理（甚至逻辑炸弹）攻击而将敌人从互联网隔离——后者显然是迫不得已的最后做法，说起来容易做起来难。

结语

网空作为一种作战环境，因其主要特征为代码逻辑或虚拟性质，而与传统的物理领域有着根本的区别。对其之基本作战原则应从根本上加以再思考，正如当年对天空之于陆地战争和海洋战争的思考一样。网空以其独有的特征，挑战着和战争相关的许多现成假设。如果我们甚至无法将诸如消耗战略及打击军事力量战略等基本作战概念（直接）运用于网空战争，在企图把其它作战原则套用于网空作战时就更应多加小心。

迄今为止,有说服力的“网空战例”极少，想从中归纳出成熟的作战经验教训谈何容易。[29] 故而，我们在编写网空作战准则时，就自然会倾向于借鉴其它作战领域验证过的作战概念，将现成的智慧试着套用于网空新领域。然而，即使我们能够找出理由将某些德高望重的现成理论框架套用到网空战争，却无法使我们更有效地理解和实施网空作战，那么这样的套用就毫无意义。与其费尽心思把某些现成的战争原则套用于网空，不如首先思考此原则对网空是否有任何实质性的意义。我们只有在认真理解了网空的特质之后，才能实事求是地借鉴以往战争智慧，为网空订立新的作战准则。♣

注释:

1. Jeff Boleng, Dino Schweitzer, and David Gibson, “Developing Cyber Warriors”[培养网空战士], (presentation, Third International Conference on i-Warfare and Security, US Air Force Academy, Colorado Springs, CO, September 2007), http://www.usafa.edu/df/dfe/dfer/centers/accr/docs/boleng2008a.pdf.
2. 笔者亦参加此研讨会，有关此研讨会的任何观点如未在本注释部分注明出处，则纯属笔者个人回忆。
3. Department of Defense, The National Military Strategy for Cyberspace Operations [国家网空军事战略], (Washington, DC: Department of Defense, December 2006), ix, http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf.
4. Maj Gen Bill Lord, “Air Force Cyber Command (P) Update”[空军网空司令部（暂编）最新通报], (presentation, Armed Forces Communications and Electronics Association, Boston [Lexington-Concord chapter], 23 January 2007), slide 17, http://www.afceaboston.com/documents/events/nh08/Gen_Lord.pdf.

5. 见参联会主席 2008 年 7 月 0363-08 号备忘录；另参看 Joint Publication (JP) 1-02, Department of Defense Dictionary of Military and Associated Terms [联合作战准则 JP 1-02：国防部军语词典], 8 November 2010 (as amended through 15 August 2012), 77, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

6. 要想为否定式推断提供证据比较困难，因为空军显然没有通过颁布正式文件来明确将作战系统军官划出网空专业之外，或将一般电子战划出网空领域之外。但是，空军关于网空的一些最新文件很少提及这类军官；并且，空军现在似乎经常把网空等同于信息系统和数据网络——尤其是基于互联网协议的计算机网络。至少我们可以肯定地说，专业代码 12R 类（电子作战系统军官）基本自成一类，没有像最初计划地那样全部归属到网空专业类内，对其的安排与对专业代码 33S（通信）的安排不同。具体信息参看 Headquarters Air Force Personnel Center, Air Force Officer Classification Directory [空军军官分类目录], (Randolph AFB, TX: Headquarters Air Force Personnel Center, 1 August 2012), 48.

7. 白宫的确在 2011 年 3 月颁布指导原则，限制在公共文件中把网空与陆地、海洋、天空及太空完全同等看待为一个军事行动领域。在如此高的层次上颁布这样的指南，其本身就说明网空战争正得到空前的关注。参看 White House, memorandum, subject: White House Guidance Regarding the Use of "Domain" in Unclassified Documents and Public Statements [白宫备忘录，主题：白宫关于在非保密文件和公共声明文件中使用"领域"一词的指导原则], 14 March 2011.

8. Gregory J. Rattray, Strategic Warfare in Cyberspace [网空中的战略战争], (Cambridge, MA: MIT Press, 2001), 17.

9. "信息作为一个环境概念，可能难以被理解，但是信息的确以独特方式与物理环境相关联，这一点毫无争议。网空就是让那些在电磁频谱中通过辐射能运行的计算机、通信系统等装置交汇和互动的环境。"参看 Dan Kuehl, "Defining Information Power" [定义信息力量], Strategic Forum, no. 115 (June 1997): 3, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA394366. 另参看 Dan Kuehl, "The Information Revolution and the Transformation of Warfare" [信息革命及其对战争的改变], 见 The History of Information Security: A Comprehensive Handbook [信息安全历史综合手册], ed. Karl de Leeuw and Jan Bergstra (Amsterdam: Elsevier, 2007), 823n6.

10. Lani Kass, "A Warfighting Domain" [一个作战领域], 26 September 2006, slide 14, http://www.au.af.mil/info-ops/usaf/cyberspace_taskforce_sep06.pdf.

11. "爆炸性化学反应"或许是更真实的类比，虽然可能不那么直观。和电磁频谱相对于网空一样，它也是一种关键的物理现象，不仅在陆地领域发挥巨大作用，也在其它领域中获得应用。

12. 从本科生网空训练课程的内容可以看出，其重点是放在以数据和网络为中心的教育训练上。参看 Julie R. Karr, "Cyberspace Force Development" [网空部队培养], 18 May 2011, slide 8, http://www.safxc.af.mil/shared/media/document/AFD-110614-028.ppt.

13. "4 月 30 日 10: 33S [通信] 人才 / 岗位转入 17D [网空军官]. . . . 并将空军专业代码 15 [通信和信息] 转入专业代码 11 3DXXX [网空士官]。"参看 Brig Gen David Cotton, "Cyberspace Workforce Transformation Update" [网空人才培养变革通报], May 2010, slides 14, 15. 虽然空军从各种专业代码中抽调军官人才调入网空专业，但这个新专业中人数最多的是那些有通信专业背景的军官，专业的重点放在计算机网络技能的培养上。

14. LCDR Jorge Muñiz Jr., USN, "Declawing the Dragon: Why the U.S. Must Counter Chinese Cyber-Warriors" [斩断龙爪：为什么美国必须对抗中国的网络战士], (thesis, US Army Command and General Staff College, 2009), 2, http://www.hsdl.org/?view&did=11694.

15. 同上，第 5 页。

16. Benjamin S. Lambeth, "Airpower, Spacepower, and Cyberpower" [空中力量、太空力量、网空力量], Joint Force Quarterly, issue 60 (1st Quarter 2011): 46, http://www.ndu.edu/press/lib/images/jfq-60/JFQ60_46-53_Lambeth.pdf.

17. 空军作战准则这样说："[网空] 要求……重视电磁频谱……。系统也可以设计为改变频率（在电磁频谱内的频率上运作）并操纵数据。于是物理操纵的空间就存在于网空之中。"参看 Air Force Doctrine Document (AFDD) 3-12, Cyberspace Operations [AFDD 3-12：网空作战], 15 July 2010 (incorporating change 1, 30 November 2011), 2, 3, http://www.e-publishing.af.mil/shared/media/epubs/afdd3-12.pdf.

18. Samuel E. Liles, "An Argument for a Comprehensive Definition of Cyberspace" [对网空全面定义的一点意见], Selil (blog), 18 November 2011, http://selil.com/archives/2712.

19. 引用这种看法者不乏其人，例如空军作战准则 AFDD 3-12 说："在网空中，从实施行动到产生效果之间的时间仅以微秒计。"还说："不同行动可以几乎同时发生。"见 AFDD 3-12, Cyberspace Operations [网空作战], 29, 9.

20. 太空可能作为例外，此领域有其独有特质，本文限于篇幅不予讨论。

21. 一些独立私营企业在一定程度上可以合法被视为国防力量的一部分，这也是网空的一个有趣的特点。

22. 有人可能会争辩说，有些网络访问行动可能要求行动成员在物理上靠近敌人的网络，这些人因此处于危险之中。笔者认为这种做法实属特种作战范畴，是以特战方式支援（或者实施）网空行动，而不应被视为实际的“网空进攻部队”。并且，把上述行动人员部署到有物理危险的地方的部队也肯定不属于网空部队。

23. Martin C. Libicki, Cyberdeterrence and Cyberwar [网空威慑和网空战争], (Santa Monica, CA: RAND, 2009), 60, http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

24. 参看 AFDD 3-12, Cyberspace Operations [网空作战], 52.“进攻性制网权作战”也被确定为“空军网空关键能力发展”九项优先中的第七项，参看 Cyber Vision 2025: United States Air Force Cyberspace Science and Technology Vision 2012-2025 [2025 年网空愿景：空军 2012-2025 年网空科学和技术愿景], (Washington, DC: AF/ST [Science and Technology], 15 July 2012), 19.

25. 进攻性制空权作战（OCA）指“摧毁、阻止或瘫痪敌人飞机、导弹、发射台及其支持结构与系统，无论发射之前或之后，并应将之消灭在尽量靠近其原始部位。OCA 的目的是将敌人的飞机、导弹及其整个支持结构摧毁在其未及部署就位之前，从而阻止敌人飞机升空和导弹射出。”参看 JP 3-01, Countering Air and Missile Threats, 23 March 2012 [制空权和导弹威胁], I-3, http://www.dtic.mil/doctrine/new_pubs/jp3_01.pdf. 其中称“OCA 的打击目标包括敌人的指挥控制、通信、网空以及情报节点。”另参看 AFDD 3-01, Counterair Operations [制空权作战], 1 October 2008 (interim change 2 [last review], 1 November 2011), 5-6, http://www.e-publishing.af.mil/shared/media/epubs/afdd3-01.pdf.

26. 见注释 23 中《网空威慑和网空战争》，第 59 页。

27. Libicki 在其《网空威慑和网空战争》专著的 56-59 页中有更详细的讨论，他认为网空攻击可能随着时间而慢慢失去效果，因此网空作战可能逐渐削弱消减，见第 135 页。

28. 见注释 25 中 AFDD 3-01《制空权作战》，第 1 页。

29. 网空战例只有零星几例（例如：以色利在 2007 年空袭叙利亚核反应堆的“果园”行动中据称发动了网络攻击，另一个例子是“震网”病毒攻击）。但这些例子都不足以构成网空领域中的公开战争（虽然可以视为网空攻击的现实版本，体现了秘密外科手术式打击的特征）。可能有人提出，2007 年俄罗斯对格鲁吉亚的网空攻击应算作“网空战争的有力证明”。这的确是迄今为止最具说服力的例子。即使如此，在此战例中，战争双方实力如此悬殊，很难说网空攻击对冲突结果是否产生任何实质性影响。故而很难以此例为基础编写网空战争作战准则。

肖恩・巴特勒，美国空军少校（Maj Sean C. Butler, USAF），南加州大学理学士，空军理工学院理科硕士，现在阿拉巴马州马克斯韦尔空军基地的空军指挥参谋学院任教。他自南加州大学空军后备役军官训练团获授军官衔。巴特勒少校曾在德州拉克兰空军基地第 23 信息作战中队服役，参与制定网络战战术。他曾作为美国空军军官学院助理教授管理及教授网络安全课程，并指导该院学员队在 2004 年网空防卫演习中压倒兄弟军种院校获胜。他是空军军官学院被选拔参加 2007 年“作战测试”本科网络战训练课程的空军专家之一，并参与制定成为现今空军网空部队训练课程基础的教学大纲。

来自网空用于网空：明确网空情监侦作战的概念

For and from Cyberspace: Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance

作者：美国空军上校马修·M·赫尔利（Col Matthew M. Hurley, USAF）

二十年以前，即在数码时代的初晨，我们还只能从科幻作品中看到人类在某种合成的、虚拟的领域中交往和争斗。[1] 我们曾被《创战记》和《战争游戏》等科幻电影刺激得激动不已，一想到《终结者》中的“天网”将可能如电影预示的那样具有自我意识就不寒而栗。然而，电影一结束，我们便揉去眼前的噩梦，重新步入光明的“真实”世界。

曾几何时，今天的我们已经不再把网空视为科幻的异想天开，而是一个与陆、海、空、天这四个传统环境同样重要的作战领域。[2] 当然，网空与这四个我们较熟悉的自然领域又有显然的不同。情报 / 监视 / 侦察（ISR—情监侦）作战如何在这个新的、变幻无穷的人造环境中运作和发挥？美国空军情监侦部门在努力认识这个新奇作战领域的过程中正面临那些挑战？以及，空军情监侦部门应如何应对网空与生俱来的问题和需求？本文将逐次讨论这几个根本问题。[3]

界定网空情监侦

与在自然领域中开展情监侦作战不同，网空情监侦作战还有待在联合或军种作战准则中被正式界定。尽管人们广泛谈及“网空情报”（CYBINT）及其与信号情报及公开源情报的关系、甚至有人呼吁更细地划分为如“SkypeINT”或“VoIPINT”等基于载体的不同情报分类，其实对这个主题，当前的理解仍未成熟。[4] 正如负责情监侦作战的空军副参谋长拉利·D·詹姆斯（Larry D. James）中将在 2011 年所言：“我们才刚刚开始从空军的角度来思考这些事情。”[5] 因此，虽然“网空情监侦”这一术语在空军情监侦部门已经获得了越来越多的认可，它同时也引起了国防部其它部门和空军参谋部对其含义的质疑。[6] 本文首先提供一个概念作为讨论的起点，以助澄清和完善未来的作战准则。

为正确理解网空情监侦作战，也许我们可以将网空活动分为两个行动范畴：来自网

空的情监侦和用于网空的情监侦。来自网空的情监侦可追溯到二十世纪八十年代那些设法从对手网络获取数据的最初努力，今天的分析员继续在网空搜索，梳理出詹姆斯中将所说的“从该领域搜集的任何有情报价值的信息。”[7] 搜索的对象包括比如外国的新闻媒体、威胁行动者经常出没的聊天室、出自危机地区的网络日志和录像或商业图像，等等。它也包含我们较熟悉的计算机网络利用（CNE）这一概念。从网空收集到这些信息之后，我们就能利用它来支持任何领域的作战行动。

就这一点而言，空军政策指令 10-17《网空作战》也许对网空情监侦给出最佳定义。它指示空军情监侦部门的任务是：“确保具备提供协同分析、融合情报、跨域化 / 一体化 / 自动化情监侦 PCPAD（PCPAD 是规划与收集、搜集、处理与利用、分析与生产、分发的英语首字母缩写）的能力，以开展网空作战。”[8] 这个定义揭示了全源情报在网空作战行动的规划和执行期间的重要性。在网空作战，需要的不仅是来自网空的情监侦；任何情报渠道都能为网空行动提供有关键情报价值的信息。[9] 空军情监侦局局长罗伯特·P·奥托（Robert P. Otto）少将指出：“当我们说‘用于网空的情监侦’时，我们指的是为支援网空优势而开展的情监侦作战”——无论什么来源、方法或媒介。[10]

有些人错误地把 CNE 和网空情监侦看成为同一码事，但 CNE 恰好属于第一个行动范围，即来自网空的情监侦。空军作战准则界定 CNE 为“通过使用计算机网络，从目标或对手的自动化信息系统或网络收集数据，从而保障我方的行动和情报搜集能力。”[11] 更明确地说，CNE 的“操作一般是通过网络工具潜入对手的网络系统……操作 CNE 的工具和进行计算机攻击使用的工具相似，但前者是为了情报搜集而不是系统破坏。”[12] 这两种描述都暗示蓄意入侵对手的硬件、软件或相关网络系统。[13] 然而，它们不包括被动搜集有潜在情报价值的公开来源信息。这种被动的情报搜集也是“来自网空的情监侦”的另一个重要形式，包括下载公开发布的敌方最新战斗机的录像，研读外国作战准则或军事出版物，监视聊天室，以及众多在网络系统或网上来无影去无踪的其他活动。它们都有助于达到情监侦的重要目的，即在适当的时候为适当的决策者获取适当的信息。

网络态势感知是一些相关文献中突出描述的另一个与情监侦有关的概念，涉及到察觉、识别并了解网空存在和出现的友善的、敌对的、或介于两者之间的人和事。[14] 然而，态势感知显然不限于情监侦，它还涉及指挥与控制、作战空间感知的非情监侦部分，甚至还有个体认知。[15] 所以，尽管情监侦是态势感知的核心部分，但此两者不应该混为一谈。比如，我们不认为环境监测属于情报搜集范畴，虽然它是作战空间感知的一项职能，也涉及到类似的分析过程。我们也不把所有人类知识算作“有情报价值的信息”，即便知识就意味着感知。

有了这个界定和限制网空情监侦的起始点，那么我们就必须探索我们在其中进行情监侦的环境。如下列几段论述所示，网空作为一个领域引起了重大问题，如果我们想充分了解网空，并在其中有效地作战，我们就必须解决这些问题。

网空的挑战

美国兰德公司分析专家马丁·利比奇（Martin Libicki）对美国政治和战略思维的惯

性做出了这样的概括：每当新的趋势（比如一战期间空中作战兴起，太空技术用于军事应用，等等）出现，每当可能改变游戏规则的革新发生，我们最初的反应通常都是削革新之足适成规之履。而今我们已经将网空宣称为一个作战领域，利比奇担心“我们会拿旧尺子来丈量新事物。”他警告说：“但是你不能如此对待网空，你必须根据它［自己］的法则来思考它。”[16] 当然，在所有作战领域，情监侦及其他军事活动中都存在着一些普遍和持久的共性，但是，利比奇的基本观点值得我们注意，即我们不能只是照搬现行的作战准则和战术 / 战技 / 战规，把所有出现“天空”或“太空”的地方改成“网空”就了事。网空有其独特的性质，由此带来新机遇和新挑战，要求我们创新思考，开拓新路，而不是拿旧瓶子装新酒。[17]

网空这个最新作战环境正是以其独特属性，把网空情监侦和“自然”领域里的互补性活动区别开来。首要的、也是最显著的一点是：网空是由人类创建的，人类又在不断地修改它；20 多亿用户的每一次网上点击或键击都波及整个网空。前国家安全局局长及中央情报局局长、美国空军退役上将迈克尔·V·海登（Michael V. Hayden）说：“其它领域是自然的，但网空这个领域是人类的创作。人类能真实改变其地理，网空发生的‘任何事’能在某个人的‘物理空间’产生变化。”[18] 网空既来自人造，便导致了三个特征：复杂性、适变性和变化速度，这三个特征使网空与相对稳定的自然领域有了区别。姑且承认，自然界也是复杂的，随改的，变化的，但是它的变化程度和速度都不能和网空相提并论。我们仍然能认出我们祖先就熟知的那些高山、大海和星辰。然而今日的网空与区区二十年（大致为一个人的兵龄）前的网空已然是天壤之别。[19]

谈到复杂性，网空错综得令人窒息，曲折得令人发狂，一切都彼此相连，现今已生产出 500 亿个装置连在网中，任牵一发即可动全身，效应之深之广，全然不成比例。[20] 因此，网空思维“必须要考虑互联关系，即网络，以及人类是如何构建和使用网空领域的”。网络的海量性、不稳定性、不可预测性、关系复杂性等等，都使得网空思维极难把握和适应。[21]

网空固有的适变性促成了它的复杂性和动态多变性。[22] 它随着网空内外条件（诸如新技术、威胁、政治与法律）的演进而持续不断地（通过数亿个分散用户的行动）变化着。请注意，因特网本身的设计就是为了促进科技发明的飞速扩张和对技术革新的适应。[23] 这些变化既培育了网空的适变性，变化本身也以飞快的速度发生，伴随各种创新的、常常出乎意料的技术不停地改变着网空景观，其改变之快，为其他任何技术领域所不及。[24] 一个四人组英国观察家这样描述说：“变化速度如此迅猛，致使战略演进的传统性行动 / 反应周期还未及开始就已经过时，就好比政府派一位作战分析家去观察燧发步枪交战的效果，当他到达时却发现马克沁机枪都已经发明出来了。”[25]

网空的急剧膨胀进一步加大了它的复杂性和适变性。物理领域的规模大小相对稳定，网空则不同，它在各重大方面都呈几何级数扩张。[26] 到 2011 年中期，人类在网空中已进行了 2 万多亿项交易，涉及到 50 万亿吉字节数据。[27] 让时光快进到 2025 年，我们预期到那时将有约 55 亿数字化居民，代表 60% 的世界预计人口，他们每天将使用 2500 万

个应用程序来进行数十亿项交易，每日生成或交换 50 万亿吉字节数据。网民将有大约 30 亿个因特网主机供其选择，每个主机都可能拥有数千个体网站。[28] 人们苦于想把网空梳理清楚，但它的飞速扩张令人难以招架。

传统上，军事策划者和实践者一直认为，规模大小和距离远近与所需时间成比例关系：穿越远距离或征服大面积都需要更多时间。比如二战期间，护航船队从美国航行到英国用了一周多时间，同盟国从登陆诺曼底到渡过莱茵河就用了将近 10 个月时间。然而，军事上传统的时间概念对网空毫不相干。[29] 理论上，普通人一眨眼的功夫，我们就能把一个数据包从起源地投送到目的地，从地球上的任何一点到任何另一点。网空是以“字节速度”行动。[30]

网空蔓延到全世界每个角落，加之网络效应的速度，它为美国空军的“全球到达”观念增添了一个新的、令人敬畏的维度。[31] 网空物理节点遍布每一个自然领域——五洲四海之内、之上、之周围。网空在全球纵横交错，把人与人之间的距离拉近到前所未见，同时也使敌人有了以往无法想像的攻击便利。[32] 过去，作战人员总是有独立的战区来开展行动。[33] 然而在网空，毫不夸张地说，敌对行动可以发起于或途经任何有因特网设备功能的地点。[34] 而且，网空的全球性质已经使主权实体之间的传统边界基本上失去意义。[35] 由于高超的对手有能力从多处前线进行干扰或袭击而几乎不受惩罚，“地理位置就毫不相干了。因此，判定某个服务器的地理位置根本无济于事，就算知道了某个拒绝服务攻击来自某地点某服务器也说明不了问题，因为攻击者可以利用设在美国的服务器，也可以利用设在中国、马来西亚或者文莱的服务器。容易得很，小菜一碟。”[36] 网空的全球弥散性和地理模糊性对有效开展情监侦增加了复杂性，因为你无法锁定任何静止的物理空间——这从根本上背离了情监侦的地球中心说概念。

不仅主权国家边境，而且主权国家本身，在网空中都开始失去意义。没有哪个网络化的国家政府敢声称对这个领域的力量垄断，也不敢断言完全拥有军事行动所必须的基础设施。[37] 这第一种情况是因为：进入网空成本很低，加上越来越先进的威胁软件唾手可得，使非国家行为体、甚至某些个人，都有机会进行那些以前纯属国家安全机构职责的活动。[38] 但是现在在网空，参与者“不需要受良好教育，也不必拥有充分资源……只需要有破坏意图和技术能力，就能进行破坏活动。”[39] 另外，大约 90% 的网空基础设施属私人所有，尽管它最初可能是由政府资助的，尽管政府和武装部队现在严重依赖这些商业基础设施。[40] 其结果，在网空“公与私、政府与商业、军事与非军事之间的区别和划分，都已模糊不清。”[41]

网空的这些特征帮助造成了令所有情监侦专业人士“最棘手的问题”：如何判定和追溯攻击源。[42] 空军太空司令部承认：“真实（最初）攻击源的隐蔽性使人难以找到攻击者，而且，因特网本身的结构设计就有助于匿名。”[43] 网络参与者的海量人数，也使追踪溯源更加困难，国防部在企图找出一个内部威胁时就遭遇这种困难。如果每个用户代表一个节点，每封电子邮件代表一个链接，在单独一年之内，我们就得分析 237,387,616 节点之间的 755,230,064,000 个链接——这个计数还不包括网络搜索、文件存取，或其它类型的理论上可以观察到的网络活动。[44]

不单潜在目标群规模庞大，网络工具也使追踪溯源进一步复杂化。拥有多达数百万台机器的僵尸网络、专门用于匿名化的代理网站、洋葱路由、以及相关技术等，都为积极判定攻击源设置了令人生畏的障碍。[45] 从根本上说，因特网“天生就是依据未经验证的数据交换协议运作的，”也就是说，“溯源和不可否定性常常与匿名性相冲突。”[46] 追踪溯源虽然极为不易，但也“并非不可能”，第659情监侦大队的指挥官丹尼尔·辛普森（Daniel Simpson）上校如是说；“然而，你需要精明能干的情监侦专业人士进行认真努力的分析。”[47] 尽管在溯源技术有所改进，但如前国防部副部长威廉·J·林三世（William J. Lynn III）说，“总的趋势是越来越困难。来袭导弹回路可知，网络袭击则来路不明。”[48]

攻击源的判定如果不完整或不准确，也有可能导致情监侦部门违反法律、政策和宪法规定。对攻击来源和性质（来自本国或外国，属于犯罪、军事、或情报行动性质）的不确定性，不仅会延误溯源过程，并使我们难以把握美国法典 10/18/50 卷所赋权利；而且不确切或无把握的溯源还可能导致违反这些权利的行为。[49] 如前联邦调查局局长罗伯特·缪勒（Robert Mueller）在听证会上所言：“一开始，你不知道［网空侵入者］是一个国家行为体，还是一帮受国家行为体操纵的个人，或者就是街对面的一个稚气未脱的高中生。”[50] 为应对这一挑战，有人提出了一些方案，比如：军界、情报界、工业界之间共享数据；或者为能积极防御而更大胆和全面地搜集情报；或者“重新设计”因特网以有利于追踪和判定地理位置，等等。但这些提议惹恼了那些主张网上隐私、公民自由、互联网自由的组织。[51] 本文不打算从法律层面开展讨论。[52] 但需要指出：因为有时情报活动和网空执法活动之间的界限不明确，我们可能会面临“陷入网络法律这个未知水域”的风险。[53]

前景与建议

面对网空固有的障碍，如果情监侦部门计划希望在这个最新领域有效地作战，它就必须在思想、资源、人员等方面做出并保持适当的投资。在思想领域，其首要任务是，必须明确情监侦如何参与更大范围的网络作战。目前，空军和联合部队在这一点上缺少共识。大多数军事与国家作战准则及政策文件都着重论述进攻和防御性网空活动，而把情监侦降级为支援角色。例如在 2010 年，空军太空司令部——空军网空作战核心功能的首要协调机构——把情监侦描述为网空支援、网空防御、网空兵力应用等使命所需的一种“能力”。[54]

这些观念都没有认识到，情监侦本身就是一项作战使命。在网空作战过程中的其它任何时候，它始终既是中心又是根本。的确，网空行动“浸泡在情报中”，一旦没有情监侦，网空行动“简直就是俗话说的黑灯瞎火乱开枪。”[55] 詹姆斯中将主张“我们不把情监侦和空天领域的行动分开。在网空，它们甚至连结得更加密切。”[56] 所以，我们需要在作战准则、教育和组织结构等各方面大力强调网空情监侦的核心作用和作战性质——不是为它自身的缘故，而是为了认识到这一事实：假如没有情监侦，我们就将耳聋目瞎，所有行动都将受到损害。

然而为了发挥效力，网空情监侦需要的远远不只是从制度上重视及调拨资金或人力，还必须调整自身适应作战环境。就网空而言，情监侦必须保持全球感知，时刻警戒，预测而不是反应，敏捷主动，并能应对和管理急

剧增长的海量数据。这种愿景进一步要求我们加强招聘和训练网空情监侦专业人才，通过他们更好地保护公民自由和隐私，并且更合理地将网空情监侦融入整个情报界。

建设预测性情监侦和早期预警能力

前国家情报总监迈克·麦康纳（Mike McConnell）等观察家认为，网空情监侦与国防目前的“最新技术水平”只能做到依赖“事发之后的调查取证”来评估损伤和查找攻击发起者。[57] 过去，我们也曾依赖周边防御和防火墙；但是狡猾的敌人总能找到途径绕开或突破无论有多么复杂的“网络马奇诺防线”。[58] 因此，我们需要构建一道“网络远程早期预警线”，应具备溯源和防御能力，能在敌人实施破坏之前就对威胁做出响应。[59]

为对任何瞬间可能发生的攻击做出尽早的预警，我们必须实时感知全球网络活动及其发生背景，以采取更有预测性的措施。[60] 预测性网空情监侦立足于以往经验和对当前趋势的把握，积极查找网空可能发生的破坏活动的任何迹象，诸如某些组织对美国的积怨、“爱国黑客”群体的异常动态、网聊者、新技术、对手的作战准则，等等。[61] 我们必须监视所有这些潜在线索，“不间断地进行，抓住蛛丝马迹顺藤摸瓜，从而做到防患于未然。”[62]

敏捷主动

当然，“早期”预警是相对的。冷战时期我们认为，洲际弹道导弹从发射到落地需要 30 来分钟；但是，如今的网络袭击能在 30 毫秒内从北京闪击纽约。[63] 这种速度需要的敏捷性和主动性在“物理”战争时代无异于天方夜谭，几乎是异想天开。空军研究实验室的卡莫尔·杰伯博士（Dr. Kamal Jabbour）指出：“网空敏捷性”不仅意味着迅速分析，而且还有对未来行为与效果的“预期”，以及对防御措施的有效实时安排。”[64] 这就要求情监侦部门在网空所有方面（速度、隐形、灵活性、适变性、以及使网空具有如此挑战性的其他各重大因素）都保持领先。[65] 正在进行的科技计划，比如《2025 年网空愿景》，提供了一个宝贵的起点，我们可以藉此了解这些问题并设计解决方案。空军部长迈克尔·唐利已经指挥空军领导班子积极部署，为实现此远景开拓道路。

自动化与可视化

网空数据如此浩瀚，恰如东方智语：“眩目之亮一如遮目之暗，均可致盲。”[66] 目前，网络传感器收集的数据量达到拍字节（petabytes），尧字节（yottabytes）的时代也为时不远。[67] 目前的数据收集量已经使我们无法招架，难以识别和淘出“真金”，也无从有效分析或处理成可操作的情报。因此，网空情监侦“要求我们开发算法语言和可视化能力，使网空活动智能化。”[68] 在这个等式的一边，我们需要取得能实现情监侦分析自动化的技术、操作图像和预测性软件，并为此得到人力和财力支持；在等式的另一边我们需要加上人才这个同样重要、甚至更重要的变量。

招聘与训练

我们中许多人都是所谓的数字时代移民。我们最初接触集成电路的亲身经历大概始于二十世纪七十年代的古董计算器、电子手表、也许还有早期的电子游戏机。网空的出现及其快速发展，一直令那些刚步下模拟技术之船——自愿或非自愿地——又步入数码新世界的人们感到苦恼、甚至畏惧。我们的下一代军人则属于另一种类。他们出生的

消息，可能是通过电子邮件公布于世；他们的生活中，大概从来不会经历没有电脑的时刻；他们全然不同于父辈的航空兵，但同样是世界上最优秀的军人。不过，对于玩了九年“使命召唤”电子战争游戏并主要由此获得战争概念的这一代人来说，美国空军的“飞行—战斗—必胜”座右铭自有其不同的含义，这一代人在数字化环境中长大，可能是整个网空领域最宝贵的资产。国家安全局局长兼美国网空司令部司令基斯•亚历山大上将（Gen Keith B. Alexander）显然认识到了这一点，他最近在一次自称为黑客大会的聚会上作了一次征兵宣传。[69] 需要的人才就在那里，而且人才济济。一旦被招入伍，这些人才只需接受网空作战的上层标准训练。但是这将要求“有扎实强大的技术及分析专业知识”——这些知识还必须不断更新才能适应网空领域的爆炸式进化。[70] 尽管詹姆斯中将声称：网空情监侦训练正在改善，但这项任务尚未完成。[71] 鉴于网空的不断进化，进一步完善空军技术专业编码体系、研究生课程、特定的适应性在职训练等，必须继续列为网空情监侦的首要优先任务之一。

网空情监侦的“正常化”

人力资源与训练、以及材料与技术，近来引起了国防部和空军的多项高级计划的关注，其中包括空军首席科学家的《2025 年网空愿景》研究、2012 年空军网空峰会、国防部的网空战略组合评估。具体成果——及其由此带来的未来网空情监侦能力——将取决于这些努力的结果、财政状况、持续演变的网空威胁与机遇等。然而，概念上讲，关于网空情监侦正常化的工作在今天就能、也应该开始。詹姆斯中将和其他空军情监侦领导人一直极力坚持认为：欲求情监侦有效运作，必须做到无缝衔接和抹除域间界线。情监侦在于为决策者投送及时、相关、可操作的情报，搜集情报信息的地点和方式对终极目标而言相对无关紧要。这样看来，正常化涉及到拆除我们在所有网空领域内外竖起的各自为阵的“烟囱”型指挥关系，承认对使命最重要的是从最终分析中获得的有用信息本身，而不是我们获取信息的方式或领域。鉴于网空领域的独特性、我们在该领域作战的相对生疏、作战计划有待实战验证等，我们在思维方式和体制上仍有许多障碍需要清除。然后，网空情监侦才能像天空情监侦和太空情监侦那样获得充分理解、承认和利用。说到底，这是一个教育和领导问题；但是在做好教育和领导之前，我们首先必须清楚认识到：网空本身已经形成一个领域，它像其它领域那样，以本质上相同的方式为情监侦带来了需求和机遇。在并不久远的过去，太空情报运作也曾有过生疏的、概念破碎的时期，但是它对作战效力的贡献却随着本身的成熟而迅速增长。

保护公民自由和隐私权

然而，对网空情监侦的各种人力物力投资，都必须坚守政府保护公民自由和宪法权利的义务。[72] 辛普森上校承认：“目前尚处婴儿期的网空法律和政策为情监侦运作造成权限与界限确定及管理方面的困难。”[73] 网空意识、安全和公民自由之间的平衡在不断演变，需要连续关注，并可对公众信任产生相当大的影响。[74] 对情监侦部门来说，这不只是一个次要的担忧。军人必须服务公民和捍卫宪法，因此在这些问题上应始终保持警觉和严格遵守规程。尽管今日网空法规仍模糊不清，也无论将来会出现什么相关的法院裁定，整个情报部队必须坚定不移地保护宪法及每个公民的隐私权。

结语

过去百年来，空军及其前身已经展现了征服新作战领域的强大能力——首先是天空，之后是太空。两次征服过程中，情监侦作战都证明对开创和维持新领域发挥了关键作用。相较而言，网空尽管有其种种独特属性，也同样拥有与前两个领域相同的根本特征：一旦缺少及时、相关、可操作的情监侦，其它所有军事活动的成功就只好听凭运气。这个新领域的将士们正遇到重重困难，但将作战成败付诸运气不是我们的选择。[75] 网空情监侦面临的困难有时似乎无法解决，但是我们不可迷惑于表象。当年空中力量也曾风驰电掣般快速发展和成熟，造成巨大的思维错位和滞后；在此之后开发浩瀚太空的几十年里，同样的现象再次发生。毫无疑问，现今我们又进入一个新的作战领域，必定遭遇许多同样的智力成长之痛。然而我们应该坚信：只要坚持不懈地深入全面了解网空，定能克服这些烦恼，网空情监侦帮助我们了解网空，又反过来加快网空情监侦的发展。为了继续这种积极的趋势，我们必须投资；要投资，我们就必须获得政府领导的承诺；但是要承诺，我们首先必须充分了解我们作为一支空军和一个国家所面临的挑战和机会以及其之性质和程度。情监侦作战是获得这种了解的关键——人类过去征服其他各种领域如此，现在征服网空亦然。♣

注释:

1. 在《神经漫游者》(Neuromancer）这本书中，威廉·吉布森（William Gibson）预言性地杜撰了“网空”(Cyberspace）一词来假设一种科幻奇思：“数亿人每日体验共意幻觉……从人体系统的每个计算机库里提取数据，无法想象的复杂性。”参看 William Gibson, Neuromancer (New York: Ace Books, 1984), 第 69 页。

2. 联合作战准则把网空界定为“信息环境内的一个全球性领域，由相互依存的信息技术基础设施网所组成，包括因特网、电信网、计算机系统、嵌入式处理器和控制器。”参看 Joint Publication (JP) 1-02, Department of Defense Dictionary of Military and Associated Terms [联合作战准则 JP 1-02：国防部军语辞典], 8 November 2010 (as amended through 15 August 2012), 77, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf. 然而笔者同意 Daniel Wasserbly 所说：“‘网空’本身就是一个如此模糊的概念，仅仅为了确定它的基本原理以及它如何影响军事领域就已经花费了数年的计划时间和人力。”参看 Daniel Wasserbly,“Charting the Course through Virtual Enemy Territory”[制定突破敌方虚拟领土的方针], Jane's International Defence Review, 44, no. 5 (May 2011): 60。或者如美国空军退役将军 Michael V. Hayden 所观察：“很少有什么事比这个现象更模糊，更缺乏明确理解，但却如此被看重被热论。”参看 Michael V. Hayden,“The Future of Things 'Cyber' ”[未来‘网络’之事], Strategic Studies Quarterly, 5, no. 1 (Spring 2011), 3, http://www.au.af.mil/au/ssq/2011/spring/hayden.pdf.

3. 本文不讨论威胁——有关这个主题的文字资料就像威胁本身那样包罗万象且五花八门。然而，在所有军事行动中，对威胁的有效响应始于概念健全、计划周密、执行得当的情监侦。

4. 关于 CYBINT（网空情报），参看 Dr. Kamal T. Jabbour, 50 Cyber Questions Every Airman Can Answer [每个航空兵都应能回答的 50 个网空问题], (Wright-Patterson AFB, OH: Air Force Research Laboratory, 7 May 2008), 20, http://www.au.af.mil/au/awc/awcgate/afrl/50_cyber_questions.pdf; 关于 CYBINT 与信号情报的关系，可参看 Air Force Doctrine Document (AFDD) 2-0, Global Integrated Intelligence, Surveillance, & Reconnaissance Operations [空军作战准则 AFDD 2-0：全球一体化情报 / 监视 / 侦察作战], 6 January 2012, 40, http://www.e-publishing.af.mil/shared/media/epubs/afdd2-0.pdf; 关于 Frederick J. Wettering 所描述的公开来源情报，参看“The Internet and the Spy Business”[互联网和间谍工作], International Journal of Intelligence and Counterintelligence, 14, no. 3 (Fall 2001), 344; 另参看“Cyber Vision 2025: United States Air Force Cyberspace Science and Technology Vision 2012-2025”[2025 年网空远景：2012-2025 年美国空军网空科学技术愿景], draft, AF/ST TR 12-01, 1 September 2012, 42.

5. Ben Iannotta,“Voice for Balance”[呼吁平衡之声], DefenseNews, 1 November 2011, http://www.defensenews.com/article/20111101/C4 情监侦 01/111010318/Voice-balance.

6. 从写这篇文章开始时算，作者在过去的几个月里已多次亲身经历。

7. Larry D. James 中将 2012 年 7 月 30 日与笔者交谈。

8. Air Force Policy Directive 10-17, Cyberspace Operations, [空军政策指令 10-17：网空作战], 31 July 2012, 3, http://www.e-publishing.af.mil/shared/media/epubs/AFPD10-17.pdf.

9. Intelligence and National Security Alliance, Cyber Intelligence: Setting the Landscape for an Emerging Discipline [网空情报：设置新兴学科的景观], (Arlington, VA: Intelligence and National Security Alliance, September 2011), 14, https://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Security/Meetings/ISOAG/2012/Sept_ISOAG_CyberIntel.pdf; 另参看 AFDD 3-12, Cyberspace Operations [网空作战], 15 July 2010, 24, http://www.e-publishing.af.mil/shared/media/epubs/afdd3-12.pdf, 它指出“运用全频谱网空效应需要一个多元信息分析途径”和“聚焦全源网空的情监侦。”

10. Robert P. Otto 少将 2012 年 8 月 14 日与笔者书面交谈。

11. 见注释 9 中 AFDD 3-12《网空作战》，第 49 页。

12. Clay Wilson, Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues [信息战、电子战和网空战：能力与相关政策问题], CRS Report for Congress, (Washington, DC: Congressional Research Service, 20 March 2007), 5, http://www.au.af.mil/au/awc/awcgate/crs/rl31787.pdf.

13. Bryan Krekel, Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation [中华人民共和国进行网空战和计算机网络利用的能力], (McLean, VA: Northrop Grumman Corporation, 9 October 2009), 8-9, http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf.

14. Dr. Kamal Jabbour,“The Science and Technology of Cyber Operations”[网空作战的科学技术], High Frontier, 5, no. 3 (May 2009): 11, http://www.afspc.af.mil/shared/media/document/AFD-090519-102.pdf; 另参看注释 4 中“2025 年网空远景”，第 20 页；另参看 Air Force Space Command, Functional Concept for Cyberspace Operations [网空作战的职能概念], (Peterson AFB, CO: Air Force Space Command, 14 June 2010), 7; 另参看 Lt Gen Michael J. Basla,“Cyberspace from a Service Component Perspective”[从军种视角看网空], (address, Cyberspace Symposium, US Strategic Command, 15 November 2011), http://www.afspc.af.mil/library /speeches/speech.asp?id=686. 在此讲话中，Basla 中将把网空态势感知描述为“对作战空间作战情况（包括联合作战网、空军网、友好或非友好部队部署等状况）的了解。”

15. The Manual for the Operation of the Joint Capabilities Integration and Development System [联合能力集成与开发系统操作手册], (Washington, DC: Joint Staff J8 / Joint Capabilities Division, Pentagon, 19 January 2012), https://www.intelink.gov/inteldocs/action.php?kt_path_info=ktcore.actions.document.view&fDocumentId=1517681, 此文件把联合能力领域“作战空间感知”界定为“通过利用情报、监视、侦察、气象、海洋等全源信息，来了解对国家和军事决策起影响作用的作战环境的部署、意图、特点及状况之能力”（B-B-2）。要说明态势感知的个人认知方面，最好的例子也许是 John Boyd 的 OODA（观察、定向、决定、行动）决策环理念，此理念后为单座战斗机飞行员广泛接受。可参看 Col Phillip S. Meilinger, ed., The Paths of Heaven: The Evolution of Airpower Theory [登天之道：空权演变理论], (Maxwell AFB, AL: Air University Press, 1997), xxiii; 另参看 Maj David S. Fadok,“John Boyd and John Warden: Air Power's Quest for Strategic Paralysis”[约翰・博伊德和约翰・沃登：空中力量追求战略性瘫痪打击], (Maxwell AFB, AL: School of Advanced Airpower Studies, 1995), 13.

16. Martin Libicki,“Cyberpower and Strategy”[网空力量与战略], (remarks at the 8th International Institute for Strategic Studies Global Strategic Review,“Global Security Governance and the EmergingDistribution of Power,”Sixth Plenary Session, 12 September 2010), [3], http://www.iiss.org/EasySiteWeb/getresource.axd?AssetID=46892&type=full&servicetype=Attachment.

17. Lt Col Steven E. Cahanin, USAF,“Principles of War for Cyberspace”[网空的战争原则], research report, (Maxwell AFB, AL: Air War College, Air University, 15 January 2011), 1, http://www.airpower.au.af.mil/digital/pdf/articles/Jan-Feb-2012/Research-Cahanin.pdf.

18. 见注释 2 中 Michael V. Hayden“未来‘网络’之事”，第 4 页。

19. 比如，把今日的网空与其二十世纪九十年代早期相比，我们也许看到某些相似之处，诸如电子邮件、留言板、网联、信息库等。但现在回想起来，一些根本性的变化，诸如无处不在的社交媒体、视频流、网上语音视频通信、移动连接，还有今日复杂精密又无孔不入的网络威胁等，都远远超越了甚至二十年前最大胆的预测。

20. 见注释 17 中 Cahanin“网空的战争原则”，第 2 页；另参看 Brookings Institution, Deterrence in Cyberspace: Debating the Right Strategy with Ralph Langner and Dmitri Alperovitch [网空的威慑：与 Ralph Langner 和 Dmitri Alperovitch 辩论

正确战略问题], (Washington, DC: Brookings Institution, 20 September 2011), 2, http://www.brookings.edu/~/media/events/2011/9/20%20cyberspace%20deterrence/20110920_cyber_defense.pdf; 另参看 Paul W. Phister Jr.,“Cyberspace: The Ultimate Complex Adaptive System”[网空：最终的综合自适应系统], International C2 Journal, 4, no. 2 (2010-11): 13-14.

21. 见注释 17 中 Cahanin“网空的战争原则”，第 2 页。

22.“Remarks of the Honorable Michael B. Donley, Secretary of the Air Force[空军部长唐利在空军协会网络未来研讨会上的讲话], Air Force Association Cyber Futures Conference, Gaylord National Resort, Friday, March 23, 2012, 3, http://www.af.mil/shared/media/document/AFD-120326-056.pdf.

23. Department of Defense, Department of Defense Strategy for Operating in Cyberspace [国防部对网空作战的战略], (Washington, DC: Department of Defense, July 2011), 2, http://www.defense.gov/news/d20110714cyber.pdf.

24. 见注释 17 中 Cahanin“网空的战争原则”，第 3-4 页。

25. Paul Cornish et al., On Cyber Warfare [论网空战], Chatham House Report (London: Chatham House [Royal Institute of International Affairs], November 2010, 29, http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf.

26. 虽然太空无限大，或有限但在扩大或缩小（理论各不相同），但是人类的太空空间，也就是说人类已经建立了或多或少永久性存在（即便极遥远）的空间，几乎完全局限在我们自己的太阳系内。除了阿波罗月球登陆和行星际、月球、或太阳探测之外，人类所及空间位于距地球表面 50-22000 英里之间。

27. 见注释 20 中 Brookings Institution“太空的威慑”第 2 页。到 2012 年的年中，我们每一天的每一分钟都会看到网空中传输着：长达 48 小时的 Youtube 视频、204166667 封电子邮件、2000000 次 Google 搜索、684478 个 Facebook 帖子、571 个新因特网网站、27778 篇 Tumblr 博文、100000 多条 Twitter 信息。参看 Oliur Rahman,“How Much Data Is Created on the Internet Every Minute?”[因特网上每分钟产生多少数据 ?], Ultralinx, 24 June 2012, http://theultralinx.com/2012/06/data-created-internet-minute.html.

28. 参看注释 4 中“2025 年网空远景”，第 9 页。

29. Richard M. Crowell, War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare [信息时代的战争：二十一世纪战争中的网空作战入门], (Newport, RI: Naval War College, 2010), 21, http://www.carlisle.army.mil/DIME/documents/War%20in%20the%20Information%20Age%20-%20A%20Primer%20for%20Cyberspace%20Operations%20in%2021st%20Century%20Warfare%20-%20R%20M%20%20Crowell.pdf.

30. 与大众所信相反，网空的活动不是以光速发生，确切地说，网空操作以电子速度进行。光的传播速度大约每秒 186000 英里，而电子——由于有质量——的传播速度“只是”光速的 2/3，即每秒约 125000 英里。参看注释 4 中 Jabbour“50 个网空问题”，第 11 页。

31. Mike McConnell,“Cyber Insecurities: The 21st Century Threatscape”[网空的不安全：二十一世纪威胁景观], 收录于 America's Cyber Future: Security and Prosperity in the Information Age [美国的网空前景：信息时代的安全与繁荣], vol. 2, ed. Kristin M. Lord and Travis Sharp (Washington, DC: Center for a New American Security, June 2011), 25-39, http://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%20II_2.pdf.

32. Robin Geiβ,“The Conduct of Hostilities in and via Cyberspace”[网空中的敌对行为], Proceedings of the Annual Meeting, (American Society of International Law) 104 (24-27 March 2010): 371; 另参看注释 21 中 Crowell“信息时代的战争”，第 21 页。

33. 严格地讲，即使世界大战的情况也不是如此，因为盟军指挥官不必担心轴心国有可能从瑞士或斯威士兰突袭。

34. 见注释 32 中 Geiβ“敌对行为”，第 371 页；另见注释 17 中 Cahanin“网空的战争原则”，第 5 页。

35. Susan Freiwald,“Electronic Surveillance at the Virtual Border”[虚拟边界的电子监视], Mississippi Law Journal, 78, no. 2 (Winter 2008): 329, http://www.olemiss.edu/depts/ncjrl/pdf/ljournal09Freiwald.pdf; 另见注释 32 中 Geiβ“敌对行为”，第 371 页；另见注释 17 中 Cahanin“网空的战争原则”，第 5 页。

36. 见注释 20 中 Brookings Institution“网空的威慑”，第 15 页；另见注释 29 中 Crowell“信息时代的战争”，第 21 页。

37. 例如：网空“基地”、网空“空域”或网空“兵力结构”。

38. 见注释 31 中 McConnell“网空的不安全”,第 61 页;另参看 Gregory C. Radabaugh,“The Evolving Cyberspace Threat”[进化中的网空威胁], (working paper, Air Force Intelligence, Surveillance, and Reconnaissance Agency, August 2012), 8; 另见注释 25 中 Cornish et al“论网空战”，第 30 页；另见注释 29 中 Crowell“信息时代的战争”，第 21 页。

39. 见注释 9 中 Intelligence and National Security Alliance“网空情报”，第 7 页。关于类似的评估，另参看 Kevin Coleman and John Reed,“Cyber Intelligence”[网空情报], DefenseTech.org, 3 January 2011, http://defensetech.org/2011/01/03/cyber-intelligence/.

40. 见注释 17 中 Cahanin“网空的战争原则”，第 5 页。

41. House, House Armed Services Subcommittee, Cyberspace Operations Testimony [Keith Alexander 上将在众议院武装部队小组委员会上就网空作战作证], Sept. 23, 2010, [1], 111th Cong., 2nd sess., http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/House%20Armed%20Services%20Subcommittee%20Cyberspace%20Operations%20Testimony%2020100923.pdf. 当时的众议院武装部队委员会主席 Ike Skelton 议员在开幕致词中如此说。

42. Kenneth Geers, Sun Tzu and Cyber War [孙子与网络战], (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 9 February 2011), [4], http://www.ccdcoe.org/articles/2011/Geers_SunTzuandCyberWar.pdf. 关于溯源之挑战的更透彻的讨论，参看 Martin C. Libicki, Cyberdeterrence and Cyberwar [网空威慑和网空战争], (Santa Monica, CA: RAND Corporation, 2009), http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

43. 见注释 14 中 Air Force Space Command“网空作战的功能概念”，第 10 页。

44. Rand Waltzman,“Anomaly Detection at Multiple Scales”[多规模异态检测], (presentation, DARPA Cyber Colloquium, Arlington, VA, 7 November 2011), slides 3-4.

45.“洋葱路由”指的是一项技术，最初由海军发明，目的是在网上传送邮包过程中隐蔽其出处和内容。邮包的传送是通过一个随机挑选的代理服务器网，同时依次经过不同级别的加密和随后的解密，然后作为普通文本被送达目的地。W. Earl Boebert,“A Survey of Challenges in Attribution”[对溯源挑战的调查], 收录于 National Research Council of the National Academies, Proceedings of a Workshop Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy [“慑阻网空攻击：为美国国家战略和政策建言”研讨会论文集], (Washington, DC: National Academies Press, 2010), 43-46.

46. 见注释 3 中 Jabbour“50 个网空问题”，第 9 页。

47. 第 659 情监侦大队指挥官 Daniel Simpson 上校 2012 年 8 月 8 日与笔者交谈。第 659 大队是美国空军主要的网空情监侦部队，承担“数字网络利用分析和数字网空情报工作”。参看 Capt Karoline Scott,“New 情监侦 Group Supports Cyber Operations”[新建情监侦大队支援网空作战], Air Force News Service, 10 September 2010, http://www.af.mil/news/story.asp?id=123221324; 另参看注释 9 中 AFDD 3-12《网空作战》，第 24 页。

48. Kristin Quinn, Vago Muradian, and Marcus Weisgerber,“The Pentagon's New Cyber Strategy”[五角大楼的新网空战略], DefenseNews, 18 August 2011, http://www.defensenews.com/apps/pbcs.dll/article?AID=2011108180316.

49. 见注释 42 中 Libicki“网空威慑和网空战争”，第 96 页。

50. 见注释 2 中 Wasserbly“制定方针”，第 60 页。

51. Decian McCullagh,“House Passes CISPA Internet Surveillance Bill”[众议院通过 CISPA 因特网监视议案], ZDNet, 27 April 2012, http://www.zdnet.com/news/house-passes-cispa-internet-surveillance-bill/6360341. 民主党国会议员 Jared Polis 表示反对,声称 CISPA(计算机情报共享和保护法案)将“以网络安全的名义,放弃执行有史以来制定的每一条隐私法……允许军队和国家安全局违背我们建国所依据的每一条原则，在美国的土地上暗中监视美国人。”另参看 Sanjay Goel,“Cyberwarfare: Connecting the Dots in Cyber Intelligence”[网络战：连接网空情报中的各分散点], Communications of the ACM , 54, no. 8 (August 2011): 137; 另参看 Mike McConnell,“Mike McConnell on How to Win the Cyber-War We're Losing”[如何打赢我们正在输掉的网空战], Washington Post, 28 February 2010, B01, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html. 除了像“美国公民自由同盟”这种普通维权组织外，拥护隐私权组织还包括“电子边疆基金会”（它在网站 https://ssd/eff/org 中提供正当防卫监视的辅导课程）、savetheinternet.com（主要鼓吹“因特网自由”）、电子隐私信息中心、民主与技术中心、技术解放阵线、OpenNet（该组织在网站 http://opennet.net/about-oni 宣称“我们的使命是调查、揭露和分析因特网过滤和监视做法”）。根据笔者的意见和经验，自从 1976 年的教会委员会报告以来，没有哪一类情报界的活动在美国招致了如此热切的关注和强烈的公众反弹。

52. 要深入了解最近关于网空隐私、搜查和查封及其他宪法规范的法律辩论，可参看 Susan W. Brenner,“Fourth Amendment Future: Remote Computer Searches and the Use of Virtual Force”[第四修正案的未来：远程计算机搜索和虚拟部队的使用], Mississippi Law Journal, 81, no. 5 (2012): 1229-62; 另参看 Timothy Casey,“Electronic Surveillance and

the Right to Be Secure”[电子监视和安全保障权], University of California-Davis Law Review, 41, no. 3 (February 2008): 977-1033; 另参看 Elizabeth Gillingham Daly,“Beyond 'Persons, Houses, Papers, and Effects': Rewriting the Fourth Amendment for National Security Surveillance”[超越“人身、住宅、文件和财产”：重写为国家安全监视第四修正案], Lewis & Clark Law Review, 10, no. 3 (Fall 2006): 641-71; 另参看 Dan Fenske,“All Enemies, Foreign and Domestic: Erasing the Distinction between Foreign and Domestic Intelligence Gathering under the Fourth Amendment”[所有外国和本国的敌人：第四修正案消除外国和本国情报搜集的区别], Northwestern University Law Review, 102, no. 1 (2005): 343-81; 另参看注释 35 中 Freiwald,“Electronic Surveillance”[电子监视], 329-62; 另参看 John N. Greer,“Square Legal Pegs in Round Cyber Holes: The NSA, Lawfulness, and Protection of Privacy Rights and Civil Liberties in Cyberspace”[网空方枘难容法律圆凿：美国国家安全局、合法性、网空的隐私权及公民自由保护], Journal of National Security Law and Policy, 4, no. 1 (2010): 139-54; 另参看 Orin S. Kerr,“Applying the Fourth Amendment to the Internet: A General Approach”[把第四修正案用于因特网：通用做法], Stanford Law Review, 62, no. 4 (April 2010), 1005-49; 另参看 Mike McNerney,“Warshak: A Test Case for the Intersection of Law Enforcement and Cyber Security”[Warshak：执法和网络安全交会的一个验证案例], University of Illinois Journal of Law, Technology and Policy 2010, no. 2 (Fall 2010), 345-57; 另参看 Amanda Yellon,“The Fourth Amendment's New Frontier: Judicial Reasoning Applying the Fourth Amendment to Electronic Communications”[第四修正案的新边疆：把第四修正案用于电子通信的司法理念], Journal of Business & Technology Law, 4, no. 2 (2009): 411-37; 另参看 Mark D. Young,“Electronic Surveillance in an Era of Modern Technology and Evolving Threats to National Security”[现代技术时代的电子监视和对国家安全形成的威胁], Stanford Law & Policy Review, 22, no. 1 (2011), 11-39. 这些论著及所述案例提出了一些有代表性的问题，归纳如下：

- 是否可把计算机比作“容器”受《第四修正案》保护而免受“不合理搜查和查封”？
- 是否应将网上通信与封口信件同等对待受隐私权和宪法权利保护（内容与非内容对比）？
- 对具体个人网络通信（尤其是期望受到隐私保护的电子邮件和文本）的监视是否也要接受像对窃听一样的限制和制约？
- 网空情报专业人士如何保证遵守 12333 号行政命令《美国情报活动》,从而限制为抵御外国威胁的情报搜集（亦即如何知道受监视或搜集情报的对象是不是受宪法与行政保护的“美国人”）？
- 总的问题是，个人权利与政府责任如何平衡才能保障双方都不遭受国内外的威胁？

53. 见注释 52 中 McNerney“Warshak：执法和网络安全交会的一个验证案例”，第 346 页。

54. 见注释 14 中 Air Force Space Command“网空作战的功能概念”，第 15 页。

55. 见注释 42 中 Libicki“网空威慑和网空战争”，第 155-156 页。

56. 见注释 17 中 James 中将与笔者交谈。

57. RADM J. Michael McConnell 于 2012 年 8 月 23 日与笔者电话交谈。

58. 参看 William J. Lynn III,“Defending a New Domain: The Pentagon's Cyberstrategy”[捍卫一个新领域：五角大楼的网空战略], Foreign Affairs, 89, no. 5 (September-October 2010): 99.

59. Ned Moran,“A Cyber Early Warning Model”[一个网空早期预警模型], 收录于 Jeffrey Carr, Inside Cyber Warfare [网空战内幕], (Sebastopol, CA: O'Reilly Media, 2010), 200; 另参看注释 42 中 Geers“孙子和网络战”，第 10 页。

60. Gregory C. Radabaugh,“The Evolving Cyberspace Threat”[进化中的网空威胁], (working paper, Air Force Intelligence, Surveillance, and Reconnaissance Agency, August 2012), 9.

61. Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin,“Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains”[根据对敌方战役和入侵杀伤链的分析而开展的由情报驱动的计算机网络防御], (paper presented at the 6th International Conference on Information Warfare and Security, George Washington University, Washington, DC, 17-18 March 2011), 3, http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf; 另参看注释 59 中 Moran“网空早期预警模型”,第 208 页；另参看注释 60 中 Radabaugh“进化中的网络威胁”，第 9 页。

62. 见注释 61 中 Hutchins“由情报驱动的计算机网络防御”，第 3 页。

63. 见注释 57 中 McConnell 与笔者电话交谈。

64. Dr. Kamal Jabbour,“Cyber Vision and Cyber Force Development”[网空远景与网空部队发展], Strategic Studies Quarterly, (Spring 2010), 65, http://www.au.af.mil/au/ssq/2010/spring/spring10.pdf.

65. 难怪空军中有些网络战士戏称自己为“日本武士”。

66. Richard Stiennon, Surviving Cyberwar [打赢网络战], (Lanham, MD: Government Institutes, 2010), 121.

67. 一个拍字节（petabyte）等于 10 亿个吉字节（gigabyte）；一个尧字节（yottabyte）等于 10 亿个拍字节。

68. 见注释 3 中“2025 年网空远景”，第 40 页。

69. Damon Poeter,“DefCon: NSA Boss Asks Hackers to Join the Dark Side”[国防战备：美国国家安全局老板邀请黑客加入黑边行列], PC Magazine, 29 July 2012, http://www.pcmag.com/article2/0,2817,2407783,00.asp.

70. 见注释 9 中 Intelligence and National Security Alliance“网空情报”，第 14 页。另参看 Wayne Michael Hall and Gary Citrenbaum, Intelligence Collection: How to Plan and Execute Intelligence Collection in Complex Environments [情报搜集：如何在复杂环境中规划和执行情报搜集], (Santa Barbara, CA: Praeger, 2012).

71. 见注释 17 中 James 中将与笔者交谈。另参看注释 47 中 Simpson 与笔者交谈，Simpson 表示：“训练是另一个需要克服的挑战，”因为“目前缺少进行细致网络空分析的技术能力。”

72. 见注释 58 中 Lynn“捍卫一个新领域”，第 103 页。

73. 见注释 47 中 Simpson 与笔者交谈。

74. 比如，2010 年的一项调查发现，88% 的美国人相信他们在网上应该享有与物理领域里一样的合法隐私权保护；只有 4% 的人持不同意见。参看 US Department of Commerce, Comments of Digital Due Process, in the Matter of Information Privacy and Innovation in the Internet Economy [就因特网经济中信息隐私和创新的问题，对数码化合法诉讼程序的评论], docket no. 1004020174-0175-01 (Washington, DC: US Department of Commerce, National Telecommunications and Information Administration, 14 June 2010), 4, http://www.digitaldueprocess.org/files/NTIA_NOI_061410.pdf.

75. 见注释 58 中 Lynn“捍卫一个新领域”，第 99 页。

马修・M・赫尔利，美国空军上校（Col Matthew M. Hurley, USAF），美国空军军官学院毕业，华盛顿大学文科硕士，空军大学军事艺术科学硕士，俄亥俄州立大学博士，现任华盛顿特区五角大楼美国空军总部情监侦副参谋长办公室准则与政策整合主任，在此职位上他确保空军情监侦规则和最佳做法被适当纳入联盟、联合及空军作战准则与政策文件中。赫尔利上校是职业情报官，曾服务于支持空中机动司令部、驻韩美军、驻欧美国空军及中北欧联盟空军的岗位，包括派赴西南亚和非洲之角的应急部署。他曾获得 Ira C. Eaker 奖，并于 1989 年获空军历史基金会颁发的空军重大历史研究奖。他的最新著作《飞行中：以色列空中力量对阿克萨群众起义，2000-2005 年》，由阿拉巴马州马克斯韦尔空军基地的空军研究所于 2010 年出版。

震网——掀起网空战争军事革命

Stuxnet: Cyberwar Revolution in Military Affairs*

保罗·沙卡良，美国陆军少校（Maj Paulo Shakarian, U.S. Army）

2010 年 6 月 17 日，白俄罗斯一家小公司 VirusBlockAda 的安全研究人员发现一种能感染可移动存储设备的恶意软件。[1] 在后来几个月中，计算机安全界经过一阵忙碌，查明上述发现只是检测到一种新型计算机蠕虫的一个部分，这款新病毒名叫“Stuxnet”（震网）。[2] Stuxnet 专门针对工业设备。由于绝大多数的病毒感染发生在伊朗，[3] 同时伊朗的纳坦兹铀浓缩厂离心机因不明原因停机，[4] 此消息被披露后，大部分媒体揣测 Stuxnet 攻击的最终目标是伊朗的核设备。2010 年 11 月，伊朗总统艾哈迈迪内贾德公开承认，一种计算机病毒对“我国（核）离心机中为数不多的几台机制造了一些问题，”[5] 至此外界的一些怀疑得到证实。计算机安全界的一些知名专家把 Stuxnet 病毒称为“前所未有”、[6]“进化性的飞跃”[7] 和“我们希望永远都不再看到的那种威胁”。[8] 笔者认为，这种恶意软件代表了在虚拟领域的一场军事革命，[9] 即 Stuxnet 从根本上改变了网空战争的性质。对此，原因有四：(1) Stuxnet 是网空武器针对工业设备的首件案例；(2) 证据显示，这种病毒攻击目标设备获得成功；(3) 这代表在开发恶意软件方面的重大进步；(4) Stuxnet 案例表明，关于网空安全的一些常见的假设并非总是正确。笔者在本文中对此四点逐一讨论，并探讨 Stuxnet 引发的军事革命对未来的影响。

> Stuxnet = 震网（蠕虫病毒）
> SCADA = 监控和数据采集系统
> PLC = 可编程逻辑控制器

Stuxnet 锁定工业设备

一些主要的计算机安全公司详尽检查了 Stuxnet，[10] 一致认定这种病毒软件的主要目的是对工业设备造成难以察觉的故障。人们长期以来一直假设用网络方式攻击工业设施的可能性，而今这种新病毒首战告捷。再者，这款恶意软件的唯一目的就是开展攻击。其他所有的恶意软件都包含一些用于实施各种犯罪活动的标准代码——如盗窃身份和密码信息、发动拒绝服务攻击、发送垃圾电子邮件，等等。[11] 但 Stuxnet 不是，它虽然技术高度复杂，却无意从事以上任何一种犯罪活动。[12] 它的设计，就是通过自身复制和扩散来感染同工业设备通信的基于微软视窗系统的计算机。这与互联网上被用于各种犯罪目的的五花八门的恶意软件截然不同。Stuxnet 的设计目的是破坏，而不是犯罪。

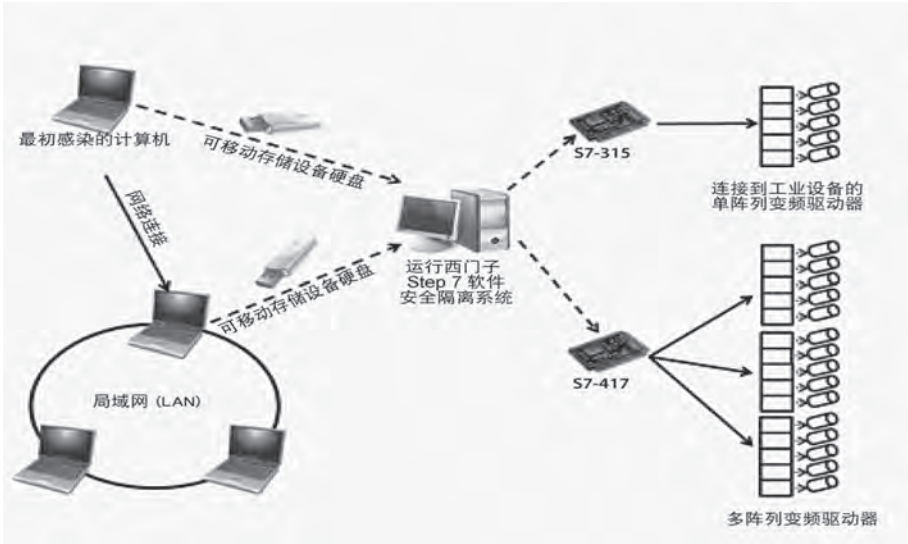
被 Stuxnet 感染的工业设备称为监控和数据采集系统（SCADA），此类系统用于对包括核电厂、石油 / 天然气管道、炼油厂、供水系统、或者其它需要计算机设备控制的关键基础设施进行实时的数据采集、控制和监控。[13] SCADA 通常使用称为可编程逻辑控制

* Translated and reprinted with permission from *Small Wars Journal*, April 2011 (smallwarsjournal.com).

器（PLC）的用来控制物理部件的计算机硬件。为了给 PLC 编程，系统管理员将 PLC 连接到标准的微软视窗计算机。PLC 在准备好使用时，通常从计算机拔下。例如，如果系统管理员希望加速运转离心机，他把 PLC 同视窗计算机相连，运行一个能与 PLC 通信的计算机软件，并上传新指令。假设 Stuxnet 感染了连接 PLC 的计算机，这种恶意软件就对该系统运行一种“拦截式”攻击。系统管理员试图向 PLC 发出指令，Stuxnet 拦截此指令，并以自己的指令取而代之发出，然后向视窗计算机发出假报告，谎称原指令已经上传。通过提供虚假报告，Stuxnet 隐蔽自身，使其很难被发现。

Stuxnet 被设计用来攻击由西门子 Step 7 软件控制的 PLC。[14] 并且，该病毒仅感染两种型号的 PLC：西门子 S7-315 和 S7-417。S7-315 是一般用途的控制器，运行单列阵的装置。例如，由 S7-315 控制的这种装置列阵和群组，运行一个制造过程的不同阶段。S7-417 是该系列中的顶级型号，能运行多列阵，因此比 S7-315 控制更多的设备。[15] 安全专家认定，Stuxnet 只在 PLC 同以一种非常特殊形式配置的设备相连时才会发动攻击。例如，当病毒发现 S7-315 时，如果 PLC 同 33 个或更多变频驱动器连接时，它才会发动攻击。变频驱动器用于控制某些设备的速度（如电动机的转速）。[16] 同样，对于 S7-417 的 PLC，它要发现 6 级联的 164 个变频驱动器，才发动攻击。[17] 该恶意软件还要在确认变频驱动器是由伊朗法拉罗巴耶利（Fararo Paya）公司或者芬兰伟肯（Vacon）公司制造时，才实施攻击。[18]

一旦 Stuxnet 确定已对被锁定的变频驱动器系统完成感染，就展开攻击。基于对该软件的分析，专家们发现，该病毒发现驱动器在 807—1210 Hz 之间运转后，定期修改此设定速度，使驱动器在 2—1410 Hz 之间不断变速。[19] 这样一来，由变频驱动器控制的装置就以意想不到的方式运转。但 Stuxnet 向操作人员发送的报告却伪称 PLC 程序正确，于是操作人员以为设备在正常范围运行。Stuxnet 修改这些设定运行值的事实说明了重要的一点——此病毒的目的就是要损坏工业



设备。如果 Stuxnet 只不过是个概念验证，或者只是想哗众取宠，或许就无必要修改运行频率。[20]

Stuxnet 极可能首战告捷

Stuxnet 以攻击工业设备为设计目的，有证据显示其攻击取得成功。成功的证据来自以下几种推理。首先，病毒的初期感染似乎发生在伊朗；第二，Stuxnet 代码的数据结构类似伊朗纳坦兹铀浓缩厂离心机的配置；第三，伊朗政府官员承认他们的离心机运行受到 Stuxnet 的感染。

伊朗似乎是这次攻击的中心，这从病毒感染的数量以及对病毒采样的分析可以看出。截至 2010 年 9 月 29 日，网络安全公司赛门铁克（Symantec）追踪了 10 万台被感染的计算机，其中大约 60000 台位于伊朗。印度尼西亚其次，有大约 15000 台感染。[21] 赛门铁克与其他安全公司合作，收集了 3280 份 Stuxnet 软件及其变种的独特样本。[22] 这些样本代表总共 12000 个感染案例。Stuxnet 有一个它以前曾感染的系统名单。因此，对于一个特定的样本来说，研究人员能确定该病毒为了进入某个计算机的传播路径。通过评估这些样本，赛门铁克能将感染历史记录追溯到 5 个不同机构的其中一个——所有机构在伊朗都有存在。[23]

从对伊朗纳坦兹铀浓缩厂的了解可知，其离心机配置和 Stuxnet 代码之间有惊人的类似。根据国际原子能机构，纳坦兹铀浓缩工厂的 IR-1 离心机系统是由 164 台离心机组成的级联系统。[24] 这与 Stuxnet 寻找攻击的 S7-417 控制器配置完全吻合。另外一个可能的指标是 IR-1 离心机的最大速度为 1,400—1,432 Hz，[25] 该频率范围非常接近 Stuxnet 在攻击时设定的最大速度：1,410 Hz。[26] 将 IR-1 离心机调到如此高的频率运行很可能导致设备损坏。

如果铀浓缩的过程被分解为一系列的阶段进行，每个阶段有多个离心机同时运行，那么浓缩过程就能获得优化。[27] 从 2006 年的一次采访得知，伊朗人正在使用这个分阶段方法，即采用 15 个阶段来进行铀浓缩。[28] 每个阶段配备规定数量的离心机，以获取最优化的生产结果。普林斯顿大学核未来研究室教授亚历山大·格雷泽（Alexander Glaser）研究了 164 台离心机级联规模的最优配置。专门从事 SCADA 监控系统研究的兰格通信技术有限公司创始人拉尔夫·兰格（Ralph Langer）将此分析同 Stuxnet 中的数据构造比较后发现，这种病毒可能严重干扰每个阶段的离心机最优配置，结果形成的配置似乎与格雷泽认定的最优配置正好相反。[29] 如果 Stuxnet 的攻击目标是纳坦兹的离心机，攻击的结果将导致浓缩铀产出达不到原定最优水平，亦即产量大大低于设计能力。

除上述技术分析外，伊朗领导人的声明中还透露出一些 Stuxnet 潜在效果的证据。艾哈迈迪内贾德总统在 2010 年 11 月证实恶意软件感染了他们的离心机，虽然他并没有明确提及 Stuxnet 的存在。[30] 伊朗最高国家安全委员会秘书长赛义德·贾利利在接受德国《明镜》周刊采访时，被特别问到 Stuxnet 被用于攻击纳坦兹的问题。虽然贾利利没有详细谈论该病毒造成的损害（再次淡化该病毒的作用），他的确承认发生了一次事件。他说："我们的专家很久前就已经阻止了这个攻击。"[31]

人们有兴趣地注意到，Stuxnet 很可能是由一名破坏者使用一个 U 盘将此病毒植入纳

坦兹的系统中。[32] 通过这种做法，病毒的设计者可极大地增加成功的几率，而不是被动地等待该病毒传播到纳坦兹。2010 年 10 月，伊朗情报部长海达尔·穆斯利赫宣布，人数不详的“核间谍”因涉嫌 Stuxnet 被捕。[33] 虽然被捕的细节和性质未知，但这（至少）说明伊朗承认 Stuxnet 可能传播的各种方式，以及给其设备运行带来的严重后果。

值得注意的是，在 2009 年末或 2010 年初，伊朗废弃并替换了纳坦兹铀浓缩厂大约 1000 台 IR-1 离心机（6 个级联，每个级联 164 台离心机）。[34] 废弃这些离心机的时机，以及替换离心机的数量，同 Stuxnet 攻击的时机和数据结构一致。对离心机故障的另外一个可能解释是设备制造缺陷，但还不清楚为什么这样的缺陷需要如此长时间才表现出来。[35] 从此前分析来看，Stuxnet 似乎并非设法立即损毁离心机，而是在一段时间内以一种更微妙的方式调整频率，这很难确定出现的问题是由病毒，还是由浓缩过程中一些其他因素造成的。恶意软件的这种行为，使废弃这些离心机的解释更加一致。除了导致将 IR-1 撤离生产线以外，纳坦兹铀浓缩厂还在 2009-2010 年期间经历了铀生产达不到最优水平的事件。国际原子能机构的报告显示，纳坦兹生产的浓缩铀数量那个时期仍保持相对稳定，尽管离心机的数量大幅度增加。[36] 这表明，整个系统在以低于最优水平生产。

虽然伊朗在 2010 年底宣称，Stuxnet 对他们核项目产生的影响微乎其微，安全专家兰格断言，这种病毒致使伊朗的核计划倒退两年。[37] 这有两个层次的原因。第一，如前所述，Stuxnet 造成的损毁更微妙，但极可能产生了有效破坏。由此恶意软件造成的设备故障难以查明来源。第二，鉴于 Stuxnet 的活跃扩散性质，要清除铀浓缩过程中全部计算机设备的病毒，极为困难。可能正是出于这些忧虑，伊朗在 2010 年 10 月（因不明原因）全面暂停了纳坦兹的浓缩铀运转。[38]

人们自然会提问：“Stuxnet 还影响了其他哪些国家？”有报道说，德国、芬兰和中国的监控设备中也发现了这种病毒，[39, 40, 41] 不过这些国家的工业系统没有因受感染而损坏。这可能是由于各自国家的 PLC 具备不同的配置，因为 Stuxnet 仅对某种特定配置发动攻击。西门子宣称，使用其软件的用户中，只有 15 个系统报告病毒感染。在这 15 个系统中，没有发生一起损害。[42] 伊朗极可能没有向西门子报告感染情况。伊朗虽然是在 2002-2003 年间购置了 S7-315 和 S7-417 控制卡，国际原子能机构认定伊朗极可能将这些硬件设备转移到其核项目，这促使西门子停止了向伊朗的销售。[43] 但是众所周知，S7-417 被安装在布什尔核电站，布什尔也可能是 Stuxnet 攻击的一个目标。[44] 在布什尔的 S7-417 并非直接从西门子获得，而是购自俄罗斯一家名为 Power Machines Corp 的电力设备公司，该公司根据与伊朗的合同，以此作为伊朗 Teleperm 系统的一部分进行了安装。

Stuxnet 是恶意软件的重大发展

像其它恶意软件一样，Stuxnet 利用了此前系统软件中未确认的安全缺陷:零日漏洞。由于这种漏洞此前未被发觉，因而未被杀毒软件识别。作为读者参考，在 2009 年底出现的对谷歌攻击的 Arora 病毒（通常被认为来自中国），[45] 就是利用一个零日漏洞。能利用两个零日漏洞的病毒已经闻所未闻，[46] 而 Stuxnet 竟然利用了微软视窗操作系统的四个零日漏洞,外加西门子软件的一个零日漏洞。在被 Stuxnet 利用的视窗系统的四个零日漏洞中，有两个漏洞与提升权限功能相关，从

而允许 Stuxnet 非法生根，或以管理员层级身份访问被感染系统。另两个漏洞与病毒传播相关，通过可移动存储设备或局域网传播病毒。写作本文之际，自我传播的计算机病毒尚不多见，因为控制起来通常很困难。以“僵尸网络”为例，一大批计算机被恶意病毒感染，又被一个与被感染计算机没有合法关联的“控制和指挥”服务器控制。[47] 这是一种从事网络犯罪的很常见的平台。僵尸网络病毒的传播，主要是通过垃圾邮件和恶意网站进行，自我传播的方式非常有限。[48]

Stuxnet 成功推翻一些安全假设

本文讨论的 Stuxnet 所引发的军事革命的最后一个方面是，它证明一些安全假设是站不住脚的。常见的第一个假设是，物理隔离的系统更安全。按照定义，SCADA 系统控制对使命具有关键意义的设备，很多管理人员不把这些计算机同外部网络相连，以物理隔离的方式来保证安全，结果是采用可移动媒介把文件传至计算机。Stuxnet 的设计者利用了这一假设，使病毒通过 U 盘等可移动存储设备来传播。一旦 U 盘被感染，病毒软件本身就在后来使用被感染驱动器的计算机上运行；使用者只要在视窗上点击相关图形，便开始被感染。这是 Stuxnet 利用其中一个零日漏洞的直接应用。

被 Stuxnet 证明是错误的另外一个关键安全假设，是数字签名证书设立的信任关系。为了提供更大的稳定性，当代操作系统，包括微软视窗，限制计算机的程序访问系统部件。一个正常的程序要求系统经由驱动软件呼叫硬件。鉴于这种情况，驱动软件比其他程序具更高权限访问低层级系统部件。为了避免轻易产生恶意驱动软件，微软视窗依赖数字签名证书识别。Stuxnet 为了防止被杀毒软件发现，使用了合法的数字签名证书。这是此前没有发现的 Stuxnet 的另外一个方面。早期的 Stuxnet 版本使用瑞昱（Realtek）半导体系统公司提供的证书，后来的版本使用智微（JMicron）科技公司的证书。使用这些证书使病毒在微软视窗面前呈现合法软件的假象。ESET 的安全专家注意到，两家公司都在台湾地区，因此怀疑这些证书系被盗窃。此外，他们相信，这极可能是实物盗窃（甚至可能是内贼所为），因为在互联网的黑市上驱动软件的数字证书并不常见。[49]

Stuxnet 对未来的影响

Stuxnet 具有很大的意义——这是一种新一代恶意软件，攻破了现有安全假设中的缺陷，能对互联网外的工业系统造成损害。作为比较，让我们看看另外两个攻击事件。第一，俄罗斯 2008 年对格鲁吉亚的网空攻击，主要使用了僵尸网络病毒和发动激进黑客，针对格鲁吉亚互联网的基础设施发动拒绝服务攻击。[50] 这些攻击主要是在俄罗斯发动常规军事行动期间，导致格鲁吉亚暂时丧失互联网的连接。虽然这种攻击方式当时在安全界众所周知，由于其规模，以及与常规军事行动同时发生，仍然具有重要意义。但是，对格鲁吉亚的这些攻击是针对计算机的基础设施——而不是 SCADA。在很多方面，那些攻击属于典型的计算机网络攻击（computer network attack - CNA），目的是降低计算机网络的效能。

在更近发生的称为 Arora（奥罗拉）的网空行动中，中国的黑客在 2009 年 12 月设法进入谷歌的公司网络，窃取了电子邮件帐户，甚至可能计算机源代码等信息。Arora 利用了微软 IE 浏览器的零日漏洞——利用个人用户每天使用的通用应用软件。[51] 这种特别

的网空攻击属于典型的计算机网络利用（computer network exploitation - CNE），黑客的目的是从攻击目标中窃取信息。

Stuxnet 在几个方面与这两个案例不同。对格鲁吉亚和谷歌的这两次攻击，是针对直接或间接与互联网相连的计算机网络。在其中任一攻击中，与网络没有连接的系统将不会受到损害。但是 Stuxnet 则不然，这种先进的病毒具有弥合“气隙”的能力。负责隔离系统安全的网络管理人员面对一种有趣的窘境：为了确保其系统能抵御最新的恶意软件，他们必须定期进行更新；但是这样做，又冒着传播感染的风险，例如用 U 盘或通过局域网进行更新，而 Stuxnet 能通过此二者传播。

另外一个关键不同是，在 Arora 和格鲁吉亚网空攻击行动中的目标都是其他的计算机。而 Stuxnet 对信息系统造成的损害则微乎其微，它的目的是破坏实物世界的一件设备。伊朗人的承认告诉我们，Stuxnet 成功地影响了一个非虚拟实体。这是武器研制的一项重大进展——在计算机打开后才存在的一个软件能成功地对真实世界造成破坏。Stuxnet 清楚地展示，网空武器在军事行动中能发挥重要作用，而先前的观点是，这种软件充其量仅能构成“大规模烦恼武器”。[52]

能对真实世界设备造成影响的恶意软件意味着什么呢？有很多问题亟待回答。参议院在 Stuxnet 发生后举行的听证会上，探讨了美国如何能更好地保护其关键的基础设施免遭类似的攻击。[53] 但是，这只是谜团的一部分，还有很多政策问题——其中有些在整体意义上和网空战争相关——现在显得越发重要。[54] 我们如何判定这类攻击的来源？我们如何应对政府外团体对 SCADA 基础设施的网络攻击？陆地战争法则如何适用于对真实世界造成损害的网空武器？

还有一些作战层次和技术层次问题也必须获得回答。在网空战争领域，对技术的和作战问题的思考常常交织在一起。例如，我们如何能更好地辨识零日漏洞（零日漏洞在定义上就是未知的漏洞）？我们如何找到诸如 Stuxnet 等蓄意不被发觉的恶意软件？我们所做的安全假设中还有哪些可能被推翻？我们如何模拟一个未知的网空威胁？

诸如 Stuxnet 的网空武器将会扩散吗？一些安全专家预计，像 Stuxnet 一样的变异病毒在 2011 年会更加普遍。[55] 已有报道说，中国的工业设备受到了非 Stuxnet 的网络攻击。[56] 值得注意的是，赛门铁克、卡巴斯基实验室、ESET 和兰格通信公司提供的免费分析，既可用于病毒防御，也能启发人们从中获得制造 Stuxnet 之类病毒的灵感。

网空战争具有快速变化的性质。政府、企业、学术界和黑客界都有充满激情的个人和团队坚持关注和分析各自系统中的最新漏洞。但是，Stuxnet 无论是作为一款先进软件，还是以其取得的成果，都代表了一种明显的飞跃。它揭示出我们的安全假设靠不住，需要进行多层次的重新审视；但最重要的或许是，它展示了软件也能用成为决定性的武器系统。♣

注释:

1. Kupreev Oleg and Ulasen Sergey, Trojan-Spy.0485 and Malware-Cryptor.Win32.Inject.gen.2 Review [特洛伊木马间谍 0485 和 Malware-Cryptor.Win32.Inject.gen.2 病毒], VirusBlockAda, July 2010.

2. “蠕虫”是定义为自我传播的一种恶性病毒软件。

3. Nicolas Falliere, Liam O Murchu, and Eric Chien, W32.Stuxnet Dossier Version 1.4 [W32.Stuxnet 档案版 1.4], Symantec Corporation, February 2011, 7.

4. David Albright, Paul Brannan, and Christina Walrond, Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? [Stuxnet 病毒是否损毁了纳坦兹铀浓缩工厂的 1000 台离心机 ?], Institute for Science and International Security (ISIS), December, 1.

5. Thomas Erdbrink, “Ahmadinejad: Iran's nuclear program hit by sabotage”[艾哈迈迪内贾德承认伊朗核项目受到破坏], Washington Post, 29 November, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/11/29/AR2010112903468.html.

6. Quote from Roel Schouwenberg, Senior Anti-Virus Researcher at Kaspersky Labs in an interview at the Virus Buletin conference [卡巴斯基实验室资深抗病毒研究员 Roel Schouwenberg 在病毒公告会议上的访谈], October 2010, http://www.youtube.com/watch?v=C9H3MrtLgUc.

7. Martin Brunner, Hans Hofinger, Christoph Krauss, Christopher Roblee, Peter Schoo, and Sascha Todt, Infiltrating Critical Infrastructures with Next-Generation Attacks W32.Stuxnet as a Showcase Threat [用新一代攻击型 W32.Stuxnet 渗透关键基础设施展现网络威胁], Fraunhofer SIT, December, 2010, 23.

8. 见注释 3，第 55 页。

9. Williamson Murray, Thinking about Revolutions in Military Affairs [思考军事革命], Joint Forces Quarterly, Summer 1997.

10. 这些包括赛门铁克、卡巴斯基实验室、ESET 和兰格通信公司。

11. Paul Barford and Vinod Yegneswaran, “An Inside Look at Botnets”[剖析僵尸病毒], in Malware Detection, ed. Mihai Christodorescu, Somesh Jha, Douglas Maughan, Dawn Song, and Cliff Wang, Springer, 2007.

12. Aleksandr Matrosov, Eugene Rodionov, David Harley, and Juraj Malcho, Stuxnet Under the Microscope [显微镜下的 Stuxnet 病毒], Revision 1.2, ESET, November, 2010, 5.

13. John D. Fernandez and Andres E. Fernandez ,“SCADA systems: vulnerabilities and remediation”[SCADA 系统：漏洞和补救], Journal of Computing Sciences in Colleges, Vol. 20, No. 4, April 2005, 160-168.

14. Thomas Brandstetter, “Stuxnet Malware”[Stuxnet 恶性软件], CIP Seminar, Siemens, November, 2010.

15. Ralph Langer, “How to Hijack a Controller - Why Stuxnet Isn't Just About Siemens PLCs [怎样劫持控制器——为什么 Stuxnet 不仅事关西门子的 PLC], Control Magazine, 13 January, 2011, http://www.controlglobal.com/articles/2011/IndustrialControllers1101.html.

16. 见注释 3，第 39 页。

17. Ralph Langer, “417 Data Structures = Cascade Structure = Reported Damage”[417 数据结构 = 级联结构 = 已报告受损], Langer Communications GmbH Blog, 29 December 2010, http://www.langner.com/en/2010/12/29/417-data-structures-cascade-structure-reported-damage/.

18. 见注释 3，第 39 页。

19. 见注释 3，第 41 页。

20. 见注释 15。

21. 见注释 3，第 5 页。

22. Stuxnet 的设计者分三阶段发动攻击，每个阶段使用该软件的更新版。有关技术详情参看注释 3 中 Falliere 文。

23. 见注释 3，第 7 页。

24. 见注释 4，第 2 页。

25. 见注释 4，第 4 页。

26. 见注释 3，第 41 页。

27. Alexander Glaser, “Characteristics of the Gas Centrifuge for Uranium Enrichment and Their Relevance for Nuclear Weapon Proliferation (corrected)”[铀浓缩气离心机的特征及其对核武器扩散的关联（更正版）], Science and Global Security, June, 2008, 14.

28. 同上。

29. Ralph Langer, “Applying Aqazadeh's revelations to Stuxnet forensic analysis”[运用阿加扎德启示对 Stuxnet 进行取证分析], Langer Communications GmbH Blog, 30 January 2011, http://www.langner.com/en/2011/01/30/applying-aqazadeh%E2%80%99s-revelations-to-stuxnet-forensic-analysis/.

30. 见注释 5。

31. Dieter Bednarz and Erich Follath, “Iran's Chief Nuclear Negotiator: 'We Have to Be Constantly on Guard”[伊朗首席核谈判代表：我们必须始终警惕], Spiegel Online, 18 January, 2011, http://www.spiegel.de/international/world/0,1518,739945-2,00.html.

32. 见注释 3，第 3 页。

33. John Leyden, “Iran boasts of Stuxnet 'nuclear spies' arrests”[伊朗炫耀抓获 Stuxnet 病毒“核间谍”], The Register, 4 October, 2010, http://www.theregister.co.uk/2010/10/04/stuxnet_conspiracy_theories/.

34. 见注释 4，第 2 页。

35. 见注释 4，第 3 页。

36. 见注释 4，第 9 页。

37. From an interview with Ralph Langer by Yaakov Katz in “Stuxnet Virus Set Back Iran's Nuclear Program by 2 Years”[Yaakov Katz 对 Ralph Langer 采访录：Stuxnet 病毒使伊朗核项目推迟两年], Jerusalem Post, 15 December 2010, http://www.studentnewsdaily.com/daily-news-article/stuxnet-virus-set-back-irans-nuclear-program-by-2-years/.

38. 见注释 4，第 6 页。

39. “Stuxnet also found at industrial plants in Germany”[德国工厂也发现 Stuxnet], The H Security, 17 September 2010, http://www.h-online.com/security/news/item/Stuxnet-also-found-at-industrial-plants-in-Germany-1081469.html.

40. “Stuxnet Spreads to Finland”[Stuxnet 蔓延到芬兰], The New Internet, October, 2010, http://www.thenewnewinternet.com/2010/10/14/stuxnet-spreads-to-scandinavia/.

41. John Leyden “Stuxnet worm slithers into China”[Stuxnet 蠕虫流入中国], The Register, 1 October, 2010, http://www.theregister.co.uk/2010/10/01/stuxnet_china_analysis/.

42. 见注释 14。

43. 见注释 4，第 5 页。

44. Ralph Langer, “417 Installed in Bushehr NPP”[417 安装在布什尔核电厂], Langer Communications GmbH Blog, 14 December 2010, http://www.langner.com/en/2010/12/14/417-installed-in-bushehr-npp/.

45. Timothy L. Thomas, “Google Confronts China's 'Three Warfares'”[谷歌面对中国的三个战争], Parameters, Summer 2010, 101.

46. 在病毒公告会议上对 Roel Schouwenberg 的采访。

47. 见注释 11，第 2 页。

48. 见注释 11，第 3 页。

49. 见注释 12，第 13 页；另参看 ESET 的相关技术博文 , http://blog.eset.com/2010/07/22/why-steal-digital-certificates.

50. 有关俄罗斯 2008 年对格鲁吉亚网空攻击的详情，参看 Stephen Korns and Joshua Eastenberg, “Georgia's Cyber Left Hook”[格鲁吉亚网空左勾拳], Parameters, Winter 2008-09, 60-76; 另参看 Paulo Shakarian 即将出版文 , “Analysis of the 2008 Russian Cyber-Campaign Against Georgia [2008 年俄罗斯对格鲁吉亚网空攻击分析], Military Review.

51. 见注释 12，第 5 页。

52. Noah Shachtman, “Terrorists on the Net? Who cares?”[网络恐怖主义 — 谁关心呀 ?], Wired, 20 December 2002, http://www.wired.com/techbiz/it/news/2002/12/56935.

53. 关于美国参议院就 Stuxnet 造成后果于 2010 年 11 月举行听证会的详情，请访问 http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_id=954c3149-042e-4028-ae23-754868902c44.

54. 对这些问题的详尽分析，参看 Jeffrey Carr, Inside Cyber Warfare [解密网空战].

55. 包括赛门铁克公司在内的数家计算机安全专业公司曾预测可能发生诸如 Stuxnet 这样的攻击（见信息实验室情报：2010 年度安全报告）。数位专家还在 专业网站做出类似的预测，例如 eWeek, http://www.eweek.com/c/a/Security/Stuxnet-Variants-Will-Wreak-Havoc-on-More-Information-Systems-in-2011-373179/); 以及 ComputerWeekly (http://www.computerweekly.com/Articles/2010/12/22/244626/StuxNet-prepare-for-worse-in-2011.htm).

56. Fahmida Rashid, "Stuxnet-Like Trojans Can Exploit Critical Flaw in Chinese Industrial Software" [类似 Stuxnet 的特洛伊木马能利用中国工业软件的致命漏洞], eWeek, 12 January 2011, http://www.eweek.com/c/a/Security/StuxnetLike-Trojans-Can-Exploit-Critical-Flaw-in-Chinese-Industrial-Software-296674/.

保罗·沙卡良博士，美国陆军少校（Maj Paulo Shakarian, U.S. Army），西点军校电气工程与计算机科学系助理教授。他持有西点军校专修信息保障的计算机科学理学士、马里兰大学计算机科学理科硕士、博士学位。他在多种学术和专业刊物就网空作战、计算机科学及人工智能等课题发表过多篇论文。

Cyberspace is "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."

——Joint Publication (JP) 1-02, Department of Defense Dictionary of Military and Associated Terms

网空是"信息环境内的一个全球性领域，由相互依存的信息技术基础设施网所组成，包括互联网、电信网、计算机系统、嵌入式处理器和控制器。"

——美国联合作战准则 JP 1-02《国防部军语词典》

关于网空战争的法律与伦理交会的一些思考

The Intersection of Law and Ethics in Cyberwar: Some Reflections

查尔斯·邓洛普，美国空军退役少将（Major General Charles J. Dunlap, Jr., USAF, Retired）

网空战争的幽灵在徘徊，成为公众严重关注的重大安全问题。奥巴马总统在最近发表的一篇专栏文章中提出警告："对我们国家的网空威胁是我们面临的最严峻的经济和国家安全挑战之一。"[1] 这种状况反过来又引发和网空作战行动相关的许多法律思考，包括对真实网空战争所适用规则的思考。[2]

随着对网空战争的法律思考升温，越来越多的问题涉及到伦理层面。伦理是任何军事行动的一个重要考虑因素，但与网空作战有关的伦理考量却是刚开始显现。[3] 鉴于人们对网空活动伦理层面的关注逐步加深，美国海军军官学院在 2012 年春季主办了一场专门探讨这一主题的学术会议。[4] 最近，《大西洋》杂志也刊登题为"有无可能发动正义的网空战争？"的文章，其中讨论了一些发人深省的议题。[5]

本文拟探讨几个问题，目的在于揭示法律和伦理在网空领域中如何交会。这样的交会不应令人特别惊奇，先前，历史学家杰弗里·贝斯特（Geoffrey Best）已经指出："切不可忘记，战争法无论起源于何处，其初衷主要关乎宗教和伦理……战争法始于伦理，并且始终把一只脚踏在伦理之上。"[6] 了解这层关系，对于充分理解二十一世纪网空战士的全部责任范围至关重要。

法律和伦理

法律和伦理如何相关？自不必说，遵守法律是伦理责任的底线，但也仅此而已：只是底线。在《武装部队杂志》2012 年 3 月刊中，美国海军中尉加布里埃尔·布雷德利（Gabriel Bradley）指出："武装冲突法确立了最起码的标准，"接着他令人信服地说，灌输个人和公认道德及伦理价值观——不妨称其为荣誉感——才是确保真正遵守法律的关键。他还非常贴切地引用了克里斯托弗·科克（Christopher Coker）的观点："法律可以肯定勇士风范，但不可取而代之。"[7]

当然，即使只想为二十一世纪的作战行动确定行为底线——亦即法律——并非易事，对网空作战而言，难度更大。究其众多原因，其中之一是，武装冲突法大多是针对以动能武器为主的冲突而制定的。尽管如此，笔者认为现行法律对网空作战仍具适用性。这也许可把我们带回到有关法律、伦理和网空作战交会的第一个问题。[8] 具体而言，我们有时听到这样的观点：网空是一个全新的领域，因而现行法律不能够——甚至不应该——适用于网空作战。

这个观点根本不对。武装冲突法的大部分内容并不针对任何特定领域。顺此思路，我们来看一看哈佛大学最近做的一个"哈佛人道政策和冲突研究计划"项目，其目标是就空中和导弹战争所适用的国际法编写一本手册。[9] 他们最后确实写出了一本有用的手册，只是篇幅较单薄，因为他们发现，真正

只针对天空和太空领域的独特法律其实不多。对于网空领域，大致也是如此，包括伦理考量。[10]

此外，网空作战中所面对的某些问题貌似法律问题，实则是技术问题或政策难题，而非真正的法律问题。让我们以网空领域中什么构成“战争行为”这个被讨论得沸沸扬扬的问题为例。“战争行为”本身是政治词语而非法律用语，不过“使用武力”和“武装攻击”等词语确实有法律含义，可能引发对方强烈反应，故有机会和“交战理由”联系起来。[11]

实际上，网空领域的这些词语可以依据法律诠释，如果——前提是如果——技术手段能够提供充分的数据，譬如，能显示所谓的“攻击”造成实际伤害，并能提供充分的信息证明谁是实际攻击者。当然，在网空领域想取得能证明攻击来源的数据的确有很大的技术难度，而这类溯源性数据的缺乏无疑构成难以逾越的法律和伦理门槛，使被攻击方缺少作出强烈反应的正当理由。在网空中莫名其妙地遭人暗算，但法律——和伦理——却要求你必须找出指向暗算者的可靠证据，才能出手反击，这的确令人感到沮丧和荒唐。

现有技术难以确定攻击源，但这个难题不应该由律师或者伦理学家来解决，而应由技术人员来解决。[12] 因此，上述《大西洋》杂志文章的作者在评论有人使用 Stuxnet（震网病毒）这个网空武器攻击伊朗核开发设施事件时，有趣地指出：“无法找出‘震网’病毒的攻击源，引发了伦理方面的关注，因为它使得被暗算的伊朗无从反击，于是变本加厉向更极端的行为发展。”[13]

暂且不谈伊朗在受到所谓的“震网”病毒攻击之后是否必须有法律或道德依据才能反击，更有趣的是，《大西洋》杂志这篇文章的作者进一步提出：“为判定攻击源，国际间应签署协议。”文章作者认为，这些协议将规定“网空攻击中应含有攻击方的数字签名，”并且，可以使用某些网络协议“使溯源的过程更加容易。”[14]

大多数专家也许会说，现行法律并未要求推动对网空攻击的溯源，[15] 但是，《大西洋》杂志的那篇文章主张“加强［合作］改善国际网络监控，藉以追踪攻击来源，”而且作者似乎相信“经济刺激措施，例如贸易制裁威胁，可以促成这类协议。”[16] 人们可以不同意这些建议中的许多观点，但是文章的作者应受嘉许，因为他们至少启动了关于如何应对网空战争中一个最令人困扰的法律和道德问题的对话。

和网空攻击源难以判定一样，网空武器的打击目标选定也面临巨大的技术挑战——而不是单纯的法律问题。战争法中的“区分原则和相称原则”是基本的法律和伦理原则，要求决策者立足技术数据，知道使用某项特定打击技术之后，哪些人将受到影响以及影响程度如何。[17] 如上所述，这样的数据在技术上很难获取，但这不是法律或伦理问题，而是科学技术问题。实际上，我们可以说，网空作战领域最需要的能力之一是如何制作出具备可靠精确度的作战效应模型，从而向决策者——当然还有律师和伦理学家——提供至为关键的信息，便于他们对网空作战方式的运用作出明智的判断。

法律和伦理价值是否过分束缚了网空战士的行动?

在上文所讨论的关于法律和伦理如何应用到具体网空作战的论题之上，还有一个范

畴更宽广的论题：究竟是否需要有任何约束？具体而言，有些人认为，应用法律条文会约束美国的网空作战能力，从而给美国的安全带来风险。笔者和斯图瓦特·贝克（Stewart Baker）曾在美国律师协会主持的一场辩论中有过严肃的交锋，而争论的焦点就是刚才提及的那个令人颇感意外的问题。[18]

请允许我略微介绍一下那场辩论的背景。贝克先生是一位德高望重的律师，在著名的华盛顿世强律师事务所（Steptoe & Johnson）任职。他亦曾服务于政府部门，先后担任国家安全署总法律顾问和联邦国土安全部主管政策的助理部长。他在辩论开始时说："律师不能打赢战争。但是，律师可能会导致战争失败吗？我们可以找到答案，很快就能找到。政府各部门的律师对于网空战争提出了各种喧扰的法律问题，使我们的武装部队束手无策，无法开展网空作战，甚至无法规划网空作战。"[19]

贝克先生进一步声称，他认为试图"对网空战争施加限制"的任何做法都是"注定要失败的"。[20] 在他提出的许多令人不安的观点中，最具争议者其实和伦理相关。他提到第二次世界大战中空中作战造成了毁灭性伤害，并且引用前英国首相斯坦利·鲍德温在1930 年代的言论：在空战中"唯一的防御就是进攻，也就是说，如果你想要让自己人活下来，就必须比敌方更快速地杀害更多的妇女和儿童。"[21]

接着，贝克先生似乎表示赞同鲍德温先生关于"更快速地杀害更多的妇女和儿童"的观点，因为他声称，如果"我们要抵御网空战争的恐怖景象，首先需要面对这些恐怖景象，用鲍德温的坦率态度来面对。"[22] 贝克先生认为，只有在遵循这样的指导思想构建出网空战争战略之后，才有必要"请律师表达他们的想法"。[23]

本文限于篇幅，无法详细复述我当时的反驳（但是我的发言标题——"无法无天的网空战争？绝非制胜之道"——也许能说明我发言中的观点）。[24] 此处只要提及一点即可说明问题：至关重要的是，在网空战争（以及任何军事作战行动）中，只要有可能，不仅从法律或论理角度，而且从现实作战思考角度，都必须设定"限度"。就网空战争而言，要做到这一点并不特别难，尤其是，只要实际参战的网空战士不把法律和伦理要求看成是对他们为完成任务而认定需采取的行动的非对称阻碍。

尽管贝克先生认为法律纠缠使得我们的武装部队"束手无策，无法开展网空作战，甚至无法规划网空作战"，空军上将罗伯特·凯勒（Robert Kehler）似乎并不同意他的观点。凯勒将军是美国战略司令部司令，其属下的网空司令部是网空作战规划和行动的主力军。凯勒将军在 2011 年 11 月宣布，他"不相信我们需要新的明确的授权才能进行任何类型的进攻行动。"他并表示自己"不认为进行［网空］作战的授权有任何问题。"[25] 简言之，作战部队显然不认为法律和伦理约束与他们有效"规划网空战争"的能力有什么矛盾。

遵守法律在网空领域尤其重要，因为几乎所有的专家都同意，抵御网空威胁需要外国的合作，才能追踪网空威胁和摧毁其行动能力——在平时和战时都是如此。[26] 毫无疑问，在抵御网空威胁中起重要作用的国家，尤其是世界上主要的民主国家，不会和那些在网空或其他领域不设限度地开展军事行动的任何国家进行合作。迈克尔·利斯曼（Michael Riesman）教授和克里斯·安东尼欧（Chris T.

Antoniou）教授在其 1994 年的著作《战争的法律》中指出："在广受拥护的现代民主国家中，即使是一个有限的武装冲突，也需要有充分的民意支持基础。如果民众认为正在进行的战争是不公正的、不人道的或邪恶的，无论其政治目标如何站得住脚，他们的支持可能很快消退，甚至变成反对。"[27]

但是，摈弃贝克先生的网空战争观念并不表示我们对于网空战争的伦理和法律担忧可以消除。例如，最严重的担忧之一，是关于平民在网空作战中的作用。

网空中的平民战士

自不必说，民间中拥有大量的网空专业人才，而军方必须取用这些专业人才。但是，取用到什么程度，以及这种取用究竟意味着什么——或者说，应该意味着什么——正是法律和伦理必须关注的问题。

基本论点不难理解。若要享有作战人员的特权，也就是拥有——比方说——"行动许可证"，可参与合法毁损敌方人员或财产的行动而不必担心受到起诉，这些人员通常必须是某冲突交战方合法组建的武装部队的成员。[28] 人们经常把这个条件误读为平民不能直接参与对敌作战。实际上，平民可以参战而不一定被定为战争罪，但是会产生后果。

主要的后果是，如果这些平民落入敌方手中，可能会受到敌方国内有刑法依据的惩处，而武装部队成员参与同样的行动，却能借助作战人员的特权而免受起诉。此外，根据战争法，平民如直接参战，都可以成为动能打击或网络打击的目标。在网空范畴内，我们应该明白，甚至国际红十字会也明确地把人们通常视为网空战士常有的一些行为列举为直接参战的例子："用电子方式干扰军事计算机网络（计算机网络攻击）和传输用于某个特定攻击的战术目标情报。"[29]

从伦理角度看，这一切意味着什么？首先，平民必须要理解参战的潜在后果，尤其是当平民不在工作地点的时候，例如和家人一起在家里的时候。国际上对于在什么情况下平民可像武装部队成员一样成为打击目标仍在争论不休，但是国际红十字会同意：执行"连续作战功能"（不同于仅仅"以自发、断续或无组织方式参战"）的平民可以像武装部队成员一样成为打击目标。[30]

武装部队成员——以及经常执行计算机网络攻击等"连续作战功能"的平民——无论在何时何地被发现，都有可能受到敌方使用任何合法武器的打击，无论此时此刻该武装部队成员或平民是否构成迫近威胁或是否正执行某个军事功能。这意味着，例如，经常参与计算机网络攻击行动的某个网空平民战士可能会在华盛顿郊区的家里受到某个合法交战方（不是恐怖分子）的合法打击。而且这种打击不仅是使用网络武器；如果符合战争法的规定，可使用任何合法武器。因此，如果这位平民对于网空军事行动很重要，他在任何地方被发现，都有可能受到强大武力打击；只是，打击过程中可能发生的无辜平民(例如网空战士的家人)意外死亡或伤害"与预期的具体和直接的军事效益相比不应该过度"（在这里，"军事效益"当指消灭敌方网空战士或瘫痪其行动能力）。[31]

于是，与网空战士有关的伦理问题可能是：要求平民承受此类风险到什么程度算合适？武装部队成员自愿接受众所皆知的服兵役"无限责任合约"，让他们承受风险是一回事，而要求平民承受此等风险则是另一回事，更遑论让平民的家人去承受暴力冲突的附带

伤害和非动能打击造成的网空破坏。在网空战争中，“前线”也许远离人们所知道的传统战场。

没有人知道这种威胁具有多大的真实性。但是，在“潜伏特工”防不胜防的时代，在伪装特战部队遍布于许多国家的时代，对美国网空能力的这种攻击并非像有些人所想的那样是天方夜谭。讨论到此，我们看到这场关于网空作战可能带来个人风险的讨论，映射出网空战士需要勇敢承受某些批评者对他们的伦理观和专业道德的无情攻击，个中意味颇具讽刺。

对网空战士专业道德的挑战?

随着先进技术在战争中的应用日益增多，出现了许多令人极为困惑的批评，其中包括一些当代评论家固执地认为采用这些技术是“缺乏男子气”或“不足取”。无人机操作员的遭遇就是一例，他们像网空战士一样，也是在计算机操作台上进行作战。最近有一位大师发表了题为“美国正使用致命无人机打一场懦夫的战争”的文章，可谓这类胡言乱语的代表之作。[32] 尽管诸如此类的诽谤还没有落到网空战士的头上，但是他们的专业道德迟早也会遭遇同样的中伤，早晚而已。

这一切都是怎么开始的？根源可追溯到大卫·基尔卡伦博士（Dr. David Kilcullen）几年前讲的一些言论。基尔卡伦博士是澳大利亚陆军退役中校，现在已成为以地面作战为中心的人力密集型平叛作战理论的最积极创导者之一，他的观点已反映在 2006 年出版的美陆军野战手册 FM3-24/ 美海军陆战队作战出版物 3-33.5《平叛作战》中。[33] 需要指出的是，总体来讲，该手册对空中作战很不友好，300 页篇幅中只用了 5 页谈论空中作战，因此基尔卡伦博士对无人机的批评与其对空中力量的总体看法是一致的。

基尔卡伦博士于 2009 年在国会作证时声称，用无人机攻击恐怖分子是“结果适得其反”，他说道：“在普什图族的荣誉和复仇文化中，当面对打被视为勇敢，从 20,000 英尺高空用导弹打人算不得好汉。”基尔卡伦认为：“从空中使用机器人……乃懦夫所为。”[34] 显然，他的理论可以很容易地套用到网空作战和网空战士头上。

基尔卡伦的这些观点荒谬得简直令人目瞪口呆，正是此君所称的敌方，不仅躲在安全距离之外使用遥控引爆的简易爆炸装置来杀害美国军人，而且还利用儿童来放置这些爆炸物。[35] 按照他们自己的“荣誉文化”标准，难道这些作为不是“懦夫所为”吗？简言之，这整个讨论无论多么令人泄气和欠缺准确性，从实际作战角度来看，其实无足轻重。“战争的目的”，如巴顿将军形象地表述，“不是要你为国牺牲，而是要让对方为他的国家捐躯。”

躯体之勇，无论多么令人钦佩，不是在二十一世纪赢得战争所需的唯一素质，也许从来都不是。例如，美洲印第安人在打仗时可谓视死如归。然而历史学家安东尼·麦基尼斯（Anthony R. McGinnis）在 2012 年 4 月发行的《军事史杂志》中指出，美洲印第安人的个人英雄主义和风格化战争模式根本无法抗衡“以最终胜利为目标的”、“拥有现代先进技术的国家”。[36] 当然，只要这些先进技术的使用方式从法律和伦理角度来看是适当的，就无需指责“以最终胜利为目标的、拥有现代先进技术的国家”。

现实中，远距离作战并无悖伦逆道之说，也无非同寻常之处。有史以来，交战一方总

是试图剥夺对方拿起武器对抗的机会。例如，笔者曾在其他文章中说过：

> 大卫用一个投石器砸死了巨人哥利亚，后者连拿起武器还手的机会都没有；亚历山大大帝的士兵排列成方阵，用16英尺长矛长趋直入，使得挥舞12英尺长矛的对手无法招架；英格兰弓箭手用长弓密集攻击法国骑兵，在阿让库尔远距离歼灭了法国骑士团精锐；在近代史中，美国和英国坦克在1991年的“东73公里战役”（Battle of 73 Easting）中摧毁了萨达姆的主力装甲部队，主要是因为美英的火炮射程超过伊拉克T-72坦克。远距离杀伤不是什么新鲜事。[37]

尽管鄙视计算机化作战的观点是错误的和不公正的，有些人却总是放不下这种思维。例如，纽约大学法律教授菲利普·埃尔森（Phillip Altson）由联合国聘用为“特约撰稿人”，负责撰写一份关于定点打击的报告。他在此报告中还表达了自己对无人机作战的看法，认为由于无人机作战的控制“完全可以通过计算机屏幕和远程声频反馈来实施，因此存在以游戏机心态来看待杀人的风险。”[38]

以游戏机心态来看待杀人？这种侮辱性用词反映了专业道德缺失，而它竟然会出现在联合国官方报告中，确实令人不安。埃尔森教授提出这个结论所依据的主要证据似乎是他自己对于无人机操作员的心态的猜测，而他本人则从来没有参与过无人机作战任务。但是，实际证据显示的情况与埃尔森的指称大相径庭，这些证据表明，执行无人机操作的军官并未将这种作战责任视为玩电子游戏。布鲁金斯学会的彼得·辛格博士（Dr. Peter Singer）在其2010年的研究中说过，他发现“[有些无人机]作战部队的作战精神压力高于在阿富汗的某些作战部队。”报告得出结论说，无人机操作员经历着“远更明显的身心困顿和精疲力竭感。”[39] 这些心理疲劳是电子游戏玩家很少体验到的。

最近，美国《空军时报》引用了一名空军官员对“电子游戏”指控的直接反驳，他指出，无人机操作员的责任压力极大，无人机作战是“情绪非常、非常投入的过程，不能有丝毫懈怠，不是电子游戏。”[40] 对于这个问题的辩论方兴未艾，有些批评者已经迫不及待，肆意嘲笑那些认真履行国家重托的将士所展现的专业道德。[41] 显然，无人机作战同网空作战并不完全一样，尽管如此，网空战士也是在履行保卫国土的庄严使命，随时等待召唤，通过网空途径沉重打击敌人。网空打击手段可能不同于无人机作战，但是网空作战也要求高度的专业道德，网空战士所承受的心理压力同样很大。

无人机作战还有一个特点，也许可以同网空战士必须展现的伦理和专业道德相比。《滚石》杂志在2012年4月16日刊登了迈克尔·黑斯廷斯（Michael Hastings）写的一篇颇有争议的文章，文章声称：

> 通过无人机执行遥控任务……五角大楼和中央情报局现在不必向地面派出一兵一卒，就可以实施军事打击或暗杀，也不用担心阵亡美国士兵被装在殓尸袋中运回国内而引发的公众反弹。无人机的迫近性和隐秘性，使得国家领导人能够比以前更方便地发挥美国的军事力量——也使得这些秘密攻击的后果比以前更难评估。[42]

暂且不论黑斯廷斯的唬人语气，他提到“无人机的迫近性和隐秘性，使得国家领导人能够比以前更容易投放美国的军事力量”，这样说不无道理。笔者根据自身经验，相信高层决策者清楚地知道任何军事行动都可能会

有意外的后果——无论在行动策划阶段显得多么“无代价”。但是，他对于无人机的评论也许能适用于网空作战，可能要求网空战士具备高度的伦理素质，特别是包括坦诚和勇敢。

需要坦诚和全面的建言

网空作战的新颖性、其准确效应的不确定性及其执行难度，并非总是被网空作战决策链的所有参与者所完全理解，这种状况引起另一个伦理责任，即需要有人提供坦诚和全面的建议。在某种情况下，参与决策流程的人员也许不得不一反常态，提出某些尖锐的问题或指出某些尴尬的事实。如果美国要像黑斯廷斯所说的那样“发挥”网空力量，则必须像运用更传统的军事能力一样小心谨慎。需要强调的是，这可能要求超越习惯做法，以确保所有的相关因素——包括伦理和法律因素——都得到慎重考虑，从而做出最佳决策。

幸运的是（至少对于律师来讲），美国律师的伦理“圣经”《美国律师协会专业行为规范》明确地允许律师提供此类全面的建议。《规范》第 2.1 条规则要求律师“行使独立的专业判断和提供坦诚的建议”。 而且《规范》并未限制律师只能提供法律建议，因为该条规则又说：“律师提供建议时，不仅可以考虑法律因素，也可以考虑与当事人的情况有关的道德、经济、社会和政治等其他因素。”[43] 实际上，这样的指导原则不仅适用于律师，而且毫无疑问也适用于参与网空作战的所有的军方和民间专业人士，网空作战的成功取决于多种因素，因而所有人员都必须协力合作，确保所有相关因素得到适当的考虑。

该条规则提到坦诚。如上所述，这不是只是对律师的要求，而是所有的国防专业人员都必须具备的一个基本伦理品德。[44] 在评估网空中的潜在威胁时，必须保持坦诚的态度。如果不准确地描述威胁，或者甚至蓄意歪曲威胁，可能导致资源分配不当和其他判断错误。对威胁的规模和性质，可谓众说纷纭，在 PBS 电视台 Newshour 新闻频道于 2012 年春天播放的一个访谈节目中，信息研究学会的特里•本泽尔（Terry Benzel）说：“[网空界] 的每个人都在谈论所谓的‘网空珍珠港’事件，不是谈论是否发生，而是何时发生。”[45] 同样地，一位“著名的欧洲网空安全专家说，需要采取国际行动才能防止灾难性的网空战争和网空恐怖主义。”[46]

但是并非所有人都同意这个观点。据报道，美国网空司令部情报主任塞缪尔・考克斯海军少将（Rear Admiral Samuel Cox）曾在 2012 年 4 月“表示不必过分担忧美国的敌人的能力，认为敌人很难瘫痪美国电网或互联网，因为美国的这些系统具备抵御强大网空攻击的能力。”[47]《连线杂志》2012 年 2 月刊登的一篇文章使用了更加尖锐的措辞，两位研究专家杰瑞・布莱托（Jerry Brito）和泰特・瓦特金斯（Tate Watkins）在此文中批驳有关网空战争威胁的种种夸张说法：“诸如此类 [关于网空战争的] 的警告耸人听闻，却明显缺乏证据支持。”[48] 经济合作与发展组织在 2011 年发表的一份研究报告与布莱托和瓦特金斯的结论不谋而合，该报告的作者尽管认为各国政府“需要做好周详的准备，以抵御网空中各种意外的或蓄意的攻击事件并做好恢复”，但是又断言“很少有单一的网空事件能够导致全球性震荡。”[49] 分析家托马斯・里德（Thomas Rid）在《外交政策》杂

志上撰文说，网空战争“仍然是凭空臆测多于实际危险。”[50]

所有这些都令人不安，正如布莱托和瓦特金斯所言：“在许多方面，关于网空灾难的言论与我们在伊拉克战争前夕所看到的威胁渲染颇为相似。”他们进一步指出：“网空安全是一个规模庞大和蓬勃发展的产业”，并称“华盛顿充满了既得利益者，他们热衷于炒作和夸大对我们的数字网络安全的威胁。”这两位作者总算没有直截了当地指称某些人为了私利而散布网空战争恐怖论，但是明确号召“停止那些预言世界末日的蛊惑”，并坚持认为：“政策对话中充满着惶惶然不可终日的种种警报，也许让网空安全商有利可图，对真正的安全却并无助益。”[51]

我们的确需要对威胁的规模和迫近性展开辩论，但是所有人也许都会同意，在任何情况下，故意夸大（或淡化）威胁，即使是出于好心支持某个论点，也可能引致伦理和专业道德问题。诚如布莱托和瓦特金斯所说，审视 2003 年伊拉克战争爆发前夕的事态，可清楚地看到，错误判断威胁可能导致什么情况，这也许是他们把辩论命题称为“网空战争犹如新的核反应燃料黄饼”的原因。总之，坦诚——以及必要的言辞节制——是网空战士应具备的重要品质。奥巴马总统使用经过慎重斟酌的词语要求人们“认真”对待网空威胁并把网空防御规划列为一项“首要任务”，他的讲话体现了一种负责任的态度，既强调了危险，又避免了无益的和误导性的恐慌渲染。[52]

要求具备胜任能力

最后，网空战士的关键伦理责任还包括具备胜任能力。如上所述，《美国律师协会专业行为规范》提供了指导原则，所有的网空专业人士也许可以借鉴，用于对照他们自己的责任。《规范》第 1.1 条规则说，“具备胜任能力的代理要求代理人拥有实施代理而合理所需的法律知识、技能、透彻性和准备。”[53]对于关心网空战争的法律和伦理问题的人士而言，对胜任能力的伦理要求并不局限于对法律和 / 或伦理本身的知识及理解。

毋庸置疑，网空作战的许多方面极为复杂。因此，法律顾问——以及其他领域的顾问——必须尽量熟悉网空客户的“业务”，包括其中的技术层面知识。掌握有用的技术知识不仅可帮助这些顾问充分了解事实，适当应用法律和伦理原则，而且能够使顾问从一开始就获得求助者的至关重要的信任。像其他领域的求助者一样，网空领域的决策者会自然地向那些真正精通网络奥秘的专业顾问求教。

要做到精通当然不易，要想在这个异常复杂的领域保持对最新技术的了解，不仅费时而且没有穷尽。但是它非做不可且越早越好，一旦贻误时机将遗憾终身。丘吉尔曾经说过：“人生一世，都会撞着机遇，此时时刻，仿佛机遇拍肩，促动他义不容辞，机遇非他莫属，惟他有此才能。如果在这人生最幸运的时刻有机遇降临，他却毫无准备或者心余而力绌，那将情何以堪。”[54]

结语

本文试图通过几个例子说明法律和伦理的交会。然而一个问题可能接踵而来：在这诸项要素中，哪一项要素最能有效设立网空战争的限度并约束那些正直的然而现实的网空战士的行为？美利坚大学法律教授肯尼思·安德森（Kenneth Anderson）最近重温了

他过去撰写的一部探讨法律和荣誉在武装冲突中发挥“发动机”作用促使军人正确行事的著作。安德森教授认为：

> 但是我认为，那种以合法性作为发动机来促使军人遵守战争法、信奉合法性能约束一切的观点，是完全错位的看法；它是为律师，尤其是为美国律师特制的一个幻想。律师们相信对战争法的遵守是一个执法问题，而实际上这是一个忠诚问题。国际法汇编是有效的模板，能把战士的责任分类整理清楚。但是说到底，战士对国际人道法的尊重，不是基于其合法性，也不是基于对律师的崇拜，而是基于他们的专业军人荣誉感，这种文化思维指引着他们在战场上愿意做什么和不愿意做什么。[55]

“荣誉感”究竟是与伦理并存还是伦理的一个分支，这个问题固然可以在大学校园里热烈辩论。但是更重要的是，我们应该像安德森一样注意到，当代中可能最杰出的军事史家约翰·基根（John Keegan）曾经毫无保留地说过：“是荣誉感规范着战场行为，其作用无可取代，过去没有，今后亦无。”[56]

网空“战场”虽然不全然相似于基根所说的战场，但是他的观点无疑同样适用于网空战场。说到底，荣誉感及其隐含的伦理思维定势不可或缺。但是，讨论不能到此为止，因为仅仅培育能区分对与错的品质是不够的，还需要有坚持这种品质的勇气或者勇敢。

网空战士需要的勇敢，不一定是传统战场上战士必不可少的躯体之勇，更多的可能是道德之勇。[57] 随着网空领域开始制订作战行为规范，道德勇气这种品质更是必不可少。如何正确行事，尤其是在需要当机立断而无明确引导、只能凭借经典的法律和伦理依据时如何正确行事，挑战显而易见。

网空战士也许应该知道，另一位英国历史学家马克斯·黑斯廷斯（Max Hastings）在其经典的军事英雄主义研究中曾经说过：“[在军队中] 常见躯体之勇，而鲜见精神之勇。”他声称：“道德勇气很罕见。”[58] 但是，网空战士需要展现的正是这种罕见的勇气。法律可以提供框架，但是只有当荣誉感和道德勇气交会，我们才能真正地维护那些值得我们捍卫的伦理原则。♣

注释：

1. Barack Obama, Taking the Cyberattack Threat Seriously [认真对待网空攻击威胁], Wall Street Journal, Jul. 19, 2012, http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html.
2. 例如，美国海军战争学院国际法系于 2012 年 6 月举行了一场专门研讨网空战争法律问题的会议，http://www.usnwc.edu/ILDJune2012.
3. 例如，参看 Randall R. Dipert, The Ethics of Cyberwar [网空战争的伦理], Journal of Military Ethics 9, no. 4 (December 2010): 384, 385. 作者在第 385 页中说：“关于此类 [网空] 武器使用的符合伦理要求和明智的政策到底是什么，至今没有知情的、公开的、公众参与的或政治性的讨论。”
4. “McCain Conference: Warfare in a New Domain; The Ethics of Military Cyber Operations”[新领域的战争：网空军事行动的伦理], United States Naval Academy, Stockdale Center for Ethical Leadership, 26-27 April 2012, http://www.usna.edu/ethics/publications/mccain2012.php. 本文的大部分内容取自作者在该次会议上所做的演讲。
5. Patrick Lin, Fritz Allhoff, and Neil Rowe, Is it Possible to Wage a Just Cyberwar? [有无可能发动正义的网空战争?], Atlantic, 5 June 2012, http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/
6. Geoffrey Best, War and Law since 1945 [1945 年以来的法律和战争], (Oxford, UK: Oxford University Press, 1994), 289.

7. Lt Gabriel Bradley,“Honor, Not Law”[是荣誉感而不是法律], Armed Forces Journal 149, no. 7 (March 2012), http://www.armedforcesjournal.com/2012/03/9563756.

8. Harold Hongju Koh, legal advisor, Department of State,“International Law in Cyberspace”[网空领域的国际法], (remarks, USCYBERCOM Interagency Legal Conference, Fort Meade, MD, 18 September 2012), http://www.state.gov/s/l/releases/remarks/197924.htm.

9. Program on Humanitarian Policy and Conflict Research, Manual on International Law Applicable to Air and Missile Warfare [适用于空中和导弹战争的国际法手册], (Cambridge, MA: Program on Humanitarian Policy and Conflict Research, Harvard University, 2009), http://ihlresearch.org/amw/HPCR%20Manual.pdf.

10. 例如，参看 Roger Crisp,“Cyberwarfare: No New Ethics Needed”[网空战争：不需要新伦理], Practical Ethics (blog), 19 June 2012, http://blog.practicalethics.ox.ac.uk/2012/06/cyberwarfare-no-new-ethics-needed/.

11. 例如，这些词语见于《联合国宪章》第 2 条和第 52 条。参看 United Nations, Charter of the United Nations and Statute of the International Court of Justice, (Washington, DC: Government Printing Office, 1946), http://treaties.un.org/doc/Publication/CTC/uncharter.pdf.

12. 国防部长帕内塔说：“在过去两年中，国防部做出重大取证调查努力，试图判定攻击源，现在我们正在看到调查的结果。潜在攻击者必须意识到，美国有能力找到他们，只要他们胆敢伤害美国，我们就必将让他们付出代价。”参看帕内塔演讲：Remarks on Cybersecurity to the Business Executives for National Security, New York City, 11 October 2012, http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

13. 见注释 5。

14. 见注释 5。如果一个国家能够依据事实举出实施先行自卫的正当理由，伊朗将没有进行反击的法律或道德基础。关于先行自卫的论述，请参看 Kinga Tibori Szabó, Anticipatory Action in Self-Defence: Essence and Limits under International Law [先行自卫行动：国际法准则下的实质和限度], (Hague, Netherlands: T. M. C. Asser Press, 2011).

15. 见注释 10，第 9 页。

16. 见注释 5。

17. 美国国务院法律顾问 Harold Koh 对这两个词语作了如下解释：“第一，区分原则，要求攻击必须限于军事目标，不得将平民或平民财产作为攻击目标；第二，相称原则，即如果攻击导致的附带平民死亡、伤害或平民财产损坏或三者兼之的程度与预期的具体和直接的军事效益相比不应该过度，否则必须禁止此攻击。”参看 Harold Hongju Koh,“The Obama Administration and International Law”[奥巴马政府和国际法], (speech, Annual Meeting of the American Society of International Law, Washington, DC, 25 March 2010), http://www.state.gov/s/l/releases/remarks/139119.htm.

18. Stewart A. Baker and Charles J. Dunlap Jr.,“What Is the Role of Lawyers in Cyberwarfare?”[律师在网空战争中的作用是什么 ?], ABA Journal, 1 May 2012, http://www.abajournal.com/magazine/article/what_is_the_role_of_lawyers_in_cyberwarfare/.

19. 同上。

20. 同上。

21. 同上。

22. 同上。

23. 同上。

24. Charles J. Dunlap Jr.,“Lawless Cyberwar? Not If You Want to Win”[无法无天的网空战争？绝非制胜之道], American Bar Association, http://www.americanbar.org/groups/public_services/law_national_security/patriot_debates2/the_book_online/ch9/ch9_ess2.html.

25. 参看 Jim Wolf,“U.S. Military Better Prepared for Cyber Warfare: General”[美军为网空战争做了更好准备：概述], Reuters, 16 November 2011, http://www.reuters.com/article/2011/11/17/us-usa-cyber-military-idUSTRE7AG03U20111117?feedType=RSS&feedName=everything&virtualBrandChannel=11563.

26. 例如，参看 Department of Defense, Department of Defense Strategy for Operating in Cyberspace [国防部网空作战战略], (Washington, DC: Department of Defense, July 2011), 9, http://www.defense.gov/news/d20110714cyber.pdf. 其中说：“网空是许多网络的集成体，包括分布在全球的数千个互联网服务商；没有任何一个国家或组织能够独立维持有效的网空防御。

27. W. Michael Reisman and Chris T. Antoniou, eds., The Laws of War: A Comprehensive Collection of Primary Documents on International Laws Governing Armed Conflict [战争的法律：管辖武装冲突的国际法综合汇编], (New York: Vintage Books, 1994), xxiv.

28. 例如，参看 Gary D. Solis, The Law of War [战争法], (New York: Cambridge University Press, 2010), 41-42.

29. “Direct Participation in Hostilities: Questions and Answers”[直接参与敌对行为：问题解答], International Committee of the Red Cross, 6 February 2009, http://www.icrc.org/eng/resources/documents/faq/direct-participation-ihl-faq-020609.htm.

30. 同上。

31. 见注释 17。

32. George Monbiot, “With Its Deadly Drones, the US Is Fighting a Coward's War”[美国使用致命的无人机，正在打一场懦夫的战争], Guardian (United Kingdom), 30 January 2012, http://www.guardian.co.uk/commentisfree/2012/jan/30/deadly-drones-us-cowards-war.

33. Field Manual 3-24 / Marine Corps Warfighting Publication 3-33.5, Counterinsurgency [美国陆军战地手册 FM 3-24/ 海军陆战队作战出版物 3-33.5：平叛作战], December 2006, http://armypubs.army.mil/doctrine/DR_pubs/DR_a/pdf/fm3_24.pdf.

34. 参看 Doyle McManus, “U.S. Drone Attacks in Pakistan 'Backfiring,' Congress Told”[国会被告知美国在巴基斯坦使用无人机攻击，“结果适得其反”], Los Angeles Times, 3 May 2009, http://articles.latimes.com/2009/may/03/opinion/oe-mcmanus3.

35. Christopher Leake, “Taliban Make Children Plant IEDs to Thwart Army Snipers”[塔利班派儿童埋置简易炸弹企图挫败陆军狙击手], Daily Mail, 6 February 2010, http://www.dailymail.co.uk/news/article-1249044/Taliban-makes-children-plant-IEDs-thwart-Army-snipers.html.

36. Anthony R. McGinnis, “When Courage Was Not Enough: Plains Indians at War with the United States Army”[单凭勇敢无法取胜，大平原印第安人与美国陆军交战], Journal of Military History 76, no. 2 (April 2012): 473.

37. Charles J. Dunlap Jr., “Does Lawfare Need an Apologia?”[法律战是否需要自辩], Case Western Reserve Journal of International Law 43, no. 1/2 (2011): 132.

38. United Nations, General Assembly, Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Philip Alston: Addendum, Study on Targeted Killings, A/HRC/14/24/Add.6 [特约撰稿人提交给联合国大会的报告：关于未经法律许可的、迅即执行的或随意执行的处决；Philip Alston：附录：定点打击研究], (New York: United Nations, General Assembly, 28 May 2010), 25, http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.24.Add6.pdf.

39. Marc Pitzke, “Interview with Defense Expert P. W. Singer: 'The Soldiers Call It War Porn' ”[采访防务专家 P.W. Singer：战士称之为充满感官刺激的色情战], Spiegel Online International, 12 March 2010, http://www.spiegel.de/international/world/0,1518,682852,00.html.

40. Jeff Schogol and Markeshia Ricks, “Demand Grows for UAV Pilots, Sensor Operators”[对无人机飞行员和传感器操作员的需求不断增长], Air Force Times, 21 April 2012.

41. 例如，参看 Kenneth Anderson, “Laurie Blank on Mark Mazzetti's 'The Drone Zone'—Last in Series from Lewis, Dunlap, Rona, Corn, and Anderson”[Laurie Blank 评论 Mark Mazzetti 撰写的“无人机区域”– Lewis、Dunlap、Rona、Corn 和 Anderson 的系列评论之最后一篇], Lawfare (blog), 21 July 2012, http://www.lawfareblog.com/2012/07/laurie-blank-on-the-mazzetti-the-drone-zone-last-in-series-from-lewis-dunlap-rona-corn-and-anderson/.

42. Michael Hastings, “The Rise of the Killer Drones: How America Goes to War in Secret”[猎杀型无人机的兴起：美国如何隐秘发动战争], Rolling Stone, 16 April 2012, http://www.rollingstone.com/politics/news/the-rise-of-the-killer-drones-how-america-goes-to-war-in-secret-20120416#ixzz22VDkfR00.

43. “Rule 2.1: Advisor”[《美国律师协会专业行为规范》规则第 2.1 条：顾问], American Bar Association, Center for Professional Responsibility, http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_2_1_advisor.html.

44. 请比较国防部《联合部队伦理条例》“主要伦理价值观”列表对下列词语的定义：

a. 诚实。诚实包括讲真话、直爽和坦率。

(1) 讲真话是必要的。欺骗很容易被戳穿，而且确实经常被戳穿。谎言腐蚀可信度，削弱公众的信心。出于似乎为他人着想的理由（避免伤害感情、促进友善关系等）讲假话，却会引起对方反感。

(2) 直爽可给真话增添坦诚的感觉，对于提升公众信心和确保有效实施联邦政府的行动很有必要。讲了真话，但是方式不当，导致对方不知所云、误解或得出不正确的结论，因而并无益处。此等间接欺骗会产生恶意，削弱开诚布公的感觉，尤其是当对方期望坦诚相见时。

(3) 坦诚就是直截了当地主动提供信息。根据事态的重要性和双方关系的性质，有必要做到坦率直言。如果拒绝提供信息会使理智人士产生被出卖的感觉，则应做到坦率。在有些情况下，沉默就是不诚实，但是在另外一些情况下，透露信息可能是错误的，甚至可能是违法的。

参看 Department of Defense Regulation 5500.07-R, Joint Ethics Regulation, 17 November 2011, 118, http://www.dtic.mil/whs/directives/corres/pdf/550007r.pdf.

45. "Preventing a 'Cyber-Pearl Harbor' "[防止网空珍珠港事件], PBS Newshour, 16 April 2012, http://www.pbs.org/newshour/bb/science/jan-june12/deterlab_04-16.html.

46. "Expert Warns on Cyberwar Threat"[专家提出网空战争威胁警告], UPI.com, 16 March 2012, http://www.upi.com/Science_News/2012/03/16/Expert-warns-on-cyberwar-threat/UPI-33781331937216/#ixzz1sRYZauJc. 此文章中援引了声称是欧洲最大防毒软件公司 Kaspersky Lab 公司首席执行官和共同创建人 Eugene Kaspersky 的表述。

47. 参看 Richard Lardner, "US Needs Top-Level Approval to Launch Cyberattacks"[美国需要高层批准才能发起网空攻击], Salon, 24 April 2012, http://www.salon.com/2012/04/24/us_needs_top_level_approval_to_launch_cyberattacks/.

48. Jerry Brito and Tate Watkins, "Wired Opinion: Cyberwar Is the New Yellowcake"[连线观点：网空战争犹如新的核反应燃料黄饼], Wired, 14 February 2012, http://www.wired.com/threatlevel/2012/02/yellowcake-and-cyberwar/.

49. Peter Sommer and Ian Brown, Reducing Systemic Cybersecurity Risk [减小系统性网空安全风险], ([Paris, France:] Organization for Economic Cooperation and Development, 14 January 2011), 5, http://www.oecd.org/dataoecd/57/44/46889922.pdf.

50. Thomas Rid, "Think Again: Cyberwar"[网空战争三思而行], Foreign Policy, no. 192 (March/April 2012): 80, http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=full.

51. 见注释 48。

52. 见注释 1 中奥巴马讲话：认真对待网空攻击威胁。

53. "Rule 1.1: Competence"[《美国律师协会专业行为规范》规则第 1.1 条：胜任能力], American Bar Association, Center for Professional Responsibility, http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence.html.

54. Maj Gen Stephen R. Lorenz, "Lorenz on Leadership"[带兵之道], Air and Space Power Journal 19, no. 2 (Summer 2005): 7-8.

55. Kenneth Anderson, "Sir John Keegan, Ave Atque Vale"[约翰・基根爵士，珍重再见], The Volokh Conspiracy (blog), 3 August 2012, http://www.volokh.com/2012/08/03/sir-john-keegan-ave-atque-vale/.

56. 同上。

57. 笔者在其他场合也讨论过道德勇气的必要性，例如参看：Charles J. Dunlap Jr. "The Ethical Issues of the Practice of National Security Law"[国家安全法适用中的伦理问题], Ohio Northern University Law Review 38 (2012): 1093-95.

58. Max Hastings, Warriors: Portraits from the Battlefield [勇士：战场写照], (New York: Vintage Books, 2005), xvii.

查尔斯・邓洛普，美国空军退役少将（Major General Charles J. Dunlap, Jr., USAF (Ret.)），杜克大学法学院法律、伦理和国家安全中心执行主任。他曾担任军事法官三十四年，派驻英国和韩国，并曾参加非洲和中东的军事行动。邓洛普将军是美国国家战争学院的优秀毕业生，他在最近发表的与网空相关的著作包括：Perspectives for Cyber Strategists on Law for Cyberwar [网空战略家对于网空战争法律的看法]（战略研究季刊，2011 年）以及 Towards a Cyberspace Legal Regime in the 21st Century: Considerations for American Cyberwarriors [努力建立二十一世纪网空法制：美国网空战士的考虑因素]（内布拉斯加大学法律评论，2009 年）。他和斯图瓦特・贝克（Stuart Baker）关于网空法律问题的辩论收录于 Patriot Debates [爱国者的辩论]，由美国律师协会在 2012 年出版。

网空冲突中的软性竞争

The Friendly Side of Cyber Conflict*

帕纳约提斯·雅纳科乔戈斯博士，美国空军防务分析员（Dr. Panayotis A. Yannakogeorgos, Research Professor, USAF）

互联网治理定义宽广，治理内容包括基础结构、标准化，以及法律、社会文化、经济和开发等事项。但是，与互联网关键资源治理及其对美国国家安全的影响相关的思考，却经常被忽视。美国以外国家试图改变互联网的技术管理和技术标准设计，长远而论，他们的行为可能会危害美国国家利益。鉴于目前的互联网治理现状面临诸多全球性挑战，包括那些意在取而代之的另类计算机网络在网空的崛起，确实需要集思广益加以应对，本文探讨美国国家安全政策背景，并提出软性征服概念和保障信息自由流动的互联网治理多相关方共管格局建议。

互联网治理对美国国家网空战略的意义

技术标准和规范不像那些对国家网空安全的较为明显的威胁那样受到重视。在人力资本和资源受限的环境中，人们关注的重点是犯罪行为、间谍活动和其他形式的网空冲突，而不是与互联网关键资源治理、技术标准的制定以及新型电信设备设计有关的事项。一些政策学究们原来谈到网空就发怵，面对错综复杂的互联网治理，就更不赞成把资源投入在物理世界找不到类比的这个领域。网空目前处于自由和开放形态，但是不会永远如此。因此，理解互联网治理的战略层面意义，和理解攻击者可能如何利用美国的网络漏洞破坏美国国家安全，两者同样重要。从国家安全角度考虑，互联网的技术管理很重要，因为极权国家也许能通过技术手段对互联网的内在基础结构施加威力和影响。而从全球安全角度考虑，通过互联网治理机构的管理来维护信息自由流动的价值，将有助于继续推动发达国家及发展中国家促进创造发明和经济繁荣。

ICANN = 互联网名称与数字地址分配机构
ITU = 国际电信联盟

美国目前关于国家战略的主要政策文件和论述都主张对网空威胁做出国家反应。[1] 这些战略观点所关注的是灾难性国家安全事件，而不是设定技术标准或管理互联网日常运行的组织机构之间的纷争。白宫的发言倒是强调了通过现行的多相关方共管平台制定和实施统一技术标准的重要性，具体提出："协作开发一致同意的信息和通信技术国际标准……是保障开放性和交互操作性、发展我们的数字化经济、推动社会进步的一个重要方面。"[2] 此外，政府也看到了国际标准制定机构面临的挑战，认为"在设计下一代标准体系方面，我们必须以共同利益为重，支持最合理的技术标准和治理结构，而不是那些只着眼于提高国家威望或政治控制力的技术标准和治理结构。"[3] 但是，这些考虑被淹没在种种耸人听闻的、臆想的网空末日的讨论之中。

* 此文原刊登在美国空军大学《战略研究季刊》2012 年秋季号，标题为"Internet Governance and National Security"。本刊请作者对之删减并做适当改动后，翻译和重新发表，以飨中文读者。

要保障国家安全，就要求互联网所赖以立足的语言——技术标准和协议——继续保障信息自由流动。如果像某些人所说的，在网空中“编码就是法律”，[4] 那么标准和协议就是经脉，使这些编码通过网空现实而获得意义。在政策界，网空已经被视为一块“无形的领域”。因此，技术标准和协议更是加倍的“无形”。然而，这些协议界定着互联网及其关键的基础结构的特征。一如有人指出:“软件和硬件设计所遵循的基本协议代表了制约行为和制定公共政策的一种更加内在和更加无形的体系结构……在这个意义上，协议有其政治赋形——它不是一个虚无的躯壳，而是由协议设计者及实施者演化而成。”[5] 过去，美国引领世界制定协议和标准，因此，互联网的设计和特征渗透着自由价值观，孵育了不断推动全球社会经济发展的创新精神。

网空冲突中的软性竞争

有关互联网标准和治理机构的纷争酝酿已久，一触即发，将对未来互联网的特征起决定性影响。俄罗斯和中国部署了先进的 IPv6 协议，实力相当的其他国家也在制定新的标准，他们都在把新的技术标准推向全球市场，形成网空冲突的软性竞争。

当某个系统的非核心运行者与核心运行者结成伙伴合作关系，藉以取得某个所需信息系统的访问权限时，即发生软性征服。网空理论家马丁·利比奇（Martin Libicki）认为:

> 控制系统者也许会允许其他人访问该系统，让他们使用其内容、服务和连接。随着时间推移，如果这样的访问很有用……用户也许会逐渐依赖该系统，于是把标准和协议应用于自己的系统，从而加深这种依赖，并投入人力物力，以便更好地使用他们喜欢的内容、服务或连接。[6]

在这种联盟关系中，核心合作伙伴逐渐处于支配非核心伙伴的地位，后者越来越依赖核心伙伴提供的网络系统服务，连同其漏洞。于是出现担心：“对别人的全面依赖性渗透自己的内部系统，可能使自己受制于别人……系统易受攻击可能有多种原因，例如合作伙伴对网络基础结构的安全性有全面的了解，或者利用对基础结构的访问权限更轻易地启动攻击。”[7]

互联网及其基础技术结构明确地显示了美国作为信息系统的核心运行者，如何通过创建互联网技术和设定其运行规则，软性地支配着盟友和敌邦。互联网依赖美国实体设计及运行的产品，这些实体包括域名系统、互联网名称与数字地址分配机构（ICANN）、微软公司、思科公司，等等。世界各地的用户，例如谷歌和脸书，现在也依赖这个平台上提供的各项服务。然而美国实体目前享有的支配地位不可能永久。爱沙尼亚开发的 Skype 就是一个例子，说明网络服务并非一定要来自美国。但是，即使某项基于互联网的服务是外国创建的，该项应用程序传送的大部分信息还是要经过位于美国的硬件设备。当发现有网络漏洞时，其他国家也许会尝试退出我们的信息系统，以保护他们自己的网空主权，并且扩大他们的影响力，吸引客户离开互联网，改为使用他们自己创建的系统。[8] 因此，美国在网空的战略优势不是无限期的，而且目前正在不同程度上受到实力相当的竞争者的挑战。有鉴于此，我们应该了解其他国家对美国技术优势的反应，从网空软性征服的角度调整我们的网空战略。

软性征服所关注的，并不限于敌方仅能渗透供应链及在对美国国家安全至关重要的

服务器上创建后门程序然后潜入美国信息系统。[9] 我们面临的威胁还来自国外新技术的出现，而美国并非这些新技术的核心运行者，并且可能会依赖这些新技术。我们关注恶意网空攻击，却没有重视网空世界的柔软腹部——那些使得网空能够从电磁频谱中兴起的技术和标准。

中国正在网空中播撒全球软性征服的种子，且进展神速。根据美中经济与安全评估委员会的报告，“如果照目前的趋势继续发展，就消费、生产和创新而言，中国（及其利益代理人）将在许多领域有效地成为市场主要推动力，其中包括电信领域。”[10] 美国依赖中国制造的计算机芯片和其他信息及通信技术硬件，使得病毒和后门程序能够进入包括军方在内的美国机构和企业所用的设备中。中国制造的计算机硬件的价格异常低廉，畅销于亚洲和发展中国家。[11] 此外，在下一代移动式 4G LTE 网络的标准制定方面，中国实体，例如华为，正在引领全世界。[12]

互联网治理与多相关方共管模式

跨国公司等企业实体在国际电信联盟（ITU）内对国际通信监管政策的制定做出直接贡献，并通过其员工在 ICANN、互联网工程任务组和其他组织内做出非直接的个人贡献。

美国政府在 1990 年代出于战略理由禁止出口强化加密软件，但遭到私有企业的反对，最后在这场所谓的加密技术战争中败给后者。也有些公司为了防止犯罪分子使用无法解开的密码进行通信，采用执法部门拦截机制，以便国家安全机构能够监控可疑的犯罪分子和恐怖分子的通信。还有些制定、维护和修订核心标准及基础技术结构的美国公司和相关个人因为与政府安全部门合作，而遭致贬毁，被指责为私有公司与流氓手法的国家安全机构同流合污，捕获全世界的所有数据。事实并非如此，美国和那些极权国家不同，只要严格认真遵守旨在保护用户隐私的美国法律，就可明确保持政府与私有企业之间的界限。有些媒体为追求轰动效应，动辄刊登这类指责，导致全球对美国私有企业的信任减退，同时为互联网治理机制必须国际化的主张提供了支持。

在美国，电信服务提供商（可追溯到电报系统时代）从来都不是国有垄断体制的一部分，世界其他地区则并非如此。[13] 例如，英国电信公司和德国电信公司一直都是国有企业，到 1990 年代才转为私营。当然，在美国，电信公司尽管没有国家直接控制，仍接受国家的监管。在国际电信谈判中，国家与各大信息及通信技术公司有一种共生关系。[14] 自 ITU 的前身国际电报联盟在十九世纪中期开始开会监管电信政策以来，始终如此。[15] 因此，发展中国家认为，“由于大部分垄断性互联网公司都是美国公司，目前……美国法律便当仁不让地套用于全球。”[16]

那种认为美国政府实际上控制着互联网关键资源的全球通行观点，在很大程度上是因为其他国家的电信公司同其本国政府有密切的关系，于是以为美国也不例外。其实美国的情况很独特，美国政府从来没有拥有或运行任何一家电信公司。随着世界上其他国家向美国电信行业私有化模式转化，过去由政府控制电信行业的经历仍记忆犹新。今天，这些经历给 ICANN 与美国商务部之间签订的特殊协议蒙上了一层怀疑的阴影。

事实上，域名系统最初是由美国国防部发明的，并在其成形阶段由国防部负责技术

管理，然后在 1998 年移交给商务部，后来逐步演变成目前的非政府多相关方共管模式。[17] 这个模式的名称反映了互联网基本技术以及参与制定互联网技术功能标准的组织机构。

互联网关键资源“在互联网治理意义上通常是指互联网独有的逻辑资源，而不是指并非互联网独有的实体基础结构部件或虚拟资源。关键的互联网资源必须提供一个需要中央协调的、具有全球独特性的技术要求：互联网地址、域名系统、自主系统号码。”[18] 一般人认为互联网是无极限的，实际上，基本的地址空间是有限的。事实是，互联网协议地址空间几乎已经用完。工程师们预见到互联网协议的这个问题，研发了 IPv6 协议。它有许多优点，例如，IPv4 的可用 IP 地址数目是 4,294,967,296，而 IPv6 则增加到 2^{128}。今天，许多人认为：“部署 IPv6 是长期舒缓公共 IPv4 地址库压力的唯一途径……”[19] 在全世界开始采用 IPv6 作为全球互联网主要通信协议，逐步取代 IPv4 之际，美国并未在这方面领先。目前，就市场渗透率而言，俄罗斯的部署范围最广；按数量计算，中国的部署量最大。[20] 部署迟缓的后果牵涉到互联网治理和传统型安全威胁。关于后者，美国国家标准局指出：“在 IPv6 部署的最初几年里，防止未获授权而进入 IPv6 网络可能会更加困难。”[21] 因此，在全国部署 IPv6 方面有较多经验的竞争国家对于该协议在现实世界的运行技术有更多的了解。整个美国空军非保密互联网协议路由器网络在 2014 年之前不会全部使用 IPv6。根据计划，即使到那个时候，也会继续在 10 至 15 年之内同时使用 IPv4 和 IPv6。[22] 随着 IPv6 逐渐成为互联网主干协议，俄罗斯和中国也许会被人们理所当然地视为 IPv6 主导国家，而且它们将会利用这个机会试图把紧缺的地址空间的控制权从 ICANN 转移到某个跨政府机构，例如在联合国架构下的某个机构。

由于网空是一个人造领域，因而其基础结构和标准化非常重要。一些以计算机科学家和工程师为主的全球性组织创建了互联网的运行标准和规则。这些全球性组织中包括前身是美国国防信息系统局、美国国防部高级研究项目局或其他美国政府计划机构、后来在 1990 年代中期实行私有化的那些机构。在下一代互联网的开发中，美国可能不是主要推动国。目前，俄罗斯、中国和其他外国科学家和工程师们正在制定标准和流程。今天的网络设备使用英语作为相互通信语言。如果美国的科学领先地位继续走下坡路，今后的网络也许会依赖讲外语的设备。另外，域名系统和 IP 地址分配的管理也将受到挑战，有些人试图把管理权从目前的多相关方共管平台转移到 ITU 体制内的某个跨政府机构。这就是网空冲突中的软性竞争。

围绕互联网政策的争论证实了多边主义无济于事，因为尽管美国竭力尝试牵头，其他国家并不响应。美国拥有互联网主干结构开发和维护方面的创新技术，这毋庸置疑。但是，世界各国竭力推行监管改革，例如力主让 ITU 之类的全球治理机构监督 ICANN。这已成为一个剑拔弩张的政治问题，与国家网空安全密切相关，对于民主国家和极权国家都是如此。总之，美国在平等国家之间的“领先地位”反而导致争论进入一个又一个的死胡同。我们现在看到，无论是盟友还是竞争对手都在采取反制行动，并且这些行动可能在 2012 年世界国际电信会议期间会加大力度。[23]

世界各国对现状的挑战

信息经由互联网等网空开放元实行全球流通，受到相关国家和区域机构的监管，这些机构在国际上相互协调政策。为网空某些组成元制定的标准都经过如国际标准化组织和 ITU 等不同机构的漫长审查流程，是为确保各国之间有充分的技术和政治合作。过去，互联网技术标准由美国实体制定；现在，华为和中兴等中国实体正在互联网治理机构内发挥越来越大的作用，他们参与起草重要的国际标准，将影响世界上下一代网络的架构。这不是最近才发生的事情。早在 2004 年，在 ITU 电信标准化部门担任高级职务的几名中国籍专家就开始谈论利用向 IPv6 协议过渡的机会纠正他们认为美国和发展中世界之间的地址分配不平衡问题。“IPv4 地址的早期分配导致地理区域不平衡，较早采用该协议的国家占有过多的地址空间。区域互联网注册管理机构（RIR）注意到这种情况并采取了一些对策……有些发展中国家对 IP 地址分配提出质疑。重要的是，应确保 IPv6 不会出现类似的问题。”[24] 这种情况说明有些国家希望能把 IPv6 地址分配管理转移到 ITU 等全球性机构。

在联合国的政治论坛上，要求改革互联网治理的呼声越来越高。竞争对手和合作伙伴在俄罗斯和中国的带领下，携手要求互联网技术管理国际化。中国和俄罗斯，联合了印度、南非及巴西，带领各国反对美国在 ICANN 中的支配地位。这些活动已经持续了将近十年。[25] 随着美国国防部高级研究项目局网络 ARPAnet（互联网前身）实验成功，现已成为全球社会经济发展的一个重要部分，而且各国政府越来越意识到该网络的重要性，要求将网络主干机构 ICANN 国际化的活动力度也越来越大。前面说过，这种国际化呼声的部分起因是，其他国家因为自己的政府与电信公司在历史上有特殊关系，故而以此类推，认为美国政府也是通过商务部和国家电信与信息管理局控制着 ICANN。

本文认为，由 ITU 控制 IPv6 空间的一个较为可行的方法是，ICANN 向 ITU 提供自己的 IP 地址块，并担任其本身的区域互联网注册管理机构，形成在国家层面分配国家级互联网注册管理机构的做法。这样做既可以保持目前管辖互联网关键资源的多相关方共管框架，同时又能充分照顾到中国和发展中世界的需求。它可减少摩擦，并且让喜欢现行模式者能继续使用该模式监管互联网的日常技术运作。

在信息社会世界首脑会议（WSIS）筹备阶段，对现有互联网治理体制的强烈反对声浪开始涌现，使会议成为关于 ICANN 国际化争论的一个战场。例如，在 2004 年 3 月联合国主持召开的全球互联网治理论坛上，[26] 巴西代表玛丽亚·路易泽·维沃提声称互联网治理需要改革，因为它没有包括发展中国家，而且似乎被某些国家或利益相关方所霸占。[27] 南非全国委员会主席琳达·肖普 - 马弗尔也持类似的观点，认为发展中国家最担忧的是 ICANN 流程的合法性，而不是其功能运作。[28] 于是，与会代表经过认真讨论，根据发展中国家提出的关注事项，最终同意 ICANN 需要进一步改革。在整个 WSIS 会议期间，以及随后召开的讨论互联网治理和全球网空安全的其他会议上，巴西始终强烈反对美国在 ICANN 的支配地位。2011 年，印度声援南非和巴西，建议“具体落实突尼斯指令”，其建议内容为：

> 鉴于对透明、民主和多边机制之需要，以便所有的利益相关方能发挥各自的作用，处理需要引起关注但现有机制未能

妥善处理的许多跨国国际公共政策问题，并鉴于对加强合作之需要，以便各国政府能在平等的基础上履行与互联网相关的国际公共政策领域的各自义务和责任，印度建议在联合国建立一个新的主管全球互联网相关政策的机构，该机构可称为联合国互联网相关政策委员会(CIRP)。[29]

成立互联网相关政策委员会的建议被视为对目前互联网技术管理的反制手段，在发展中世界获得很大反响。实际上，这个建议在很大程度上反映了中国政务和公益机构域名注册管理中心(CONAC)所表达的中国观点，该中心认为“美国政府掌握了互联网资源的控制权。因此，我们建议应该使所有的多相关方都能够对计算机安全计划发表意见，因为维护网空安全不是美国政府单方面的使命，也没有任何一个国家能够单独完成这项使命。”[30]

俄罗斯前总理普京也表示：ITU 是年代最久远的国际组织之一；它的历史比联合国还长出一倍。俄罗斯是其共同创建国之一，愿意成为一个积极的成员。我们感谢各位提出的各种讨论议题。其中一个是利用 ITU 的监控和监督能力对互联网实行国际监管。[31]

因此，美国在 ITU 内面临着来自极权国家带领的发展中世界的严重挑战，他们要求把互联网关键资源的控制移交给一个多边机构。这个要求内含的基本危险是，具有信息自由流动关键特征的互联网将演变到听任非民主国家的政治日程控制信息流动的模式。因此，美国以及观念相同的其他国家必须在外交上挺身而出，确保互联网保持信息自由流动的特性，避免受到多边机构的政治控制。

围绕互联网控制权的外交斗争在其他各种论坛上也有发生，例如联合国科技发展委员会。人们提出了许多建议，包括：

建立一个隶属于科技发展委员会的临时工作组，在联合国秘书长的支持下制定机构设计和路线图，以便在互联网相关公共政策问题上加强合作……

在联合国系统内建立一个较永久的互联网相关国际公共政策问题委员会，可以参照经济合作与发展组织信息、通信与计算机政策委员会的模式……

更具体的是，全球政策问题应该由一个具有全球代表性的机构来处理，例如联合国；而区域问题则应该由具有区域代表性的机构来处理，例如欧盟委员会……[而且] 相关组织应该参与每四年举行一次的 ITU 全权委员会关于互联网治理的讨论，以及 ICANN 的公共审议流程和政府顾问委员会讨论。[32]

鉴于世界电信会议将在 2012 年 12 月召开，上述言论表明人们会再次提出这些主张，要求 ITU 修订《国际电信条例》，把对下一代互联网关键资源的管理包括在 ITU 条例内，推动此国际机构在互联网治理方面发挥更大的作用。[33]

让互联网治理向跨政府流程开放，可能给全球经济安全带来风险，因为责任心不强的国家也许会对互联网治理采取目前私有化放任自流的态度，并且让国家和国内公司实体控制互联网关键资源的管理。

影子域名系统的崛起

互联网关键资源之所以能保障普遍可解析的 URL 地址和全球互联网通信，应归功于 ICANN 管理的根系统以及互联网工程任务组

（和其他机构）内部设计、开发和论证的各种协议。尽管这个流程可确保自由和开放的互联网运行，ICANN 用于维护域名注册管理机构的标准和协议也可被个人、临时网络和某些国家用来设计及部署自己的另类域名系统，这些替代系统可以独立于互联网或“搭载”于互联网之上。公司的局域网（LAN），例如公司内部使用的“.company name”网络，就是独立于互联网的网络。当某个组织想要搭载于全球域名系统根名之上，并把自己的伪顶级域置入其中时，伪域的核心运行者可以使用特定的软件资源在其替换域名系统内解析全球可用的域名。美国浏览用户可以通过洋葱路由器（TOR）网络进入另类域名系统，获得亲自感受。用户可以下载洋葱路由器套装软件，导航到想要匿名访问的网站（这是 TOR 的典型用途），用 TOR 浏览器指向“.onion”域上的相关网站，进入网空地下社会；在这片空间中，业务运作管理已经开始躲闪转移，目的就是想摆脱执法机构的监视，为自己的真实身份再加一层保护。

如果大量使用这类影子互联网，可能导致人们对互联网的信心减弱，其使用量也会下降。最大的风险是，当某些国家开发和部署供其自己内部使用的另类域名系统时，他们会与全球互联网隔离。这种情况不同于控制进入点和实际开发国家级内联网且自行作主是否接入全球互联网的做法。[34] 俄罗斯和中国在部署供国内使用的潜在的新内联网方面已经有所作为，伊朗等其他国家也在学样。

美国参与公开倡导和组织“数字活动分子”（digital activists），为确保信息自由流通而斗争，结果造成国际摩擦；美国调拨高达三千万美元的资金，用于提升互联网的开放式访问性能，支持数字活动分子，并反击任何国家对互联网的压制。[35] 这么做对于促进网空安全问题的国际合作并无助益。“互联网自由议程”就是这种情况的一个例子。[36] 此类技术使得公民活动分子能够有效地绕过政府的系统监控工具，传播被禁止的信息。还有一些其他工具，使得活动分子能够披上数字伪装，组织以推翻现有政权为目的的社会运动。结果是，导致产生了另类国家网络，创建了供国内使用的另类域名系统，使得执政当局能够审查网络内容和抑制现有互联网结构所促进的生产率。中国已经在国家范围内做到了这一点。在国务院国有企业改革办公室以及工业和信息化部的授权下，中国政务和公益机构域名注册管理中心管理“.政务 .cn”和“.公益 .cn”两类国内网站的域名注册。

分裂性互联网的崛起肯定会改变现有互联网的特征，对全世界的创新和繁荣造成负面影响。那些希望互联网保持自由和开放特征的人们将受益于自由和开放，并且与那些企图控制互联网一个总开关的人形成显著的道德对比。因此，维持现有的互联网治理模式，同时妥善处理友方和盟国的合理疑虑，将有助于确保互联网继续发挥人类经济发展的稳健平台的作用。

结语

如果不重视我们在互联网治理方面的漏洞和软性征服，可能使我们的敌人在网空冲突中获得战略优势，并使我们自己的网空攻击行动变得更复杂，因为我们的竞争对手正在部署以非美国实体开发的协议和标准为基础的网络。我们必须就这些问题开展广泛的对话，以加深对网空的了解，并且适应网空环境中发生的变化。尽管在历史上互联网起源于美国国防部，但是美国从来没有很好地组织人力去影响与互联网治理有关的技术标

准和政策的制定。目前，国防部依然采取被动响应态度，只是协调和评论美国政府流程中正在考虑的与互联网治理有关的各种全球规范和标准。由于这种被动态度，国防部和美国空军可能被外界视为不具备互联网治理的法律知识或技术资历。国防部，尤其是美国空军，应该像以前一样发扬领导责任，在信息技术基础结构标准的制定方面发挥更积极的作用。此外，国防部应该更加仔细地制定书面政策，界定其作用，系统地指引自己如何参与互联网治理机构的活动和其在其中的地位。空军应该在国防部和整个政府体制内起到带头作用，软性征服概念已经隐含在空军的政策、战略和作战准则之中，现在空军需要更明确地重视更广义的软性征服概念。将于 2012 年 12 月举行的世界电信会议也许可以成为开始这项努力的一个合适场所。

随着作为全球互联网基础的硬件和软件不断演变，以及非美国实体开始研发新硬件、标准和协议，美国实体的市场占有率有可能被挤占，美国的网空基础结构核心运行者地位将会削弱。目前，美国凭借 ICANN 和顶级域名系统，占据着互联网服务开发者和核心提供者的地位，拥有技术支配权。但是，我们的国家网空安全战略没有充分正视其他国家通过开发将成为下一代网络基础的协议、标准和技术所构成的威胁。美国空军拥有大量的科学家和工程师等优秀技术人才，可以发挥关键作用。但是，它不能单独行动，而国防部则需要从已经有限的网空资源中调拨一部分到互联网治理。如果不这样做，国外设计的技术标准和协议可能会构成下一代信息技术的主干，也许会逆转国防部目前所依赖的互联网信息自由流动的特征，使国防部的作战行动遭遇风险。美国空军始终是对网空最有影响力的美国军种，因此空军在互联网治理争论中的作为或不作为有举足轻重的意义。♣

注释:

1. The National Strategy to Secure Cyberspace (NSSC) [国家网空安全战略], (Washington: The White House, y 2003); 另参看 John Rollins and Anna C. Henning, Comprehensive National Cybersecurity Initiative (CNCI) [全面的国家网空安全计划], (Washington: Congressional Research Service, 10 March 2009; declassified in March 2010); 另参看 International Strategy for Cyberspace [网空国际战略], (Washington: The White House, May 2011); 另参看 the Department of Defense Strategy for Operating in Cyberspace [国防部网空作战战略], (Washington: DoD, July 2011). 这些文件是迄今关于网空安全的最主要的指导文件。
2. 见注释 1 中“网空国际战略”，第 12 页。
3. 见注释 1 中“网空国际战略”，第 15 页。
4. Lawrence Lessing,“Code is Law”[编码就是法律], 见 Code: And Other Laws of Cyberspace, Version 2.0 [编码：以及其他网空定律，2.0 版], (New York: Basic Books, 2006), 11-10.
5. Laura DeNardis, Protocol Politics: The Globalization of Internet Governance [协议政治：互联网治理的全球化], (Cambridge: MIT Press 2009), 11.
6. Martin Libicki, Conquest in Cyberspace [网空征服], (New York: Cambridge University Press, 2007), 12.
7. 同上，第 137 页。
8. 全球定位系统（GPS）是争夺软件和硬件控制权的一个例子。尽管使用 GPS 的基本服务是免费的，友方和竞争对手都意识到他们对这套美国系统的依赖性使他们易于陷入受人摆布的境地。俄罗斯正在革新其 GPS 系统，欧盟和中国则在自行开发独立的 GPS 系统。这些新系统从意图形成到具体落实有一个很长的时间周期，因为部署一个太

空网络涉及巨额投资。网空系统的时间周期可能短一些，因为与发射多个高科技卫星到太空相比，部署一个国家级计算机网络的成本较低。关于另类 GPS 系统的详细论述，请参看 Lt Col Scott W. Beidleman, GPS versus Galileo: Balancing for Position in Space [GPS 与伽利略卫星导航系统：空间定位竞技], (Maxwell AFB, AL: Air University Press, 2006).

9. Bruce Rayner, "Ferreting out the Fakes" [揪出赝品], Electronic Engineering Times, 15 August 2011, 24; 另参看 John Markoff, "Computer Gear may Pose Trojan Horse Threat to Pentagon" [计算机零部件可能给五角大楼带来木马病毒威胁], New York Times, 10 May 2008, 12.

10. The National Security Implication of Investments and Products from the People's Republic of China in the Telecommunications Sector [美国电信行业中来自中国的投资和产品对国家安全的影响], U.S.-China Economic and Security Review Commission Staff Report, January 2011, 7, http://www.uscc.gov/RFP/2011/FINALREPORT_TheNationalSecurityImplicationsofInvestmentsandProductsfromThePRCintheTelecommunicationsSector.pdf.

11. LCDR A. Anand, “Threats to India's Information Environment” [印度信息环境面临的威胁], 见 Information Technology: The Future Warfare Weapon [信息技术：未来战争的武器], (New Delhi: Ocean Books Pvt. Ltd., 2000), 56-62.

12. "Huawei Conducts World's First Commercial Network LTE Category 4 Trial” [华为进行世界上首次商业网络 LTE Category 4 测试], Cellular News, 9 May 2012, http://www.cellular-news.com/story/54329.php.

13. Anton A Huurdeman, The Worldwide History of Telecommunications [世界电信史], (Hoboken, NJ: John Wiley & Sons, 2003), 91-146, 153-85; 另参看 Jill Hills, “International Market Structure and the ITU” [国际市场结构和国际电信联盟], 见 Telecommunications and Empire [电信与帝国], (Champaign: University of Illinois Press, 2007) 91-116.

14. Edward Comor, “Communication Technology and International Capitalism: The Case of DBS and US Foreign Policy” [通信技术和国际资本主义：DBS 和美国外交政策案例研究], 见 The Global Political Economy of Communication: Hegemony, Telecommunication and the Information Economy [全球通信政治经济学：霸权、电信和信息经济], ed. Comor (New York: St Martin's Press, 1994), 83-102.

15. Jill Hills, The Struggle for Control of Global Communications: The Formative Century [争夺全球通信控制权：格局形成的世纪], (Champaign: University of Illinois Press, 2002.)

16. Parminder Jeet Singh, “India's Proposal Will Help Take the Web out of U.S. Control” [印度的建议有助于使互联网摆脱美国的控制], Hindu Online, 17 May 2012, http://www.thehindu.com/opinion/op-ed/article3426292.ece.

17. Department of Commerce, Management of Internet Names and Addresses [互联网名称和地址的管理], 63 Fed. Reg. 31741 (1998).

18. 见注释 5 中“协议政治”，第 11 页。

19. M. Ford, M. Boucadair, A. Durand, P. Roberts Issues with IP Address Sharing [IP 地址共享问题], (Internet Engineering Task Force, RFC 6269) June 2011 http://www.hjp.at/doc/rfc/rfc6269.html

20. Ingrid Marson, “China launches largest IPv6 network” [中国开始筹建最大的 IPv6 网络], CNET News, 29 December 2004, http://news.cnet.com/China-launches-largest-IPv6-network/2100-1025_3-5506914.html.

21. Sheila Frankel et al., Guidelines for the Secure Deployment of IPv6 [安全部署 IPv6 指南], (Gaithersburg, MD: National Institute of Standards, December 2010).

22. Katherine Kebisek, “AFNIC prepares Air Force for IPv6 transition” [空军网络整合中心准备协助空军过渡到 IPv6], Air Force Space Command (4 April 2011), http://www.afspc.af.mil/news1/story.asp?id=123249968

23. 关于互联网治理的争论已有大约十年的历史，肯定将持续到 2012 年以后的年份。信息社会世界首脑会议的下一次聚会将在 2015 年。

24. H. Zhao, “ITU and Internet Governance—input to the 7th meeting of the ITU Council Working Group on WSIS, 12-14 December 2004” [国际电信联盟和互联网治理 — 提请 2004 年 12 月 12-14 日召开的国际电信联盟委员会信息社会世界首脑会议工作组第 7 次会议考虑的几点意见], www.itu.int/ITU-T/tsb-director/itut-wsis/files/zhao-netgov02.doc.

25. Panayotis A. Yannakogeorgos, “Cyberspace: The New Frontier and the Same Old Multilateralism” [网空：新疆域和旧多边主义], 见 Global Norms, American Sponsorship, and the Emerging Pattern of World Politics [全球规范、美国赞助和世界政治的新兴模式], ed. Simon Reich (New York: Palgrave, 2010).

26. “UN ICT Task Force Global Forum on Internet Governance to be Held in March”[联合国信息及通信技术任务组互联网治理全球论坛将于 3 月召开], UN press release, Paris, 13 February 2004, http://portal.unesco.org/ci/en/ev.php-URL_ID=14347&URL_DO=DO_PRINTPAGE&URL_SECTION=201.html.

27. "Global Internet Governance System is Working But Needs to Be More Inclusive, UN Forum on Internet Governance Told" [联合国互联网治理论坛被告知，全球互联网治理系统在发挥作用，但需要有更大的包容性], UN press release, 26 March 2004, http://www.un.org/News/Press/docs/2004/pi1568.doc.htm.

28. 同上。

29. “Statement by Mr. Dushyant Singh, Member of Parliament, on Agenda Item 16—Information and Communication Technologies for Development, at the 66th Session of the United Nations General Assembly on October 26, 2011”[Mr. Dushyant Singh 在第 66 届联合国大会 2011 年 10 月 26 日全体会议上就议程第 16 项“信息和通信技术的发展”发表的讲话], http://content.ibnlive.in.com/article/21-May-2012documents/full-text-indias-un-proposal-to-control-the-internet-259971-53.html.

30. Yang Yu, Chinese response to “Further Notice of Inquiry on the Internet Assigned Numbers Authority Functions”[中国对“关于互联网号码分配机构功能质询的进一步通知”的反应], China Organizational Name Administration Center (CONAC), http://www.ntia.doc.gov/files/ntia/conac_response_to_fnoi.pdf.

31. “Prime Minister Vladimir Putin meets with Secretary General of the International Telecommunication Union Hamadoun Toure”[普京总理会见国际电信联盟秘书长哈马顿・杜雷], Working Day, 15 June 2011, http://premier.gov.ru/eng/events/news/15601/.

32. UN General Assembly, “Enhanced Cooperation on Public Policy Issues Pertaining to the Internet”[在互联网相关的公共政策问题方面加强合作], Report of the Secretary-General, http://unctad.org/meetings/en/SessionalDocuments/a66d77_en.pdf.

33. 国际电信条例（ITR）有 178 个签约国，是一个全球适用的条约。

34. 这不同于 Chris Demchak 在“Rise of a Cybered Westphalian Age”[网空威斯特伐利亚和约时代的到来] 中所指的情况，此文见 Strategic Studies Quarterly 5, no. 1 (Spring 2011): 32-61.

35. US Department of State, Internet Freedom Fact Sheet [互联网自由简介], (15 February 2011) http://www.state.gov/r/pa/prs/ps/2011/02/156623.htm

36. Spencer Ackerman, “Does Obama's 'Net Freedom Agenda' Hurt the U.S.?”[奥巴马的“网络自由议程”伤害美国吗 ?], Wired, 28 January 2011, http://www.wired.com/dangerroom/2011/01/does-obamas-internet-freedom-agenda-hurt-the-u-s-without-helping-dissidents/.

帕诺・雅纳科乔戈斯博士（Dr. Pano Yannakogeorgos）是美国空军大学空军研究所的网空政策与全球事务研究教授，其研究领域包括网空与全球安全交汇、网空规范、网空武器控制、非国家暴力行为体，以及东地中海研究。他曾是罗格斯大学（Rutgers University）全球事务中心资深项目协调员，并曾担任联合国安全理事会顾问。他拥有罗格斯大学全球事务硕士和博士学位，以及哈佛大学文科学士学位。

F-35——和时间赛跑

The F-35's Race Against Time*

约翰·A·图帕克，美国空军协会《空军杂志》执行编辑（John A. Tirpak, Executive Editor of the Air Force Magazine）

自从美国军方为其新一代先进隐身攻击战斗机——即后来命名的F-35“闪电 II”——编制出全套性能要求，或者说画出飞机蓝图至今，已经过去十六年。按照这项豪气干云的计划，F-35A 现在应已列装美国空军，赶在俄罗斯和中国部署他们自己研制的隐身战斗机之前。

然而天不遂人愿，计划多次修改，进度严重延误，飞机的交付日期一推再推。而今，已经无人敢奢望 F-35A 能在 2017 年之前投入作战服役，届时若能如愿，已属万幸。

届时，F-35 的那些原先预期的作战优势还存在吗？等到飞机终于交付给战斗机中队的时候，和世界上其他先进战斗机相比，它还承负得起优势战斗机的盛名吗？说到底，对这 F-35A，还值得再等下去吗？

洛克希德马丁飞机公司的回答，是斩钉截铁的“是”。作为这款飞机的设计和制造者，该公司最近对此飞机的隐身设计、使用概念、现代空战能力等方面，给出了一些新的重要介绍。

四机编队，所向披靡

洛马公司副总裁史蒂芬·奥布赖恩（Stephen O'Bryan）作为 F-35 飞机研制的对外

宣讲人，宣布这款飞机能满足所有性能要求。以海军 F/A-18“大黄蜂”飞行员身份退役的奥布赖恩指出，F-35，即便是其最初的基线型号，其战斗能力也已远远强于任何经过重大升级的四代战斗机和攻击机，无论是 F-15、F-16，还是 F-18。

就能力而言，F-35 是一种三合一或者四合一型战斗机。亦即同一架飞机，能同时发

* Translated and reprinted by permission from *Air Force Magazine*, published by the Air Force Association.

挥数种飞机的效能，包括空中打击、电子攻击、指挥控制、战场侦察，等等。

奥布赖恩点出了一个有关空中作战的重要事实：第四代战斗机奔赴防守严密的所谓阻入 / 禁行（A2/AD）空域执行目标攻击任务时，需要各种配套支援："机载预警（AWACS）、电子攻击、巡弋护航、压制防空（SEAD），可谓林林总总。"这些挂载各式巡航导弹和设备的配套飞机，可能不下几十架才能形成组合。同样的任务，如果让 F-35 来承担，一个四机编队足矣。每一架 F-35，岂止是只能发动对地攻击；一组四机编队，能够奔赴任何需要空中力量的场合威震八方。换言之，F-35 本身就是一个着眼于未来打击任务的"高效组合"，成功几率高而"损失几率低"。

在隐身材料的可维护性方面，F-35 代表着现代最高水平，甚至令美国空军顶级优势战机 F-22"猛禽"相形见拙。F-22 需要定期维护，加覆昂贵的低显材料。与之相比，F-35 的隐身表面在任何环境中都极其耐用，优势显然，如奥布赖恩所言，"我们已将之提升到一个全新水平。"F-35 的隐身性亦值得称道，经过按照西方保密测试标准的雷达横截面试验验证，证明仅次于 F-22 而优于其它任何战机。

这种维护上的优势，部分得益于技术的先进性，在 F-35 上，吸收和分散雷达照射能量的导体材料是直接烘烤到飞机的多层复合蒙皮材料及结构之中。表面覆盖材料经历长期使用会逐步磨损，稍微减弱飞机的雷达显迹性。但只有在发生结构严重损坏的情况下，F-35 的低显性才会受到实质性影响。洛马公司已经研制出一整套现场修理技术，可以在几个小时之内全面修复飞机的隐身性。

隐身突破，势不可挡

F-35 的雷达横截面（RCS）具备一个"维护裕度"，意即"总是超过技术指标"。一些轻微刮伤甚至凹坑都不太可能实质性影响飞机的隐身质量而降低其作战效能。机场配备的设备可以做到直接在保养区检测飞机的 RCS，而过去要做这样的测定需要一大批笨重的设备。

洛马工程师在设计这款新型战机时，想到了飞机的一些通道口可能出现损坏，就是说，必须考虑到飞机的整个寿期内，这些出入口可能会安排在不同的部位上。于是设计者在机身上预留出多个通道，便于机场维修中如必要时在蒙皮上开口做出临时通道。其它隐身飞机如碰到这种情况，需要对这些通道口做胶合或封补才能恢复隐身性，由此耗费大量时间和成本。飞机低显性的修理和维护，一直是 F-22 的一个"重大技术难题，但 F-35 没有这种忧虑。"

F-35A 有一个蛇形入口，将发动机风扇叶片隐藏起来，确保从机身之外的任何角度都无法发现，由此解决了战机隐身设计中一个最大的 RCS 难题。另外，进气道用整片复合材料制造，没有任何焊缝、铆钉、固定件。这些部件都可形成巨大的 RCS 反射面，使上一代战机在雷达上留下巨大印迹，无可遁形。现在抹除了这些印迹，使 F-35 的隐身性能得到巨大的改进。不仅如此。F-35 机身表面没有任何突出的天线，它们都被埋置在机翼的前缘和后缘中。这样做不仅降低了飞机的雷达显迹性，还获得对整个战空更宽更深更精确的画面。

隐身性能必须"从最初就纳入设计考虑"，而不可事后补充或升级改造。这意味着雷达、电子战、数据链、通信，以及电子攻击等能

力必须“按部就班”，按照飞机机身的特殊形状和材料设计，从一开始就统筹兼顾。

F-35A 配有一套有源电子扫描阵列雷达，在机身周围还分布了独特的天线，可以精确指引雷达能量，使向非预定方向的“溢散”降低到最低程度。如此可聚集能量对准必要的方向,减少辐射耗散,避免暴露自己的位置。

并且，这款战机和其他 F-35 之间采用机器对机器通信。在飞行中，F-35 之间的雷达和电子战系统等发射体都可以闪开闪闭。例如，领队机可以叫其殿后机用雷达照射目标，其数据可通过激光动力多功能先进数据链分享，飞行员之间甚至无需语音交流。

为求隐身,燃料和武器都需要置于舱内。为美国空军研制的 F-35 版本即使满载作战负荷（燃料和导弹等），仍能做 9-G 机动。任何外挂武器和燃料箱的飞机都无法完成这样的动作。

其他国家飞机公司声称其所设计的第四代飞机能将雷达印迹减少 75%，奥布赖恩对此表示怀疑。他认为这种说法难以置信，因为它们的飞机的原始雷达印迹十分巨大，即便减去 75%，还能在雷达上留下强大回波。这些升级换代后的飞机，仍将暴露在对手的空对空导弹的最大射程之内。按照洛马公司这位官员的说法：“你基本上并没有在与对手交战的实际战术优势上做任何改进。”更糟糕的是，一旦本来“干净”的飞机挂载了那些非隐身的弹药、燃料箱等，原先费尽心机减少的 RCS 便统统前功尽弃。“除非你的飞机真正具备先机发现、先机发射、先机击中能力，你就还是只能待在防区之外，只能想着如何通过训练和战术手段来打败对手。”

中国和俄罗斯都已认识到，想从不具备隐身功能的旧机设计翻新出新一代隐身机，只能是一厢情愿。这也可以说明为什么中国和俄罗斯分别都在脚踏实地的从头研制 J-20 和 T-50(PAK-FA)。如果他们的研制取得成功，“我们的第四代战机必将处于严重的劣势。”

奥布赖恩认为，在现代 A2/AD 环境中，任何第四代飞机都无法生存，无论其获得的电子干扰支援有多强大。但是，在这样的环境中，F-35 可以比较安全地长驱直入，它能携带和 F-16 差不多的战斗载荷，但飞得更远。

在瓦解敌人的防空体系之后，隐身性能不再重要，后续 F-35 便可同时采用内置和外挂武器手段打击敌人，这样，其载弹能力可达到 18,000 磅，比 F-16 的 5,200 磅最大载弹量超出两倍以上。

奥布赖恩的总体评价是，F-35 是一款全方向隐身的全效能战机。

该省则省，存疑由人

在 F-35 的排气系统设计上，洛马公司充分思考了费效比的平衡,决定不选择 F-22“猛禽”所采用的二维推力换向喷管。原因之一是节省成本，原因之二是减轻对 F-35 隐身性能的维护。F-35 排气喷管所采用的是保密的“锯齿”环形设计，可将所有排气汇聚成一种所谓的“尖峰”（Spike）印迹。整个排气系统中还采纳了其他多项保密技术，以将发动机排气的热印迹控制在最低程度。

F-35 达到或超过了军方对热红外印迹的规范要求。在一般的标准战斗机发动机系统中，都有一个巨大的补燃器喷焰棒组件以及相关的管道，此部分在 F-35 中被省略。由普

惠公司为 F-35 研制的 F135 动力系统可以说是名副其实的“隐身”发动机。

外界对 F-35 的电子战和电子攻击（EW/EA）能力一直存疑，美国空军对此保持缄默，从不置评。但有专家指出，在美国空军最近的 EW/EA 能力建设规划中，没有提及专门的电子干扰战飞机。这是一项引人注目的省略。

奥布赖恩自然也不会详细解说 F-35 的 EW/EA 配置，亦不会提及此战机是否需要与专门的电子战飞机——例如 E-3 机载预警和控制机、RC-135“铆钉接合”、E-8“联合星”、EA-18G“咆哮者”电子干扰机——搭配作战。他只是承认，军方对 F-35 的性能需求规范中规定此战机必须做到能单枪匹马投入战斗而“不要任何［此类系统］支持”。“当然了，作为飞行员，自然是外部支援多多益善。然而，我们接到的性能需求规范中没有指示我们在这款飞机中配置任何与此类支援协调的功能。换句话说，这款战机不得不自己寻找发现目标…突破阻入空域…验证锁定目标…然后实施打击，一切必须独立完成。”

奥布赖恩进一步提醒说，还可以从海军陆战队的做法来推断 F-35 的 EW/EA 能力。海军陆战队“已经决定把 EA-6B［专用电子干扰机］清理掉，换成 F-35B 的基本型，”不需要加装任何外部吊舱或内部系统。至于空军如何做，奥布赖恩没有直接回答，而是技巧地以反问作答：“空军在投资建设庞大的电子干扰机群吗？”“空军在购置［EA-18G］“咆哮者”吗？”然后加上一句：“这些能力这里都有啦。”

奥布赖恩还说，F-35A 的电子战能力“能达到专门用于电子战的四代机，甚至更胜一筹。”F-35 的灵敏度和数据处理能力——其中大部分已经自动化——辅之以传感器与机载及非机载系统的融合，赋予飞行员前所未有的态势感知，以及发现、定位、锁定打击目标的能力。

至于 F-35 的电子作战能力，奥布赖恩认为这款战机将生成新的作战概念，其目标不只是压制敌防空体系，还要予以摧毁。如他所言：“我们想做的，不是每几个小时打掉一枚俄制先进地空导弹，而是把一枚 2,000 磅炸弹一下子砸到敌人的整个防空阵地上，一炸了结，再不用在战斗中担心还有什么来袭的地空导弹。”我军目前还难以做到这一点。我们的对手知道美国的 AGM-88 高速反辐射导弹配备轻型弹头，能给对手的一个个防空阵列实施不太严重的损坏。因此它们相应做出调适，为其移动防空系统加配了冗余阵列。我军列装 F-35 之后，希望能结束这种形势。

F-35 的隐身功能与 EW/EA 能力以及全天候自动化目标识别及定位结合起来，形成强大的作战效能，对敌人造成规模空前的常规“威慑”。

这款战机装备的 3.0 版自动目标识别软件不能把不同类型的作战坦克区分开来，但能够从各种类型机车群中辨识出地空导弹发射系统并将之拔除。

许多战斗机能发现和辨识出对手阵地的电子辐射，辅之以详细的合成孔径雷达图像，然后进一步导引打击机群袭击这些目标，而自己不被发现。F-35 的电子攻击能力更强一筹，能直接深入到“其他战机无法达到的空域”，故而“将对手的战略目标置于危险之中。”这些能力，为 F-35 所独有。

先机制敌，力免胶着

F-35 闯入敌方纵深空域之后，可以自动收集敌人兵力分布情报，并能像 E-8“联合星”那样，将地面运动目标处理成图像，通过数据链传递给己方部队。这意味着，F-35 将能够静悄悄地隐身传递情报，通知己方的天空和地面部队。

F-35 在设计上要求做到能在满载内置作战负荷的状态下机动到其飞行包线边缘，因此应能随心所欲地追赶包抄绝大部分战斗机，虽然在通常情况下无需发挥到这种极致。

“空战中，你如果希望将杀伤率提高到 1:1 以上，那么最好是避离对方。”奥布赖恩说这句话的意思是，为让自己毫发无伤，就必须和敌人保持一定的距离。如果卷入贴身盘旋格斗，即便是 1960 年代的 F-4 战斗机，也有可能在近距离将先进的四代机打下去，形成“胜负互见”。这就是为什么 F-35 配备了多来源信息传感器融合能力，能够与其他 F-35 互相配合，形成三角交叉，定位、确认和消灭敌机——在对方未及揿发射按钮之前。

F-35 配有 360 度传感器，甚至能够打掉“几乎完全在你身后的目标”。它还能询查处于自己身后的目标，这种能力在所有战斗机中独一无二。奥布赖恩认为，如果说战斗机能从现代格斗中存活下来，“那是因为你拥有先进的对抗手段，而不是因为你善于盘旋机动。”

如果万不得已进入盘旋格斗，F-35 也必能占先于其他任何战斗机，表明这款战斗机的敏捷性极佳。还有一点值得注意，在 F-35 潜在的未来升级版本中，空空导弹的载弹量将从目前的四枚 AIM-120 AMRAAM 提高到六枚。

以严格的技术标准衡量，F-35 不能算是“超音巡航”机，但是，它能保持 1.2 马赫速度直冲 150 英里，而无需启动耗油巨大的补燃器。对飞行员而言，1.2 马赫速度已经很够刺激。

这样的高速度，还顺便给 F-35 发射的炸弹和导弹等加力，就是说，这款战斗机能借助速度，将弹药“扔”得更远。

如果把飞行速度保持在 0.9 马赫的话，F-35 还能飞得更远。但是 F-35 的跨音速过渡性能可以说卓越绝伦，“它能轻而易举地穿越 1［马赫］，”而如何“穿越跨音速区大有讲究。”

最后一点，在战斗配置上，F-35 的航程比四代机超出 25%。奥布赖恩说，这只是空军公布的数据。“我们其实是把 F-35 和四代机中的最高档机相比较，”F-35 能在飞行包线的任何区域把对手轻松比下去。♣

空军后备役单兵动员增补现役计划：目前的组织结构是否可行?

The Air Force's Individual Mobilization Augmentee Program: Is the Current Organizational Structure Viable?

罗萍·G·斯尼德，美国空军后备役上校（ Col Robin G. Sneed, USAFR）
罗伯特·A·基尔默，美国陆军退役中校 / 博士（Lt Col Robert A. Kilmer, PhD, USA, Retired）

空军后备役的单兵动员增补现役（IMA）计划是为着在空军需要作战兵员支持时，提供经训练、懂装备、能打仗的后备役队员。“沙漠风暴”行动给后备役带来重大变化，这种变化至今影响着这项计划。他们是后备役队员身份，但被分配到现役部队而不是后备役部队，这使得他们所处的组织结构不仅独特，而且经常令人困惑。由于一个组织的配置可以显著地影响其支持行动和任务的能力，人们有理由质疑空军目前 IMA 计划的指挥结构的可行性。本文使用了斯塔福德·比尔（Stafford Beer）可行系统模型作为分析工具来检查该结构。[1] 文中的评估方法着重探讨如何优化 IMA 编员的管理，确保增强危机时期的战备能力；该评估方法还有助于满足后备役队员的合理预期，确保空军将按照他们的专业训练背景安排他们到适合的岗位，保证他们的角色符合一体化“全志愿部队”的原则。

单兵动员增补现役计划下的编员

单兵动员增补现役计划即 IMA 计划能够在国家面对战争或危机之时，立即提供 IMA 计划下的编员扩充现役部队，为此，该计划提前将后备役队员分配到到现役部队中参加

训练。IMA 编员经过训练而熟悉该现役部队的人员和结构关系，一旦现役部队提出紧急增补需求，IMA 编员就能立刻补入现役，独当一面，而无需临时花费数周或数月时间参加训练。后备役支持现役这个概念从后备役部队于 1948 年启动以来一直是空军的一个组成部分，当时的空军防空司令部司令乔治·斯特拉特迈耶中将就曾将后备役队员分配到关键指挥岗位，作为实习人员加以培训，一旦启动总动员时就能招之即用。[2] IMA 概念虽然在和平时期经常受到质疑，但自上次总统依据美国法典第十卷条文启动 IMA 计划之后，IMA 编员在“沙漠盾牌”/“沙漠风暴”行动中有力地支持了现役部队。目前，通过志愿转现役，IMA 计划为空天远征部队和其它任务的部署，提供以出征日 / 人计量的现役支持。[3]

空军将 IMA 编员定义为“填补被认为能够增扩国防部现役部队或者美国政府其它机构与部门的军事岗位的个人。”[4] 对 IMA 编员的作用，虽然普遍看法上一直是将之作为一种候补角色，但是实际批准的使用已扩大到包括:战争动员、应急行动、特种或技术需求，甚至是经济方面的考虑。[5] 同大多数后备役队员一样，IMA 编员必须投入一些时间服现役，通常每年 30 天，其主要军事责任是满足空军动员的需要。对后备役队员及其现役上司来说，这意味着必须保持满足本军种的体能锻炼、医疗和牙科检查、密级审查等要求以及专业代码训练要求，并将所有训练和检查记录在案；还可能需要达到具体司令部和具体部队的训练要求。

对现役上司及指挥官而言，现役部队中夹入来自后备役的兼职战士，管理上势必面对独特的挑战。这些兼职战士的某些方面，如入伍训练日期灵活，拥有独特的民用技能等，对部队是有益的；但他们的档案更新和表现考评等事务有所不同，对即使是最认真的上司来说，也是个难题。而且每个部队有自己的任务重点和优先，有时不免忽视对这些 IMA 编员的训练和支持。因此，IMA 编员经常必须采取主动，自己安排训练和现役活动，自己管理本人前程。有人将“IMA”戏谑为“I'm alone”（独来独往）的缩写，其实也反映了后备役队员哭笑不得的苦衷。

尽管有这些困难，IMA 计划继续存在，指挥官也总是设法为入伍的后备役队员安排适当的训练以支持部队的目标。只要做到人尽其用，后备役中的专业人才经过适当训练，应能弥补现役部队中的不足。空军可以利用他们的民用技能和经验，解决现役部队的技能缺口。此外，IMA 编员定期来现役部队训练，同时带来新的视角和非常规的观点，有助于克服一成不变的群体思维，帮助发现新的解决方案。说实话，一个人如果在现役中是一名优秀的 IMA 编员，他在其它方面也会有所作为，因为他带着以“公民战士”身份支持国防的责任感，知道如何把握好公民战士责任、民间工作责任和家庭责任三者之间的平衡。随着现役成员的数量持续下降，IMA 编员在自己的社区和企业中，逐步代表空军的形象。

单兵动员增补现役计划的组织结构

由于 IMA 编员是分配到现役部队的后备役队员，无论是后备役部队还是主要司令部的组织层次，都难以有效地管理这项计划。于是，这项计划的责任被切割开来——主要司令部负责作战控制，空军后备役司令部负责行政控制。[6] 作战控制的责任是指定目标、分配任务、组织和运用部队直接支持作战任务，此权限可下放给下级部队，但不能超出

主要司令部以外。[7] 行政控制的责任包括管理薪酬、物流、人事等方面的支持和行政职能。这样的责任分工虽有其道理，但也造成问题，因为同一个 IMA 编员的档案却被分拆到两个独立的数据系统中，一个是后备役部队数据库，另一个是现役部队数据库。对这两个系统的对接虽然做了大量的协调努力，结果却不尽人意，错误和矛盾时有发生。

在动员和派遣 IMA 编员参加“沙漠盾牌 / 沙漠风暴”作战行动的过程中，就发现了两种人事跟踪系统之间的一些断裂，也指出了哪些地方需要改进，是以帮助空军后备役司令部加强对其后备役队员在现役部队中的表现的跟踪。此后，政府问责局也进行过审核，指出了 IMA 计划在哪些方面符合公共法律，以及国防部和空军的规章在哪些方面需要调整。为解决这些问题，空军后备役司令部司令约翰·布莱德利将军于 2005 年成立了一个“战备管理部”，该管理部直接向空军后备役副司令报告，负责将“战时就绪”的后备役部队无缝整合到空军的任务之中，支持各种稳态行动和应急行动。[8] 战备管理部通过一名 IMA 计划总监（上校衔）和其领导下的 19 个分队，来跟踪空军内 8,000 名 IMA 编员的战备情况（图 1）。由于后备役和现役部队的跟踪和管理系统不兼容，许多行政控制

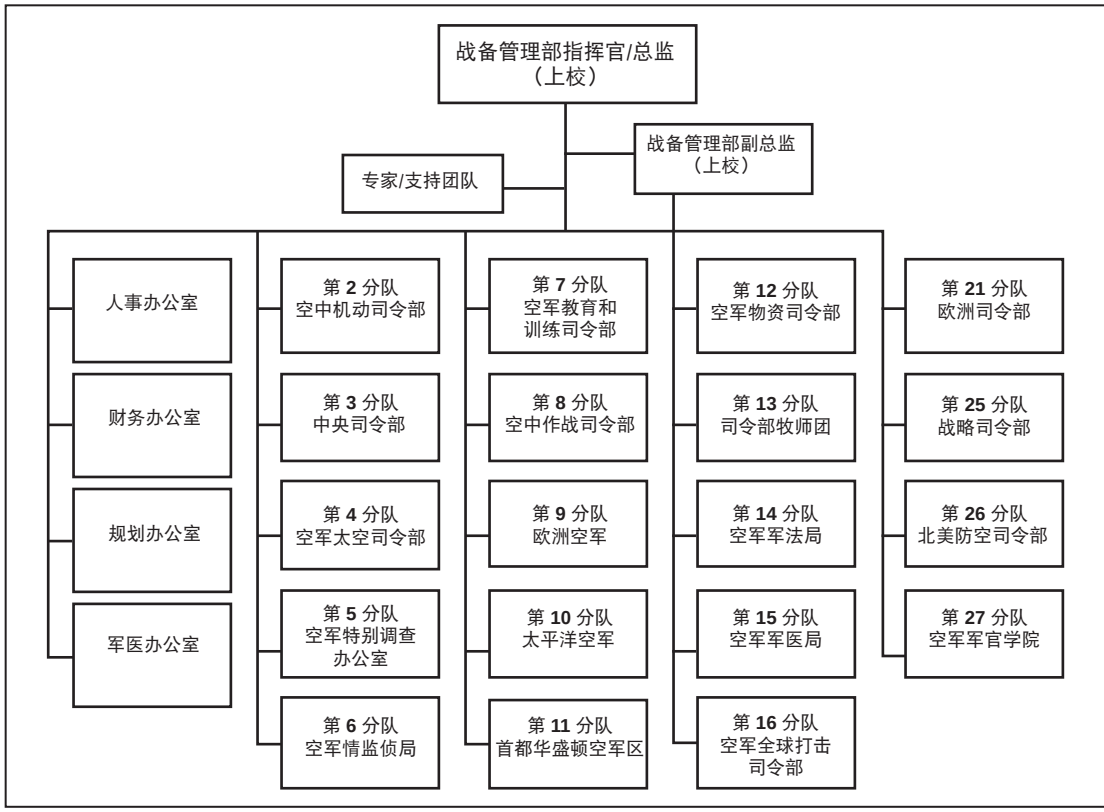


图 1：战备管理部的组织结构。（改编自 CMSgt James R. Pascarella, “Readiness Management Group Overview”［战备管理部简介］, PowerPoint presentation [Robins AFB, GA: Air Force Reserve Command, 19 October 2011], 23.）

功能已成为共同的责任，主要司令部实施行动，后备役司令部负责跟踪。这些职责还包括战备、动员、训练、纪律和人事管理。[9]

可行系统模型

斯塔福德·比尔在二十世纪八十年代开发出一种“可行系统模型”，用于评估和诊断组织结构，此模型帮助了各类企业更好地理解和优化企业管理。[10] 这是一个运用组织控制论的详细而优雅的模型，可以跟踪一个复杂企业的相互作用和关系，为一个组织确定必要和充分的子系统，使其能够自我调节和独立存在。[11] 管理者通过检验这些系统——指定的系统 1、系统 2，系统 3 和 3*、系统 4、系统 5——能够确定其组织的可行性，并查出缺陷（图 2）。

图中各组成部分的定义如下：

- 系统 1 的作用是实施组织的目标，直接提供商品或服务，这类系统代表组织的主要部门，这些部门每天与环境对接，并创造该组织的价值。[12]
- 系统 2 的作用是协调系统 1 各部门间关系，平衡输出，实现一致，减少振荡。[13] 作为一种管理功能，它保证运作顺畅，并且充当信息渠道，允许系统 3 来管理作为模型中各组成部分的系统。
- 系统 3 涉及当前组织的行动计划和控制，通过建立规则、平衡资源和优化形势，将所有系统 1 整合到一个连贯的企业之中。[14] 系统 3 并与系统 4 和系统 5 一道，提供监督管理功能。
- 系统 3* 是一种选择性的审核和监督功能，它协助系统 3 管理系统。[15] 此操作向系统 3 提供无法在系统 2 持续获得的具体和详细信息，以满足系统 3 的需求。
- 系统 4 作为该组织的战略规划部门，负责长期项目的制定开发，以及组织的“外部和未来”界面。它直接与环境互动，预测未来的发展趋势，并且规划当前和未来状态的整合。[16]
- 系统 5 提供全面的组织政策，平衡当前和未来的行动，并确定该组织的身份和文化。[17] 它通过平衡系统 3 和系统 4 的计划来完成此任务。

可行系统模型的另一基本方面，涉及其重复和嵌套特性——即任何可行系统包含并被包含于一个可行系统。[18] 此特征使管理者能够以相同的方法和工具，锁定组织的每个

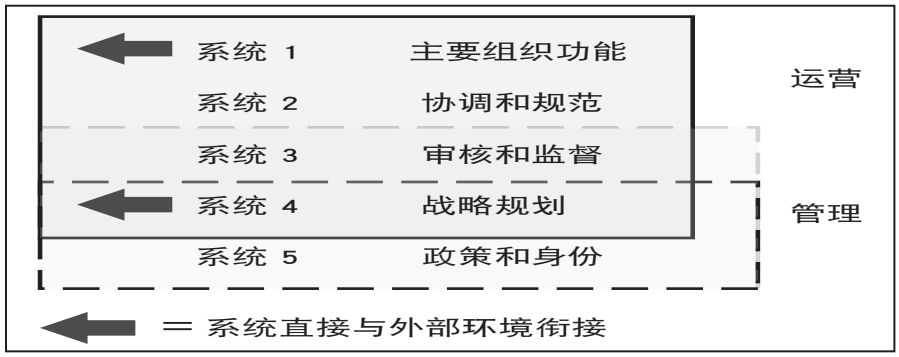


图 2：可行系统模型所需的组成部分

递归层。在不影响企业固有复杂性的情况下，研究人员能够锁定并且简化一个组织，以增加模型之实用价值的方式进行分析。

利用该模型来分析某组织需要三个步骤：

1. 确定递归层级和选择拟分析的层级（焦点系统）。
2. 定义焦点系统的目标和身份。
3. 分析焦点系统，了解其必需的子系统 1—5 以及必要和充分的元素。[19]

把这些步骤应用到对 IMA 计划的分析，可以确定此计划面对变化时是否仍然可行，并指出优化该计划需采取哪些行动，从而对后备役和现役空军都改进指导意义。

模型的应用

按照上述步骤，并且借鉴空军的规章、组织和任务简报、高层领导人的出版物，以及本文主要作者管理空军 IMA 计划 20 年的经验，我们使用可行系统模型来评估 IMA 的组织结构。第一步是选定一个焦点系统供分析。我们选择了空军这个军种层级作为合理的边界，因为空军承担主要司令部和后备役司令部的共同责任，最好地涵盖了此计划的范围和领域。我们没有选择国防部的 IMA 计划作为分析对象，觉得过于宽泛；我们也没有选择 IMA 编员的上司，即系统 1 部分，觉得过于狭窄，难以在此层级上形成有意义的分析。

在空军层级上，IMA 计划的目标和身份是组织、训练和维持后备役队员，保证他们能迅速扩编到现役部队。通过高层领导的监管和支持，IMA 计划已成为重要的人力储备资源，随时向空军提供战时能力、专业技能，以及动员期间现役部队的连续性。[20]《战备管理部单兵后备役指南》要求 IMA 编员：在和平时期的主要任务是保持良好战备状态，包括达到空军规定的训练、体能锻炼和身体健康要求，确保随时接受动员。[21] 基于这些来源，空军的 IMA 计划必须为参加 IMA 计划的后备役队员配备必要的组织、训练和装备条件，使他们能够在国家面临危机、紧急状态和战争时能立刻加入现役保卫国家。[22]

分析的连续性要求检讨“焦点系统”的必要的和充分的系统。以下各节描述分析的结果（见下表），以实例来说明各项发现，并指出任何不足之处。

主要运作——系统 1

IMA 编员的上司根据空军 IMA 计划指示这些后备役队员参加哪些主要活动，保证他们在需要时能立刻增补到空军现役，及确保达到所有动员要求并保持文件齐备。[23] 这些上司是常备部队的成员，可能是现役身份也可能是文职身份，被指定管理数量有限的 IMA 编员（通常仅一到两个人），作为一项额外的责任。这些上司中很少有人真正熟悉现役和后备役在文件要求上的差异，因此只能从后备役队员了解 IMA 计划的细节要求。

虽然 IMA 编员的上司身为专业军事工作者能认真履行这份职责，并努力满足所有要求。[24] 然而障碍处处存在，因为后备役队员一般每年在现役部队的时间只有 30 天，而其上司必须全力处理每天的日常任务。此外，现役军人配有各种现成的手段和提示工具，诸如军官 / 士兵定期表现报告文件夹等，IMA 编员则可能没有。这些上司可以借助一些资源来完成这份职责。经常，位居这名上司之上的某位后备役队员——通常称为资深 IMA 编员——可能被要求承担起额外任务，即帮助所述之 IMA 编员及其上司处理好和 IMA

空军后备役司令部 IMA 计划可行系统模型之各系统					
系统 1 主要运作	系统 2 协调和规范	系统 3 作战控制	系统 3* 审核和监督	系统 4 战略规划	系统 5 总体政策
编员的上司	现役报告系统	主要司令部	战备管理部（空军后备役司令部）	无	空军后备役司令部
	后备役报告系统				
	国防部指令 / 空军指令				

计划要求相关的问题。这支部队也可能指定专人管理 IMA 编员的档案记录。战备管理部属下各支队和基地 IMA 管理员也可以负责回答相关疑问，为这些上司和 IMA 编员提供指导。[25] 但是，IMA 编员由于身份独特，常常必须自行解决某些问题。如果这名 IMA 编员本身不太主动，缺乏条理，没有能力就这项计划向相关人员解说清楚，就可能导致效果不好，最终离开 IMA 计划。图 3 列出 IMA 计划管理的多层复杂组织结构。

协调规范——系统 2

管理 IMA 编员的协调渠道，主要包括医疗和牙科检查、体能锻炼、密级审查，以及军事训练完成情况的跟踪系统。IMA 编员及其上司还需访问浏览的其它系统，包括订单生成系统（空军后备役订单书写系统）和上岗排程系统（部队训练集合参加系统）。由于 IMA 编员是被分配到现役部队，指定岗位（部队配员文件）和指定上司也很重要。和执行 IMA 计划相关的空军规章也构成系统 2 的一部分。

由于常备部队和后备役部队系统之间的隔离，现有的协调和跟踪工具一再表现为低效。使用者对系统不熟悉，常常导致系统信息断裂，输入出错，延误了问题的识别与解决。还有，空军后备役司令部所跟踪的数据必须首先送达主要司令部，然后再下发给 IMA 编员的上司，这个过程也造成耽搁。再者，有两个趋势会影响协调系统：一个是 IMA 编员的数据自我报告，另一个是战备管理部对战备状况的监督。IMA 电子系统每次升级，几乎都要求 IMA 编员在没有和所分配部队协调的情况下，直接输入战备数据。与此同时，战备管理部试图使主机系统数据相关联，以跟踪 IMA 编员的战备状况。这两个处理过程截然相反，导致两种不同的结果。此外，这两种趋势将 IMA 编员的上司和其部队单位排除在信息渠道之外，导致管理和协调低效。

这些趋势也是最近发生的几起协调失误的原因之一。例如空军后备役司令部在 2010 年 5 月更新了 IMA 编员值现役岗的批准程序，并把信息发送到各分队要求下达到相关人员。但是因为该数据与作战控制相关，各分队便没有传达给相关的 IMA 编员或者上司。因此在过渡到新程序那天，三分之二的 IMA 编员不符合要求，主要是因为他们不知晓程序的变化。另一个例子是，空军前些时候发出指示，要求所有现役和后备役人员参加“不问，不说”军队同性恋政策被废除后的相关培训，这项行动要求发给了 IMA 编员的上司。遗憾的是，由于时间的限制，那些当时不值现役岗的 IMA 编员常常被遗漏，而

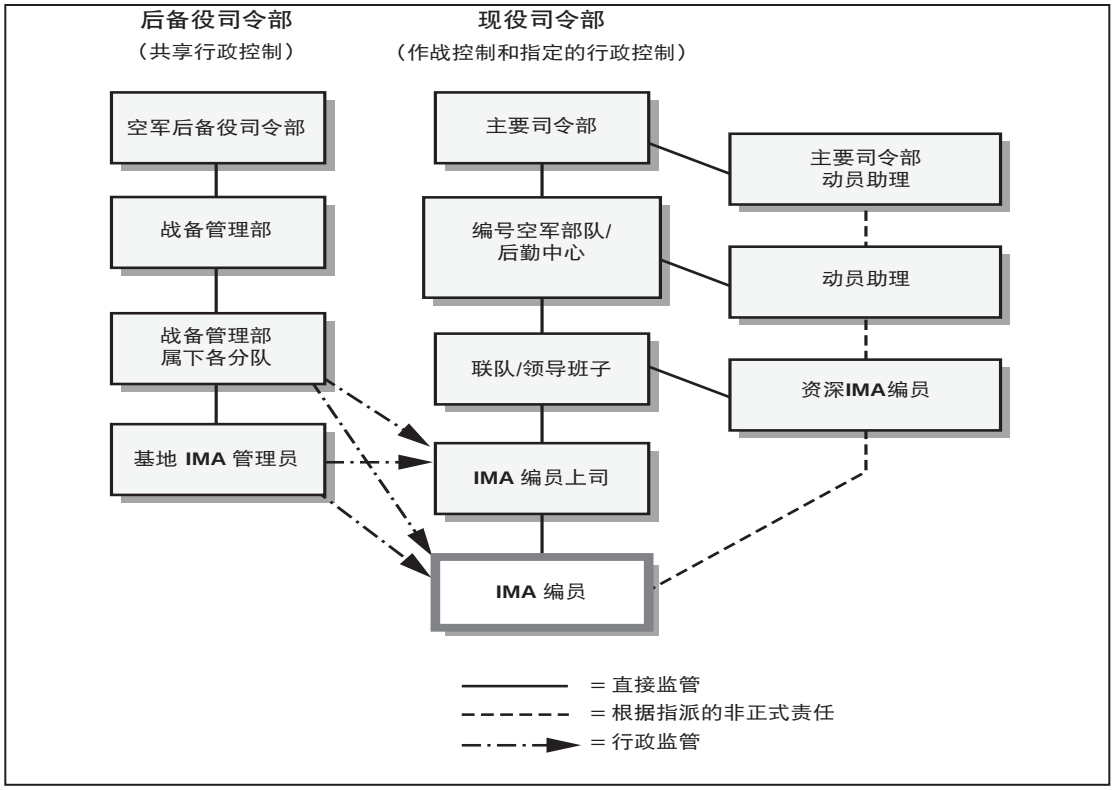


图 3：IMA 组织结构图（数据来自 Air Force Instruction 36-2629, Individual Mobilization Augmentee Management [空军指令 36-2629：单兵动员增补现役管理], 10 December 2001, http://www.e-publishing.af.mil/shared/media/epubs/AFI36-2629.pdf; 另参看 Readiness Management Group, Readiness Management Group Individual Reserve Guide [战备管理部单兵后备役指南], Robins AFB, GA: Air Force Reserve Command, March 2008, http://www.afrc.af.mil/shared/media/document/AFD-080408-050.pdf.）

那些完成了这项培训要求的人中，又有些人无法把完成信息录入现役跟踪系统。直到最终报告上报期限将至的前几天，现役部队才发现有些 IMA 编员没有完成此培训，而培训完成率不达标将严重影响部队合规评比，最后只好将 IMA 编员的培训上升为一项紧急优先。[26] 战备跟踪系统的故障和信息断裂给 IMA 编员的上司增加了压力，并影响空军对 IMA 计划价值和管理能力的印象。

运作控制——系统 3 和系统 3 *

IMA 编员数量相对较少，使得大多数主要司令部能够在总部层级通过后备役顾问办公室行使对这些人员的作战控制。这个过程由分配给主要司令部司令作为其动员助理的 IMA 编员协助执行，这些助手肩负着行政层级的职责，互相协作，在主要司令部之间协调 IMA 计划。此外，由于 IMA 编员的档案包括在现役部队的行政档案管理系统之内，而不是后备役所使用的系统之内，后备役司令部必须与现役部队共享行政控制责任 。这些共享的责任包括前面提到的战备、动员、

训练、纪律和人事管理，要求主要司令部正确实施，以及后备役司令部跟踪正确遵守情况。[27]

有关主要司令部 IMA 计划总监的规定和做法都有模糊之处，给作战控制带来了不利影响。在组建战备管理部之前，分配到主要司令部的 IMA 计划总监曾被列入作战控制的指挥链之内。当空军手册 36-8001《后备役队员参与和训练程序》在 2010 年更改为空军指令 AFI 36-2254《后备役队员参与》之后，这个职位转换为战备管理部计划总监，该项调整将职位的权限转入行政控制的指挥链中。但这种更改和由此产生的变化并没有被清楚地识别并包括到上述规定之内。此规定将任务分配给了“指挥官 / 战备管理部计划总监”，这意味着两人中任何一人都可以授权某特定任务（依据作战控制和行政控制的权限）。[28] 这是模糊和混乱的，明显违反了作战控制和行政控制的组织结构要求。

作战控制的另一个组成部分，即系统 3* 审核和监督功能，被确定为后备役司令部的战备管理部及其各分队的职能。基地的 IMA 管理员，即基地层级的 IMA 支持环节（战备管理部的一部分），发挥着向所分配部队、后备役司令部和 IMA 编员提供人事及战备咨询的顾问作用，还就后备役队员的正确使用和管理向指挥官及 IMA 编员的上司提供各种指导。[29] 正如前面提到的，战备管理部主要监督和跟踪行政控制共享责任的执行。 战备管理部与 IMA 编员及其上司保持直接互动，战备管理部的组织结构——具体来说由上校衔军官担任计划总监的做法——实际上意味着自治，而这样做不符合该组织的授权规定及其行政要求。[30] 此外，上校在战备管理部中担任副职违反空军指令 AFI 38-201《人力资源管理的要求与授权》，该指令禁止这种做法。[31] 虽然我们可以找到理由来要求豁免执行此空军政策，但现役部门对支持机构这种做法所带来的负面解释，将有损联合行动。如果战备管理部的组织结构与空军政策相符合，对该计划的看法能够得到改善。

战略规划——系统 4

本文的分析无法在空军 IMA 计划中找到属于系统 4 的功能，即战略规划功能。空军总部的后备役总监负责整体的 IMA 管理政策，但空军指令 AFI 36-2629《单兵动员增补现役管理》没有提到应由哪个下属机构负责 IMA 长远规划。后备役司令部总部的明确责任只是负责 IMA 编员的招聘、报酬和住宿报销。虽然后备役总监的动员助理被指定负责 IMA 计划的宣传，但是长期战略规划的概念并不存在。

同样，主要司令部和机构也没有负责 IMA 计划的战略规划部门。AFI 36-2629 要求这些组织支持现在成为战备管理部各支队之一部分的 IMA 计划总监，并参与有关司令部管理层次的验证和拨款过程，以确保随时提供训练有素战备完好的后备役队员。主要司令部人力资源办公室负责处理由下属部队提出的、必须由后备役司令部批准的 IMA 现役岗位请求。后备役司令部的顾问办公室负责实施 IMA 计划，但是不负责处理空军层级的 IMA 计划规划。由于没有指定统一的部门来制订或实施长期 IMA 计划的目标，各司令部和机构仅提供战役层次的支持，而不提供战略计划层次的支持。因此，基于本文观察，空军 IMA 计划中不存在系统 4 的成分。

总体政策——系统 5

根据空军指令 AFI 36-2629，空军后备役司令部——负责 IMA 计划政策的组织——

负责全部后备役资源（包括 IMA 编员）的整体管理政策。空军总部的后备役总监一职由空军后备役司令部司令担任。此外，后备役司令部将 IMA 计划视为自己的责任之一，并将该计划包括在正式任务简报中。最后，空军现役人员通常都将 IMA 计划与空军后备役联系在一起，因为 IMA 编员都是后备役队员，而不是现役空军。

然而，作为一个实际问题，IMA 计划以及 IMA 编员的正式身份没有得到很好的理解。IMA 编员的上司和指挥官将 IMA 编员看作是本单位资产，因为他们被分配到了这支部队。后备役司令部也视他们为后备役储备资产，因为他们是后备役队员。相关规程支持这种身份的分裂做法，一方面规定由主要司令部提出 IMA 现役岗位申请和理由，另一方面把最终的批准、拒绝和拨款权限留给了后备役司令部。大多数现役空军军人根本不考虑 IMA 编员的正式身份，或者是因为他们相互之间并没有大量交往，或者是因为 IMA 编员已经完全融入到现役部队中，以至于部队成员没有注意到这些战友的独特身份。与此同时，国防部 2011 年的《后备役部队未来作用的全面审查报告》将每个后备役队员认定为未来后备役的重要组成部分。[32]

因此，在空军努力实现作战后备役目标的过程中，仍需解答一个重要的问题：谁来决定 IMA 编员的技能要求和贡献？后备役是否应该评估整体空军的需求，并且让主要司令部来训练和管理这些资源？还是应该由主要司令部确定对这些编员的需求，并让后备役司令部继续提供跟踪和行政支持？战争性质在不断变化，充满令人不安的政治和经济前景，在目前这样的环境下，这个基本的身份问题可能影响 IMA 计划的长期可行性。

关系，连接，分析结果

本文的分析表明，空军 IMA 计划的组织结构是不可行的，因为它不包括“比尔模型”中所有必要的子系统。具体来说，就是缺少战略规划组成，即系统 4；而系统 5 塌陷并混淆到系统 3 中；另外，组织机构只能对环境变化做出被动反应，而不是预期和规划结构化的转型。[33] 本分析还确定了其它两个重要的问题。第一，在处理 IMA 编员身份方面有功能缺陷，这是系统 5 的问题，涉及到 IMA 计划不明确和模糊的性质。第二，现役与后备役系统之间缺少充分兼容，数据系统向不同方向移动的倾向使得管理信息渠道断裂和低效。如果不做组织修复，IMA 计划将沦往无法支持空军使命的地步。

建议

我们通过审视 IMA 计划结构，发现了一些问题，认为这些问题可能削弱其未来的成功以及对空军的价值。我们运用可行系统模型取得一些分析结果，有助于解决这些问题及实施四项主要行动：(1) 确定并传达正确的 IMA 编员身份（系统 5）；(2) 建立战略规划部门（系统 4）；(3) 将战备管理部的组织结构据其职责使命调整（系统 3）；(4) 改进通信和信息渠道（系统 2）。落实这些建议，将有利于 IMA 编员的上司（系统 1），尽管本文分析无法确定这方面的具体改进措施。

空军总部必须主导解决 IMA 编员身份混淆和战略规划缺失的问题。首先，空军总部需要界定和以政策文件方式确定后备役队员在未来空军中的作用。对后备役部队未来作用的分析已于最近完成，因此空军只需要审查和确定对 IMA 编员的预期角色和作用。[34] 第二，空军总部应该给后备役总监增加 IMA

计划之战略规划的责任。还有，空军需将这些信息传达至所有相关部门——空军后备役司令部、所有主要司令部、相关作战部队、IMA 编员的上司和 IMA 编员本人——这个传达和理解过程可能费时但并不困难。IMA 编员都是兼职战士且十分分散，把空军的政策和计划传达他们将比通常要更长一些（例如，两到三年）。通过有效传达连贯一致且长期有效的信息，将有助于重振 IMA 计划，提高此计划对空军的贡献。设定战略规划责任，将支持后备役司令部司令施坦纳中将的愿景，这就是将后备役转变成一支战役性的、费效比高的、战力增强的部队。[35]

调整 19 个分队的军阶结构，由中校而不是上校担任计划总监，这样做将有效地调整战备管理部更匹配其行政控制职责。这一变化对办公室管理工作影响不大，因为中校军官完全有能力管理这种规模的群体，但它将改变现役人员和参谋人员对此任务的看法。毕竟上校与中校不同，上校通常被认为具备自主权限，是政策的构建者而非简单的执行者。既然战备管理部负责管理和跟踪后备役的战备状况，就应该在所有分队实施标准做法而非各行其是。况且中校级别作为空军后备役的有效代表已经足够，因此，任何失误不会被认为是 IMA 计划本身的缺陷，而只是人事的问题。这样，战备管理部的副职可转而负责分队管理，消除安排上校担任副职而违反空军政策的负面印象。

再者，空军应该认真检查 IMA 计划使用的信息系统和通信渠道，发现其中的问题，进行现代化升级，并将此任务提到优先日程。为不妨碍日常运作，也因为经费不够，全面升级或更新虽不现实，但是检查和记录系统中的问题仍有必要。发现问题之后，就能标记出信息系统中的明显断裂，未来有机会升级时便可加以改正，现行运作中也可考虑如何变通避让。项目总监和承包方在考虑与 IMA 计划相关的沟通时也必须改变自己的观点。由于现役和后备役数据系统都记录 IMA 编员的信息，而现役部队的战友们可能不注意他们的身份，因此，规划和实施的所有方面，都应该认识并考虑这些后备役队员的独特要求。IMA 编员长期担当传统的兼职角色，发挥他们的才能必能提升任何信息项目团队的能力。实施本文的这些建议将解决可行系统模型分析所发现的问题，并改进 IMA 计划的组织结构，以继续支持空军的使命。

目前的 IMA 计划虽然并没有设计为作战后备役，只要稍加调整，就能成为这样一支队伍。得益于现行法规的灵活性而获得充分发挥的组织早有先例。以空军后备役弹药团队为例，这个组织是 1990 年代初作为解决一个困难问题的独特方案而设立的。1993 年，“批量弹药储备计划”报告发现，空军弹药储存的 25% 低于可使用状态标准，参战弹药的战备完好率也有所下降。空军领导层判定，这种情况归咎于国防部军需品仓库的归并和整合，以及另一个原先未认识到的现实，即空军弹药不同于子弹和哑弹，需要定期检查和升级。由于这项任务要求特殊的弹药技能，但现役或后备役都没有为之设立全职支持部门，所以空军为此建立了一个 IMA 结构。空军装备司令部的弹药供给部门得到授权，IMA 编员被派往不同地点的仓库接受培训。由于弹药管理所具有的团队工作性质，团队成员和团队主管都由 IMA 编员担任，获得培训后负责管理无用弹药库存，使前线将士和整个空军都直接受益。

随着时间的推移，空军后备役弹药团队的技能和能力成为“全球弹药控制节点”经常倚重的选项之一。全球弹药控制节点是现

役组织，负责整个空军弹药的分发和储备。自空军后备役弹药团队创建以来，团队志愿成员积极响应动员，在“沙漠风暴”期间支持弹药需求，参与核储备管理，以及其他力所能及的弹药工作。这支后备役弹药团队的规模和组织使得它能够在符合 IMA 的规定的同时，满足空军和平与战时的应急需求。[36] 在过去的二十年中，这个团队将超过 30 亿美元的弹药修复后又返送到前线，并于 2009 年创出了 230% 的投资回报率。启用这些后备役队员参加动员前的各种任务，如弹药分发，并发挥他们支持当前作战需求的能力，为空军创造了独特的价值。在纠正了那种视 IMA 编员为补缺或候补角色的普遍观点之后，后备役弹药团队的潜力得到挖掘，为整个空军的弹药维持需求提供了重要的且费效比高的支持。其他的 IMA 计划，包括承包或修补空战损伤等工程，都可以很容易地采纳类似于后备役弹药团队的组织结构。通过使用这种经过验证的组织方式，空军后备役司令部和各主要司令部领导人可以实现斯坦纳将军所提出的战役性单兵后备役计划的愿景。

结语

国防部依靠后备役协助应对未来国家安全的挑战。面对经济和政治束缚，军队需要优化所有的计划，以实现最大的效益。在后备役从战略后备向战役后备过渡的大环境中，IMA 计划仍然继续支持空军的使命。使用可行系统模型来分析空军 IMA 组织，我们发现，它缺乏一个长期、可行的结构，具体表现为这个计划身份不清，缺乏战略规划要素，以及信息渠道效能不高。然而，如果高层领导能加以重视，主导一些细微的调整，就能改进 IMA 计划的功能，从而保证 8000 名公民航空兵保持战备，随时听从召唤，在国家面对战争和危机时有效地支持空军。♣

注释：

1. Stafford Beer,“The Viable System Model: Its Provenance, Development, Methodology and Pathology”in The Viable System Model: Interpretations and Applications of Stafford Beer's VSM [《斯塔福德·比尔可行系统模型之阐释与使用》中“可行系统模型：起源、发展、方法论和病理学”一章], ed. Raúl Espejo and Roger Harnden (Chichester, UK: J. Wiley, 1989), 11-37.
2. Roma K. Simons and Lyn Hellwig, History of the Individual Mobilization Augmentee Program [单兵动员增补现役计划历史], (Lowry AFB, CO: Air Reserve Personnel Center, 1991), 5-6.
3. Lt Gen Charles E. Stenner, Total Force Policy 21: A 21st Century Framework for Military Force Mix Decisions, [二十一世纪全员部队政策：二十一世纪的军队混编决策框架], Air Force Reserve White Paper, (Washington, DC: Air Force Reserve Command, 15 July 2010), 3-4, http://www.afrc.af.mil/shared/media/document/AFD-101202-018.pdf.
4. Air Force Instruction (AFI) 36-2629, Individual Mobilization Augmentee Management, [空军指令 AF I36-2629：单兵动员增补现役管理], 10 December 2001, 17, http://www.e-publishing.af.mil/shared/media/epubs/AFI36-2629.pdf.
5. AFI 38-201, Management of Manpower Requirements and Authorizations, [AFI 38-201：人力资源需求与授权管理], 26 September 2011, 36, http://www.e-publishing.af.mil/shared/media/epubs/AFI38-201.pdf.
6. 见注释 4，“AF I36-2629：单兵动员增补现役管理”；另参看 Readiness Management Group, Readiness Management Group [RMG] Individual Reserve Guide [战备管理部单兵后备役指南], (Robins AFB, GA: Air Force Reserve Command, [March 2008]), 7, http://www.afrc.af.mil/shared/media/document/AFD-080408-050.pdf.
7. Readiness Management Group, 2010 AFRC Readiness Management Group Strategic Plan [2010 空军后备役司令部战备管理部战略规划], (Robins AFB, GA: Air Force Reserve Command, April 2010), 13.

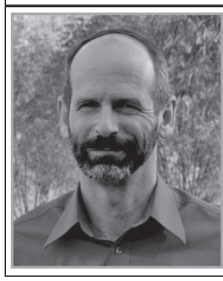
8. CMSgt James R. Pascarella, “Readiness Management Group Overview”[战备管理部简介], PowerPoint presentation (Robins AFB, GA: Air Force Reserve Command, 19 October 2011), 2.
9. 见注释 7，第 13-14 页。
10. Benjamin GmÜr, Andreas Bartelt, and Ramon Kissling, “Organization from a Systemic Perspective: Application of the Viable System Model to the Swiss Youth Hostel Association”[组织之系统观：瑞士青年旅舍协会可行系统模型的应用], Kybernetes 39, issue 9/10 (2010): 1627-44, doi:10.1108/03684921011081204; 另参看 José Pérez Rios, “Models of Organizational Cybernetics for Diagnosis and Design”[用于诊断和设计的组织控制论模型], Kybernetes 39, issue 9/10 (2010): 1529-50, doi:10.1108/03684921011081150; 另参看 Markus Schwaninger, “Design for Viable Organizations: The Diagnostic Power of the Viable System Model”[设计可行组织：可行系统模型的诊断能力], Kybernetes 35, issue 7/8 (2006): 955-66, doi:10.1108/03684920610675012.
11. 见注释 1，第 21-26 页。
12. Dr. S. M. Burnett and Col G. A. Durant-Law, “Applying the RAAAKERS Framework in an Analysis of the Command and Control Arrangements of the ADF Garrison Health Support”[应用 RAAAKERS 框架分析澳大利亚国防军驻军基地健康保障的指挥与控制], Journal of Military and Veterans’ Health 17, (2008): 24-25; 另参看注释 10 中 Rios“组织控制论模型”文，第 1531-32 页。
13. 见注释 12 中 Burnett and Durant-Law “应用 RAAAKERS 框架分析”文，第 24-25 页；另参看注释 10 中 Schwaninger “可行组织设计”文，第 955-56 页。
14. Allenna Leonard, “The Viable System Model and Its Application to Complex Organizations [可行系统模型及其在复杂组织中的应用], Systemic Practice and Action Research 22, no. 4 (2009): 227-29, doi:10.1007/s11213-009-9126-z.
15. 见注释 10 中 GmÜr, Bartelt, and Kissling “组织之系统观”文，第 1630 页。
16. 见注释 1，第 22-23 页；另参看注释 10 中 GmÜr, Bartelt, and Kissling “组织之系统观”文，第 1630 页；另参看注释 14，第 228-29 页。
17. 见注释 12 中 Burnett and Durant-Law “应用 RAAAKERS 框架分析”文，第 24-25 页；另参看注释 14，第 229 页；另参看注释 10 中 Rios “组织控制论模型”文，第 1532 页。
18. 见注释 1，第 34 页。
19. 见注释 10 中 Rios “组织控制论模型”文，第 1534 页；另参看注释 10 中 Schwaninger “可行组织设计”文，第 955-66 页。
20. 见注释 3，第 3-5 页。
21. 见注释 5 中 Readiness Management Group “战备管理部单兵后备役指南”文，第 8-9 页。
22. 见注释 5 中 Readiness Management Group “战备管理部单兵后备役指南”文，第 8-9 页；另参看注释 3，第 5-6 页。
23. 见注释 4；另参看注释 5 中 Readiness Management Group “战备管理部单兵后备役指南”文，第 7-12 页。
24. 见注释 4，第 1.16 节。
25. 见注释 5 中 Readiness Management Group “战备管理部单兵后备役指南”文，第 7 页。
26. Maj A. R. Rutkowski, executive officer, Ogden Air Logistics Center 电子邮件 , 29 June 2011.
27. 见注释 5 中 Readiness Management Group “战备管理部单兵后备役指南”文，第 13-14 页。
28. AFI 36-2254, Reserve Personnel Participation, [AFI 36-2254：后备役队员参与], vol. 1, 26 May 2010, 34, http://www.e-publishing.af.mil/shared/media/epubs/AFI%2036-2254V1.pdf.
29. 见注释 5 中 Readiness Management Group “战备管理部单兵后备役指南”文，第 7 页。
30. 见注释 5 中 “AFI 38-201：人力资源需求与授权管理”，第 22 页。
31. 见注释 5 中 “AFI 38-201：人力资源需求与授权管理”，第 20 页，第 4.4.4.1.1 节。
32. Office of the Vice Chairman of the Joint Chiefs of Staff and Office of the Assistant Secretary of Defense for Reserve Affairs, Comprehensive Review of the Future Role of the Reserve Component, [后备役部队未来作用的全面审查报告], vol. 1, Executive Summary and Main Report, (Washington, DC: Department of Defense, 5 April 2011), 35-41, http://ra.defense.gov/documents/publications/Comprehensive%20Reserve%20Review%20(5Apr11)%20Ver26h%20-%20Final.pdf.
33. 见注释 1，第 28 页。

34. 见注释 32。

35. 见注释 3，第 1-6 页。

36. 见注释 28；另参看 Department of Defense Instruction 1235.11, Management of Individual Mobilization Augmentees (IMAs) [单兵动员增补现役管理], 24 May 2007, http://www.dtic.mil/whs/directives/corres/pdf/123511p.pdf.

罗萍・G・斯尼德，美国空军后备役上校（Col Robin G. Sneed, USAFR），美国空军军官学院毕业，菲尼克斯大学工商管理硕士，现为单兵动员增补现役（IMA）后备役队员，分配到尤他州希尔空军基地奥格丹空军后勤中心空天补给部，在该部主任指挥下，支持 A-10、F-16 等旧型飞机的维护、太空与指挥、控制、通信和情报系统，以及空军弹药储备。在她作为单兵动员增补现役后备役队员的 22 年经历中，曾担任第 84 作战补给联队工程主任、空天维护改造中心规划与项目副主任，及空军科研办公室科研主管等职。斯尼德上校的文职专业是管理医疗器械的临床应用研究。



罗伯特・A・基尔默，美国陆军退役中校 / 博士（Lt Col Robert A. Kilmer, PhD, USA, Retired），印第安纳大学理学士，海军研究生院理科硕士，匹兹堡大学博士，现为弥赛亚学院工商信息系统与管理副教授，及瓦尔登大学管理学院博士班导师。基尔默博士在美国陆军服役 22 年之后，现致力于与优秀学生和教员共同探索现实世界困难问题的长期解决方案。基尔默博士曾在西点军校教授系统工程，并在宾州卡莱尔美国陆军战争学院教授人工智能。基尔默博士的研究领域包括运营管理、信息系统、人工智能及非营利组织。

载人航天国际五种合作模式与中国的战略选择

Five Patterns of International Cooperation in Manned Space Exploration and China's Strategic Choice

蒋翊民，博士候选人，北京大学（Jiang Yimin, PhD Candidate, Beijing University）
余万里博士 / 副教授，北京大学（Dr. Yu Wanli, Associate Professor, Beijing University）

在当今载人航天领域，国际合作方兴未艾，是世界各主要国家提升载人航天经济收益、分担载人航天风险，推动载人航天事业快速发展的重要途径之一。本文回顾了自人类开启载人航天事业以来国际合作的重要案例，归纳总结出载人航天国际合作的五种模式，并在具体分析不同模式的特点的基础上，为中国载人航天国际合作的模式选择提出建议。

载人航天国际合作的五种模式

人类在航天领域进行国际合作的历史可以追溯到二十世纪五十年代。起初，受东西方冷战的制约，航天国际合作主要发生在美苏两大阵营内部，合作水平较低，合作领域也局限于无人飞行。二十世纪七十年代起，东西方关系逐步缓和，美苏两国在航天领域开始尝试有限合作，合作领域也从无人飞行扩展到载人联合飞行。[1] 冷战结束之后，载人航天国际合作更加活跃，合作水平更高，范围更广，方式也趋于多样化，具体而言可以归纳为“合伙企业”、“资产共享”、“以货易货”、“超级市场”以及“培训学校”五种模式。

“合伙企业”模式：合伙企业是一个经济概念，指两人以及两人以上按照协议投资，共同经营，共负盈亏的营利性组织。合伙企业具有财产共有，责任连带等特点。顾名思义，在载人航天领域，以“合伙企业”模式开展的国际合作主要指参与合作的各方，多是具有一定航天技术的国家，通过联合投资、明确分工，共同完成载人航天工程。当前世界上规模最大、水平最高的载人航天合作项目——国际空间站——就是“合伙企业”模式的典型案例。

“资产共享”模式：载人航天器等空间设施是一个国家重要的战略资产。由于载人航天工程“高投资、高风险”的特征，世界绝大多数国家无力全面发展载人航天系统，宇宙飞船、空间站等载人航天器成为各国开展载人航天活动的“稀缺资源”。“资产共享”模式主要指国家通过“相互利用空间设施”的方式进行合作。历史上，各国已经采用“资产共享”模式进行了多次合作。1988 年，苏联同法国签署载人航天合作协议，规定法国向苏联“联盟号”空间站派驻宇航员进行太空活动。[2] 1993 年，美俄签署协议，由俄罗斯向美国提供“TM 号”宇宙飞船，作为美国“自由”号空间站的救援飞船。[3] 特别值得注意的是，近年来民营公司在载人航天领域异军突起，美国航天局于 2011 年就曾租用 Space X 公司拥有的“龙飞船”向国际空间站运送物资。[4]

“以货易货”模式：外太空是进行科学实验的理想场所，载人航天活动的重要组成部分就是通过太空科研活动获取科技以及应用成果。在载人航天国际合作中，所谓“以货易货”模式，就是各主要航天强国根据取长补短，互惠互利的原则，通过交换太空技术以及应用成果的方式进行合作。当前，各主要航天强国在载人航天科技以及太空应用方面各有所长，比较优势明显，“以货易货”模式具有一定的可行性。历史上，各国采用该模式进行了一些合作尝试，例如冷战时期，苏联与澳大利亚就曾达成协议，交换外空科研数据并进行人员交流。[5]

“超级市场”模式：超级市场是以顾客自选方式经营的大型综合性零售商场，又称自选商场。超级市场的主要特点是商品种类齐全，消费者根据需要自行选择。载人航天活动的成果涵盖从基础科学到应用科学等多个领域，数量多，价值大，恰似商品玲琅满目的“超级市场”。由于目前世界上仅有少数国家具备独立实施载人航天工程的能力，因此客观上形成了少数国家垄断载人航天科技成果的局面。大部分尚未具备独立航天能力，但对太空科技成果有需求的国家只能根据自身需求，同航天强国进行合作，从强国的航天成果“超级市场”寻求引进相关技术产品。这种客观存在的供给和需求决定了“超级市场”模式在未来具有相当大的发展空间。

“培训学校”模式：众所周知，学校是有计划、有组织的提供系统教育的机构。纵观人类发展载人航天科技的历史，任何有计划发展载人航天事业的国家都必须吸收先进国家的技术与经验。推而广之，载人航天领域的培训学校主要是先进航天国家在国际协议允许的范围内为其他国家传授航天技术和培训航天员。冷战时期，苏联的加加林航天中心曾经为捷克斯洛伐克、波兰以及东德的宇航员提供培训。[6] 在冷战结束之后，俄罗斯为提高载人航天活动的经济效益，也先后培训了韩国、中国等国家的宇航员。

显而易见，载人航天国际合作的五种模式各有特点。不同合作模式的准入门槛各异，合作方式有别。在载人航天国际合作的五种模式中，“合伙企业”以及“以货易货”两种模式要求参与合作的国家具备一定的载人航天科技水平，拥有一定规模的太空设施，可以独立承担分工并有能力获取可供交换的太空科研成果。而针对尚未具备独立载人航天能力的国家，国际合作往往或是通过“资产共享”模式“借用”或者“租用”先进国家的空间设施，或是通过“超级市场”模式购买先进成果，或是通过“培训学校”模式吸收先进经验。

除此之外，五种载人航天国际合作模式的运作方式不同，风险与收益也有差别。“合伙企业”模式主要通过合作方分工协作，而其他模式下的国际合作则主要通过参与方之间的交换交易来进行。采用“合伙企业”模式进行的国际合作，往往是大型或者特大型载人航天项目，投资规模大，周期长，流程复杂，容易受到诸如合作参与方经济情况、政治关系乃至项目内部协调等因素的影响。相对于“合伙企业”模式而言，其他四种合作模式主要是通过交换以及交易实现合作，投资规模有限，周期较短，因此抵御经济风险的能力较强。

值得注意的是，载人航天国际合作不论采取何种模式，都会不同程度地受到国际政治因素的影响。而且，由于大部分载人航天国际合作均涉及到敏感技术交流乃至技术转让，因此也都不同程度地存在法律、信息和

国家安全风险。载人航天工程具有政治经济安全等战略价值，是当今世界各主要国家竞相争夺的制高点之一。当今世界的载人航天工程绝大多数是由政府投资，国有机构或企业运作，具有浓厚政治背景。这就决定了载人航天国际合作大多发生在政治关系稳定密切的国家之间，合作的成败很大程度上取决于国家间政治关系的走向。以美苏载人航天合作为例，冷战时期，美苏关系波动频繁，导致两国在载人航天领域的合作同样起伏不定。只有在苏联解体以及东西方关系缓和之后，美俄两国的合作才得以逐步深化。

中国进行载人航天合作的战略目标

中国是世界上第三个具备独立载人航天能力的大国，有能力同世界各国开展不同水平、不同层次的国际合作。2012 年 6 月，中国“神舟九号”成功完成与“天宫一号”空间站手动交会对接、自动交会对接等任务，标志着中国载人航天工程再度迈上新台阶。[7] 在随后的新闻发布会上，中国载人航天工程办公室主任王兆耀强调“中国将在坚持独立自主、自力更生的基础上，本着相互尊重、平等互利、透明开放的原则，积极与世界有关国家和地区开展载人航天领域的合作，共同推动世界航天技术的进步和发展。”[8]

与此同时，中国也认识到同美俄相比，中国载人航天工程科技水平尚处在较低水平，航天产业资源转化能力、市场化能力和产业技术能力不强，削弱了中国航天的总体竞争力。[9] 随着中国载人航天“三步走”战略的逐步推进，中国载人航天事业也面临着投资风险加大、技术攻关难度提升等问题。为此，中国载人航天办公室主任王兆耀曾表示，中国希望未来在“技术合作”、“太空应用”、“航天成果”以及“航天员培养和联合飞行”等方面重点开展国际合作。

具体而言，在航天科技方面，尽管随着“天宫一号”空间站的成功发射以及“神舟九号”飞船圆满完成任务，中国已经掌握了载人飞行、交会对接等载人航天关键技术，但在新一代运载火箭研制、空间基础设施建设、太空行走，以及航天科技体系建设方面仍然同美俄等国存在巨大差距。目前，中国正处在从运营短期空间站到建立长期空间站的关键时期，在火箭发动机等关键技术方面也有待更进一步突破，在对地观测、航天医学、材料加工、生物技术、天体物理以及太空环境等多个领域也有继续发展的空间，因此，中国需要通过开展国际合作，借鉴美俄等先进国家的载人航天领域的经验，促进本国载人航天工程发展。

在载人航天工程投入方面，中国在载人航天工程领域投入同美俄等国家相比仍然有限。根据美国国家科学院在 2009 发布的报告显示，当前世界上各国开展载人航天国际合作的主要动因之一就是分担投资与风险，提升航天活动的经济收益。[10] 目前，中国载人航天事业仍然主要以国家投入为主，按照国家指导下的商业化模式运行。[11] 根据中国载人航天办公室新闻发言人武平披露：自 1992 年启动载人航天工程起，中国在该领域已经投资接近 400 亿元人民币。[12] 尽管这一投资规模远远低于美国和前苏联，在世界范围内也属于较低水平，但已经引起了中国国内关于载人航天投入是否值得的激烈讨论。有观点认为载人航天的巨额投资挤占了原本应该流向航天其他领域的投资，导致了航天事业发展不均衡，应用卫星发展停滞。更有观点认为载人航天领域的投资挤占了民生投资。[13] 正如中国空间技术研究院一位工作人

员表示：中国载人航天工程面临的一个重要问题就是载人航天的许多技术突破如何尽快转化为生产力，实现对技术的牵引和对国民经济的带动作用。同时，资金渠道单一、管理体制条块分割等问题仍然制约着中国航天事业的进一步发展。[14] 因此，中国有必要通过开展国际合作，多元化资源来源渠道，提升载人航天活动的经济效益。

载人航天工程是国家强国战略的重要组成部分，不仅具有科技和经济价值，更具有政治和战略意义。冷战时期，美苏两国推动载人航天工程，开展国际合作的背后都存在深层次的战略考虑。两国在载人航天领域展开激烈竞争的同时，还以载人航天工程为平台，广泛开展同欧洲国家以及第三世界国家的合作，争相提升国际影响力。[15] 近年来，中国在载人航天领域的突破性进展既令全球瞩目，也引起了部分国家的猜疑。[16] 因此，中国应当以开放的姿态主动推进国际合作，提升中国的国际影响力，树立负责任大国的国际形象。

中国进行载人航天国际合作的模式选择

载人航天国际合作的五种模式为中国开展国际合作提供了多种备选方案。由于不同合作模式适用于载人航天的不同领域，准入门槛不同，收益和风险也有所差异，因此中国选择何种模式开展载人航天合作，需要综合权衡合作目标与自身情况，在合理评估收益与风险的基础上做出选择。

“合伙企业”模式：要求参与合作的各方具备较高的载人航天技术，并在一些领域具有比较优势，可以独立承担大型载人航天项目的分工。采用“合伙企业”模式进行的国际合作，一般是类似于国际空间站的尖端大型项目。中国采取该模式开展国际合作，可以加强与他国交流合作，吸收他国的先进科技，同时也有利于以开放的姿态，化解国际社会部分国家对中国发展载人航天工程的无端质疑，有助于塑造中国在国际社会上负责任的大国形象。

在风险方面，“合伙企业”模式要求合作参与方具有一定的资金保障与经济基础。由于合作项目往往具有投资规模大，运行周期长的特点，因此抵御经济风险的能力相对脆弱，参与合作的任何国家一旦因为经济原因无法确保投资，将导致整个工程陷入停滞。在合作过程中，由于涉及到载人航天尖端科技的交流，因此容易出现法律纠纷以及泄密风险。与此同时，载人航天工程具有浓厚的

中国开展载人航天国际合作收益风险分析

	合伙企业	资产共享	以货易货	超级市场	培训学校
技术收益	高	中	高	中	低
经济收益	高	高	低	高	高
政治收益	高	高	中	中	高
投资风险	高	低	低	低	低
技术风险	高	中	低	低	低
政治风险	高	高	中	中	中
法律风险	高	中	高	高	高
信息安全风险	高	高	中	中	高

政治色彩。国家间能否进行高水平的载人航天合作，很大程度上取决于国家间政治关系是否稳定，战略互信是否建立。当前，正是由于中美战略互信缺失，美国质疑中国发展载人航天工程的意图，阻碍中国参与国际空间站等大型合作项目。[17]

“资产共享”模式：一国从事太空活动的设备是该国重要的战略资产。中国在“天宫一号”成功发射之后，已经拥有运营短期空间站的能力，通过共享空间资产的方式开展国际合作的条件开始成熟。采用“资产共享”模式参与国际合作，既可以获得可观的经济收益，也有利于实现学习他国先进科技以及经验的战略目标，提升同合作方的双边关系。但该模式进行的国际合作可能涉及到诸如不同航天器交会对接等“高难度动作”，因此有较高的技术风险。同时，该模式涉及到载人航天器等核心航天科技的交流，因此需要明确的协议框架防范法律风险，以及严格的制度防范信息安全风险。目前，中国已经尝试以“资产共享”模式开展国际合作，中国的“神八”飞船上就搭载了德国的 SIMBOX 科研项目。[18]

“以货易货”模式：太空是进行科学实验的理想场所。载人航天活动的重要内容之一就是利用太空的特殊环境进行科学实验，获取在地球正常状态下难以取得的成果。据统计，中国自启动载人航天工程以来，已经通过载人航天活动取得了上千项科研成果，[19]具备了开展“以货易货”的条件。中国同其他国家交换太空科研活动的成果，可以取长补短，优势互补。由于这一模式主要通过科研成果的交换来实施，相比合伙企业和资产共享模式而言，合作方式简单，不涉及到联合投资与技术协作等高风险环节。该模式合作周期通常较短，因此可以抵御经济动荡以及国际关系波动等外部影响。但鉴于这一模式涉及到高水平技术成果交流以及交换，因此在合作中需要特别注意相关国际机制，避免触犯国际规则，严格防范泄密等信息安全风险。

“超级市场”模式：当前，在载人航天科研成果的“超级市场”中，中国既是“供货商”，也是“消费者”。中国载人航天工程已经启动数十年，积累了大量的太空科研成果，部分成果可以向他国出售或转让以获取经济利益。同时，出于推动航天事业快速发展的考虑，中国也有引进其他国家的先进科研成果的需求。中国作为“供货商”参与合作，既有利于提高载人航天活动的经济收益，也有利于树立中国负责任的大国形象。在风险方面，由于该模式不涉及到投资，技术协作等环节，仅涉及到科技成果的转让，因此合作方式简单，合作周期较短，投资风险和技术风险较低；在该模式中，中国作为“供货商”可以在一定程度上控制政治风险；若作为“消费者”，则需要充分评估国际关系波动对合作的影响，审慎进行合作。

“培训学校”模式：航天工程高度复杂，不仅需要大规模的资源投入，也需要先进国家的经验指导。特别是载人航天工程，由于直接涉及航天员的人身安全和身体健康，因此更需要先进国家运营经验的支持。长期以来，美俄是世界上仅有的具备独立载人航天能力的国家，因此也是国际社会仅有的载人航天系统培训的提供者。目前，中国成为了继美俄之后第三个拥有独立自主载人航天能力的国家，初步具备了提供载人航天培训的能力。[20] 中国开展宇航员培训等方面的国际合作，一方面可以获取合理的经济回报，另一方面也有助于提升与合作方的双边关系，扩大国际影响力。在风险方面，尽管国际上

相关经验已经较为成熟，形成了一系列完善的规章制度预防风险，但在合作过程中，仍要特别重视信息安全工作。[21]

结论和建议

综上所述，中国开展载人航天领域的国际合作，有多方面的必要性，包括吸收国际先进经验与科技，促进本国载人航天工程的跨越性发展；分散投资风险，提升载人航天工程的经济效益；提升国际影响力，塑造中国负责任大国的国际形象，与世界各国共同推动航天事业，为推动人类向太空发展做出中国的贡献。由于载人航天国际合作的五种模式各具特点，因此中国载人航天应当在确定国际合作战略目标主次的基础上，综合考虑国家间关系等国际因素以及目标合作方特点等国别因素，衡量收益与风险，在此基础上具体选择载人航天国际合作的模式。

从短期看，由于目前世界尚处在后金融危机时代的调整期，国际格局与大国关系还处在调整与重组的进程当中，因此，中国开展载人航天国际合作，应当慎重选择具有一定风险的“合伙企业”模式，重点开展风险较小、具有一定经济效益以及国际影响力的国际合作。对于美俄等航天强国，可以择机以“资产共享”以及“以货易货”模式开展合作，一方面实现互利共赢，另一方面也有助于消除猜疑，增进互信，夯实未来进一步合作的基础。而针对广大发展中国家，则可采取“超级市场”以及“培训学校”模式，进行成果转让以及科技援助，提高载人航天活动的经济效益，塑造“负责任大国”的国际形象。

从中长期看，在国际局势、特别是大国间关系相对稳定的前提下，中国可以尝试通过“合伙企业”模式，同其他航天强国合作共建大型载人航天项目。与此同时，中国仍应当重点推动同广大发展中国家的载人航天合作，一方面发挥载人航天工程的政治效应，另一方面提升载人航天活动的经济效益；既确保中国载人航天事业可持续发展，也有助于推动整个人类的航天事业。而在可预见未来，随着信息科学技术以及人工智能技术的发展，无人航天的优势将逐步显现，作为载人航天的重要补充将更趋成熟，也将为国家间进行航天合作开辟新的路径，进一步推动整个人类的航天事业达到一个全新高度。♣

注释:

1. 王金华，载人航天国际合作的历史和现实，国际太空，1996 年第 4 期。
2. 张希舜编译，法苏新的空间合作，中国航天，1987 年第 5 期。
3. 秦德岐、白雪编译，美国俄罗斯空间合作协议，国际太空，1992 年第 9 期。
4. “美国‘龙飞船’平安返回地球”，搜狐新闻，2012 年 6 月 1 日，http://news.sohu.com/20120601/n344601196.shtml。
5. 安晓力，澳苏签订空间科学协定，国际科技交流，1988 年第 7 期。
6. 王金华，载人航天国际合作的历史和现实，国际太空，1996 年第 4 期。
7. 中国载人航天工程网，神舟九号专题，http://www.cmse.gov.cn/Shenzhou9/。
8. “中国积极与世界有关国家和地区开展载人航天领域国际合作”，新华网，2012 年 6 月 29 日，http://www.gov.cn/wszb/zhibo520/content_2173153.htm。
9. 李斌，载人航天后的冷思考—我们离航天强国还有多远，中国网，2003 年 10 月 22 日，http://www.china.com.cn/chinese/zhuanti/426863.htm。

10. James V. Zimmerman, Rapporteur: Approaches to Future Space Cooperation and Competition in a Globalizing World: Summary of a Workshop [在全球化环境下开展太空合作与竞争的方式：研讨会总结], 2009, http://www.nap.edu/catalog/12694.html.

11. “载人航天：仰望星空与脚踏实地”，中国网，2012 年 6 月 29 日，http://www.china.com.cn/opinion/2012-06/29/content_25768543.htm。

12. 武平，中国载人航天工程共计花费 390 亿元，人民网，2012 年 6 月 25 日，http://www.people.com.cn/h/2012/0625/c25408-1373359637.html。

13. 中国国内就载人航天工程的讨论参看：“载人航天工程究竟值不值？”，新华网，2012 年 7 月 5 日，http://news.sina.com.cn/pl/2012-07-05/141024718026.shtml；另参看：“中国创新需要复制航天体制”，21 世纪经济报道，2012 年 6 月 19 日，http://money.163.com/12/0619/02/84B2HJ6C00253B0H.html。

14. 见注释 9。

15. 王金华，载人航天国际合作的历史和现实，国际太空，1996 年第 4 期。

16. “外媒猜测中国载人航天军事用途，国防部回应”，国际在线，2012 年 6 月 28 日，http://news.qq.com/a/20120628/001526.htm。

17. Can China Enter International Space Station Family? [中国能否加入国际空间站大家庭], Universetoday.com, 10 January, 2011. http://www.universetoday.com/82368/can-china-enter-the-international-space-family/.

18. “中德牵手‘神八’空间生命科学实验”，人民网，2011 年 11 月 2 日，http://scitech.people.com.cn/h/2011/1102/c227887-1596652330.html。

19. “辉煌成就耀太空——中国载人航天工程 16 年回顾”，新华网，2008 年 11 月 6 日，http://news.xinhuanet.com/newscenter/2008-11/06/content_10318363_1.htm。

20. “探访中国航天员训练中心：在地面体验神六飞行”，中国网，2005 年 10 月 21 日，http://www.china.com.cn/chinese/zhuanti/aytk/1006049.htm。

21. 韩国宇航员高山在俄罗斯受训期间因意图窃取俄方情报而遭驱逐，参看：“韩宇航员涉嫌窃密被换、俄航天城常抓到‘间谍’”，新华网，2008 年 3 月 25 日，http://news.xinhuanet.com/world/2008-03/25/content_7856741.htm。

蒋翊民（Jiang Yimin, PhD Candidate），北京大学国际关系学院外交学在读博士生，北京大学国际关系学院外交学学士，国家发展研究院经济学学士，国际关系学院外交学硕士，加拿大麦吉尔大学(McGill University)索维学者(Sauvé Scholar 2011 ～ 2012)，主要研究领域与兴趣为美国对外政策与中美关系。

余万里（Dr. Yu Wanli, Associate Professor），国际政治学博士，北京大学国际关系学院副教授，北京大学国际战略研究中心学术委员，教育部中美人文交流研究基地执行副主任。从事美国问题、中美关系、中国外交研究和教学，发表有《美国政治风向标：2008 年美国大选现场观察》、《美国在东亚的作用：观点、政策及影响》、《改革开放三十年的中国外交》、《冷战后的美国外交》、《中美关系史 1949 — 1972》、《意识形态与美国外交政策》、《国际关系理论史导论》等著译作，学术论文与研究报告数十篇。

本期词汇

本刊选登词汇多来自当期或近期美军文章，但在主流英汉军事词典中未能找到相应词条或贴切译文。一家之“译”，仅供参考。

- all-source intelligence = 全源情报（包括来自人力 / 天空 / 太空 / 网空 / 跨部门等各种来源的情报）
- anticipatory self-defense = 先行自卫
- attribution =（网空战中的）攻击源判定，溯源
- coalition operation = 联盟作战（指多国部队联合作战，注意与 joint operation 即同国多军种联合作战相区别）
- contested sky = 危险天空，凶险天空，对抗天空，布防天空
- distinction and proportionality =（战争法中的）区分原则和相称原则
- double digit SAMs = 俄制先进移动式地空导弹（北约将俄 / 中制造的移动式地空导弹标以两位数字，例如 S-300P 被标为 SA-10。）
- EW/EA (electronic warfare and electronic attack) = 电子战 / 电子攻击（美国国防部军语辞典将后者即电子攻击解释为前者即电子战的一个类别），电子作战，电子对抗
- flash on and off =（雷达和电子战系统等发射体）闪开闪闭（以在保持通信的同时尽量避免暴露）
- fused intelligence = 融合情报（对全源情报进行筛选分析归纳而形成完整准确的情报）
- info-tecture = 信息架构
- ISR enterprise = 情监侦界，情监侦体系，情监侦部队，情监侦能力
- low observability = 低显性
- low observable material = 低显材料，亚隐身材料
- near space = 介空（介于天空和太空之间的、由平流层、中间层和热层组成的空间。目前多直译为“邻近空间、近空间、近地空间、近太空、近外空”等）
- PED (processing, exploitation, and dissemination) = 情报信息处理 / 归纳 / 分发
- permissive environment = 准入作战环境（和 anti-access 即阻入作战环境相对）
- radar signature =（飞行器的）显迹性，雷达印迹
- requirements =（项目论证、采办、作战策划中开列的）需求（而非“要求”）
- RPA (remote piloted aircraft) = 遥驾飞机（美国空军规定使用此术语，其中突出动词“驾”字，意含无人机操作员也是飞行员。其他军种继续习惯使用 UAV [unmanned aerial vehicle]。）
- sensor-agnostic / device-agnostic = 传感器通用（指所有品牌的传感器都可接入使用）
- subunified command = 二级统辖司令部（2010 年成立的 US Cyber Command 就是这样的司令部，由国防部下诸军种集成的战略司令部统辖。建议不要将 unified command 译成“联合司令部”，免与 joint command 混淆。）
- tactics, techniques, and procedures = 战术 / 战技 / 战规
- targeted killing = 定点打击，针对性杀伤
- targeting =（作战策划阶段的）攻击目标选定
- versatility = 普用性，普适性
- weaponeering =（作战策划阶段的）武器选定